Katedra informatiky
Přírodovědecká fakulta
Univerzita Palackého v Olomouci

DIPLOMOVÁ PRÁCE

Způsoby identifikace konkrétních skupin útočníků typu APT a FIN v rámci prověřování kybernetických útoků

2023

Bc. Vít Řehák

Vedoucí práce:
doc. Mgr. Jan Outrata, Ph.D.

Studijní program: Aplikovaná informatika,
Specializace: Počítačové systémy a technologie

Bibliografické údaje

Autor:	Bc. Vít Řehák
Název práce:	Způsoby identifikace konkrétních skupin útočníků typu APT a FIN v rámci prověřování kybernetických útoků
Typ práce:	diplomová práce
Pracoviště:	Katedra informatiky, Přírodovědecká fakulta, Univerzita Palackého v Olomouci
Rok obhajoby:	2023
Studijní program:	Aplikovaná informatika, Specializace: Počítačové systémy a technologie
Vedoucí práce:	doc. Mgr. Jan Outrata, Ph.D.
Počet stran:	53
Přílohy:	elektronická data v úložišti katedry informatiky
Jazyk práce:	český

Bibliographic info

Author:	Bc. Vít Řehák
Title:	Methods of identification of specific APT and FIN cyber attack groups in the scope of cyber attack analysis
Thesis type:	master thesis
Department:	Department of Computer Science, Faculty of Science, Palacký University Olomouc
Year of defense:	2023
Study program:	Applied Computer Science, Specialization: Computer Systems and Technologies
Supervisor:	doc. Mgr. Jan Outrata, Ph.D.
Page count:	53
Supplements:	electronic data in the storage of department of computer science
Thesis language:	Czech

Anotace

Diplomová práce popisuje kybernetické útoky, které byly v minulosti uskutečněny skupinami APT (Advanced Persistent Threat) a FIN (Financial). Z historické perspektivy se zaměřuje na zaznamenané útoky, metody útoků a nástroje, jež byly v průběhu těchto útoků využity. Práce rovněž popisuje konkrétní malware použitý útočníky. Jsou také uvedeny společnosti a instituce, které se podílely na vyšetřování a identifikaci jednotlivých útočníků či skupin.

Synopsis

Diploma thesis discusses cybernetic attacks that were carried out in the past by APT (Advanced Persistent Threat) and FIN (Financial) groups. From a historical perspective, it focuses on recorded attacks, attack methods, and tools used during these attacks. The thesis also describes specific malware used by the attackers. The work includes facilities and institutions that participated in the investigation and identification of individual attackers or groups.

Klíčová slova: Advanced Persistent Threat; Threat Actors; Kybernetická bezpečnost; Red Teaming

Keywords: Advanced Persistent Threat; Threat Actors; Cybersecurity; Red Teaming

Chtěl bych poděkovat panu doc. Mgr. Janu Outratovi, Ph.D. a panu pplk. Mgr. Vlastimilu Hruškovi za vedení mé práce, cenné rady a jejich pomoc.

Odevzdáním tohoto textu jeho autor/ka místopřísežně prohlašuje, že celou práci včetně příloh vypracoval/a samostatně a za použití pouze zdrojů citovaných v textu práce a uvedených v seznamu literatury.

Obsah

Seznam tabulek

1 Úvod

Kybernetická bezpečnost se v dnešní době, kdy dochází k růstu propojenosti světa společně s neustálým a rychlým rozvojem digitálních služeb, stala jednou z kritických oblastí. Každodenní používání počítačových systémů je nedílnou součástí moderního života, ať už v oblasti komunikace, komerce, infrastruktury, vládních organizací nebo například zábavy. To přináší rizika, kdy mohou tyto systémy být narušeny a zneužity, případně poškozeny. Pokusy o kybernetické napadení systémů se odehrávají v podstatě každý den. Pro ochranu těchto systémů je používáno široké spektrum strategií, technik a metod.

1.1 Mitre Att&ck

Jedná se o framework[1] a databázi technik, taktik a praktik (dále TTP), které jsou používány kybernetickými zločinci. Attack tyto TTP rozděluje do fází, při kterých se používají. Framework je běžně používán bezpečnostními profesionály.

Pojem „skupina“ je v rámci kybernetické bezpečnosti definován jako množina útočných aktivit, které vykazují podobnost v následujících oblastech:

1. Využívají stejné či blízce podobné techniky, taktiky a praktiky při vedení útoků
2. Posuzování cílů, na které jsou útoky vedeny (Útočí se na banky? Vojenské cíle? . . .)
3. Úroveň sofistikovanosti provedeného útoku (Útočil amatér, nebo byl útok veden profesionálně?)

Mitre jednotlivým skupinám uděluje unikátní názvy, jako může být například „APT15“, „APT28“, „FIN10“ apod.

Práce vychází ze znalostí, informací, zdrojů a dat poskytovaných Mitre.

1.2 Fáze kybernetického útoku

Průzkum (angl. „Reconnaissance“) Prvotní fáze útoku, kdy útočníci sbírají dostupné údaje o oběti. Může se jednat o veřejně dostupné informace (tzv. OSINT – Open Source Intelligence), telefonní čísla, emailové adresy, technické zázemí, infrastrukturu sítě apod. Útočníci aktivně hledají zranitelnost v systému, případně možnosti pro zneužití sociálního inženýrství.

Zajištění zdrojů pro vedení útoků (angl. „Resource Development“) Útočník se bude snažit koupit, vytvořit, ukrást nebo jiným způsobem získat zdroje, které využije pro vedení útoku. Může se například jednat o získání infrastruktury a nástrojů, jako jsou domény, DNS servery, uživatelské účty, webové služby, botnety, Command and Control základna apod.

Prvotní infiltrace sítě (angl. „Initial Access“) útočník pomocí různých metod nebo sociálního inženýrství nalezne cestu pro vstup do sítě nebo systému oběti. Útočník zde vytvoří pevný bod, ze kterého bude podnikat další kroky.

Dlouhodobější vytrvání v síti oběti (angl. „Persistence“) Útočník rozšíří a vylepší pevný bod tak, aby byl například schopný v síti nebo systému oběti přetrvat i v případě restartů, změně přihlašovacích a autorizačních údajů a podobných přerušení, které by mohly způsobit ztrátu přístupu.

Vyhýbání se detekci (angl. „Defense Evasion“) V této fázi jsou používány techniky pro skrytí a zamaskování nelegitimního přístupu do sítě nebo systému oběti. Může se jednat o snahu zasahovat do nastavení bezpečnostních systémů, mazání logů a dalších stop po aktivitách útočníků apod.

Eskalace pravomocí (angl. „Privilege Escalation“) Útočník se snaží pomocí různých technik docílí získání co nejvyšších oprávnění pro akce v síti nebo systému. Cíl v této fázi může být získání přístupu k „root“ nebo „SYSTEM“ účtům, administrátorským účtům, uživatelským účtům s vysokou pravomocí apod. Fáze částečně souvisí s předchozí fází kvůli získání trvalého přístupu k některému z účtů.

Krádež přihlašovacích a autorizačních údajů (angl. „Credential Access“) Záměrem této fáze je ukradení údajů, pomocí kterých by útočníci získali autorizovaný přístup do dalších částí systému. Může se například jednat o licenční klíče, jména, hesla, hashe hesel apod.

Průzkum lokální sítě oběti (angl. „Discovery“) Pomocí různých nástrojů a technik útočníci prohledávají síť oběti za účelem nalezení zájmových stanic apod.

Šíření malwaru na další stanice (angl. „Lateral Movement“) Útočníci se pomocí malwaru budou snažit dál šířit na další objevená nebo zájmová zařízení v síti oběti. Může dojít k vytváření dodatečných přístupových bodů pro útočníky.

Signalizovaní „Command and Control“ (dále jen CnC) serverů Malware z napadeného systému vytvoří komunikační kanál pro servery útočníků. To jim umožní malware dále ovládat, získávat a nahrávat data. CnC servery slouží jako komunikační stanice mezi útočníky a napadenými systémy.

Exfiltrace dat Po nalezení zájmových dat nebo informací útočníci data odešlou buď na některé ze svých CnC serverů nebo na jiný externí server, který mají pod kontrolou. Útočníci se snaží data dostat pryč ze sítě oběti tak, aby nebyli detekování. Podle situace buď zůstanou v systému oběti pro další sběr dat, nebo po sobě odstraní stopy a síť opustí.

Poškození nebo manipulace systému (angl. "Impact") V poslední fázi se útočníci pokusí systém zmanipulovat, poškodit nebo zničit. Může například dojít k narušení procesů systémů apod. Tato technika je používána za účelem dosažení jejich cíle nebo zamaskování jejich přítomnosti v systémů.

1.3 Atribuce

Důležitým pojmem při vyšetřování kybernetických útoků je tzv. „Atribuce“. Jedná se o proces identifikace, vyšetřování a zpětného trasování s cílem přiřadit útok konkrétnímu útočníkovi, skupině útočníků nebo státu a to s **určitou mírou pravděpodobnosti**.

Proces Atribuce pomáhá organizacím analyzovat motivy a tzv. „TTP“ (zkratka angl. „Tactics, Techniques and Procedures“ — taktiky, techniky a procedury) útočníků a tím v budoucnu předejít dalším podobným kybernetickým útokům.

Atribuce kybernetického útoku je velmi složitý proces, který ztěžují následující faktory:

Anonymita útočníci používají metody pro skrytí jejich identity (Proxy, VPN apod.)

„False Flag“ operace útočníci se často snaží svalit vinu na jinou organizaci nebo skupinu útočníků. Záměrem je snaha oklamat vyšetřovatele a odvést od sebe pozornost.

Likvidace forenzní stopy útočníci se po sobě budou aktivně snažit vymazat jakoukoliv stopu. Vyšetřovatelé jako důkazy většinou mají pouze částečné a neúplné informace.

2 APT versus FIN

Oba typy útoků jsou odlišné ve více směrech – zejména v charakteristice, záměru a motivaci útoku.

2.1 Advanced Persistent Threat

APT útok je ve většině případů prováděn útočníky, kteří jsou sponzorováni státem nebo se jedná o dobře zajištěný a organizovaný kriminálním syndikát. Záměr je infiltrovat systém oběti ve kterém se útočníci snaží zůstat co nejdelší možnou dobu, kdy se snaží vyhýbat detekci. APT klade důraz na utajení celého průběhu útoku. Vynakládá velkou snahu vytrvat v systému oběti co nejdéle. Vzhledem k téměř „neomezeným“ zdrojům, které mají útočníci s k dispozici jsou schopni vytvářet velmi sofistikované a specializované malwary, metody a sociální inženýrství. Záměrem je získání citlivých dat pro dosažení politických nebo strategických cílů, případně snaha o sabotáž nebo špionáž. Mezi napadené instituce často patří vojenské cíle, vládní organizace, výzkumná zařízení apod.

2.2 FIN

FIN útoky (zkratka od anglického slova „Financial“ případně "Financially motivated") jsou prováděny za účelem rychlého finančního zisku místo dlouhodobého sbírání informací. Útočníci se snaží získat a odcizit klíčová a citlivá data, která jsou pro chod instituce nezbytná. Může dojít i k zveřejnění ukradených dat pro poškození jména společnosti nebo k jejich zašifrování. Následuje vydírání oběti a požadování výkupného za nezveřejnění nebo obnovení dat. Mohou to být osobní údaje o klientech instituce, detaily o jejich kreditních kartách apod. Takováto data mohou být prodána třetí straně a zneužita pro nelegální aktivity. Na rozdíl od APT se FIN útoky zaměřují na podniky a instituce všech velikostí.

3 APT15

APT15[2] je skupina kybernetických útočníků s předpokládanou základnou v Číně. Mezi cíle jejich útoků patří ropný průmysl, vládní organizace, letectví a armádní cíle. Předpokládá se, že skupina je aktivní minimálně od roku 2010. [3]

V srpnu roku 2013 bezpečnostní analytici soukromé společnosti Trellix (dříve FireEye) odhalili kampaň kybernetické špionáže, kterou nazvali „Ke3chang“. Kampaň se odehrávala během eskalace Syrské krize. Cílem byly ministerstva zahraničních věcí Evropských států. Analytici se domnívají, že načasování útoků předcházelo setkání zemí G20, které se konalo v Rusku. Útočníci úspěšně kompromitovali devět ministerstev zahraničních věcí v pěti Evropských zemích.

3.1 Malware využívaný APT15

Skupina při útocích používala malwary s názvy „BS2005“[4], „BMW“[3] a „MyWeb“[3]. Funkcionálně se jedná o backdoory, které umožňují komunikaci s CnC servery, vykonávání podstrčených příkazů shellu, stahování/nahrávání souborů a uspání škodlivého programu na libovolnou nebo přednastavenou dobu. Veškerá komunikace probíhá pomocí HTTP protokolu.

3.2 Malware „BS2005“

Okamžitě po informování veřejnosti o zahájení intervence armády USA v Sýrii, začal Ke3chang využívat těchto informací k nalákání a oklamání obětí. Ke3chang této kampani udělil krycí název „moviestar“.

Jeden ze vzorků malwaru byl nalezen ve zkomprimovaném archivu, který obsahoval soubor s podvodným názvem:

```
1 US_military_options_in_Syria.zip
2 US_military_options_in_Syria.pdf.exe
```

Zdrojový kód 1: Názvy souborů

Je zřejmé, že dvojitá koncovka má za cíl oklamat oběť, aby spustila škodlivý program. Jedná se o „loader“, který stáhne další program s názvem „ie.exe“. Z debugovacího souboru tohoto programu (.pdb) se analytikům podařilo zjistit, že malware byl zkompilován 23.7.2013. Jednalo se tedy o v té době nejaktuálnější iteraci backdooru. Po spuštění programu „ie.exe“ dojde k signalizaci CnC serveru POST požadavkem na předdefinovanou adresu.

Hlavička HTTP požadavku vypadá následovně:

```
// Analyzovaná verze malwaru používá v URI /p3oahin/
// Jiné vzorky tohoto malwaru používají /ke3chang/ nebo /shfam9y/
// Parametr  r , který obsahuje data zakódovaná ve formátu base64

----------------------------------------------------------------------
POST /p3oahin/<filename>.aspx=?r=<Base64 Encoded Data>=&a=HTTP/1.1
----------------------------------------------------------------------

Accept: */*
Accept-Language: en-us
UA-CPU: x86 // Architektura procesoru oběti
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET
CLR 2.0.50727; .NET CLR 3.0.04506.30)
Host: cascais.epac.to
Adresa CnC serveru
Content-Length: 4
Connection: Keep-Alive

// Zakódovaná data souborů, nebo výstupu z podstrčených příkazů
<Data ve formátu base64>
```

Zdrojový kód 2: Struktura hlavičky POST požadavku odeslaného backdoorem

V URI je *<filename>* nahrazen náhodně jednou z následujících pevně zadaných možností:

- albumtop.aspx
- blogvideo.aspx
- celebrity.aspx
- modules.aspx

Útočnici v rámci kampaně sledují, kde byl malware aktivován. Údaj je zakódován ve formátu base64 a k jeho odeslání dochází ve výše zmíněném POST požadavku. Ve vzorku použitém během Syrské krize je vždy používáno označení „moviestar“.

Útočníci obfuskují odesílaná data. Každý odeslaný byte CnC serveru je transformován následujícími způsoby:

1. Každý byte je navýšen o konstantní hodnotu 0x27 (39 decimálně) a o hodnotu svého pozičního indexu
2. Následně je na byte aplikována operace Exkluzivní Disjunkce (XOR) vůči svému pozičnímu indexu
3. Data jsou zakódována do formátu base64

Zmíněný parametr „r“ v URI po dekódování obsahuje tyto údaje o oběti:

1. Lokální IP adresa
2. Název počítače
3. Doména
4. Krycí jméno kampaně (například „moviestar“)
5. Datum a čas
6. Identifikátor vykonaného příkazu
7. Identifikační kód svazku disku
8. Značka *<yes/no/nn>* – značka, která indikuje zda jsou k dospozici další data z výstupu příkazu, nebo nahrávání souboru (*"nn"* značí "NOOP"– "NO OPERATION")

Různé verze malwaru BS2005 používají rozdílné konstanty pro zkreslení šifrovaných dat a sbírají lehce odlišné údaje. Například verzi nainstalovaného mailového klienta, verzi Internet Exploreru, verzi Windows a zda byl malware spuštěn na virtuálním stroji.

Dodatečně k nasbíraným údajům v URI parametru „r“ jsou další nasbíraná data obsažena v těle POST požadavku. Obsah se dekóduje na jednu ze třech možností:

1. Značka *„no“* - nejsou přítomna žádná data
2. Obsah nahraného souboru
3. Výstup z podstrčeného příkazu shellu

POST požadavek je zpracován serverem útočníka a jako odpověď je oběti vrácena HTML stránka. Po bližším prostudování HTML kódu stránky můžeme vidět skrytý box pro uživatelský vstup (html tag „input“ s atributem *„hidden“*). Jako atribut hodnoty (*„value“*) je malwaru po kompromitaci oběti vrácen příkaz s parametry v podobě transformovaného textového řetězce.

Útočníci použili rozhraní IWebBrowser2 z platformy .NET. Toto rozhraní umožní vývojáři ve vyvíjené aplikace použít webový prohlížeč, který má uživatel aplikace už nainstalovaný. Připomínám, že se pohybujeme okolo roku 2010, - byl tedy do takovéto aplikace převážně integrován tehdy dominující Internet Explorer. Útočníci veškerou komunikaci mezi obětí a CnC serverem prováděli využitím tohoto rozhraní. Bezpečnostním analytikům tímto krokem ztížili práci, protože je komplikovanější zjistit, který proces je zodpovědný za škodlivou síťovou komunikaci.

APT15 v následujících letech vedli s lehce pozměněnými verzemi malwaru BS2005 několik dalších kampaní. Další kampaň zahájená v roce 2011, která byla pojmenována „snake“. Útočnici tentokrát jako návnadu použili emaily, které měly údajně obsahovat odkaz na soukromé fotografie manželky tehdejšího Francouzského premiéra.

Pomocí odkazu v emailu si oběť stáhla zaheslovaný .RAR adresář, který měl tyto fotky obsahovat. V adresáři byl přítomen jeden spustitelný malwarový soubor s návnadným názvem. Když oběť malware spustila, postup kompromitace oběti byl velmi podobný, jako je popsáno výše v kampani „moviestar“. Malware pomocí post požadavku informuje CnC server. Specifikovaná URI adresa v hlavičce požadavku obsahovala klíčové slovo „G20news“. Bezpečnostní analytici se vzhledem k tomuto faktu domnívají, že útoky mají souvislost se setkáním ministrů financí G20, které se konalo 15. října 2011 v Paříži.

3.2.1 Kampaň „dream/doplhin“

V roce 2012 následovaly další útoky. Pro oklamání oběti byly tentokrát opět použity falšované informace o probíhajícím Olympijských hrách v Londýně. Cílem se stala nejmenovaná společnost podnikající v chemickém, výrobním a těžebním průmyslu.

Útočníci zneužili závažnou chybu v Adobe Readeru (kód exploitu CVE-2010-2883). Pomocí speciálně naformátovaného .pdf souboru útočníci dosáhli přetečení bufferu (stack-buffer overflow), což jim umožnilo oběti podsunout a vykonat libovolný kód.

Po aktivaci malwaru jsou kontaktovány dva CnC servery. Útočníci pozměnili endpoint POST požadavku, kterým informuje CnC servery. Snahou bylo vyhnout se automatické detekci kvůli použití stejné URL jako v předchozích verzích malwaru. Další změnou byla odlišná přičítaná konstanta bytů dat před transformací do kódování base64.

3.3 Malware „MyWeb“

Dle bezpečnostních analytiků společnosti FireEye [4] APT15 tento malware používali v období mezi rokem 2010 a 2011. Podle přítomných metadat byl analyzovaný vzorek zkompilován 1. ledna 2011. Útočníci se snažili oběti oklamat a nalákat pomocí témat týkajících se Evropské bezpečnosti a vojenské obrany.

MyWeb byl oproti předchozím malwarům APT15 specifický tím, že používal lepší techniky pro detekci virtuálního prostředí/stroje. Z knihovny WinAPI malware zavolal funkci *„GetSystemTime“* a navrácenou hodnotu milisekund si uložil. Následně provedl cyklus, který opakoval ve vyšších statisících iteracích. V tomto cyklu si malware opět volal funkci *„GetSystemTime“*, kterou si uložil do druhé proměnné a v každé iteraci cyklu ji aktualizoval. Po dokončení cyklu byla srovnána prvotní hodnota s druhou. Pokud si obě hodnoty byly rovny, malware se ukončil.

Na konci souboru malwaru byl přidán blok o velikosti 104 bytů. Blok obsahoval šifrované konfigurační parametry. Každý byte tohoto bloku byl při šifrování snížen o jeho poziční index. Oproti předchozím malwarům APT15 je možné za běhu měnit adresu CnC serveru. Tato adresa je v konfiguračním bloku uložena na začátku, tedy na offsetu 0x0. Útočníkům to otevřelo možnost „stěhovat“ CnC servery a udržovat si oběti za běhu. Nebylo už nutné malware pro změnu adresy znovu rekompilovat.

Když malware úspěšně informuje CnC server, je uspán na předdefinovaný počet sekund. Tato hodnota je obsažena v konfiguračním bloku za adresou CnC serveru, konkrétně na offsetu 0x20. Pokud bylo připojení na CnC server neúspěšné, malware se uspí na několik minut. Počet minut pro opakované uspání je opět přednastaven v konfiguračním bloku.

MyWeb slabě šifruje pouze výstup z podstrčeného příkazu. Používá k tomu stejný algoritmus, jako u mawlaru „BS2005“. Také je opět odečtena konstantní hodnota od každého bytu. Překvapivě přenos souborů už šifrován není. Je proveden ve formátu base64. Údaje o oběti jsou předány v URL adrese jako parametry v čistě textovém formátu bez jakékoliv úpravy nebo šifrování.

3.4 Malware „BMW“

APT15 tento malware prvně použila během začátku roku 2010[4]. FireEye první vzorek zanalyzovala až v červnu téhož roku. Situaci komplikovalo to, že nebyla přesně známa příčina prvotního prolomení systému. Odhady ovšem vinu přisuzují spear-phishingovým emailům, tak jak tomu bylo u BS2005 a MyWeb.

Po aktivaci BMW odeslal CnC serveru signál POST požadavkem. Adresa napodobovala emailové služby portálu Yahoo, v analyzovanému vzorku byla její konkrétní podoba následující – *„mail.yahoo.sendsmtp.com“*. Program v sobě měl několik předdefinovaných endpointů, ze kterých náhodně jeden vybral pro sestavení celé URI.

Stažené a nahrané soubory jsou opět před transformací do formátu base64 slabě šifrovány tím, že od bytů je odečtena přednastavená konstantní hodnota.

V těle POST požadavku byly ve formátu base64 obsaženy následující informace o oběti:

1. IP Adresa
2. Název počítače
3. Doména
4. Verze internetového prohlížeče
5. Mailový klient
6. Jméno kampaně
7. Datum a čas
8. Informace o proxy
9. Značka, zda malware běží na virtuálním stroji
10. Druhý parametr z odpovědí CnC serveru
11. Poslední vykonaný příkaz
12. Počet bytů, které byly staženy po vykonání posledního příkazu příkazem

3.5 Další metody používané APT15

Tradičně, jedna z metod byly spear-phishingové emaily, které buď obsahovaly škodlivou přílohu, nebo odkaz na škodlivý soubor.[3]

Co se týče zajímavějších a sofistikovanějších metod, skupina například využila v roce 2010 zranitelnost v Microsoft Word (kód exploitu CVE-2010-3333). Pomocí uměle vyrobeného a upraveného .rtf souboru bylo možné docílit přetečení a zápisu na zásobník, což umožnilo vykonání libovolného cizího kódu. Podobnou zranitelnost skupina využila i ve velmi používaném softwaru Adobe Reader (kód exploitu CVE-2010-2883).

Infrastruktura CnC serverů je postavena na dynamické DNS. Útočníci pravidelně měnili IP adresy, aby ztížili případnou detekci malwaru. Bylo zjištěno, že různé malwary vytvořené APT15 komunikovaly přes stejné IP adresy. FireEye analyzovala IP adresy CnC serverů nasbíraných během útoků a při reverzním IP lookupu společně s dalšími už nezveřejněnými metodami nalezla minimálně 99 dalších CnC serverů APT15. Majorita těchto serverů se nacházela v Číně, Hong Kongu a USA.

Analytikům se podařilo získat přístup k jednomu z CnC serverů. Server byl ovládán pomocí webového rozhraní, které zobrazilo seznam narušených strojů a bylo možné s nimi komunikovat nebo je ovládat. Webové rozhraní také obsahovalo skenovací funkci, která narušeným strojům odeslala několik předepsaných příkazů pro průzkum sítě, ke které jsou připojeni.

Konkrétní příklady používaných příkazů:

ipconfig /all - nastavení všech síťových adaptérů oběti

set - všechny hodnoty proměnných prostředí

netstat -ano - seznam aktivních spojení, TCP/UDP portů včetně ID příslušných procesů

tasklist - seznam všech běžících procesů

net start - seznam běžících síťových služeb

net localgroup administrators - seznam uživatelů ve skupině administrators

net use - seznam sdílených prostředků v síti (např. síťový disky, ...)

net view /domain - informace o doméně, ke které je oběť připojena

systeminfo - podrobné informace o systému (OS, CPU, vlastník, RAM, ...)

Několikrát příkaz „dir“ - V některých případech přednastavený průzkum adresářů Program Files a .NET framework

3.6 Metody rozšíření malwaru po kompromitaci

Po signalizaci CnC serveru spuštěným malwarem dochází ke sběru informací o napadeném stroji a sítí ke které je připojen. Mezi použité nástroje patří například *„gsecdump“* – nástroj pro získávání hashů hesel a bezpečnostních údajů z LSA (Local Security Authority) na Windows[3].

Po naskriptovaném skenu útočníci dále zkoumali síť manuálně. Analytici jako důkaz dodávají fakt, že v lozích se objevují příkazy s překlepy nebo byly špatně zadány [3]. Pomocí nástroj „net“ útočníci získali informace o uživatelích. Vytipovali si uživatele se zvýšenými pravomocemi, nebo rovnou s pravomocemi administrátora. V některých případech se útočníci snažili nakopírovat škodlivý soubor na ostatní stroje v síti. Akci se snažili zamaskovat častou změnou názvu souboru a pravidelným přesouváním do různých adresářů.

V další fázi následoval sběr zájmových dat, například soubory nebo výpis obsahu vybraných adresářů. Data byla zkomprimována do formátu *„.rar“* a odeslána CnC serveru. Po úspěšném odeslání byl archiv u oběti vymazán.

3.7 Vyšetřování a přisouzení zodpovědnosti za útoky APT15

Je složité s jistotou určit, kdo je za útoky zodpovědný. Analytik musí dobře porozumět chování útočníků v rámci celého útoku/kampaně. Mezi některé další proměnné, ke kterým je nutné přihlédnout patří načasování útoků, na koho jsou útoky zaměřeny, sofistikovanost malwaru, sofistikovanost použitých metod a rozsah celého útoku. Analytik v drtivé většině případů nemá všechny informace,

takže v analýzách bývají mezery. Musí se opírat i o nepotvrzené hypotézy ostatních analytiků nebo společností kybernetické bezpečnostní.

Útoky je také možné „přisoudit“ více způsoby. Útok může být přisouzen jedné skupině, konkrétním provozovatelům CnC serverů nebo rovnou státu (Čína, Rusko, další země ze sankčních seznamů . . .).

FireEye[4] se při vyšetřování útoků zaměřila na stopy v technickém provedení malwarů a styl fungování CnC serverů. Samotné binární soubory malwaru obsahovaly v hlavičkách stopy Čínského jazyka a Čínských znaků písma. Webové rozhraní, kterým byl ovládán CnC server obsahovalo kombinace anglického a čínského jazyku. Zároveň analytici malware BS2005 vyzkoušeli na jednom z CnC serverů, ke kterému získali přístup. Sesbírané informace dorazily zpět s popisky v čínském jazyce. Hostované servery, které neměly dynamickou DNS byly registrovány u čínského poskytovatele.

FireEye[3] nezveřejnila přesný způsob, ale podařilo se jim zjisti, že malware byl při vývoji testován na virtuálních strojích. Při zrekonstruování historie příkazů a jejich výstupů bylo zjištěno, že malware byl testován na Windows s nastaveným výchozím čínských jazykem.

Vzhledem k nasbíraným důkazům byl původ útoků přisouzen skupině operující z Číny. Nepodařilo se ovšem získat jejich identity. Motivace k útokům také není známa.

3.8 Malware *„RoyalCLI“* a *„RoyalDNS“*

V roce 2017 bezpečnostní analytici společnosti NCC Group detekovali narušení systému svého klienta, který poskytoval velké množství služeb vládě Velké Británie. Byly odcizeny citlivé dokumenty týkající se armády Spojeného Království a několika ministerstev. K útokům byly použity dva nové backdoory – „RoyalCLI“ a „RoyalDNS“[5].

RoyalCLI je v několika směrech podobný malwaru BS2005. Používá stejné postupy pro přenos dat a opětovně využívá rozhraní IWebBrowser2 z aparátu .NETu pro komunikaci s CnC servery.

Útočnici pro vytvoření perzistence a opěrného bodu použili batch skripty, kterými upravili registry Windows Run Keys. Tedy došlo k „zavrtání“, aby se malware spustil při prvotním bootu nebo přihlášení ke kompromitovanému počítači. Z pohledu analytiků tato metoda není nějak zásadně sofistikovaná. Spíše se ale přiklánějí k názoru, že se tímto krokem útočníci chtěli vyhnout detekci IDS (systémů pro odhalení průniků) na základě „chování“ programu. Nejedná se tedy o situaci, kdy by APT15 neměla kapacity na vývoj sofistikovanějšího softwaru.

Po nastolení perzistence útočníci v dalším kroku začali sbírat a skenovat síť napadeného stroje. Na oběti byly také použity keyloggery a nástroje pro odcizení emailů a dat. Zaměřili se hlavně na hledání a vyčtení sdílených prostředků SharePointu. K tomuto využili nástroj „spwebmember“.

Nástroj byl vytvořen v .NETu a obsahoval před-konfigurované hodnoty a řetězce pro sestavení SQL příkazů. Po aktivaci se připojil k Sharepointové SQL

databázi a provedl zadání dotazu. Dotaz měl za úkol exportovat všechna data z databáze, včetně metadat. Sesbíraná data byla zkomprimována do .rar archivu.

Velice dobrým a oblíbeným nástrojem je Mimikatz. Služba Windows LSASS (Local Security Authority Subsystem Service) je zodpovědná za vynucování bezpečnostních politik. Uživatelská hesla nikdy nejsou uložená v čistě textové podobě. Vždy jsou přetransformována do hashe, což výrazně komplikuje potenciálním útočníkům snahu získat původní heslo. Mimikatz se umí vložit do procesu LSASS v momentě, kdy se uživatel chce přihlásit.

Po přihlášení je v Mimikatzem narušeném prostředí heslo v čisté textové podobě ukradeno. Tím se útočníkům ušetří velká práce s potencionálním prolamováním hashe. Navíc se útočníci prolomení hashe nemusí dočkat.

Dalším způsobem, jak pomocí Mimikatzu dosáhnout eskalace pravomocí je tzv. „Pass the Hash“ útok. Pokud útočníci získají hash hesla uživatele, nemusí ani znát heslo v čisté podobě. Mimikatz je schopný procesům rovnou podstrčit hash hesla uživatele a získat tak přístup k jeho zdrojům.

Po prvotní exfiltraci dat se útočníkům po několikatýdenní pauze podařilo opět získat přístup do systému. Dosáhli toho díky ukradenému VPN certifikátu jedné z obětí, který získali v prvním útoku. APT15 nyní využili druhý zmíněný malware – RoyalDNS.

Hlavní charakteristikou malwaru byla komunikace s CnC servery pomocí DNS protokolu. Zprávy byly odesílány v TXT záznamu DNS dotazu. TXT záznamy se používají pro ukládání textových dat. Útočníci mohou vložit například powershellový příkaz, parametry pro příkazy nebo posílat malwaru instrukce k dalším krokům.

Útočníci pro skenování a perzistenci používali zabudované nástroje Windows, jako například net, tasklist, ping, netstat, ipconfig, apod. Pro rozšíření malwaru na další stroje v síti útočníci využili sdílené disky v sharu. Po namountování disku začali kopírovat škodlivé soubory na ostatní stanice.

3.9 OKRUM

Kocem roku 2016 analytici společnosti ESET[5] [6] objevil dosud neznámý backdoor, který pojmenovali *„Okrum“*. Byl použit k distribuci malwaru *„Ketrican“* (podrobnosti v další kapitole). Objekty a instituce, které byly napadeny Okrumem už se v minulosti staly cílem napadení pomocí starších malwarů APT15.

Okrum podobně jako předchozí malwary APT15 umožňuje stahovat a nahrávat soubory, vykonávat shellové příkazy, spouštět soubory, uspat se na předepsanou dobu nebo aktualizovat se na novější verzi.

Aktivace a zprovoznění Okrumu má několik fází. Okrum je nainstalován a nahrán do operační paměti dvěma komponentami – loaderem a instalátorem. Obě komponenty byly často a pravidelně upravovány, aby se zamezilo a zároveň ztížilo detekování malwaru. I s úpravami funkcionalita zůstala totožná. ESET [6] zajistil více než sedm vzorků loaderu a minimálně dvě verze instalátoru.

3.9.1 Loadery

Loadery vytvořené APT15 byly *.dll* (dynamicky linkované knihovny) soubory. Hlavní úlohou loaderů je skrytí malwaru před Firewallem nebo anti-virovými systémy. Loader po aktivaci na zařízení oběti malware zprovozní. Loader může malware v sobě nést v šifrované podobě. Po aktivaci nesený malware dešifruje ho a spustí.

První varianty loaderů Okrumu obsahovaly malware uložený ve svém zdojovém kódu. Ve čtyřech posledních bytech loaderu byla zakódována celková velikost malwaru. Celý blok s malwarem byl šifrován algoritmem RC4. Klíč pro dešifrování byl v nezměněné podobě obsažen před blokem s hodnotou určující velikost malwaru.

Objevila se i pokročilejší a zajímavější varianta loaderu. Malware už nebyl zabalen do loaderu, ale byl vložen do souboru .png obrázku. Z pohledu uživatele je obrázek při prohlédnutí naprosto v pořádku. Uživatel už ale nevidí, že v souboru s obrázkem je malware skrytý v tzv. *„zTXt“* bloku. Podle specifikace formátu *.png* se v tomto bloku vyskytují textová data s dodatečnými podrobnostmi. Tento blok není ale pro správné zobrazení nutný. Toho využili útočníci a do tohoto bloku vložili šifrovaný malware. Klíč pro dešifrování následoval hned za daty backdooru. Tato metoda skrývání dat se nazývá *„steganografie“*[7].

Loadery předpokládají, že upravený soubor s obrázkem je už na stroji oběti přítomen. Analytici ESETu[6] zjistili, že při aktivaci loader rekurzivně prohledává adresář *„Program Files“*, kde by se v náhodném podadresáři obrázek měl vyskytovat.

Po každém bootu nebo přihlášení uživatele je vytvořená nová nadefinovaná úloha, která spustí předepsaný soubor.

Oproti starším malwarům APT15, loadery pro Okrum obsahovaly čtyři testy pro detekci virtuálního stroje:

1. Metodu s funkcí „GetTickCount“, která je popsána výše u malwaru *„MyWeb“*
2. Dvě hned po sobě jdoucí volání funkce *„GetCursorPos“*. Pokud se souřadnice kurzoru liší, může jít o vlastnost virtuálních strojů, kdy vrací souřadnice kurzoru náhodně. Tím se prozradí, že malware byl spuštěn na virtuálním stroji
3. Pokud má stroj méně než 1.5 gigabytů RAM, loader se ukončí
4. Loader se spustí pouze tehdy, pokud bylo alespoň třikrát stisknuto libovolné tlačítko myši

Pokud napadené zařízení projde všemi testy, je malware dekódován a spuštěn.

3.9.2 Instalátory

První analyzovaný instalátor se maskoval jako falešný instalátor služby *„Ntmssvc“* (služba pro správu a obsluhu vyměnitelných úložišť). Bylo možné nastavit dva módy instalace, výběr se provedl klamavým argumentem *„install“* a *„uninstall“*. Falešná služba je spuštěna při každém bootu systému. Datum a čas kompilace v metadatech instalátoru je velmi podobný jako u první varianty loaderu. To naznačuje, že tyto dvě komponenty mají být použity společně.

Druhý instalátor při spuštění očekává tři argumenty:

<md> - určuje, zda se má vytvořit nová úloha, nebo zda má být backdoor nakopírován do startup adresáře Windows

<tn> - jméno úlohy

<fp> - cesta k souboru

Při každém bootu nebo přihlášeni uživatele je vytvořena nová úloha, která spustí soubor na předepsané cestě. Pokud je zvolena možnost nakopírování do startup adresáře, je do něj umístěn zástupce na předepsaný soubor, který útočníci chtějí spustit.

3.9.3 Backdoor

Backdoor je .dll (dynamicky linkovaná knihovna). Hlavička spustitelného souboru je speciálně upravená tak, že zůstává validní a zároveň se dá interpretovat jako shellcode. Díky tomu může loader backdoor nahrát do paměti svého procesu. Pomocí instrukce *jump* a *call* je registr ukazatele na instrukce (eip) posunut na první instrukci .dll knihovny. Tím se začne vykonávat podstrčený shellcode.

Útočníci využili metodu *„Reflective Loader“*. Spočívá v tom, že škodlivý kód je možné načítat přímo z operační paměti a tím se vyhnout jeho čtení z pevného disku. Tím se dá obejít několik bezpečnostních opatření Windows.

Backdoor obsahuje tyto funkce:

- *DllEntryPoint*
- *ReflectiveLoader*
- *Payload*

V momentě, kdy se začne vykonávat Shellcode, je zavolána funkce *„ReflectiveLoader“*. Tato funkce je obsažena v tabulce exportů knihovny. *„ReflectiveLoader“* zanalyzuje systémovou knihovnu kernel32.dll hostitelského procesu, aby mohl dopočítat a zjistit adresu tří zmíněných funkcí. V dalším kroku je alokována oblast

v paměti hostitelského procesu, kam si knihovna nakopíruje hlavičky a sekce „.text“, „.data“). Nyní jsou nalinkovány .dll, které jsou potřeba pro správnou funkci knihovny. Po dokončení linkování se začíná vykonávat payload.

Okrum se umí získat bezpečnostní oprávnění právě přihlášeného uživatele, využívá k tomu systémovou funkci *„ImpersonateLoggedOnUser“*. Pomocí získaných pravomocí sbírá tyto informace:

1. Jméno počítače v síti
2. Uživatelské jméno přihlášeného uživatele
3. IP Adresu
4. informace o DNS záznamech
5. Informace o operačním systému
6. Identifikační token uživatele
7. Architekturu CPU
8. Detaily o prostředí uživatele (země původu, jazyk . . .)

Pro komunikaci s CnC servery je využita symetrická kryptografie a HTTP. Konkrétně šifra AES. Oběť se pokusí vyjednat s CnC serverem klíč. Pokud se to nepodaří, je použit předdefinovaný klíč v backdooru. Po zprovoznění šifrované komunikace jsou CnC serveru odeslána nasbíraná data. Oběť povely od CnC serveru dostává přes cookies v HTTP požadavku. Příkaz šifrovaný AES je přijat ve formátu base64. Všechny příkazy mají svůj unikátní hash.

Pro krytí svých operací CnC servery útočníků byly registrovány na zdánlivě legitimních doménách. Příkladem může být *„support.slovakmaps[.]com“*, při útocích na cíle na Slovensku.

3.10 Ketrican

Předpokládá se, že se jedná o další backdoor z „dílny“ APT15[6]. Ketrican má stejné schopnosti, jako měly malwary použité v kampani *Ke3chang*. Umí tedy nahrávat a stahovat soubory, „uspat“ se na zadanou dobu a spouštět programy nebo shellové příkazy. Stejně jako u předchozích malwarů, Ketrican v sobě má zadefinovaná klíčová jména kampaní (například slova jako *„water“*, *„baby“*, *„warm“*, *„pictu“*, . . .) a adresy CnC serverů.

3.10.1 Shody s předchozími malwary APT15

Stejně jako to dělá BS2005, Ketrican si udělá ve svém adresáři kopii programu příkazové řádky (cmd.exe). Pomocí ní vykonává podstrčené příkazy. Vytvořené soubory jsou vkládány do skrytých systémových adresářů Shellu. Malware přesnou cestu k těmto adresářům získá pomocí klíče v registrech, který odkazuje

na „Shell Folders“. Záznam je v registrech přítomen už pouze z důvodů zpětné kompatibility starších verzí Windows a aktuálně není používán. Tento krok byl zjištěn i u ostatních malwarů APT15, které byly používány během kampaně Ke3chang.

Dalším pojítkem je použití stejné metody pro detekci virtuálního prostředí jako u malwaru z rodiny „MyWeb“, kde je použita již zmíněná metoda využívající systémovou funkci „GetTickCount“.

Třetí shodou je opětovné využití rozhraní *„IWebBrowser2“*, které se opět ve snaze maskovat škodlivou komunikaci útočníků. K přenosu dat pomocí HTTP protokolu využívají Internet Explorer. Po zpracování požadavku CnC serverem je vrácena stránka, která také obsahuje skryté *„input“* pole, jehož atribut „value“ obsahuje obfuskované příkazy nebo argumenty pro agenta.

4 APT28 a APT29

4.1 APT28 „Fancy Bear“

APT28[8] je skupina kybernetických útočníků, která podle sesbíraných důkazů patří pod Ruské vojenské zpravodajství GRU (Hlavní správa rozvědky) a jedná se o speciální jednotku. Skupina je aktivní minimálně od roku 2004. APT28 je známa útoky na volební kampaň Amerického prezidenta v roce 2016, útoky na Světovou anti-dopingovou Agenturu a jaderné zařízení Spojených států amerických.

4.2 APT29 „Cozy Bear“

APT29[9] je skupina kybernetických útočníků přiřazována pod Službu vnější rozvědky (SVR) Ruské federace. Skupina operuje minimálně od roku 2008 a útočí primárně na vládní organizace zemí Evropy a NATO a výzkumná zařízení. Společně s APT28 provedli útoky na Americké DNC a softwarovou společnost SolarWinds.

4.3 GRU a SVR

Chtěl bych upozornit na rozdíl mezi GRU a SVR. GRU spadá pod ruské vojenské velení, tedy se hlásí Ruskému ministru obrany a náčelníku generálního štábu. SVR je podřízena přímo Ruskému prezidentu. Jedná se tedy o dvě odlišné speciální jednotky, které na sobě nejsou závislé.

4.4 Kybernetické napadení demokratického národního výboru (DNC) USA

V roce 2015 a 2016 došlo k závažnému útoku na DNC[10] v USA [11]. Jedná se o období volby nového Amerického prezidenta, kdy mezi sebou soupeřili Donald Trump a Hillary Clintonová.

Útočníkům se podařilo získat citlivá data, textové konverzace, dokumenty a zásadní množství emailů. Ukradená data obsahovala důležité informace o strategických krocích a rozhodnutích DNC, včetně v té době probíhající kampaně Clintonové. Ukradená data se objevila na WikiLeaks – organizaci, která anonymně zveřejňuje utajené informace.

Zástupci DNC si pro vyšetřování incidentu zvolili Americkou soukromou bezpečnostní společnost CrowdStrike[12]. Důvodem, proč se DNC neobrátilo na Americkou FBI byla hrozba zpolitizování vyšetřování. CrowdStrike je nestranná soukromá společnost. Vyšetřování vládní FBI by se mohlo dostat pod politický tlak některé z volených stran. Nebylo možné zaručit, že by nedošlo k únikům citlivých údajů o vyšetřování za účelem politického zisku. Dalším důvodem je fakt, že CrowdStrike patří k suverénně nejlepším a nejzkušenějším společnostem v oblasti kybernetické bezpečnosti.

CrowdStrike v pozdější fázi vyšetřování sdílel s FBI podrobnosti o forenzní analýze útoku. Okolnostmi útoku se zabývala i společnost SecureWorks, která se domnívá, že útočníci napadli zaměstnance DNC pomocí spear-phishingových emailů. DNC vlastnilo doménu „www.hillaryclinton[.]com“, která byla registrována na Google Domains. Prozkoumání DNS záznamu „MX“ (emailový záznam) odhalilo, že doména pro emailové služby používá Google Apps, tedy řešení nabízené Googlem. Google Apps umožňovalo používat Gmailové účty pro autorizaci a přihlašování. Toho zneužili útočníci, kteří vytvořili přesnou kopii přihlašovacího formuláře do Gmailu. V URL ve formátu base64 byl předán email oběti, který byl předvyplněn ve formuláři, aby se zvýšila důvěryhodnost falešného přihlašovacího formuláře.

Prolomení systémů DNC během léta roku 2015 je přisuzováno skupině APT28, které byla přidělena přezdívka „Fancy Bear“. O rok později začaly útoky APT29, přezdívané „Cozy Bear“. K útokům APT28 byly použity malwary *„X-Agent“* a *„X-Tunnel“*. Jejich kopie byly nalezeny na narušených serverech a systémech při útocích na DNC.

4.5 Malware X-Agent

X-Agent[13] je multiplatformní spyware vytvořen APT28. Bývá označován jako „Vlajková loď“ APT28. Umožňoval útočníkům zaznamenávat stisknuté klávesy (keylogging), vykonávat shellové příkazy a exfiltrovat zájmové soubory patřící oběti na CnC servery útočníků. Spyware byl kompatibilní s operačními systémy Linux, Windows, Android a iOS. Spyware byl poprvé detekován v listopadu roku 2012 a s velkou pravděpodobností se používá dosud. X-Agent umožňuje komunikaci s CnC servery pomocí dvou protokolů. Prvním je HTTP protokol a druhým je SMTP/POP3, tedy emailový protokol.

Spyware byl vytvořen v jazyce C++. Analytikům slovenské společnosti ESET[13] se podařilo zajistit celý zdrojový kód spywaru, který byl zkompilován pro napadení systému s Linuxem. Ze získaného vzorku se analytici domnívají, že verze pro Linux vznikla z verze pro Windows. Naznačují tomu zakomentované příkazy ve zdrojovém kódu, které pocházejí z Win32. Tedy verze pro Linux byla znovu implementována a systémové funkce Windows byly vyměněny za Linuxové systémové funkce. Například funkce jádra Linuxu „pthread_exit“ zastoupila funkci „TerminateThread“ z Win32. Funkcionálně spyware zůstal totožný.

```
int startXagent(wstring path)
{
    [...]

    AgentKernel krnl( (wchar_t *)path.c_str() );  ❶

    IAgentChannel* http_channel = new HttpChannel();  ❷
    //IAgentChannel* smtp_channel = new MailChannel();

    IAgentModule* remote_shell = new RemoteShell();  ❸
    IAgentModule* file_system = new FSModule();
    //IAgentModule* key_log = new RemoteKeylogger();

    krnl.registerChannel(http_channel);  ❹
    //krnl.registerChannel(smtp_channel);
    krnl.registerModule(remote_shell);
    krnl.registerModule(file_system);
    //krnl.registerModule(key_log);

    krnl.startWork();  ❺

    [...]
}
```

Obrázek 1: Zdrojový kód hlavní funkce X-Agentu [13]

Na obrázku 1 můžeme vidět inicializační funkci ze zdrojového kódu spywaru.

Zdrojový kód analyzované verze spywaru je složen ze čtyřech částí (modulů):

1. AgentKernel – Spravuje běh spywaru a je rozhraní pro předávání zpráv mezi ostatními moduly a CnC servery
2. RemoteKeyLogger – Zaznamenává stisknuté klávesy
3. FSModule – Obstarává systémová volání pro práci se soubory (read, write, execute, . . .)
4. RemoteShell – Podstrkuje příkazy útočníků do Linuxového terminálu

4.5.1 AgentKernel

Instance „hlavní“ třídy AgentKernel je složena z následujících objektů:

1. AgentKernel – Spravuje běh spywaru a je rozhraní pro předávání zpráv mezi ostatními moduly a CnC servery
2. RemoteKeyLogger – Zaznamenává stisknuté klávesy
3. FSModule – Obstarává systémová volání pro práci se soubory (read, write, execute, ...)
4. RemoteShell – Podstrkuje příkazy útočníků do Linuxového terminálu

4.5.2 Běh malwaru

Po aktivaci spyware odešle CnC serveru informace o zprovozněných modulech. Zprávy mají pevnou strukturu. Ve zdrojovém kódu je třída zapouzdřující zprávu nazvána „CryptRawPacket“. Zajímavostí ve zdrojovém kódu je přítomnost komentářů v Ruském jazyce.

První segment zprávy – hlavička není nijak šifrována. Obsahuje dvě položky:

1. ID agenta => unikátní ID, pomocí kterého CnC server identifikuje spyware
2. Checksum => Kontrolní součet pro ověření integrity zprávy (metoda CRC)

Tělo je šifrované algoritmem RC4 a obsahuje pět položek:

1. ID agenta – Má stejný účel jako totožně pojmenovaná položka v hlavičce. Rozdíl je v tom, že údaje můžou být nasbírané jiným napadeným zařízením ve stejné síti, než ze kterého je zpráva odeslána. ID se tedy v hlavičce a v těle může lišit.
2. ID modulu – identifikace modulu, který zprávu buď odeslal nebo kterému je zpráva od CnC serveru adresována
3. ID příkazu – Identifikuje příkaz, který byl vykonán nebo teprve vykonán bude
4. Data – pointer, který odkazuje na místo v paměti, kde jsou data přítomna
5. DATA_TOKEN – Konstantní hodnota ve zdrojovém kódu, jejíž význam analytici nedokázali přesně určit. Domnívají se ale, že se jedná o kontrolní hodnotu pro ověření integrity těla zprávy při procesu dešifrování.

Patička stejně jako hlavička zprávy není šifrována a obsahuje jedinou položku – klíč pro dešifrování těla zprávy (RC4).

Při spuštění je inicializován soubor modulu LocalStorage, do kterého jsou ukládána nasbíraná data. Tento soubor je slabě šifrován, aby soubor s nasbíranými daty nebyl u oběti přítomen v úplně „čisté“ podobě. Odesílání zpráv je realizováno zmíněným rozhraním ChannelController. Podle zprávy z CnC serveru se v tomto modulu volí i metoda odeslání dat, tedy zda bude použit HTML protokol nebo emailový protokol. Spyware si také kontroluje funkčnost komunikace s CnC serverem. Pokud se server nedaří kontaktovat aktuálně používaných protokolem, zkusí použít druhý protokol.

Přijaté úkoly od CnC serveru jsou ukládány na straně malwaru do dynamického pole, vzhledem k používanému jazyku c++ byla konkrétně použita struktura „vector“. Všechny záznamy vektoru jsou uloženy v šifrované podobě. Z vektoru příkazy načítá AgentKernel, který je předává modulům. Dešifrovaní úkolu provádí AgentKernel těsně před předáním konkrétnímu modulu.

4.5.3 Komunikace HTTP protokolem

Úvodní komunikace CnC serveru se Spywarem je vždy GET požadavek. Pokud Spyware kontaktuje CnC server, odesílá POST požadavek. Pro oba typy požadavků má adresa přibližně takovouto šablonu:

```
1    http://x.x.x.x/path/?parameter1=value1&parameter1=value1&&mark-
        token&...
```

Zdrojový kód 3: URI Šablona X-Agentu

„Path“ specifikuje endpoint, v programu je přednastaveno 7 možných hodnot. „parametr1“ a „parametr2“ může nabývat jedné z 15 možností a přidělená hodnota je pseudonáhodný řetězec. Oba parametry jsou v podstatě zbytečné a nemají žádný význam. Důležité jsou pouze parametry „mark“ a „token“. V případě, že malware běží na stroji s Linuxem, je „mark“ nastaven na hodnotu „ai“. Parametr “token” je 20 bytová hodnota. V těch 20 bytech jsou zakódovány tyto položky:

1. Prvních 5 bytů nemá žádný význam a slouží pouze jako výplň
2. Key – čtyřbytová hodnota, náhodně generovaná
3. URL_TOKEN => Přednastavená hodnota, na kterou byl aplikován XOR vůči předchozímu parametru „key“. Není přesně jasné, jakou roli položka hraje. Pravděpodobně slouží k ověření integrity.
4. ID agenta

Všechny položky kromě úvodních pěti bytů jsou transformovány do formátu BASE64.

4.5.4 Komunikace emailovým protokolem

Analytikům se během vyšetřování podařilo zajistit celý zdrojový kód emailového proxy serveru. Proxy byl naprogramován v Pythonu a zprostředkovával emailovou komunikaci mezi aktivními spywary a CnC servery. Proxy byl schopen převádět emaily přijaté od spywarů (agentů) na http protokol pro komunikaci CnC servery.

Spyware má ve svém kódu pevně zadanou SMTP adresu serveru, přihlašovací emailovou adresu a heslo, které použije, aby se autorizoval a přihlásil. V různých vzorcích spywaru se nachází různé emailové servery. Často využívali bezplatné poskytovatele emailových služeb, případně cizí servery, ke kterým se jim podařil získat přístup. Objevily se i případy, kdy útočníci pro server zaregistrovali vlastní doménu.

Při používání emailu pro komunikace s CnC servery nastávají dvě komplikace. Server musí být schopný rozlišit emaily agentů od ostatních emailů, například nevyžádané pošty. Také musí být filtr proti nevyžádané poště upraven tak, aby nefiltroval emaily od agentů. APT28 si implementovali vlastní upravený protokol, který v názvu předmětu příchozího emailu hledá tyto položky:

1. Key – podobně jako u položky se stejným názvem výše, jedná se o náhodně generovaný klíč

2. SUBJ_TOKEN – konstantní předdefinovaná hodnota, na kterou je aplikován XOR vůči klíči. Položka slouží k odlišení emailů odeslaných agenty od ostatních přijatých emailů.

3. ID Agenta – identifikace agenta, opět je na hodnotu aplikován XOR vůči klíči

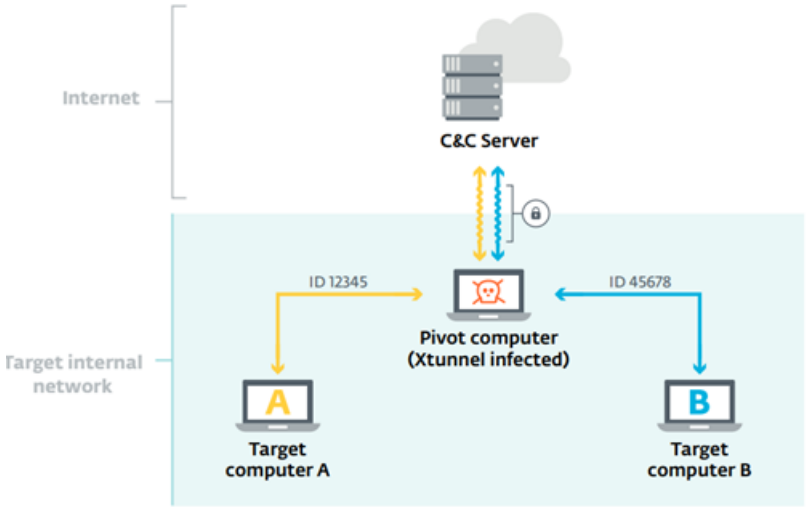
Obsah emailu je náhodně generovaná hodnota transformovaná do formátu BASE64. Stejným způsobem je pojmenován soubor s nasbíranými daty v příloze.

Proxy server v pravidelných intervalech kontroluje příchozí poštu. U každého emailu se zkouší dekódovat název předmětu. Pokud se podaří získat platný subject token (SUBJ_TOKEN), jedná se o platný email od některého z agentů spywaru. V takovém případě bude příloha emailu na straně serveru uložena do adresáře „FROM“. Každý agent má na serveru svůj podadresář, útočníci si tak udržují evidenci, co který agent získal a odeslal. Proxy všechna nová data z adresáře „FROM“ v těle POST požadavků http protokolu odesílá CnC serveru. Komunikace v opačném směru probíhá tak, že proxy v intervalech kontaktuje CnC server, kterému odesílá GET požadavek s přiloženým seznamem aktivních agentů. Odpověď CnC serveru obsahuje instrukce pro všechny agenty. Proxy po přijetí rozpisu příkazů od CnC serveru vytvoří pro adresované agenty soubor s instrukcemi. Tyto přílohové soubory jsou kódovány stejným způsobem, jak při odesílání agentem. Po připravení souborů jsou tedy vloženy do emailové přílohy a odeslány vybraným agentům.

4.6 Malware X-Tunnel

Další malware, který byl nalezen na serverech napadeného DNC byl tzv. „x-tunnel“ [13]. APT28 jednu z prvních verzí malwaru nasadili v roce 2013 a v tentýž roce byla zaznamenán analytiky společnosti ESET. Specifickou charakteristikou malwaru byl upravený a na míru vytvořený síťový protokol, který byl zapouzdřen v protokolu TLS.

Při úspěšném napadení jednoho zařízení oběti (dále „pivot“) malware umožňoval monitorovat a skenovat a sledovat komunikaci v lokální síti. Útočníci se tímto dostali k datům zařízení v interní síti, které nejsou z venkovní sítě dostupné a dosažitelné.



Obrázek 2: Znázornění funkce X-Tunnelu [13]

4.6.1 Handshake

Pivot pro komunikaci CnC serverem provede handshake a pokusí se navázat zabezpečenou komunikaci, kterou šifruje algoritmem RC4. Cílem handshaku je předání klíče, jelikož RC4 je symetrická šifra. IP adresa a port serveru je definován ve zdrojovém kódu malwaru nebo je případně sdělen ve formě parametrů při volání příkazu v příkazové řádce.

CnC server a agenti malwaru mají společnou pevně definovanou strukturu. V této struktuře se nachází 256 hodnot o velikosti 32 bytů. Při provádění handshaku je CnC serveru odeslán offset pozice hodnoty ve struktuře, která bude použita jako klíč pro symetrickou šifru. Agent k offsetu přidává i další hodnotu, která funguje jako důkaz. Jde o ověření, že CnC serveru nepřichází jen náhodná čtyřbytová hodnota a odesílatel opravdu má přístup ke kódovací tabulce. Malware vezme hodnotu, která se v kódovací tabulce nachází o 128 záznamů dále.

Pokud je přesažena velikost kódovací tabulky, je provedena operace modulo pro výpočet ověřovacího indexu. Na tuto hodnotu je aplikována RC4. Samotný klíč tedy nikdy necestuje přes síť, je odesílán pouze jeho offset a důkaz. CnC server si hodnotu ověří a pokud je vše v pořádku, odpoví zprávou „OK“ již šifrovanou domluveným klíčem zpět agentu. Tím je spojení navázáno. CnC server zvolí port. Volba portu už probíhá šifrovanou komunikací mezi oběma stranami.

4.7 Tunelování

Útočníci se tunelováním snaží obejít bezpečnostní opatření sítě oběti. Lze tím například v některých případech obejít Firewall. Pokud je blokován port 80 (předpokládaný port pro HTTP), ale není zakázán port 22 (předpokládaný port pro SSH) útočník může pomocí tunelu toto nastavené omezení obejít a připojit se k webovému serveru v cílové interní síti. Samozřejmě to určitě není tak jednoduché, protože dnešní Firewally mají k dispozici pokročilé techniky jako hloubkovou analýzu paketů, „behaviorální“ analýzu aplikační vrstvy síťového modelu a mnoho dalších.

Pivot se snaží s ostatními zařízeními v interní síti navázat TCP spojení, například pomocí SSH. V analýzách není přesně specifikován konkrétní způsob, ale pro tento účel je k dispozici několik nástrojů. Například nástroje „Sshuttle“, „RPivot“, „Chisel“ a spoustu dalších.

Po zprovoznění zabezpečení komunikace CnC server využívá pivota pro komunikaci s ostatními zařízeními v jeho lokální síti. CnC server si u každého pivota vede evidenci jeho „tunelů“, tedy zařízení, kterým je pivot schopen delegovat zprávy.

Po úspěšném zprovoznění tunelu jsou všechny zprávy odeslané CnC serverem delegovány pivotem konkrétnímu zařízení přes vytvořený tunel. Komunikace funguje i opačným směrem, kdy je do zprávy doplněno ID tunelu, přes který zpráva cestovala.

Zpráva CnC serveru s požadavkem má dvě podoby. Záleží, zda je chtěný tunel označen IP adresou nebo názvem domény.

Adresace IP adresou (9 bytů):

1. ID tunelu (2 byty) -– identifikace, který tunel bude používán
2. ID příkazu pro otevření tunelu (1 byte)
3. IP adresa (4 byty)
4. Port (2 byty)

Adresace názvem domény (proměnlivá velikost):

1. ID tunelu (2 byty)
2. ID příkazu pro otevření tunelu (1 byte)
3. Délka názvu domény (proměnlivá velikost)
4. Jméno domény (Délka je určena předchozí položkou
5. Port (2 byty)

4.8 Další vývoj malwaru

Malware od první zachycené verze v roce 2013 postupně dostával řadu vylepšení. To na jednu stranu zvyšovalo nebezpečnost malwaru, ale analytici podle přidaných nebo upravených funkcionalit mohli lépe odhadovat a předvídat účel malwaru, na který je připravován.

4.8.1 Přidání UDP připojení

Na konci roku 2013 byla malwaru přidána schopnost navazovat kromě TCP i UDP spojení. UDP se ale v laboratorních analýzách malwaru chovalo velmi nespolehlivě a pro obecné použití mělo velkou chybovost. Pravděpodobně se jednalo o jednorázovou operaci a použití UDP u tohoto malwaru už se nikdy znovu nepotvrdilo.

4.8.2 Šifrování pomocí TLS

V dubnu 2014 byla přidána podpora TLS pro komunikaci mezi pivotem a CnC serverem. Původní komunikace (šifra RC4 s kódovou tabulkou) zůstala nezměněna, ale vše bylo zapouzdřeno do TLS protokolu.

4.8.3 Komunikace přes HTTP protokol

V polovině roku 2015 byl zajištěn vzorek malwaru, který nově umožňoval komunikaci s CnC serverem pomocí http protokolu. TLS pro zabezpečení komunikace pořád zůstává. V dešifrované hlavičce požadavku se v tagu „Accept-Language“ objevuje „RU“, tedy zkratka pro ruský jazyk.

4.8.4 Obfuskace kódu

Obfuskování kódu je proces, kdy se útočníci snaží maximálně ztížit pochopení zdrojového kódu a výrazně zkomplikovat jeho analýzu nebo případné reverzní inženýrství. Metod, jak obfuskovat kód je mnoho a pořád se vyvíjí nové. Pro představu, obfuskování kódu může například provést tyto kroky:

1. Jména proměnných a funkcí – Jsou upraveny na nesmyslné a dlouhé názvy, které se snaží mezi nimi skrýt jakýkoliv náznak provázanost nebo návaznost

2. Přidávání „junk“ (zbytečného) kódu – Vkládání zbytečných a pro funkcionalitu programu/malwaru naprosto nepotřebných podmínek, cyklů, zapouzdřování do uměle vytvořených struktur, rozdělení kódu na segmenty a následné promíchání apod. Velký efekt to má například na případnou analýzu strojového kódu (assembleru).

3. Kódování řetězců a dat =–Data jsou transformována do pro člověka nečitelné podoby. V případě řetězců se může například jednat o několikrát zmíněný formát base64.

Pro obfuskaci je k dispozici velké množství nástrojů. Nástroje můžou být jak obecné (nástroj frameworku Metasploit „Invoke-Obfuscation“), tak zaměřené na konkrétní jazyk („ProGuard“ pro Javu, „CodeVeil“ pro .NET apod.)

Binární soubory malwaru, které prošly procesem obfuskace byly zajištěny v roce 2015. Prošly drastickou změnou ze syntaktického hlediska a velikost malwaru se zdvojnásobila. Čitelnost kódu byla tím pádem nesčetněkrát horší, protože i sebeprimitivnější funkce výrazně nabobtnala.

4.9 Napadení společnosti Solarwinds

Solarwinds je americká společnost, která vyvíjí software pro podniky, konkrétně Software pro monitoring sítě, podnikové systémy a informační technologie. Společnost v roce 2020 měla více 300 000 klientů.

Společnost se stala obětí útoku APT29[14]. Útočníkům se podařilo napadnou jejich produkt „Orion“ a úspěšně se vyhýbali detekci průniku několik měsíců. To je velmi dlouhá doba a počet narušených systémů byl vysoký, Orion používalo více než 33 tisíc podniků. Útočníci tedy měli přístup k citlivým datům. Orion byl používán i významnými institucemi. Mezi ně se například patří vojenské instituce jako je například Pentagon, dále ministerstvo zdravotnictví a financí spojených států Amerických a mnoho dalších.

4.9.1 Malware „SUNBURST“

Sunburst[15] [16] je backdoor vytvořený APT29. Poprvé ho zaznamenali analytici společnosti FireEye na jaře roku 2020. K prvotnímu průniku do systému oběti došlo pomocí tzv. „supply chain compromise“, jedná se o metodu, kdy útočníci zmanipulují produkt nebo jeho dodávku před tím, než ho obdrží koncový spotřebitel.

Například může dojít k manipulaci s následujícími prvky:

1. Manipulace vývojářských nástrojů
2. Manipulace úložišť zdrojového kódu
3. Manipulace open-source zdrojových kódů, které nějaká aplikace využívá
4. Manipulace aktualizací nebo distribuce softwaru
5. Prodej/Dodávka padělaného softwaru

Konkrétně Sunburst byl vložen do oficiální aktualizace softwaru Orion a tím byl rozšířen na velké množství zařízení. Malware byl vložen do jedné z legitimních .dll knihoven, které Orion používal. Útočníci tím tedy obešli problém s digitálním podpisem souboru, který se tím pádem jevil jako legitimní i přes to, že v něm byl obsažen škodlivý kód.

Digitální podpis je důležitá technika pro ověřování autentičnosti dokumentu, souboru, zprávy apod. Poskytovatel vytvoří unikátní klíč, který je odvozen od jeho privátního klíče. Příjemce si může autenticitu ověřit vůči veřejnému klíči poskytovatele a tím potvrdit, zda přijatý objekt opravdu patří poskytovateli. Velkým problémem bylo to, že Sunburst se kvůli přítomnosti legitimního podpisu obešel řadu bezpečnostních opatření jako antivirus, případně specializované EDS (Endpoint Detection Systems).

4.9.2 Běh malwaru

Malware se maskoval jako oficiální plugin, který měl sbírat informace pro zlepšení a zjednodušení uživatelské zkušenosti při používání Orionu. Pluginy si Orion při svém startu, včetně zmíněného modifikovaného pluginu. Předtím, než se malware vůbec pokusil kontaktovat CnC servery, se na náhodnou dobu v rozmezí 10 až 14 dnů uspal. Zároveň před jakýmkoliv pokusem kontaktovat servery se malware snažil skenovat běžící procesy a hodnoty v registrech, kde hledal antivirové nebo forenzní služby. Vše vyhledával podle seznamu, který má v sobě uložený. Pokud je nalezena shoda, podle typu programu se malwaru buď úplně deaktivuje, uspí nebo provede další kroky. Některé vzorky malwaru se snažily obcházet bezpečnostní protokoly tím, že se snažily upravovat jejich hodnoty v registrech.

Po uplynutí úvodní doby „spánku“ malware odešle CnC serverům základní informace jako je název počítače v síti, jeho IP adresu a detaily o operačním systému. Malware se dále snažil vyhnout detekci tím, že úvodní a menší zprávy jsou CnC serveru odesílány pomocí DNS protokolu v nepravidelných a dlouhých intervalech, většinou v řádu dvou a více hodin mezi sebou.

Kromě zpráv pomocí DNS protokolu je využit také HTTP protokol, který v těle požadavku obsahuje ve formátu JSON instrukce pro agenta. HTTP požadavek v URL obsahuje několik parametrů, nicméně podle analýz nemají žádný význam pro funkcionalitu.

Zajímavostí je i fakt, že SolarWinds ve své aplikační dokumentaci doporučoval svým klientům udělit v antivirových, EDR a v GOP politikách Orionu výjimku pro dosažení „optimálního“ běhu programu. Zároveň bylo doporučováno přidat několik servisních uživatelů, kterým měl být přidělen plný přistup do všech částí Orionu včetně bezpečnostních výjimek.

V seznamu níže můžeme vidět příkazy, které v kódované podobě mohly přijít od CnC serveru. Vždy přišel jen jejich kód, který byl přednastaven ve zdrojovém kódu:

```
private class HttpHelper
{
    private enum JobEngine
    {
        Idle,
        Exit,
        SetTime,
        CollectSystemDescription,
        UploadSystemDescription,
        RunTask,
        GetProcessByDescription,
        KillTask,
        GetFileSystemEntries,
        WriteFile,
        FileExists,
        DeleteFile,
        GetFileHash,
        ReadRegistryValue,
        SetRegistryValue,
        DeleteRegistryValue,
        GetRegistrySubKeyAndValueNames,
        Reboot,
        None
    }
```

Obrázek 3: Seznam příkazů pro Sunburst s jejich unikátními ID [14]

4.9.3 DGA algoritmus (Domain Generation Algorithm)

Zajímavostí je funkcionalita[17], kdy instance malwaru používají jeden CnC server jako „koordinátora“. Koordinátor konkrétnímu agentovi odešle parametry pro generování finální adresy koncového CnC serveru, na kterou agent odešle nasbíraná zájmová data . Koordinátor také posílá instrukce, například zda se má agent na určený čas odmlčet, tedy přestat posílat pravidelné „beacon“ signály anebo posílání signálů obnovit.

Koordinátor byl také zároveň schopen udržovat všechny koncové CnC servery pod vyrovnanou zátěží. Nestávalo se tedy, že by jeden server útočníků byl přetížen a byla by s ním obtížná komunikace, zatímco ostatní servery by byly zatíženy málo nebo vůbec.

Dynamické určování koncových CnC serverů značně ztěžovalo jejich detekci a obranu. Nebylo tedy možné jednoduše zablokovat pár adres, které byly odhaleny jako CnC servery útočníků.

Koordinátor byl nastaven jako autoritativní DNS server. Konkrétně u zkoumaného vzorku byla doména „avsvmcloud[.]com“, může nás napadnout podobnost s cloudovou službou AVS, tedy „Azure VMware Solution“ poskytovanou

společností Microsoft.

DGA pro výše zmíněnou doménu generuje a doplňuje subdomény a šablona kompletní adresy může vypadat například takto:

```
1 {GUID}{Encoded_AD_domain}.appsync-api.{region}[.]avsvmcloud[.]com
```

Zdrojový kód 4: šablona URI adresy pro Sunburst [17]

Kde „GUID“ je hash vytvořený na základě různých informací o oběti, například aktuální datum, čas, den v týdnu, MAC adresy zařízení, hodnoty vybraných záznamů v registrech apod. Je komplikované tohle přesně určit, kvůli nutnosti zpětně prolamovat hash.

„region“ je určení, v jaké oblasti agent běží. Může nabývat jednu ze možných čtyřech hodnot:

1. eu-west-1
2. us-west-2
3. us-east-1
4. us-east-2

„Encoded_AD_domain“ je hodnota navrácená utilitní funkcí .NETu pro zjištění jména domény, ke které je zařízení připojeno. Pomocí tohoto kroku je většinou možné zjistit, které společnosti napadené zařízení patří. V pozdějších verzích malwaru začali útočnici tuto hodnotu šifrovat.

4.9.4 Exfiltrace dat

Pravděpodobně nejdůležitější a nejrizikovější krok pro útočníky. V případě Sunburstu byly pro exfiltraci použity emaily vytvořené a odeslané pomocí Powershellových příkazů. Pokud to situace dovolila, tak byl použit i HTTP protokol, kdy byla data odeslána v těle požadavku. V některých případech útočníci data exfiltrovali manuálně pro minimalizování rizika detekce Firewallem a dalšími bezpečnostními systémy. Bylo zaznamenáno i použití protokolu ICMP pro přenos dat. Data byly vždy před odesláním obfuskována, šifrována a zkomprimována pro ztížení detekce.

5 FIN10

FireEye[18] v Kanadě v roce 2017 objevila sérií útoků s podobnými použitými technikami a stejně cílenými útoky se zaměřením na finanční zisk. Těmto útokům udělila FireEye přezdívku FIN10[19]. Po napadení systému se útočníci snažili společnost vydírat a vytěžit za získaná data co nejvíce finančních prostředků. Když se nepřistoupilo na požadavky útočníků, několikrát byla data trvale znehodnocena nebo zveřejněna.

Útoky probíhaly mezi roky 2013 a 2016. Cíle útoků byly organizace v severní Americe, především kasina a těžební průmysl.

5.1 Používané metody

Ve většině intruzí přisuzovaných FIN10 bohužel nebyl dostatek důkazů[18], aby se s jistotou přesně určilo, jak k prvotnímu napadení systému došlo. Vzhledem k tomu, že u dvou útoků byly prokázány spear-phishingové emaily se škodlivými přílohami, byla tato metoda přisuzována i ostatním provedeným útokům.

U jednoho vzorku emaily obsahovaly odkaz na HTML Aplikaci (koncovka formátu .hta). HTA používá kombinaci HTML, dynamické HTML a skriptovací jazyky jako jsou VBScript, JavaScript, JScript. Skriptovací jazyky umožňují vykonávat kód. Vše běží v enginu Internet Exploreru, avšak už mimo jeho bezpečnostní model. HTA bylo relativně pohodlné na používání, ale stalo se jedním z často používaných nástrojů kybernetických útočníků.

V druhém případě email obsahoval wordovský dokument se zapnutými makry. Dokument imitoval dotazník pro zaměstnance, kde byly předvyplněna konkrétní a přesná data, jako bylo jméno zaměstnance a podobně. Pro dodatečné doplnění důvěryhodnosti útočníci připravili i falešné profily společností na portálu LinkedIn.

Pro vytvoření pevného bodu v systému oběti útočníci použili několik nástrojů – „Metasploit“, „Empire“ a „SplinterRAT“. Můžeme si všimnout, že útočníci nepoužili žádný vlastnoručně vytvořený malware. Spoléhali se spíše na veřejně dostupný software a skripty.

5.2 Metasploit

Jedná se o open-source framework určený pro penetrační testování aplikací[20]. Je to velice populární a účinný nástroj pro bezpečnostní analytiky a správce sítě, ale zároveň velmi silnou zbrání pro útočníky. Metasploit má v repertoáru přes 2000 různých přizpůsobitelných exploitů pro velké množství platforem (například Android, Cisco, Java, .NET, Linux, Windows a mnoho dalších). Stejně tak dává k dispozici vyšší stovky různých payloadů. Například různé shellové příkazy, které u oběti umožní vykonat různé skripty nebo příkazy. Dále také dynamickou podobu payloadu, kdy je různě transformován nebo obfuskován, aby nebyl odhalen anti virovými systémy.

Nejzajímavějším payloadem je tzv. „Meterpreter“. Meterpreter obsahuje velké množství pokročilých možností pro ovládání napadeného stroje a kontrolování vzdáleného přístupu. Aktivace Meterpreteru dává útočníkovi významnou verzatilitu, která zjednodušuje například exfiltraci dat, eskalaci pravomocí, napadení dalších zařízení v síti apod. Útočníkovi je umožněno vykonávání shellových příkazů, přístup k příkazové řádce, souborovému systému a registrům.

Výhoda Meterpreteru spočívá také v tom, že se nahraje do paměti již běžícího procesu metodou DLL injection. Umí i různě střídat hostitelské procesy. Nikdy tedy není vytvořen nový proces a Metepreter se nikdy neuloží na pevný disk. Tím se minimalizuje forenzní stopa.

FIN10 Meterpreter několikrát použili. Umožnilo to velké zjednodušení práce, protože Meterpreter obsahuje funkcionality, které jsou na komplexní a náročné na implementaci. Obsahuje velké množství metod a funkcionalit například na obcházení antivirových systémů. Útočníkům stačilo přidat jen vlastní .dll knihovny.

5.3 Empire (Do roku 2019 PowerShell Empire)

Podobně jako Metasploit, Empire [21] je framework pro penetrační testování a nasazuje se v druhé fázi útoku, po kompromitování systému oběti. Framework je open-source a je dostupný na jeho GitHubu. Jeho oficiální podpora byla ukončena v roce 2019, ale komunita ho pořád nějakým způsobem udržuje a byl vytvořen jeho fork.

V době útoků, v rozmezí let 2013–2016 byl Empire jeden z nejúčinnějších a nejlepších nástrojů. FIN10 ho používali k vytváření vlastních škodlivých utilit v PowerShellu. Empire byl například použit pro manipulaci s registry zařízení, upravování plánovače úloh oběti, vytváření nových služeb a k provádění skriptů, které komunikovaly s CnC servery. Konkrétním příkladem byla služba „updater“, kterou FIN10 přidali do plánovaných úloh za účelem posílání pravidelných hlášení CnC serverům.

5.4 Remote Access Trojan (například zmíněný SplinterRAT)

RAT jsou programy, které si jsou relativně podobné s keyloggery – sbírají informace o stisknutích kláves, přihlašovacích jménech, heslech, občasný screenshot obrazovky oběti, emaily, chaty apod. Odlišují se ale v tom, že umí získat přístup k zařízení oběti. K tomu používají předkonfigurované komunikační protokoly, které jsou většinou zprovozněny během prvotní intruze. Tím můžou útočníci získat přístup plnohodnotný a neomezený přístup k zařízení.

SplinterRAT [22] je open-source framework pro operátory „červeného“ týmu při penetračním testování a je volně dostupný na jeho GitHubu. Aktivní instance uměla stahovat soubory, nahrávat soubory na CnC server útočníků, spouštět programy, vysílat „Beacon“ signály a procházet souborový systém oběti. FIN10 SplinterRAT použili několikrát, později byl vyměněn a plně nahrazen Meterpreterem a jeho funkcionalitami.

5.5 Narušení systému

FIN10 hojně používali skripty[18], které měly způsobit poškození, případně rovnou zničení dat. Několik dalších skriptů, které FireEye zajistila se snažily vymazat klíčové systémové soubory, například v adresáři Windows System32 a tím způsobit kolaps operačního systému. Případně se zaměřovaly na vybrané ovladače různých zařízení nebo síťových adaptérů.

V jednom z ze skriptů FIN10 byl nalezeny tyto dva PowerShellové příkazy:

```
mkdir "C:\emptydir"
robocopy "C:\emptydir" "C:\windows\system32"/MIR | shutdown /s /t 1800
```

Obrázek 4: Příkaz používaný FIN10 při útocích [23]

První příkaz prostě a jednoduše vytvoří prázdný adresář. V druhém příkazu můžeme vidět nástroj „robocopy“ – nástroj Windows pro kopírování souborů nebo adresářů. Oproti klasickému „copy“ má řadu pokročilých a velmi užitečných funkcionalit.

První dva parametry určují zdrojový a cílový adresář. Můžeme ale vidět třetí parametr „MIR“, významově zkratka slova „mirror“ – zrcadlit. Zrcadlení spočívá v tom, že Robocopy nakopíruje všechny soubory ze zdrojového adresáře do cílového a následně odstraní všechny soubory cílového adresáře, které nejsou ve zdrojovém adresáři. Vzhledem k tomu, že zdrojový adresář je prázdná složka tak dojde k vymazání souborů (které nejsou otevřeny nebo používány nějakým procesem) v systémovém adresáři „System32“, což způsobí pro operační systém katastrofální následky.

FIN10 se tímto chytrým trikem snažila skrýt před antivirovými systémy svůj záměr poškodit systém. Kdyby použili nástroj „del“ nebo „rmdir“, pravděpodobně by akce byla ihned zablokována bezpečnostními systémy.

Příkaz „shutdown“ dle zadaných parametrů „s“ a „t“ zařízení vypne za 1800 sekund, tedy za půl hodiny. Windows už kvůli vymazaným systémovým souborům už nikdy nenabootuje.

5.6 Vydírání oběti

Po úspěšné kompromitaci sítě útočníci začnou oběti vyhrožovat zveřejněním, zničením nebo znehodnocením dat. V tomto ohledu je nutné se opravdu ujistit, zda došlo ke kompromitaci sítě a zařízení. Často se objevují „false-alert“ výhružky, kdy podvodníci v síti nejsou a nikdy se tam nedostali. Jedná se vyloženě o pokus od oběti získat nějaké zdroje, který lze s klidem v duši ignorovat.

Tohle ale samozřejmě není případ FIN10. Běžnou praktikou je předvedení důkazu, že útočnici data opravdu mají k dispozici. Nějaká malá část ukradených dat je vydírané oběti ukázána. Oběti jsou předány instrukce a požadavky. FIN10 v drtivé většině případů požadovali platbu v rozmezí 100-500 Bitcoinů. Pro představu, jeden Bitcoin měl v roce 2014 hodnotu cca třiceti tisíc amerických dolarů. Bitcoin je pro útočníky výhodný kvůli faktu, že Bitcoinová peněženka je anonymní a je velmi složité ji zpětně vystopovat.

Kromě vystrašení oběti je záměrem i vyvolat časový nátlak. Je v zájmu útočníků, aby se operace neprotahovala a oběť jejich požadavky splnila v co nejkratším časovém úseku. To je jeden z hlavních již zmíněných rozdílů oproti metodice APT útoků.

Na obrázku níže můžeme vidět jeden z vyděračských emailů od FIN10:

At this point your company has two options:

1. Meet our demand and pay the one time price of 500 BTC (Bitcoin)
   -all of the stolen data is permanently deleted, none of it gets posted on the internet, your computer network will remain safe and functional and your organization wont be bothered again.
   -Bitcoin transactions are anonymous no one will know you cooperated

2. Refuse to pay and let the deadline pass:
. if payment is not received in 10 days or less the first data dump of your company/patrons data will be posted all over the internet for the world to see. we will also send emails to each one of your customers/patrons directing them to see their leaked data on the internet.
. if still after another 72 hours payment isnt received, a 2nd data dump will happen, and every 72 hours after that until all other data listed above along with much more will be leaked and available for download on both the dark web and on torrent sites to anyone who wants to download it.
. Your computer network will be taken down in a large scale attack and will require weeks if not months to get functional again.

It is not our goal to cripple your company, our goal is simply to receive 500 BTC (Bitcoin). Calling the authorities might seem like an obvious choice. However realize that they will not be able to help you in this case as they have no jurisdiction where we are. And bringing it to them makes your sensitive situation that much more public.
make the right choice.

-TeslaTeam

Obrázek 5: Vyděračeský email přisuzovaný FIN10 [23]

FIN10 během svého působení pro zveřejňování sesbíraných dat použila cloudové úložiště DropBox, webové služby pro ukládání a sdílení textu jako je například „pastebin“ a „justpasteit“ nebo se údaje objeví na torrentových službách.

Svoji snahu zůstat neodhaleni útočníci podporují i tím, že si často kompletně vymyslí záminku pro provedení útoku. FIN10 konkrétně jedné ze svých obětí

sídlící v Kanadě tvrdili, že útok je odvetou za uvalené sankce na některé odvětví průmyslu Ruské Federace. FireEye se ale vzhledem k velmi špatné kvalitě použitého Ruského jazyka (která spíše naznačovala použití internetového překladače) přiklání k tomu, že útočníci z Ruska nepocházejí.

Jak můžeme vidět na obrázku s vyděračským emailem, FIN10 se podepsali jako „TeslaTeam“ [24]. TeslaTeam jsou hackeři s potvrzenou základnou v Srbsku, kteří prováděli útoky hlavně na webové stránky Albánských vládních organizací, protisrbská média a aktivisty. FIN10 se ale zaměřuje na úplně jiné cíle, což nasvědčuje tomu, že FIN10 se jako TeslaTeam pouze snaží maskovat.

6 FIN5

Analýza[25] [26] metodologii útoků FIN5 označuje zajímavým pojmem „Honed Attack Methodology“. Význam pojmu v rámci kybernetické bezpečnosti představuje velice opatrné, dobře plánované, přesné a sofistikované vytváření a upravování malwaru a provádění útoků.

Dalším pojmem, který útočníky popisuje je „noisy“ – tedy hlučnost. Útok s touto vlastností způsobuje na systémech velké množství upozornění, varování a dalších náznaků kompromitace. To může naznačovat, že útok je veden amatéry s omezenými znalostmi a schopnostmi. Na druhou stranu tuto metodu používají i „ostřílení“ a zkušení útočníci se záměrem vystrašení a zmatení systémových správců systémů oběti. Útočníci se můžou tímto krokem například pokusit odvést pozornost správců od opravdového cíle útočníků.

Mezi nejmazavější nástroje, které FIN5 používali patří malware „RawPOS“ a upravená verze nástroje „PsExec“.

6.1 Prvotní kompromitace systému

Podle informací z analýz FIN5 se do systémy oběti dostali pomocí legitimních přihlašovacích údajů. Útočníci údaje získali kompromitací některého z dodavatelů, který s obětí spolupracuje a má legitimní přistup do sítě, například pomocí VPN. Detekce zneužití legitimních údajů je extrémně složitá i v situaci, když už správce sítě ví, že došlo k napadení systémů. Natož, když to správce netuší. Dodavatelé často velmi frekventovaně komunikují se systémy oběti, takže se ojedinělý škodlivý přístup v lozích ztratí a je jednoduše přehlédnut.

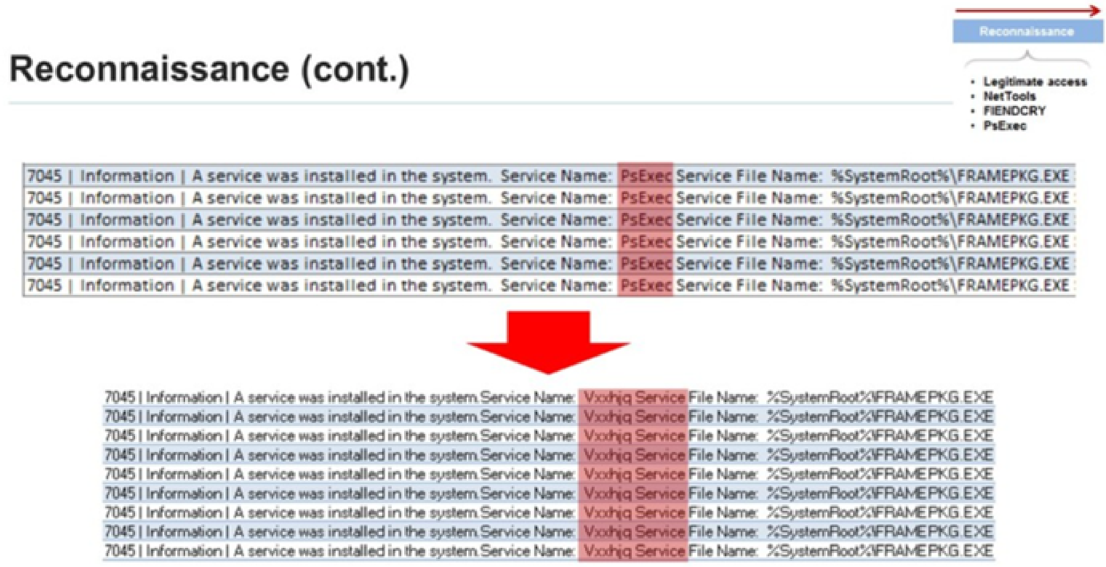
Po vytvoření pevného bodu v síti oběti útočníci použili pro skenování sítě defaultní nástroje, jako je „nmap“ a „NetTools“.

6.2 PsExec

PsExec[27] je jeden z balíčku nástrojů pro příkazovou řádku Windows. Nástroj umožňuje systémovým správcům vzdáleně zadávat příkazy a spravovat běžící procesy na ostatních zařízeních připojených ve stejné síti. Často se používá pro vzdálenou správu serverů, instalování softwaru nebo k diagnostice systémů.

FIN5 provedli úpravu nástroje, aby po instalaci přeskočil dotazy a informace ohledně podmínek EULA (End User Licence Agreement) a byly automaticky akceptovány. Zároveň byl přenastaven název služby tak, že imitoval některou z legitimních služeb. PsExec je velice užitečný nástroj, ale je také velmi známý tím, že bývá zneužíván během útoků. Například ve fázi šíření malwaru na další stanice v síti. Pokud bezpečnostní analytik uvidí v lozích nějakou zvláštní aktivitu PsExecu, ihned ho začne podezírat.

Na obrázku níže můžeme vidět část logů činnosti služeb, kdy je služba PsExec proměnlivě přejmenována a je velice těžce spatřitelná:



Obrázek 6: Originální a zamaskované logy akvitiy FIN5 [26]

6.3 Malware RawPOS

RawPOS[28] je tzv. PoS (zkratka Point-of-Sale) malware. Pojem PoS ve virtuálním světě označuje software a hardware, který je používán pro zpracovávání plateb a transakcí. Tyto systémy se běžně stávají terčem škodlivých malwarů, které se z nich snaží vytěžit údaje o použitých platebních kartách a další citlivé údaje s nimi spojené.

Malware byl poprvé detekován v roce 2008 bezpečnostními analytiky společnosti VISA. RawPOS se snažil procházet operační paměť napadených a běžících PoS systémů při platbách a vyhledával v nich údaje o použitých platebních kartách. Malware je složený ze tří částí.

První částí je vytvoření pevného bodu. Pro udržení přístupu do napadeného systému je použit backdoor pojmenovaný „FlipSide“, který útočníkům umožňuje používat RDP tunel. Backdoor se maskuje jako jedna ze služeb Windows a název

služby imituje některou z opravdových legitimních služeb, například „CertSvc“ - služba pro certifikace, „sppt32“ – služba pro podporu Windows apod. FIN5 se snaží backdoor šířit na všechny dostupné zařízení, které se v síti nachází. Během šíření vyhledává stanice, které provozují služby PoS.

Druhou částí je aktivace tzv. „memory dumperů“. Jedná se o programy, které jsou schopny vypsat stav paměti procesů napadeného systému. V případě RawPOSu byly použity dva dumpery. První generický dumper „MemPDumper“ byl používán pro získání stavu paměti konkrétního vybraného procesu. Druhý dumper nazývaný „FiendCry“ byl na míru vytvořený pro prohledávání paměti PoS softwarů.

V třetí části jsou nasazeny tzv. upravené „scrapery“. Úlohou scraperů je vytěžení už použitelných údajů z kopií paměti, které byly získány dumpery z předchozí části. Scrapery jsou v případě RawPOSu rozšířeny ještě o funkcionalitu šifrování získaných údajů.

6.4 Dokončení mise

Dle analýzy společnosti FireEye útočníci v systémech těžili data průměrně několik měsíců, přičemž nejdelší intruze trvala půl roku. Pokud došlo k rozhodnutí opustit systém oběti, FIN5 po sobě důkladně odstraní data a přepíší pevné disky. Následně zlikvidují systémovou infrastrukturu oběti. Tento radikální krok byl prováděn z toho důvodu, že kdyby po úspěšné exfiltraci dat došlo k odhalení jejich přítomnosti, forenzní analytici by byli schopni získat seznam platebních karet, které by mohly být nebo byly kompromitovány.

Nakradené údaje o platebních kartách musí útočníci ještě pomocí nelegálních praktik zpeněžit. V případě odhalení poskytovatelé platebních karet ihned podniknou kroky pro zablokování nebo znehodnocení platební karty. Tím by byly sesbírané údaje útočníků znehodnoceny. Pro FIN5 jakožto prodejce nelegálních dat je velmi důležitá pověst a renomé, kterou má u svých klientů.

7 Praktická část

Dokument s praktickou ukázkou je z důvodu obsahu neveřejný. Naleznete ho v elektronické příloze práce nahrané v systému katedry.

Závěr

Cílem práce bylo přiblížit a uvést problematiky kybernetických útoků prováděných skupinami APT a FIN. V práci jsou popsány používané metody, techniky a praktiky vybraných konkrétních skupin.

Je nutné si uvědomit, že útoky zmíněných skupin patří k těm nejnebezpečnějším a představují hrozbu zvláště pro významné a důležité cíle.

Práce sbírá informace pouze z ověřených a věrohodných zdrojů a analýz, které byly provedeny profesionálními institucemi zaměřenými na kybernetickou bezpečnost.

Conclusions

The purpose of the Diploma thesis is to introduce and explain the problematics of cybernetic attacks conducted by APT and FIN groups. Thesis describes used techniques, practices and methods used by the attackers.

It is important to realize that the APT and FIN attacks are one of the most dangerous a pose greath threat especially to important and critical facilities.

Diploma thesis uses data only from verified and trustworthy sources and public analyses, that were conducted by professional institutes focused on cybernetic security.

A Obsah elektronických dat

`text/`
: Adresář s dokumentem obsahující diplomovou práci ve formátu PDF a zdrojový kód dokumentu diplomové práce včetně potřebných příloh ve formátu .zip.

`praktická-cast/`
: Adresář obsahuje .pdf dokument s textem praktické části práce.

`Readme.txt`
: Soubor s odkazy pro stažení čistých obrazů virtuálních strojů používaných při demonstraci. Obrazy nejsou fyzicky přiloženy z důvodu jejich velikosti, která se pohybuje v rozsahu dvou desítek gigabytů.

`install/`
: Adresář obsahuje instalátor Virtualboxu, archiv se soubory potřebnými k instalaci frameworku používaného při demonstraci.

Literatura

[1] *Mitre Att&ck*. Dostupný z: ⟨https://attack.mitre.org/⟩.

[2] *Mitre Att&ck APT15*. Dostupný z: ⟨https://attack.mitre.org/groups/G0004/⟩.

[3] *Operation "Ke3chang"*. Dostupný z: ⟨https://www.mandiant.com/resources/reports/operation-ke3chang-targeted-attacks-against-ministries-foreign-affairs⟩.

[4] FireEye. *OPERATION "KE3CHANG": Targeted Attacks Against Ministries of Foreign Affairs*. Dostupný z: ⟨https://www.mandiant.com/sites/default/files/2021-09/wp-operation-ke3chang.pdf⟩.

[5] Group, NCC. *APT15 expands its arsenal*. Dostupný z: ⟨https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/⟩.

[6] Hromcová, Zuzana. *OKRUM AND KETRICAN: AN OVERVIEW OF RECENT KE3CHANG GROUP ACTIVITY*. Dostupný z: ⟨https://www.welivesecurity.com/wp-content/uploads/2019/07/ESET_Okrum_and_Ketrican.pdf⟩.

[7] *Steganografie, Wikipedia*. Dostupný z: ⟨https://cs.wikipedia.org/wiki/Steganografie⟩.

[8] *APT28 Mitre*. Dostupný z: ⟨https://attack.mitre.org/groups/G0007/⟩.

[9] *APT29 Mitre*. Dostupný z: ⟨https://attack.mitre.org/groups/G0016/⟩.

[10] *Democratic National Committee cyber attacks*. Dostupný z: ⟨https://en.wikipedia.org/wiki/Democratic_National_Committee_cyber_attacks⟩.

[11] *Secureworks, Threat Group 4127 Targets Hillary Clinton Presidential Campaign*. Dostupný z: ⟨https://www.secureworks.com/research/threat-group-4127-targets-hillary-clinton-presidential-campaign⟩.

[12] *CrowdStrike's work with the Democratic National Committee: Setting the record straight*. Dostupný z: ⟨https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/⟩.

[13] *En Route with Sednit*. Dostupný z: ⟨https://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part-2.pdf⟩.

[14] *SUNBURST backdoor malware: What it is, how it works, and how to prevent it | Malware spotlight*. Dostupný z: ⟨https://resources.infosecinstitute.com/topic/sunburst-backdoor-malware-what-it-is-how-it-works-and-how-to-prevent-it-malware-spotlight/⟩.

[15] *SUNBURST Additional Technical Details*. Dostupný z: ⟨https://www.mandiant.com/resources/blog/sunburst-additional-technical-details⟩.

[16] *SolarWinds SUNBURST Backdoor: Inside the Stealthy APT Campaign*. Dostupný z: ⟨https://www.varonis.com/blog/solarwinds-sunburst-backdoor-inside-the-stealthy-apt-campaign⟩.

[17] *SolarWinds SUNBURST Backdoor DGA And Infected Domain Analysis*. Dostupný z: ⟨https://cybersecurityventures.com/solarwinds-sunburst-backdoor-dga-and-infected-domain-analysis/⟩.

[18] *FIN10 Anatomy of a Cyber Extortion Operation*. Dostupný z: ⟨https://www.mandiant.com/sites/default/files/2021-09/rpt-fin10-2.pdf⟩.

[19] *FIN10 Mitre*. Dostupný z: ⟨https://attack.mitre.org/groups/G0051/⟩.

[20] *Metasploit - The world's most used penetration testing framework*. Dostupný z: ⟨https://www.metasploit.com/⟩.

[21] *Empire: A Powerful Post-Exploitation Tool*. Dostupný z: ⟨https://www.ciso.inc/blog-posts/empire-powerful-post-exploitation-tool/⟩.

[22] *SplinterRAT*. Dostupný z: ⟨https://github.com/javiarago1/SplinterRAT⟩.

[23] *FIN10: Anatomy of a Cyber Extortion Operation*. Dostupný z: ⟨https://www.mandiant.com/resources/reports/fin10-anatomy-cyber-extortion-operation⟩.

[24] *TeslaTeam*. Dostupný z: ⟨https://en.wikipedia.org/wiki/TeslaTeam⟩.

[25] *Attacking the Hospitality and Gaming Industries Tracking an Attacker Around the World in 7 Years*. Dostupný z: ⟨https://www.youtube.com/watch?v=fevGZs0EQu8&ab_channel=AdrianCrenshaw⟩.

[26] *Attacking the Hospitality and Gaming Industries Tracking an Attacker Around the World in 7 Years*. Dostupný z: ⟨https://speakerdeck.com/bromiley/attacking-the-hospitality-and-gaming-industries-tracking-an-attacker-around-the-world-in-7-years⟩.

[27] *Lateral Movement with PSExec*. Dostupný z: ⟨https://www.mindpointgroup.com/blog/lateral-movement-with-psexec⟩.

[28] *RawPOS Technical Brief*. Dostupný z: ⟨http://sjc1-te-ftp.trendmicro.com/images/tex/pdf/RawPOS%5C%20Technical%5C%20Brief.pdf⟩.

[29] *Kali Linux*. Dostupný z: ⟨https://www.kali.org/⟩.

[30] *Trellix*. Dostupný z: ⟨https://www.trellix.com/⟩.