Ing. Vladimír Šulc, Ph.D.
Fakulta bezpečnostního managementu PA ČR v Praze
Katedra managementu a informatiky

Aktuální trendy a nové techniky používané v rámci spear phishing kampaní

Cíl

V rámci našeho výzkumu na fakultě Bezpečnostního managementu Policejní akademie ČR jsme si položili otázku, zda stávající bezpečnostní opatření ohledně spear phishingu zavedená v korporacích jsou dostatečně účinná a mají potenciál ochránit příjemce e-mailu před přijetím podvrženého e-mailu, který bývá dost často použit v rámci APT útoků, a rovněž zda příjemce e-mailu má šanci rozpoznat, že se jedná o spear phishing. Vyslovili jsme hypotézu, že stávající opatření jsou velice nedostatečná a že příjemce e-mailu v mnoha případech není schopen phishingový e-mail rozpoznat. Rozhodli jsme se v rámci vlastního experimentu ověřit, jak si s nejnovějšími technikami používanými v rámci phishingových kampaní poradí tradiční řešení používaná ve většině organizací.

Úvod

Phishing by se dal do češtiny přeložit jako „rhybaření“. S ním má společné to, že útočník stejně jako rybář nadhodí pro oběť atraktivní návnadu, v tomto případě e-mail s odkazem nebo přílohou, která by příjemce měla zaujmout natolik, že na ni klikne nebo ji otevře a tím dojde k jeho nakažení nebo přesměrování na podvodnou stránku.

Cílem phishingu je přesvědčit příjemce zprávy ke kliknutí na přílohu v e-mailu či na odkaz, který se v něm nachází. Jedná se vůbec o jednu z nejčastějších technik, jak dochází k napadení koncového zařízení uživatele nebo k získání jeho přihlašovacích údajů.

Při tomto typu útoku je úspěšnost útoku založena především na použití technik sociálního inženýrství[1] a vše do značné míry závisí na tom, zda se odesilateli e-mailu podaří přesvědčit příjemce, aby e-mailu věnoval dostatečnou pozornost a kliknul na přílohu nebo odkaz v něm uvedený.

Dochází zde k využívání klasických technik sociálního inženýrství, které působí na emoce a které se snaží příjemce dostat do časové tísně, např. tím, že je v e-mailu uvedeno, že musí reagovat do určité doby, jinak bude jeho účet uzamčen nebo mu bude z účtu stržena určitá částka.

V okamžiku, kdy takový e-mail přichází od na první pohled důvěryhodné a známé osoby či autority, tak je nasnadě, že většina příjemců přestane být v takovém případě dostatečně ostražitá a na odkaz nebo přílohu v e-mailu klikne.

[1] CHMELÍK, Jan a Viktor PORADA. Vybrané problémy vyšetřování a dokazování počítačové kriminality I. In: *Identifikace potřeb právní praxe jako teoretický základ pro rozvoj kriminalistických a právních specializací*. Sborník vědeckých prací. Karlovy Vary: Vysoká škola Karlovy Vary, 2011, s. 334-346.

Takto pečlivě připravený e-mail obsahující přílohu se škodlivým kódem se užívá v rámci APT útoku, kdy nic netušící oběť e-mail otevře, klikne na přiloženou přílohu a spolu s přidruženou aplikací spustí i škodlivý kód, který zneužije nějaké (zero-day) zranitelnosti k tomu, aby se úspěšně zavedl do paměti a zajistil si své spuštění také po restartu počítače.[1]

Právě v přípravě samotného e-mailu je patrný podstatný rozdíl mezi tradičním phishingem a spear phishingem. Tradiční phishing, který je cílen na větší počet klientů určité služby, není příliš sofistikovaný a přípravě samotného e-mailu není věnována dostatečná pozornost, neboť útočník spoléhá na to, že se (obrazně řečeno) do jeho sítě nebo na jeho návnadu nějaká ta „čudla“ vždycky chytne.

V případě spear phishingu, kdy je cílem útočníka ulovit velkou rybu (pokud se budeme dále držet uvedeného příměru), však není možné její inteligenci podceňovat a útočník musí nejprve důkladně prozkoumat teritorium, ve kterém se rozhodne lovit a vyzbrojit se harpunou (anglicky spear, odtud spear phishing), protože velkou rybu na nějakou zapáchající návnadu nechytí.

V následující tabulce je zachycen rozdíl mezi obyčejným phishingem a spear phishingem. Vidíte, že něco mají obě formy společného a v něčem se zase liší.

Tabulka č. 1: Rozdíl mezi phishingem a spear phishingem.

Phishing	**Spear phishing**
E-mail je rozeslán na velký počet adres.	E-mail je zaslán pouze jednomu či několika málo příjemcům.
V e-mailu se nachází odkaz do internetu, který vede na doménu se zcela jiným názvem.	E-mail obsahuje odkaz do internetu, který vede na správnou doménu nebo doménu s velice podobným názvem.
E-mail se tváří, že přichází od osoby nebo firmy, kterou příjemce zná.	E-mail přijde od osoby nebo firmy, kterou znáte.
Příjemce e-mail zpravidla neočekává.	Příjemce e-mail zpravidla očekává.
Může být požadováno zadání určitých údajů.	Není požadováno zadání žádných údajů.
E-mail obsahuje neúmyslné chyby.	E-mail neobsahuje (neúmyslné) chyby.
E-mail může obsahovat přílohu, jež zneužívá nějaké dlouho známé zranitelnosti.	E-mail zpravidla obsahuje přílohu, jež zneužívá zranitelnosti nultého dne.

Zdroj: vlastní výzkum

Zatímco pro tradiční phishing je typické rozeslání obrovského množství e-mailů, často i na špatné adresy, v případě spear phishingu je tomu přesně naopak. Útočník v takovém případě zašle e-mail konkrétní osobě, zpravidla zaměstnanci na určité pozici či vysoce postavenému manažerovi dané společnosti. Takový e-mail adresovaný konkrétní osobě může být těžko zachycen antiphishingovým filtrem,

[1] Sputnik Česká republika. (2015) [online]. Dostupné z: http://cz.sputniknews.com/svet/20151014/1401307/internet-hackeri-usa-valka.html

především proto, že se nevyskytuje ve větším množství, nevykazuje žádné znaky typické pro phishingový e-mail a adresa odesílatele a adresa SMTP serveru se nenachází na žádném blacklistu.[1]

Pokud je navíc takový e-mail poslán oběti přímo z prostředí dané společnosti, tak ta zpravidla ani nepojme podezření, že by se mohlo jednat o phishing, a to i přesto, že je v tomto směru poučená. Jak by také mohla, když e-mail přišel od osoby, kterou dobře zná, z e-mailu nevedou odkazy na internet, není po ní požadováno zadání žádných údajů a e-mail po formální i obsahové stránce odpovídá zvyklostem v dané společnosti.[2]

Na tomto místě je nutné zdůraznit, že přípravě samotného e-mailu je ze strany útočníka věnována značná pozornost a útočník se za tímto účelem neváhá detailně seznámit s firemní kulturou, organizační strukturou a poměry, které v dané společnosti panují. Je tedy použit správný jazyk, v textu e-mailu nenalezneme gramatické chyby ani stylistické nedostatky, tedy pokud se jich běžně nedopouští samotná osoba, jejíž identita je pro tento účel zneužita.

Odhalit spear phishing je mnohem náročnější a obrana před spear phishingem není snadná. Těžko lze předpokládat, že příjemce bude před každým otevřením přílohy kontaktovat odesílatele a zjišťovat, zda mu danou zprávu opravdu poslal. Nehledě na to, že i v případě, kdy by odesílatel tuto skutečnost potvrdil, příjemce nemá jistotu, že malware nacházející se na počítači odesílatele do jím zaslané přílohy nějaký ten škodlivý kód nezačlenil.

Vývoj phishingu v ČR od roku 2013

V létě roku 2013 se začínají objevovat poměrně dobře připravené phishingové kampaně, kdy se útočník vydává za Českou poštu a rozesílá informaci o nevyzvednuté zásilce. Pokud příjemce tohoto e-mailu přílohu spustil, došlo napadení jeho počítače bankovním malwarem.[3]

Tato kampaň pokračovala i v roce 2014, kdy se k ní přidal ještě tzv. pohledávkový SPAM, kdy se útočník vydával za exekutora a sledoval stejný cíl (tj. napadení počítače příjemce e-mailu bankovním malwarem). Rok 2014 byl v tomto směru přelomový a dal by se označit jako rok phishingu, neboť v jeho druhé polovině bylo rozesláno tolik phishingových e-mailů jako nikdy předtím a hlavně všechny byly psány česky. Phishing byl sice plošný, ale byl cílen na klienty největších českých bank, konkrétně pak Českou spořitelnu, Československou obchodní banku a Komerční banku. Plošný byl proto, že e-mail obdrželi rovněž neklienti, což znamenalo, že útočník nedisponoval e-mailovými adresami klientů, ale e-maily rozesílal na všechny adresy, které měl k dispozici. Banky evidovaly několik 1000 případů ročně, ČSOB uvádí kolem 100 případů,[4] KB kolem 150

[1] GŘIVNA, Tomáš a Radim POLČÁK. *Kyberkriminalita.* První vydání. Praha. Auditorium, 2008. ISBN 978-80-903786-7-4.
[2] SMEJKAL, Vladimír. Současné možnosti boje proti počítačové kriminalitě. *Data Security Management.* XV., 2011, č. 4, s. 18-23.
[3] SMEJKAL, Vladimír. *Bankovní loupeže a počítačová kriminalita v České republice*. Seminář Kontrola informačních systémů a počítačová kriminalita (Českobritská-irská účetní asociace). Praha, 25. 5. 1995, s. 13-19.
[4] ČSOB (2015) [online] Dostupné z: https://www.csob.cz/portal/-/tz150115.

případů[1] měsíčně a škody se dle ČBA měly pohybovat v řádu několika desítek miliónů korun. Největší škoda připadající na jednoho klienta měla dle zveřejněných informací činit 2 milióny korun.[2]

Tyto phishingové kampaně pak pokračovaly i v roce 2015, ovšem již s menší intenzitou. Zaznamenat jsme mohli kampaň snažící se příjemce e-mailu přesvědčit, aby kliknul na přílohu obsahující potvrzení o zaplacení platební kartou a vystavenou fakturu. Na pozadí pak docházelo k instalaci bankovního trojana Tinba.[3]

V roce 2016 phishingové kampaně pokračovaly, ale vzhledem k tomu, že banky již v minulých letech zvýšily úroveň svých bezpečnostní opatření a detekční schopnosti FDS, bylo cílem útočníka už spíše napadení počítače příjemce e-mailu ransomwarem než bankovním malwarem.

V roce 2017 se objevilo několik zajímavých kampaní, které se oproti předchozím lišily v tom, že odkazy vedly na větší počet hacknutých webů umístěných v zahraničí v zemích bývalého východního bloku. Dále se objevily zcela nové techniky, které vedly k tomu, že mnozí bezpečnostní experti měli problém rozpoznat phishing od legitimního e-mailu.

Phishingové e-maily rozesílané v posledních kampaních už nelze rozpoznat jen dle gramatických a stylistických chyb, ale je nutné vyhodnocovat i další charakteristiky.[4] Už neplatí, že stačí neotvírat podezřelé e-maily od neznámého odesílatele. Maily v nedávno proběhnuvších phishingových kampaních se vyznačovaly takřka bezchybnou češtinou, přišly od známého odesílatele a byly příjemcem dokonce očekávány.

Nejnovější techniky užívané v posledních phishingových kampaních

V této kapitole jsou uvedeny nejnovější techniky používané v rámci phishingových kampaní, se kterými jsme se mohli v roce 2017 ve světě setkat a které jsme si osvojili a následně použili i v rámci vlastního výzkumu.

Data URI

V roce 2017 jsme mohli zaznamenat spear phishingovou kampaň na uživatele Gmailu, v rámci které byla navíc použita i technika „data URI“, která byla později použita rovněž při obdobném phishingovém útoku na klienty České spořitelny.[5]

---

[1] Finparáda (2015) [online] Dostupné z: http://finpoplatky.cz/2709-Komercni-banka-nabizi-svym-klientum-ochranu-pred-novymi-sofistikovanymi-vykradaci-kont.aspx.

[2] iDNES.cz (2013) [online] Dostupné z: https://plzen.idnes.cz/pishingovy-utok-pripravil-firmu-z-plzenska-o-dva-miliony-pms-/plzen-zpravy.aspx?c=A131003_110415_plzen-zpravy_pp.

[3] SMEJKAL, Vladimír. Kybernetické nebezpečí a kybernetická válka. In: *Sborník příspěvků z 6. ročníku mezinárodní vědecké konference „Bezpečná Evropa 2013“.* 25. 11. 2013. Karlovy Vary: Vysoká škola Karlovy Vary, 2013, s. 142-149.

[4] Nebezpečné triky počítačových pirátů. (2016). [online]. Dostupné z: https://www.novinky.cz/internet-a-pc/bezpecnost/412299-nebezpecne-triky-pocitacovych-piratu.html.

[5] escan (2017) [online] Dostupné z: http://blog.escanav.com/2017/01/data-uri-schema-phishing-attacks-targeting-gmail-users.

Způsob, jak útok na uživatele Google probíhal, byl poměrně jednoduchý. Útočník kompromitoval e-mailový účet oběti, poté v doručené poště vyhledal e-mail s přílohou a udělal její screenshot. Poté vytvořil nový e-mail jako odpověď na tento e-mail se stejným či podobným předmětem, do něj vložil screenshot této přílohy a odeslal jej.

V těle tohoto e-mailu se pak nacházel odkaz na phishingový web. Aby se zvýšila šance, že oběť na odkaz klikne a dojde k přesměrování, nebyl vyveden jako prostý text, nýbrž byl svázán s obrázkem, který se tvářil jako náhled dokumentu. Dostatečně malým na to, aby oběť motivoval na něj kliknout a zobrazit v plné velikosti.

Když uživatel na náhled obrázku kliknul, tak se mu v prohlížeči otevřela nová stránka a pokud uživatel nebyl dostatečně pozorný a nevšiml si, že spojení není bezpečné (tedy že se v adresním řádku nenachází zámeček) tak nepoznal, že se stal obětí podvodu. Celý trik spočíval v tom, že v adresním řádku prohlížeče je uveden text: *data:text/html*, po němž může následovat prakticky cokoliv, třeba *https://www.xbank.cz* či dokonce jméno banky, např. *Xbank a.s. [CZ]* | *https://www.cz*; jak to ostatně bývá běžné u webů s certifikátem.

Za dalším středníkem pak následuje vlastní kód stránky, který má protokol „data“ interpretovat. Jelikož by si však oběť mohla všimnout HTML tagů, které jsou de facto předávány jako parametr, tak je provedeno jejich enkódování do base64 formátu.

V takovém případě se pak v adresním řádku objevuje jen dlouhý hexadecimální řetězec znaků, na který je oběť zvyklá, protože vypadá jako token. Není ale problém i tento řetězec odsunout zcela mimo zorné pole oběti vložením většího počtu mezer.

Enkódovat do base64 může útočník celou stránku nebo může enkódovat jen kód, který mu libovolnou, předem připravenou stránku uloženou na kompromitovaném webu zobrazí v iframu. Útočník může do base64 enkódovat něco jako:

<html>

<head>

</head>

<title>XBANK InternetBanking</title>

<body>

<iframe src=“http://ib.utocnikova-domena.cz/“ width=“100%“ height=“100%“ fullscreen=“yes“ frameborder=“0" scrolling=“no“>

</iframe>

</body>

</html>

Výsledkem enkódování, např. pomocí online nástroje base 64encode, je pak takovýto řetězec:

PGh0bWw+PGhlYWQ+PC9oZWFkPjx0aXRsZT5YQkFOSyBJbnRlcm5ldEJhbmtpbmc8L3RpdGxlPjxib2R5PjxpZnJhbWUgc3JjPSJodHRwOi8vaWIudXRvY25pa292YS1kb21lbmEuY3ovIiB3aWR0aD0iMTAwJSIgaGVpZ2h0PSIxMDAlIiBmdWxsc2NyZWVuPSJ5ZXMiIGZyYW1lYm9yZGVyPSIwIiBzY3JvbGxpbmc9Im5vIj48L2lmcmFtZT48L2JvZHk+PC9odG1sPg==

Ten útočník použije v odkazu, který pak celý vypadá takto:

https://ib.xbank.cz

V takovém případě se v prohlížeči zobrazí v adresním řádku text, který chceme, a pod ním se načte naše stránka. Pokud si uživatel zkontroluje jen, že je tam uvedeno https a správná adresa webu a nezajímá ho ikona zámečku a text, který se nachází před https, tak je ztracen.

Takto lze zobrazit i to, co běžně vypisuje prohlížeč jen na stránkách, které jsou chráněny certifikátem. Jméno společnosti může být dokonce napsáno s nabodeníčky, které nejsou uvedeny v adresním řádku ani na originální stránce dostupné přes https a chráněné certifikátem od důvěryhodné certifikační autority.

Z výše uvedeného vyplývá, že návštěvník webu si musí kontrolovat nejen adresu webu a zda je adresa uvedena oním obligátním https, ale především to, zda je dané připojení opravdu bezpečné a jaký web používá certifikát. Jinými slovy, v okamžiku, kdy se před https nachází něco jako je *data:text/html*, tak by měl zbystřit.

Punycode

Čínský bezpečnostní expert Xudong Zheng[1] zveřejnil informaci, jak může být zneužito způsobu, jakým Google Chrome a Mozila Firefox zacházejí s názvy domén, které jsou zakódovány pomocí algoritmu Bootstring známého pod jménem Punycode, k homografním útokům.

Tuto zprávu převzala další média, ale nesprávně uvedla, že ochrana proti tomuto útoku selže v okamžiku, kdy doménové jméno obsahuje znaky z různých jazyků. Je tomu přesně naopak.

Pomocí výše uvedeného algoritmu může být libovolných řetězec (např. i název domény) převeden z Unicode na ASCII a naopak.[2] Výstupem tohoto algoritmu je pak řetězec složený jen ze základních písmen, číslic a pomlček.

Takže např. čínský název domény *„短.co“* lze pomocí Punycode zapsat jako *„xn--s7y.co“*, což je pro našince jistě srozumitelnější. Punycode však nefunguje pouze pro enkódování čínštiny, ale i cyrilice a zde nastává zásadní problém.

V okamžiku, kdy tento algoritmus v adresním řádku prohlížeče má zobrazit doménu *„xn--80ak6aa92e.com“* zobrazí místo ní *„apple.com“*, a pokud je tato doména navíc opatřena i certifikátem, nikoho nenapadne zkoumat, že uvedený název není v latince, nýbrž v cyrilici, a že ony dvě „pé“ jsou vlastně „er“ a „el“ je tzv. paločka, kterou je možné zadat jako Alt+1231.

[1] xudongz.com (2017) [online] Dostupné z https://www.xudongz.com/blog/2017/idn-phishing.
[2] https://www.punycoder.com.

Důležité je v cyrilici napsat celý název domény, protože v okamžiku, kdy je část názvu domény napsána v jednom jazyce a část zase v jiném, tak zafunguje ochrana a prohlížeč zobrazí punycode.

Byť je tato staronová zranitelnost jistě závažná, možnosti jejího zneužitá jsou částečně omezené množinou znaků, které lze použít.

Ropemaker

Bezpečnostní experti z Mimecast objevili staronovou zranitelnost,[1] ale spíš by se dala označit za vlastnost HTML e-mailů, které lze zneužít k zaslání maligního e-mailu. Ten jako benigní projde skrz různá antispamová řešení a až v e-mailovém klientovi ukáže svou pravou tvář. V zásadě se jedná jen o využití CSS uložených na serveru, které se po otevření HTML e-mailu načítají, a samozřejmě, pokud dojde mezitím k jejich změně, může dojít i ke změně obsahu e-mailu.

U desktop verze by se mělo navíc objevit i hlášení ohledně nutnosti stažení externích zdrojů, které mnoho uživatelů bez přemýšlení odklikne. Závažnější je, že zranitelní jsou např. uživatelé Apple Mail nebo mobilní verze MS Outlook, kde k automatickému blokování JS, CSS a obrázků nedochází.

Útok je v zásadě jednoduchý, stačí jen mít např. v těle e-mailu umístěné dva různě pojmenované elementy a v CSS, které jsou uloženy na serveru, pak u nich zaměnit hodnotu display z none na inline. To však předpokládá, že ke změně musí dojít krátce po odeslání daného e-mailu. To ale není pro útočníka, který má server, na kterém jsou CSS uloženy, problém. Zatím se této vlastnosti aktivně příliš nezneužívá, protože už skutečnost, že je v emailu schovaný nějaký obsah, je podezřelá. Pravděpodobnější je, že přes antispam řešení projde e-mail, který nebude nic schovávat.

Proč stávající ochrany selhávají

E-mail přichází od osoby, kterou dotyčný zná a od níž odpověď očekává. Ne vždy se ale útočníkovi podaří hacknout e-mailový účet odesílatele, a proto musí podvrhnout adresu odesílatele, čímž šance na odhalení roste.

Od koho e-mail přišel, poznáte celkem snadno podle toho, co je uvedeno v poli „from“. Jenže to není tak docela pravda. Potíž je v tom, že v e-mailu jsou pole „from“ hned dvě. Jedno se jmenuje „envelope-from“ a v něm je uvedena skutečná adresa odesílatele a do druhého, které se jmenuje jen „from“, si může každý napsat, co chce.

A právě z tohoto pole přebírá e-mailový klient adresu odesílatele, kterou vám následně zobrazí. Kontrolu by mohl provést SPF, který zajistí, že není možné přijmout e-mail z mailserveru, který není oprávněn k rozesílání e-mailů za danou doménu. Jenže v tomto případě vůbec nepřijde ke slovu, protože SPF pouze kontroluje, co je uvedeno v „envelope-from“, nikoliv co je uvedeno v poli „from“.

Kdyby se útočník snažil změnit i hodnotu v „envelope-from“, tak pak by SPF zafungoval, ale proč by to útočník dělal, když stačí změnit pole „from“, které SPF

[1] mimecast (2017) [online] Dostupné z https://www.mimecast.com/blog/2017/08/introducing-the-ropemaker-email-exploit.

nekontroluje. A koho napadne si zobrazovat u každého e-mailu hlavičku a prohlížet si, zda náhodou není uvedeno něco jiného v „envelope-from“, než ve „from“.

Možnou ochranou by bylo DKIM,[1] jenže tady je problém v tom, že tato ochrana nedělá v zásadě nic jiného, než že se vytvoří hash e-mailu nebo jen jeho určité části, který se zašifruje privátním klíčem, ke kterému má právo jen osoba, která se v dané doméně skutečně nachází. Při kontrole se následně zjistí, že daný e-mail byl chráněn pomocí DKIM, a tak se udělá dotaz na danou doménu. Získá se tak veřejný klíč a tím se dešifruje zpráva a získá se její hash. Ten se následně porovná s hashem spočteným na straně příjemce zprávy. Pokud sedí, tak e-mail přišel opravdu z dané domény.

Vlastní výzkum

V rámci vlastního výzkumu, který se realizoval v letech 2016 a 2017 v jedné nejmenované korporaci, kde již proběhla bezpečnostní osvěta mezi zaměstnanci ohledně phishingových kampaní, byly spuštěny 2 phishingové a 2 spear phishingové kampaně využívající výše uvedené techniky punycode a ropemaker.

Na internetu jsem zaregistroval doménu, ze které jsem během jednoho měsíce rozeslal 1 000 e-mailů, které byly doručeny do schránek koncových uživatelů. E-maily obsahovaly text vybízející k otevření přílohy, kterou byl excelovský sešit obsahující makro a odkaz do internetu.

Makro neprovádělo na koncovém zařízení uživatele žádnou škodlivou činnost, pouze otevřelo prohlížeč internetu a zobrazilo stránku, která byla součástí awareness kampaně a informovala příjemce e-mailu o tom, že se nezachoval správně, neboť otevřel přílohu e-mailu, která mu přišla od neznámého odesílatele, a povolil makro. To by v případě, že by se jednalo o skutečný útok, mohlo vést k zašifrování veškerých jeho dat, zcizení citlivých informací nebo k jakékoliv jiné akci plně v režii útočníka. Kromě toho makro zapsalo do logu informaci o tom, kdy a kým bylo spuštěno, takže jsme pak mohli tuto informaci předat vedení společnosti, s jehož souhlasem byl tento test proveden.

V roce 2016 bylo dosaženo 10 % úspěšnosti, v následujícím roce 2017 necelého 1 %. To lze vysvětlit tím, že od prvního testu byli zaměstnanci v této oblasti intenzivně školeni, takže se již naučili phishingový e-mail rozpoznat a správně na něj reagovat, tedy na odkaz neklikat a přílohu neotvírat.

Rovněž spear phishingová kampaň realizována v rámci této společnosti se souhlasem představenstva a cílená na ředitele odborů byla úspěšná. V prvním roce bylo rozesláno celkem 5 různých e-mailů, které obsahovaly wordový dokument s dalším vloženým objektem, který obsahoval vlastní kód. V této kampani jsem se vydával za uchazeče o práci a na nabízenou pozici zveřejněnou na stránkách společnosti jsem reagoval zasláním fiktivního životopisu a motivačního dopisu. V tomto případě jsem byl rovněž úspěšný, neboť 3 z 5 ředitelů na objekt ve wordovém dokumentu kliklo.

V druhém roce, tj. 2017, jsem rozeslal rovněž 5 e-mailů, ale tentokrát jako fiktivní dodavatel produktů a služeb, které společnost poptávala. V tomto případě jsem byl

[1] SMEJKAL, Vladimír. *Kybernetická kriminalita*, Plzeň: Aleš Čeněk, 2015. ISBN 978-80-7380-501-2.

rovněž úspěšný, neboť 4 z 5 ředitelů na objekt ve wordovém dokumentu kliklo. Této skutečnosti přispěl také fakt, že jim byl e-mail přeposlán z oddělení marketingu a tudíž ho považovali za důvěryhodný.

Závěr

Cílem tohoto výzkumu bylo ověřit, jak snadné je pro útočníka vytvořit takovou phishingovou kampaň, která by byla úspěšná, a jak a případně zda vůbec může příjemce takového e-mailu ověřit jeho pravost a zjistit, že se jedná o podvrh ještě dříve, než klikne na odkaz v e-mailu a dojde k jeho přesměrování na podvodné stránky, kde je vyzván k zadání přihlašovacích údajů.

Dospěl jsem k závěru, že v roce 2017 se objevilo několik závažných zranitelností (popsaných v části Nejnovější techniky používané v posledních phishingových kampaních), které jsem v rámci uvedeného experimentu (viz Závěr) ověřil a následně jsem zjistil, že mnou podvrhnuté e-maily byly bez problémů doručeny do e-mailových schránek příjemců a nebyly jimi označeny jako phishing.

Řešení DKIM by zcela jistě zabránilo v podvrhnutí e-mailu, protože útočník, který falšuje adresu odesílatele, se zpravidla nenachází v dané doméně a nemá přístup k privátnímu klíči, kterým se podepisuje. Je zde však stejný problém jako v případě SPF, tedy že se nekontroluje pole „from“. Jediným možným řešením je DMARC, který porovnává hodnotu uvedenou v poli „from“ a „envelope-from“ a je zde možné nastavit, jak se má zacházet s e-mailem, který má v obou polích uvedenou rozdílnou adresu. V praxi se ale příliš nepoužívá, protože v mnoha případech jsou tato pole rozdílná i ze zcela legitimních důvodů.[1]

Tato technická opatření ovšem příjemce e-mailu ochrání jen před podvrhnutím emailové adresy odesílatele nebo při pokusu o zaslání e-mailu ze serveru, který není k zasílání e-mailu z dané domény oprávněn. V případě technik punycode a ropemaker však příjemce e-mailu neochrání a je nutné nasadit antimalware řešení s technologií HIPS, případně nástroj na detekci anomálií na vnitřní síti NBA.

Určitým řešením pak je blokovat přílohy e-mailu, podepisovat makra, omezit přístup do internetu a především vést účinnou bezpečnostní osvětu, a to nejen mezi zaměstnanci, ale také manažery.

Literatura

Agari (2017) [online] Dostupné z: https://www.agari.com/wp-content/uploads/2017/08/Agari_DMARC_Adoption_Report_2017-new.pdf.

ČSOB (2015) [online] Dostupné z: https://www.csob.cz/portal/-/tz150115.

escan (2017) [online] Dostupné z: http://blog.escanav.com/2017/01/data-uri-schema-phishing-attacks-targeting-gmail-users.

Finparáda (2015) [online] Dostupné z http://finpoplatky.cz/2709-Komercni-banka-nabizi-svym-klientum-ochranu-pred-novymi-sofistikovanymi-vykradaci-kont.aspx.

[1] Agari (2017) [online]. Dostupné z: https://www.agari.com/wp-content/uploads/2017/08/Agari_DMARC_Adoption_Report_2017-new.pdf

GŘIVNA, Tomáš a Radim a POLČÁK. *Kyberkriminalita.* První vydání. Praha: Auditorium, 2008. ISBN 978-80-903786-7-4.

CHMELÍK, Jan a Viktor PORADA. Vybrané problémy vyšetřování a dokazování počítačové kriminality I. In: *Identifikace potřeb právní praxe jako teoretický základ pro rozvoj kriminalistických a právních specializací.* Sborník vědeckých prací. Karlovy Vary: Vysoká škola Karlovy Vary, 2011, s. 334-346.

iDNES.cz (2013) [online] Dostupné z: https://plzen.idnes.cz/pishingovy-utok-pripravil-firmu-z-plzenska-o-dva-miliony-pms-/plzen-zpravy.aspx?c=A131003_110415_plzen-zpravy_pp.

KŘUPKA, Jiří. *Základy technickej kybernetiky*, Liptovský Mikuláš: Akadémia ozbrojených síl gen. M. R. Štefánika, 2008. ISBN 978-80-8040-357-7.

mimecast (2017) [online] Dostupné z: https://www.mimecast.com/blog/2017/08/introducing-the-ropemaker-email-exploit

Nebezpečné triky počítačových pirátů. (2016). [online]. Dostupné z: https://www.novinky.cz/internet-a-pc/bezpecnost/412299-nebezpecne-triky-pocitacovych-piratu.html.

SMEJKAL, Vladimír. *Bankovní loupeže a počítačová kriminalita v České republice*. Seminář Kontrola informačních systémů a počítačová kriminalita (Českobritská-irská účetní asociace). Praha, 25. 5. 1995, s. 13-19.

SMEJKAL, Vladimír. *Kybernetická kriminalita*, Plzeň: Aleš Čeněk, 2015. ISBN 978-80-7380-501-2.

SMEJKAL, Vladimír. Kybernetické nebezpečí a kybernetická válka. In: *Sborník příspěvků z 6. ročníku mezinárodní vědecké konference „Bezpečná Evropa 2013“*, 25. 11. 2013. Karlovy Vary: Vysoká škola Karlovy Vary, 2013, s. 142-149.

SMEJKAL, Vladimír. Současné možnosti boje proti počítačové kriminalitě. *Data Security Management.* XV., 2011, č. 4, s. 18-23.

Sputnik Česká republika. (2015) [online]. Dostupné z: http://cz.sputniknews.com/svet/20151014/1401307/internet-hackeri-usa-valka.html

xudongz.com (2017) [online]. Dostupné z: https://www.xudongz.com/blog/2017/idn-phishing.

Slovník pojmů

Zero-day vulnerability - zranitelnost nultého dne je taková zranitelnost v systému, pro kterou není k dispozici oprava a uživatel resp. jeho systém se v tomto stavu nachází do doby, než je výrobcem příslušná oprava uvolněna.

SPF – Sender Policy Framework by měl příjemce chránit před podvrhnutou zprávou a to kontrolou, zda je daný server, který mail odeslal, skutečně oprávněný posílat e-maily z dané domény.

DKIM – Domain Keys Identified Mail neboli e-mail, resp. hlavička podepsaná privátním doménovým klíčem, kdy ke kontrole je pak možno použít veřejný klíč.

DMARC - Domain-based Message Authentication, Reporting and Conformance je postaven na SPF a DKIM a navíc může i kontrolovat pole from.

Benigní – kód, který není škodlivý, ale antimalware ho přesto může označit jako maligní.

Maligní – kód, který je škodlivý, ale antimalware ho přesto jako škodlivý označit nemusí.

JS – Java Script kód může manipulovat s obsahem stránky v závislosti na akcích uživatele.

CSS – Cascade Style Sheet obsahuje definici fontů, barev a rozložení, a jak se mají zobrazovat jednotlivé části stránky

Homografní – v tomto kontextu písmena, která vypadají stejně, ale pocházejí z odlišné znakové sady a mající i jiný význam.

R E S U M É

Hlavním cílem tohoto výzkumu je testování hypotézy, že běžný uživatel není schopen detekovat phishingové útoky a už vůbec ne sofistikované spear phishing cílené na něj. Tradiční bezpečnostní kontroly založené na antiphishingových filtrech, SPF a DKIM záznamech též selhávají. Pro otestování této hypotézy jsme se rozhodli provést analýzu posledních phishingových a spear phishingových kampaní ve světě, které jsme zaznamenali v posledních několika letech. Na základě tohoto výzkumu jsme připravili jednoduchou phishingovou kampaň a testovali reakci příjemců, zaměstnanců v jedné komerční organizaci. Výsledky potvrdily naši hypotézu, že zaměstnanci ve většině případů nedokázali zjistit phishing a současná technická opatření rovněž selhala. Na základě tohoto testu byla přijata a zavedena další bezpečnostní opatření.

Klíčová slova: Phishing, spear phishing, zranitelnost nultého dne, social engineering, puny kód, bezpečnostní kontroly, SPF, DKIM, DMARC, hlavičky pošty, certifikáty.

S U M M A R Y

ŠULC, Vladimír: CURRENT TRENDS AND NEW TECHNIQUES USED IN SPEAR PHISHING CAMPAIGNS

The main aim of this research consists in testing hypothesis that an ordinary user is not able to detect phishing not a bit of sophisticated spear phishing campaign targeted at him, and traditional security controls based on antiphishing filters, SPF and DKIM fail as well. To test this hypothesis we decided to perform analysis of last phishing and spear phishing campaigns in the world we have detected in last few years. On the basis of this research we prepared a simple phishing campaign and tested the reaction of recipients, employees in one commercial organization. The results confirmed our hypothesis; employees were not able to detect phishing in most cases and the current technical measures failed as well. On the basis of this test additional security measures were accepted and implemented.

Keywords: phishing, spear phishing, zero-day, social engineering, puny code, security controls, SPF, DKIM, DMARC, mail header, certificate.