FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Zadání diplomové práce

Název:	Nástroj pro realizaci phishingové kampaně
Student:	Bc. Tomáš Arazim
Vedoucí:	Ing. Tomáš Luňák
Studijní program:	Informatika
Obor / specializace:	Počítačová bezpečnost
Katedra:	Katedra informační bezpečnosti
Platnost zadání:	do konce letního semestru 2024/2025

Pokyny pro vypracování

V současné době se v sektoru bezpečnosti používá mnoho různých softwarových řešení pro realizaci phisingových kampaní. Diplomová práce bude rozdělena na analytickou a technicko-realizační část.
V analytické části student provede průzkum existujících phisingových nástrojů, detailní porovnání vlastností různých open source řešení, základní porovnání vlastností komerčních řešení v kontrastu s open source produkty a vybere vhodné open source řešení na základě jeho vlastností.
V technicko-realizační části student provede instalaci vybraného řešení. Dále student zprovozní a integruje řešení na další dostupné prostředky (active directory, mail server a další). V případě potřeby provede úpravu či dopsání modulů do vybraného řešení a provede reálnou phishingovou kampaň s jejím vyhodnocením.

Elektronicky schválil/a prof. Ing. Róbert Lórencz, CSc. dne 30. října 2023 v Praze.

Diplomová práce

NÁSTROJ PRO IMPLEMENTACI PHISIHNGOVÉ KAMPANĚ

Bc. Tomáš Arazim

Fakulta informačních technologií
Katedra informační bezpečnosti
Vedoucí: Ing. Tomáš Luňák
6. května 2024

Obsah

Seznam obrázků

Seznam tabulek

Seznam výpisů kódu

Chtěl bych poděkovat především svému vedoucímu práce Ing. Tomáši Luňákovi za vedení práce, zpětnou vazbu při jejím psaní, konzultace a všechen čas. Dále bych rád poděkoval svým rodičům za psychickou podporu. Také bych rád poděkoval svým přátelům za odreagování v chvílích nestrávených na této práci.

Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval samostatně a že jsem uvedl veškeré použité informační zdroje v souladu s Metodickým pokynem o dodržování etických principů při přípravě vysokoškolských závěrečných prací.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona, ve znění pozdějších předpisů. V souladu s ust. § 2373 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů, tímto uděluji nevýhradní oprávnění (licenci) k užití této mojí práce, a to včetně všech počítačových programů, jež jsou její součástí či přílohou a veškeré jejich dokumentace (dále souhrnně jen „Dílo“), a to všem osobám, které si přejí Dílo užít. Tyto osoby jsou oprávněny Dílo užít jakýmkoli způsobem, který nesnižuje hodnotu Díla a za jakýmkoli účelem (včetně užití k výdělečným účelům). Toto oprávnění je časově, teritoriálně i množstevně neomezené.

V Rovném dne 1. ledna 2024

Abstrakt

Práce se zabývá zkoumáním open-source nástrojů pro simulaci phishingových kampaní. Cílem bylo poskytnout hodnotící kritéria, přehled vlastností a hodnocení open-source programů na základě užitečnosti. Ze zhodnocených nástrojů byl vybrán nejlépe hodnocený a použit k realizaci dvou phishingových simulací. Práce by měla pomoci organizacím při výběru řešení, jeho implementaci a při následné realizaci vlastních simulací.

Klíčová slova phishing, opensource, open source, open-source, nástroje, open-source nástroje, praxe, phishingová kampaň

Abstract

The focus of this thesis is the examination of open-source tools for simulating phishing campaings. The goal was to was to provide evaluation criteria, feature overview and the actual evaluation of open-source programs based on usefulness. From the tools evaluated, the best was picked and used for realisation of two phishing simulations. This work should help organisations with choice of solution, its deployment and the realisation of their own simulations.

Keywords phishing, opensource, open source, open-source, tools, open-source tools, field work, phishing campaign

Seznam zkratek

AI	Artificial Intelligence
AD	Active Directory
BEC	Bussiness Email Compromise
BeEF	The Browser Exploitation Framework
CFO	Chief Financial Officer
CN	Common Name
CSV	Comma-Separated Values
DBIR	Data Breach Investigations Report
DKIM	DomainKeys Identified Mail
DN	Domain Name
ENISA	The European Union Agency for Cybersecurity
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IMAP	Internet Message Access Protocol
JSON	JavaScript Object Notation
LDAP	Lightweight Directory Access Protocol
NIST	National Institute of Standards and Technology
NÚKIB	Národní Úřad pro Kybernetickou a Informační Bezpečnost
OSINT	Open Source Intelligence
PDF	Portable Document Format
PHP	Hypertext Preprocessor
QoL	Quality of Life
SaaS	Software as a Service
SMB	Server Message Block
SPF	Sender Policy Framework
SSH	Secure Shell
TLS	Transport Layer Security
XLS	Office Open XML
XML	Extensible Markup Language

Úvod

S elektronickou komunikací se denně setkává velká část dnešní společnosti. V této komunikaci se skoro od samého počátku vyskytují nebezpeční aktéři, kteří chtějí této komunikace zneužít ke svému prospěchu. K tomu využívají všemožných metod, ale hlavně proti svým cílům využívají lidské podstaty. Oklamat člověka je mnohdy jednoduší nežli útočit na zabezpečený informační systém. Na každý podnět těchto protivníků většinou přichází odpověď, což ale znamená, že podvodníci vždy vymýšlí nové nebo sofistikovanější metody.

Útočníci buď již mají nebo budou mít k dispozici technologie, s jejichž pomocí mohou generovat pro člověka smysly nedetekovatelná falza (obrázky, zvukové stopy, videa). Jediný způsob jakým se proti nim bránit je nasadit zdravého rozumu, držet se motta důvěřuj, ale prověřuj a v poslední řadě vzdělávat se na téma existujících hrozeb.

Jako předmět má tato práce obranu proti jedné z nejčastějších forem tzv. sociálního inženýrství - phishingu. Jednou z možných obran je provádění obranných (či simulovaných) kampaní, které zvýšují odolnost za pomocí tréninku. Nejčastěji se trénink provádí pomocí komerčního software nebo skrze objednání služby, to ale může být peněžně nákladnější. Existují ale i open-source řešení, které peněžní náklady nevyžadují. Nicméně orientace ve velkém počtu různých programů má pro změnu náklady časové.

Cílem této práce je proto zhodnotit open-source nástroje pro tvorbu obranných phishingových kampaní. Toto zhodnocení by mělo samostatným subjektům posloužit k výběru vhodného řešení, pomoci s jeho implementací, včetně provedení samotné phishingové kampaně. Součástí práce je i stručné porovnání open-source variant s komerčním software.

Práci jsem si vybral jelikož jsem již v minulosti prováděl simulovanou phishingovou kampaň. V té době jsem této tématice rozumněl pouze napovrchu a využíval poměrně primitivních metod. Při této práci jsem své znalosti chtěl prohloubit.

Kapitola 1
Teoretická část

1.1 Sociální inženýrství

Sociální inženýrství se dá popsat různě, v sociálním kontextu o něm lze uvažovat jako *akt, který přiměje druhou osobu udělat takovou akci, která může, ale nemusí být nutně v jejím nejlepším zájmu* [1]. Všeobecně se jedná o vhodnou definici, která zahrnuje celý obor, jelikož v společenských situacích se nacházíme denně. Sociální inženýr dokáže využít svých znalostí a psychologických technik (v podstatě manipulaci), k dosažení svého cíle.

Tyto techniky a znalosti nemusí být vždy problémové. Protože denně existují případy, především v zaměstnání, kdy odpovědná osoba má určitý náhled na problém. Tento pohled bývá mnohdy zcela rozdílný od pohledu technika, nebo obecně specialisty. Kde specialista vidí problém, který eventuálně přeroste v katastrofu, odpovědná osoba může vidět zpomalení vývoje, snížení efektivity, produktivity pro malý zisk (z pohledu odpovědné osoby), atd. Specialista pak má dvě možnosti, buď bude problém ignorovat do doby, než skutečně nabude na závažnosti, kdy ho už ignorovat nelze. Tato situace je o to horší, že takový problém dokáže způsobit pro daný podnik větší ztrátu, než kdyby se řešil okamžitě. Proto jako alternativní krok může specialista nasadit sociálního inženýrství, s pomocí kterého přivede odpovědnou osobu k činu, který pak povede k vyřešení problému včas. Dojde tedy k výhře pro obě strany, přestože odpovědná osoba plně nespolupracuje.

Bohužel sociální inženýrství není vždy využito k benefitu obou stran. Využívají jej především aktéři, jež z pohledu informační bezpečnosti nazýváme útočníky. V tomto ohledu je sociální inženýrství brané jako použití sociální zástěrky, kulturních triků a už zmíněných psychologických triků, za účelem získání asistence zaměstnance cílové společnosti k vniknutí do počítačového systému či sítě [2].

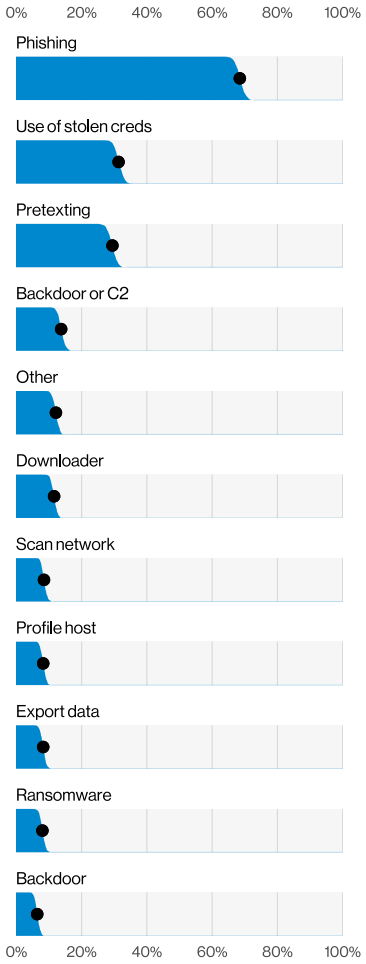
ENISA specifikuje následující čtyři časté techniky [3]:

- Pretexting - útočník si vytvoří nějakou záminku kvůli které je nutná vykonat specifická akce, za účelem získání důvěry.
- Baiting - útočník využívá faktu, že cíl bude chtít vykonat určitý úkon, jelikož tím oběť získá jednoduchý přístup k něčemu po čem touží.
- Quid pro quo - útočník se zkouší vyměnit informaci pomocí nějaké kompenzace.
- Tailgaiting - neautorizovaná osoba následuje cíl, za účelem získání přístupu do veřejnosti omezených oblastí nebo systémů.

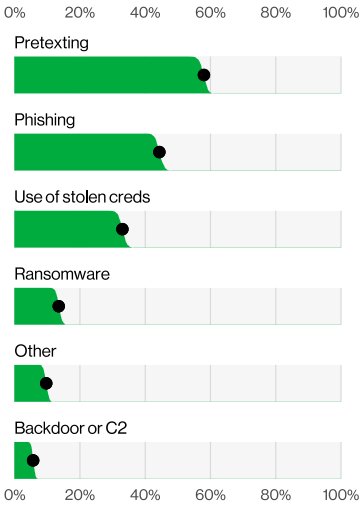
Kromě zmíněných způsobů se v sociálním inženýrství spoléhá na dostupné informace, či metadata. Každý kus komunikace se počítá. Ty pak sociální inženýr úspěšně využívá k cílenějšímu

kontaktu. [4]

Sociální inženýrství je stále masivně populární, podle Verizon DBIR v roce 2022 zahrnovalo 82% odhalených průniků lidský faktor. Z toho ~68% zahrnoval phishing, pretexting až 27%. Pretexting má v tomto kontextu souvislost s tzv. BEC, jedná se většinou o více propracované podvody. [5] Rok 2023 polepšil na lidském elementu, ale pořád odhalených útoků s lidským faktorem bylo nemalých 74%. Phishing propadl na 44%, s mnohem větším podílem pretextingu, to ~58%. [6] Porovnání lze vidět na obrázcích 1.1a a 1.1b.



(a) Figura 49 z DBIR [5] zobrazuje akce sociálního inženýrství po průniku (n=1063) pro rok 2022



(b) Figura 35 z DBIR [6] zobrazuje akce sociálního inženýrství po průniku (n=1696) pro rok 2023

Obrázek 1.1 Obrázky 1.1a a 1.1b zobrazují data firmy Verizon pro roky 2022 a 2023.

1.1.1 Využití AI v sociálním inženýrství

Přestože nebyly v roce 2023 ještě nástroje strojového učení využívány na masové úrovni, objevily se první případy zneužití generativních modelů k vishingu. V několika situacích pachatelé naklonovali hlasy rodinných příslušníků, aby je využili při vydírání. Případ Jennifer DeStafano zahrnoval vydírání s pomocí naklonovaného hlasu její 15 leté dcery, kdy pachatel předstíral její únos. Falešným únoscům nejspíš stačilo několik videoklipů z platformy TikTok, aby dokázali

napodobit dceřin hlas.[7] Jiným příkladem, s podobnou zápletkou byla situace Debbie Shelton Moore. [8] Jiný pretext používali útočníci proti Garymu Shildbornovi, kterému zdánlivě volal jeho syn, který se dožadoval peněžní částky na zaplacení kauce, poté jej přesměroval k domnělému právnímu zástupci. Tento zástupce ho nasměroval k zaplacení částky skrze Bitcoinový kiosk. [9]

Zatímco všechny uvedené příklady skončily šťastně, demonstrovaly rostoucí propracovanost novodobého phishingu. Úspěšný příklad sociálního inženýrství se objevil na začátku tohoto roku. Hong Kongský finančník dostal po emailu instrukce na provedení tajné transakce od v Británii sídlícího CFO. Přestože byl nejprve skeptický, byl přizván do online konference, ve kterém na něj čekalo několik, pro něj známých kolegů, včetně zmíněného CFO. Ti jej instruovali k provedení transakcí na několik účtů. Po několika dnech a kontaktu s centrálou ale zjistil, že se stal cílem podvodu. Celá videokonference byla vyrobena pomocí technologie deepfake, kterou naučili z veřejně dostupných záznamů.[10]

Strojové učení (populárně AI) už začalo měnit celou krajinu sociálního inženýrství. Přestože v minulosti bylo možné věřit tomu, co vidíme nebo slyšíme, z nových trendů vyplývá, že vizuální ani hlasové podněty nejsou dostatečnou zárukou identity. Uživatelé počítačové sítě, kteří i přes školení a simulované phishingové kampaně opakovaně selhávají (klikají a vyplňují své údaje), budou nepochybně obětí i v případě propracovanějších pokusů.

1.1.1.1 Útok

Útočníci pro útok mohou využít řadu nástrojů. Průlomy v jazykových modelech dovolují automatizaci psání textu emailu. Mimo to, pomáhají s překladem textů do cizích jazyků, kde v dřívějších dobách šlo phishing odhalit podle chyb ve skloňování, skladby vět nebo gramatických chyb. Současným trendem je využívání jazykových modelů k eliminaci těchto nedostatků, což zlepšuje jak kvalitu, tak účinnost plošných phishingových kampaní. Další výhoda těchto modelů spočívá v možnosti trénování nad vlastní sadou dat, do kterých se dají zařadit i weby cílového subjektu. Takto může útočník snížit potřebnou dobu přípravy útoku na zlomek, díky kombinaci jazykového modelu napojeného na vyhledávání v otevřených zdrojích.

Úprava video záznamů pomocí deepfake bude s rostoucí dostupností této technologie taktéž přibývat. Deepfake je video nebo zvukový záznam, v němž byl něčí obličej nebo hlas nahrazen jiným, tak že tento výtvor vypadá věrohodně [11]. Adaptace deepfaků má velké bezpečnostní dopady, především kvůli realističnosti vyrobených podvrhů. Navíc už existují projekty, jenž dokážou vygenerovat podvrh v reálném čase[1].

Dle definice [11] mohou tedy kromě videa pracovat deepfake i s audio záznamy. I když pro samotné audio není deepfake terminologie až tak běžná. Z příkladů výše je patrné, že už také tato technologie nejen používá ale zneužívá. Existují společnosti, které veřejně službu poskytují[2][3] (i když třeba ne nutně pro libovolnou osobu nebo k nekalým účelům). Kromě generátorů v reálném čase se na webu vyskytují i projekty pro převod textu na hlas[4].

Koncem února 2024 společnost OpenAI odhalila svůj nový video model Sora[5]. Jedná se o model pro tvorbu realistických videí s pomocí textového vstupu. Přestože prezentované video bylo tzv. *state of the art* (používalo nejnovější technologie, v nejpokročilejším stádiu svého vývoje), pokroky v oblasti generativních modelů nelze zavrhnout. Kde deepfake má nedostatek, že potřebuje živý zdroj originálního videa, generativní modely tímto problémem netrpí. Modelu popíšeme, co se jak má stát a získáme vygenerované video. Tedy dostatečně flexibilní útočník by dokázal zkombinovat několik metod k získání až děsivě přesvědčivých výsledků. Uznávám ale, že naštěstí zatím není využití běžné, nicméně je jen otázkou času, než i tento typ technologie bude zneužit.

[1] DeepFaceLive: `https://github.com/iperov/DeepFaceLive`
[2] Respeecher: `https://www.respeecher.com/`
[3] Voice.ai: `https://voice.ai/`
[4] NVIDIA Tacotron 2: `https://github.com/NVIDIA/tacotron2`
[5] Sora: `https://openai.com/sora`

1.1.1.2 Obrana

Obrana proti AI není snadná. Proti jazykovým modelům se technologická obrana téměř ani vytvořit nedá. Jelikož pointa těchto modelů je psát jako člověk, proto jakákoli ochrana by velmi rychle dokázala odfiltrovat i skutečné lidi. Bránit se mohou uživatelé čistě skrze obezřetný přístup, maximálně lze uživatele varovat o podezření na takto vytvořený text. K tomu také patří pravidelné vzdělávání, aby věděli jakých znaků si všímat. Vždycky ve finále dojdeme k tomu, že podezřelé požadavky je potřeba prověřovat.

Další možnou ochranou jsou databáze hrozeb nebo indikátory útoku. Tuto obrannou strategii lze aplikovat hlavně na úrovni zpráv. Pokud tedy přijde například zpráva od databází identifikované hrozby (účet nebo doména patřící známému útočníkovi), můžeme ovlivnit to, zda zpráva vůbec dorazí. Obecně informace z takovéto databáze dovolují informovat naše další kroky (třeba nám pomoci s mitigací problému).

Proti deepfake a generativním videům se ještě stále dá využít některých strategií. Obě technologie zanechávají ve videích (nebo obrázcích) své specifické artefakty [12][13]. Zatím ještě lze spatřit tyto nesrovnalosti holým okem, ale s postupným vylepšováním eventuálně zůstane detekce čistě na strojové kontrole. Podobně by se dala popsat i situace u falešných audio stop.

Kromě zavedení strojových kontrol příchozí komunikace, budou podniky nevyhnutelně muset vymyslet některé nové postupy týkající-se vzájemné identifikace skrze elektronickou komunikaci. Především tedy takové firmy, které operují přes širší geografické oblasti. Jako nejjednodušší se zdá autentizace skrze více faktorů, ani ta však není neprůstřelná.

1.1.2 Phishing

Phishing je technika sociálního inženýrství, jenž se pokouší získat citlivá data, skrze elektronickou komunikaci, kdy se pachatel vydává za důvěryhodnou entitu[14][15].

Tato technika vznikla v dobách zvýšené adopce Internetu, kdy téměř od samého počátku byla využívána finančně motivovanými osobami, hlavně k vylákání čísel kreditních karet, nebo k získání přihlašovacích údajů. Prvním výše profilovým ukázkovým případem automatizace byl program AOHell, který mimo jiné celý proces zjednodušoval. [16][17]

Postupem času se phishing zdokonaloval, hlavně díky lepší organizaci a cílenému využití. První vysokoprofilové případy jsou falešné emaily platformy e-gold [18][19] nebo šíření první velké malwarové infekce Lovebug (ILOVEYOU) [20]. Postupná adopce elektronického mailu snížila počet kampaní konajících se přes internetová fóra. Skrze druhé desetiletí 21. století docházelo k postupnému nárůstu v počtu phishingových kampaní [21][22], součástí i další vysoko-profilový případ, tentokrát ransomware CryptLocker [23] (druhý potenciální případ by byl malware WannaCry, nicméně navzdory počátečním přesvědčením se nejspíš začal šířit přes zranitelný SMB port [24]).

Ve zdrojích se často rozlišuje mezi phishingem jako takovým a tzv. BEC, které je všeobjímající termín, který zahrnuje kromě phishingu ještě akty navíc. Útočník nejprve nějakou dobu sleduje svůj cíl, po nějakém čase využije získané informace k navázání kontaktu s obětí, kdy si vypůjčí identitu někoho, koho cíl alespoň částečně zná. [25] Tento typ útoku spadá do kategorie tzv. spearphishingu, který se zaměřuje na užší okruh cílů. Specifičtější může být ještě tzv. whaling, kdy si pachatel vyhlídne specifickou hierarchicky výše postavenou oběť. Phishing se také běžně rozlišuje podle přenosového média. V tomto kontextu máme vishing (voice phishing), smishing (SMS phishing) nebo qishing (QR code phishing).

Jako nejčastější metody podvodníci využívali hlavně příloh a webů, ať už phishingových nebo infikovaných malwarem. Přestože tyto způsoby se v posledních letech využívaly hojně [26], objevil se v poslední době i trend častějšího BEC. V takových případech není neobvyklé, že je častěji použito samotné sociální inženýrství. Konkrétně lze zmínit případ kompromitace platformy X z roku 2020 (v době útoku ještě Twitter). Útočníci získali nejprve přístup k účtům několika zaměstnanců, které nalákali za účelem *opravení VPN* k navštívení věrohodně vypadajícího fa-

lešného webového portálu. S těmito účty vytěžili informace o interních nástrojích. Po obdržení těchto informací záhy zaútočili na zaměstnance s přístupem k těmto nástrojům. Ve finále pak s pomocí těchto nástrojů dokázali získat kontrolu nad účty několika nejstarších uživatelů na platformě (které se pokusili prodat). Ve finální fázi zneužili účtů veřejných osob, aby rozšířili povědomí o bitcoinovém podvodu. [27]

Kromě technik sociálního inženýrství útočníci používají technické znalosti. Primárním cílem jde o to ztížit identifikaci falešného odesílatele. Druhý účel těchto technik spočívá v obcházení filtrování spamu. Častý je domain spoofing, kdy útočník využije cizí doménu v těle emailu (hlavička MAILFROM se ve většině případů liší od této domény), aby se tvářil jako skutečný odesílatel. V textu mailu není neobvyklé ani zneužití IDN homografu (normálně vypadající písmena jsou ve skutečnosti znakem cizí abecedy; např.: example.com, zde je a nahrazeno písmenem a cyrilice). Domény s názvem připomínajícím nebo blízkým reálnému subjektu (např. *googleadmin.co*, *amazon-financial.org*). [28] Další běžnou záležitostí jsou přílohy s více příponami. Tato technika se zaměřuje na operační systém Windows, jenž ve výchozím nastavení skryje poslední z přípon, díky čemuž přiměje oběť myslet si, že neotevírá nespustitelný soubor. [29]

1.1.2.1 Phishingové kampaně

Nárůst phishingu s sebou nese potřebu omezit útočníky v jejich snahách. Jednou z těchto obran jsou phishingové kampaně. Toto slovní spojení se také dá použít jak pro popsání samotného phishingu, tak popsání celé operace útočníka. [30][31] V zahraničních zdrojích se mezi těmito pojmy rozlišuje pomocí vyjádření explicitní simulace, tedy kampaň určená k obraně se nazývá simulovaná phishingová kampaň (angl. *simulated phishing campaing*) či simulovaný phishing (angl. *simulated phishing*). [32] V kontextu této práce phishingová kampaň bude znamenat obranu.

Účel simulovaného phishingu spočívá v seznámení uživatelů s touto technikou. Pokud by se stalo, že se daný člověk v kampani neuspěje, nebudou potenciálně citlivé údaje získány reálnými útočníky, ale jenom pověřenými osobami. U simulovaného phishingu chceme testovat samotného člověka, tedy sitauci kdy podvodník již zvládl obejít všechny ostatní protiphishingové obrany (víc o obraně lze neléz v kapitole 1.4), proto taky při simulacích nejsou aplikovány spam filtry. Kampaně dovolují situaci zlepšit, už jen seznámením uživatelů s hrozbou, nicméně jako s každou znalostí, pokud není pravidelně využita, může být snadno zapomenuta. Proto by měly by být opakovány alespoň ročně, jelikož za rok mohou útočníci vyvinout nové taktiky. Zároveň pravidelná zkouška dovoluje získat aktuální stav bezpečnostního povědomí uživatelů. Kromě toho, že má samotná kampaň vzdělávací účel, nemusí jako taková stačit. Po selhání v kampani by uživatel měl být řádně proškolen. [32][33]

1.2 Vektory útoku

Vektor útoku je způsob, kterým se útočník dostane do sítě nebo systému [34]. Způsobů jak se dostat do systému nebo sítě je spousta, v této sekci proto uvádím příklady pouze o těch aktuálně nejpoužívanějších. Jedná se o mapování 1:1 na MITRE AT&CK, jelikož se tato klasifikace často využívá.

Přístupy přes odcizené uživatelské údaje Útočníci si mohou obdržet nebo zneužít údaje existujících účtů jako způsob získání počátečního přístupu, perzistence, provedení eskalace privilegií nebo pro vyhýbání-se detekci. Kompromitované údaje (ty můžou zahrnovat i administrátorské) jde použít k obcházení přístupových omezení nasazených na různé systémové zdroje uvnitř sítě. Dají se využít ke zřízení trvalého přístupu k vzdáleným systémům nebo službám [35]. Z logiky věci také útočníkovi poskytují zvýšená privilegia ke specifickým systémům nebo veřejnosti omezeným oblastem sítě.

V některých případech se útočníkovi mohou hodit i neaktivní účty, třeba v případech, kdy už daná osoba není součástí organizace, takové účty pak jednodušeji ujdou pozornosti, jelikož jejich vlastník není přítomen k identifikaci podezřelé aktivity na jejich účtu [36]. [37]

Zneužití veřejně přístupných služeb Útočníci se mohou pokusit zneužít zranitelnosti služby, aplikace nebo operačního systému, který je vystaven a zpřístupněn z veřejné sítě Internet. Zranitelností systému může být softwarový bug, dočasná chyba nebo špatná konfigurace. Mezi často zneužívané aplikace patří webové servery, databáze [38], standardní služby (SMB [39] nebo SSH [40]) nebo protokoly pro administraci či management zařízení [41][42]. Konkrétní nedostatek může zahrnovat i způsob, kterým jdou obejít bezpečnostní prvky. Pokud jde o kontejnerizované prostředí, tak takovéto zneužití může vést ke kompromitaci kontejneru nebo celé instance. [43]

Využití externích vzdálených služeb Útočníci mohou využít do Internetu otevřených služeb, aby získali přístup nebo přetrvali v síti. Jedná se o vzdálené služby jako VPN, Citrix a jiné mechanizmy které dovolují uživatelům připojit se do interní firemní sítě z externích lokací. Přístup k platných uživatelským účtům je mnohdy vyžadován, ale není podmínkou, služby které nevyžadují autentizaci, například Docker API [44], Kubernetes API server, kubelet [45], aj. jsou také součástí tohoto vektoru. [46]

Phishing Útočníci mohou použít zprávy, aby získali přístup k systému oběti. Všechny formy phishingu jsou elektronicky doručené sociální inženýrství. Součástí těchto zpráv mohou oběti obdržet nebezpečné přílohy nebo odkazy, které mají za úkol na cílovém počítači spustit kód. Phishing nemusí probíhat čistě přes email, ale i přes služby třetích stran (např. sociální média). [47] Toto téma bylo rozebráno blíže v kapitole 1.1.2.

1.3 Moderní kybernetické útoky

Kybernetičtí útočníci každodenně vykonávají mnoho různých kybernetických útoků. Data která máme jsou většinou nekompletní, jelikož samotná detekce útoků není snadná (také díky samotným útočníkům, kteří chtějí být ve svých pokusech nezjistitelní) a je předmětem výzkumu. Jenom v české republice NÚKIB řešil 227 incidentů [48–59], to je cca. 55% nárůst oproti předchozímu roku [60], nejvyšší hodnota za poslední čtyři roky [61][62][60]. S nárůstem počtu incidentů poměrně poklesla jejich závažnost. Není jisté, zda stojí za nárůstem zvýšený počet útoků nebo jde pouze o navýšení počtu subjektů jenž musí incidenty hlásit podle zákona o kybernetické bezpečnosti.

Velkou většinou bezpečnostních incidentů za rok 2022 bylo v ČR omezení dostupnosti služeb, [61] tento trend se zjevně promítl i do roku 2023, více bohužel z dostupných dat není zcela patrné, jelikož měsíční zprávy nabízejí pouze agregovaná procentuální čísla několika typů incidentu. U trendů je potom nesrovnalost mezi udávanými počty a indikátorem růstu/poklesu vůči předešlému měsíci. Mezi další zmíněné trendy patří phishingové a ransomware útoky.

V globálním měřítku za rok 2023 nejčastějším cílem útoku bylo dostat k oběti ransomware, byť tento cíl oproti roku 2022 mírně ustoupil, těchto případů je až 20% (u nás ~12% [48–59]), v 18% případů se pokoušelo dostat přístup k serveru, u 13% zkoušelo získat přihlašovací údaje, u 11% zkoušelo exfiltrovat data a u 10% chtělo získat vzdálený přístup.

Obecně se v roce 2023 ukázalo, že útočníci začali častěji používat legitimní software, k nekalým účelům. I u ransomware se ukazuje posun, kdy spíše nežli využívat přímo infekci cíle, útočník získá od oběti citlivá data (nebo bude předstírat, že je má) a pokusí se jej vydírat s jejich pomocí (nebo taková data rovnou někde prodá). Z tohoto důvodu narostl počet aktivních tzv. *infostealerů* o 266%. Přispěl k tomu i trend vektoru útoku, jenž zneužívá ukořistěných údajů reálných uživatelů. Trendy útoků na dostupnost světově nejvíce zasáhly hlavně vládní sektor, nicméně ne dostatečně na to, aby se tento cíl dostal mezi ty světově nejčastější, i tak se ale dostal

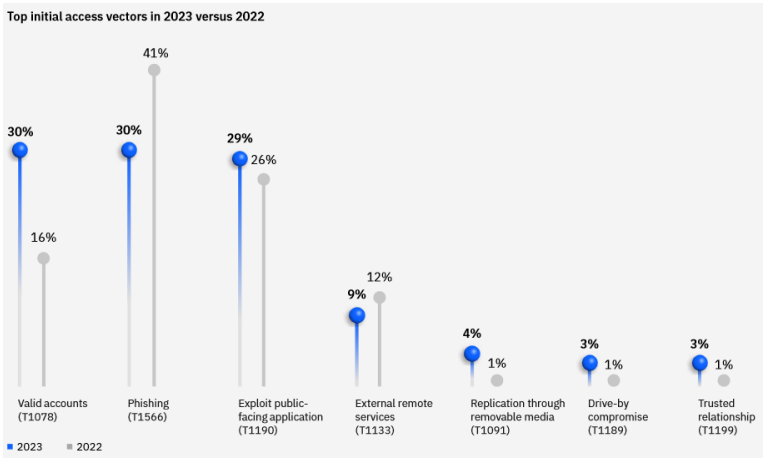
mezi 17% nejčastějších cílů v regionech Středního Východu a Afriky, především tedy u pár zemí Středního Východu. [63]

Přestože u nás byly útoky na dostupnost občas pozorovány i mimo státní sektor, připusťme si, že i když se nejednalo o útoky přímo na státní správu, šlo většinou o útoky skupin [48–59], které obecně chtějí narušit fungování českého státu jakýmkoli způsobem (v tomto případě ekonomickým). Takže proto lze uznat, že nejsme na evropské úrovni ojedinělý případ.

1.3.1 Statistiky vektorů útoku

Za rok 2022 byl nejběžnějším vektorem útoku phishing, konkrétně spear phishing, email s přílohou byl zdaleka nejoblíbenější formou, celkově phishing byl použit u 41% z odhalených útoků. Samostatně se nacházelo na dalším místě zneužití veřejně přístupných aplikací (26%). Dále se často používaly přístupy přes reálné odcizené uživatelské údaje (16%) a mezi posledními častými způsoby bylo využití externích vzdálených služeb s 12% z odhalených útoků. [26] Statistiky od firmy Verizon zmiňují, že jen zhruba 2,9% zaměstnanců interaguje s phishingovými emaily, ale prevalence phishingu naznačuje, že toto procento je pro útočníky zcela dostatečné. [5]

V roce 2023 se četnost phishingu snížila, nejspíš díky adopci novějších protiphishingových technik, ale také díky přechodu útočníků k častějšímu využívaných odcizených účtů. Stále ale byl mezi prvními třemi nejčastějšími vektory, kdy sdílel první místo se zmíněnými údaji na 30%. Zneužití veřejných aplikací taktéž posílilo, s nynějším podílem 29%. Využití externích služeb trochu opadlo na 9%. [63] Tyto údaje jsou vizualizovány na obrázku 1.2. Zprávy NÚKIB taktéž ukazují, že phishing je poměrně stálá hrozba.



Obrázek 1.2 Figura 1 z prezentace [63]. Zobrazuje nejčastější počáteční vektory útoku pro roky 2022 a 2023.

Tedy, jak je z dat patrné, phishing a jeho varianty jsou stále velmi populární metoda. Zatímco minulý rok ještě IBM X-Force neregistrovala žádné závažnější použití metod strojového učení (taktéž populárně zaměňované za AI), tak rok 2023 stejně jako 2024 přinesly několik příkladů nadcházejícího nebezpečí. V roce 2023 stoupající počet vydírajícího vishingu, na začátku toho roku incident Hong Kongského finančníka (více již míněno v kapitole 1.1.1). Další hrozbou jsou generativní sítě, které nedávno dokázaly na základě textového vstupu vytvořit realisticky vypadající trailer. Pokud zvládnou trailer, lze očekávat, že bude technologie zneužita k vytváření realistických video hovorů, nebo přímo důkazních materiálů (taktéž blíže rozebráno v kapitole 1.1.1).

Musíme se proto připravit, hlavní ochranou proti phishingu je školení. Lidé se proto musí naučit rozpoznávat phishingové pokusy, bohužel rostoucí komplexita dělá toto vzdělávání tež-

ším, protože takové vzdělání se soustředí na spatřování nesrovnalostí, oproti přímému důkaznímu materiálu. Mezi toto vzdělávání patří simulované phishingové kampaně, jenž jsou samy o sobě neškodné, a které dříve nebo později stejně budou muset začít využívat pokročilejších technik podobně jako útočníci. Bez patřičného školení s tréninkem je pak pravděpodobnost selhání uživatele, při použití pokročilejších technik útoku, velmi vysoká.

1.4 Ochrana proti phishingu

S rostoucí adaptací elektronického mailu narostl i počet nevyžádaných zpráv. Nevyžádané zprávy (spam) mohou obsahovat phishing, ale většinou se jedná o nechtěná reklamní sdělení. Podniky rozesílající spam, ale domény nepodvrhují. Výskyt těchto zpráv proto vyvolal potřebu se nějak bránit. Tato potřeba vyústila v strategie, které se pokoušejí zabránit nevyžádaným zprávám, především phishingu, dostat se k cíli.

1.4.1 Sender policy framework

Častou taktikou, hlavně jednoduššího phishingu, bylo odesílání zpráv z cizích domén. To mělo dvojí efekt. V první řadě šlo jednodušeji předstírat legitimnost využitím domény podniku s reputací, v druhé řadě se tím daly obcházet dobové ochrany (jako např. blokování známých závadných doménových jmen). [64]

SPF zmírňuje problém spoofingu domén. Zavádí totiž následující mechanizmus: poté co SMTP server obdrží zprávu, zkontrolují se identity v *HELO* (nebo *EHLO*) příkazu společně s polem *MAIL FROM*. Pro obě identity se pokusí získat z DNS textové SPF záznamy. Tyto záznamy obsahují seznam hostitelů, kteří mohou pomocí domény odesílat zprávy. Pokud mechanismus pro kontrolu hostitele nedokáže nalézt v DNS hostitele, jenž serveru mail poslal, tak se s emailem dále zpracovává (toto zpracování může být odmítnutí). [65]

1.4.2 DomainKeys identified mail

Zavedení SPF ztížila útočníkům jejich práci, ale úplně ji neodstranila. Přestože útočník nadále nemůže používat úplně libovolnou doménu, v Internetu se nachází miliony[6] emailových serverů. S takovým číslem nic nebrání útočníkovi vzít doménu, která už záznam se SPF má, a poslat mail z této domény za pomocí spoofingu celé zprávy (vč. IP adres).

Zavedení mechanizmu DKIM tomuto zneužití zabraňuje pomocí podepisování polí zprávy. Do textového záznamu v DNS se přidá veřejný klíč domény, ze které se odesílá email. Odesílající strana má za úkol svoji zprávu podepsat pomocí svého privátního klíče (tento podpis nemusí nutně zahrnovat všechna pole). Příjemce pak zjistí z polí zprávy, která z nich jsou zarhnuta v podpisu, vytvoří hash, který ověří oproti hashi získanému z podpisu pomocí věřejného klíče získaného z DNS záznamu. Pokud podpis nesedí, email je označen k dalšímu zpracování (včetně odmítnutí). [66]

1.4.3 Reputační databáze

Reputační databáze zabezpečují především identifikaci známých rizikových aktérů, pomocí sestavení reputačního profilu. Systémy obvykle schraňují známé informace o daném riziku, včetně lokace, přítomnost na blacklistech, aj. [67][68] Pro účely ochrany emailu se využívají nejprve pro zjištění reputace (včetně jeho přítomnosti v blacklistu) odesílatele ze jména příchozí domény (pokud projde skrze kontroly SPF a DKIM), pokud doména projde, dojde ke zhodnocení samotného obsahu emailu pomocí otisku [69], ve finále jsou reputací ozkoušeny přílohy. [70]

[6] Velmi hrubý odhad podle statistik: Verisign a The Radicati Group

1.4.4 Pravidla pro vnější doménu

Novodobé filtry spamu dovolují přidat pravidla v závislosti na podmínkách. Mezi těmito podmínkami se může vyskytnout i externí doména. Takovéto pravidla dovolují modifikovat pole zprávy specifickým způsobem. Vzhledem k rostoucí běžnosti a propracovanosti phishingu přidali vývojáři protispamových řešení celkem jednoduchou, ale účinnou metodou - modifikovat zprávu, přidáním varování, buď do aliasu odesílatele nebo textu emailu. Takto příjemce napadne mnohem dříve chovat se vůči emailu obezřetně.

Nejčastější úprava zahrnuje přidání textu, že se jedná o externího odesílatele. [71][72] Druhé pravidlo existuje pro vnější entity, které navazují s lokální doménou častý kontakt (např. obchodní partneři), půjde tedy o domény, které technicky vzato jsou externí, ale nemusí nutně představovat riziko. Toto riziko ale představovat mohou, pokud dojde ke kompromitaci této vnější entity. Takže pokud se stane, že přijde email, jenž neodpovídá standardní komunikaci, je do něj přidáno varování o neobvyklosti komunikace. [73][74]

1.5 OAuth 2.0

Autorizační framework OAuth 2.0 dovoluje aplikacím třetí strany získat limitovaný přístup k HTTP službě, buď jménem majitele zdroje pomocí zprostředkování interakce pro povolení mezi vlastníkem zdroje a HTTP službou, nebo zřízením vlastního přístupu pro aplikaci třetí strany. [75]

1.5.1 Device authorization flow

Tento grant je určen pro zařízení připojená k Internetu, kterým buď chybí prohlížeč, kterým by jinak prováděli autorizaci skrze user-agent nebo je jejich vstup tak omezen, že vyžadovat po uživateli napsat text za účelem autentizace je nepraktické. Umožňuje klientům OAuth na takových zařízeních získat uživatelskou autorizaci pro chráněné zdroje použitím user agentu na zařízení jiném.[76]

1.5.1.1 Zranitelnost některých implemetací

Některé implementace využívají volnosti definic dokumentů rfc do extrému. V první řadě, podle rfc nemusí uživateli říkat, že autorizuje nové (útočníkovo) zařízení (byť je to silně doporučeno. [77] V druhé řadě, mohou implementace ignorovat libovolnou část scope vyžádaného uživatelem. [75] To pak může vést k tomu, že si útočník vyžádá arbitrární oprávnění (a server je přijme). [78]

Kapitola 2
Analytická část

V rámci analytické části jsem nejprve sestavil seznam různých, k phishingu určených, aplikací. Po výběru byly nasazeny na virtuální prostředí, vyzkoušeny za účelem ověření využitelnosti při obranné kampani. Dále jsem stanovil trojici pohledů na aplikace, podle kterých hodnotím využitelnost nástroje v praxi. Výstupem je detailní porovnání relevantních vlastností pro účely tvorby phishingové kampaně modrého týmu.

Z veřejně dostupných zdrojů jako jsou organizace ENISA a NIST jsem nenalezl seznam vhodných kritérií pro hodnocení nástrojů pro provádění simulovaných phishingových kampaní.

2.1 Definice uživatele a cíle

Pro účely této práce rozlišuji mezi uživatelem a cílem. Uživatelem budu rozumět uživatele aplikace, tedy systémového administrátora, bezpečnostního profesionála, nebo obecně pověřenou osobu, která chce realizovat phishingovou kampaň. Cílem potom označuji ty osoby, proti kterým je simulace směřována.

2.2 Aplikace

Tato práce se primárně zabývá prozkoumáváním existujících open-source řešení nástrojů pro tvorbu phishingových kampaní. Potřeby každého uživatele při tvorbě phishingových kampaní jsou různé. Stejně to platí i u vývojářů daných nástrojů. Tedy jak potom tedy vyhledávat konkrétní představu? Nejčastější termín pro takové programy bývá *phishing toolkit*, *phishing manager* nebo *phishing campaign manager*, ale takto označený software jistě nebude mít stejné vlastnostmi. Vyjma zmíněných frází budou existovat další. Díky této různorodosti bývá nezbytné program vyzkoušet.

Se stanovenými parametry pro vyhledání vhodného software jsem přistoupil k hledání vhodných zdrojů. Vyhledávat open-source software lze několika způsoby. Nejúspěšnější, alespoň z hlediska kvantity, bude využít repozitářů jako jsou github, či gitlab. Na druhou stranu se v těchto adresářích nacházejí stovky různě popsaných projektů. Nejlépe se vyhledává podle klíčových slov, nicméně projekty často nebývají správně označeny. V tomto ohledu mají vyhledávače repozitářů na většině těchto platforem nedostatek. Buď lze hledat fulltextovým vyhledáváním nebo podle jediného klíčového slova (známé jako téma). Fulltext má poté tu nevýhodu, že popisy projektů mnohdy nezahrnují zmíněné fráze.

Jednodušší je namísto prohledávání repozitářů využít standardního vyhledávače. Tímto způsobem bude hledat i většina administrátorů, kteří budou chtít realizovat kampaň. Nedozví se tak jen o existenci daného projektu, ale i o jeho případné užitečnosti. Mimo první výsledky, které

jsem našel, existují weby, jenž poskytují seznamy bezpečnostních nástrojů (např. Phishgrid [1], Aware7[2]). Pokud jsem program viděl v seznamu phishingového software, přidal jsem ho i do toho svého. Hlavní výjimku zde tvoří Phishingator, na nějž mě odkázal vedoucí práce, proto byl hodnocen až jako poslední.

Ve finále jsem skončil s následujícími aplikacemi. Tyto aplikace jsem rozdělil do tří kategorií. Tyto kategorie jsem vyčlenil až po vyzkoušení daného software. Informace o většině těchto programů jsou záměrně převzaty od samotných tvůrců. Aby bylo vidět, jak svůj software prezentují.

První skupinou jsou aplikace sloužící primárně pro rychlé hostování phishingových webů. Tento software často využívá tzv. tunelovacích služeb. Ty zabezpečují vytvoření tunelu mezi lokálním strojem a službou. Následně směrují komunikaci z domény patřící dané internetové službě na lokální stroj. Mezi tyto programy jsem zařadil následující.

CredSniper CredSniper je phishingový framework napsaný v Pythonovém mikro-frameworku Flask s šablonovacím modulem Jinja2. Podporuje zachytávání dvoufaktorových tokenů. [79]

Hidden Eye je moderní phishingový nástroj s pokročilou funkcionalitou. [80]

PhishInSuits je jednoduchý nástroj napsaný v jazyce Python, který zvládá automatizovat phishing pro OAuth autorizaci zařízení. Konkrétní zranitelnost je popsána v kapitole 1.5.1.1.

ShellPhish Shellphish je nástroj pro phishing uživatelských údajů.

The Social-Engineer Toolkit (SET) je open-source framework pro penetrační testování designovaný pro sociální inženýrství. SET má mnoho přizpůsobených vektorů útoku, které dovolují rychle uskutečnit důvěryhodný útok. [81]

SayCheese v 1.0 (autor: thelinuxchoice) je malá užitečná aplikace, jenž po navštívení stránky využije fotoaparát, k tomu, aby pořídila fotografii cíle.

SpeedPhish Framework je nástroj napsaný v jazyce Python, designovaný pro rychlý průzkum a nasazení jednoduchých cvičení proti phishingu. [82]

SquarePhish je nástroj napsaný v jazyce Python, který automatizuje phishing pro OAuth autorizaci zařízení. Tedy dělá to samé co PhishInSuits, viz. 1.5.1.1.

Zphiser je začátečníkům přívětivý nástroj pro automatizaci phishingu. [83]

Další skupinou byly specializované proxy nástroje, jejichž cílem je odchytávání komunikace, specificky uživatelských údajů a session, jakožto man-in-the-middle element. Specificky u této skupiny většinou bylo ze začátku jasné, že nebudou tolik schopné zabezpečovat celou phishingovou kampaň, nicméně jsem se rozhodl nad rámec zadání práce zhodnotit i tyto nástroje, za účelem jejich případné integrace.

Evilginx2 je man-in-the-middle útočný framework používaný pro phishing přihlašovacích údajů společně se session cookies. Tímto dokáže obejít proces dvoufaktorového ověření. [84]

Muraena je (skoro) transparentní reverzní proxy nástroj zaměřený na automatizaci phishingu a aktivit po phishingu. [85]

Posledním typem software byly *kampaňové manažery*. Pod tímto termínem mám na mysli takový software, který dokáže pomoci s realizací phishingové kampaně, tedy zabezpečit většinu nebo nejpodstatnější z kroků. Ty zahrnují přípravu šablon, rozesílání zpráv, sběr výsledků nebo agregace dat (pro specifické kroky při tvorbě kampaně viz. 2.3.6).

[1] `https://phishgrid.com/blog/top-10-best-phishing-tools/`
[2] `https://aware7.com/blog/the-12-best-tools-for-phishing-simulations/`

FiercePhish FiercePhish je plně rozvinutý phishingový framework pro správu phishingových akcí. [86]

Gophish je open-source phishingový toolkit designovaný pro podniky a penetrační testery. Zajišťuje schopnost rychle a jednoduše nastavit a provést phishingové střety a trénink povědomí o bezpečnosti. [87]

King Phisher King Phisher je nástroj pro testování a šíření povědomí o phishingových útocích za pomocí jejich simulace. [88]

Phishingator je webová aplikace, jejímž cílem je provádět praktické školení uživatelů v oblasti phishingu a sociálního inženýrství, a to odesíláním cvičných phishingových e-mailů. [89] Phishingator byl vytvořen v rámci bakalářské práce, jejímž dílčími cíli bylo navrhnout a implementovat systém pro automatizované rozesílání cvičných phishingových zpráv. [90]

Phishing Frenzy je open-source Ruby on Rails aplikace využívána penetračními testery k správě emailových phishing kampaní. [91]

Simple Phishing Toolkit je phishingový framework vytvořený pro profesionály informační bezpečnosti k odhalení lidských zranitelností. [92]

SocialFish je nástroj pro phishing a sběr informací. [93]

SniperPhish je phishingový toolkit pro penetrační testery a bezpečnostní profesionály, určený pro vylepšení uživatelského povědomí pomocí simulování phishingových útoků. [94]

2.3 Metodika hodnocení - uživatelská stránka

Uživatelskou stránku budu v kontextu této práce brát jako sbírku vlastností, která není příliš technická. Nabízelo by se porovnání kvality uživatelského rozhraní (UI), to ale není úplně na místě, jelikož by se mi těžce posuzovala objektivní kvalita. Myslím, že mnohem objektivněji dokážu posoudit kvalitu uživatelského zážitku (UX). Pro účely shrnutí jsou hodnotící kategorie označeny zkratkou podle anglického názvu. Do této kategorie spadá lokalizace (angl. (L)ocalization), způsob vytváření šablon (angl. (T)emplate (C)reation), import (angl. (V)ictim (I)mport) a kategorizace cílů (angl. (V)ictim (C)ategorization), jednoduchost vytváření kampaní (angl. (C)ampaign (C)reation), vizualizace či generování zpráv (angl. (V)isualization & (R)eports).

Přestože jsem specifikoval, že se má jednat o méně technickou stránku, nasazení (angl. (D)eployment) jsem do této oblasti taktéž zahrnul. Protože nelze posuzovat objektivní kvality uživatelského zážitku, když bude program obtížné zprovoznit.

2.3.1 Nasazení (D)

Pokud má být software použitelný v produkčním prostředí, musí jeho nasazení být bezproblémové. Pokud už se nějaký problém vyskytne, měl by program uživatele alespoň vést k úspěšné konfiguraci. Aplikace může být sebelepší, pokud čas pro uvedení do provozu přeroste den, není takový software použitelný. Jednoduše protože se málokdo bude chtít pouštět do nastavování něčeho, co nakonec ani nemusí fungovat.

Samotné nasazení si žádá několik individuálních kategorií.

Obtížnost instalace (D1)

4 - Aplikace se spustí nativně na systému, netřeba instalovat dodatečné balíky.

3 - Instalace probíhá bez uživatelského vstupu nebo by se dala nahradit skriptem bez uživatelského vstupu.

2 - Instalace může vyžadovat uživatelský vstup či interakci.

1 - Instalace sama od sebe nefunguje, je vyžadována úprava instalačního skriptu nebo manuální opravení závislostí.

0 - Z technických důvodů se aplikaci nezdařilo neinstalovat. To i přes úpravu instalačního kódu.

Obtížnost počáteční konfigurace (D2)

4 - Konfigurace není potřeba nebo se jedná o naprosto triviální úkon.

3 - Konfigurace je intuitivně jasná.

2 - Konfigurace není intuitivně jasná, ale existují zdroje podpory, jenž problém zmírňují.

1 - Konfigurace není intuitivně jasná, žádné zdroje neexistují nebo nemají dostatek potřebných informací. Pro zdárnou konfiguraci může být nutné nahlédnout do zdrojových souborů.

2.3.2 Lokalizace (L)

Lokalizace je pěkná podpůrná vlastnost, dovoluje používat program lidem, kteří neumějí cizí jazyk. Díky časté světové adopci angličtiny jako druhého jazyka sice její důležitost upadla, nicméně i dnes se můžeme setkat s lidmi, jenž cizí jazyk tolik neovládají. Obecně lokalizovaný produkt většinou působí důvěryhodněji. Tato důvěra může být klíčová například při použití statických šablon, protože velké firmy mají ve zvyku své stránky lokalizovat v podporovaných regionech.

Podpora lokalizace (L1) Lokalizačním souborem je myšlen takový soubor, který obsahuje lokalizovaný text s minimální informací o rozložení, či struktuře nelokalizovaného dokumentu. Tedy HTML soubor, ve kterém lze manuálně dohledat a vyměnit texty se nepočítá jako lokalizační!

Plná - Existují lokalizační soubory pro program nebo šablony. Ty lze upravit pro přidání podpory nového jazyka. Pokud pro šablony neexistují lokalizační soubory, aplikace je dokáže vytvářet takovým způsobem, že je jejich lokalizace automatická.

Software - Pro program existují lokalizační soubory, které lze upravit pro přidání podpory jazyku UI. Šablony je potřeba upravovat manuálně.

Šablonová - Pro šablony buď existují lokalizační soubory, které lze upravit pro změnu jejich textů. Nebo dokáže stránky vytvářet takovým způsobem, že je jejich lokalizace automatická.

Žádná - Program neobsahuje lokalizační soubory nebo takové soubory pokrývají minimum aplikace. Šablony je nutné editovat manuálně.

Česká lokalizace (L2) Značí čistě přítomnost českého jazyka UI aplikace.

2.3.3 Vytváření šablon (TC)

Z hlediska uživatelského komfortu nechceme upravovat konfigurační soubory ani zdrojový kód programu, kvůli změně šablony. Pro mail navíc vyžadujeme, aby se počet nutných manuálních úprav udržel na minimu. Budeme chtít odesílat email mnoha uživatelům, proto není přípustné, aby bylo potřeba editovat text zprávy pro každého uživatele zvlášť, navíc manuálně. K tomu by nám měla pomoci makra, která by ideálně měla být taktéž přítomna při tvorbě webu.

Tvorba emailových předloh (TC1)

5 - Vyplnitelné pole šablony zahrnují text zprávy (prostý text i HTML), předmět a odesílatele. V předmětu i textu zprávy systém dokáže vyplnit jméno, příjmení jak cíle, tak odesílatele. Taktéž jde do emailu vložit identifikátor cílové osoby.

4 - Vyplnitelné pole šablony zahrnují text zprávy (prostý text i HTML) a předmět. V textu zprávy systém dokáže vyplnit jméno, příjmení jak cíle, tak odesílatele. Taktéž jde do emailu vložit identifikátor cílové osoby.

3 - Vyplnitelné pole šablony zahrnují text zprávy (prostý text i HTML) a předmět. V textu zprávy systém dokáže vyplnit jméno, příjmení cíle. Do jde emailu vložit identifikátor cílové osoby.

2 - Vyplnitelné pole šablony zahrnují text zprávy (alespoň prostý text) a předmět. V textu zprávy systém dokáže vyplnit jméno, příjmení cíle.

1 - Vyplnitelné pole šablony zahrnují text zprávy (alespoň prostý text). Pokud v textu zprávy poskytuje makra, nezahrnují jméno, příjmení, ani identifikátor osoby.

0 - Šablonu buď upravit nelze, nebo by vyžadovalo zásah do kódu. Pokud poskytuje makra, nezahrnují jméno, příjmení, ani identifikátor osoby.

Tvorba webových předloh (TC2)

4 - V rámci aplikace je možné vytvořit novou šablonu. Tuto šablonu dokáže vytvořit z existujícího zdroje.

3 - V rámci aplikace je možné vytvořit novou šablonu. Pokud dokáže šablonu vytvořit z existujícího zdroje, je vyžadována další uživatelská interakce.

2 - Novou šablonu je potřeba vytvořit externě, ale program ji dokáže použít bez nutnosti úpravy kódu programu.

1 - Nová šablona může být vložena jen nahrazením již existující šablony.

0 - Šablony vytvářet nelze nebo by byl vyžadován zásah do kódu.

Úprava emailových (TC3) a webových (TC4) předloh

4 - Úprava je možná skrze integrovaný WYSIWYG editor nebo rich-text editor s náhledem.

3 - Úprava je možná skrze integrovaný rich-text editor.

2 - Úprava je možná skrze integrovaný textový editor.

1 - Úprava je možná skrze externí textový editor.

0 - Šablony upravit nelze, nebo by byl vyžadován zásah do kódu.

2.3.4 Import cílů (VI)

Import cílů je klíčová vlastnost pro jakéhokoli administrátora, neboť manuální zadávání cílů je proveditelné pouze pro menší počet osob. Importem se zde myslí jakýkoli způsob rychlejší než manuální zadávání nebo kopírování ze schránky. Na formátu nezáleží, ať už je to CSV, XML nebo adresářové služby. Ideálně by takový cíl měl být do systému vložen tak, aby si zachoval příslušnosti ke skupinám. Každý nutný dodatečný zásah přidává nutnou časovou investici, nehledě na to, že se jedná o nezáživnou činnost. Zde nám stačí ano/ne.

2.3.5 Kategorizace cílů (VC)

Pro komplexní správu kampaní by měl program podporovat podobnou skupinovou hierarchii cílů jako adresářové služby - vícero skupin, s možným zanořením (skupiny ve skupinách), včetně případných exkluzí. Minimálně pak alespoň jednu skupinu předem definovaných účastníků.

Skupiny získané přes import nám dodají cíle do systému. Rozdělení cíle do několika různých (i protínajících-se) skupin může pomoci s řízením průběhu kampaně či při jejich následném vyhodnocením. Často uživatel bude mít kategorizaci naimportovanou podle příslušnosti k oddělením, nicméně v adresářových strukturách se mohou vyskytovat další, paralelní dělení, například podle bezpečnostní politiky. I tato paralelní dělení by měla být k dispozici. Uživatele větších organizací bude tato vlastnost zajímat, jelikož tato politika může diktovat, které specifické skupiny (nesouvisející s oddělením) musíme testovat.

Exkluze z takového seznamu je také celkem důležitá, jelikož můžeme mít zaměstnance, jejichž testování je nepřípustné. Manuální výběr exkludovaných jednotlivců je nevhodný, jelikož pokud víme, že se mají ověřovat dvě oddělení bez tři cílů ve speciální skupině, tak kvůli tomu schraňovat speciální CSV s danými uživateli je poměrně pracné. Ničemu ovšem nevadí, pokud bude možnost odeslat email pouze jednotlivci.

3 - Kategorizace cílů odpovídá struktuře, kdy jeden cíl může být ve více skupinách. Je podporována skupinová zanořenost (skupina ve skupině). Pro zvolené skupiny existuje exkluze jedinců nebo skupin. Skupiny lze importovat. V rámci kampaně lze využít jednu nebo více skupin.

2 - Kategorizace cílů odpovídá struktuře, kdy jeden cíl může být ve více skupinách. Skupiny lze importovat. V rámci kampaně lze využít jednu nebo více skupin.

1 - Kategorizace cílů odpovídá struktuře, kdy jeden cíl může být ve více skupinách. V rámci kampaně lze využít právě jednu skupinu.

0 - Program nepodporuje kategorizaci cílů, nebo se jedná o údaj ekvivalentní poznámce.

2.3.6 Jednoduchost vytváření kampaní (CC)

Rozeberme si phishingovou kampaň na posloupnost kroků. Nejprve vymyslíme metodiku kampaně, což zahrnuje určení jakým způsobem budou tvořeny phishingové zprávy (zde nám žádný software nepomůže).

1. Sestavíme nějaký seznam cílů.
2. Podle metodiky vytvoříme předlohu zprávy, ta může, ale nemusí obsahovat URL nebo přílohu (tedy URL by nemělo být povinné).
3. Do textu jsou dosazeny konkrétní údaje, které jsou následně odeslány patřičnému příjemci.
4. Po spuštění probíhá sběr výsledků,

5. které jsou nejpozději po konci kampaně agregovány do konkrétních kategorií.

Čím více předešlých kroků nám program umožní vykonat, tím jednodušší bych označil vytváření kampaně. Obtížnost negativně ovlivňuje i to, zda je nutné některé nedostatky obcházet. Agregací dat zde chápu jako sdružení několika typů podstatných dat, tedy třeba samotný status odeslání emailu není dostatečně podstatná informace, aby její sdružení bylo užitečné.

4 - Aplikace nám zabezpečuje, nebo je schopna zabezpečit všechny kroky od tvorby předlohy zprávy (přílohy musí být podporovány a musí být možné odeslat email bez specifikovaného URL), po agregaci výsledků.

3 - Aplikace nezabezpečuje jeden krok ze zmíněných. Musí být schopná: dosazovat konkrétní údaje do předloh, odesílat zprávy konkrétním cílům a dělat agregaci dat.

2 - Aplikace nezabezpečuje dva až tři kroky ze zmíněných. Musí být schopná: dosazovat údaje do předloh, odesílat zprávy konkrétním cílům (odeslání zprávy pouze jedinci se nepočítá).

1 - Více jak tři kroky je nutné dělat pomocí externích nástrojů.

2.3.7 Vizualizace dat a vyhodnocovací zprávy (VR)

Sesbíraná data sama o sobě nemají váhu. Pokud někomu chceme prezentovat naše závěry, dotyčná osoba si musí předestřené informace být schopna představit. Především pokud se jedná o historické údaje. Graf meziročního nárůstu (nebo poklesu) neúspěšných uživatelů je mnohem přehlednější, nežli tabulka těchto stejných dat. Budou nás zajímat jak nějaké agregované výsledky pro celou naší kampaň, tak rozdělení podle odesílaných skupin nebo oddělení, ale v případě zájmu i individuální výsledky samotných zaměstnanců (technické detaily jako, kdo používal co za prohlížeč nebo jiné nepodstatné údaje nás v této kategorii moc netrápí). **V této sekci se nehodnotí relevantnost vizualizací**, tedy pokud program vyobrazuje data, která nějakým způsobem sbírá, pak bude hodnocena kladněji, než taková která svá data nevizualizuje nijak. Samotná aplikace nemusí zobrazovat ani vizualizovat zmíněné grafy, pokud jsou obsaženy ve vygenerované zprávě (musí být vygenerována přímo programem, nestačí program 3. strany).

Když už pak máme výsledky řádně vizualizovány, tak by ideální program také měl být schopen vygenerovat určitou zprávu. Vytvoření zprávy obecně není jednoduché, každý má jinou představu o tom, která data zobrazit. Na druhou stranu se nic nezkazí, když zpráva bude obsahovat přesně ty agregované grafy, o kterých byla řeč v předchozím odstavci. Individuální výsledky je dobré zahrnout, ale nejedná se o nezbytný požadavek. Zprávou není myšlen export dat z kampaně (raw data, jenž se pak dají dále zpracovávat).

Vizualizace dat (VR1)

3 - Aplikace nebo její zpráva vizualizuje jak agregované výsledky celé kampaně, tak výsledky podle skupin. Výsledky jednotlivců jsou taktéž součástí nebo je lze někde zobrazit.

2 - Aplikace nebo její zpráva vizualizuje agregované výsledky celé kampaně. Výsledky jednotlivců jsou taktéž součástí nebo je lze někde zobrazit.

1 - Sesbíraná data aplikace nebo její zpráva vizualizuje agregované výsledky celé kampaně.

0 - Program ani její zpráva sesbíraná data nijak nevizualizuje.

Zprávy (VR2)

2 - Zpráva obsahuje vizualizaci výsledků společně s textovou reprezentací.

1 - Zpráva obsahuje pouze textovou reprezentaci dat.

0 - Program nedokáže vytvořit zprávu.

2.3.8 Zhodnocení z uživatelské stránky

Přehledy v tabulkách 2.1 a 2.2 mohou poskytnout jenom omezené informace o kvalitě software, jelikož neberou v úvahu menší vlastnosti, které nebyly pro dané sekce zcela relevantní. Pro plný přehled malých i velkých vlastností lze referovat k přiloženému souboru `PhishingSWFeatureTable.ods`.

Software \ Vlastnost	D1	D2	L1	L2	TC1	TC2	TC3	TC4
SayCheese	3/4	4/4	žádná	NE	n/a	1/4	n/a	1/4
ShellPhish	3/4	4/4	žádná	NE	n/a	1/4	n/a	1/4
SocialFish	3/4	4/4	šablonová	NE	1/5	4/4	2/4	1/4
CredSniper	0/4	4/4	žádná	NE	n/a	2/4	n/a	1/4
FiercePhish	2/4	3/4	žádná	NE	4/5	n/a	4/4	n/a
Muraena	4/4	2/4	šablonová	NE	n/a	4/4	n/a	1/4
PhishInSuits	3/4	3/4	žádná	NE	0/5	n/a	0/4	n/a
SquarePhish	3/4	3/4	šablonová	NE	1/5	n/a	1/4	n/a
SPT	2/4	3/4	žádná	NE	n/a	n/a	n/a	n/a
HiddenEye	3/4	4/4	software	NE	n/a	1/4	n/a	1/4
Evilginx2	3/4	2/4	šablonová	NE	n/a	4/4	n/a	1/4
Zphisher	4/4	4/4	žádná	NE	n/a	1/4	n/a	1/4
SniperPhish	2/4	3/4	žádná	NE	4/5	3/4	4/4	4/4
King Phisher	1/4	3/4	šablonová	NE	5/5	4/4	4/4	2/4
Phishing Frenzy	1/4	3/4	šablonová	NE	1/5	3/4	2/4	2/4
The SET	3/4	3/4	žádná	NE	1/5	4/4	1/4	1/4
SPF	3/4	3/4	žádná	NE	1/5	3/4	1/4	1/4
Gophish	4/4	3/4	šablonová	NE	4/5	4/4	4/4	4/4
Phishingator	n/a	1/4	žádná	ANO	1/5	2/4	2/4	1/4

Tabulka 2.1 Tabulka nasazení, lokalizace a vytváření šablon.

Hodnocení z jednoho úhlu pohledu není vždy směrodatné, už z hlediska kvantity vlastností měly některé programy náskok oproti jiným. Po zhodnocení dat jsem identifikoval tři kategorie softwaru, první je software pro hostování stránek. Z nich by se nejlépe dal hodnotit The Social-Engineer Toolkit, který kromě hostování nabízí více vektorů útoku, a posílání emailů.

Software druhé kategorie, si z uživatelského hlediska moc dobře nevedl. Sada proxy nástrojů se nemůže vlastnostmi vyrovnat nástrojům pro phishingové kampaně. Takže v této sekci dopadly obě více-méně stejně.

Pro phishingové manažery zde vítězil Gophish, s poměrně blízkým SniperPhishem, kde práce se skupinami nebo tvorba phishingových webů dělá asi největší rozdíl.

Software \ Vlastnost	VI	VC	CC	VR1	VR2
SayCheese	NE	0/3	1/4	0/3	0/2
ShellPhish	NE	0/3	1/4	0/3	0/2
SocialFish	NE	0/3	1/4	0/3	1/2
CredSniper	NE	0/3	1/4	0/3	0/2
FiercePhish	ANO	1/3	2/4	2/3	0/2
Muraena	NE	0/3	1/4	0/3	0/2
PhishInSuits	NE	0/3	1/4	0/3	0/2
SquarePhish	ANO	0/3	1/4	0/3	0/2
HiddenEye	NE	0/3	1/4	0/3	0/2
Evilginx2	ANO	0/3	1/4	0/3	0/2
Zphisher	NE	0/3	1/4	0/3	0/2
SniperPhish	ANO	1/3	4/4	2/3	1/2
King Phisher	ANO	0/3	4/4	3/3	0/2
Phishing Frenzy	NE	0/3	4/4[a]	2/3[b]	1/2[b]
The SET	ANO	0/3	2/4	0/3	0/2
SPF	ANO	0/3	2/4	0/3	1/2
Gophish	ANO	2/3	4/4	2/3	0/2
Phishingator	ANO	2/3	3/4	3/3	0/2

Tabulka 2.2 Tabulka vytváření kampaní, importu, kategorizace a vizualizace.

a - Nelze plně podložit díky problémům s implmentací.
b - Založeno na historických důkazech.

2.3.8.1 SayCheese

Nasazení bezproblémově proběhlo na virtuálním stroji s Kali, stránka pracovala dle očekávání. K ovládání slouží konzolová řádka. Instalace probíhá za běhu programu a to jen do míry doinstalování chybějících závislostí. Konfigurace je vždy jasná, program se ptá na specifická nastavení.

Program lokalizační soubory nemá, ani samotná stránka. Přítomná šablona je spíš taková ukázka, takže ani není moc co lokalizovat. Úpravu existující šablony je nutné dělat manuálně pomocí externího textového editoru.

Program odesílání emailu neumožňuje. Jelikož nemá emailové funkce, import cílů, ani jejich kategorizace nejsou k dispozici. Proto by tvorba plnohodnotné kampaně byla dle specifikace obtížná. Zaznamenaná data aplikace nijak nevizualizuje, ani nevyrábí reporty.

Pro praktické použití by bylo potřeba upravit webové UI nebo skript osamostatnit, aby se dal vložit do jiné stránky.

2.3.8.2 ShellPhish

Nasazení proběhlo bez problémů na virtuálním Kali linuxu. Program nabízí konzolovou řádku, kde lze vybírat mezi různými webovými šablonami. Program běží nativně, ale může provádět instalaci některých závislostí za běhu programu. S nastavením nebyly obtíže, jelikož se program ptá na vše potřebné.

Celý software včetně šablon je tvořen v anglickém jazyce. Program nemá lokalizaci. V neposlední řadě jsou šablony vytvořeny celkem podivným způsobem (nejspíš klonování), takže kontrola/úprava samotných šablon by byla časově náročná. Šablony používají typické HTML, takže úpravu je možné udělat pomocí textového editoru. Odchytávání údajů sice funguje, nicméně notifikace o zachycení se v konzoli občas neukáže.

Kvalita šablon je následující:

- Instagram - Vypadá v pořádku, přestože není zcela aktuální, dokázala by obelstít nepozorného člověka.
- Facebook a Github - Naprosto tristní, na prohlížeči se ani neblížila staré přihlašovací stránce. Téměř nepoužitelná.
- Snapchat a Google - Velmi stará šablona, každý běžný uživatel by si všiml rozdílu na první pohled.
- Twitter - Taktéž stará šablona, velmi nápadná vzhledem k nedávnému rebrandu na platformu X.

Program neposílá emaily, proto neřeší import ani kategorizaci cílů. Z těchto důvodů by bylo vytvořit plnou kampaň celkem obtížné (1/4).

Sesbíraná data program nijak nevizualizuje ani z nich negeneruje zprávy.

2.3.8.3 SocialFish

Web byl nasazen na virtuálním Kali linux. Instalace proběhla v pořádku, je potřeba nainstalovat Python a potřebné závislosti. Na začátku uživatel zadá jméno s heslem, toto bude jediný uživatel, který se bude moci do webu přihlásit. V konzoli se ukáže na jaké URL se uživatel má podívat, aby se dostal k přihlášení.

V dashboardu se nalevo nahoře nacházejí vstupní pole do kterých lze zadat postupně zdrojovou stránku, která bude naklonována, a stránku na kterou bude cíl přesměrován po zadání svých údajů. Vůči klonování jsem byl poněkud skeptický, nicméně výsledky nebyly špatné. Klonování vytvořilo výsledek, který sice nebyl identický se zdrojovou stránkou, ale poměrně dobře se ji blížil. Proces nezvládá zpracovávat UTF-8, tuto chybu ale jde opravit modifikací klonovací funkce. Neklonuje celý web, jen jednu stránku. Navíc nám zde odpadá problém lokalizace jelikož se klon provede pro konkrétní user-agent. U sběru přihlašovacích údajů se ukázal jeden nedostatek, v případě, že se na klonované stránce vyskytoval formulář ovládaný pomocí javascriptu. Takový formulář totiž neodeslal POST, čímž se data neuložila.

Každou zkopírovanou stránku potom lze dále upravovat, případně zadat lokaci svojí připravené šablony, takže člověk není omezen čistě klonovací funkcí. Úpravy už je nutné dělat pomocí textového editoru.

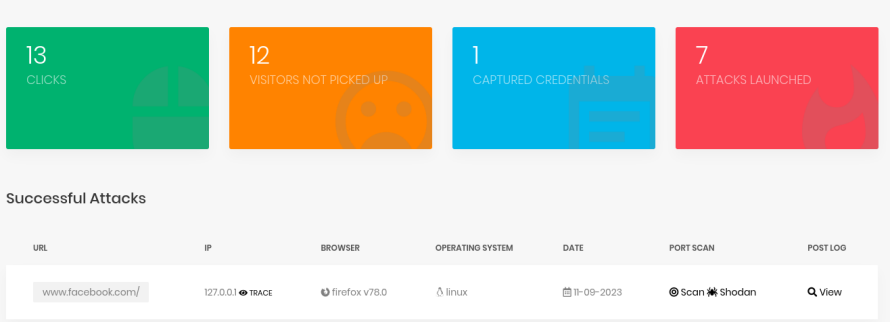
Emailová předloha je čistě textové pole, program nemá žádná makra, takže konkrétního člověka program nedoplňuje. Email jde odeslat pouze jedinému člověku.

Import ani kategorizaci cílů program nezajišťuje. Jelikož má program poměrně malé schopnosti v oblasti odesílání emailu, a neobsahuje některé klíčové vlastnosti, byla by tvorba kampaně poněkud obtížná (1/4).

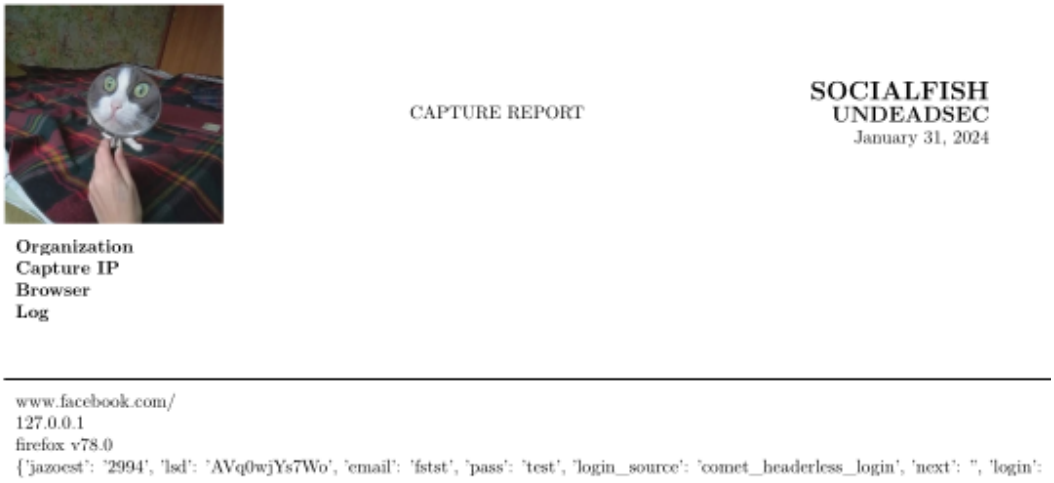
Dashboard, jak je vyobrazen na obrázku 2.1, obsahuje čtyři agregované statistiky: kolikrát byla hostovaná stránka navštívena, kolik návštěvníků odolalo, kolik uživatelských údajů se podařilo zachytit a kolik útoků proběhlo. Bohužel neexistuje zde žádné rozlišení mezi kampaněmi, jediný způsob jak lze čísla resetovat je zásah do databáze. Tyto statistiky nejsou vizualizovány grafem, pouze textovou formou. SocialFish poskytuje reporty z kampaně, nicméně sám o sobě tvoří pouze .tex soubory, vygenerované PDF je kvalitativně ekvivalentní logovému souboru. Ukázku zprávy můžete vidět na obrázku 2.2. Každopádně díky agregaci výsledků má software celkem svázané ruce v možnostech vizualizace.

2.3.8.4 CredSniper

Nasazení proběhlo na aplikací vyžádaném Ubuntu, bohužel s neřešitelnými problémy. Instalace software se provádí přes bashový skript, který volitelně vyžádá let's encrypt certifikát (ten je pro 2FA obcházení vyžadován i v případě, kdy není nevyužito http). Na zvoleném stroji ale nebyl schopen projít až do konce. Pro let's encrypt nenašel specifický adresář, což bylo možné obejít.



Obrázek 2.1 Dahboard programu SocialFish.



Obrázek 2.2 Úryvek ze zprávy SocialFish (logo v levo nahoře ve výchozím stavu neodkazuje na existující soubor, nahradil jsem ho proto příhodným obrázkem.)

Důvodem pro selhání nastavení virtuálního prostředí bylo používání starého API ve skriptu, pod novým nefungoval.

Program lokalizaci nezajišťuje. Před-vytvořená je dvojice šablon - gmail a github. Dále se v adresáři nachází i šablona pro nové moduly. Princip už byl ve skrze popsán v kapitole 2.2, díky tomu, jak program funguje je náchylný ke změnám webových předloh. To se stalo v případě té githubové. Google šablona vypadá funkčně. Tedy bohužel i zde je problém zastarání předloh, byť je možné dopsat vlastní. Přestože tvorba nové šablony vyžaduje nějakou práci s kódem (jedná se o kód zabezpečující právě 2FA, nejedná se o manipulaci šablony v kódu), zbytek úpravy existujících se dělá pomocí textového editoru.

Aplikace sama emaily neposílá, takže není k dispozici ani import nebo kategorizace. Jelikož aplikace nezabezpečuje více jak tři kroky specifikované v 2.3.6, obtížnost tvorby kampaně hodnotím jako 1/4. Vizualizace a reporty taktéž nejsou k dispozici.

2.3.8.5 FiercePhish

Instalace je podporována pro 3 specifické verze Ubuntu. V rámci diplomové práce nebylo nutné testovat kompatibilitu s jinými operačními systémy, proto byl použit virtuální obraz jedné z pod-

porovaných verzí Ubuntu. Na tento obraz byl nasazen program verze 1.2.4. Nasazení neproběhlo zcela bezchybně: instalátor využívá ke spouštění shell příkaz syscmd, ten ale schovává výstup spuštěných příkazů. Jelikož instalátor spustil závislost composer v interaktivním módu, zpráva o potvrzení instalace jako root uživatel zůstala skryta, čímž se instalace zasekla. Problém jsem vyřešil nahrazením spuštění composeru v neinteraktivním módu. Za zmínku možná stojí, že přestože nevyžaduje nutně starší PHP, některé závislosti nejsou s PHP 8+ plně kompatibilní. První konfigurace se píše přímo do instalačního souboru.

Lokalizaci program neposkytuje.

V záložce email jako první můžeme poslat testovací email, který dokonce poskytuje i přílohu (ale jedná se jen o mail jedné osobě). V této sekci jsem narazil na další problém, nic nešlo posílat a šablony byly zaseklé na nekonečném načítání, po kontrole javascript konzole, jsem zjistil, že problém způsobil CKEditor. Z chybové zprávy jsem se dozvěděl, že licenční klíč pro editor vypršel. Tento problém byl způsoben licencováním knihovny, CKEditor má open-source licenci pro verzi 4. Tato verze je používána projektem. Té ale už skončila dlouhodobá podpora (LTS), nicméně existuje rozšířená podpora dostupná pouze s komerční licencí. Problém byl způsoben Bower[3] závislostí, jenž vyžadovala jakoukoli minor verzi vyšší než specifickou, nicméně od verze 4.23+ je editor pouze pro produkty se zmíněnou licencí. Problém jsem vyřešil nahrazení specifickou verzí CKEditoru. V době psaní tohoto textu už autor tuto chybu opravil.

Šablony emailu jsou typický rich text editor, tedy pokud emailový klient podporuje HTML, lze vyrobit dobře formátovaný text. Fiercephish podporuje makra, která jsou substituována za údaje účastníků. Dostupná makra jsou následující:

- celé jméno účastníka
- jméno účastníka
- příjmení účastníka
- uživatelské jméno (vytvořené z adresy)
- email účastníka
- uid účastníka
- jméno odesílatele
- email odesílatele

Aplikace umožňuje import adres z CSV souboru, společně s manuálním zadáváním. Formát CSV souboru je popsán pod importním tlačítkem. Nelze zadat informace o pozici, byť lze takovou informaci doplnit pomocí poznámkového pole. Ze seznamu cílů FiercePhishe přidané cíle již nelze odebrat. Další submenu jsou seznamy cílů, zde lze přidávat uživatele do odesílacích skupin. Jeden uživatel může být přítomen ve více seznamech, lze vybírat nepřiřazené, nebo vybrat náhodně x uživatelů. Skupiny nelze importovat, ani využít poznámek k jejich vytvoření, nelze vložit skupinu do skupiny.

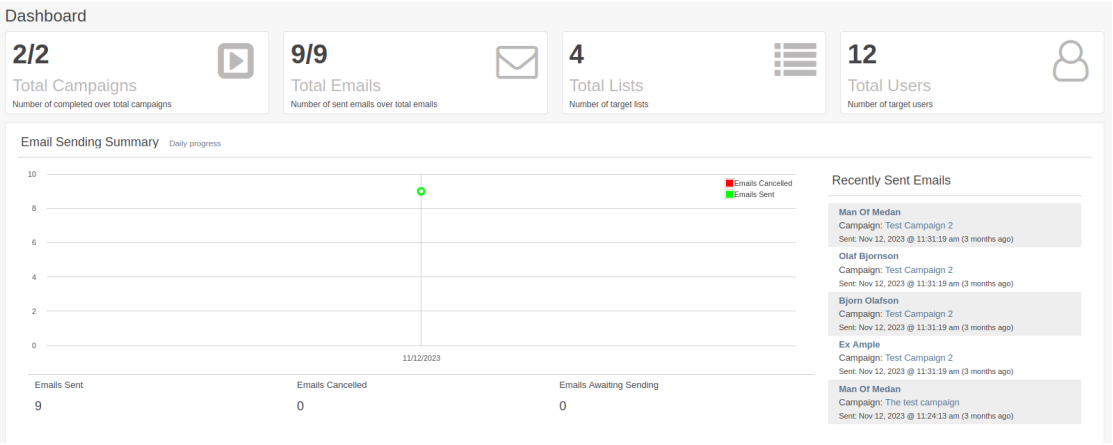
Kampaně vyžadují jméno, zvolení seznamu účastníků a příslušnou šablonu. Dále lze doplnit údaje odesílatele emailu, kdy kampaň započne společně s limitem mailů za interval.

Jelikož aplikace nezabezpečuje agregaci podstatných výsledků, tak nelze hodnotit z hlediska jednoduchosti vytváření kampaní lépe než 2/4.

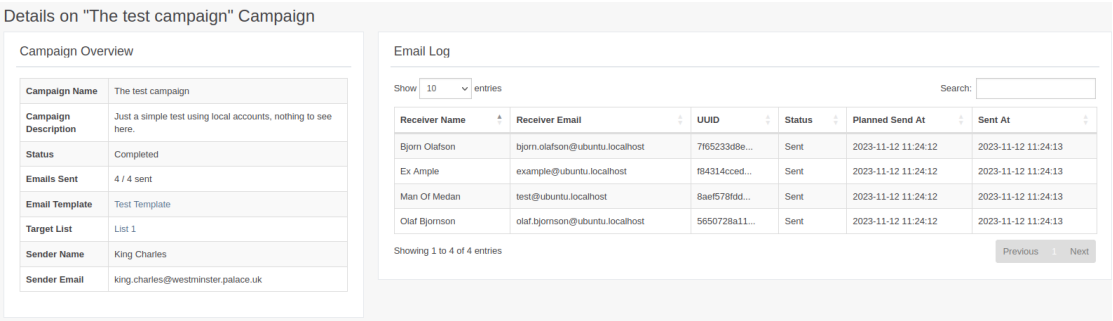
Dashboard (k představě na obrázku 2.3) agreguje statistky všech kampaní, ale nejedná se o nijak zajímavé grafy. Jde pouze o počet úspěšně odeslaných mailů, taktéž zobrazuje počet odeslaných mailů za určitou dobu. Detail kampaně (viz. obr. 2.4) své výsledky taktéž nevizualizuje. Zprávy aplikace neposkytuje.

Veškerou dodatečnou konfiguraci je možné dělat ve webovém portálu.

[3] Balíčkový manažer pro web.



Obrázek 2.3 Dahboard programu FiercePhish.



Obrázek 2.4 Detaily kampaně programu FiercePhish.

2.3.8.6 Muraena

Tento nástroj byl nasazen na virtuálním stroji s Ubuntu. Program běžel nativně. Ovládání probíhá přes interaktivní konzoli. Muraena je bohužel limitována především nedostatečnou dokumentací. Wiki je tak zastaralá, že informace z ní jsou naprosto nepoužitelné. Nejvíc aktuální dokumentace se nachází v dokumentu docs/README.md. Pro korektní vyplnění konfiguračních suborů ani tento dokument nestačí, je nutné prohlédnout si příklady nastavení, nahlédnout do dokumentace, načež je občas potřeba podívat se do zdrojového kódu. Za tímto účelem jsem sestavil menší návod, který je k dispozici v příloze A.

Zprovoznění nástroje do funkčního stavu bylo velmi obtížné, ale eventuálně se mi to podařilo. Pro sledování session jsem využil *__gid*, kterou používá google k analytice. Jelikož se session cookie měnila kvůli IV a MAC. Tento přístup sice vyrobil několik falešných positiv, ale těch bylo jenom několik. Útok jsem provedl proti FiercePhish portálu. Jelikož se jednalo o první pokus práce s takovým typem proxy, zabralo to celkem dost času a vyžadovalo určitou znalost systému, na který se nasazoval. Nevím jistě jak bych takový problém řešil kdyby stránka nevyužívala žádnou formu sledování uživatel externích poskytovatelů (což se může stát). Ale předpokládám, že při bližším zaměření-se na tento nástroj by se dala sledovat i přímo cookie.

Díky tomu, že se jedná o proxy, jazyk závisí na přistupovaném zdroji, samotné UI lokalizaci nepodporuje. S tím souvisí i tvorba webových šablon, která je z principu automatická.

Posílání emailů nezabezpečuje, takže nemá ani žádný import cílů. Protože jde pouze o proxy, a nezabezpečuje více jak tři nezbytné kroky, musím obtížnost tvorby kampaně hodnotit jako 1/4. Získaná data nejsou vizualizována, nejblíže je tabulka zachycených údajů.

2.3.8.7 PhishInSuits

Program byl nasazen na Kali, nicméně jeho nasazení nebylo plné. Instalace vyžaduje vedle samotného interpretu Python doinstalovat patřičné knihovny. Dostupná konfigurace je řešena skrze argumenty příkazové řádky. Nástroj je spíše proof-of-concept, využívá pevně daný Microsoft API koncový bod. Tato adresa je ta, na které se nachází služba OAuth. Protože je ale tato adresa pevně stanovená, není dostatečně flexibilní. Přestože bych byl schopen si vytvořit vlastní SSO a přepsat URL, zase tak velikou užitečnost v programu nevidím, abych podstupoval takto rozsáhlé akce.

Jako v jiných programech i zde je problém lokalizace, hlavně tedy emailu, který by si musel každý přepsat uvnitř zdrojového kódu. Jednoduchost vytvoření plné kampaně je 1/4, neboť neposkytuje mnoho vlastností, které by její tvorbu zjednodušovaly. Získaná data nejsou nijak vizualizována.

2.3.8.8 SquarePhish

Program byl nasazen na Kali bez problému. Instalace vyžaduje přítomnost interpretu Python včetně patřičných knihoven. Dostupná konfigurace je řešena skrze výborně popsaný konfigurační soubor. Oproti PhishInSuits, se nasazení podařilo do míry otestování prvního kroku. Nicméně jelikož je proces autorizačního toku dobře dokumentován, nemám pochyb, že by útok proběhl bez problémů.

Email je nově podporován, aplikace separovala zprávu z kódu, i když je jeho formátování limitováno čistě tím, co jde zadat do HTML. Lokalizace šablon je proto mnohem snazší.

Import cílů není přítomen, ani kategorizace cílů. Zprávu jde poslat vždy právě jednomu člověku. I přes vylepšení program stále neumožňuje posílat zprávy více cílům a neulehčuje dostatečně práci s kampaní, proto její hodnocení zůstává na 1/4. Vizualizace taktéž nejsou k dispozici.

2.3.8.9 Simple Phishing Toolkit

Pokus o nasazení se konal na virtuálním Ubuntu. Nicméně z důvodu extrémního zastarání nebylo dokončeno. Podle archivovaných stránek není projekt udržován od 31. 7. 2013. Což znamená, že nasazení aplikace by přinášelo další přidané problémy. Konkrétně PHP 5, staré PHP znamená, buď starý operační systém, nebo backportovanou verzi. I přesto jsem hodlal zkusit dát SPT šanci, protože zastaralost by se dala vyřešit úpravou kódu, či jeho převzetím pod nového udržovatele. Pokusil jsem se proto zjistit, zda se mi nepodaří portál zprovoznit pod PHP 8. Bohužel se ukázalo, že úplně od začátku databázové přístupy vyžadovaly funkci odebranou ve verzi 7. Nasazení pod bezpečnější verzí PHP by tedy znamenalo přepsání celé aplikace.

2.3.8.10 HiddenEye

Program byl nasazen na virtuálním Kali bez problémů. Instalace zahrnuje jak interpreta jazyka Python, tak potřebné knihovny. Nastavení hostingu probíhá přes konzoli a je zcela triviální.

Jako jeden z mála programů poskytuje HiddenEye lokalizační soubory pro text programu.

HiddenEye nabízí 45 šablon. V kódu jsou jejich umístění zadané staticky, tedy přidáváním složek do patřičného adresáře se nová nepřidá, nicméně obsahuje dvě tzv. „custom“ volby, jenž jsou určeny k úpravám. Pro úpravu je nutný textový editor.

Sám o sobě neposílá maily cílům, takže neřeší import cílů ani kategorizaci. Jelikož neposkytuje dostatek klíčových vlastností, dle definice v 2.3.6 spadá pod 1/4. Sesbírané údaje nejsou ani vizualizovány, ani z nich program negeneruje zprávy.

2.3.8.11 Evilginx2

Evilginx2 byl nasazován nejprve na virtuálním Ubuntu, posléze na Kali. Ovládání probíhá přes interaktivní konzoli. V ostrém kontrastu s Muraenou, Evilginx má všechnu potřebnou dokumentaci. Autor také publikuje blogové příspěvky, většinou k příležitosti aktualizace. Navíc je k dispozici placený kurz. Příspěvky autora na jeho blogu o Evilginx mi paradoxně daly větší náhled do konfigurace nástroje Muraena, který jsem už v době zkoušení Evilginx zprovoznil.

Přes všechnu dokumentaci bylo nasazení paradoxně těžší, než v případě Muraeny. Proxy byla nasazena proti FiercePhish portálu. Obě aplikace se tedy nacházely na stejném stroji (Toto jsem udělal záměrně, aby se případně dal přímo porovnat s Muraenou). První nastavení nevyžaduje moc konfigurace, stačí nastavit adresu proxy, port, vytvořit phislet (jeden řádek filtru díky funkcionalitě autofilter) a aktivovat jej. První překážka - neexistující spouštěcí argument (-P, v nějaké verzi nastavoval adresu proxy).

Evilginx2 evidentně fungoval jako proxy (web se zobrazil), adresa byla přepsána, nicméně po přihlášení nic - nezachytil ani uživatelské údaje, ani cookie. Ani nebyly vyprodukovány žádné informace o připojení k serveru. Jediná informace vycházející z logu tvrdila, že certifikát má neznámého vydavatele, což byla pravda, byť jsem dle požadavků dokumentace evilginx certifikační autoritu zařadil mezi důvěryhodné. Validní sebou podepsaný certifikát ale nemohl způsobit problémy se zachytáváním formulářových údajů. Taktéž nemohlo jít o chybu v regulárních výrazech, jelikož by musel být zachycen alespoň prázdný znak. Napadlo mě tedy, že by mohla být chyba v nepoužívání tzv. *lures* - přístupové odkazy k proxy stránkám (ochrana proti automatickým skenerům). Chování proxy ale nereflektovalo očekávané zamítnutí přístupu.

Abych mohl vytvořit *návnadu* (angl. lure), musel jsem podstatně změnit aktuální nastavení. Nejprve jsem začal měnit konfiguraci portů, z čehož později vyplynuly další obtíže. Do této chvíle jsem používal alternativní https port 8443, jelikož na 443 mi běžela skutečná stránka. *Návnadám* se úplně nedařilo generovat URL na nestandardním portu (v zpětném pohledu jsem měl vyzkoušet ještě použití návnady s manuálním doplněním portu). Proto jsem musel udělat další ústupek, změnil jsem naslouchací porty Apache. To se *návnadám* také nelíbilo, poněvadž přidáním dvojtečky do hostovacího jména se nedokázal korektně odvodit odkaz. Bez řešení v dohledné době jsem se rozhodl přesunout na Kali, kde jsem začal od znovu.

Tento krok byl zdárný, konečně vše začalo fungovat očekávaným způsobem. Proxy stránka se už neukazovala, problémy s certifikátem utichly. Jak se ukázalo moje hypotéza byla pravdivá, *návnady* jsou potřeba k přistoupení. Po prvním navštívení dostane klient cookie, takže už nemusí přistupovat přes odkaz. U návštěvníka bez dané cookie mělo dojít k přesměrování na přednastavenou adresu, k tomu ovšem na Ubuntu nedocházelo.

Změna počítače nevedla jen k pozitivům, z nějakého důvodu přestala fungovat vlastnost autofilter, která má automaticky generovat přepisovací subfiltry pro doménu. Web Fiercephish ale není složitý, proto stačil jediný subfiltr, abych dostal proxy web do provozu. Poté jsem už byl schopen bez problémů sesbírat uživatelské údaje a přihlašovací tokeny.

UI lokalizaci nepodporuje, jazyk webů závisí na přistupovaném zdroji. Tvora webů/šablon je automatická.

Sice nezabezpečuje posílání emailů, ale můžeme importovat cíle, z nich je poté možné generovat *návnady*. Díky tomu, že nedokáže odesílat emaily, nemůže nástroj získat hodnocení vyšší jak 1/4. Získaná data nejsou vizualizována, nejblíže je výpis zachycených údajů. Program zprávy neposkytuje.

2.3.8.12 Zphisher

Nasazení probíhalo na Kali, bez jakýchkoli problémů. Instalace se provádí za běhu programu v případě, že na počítači není přítomna závislost. Nastavení probíhá pomocí konzole.

Stejně jako u jiných programů podobného typu, je nedostatkem lokalizace, kdy jsou stránky vytvořené s pomocí anglických verzí.

Nabízí statické šablony, celkem 45, stejný počet jako u HiddenEye. Přesměrování jsou v šablonách specifikovány na více pravděpodobné stánky (například stránka neexistuje), což je méně vypovídající, oproti nasměrování na pravou přihlašovací stránku. Některé weby mají v Zphiseru varianty, podle konkrétní záminky. Ne všechny šablony jsou vytvořené pomocí klonovacího nástroje, jelikož některé jsou připsány konkrétním autorům. Byly tedy upraveny, nejspíš za účelem přesvědčivosti. I Zphisher bohužel má šablony hard-coded ve spouštěcím skriptu, takže nelze rychle přidat vlastní. Pro úpravu musíme použít externí textový editor.

Program nepracuje s emaily. Neposkytuje import ani kategorizaci cílů. Na základě těchto nedostatků nelze hodnotit jednoduchost tvorby kampaně lépe než 1/4. Sesbíraná data nijak nevizualizuje.

2.3.8.13 SniperPhish

Nasazována byla jeho verze 2.1 na virtuálním Ubuntu. Nasazení bylo bezproblémové. Po instalaci se objevila jedna maličkost, kdy nebyla v .htaccess souboru nastavená správná přesměrovací lokace indexu, díky čemu vracel SniperPhish chybu 404.

Program nemá lokalizační soubory, ale jelikož neposkytuje vlastní šablony, nejedná se o velkou překážku.

Pro vytváření šablon využívá SniperPhish klasický rich text editor. Při tvorbě emailu můžeme vidět náhled příkladného uživatele. Jako ostatní manažery, uvnitř textu lze využít následující makra:

- uid účastníka
- id kampaně
- celé jméno účastníka
- jméno účastníka
- příjmení účastníka
- poznámka o účastníkovi
- email účastníka
- email odesílatele
- URL sledovacího obrázku
- HTML sledovacího obrázku
- SniperPhish base URL
- uživatelské jméno (vytvořené z adresy)
- uživatelova doména (vytvořená z adresy)
- náhodný alfanumerický řetězec

Konkrétní vzezření sledovacího obrázku lze vybrat přímo pro mailovou šablonu. K emailu lze taktéž připnout přílohy. Jména příloh lze taktéž měnit v závislosti na odesílaném mailu s pomocí maker. SniperPhish je schopen hostovat vlastní soubory. Lze sem nahrát libovolný soubor, nebo vstupní stránku. Stránky lze také editovat pomocí rich text editoru. Oba editory přímo zobrazují HTML prvky.

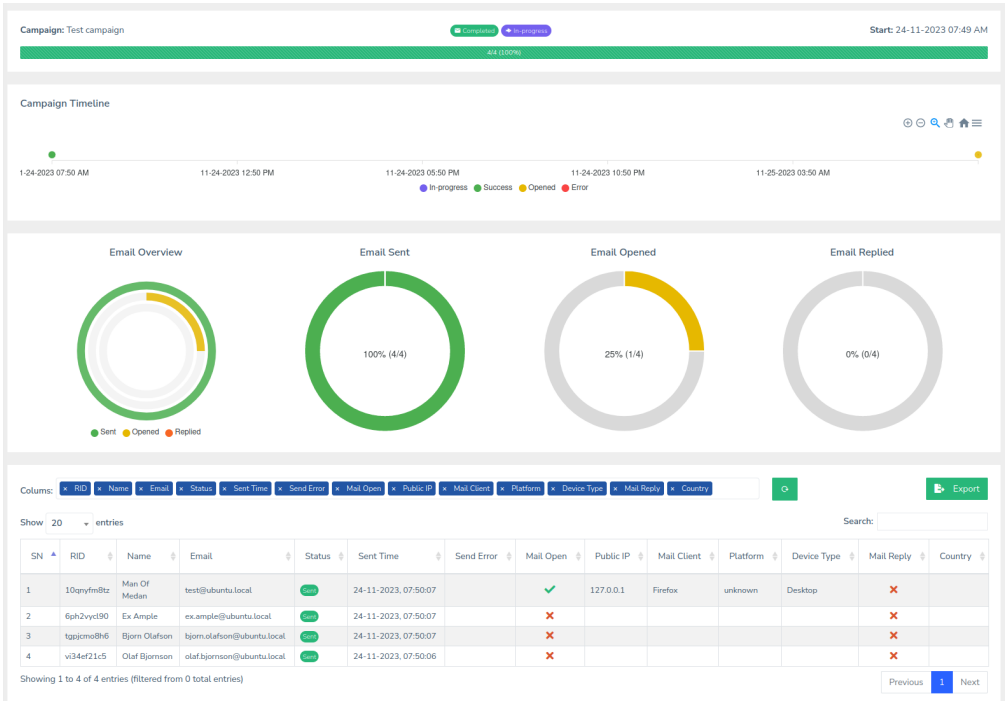
Vkládání cílů funguje pomocí uživatelských skupin. Sem je lze buď zadat manuálně, nebo importovat za pomocí CSV souboru. Zadaní uživatelé jdou exportovat. Typy polí jsou jméno, email a poznámka. Toto je celá dostupná kategorizace.

Kampaně se tvoří v seznamu kampaní, vyžadují jméno, právě jednu skupinu uživatelů, šablonu, odesílatele a konfiguraci zpráv. Lze zvolit čas začátku kampaně společně s časem mezi zprávami. Kampaň lze v průběhu upravit, či zkopírovat. Smazat ji lze až po ukončení. Program zabezpečuje všechny potřebné kroky pro zjednodušení tvorby kampaně, proto jej v této kategorii lze hodnotit 4/4.

Home zobrazuje statistiky počtu kampaní a trackerů (sledovacích prvků), společně s časovou linií. SniperPhish má dva typy kampaně - webové kampaně a čistě emailové, každá má svůj vlastní dashboard. Tato data nejsou nikde agregována, každá kampaň má své vlastní. Dashboard webových kampaní umožňuje korelovat sledovací prvky. Menu trackerů má určité nedostatky, pokud je tracker vytvořen bez patřičné kampaně, pak nepůjde pozastavit. Nepůjde pozastavit ani v případě, že není dokončen, přestože se bude tvářit aktivně (toto není záměrné, javascriptová konzole vrací chybu 500).

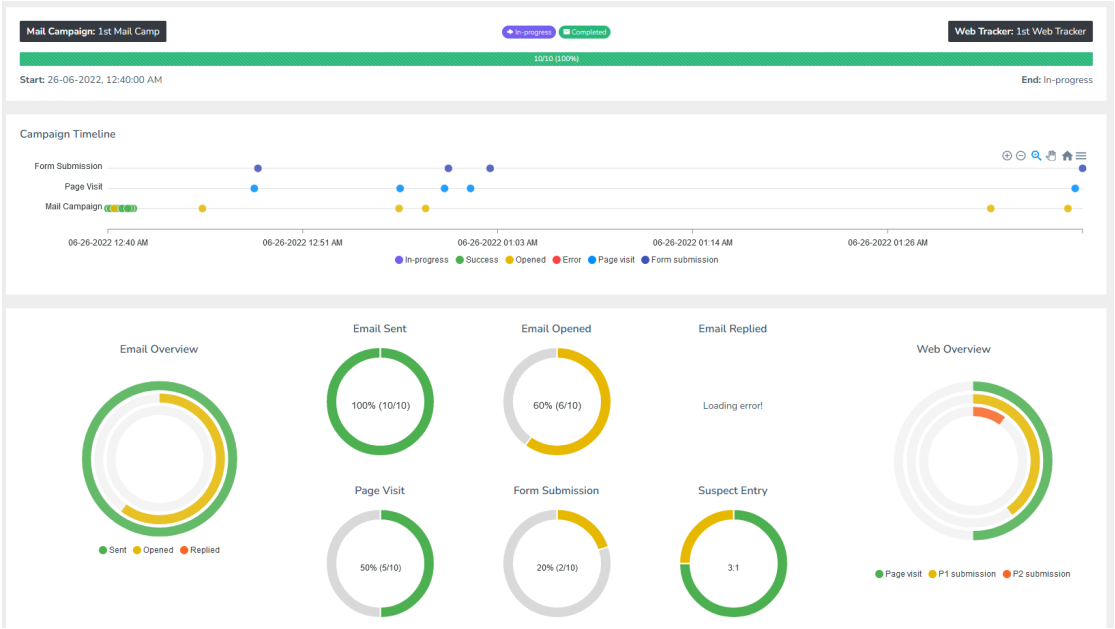
Oba dashboardy (zobrazeny na obrázcích 2.5 a 2.6[4]) ukazují očekávané grafy: status odesílání mailu, počet otevřených mailů. Pro webové kampaně se navíc ukazuje kolik lidí navštívilo web a kolik zadalo data. Nejenom to, ale i na kolika stránkách zadali ona data, pokud je webový tracker více-formulářový. Jako další graf je zobrazeno i kolik účastníků mail nahlásilo (přeposlalo na patřičnou mailovou adresu). Agregaci některých dat, včetně skupin jde teoreticky udělat s pomocí trackerů, ale je to taková obezlička. Výsledky kampaní lze vyexportovat do CSV, XLS nebo PDF, nicméně pro PDF se export, v porovnání s webovým pohledem, tváří jen jako nedomyšlená nadstavba CSV.

Veškerou dodatečnou konfiguraci je možné dělat ve webovém portálu.



Obrázek 2.5 Emailový dashboard programu SniperPhish.

[4]Snímek pořízen z online dema Sniperphish, k dispozici na: `https://demo2.sniperphish.com/spear/`



(a) Grafy dashboardu

SN	RID	Name	Email	Status	Sent Time	Mail Open	Public IP (W)	Browser	Platform (W)	Country (W)	Page Visit	Form Submission	Page-1 Submission	Page-2 Submission
1	2brpqszmjk	Jon Snow	john@demo2.sniperphish.com	Sent	26-06-2022, 12:40:00 AM	✓	84.39.112.158	Chrome 87.0.4280.77	iOS 13.3	Switzerland	✓	✓	✓	✗
2	3tmwb1r9jg	Eddard Stark	eddard@demo2.sniperphish.com	Sent	26-06-2022, 12:41:32 AM	✗					✗	✗	✗	✗
3	7o4q6yhbgp	Khal	1testacc01@gmail.com	Sent	26-06-2022, 12:40:21 AM	✓	157.46.174.194	Chrome 103.0.0.0	Android 12	India	✓	✓	✓	✗
4	hgnje7uckm	Cersei Lannister	cersei@demo2.sniperphish.com	Sent	26-06-2022, 12:40:41 AM	✗					✗	✗	✗	✗
5	me2pjuclih	Joffrey Baratheon	joffrey@demo2.sniperphish.com	Sent	26-06-2022, 12:40:31 AM	✗					✗	✗	✗	✗

(b) Ukázka sesbíraných detailů, část 1

Email	Status	Sent Time	Mail Open	Public IP (W)	Browser	Platform (W)	Country (W)	Page Visit	Form Submission	Page-1 Submission	Page-2 Submission	Field-uname	Field-cellphone	Field-dob	Field-age_grp
john@demo2.sniperphish.com	Sent	26-06-2022, 12:40:00 AM	✓	84.39.112.158	Chrome 87.0.4280.77	iOS 13.3	Switzerland	✓	✓	✓	✗	John	9425142564		
eddard@demo2.sniperphish.com	Sent	26-06-2022, 12:41:32 AM	✗					✗	✗	✗	✗				
1testacc01@gmail.com	Sent	26-06-2022, 12:40:21 AM	✓	157.46.174.194	Chrome 103.0.0.0	Android 12	India	✓	✓	✓	✗	TestName	0980980987		
cersei@demo2.sniperphish.com	Sent	26-06-2022, 12:40:41 AM	✗					✗	✗	✗	✗				
joffrey@demo2.sniperphish.com	Sent	26-06-2022, 12:40:31 AM	✗					✗	✗	✗	✗				

(c) Ukázka sesbíraných detailů, část 2

Obrázek 2.6 Webový dashboard programu SniperPhish.

2.3.8.14 King Phisher

Program byl nasazován nejprve na Kali, později na Ubuntu. Při instalaci došlo k obtížím. Nejprve starý postgres, který spouští při instalaci interaktivní dialog, který se nezobrazí. Poté nešlo nainstalovat virtuální Python prostředí na Kali (instalace na Kali má být podporovaná). Nejprve selhalo shromažďování závislostí, pak neznámé parametry a po manuální opravě skriptu několik nesmyslných chyb. Rady z internetu nebyly použitelné, konkrétně instalace chybějících ez_tools (které jsou obstarožní od roku 2004), nebo aktualizace některých balíků (všechny aktuální). Poté, co jsem „opravil“ všechny hlášené chyby, se pro změnu instalace pokoušela nainstalovat něco, co vypadalo jako náhodný alfanumerický řetězec. Po těchto problémech jsem se rozhodl změnit distribuci.

Virtuální prostředí Ubuntu alespoň okamžitě nevypisovalo chyby. Rychlá instalace sice selhala, ale po semi-manuálním nastavení prostředí se služba úspěšně spustila. První nastavení se píše dovnitř instalačního skriptu nebo je možné instalaci provést interaktivně.

King Phisher je první aplikace, která přichází s vlastním klientem. Lokalizace uživatelského rozhraní není podporována, vyjma webové šablony, kterou dokáže naklonovat.

Odesílání emailu vyžaduje URL serveru (tj. lokace, kde se bude nacházet vstupní stránka), předmět, šablonu emailu, příloha, a příjemce (nebo seznam příjemců). Velkou silou King Phisheru je specializovaný šablonový engine Jinja2. Obojí, email i stránky (pokud je použit hosting skrz aplikaci) jej mohou používat. Ve zkratce, Jinja poskytuje skriptovací jazyk uvnitř těchto maker. Díky tomu umožňuje jak to, co dělají ostatní manažery, ale mnohem víc. Uvnitř emailových zpráv (včetně předmětu) jsou k dispozici následující proměnné:

- jméno společnosti
- uid účastníka
- jméno účastníka
- příjmení účastníka
- email účastníka
- email odesílatele
- jméno odesílatele (alias)
- hodnota pole „odpověď na“
- url
- url bez uid parametru
- url trackeru
- předformátovaný tracker (HTML <img>)
- náhodný alfanumerický řetězec
- typ zprávy
- cesta k šabloně
- atd.

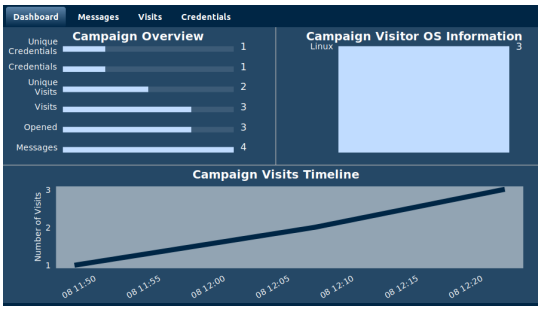
Zmíněné věci jsou ale pouze proměnné, díky potenciálu enginu je možné vložit datum, čas, libovolnou doménu, uživatelská jména. Lze takto sestavit nejen celý mail, ale i stránku pomocí rozdílných sekcí v závislosti na proměnných.

Program neposkytuje sdílený seznam příjemců pro danou společnost. Import lze provést až po vytvoření kampaně, probíhá skrze CSV soubor, který má pouze sloupce pro jméno, příjmení, emailovou adresu a volitelně oddělení.

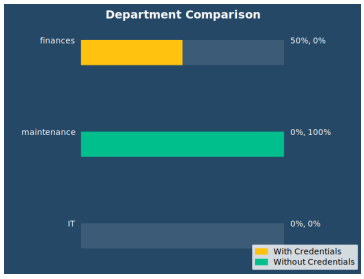
Kampaně se vytváří po přihlášení, kdy se otevře okno vytváření kampaně. Zde lze zadat jméno, popis a typ kampaně. Pro každou z nich se také zadávají údaje společnosti, pro kterou je kampaň dělána. Buď můžeme vytvořit novou, vybrat existující nebo také žádnou nepřiřadit. V rámci pokročilého nastavení se zadávají regulární výrazy, kterými se validují údaje zadané na vstupní stránce. Též tu lze zvolit datum konce kampaně. Po uzavření okna je možné nahlédnou do průzkumníku kampaní. Na to, že účelem programu je poskytovat kampaně více subjektům, tak se v průzkumníku nachází tristní množství filtrovacích možností.

Jednoduchost tvorby kampaně splňuje hodnocení 4/4.

Zobrazení dat není tak barevné jako jiné manažery, ale ukazuje několik rozdílných informací. Grafy a detaily kampaně jsou zobrazeny na obrázku 2.7. Všechny výsledky lze porovnávat s ostatními kampaněmi. Můžeme porovnávat nejenom výsledky, ale i síly hesel, časy návštěv či info o operačním systému, geolokaci, aj. Všechny grafy je možné exportovat, ale jsou to jenom grafy, nikoli celá zpráva.



(a) Souhrnné grafy kampaně. Popisky od shora dolů: unikátních přihl. údajů, přihl. údajů, unikátních návštěv, návštěv, otevřeno, zpráv. Na grafu dole zobrazen počet návštěv skrz čas. V pravo nahoře se vyskytují grafy operačních systémů.



(b) Porovnání v závislosti na odděleních.

Email Address	Submitted	Validation	Username	Password	MFA Token
ex.ample@ubuntu.local	2024-03-08 12:21:41		ex.ample	passwrd	

(c) Ukázka sesbíraných detailů.

Email Address	IP Address	Visit Count	Visitor User Agent	Visitor Location	First Visit	Last Visit
ex.ample@ubuntu.local	127.0.0.1	1	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:123.0) Gecko/20100101 Firefox/123.0	N/A (Loopback)	2024-03-08 11:48:26	2024-03-08 11:48:26
olaf.bjornson@ubuntu.local	127.0.0.1	1	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:123.0) Gecko/20100101 Firefox/123.0	N/A (Loopback)	2024-03-08 12:06:52	2024-03-08 12:06:52
ex.ample@ubuntu.local	127.0.0.1	2	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:123.0) Gecko/20100101 Firefox/123.0	N/A (Loopback)	2024-03-08 12:21:25	2024-03-08 12:21:41

(d) Záznamy o návštěvách stránek.

Obrázek 2.7 Souhrn kampaně programu KingPhisher.

2.3.8.15 Phishing Frenzy

Nasazování probíhalo nejprve na Ubuntu, později jsem zkoušel archivovaný docker kontejner. Dokumentace programu je nekompletní, jelikož originální web je mimo provoz od začátku roku 2022. Phishing Frenzy běží na velmi staré verzi ruby (2.3) a na staré verzi rails (4.2 - EOL 2020). Proto podobně jako u jakéhokoli jiného zastaralého software se daly očekávat problémy s instalací. V tomto případě se problémy týkaly závislostí rails a nastavení Sidekiq služby (který sám o sobě není designovaný jako služba, navíc musí být spouštěn jako root). Od spouštění

Sidekiqu jako služby jsem upustil, jelikož neustálé restarty působily vysokou zátěž CPU. Samotná konfigurace nebyla obtížná, zahrnovala pouze vyplnění správných údajů pro databázi a službu Sidekiq v adresáři `config`.

Lokalizaci podporují jenom šablony, díky klonovacímu nástroji. Phishing Frenzy sice obsahuje nějaké lokalizační soubory, ale nepokrývají celý software.

Šablony emailů jsou textové soubory. Nějaká makra jsou podporována, nicméně pokud oficiální dokumentace někdy uváděla všechna, pak se jednalo o obrázky k jejichž archivaci nedošlo. Mohu uvést s jistotou, ty které byly nalezeny ve dvou předpřipravených šablonách Phishing Frenzy.

- uid účastníka
- email odesílatele
- jméno odesílatele
- url
- url sledovacího obrázku
- datum

Šablon je nejspíš podporováno více, ale tato informace by žádala prohledání zdrojového kódu. Jiné programy mají makra zahrnutá přímo v editoru. Který Phishing Frenzy také má, byť se jedná jen o klasický textový editor. Tímto editorem jdou upravovat všechny textové soubory. Makra nejde použít v předmětu zprávy.

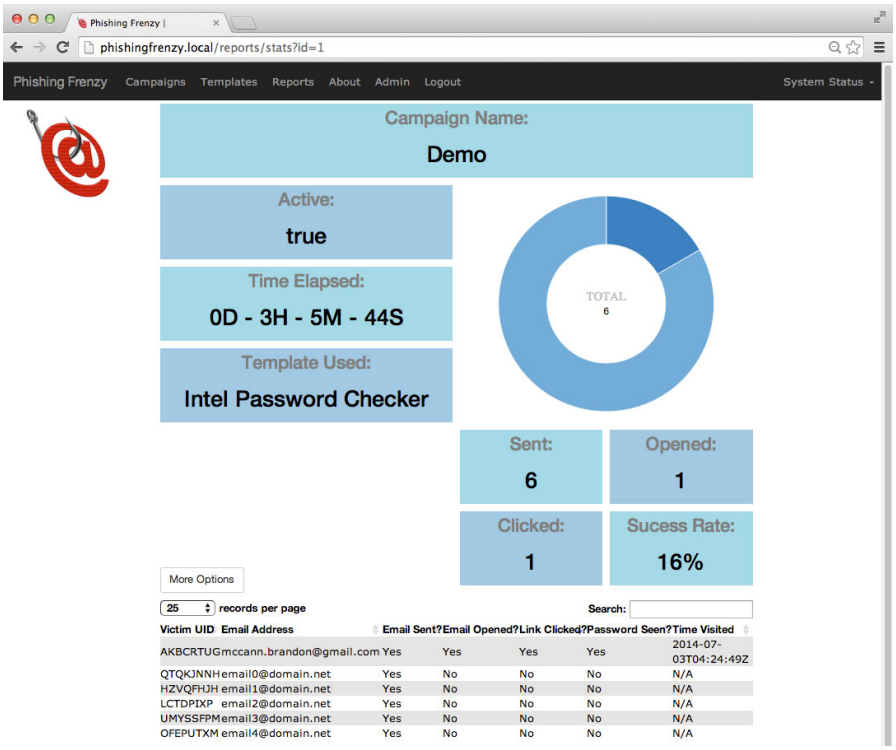
Před začátkem kampaně lze vyplnit jméno, popis kampaně a seznam cílů. Formát pro tuto akci je totožný s CSV, ale vyžaduje překopírování obsahu souboru. Mezi cíli se dá specifikovat, který uživatel bude testovací, tomu bude poslán email nikoli jako součást kampaně, ale mimo, takže se dá otestovat nastavení pro emailový server. Poté je nutné zvolit připravenou šablonu pro kampaň.

Kampaně ve Phishing Frenzy se skládají ze dvou částí, emailu a webové stránky. Při použití Phishing Frenzy nelze hostovat stránky na jiném webovém serveru. Tvorba šablony očekává soubor indexu, takže není možné použít externí stránku. Mysql2 řadič mi po uložení nebo po prohlédnutí náhledu šablony zobrazil chybu. Tohle mohl být problém příliš nové verze MySQL serveru, ale mohu jen hádat, jelikož není jasné, na kterou verzi je software koncipován. Zkoušel jsem i vyměnit mysql2 řadič na nejnovější verzi pro danou verzi ruby, aby případně povolil její použití, nicméně to také nefungovalo. Při druhém pokusu, který se odehrával na Docker kontejneru, už vytvoření šablony vyšlo.

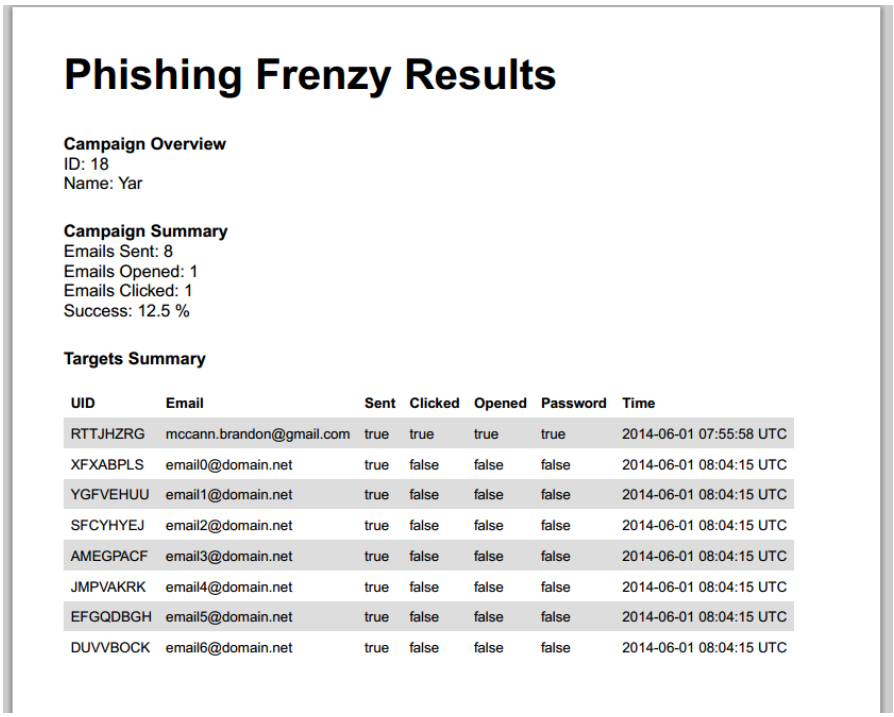
Tady končí to co mohu na software ověřit. Testovací email odešel bez problému, ale kampaň se nedokázala spustit, při obou pokusech selhal tento krok na databázi. Proto nelze říct jak vypadají výsledky kampaně ani nejde pořádně posoudit funkčnost šablon. Protože weby těchto šablon se bez kampaně neaktivují.

Podle prozkoumaných informací a vlastností by měla být jednoduchost tvorby kampaně 4/4. Kvůli problémům, ale nelze plně ověřit tento poznatek.

Historická data ukazují, že má, nebo alespoň měl software vizualizaci i PDF exporty (viz. obrázky 2.8, 2.9). Hodnocení v souhrnných tabulkách je odvozeno z dostupných veřejných snímků obrazovky.



Obrázek 2.8 Historický obrázek vizualizace výsledků ve Phishing Frenzy. [95]



Phishing Frenzy Results

Campaign Overview
ID: 18
Name: Yar

Campaign Summary
Emails Sent: 8
Emails Opened: 1
Emails Clicked: 1
Success: 12.5 %

Targets Summary

UID	Email	Sent	Clicked	Opened	Password	Time
RTTJHZRG	mccann.brandon@gmail.com	true	true	true	true	2014-06-01 07:55:58 UTC
XFXABPLS	email0@domain.net	true	false	false	false	2014-06-01 08:04:15 UTC
YGFVEHUU	email1@domain.net	true	false	false	false	2014-06-01 08:04:15 UTC
SFCYHYEJ	email2@domain.net	true	false	false	false	2014-06-01 08:04:15 UTC
AMEGPACF	email3@domain.net	true	false	false	false	2014-06-01 08:04:15 UTC
JMPVAKRK	email4@domain.net	true	false	false	false	2014-06-01 08:04:15 UTC
EFGQDBGH	email5@domain.net	true	false	false	false	2014-06-01 08:04:15 UTC
DUVVBOCK	email6@domain.net	true	false	false	false	2014-06-01 08:04:15 UTC

Obrázek 2.9 Zpráva vygenerovaná z výsledků Phishing Frenzy. [96]

2.3.8.16 The Social-Engineer Toolkit

SET je součástí výchozí instalace Kali, a jelikož má svůj vlastní balík, tak je instalace velmi snadná. Zkoušena byla verze 8.0.3 Maverick. Program se ovládá pomocí interaktivní konzole. Kromě toho jde program konfigurovat pomocí souboru s pomocí automatizačního modulu. Hlavní důvod proč byl program přidán do sezamu, bylo ověřit zda by šlo některou ze součástí využít pro modrý tým. Ze seznamu útoků následují moduly, které jsou pro tento cíl do nějaké míry použitelné.

Přímo použitelné

Mass Mailer - Odesílá mail, což je všechno co modul dělá. Funguje dobře, ale určitě existuje lepší nástroj, kterým odesílat mail. Šablony jsou limitovány na to, co jde napsat v HTML - žádné placeholdery (makra), jen jednoduchý klient. Můžeme přidat i přílohu.

Password Harvester - Naklonuje stránku, nebo využije šablony, ze které po odeslání formuláře uloží POST data. Na konci vygeneruje zprávu.

Web Jaking Attack - Nejprve vyrobí vstupní stránku, s „reálným“ webem, který uživateli oznámí, že byl web přesunut na novou URL, ta odkazuje na Password Harvesterem naklonovaný podvrh. Přesměrování je v tomto případě dostatečně rychlé na to, aby uživatel ve zmatení zadal do nové stránky údaje.

Potenciálně použitelné

Spear Phishing - Dovoluje otestovat, zda uživatel otevře kontaminovanou přílohu. Vyžaduje aby nebyl přítomen antivirus (protože pochybuju, že přítomné ochrany jsou dostatečně silné na to, aby útok prošel).

Full Screen Attack - Po kliknutí na link pod falešnou záminku se uživatel dostane na stránku, která okamžitě přejde do fullscreen módu, čímž skryje adresový řádek. Tento útok lze použít pouze na dvou šablonových stránkách, nebo na reálných webech, které mají zranitelnost vůči XSS. Využívání zranitelností nelze praktikovat jako modrý tým.

Tabnabbing Attack - Velmi situační, pro lidi, kteří na webu mají otevřeno mnoho záložek a často mezi nimi přepínají. Nejprve předstírá načítání, a když cíl přepne záložku, změní vzezření, tak aby to vypadlo, že ho reálná stránka odhlásila.

QRCode Generator - Nástroj, který vygeneruje QR kód pro phishingovou stránku.

SET Automation - Dovoluje generovat útoky ne-interaktivně.

Lokalizace šablon díky klonování není problém, software ale sám o sobě lokalizaci nepodporuje.

Šablona se umístí do složky `/root/.set`. Upravit ji můžeme jen s pomocí externího editoru. Vytváření i úprava emailové předlohy je čistě textovým způsobem. Jelikož jsem již zmiňoval jiný software, který používal klonování, musel jsem otestovat jeho kvalitu. Nejprve jsem zkusil naklonovat přihlašovací stránku Facebooku, portál FiercePhish, poté portál SniperPhish. Kvalita se různila, facebook vypadal v pořádku, klon FiercePhish webu nejprve selhal a vypadal jako prosté HTML bez stylů, další pokus už ale vypadal správně. Zde se domnívám, že při prvním pokusu jsem nepoužil protokol HTTPS a proto došlo k nějakému problému. Portál SniperPhish by se dal splést s tím reálným, ale u některých ikony neměly správné znaky. Důležité je, že klonování funguje.

Cíle se importují přes CSV, kategorizaci program nijak neřeší.

Kampaň je potřeba realizovat s pomocí několika modulů, ale je možné tak učinit. Přesto by jednoduchost tvorby kampaně byla obdržela hodnocení 2/4, jelikož program sice sbírá výsledky, ale nijak je neagreguje.

Sám o sobě software nic nevizualizuje. Pro každý útok existuje generace zprávy, nicméně jde v podstatě jen o XML log provedeného útoku, který je možný dále zpracovat.

2.3.8.17 SpeedPhish Framework

Program byl nasazován na Kali, bez problémů. Program se ovládá pomocí interaktivní konzole. Konfigurační soubor má v programu zahrnuté výchozí nastavení, ale je intuitivně vyplnitelné.

Lokalizace je k dispozici pouze pro naklonované šablony.

Šablony mailu jsou velmi omezené, nicméně každá stránka přichází se svou vlastní šablonou. To může být užitečné i nepraktické, záleží na použití. Uvnitř šablon lze použít jediné makro - `[[target]]`, které vloží do textu URL phishingového webu. S emailovou zprávou lze poslat nejvýše jednu přílohu.

Webová část poskytuje klasické šablony, zobrazené v seznamu stejně jako u ostatních programů na seznamu. Na rozdíl od nich, ale nejsou výběry šablon tvrdě zakódovány a je možné vložit vlastní. Program má klonovací funkcionalitu, ta ale funguje snad nejzvláštněji ze všech přítomných variant. Nejprve se pokusí najít doménu v DNS, pokud ji nalezne, zkusí je spárovat s již přítomnými šablonami. K tomu používá profily, s nějakými indikátory, pokud toto selže, ale na stránce se nachází formulář, pak stránku naklonuje. Nelze klonovat stránky webů, které nemají záznam v DNS. Klonování stránek lze spustit manuálně, použil jsem ji na FiercePhish portál, což vyprodukovalo dobrou kopii. Korektní nasazení stránky jde otestovat za pomoci simulačního módu.

SpeedPhish nabízí crawler, jenž dokáže prohledat web za účelem nacházení emailů. Tohle může být užitečné pro oba týmy, hlavně pro červený, pokud nevědí jak vypadá organizační struktura dané společnosti. Obecně to v takových situacích dělá hledání příjemců obtížným. Každý nalezený mail je poté přidán do seznamu příjemců. Je možné přidat vlastní, ten se importuje skrze CSV soubor.

Kategorizaci cílů SpeedPhish nenabízí. Kampaň začíná odesláním mailu, a trvá do ukončení programu. Jednoduchost tvorby kampaně odpovídá hodnocení 2/4, jelikož program sice sbírá výsledky, ale nijak je neagreguje.

Sbíraná data nejsou nijak vizualizována. Na konci každé kampaně SpeedPhish vygeneruje HTML zprávy pro každou phishing stránku. Jméno stránky v tomto reportu občas zmiňuje předchozí hodnotu domény. Tato zpráva obsahuje odeslaný email (který se ale většinou nepropíše), porovnávající foto obou stran - phishing i originálu (které ovšem většinou nejsou vygenerovány korektně) a ukořistěné údaje.

2.3.8.18 Gophish

Gophish v0.12.1 byl nasazován na Kali, kde Gophish přichází jako součást systémového prostředí. Na linuxových, nebo jiných široce používaných systémech (Win, OSX) poskytuje Gophish binární soubor. Stačí jej spustit. Konfigurace databáze, adres a portů se provádějí skrze soubor config.json. Zbytek, jako je nastavení emailového serveru, je řešen skrze webové UI.

Lokalizace je podporována čistě pro klonované stránky.

Emailové předlohy se tvoří pomocí rich text editoru. Jako jediný manažer dovoluje specifikovat odesílatele v šabloně. Tento odesílatel bude specifikován jako odesílatel v těle obálky (rozdílná hodnota od odesílatele v nastavení může způsobit zachycení spam filtrem). Jsou podporovány následující makra:

- uid účastníka
- jméno účastníka

- příjmení účastníka
- pozice účastníka
- email účastníka
- email odesílatele
- URL sledovacího obrázku
- HTML sledovacího obrázku
- phishing URL
- phishing URL bez uid

Obrázkový tracker nelze přizpůsobit. K mailům můžete přidat libovolný počet příloh, kdy všechny makra dostupná v editoru, můžeme použít v podporovaných typech příloh, obecně v textových dokumentech, ale i wordových. Takto se dají kontrolovat otevírání infikovaných příloh. Ale pozor, toto sledování není odlišené od kliknutí na odkaz. Pokud tedy chceme zkoumat samotné otevření přílohy, je potřeba udělat to pro separátní kampaň.

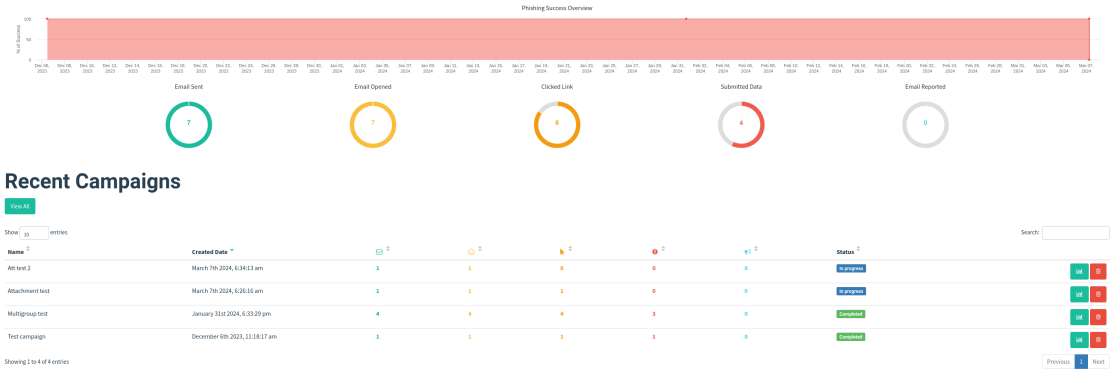
Pro editaci webových šablon nabízí rich text editor, HTML pohled ale i náhled. Při tvorbě lze využít výše zmíněné šablony. Gophish nabízí klonovací nástroj, který stránku nakopíruje do příslušného textového pole, které poskytuje funkcionalitu WYSIWYG editoru. Pokud se tedy klonování nezdaří, je to napohled jasné, načež můžete udělat úpravu. Na této stránce software dovoluje ukládat formulářová data, speciálně lze zachytávat i hesla, kde jako jediný software varuje, že ukládá potenciálně citlivá data do databáze v nehashované podobě.

Cíloví uživatelé se přidávají přes skupiny. Buď lze manuálně zadat jméno, příjmení, email a pozici nebo si lze podle stáhnutelné šablony importujeme CSV soubor. Zadané cíle nelze exportovat, což může být problém v případě rychlých záloh (tedy, když nechceme dělat zálohu celé databáze).

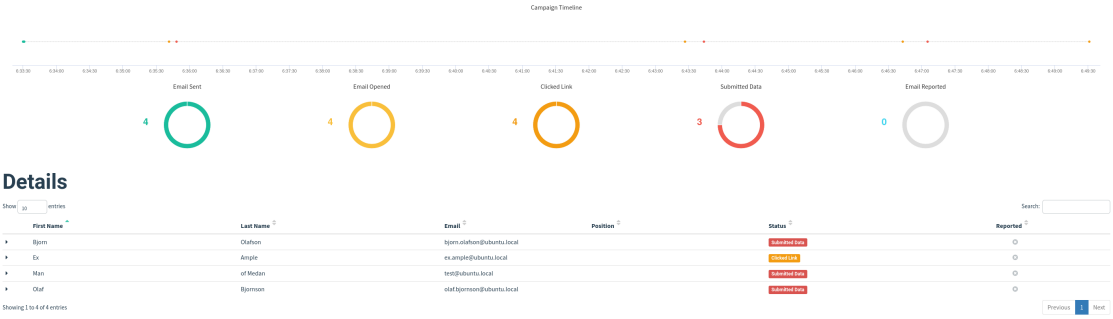
Pro vytvoření kampaně vybereme šablonu, odesílací profil (i zde lze využít testovací email, s již vyplněnou šablonou), vyplníme URL (lokace dosažitelná cílovými uživateli, která odkazuje na Gophish; důležité je součástí URL napsat protokol, jinak mohou emailoví klienti selhat v interpretaci). Na této URL se bude nacházet vstupní stránka. Pak ještě vybereme vstupní stránku, specifikujeme čas a dobu začátku, případně do kdy odeslat emaily. Ve finále vybereme skupiny kterým mail odeslat. Tento krok (více skupin na jednu kampaň) sice má od LDAPové struktury daleko, ale jedná se rozhodně o krok kupředu.

Jednoduchost tvorby kampaně pro Gophish odpovídá 4/4, program zjednodušuje všechny podstatné kroky simulace.

V dashboardu se dá vidět agregovaná úspěšnost kampaní, společně s agregovanými čísly kolika lidem se mail odeslal, kolik lidí mail otevřelo, atd. Tento přehled je vidět na obrázku 2.10. Každá kampaň sleduje otevírání emailů, prokliknutí, sbírání údajů. Taktéž lze nastavit adresu, na kterou mají být nahlašovány podezřelé maily, tato statistika je taktéž zobrazena. Nasbíraná data můžeme exportovat pouze do CSV. V grafech je též zobrazena časová linie událostí (jak rychle někdo interagoval s webem). Celý detail kampaně je vidět na obrázku 2.11. Kromě exportu CSV nemá v základu žádné jiné formy tvorby zprávy.



Obrázek 2.10 Přehled programu Gophish.



(a) Souhrnné grafy kampaně s uživatelskými detaily.

(b) Časová linie individuálního cíle.

Obrázek 2.11 Detaily kampaně programu Gophish.

2.3.8.19 Phishingator

Pro testování jsem používal verzi 1.5. Manuál pro nasazení nespecifikuje kompatibilní systémy, pouze se odvolává na použití docker kontejneru. K dispozici jsou dva typy, pro vývoj a pro produkci. Pokud bych chtěl Phishingátor nasadit čistě na virtuální stroj nebo zcela bez virtualizace, pak si musím konfiguraci získat z docker obrazu. Očekával jsem, že když je aplikace v kontejneru, tak bude plně připravena pro provoz. To jest s úpravou vzorového konfiguračního souboru.

Ze vzorového souboru není zcela jasné, co je nutné vyplnit pro minimální funkci. Tou zde rozumím zobrazení portálu. Manuál pro správu svádí v sekci testovací instance [97] ke čtyřem, nicméně je potřeba vyplnit 20 položek (což je zhruba polovina .env souboru). Na to, že je s aplikací docker compose soubor, tak je potřeba připsat adresu správného hostitele databáze (která se ve vzorovém env souboru nevyskytuje). Aplikace je tak spjatá s LDAPem, že vyžaduje před zprovozněním vyplnit platné LDAP údaje. Přestože se autor pokusil vytvořit docker obraz openLDAPu, v současném stavu není dokončen, ani neposkytuje vzor struktury, kterou Phishingator požaduje (nebo jak s ní pracovat). Určitou oporu poskytuje soubor config.PHP, ke kterému je v manuálu krátce referováno, v něm existuje poměrně uspokojivé množství komentářů. Na můj vkus by tyto komentáře nejspíš měly být už v env souboru.

Pokud se nezdaří připojení k databázi (což je velmi možné ve výchozí konfiguraci), aplikace se snaží pokračovat.

Kromě okamžité funkce LDAP, požaduje aplikace také funkční SSO. SSO není součástí obrazů. Pro tento účel jsem využil fake OIDC server, který poskytuje Cesnet v jednom z jejich repositářů. Předchozí pokusy o obcházení OIDC skončily chybou HTTP 500. Chyby aplikace jsou skryté, nicméně nejedná se o bezpečnostní opatření, souvisí to s tím, jak celá aplikace řeší chyby. Skrytí chyb dále může komplikovat počáteční konfiguraci. Díky použití docker kontejneru je jednodušší si chyby zobrazit oproti dohledávání logů uvnitř kontejneru. Aplikace sice má svou vlastní dobře přístupnou log složku, do které se zapisují očekávané chyby, pokud se ovšem jedná o chybu neočekávanou, tak se log do této složky nezapíše a je třeba jej hledat ve výchozí složce.

Práce s doménami LDAPů není zcela uspokojivá (viz. 2.1), jelikož Phishingator vždy bere jako doménu vrchní dvě. Pro určité případy toto není vhodné, jelikož pokud někdo chce omezit přístup pouze pro specifickou poddoménu vyšších řádů, tak to nebude možné, taktéž pokud je používána pouze doména prvního řádu.

Vytváření mailu je v pořádku. Líbí se mi zvýrazňování maker (jako potvrzení, že jsou správně zadaná), nápovědy pro rozpoznávání phishingu jsou také pěkně udělané. Hlavní nedostatek bych viděl v nedostatečné kvantitě emailových maker. Máme k dispozici pouze:

- uživatelské jméno účastníka
- email účastníka
- datum (2 varianty)
- phishing URL

Chybí jméno i příjmení, takže možnosti z hlediska více cílené kampaně s vyšší mírou důvěryhodnosti jsou celkem omezené. Je otázka proč to není možné, když jsou data načítána z LDAPu, kde určitě tyto údaje jsou, na druhou stranu rozumím, že možná autorovi bylo řečeno, že dostane na ověření účet, jenž bude mít k dispozici čtení pouze uživatelského jména a emailu. K emailu nelze přidat přílohu.

Vytváření s úpravou samotných webových šablon je k dispozici pouze přes externí editor.

Import cílů probíhá buď skrz textový soubor nebo je lze vybrat ze systému. Tento výběr můžete učinit za určitých, mně zcela neznámých, podmínek (zde uznávám, že konfigurace openLDAP uživatelů nejspíš nebyla zcela podle toho, co by Phishingator očekával). Každý email je ověřen vůči LDAPu. Pokud mail v LDAP neexistuje, je ze seznamu po rozeslání kampaně vyřazen (takto může klidně vzniknout i kampaň o nula uživatelích, což validace pole cílů sama o sobě zakazuje).

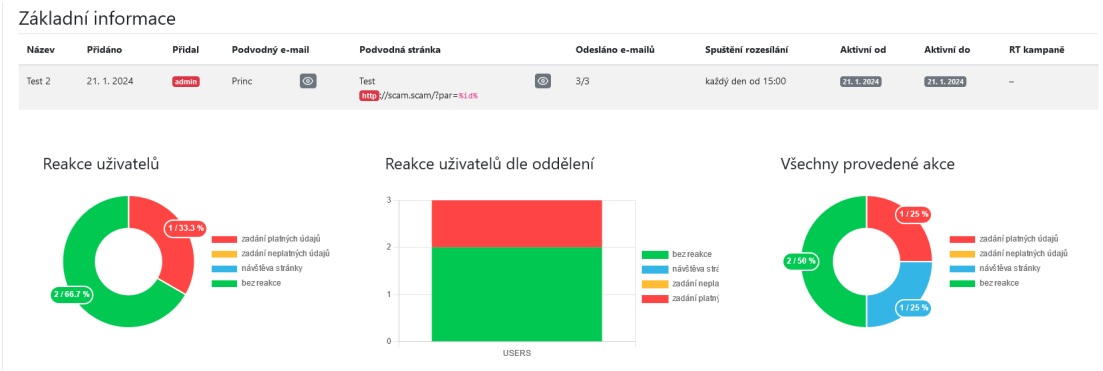
Výpis kódu 2.1 Problematický kód zúžený na čistě podstatné části. Kódy ze souborů respektive: globalFunctions.PHP:132 [98], PermissionsModel: 73, 86 [99]

```
function get_domain_from_url($url) {
    $domain = parse_url($url, PHP_URL_HOST);
    $secondLevelDomain = null;

    if ($domain != null) {
                $hostNames = explode('.', $domain);

                if (count($hostNames) >= 2) {
                        $secondLevelDomain = $hostNames[count($hostNames) -
                            2] . '.' . $hostNames[count($hostNames) - 1];
                }
    }

    return $secondLevelDomain;
}

private function isRemoteUserFromOrganization($identity) {
        return get_domain_from_url('https://' . get_email_part($identity, '
            domain')) == getenv('ORG_DOMAIN');
}

public function login($identity) {
        $identity = $this->getRemoteUser($identity);

        ...

        if (!$this->isRemoteUserFromOrganization($identity)) {
                Logger::error('The user identity provided by SSO does not
                    match this Phishingator instance.', $identity);

                echo 'Jste přihlášeni jinou identitou, která nespadá do
                    organizace ' . Controller::escapeOutput(getenv('
                    ORG_DOMAIN')) . '. Odhlaste se, prosím, a přihlaste
                    správnou identitou.';
                exit();
        }

        ...
}
```

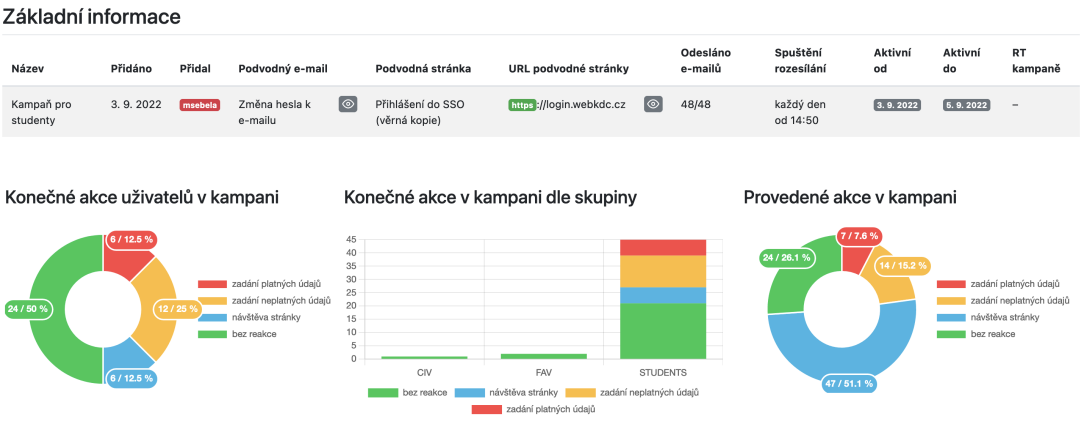
Samotné kampaně fungují dobře. Pro tvorbu se volí název, případně číslo ticketu (v libovolném systému), šablona emailu, webová stránka, datum začátku a konce. Minimální délka kampaně je den. Předčasné ukončení kampaně není podporováno. Dále umožňuje vložit účastníky kampaně. Krom toho, se zde volí jak mají být zadané údaje ověřovány, respektive jaká má být reakce na jejich zadání. Spuštění kampaně dokáže odeslat notifikace o kampani na email.

Jednoduchost vytváření kampaně spadá dle definice na 3/4, čistě jelikož nepodporuje přílohy a vyžaduje phishing pomocí URL. Bez těchto dvou požadavků by se jednalo o hodnocení 4/4.

Pokud je nakonfigurováno správně LDAP prostředí, pak se ukazují podrobné grafy o úspěšnosti dle oddělení, včetně agregované úspěšnosti, viz. obr. 2.12. Phishingator sleduje odeslání emailu (pouze souhrnně), návštěvu stránky nebo zadání údajů, kde jsou děleny na platné a neplatné. Taktéž máme záznamy o událostech přístupů. Exporty výsledků jsou pouze samotné grafy úspěšnosti, žádné pokročilé přehledy.



(a) Souhrnné grafy kampaně ve Phishingatoru - můj nejlepší pokus.



(b) Souhrnné grafy kampaně ve Phishingatoru - ukázkový snímek [100].

Obrázek 2.12 Dashboard kampaně programu Phishingator.

2.4 Metodika hodnocení - technická stránka

Technická stránka popisuje vlastnosti, které se netýkají tolik samotné uživatelsské interakce. Různá nastavení a funkce spojené s konfigurací, či vlastnosti, které nemusejí mít přímou grafickou reprezentaci. Taktéž je toto hodnocení spíše kvantitativní, kdy lepší bude takový program, který poskytuje více.

Pro účely shrnutí má každá kategorie svojí zkratku podle anglického jména. Kategorie jsou

rozesílání emailových zpráv ((E)mail sending), sledování stavu ((T)racking), hosting phishingového webu ((H)osting), moduly a api ((M)odules and (A)pi).

2.4.1 Rozesílání emailových zpráv (E)

Připravenou zprávu je potřeba rozeslat, pro to musí program vědět, kam mail poslat. Aplikace pro účel kampaní by určitě měla zvládat připravené zprávy odesílat na předem stanovený emailový server. Mít připravenou šablonu bez možnosti mail odeslat přímo ze systému by znamenalo zbytečný dodatečný krok, byť se tak v praxi někdy odesílají.

Pokud by jsme zpravovali více subjektů, pak můžeme mít několik emailových serverů, na které budeme chtít emaily odesílat. Každý může mít také své vlastní nastavení. Tedy vlastně jde o mailové profily. Při nejlepším by měla poskytovat všemožná nastavení pro daný server, šifrování komunikace, autentizace aj. Tato nastavení by měla zjednodušit připojení k mailovému serveru, a tím třeba i snížit čas věnovaný konfigurací.

Programy ze seznamu mají různé množství dalších menších vlastností, které nelze vyjádřit pomocí stručného souhrnu. Především protože každý má něco sobě specifického. Proto jsem do této části zahrnul pouze ty vlastnosti, které nás mohou zajímat univerzálně. Jak dokáže program zabezpečit komunikaci, zda je podporováno anonymní přihlášení, zda můžeme tvořit emailové profily a ve finále ochranu proti zahlcení.

Zabezpečení komunikace (E1)

Auto - Režim zabezpečení se vyjedná na základě módů podporovaných serverem. Vetšinou se nejspíš bude jednat o metodu starttls, ale není to jisté.

Manuál - Režim zabezpečení se dá nastavit. Konkrétně si označme trojici možných metod:

1. Žádné - pro komunikaci není použito žádné šifrování.
2. Starttls - klient zavolá starttls aby započal šifrovanou komunikaci.
3. SMTPs - klient se připojuje rovnou skrze šifrovaný kanál.

Přednastavené - Režim zabezpečení je stanoven programem, nelze jej změnit mimo úpravu kódu.

Podpora anonymního přihlášení (E2) Určuje zda nás program na mail server připojí i pokud nastavovaný server nevyžaduje žádného uživatele.

Emailové profily (E3) Určuje, zda program dokáže pracovat s více emailovými servery.

Ochrana proti zahlcení (E4) Jelikož pro poslední dva stupně hodnocení se může hodit vědět, která možnost je přítomna v daném programu, bude u hodnocení specifikováno v závorce, kterou vlastnost program má: A (absolutní limit počtu zpráv), D (interval mezi zprávami), R (počet emailů za časový interval).

Vícestupňová - Systém dokáže limitovat absolutní počet zpráv, specifikovat interval mezi zprávami a limitovat počet mailů za časový interval.

Pokročilá - Systém dokáže alespoň dvě z následujících: limitovat absolutní počet zpráv, specifikovat interval mezi zprávami nebo limitovat počet mailů za časový interval.

Základní - Systém dokáže buď limitovat absolutní počet zpráv, specifikovat interval mezi zprávami, nebo limitovat počet mailů za časový interval.

2.4.2 Sledování stavu (T)

Sledování stavu je z technické strany kampaně nezbytné, jelikož se vlastně jedná o samotné výsledky, který by takový software měl poskytovat. Pokud by nám zobrazil čistě výsledek o úspěšném odeslání, tak nezískáme žádná cenná data. Proto by ideální software měl na konci kampaně být schopen odpovídat na následující otázky:

Byla kampaň úspěšně a plně rozeslána? (T1) Systém by měl podávat informace o stavu odeslání, pokud se podařilo nebo jestli v některých případech selhalo. Díky těmto informacím lze posléze nezdařené odeslání vyřešit.

Otevřela oběť email? (T2) Bez tohoto údaje data o navštívení webu nemusí být směrodatná, jelikož pokud si cíl kampaně ani nevšiml mailu ve schránce, nemohl logicky ani navštívit odkázaný web.

Navštívila oběť phishingový web? (T3) Říká nám informaci o tom, zda cíl prozkoumal cílový web. Sama o sobě není tato statistika vypovídající, nicméně poskytuje nám indicii, že je uživatel potenciálně zranitelný vůči zero-day prohlížečovým útokům.

Interagovala oběť s phishingem? (T4) Interakce už na rozdíl od navštívení webu je více vypovídající, neboť nám dokládá, že je cíl dostatečně zvědavý na to, aby s potenciálně nebezpečným obsahem do určité míry spolupracoval. Stejně jako u navštívení, máme data pro případ zero-day zranitelnosti, ale zároveň se do této kategorie počítá zadání jakýchkoli (i chybných) údajů do polí. To, že se na první pohled odešlou dvě pole (s třeba falešnými údaji), nemusí nutně znamenat, že uživatel nechtěně neodeslal nějakou část dat nějakého intranetového nechráněného webu přes skrytý iframe.

Nechala oběť uniknout své systémové údaje? (T5) Toto vypovídá o odeslání svých platných přihlašovacích údajů. Taková akce je nejvíc alarmující, jelikož takto by útočník dokázal získat přístup do sítě či vnitřních nástrojů.

2.4.3 Hosting phishingového webu (H)

Phishingová kampaň obvykle zahrnuje phishingový web, na který vás email přesměruje. Tento požadavek není univerzální, jelikož existují útočníci, kteří budou chtít po zaměstnanci otevřít přílohu nebo mu pošlou instrukce bez jakýchkoli odkazů a příloh. Pokud ale plánujeme sesbírat data o webovém nasazení, potřebujeme web. Jelikož tvorba samotné stránky už byla prozkoumána, zaměřím se v této kapitole na hosting webu, nebo alespoň vstupní stránky (angl. landing page, stránka na kterou mail odkáže, většinou přihlašovací stránka). Přestože tato vlastnost šetří čas, může tato iniciativa být i na škodu, jelikož mnohdy klade specifické požadavky na server, kde probíhá nasazení samotného programu.

Typ hostovaného webu (H1) Phishingovým webem označuji vlastnost, se kterou dokáže hostovat hned sadu stránek s jejich možným prolinkováním, kdy není potřeba hostovat každou stránku zvlášť. Specifičtěji, není potřeba vytvářet novou kampaň, aby se daly prolinkovat.

3 - Systém dokáže pro kampaň vytvořit hosting phishingového webu i phishingové stránky. Pro každý hostovaný web poskytuje vlastní konfiguraci.

2 - Systém dokáže pro kampaň vytvořit hosting phishingového webu i phishingové stránky. Konfigurace webu není možná nebo je nastavitelná hromadně.

1 - Systém dokáže pro kampaň vytvořit hosting phishingové stránky.

0 - Systém hostování nezajišťuje.

Úzká integrace (H2) Úzce integrované hostingy vyžadují jejich využití, tj. nelze si zvolit hostování na jiném stroji, než na kterém je software nasazen.

2.4.4 Moduly a API (MA)

Každý software se dokáže stát mnohem lepším, pokud dovoluje svým uživatelům rozšířit funkcionalitu nezávisle na originálním autoru. Každý teoreticky může upravit zdrojový kód původního projektu, ale to není způsob, kterým by většina lidí program modifikovala. Hlavním prostupem pro modifikaci by měla být nějaká tvorba modulů. Kromě modulů existuje druhá cesta, tou je API, které dává stejnou moc jako modularizace, jenom přidané vlastnosti nepřijdou zevnitř aplikace ale z vnějšku.

Pro účely hodnocení bude v tabulce uvedeno M pro modul, respektive A pro API.

2.4.5 Zhodnocení z technické stránky

Z technického hlediska jsou některé aplikace poměrně vyrovnané. Nejvíc napřed by se dal označit SniperPhish, který jako jediný poskytuje vícestupňovou ochranu proti zahlcení, neváže se úzce na specifický hosting a dokáže sbírat data ze vzdálených serverů. Nedaleko se umístil Gophish s aplikací KingPhisher, jenž oba poskytují API, díky čemuž by v některých případech mohly dohnat SniperPhish v některých vlastnostech. Dále pak máme Phishingator, a naposledy Phishing Frenzy. Jak je patrné z tabulek 2.3, 2.4, tak byly programy celkem vyrovnané.

Samozřejmě čistě hostingové programy se nemohly s plnohodnotnými manažery rovnat. Z této kategorie vychází nejlépe SpeedPhish Framework, těsně za ním The Social Engineering Toolkit. Zbytek, především čistě hostovacího software, je na tom v podstatě stejně.

Proxy nástroje samozřejmě také nemohly dostihnout manažery, takže na pohled vlastnostně jsou na tom téměř totožně.

Software \ Vlastnost	E1	E2	E3	E4
SayCheese	n/a			n/a
ShellPhish	n/a			n/a
SocialFish	přednastavené			n/a
CredSniper	n/a			n/a
FiercePhish	manuál 12	x		jednoduchá R
Muraena	n/a			n/a
PhishInSuits	n/a			n/a
SquarePhish	manuál 123			n/a
HiddenEye	n/a			n/a
Evilginx2	n/a			n/a
Zphisher	n/a			n/a
SniperPhish	auto		x	vícestupňová
King Phisher	manuál 13	x		jednoduchá R
Phishing Frenzy	manuál 12	x		jednoduchá D
The SET	auto	x		jednoduchá D
SPF	auto	x		pokročilá AD
Gophish	auto		x	pokročilá DR
Phishingator	manuál 1*2	x*		pokročilá DR

* - Nefunguje díky specifické vlastnosti knihovny.

Tabulka 2.3 Souhrnná tabulka rozesílání zpráv.

Software \ Vlastnost	T1	T2	T3	T4	T5	H1	H2	MA
SayCheese			x			2/3	x	
ShellPhish				x		2/3	x	
SocialFish				x		1/3	x	
CredSniper				x		2/3	x	MA
FiercePhish	x[a]					0/3		
Muraena			x	x	x	3/3[c]		M
PhishInSuits				x		0/3	x	
SquarePhish				x		0/3	x	
HiddenEye				x		2/3	x	
Evilginx2			x	x	x	3/3[c]		
Zphisher				x		2/3	x	
SniperPhish	x[a]	x[b]	x	x		2/3		
King Phisher	x[a]	x	x	x		3/3	x	MA
Phishing Frenzy	x[a]	?	?	?		3/3	x	
The SET				x		3/3	x	M
SPF			x	x		3/3	x	
Gophish	x[a]	x	x	x		2/3[d]	x	A
Phishingator	x[a]		x	x	x	3/3	x	

a - Software hlídá pouze úspěšné přijetí serverem.
b - Backend skript není připraven na kódování (quoted printables) odesílaných emailů.
c - Jelikož funguje jako proxy, prolinkování je implicitní.
d - Hosting více stránek je možný, ale je určen k hostování statických zdrojů.

Tabulka 2.4 Souhrnná tabulka sledování stavu.

2.4.5.1 SayCheese

SayCheese s emailovými zprávami nepracuje.

Jelikož hostuje a sbírá některé údaje, dokáže identifikovat, že cíl navštívil web pomocí průkazového foto, které pořídí při návštěvě. Na většině prohlížečů ale žádá oprávnění používat kameru, bez které je pořízen proud černých snímků. Vedle foto sbírá i IP adresu a user-agent cíle.

Hostovat zvládne jeden celý PHP web s globálním nastavením.

Moduly, ani API neposkytuje.

Z hlediska vlastností mimo samotného focení podporuje v rámci hostování dvoje tunelovací služby - servero a ngrok, ngrok ale není z důvodu změny API funkční. Spuštění čistě na lokálním serveru (bez tunelu) bohužel není k dispozici. Pro reálné nasazení by bylo nutné zrušit pořizování záznamu, pokud je kamera zakázaná, nebo nějak kontrolovat, že snímek není černý.

2.4.5.2 ShellPhish

Shellphish neprovádí rozesílání emailových zpráv.

Dokáže určit, že cíl navštívil web a odeslal nějaké údaje, čímž interagoval s webem. Údaje u sebe ale nemají evidované, ze které IP adresy nebo z jakého user-agentu přišly, takže je obtížné spárovat návštěvy s interakcemi.

Shellphish využívá jednoduchý PHP server, mezi jednotlivými stránkami šablony jde odkazovat, ale nedává přístup k podrobnější konfiguraci. Aplikace se po shromáždění údajů jednoho cíle ukončí, čímž si omezuje použitelnost.

Software neposkytuje ani moduly, ani API.

Vlastnostně nenabízí mnoho: jediný tunel - ngrok, bez něj aplikaci nespustíme. Navíc není tunel připraven na změny ngrok API, díky čemuž spojení fungovat nebude (ale samotný ShellPhish ano). Jedná se o PHP server na který je nasazena šablona. Hosting nelze nijak přenastavit nebo upravit.

2.4.5.3 SocialFish

SocialFish podporuje posílání mailů, jedná se ale o nedodělanou vlastnost. Zaprvé nelze poslat email více jak jednomu příjemci. Za druhé, uživatel který mail odesílá musí být ten, který se bude přihlašovat na mailový server. Server lze zadat jen jeden. To téměř nikdy není žádoucí. Neautentizované přihlášení není podporováno. Pro připojení je vždy použit příkaz strarttls. Díky tomu že posílá vždy právě jeden email nemusí řešit ochranu proti zahlcení.

Ze sesbíraných údajů dokáže určit pouze zda cíl interagoval s webem (navštívení sleduje pouze jako agregovanou statistiku).

Program hostuje pouze phishingovou stránku.

Kromě vložení BeEF háčků, dokáže s pomocí dat sesbíraných phishingem na stanici oběti provést sken portů. Zatímco tyto vlastnosti jsou dobré pro červené týmy, pro účely této práce se nejedná o klíčové vlastnosti. Mezi další malé plusy patří vlastní mobilní aplikace, přihlášení přes qr kód a případný ngrok tunel (tato poslední vlastnost je jen pro starší verzi SocialFish).

2.4.5.4 CredSniper

Aplikace neřeší odesílání emailů.

Zaznamenává IP adresu, lokaci cíle i user-agent. Díky tomu dokáže utrčit zda cíl interagoval s webem, ale činí tak až těsně před ukončením phishingu, nedokáže proto určit jen samotné navštívení.

Hostování dokáže obsluhovat web o více stránkách, nicméně lze jej konfigurovat pouze globálně.

Credsniper nabízí vytváření vlastních modulů, tyto moduly jsou v podstatě jen další weby. Kdy kód těchto modulů slouží právě pro obcházení autentizace. API nabízí cílové body pro: sesbírané údaje, označení údajů a upravení konfigurace.

2.4.5.5 FiercePhish

Pro zabezpečení emailové komunikace lze zvolit mezi starttls příkazem a žádným ověřením. Ochrana proti zahlcení se sestává z limitu mailů za interval, a nastavuje se skrze kampaň.

Aplikace sleduje pouze zda byly emaily úspěšně rozeslány.

Ostatní data musejí být sbírána externě, jelikož neposkytuje hostování phishingového webu.

Moduly ani API nenabízí.

Pro testování dokáže zobrazit emailovou schránku. Další celkem užitečná vlastnost týkající-se emailů je kontrola DNS záznamů. S pomocí tohoto nástroje se dá ověřit, že přijímající SMTP server zprávy nezahodí jako spam už na základě třeba požadavku DKIM.

Data je možné zálohovat pomocí dedikovaných tlačítek, které poskytují export databáze. Dále je možné v portálu zobrazit logy (tato vlastnost občas nefunguje).

FiercePhish má management uživatelů, ale jedná se jen o administrátorské účty. Každý účet může využívat dvoufaktorové autentizace. Pro vytvoření nového účtu vyžaduje telefonní číslo, nicméně tento nedostatek vypadá spíše jako chyba. Formát navíc není kompatibilní s evropskými čísly.

2.4.5.6 Muraena

Jelikož se jedná o proxy, nezabývá se rozesíláním emailových zpráv.

Dokáže určit zda cíl navštívil web, zda s ním interagoval, i zda zadal platné údaje.

Hosting funguje na bázi proxy, tedy nastavení se netýká statického obsahu. Ten ale také dokáže hostovat, nicméně jej není možné příliš podrobně konfigurovat.

Muraena má vyjma proxy několik dalších modulů. Modul pro telegram, kde dokáže zprostředkovat notifikace. Watchdog, který zabezpečuje pravidla pro připojení (s jeho pomocí se dá zařídit whitelisting a blacklisting). A ve finále necrobrowser. Což je nástroj, který masivně zrychluje práci s ukradenými relacemi. Mělo by se jednat o prohlížeč bez grafického rozhraní, který dokáže automatizovat práci s ukradenou session. Tak lze měnit hesla, rušit notifikace, vytěžit emailovou schránku, atd. [101]

Muraena umí prohledávání hlavičky i těla požadavku, v dané části zprávy dokáže hledat podle regexu. Pomocí regexu dokáže výraz i nahradit. Muraena funguje jak nad HTTPS tak nad HTTP. První konfiguraci si dokáže vytvořit pomocí automatického webového crawleru. Jinak má vlastnosti co se od proxy dají čekat.

Pro velmi detailní souhrn vlastností této proxy bych musel strávit s nástrojem mnohonásobně vyšší míru času. Tento celkem stručný seznam vlastností proto nelze brát jako limit toho, co nástroj umí.

2.4.5.7 PhishInSuits

Tento software posílá čistě SMS.

Sám o sobě dokáže zjistit, zda uživatel interagoval, ani ne nutně s webem, ale s phishingovou zprávou.

Phishingový web aplikace nezajišťuje.

Moduly ani API nejsou součástí.

Z technického pohledu je nedostatkem hlavně použití služby Twilio. To je využito z důvodu SMS, které jsou zde hlavním nosičem phishingové zprávy. Pro jakékoli nasazení v praxi by musel být upraven kód, buď pro podporu emailu nebo vlastního SMS poskytovatele. Teoreticky je tento skript schopen načíst uživatelská data z cloudu, s pomocí definovaných graphAPI koncových bodů, což se může hodit, nicméně ne pro účely této práce.

2.4.5.8 SquarePhish

Na rozdíl od PhishInSuits, poskytuje SquarePhish více nastavení. Jelikož je email již plně podporován, program dovoluje využít více typů zabezpečení komunikace, jak smtps, starttls tak kompletně bez šifrování.

Sám o sobě dokáže zjistit, zda uživatel interagoval s phishingovou zprávou.

Aplikace sice hostuje jednu stránku, nicméně se jedná pouze o jeden krátký krok procesu a není určena pro phishing, ani se tak nepoužívá. Pro tuto stránku jde specifikovat certifikát.

Moduly ani API neposkytuje.

SquarePhish na rozdíl od PhishInSuits neposílá požadavky na koncový bod hned od počátku, čeká až oběť naskenuje QR kód z mobilního telefonu, takže nehrozí vypršení platnosti požadavku. Jediná věc, která zůstala je bohužel vazba na Microsoft API koncový bod.

2.4.5.9 HiddenEye

Sofware phishingové zprávy nerozesílá.

HiddenEye dokáže určit pouze zda cíl s webem interagoval. Dvě speciálních šablony, dovolují získat od cíle lokaci.

Lokální PHP hosting nemá přenastavitelné parametry. HiddenEye podporuje několik tunelovacích služeb: ngrok, servero, localxpose, localtunnel, openport, pagekite, localhost.run a cloudflared. Jejich funkčnost je sporná, program tvrdí, že nejsou aktuálně dostupné, kód pro ně ale existuje. Jediná služba, která je podle aplikace funkční, je ngrok. Lokální hostování podporuje pouze HTTP.

Moduly ani API program nemá.

HiddenEye může pro každou šablonu aktivovat extra vlastnosti. Konkrétně keylogger, falešnou cloudflare obrazovku a posílání výsledků na email. Mimo samotný hosting umožňuje odeslat emaily s výsledky, bohužel je tento modul limitován pouze na gmail, při čemž modifikace parametrů není interaktivní (řešená přes konfigurační soubor).

2.4.5.10 Evilginx2

Evilginx2 s emailovými zprávami nepracuje.

Stejně jako Muraena dokáže určit zda cíl navštívil web, interagoval s ním, i zda zadal platné údaje.

Hosting funguje na bázi proxy. Je také schopen provozovat vlastní statický obsah.

Tvorbu klasických modulů nepodporuje, ani nemá API.

Nepodporuje HTTP, i když je pochopitelné, že na stránky pod čistým HTTP na webu už moc často nenajdeme. Dokumentace říká, že nelze použít vlastní certifikát, proto jsem musel buď použít certifikát let's encrypt nebo ten vygenerovaný programem. Na druhou stranu, pro účely integrace jsem stejně tuto podporu nepotřeboval, protože pointou je naučit uživatele rozpoznávat certifikáty.

Až na neúspěch s localhostem (viz. 2.3.8.11), vidím v integraci potenciál. Vypadá, jako že má více možností než Muraena. Pro začátek podporuje více souběžných konfigurací na jeden server. Skrze *návnady* lze vytvářet libovolné cookies a parametry, které lze později využít. Je skrze ně možná i určitá filtrace (například skrze user agenty). Má přímočařejší ochrany proti skenování: blacklisting, whitelisting nebo outbound proxy. Sběr dat vypadá taktéž jednodušeji na pochopení. Hlavně je jasnější, jak využít ukořistěnou session. *Phishlety* mají mnoho nastavení: přihlašovací tokeny v hlavičce požadavku, tělu i cookie (všechny podporují regulární výrazy). Sbírání je podporováno i pro JSON. *Force post*, který nastaví hodnotu pole bez vědomí uživatele (i zde je podporován regex). Dále je možné injektovat javascript. Navíc má určitě ještě další nezmíněné vlastnosti, protože je ani nebylo možné v krátkém časovém rámci projít všechny.

2.4.5.11 Zphisher

Aplikace emailové zprávy neodesílá.

Program si ukládá přihlašovací údaje uživatelů, kteří s webem interagovali společně s IP adresou a user-agentem.

Dokáže hostovat celý web s jedním nastavením na lokálním stroji, ale podporuje pouze HTTP.

Nepodporuje moduly, ani nemá API.

Vyjma běhu bez tunelu, podporuje dva poskytovatele: cloudflared a localxpose. Nejen, že pro ně má podporu, ale nabízí k nim i interaktivní přihlášení. Konfigurace webu zahrnuje pouze číslo portu.

2.4.5.12 SniperPhish

Posílání mailu funguje bez problému. Funkčnost spojení lze otestovat pomocí příhodného tlačítka, jenž pošle testovací zprávu. Pro nastavení emailu jsou zde seznamy odesílatelů, společně s konfigurací zpráv. Seznam odesílatelů obsahuje pole pro autentizaci k emailovému serveru (rozpoznání je děláno automaticky), dále volbu odesílatele. Anonymní přihlášení není podporováno. Konfigurace zpráv obsahuje dodatečná nastavení pro odeslané zprávy: šifrování, podepisování, typ příjemce (TO, CC, BCC), prioritu, potvrzení přečtení nebo podporu IDN znaků v emailové adrese. Program má vícestupňovou ochranu proti zahlcení - kolik emailů poslat zároveň, jaký limit bude na počet poslaných zpráv a specifikace mezery mezi odchozí poštou.

Podstatnou vlastností SniperPhishe jsou sledovací prvky, které lze vkládat do phishingových webů. Komunikují s backendem, kterému poskytují různé typy informací. Rychlé trackery jsou jenom neviditelné obrázky, plné mohou poskytovat i obsah polí. Takto může aplikace sledovat nejen stav odeslání mailů a jejich otevření, ale i navštívení webu, interakci s webem nebo dokonce

zvládne ověřovat únik skutečných údajů. Tento poslední sledovač ale nelze počítat pro přehled, jelikož by zahrnoval dopsání podstatnější části kódu.

SniperPhish dokáže hostovat vlastní soubory. Lze nahrát libovolné soubory, vstupní stránky nebo libovolný webový soubor. Stránky na sebe mohou bez problémů odkazovat, přestože jejich tvorba je individuální. Samotný web nelze nijak konfigurovat. Generace plnohodnotných trackerů dává k dispozici kód, který lze vložit do dané stránky. Tímto se aplikace zbavuje úzké vazby na hostovaný web, stačí využít kód sledovacího prvku a přidat jej na libovolný server.

Aplikace nepracuje s moduly, ani s API.

Jednu věc kterou jsem zaznamenal o sledovacích prvcích v mailu, je že používají tzv. *double quoted printables*. Trackovací backend ale s tímto kódováním nepočítá. Díky tomu se v mailu obrázek nezobrazí (tento problém by šlo opravit, kdyby byla použita specializovaná třída emailu, alternativně úprava sledovacího skriptu na detekci quoted printables). Po lokální úpravě HTML už SniperPhish sledoval otevření mailu korektně.

V poslední řadě má SniperPhish jednoduchou administraci, kde se dají vytvářet noví administrátoři.

2.4.5.13 King Phisher

Pro kampaň lze specifikovat adresu odesílatele, jak bude zpráva adresována (TO, CC, BCC), prioritu ale i její citlivost. Kromě klasické emailové zprávy můžeme poslat pozvánku do kalendáře. Přihlašování k SMTP serveru probíhá přes předvolby a podporuje jak autentizovaný, tak anonymní SSL nebo nešifrovaný provoz. Program dovoluje specifikovat pouze kolik je maximální počet odchozích zpráv za interval (není jasné jaký to je interval). King Phisher by měl mít integrovanou kontrolu SPF, nikde jsem ale nenašel prvek, který by kontrolu provedl (je možné že se provádí automaticky).

Sledování webů provádí skrz speciální, dynamicky generovaný kp.js soubor. Tedy jedná se o podobnou techniku jako užitkuje SniperPhish. Tady skript přímo sbírá zadaná data. Po tom, co uživatel projde takovou stránkou, lze přidat přesměrování na naučnou stránku, kde se může dozvědět o svém zúčastnění v kampani nebo lze do hostované stránky přímo *embeddovat* youtube video. Kromě specializovaných sledovačů, dokáže kontrolovat otevření a odesílání emailů.

Hostování stránek je jediný způsob jak získat pokročilé statistiky (kp.js nelze použít mimo King Phisher, jelikož se sestavuje dynamicky). Hostovat lze jednu nebo více stránek (jde použít vhosts). Konfigurace je velmi blízká Apache. Procházet celou konfiguraci mi přijde nadbytečné, ale zmíním alespoň *require_id*, pokud zůstane toto nastavení ve výchozí hodnotě, pak se stránka nezobrazí bez korektní hodnoty argumentu HTTP GET požadavku. Do webu může King Phisher přidat BeEF háčky. Další extra vlastností je klonování stránek, které mi ale nefungovalo.

Aplikace poskytuje několik API, především GraphQL a RPC. REST je spíše doplňující. Do aplikace lze dodávat pluginy.

2.4.5.14 Phishing Frenzy

SMTP nastavení obsahuje všechna potřebná pole, zahrnuje autentizační metody (včetně žádné), podporuje šifrování komunikace přes TLS. Dá se dokonce ověřovat skrz Open SSL. Není zde možnost podepisování nebo šifrování zpráv. ani nelze zvolit v jakém poli se má objevit náš příjemce. Jediná ochrana proti zahlcení je zde interval do další zprávy.

Z toho co se mi podařilo zprovoznit, Phishing Frenzy zvládá zjistit, zda jsou emaily odeslány, měl by zvládat sledování otevřeného emailu, a historická data ukazují, že by měl umožňovat i sledování návštěv a sbírání údajů.

Hlavní idea za Phishing Frenzy je využívání Apache virtuálních hostitelů. Díky tomuto nastavení se může chovat podobně jako King Phisher, kdy do každého hostingu vloží svůj kód, díky kterému se dají sbírat pokročilá data. Na každou šablonu lze přiložit webovou stránku, email a obrázek. Pokud nemáme stránku k dispozici, je možné využít klonovače stránek. Bohužel user

agent, který slouží pro tento účel je zastaralý, na některých stránkách selže, protože nevyužívá TLS, na jiných (youtube konkrétně) je upozorněn, že prohlížeč není podporován. Výsledkem klonovače je HTML soubor, který je možné stáhnout a následně nahrát. Phishing Frenzy dokáže do webů vložit háčky pro BeEF.

Program nemá moduly, ani API.

Program má formu metasploit integrace.

2.4.5.15 The Social-Engineer Toolkit

Odesílání emailů nenabízí mnoho možností. Typ šifrování je rozhodnut automaticky, ale podporuje anonymní přístup. Mezi odchozími maily dovoluje nastavit pauzu.

SET sleduje odeslané formuláře, tedy interakci s webem. Návštěvy sice také zaznamenává, ale jedná se čistě o poznámku o návštěvě, nejde o plnohodnotné sledování (pro tento cíl by bylo potřeba aktivovat Apache a podívat se do jeho přístupových logů).

Hosting můžeme nasadit jak přes HTTP, tak HTTPS. Pro zprovoznění serveru je možné použít Apache, a tím zpřístupnit pokročilejší nastavení webu.

API neprovozuje, ale operuje skrze několik modulů.

Samotný SET má ještě mnoho dalších vlastností, kterým jsem nevěnoval velkou pozornost, jelikož se jedná především o moduly určené pro červený tým. Jde hlavně o spoustu různých payloadů a metod útoku. Dále má také integraci Metasploitu.

2.4.5.16 SpeedPhish Framework

Ochrana proti návalu emailů je dělána jednoduše - limituje maximální počet emailů, společně s pauzou. Pokud cílíte na specifickou doménu, SPF se pokusí nalézt SMTP server pomocí MX záznamů v DNS. Tuto vlastnost lze vypnout specifikací vlastního SMTP serveru. Program neumožňuje specifikovat jakým způsobem proběhne výměna hesel, taktéž nemá k dispozici žádné TLS možnosti (tato část doslova chybí ve zdrojovém kódu). Pokud tedy není použit specificky gmail.

SpeedPhish sleduje zda uživatel navštívil stránku, i zda na s ní interagoval. Tyto údaje vypisuje i do logového souboru.

Pro korektní funkci webu je potřeba opravit regulární výraz na začátku souboru web.py. Tohle by mohl být problém způsobený špatnou verzí Pythonu. Server vypisuje chyby do konzole, včetně varování o zastarání, ale zapomíná sdělovat, že přestože konfigurace stanovuje port, na kterém má aplikace běžet, tak se ve skutečnosti spustí na portech začínajících na 8000. Když je web spuštěn napřímo, tak server toto varování vypíše. Hosting dokáže přesměrovávat specifické adresy a adresové rozmezí. Dokáže používat virtuální hostitele.

Nemá moduly, ani API.

Hosting dále nabízí keylogger, uživatelské sledování (pomocí cookie) a integraci BeEF. Dále se program integruje s programem Harvester, který se používá pro prohledávání DNS. Kdysi SPF uměl získávat certifikát skrze certbota, ale tato funkcionalita je momentálně nefunkční (v kódu zakomentovaná). Aplikace zvládá také hostovat vlastní SMB server.

2.4.5.17 Gophish

Odesílání emailů vyžaduje vytvoření profilu. Tady se konfiguruje SMTP, každý profil lze pojmenovat. Jde tu nastavit kdo bude odesílatel v SMTP obálce, adresu hostitele, uživatelské jméno a heslo. Můžeme zaškrtnout ignorování chyb certifikátů. Finálně lze přidat vlastní emailové hlavičky. Určitou možnou nevýhodou přítomných nastavení spočívá v jejich automatickém nastavení. Balík, který zprostředkovává práci s mailem používá textproto, aby od serveru zjistil, co používá za nastavení. Není jisté co se stane, kdyby server takovou informaci neposkytl. Výchozí chování podporuje anonymní přihlášení. Přímo profil nám nabízí odesílání testovacího mailu. Ochrana před zahlcením je pouze jednoduchá, umožňující v rámci kampaně zadat nepřímo

pauzu mezi odchozími zprávami, kdy se program pokusí odeslat emaily do určitého termínu rovnoměrně rozprostřené.

Gophish sleduje otevírání emailů, prokliknutí i sbírání údajů. Taktéž lze nastavit adresu, na kterou mají být nahlašovány podezřelé maily.

Hostovat dokáže jednu vstupní stránku na kampaň, kromě toho jdou hostovat ještě statické zdroje (ty nelze na server nahrát skrze webové rozhraní), nicméně ty jsou pro použití poněkud neflexibilní. Žádnou další konfiguraci hostingu nedovoluje.

Gophish podporuje webhooks a REST API. Webhooks fungují pouze směrem ven, tedy odesílají informace na požadovanou adresu. Nemají filtrování, odesílány jsou vždy všechny události. Oproti ostatním kategoriím tohoto software, nejsou webhooks oddělené pro každého uživatele. Moduly neposkytuje.

Správa uživatelů Gophish má 2 skupiny, uživatel může pouze vytvářet kampaně, cíle, šablony nebo profily. Admin potom navíc může obstarávat správu uživatelů nebo webhooků. Uživatelé (ani administrátoři) mezi sebou nesdílí cíle, šablony, kampaně ani profily (toto chování je možné obejít pomocí API).

2.4.5.18 Phishingator

Posílání mailů může narazit na problém, pokud není používané TLS. Sice by samotný program ničemu bránit neměl (v konfiguraci se dá TLS „vypnout“), nicméně knihovna PHPMailer má ve výchozím nastavení zapnutou funkci autotls, pokud server TLS podporuje, bez ohledu na to jestli je TLS zvolené jako možnost přenosu, je použito TLS. Po manuální opravě, umí jak šifrovaný, tak nešifrovaný přenos. Také podporuje anonymní přihlášení. Aplikace má pokročilou ochranu proti zahlcení, kdy můžeme zvolit pauzu mezi emaily a počet emailů odeslaných po zvolené pauze. Po spuštění kampaně může notifikovat administrátora o jejím zahájením.

Mimo status odesílání emailu, dokáže aplikace sledovat jak navštívení, interakci s webem, tak i zkontrolovat, zda unikly opravdové uživatelské údaje. Pěkná vlastnost šablon je ověřování platnosti hesel. Aplikace podporuje více možných způsobů ověření (LDAP, web, Kerberos, IMAP, policy), ověřování přes LDAP vede na připojení do LDAPu (ldap_bind). To ale nejde jen s pomocí CN, nebo jiného ekvivalentního atributu, připojení bude fungovat pouze pro kompletní DN. Tedy uživatel zadá své CN do pole, ale to není jeho DN, pokud zadá celé DN, aplikace (správně) selže na validaci. Tedy chybí konfigurace pro toto přihlašování. Dá se sice do uživatelského jména přidat předpona a přípona, nicméně jelikož posléze takto upravený řetězec prochází sanitací, tak nebude upravený řetězec validní. Tato funkcionalita nevypadá z principu funkčně, pokud byla testována, pak musela patrně být struktura adresářových služeb vhodně vytvořená (pro relevantní kód viz. 2.2).

Vytváření phishingových stránek není zcela bezproblémové. Můžeme stránku pojmenovat, napsat její URL, vybrat šablonu pro web nebo zvolit název služby šablony (toto pole aplikace zdánlivě nepoužívá). URL musí být registrováno ve Phishingator proxy a aktivní buď v host tabulce nebo DNS. Hosting stránek probíhá na stejném serveru, jako na kterém je umístěna aplikace. Přestože tohle může mít své nevýhody, dává nám tím možnost upravit konfiguraci phishingového webu.

Po aktivaci šablony (tedy započetí kampaně) sice server vyrobí konfiguraci webu, ale už nepřekopíruje šablonu do správné složky (tento krok je nutné udělat manuálně). Nejsou podporovány jiné porty než 80 (a to ani 443 pro HTTPS). Přesměrování na náhled stránky se může chovat podivně - nebylo možné zobrazit náhled přes přímé kliknutí na odkaz, ale až přes nový panel (uznávám, že v tomto případě bych sám netušil, co udělat, abych takové chování opravil). Obecně počet přesměrování dokáže, v některých prohlížečích (MS Edge) způsobit chybu „too many redirects“ (která nebyla způsobena cookies/mezipamětí). Další problémy se mohou objevit díky tomu, že aplikace spoléhá na to, že stránka uživatele přesměruje v moment aplikační chyby. Pokud si potom někdo povolí zobrazování chybových hlášek, namísto přesměrování se začne odesílat HTTP 200, čímž se aplikace jednoduše rozbije.

Výpis kódu 2.2 Funkce testování přihlašovacích údajů přes LDAP společně s kódem funkce connect. Kód ze souborů: CredentialsTesterModel.PHP:64 [102], LdapModel.php:40 [103]

```
private static function tryLdapLogin() {
        $ldap = new LdapModel(false);

        $username = AUTHENTICATION_LDAP_USER_PREFIX . self::$username;

        if (!empty(AUTHENTICATION_LDAP_USER_SUFFIX) && !str_contains(
            $username, AUTHENTICATION_LDAP_USER_SUFFIX)) {
                $username .= AUTHENTICATION_LDAP_USER_SUFFIX;
        }

        $username = ldap_escape($username, '', LDAP_ESCAPE_FILTER);

        $validCreds = $ldap->connect($username, self::$password,
            AUTHENTICATION_LDAP_HOST, AUTHENTICATION_LDAP_PORT, true);

        $ldap->close();

        return $validCreds;
}

public function connect($username = null, $password = null, $hostname = null
    , $port = null, $notLogging = false) {
        $connected = false;
        $ldapBind = false;

        if ($hostname == null) {
                $hostname = LDAP_HOSTNAME;
                $port = LDAP_PORT;
        }

        $this->ldapConnection = ldap_connect($hostname . ':' . $port);

        if ($this->ldapConnection) {
                ldap_set_option($this->ldapConnection,
                    LDAP_OPT_PROTOCOL_VERSION, 3);

                if ($username == null || $password == null) {
                        $username = LDAP_USERNAME;
                        $password = LDAP_PASSWORD;
                }

                $ldapBind = ldap_bind($this->ldapConnection, $username,
                    $password);
        }

        if (!$this->ldapConnection || !$ldapBind) {
                Logger::error('Failed to connect or authenticate to LDAP.',
                    ldap_error($this->ldapConnection));
        }
        else {
                $connected = true;
        }

        return $connected;
}
```

Program nepodporuje moduly, ani nemá API.

Phishingator dává na výběr z trojice oprávnění. První jsou samotné cíle, které se mohou přihlásit nejen k aplikaci, ale také k obdržování phishingu. Tito uživatelé vidí jen své vlastní výsledky. Správce testů může tvořit kampaně a podvodné maily, ale nemůže se podívat skupiny uživatelů. Skupiny se v kontextu Phishingatoru týkají čistě oprávnění, taktéž je lze importovat ze LDAPů. Takto vytvořené skupiny nelze používat jako cíle kampaně!

Přihlašování využívá SSO, jiné způsoby nejsou k dispozici.

2.5 Metodika hodnocení - podniková stránka

V této kapitole jsem zvážil podnikovou perspektivnost. Některé nároky souvisí úzce s technickým provedením, ale hlavně jde o to jak dobře dokáže produkt škálovat. Je to software, který dokáže zabezpečit phishingové akce pro stovky nebo až tisíce uživatelů pro několik, třeba organizačně rozdílných subjektů? Nebo to je aplikace, kde bude problém nasadit systém nad stovkou uživatelů, protože práce s ní bude jinak tak časově a pracovně náročná, že tvorba větších kampaní nebude proveditelná.

Pro účely shrnutí má i v této sekci každá kategorie svojí zkratku podle anglického jména. Kategorie jsou použitelnost pro heterogenní prostředí ((S)ubsidiary (V)iability), a podpora ((Su)pport).

2.5.1 Použitelnost pro heterogenní prostředí (SV)

Většina programů je připravena na situaci, kdy nám stačí provést kampaň čistě pro naší společnost. Problém se může objevit v případě, kdy nechceme kampaň realizovat lokálně, ale využít software k obsloužení několika dalších firem. Nezáleží nutně na tom, jestli se jedná o společnosti dceřiné, nebo společnosti, jenž si za službu zaplatily. Daná organizace potom může očekávat buď detailní přehled podle předdefinovaných skupin, nebo může z rozličných důvodů požadovat protestování konkrétních uživatelů bez třídění.

Není úplně triviální definovat, jakým způsobem by měla být podpora zavedena. Nejvíc toto kritérium souvisí s organizací skupin, ale také nás bude zajímat, jakým způsobem jsou implementovány kampaně. Taktéž bude vhodnější takový program, který zvládne zabezpečit co nejvíce úkonů kampaně. V poslední řadě by se hodilo vkládání specifické hlavičky jako možnost ověření odesílatele.

3 - Tento program dokáže pracovat se složitější organizační strukturou. Konkrétně by měl být schopen definovat cíle pro specifickou společnost se všemi relevantními informacemi, podle kterých se dají uživatelé třídit (organizační skupiny), třebaže je pro takové třídění nutné použít API společně s nástrojem třetí strany. Předchozí vlastnost nesmí přítomnost skupin vyžadovat. Dokáže nějakým způsobem filtrovat kampaně podle společnosti. Program dokáže zabezpečovat celé kampaně od přípravy šablon, po sběr dat (nemusí nutně poskytovat webový hosting). Do odeslaných mailů musí být možnost vložit specifickou hlavičku.

2 - Tento program dokáže pracovat alespoň s plochou organizační strukturou. Cíle můžeme definovat globálně nebo přímo pro kampaň, jejich třídění aplikace nemusí zajišťovat. Dokáže nějakým způsobem filtrovat nebo alespoň seřadit kampaně podle společnosti. Program dokáže zabezpečovat celé kampaně od přípravy šablon, po sběr dat (nemusí nutně poskytovat webový hosting). Do odeslaných mailů musí být možnost vložit specifickou hlavičku.

1 - Program buď nepracuje s organizační strukturou nebo s ní pracuje takovým způsobem, že není schopen akceptovat skupiny mimo organizaci. Program dokáže zabezpečovat celé kampaně od přípravy šablon, po sběr dat (nemusí nutně poskytovat webový hosting).

0 - Program nepracuje s organizační strukturou, ani nezabezpečuje celou kampaň.

2.5.2 Podpora (SU)

Poslední věci, která se váže na podnikovou stranu je podpora. Pokud aplikace už není udržována, nebo delší dobu nebyla aktualizována, pak není možné očekávat opravy chyb. Samozřejmě, to že není software udržovaný neznamená automaticky, že není užitečný. Každopádně u neudržovaných projektů nelze počítat ani s bezpečnostními záplatami, které jsou mnohdy důležitější nežli opravy některých vlastnostních nedostatků. Navíc pokud by někdo nasadil program bez podpory, tak by mu postupně zastarával a je jen otázkou času, než takový software nebude kde nasadit, bez použití starých verzí operačních systémů.

Pod aktualizaci software nespadá dokumentace.

Živá - Podpora software oficiálně neskončila. Zdrojový kód software byl aktualizován (třeba jen na vývojové větvi) v posledním roce.

Údržba - Podpora software oficiálně neskončila. Zdrojový kód software byl aktualizován (třeba jen na vývojové větvi) v posledních dvou letech nebo udržovatel alespoň komunikuje skrze issues a pull requesty.

Opuštená - Podpora software oficiálně neskončila, ale zdrojový kód software už přes dva roky nebyl aktualizován. Autor nijak nekomunikuje skrze issues nebo pull requesty.

EOL - Podpora software buď oficiálně skončila, nebo projekt není oficiálně udržován.

2.5.3 Zhodnocení z podnikové stránky

Z podnikové perspektivy nejlépe vypadá Gophish, který je jako jediný alespoň do určité míry použitelný v heterogenním prostředí. Další máme Sniperphish, který má trochu nižší vhodnost, hlavně kvůli horším schopnostem seskupení uživatelů. Následuje King Phisher, kterému pro změnu už skončila životnost. V tabulce 2.5 se nachází hodnocení všech programů, ale nejvhodnější už jsem zmínil.

Opět se tu nachází skupiny programů, které nemohly dosáhnout dobrého hodnocení. Tyto programy skončily v podstatě všechny stejně, alespoň v kontextu metriky SV (2.5.1), nicméně hodnocení probíhalo podle předem stanovené metodiky a kritérií, a nebylo by vhodné tato kritéria měnit na základě výsledků.

2.5.3.1 SayCheese

Aplikace sama o sobě, není použitelná v heterogenním prostředí už jenom proto, že neposkytuje odesílání emailu. Poslední aktualizace projektu byla v době psaní před pěti lety. Autor zároveň nijak nereaguje na žádné issues nebo pull requesty, takže nelze ani očekávat žádné aktualizace.

2.5.3.2 ShellPhish

Nemohu doporučit jakékoli nasazení, hlavně díky zastaralým šablonám, které byly naposledy aktualizovány před 4 lety. Pro více podniků se nehodí jelikož nezabezpečuje celý proces kampaně. Navíc v době psaní této práce není repozitář suljot/shellphish (mirror originální aplikace) k dispozici, neboť byl z platformy github odstraněn z důvodu porušení podmínek.

2.5.3.3 SocialFish

SocialFish nelze nasadit proti skupinám uživatelů. Obecně má zásadní nedostatky v technické oblasti, hlavně sběr dat a import cílů. Sám o sobě neposkytuje plné kampaně, díky čemuž se nedá použít pro heterogenní prostředí. Software je stále aktivně vyvíjen a proto je možné že se jeho stav vylepší.

Software \ Vlastnost	SV	SU
SayCheese	0/3	opuštená
ShellPhish	0/3	opuštená
SocialFish	0/3	živá
CredSniper	0/3	opuštená
FiercePhish	0/3	živá
Muraena	0/3	živá
PhishInSuits	0/3	opuštená
SquarePhish	0/3	živá
SPT	n/a	EOL
HiddenEye	0/3	údržba
Evilginx2	0/3	živá
Zphisher	0/3	živá
SniperPhish	2/3	živá
King Phisher	2/3	EOL
Phishing Frenzy	1/3	živá*
The SET	1/3	údržba
SPF	1/3	opuštená
Gophish	3/3	živá
Phishingator	1/3	živá

Tabulka 2.5 Souhrnná tabulka podnikových vlastností.

2.5.3.4 CredSniper

V současném stavu není hostovací služba použitelná v žádném prostředí. Software nezabezpečuje proces plné kampaně, proto se tedy nehodí pro heterogenní prostředí. Poslední aktualizace software byla vydána před pěti lety. Od této doby autor software nereaguje na issues ani pull requesty. Software je tedy bez údržby a aktivního rozvoje.

2.5.3.5 FiercePhish

Ve stavu v jakém FiercePhish je, ho rozhodně nelze nasadit do heterogenního prostředí. Kampaně sice zvládne začít, ale nedokáže zabezpečit sběr, ani agregaci dat. Přestože dle stanovených kritérií hodnocení podpory spadá do živé podpory, jednalo se jen o malou aktualizaci, která neměla vliv na využití aplikace.

2.5.3.6 Muraena

Jelikož se jedná pouze o proxy, tak se do heterogenního prostředí pro tvorbu kampaní nehodí. Sama o sobě neposkytuje vlastnosti zajišťující kampaň. Vývoj Muraeny je pořád ještě živý.

2.5.3.7 PhishInSuits

Celou kampaň nezajišťuje, už z tohoto důvodu se nehodí do heterogenního prostředí. Po vytvoření už nebyl dále vyvíjen, a je ponechán od autora ladem.

2.5.3.8 SquarePhish

Stejně jako u předchůdce, není u SquarePhish důvod nasazovat v různorodých podnicích pro účely tvorby phishingové simulace, jelikož nedokáže pomoci s celou kampaní. U software dochází

k aktualizacím, ale ty obsahují pouze malá vylepšení. Nedochází zde k vývoji nových funkci, které by měly na využívání programu velký dopad.

2.5.3.9 Simple Phishing Toolkit

Podle archivovaných stránek není projekt udržován od 31. 7. 2013 [104]. Z těchto důvodů ponechávám Simple Phishing Toolkit bez dalšího zhodnocení, jelikož nasazovat starou, neudržovanou aplikaci, navíc se starými závislostmi není už z principu bezpečné.

2.5.3.10 HiddenEye

HiddenEye nezabezpečuje celou kampaň a proto se nehodí do různorodého prostředí. Původní repozitář se poslední čtyři roky neměnil, a fork použitý pro ozkoušení provádí jen minimální změny, hlavně týkající-se závislostí.

2.5.3.11 Evilginx2

Jelikož se jedná pouze o proxy, tak se do heterogenního prostředí nehodí, jelikož nesplňuje požadavek tvorby celé kampaně. Pokud ovšem hledáte nástroj, který kombinuje tvorbu kampaní s možnostmi proxy nástroje, tedy odchytávání uživatelských sessions a údajů, věrné klonování originálních webů nebo vás zajímá náročnější cvičení pro vaši organizaci, tak autor Evilginx vytvořil nový fork aplikace GoPhish, která v sobě má integraci s nástrojem Evilginx2 [105][106]. Podpora stále trvá, software je pravidelně aktualizován.

2.5.3.12 Zphisher

Zphisher nelze použít v heterogenním prostředí, protože zajišťuje jen málo kroků při tvorbě kampaně. Program bývá čas od času aktualizován, takže zastarání šablon zatím nehrozí.

2.5.3.13 SniperPhish

Z podnikové stránky by bylo dobré mít lepší import skupin s jejich odlišením. Dle mého názoru by SniperPhish mohl být vhodným řešením pro firmy do 500 zaměstnanců. Pro správu více firem se použít dá, ale práce s organizační strukturou může být celkem omezující. Také má několik málo aplikačních chyb, které mohou ztížit aktivní použití. Poslední aktualizace byla před rokem v době psaní, autoři aktuálně nekomunikují skrze issues ani pull requesty, nicméně se nejedná o dostatečně dlouhou dobu, aby se dalo říct, že je software opuštěný.

2.5.3.14 King Phisher

V heterogenním prostředí by se s ním dalo pracovat dalo, ale konfigurace webu pro složitější statistiky nebo filtrování kampaní pro více společností by mohlo představovat problém. Z pohledu údržby se přes dva roky jedná o software po konci životnosti. Pokud přidáme ještě nějaké problémy s nasazením, musím konstatovat že jsou zde lepší volby.

2.5.3.15 Phishing Frenzy

V současném stavu není použitelný - běží na starých závislostech, oficiální dokumentace již není k dispozici a ani archivní instalace není v plně funkčním stavu. Software dostal před několika měsíci aktualizaci. Ta adresovala pouze závislosti programu, tedy nešlo o opravy chyb.

2.5.3.16 The Social-Engineer Toolkit

Program sice dokáže zabezpečit kampaň od začátku do konce, nicméně nepracuje s organizační strukturou. Tento problém může vést na velmi nepohodlnou až pracnou kampaň v případě více podniků. Ukládané údaje v sobě nezahrnují informace o příchozí adrese, ani user-agentu, a proto by nebylo spolehlivě možné odlišit mezi několika různými cíli, natož mezi více organizacemi. SET už přes dva roky neobdržel aktualizaci, nicméně udržovatel nadále reaguje na issues a pull requesty, takže jej nelze klasifikovat jako opuštěný.

2.5.3.17 SpeedPhish Framework

Pro nasazení nad větším počtem uživatelů není vhodný, kvůli technickým nedokonalostem. Kromě technických nedokonalostí nepracuje s organizační strukturou a použití v heterogenním prostředí by bylo pracné. SpeedPhish Framework už roky nebyl aktualizován, autor nijak aktivní u projektu není, takže je projekt aktuálně opuštěný.

2.5.3.18 Gophish

V heterogenním prostředí se jedná asi o nejlepšího kandidáta. Přestože definice účastníků kampaně je daleko od dokonalosti, dělá nejlepší práci na tomto seznamu. Hlavně díky tomu, že se nedostatky dají alespoň z části překlenout pomocí API (pozor, překlenutí není nutně malá dávka práce). Navíc je pravidelně aktualizován.

2.5.3.19 Phishingator

Aby bylo možné použít Phishingator na heterogenní organizaci, nesměl by být LDAP integrován tak úzce, jako je. Tato integrace znamená, že ho nelze nasadit bez LDAPů nebo použít pro subjekty, se kterými nesdílíme doménu. Z těchto důvodů Phishingator lze uvažovat pouze pro jednolité podniky. Software je v době psaní stále aktivně vyvíjen.

2.6 Komerční software

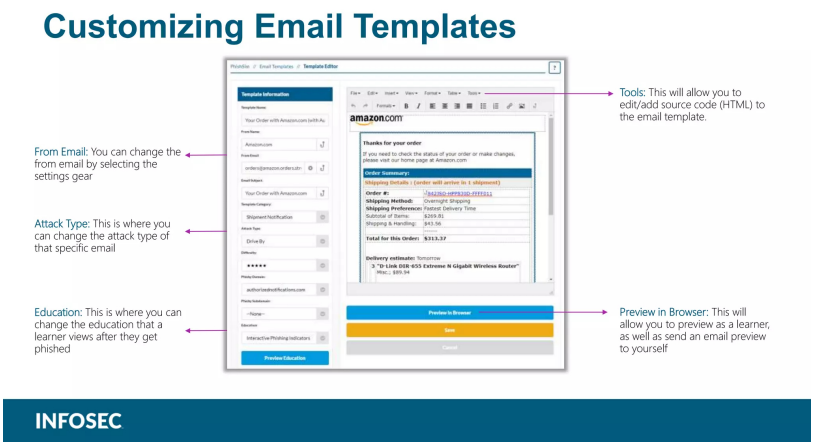
Kromě open-source programů se na trhu nachází také řada komerčních řešení, v následující sekci jsem prošel výběr několika z nich. Vzhledem k tomu, že jsou komerční, nešlo otestovat přímo jejich funkcionalitu, ani to nebyl cíl této práce. Mohl jsem si ovšem prohlédnout, co o svém produktu říká vývojář nebo uživatelé, kteří produkt vyzkoušeli.

Z dostupných zdrojů jsem se pokusil ohodnotit software na základě stejných metrik jako jsem učinil i u opensource. Mnohdy jsem využil předpoklad, že vývojář o své aplikaci nevydává klamavou reklamu, proto jsem se zdržel hodnocení takových vlastností, které byly zmíněny třetí stranou bez přiloženého důkazního obrázku nebo o nichž jsem neměl dostatek informací.

2.6.1 Infosec IQ

Prvním software je cloud platforma IQ, od firmy Infosec. O svém produktu nesdílí příliš mnoho informací. Těch pár zmíněných vlastností je trénink uživatelů, statistiky uživatelské úspěšnosti, simulace phishingu, automatizace a integrace. [107] Materiál, že kterého lze čerpat nejvíce, je prezentace vytvořená pro navigaci z roku 2019.

Phishingové simulace zahrnují kolem 1000 šablon s různými obtížnostmi. Šablony emailů je možné vytvořit vlastnoručně, nebo si je je možné nasdílet s ostatními uživateli platformy. Emaily mají náhledy, z obrázku 2.13 je patrné, že by úprava emailů měla hodnocení **TC3** 4/4. Do emailu se dají přidat přílohy, včetně kontroly, zda cíl povolil makra. [108]



Obrázek 2.13 Slide [109] z prezentace [110]. Zobrazuje jakým způsobem vypadá editor emailové předlohy.

Přidávání cílů je možné skrz AD, CSV soubory nebo manuálně. [108] Takže splňuje metriku **VI**.

Každá kampaň se může sestávat z více emailových předloh (lze i limitovat kolik mailů každý dostane, ve výchozím nastavení dostane každou předlohu). Kampaň lze odeslat specifické skupině cílů nebo individuálním cílům. Sledování by pak mělo minimálně být schopno zjistit, zda uživatel klikl na odkaz (**T3**). Taktéž je platforma schopná kontrolovat odpovědi na phishingové emaily, dokonce v nich je schopná hledat specifické znaky, takže není vázána na čistě webový phishing. Phishing lze plánovat skrz rozprostřenou časovou dobu. [108]

Kurzy jsou sice společností vyzdvihovány, ale žádný materiál nepojednává o jejich obsahu. Kromě celé knihovnu kurzů, které platforma poskytuje, je možné tvořit vlastní. Bohužel prezentace moc světla do tohoto tématu nevnáší. Jenom poskytuje náhled, že v kurzu je možné splnit nějaké úkony, včetně shlédnutí videa. Kolem těchto kurzů lze taktéž vytvářet kampaně. [108]

Aplikace dokáže vyrobit reporty. Z dostupných obrázků, obsahuje očekávané grafy. Zdánlivě se dají zprávy a vizualizace upravit podle svého uvážení. [110]

Pro přihlášení jde použít organizační SAML 2.0 kompatibilní SSO. Dále má program API [108], tedy **MA** - A.

Na první pohled se jedná o cluodovou aplikaci podobnou některým z manažerů kampaní ze seznamu software. Navíc má především kurzy, které mají uživatele vzdělávat o kybernetických hrozbách. Prezentované generování zpráv vypadá lépe nežli u open-source řešení.

2.6.2 Lucy

Lucy je software, který má poměrně rozsáhlou dokumentaci vlastností na svojí wiki.

Aplikace poskytuje emailové profily. Můžeme nastavit autentizaci a způsob šifrování. Tedy z technologického hlediska splňuje **M1** - manual 123, **M2** i **M3**. Z wiki je patrné, že způsobů doručení je více než jen SMTP, třeba přes HTTP nebo SMS. [111]

Kampaně se tvoří pomocí průvodce nastavením, jde zvolit: typ útoku, klient (organizace, na kterou se útočí), šablona (včetně jazyka šablony). Příjemce je možné buď přidat jako existující skupinu nebo vepsat manuálně. Tento přístup by odpovídal **VC** - 1/3. Kampaň je také možné vytvořit v tzv. expert módu, který zpřístupní všechny možné nastavení. [112]

Scénáře i šablony podporují lokalizaci. Také dokáže sledovat odeslání emailů **T1**, jejich otevření **T2**, navštívení stránky **T3** i sběr údajů **T4**. Mimo specifikované sledovací prvky obsahuje i další, tj. odpovědi na phishingový email nebo přeposlání na hlásící adresu. Ověřování hesla

funguje čistě pomocí regulárního výrazu.

Kampaň může hostovat vlastní vstupní stránky. Ty můžeme založit naklonováním existujícího webu, proto by hodnocení **TC2** odpovídalo 4/4. Vstupní stránku i zprávu je možné upravit pomocí WYSIWYG editoru. [112] **TC3**, **TC4** splňují hodnocení 4/4.

Odeslání mailů jde naplánovat, se specifickým počtem emailů přes časové období, včetně opakovaných odeslání. Uživatele skupiny v kampani můžeme dále třídit.

Kampaň zobrazuje přehled grafů s úspěšností uživatelů, jelikož jsou kampaně určené pro právě jednu skupinu, není nikterak seskupený. Pro každou kampaň je možné zobrazit výsledky jednotlivých uživatelů, odpovídalo by **VR1** - 2/3. Zprávy jsou velmi podrobné kombinující přizpůsobitelný text i grafy [113], a vysloužily by si hodnocení **VR2** - 2/2.

Program podporuje poměrně komplexní management uživatelů, včetně přiřazení různých práv různým uživatelským skupinám. Přihlašovat se je možné i přes SSO. [114]

Kromě samotné phishingové kampaně má Lucy i e-learningové kurzy, které lze přizpůsobit a využít. V neposlední řadě má API, podporuje i pluginy, splňuje tak **MA** - MA.

Lucy je velmi rozsáhlý, a široce zdokumentovaný program, o němž si můžeme přečíst téměř vše nutné, nicméně jelikož komerční software nebyl cílem této práce, nešel jsem ve zkoumání až příliš do hloubky. Z toho, co je vidět se jedná o jeden z nejpokročilejších kampaňových manažerů, a tedy dává smysl že si autoři nechávají za takový software zaplatit. Kromě samotného managementu má k dispozici i zmíněné kurzy, což se zdá jako trend mezi komerčním software.

2.6.3 Phished.io

Jedná se o další cloudové řešení, které využívá nástroje strojového učení ke generování personalizovaného obsahu.

Oficiální stránky poskytují velmi málo užitečných informací o samotném produktu. Program předává uživateli aktuální znalosti ze světa kybernetické bezpečnosti, pomocí konkrétních pravidel co dělat, či nikoli. Poskytuje administrátorovi skóre rizika pro každého uživatele. Součástí je AI asistentka. Phished.io obsahuje integraci s mailovou schránkou, pomocí které je možné podezřelé emaily nahlásit. [115] Trochu podrobnější recenze potvrzuje, že každá zpráva je vždy šitá na míru, založená na historických vzorech prokliknutí. Hlášení emailu funguje pro MS Teams nativně, nebo s pomocí specifické adresy, na kterou se emaily přeposílají. Po selhání identifikace phishingu je cíli přiřazeno školení na dané téma. Toto školení je kombinace textového materiálu s volitelnými kvízy, které může uživatel vytvořit. Šablony jsou k dispozici pouze v devíti jazycích [116], čeština jedním z nich patrně nebude.

Cíle se do aplikace importují buď přes CSV nebo skrze integraci Azure Active Directory, prokazatelně tedy splňuje **VI**. Manuální zadávání je taktéž možnost. [116]

Dalším hlavní vlastností má být automatizace celého procesu, kdy jsou nové maily vždy automaticky vygenerované a systém si vlastně žije vlastním životem. Ve finále program dokáže vytvořit zprávu s výsledky. Zprávy mohou obsahovat jak síň slávy, zeď hanby, tak agregaci dle oddělení [116].

Podle dostupných informací se zdá jako relativně odlehčený manažer, ale nelze to říct s jistotou díky malému objemu dostupných informací o produktu. Opět zde vidíme kurzy jako hlavní bod navíc oproti software zdarma.

2.6.4 Phishingbox

Cloudové řešení, které kromě phishingových simulací nabízí i kurzy zaměřené na internetové hrozby nebo skenování a nahlašování emailů.

Pro kampaň může hostovat vlastní vstupní stránky, jejich zdrojem je rozsáhlá knihovna šablon, které podle oficiálních stránek podporují přes 70 jazyků. [117] Minimálně zprávu je možné upravit pomocí WYSIWYG editoru. [118] **TC3** proto splňuje hodnocení 4/4.

Do kampaně lze zakomponovat více skupin. Skupiny je možné importovat při nejmenším alespoň z LDAPů. [118]

Odesílání mailů jde limitovat pomocí počtu emailů za specifikovaný interval, ale nejde určit zda nepodporuje ještě další možnosti. Z obrázků detailů je patrné, že aplikace sleduje odeslání mailů (**T1**), otevření (**T2**), proklik (**T3**) i interakci s webem (**T4**), dále také počet uživatelů, kteří obdrželi trénink a počet nahlášení emailu. [118]

Z dostupných obrázků není zcela jasné, zda lze zobrazit výsledky podle skupiny nebo jestli jde vždy o výsledky celé kampaně, stejně jako u Gophish. Na některých obrázcích jsou kontextovém menu vidět zprávy, ale jejich kvalitu nelze odhadnout. Stejně jako u Gophish zde existuje API, pomocí kterého by určitě šlo tyto spojitosti získat.

Informace o kurzech dostupných ve Phishingbox nejsou dostupné. Kromě toho nabízí několik integrací, především s Office 365, kde přináší skenování a nahlašování emailů. [118]

Znovu je vidět, že kromě phishingových kampaní software nabízí kurzy, nebo detekci phishingu.

2.6.5 Phish Threat

Další cloud platforma specializovaná na phishingové simulace.

Podle oficiálního katalogového listu zahrnuje přes 500 realistických phishingových útoků, všechny tyto šablony jsou přeloženy do deseti jazyků, čeština není jedním z nich. Jako ostatní cloudové platformy Phish Threat od firmy Sophos dává k dispozici tréninkové moduly, které by měly uživatele poučit o bezpečnostních hrozbách. [119] Všechny kurzy jsou stejně jako šablony lokalizovány.

Kampaně se tvoří pomocí průvodce, podle dostupného videa z oficiálních stránek ale už není patrné, jak nebo do jaké míry je možné kampaně upravovat. [120]. Phish Threat taktéž přichází s pluginem do MS Outlook, který přepošle phishingový email na nahlašovací adresu. [121]

Výsledky jsou potom zobrazeny v dashboardu v patřičných grafech, s časovou linií, včetně zobrazení agregovaných výsledků jednotlivých uživatelů. Program také obsahuje možnou generaci zpráv. Poslední často zmiňovanou vlastností je integrace se Sophos central [120].

Zdá se jako jeden z méně obsáhlých manažerů, ale zároveň je potřeba mít na paměti, že se jedná o jeden produkt, nikoli celou platformu. Jako každý jiný komerční produkt obsahuje kurzy a mnoho šablon.

2.7 Shrnutí

Na Internetu jde nalézt spousta aplikací pro účely phishingu. Některé zvládnou zjednodušit pouze jednotlivé kroky nutné k realizaci phishingové kampaně, jiné zvládnou zajistit celou kampaň.

Ze seznamu aplikací se dají vyčlenit tři rozdílné skupiny aplikací, mezi kterými nebylo úplně fér porovnávat. První skupina aplikaci zajišťovala hostování rychlých phishingových webů. V této kategorii se celkem rovnaly SpeedPhish Framework a The Social-Engineer Toolkit. Přesto má SET více možností, hlavně díky tomu, že obsahuje další vlastnosti určené pro penetrační testování. Jako čestné uznání uvedu aplikaci Hidden Eye, která se zaměřovala především na hostování webů, ale jako jediná z vybraného open-source software poskytovala lokalizační soubory.

Skupina proxy nástrojů byla také vyrovnaná, kdy se osobně přikláním spíše k aplikaci Evilginx2 jako lepší variantě. Hlavně díky dokumentaci a jasnějším způsobům nastavení.

Poslední, ale hlavní skupina, byly plnohodnotné kampaňové manažery, kde vítězným byl Gophish, proto jsem jej implementoval na produkční prostředí. Tento závěr není překvapivý, neboť se jedná o nepopulárnější open-source řešení. Na druhém místě se umístil program SniperPhish. V kontrastu s komerčními řešeními se tato softwarová řešení soustředí hlavně na jednu specifickou věc, proto také nenabízí osvětu uživatelů po selhání kampaně. Jedinou výjimkou v tomto ohledu byl Phishingator, který se soustředí nejen na tvorbu kampaní, ale také na samotné vzdě-

lávání uživatelů. Bohužel jeho konfigurace není úplně triviální, má celkem specifické požadavky na nasazení, a v některých vlastnostech se nevyrovná dříve zmíněným.

Seznam všech možných vlastností open-source programů si lze prohlédnout v souboru `PhishingSWFeatureTable.ods`.

Komerční software nabízí oproti open-source variantám větší knihovny předpřipravených šablon, ale hlavně kurzy. Tyto kurzy mají uživatele seznámit s kybernetickými hrozbami. Technické vlastnosti u této skupiny nemohu dobře posoudit, jelikož jsem měl přístup jen k jejich reklamnímu materiálu.

Bez ohledu na to, jak obsáhlý komerční software může být, přichází taky s řadou vlastních problémů, speciálně problematické mohou být cloudová řešení. Alghenaim, Bakar a Rahim ve svém článku [122], ve kterém hodnotili komerční phishingový software, mimo jiné zmiňují, že nástroje vlastněné organizacemi cizích zemí mohou představovat bezpečnostní riziko. Stačí málo, aby sbíraná data byla zneužita, namísto preventivní kampaně, k taktickému útoku. Také zmiňují, že některé z nich kladou nároky na nepřetržitý přístup k internetu, bez něhož organizace nástroj využít nemůže, nebo hůř, pokud specificky nástroj potřebuje data organizace (třeba k predikci budoucího útoku), pak bez nepřetržitého kontaktu může přestat fungovat spolehlivě.

Kapitola 3
Technicko-realizační část

Tato kapitola popisuje jak byl nástroj Gophish implementován pro realizaci phishingové kampaně proti dvěma společnostem, které měly mail hostovaný na platformě Exchange online.

Dále je zde popsána metodika použitá pro vytváření obou kampaní. Text popisuje tři alternativy textů využívajících sociálního inženýrství k simulaci reálného phishingu, také uvádí indicie, kterými se dá rozpoznat, že jde o phishingový pokus. Po těchto záminkách je prezentována dvojice poučných vzdělávacích stránek, které bylo možné zobrazit neúspěšným cílům.

Následuje krátký popis kampaní společně s průběhem, výsledky a jejich vyhodnocením.

Ve finále představuji trojici vylepšení nástroje Gophish, o kterých jsem uvažoval. V rámci této části bylo vytvořeno vylepšení pro integraci se vzdělávací platformou Moodle, které na základě zpětné vazby z nástroje Gophish, přihlašuje neúspěšné cíle do vzdělávacího kurzu.

3.1 Implementace nástroje Gophish

Gophish byl implementován na virtuální stroj s operačním systémem Rocky Linux. Jelikož na této distribuci Gophish nemá instalační balík, bylo nutné stáhnout předkompilovaný binární soubor pro Linux. Po jeho stažení bylo ještě potřeba vytvořit daemon, který z Gophish udělal službu, struktura tohoto souboru není těžká najít[1], i když k němu instalační manuál pouze referuje.

Kromě samotného Gophishe musel být vytvořen emailový server pomocí kterého se distribuovaly emaily. Sám o sobě interním emailovým serverem Gophish nedisponuje. Virtuální stroj se službou Postfix byl separátní od stroje s Gophish. Z hlediska nasazení proti jiné organizaci je tato možnost lepší, nežli vyžadovat nasazení nástroje do její vnitřní sítě.

3.1.1 Nastavení ochran emailu

Jelikož není cílem phishingové simulace obcházet ochrany popsané v teoretické části, musel být aplikován proces tzv. whitelistingu. Na straně Exchange Online byla, na základě oficiální dokumentace Microsoft[2], zapsána doména (pole *MAIL FROM*), pod kterou mohou emaily přicházet, síťová adresa a URL (jenž se mohla vyskytovat v těle zprávy). Whitelistovaná doména byla využita pouze v hlavičce emailu, v těle zprávy se vyskytovala adresa podvrženého odesílatele. Přítomnost obrazovky v Exchange Online pro whitelisting phishingových kampaní třetích stran svědčí o tom, že tento proces je běžně využíván. Ideálně by se kromě těchto základních nastavení měla také přidat speciální hlavička, která by zajišťovala alespoň základní autentizaci.

[1] Gophish linux daemon issue: `https://github.com/gophish/gophish/issues/586`

[2] Dokumentace k whitelistingu: `https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/advanced-delivery-policy-configure?view=o365-worldwide`

3.2 Metodika tvorby kampaně

Před samotným spuštěním kampaně bylo třeba vyrobit šablonu a vstupní stránku pro samotnou kampaň. Značnou roli v přípravě hrála anonymita testovaných subjektů. V době přípravy mi totiž nebylo známo, nad jakou společností bude kampaň probíhat. Což znamenalo nejen, že nelze připravit scénář bližší dané společnosti (což není standard u phishingových simulací), ale ani nebylo možné určit na jaký systém chceme získat údaje. Tato nevýhoda, ale nakonec přinesla celkem pozitivní výsledky. Jedinou dodatečnou informací mi bylo, že se jedná o zaměstnance nějaké společnosti. Toto mi posloužilo jako základ.

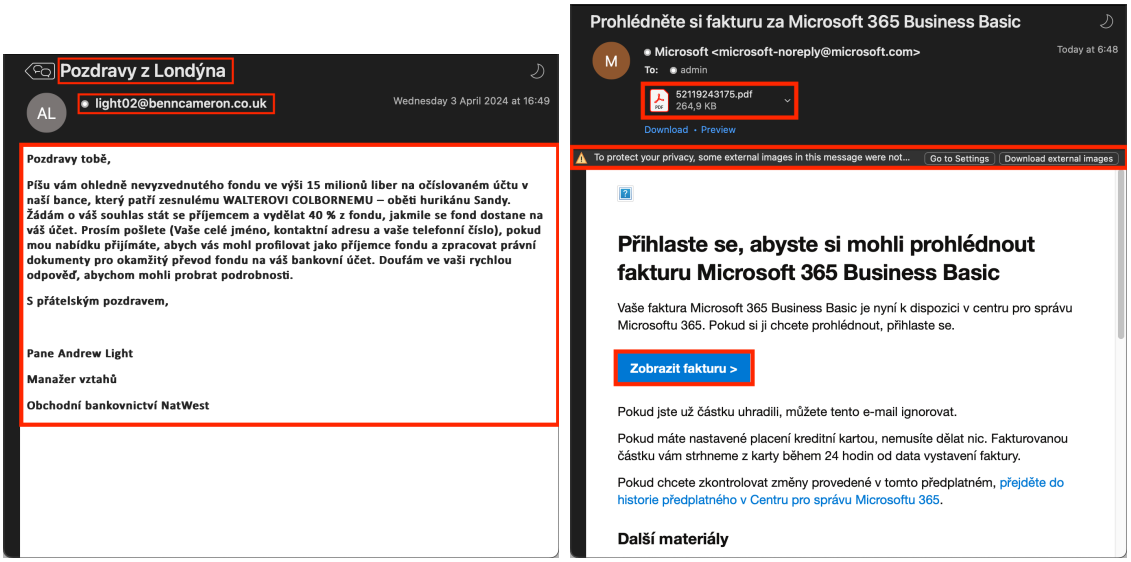
Když víme, že se jedná o společnost, jediné co může generický phishing chtít jsou přihlašovací údaje do pracovního systému či sítě. Alternativně by mohl phishing chtít přihlašovací údaje do systémů třetích stan. Záminky sice míří na sběr údajů k nespecifickému systému, ale jejich úprava by neznamenala zásadní změny v šablonách.

Pro následující sekci se hodí nejprve zmínit klasifikaci obtížnosti detekce phishingových pokusů.

Úroveň 1 (nejjednodušší) U těchto mailů se setkáváme s nejmenším úsilím na straně útočníka. Na druhou stranu, využívat jednoduchých technik dokáže být poměrně efektivní. Email takovéto obtížnosti může obsahovat syntaktické i diakritické chyby, většinou způsobené překladem z cizího jazyka. Příběh z mailu bude na první pohled podezřelý, obzvlášť při drobnějším přezkoumání. Text mailu zpravidla nebude nijak speciálně adresován s minimální vazbou na oběť a jeho pracovní pozici. Jedná se téměř vždy o zprávu odesílanou plošně. V rámci sociálního inženýrství je nejefektivnější využívání emocí strachu nebo snadného výdělku, proto příběhy často na tyto emoce cílí. Formátování u takovýchto emailů bývá jednoduché, mnohdy jenom prostý text. Emailová adresa odesílatele bude buď připomínat reálnou doménu (např. záměnou znaků, extra znaky), bude zcela nesmyslná (vygenerovaná náhodným generátorem) nebo se bude jednat o doménu poskytovatele tzv. freemailů (emaily pro běžné použití zdarma - seznam.cz, email.cz, gmail.com, aj.). Příklad takové zprávy lze vidět na obrázku 3.1a.

Úroveň 2 Tyto maily už jsou propracovanější. Příběh emailu může být podezřelý, ale většinou už nebude spoléhat na čistě emoční reakci. Text mailu pořád není nijak speciálně adresován, a pokud, pak se jedná jen o základní údaje (jméno, příjmení) vytěžené buď přímo z emailové adresy nebo z nějaké pořízené datové sady. Není neobvyklé, že jsou tyto údaje často zkomolené. Využívají důvěryhodných lokálních služeb třetích stran, které v regionu operují (u nás třeba Česká Pošta, Alza, atd.). I tento typ emailu bývá většinou posílán plošně. Emaily této kategorie se nejvíce liší od té první formátem, kdy mnohdy využívají designu stránek legitimních společností k formátování svého mailu. Jako odesílatelé se používají už jenom podezřelé domény, které připomínají ty reálné. Příklad takové zprávy lze vidět na obrázku 3.1b.

Úroveň 3 (nejtěžší) Nejpropracovanější typ. Příběh už je adresován na míru osobě, či firmě. Na rozdíl od předchozích úrovní nebývá plošný, většinou bývá cílený na užší kruh lidí. Pro získání informací útočník využívá OSINT, takže v mailu zahrnuje jména kolegů, vztahy ve firmě atp. Formátování mailu bývá dobře propracované, připravené na míru. Tato úroveň se dá poznat pomocí podezřelé domény, nebo na základě porušení vnitřních předpisů subjektu útočníkem.



(a) Příklad phishingu úrovně 1.

(b) Příklad phishingu úrovně 2.

Obrázek 3.1 Příklady phishingu.

3.2.1 Záminka: Odvolání vůči obvinění

Pro účely kampaně jsem se zaměřil na úroveň 2, obtížnost takového emailu se totiž dá jednoduše snížit. První otázkou, kterou jsem musel zodpovědět: Proč by mi měl cílový uživatel svěřit své přihlašovací údaje. Nejjednodušší mi přišlo zvolit nejprve strategii strachu. Celý finální text následuje:

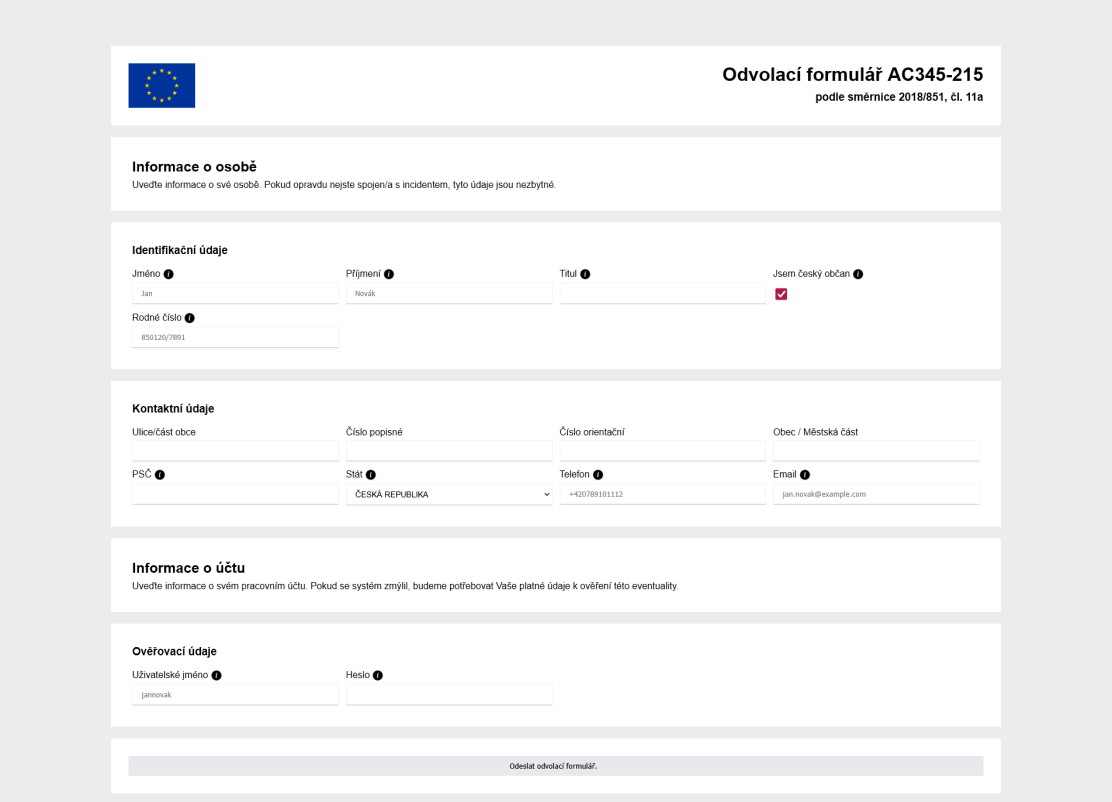
> Dobrý den,
> mé jméno je Marek Novotný, jsem právní zástupce, a bohužel pro Vás nemám zrovna příjemné zprávy. Evropský bezpečnostní systém, který váš zaměstnavatel provozuje podle směrnice 2018/851 článku 11a odstavce 2 Evropské Unie, zachytil použití zdánlivě Vašich přihlašovací údajů během rozsáhlého kybernetického útoku na systémy kritické infrastruktury několika evropských zemí. Jak si jistě uvědomujete, jedná se o závažnou situaci, která pro Vás může mít vážné dopady. Nebojte se ale, není vše ztraceno. Kdybych věřil, že se jedná o černobílý případ, tak Vás nekontaktuji.
>
> Jedná se o poměrně nový systém, takže má své nedostatky, je proto možné, že neidentifikoval údaje Vaše, ale třeba nějakého vašeho jmenovce. Taktéž se prý mohlo stát, že se cizí údaje špatně spárovaly na Vaší osobu. Pokud si tedy myslíte, že nešlo o Vaše údaje, tak Vám důrazně doporučuji na následujícím odkazu vyplnit a odeslat formulář `https://fake.link.example.com`. V rámci formuláře je potřeba vyplnit některé základní údaje, včetně vašich aktuálních přihlašovacích údajů do pracovního systému. Ty nám poslouží pro ověření korektnosti spárování. Z důvodu závažnosti zmíněného ohrožení tuto informaci nešiřte, jedná se o citlivou záležitost. Doufám, že se nám společně podaří uvést tuto událost na pravou míru.
>
> S pozdravem,
> RNDr. Marek Novotný.

Jak je z textu vidět, přestože byl cílený spíše na úroveň 2, díky formátování emailu spadá pod úroveň 1. Text sice neobsahuje žádné do očí bijící chyby, ale rozhodně je plný indicií. Největšími varovnými signály by měl být titul samozvaného právního zástupce, který nesouvisí s právy, ale

přírodními vědami. Dále odkaz k evropské směrnici, která se netýká informačních systémů, ale nakládání s odpady. Záměrně jsem využil právní předpis evropské unie, jelikož většina lidí se u nás v těchto nařízeních nevyzná, a proto by si měla zvládnout odůvodnit přítomnost systému jako „další evropský výmysl“. Samo o sobě by mělo být podezřelé, proč by měla daná osoba zadávat údaje do nějakého formuláře, když už údajný přítomný systém údaje má. Navíc také lze velmi rychle namítnout, že by zaměstnanec mohl zadat falešné údaje, aby se z tohoto „obvinění“ dostal. Text odkazu byl taktéž zaměněn za text představující doménu evropské unie.

Odkaz z této zprávy vedl na formulář zobrazený na obrázku 3.2. Pro design formuláře jsem využil formulář státní správy pro daňové přiznání. Spousta z polí ve formuláři požaduje identifikující, či citlivé údaje, tato pole ale nejsou formulářem sbírána. Jejich přítomnost ale pomáhá náš nedokonalý příběh prodat. Webová stránka byla provozována pod protokolem HTTP, tedy bez certifikátu. Odkaz který se vyskytoval v emailu do formuláře vložil email příjemce.

V kampaních byl posléze formátován jako téměř prostý text a jako adresáta používal adresu na seznamu.



Obrázek 3.2 Formulář zobrazený na stránce z odkazu emailu údajného Marka Novotného.

3.2.2 Záminka: Nový zaměstnanecký benefit

Druhá záminka byla těžší na vymyšlení. Otázka opět zněla, proč by někdo chtěl přihlašovací heslo pro nákup na, řekněme Allegru. Eventuálně mě ale napadlo proč - co kdyby existoval nějaký nový zaměstnanecký benefit? A najednou vše do sebe zapadlo, plný text následuje:

> Dobrý den,
> píšu Vám za týmy marketingu a obchodních vztahů tady v Allegru. S potěšením Vám

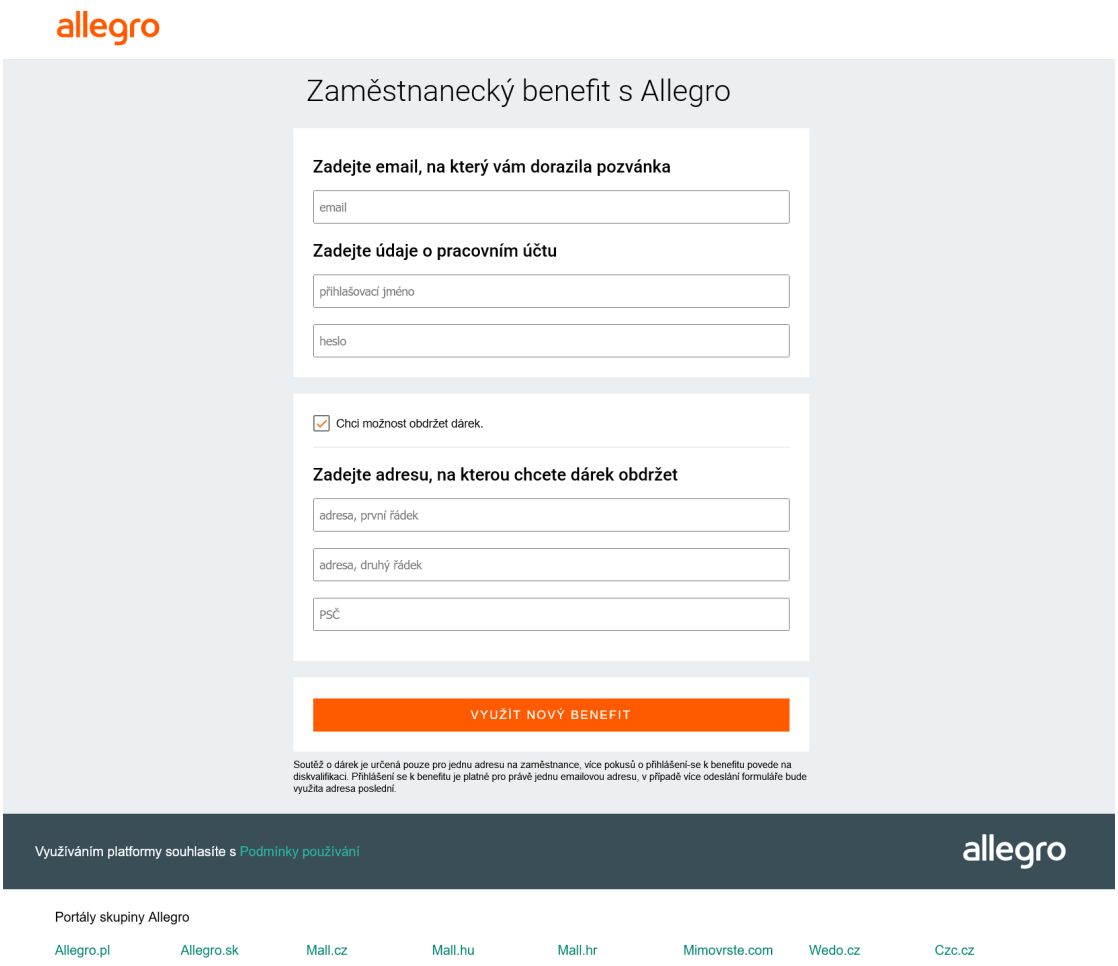
> oznamuji, že váš zaměstnavatel zřídil nový typ zaměstnaneckého benefitu, a to právě u nás, na Allegru. Vy a pár vybraných budete mezi prvními, jenž budete moci této novinky využít.
>
> Pro první měsíc, dostanete slevový poukaz na 1000 Kč při nákupu nad 1200 Kč za celý nákup, navíc ještě s dopravou zdarma. Bohužel takto výhodný bude pouze první měsíc, ale i tak každý měsíc přijde slevový poukaz v hodnotě 200 Kč při nákupu nad 1500 Kč. A pokud slevový kód osobně nevyužijete, můžete ho věnovat jako dárek. Platnost poukazu je pouze do konce daného měsíce. Na následujícím odkazu můžete svůj benefit aktivovat: `https://fake.link.example.com`.
>
> Aby jsme ověřili, že jste si zažádal(a) o benefit opravdu vy, je potřeba zadat do formuláře Vaše systémové heslo (pozor, nikoli heslo pro allegro, neboť je možné, že jste u nás ještě nic nepořizoval(a)). Do formuláře taktéž můžete uvést svojí adresu, aby bylo možné Vám na ni případně zaslat malou pozornost ☺ (obdržitel bude určen slosováním). Jakmile si Vaše údaje ověříme, na tento email Vám každý měsíc pošleme slevový poukaz, který budete moci využít při svém dalším nákupu.
>
> Přeju Vám hezký zbytek dne a těším se na Váš nákup,
> s pozdravem,
> Martina Zahradníčková
> Oddělení Marketingu, Allegro Group Czech

Text byl navržen na obtížnostní úroveň 2. Nabídku v e-mailu bych označil za dobrou, ale ne zase příliš dobrou, takže na první pohled není až tolik podezřelá. Až na malý detail - že přichází na firemní účet. V tomhle ohledu se mail ospravedlňuje jako nový zaměstnanecký benefit. První indicie by měla libovolném člověku prozradit, že je neobvyklé, aby někdo zřizoval benefit zahrnující čistě slevové poukazy u relativně náhodného obchodníka. Ale i kdyby, tak by zajisté obchodník neposílal info přímo na zaměstnance. Celý proces by šel přes nějaké personální oddělení, což je spolehlivější cesta, na rozdíl od elektronické komunikace.

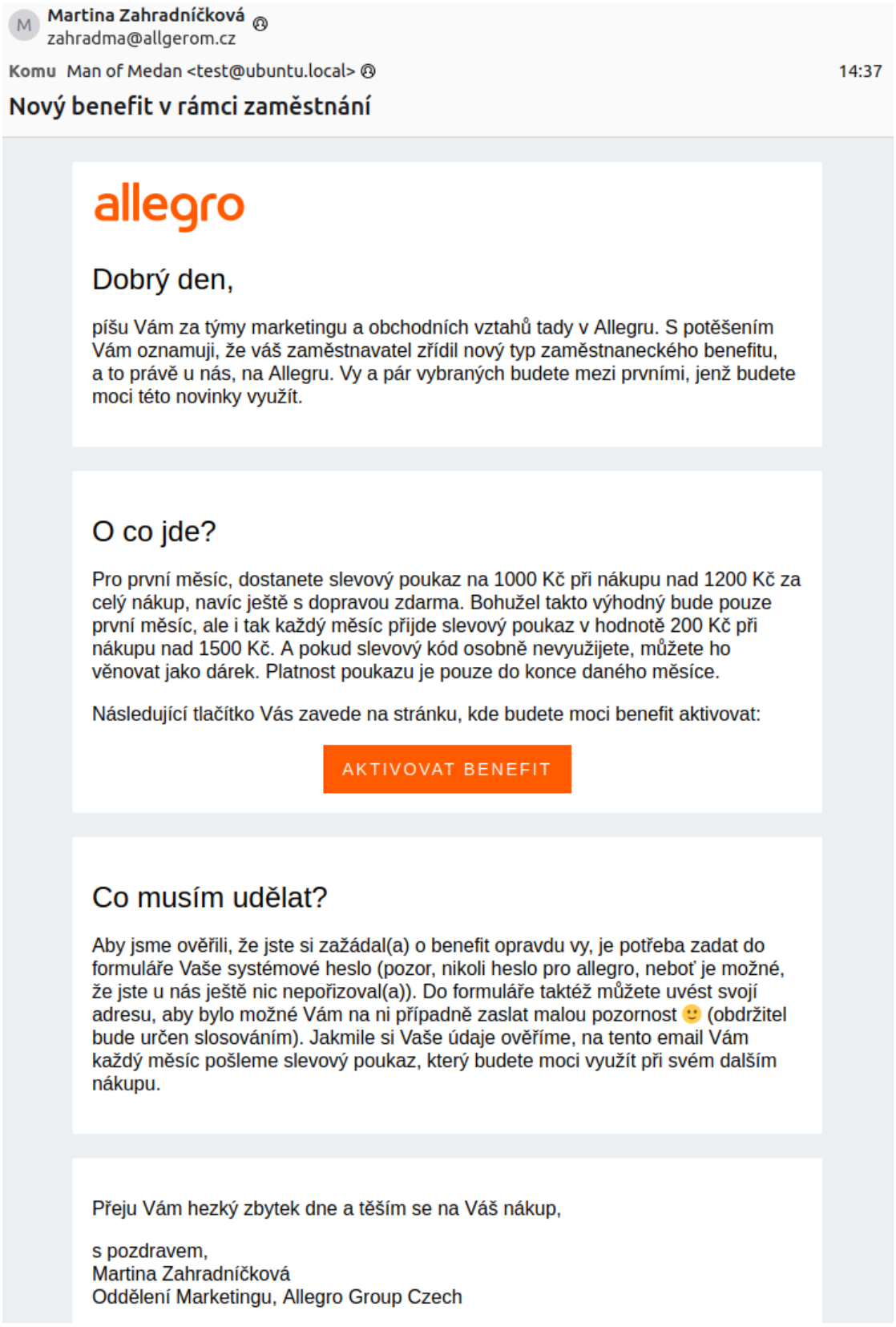
Odkaz ve zprávě vedl na formulář z obrázku 3.3. Design věrně kopíruje Allegro styl přihlašovacích formulářů, které jsem použil jako vzor. Stejně jako první formulář obsahuje pole pro určité citlivé údaje, ale totožně s prvním formulářem, se sběr těchto údajů ve výchozím stavu nekoná. Důvodem pro tato pole byla soutěž zmíněná v textu emailu, z důvodu prodání příběhu. I tento formulář byl provozován pouze pod HTTP protokolem. I v tomto případě odkaz z emailu do formuláře vložil email příjemce.

Poslaný email měl jako odesílatele zvolenou doménu, která vizuálně připomínala allegro.cz - allgerom.cz.

Největší změnou bylo formátování emailu, které kopírovalo design Allegro stránek, je jej možné vidět na obrázku 3.4. Z obrázku je patrná záměna odkazu za tlačítko, k tomuto designu došlo po dohodě s vedoucím práce. Tato část zabrala celkem dost času. První design nebyl složitý, jelikož už jsem měl hotový webový formulář. Problém nastal po první testovací kampani, při které došlo k tomu, že se na polovině emailových klientů email zobrazoval špatně. Konkrétně se používaly dvě rozdílné verze MS Outlook, pracovně označené nové a staré. Tento problém se ukázal jako poměrně obtížný k vyřešení.



Obrázek 3.3 Formulář zobrazený na stránce z odkazu emailu údajné Martiny Zahradníčkové.



Obrázek 3.4 Snímek formátu emailu (pořízen pro testovací účely na virtuálním stroji).

3.2.2.1 Problémy s formátováním

Formátování emailu je jak jsem díky práci zjistil nejtěžší část phishingového procesu. I když toto úsilí bývá věnováno spíše výše-profilovým cílům. Podle výsledků vyhledání jsem si dočetl o problémech v zobrazování HTML emailů v různých emailových klientech. Získaná informace znamenala, že musím celý email znovu vytvořit, ideálně pomocí tabulek s inlined CSS styly.

Změna struktury nebyl obtížný úkol, ale testování celkem ano. Microsoft svého klienta zadarmo neposkytuje, ale dá se využít trial verze. Ta ale už problém s novějším formátováním HTML nemá. Ideálně bych si nainstaloval starou verzi, ta už ovšem na internetu není jednoduše k dispozici. Také jsem nevěděl, jaká verze přesně vykazovala problémy. Údajně mají být nové a staré Outlooky. Test na Outlooku 2016 ukázal, že je evidentní rozdíl mezi Outlokem novým, starým a ještě nejstarším. Kde se v starém ukazovalo alespoň správné pozadí, nejstarší ukázal pozadí zcela bílé (tento email lze vidět na obrázku 3.5a).

Jak už jsem zmínil, dokázal jsem udělat několik testů na Outlooku 2016, k němuž jsem získal přístup s pomocí otce. Celé původní zobrazení mělo hned několik nedostatků:

- email nebyl vystředěn
- sekce mezi sebou neměly margin ani padding
- písmo bylo patkové
- čistě bílé pozadí
- odkaz neměl žádný design
- odkaz se zobrazoval čistě jako hypertextový odkaz
- vektorové Allegro logo chybělo

Po hlubší analýze jsem postupně vyřešil většinu problémů. Vystředění emailu bylo vyřešeno převodem na tabulku. Pozadí také vyřešila tabulka, konkrétně obarvení pozadí tabulky na správné pozadí těla. Stejně tak byly opraveny vlastnosti margin a padding - vhodné nastavení tabulky. Allegro logo se nezobrazovalo kvůli tomu, že se jednalo o vektorovou verzi, ve finálním mailu ho proto bylo potřeba odeslat jako přílohu a referovat jej pomocí Content-Id. Patkovost písma muselo vyřešit využití fontu Arial namísto webového fontu Open Sans, jelikož v emailech mají málokdy podporu. Nejtěžší bylo dostat pod kontrolu odkaz. Správné obarvení pozadí s odsazením zachránila opět tabulka. Už ale nepomohla při opravě dekorace nebo obarvení textu. Ani jednu z těchto vlastností jsem nedokázal zprovoznit, neboť Outlook vyloženě všechny pokusy ignoroval. Kromě klasického odebrání dekorace, jsem zkusil použít span uvnitř odkazu, různě je obarvovat, zadat validní URL (bez šablonového makra), na několika různých elementech několikrát specifikovat, že nemá dojít k dekoraci - nic. Zde mi došly způsoby jak problém napravit, ale finální produkt již nevypadá špatně (tuto verzi emailu lze vidět na obrázku 3.5b).

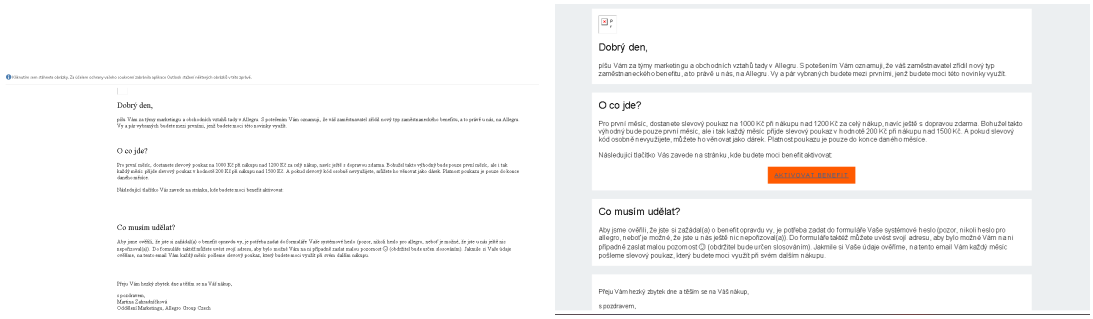
3.2.3 Záminka: Změna firemního hesla

Pro tuto záminku byl upraven naprosto legitimní email firmy Microsoft s textem nahrazeným patřičnými makry. Jako web posloužila upravená šablona přihlašovací obrazovky z veřejného github repozitáře[3].

Nápovědy pro tento mail zahrnovaly:

- Doména odesílatele: microsoft@campaign.securityguru.cz.
- Vstupní stránka je hostována na serveru bez domény.

[3] Šablona: `https://github.com/Octagon-simon/microsoft-login-clone`



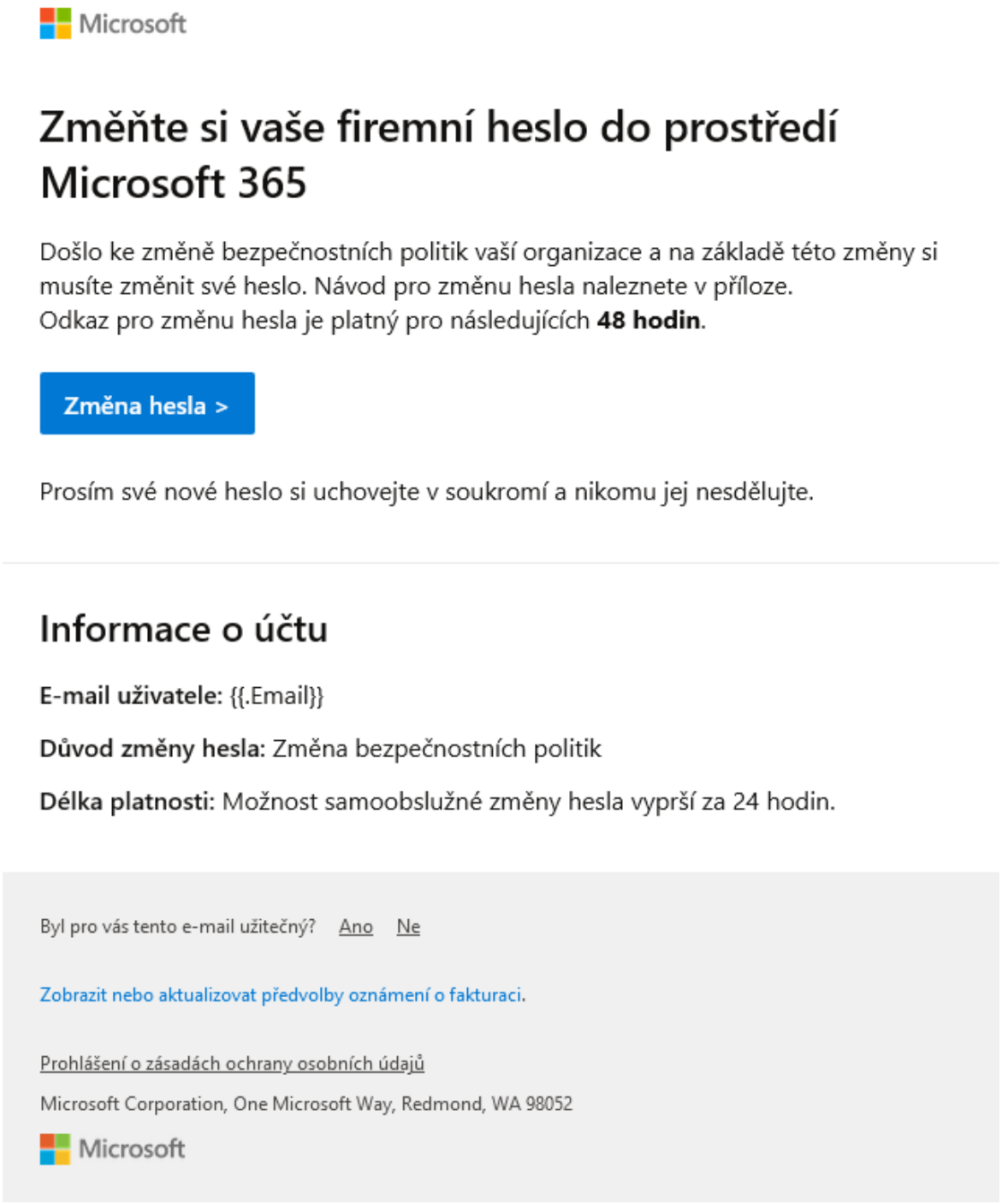
(a) Zobrazení emailu s totožným HTML jako na 3.4 v MS Outlook 2016.

(b) Zobrazení emailu v MS Outlook 2016 po úpravě HTML kódu.

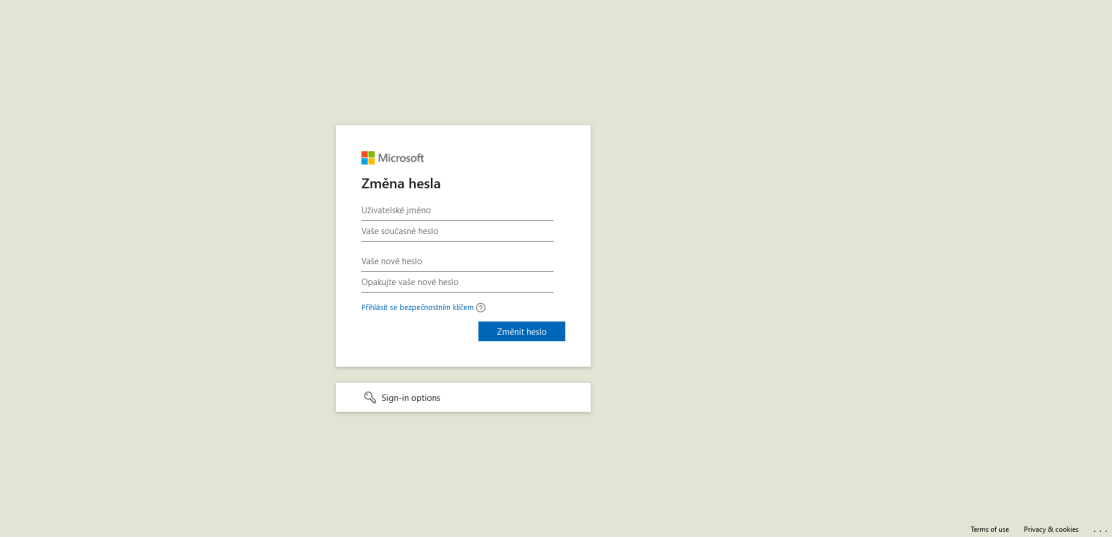
Obrázek 3.5 Zobrazení na emailovém klientu MS Outlook - před a po.

- Vstupní stránka běží pod protokolem HTTP.
- Formulář pro změnu hesla je oproti emailu hůře formátován.
- Ve formuláři se nachází odkaz na přihlášení bezpečnostním klíčem, přestože se jedná o údajnou změnu hesla.
- Kromě odesílajícího tlačítka, žádné odkazy, ani tlačítka nevedou na doménu společnosti Microsoft.

Jelikož email neobsahuje žádné chyby, očividné logické problémy a je dobře formátován, lze jej klasifikovat mezi obtížnostní úroveň 2. Tyto šablony si lze prohlédnout na obrázcích 3.6 a 3.7. K emailu byla taktéž přiložena příloha obsahující instrukce pro zadání údajů, taktéž obsahovala sledovací obrázek.



Obrázek 3.6 Použitá šablona emailu pro „resetování“ hesla Microsoft 365.

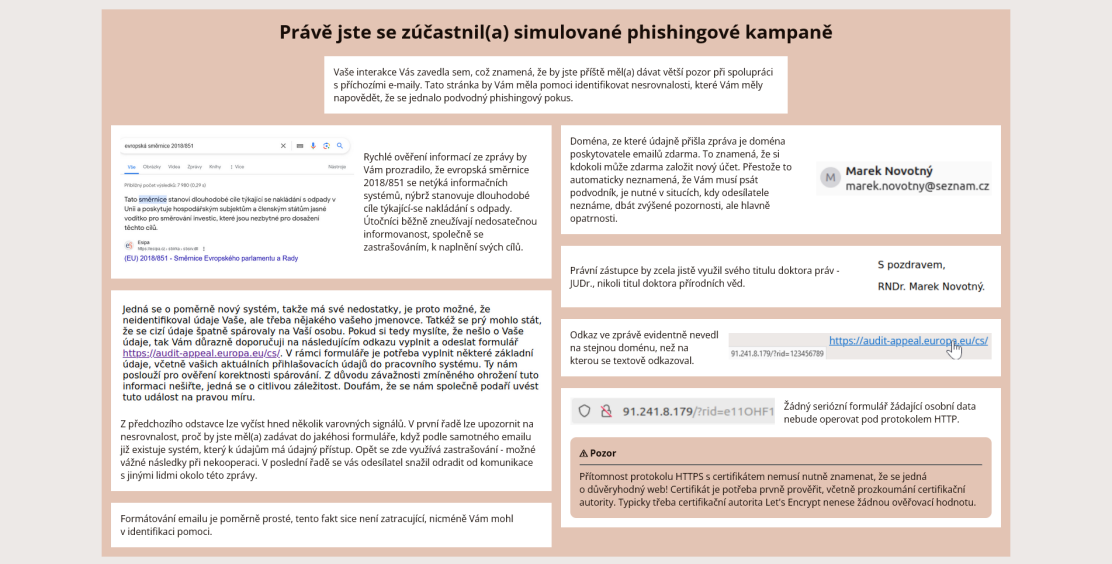


Obrázek 3.7 Vstupní stránka pro „resetování“ hesla Microsoft 365.

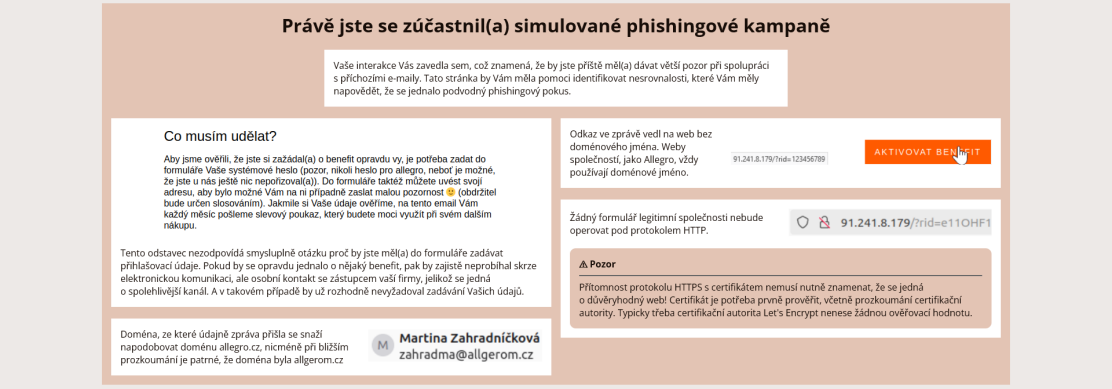
3.2.4 Vzdělávání neúspěšných

Aby byl daný neúspěšný účastník informován o jeho selhání ve cvičné kampani, bývá zvykem jej informovat. To lze udělat buď přímo v průběhu simulace phishingové kampaně. Nebo častěji, po ukončení kampaně.

Proto jsem vytvořil pro dvě záminky informační stránky, na které formuláře mohou přesměrovat účastníka po zadání přihlašovacích údajů. Součástí těchto informací je i seznam indikací, pomocí kterých šlo poznat phishingový pokus. Konkrétní indicie jsem již rozebral v předchozích kapitolách. Poslední záminka svou poučnou stránku nemá, neboť ji cílová organizace nevyžadovala. Briefingové stránky lze vidět na obrázcích 3.8 a 3.9, nebo je možné načíst si originály (viz. obsah adresáře `/phishing/briefing/`).



Obrázek 3.8 Briefingová stránka pro záminku Marka Novotného.



Obrázek 3.9 Briefingová stránka pro záminku Martiny Zahradníčkové.

3.3 Průběh kampaní

Kampaně byly provedeny dvojici organizací - menší a větší. Z důvodu anonymity budu dále označovány jako organizace A a organizace B. První kampaň byla testovacího charakteru, aby se zjistilo, zda implementace funguje dle představ na větším rozsahu.

3.3.1 Kampaň organizace A

Akce proběhla na skupině 6 lidí. Použita byla záminka zaměstnaneckého benefitu.

Simulace proběhla během jednoho dne bez zásadních problémů. Odeslat se podařilo všechny maily. Hlavním výstupem bylo zjištění problému popsaného v kapitole 3.2.2.1.

3.3.2 Kampaň organizace B

Druhá kampaň se prováděla na 59 zaměstnancích. Jako záminka se využilo resetování přihlašovacího hesla.

Testování této kampaně začalo s problémy, jelikož prostředí Exchange Online, které se nacházelo, jak na testovacím serveru, tak na serveru organizace B, začalo z ničeho nic pozdržovat emaily. Maily se zdržovaly na náhodné intervaly, některé ani nedorazily. Většina končila na chyby *4.2.0* nebo *451 4.7.0*. Na začátku server neměl ani doménu. Za účelem zvýšení doručitelnosti byly postupně přidány záznamy SPF, MX a DKIM. Systém emaily zdržel, i když byl email SPF aligned (tedy hlavička MAIL FROM / Return-Path = From). Poslední test sice ukázal, že SPF a DKIM aligned mail byl propuštěn okamžitě, nicméně se jednalo o jediný pokus, proto není jisté, zda se tak stalo právě díky splnění obou požadavků nebo šlo jen o propustný časový interval na straně Exchange Online. Časový tlak způsobil, že se kampaň konala bez tzv. *aligned SPF* (aby nebylo potřeba měnit nastavení emailové ochrany organizaci B). Emaily byly očekávaně zdrženy, ale v průběhu dne všechny zprávy na cílový mail server dorazily.

3.4 Výsledky

Kampaň v organizaci A byla úspěšně provedena s následujícím výsledkem: Všech 6 cílů email prokazatelně otevřelo, 3 přistoupily na phishingovou stránku a 2 zadaly data.

Kampaň v organizaci B dopadla následovně: z 59 osob, email s jistotou otevřelo pouze 14 zaměstnanců (~24%), na stránku přešli dva (~3%) a údaje zadal jediný (~1,7%). Údaje zadané jednou osobou byly očividně falešné, nejpravděpodobněji se jednalo o zvědavost, jelikož zaměstnanec stránku navštívil až den po údajné „expiraci“ odkazu z emailu.

Kampaň se konala nad 6 skupinami uživatelů, nicméně velké rozdíly mezi skupinami neexistovaly. Největší odchylkou bylo paradoxně IT oddělení, ze kterého jeden člověk zadal zmíněné falešné údaje, druhý člověk, který navštívil stránku byl ze skupiny běžných uživatelů.

Počet uživatelů, kteří email viděli je ale nejspíš větší, lze takto usuzovat, podle jedné uživatelské skupiny, která nebyla technicky zaměřená. Tento uživatel evidentně nezkoumal přílohu, ani nezvolil zobrazení externích obrázků, protože nástroj u něho zaznamenal jenom událost navštívení webu. Jeden uživatel sice není dostatečně velký vzorek ke statisticky významnému odůvodnění pro neotevírání emailů, ale i přesto jsem ochoten tyto hypotézu přijmout.

Výsledky jsou vypsány v tabulce 3.1. Tytéž výsledky jsou zobrazeny ve grafech buď jednotlivě na obrázcích 3.10a, 3.10b nebo sdruženě v procentech 3.10c

3.4.1 Vyhodnocení

Z celkového počtu 3 osob, které přistoupily na phishingovou stránku v kampani proti organizaci A, 2 zadaly data. Toto je na první pohled abnormální vzhledem k technickému zaměření

	Organizace A	Organizace B
Odesláno	6	59
Zobrazeno	6	14
Navštívilo	3	2
Zadalo	2	1

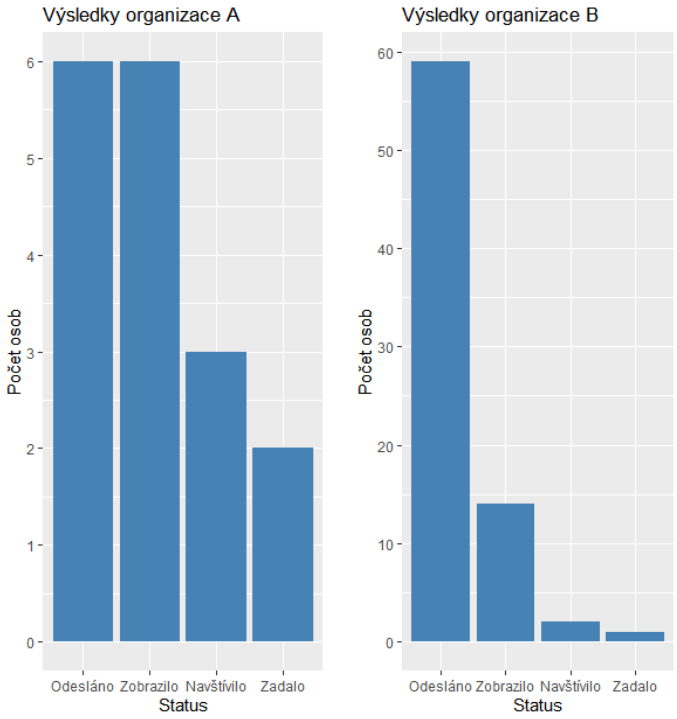
Tabulka 3.1 Výsledky mezi organizacemi.

organizace i skupiny uživatelů. Nicméně při bližším zkoumání dat bylo zjištěno, že jsou na první pohled fiktivní. Nešlo tedy o kompromitaci, ale čistě o ověřování funkčnosti ze strany cílů.

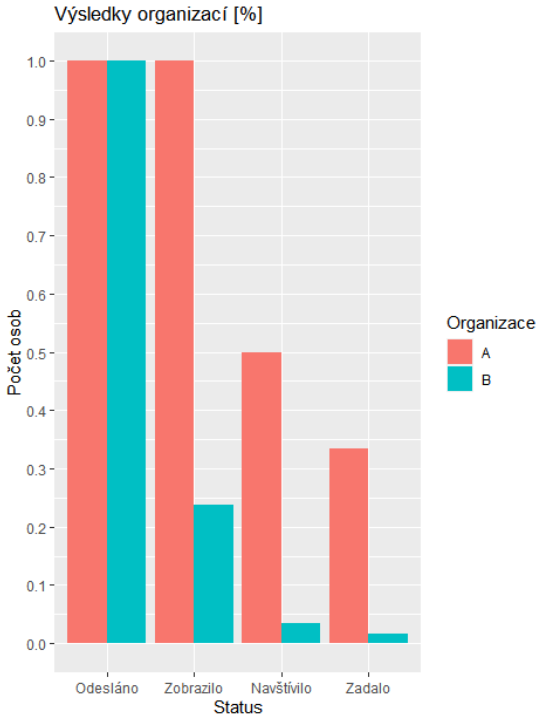
U organizace B výsledky vypadají velmi dobře. Z celkového počtu 2 cílů, jenž na stránku přistoupily zadala data jen jedna. Tato byla taktéž zcela fiktivní, navíc byla zadána až dva dny po datu expirace zmíněném v emailu. Celková interakce s phishingem je pod úrovní 5%. Tedy uživatelé jsou jen na základě dostupných dat buď dobře proškoleni, nebo došlo ke zkreslení vlivy mimo naší kontrolu (např. prozrazení akce v organizaci B).

Také je možné, že nebyla zvolena vhodná záminka. Každý člověk reaguje na situace jinak. Jedna je citový podnět ze strany prvních dvou záminek, něco jiného je poměrně neškodně vypadající „resetování“ hesla. Abych situaci přiblížil, představme si na chvíli, že připravené scénáře jsou naprosto legitimní. V případě prvních dvou buď cíl obdrží něco za odměnu nebo naopak se něčemu nepříjemnému vyhne. Nezměnění hesla pro nějakou službu při nejhorším znemožní práci na jeden den, po čemž by při nejhorším zasáhlo oddělení IT, tedy nejedná se o zásadně hrozivý předpoklad. Takže z tohoto hlediska se dal obsah emailu ignorovat.

Z tohoto důvodu, a za účelem zvýšení odolnosti uživatelů je vhodné simulované phishingové pokusy pravidelně opakovat. Odstraní se tím problém, kdyby náhodou šlo o moc *neškodně* vypadající záminku, protože při další kontrole se použije jiná, což může odkrýt jiné zranitelné uživatele. Také se tak dá zjistit průběžný stav, který se mění skrz čas (lidé stárnou, mění kariéry, atd.).



(a) Výsledky organizace A. **(b)** Výsledky organizace B.



(c) Procentuální výsledky obou organizací.

Obrázek 3.10 Výsledky organizací A a B.

3.5 Vylepšení nástroje

Aby tato práce sloužila nejen k výběru nástroje, přišlo v úvahu rozšířit vybraný nástroj o nějakou funkcionalitu. Přišel jsem se třemi možnostmi jak nástroj rozšířit. První možností byla integrace jednoho z proxy nástrojů. Druhá možnost bylo rozšíření o detekci doručení emailu, neboť všechny nástroje provádějí kontrolu odeslaných emailů pouze do úrovně SMTP klienta. Poslední možnost byla integrace e-learningové části.

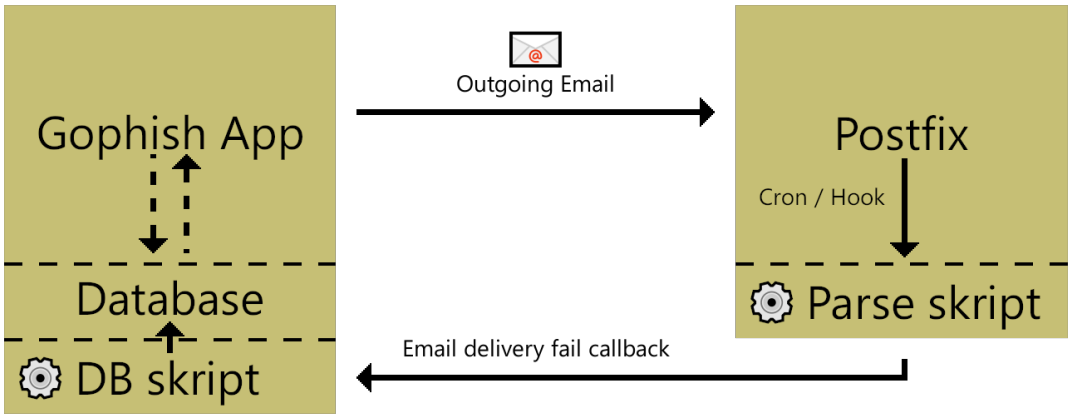
3.5.1 Integrace nástroje Evilginx

Hlavním důvodem pro neuskutečnění této integrace byla obtížnost takového cvičení, které by téměř vždy znamenalo kontrolu platného certifikátu (což většina koncových uživatelů nedělá). Dále toto rozšíření zabralo podstatnější časovou alokaci. nástroj Gophish navíc nepodporuje moduly a musel by se dělat zásah přímo do zdrojového kódu. Tento kód by následně někdo musel udržovat.

3.5.2 Lepší detekce odeslání

Potažmo všechny open-source manažery kampaní ukazují status odesílání emailu. Zatímco ale sledují základní status v závislosti odpovědi serveru, neřeší neexistující uživatele, zdržení, odmítnutí nebo jiné problémy s odesláním. Přestože se jedná o krajní případ, hodí se vědět, že email nebyl odeslán z důvodu chyby. Samozřejmě pokud nemáme pod kontrolou všechny servery po cestě emailu, není šance odchytit všechny, ale s trochou štěstí budou v cestě nanejvýše dva mailové servery. Za tímto účelem jsem původně chtěl vytvořil skript, jenž by s touto eventualitou počítal.

Mělo jít o skript který by se spouštěl periodicky buď jako cron úloha nebo by jej spouštěl přímo Postfix po odeslání emailu. Skript samotný pak měl zparsovat logovací soubor postfix mail-severu. Po tom měl poslat data o neodeslaných emailech na server, který by měl přístup ke Gophish databázi. Na tomto serveru by se nacházel skript další, který by data přijal a zapsal do je dané databáze (Samotné Gophish API neumožňuje učinit změnu statusu kampaně). Webový klient by si pak pouze přečetl daný status a ukázal jej (byť by třeba byla chvíle, kdy by se status ukázal jako *odesláno*). Takto by se teoreticky dalo zařídit přesnější sledování. Komunikační schéma je na obrázku 3.11.



Obrázek 3.11 Schéma komunikace plánovaného detekčního vylepšení.

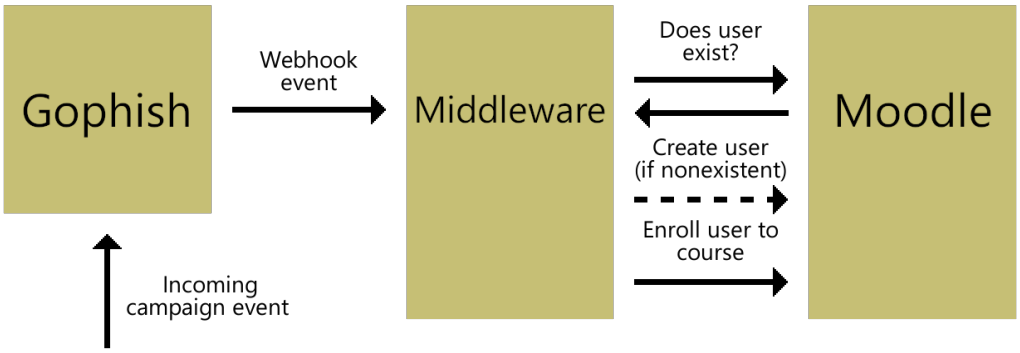
Tento přístup má bohužel ale několik vážných nedostatků. Pokud by jsme měli v kampani vždy unikátní cíle, pak by se nejednalo o problém, ale v případě, kdy by se vyskytlo více souběžných kampaní s tou stejnou osobou, nedalo by se čistě z emailové adresy jednoduše odlišit, ke které kampani patří. Jediný způsob jak v takovém případě odhalit, ke které kampani patří je pouze skrze *RId*, to je ale k dispozici pouze v textu emailu.

Takže najednou už nestačí jednoduchá cron úloha a parser, najednou potřebujeme sledovat emailovou schránku, jestli nám náhodou nepřišel email. Ten je potřeba zpracovat (pokud máme nakonfigurovanou schránku, tak je třeba zařídit, aby info o stavu obsahovalo originální zprávu). Navíc to neřeší menší problémy týkající se synchronizace přístupu k databázi. Tento problém není tak zásadní, pokud by se využíval plný databázový systém. Pokud ale pracujeme se souborovou databází, může to vyvolat určité další komplikace. Takže se najednou jedná o poměrně složitě implementovatelnou vlastnost, jejíž přínos je relativně nízký (něco jiného by bylo, kdyby nám status dal naprostou jistotu odeslání).

3.5.3 E-lerningová integrace

Jelikož se open-source projekty nesoustředí na aspekt vzdělání po provedení kampaně. S vedoucím práce jsme se proto dohodli na modulu pro platformu Moodle. Plán byl jednoduše: pokud cíl klikne na odkaz nebo odešle data (preferovaně volitelně s pomocí konfigurace), pak jej skript zaregistruje ke kurzu na Moodle.

Pro tento účel jsem využil webhooku nástroje Gophish. Ten odesílá zprávy o průběhu všech kampaní na middleware. Tato malá aplikace, napsaná v PHP, nejprve ověří, že obdržela zprávu od Gophish. Odfiltruje nechtěné akce, jako je odeslání emailů nebo události o nahlášení emailu. Po filtraci zkusí nalézt uživatele podle emailu na Moodle, a pokud jej nenalezne, založí mu účet. Účet je posléze přiřazen k patřičnému e-lerningovému kurzu. Schéma komunikace je na obrázku 3.12. Jedná se o přímočarý skript, který se případně dá volat i přes javascript ze vstupních stránek (byť samotný javascript není součástí tohoto rozšíření). Zdrojový kód aplikace je k dispozici pod adresářem `/addon/`.



Obrázek 3.12 Schéma komunikace integrace e-learning modulu.

Závěr

V teoretické části jsem uvedl problematiku sociálního inženýrství, phishingu a provádění simulovaných phishingových kampaní.

Pro analytickou část jsem nejprve shromáždil seznam 19 open-source aplikací. Pro jejich zhodnocení jsem vytvořil metodiku a hodnotící kritéria. Nainstaloval jsem a zhodnotil všech 19 open-source nástrojů.

Vedle open-source software jsem z dostupných zdrojů zanalyzoval 5 komerčních řešení.

Z open-source nástrojů jsem vybral vítězný, nejlépe ohodnocený, open-source nástroj - Gophish. Tento nástroj byl uveden do provozu a použit k realizaci dvou simulovaných phishingových kampaní proti dvěma organizacím.

V rámci realizace těchto kampaní došlo k vytvoření tří emailových šablon a phishingových stránek. Během jejich přípravy byla důkladně prozkoumána problematika formátování emailů pro různé mailové platformy. Společně se dvěmi šablonami byl vytvořen i poučný materiál, informující účastníka, jak měl phishing rozpoznat.

Analyzoval jsem a vyhodnotil výsledky obou kampaní.

Kromě kampaně byl nástroj Gophish obohacen o malou PHP aplikaci, která se integruje do e-learningového prostředí Moodle. Tento doplněk byl vytvořen za účelem zefektivnění pozitivních dopadů simulovaných phishingových kampaní.

Předchozí body jednotlivě shrnují splněnost všech cílů stanovených při zadání diplomové práce.

Příloha A

Počáteční nastavení Muraeny

1. Stáhněte software (ideálně předkompilovaný).
   a. Zkompilujete zdroj (požadovaný balík go-lang).
2. Stáhněte zdrojový kód konfiguračního adresáře, minimálně jsou potřeba soubory **geoDB.mmdb**, **watchdog.rules** a **config.toml**.
3. Nainstalujte redis pokud chcete používat lokální databázi.
   a. Alternativně nastavte vzdálený redis.
4. Upravte config.toml:
   a. Zapněte crawaler.
   b. Pokud víte, že cílový web používá externí zdroje jakou součást svojí služby, přidejte je do **crawler.externalOrigins**.
      ▶ Poznámka A.1. Přestože je prefix zahrnut v sekci *crawler*, je používán uvnitř proxy modulu.
   c. Nahraďte destinaci cílovou doménou.
   d. (Volitelně) Vypněte TLS konfiguraci (pokud cíl běží čistě pod HTTP, tak může zůstat později vypnutá).
      i. Pokud to neuděláte, je nutné poskytnout certifikát, přestože ještě nebude proxy spuštěna.
         A. Nastavte certifikát pro phishing doménu.
   e. Upravte redis nastavení, aby seděl na Vaší konfiguraci.
5. Spusťte program (nezapomeňte specifikovat cestu ke konfiguračnímu souboru)
6. Ukončete Muraenu
7. Znovu upravte config.toml:
   a. Změňte **proxy.phishing** na libovolnou doménu (používáno pro účely certifikátů).
   b. (Volitelně) Povolte TLS nastavení.
      i. Nastavte certifikát pro **proxy.phishing** doménu.
   c. Zapněte tracking.
   d. Nastavte tracking:

Tracking je podstatný k identifikaci nových úlovků a pro zachytávání údajů. **Tracking.type** je použit k nastavení buď URL (hodnota: *path*) nebo HTTP požadavku (hodnota: *query*). Výběrem *path* se stane identifikátor částí regulárního výrazu, kdy bude předcházet specifikovanému regexu. Identifikuje cíl tím, co zbyde ve vstupu po odebrání výrazu (účelem jsou RESTová API).

Tracking.landing je použit jenom pokud se využívá *path*, kde hodnota této hlavičky se nastaví na extrahovanou cestu, kam je uživatel přesměrován po přihlášení (tu část URL cesty bez uživatele).

Tracking.header je hlavička kam je vložena hodnota trackovacího id (tedy jendá se o způsob, kterým muraena určuje zda je sledování použito). Za normálních okolností takovéto informace bývají posílané jako součást cookies, nicméně v případě že klient nepošle cookie, tato hlavička se používá jako redundantní zdroj.

V případě že je použita hodnota *query*, identifikátor je nejprve nalezen uvnitř dotazu, což funguje na post požadavky, nicméně pro ostatní HTTP metody bude většinou prázdná. Pokud žádné pole s tímto identifikátorem není v požadavku nalezen, jsou prohledány cookies. Potom, co je nalezen záznam, je validován oproti nastavenému regulárnímu výrazu.

Tracking.urls je velmi důležité nastavení. Zachycení údajů probíhá výhradně na této URL. **Tracking.authSession** je pokud tomu správně rozumím URL, která spustí proces odcizení session. Lze to udělat přes modul necrobrowser, ale tuto část přeskočím. Jelikož mým cílem nebylo ukrást session, ale ukázat, že to nástroj zvládne.

Poslední jsou v nastavení **tracking.patterns**. Ty jsou použity na **tracking.credentials** URL, slouží k zachycení údajů z formulářů. **Tracking.patterns.label** neslouží k označení nějakého popisku pole html formuláře, jedná se pouze o jméno klíče, jehož jméno bude použito při ukládání do databáze. **Tracking.patterns.start** a **Tracking.patterns.end** jsou celkem jasné. Obě tyto nastavení mohou být prázdná.

Bibliografie

1. HADNAGY, Christopher. Social Engineering: The Science of Human Hacking. In: Second. Indianapolis, IN: John Wiley & Sons, 2018, s. 7. ISBN 978-1-119-43338-5.
2. ERBSHLOE, Michael. TROJANS, WORMS, AND SPYWARE, A Computer Security Professional's Guide to Malicious Code. In: Oxford: Elsevier Butterworth–Heinemann, 2005, s. 61. ISBN 0-7506-7848-8.
3. What is "Social Engineering"? [Online]. © 2005-2024 [cit. 2024-02-28]. Dostupné z: https://www.enisa.europa.eu/topics/incident-response/glossary/what-is-social-engineering.
4. HADNAGY, Christopher. *Social Engineering: The Science of Human Hacking*. Second. Indianapolis, IN: John Wiley & Sons, 2018. ISBN 978-1-119-43338-5.
5. *Scratching the Surface* [online]. New York, NY: Verizon, 2023 [cit. 2024-02-28]. Dostupné z: https://www.verizon.com/business/resources/reports/dbir/2022/results-and-analysis-not-the-human-element/.
6. *Social Engineering* [online]. New York, NY: Verizon, 2024 [cit. 2024-02-28]. Dostupné z: https://www.verizon.com/business/resources/reports/dbir/2023/incident-classification-patterns-intro/social-engineering/.
7. KARIMI, Faith. *'Mom, these bad men have me': She believes scammers cloned her daughter's voice in a fake kidnapping* [online]. CNN, 2023-04 [cit. 2024-02-26]. Dostupné z: https://edition.cnn.com/2023/04/29/us/ai-scam-calls-kidnapping-cec/index.html.
8. LEPORE, Stephen M. *Georgia mother gets fake ransom call where scammers used AI to impersonate her 22-year-old daughter's voice* [online]. Dailymail, 2023-07 [cit. 2024-02-26]. Dostupné z: https://www.dailymail.co.uk/news/article-12317821/Georgia-mother-tells-sheer-panic-scammers-used-AI-impersonate-16-year-old-daughters-voice-demand-50K-ransom.html.
9. BLANCO, Andrea. *A father is warning others about a new AI 'family emergency scam'* [online]. Independent, 2023-12 [cit. 2024-03-04]. Dostupné z: https://www.independent.co.uk/news/world/americas/ai-phone-scam-voice-call-b2459449.html.
10. KONG, Harvey. *A father is warning others about a new AI 'family emergency scam'* [online]. South China Morning Post, 2024-02 [cit. 2024-03-04]. Dostupné z: https://www.scmp.com/news/hong-kong/law-and-crime/article/3250851/everyone-looked-real-multinational-firms-hong-kong-office-loses-hk200-million-after-scammers-stage.
11. *deepfake* [online]. Cambridge: Cambridge University Press [cit. 2024-03-04]. Dostupné z: https://dictionary.cambridge.org/dictionary/english/deepfake.

12. *Detect DeepFakes: How to counteract misinformation created by AI* [online]. Cambridge, MA: MIT Media Lab [cit. 2024-03-04]. Dostupné z: https://www.media.mit.edu/projects/detect-fakes/overview/.
13. WIND, Daria. *How to remove artifacts on generations with people: fixing weird faces in DALL-E 3* [online]. Medium, 2024-02 [cit. 2024-03-04]. Dostupné z: https://medium.com/phygital/how-to-remove-artifacts-on-generations-with-people-fixing-weird-faces-in-dall-e-3-2bef02102e0e.
14. SHIREY, Robert W. *Internet Security Glossary, Version 2* [RFC 4949]. RFC Editor, 2007 [cit. 2024-03-01]. Request for Comments, č. 4949. Dostupné z DOI: 10.17487/RFC4949.
15. STOUFFER, Keith; PEASE, Michael; TANG, CheeYee; ZIMMERMAN, Timothy; PILLITTERI, Victoria; LIGHTMAN, Suzanne; HAHN, Adam; SARAVIA, Stephanie; SHERULE, Aslam; THOMPSON, Michael. *Guide to Operational Technology (OT) Security* [online]. NIST, 2023 [cit. 2024-03-01]. NIST Special Publication. Dostupné z DOI: 10.6028/NIST.SP.800-82r3.
16. LANGBERG, Mike. *AOL ACTS TO THWART HACKERS* [online]. San Jose, CA: Mercury News, 1995-09 [cit. 2024-03-01]. Dostupné z: https://simson.net/clips/1995/95.SJMN.AOL_Hackers.html.
17. REKOUCHE, Koceilah. *Early Phishing* [online]. Ithaca, NY: arXiv, 2011-06 [cit. 2024-03-01]. Dostupné z DOI: 10.48550/arXiv.1106.4692.
18. ESSER, Alexandre. *The slow but steady evolution of phshing — PART I* [online]. Arsen, 2023-01 [cit. 2024-03-01]. Dostupné z: https://arsen.co/en/blog/phishing-evolution-part1/.
19. IANG. *GP4.3 - Growth and Fraud - Case #3 - Phishing* [online]. Financial Cryptography, 2005-12 [cit. 2024-03-01]. Dostupné z: https://financialcryptography.com/mt/archives/000609.html.
20. POULSEN, Kevin. *May 4, 2000: Tainted 'Love' Infects Computers* [online]. Wired, 2000-05 [cit. 2024-03-01]. ISSN 1059-1028. Dostupné z: https://www.wired.com/2010/05/0504i-love-you-virus/.
21. SARAVANAN, Priya; SELVAKUMAR, Santhanalakshmi; VELUSAMY, R. Evidential theoretic deep radial and probabilistic neural ensemble approach for detecting phishing attacks. *Journal of Ambient Intelligence and Humanized Computing*. 2021, roč. 14, s. 1–25. Dostupné z DOI: 10.1007/s12652-021-03405-4.
22. GEER, Dan; OEST, Adam; FARROW, Rik. *For Good Measure, Effectively Monitoring the Health of the Anti-phishing Ecosystem* [online]. usenix, 2021-04 [cit. 2024-03-01]. Dostupné z: https://www.usenix.org/publications/loginonline/effectively-monitoring-health-anti-phishing-ecosystem.
23. *CryptoLocker Ransomware Information Guide and FAQ* [online]. Bleeping Computer, 2013-10 [cit. 2024-03-01]. Dostupné z: https://www.bleepingcomputer.com/virus-removal/cryptolocker-ransomware-information.
24. BRENNER, Bill. *WannaCry: the ransomware worm that didn't arrive on a phishing hook* [online]. Naked Security, 2017-05 [cit. 2024-03-01]. Dostupné z: https://web.archive.org/web/20170711015125/https://nakedsecurity.sophos.com/2017/05/17/wannacry-the-ransomware-worm-that-didnt-arrive-on-a-phishing-hook/.
25. *What is business email compromise (BEC)?* [Online]. Microsoft, © 2024 [cit. 2024-03-01]. Dostupné z: https://www.microsoft.com/en-us/security/business/security-101/what-is-business-email-compromise-bec.
26. *X-Force Threat Intelligence Index 2023* [online]. Armonk, NY, 2023-02 [cit. 2024-02-26]. Tech. zpr. IBM. Dostupné z: https://mysecuritymarketplace.com/mp-files/x-force-threat-intelligence-index-2023.pdf/.

27. *Twitter Investigation Report* [online]. Department of Financial Services, 2020-10 [cit. 2024-03-01]. Dostupné z: https://www.dfs.ny.gov/Twitter_Report.
28. *What is domain spoofing? | Website and email spoofing* [online]. Cloudflare [cit. 2024-03-01]. Dostupné z: https://www.cloudflare.com/learning/ssl/what-is-domain-spoofing/.
29. *Masquerading: Double File Extension* [online]. Mitre ATT&CK, 2024-08 [cit. 2024-03-01]. Dostupné z: https://attack.mitre.org/versions/v14/techniques/T1036/007/.
30. *Phishingová kampaň* [online]. Pentesty, © 2023 [cit. 2024-03-04]. Dostupné z: https://pentesty.cz/sluzby/phishingova-kampan/.
31. WEDOS. *Phishingové kampaně a na co si dát pozor* [online]. Blog WEDOS, 2022-04 [cit. 2024-03-04]. Dostupné z: https://blog.wedos.com/cs/phishingove-kampane-a-na-co-si-dat-pozor.
32. BADMAN, Annie. *What is a phishing simulation?* [Online]. Armonk, NY: IBM, 2023-08 [cit. 2024-03-04]. Dostupné z: https://www.ibm.com/blog/phishing-simulation/.
33. *How To Phish Your Employees* [online]. KnowBe4 [cit. 2024-03-04]. Dostupné z: https://www.knowbe4.com/resources/how-to-phish-your-employees/.
34. *What is an attack vector?* [Online]. Cloudflare, © 2024 [cit. 2024-02-26]. Dostupné z: https://www.cloudflare.com/learning/security/glossary/attack-vector/.
35. ADAIR, Steven; LANCASTER, Thomas; RESEARCH, Volexity Threat. *DriftingCloud: Zero-Day Sophos Firewall Exploitation and an Insidious Breach* [online]. Volexity, 2022-06 [cit. 2024-02-26]. Dostupné z: https://www.volexity.com/blog/2022/06/15/driftingcloud-zero-day-sophos-firewall-exploitation-and-an-insidious-breach/.
36. *Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and "PrintNightmare" Vulnerability* [online]. CISA, 2022-03 [cit. 2024-02-26]. Dostupné z: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-074a.
37. *Valid Accounts* [online]. Mitre ATT&CK, 2017-05 [cit. 2024-02-26]. Dostupné z: https://attack.mitre.org/versions/v14/techniques/T1078/.
38. MITRE. *CVE-2016-6662 Detail* [online]. NIST, 2016-09 [cit. 2024-02-26]. Dostupné z: https://nvd.nist.gov/vuln/detail/CVE-2016-6662.
39. *Microsoft Security Bulletin MS17-010 - Critical* [online]. Microsoft, 2017-03 [cit. 2024-02-26]. Dostupné z: https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010.
40. MITRE. *CVE-2014-7169 Detail* [online]. NIST, 2014-09 [cit. 2024-02-26]. Dostupné z: https://nvd.nist.gov/vuln/detail/CVE-2014-7169.
41. *Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices* [online]. CISA, 2018-04 [cit. 2024-02-26]. Dostupné z: https://www.cisa.gov/news-events/alerts/2018/04/16/russian-state-sponsored-cyber-actors-targeting-network-infrastructure.
42. SANTOS, Omar. *Attackers Continue to Target Legacy Devices* [online]. Cisco Systems, 2020-10 [cit. 2024-02-26]. Dostupné z: https://community.cisco.com/t5/security-blogs/attackers-continue-to-target-legacy-devices/ba-p/4169954.
43. *Exploit Public-Facing Application* [online]. Mitre ATT&CK, 2018-04 [cit. 2024-02-26]. Dostupné z: https://attack.mitre.org/versions/v14/techniques/T1190/.
44. II, Augusto Remillano; COLLADO, Patrick Noel; TITIWA, Karen Ivy. *XORDDoS, Kaiji Variants Target Exposed Docker Servers* [online]. Trend Micro, 2020 [cit. 2024-02-26]. Dostupné z: https://www.trendmicro.com/en_us/research/20/f/xorddos-kaiji-botnet-malware-variants-target-exposed-docker-servers.html.

45. CHEN, Jay; SASSON, Aviv; ZELIVANSKY, Arial. *Hildegard: New TeamTNT Cryptojacking Malware Targeting Kubernetes* [online]. Palo Alto Networks, 2021-02 [cit. 2024-02-26]. Dostupné z: https://unit42.paloaltonetworks.com/hildegard-malware-teamtnt/.
46. *External Remote Services* [online]. Mitre ATT&CK, 2017-05 [cit. 2024-02-26]. Dostupné z: https://attack.mitre.org/versions/v14/techniques/T1133/.
47. *Phishing* [online]. Mitre ATT&CK, 2020-03 [cit. 2024-02-26]. Dostupné z: https://attack.mitre.org/versions/v14/techniques/T1566/.
48. *Kybernetické incidenty pohledem NÚKIB, LEDEN 2023* [online]. Brno, 2023-01 [cit. 2024-02-23]. Tech. zpr. NÚKIB. Dostupné z: https://nukib.gov.cz/download/publikace/vyzkum/2023-01_Kyberneticke_incidenty.pdf.
49. *Kybernetické incidenty pohledem NÚKIB, ÚNOR 2023* [online]. Brno, 2023-02 [cit. 2024-02-23]. Tech. zpr. NÚKIB. Dostupné z: https://nukib.gov.cz/download/publikace/vyzkum/2023-02_Kyberneticke-incidenty.pdf.
50. *Kybernetické incidenty pohledem NÚKIB, BŘEZEN 2023* [online]. Brno, 2023-03 [cit. 2024-02-23]. Tech. zpr. NÚKIB. Dostupné z: https://nukib.gov.cz/download/publikace/vyzkum/Kyberneticke%20incidenty%20pohledem%20NUKIB_brezen%202023.pdf.
51. *Kybernetické incidenty pohledem NÚKIB, DUBEN 2023* [online]. Brno, 2023-04 [cit. 2024-02-23]. Tech. zpr. NÚKIB. Dostupné z: https://nukib.gov.cz/download/publikace/vyzkum/Kyberneticke%20incidenty%20pohledem%20NUKIB%20-%20duben%202023.pdf.
52. *Kybernetické incidenty pohledem NÚKIB, KVĚTEN 2023* [online]. Brno, 2023-05 [cit. 2024-02-23]. Tech. zpr. NÚKIB. Dostupné z: https://nukib.gov.cz/download/publikace/vyzkum/Kyberneticke%20incidenty%20pohledem%20NUKIB%20-%20kveten%202023.pdf.
53. *Kybernetické incidenty pohledem NÚKIB, ČERVEN 2023* [online]. Brno, 2023-06 [cit. 2024-02-23]. Tech. zpr. NÚKIB. Dostupné z: https://nukib.gov.cz/download/publikace/vyzkum/Kyberneticke%20incidenty%20pohledem%20NUKIB%20-%20cerven%202023.pdf.
54. *Kybernetické incidenty pohledem NÚKIB, ČERVENEC 2023* [online]. Brno, 2023-07 [cit. 2024-02-23]. Tech. zpr. NÚKIB. Dostupné z: https://nukib.gov.cz/download/publikace/vyzkum/kyberneticke-incidenty-pohledem-NUKIB-cervenec-2023.pdf.
55. *Kybernetické incidenty pohledem NÚKIB, SRPEN 2023* [online]. Brno, 2023-08 [cit. 2024-02-23]. Tech. zpr. NÚKIB. Dostupné z: https://nukib.gov.cz/download/publikace/vyzkum/kyberneticke-incidenty-pohledem-NUKIB-srpen-2023.pdf.
56. *Kybernetické incidenty pohledem NÚKIB, ZÁŘÍ 2023* [online]. Brno, 2023-09 [cit. 2024-02-23]. Tech. zpr. NÚKIB. Dostupné z: https://nukib.gov.cz/download/publikace/vyzkum/kyberneticke-incidenty-pohledem-NUKIB-zari-2023.pdf.
57. *Kybernetické incidenty pohledem NÚKIB, ŘÍJEN 2023* [online]. Brno, 2023-10 [cit. 2024-02-23]. Tech. zpr. NÚKIB. Dostupné z: https://nukib.gov.cz/download/publikace/vyzkum/kyberneticke-incidenty-pohledem-NUKIB-rijen-2023.pdf.
58. *Kybernetické incidenty pohledem NÚKIB, LISTOPAD 2023* [online]. Brno, 2023-11 [cit. 2024-02-23]. Tech. zpr. NÚKIB. Dostupné z: https://nukib.gov.cz/download/publikace/vyzkum/Kyberneticke-incidenty-pohledem-NUKIB-listopad-2023.pdf.
59. *Kybernetické incidenty pohledem NÚKIB, PROSINEC 2023* [online]. Brno, 2023-12 [cit. 2024-02-23]. Tech. zpr. NÚKIB. Dostupné z: https://nukib.gov.cz/download/publikace/vyzkum/kyberneticke-incidenty-pohledem-NUKIB-prosinec-2023.pdf.

60. *ZPRÁVA O STAVU KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY ZA ROK 2022* [online]. Brno, 2023-07 [cit. 2024-02-23]. Tech. zpr. NÚKIB. Dostupné z: https://nukib.gov.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kyberneticke_bezpecnosti_CR_za_rok_2022.pdf.
61. *ZPRÁVA O STAVU KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY ZA ROK 2020* [online]. Brno, 2021-07 [cit. 2024-02-23]. Tech. zpr. NÚKIB. Dostupné z: https://nukib.gov.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_KB_2020.pdf.
62. *ZPRÁVA O STAVU KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY ZA ROK 2021* [online]. Brno, 2022-06 [cit. 2024-02-23]. Tech. zpr. NÚKIB. Dostupné z: https://nukib.gov.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kybernetick_bezpenosti_2021.pdf.
63. *X-Force Threat Intelligence Index 2024* [online]. Armonk, NY, 2024-02 [cit. 2024-02-23]. Tech. zpr. IBM. Dostupné z: https://branden.biz/wp-content/uploads/2024/02/IBM-XForce-Threat-Intelligence-Index-2024.pdf.
64. PETERKA, Jiří. Spamming. *CHIPweek* [online]. 1998, s. 29–30 [cit. 2024-03-05]. ISSN 1211-1007. Dostupné z: https://www.earchiv.cz/a98/a801k180.php3.
65. KITTERMAN, Scott. *Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1* [RFC 7208]. RFC Editor, 2014 [cit. 2024-03-05]. Request for Comments, č. 7208. Dostupné z DOI: 10.17487/RFC7208.
66. KUCHERAWY, Murray; CROCKER, Dave; HANSEN, Tony. *DomainKeys Identified Mail (DKIM) Signatures* [RFC 6376]. RFC Editor, 2011 [cit. 2024-03-05]. Request for Comments, č. 6376. Dostupné z DOI: 10.17487/RFC6376.
67. *What is Reputation Database?* [Online]. Reason Labs, © 2023 [cit. 2024-03-05]. Dostupné z: https://cyberpedia.reasonlabs.com/EN/reputation%20database.html.
68. BARTOŠ, Václav; ŽÁDNÍK, Martin. *NERD: Network Entity Reputation Database* [online]. CESNET, 2016-06 [cit. 2024-03-05]. Dostupné z: https://sabu.cesnet.cz/_media/cs/reputace-20-6-2016.pdf.
69. PRAKASH, Vipul; O'DONNELL, Adam. Fighting Spam with Reputation Systems. *ACM Queue*. 2005, roč. 3, s. 36–41. Dostupné z DOI: 10.1145/1105664.1105677.
70. LABIANCA, Ivan. *How Spam Filters Work (And How to Stop Emails Going to Spam)* [online]. The Seventh Sense, 2022-05 [cit. 2024-03-05]. Dostupné z: https://www.theseventhsense.com/blog/how-spam-filters-work-and-how-to-stop-emails-going-to-spam.
71. SHERRY, Steve. *How to Use the Microsoft Office 365 External Email Warning* [online]. ATA Learning, 2022-08 [cit. 2024-03-06]. Dostupné z: https://adamtheautomator.com/external-email-warning/.
72. *Zimbra External Email warning* [online]. Zimbra, © 2005 - 2024 [cit. 2024-03-06]. Dostupné z: https://wiki.zimbra.com/wiki/External_domain_warning.
73. *Email Warning Tags* [online]. Seattle, WA: University of Washington, 2024-01 [cit. 2024-03-06]. Dostupné z: https://itconnect.uw.edu/guides-by-topic/email-calendaring/protecting-your-email/email-tags/.
74. ABERLE, Ian. *New Email Tags Provide Warning for Suspicious Messages* [online]. Dallas, TX: Office of Information Technology, Southern Methodist University, 2023-09 [cit. 2024-03-06]. Dostupné z: https://blog.smu.edu/itconnect/2023/09/08/new-outlook-email-tags-warning-suspicious-messages/.
75. HARDT, Dick. *The OAuth 2.0 Authorization Framework* [RFC 6749]. RFC Editor, 2012 [cit. 2024-01-31]. Request for Comments, č. 6749. Dostupné z DOI: 10.17487/RFC6749.

76. DENNISS, William; BRADLEY, John; JONES, Michael B.; TSCHOFENIG, Hannes. *OAuth 2.0 Device Authorization Grant* [RFC 8628]. RFC Editor, 2019. Request for Comments, č. 8628. Dostupné z DOI: 10.17487/RFC8628.

77. DENNISS, William; BRADLEY, John; JONES, Michael B.; TSCHOFENIG, Hannes. *OAuth 2.0 Device Authorization Grant* [RFC 8628]. RFC Editor, 2019 [cit. 2024-01-31]. Request for Comments, č. 8628. Dostupné z DOI: 10.17487/RFC8628.

78. NROMSDAHL-SCWX. *PhishInSuits: OAuth Device Code Phishing with Verified Apps* [online]. Github, 2021 [cit. 2024-01-31]. Dostupné z: https://github.com/secureworks/PhishInSuits/blob/main/README.md.

79. USTAYREADY. *ustayready / CredSniper : About* [online]. Github [cit. 2024-04-19]. Dostupné z: https://github.com/ustayready/CredSniper.

80. SINGH, Udayveer; SATTAR, Usama Abdul; MORSMALLEO; MOLTIVIE; DARKMIDUS; EVSEENKO, Ilja; DESHDEEPAK. *HIDDEN EYE* [online]. Github, 2020 [cit. 2024-01-31]. Dostupné z: https://github.com/Morsmalleo/HiddenEye_Legacy.

81. CRAWL3R41; JALALI, Daniel; KENNEDY, David; HESHAM, Youssef; MYKINGS; HEXWAXWING; MCJUNKIN, Jeff; LECHTHALER, Brian; ROBERTS, Sol; KRASNOV, Aleksandr. *The Social-Engineer Toolkit (SET)* [online]. Github, 2020 [cit. 2024-01-31]. Dostupné z: https://github.com/tatanus/SPF/blob/master/README.md.

82. COMPTON, Adam. *README* [online]. Github, 2019 [cit. 2024-01-31]. Dostupné z: https://github.com/tatanus/SPF/blob/master/README.md.

83. RAYAT, Tahmid; SHAKYA, Aditya; SAVAGE, Russ; TAPIA, Moises; 1RAY-1. *Zphisher* [online]. Github, 2023 [cit. 2024-01-31]. Dostupné z: https://github.com/htr-tech/zphisher/blob/master/README.md.

84. GRETZKY, Kuba; WIKIJM; FLORES, Alex; PIAZZA, Antonio; 0XACAB. *Evilginx 3.0* [online]. Github, 2018 [cit. 2024-02-02]. Dostupné z: https://github.com/kgretzky/evilginx2/blob/master/README.md.

85. ANTISNATCHOR; TROTTA, Giuseppe. *Muraena README* [online]. Github, 2019 [cit. 2024-02-02]. Dostupné z: https://github.com/muraenateam/muraena/blob/master/README.md.

86. KING, Chris. *FiercePhish* [online]. Github, 2016 [cit. 2024-01-31]. Dostupné z: https://github.com/Raikia/FiercePhish/blob/master/README.md.

87. WRIGHT, Jordan; WILKINSON, Glenn; WOODSON, Will; SWITHAK; KITAGAWA, Shuhei; TUYL, Russel Van; XTRASIMPLICITY; BUTLER, Allen. *Gophish* [online]. Github, 2022 [cit. 2024-01-31]. Dostupné z: https://github.com/gophish/gophish/blob/master/README.md.

88. MCINTYRE, Spencer; Y4UTJ4; GATES, Tim. *King Phisher* [online]. Github, 2022 [cit. 2024-01-31]. Dostupné z: https://github.com/rsmusllp/king-phisher/blob/master/README.md.

89. ŠEBELA, Martin. *Phishingator* [online]. Github, 2024 [cit. 2024-01-31]. Dostupné z: https://github.com/CESNET/Phishingator/blob/main/README.md.

90. ŠEBELA, Martin. *Systém pro rozesílání cvičných phishingových zpráv* [online]. 2019. [cit. 2024-01-31]. Dostupné z: https://dspace5.zcu.cz/bitstream/11025/38276/1/BP_Sebela_Martin.pdf. SUPERVISOR: Ing. Aleš Padrta, Ph.D.

91. MCCANN, Brandon; MCCARTHY, Thomas; RINGWOOD, Adam; DALTON, Adam; ORRU, Michele; JOHNSON, Alton. *About* [online]. Wayback Machine [cit. 2024-01-31]. Dostupné z: https://web.archive.org/web/20220122122610/https://www.phishingfrenzy.com/about.

92. SHORT, Chris. *chris-short / sptoolkit : About* [online]. Github [cit. 2024-04-19]. Dostupné z: https://github.com/chris-short/sptoolkit.

93. *UndeadSec / SocialFish: About* [online]. Github [cit. 2024-04-19]. Dostupné z: https://github.com/UndeadSec/SocialFish.

94. GEORGE, Gem; HARIDAS, Sreehari; SVEN-HASH. *SniperPhish* [online]. Github, 2023 [cit. 2024-01-31]. Dostupné z: https://github.com/GemGeorge/SniperPhish/blob/main/README.md.

95. ZION3R. *Phishing Frenzy - Ruby on Rails Phishing Framework* [online]. KitPloit - PenTest & Hacking Tools, 2016-05 [cit. 2024-03-11]. Dostupné z: https://www.kitploit.com/2016/05/phishing-frenzy-ruby-on-rails-phishing.html.

96. MCCANN, Brandon. *Phishing Frenzy: Increase Reporting Fu* [online]. Pentest Geek, 2014-06 [cit. 2024-03-11]. Dostupné z: https://www.pentestgeek.com/phishing/phishing-frenzy-increase-reporting-fu.

97. ŠEBELA, Martin. *Phishingator – Uživatelská příručka* [online]. Github, 2023 [cit. 2024-01-31]. Dostupné z: https://github.com/CESNET/Phishingator/blob/main/MANUAL.md.

98. ŠEBELA, Martin. *globalFunctions.php* [online]. Github, 2023-11 [cit. 2024-03-29]. Dostupné z: https://github.com/CESNET/Phishingator/blob/95c8ba5795cd2ee5508d424cc038bd97dd5d487e/src/globalFunctions.php.

99. ŠEBELA, Martin. *PermissionsModel.php* [online]. Github, 2023-11 [cit. 2024-03-29]. Dostupné z: https://github.com/CESNET/Phishingator/blob/95c8ba5795cd2ee5508d424cc038bd97dd5d487e/src/core/models/PermissionsModel.php.

100. ŠEBELA, Martin. *Phishingator* [online]. Github, 2022-11 [cit. 2024-03-29]. Dostupné z: https://github.com/CESNET/Phishingator/blob/main/doc/images/05-campaign-stats.png.

101. KROMPHARDT, Timothy. *MFA Bypass PSA, Oh My!* [Online]. Proofpoint, 2022-02 [cit. 2024-04-28]. Dostupné z: https://www.proofpoint.com/us/blog/threat-insight/mfa-psa-oh-my.

102. ŠEBELA, Martin. *CredentialsTesterModel.php* [online]. Github, 2023-11 [cit. 2024-04-12]. Dostupné z: https://github.com/CESNET/Phishingator/blob/95c8ba5795cd2ee5508d424cc038bd97dd5d487e/src/core/models/CredentialsTesterModel.php.

103. ŠEBELA, Martin. *LdapModel.php* [online]. Github, 2023-11 [cit. 2024-05-05]. Dostupné z: https://github.com/CESNET/Phishingator/blob/95c8ba5795cd2ee5508d424cc038bd97dd5d487e/src/core/models/LdapModel.php.

104. *The end of the road* [online]. Wayback Machine, 2013-07 [cit. 2024-04-25]. Dostupné z: https://web.archive.org/web/20150321031053/http://sptoolkit.com/the_end.php.

105. GRETZKY, Kuba. *Evilginx 3.3 - Go & Phish* [online]. Kuba Gretzky, 2024-04 [cit. 2024-04-25]. Dostupné z: https://breakdev.org/evilginx-3-3-go-phish/.

106. GRETZKY, Kuba. *added integration with evilginx 3.3* [online]. Github, 2024-04 [cit. 2024-04-25]. Dostupné z: https://github.com/kgretzky/gophish/commit/c54f868a6f0b14dea720d274957a75bcb55a0d5a.

107. *Security awareness training & phishing simulations* [online]. Infosec Institute, © 2023 [cit. 2024-02-20]. Dostupné z: https://www.infosecinstitute.com/iq/.

108. WAITE, Emma; REED, Hunter. *Infosec IQ Essentials* [online]. slideshare, 2019 [cit. 2024-02-20]. Dostupné z: https://www.slideshare.net/InfoSecInstituteEdu/infosec-iq-essentials-162358063.

109. WAITE, Emma; REED, Hunter. *Customizing Email Templates* [online]. slideshare, 2019 [cit. 2024-02-20]. Dostupné z: https://image.slidesharecdn.com/infoseciqessentialsupdatedaugust2019-190808162559/75/infosec-iq-essentials-9-2048.jpg?cb=1668883849.

110. *Track security awareness results easier than ever* [online]. Infosec Institute, © 2023 [cit. 2024-02-20]. Dostupné z: https://www.infosecinstitute.com/iq/reporting/dashboards/.

111. LUCY. *Introduction* [online]. LUCY, 2022 [cit. 2024-02-20]. Dostupné z: https://wiki.lucysecurity.com/doku.php?id=mail_delivery_methods_in_lucy.

112. LUCY. *How to Create a campaign by enabling the Expert Setup* [online]. LUCY, 2021 [cit. 2024-02-20]. Dostupné z: https://wiki.lucysecurity.com/doku.php?id=expert_mode_campaign_creation.

113. LUCYSECURITY. *Where can I create my phishing reports?* [Online]. LUCY, 2021 [cit. 2024-02-20]. Dostupné z: https://wiki.lucysecurity.com/doku.php?id=create_campaign_reports.

114. LUCYSECURITY. *Introduction* [online]. LUCY, 2021 [cit. 2024-02-20]. Dostupné z: https://wiki.lucysecurity.com/doku.php?id=user_management.

115. *Prevent cyber incidents by changing employee behaviour* [online]. Phished, © 2024 [cit. 2024-02-20]. Dostupné z: https://phished.io/product-overview.

116. JONES, Caitlin. *Phished Automated Cybersec Awareness Training* [online]. Expert Insights, 2022 [cit. 2024-02-20]. Dostupné z: https://expertinsights.com/reviews/phished.

117. *Cost-effective, Flexible Plans* [online]. PhishingBox, © 2024 [cit. 2024-02-21]. Dostupné z: https://www.phishingbox.com/pricing.

118. *Phishing Simulator* [online]. PhishingBox, © 2024 [cit. 2024-02-21]. Dostupné z: https://www.phishingbox.com/platform/phishing-simulator.

119. *Sophos Phish Threat* [online]. Sophos, © 2022 [cit. 2024-02-21]. Dostupné z: https://assets.sophos.com/X24WTUEQ/at/2zknxxmrgtvv5z36qnc66wfc/sophos-phish-threat-ds.pdf.

120. SOPHOS. *Sophos Phish Threat Overview* [video]. Vimeo, 2017 [cit. 2024-02-21]. Dostupné z: https://vimeo.com/197921680.

121. *Sophos Phish Threat* [online]. Sophos, 2019-04 [cit. 2024-04-25]. Dostupné z: https://assets.sophos.com/X24WTUEQ/at/5x4w2g3r6hkgs8sm4jcp26fv/sophos-phish-threat-outlook-addin-ds.pdf.

122. FAHAD ALGHENAIM, Mohammed; AZALIAH ABU BAKAR, Nur; ABDUL RAHIM, Fiza binti. Reviewing Cybersecurity Awareness Training Tools Used to Address Phishing Attack at the Workplace. *Information Sciences Letters* [online]. 2022, roč. 11, č. 2. Dostupné také z: https://digitalcommons.aaru.edu.jo/isl/vol11/iss2/10.

Obsah příloh

- `readme.txt` ..... stručný popis obsahu média
- `addon` ..... zdrojový kód pro PHP aplikaci
- `phishing` ..... podkladové soubory které byly importovány jako emaily do aplikace Gophish
  - `briefing`
    - `d1` ..... adresář s poučným textem pro první záminku
    - `d2` ..... adresář s poučným textem pro druhou záminku
- `PhishingSWFeatureTable.ods` ..... tabulka se soupisem vlastností zkoumaných programů