Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

3953/2020-NÚKIB-E/310 • BRNO • 7. SRPNA 2020

ANALÝZA HROZBY

VYDĚRAČSKÉ ÚTOKY RANSOMWAREM JSOU CÍLENĚJŠÍ: MÍŘÍ NA VELKÉ FIRMY, STÁTNÍ A VEŘEJNÉ INSTITUCE

SHRNUTÍ

- **Ransomwarový útok je vždy závažný a může kromě dostupnosti dat narušit i jejich integritu a důvěrnost. Ransomware může zcela paralyzovat podniky, ale i veřejné a státní instituce či obce. Lákavým a častým cílem je především zdravotnictví a samospráva.**
- **Česká republika se stala obětí několika útoků s významnými dopady. Za poslední dva roky byly nejvýznamnější útoky vedeny vůči těžební společnosti OKD a dvěma zdravotnickým zařízením (Nemocnici Rudolfa a Stefanie v Benešově a Fakultní nemocnici Brno). Je pravděpodobné (55-70 %), že na území ČR dojde během následujícího roku k dalším významným útokům. Globální trendy ransomwarových útoků identifikují jako nejohroženější sektory zdravotnictví, energetický sektor, samospráva, doprava, automobilový průmysl a akademický sektor.**
- **DOPORUČENÍ: Nejefektivnější ochranou před ransomwarem jsou preventivní opatření. Jedná se především o segmentaci sítí, vzdělávání zaměstnanců v rozpoznávání phishingu, aktualizování softwaru a vypnutí maker v nástrojích Office. Pro případ, že prevence nebude úspěšná, lze omezit škody udržováním oddělených a aktuálních záloh, ze kterých lze obnovit chod systému. Platit výkupné NÚKIB výrazně nedoporučuje.**

ZÁKLADNÍ FAKTA

Cíl	Primárně velké firmy a obecní nebo státní instituce, v menší míře běžní uživatelé.
Útočník / atribuce	Nestátní kyberkriminální skupiny motivované ziskem. Výjimku tvoří KLDR a ruští aktéři.
Metody útoku	Exploit kity, phishing a metody sociálního inženýrství. Následně omezení přístupu k souborům a požadování výkupného za jejich zpřístupnění.
Způsobená škoda	Částečná nebo úplná paralýza zasažené organizace.

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

Ransomware v horizontu posledních tří let cíleně útočí na velké společnosti, na veřejné i státní instituce, samosprávy, zdravotnická zařízení nebo univerzity. Tyto organizace jsou pod větším tlakem zaplatit výkupné, jelikož se výpadek jejich služeb citelně dotkne velkého množství lidí. Tento typ útoků již zasáhl i Českou republiku. Obzvlášť české zdravotnictví zaznamenává zvýšený výskyt těchto útoků.

GLOBÁLNÍ TREND: CÍLEM JSOU VELKÉ FIRMY A STÁTNÍ NEBO VEŘEJNÉ INSTITUCE

V současnosti lze sledovat změny trendů na poli ransomwaru, konkrétně v jeho zacílení. Po většinu času existence ransomwaru byly jeho primárními oběťmi jednotliví soukromí uživatelé, nebo náhodné společnosti. V posledních letech lze ale sledovat v této oblasti posun, a ransomware nyní cíleně útočí na konkrétní firmy, podniky a organizace.

V posledním čtvrtletí 2018 však podle informací společnosti Malwarebytes vzrostlo množství zasažených podniků a firem o téměř 400 %[1] a v roce 2019 tento trend dále pokračoval. V roce 2020 pak ještě posílil skrze pandemii COVID-19, kdy se zvýšilo množství útoků na zdravotnická zařízení jak globálně[2], tak i v ČR.[3]

K tomu jsou dva hlavní důvody. Prvním je fakt, že firmy nebo veřejné instituce jsou svými zákazníky

nebo veřejností tlačeny k co nejrychlejšímu obnovení služeb. V případě, že se ransomwaru podaří paralyzovat obchodní společnost zašifrováním dat klíčových pro její provoz, s každým dnem, kdy není schopná plnit své zakázky, přichází o zisk. V případě dopravní infrastruktury jako letišť, přístavů a vlakových nádraží pak kromě ušlého zisku zasažená organizace čelí i hněvu zákazníků a poškození reputace. V případě státních nebo městských institucí oběť útoku v důsledku nedostupnosti služeb naráží na negativní reakci veřejnosti, a v případě zdravotních zařízení může paralyzování služeb vést k ohrožení zdraví či ztrátách na životech. Druhým faktorem je, že tyto subjekty zpravidla disponují vyššími finančními prostředky. V kombinaci s tlakem na obnovení služeb a zachování svého dobrého jména se tak leckdy oběti z řad firem a státních organizací podvolí a zaplatí požadovanou sumu.

Trend v cílení útoků na velké firmy a instituce dále sílí a je velmi pravděpodobné, že bude pokračovat i v horizontu alespoň dalších tří let.

BOX 1: Co je ransomware?

Ransomware je druhem škodlivého softwaru (malware) který bere zasažený systém a data jako rukojmí („ransom“ – anglicky výkupné). Ransomware je zpravidla nástrojem nestátních kyberkriminálních skupin motivovaných ziskem. Znepřístupní data a vyžaduje platbu v kryptoměnách za jejich odblokování.

KONCOVÝ UŽIVATEL NEJSLABŠÍM ČLÁNKEM, NEJČASTĚJŠÍM CÍLEM JE OS WINDOWS

Ačkoliv ransomware může z principu existovat na jakékoliv platformě, dominantní postavení mají formy namířené na počítače s operačním systémem Microsoft Windows. Druhou kategorií jsou mobilní zařízení s operačním systémem Android. Ačkoliv zde není ransomware rozšířen tolik jako na počítačích s Windows, vyskytlo se zde několik významných případů[4] a jejich množství bude pravděpodobně dál narůstat vzhledem k popularitě platformy (Android má více než 85% podíl na trhu s chytrými telefony).[5]

Nejčastějšími vektory, kterými ransomware nakazí zařízení, jsou (primárně u Windows) phishingové e-maily a tzv. „exploit kits“. Phishingový e-mail se oběť snaží přesvědčit, že se jedná o legitimní komunikaci od společnosti nebo organizace. Ve variantě spearphishing se jedná o zprávu, která je přímo adresována oběti. Účel je ovšem stejný: přesvědčit oběť, aby klikla na škodlivý odkaz, nebo aby stáhla a spustila nakaženou přílohu. Tak dojde k infekci zařízení a následnému uzamčení přístupu nebo dat.

Příloha může mít formu spustitelného [.]exe souboru, ale v poslední době jsou populární především soubory z kancelářské sady Microsoft Office, které zneužívají funkce makro. Tato funkce umožnuje útočníkovi naprogramovat škodlivý kód přímo do souboru Office. Z pravidla se jedná o tzv. „downloader“ skript, který po spuštění na pozadí stáhne samotný malware. Funkci makro musí uživatel zpravidla nejprve povolit, proto se dokument snaží potenciální oběť přesvědčit, že nemá aktuální program sady Office a že pro přístup k obsahu dokumentu musí tento obsah spustit.

Exploit kits jsou pak sofistikované nástroje, které zneužívají konkrétní zranitelnosti internetových prohlížečů. Spustí se, když oběť navštíví škodlivou stránku (může se ale jednat i o škodlivou reklamu na jinak legitimní stránce, tzv. malvertisement). Pokud má oběť ve svém systému zranitelnost, na kterou exploit kit cílí, ransomware se bez vědomí uživatele může stáhnout do jeho systému.

V případě mobilního ransomwaru na systému Android se nejvíce prosazují falešné aplikace. Ty jsou ve skutečnosti ransomware, ale tváří se jako legitimní aplikace, a snaží se tak oběť přimět k instalaci.

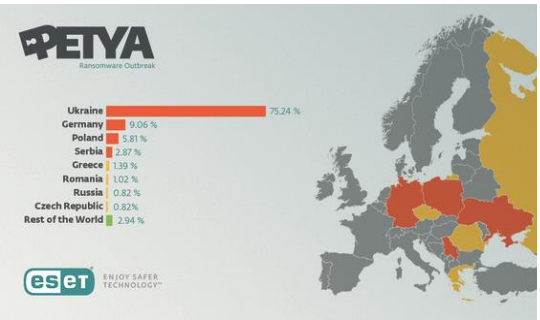
Obrázek 1: Android ransomware zamaskovaný jako aplikace pro aktualizaci systému

Zdroj: WP.com

NÁSTROJ K OBOHACENÍ KYBER KRIMINÁLNÍCH SKUPIN

U ransomwarových útoků většinou absentuje vazba na státní aktéry a širší politickou agendu. Ačkoliv autory a operátory ransomwaru je velmi těžké dopadnout a usvědčit, jejich modus operandi výrazně nasvědčuje faktu, že se většinou jedná o soukromé kyberkriminální

Obrázek 2: Šíření ransomwaru Petya, který disproporčně cílil na Ukrajinu



Zdroj: eset.com

aktéry, jejichž primárním cílem je zisk. Své oběti si vybírají buďto náhodně, nebo na základě potenciální výnosnosti. Projevem této mentality je pak specifický model RaaS („Ransomware as a Service" – ransomware jako služba). V tomto modelu pronajímají autoři ransomwaru svůj produkt zájemcům o kyberkriminální aktivity, kteří sami nemají dostatečné know-how na tvorbu sofistikovaného malwaru. Platba pak probíhá ve formě podílu na zisku z vybraných výkupných. Nejznámějším RaaS byl GandCrab, který ukončil svou činnost v roce 2019.[6]

Ačkoliv je většina ransomwarových útoků motivována ziskem, existují výjimky. Pověst ransomwaru jakožto nástroje finančního obohacení může totiž sloužit jako krytí jinak motivovaného útoku. Příkladem může být ransomwarová kampaň Petya, která cílila primárně na Ukrajinu (viz obrázek 3), u které existuje reálná možnost (25-50 %) že byla vytvořena ruskými APT (z anglického termínu Advanced Persistent Threat) skupinami. Následná kampaň wiperu NotPetya, který se snažil působit jako ransomware Petya, ale cíleně ničil data, byla přiřazena ruským APT skupinám Bílým domem[7] nebo britskou NCSC.[8] Specifickým hráčem na poli ransomwaru (a kyberkriminality obecně) je Severní Korea, která stála za jednou z největších ransomwarových kampaní v poslední době. Přestože je KLDR státním aktérem, v kyberprostoru se chová z velké části jako kyberkriminální subjekt. Severní Koreji atribuovaná skupina Lazarus stála za masivně rozšířeným ransomwarem WannaCry[9] a stejná skupina je obviňována i z dalších finančně motivovaných útoků.[10] Důvodem je primárně ekonomická situace KLDR. Kyberkriminalita dokáže pro KLDR generovat významné a těžko sledovatelné příjmy, které může využít i pro svůj jaderný program.[11]

DATA JSOU KOMPROMITOVÁNA NA VŠECH ÚROVNÍCH

Kyberbezpečnost lze vnímat jakou souhru tří faktorů: zda jsou data přístupná (dostupnost), zda s nimi nebylo manipulováno (integrita) a zda nebyla zpřístupněna někomu, kdo by neměl znát jejich obsah (důvěrnost). **Tento koncept představuje triádu kybernetické bezpečnosti** (viz obrázek 3). **Ransomware cílí primárně na dostupnost dat. Jejich zašifrováním se data stanou nedostupná.** Ransomware používá silné šifrování s unikátními klíči, které je téměř nemožné prolomit. U některých forem ransomwaru se časem podaří vytvořit tzv. decryptor, tedy nástroj, který data rozšifruje. Takovéto nástroje ale mohou vzniknout až roky po útoku, nemusí být stoprocentně spolehlivé a v některých případech nemusí vzniknout vůbec.

I v případě úspěšného rozšifrování dat (jak decryptorem, nebo i zaplacením výkupného) **je ovšem třeba mít na paměti, že úspěšný ransomwarový útok kompromituje data na všech úrovních triády**. Aby ransomware mohl zašifrovat data, musí k nim získat přístup, a může narušit jak jejich **integritu**[12] (tedy pozměnit jejich obsah), tak i **důvěrnost**. V současnosti vzniká na poli ransomwaru trend, kdy útočník kromě zašifrování data i exfiltruje a hrozí, že pokud nedojde k zaplacení výkupného, budou zveřejněna[13] (např. ransomware Maze). I v případě, kdy oběť zaplatí, neexistuje žádná záruka, že útočník data nezveřejní, nebo neprodá, čímž by byla narušena také jejich **důvěrnost**. **Je výrazně doporučováno výkupné neplatit** (viz box 2).

Obrázek 3: Triáda kybernetické bezpečnosti

Zdroj: NÚKIB

Dopady a škody ransomwarového útoku se odvíjejí od typu zasaženého subjektu, povahy zasažených dat a opatření, která dotyčný postižený subjekt přijal (viz níže doporučení). Vždy se však jedná o závažný incident. Ransomware může znepřístupnit jak data z informačních databází, tak soubory potřebné

k provozu konkrétních zařízení. Ransomwarový útok navíc vždy znamená nutnost přeinstalovat veškerá napadená zařízení. **I v případě zaplacení výkupného a rozšifrování totiž nedojde k odstranění samotného škodlivého kódu, který může mít další podružné funkce.**

V situaci, kdy je napadena firma, může být zastaven její provoz jak skrze administrativní části infrastruktury a sítí, tak ty, které řídí výrobní část. Společnost tak může přijít o významné finanční příjmy. Pokud útočník navíc data zveřejní nebo prodá, může firma ztratit cenná obchodní tajemství, případně utrpět reputační škody. V případě veřejných a státních organizací mohou být přerušeny klíčové služby občanům jako například zdravotní péče. Zde může dojít k zašifrování zdravotních dat pacientů, která jsou klíčová pro jejich péči, a stejně tak mohou být z provozu vyřazena klíčová pracoviště jako rentgeny, magnetické rezonance nebo laboratorní vybavení. Útočník může následně zveřejnit nebo prodat vysoce citlivá osobní data pacientů.

BOX 2: Proč neplatit výkupné

V případě napadení ransomwarem jsou subjekty vystaveny silnému tlaku veřejnosti. Postižené organizace proto mohou být nakloněny zaplacení výkupného. I přes možné ohrožení zdraví a životů se ovšem světová bezpečnostní komunita shoduje, že by výkupné nemělo být za žádných okolností placeno:

1) **Zaplacení utvrdí útočníka v ziskovosti jeho jednání a motivuje jej k dalším útokům;**
2) **Neexistuje záruka, že útočník data skutečně odblokuje;**
3) **Odblokování dat neodstraní samotný ransomware ani další potenciální malware;**
4) **Z právního hlediska může představovat zaplacení výkupného porušení zásad péče řádného hospodáře.**

IMPLIKACE PRO ČR

Doposud nejzávažnější ransomwarové útoky v ČR se udály na konci roku 2019 a v prvním čtvrtletí roku 2020, kdy se v ČR staly tři prominentní incidenty. Konkrétně se jednalo o útoky na nemocnici v Benešově, Fakultní nemocnici Brno a na těžební společnost OKD. Další menší útoky postihly zdravotnická zařízení jako například psychiatrickou léčebnu Kosmonosy.

Nelze s jistotou určit, ke kolika takovým případům v Česku ročně dochází. **Ransomwarové útoky jsou ze své podstaty nadnárodní, tj. útočníci zpravidla nevybírají své potenciální oběti na základě státní příslušnosti**. Z dostupných dat je zřejmé, že Česká republika je subjektem stejných trendů jako globální ransomwarová scéna, ve které se cílem stávají velké organizace. Stejně jako v globálním měřítku ukazuje i zamíření útoků v Česku, že jednou z nejvíce ohrožených oblastí je zdravotnictví. To představuje lákavý cíl skrze svou snadnou vydíratelnost a v první polovině roku 2020 je ještě více ohroženo v souvislosti s pandemií COVID-19. Je pravděpodobné (55-70 %), že se ČR dalším podobným útokům v horizontu následujícího roku nevyhne. **ČR se proto musí připravovat na útoky vedené proti zdravotnictví a dalším státním anebo obecním organizacím. V ohrožení je rovněž akademický sektor a velké významné podniky.** Útok na společnost Honda poukázal **na zranitelnost automobilového průmyslu[14], který tvoří klíčový pilíř české ekonomiky (téměř 10% HDP[15]). Ohroženy můžou být ale i energetické společnosti, pošta, nebo dopravní infrastruktura (železnice, letiště, atd.)**

Příprava na možný útok musí probíhat jak v rámci příprav na nápravu škod, tak především na úrovni prevence. Přestože se někdy může jednat o nákladné investice do personálu, vybavení a materiálu, jde o menší náklady než potenciální škody. Část rizik je možné eliminovat dodržováním zásad kybernetické bezpečnosti (viz přílohy). Ačkoliv útok i tak nebude možné vyloučit (25-50 %), dodržování těchto doporučení riziko zmírní.

DOPORUČENÍ

Organizace a firmy, bez ohledu na to, zda spadají pod zákon o kybernetické bezpečnosti, či nikoliv, by měly důsledně dodržovat obecné zásady kybernetické bezpečnosti. Využít mohou základní bezpečnostní doporučení pro správce (příloha 2), minimální bezpečnostní standard nebo vyhlášku o kybernetické bezpečnosti. Stejně tak by měly mít připravené plány komunikace v případě incidentu (viz příloha 4).

- **Mezi konkrétní základní opatření se řadí pravidelné aktualizace softwaru i hardwaru, segmentace sítě, tvorba záloh, důsledně oddělená administrátorská práva, a využívání antivirové ochrany.**

- **Účinným opatřením jsou rovněž školení zaměstnanců v rozpoznávání phishingu a namátkové testy, které zvýší jejich pozornost. Je dobré rovněž mít krizové plány jak na útok reagovat.**

V případě, že jsou systémy i přes veškerá přijatá opatření nakaženy ransomwarem, je řešením obnovení systému ze záloh. K tomu je třeba preventivně zřídit a udržovat aktuální a oddělené zálohy (jak online tak offline), ze kterých je možné provoz následně obnovit. Důležitá je i příprava krizových plánů, jak v takové situaci postupovat. Je dobré mít připravené i postupy, jak alespoň částečně obnovit služby bez informačních systémů. V případě úspěšného útoku je však integrita a důvěrnost dat nenávratně narušena a vždy je potřeba nákladně reinstalovat veškeré napadené systémy, aby byl ransomware odstraněn, bez ohledu na efektivitu záloh.

- **Napadený subjekt by měl v případě ransomwarového útoku či pouze pokusu o něj zvážit ohlášení útoku národnímu či vládnímu CERT[16] a Policii ČR, a to i s ohledem na možnou existenci ohlašovací povinnosti dle zákona o kybernetické bezpečnosti či oznamovací povinnosti dle trestně právních předpisů.**

Je dobré se vyvarovat používání softwaru, který už vydavatel nepodporuje, záplatami. Například operační systém Windows XP a nově i Windows 7 již nemají oficiální podporu výrobce (i když je možné ji ještě dočasně dokoupit).

- **V případě, že je aktualizování příliš nákladné, nebo neexistuje alternativa, je řešením segmentace sítě – oddělení rizikového zařízení od zbytku sítě.**

Koncoví uživatelé by měli dbát zvýšené pozornosti na podezřelé odkazy a přílohy v e-mailech. Primárně by se měli vyvarovat spustitelným souborům, ale neměli by podcenit ani jakýkoliv jiný typ. Specifické riziko tvoří přílohy souborů sady Office se spustitelným škodlivým kódem vepsaným pomocí funkce makro.

- **Makro je pokročilá funkce, kterou většina běžných uživatelů při práci s MS Office vůbec nevyužije. Administrátoři dané organizace by měli zvážit, zda její zaměstnanci ke své práci tuto funkci potřebují, a eventuálně ji plošně zakázat, nebo ji případně povolit jen určitým zaměstnancům.**

PŘÍLOHA 1: NEJČASTĚJŠÍ TYPY RANSOMWARU

Ransomware může být ze své podstaty jakýkoliv software, který uživatele vydírá. Existuje několik jeho rozšířených variant.

Obrázek 4: Scareware snažící se oběť přimět koupit „plnou verzi“ antivirového softwaru

Zdroj: bp.blogspot.com

Nejméně závažnou formou je tzv. „scareware“[17] („scare“ – vyděsit) snažící se uživatele přesvědčit, že na jeho zařízení byl nalezen fatální problém, jehož opravení vyžaduje platbu. Tento škodlivý kód se obvykle snaží působit jako legitimní antivirový software. Scareware většinou aktivně nepoškodí zařízení nebo data uživatele, ale funguje pouze na principu psychologického nátlaku, podobně jako tzv. sextortion e-maily (viz níže).

Druhou rozšířenou formou jsou tzv. „screenlockers“ („zamykače obrazovky“).[18] Ty blokují možnost uživatele dostat se do svého zařízení, dokud nezaplatí patřičnou částku. Screenlockers rovněž leckdy aplikují formy psychologického nátlaku, jelikož často působí jako nástroj legitimní instituce (například policie), která uzamkla uživateli počítač z důvodu nelegální činnosti.

Obrázek 5: Screenlocker zneužívající logo FBI

Zdroj: managenegine.com

Obrázek 6: Vzkaz o zašifrování dat a platbě za dešifrování filecoderu WannaCry

Zdroj: HKcert.com

Zdaleka nejrozšířenější (až 90 %) formou ransomware jsou ale tzv. filecoders („šifrovače souborů“).[19] Ty zašifrují data v počítači a vyžadují platbu za jejich dešifrování. Vzhledem k pokročilým metodám šifrování, jež některé z filecoderů používají, je prakticky nemožné data obnovit jinak než ze strany útočníka. Z tohoto důvodu jsou šifrovače souborů velmi účinné.[20] Odstraněním samotného ransomwaru navíc nedojde k dešifrování dat.

Ačkoliv se nejedná přímo o ransomware, příbuznou hrozbou k scareware jsou vyděračské e-maily, tzv. sextortion. Oběť obdrží zprávu, že její počítač byl zasažen malwarem, který ji natočil přes kameru zařízení při sledování pornografických materiálů a požaduje výkupné za nezveřejnění těchto záběrů. Tyto emaily nebyly nikdy spojeny s reálným případem proniknutí do webkamery, ale využívaly sofistikované psychologické metody, aby přidaly na své legitimitě, jako například iluze, že dotyčný e-mail přišel z uživatelovy vlastní schránky.

Obrázek 7: Příklad sextortion zprávy


Ahoj, drahý uživatel
Do vašeho přístroje jsme nainstalovali jeden software RAT.
Pro tento okamžik je váš emailový účet napaden (viz , nyní mám přístup k vašim účtům)..
Stahoval jsem všechny důvěrné informace z vašeho systému a dostal jsem další důkazy.
Nejzajímavějším okamžikem, který jsem objevil, jsou videozáznamy o vás masturbující.

Zveřejnil jsem virus na pornografickém webu, a pak jste jej nainstalovali do svého operačního systému.
Po klepnutí na tlačítko Přehrát na porno video, v tom okamžiku byl můj trojan stažen do vašeho zařízení.
Po instalaci vám přední fotoaparát natáčí video pokaždé, když masturbujete, software se synchronizuje s vybraným videem.

Prozatím software získal všechny vaše kontaktní informace ze sociálních sítí a e-mailových adres.
Pokud potřebujete smazat všechny shromážděné údaje, pošlete mi $250 v BTC (krypto měně).

Toto je moje Bitcoin peněženka: 1GL9JtXPRTPetxgiJ8UcgrEECp12spD4tt
Máte 48 hodin po přečtení tohoto dopisu.

Po transakci vymažu všechna data.

Zdroj: novinky.cz

PŘÍLOHA 2:

TLP: WHITE

BEZPEČNOSTNÍ DOPORUČENÍ NÚKIB PRO ADMINISTRÁTORY 4.0

INFRASTRUKTURA

ČLEŇTE SÍŤ NA MENŠÍ CELKY (SEGMENTACE) A STRIKTNĚ ODDĚLUJTE UŽIVATELSKÁ PRÁVA NAPŘÍČ UŽIVATELI (SEGREGACE)
s cílem oddělit citlivé informace a kritické služby typu autentizace uživatelů (např. Microsoft Active Directory) a vytvořit zóny s různou úrovní bezpečnostních omezení.

BLOKUJTE ŠKODLIVÉ IP ADRESY A DOMÉNY NA ÚROVNI GATEWAY (BLACKLISTY).

NASAĎTE SÍŤOVÉ SYSTÉMY DETEKCE / PREVENCE PRŮNIKU (IDS/IPS)
používající signatury a heuristiky k identifikaci anomálního provozu v rámci sítě i překračujícího perimetr.

SLEDUJTE SÍŤOVÝ PROVOZ
pomocí vybraných síťových prvků nebo rozmístěním dedikovaných síťových sond. Sledujte komunikaci mezi klienty a servery, komunikaci klientů do internetu, komunikaci mezi servery i provoz na perimetru sítě a identifikujte provozní a bezpečnostní problémy.

UCHOVÁVEJTE SÍŤOVÝ PROVOZ
z/do kritických pracovních stanic a serverů a provoz překračující perimetr sítě pro případné forenzní zkoumání po průniku do sítě a systémů. Záznamy síťového provozu doporučujeme uchovávat po dobu minimálně 12 měsíců, více podle místních okolností a významu sítě – v případě kritické informační infrastruktury (KII) a u informačních systémů základní služby (PZS) podle zákona o kybernetické bezpečnosti a návazných vyhlášek je minimální lhůta 18 měsíců. V případě sítí strategického významu zvažte i možnost automaticky aktivovaného plného záznamu datového provozu (PCAP), a to jak na primárních, tak záložních systémech (např. webových nebo systémových serverech).

KONTROLUJTE PŘÍCHOZÍ E-MAILY
pomocí mechanismů Sender ID, SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) a DMARC (Domain-based Message Authentication, Reporting and Conformance) a blokujte podvržené zprávy. Tyto mechanismy nastavte i pro možnou kontrolu odchozích zpráv druhou stranou.

POUŽÍVEJTE ŠIFROVANÉ SPOJENÍ MEZI POŠTOVNÍMI SERVERY (TLS)
pro zajištění důvěrnosti e-mailové komunikace, v ideálních případě použijte DANE (DNS-based Authentication of Named Entities). Kontrolu obsahu provádějte až poté, co je e-mailový provoz dešifrován.

PROVÁDĚJTE AUTOMATIZOVANOU DYNAMICKOU ANALÝZU OBSAHU E-MAILŮ A WEBŮ
prováděnou v sandboxu – hledejte podezřelé chování podle síťového provozu, tvorby nových souborů, úpravy stávajících souborů nebo změn konfigurace.

POVOLTE NA FIREWALLU POUZE ŽÁDOUCÍ SLUŽBY A STANDARDNÍ PROVOZ.
V případě koncových stanic nezapomeňte také blokovat spojení z Vámi nekontrolované sítě.

KONTROLUJTE POUŽÍVANÉ KLÍČE/CERTIFIKÁTY
především pro SSH autentizaci, webové servery, vzdálenou plochu apod. Kde je to možné, použijte šifrovanou komunikaci.

ZAJISTĚTE CENTRALIZOVANÉ A ČASOVĚ SYNCHRONIZOVANÉ LOGOVÁNÍ SÍŤOVÝCH UDÁLOSTÍ
(povolených a blokovaných) s okamžitým automatickým vyhodnocováním a uložením po dobu minimálně 18 měsíců, více podle místních okolností a významu sítě.

APLIKUJTE WHITELISTING WEBOVÝCH DOMÉN
pro všechny domény – pokud to dovoluje charakter práce uživatelů. Tento přístup je účinnější než blacklistovat malé procento škodlivých domén.

VOLTE JEDNODUCHÉ DOMÉNOVÉ NÁZVY,
aby byly jasně viditelné případné záměny písmen ve phishingových e-mailech.

NASAĎTE ANTI-DDoS TECHNOLOGIE,
které můžete po důkladné úvodní analýze řešit buď vlastními silami, nebo ve spolupráci s poskytovatelem internetového připojení. Anti DDoS ochranu nasaďte na kompletní IP rozsahy vaší organizace.

VYPRACUJTE DISASTER RECOVERY PLAN (DRP)
a mějte připravené správné a funkční emailové adresy a telefonní čísla na ostatní administrátory, nadřízené pracovníky a CERT/CSIRT týmy.

STANICE A SERVERY

UDRŽUJTE AKTUÁLNÍ OPERAČNÍ SYSTÉM
pravidelnými aktualizacemi a v co nejkratší době aplikujte všechny vydané bezpečnostní záplaty.

UDRŽUJTE AKTUÁLNÍ SOFTWARE,
pravidelně kontrolujte verze instalovaného softwaru. U neaktuálního softwaru proveďte v rámci možností update. Zastaralé mohou být i verze použitých doplňků či modulů nebo firmware zařízení.

NEPOUŽÍVEJTE NEPODPOROVANÉ PRODUKTY,
používejte pouze produkty (software i operační systémy), pro které jsou dostupné bezpečnostní záplaty.

OVĚŘUJTE IDENTITU APLIKACÍ A SOUBORŮ
a povolte jen ty důvěryhodné včetně skriptů a DLL knihoven. V prostředí Windows použijte Device Guard, AppLocker, popřípadě Zásady omezení softwaru (SRP).

PROVÁDĚJTE HARDENING KONFIGURACE UŽIVATELSKÝCH APLIKACÍ
– povolte jen funkcionalitu, která je vyžadována pro práci uživatelů. Dodatečné funkce (např. Java a Flash ve webovém prohlížeči, makra v MS Office) povolte pouze, je-li to nutné.
POUŽÍVEJTE OBECNÉ PREVENTIVNÍ MECHANISMY, které mohou pomoci ochránit systém před zero-day zranitelnostmi, jako např. DEP (Data Execution Prevention) nebo SELinux v linuxových systémech.

AKTIVUJTE IDS/IPS SYSTÉMY NA KONCOVÝCH STANICÍCH
detekující anomální chování jako např. injekci kódu do jiných procesů, změnu chráněných registrových klíčů, zachytávání stisků kláves, načítání neznámých ovladačů, snahu o zajištění perzistence a další.

ZAJISTĚTE CENTRALIZOVANÉ A ČASOVĚ SYNCHRONIZOVANÉ LOGOVÁNÍ SÍŤOVÝCH UDÁLOSTÍ
(povolených a blokovaných) s okamžitým automatickým vyhodnocováním a uložením pro kritickou informační infrastrukturu (KII) a provozovatele základní služby (PZS) po dobu minimálně 18 měsíců, pro významné informační systémy (VIS) po dobu minimálně 12 měsíců a pro ostatní systémy podle místních okolností a významu sítě.

FILTRUJTE OBSAH E-MAILŮ A PROPOUŠTĚJTE POUZE RELEVANTNÍ DRUHY PŘÍLOH
– po důkladné analýze chování uživatelů určete typy souborů, které potřebují posílat e-mailem. Ostatní formáty příloh blokujte – především spustitelný kód. Dále ověřujte soulad přípony souboru a jeho skutečného formátu.

PRAVIDELNĚ ZÁLOHUJTE DŮLEŽITÁ A CITLIVÁ DATA
jako např. obsah webového serveru, databází nebo konfiguraci služeb. Zálohu umístěte do odděleného prostředí mimo produkční síť. Pravidelně testujte, jestli dokážete data obnovit a jestli jsou data po obnově funkční.

ZAVEĎTE STANDARD OPERATING ENVIRONMENT (SOE)
se standardizovanou konfigurací pro pracovní stanice i servery, kde budou vypnuty všechny nevyžádané funkcionality.

PRAVIDELNĚ ZÁLOHUJTE DŮLEŽITÁ A CITLIVÁ DATA
jako např. obsah webového serveru, databází nebo konfiguraci služeb. Zálohu umístěte do odděleného prostředí mimo produkční síť. Pravidelně testujte, jestli dokážete data obnovit a jestli jsou data po obnově funkční.

ZAVEĎTE STANDARD OPERATING ENVIRONMENT (SOE)
se standardizovanou konfigurací pro pracovní stanice i servery, kde budou vypnuty všechny nevyžádané funkcionality.

ZAMEZTE PŘÍMÉMU PŘÍSTUPU PRACOVNÍCH STANIC NA INTERNET
a směrujte provoz přes split DNS server, e-mailový server nebo autentizovaný web proxy server. Nezapomeňte vynutit pro IPv4 i Ipv6.

POUŽÍVEJTE ANTIVIROVÝ A BEZPEČNOSTNÍ SOFTWARE
a nástroje, které zakazují spouštění nebezpečných aplikací (mimo přesně definovaný seznam privilegovaných aplikací), či nástroje, které pomáhají chránit systém v době, kdy nejsou dostupné klasické bezpečnostní aktualizace.

ŠIFRUJTE DISKY
– zejména u přenosných počítačů – včetně centrální evidence klíčů.

VYUŽÍVEJTE TRUSTED PLATFORM MODULE (TPM),
tedy zabezpečený kryptografický modul pro generování a uložení hesel a kryptografických klíčů, je-li jím počítač vybaven.

NASTAVTE HESLO UEFI/BIOS
unikátní pro každou stanici s centrální správou hesel.

VYNUCUJTE SECURE BOOT
a nastavte pořadí zařízení určených pro boot systému. Boot manager musí být zabezpečen heslem.

CHRAŇTE SE PŘED ÚTOKY NA HESLA
u všech služeb, kam se přihlašují uživatelé. Například pomocí fail2ban, využití funkcí určených pro ukládání hesel (Argon2, bcrypt, scrypt, PBKDF2) nebo CAPTCHA.

PRO SPRÁVU SERVERŮ POMOCÍ SSH VYUŽÍVEJTE PRO PŘIHLÁŠENÍ KLÍČE, ZAKAŽTE HESLA.
Pro svázání otisku klíče se serverem, kde je použitý, využívejte SSHFP záznamy v DNS ideálně v kombinaci s DNSSEC, který zajistí autenticitu odpovědi obsahující SSHFP záznam.

PROVÁDĚJTE HARDENING KONFIGURACE SERVEROVÝCH APLIKACÍ
tj. databází, webových aplikací, CRM systémů, účetních systémů, HR systémů a dalších systémů ukládání dat.

KONTROLUJTE PŘENOSNÁ MÉDIA
jako součást širší strategie prevence ztráty dat, včetně vedení seznamu povolených USB zařízení, jejich skladování, šifrování, mazání a likvidace.

OMEZTE PŘÍSTUP K SERVER MESSAGE BLOCKU (SMB) A NETBIOSU
na pracovních stanicích a serverech, kdekoliv je to možné.

POUŽÍVEJTE REŽIM CHRÁNĚNÉHO PŘÍSTUPU PŘI PRÁCI SE SOUBORY NA ÚROVNI PRACOVNÍCH STANIC
může se např. jednat o Protected View nebo Protected mode.

VYNUŤTE VYTÁČENÍ VPN,
pokud se zařízení připojuje mimo síť organizace. Omezte síťovou aktivitu, dokud není navázáno VPN spojení.

ZAJISTĚTE FYZICKOU BEZPEČNOST IT TECHNIKY

POUŽÍVEJTE ŠIFROVANÉ SPOJENÍ MEZI POŠTOVNÍMI SERVERY (TLS)
pro zajištění důvěrnosti e-mailové komunikace, v ideálních případě použijte DANE (DNS-based Authentication of Named Entities). Kontrolu obsahu provádějte až poté, co je e-mailový provoz

SPRÁVA ÚČTŮ

ZAVEĎTE CENTRÁLNÍ SPRÁVU UŽIVATELSKÝCH ÚČTŮ A OPRÁVNĚNÍ
a nastavte jednotnou bezpečnostní politiku. Účtům, u kterých to není vyžadováno, odeberte rozšířená oprávnění a zakažte spouštění skriptů, instalaci softwaru, úpravy registru atd.

VYNUCUJTE VÍCEFAKTOROVOU AUTENTIZACI
zejména pro akce vyžadující vyšší úroveň oprávnění a kritické operace jako vzdálený přístup nebo přístup k citlivým informacím.

ODDĚLTE ADMINISTRÁTORSKÉ ÚČTY
Pro správu používejte speciální účty pro administraci systémů. Pro své ostatní pracovní aktivity (e-mail, web atd.) používejte běžný neprivilegovaný účet. Účet s oprávněním doménového administrátora je použit pouze ke správě Domain Controlleru (tzn. nepřistupuje na klientské stanice a servery).

PŘIĎELTE KAŽDÉMU ADMINISTRÁTOROVI VLASTNÍ ÚČET
pro správu systémů. Nepoužívejte sdílené účty.

ZABEZPEČTE LOKÁLNÍ ADMINISTRÁTORSKÉ ÚČTY.
Nastavte unikátní heslo na každé stanici, v prostředí Windows můžete využít například LAPS (Local Administrator Password Solution).

VYNUŤTE POUŽÍVÁNÍ SILNÝCH HESEL
s ohledem na vyžadovanou složitost, délku a dobu platnosti. Zamezte opakovanému použití stejných hesel a používání slovníkových výrazů. Vynutte změnu hesla, existuje-li podezření, že bylo kompromitováno.

PRAVIDELNĚ KONTROLUJTE UŽIVATELSKÉ ÚČTY A JEJICH OPRÁVNĚNÍ
a to jak lokální, tak centrálně spravované.

www.nukib.cz

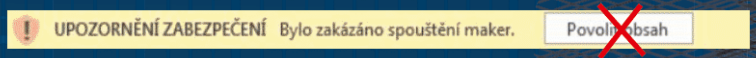
Národní úřad pro kybernetickou a informační bezpečnost

PŘÍLOHA 3:

TLP: WHITE

SPEAR-PHISHING
DOPORUČENÍ PRO PERSONÁL NEMOCNIC

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



SPEAR-PHISHING ZBLÍZKA

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

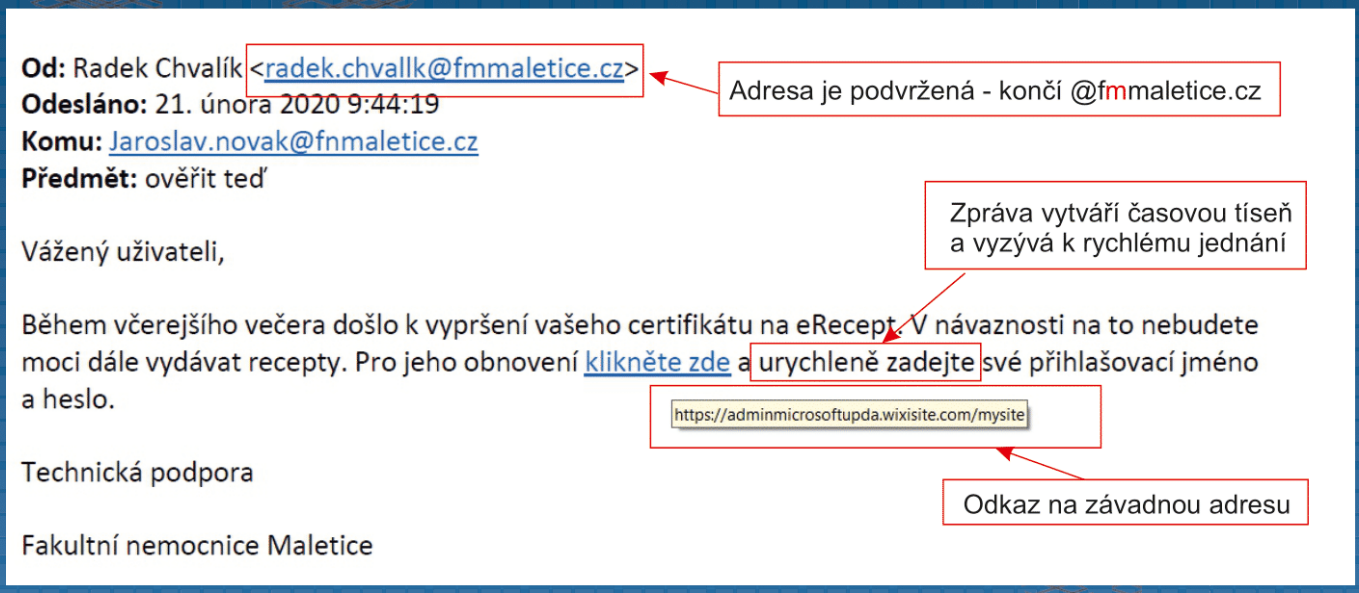
Příklad ransomwaru Petya z roku 2016, který infikoval více než 300 000 počítačů.

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

Cílem je instalace malwaru nebo krádež přihlašovacích údajů.

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

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



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

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

www.nukib.cz

Národní úřad pro kybernetickou a informační bezpečnost

ŘÍLOHA 4: DOPORUČENÍ PRO MEDIÁLNÍ KOMUNIKACI V PŘÍPADĚ INCIDENTU

1) VĚNUJTE ČAS PEČLIVÉMU OVĚŘENÍ FAKT A ZDROJŮ

Vždy si předem zkontrolujte zdroje, ze kterých čerpáte, a fakta, která uvádíte. Sice platí, že komunikace by měla být maximálně rychlá, ale ne na úkor věcné správnosti. Sledujte aktuální vývoj. Pokud uvedete nepravdivé informace nevědomě, ihned je uveďte na pravou míru. Změna ve zveřejněném materiálu musí být jasně vyznačena a zdůvodněna (změna sama o sobě je novou zprávou, která v informačním toku může přebít dřívější chybné sdělení). Mějte na paměti, že není vždy nutné publikovat všechny detaily, pokud to není ve veřejném zájmu a jejich zveřejnění by s sebou mohlo nést bezpečnostní rizika. Zvolte si jedno hlavní sdělení a zajistěte, aby toto sdělení nekomunikovala pouze Vaše instituce, ale ideálně i další partnerské subjekty.

2) MĚJTE PŘIPRAVENÝ KONTAKTNÍ LIST PRO PŘÍPAD KRIZE V OBLASTI KYBERNETICKÉ BEZPEČNOSTI

Měl by obsahovat instituce (média, partnery, dodavatele atd.) a osoby (novináře věnující se kybernetické bezpečnosti, ICT experty atd.). Výrazně Vám to usnadní práci a zrychlí reakci na nastalý problém. Kontaktní list by měl obsahovat i sloupec vhodných „komunikačních kanálů“ pro daný subjekt: někdo může Vaše sdělení sdílet na Twitteru, někdo rozhlasem, jiný televizí. Okruh příjemců každého kanálu bývá dost odlišný.

3) NEDOVOLTE ŠÍŘENÍ FAKE NEWS

Pokud třetí strana šíří fake news, úzce spolupracujte s klíčovými médii. Sledujte nejnovější vývoj, pomůže Vám to udržet situaci pod kontrolou. Na falešné zprávy reagujte na úrovni, na níž vznikly, tzn. na lživý status na Facebooku reagujte komentářem pod tímto statusem. Nesdílejte ho na svůj Facebook, ani nereagujte tiskovou zprávou apod. Nemá smysl vlastní činností dopravit lživou informaci k širšímu okruhu osob, než jaký aktuálně oslovuje.

4) VYHNĚTE SE ŠÍŘENÍ POPLAŠNÉ ZPRÁVY

Vždy se ujistěte, že svým prohlášením nešíříte paniku a strach. Vaše mediální aktivita nesmí situaci učinit horší, není vždy nutné poskytnout médiím a veřejnosti všechny detaily. Sdělitelné informace je však potřeba setřídit a formulovat tak, aby poskytly pravdivý, srozumitelný a uvěřitelný popis skutečnosti. Pokuste se vycházet spíše z toho, co je zajímavé a důležité z pohledu cílového publika, ne z pohledu Vaší instituce.

5) PRO OSLOVENÍ CO NEJŠIRŠÍHO PUBLIKA VYUŽIJTE MAXIMUM KOMUNIKAČNÍCH KANÁLŮ

Včetně sociálních sítí, tiskových zpráv, atp.

6) POSKYTNĚTE VEŘEJNOSTI NEZBYTNÉ INFORMACE

Někdy může být složité vzhledem k nedostatku informací nebo jejich citlivosti/utajení veřejnost a média uspokojivě informovat. Pokuste se spolupracovat se všemi relevantními subjekty a poskytnout alespoň základní informace, byť by byly jen obecné. Zároveň poskytněte vysvětlení nutnosti nesdílet všechny informace.

PŘÍLOHA 5: PRŮBĚH RANSOMWAROVÉHO ÚTOKU NA NEMOCNICNI V BENEŠOVĚ

(z článku „Malware Emotet – Trickbot – Ryuk v benešovské nemocnici" od V. Sikory a A. Kučinského[21])

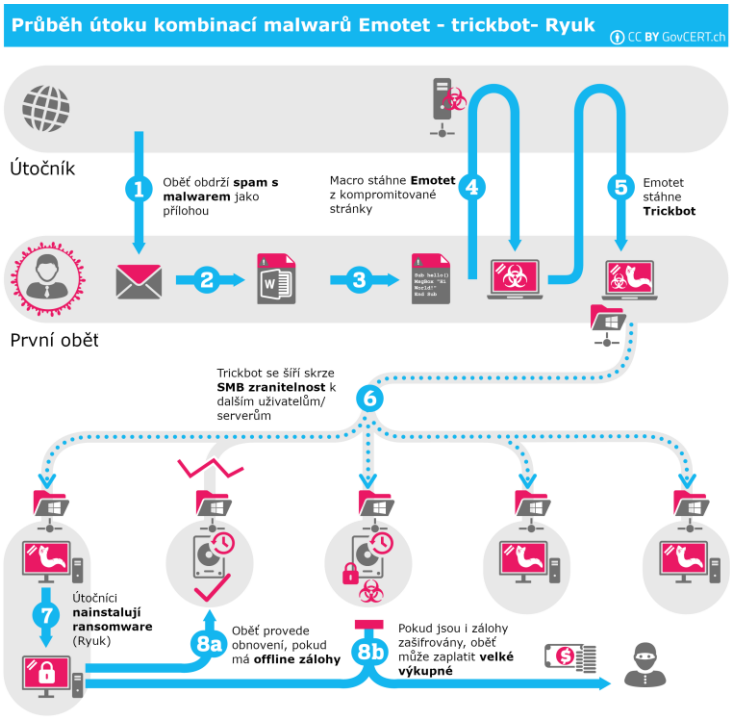
Obrázek 8: Nemocnice v Benšově

Zdroj: Novinky.cz

Zvýšenou aktivitu botnetu Emotet evidoval NÚKIB na sklonku října na základě vyhodnocování logů z honeypotů a sinkhole serverů našich zahraničních partnerů. Docházelo k mnohonásobně vyššímu počtu záchytů než obvykle a zároveň se objevovaly první zprávy o obnovení aktivit dříve dopadených a vypnutých C&C serverů. Výkyv v aktivitě je u botnetů běžný jev a často je provázen paralelními událostmi, jako je například masivní phishingová kampaň. Právě Emotet takové kampaně využívá ke svému dalšímu šíření. **Dříve se phishing vyznačoval špatnou češtinou, ale časem se jazyk v těchto kampaních zlepšoval až na dnešní úroveň, kdy narážíme na e-maily psané velmi dobrou obecnou, nebo spisovnou češtinou.** Nový trend, který sofistikovanost phishingových e-mailů dále zvyšuje, se vyznačuje využíváním kompromitovaných schránek k odesílání nakažené přílohy v odpovědi na dřívější legitimní komunikaci oběti.

Emotet byl původně vytvořen jako bankovní trojan používaný ke krádeži citlivých údajů, čísel karet nebo hesel. Dnes slouží primárně jako vstupní malware, který útočníkovi zajistí přístup do napadené sítě. Až ve druhé fázi útoku dochází ke stažení trojanu Trickbot, který se postará o sběr citlivých údajů a rozšíří portfolio dat k exfiltraci o položky typu peněženek kryptoměn, což koresponduje s trendy v době jeho vzniku v roce 2016. **Jeho zdrojový kód je navíc neustále zdokonalován. Například po zveřejnění zranitelnosti EternalBlue byl schopen vlastního laterálního pohybu a i nadále mu přibývají nové funkce.** Útočník s takto širokou paletou dat může jednoduše zničit reputaci instituce, nebo jí způsobit vážné finanční potíže. **Pro běžného uživatele je v případě nákazy Trickbotem obtížné vypozorovat nezvyklé chování počítače. Je pravděpodobnější, že nákazu zaznamená síťový administrátor v momentě, kdy počítač kontaktuje podezřelou adresu C&C serveru při exfiltraci dat, či při dotazu na další instrukce.** Jen málokterý uživatel je schopen škodlivou aktivitu detekovat přímo na nakaženém stroji. V tento moment často dochází k velmi rozšířené a v některých případech i úplné kompromitaci sítě. Malware totiž dokáže v produkční síti strávit bez detekce až několik měsíců a při tom kontinuálně sbírat informace. Po exfiltraci dat a kompromitaci důležitého prvku sítě útočníci přistoupí k poslednímu, a z jejich pohledu i logickému kroku, kterým je spuštění ransomwaru.

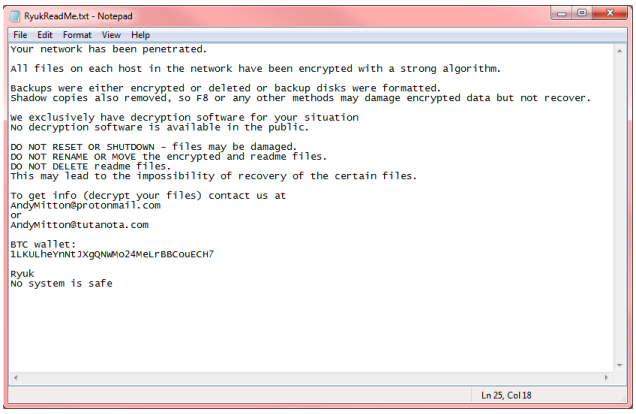
Obrázek 9: Schéma útoku kombinací malwarů Emotet, Trickbot a Ryuk



Zdroj: govcert.ch

V benešovské nemocnici došlo ke stažení ransomwaru Ryuk, který postupně mapoval všechna možná síťová úložiště na privátních adresách a šifroval na nich silnými klíči RSA-4096 a AES-256. Šifrují se buď všechna data, nebo pouze výběr souborů s předem definovanými příponami. **Takto zašifrované soubory není v dnešní době možné v reálném čase bez znalosti klíčů dešifrovat.** Na základě rychlé komunikace zejména ze strany DPO (data protection officer) benešovské nemocnice se podařilo poměrně rychle získat základní informace o incidentu a situaci na místě. Díky tomuto podnětu NÚKIB do řešení incidentu v benešovské nemocnici zapojil analytiky, kteří svými schopnostmi pokrývali oblasti Windows domény, Windows stanic, forenzní analýzy Windows a Linux, síťového provozu a monitoringu a virtualizace infrastruktury. V rámci incident response týmů, které jsou vysílány na místo útoku, je standardně zastoupen vedle jiných analytiků také forenzní specialista, neboť většinou na počátku řešení incidentu neexistuje dostatek informací o situaci, typu útoku či rozsahu zasažení. Forenzní specialista se zaměřuje na zajištění důkazů a zejména na to, aby byly důkazy použitelné i v dalším vyšetřování, případně i v trestním řízení. Při zajišťování je potřeba dodržet postupy, které zajistí důvěryhodnost a integritu dat. Forenzní specialista má mimo jiné za úkol hledání persistencí malwaru, analýzu prostředí a pomoc s čištěním infikovaných strojů. Svůj tým malware analytiků vyslal i dodavatel antivirového řešení a jeho členové na místě analyzovali infrastrukturu a vzorky malware. Po počáteční analýze situace, prostředí a rozsahu škod byl společně s dodavateli infrastruktury a zaměstnanci nemocnice vytvořen plán na postupnou obnovu infrastruktury. Paralelně s tím na pracovišti NÚKIB probíhala síťová a forenzní analýza, díky které Úřad dokázal určit šíři nákazy, persistenci malwaru a indikátory kompromitace. Zejména díky indikátorům kompromitace, které se v co nejkratší době distribuovaly organizacím v kompetenci Úřadu, se zamezilo podobné nákaze u jiné organizace. Mezi indikátory kompromitace patří nejčastěji IP adresy, domény a hashe nástrojů malware.

Obrázek 10: Vzkaz o zašifrování dat a platbě za dešifrování ransomwaru Ryuk



Zdroj: research.checkpoint.com

Mimo indikátorů kompromitace se zjišťovala zejména doba, po jakou byly systémy infikovány. **Obvyklou chybou bývá, že správci obnoví infikované zálohy, a pokud nedojde k úpravám sítě, nákaza se opět po připojení infrastruktury k internetu stává aktivní a může znovu vyeskalovat v šifrování dat.**

POUŽITÉ ZDROJE

[1] *Cybercrime tactics and techniques: Ransomware Retrospective.* 2019. Malwarebytes. Dostupné: https://resources.malwarebytes.com/resource/cybercrime-tactics-and-techniques-ransomware-retrospective/

[2] Stupp. C. 2020. *Interpol Says Hospitals Targeted With Array of Ransomware.* Wall Street Journal. Dostupné: https://www.wsj.com/articles/interpol-says-hospitals-targeted-with-array-of-ransomware-11587029402

[3] *Hrozba kybernetických útoků na nemocnice a jiné významné cíle ČR.* 2020. NÚKIB. Dostupné z: https://www.nukib.cz/cs/informacni-servis/aktuality/1425-hrozba-kybernetickych-utoku-na-nemocnice-a-jine-vyznamne-cile-cr/?fbclid=IwAR3Co8SorKKHWhVXwG7Y0S2sS3ZlEcZkh-MVDJrw7ETBpsAHte8b_ok7ZkA

[4] Sjouwerman, S. 2020. *The Evolution of Mobile Ransomware*. KnowBe4. Dostupné: https://blog.knowbe4.com/evolution-of-mobile-ransomware

[5] *Smartphone Market Share*. 2020. https://www.idc.com/promo/smartphone-market-share/os

[6] *Is 'REvil' the New GandCrab Ransomware*? 2019. Krebs on Security. Dostupné: https://krebsonsecurity.com/2019/07/is-revil-the-new-gandcrab-ransomware/

[7] *The White House Blames Russia for NotPetya, the 'Most Costly Cyberattack In History'*. 2018. Wired. Dostupné: https://www.wired.com/story/white-house-russia-notpetya-attribution/

[8] *Russian military 'almost certainly' responsible for destructive 2017 cyber attack*. NCIS. 2018. https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack

[9] Johnson, A, L. 2017. *WannaCry: Ransomware attacks show strong links to Lazarus group*. Dostupné: https://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group

[10] *Lazarus under the hood.* 2017. Kaspersky. Dostupné: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180244/Lazarus_Under_The_Hood_PDF_final.pdf

[11] Nichols, M. 2019. *North Korea took $2 billion in cyberattacks to fund weapons program: U.N. report*. Reuters. Dostupné: https://www.reuters.com/article/us-northkorea-cyber-un/north-korea-took-2-billion-in-cyberattacks-to-fund-weapons-program-u-n-report-idUSKCN1UV1ZX

[12] McGee, M, K. 2019. *Ransomware Attacks: The Data Integrity Issues*. Info Risk today. Dostupné: https://www.inforisktoday.com/ransomware-attacks-data-integrity-issues-a-11917

[13] Golubev, S. 2020. *Backing up is no panacea when blackmailers publish stolen data*. Kaspersky. Dostupné: https://www.kaspersky.com/blog/ransomware-data-disclosure/32410/

[14] Seals, T. 2020. *Snake Ransomware Delivers Double-Strike on Honda, Energy Co.* Threat post. Dostupné: https://threatpost.com/snake-ransomware-honda-energy/156462/

[15] Konicarová, K. 2019. *Automobilový průmysl*. CzechInvest. Dostupné: https://www.czechinvest.org/cz/Sluzby-pro-investory/Klicove-sektory/Automobilovy-prumysl

[16] Pokud jste se stali obětí ransomwarového útoku, doporučujeme informovat o této skutečnosti vládní CERT (www.nukib.cz) či národní CERT (www.csirt.cz), a to zejména pokud se domníváte, že by mohl mít útok široký a významný dopad. Na oba tyto týmy se může obrátit kdokoliv včetně jednotlivců, aktivní podporu nicméně poskytují dle svých aktuálních kapacit a primárně svým příslušným subjektům; vládní CERT prioritizuje službu veřejným a státním subjektům, zatímco národní CERT poskytuje službu hlavně subjektům soukromím.

[17] Seguin, P. 2020. *What is Ransomware?* Avast. Dostupné: https://www.avast.com/c-what-is-ransomware

[18] *How Screen Locker Ransomware Works*. 2019. Logix. Dostupné: http://www.logixconsulting.com/2019/12/13/how-screen-locker-ransomware-works/

[19] Seguin, P. 2020. *What is Ransomware?* Avast. Dostupné: https://www.avast.com/c-what-is-ransomware

[20] *Spotlight on ransomware: Ransomware encryption methods.* 2017. Emsisoft. Dostupné: https://blog.emsisoft.com/en/27649/ransomware-encryption-methods/

[21] Kučínský, A, Sikora V. 2020. *Malware Emotet – Trickbot – Ryuk v benešovské nemocnic.* Data Security Management. TATE International.

PODMÍNKY VYUŽITÍ INFORMACÍ

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

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

PRAVDĚPODOBNOSTNÍ VÝRAZY VE VÝSTUPECH NÚKIB

Pravděpodobnostní výrazy a vyjádření jejich procentuálních hodnot.

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