CEO Fraud

Jak jsem hacknul vaši firmu

Martin Klubal

Dnes a denně slýcháme z úst bezpečnostních analytiků varování před generickými hrozbami ve formě rozličných masových kampaní, které sice zpravidla nedisponují sofistikovanými metodami průniku do koncových stanic domácích či korporátních uživatelů, v globálním měřítku jsou ovšem nepopiratelně úspěšné. Na druhé straně pomyslných vah se pak nachází útoky cílené, kterých je sice v porovnání s předchozími jmenovanými výrazně méně, jejich úspěšnost se ovšem limitně blíží sta procentům. V případě cílených útoků je totiž pouze otázkou času a finančních prostředků útočníka, kdy k úspěšné kompromitaci dojde. Tato skutečnost nás ovšem neopravňuje k tomu, abychom na zabezpečení naší sítě a koncových stanice rezignovali. Pravděpodobnost, že si útočník vybere zrovna nás, je bez ohledu na zaměření našeho podnikání, mizivá a generickým hrozbám jsme schopni čelit technologiemi jako firewall, IPS, NBA, antivirus atp.

Samotný CEO Fraud spadá do kategorie cílených útoků a přestože může mít rozličnou podobu, v zásadě se jedná o snahu útočníků vyvést ze společnosti peníze tvorbou a modifikací platebních příkazů z pozice vedoucího pracovníka, jehož identitu úspěšně falšují.

Motivace útočníka je u podobných útoků čistě finanční, pouze v krajních případech je cílem poškodit reputaci napadeného subjektu tím, že odcizená data zveřejní. Jak tedy útočníci monetizují aktivity souhrnně označované jako CEO Fraud? Nejprve se musejí dostat do korporátní sítě, přičemž k tomu používají technik sociálního inženýrství a tzv. spoofingu (falšování identity).

Sociální inženýrství je oblast hackingu zabývající se více psychologií nežli technologií. Jejím cílem je nenápadnou formou přimět oběť k jednání, které by, vědoma si důsledku svých činů, nikdy neudělala. Příkladem může být otevření závadné přílohy e-mailu, navštívení podezřelého odkazu nebo zasunutí USB disku do firemního počítače.

Falšovat identitu kohokoliv na internetu nebo v GSM síti není složité, neboť s podobným jednáním jejich architekti nepočítali. Odeslat e-mail s libovolnou adresou odesilatele, SMS z jakéhokoliv telefonního čísla nebo hovor uskutečněný opět zdánlivě z čísla kohokoliv na světě, není nic složitého. Ve skutečnosti je internet plný služeb, které vám umožní výše popsané útoky realizovat skrz uživatelsky přívětivé webové aplikace, a to buď zcela zdarma, nebo za poplatek v řádu jednotek, nanejvýš desítek korun.

Vžijme se na chvíli do role útočníka, který chce získat přístup do interní sítě vaší společnosti. Prohledáním webové prezentace získá útočník seznam telefonních čísel a e-mailových adres, včetně vzoru, kterým jsou tvořeny (zpravidla jmeno.prijmeni@spolecnost.tld). Jména zaměstnanců s jejich pracovním zařazením získá útočník z profesní sociální sítě LinkedIn, kde stačí ve vyhledávání předsadit název společnosti klíčovým slovem „Company:“. V tento moment se následující kroky odvíjejí od toho, jak velká cílová společnost je. Čím menší, tím hůře pro útočníka, neboť je pravděpodobné, že se ve firmě všichni znají osobně, sdílí společné pracoviště a komunikace mezi zaměstnanci má spíše neformální charakter. Navzdory tomu u velkých společností mnohdy osobně známe pouze úzký okruh lidí, společnost sídlí na více než jednom místě, komunikace s kolegy má formální charakter a mnohé procesy jsou řešeny formou outsourcingu. Velikost firmy včetně počtu zaměstnanců lze vyčíst buď opět z LinkedIn nebo různých veřejných registrů.

Ze seznamu zaměstnanců útočník vyřadí vedoucí pracovníky a zaměstnance IT nebo bezpečnostního oddělení. Zbývající jména podrobí analýze. Zběžným vyhledáváním ve fulltextových vyhledávačích a na sociálních sítích zjistí jejich zájmy (sport, zahrada, cestování), mimopracovní aktivity (podnikání, inzerce, spolky) a sociální vazby (partneři, rodina, přátelé). Výsledkem by měla být alespoň desítka na míru šitých personalizovaných e-mailů, které je možné vybraným zaměstnancům zaslat a vzbudit v nich zájem o otevření přílohy, navštívení odkazu nebo jinou obdobnou aktivitu. E-maily mohou mít i generický charakter. Příkladem budiž slevové akce pouze pro zaměstnance dané společnosti nebo výplatní lístek jiného zaměstnance omylem zaslaný na vaši e-mailovou adresu. V takovém případě zaměstnanci nemusí přijít podezřelý ani fakt, že je výplatní páska v přiloženém archivu chráněná heslem uvedeným v těle e-mailu. Výše mzdy je vrcholně citlivý údaj, který je potřeba chránit. Skutečným důvodem je ovšem obrana před analýzou ze strany antivirové ochrany na poštovním serveru.

V příloze výše uvedených e-mailů nejsou spustitelné soubory, jak by se mohlo na první pohled zdát. Soubor s příponou exe v e-mailu dnes totiž spustí málo kdo. Pokud má ovšem příloha příponu js, hta, vbs atp., běžní uživatelé jsou zpravidla zmatení. Uvedené přípony neznají a nejsou si tudíž vědomi jejich nebezpečnosti.

Přitom otevření takových příloh je ekvivalentní spuštění exe souboru. Kapitolou sama o sobě jsou pak makro viry. Ty jsou součástí běžně posílaných dokumentů s příponou doc a je nutná jejich aktivace ze strany uživatele. Aktivací se myslí kliknutí na tlačítko ve žlutém informačním pruhu v horní části dokumentu. Pokud na ně zaměstnanec klikne, opět je tato akce ekvivalentní spuštění exe souboru, proto se jej útočníci snaží k tomuto jednání motivovat. Příkladem může být rozbité kódování dokumentu, které se spraví pouze ve chvíli, kdy uživatel makra aktivuje. Slibuje-li obsah e-mailu a název dokumentu lákavý obsah, mnozí zaměstnanci toto riziko rádi podstoupí.

Přílohy jsou mnohdy uloženy v heslem zabezpečeném archivu. Důvodem je obrana před antivirovou kontrolou na poštovním serveru příjemce, pro zaměstnance to má ale i pozitivní psychologický dopad. V případě, že je v příloze inzerován obsah citlivého charakteru (výplatní páska, zálohy, osobní fotografie), zvyšuje heslo v příjemci důvěru v obsah archivu, neboť je heslo opodstatněné. Stejný obsah, jako v příloze, lze do e-mailu zasadit formou odkazu. Pravděpodobnost doručení do schránky příjemce se tím výrazně zvýší.

Pokud se útočníkovi nepodaří získat přístup skrz e-mailovou kampaň, může zkusit zaměstnancům zavolat. Ze sítě LinkedIn nebo dotazem na sekretariát společnosti si zjistí jméno a telefon pracovníka technického oddělení společnosti. Z tohoto čísla pak pomocí metod spoofingu zavolá zaměstnancům, kterým dříve posílal závadné e-maily. Představí se jako jejich kolega z technického oddělení, což bude podpořeno i reálným telefonním číslem. Následně zaměstnance upozorní, že se dle monitoringu šíří z jejich počítače virus a zda jim nepřišel nějaký podezřelý e-mail. Většina si zcela jistě vzpomene na e-mail se závadnou přílohou, kterou ale neotevřeli. Útočník skrývající se za identitu jejich kolegy jim vysvětlí, že přílohu spouštět nemuseli, neboť se jedná o sofistikovaný virus, jemuž ke spuštění postačí otevření daného e-mailu. V žádném případě se je nesnaží kárat, naopak, snaží se jim vyjít vstříc a nabídne pomocnou ruku. Každý zaměstnanec bez výjimky na firemním počítači občas dělá věci, které nejsou součástí náplně jeho práce, a na tyto chvíle si vzpomene ve chvílích, jako je právě tato. Pokud ho ovšem technik nekárá, ale snaží se mu pomoci, neboť navíc není jediný, komu se podobný incident stal, ale za dnešek už pátý v pořadí, s kým technik volá, stane se situace méně napjatá. Zaměstnanec vlastně žádnou chybu neudělal, to ten vir je tak neskutečně sofistikovaný. Uživatel stanice může být dokonce nápomocen, a to tak, že si ze serverů technické podpory stáhne záplatu a spustí na své stanici. IP adresu serveru technik rád nadiktuje a nezapomene zaměstnance upozornit, že je dostupná pouze z vnitřní sítě společnosti. To sice není pravda, ale v oběti to opět budí pocit důvěry. IP adresa je zvolena z více důvodů. Jen málo lidí rozumí tvaru IP oproti doménovému jménu, o lokálním a veřejném rozsahu ani nemluvě. Oproti tomu doména lišící se od té korporátní by budila nemalé podezření.

Smutnou realitou zůstává skutečnost, že podobnými akcemi útočníci nejčastěji cílí na ženy. Je to z důvodu jejich vyšší důvěřivosti a méně vřelému vztahu k výpočetní technice, než je tomu u mužů. I nám se podobný přístup vyplácí ve chvíli, kdy v rámci penetračních testů podobné útoky realizujeme.

Pokud se útočníkovi nepodaří získat přístup do interní sítě společnosti přes personalizované e-maily ani osobními telefonáty, což je velice nepravděpodobné, neboť mu k přístupu do intranetu stačí pouze jediný neškolený zaměstnanec, může přichystat několik USB disků a ty rozházet na parkovišti před budovou společnosti, nebo uvnitř jejich veřejných prostor. Nalezený USB disk totiž nebudí podezření, každý z nás někdy nějaký ztratil nebo naopak našel. Je-li USB disk nebo CD (i ty se ve zkostnatělých firmách dodnes používají) opatřeno lákavým popiskem typu „Záloha účetnictví“ nebo „Odměny vedení“, pak je zvědavost zaměstnanců a chuť spustit obsah média výrazně vyšší. Na disku se mohou nacházet dokumenty obohacené makro viry, případně upravené exe soubory tím způsobem, že budou vypadat jako adresáře. Operační systém Windows totiž ve svém výchozím nastavení skrývá známé přípony, je-li tudíž spustitelný virus opatřen ikonou, která ve Windows reprezentuje adresář, uživatel procházející strukturu disku klikne i na tento virus, neboť ho nerozezná od jiných adresářů. Zatímco ale očekává vstup do adresáře, na pozadí se nejprve spustí exe, které dodatečně otevře obsah jiného adresáře, aby uživatel nepojal podezření. O zařízeních typu Rubber Ducky, která se tváří jako USB disky, ale ve skutečnosti se jedná o klávesnice, ani nemluvě. Ty stačí ze strany zaměstnanců pouze zastrčit do USB portu počítače a v ten moment se na pozadí stáhne virus z internetu a spustí, aniž by byla vyžadována jakákoliv další akce ze strany oběti. Virus se nemusí ani stahovat, může být umístěn na paměťové kartě, která je součástí daného zařízení.

CEO Fraud má mnoho podob, nikoliv pouze výše popsané. Představte si například situaci, kdy jste účetní ve velké nadnárodní společnosti. Náhle vám přijde e-mail z adresy pana ředitele, ve kterém vás žádá o převod vysoké částky peněz na uvedený účet, případně okamžité proplacení přiložené faktury. Detaily pan ředitel, jak píše v e-mailu, vysvětlí později osobně, teď je ale potřeba co nejrychleji jednat a peníze poukázat na uvedený účet. Pro zvýšení důvěryhodnosti po pár minutách urgentnost žádosti podpoří krátká SMS z čísla pana ředitele. Jak byste se zachovali? Smutnou pravdou je, že se jedná o reálné případy z praxe, při nichž společnosti přišly o desítky tisíc Euro.

Jinou, běžnější formou těchto útoků, je manipulace s fakturami. Útočník si zjistí dodavatele nebo partnera cílové společnosti a z jeho e-mailové adresy pošle na účetní oddělení zprávu, že se mění číslo účtu, kam mají účetní nově hradit faktury. Ověřujete si podobné změny zvednutím telefonu? Málo kdo tak činí. Opět jde o případy z praxe, kdy společnosti přišly o nemalé finanční prostředky. Sofistikovanější verzí popsaného útoku je situace, kdy se útočníkovi podaří získat přístup do e-mailové schránky společnosti, kam jsou faktury zasílány. V tomto případě útočník příchozí faktury modifikuje tím způsobem, že jsou hrazeny na účet bílého koně namísto účtu dodavatele. Výsledek je stále stejný a má pro napadenou společnost podobu nemalých finančních ztrát.

Dokonalá a zároveň uživatelsky přívětivá, tudíž transparentní obrana neexistuje, ale pojmy jako SPF záznamy, SPF validace a antivirová kontrola na poštovním serveru by pro správce korporátních sítí neměly být neznámé, do značné míry totiž útočníkům znemožňují falšovat identitu a realizovat personalizované e-mailové kampaně obsahující malware. Vždy platí, že nejslabším článkem řetězce bude člověk, proto bychom neměli zanedbávat ani jejich pravidelné vzdělávání a máte-li tu možnost, podrobte svoji společnost penetračnímu testu formou sociálního inženýrství. Možná budete překvapeni, jak snadné je do ní získat přístup, stanete-li se obětí cíleného útoku. ■

Ing. Martin Klubal

Autor článku působí na pozici Senior IT Security Consultant ve společnosti AEC a.s.