Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

3. DUBNA 2020

PODVODNÉ E-MAILY NEBO ZPRÁVY NA SOCIÁLNÍCH SÍTÍCH NA MÍRU: SPEAR-PHISHING A JAK SE PŘED NÍM CHRÁNIT

SHRNUTÍ

Spear-phishing je jedním z nejčastějších vektorů kybernetických útoků (způsob infiltrace cílového zařízení) a jím způsobené škody se ročně globálně pohybují v desítkách až stovkách miliard korun. Sofistikovanost útočníků se přitom zvyšuje, a pro uživatele je stále těžší rozpoznat falešné e-maily nebo zprávy na sociální síti. Ty se stávají stále přesvědčivějšími a aktuálnějšími (využívají například pandemie koronaviru) a často obsahují přílohu se škodlivým kódem, kterou stačí otevřít, nebo odkaz na nakažené stránky, které stačí navštívit a informační systém oběti se dostane pod kontrolu hackerů. Zatímco o úspěchu útoku může rozhodnout kliknutí jediného zaměstnance, obrana proti spear-phishingu je výrazně složitější a vyžaduje technická, procesní a personální opatření. Své zkušenosti se spear-phishingem v České republice mají například nemocnice, univerzity nebo finanční instituce, od kterých chtěli útočníci podvodnými e-maily získat přihlašovací údaje a peníze.

Doporučení pro uživatele:

- Nepovolovat makra v programech
- Slepě neotevírat přílohy a odkazy v e-mailech
- Kontrolovat e-mailovou adresu v případě urgentních nebo neobvyklých požadavků
- V případě nejistoty nebo podezření kontaktovat IT oddělení
- Omezit sdílení informací o zaměstnání na sociálních sítích

UPOZORNĚNÍ: Informace a závěry obsažené v této analýze vycházejí z veřejně dostupných informací a z informací získaných v rámci činnosti NÚKIB v době publikace. Jedná se o analýzu kybernetické bezpečnosti z pohledu NÚKIB na základě jemu dostupných informací.

SPEAR-PHISHING: KYBERNETICKÉ ÚTOKY S VYUŽITÍM SOCIÁLNÍHO INŽENÝRSTVÍ

Spear-phishing je personalizovaná forma podvodných e-mailů (phishingu, viz Box 1), která cílí na konkrétní osobu nebo skupinu osob. Základem útoku je tzv. sociální inženýrství, tedy techniky manipulace oběti k tomu, aby se chovala způsobem, který není v jejím zájmu. V kontextu kybernetické bezpečnosti jde většinou o snahu získat od cílové oběti konkrétní informace (např. heslo) nebo uživatele přesvědčit ke stažení přílohy obsahující malware (obecné označení pro škodlivý software) a jejímu otevření.

Spear-phishing je jednou z primárních technik, kterou využívají zločinci i sofistikovaní útočníci (zejména státy podporované skupiny hackerů[1]) k získání přístupu do sítě oběti[2], ať už za účelem špionáže nebo způsobení škod.

Útočníci cílí spear-phishingové e-maily na řadové zaměstnance i vedení organizací. Motivací útočníků může být finanční zisk (ransomware, falešné faktury), krádež dat nebo vyřazení systémů. Zatímco kyberzločinci usilují primárně o peněžní zisk a zpeněžitelná data, APT skupiny (vysoce sofistikované skupiny útočníků) se zaměřují na utajovaná a jinak citlivá data a existují i případy sabotáže systémů, které pro zasažené společnosti a instituce znamenaly ztráty v řádu desítek až stovek milionů korun a přerušení služeb pro desítky tisíc lidí.

Podle výroční studie bezpečnostní společnosti Proofpoint[6] se v roce 2018 z 15 000 dotazovaných odborníků v informační a kybernetické bezpečnosti 64 % z nich setkalo s případy spear-phishingu. Proti roku 2017 jde o 11% nárůst.

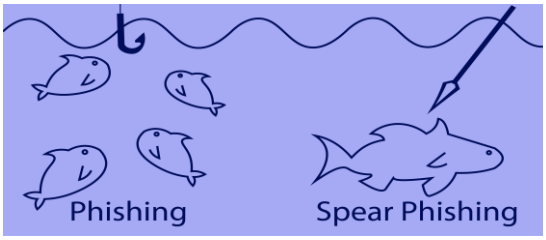
Útok vyžaduje přípravu, v rámci níž útočník musí identifikovat konkrétní osobu v organizaci, které pošle spear-phishingový e-mail. Útočník musí mít zároveň dostatečné znalosti k tomu, aby dokázal vytvořit takový e-mail, jenž bude působit věrohodně a nevzbudí u oběti pochybnosti (viz Příloha 2).

Příklad velmi závažných dopadů otevření spear-phishingového e-mailu lze najít na Ukrajině, kdy došlo k výpadku elektrické energie pro 230 tisíc lidí až na šest hodin. Na počátku útoku stál spear-phishingový e-mail se škodlivou přílohou v podobě malware BlackEnergy.[3]

Kyberzločinci v roce 2019 pomocí spear-phishingového e-mailu nakazili systémy amerického města Baltimore ransomwarem RobbinHood. Obnova systémů a ušlý zisk město přišly na 18 milionů dolarů (408 milionů Kč).[4]

Příkladem úspěšného útoku s vážnými důsledky, za kterým pravděpodobně stojí státem sponzorovaná APT skupina, je útok proti dánské lodní společnosti Maersk z roku 2017. Následkem útoku, který téměř jistě začal spear-phishingovým e-mailem obsahující přílohu s malwarem NotPetya, byla finanční ztráta Maersk až 300 milionů dolarů (6,8 miliardy Kč) a nutnost reinstalace 4 tisíc serverů a 45 tisíc počítačů.[5]

Obr.1: Zatímco při phishingu není cílová skupina vymezena, při spear-phishingu je cílem konkrétní jednotlivec nebo specifická skupina (např. zaměstnanci firmy XY)



Zdroj: crossrealms.com

S phishingem ve formě textových zpráv a telefonátů se v roce 2018 setkalo 49 % odborníků. S útokem pomocí USB (vložení nakaženého disku do počítače) se setkaly 4 % odborníků. Část těchto útoků byla téměř jistě cílena na konkrétní osoby či organizace a měla tedy charakter spear-phishingu.

Obecně lze říci, že kombinace nedostatečného vzdělání zaměstnanců v oblasti kybernetické bezpečnosti a zvyšující se sofistikovanost spear-phishingových e-mailů vede k vysoké statistice úspěšných útoků, které mají významné finanční dopady. Kromě přímých finančních ztrát zaviněných krádeží, nedostupností služeb a následnou nápravou mohou postižené firmy čelit i vysokým pokutám, pokud útočníci získají osobní a citlivé údaje zákazníků.

Box 1: Phishing

Phishing (česky také rhybaření) je typem sociálního inženýrství a má zpravidla podobu e-mailu, SMS, telefonátu nebo zprávy na sociální síti, ve které se útočník snaží přesvědčit oběť, aby mu poskytla citlivou informaci, otevřela odkaz vedoucí na škodlivou stránku, ze které stáhne malware nebo otevřela přiložený soubor obsahující malware. Na rozdíl od spear-phishingu není personalizovaný a zpravidla je odesílán velkému množství lidí najednou. Příkladem nepříliš sofistikovaného phishingu byly v ČR v roce 2018 vyděračské e-maily, ve kterých útočníci sdělují oběti, že přes webovou kameru získali choulostivé záběry a vyhrožují jejich zveřejněním. Aby tomu oběť zabránila, měla poslat částku v řádech stovek dolarů v bitcoinech.

DISTRIBUCE SPEAR-PHISHINGU: E-MAIL, TEXTOVÉ ZPRÁVY, TELEFONÁTY, SOCIÁLNÍ SÍTĚ I USB

Tradiční platformou pro spear-phishing je e-mail (podrobněji k emailovým útokům viz Příloha 2), ale výjimkou nejsou ani podvodné SMS (smishing), telefonáty (vishing) či zprávy na sociálních sítích.

V rámci vishingu se útočník může vydávat za pracovníka stejné organizace, např. z technické podpory, který po uživateli může požadovat přihlašovací údaje kvůli aktualizaci systému skrze vzdálený přístup. Pokud mu je uživatel skutečně prozradí, útočník pak získá kompletní přístup do systému oběti.

S rozvojem sociálních sítí se stále častěji vyskytují i případy phishingu a spear-phishingu na sociálních sítích. Podle společnosti Proofpoint[6] se v roce 2018 případy phishingu na sociálních sítích proti předchozímu roku zvýšily o 442 % a podobný několikanásobný meziroční nárůst byl zaznamenán i v předešlých letech.[7] **Fyzickou formou spear-phishingu (metoda, které se také říká „baiting“) může být i pohozený USB disk v blízkosti vytipovaného cíle**, například na parkovišti pracoviště zaměstnance. Útočník spoléhá na zvědavost zaměstnanců, kteří disk najdou a na to, že disk připojí do pracovního počítače připojeného k cílové síti. Disk může obsahovat například škodlivý kód, který útočníkovi umožní přístup do sítě.

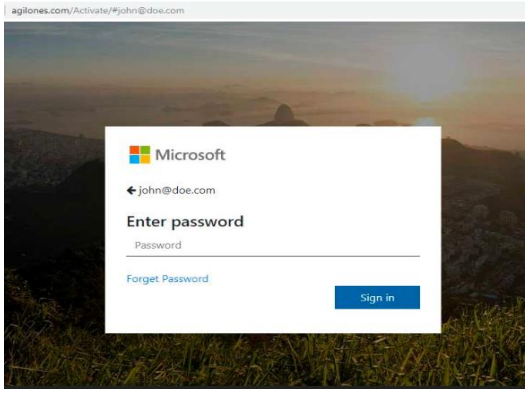
TRENDY SPEAR-PHISHINGU: POZOR NA ÚTERKY A SEXUÁLNÍ VYDÍRÁNÍ

V březnu 2019 vydala bezpečnostní firma Barracuda Networks zprávu o trendech v oblasti spear-phishing.[8]

E-maily napodobující obchodní značku

Není překvapením, že 83 % útočníků ve spear-phishingových e-mailech předstírají příslušnost ke známé značce (Microsoft, Apple, finanční instituce). Tím zvyšují legitimitu své zprávy a zároveň mají větší šanci, že se dostanou přes filtr e-mailového klienta, který blokuje podezřelé e-maily a spam. Tyto útoky se zaměřují především na instalaci malware nebo na krádež přihlašovacích údajů. V e-mailu bývá odkaz na více či méně věrnou přihlašovací stránku služby, kterou útočníci napodobují. Poté, co uživatelé zadají své heslo, získají útočníci přístup k legitimnímu účtu uživatele, a mohou ukrást důvěrná data nebo účet využít k dalším útokům.

Obr. 3: Falešná přihlašovací stránka Microsoft, která je téměř identická s pravou. Podvrh lze často poznat podle neodpovídající webové adresy.



Zdroj: bleepingcomputer.com

„Požadavek" jako nejběžnější předmět e-mailu

V rámci spear-phishingových útoků, jejichž cílem je okrást pod falešnou záminkou organizaci o peníze (tedy zpravidla útok bez použití nakažené přílohy), je nejčastějším předmětem e-mailu jednoduše „požadavek" (angl. request).

Sexuální vydírání

Podle Barracuda Networks je 1 z 10 spear-phishingových e-mailů právě sexuální vydírání. Českému uživateli je tento typ sexuálního vydírání znám například jako phishingová kampaň z roku 2018, v rámci které útočníci rozesílali e-maily, ve kterých česky nebo anglicky vyhrožovali, že pokud dotyčný nezaplatí určitou částku, rozešlou intimní video natočené webkamerou počítače oběti všem jejím kontaktům.[9] Jazyk phishingového e-mailu se nezdál být psán rodilým mluvčím a působil tedy relativně nedůvěryhodně. Před touto kampaní varovala i Policie ČR.[10]

V posledním roce se rozmohla i spear-phishingová varianta, která je cílená a mnohem sofistikovanější. Útočníci využívají databáze jmen, e-mailů, hesel a dalších uživatelských dat, které jsou dostupné na černém trhu nebo na hackerských fórech. Stejně jako v případě phishingové kampaně oběti vyhrožují, že pokud nezašle určitý obnos, zveřejní citlivé materiály (obrázky, videa), které údajně mají. Na rozdíl od předchozího případu však útočníci svou hrozbu podepřou znalostí údajů, které získali ze zmíněných databází, což jejich výhružce dodá větší důvěryhodnost.

Úterý jako nejčastější den pro spear-phishing

Uživatelé mohou spear-phishingové e-maily očekávat každý den v týdnu, útoky vrcholí především v úterý (20 %) se středou a čtvrtkem v závěsu (oba dny 19 %).

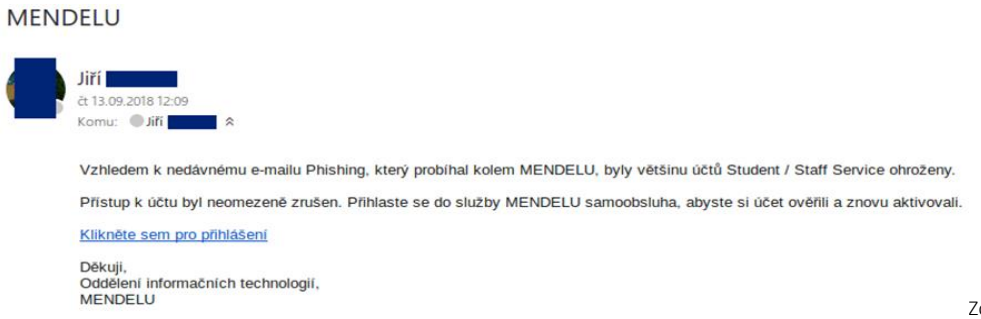
Box 2: Podvodné emaily zneužívající epidemie Koronaviru a zdravotnictví jako cíl

Kyberzločinci začali v první polovině roku využívat korona viru (Covid-19) a rozesílají podvodné zprávy napodobující legitimní e-maily od Světové zdravotnické organizace (WHO), Amerického centra pro kontrolu a prevenci nemocí (CDC) nebo rozesílají e-maily vydávající se za kolující seznam opatření uvalených na mezinárodní obchod a dopravu. První dva případy oběť přesměrují na falešné stránky, kam by měla zadat své přihlašovací údaje a ve třetím případě je u e-mailu přiložen wordový dokument, který obsahuje malware.

Cílem útočníků se ve zvýšené míře stane pravděpodobně sektor zdravotnictví. Nemocnice a další zařízení vystavené útoku ransomware mohou být v případě přetížení více ochotné zaplatit výkupné v hodnotě milionů korun, spíše než zdlouhavě obnovovat systémy. Vektorem útoku je v případě ransomware velmi často právě spear-phishing nebo phishing.

Více o varování naleznete na stránkách GovCERT.

Obr. 5: Příklad spear-phishingového e-mailu adresovaného Mendelově univerzitě obsahuje množství chyb, ale používá jméno reálného pracovníka včetně fotografie a zaštiťuje se reálným technickým oddělením univerzity, čímž nabývá na věrohodnosti.


MENDELU

Jiří [redacted]
čt 13.09.2018 12:09
Komu: Jiří [redacted]

Vzhledem k nedávnému e-mailu Phishing, který probíhal kolem MENDELU, byly většinu účtů Student / Staff Service ohroženy.

Přístup k účtu byl neomezeně zrušen. Přihlaste se do služby MENDELU samoobsluha, abyste si účet ověřili a znovu aktivovali.

Klikněte sem pro přihlášení

Děkuji,
Oddělení informačních technologií,
MENDELU

Zdroj: utb.cz

SPEAR-PHISHINGOVÉ KAMPANĚ V ČR: UNIVERZITY V HLEDÁČKŮ ÚTOČNÍKŮ

Bezpečnostní tým Masarykovy univerzity (CSIRT MU) v září 2018 varoval před phishingovou kampaní, která postihla několik českých univerzit a jejímž cílem byla krádež výzkumných dat, nepublikovaných výsledků nebo know-how výzkumných skupin. Jejich zájmem byla data z různých oborů, jako například lékařství, technické obory nebo humanitní vědy. **Jednalo se o dobře připravené útoky, při nichž útočníci prokázali znalost prostředí českých univerzit.** Text phishingového mailu sice nebyl psaný dobrou češtinou a obsahoval množství chyb, zašťiťoval se ale reálným IT oddělením univerzity a zneužíval jméno reálného správce včetně jeho fotografie, čímž nabýval na věrohodnosti.

Útočníci po svých obětech požadovali aktivaci jejich účtů v Office 365, které byly údajně z důvodů probíhající phishingových útoků dočasně zrušeny. K aktivaci měly oběti použít odkaz v e-mailu. Ten byl ale ve skutečnosti odkazem na podvržené stránky, které svým vzhledem kopírovaly reálné stránky pro přihlášení do systému Office365. V případě, že by oběť své přihlašovací údaje do podvržené stránky zadala, získali by je i útočníci, kterým by to otevřelo vstup do sítí univerzity.[11] Podle dostupných informací nedošlo k žádné kompromitaci.

CSIRT MU v roce 2018 také varoval před podvodnými e-maily, jejichž cílem bylo vylákat ze zaměstnanců ekonomického oddělení peníze. Útočníci použili podvrženou e-mailovou adresu děkana Lékařské fakulty Masarykovy univerzity a jeho jménem žádali ekonomické oddělení o provedení mezinárodní platby. [12] Útočníci s oběťmi dokonce aktivně komunikovali a odpovídali jim na jejich dotazy. K odhalení a nahlášení útoků vedly maličkosti typu vykání (přičemž si oběť s podvrženou osobou tyká) nebo použití nestandartního pozdravu, který je pro danou osobu velmi netypický.

DOPORUČENÍ: JAK SE BRÁNIT?

Zatímco útočník potřebuje od oběti pouze jediné kliknutí k otevření nakažené přílohy, obrana proti spear-phishingu se skládá ze čtyř širokých a vzájemně propojených oblastí, které kombinují technický, procesní i lidský element. V závislosti na kapacitách nejsou všechny aspekty obrany vhodné pro každou organizaci. Některé však vyžadují pouze minimální finanční, časovou i personální

BĚŽNÍ UŽIVATELÉ

Na straně běžných uživatelů je zásadní dodržovat několik bezpečnostních zásad.

- **Nepovolovat makra v programech** (zejména Microsoft Office). V případě, že je použití maker vyžadováno, vždy před jejich povolením ověřit původ dokumentu u jeho odesílatele;
- **Slepě neotevírat přílohy a odkazy v e-mailech**, zejména od neznámých odesílatelů;
- **Kontrolovat e-mailovou adresu v případě urgentních nebo neobvyklých požadavků** (zaplacení faktury, žádost o důvěrné informace);
- **V případě nejistoty nebo podezření o škodlivosti e-mailu kontaktovat IT oddělení** nebo jiné zodpovědné pracoviště;
- **Omezit sdílení informací o zaměstnání na sociálních sítích** a vyhnout se sdílení informací o hierarchii společnosti a bezpečnostních a administrativních procesech.

SPRÁVCI SÍTĚ

1) Omezit přístup útočníka k uživateli

Sofistikovanější útočníci ve svých spear-phishingových e-mailech falšují své adresy tak, aby vypadaly stejně jako adresy v rámci organizace (spoofing). **Tuto techniku lze ztížit pomocí tzv. anti-spoofing nástrojů**. Jde o technologii DMARC (Domain Message Authentication Reporting and Conformance)[12], která ověřuje odesílatelovu doménu, a technologie DKIM (DomainKeys Identified Mail)[13] a SPF (Sender Policy Framework)[14]. Tyto technologie vyhodnocují, který e-mail se dostane k uživateli a který skončí ve spamu.

Šanci na úspěch útočníků lze snížit také omezením informací, které budou o organizaci veřejně dostupné. Jde například o přesnou organizační strukturu organizace nebo životopisy vedení.

Uživatelé by měli rovněž důkladně zvážit, co a s kým budou na internetu sdílet. V tomto směru mohou jednotlivé organizace uživatele informovat o možnostech nastavení soukromí na sociálních sítích, která uživatelům umožní omezit okruh lidí, kteří mohou vidět obsah na jejich profilu. Omezení sdílení informací se týká i detailů o zaměstnání, zejména pak v oblastech kritické infrastruktury, státních úřadů a strategických podniků, o které mají zájem především sofistikované APT skupiny.

Organizace by také měla mít povědomí o tom, jaké informace o ní sdílí třetí strany (partneři, dodavatelé).

3) Pomoci uživatelům identifikovat a nahlásit spear-phishingový e-mail

Cílem tohoto kroku je vytvořit v rámci organizace prostředí, ve kterém se zaměstnanci nebudou obávat nahlásit podezřelý e-mail. K tomu je potřeba v rámci organizace jasně vymezit osobu nebo osoby, kterým lze takové e-maily nahlásit (a jak) a informovat o tom zaměstnance. Vzhledem ke stále vzrůstající sofistikovanosti spear-phishingu je nerealistické očekávat, že uživatelé identifikují 100 % škodlivých e-mailů, ale i minimální školení a seznámení s realitou hrozby může přispět ke snížení rizika.

2) Ochrana organizace před dopady úspěšných spear-phishingových útoků

Pokud včasná detekce hrozby selže, je třeba minimalizovat následky úspěšného útoku. Zde platí univerzální zásady kybernetické bezpečnosti, které se neomezují pouze na spear-phishing:

- Organizace by měla používat anti-virový software;
- V systémech by měl být nainstalovaný legální a podporovaný software aktualizovaný na nejnovější verze;
- Administrátorské účty by měly být limitovány na základě nutné potřeby a nemělo by být možné je používat pro e-mailovou komunikaci nebo surfování po internetu;
- Omezení maker pro Microsoft Office;
- Používání správce hesel dvou-faktorového ověření a (zabrání 99,9 % pokusům o krádež účtu);[15]
- Vytvářet pravidelné zálohy dat v případě jejich kompromitace nebo ztráty.
- Pravidelně provádět hodnocení toho, zda uživatel potřebuje všechna přístupová práva, která má;
- Průběžně mazat účty osob, které již nepůsobí v organizaci.

- **Rychlá reakce na incidenty**

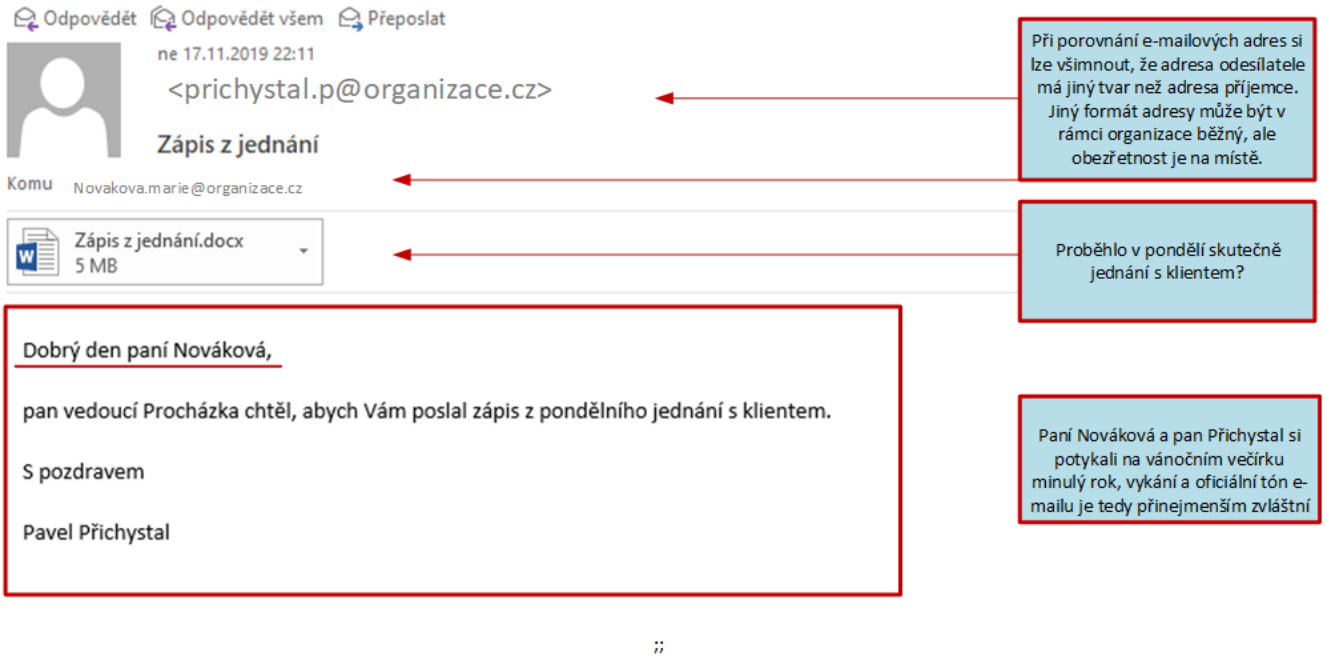
V případě, že dojde ke kompromitaci systémů organizace, měly by být připraveny procesy pro hlášení incidentů a uživatelé by měli mít povědomí o tom, jak a komu tyto incidenty hlásit i v případě, že běžný způsob není kvůli přerušení služby možný (např. přerušení internetového připojení, vyřazení počítačů).

Pokud ve velké organizaci dojde k rozsáhlému útoku, který vyřadí většinu počítačů, IT oddělení bude mít spoustu práce a nebude mít kapacity k řešení individuálních stížností. Z toho důvodu by měla mít organizace připraven plán pro podobné kritické situace, aby všichni zaměstnanci věděli, jak se v případě různých incidentů zachovat.

Další doporučení lze nalézt v dokumentu Spear-phishing a doporučení pro personál nemocnic (viz Příloha 3), Bezpečnostní doporučení NÚKIB pro administrátory 4.0 a Doporučení pro správu sociálních sítí, verze 1.0

PŘÍLOHY:

PŘÍLOHA 1: NA CO SI DÁT U PODEZŘELÝCH E-MAILŮ POZOR



;;

PŘÍLOHA 2: FÁZE SPEAR-PHISHINGU: OD IDENTIFIKACE OBĚTI PO ŠÍŘENÍ MALWARE

1. Identifikace oběti a sběr dat

Před zahájením samotné spear-phishingové kampaně potřebuje útočník **identifikovat konkrétní osobu nebo skupinu osob pracující v cílové organizaci**, proti které bude útok veden. K tomu se zpravidla využívají sociální sítě typu LinkedIn, Facebook, Twitter nebo Instragram, kde uživatelé, často neopatrně, sdílí informace o svém osobním i pracovním životě. Z kombinace informací ze sociálních sítí, webových stránek organizace a dalších dílčích zdrojů mohou útočníci identifikovat zaměstnance, jejich pracovní zařazení a rozhodnout se, kde budou mít spear-phishingové útoky pravděpodobně největší úspěch.

Box 2: Příklad síly sociálních sítí pro sběr informací

To, jak je jednoduché získat významné množství dat o specifické skupině osob ze strategického sektoru, dokázal například experiment centra excelence Stratcom. V něm se podařilo získat velké množství osobních informací o vojácích, kteří se účastnili vojenského cvičení NATO a navést je k chování, které bylo žádoucí pro útočníky (například prozrazení citlivých informací o vojenském cvičení).[18]

Po identifikaci cílových zaměstnanců zpravidla přichází na řadu druhá část první fáze, sběr dat. **Útočníci se snaží získat všechny dostupné informace, které se týkají vybrané osoby**, ať už jde o e-mailové adresy, telefonní čísla, vzdělání, pracovní historii, zájmy, názory, přátele nebo rodinné příslušníky. Důkladná znalost těchto reálií hackerovi umožní připravit útok, který bude vytvořen na míru konkrétními zaměstnanci nebo skupině zaměstnanců (ekonomické oddělení, IT). Sběr informací se netýká jen osob, ale také fungování organizace, její hierarchie a administrativních postupů.

Útočníkům práci zjednodušují i rozsáhlé úniky dat z posledních let, které obsahovaly citlivé údaje desítek až stovek milionů lidí.[17] Naprostá většina se sice netýkala českých občanů, ale to nevylučuje jejich zneužití. Uniklé či zcizené databáze mohou obsahovat jména, příjmení, kontaktní informace, ale i citlivá data jako platební údaje nebo zdravotní stav.

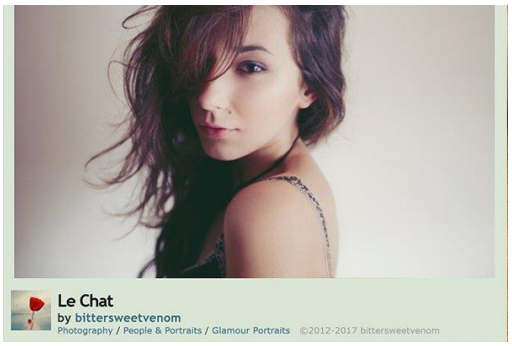
2. Tvorba legendy

Po ukončení první fáze útočník připraví podklady pro samotný útok. V případě klasického spear-phishingu jde většinou o vytvoření e-mailu sestaveného na míru z informací získaných v první fázi. Kvalita spear-phishingových e-mailů se liší v závislosti na přípravě útočníka a obezřetnosti oběti, přičemž cílem je nevzbudit e-mailem podezření a přimět adresáta otevřít přílohu.

Při spear-phishingu na sociálních sítích útočník vytváří falešné profily, které používá buď ke komunikaci s obětí (hlavní profil), nebo k podpoře svého hlavního falešného profilu (přátelé, sdílení, „lajky“ a další aktivity k podpoře autenticity). Hlavní falešné profily často ztělesňují atraktivní mladé ženy, které mají větší šanci na úspěch u mužských obětí.

Íránská APT skupina Cobalt Gypsy od roku 2016 používala falešný profil jménem Mia Ash na sociální síti LinkedIn a Facebook v dlouhodobé phishingové kampani. Z falešného profilu mladé londýnské fotografky íránští hackeři psali lidem pracujících v organizacích převážně na Blízkém východě, Severní Africe a USA. Většinou šlo o zaměstnance telekomunikačních, technologických a ropných společností, tedy zájmové oblasti Íránské vlády. Skrze profil posílali útočníci dokumenty nakažené malwarem, který dal útočníkům rozsáhlý přístup do systému obětí.[19]

Obr. 4: Velký úspěch zaznamenali íránští hackeři s falešným profilem ženy jménem Mia Ash, skrze který posílali nakažené přílohy zájmovým osobám



Zdroj: gulf-insider.com

3. Kontakt

V této fázi vrcholí přípravy z předchozích dvou. Po sběru informací a vytvoření podkladů může útočník navázat kontakt s obětí. Tradičně se jedná o jednorázový e-mail s nakaženou přílohou nebo odkazem vytvořený na míru oběti. Na sociálních sítích může mít kontakt podobu žádosti o přátelství, zprávy v chatu nebo cílené reklamy.

Kontakt je pro útočníka nejkritičtější fází celého útoku a je zcela zásadní nevzbudit u oběti žádné podezření. V případě e-mailů by oběť neměla mít pochybnosti, že jedná s kolegou, nadřízeným, partnerem organizace nebo zákazníkem, ať už jde o tělo zprávy (obsah by měl v kontextu organizace dávat smysl), tón jazyka (tykání, vykání), podpis (vizitka, křestní jméno, přezdívka, iniciály), přílohu (formát a název) a e-mailovou adresu (správný formát a odpovídající doména). Právě podoba e-mailu bývá často slabinou spear-phishingových útoků. Zatímco méně sofistikovaní útočníci použijí pouze zdánlivě podobnou adresu (například nula místo písmene O, jan.novak@0rganizace.cz), zkušený útočník bude schopen zfalšovat svou e-mailovou adresu (tzv. spoofing) tak, aby vypadala přesně jako adresa osoby, za kterou se vydává (jan.novak@organizace.cz).[20]

Obr. 5: Fáze spear-phishingu

Zdroj: NÚKIB

4. Kompromitace

Hlavním cílem útočníka je zpravidla přesvědčit oběť, aby otevřela přílohu e-mailu nebo zprávy nakaženou malwarem nebo kliknula na odkaz, ze kterého se stáhne dokument obsahující malware. Pokud k tomu dojde, systémy oběti jsou kompromitovány škodlivým kódem. Typ malwaru se odvíjí od motivace útočníků. APT skupiny preferují malware umožňující vzdálený přístup k zařízení (Remote Access Trojan, RAT), který útočníkům umožňuje získat plný přístup k systémům oběti a slouží jako předmostí pro další útoky. RAT může odesílat informace zpět útočníkům nebo může být využit k instalaci dalšího malware se specifickými úkoly (např. sabotáž systému). Kyberzločinci RAT používají zejména ke krádeži dat a inklinují rovněž k ransomware, tedy malware, který zašifruje systém oběti a požaduje finanční obnos za dešifrování.

Box 3: Miliardové pokuty za ztrátu dat svých zákazníků

Za krádež dat až půl milionu svých uživatelů a porušení směrnice GDPR hrozí pokuta 5,4 miliardy Kč britským aerolinkám British Airways. Kvůli nedostatečnému zabezpečení internetového platebního systému aerolinek byly hackery ukradeny osobní údaje zákazníků, včetně kompletních informací o platebních kartách. Incident byl zveřejněn v září 2018, ale útočníci kradli údaje od června téhož roku. [21]

Kombinace nedostatečného vzdělání zaměstnanců v oblasti kybernetické bezpečnosti a zvyšující se sofistikovanost spear-phishingových e-mailů vede k vysoké úspěšnosti útoků, které mají významné finanční dopady. Kromě přímých finančních ztrát zaviněných krádeží, nedostupností služeb a následnou nápravou mohou postižené firmy čelit i vysokým pokutám, pokud útočníci získají osobní a citlivé údaje zákazníků.

Útočníci nemusí používat pouze nakažené přílohy, ale může jít o klasický finanční podvod. Floridské město Naples se v roce 2019 stalo cílem podvodníků, kteří ve spear-phishingovém e-mailu předstírali, že jsou představitelé stavební firmy, která pro město pracovala. Útočníci chtěli po konkrétní zodpovědné osobě v rámci městské samosprávy zaplatit fakturu za stavební práce v hodnotě 700 tisíc dolarů (16 milionů Kč). Ta platbu skutečně odeslala. [22]

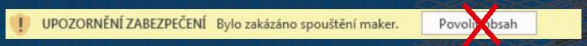
5. Šíření

V případě použití malware je pro útočníka často žádoucí, aby se z prvotního nakaženého počítače dále šířil v síti organizace a nakazil co nejvíce zařízení (např. ransomwarem). Šíření může být i součástí strategie útočníků. Ti mohou nejprve cílit na nízko postavené zaměstnance v organizaci, kteří mohou postrádat povědomí o hrozbě spear-phishingu. Po kompromitaci jejich systémů mohou z jejich adres útočníci rozesílat škodlivé soubory a odkazy, které budou díky legitimnímu odesílateli vypadat autenticky.

PŘÍLOHA 3: SPEAR-PHISHING A DOPORUČENÍ PRO PERSONÁL NEMOCNIC

SPEAR-PHISHING
DOPORUČENÍ PRO PERSONÁL NEMOCNIC

- **Slepě neotevírejte přílohy a odkazy v e-mailech** – i zde platí okřídlené "*dvakrát měř, jednou řež*"
- **Kontrolujte e-mailovou adresu, ze které je e-mail odeslán** – hledejte chyby a překlepy, například reditelstvi@fmmaletice.cz místo reditelstvi@fnmaletice.cz
- **Zpozorněte, když obdržíte e-mail vytvářející časovou tíseň** – něco je třeba udělat "*hned ted*"
- **Zpozorněte, když obdržíte e-mail s neobvyklým požadavkem** – primář Vás žádá o okamžitý převod prostředků na účet zdravotnické firmy XY
- V případě nejistoty nebo podezření **kontaktujte vaše IT oddělení** – vzhledem k rizikům a finančním škodám, které může např. ransomware nemocnici způsobit, se na vás ani v případě planého poplachu nikdo na IT oddělení zlobit nebude;)
- **Omezte sdílení informací o zaměstnání na sociálních sítích** – nesdílejte detaily o své práci, pracovní procesy ani jména nadřízených, vše jde v rámci sociálního inženýrství zneužít k tomu, aby vás někdo nachytal
- **Nepovolujte makra v programech** - především v programech MS Office (Word, Excel…)



SPEAR-PHISHING ZBLÍZKA

Spear-phishing je nejčastěji podvodný e-mail usilující o to, aby uživatel stáhnul a spustil škodlivý software, nebo vyzradil své přihlašovací údaje. Tyto podvodné zprávy zpravidla imitují důvěryhodného odesílatele a cílí přímo na adresáta. Pro nemocnice a zdravotní zařízení se tak mohou vydávat i za zdravotnické organizace, jiné nemocnice nebo dodavatelé zdravotnického materiálu. Mohou mít i formu SMS, telefonátu nebo zprávy na sociální síti.

Příklad ransomwaru Petya z roku 2016, který infikoval více než 300 000 počítačů.

83 % útočníků ve spear-phishingových e-mailech předstírají příslušnost ke známé značce (Microsoft, Apple, finanční instituce). Tím zvyšují svou legitimitu a obchází e-mailové filtry.

Cílem je instalace malwaru nebo krádež přihlašovacích údajů.

V e-mailu bývá odkaz na více či méně věrnou přihlašovací stránku služby, kterou útočníci napodobují

Poté, co uživatelé zadají své heslo, získají útočníci přístup k legitimnímu účtu uživatele, a mohou ukrást důvěrná data nebo účet využít k dalším útokům.

Od: Radek Chvalík <radek.chvallk@fmmaletice.cz>
Odesláno: 21. února 2020 9:44:19
Komu: Jaroslav.novak@fnmaletice.cz
Předmět: ověřit teď

Adresa je podvržená - končí @fmmaletice.cz

Zpráva vytváří časovou tíseň a vyzývá k rychlému jednání

Vážený uživateli,

Během včerejšího večera došlo k vypršení vašeho certifikátu na eRecept. V návaznosti na to nebudete moci dále vydávat recepty. Pro jeho obnovení klikněte zde a urychleně zadejte své přihlašovací jméno a heslo.

https://adminmicrosoftupda.wixisite.com/mysite

Odkaz na závadnou adresu

Technická podpora

Fakultní nemocnice Maletice

Doporučení pro bezpečný pohyb v kybersvětě:
https://www.nukib.cz/download/vzdelavani/doporuceni/NUKIB_doporuceni_uzivatele_plakat.pdf

Další doporučení a vzdělávací kurzy:
https://www.nukib.cz/cs/vzdelavani/

www.nukib.cz

Národní úřad pro kybernetickou a informační bezpečnost

POZNÁMKY

[1] Takzvané APT, nebo Advanced Persistent Threat (pokročilá a trvalá hrozba), je v kybernetické bezpečnosti označení pro obzvláště sofistikované aktéry. Zpravidla jde o skupiny, které jsou schopny dlouhodobé a vytrvalé infiltrace a zneužívání cílového systému za pomoci pokročilých a adaptivních technik (na rozdíl od běžných jednorázových útoků). APT skupiny jsou často přímo nebo nepřímo napojeny na státní aktéry.

[2] Fireeye. Spear-phishing Attacks: Why they are Successful and How to Stop them? Dostupné na: https://www.fireeye.com/content/dam/fireeye-www/global/en/products/pdfs/wp-fireeye-how-stop-spearphishing.pdf

[3] Zetter, Kim. 2016. Inside the Cunning, Unprecedented Hack of Ukraine´s Power Grid. Wired. Dostupné na : https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

[4] Thubron, Rob. 2019. Ransomware attack on Baltimore has cost city $18 million so far. Techspot. Dostupné na https://www.techspot.com/news/80400-ransomware-attack-baltimore-has-cost-city-18-million.html

[5] Osborne, Charlie. 2018. NonPetya ransomware forced Maersk to reinstall 4000 servers, 45000 PCs. ZDNet. Dostupné na https://www.zdnet.com/article/maersk-forced-to-reinstall-4000-servers-45000-pcs-due-to-notpetya-attack/

[6] Proofpoint. Q4 Threat Report Quarterly 2018. 2018. Dostupné na https://www.proofpoint.com/sites/default/files/pfpt-us-tr-q418-quarterly-threat-report.pdf

[7] Proofpoint. 2019. 2019 State of the Phish Report. Dostupné na: https://www.proofpoint.com/us/resources/threat-reports/state-of-phish

[8] Barracuda Networks. 2019. Spear Phishing:Top Threats and Trends. Dostupné na: https://assets.barracuda.com/assets/docs/dms/Spear_Phishing_Top_Threats_and_Trends.pdf

[9] Hoax.cz. 2018. Falešné vydírání - Sextortion - Bezbecnostní Výstraha (20181203). Dostupné na: http://www.hoax.cz/scam419/falesne-vydirani---sextortion---bezbecnostni-vystraha-20181203/

[10] Policie ČR. 2018. Upozornění na výhrůžné e-maily. Dostupné na: https://www.policie.cz/clanek/upozorneni-na-vyhruzne-e-maily.aspx

[11] CSIRT-MU. 2018. Varování: Vědecké informace v zájmu podvodníků. Dostupné na: https://csirt.muni.cz/about-us/news/phish_sci

[12] CSIRT-MU.2018. Lekářská fakulta: Varování před podvodnými e-maily. Dostupné na: https://csirt.muni.cz/about-us/news/lf_varovani

[13] Root.cz. DMARC: ověření odesilatelovy domény. Dostupné na: https://www.root.cz/clanky/dmarc-overeni-odesilatelovy-domeny/

[14] Root.cz. DKIM podpisy pro důveryhodnější e-mail. Dostupné na: https://www.root.cz/clanky/dkim-podpisy-pro-duveryhodnejsi-e-mail/

[15] Root.cz. SPF: proti spamu i přeposílání pošty. Dostupné na: https://www.root.cz/clanky/spf-proti-spamu-i-preposilani-posty/

[16] Weinert, Alex. Your Pa$$word doesn't matter. Microsoft. Dostupné na: https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Your-Pa-word-doesn-t-matter/ba-p/731984

[17] Jen za posledních 12 měsíců došlo například k úniku dat pěti milionů obyvatel Bulharska z bulharského daňového úřadu (jména, adresy, osobní informace o rodinných příslušnících, sociálním zabezpečení a výši příjmů), desítek milionů uživatelů Facebooku ze serverů třetích stran (komentáře, lajky, reakce, jména, uživatelské id, e-maily), půl miliardy zákazníků sítě hotelů Marriott International (jména, příjmení, adresy, e-maily, telefonní čísla, čísla pasů a dalších dokladů) a půl miliardy zákazníků Brittish Ariways (jména, příjmení, údaje o platebních kartách).

[18] NATO Stratcom. 2019. Responding to Cognitive Security Challenges. Dostupné na https://www.stratcomcoe.org/responding-cognitive-security-challenges

[19] ZDNet. 2017. How these fake Facebook and LinkedIn profiles tricked people into friending state-backed hackers. Dostupné na: https://www.zdnet.com/article/how-these-fake-facebook-and-linkedin-profiles-tricked-people-into-friending-state-backed-hackers/

[20] Tohoto triku na konci roku 2018 zneužila neznámá osoba, která jménem Tomia Okamury z adresy okamurat@psp.cz poslancům odeslala pozvání do prodejen Japa shop, s výzvou, aby s vánočními dárky nečekali na poslední chvíli. Japa shop prodejny jsou vlastněny právě Okamurou.

[21] The Register. 2020. UK data watchdog kicks £280m British Airways and Marriott GDPR fines into legal long grass. Dostupné na: https://www.theregister.co.uk/2020/01/13/ico_british_airways_marriott_fines_delayed/

[22] Naples Daily News. 2019. Scammers trick City of Naples out of $700,000 in spear phishing cyber attack. Dostupné na: https://eu.naplesnews.com/story/news/local/2019/08/02/scammers-trick-naples-out-700-000-spear-phishing-cyber-attack/1902321001/

PODMÍNKY VYUŽITÍ INFORMACÍ

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol (dostupná na webových stránkách www.us-cert.gov/tlp). Informace je označena příznakem, který stanoví podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Barva	Podmínky použití
Červená TLP: RED	Informace nemůže být použita jinou osobou než konkrétní osobou na straně příjemce, které byla informace poskytnuta, nebudou-li výslovně stanoveny další osoby, kterým lze tuto informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit po dohodě s původcem informace.
Oranžová TLP: AMBER	Informace může být sdílena pouze mezi pracovníky příjemce, kteří mají need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci. Jiným osobám, než výše uvedeným, nesmí být informace poskytnuta, nebudou-li výslovně stanoveny další osoby, kterým ji lze poskytnout.
Zelená TLP: GREEN	Informace může být sdílená v rámci příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály. Příjemce při předání musí zajistit důvěrnost komunikace informace. Příjemce nesmí informaci poskytnout veřejně, může ji však při splnění a zajištění stejných podmínek ochrany předat dalším partnerským subjektům příjemce.
Bílá TLP: (WHITE)	Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.

PRAVDĚPODOBNOSTNÍ VÝRAZY VE VÝSTUPECH NÚKIB

Pravděpodobnostní výrazy a vyjádření jejich procentuálních hodnot.

Výraz	Pravděpodobnost
Téměř jistě	90-100%
Velmi pravděpodobně	75-85%
Pravděpodobně	55-70%
Nelze vyloučit/Reálná možnost	25-50%
Nepravděpodobně	15-20%
Velmi nepravděpodobně	0-10%