Informačné dokumenty o výskume spoločnosti ESET

TLP: WHITE

Digital Security
Progress. Protected.

RANSOMVÉR:
zločinecké umenie škodlivého kódu, nátlaku a manipulácie

V 2.0

Autor: Ondrej Kubovič

OBSAH

V 2.0

Autor: Ondrej Kubovič
Poďakovanie: Tento aktualizovaný dokument nadväzuje na významný príspevok Stephena Cobba z roku 2018 a súčasné (2021) úsilie mojich kolegov zo spoločnosti ESET: Reneho Holta, Jamesa Shepperda, Nicka FitzGeralda, Hany Matuškovej a Kláry Kobákovej.

Pôvodný autor: Stephen Cobb
Poďakovanie: Tento informačný dokument vznikol aj vďaka práci mojich nadaných kolegov zo spoločnosti ESET Jamesovi Rodewaldovi, Benovi Reedovi a Ferovi O'Neilovi, ako aj vďaka môjmu talentovanému tímu: Aryehovi Goretskymu, Brucovi P. Burrellovi a Cameronovi Campovi.

August 2021

CIELE

Cieľom tohto dokumentu je ukázať, aké nebezpečné rozmery ransomvér nabral, opísať najnovšie techniky používané ransomvérovými gangmi a navrhnúť, ako môže vaša organizácia znížiť mieru vystavenia ransomvérovým útokom a spôsobené škody. Venujeme sa v ňom trom vektorom útoku ransomvérom v tomto poradí: vzdialený prístup, e-mail a dodávateľský reťazec.

RANSOMVÉR – TO NAJHORŠIE SPOMEDZI KYBERNETICKÝCH HROZIEB

Útok ransomvérom možno definovať ako pokus o vydieranie organizácie zamedzením jej prístupu k vlastným údajom. Ransomvér je podskupinou malvéru, ktorý zahŕňa všetky formy škodlivého kódu vrátane počítačových vírusov a červov.

Ransomvér je pravdepodobne jednou z najzávažnejších kybernetických hrozieb, ktorým bude vaša organizácia čeliť. Prečo? Pretože zločinecké gangy, ktoré vytvárajú tento typ malvéru a poskytujú ransomvér ako službu, volia v posledných rokoch iný, cielenejší prístup k týmto druhom útokov, pri ktorom je oveľa ťažšie získať metriky.

Kybernetickí zločinci takisto neustále prichádzajú s novými spôsobmi, ako zabezpečiť, aby dostali požadovanú sumu, zvyčajne tak, že zvyšujú nátlak na obeť. V roku 2019 sa začali spoliehať na dvojité vydieranie, ktoré kombinuje „bežné" šifrovanie údajov s ich exfiltráciou. Týmto spôsobom nielenže obeti zabránili v prístupe k hodnotným, dôležitým alebo inak citlivým súborom, ale mohli ich tiež zverejniť alebo predať iným škodlivým aktérom.

Niektorí ransomvéroví útočníci ešte pritvrdili a rozhodli sa pre trojité vydieranie, v rámci ktorého navyše kontaktujú obchodných partnerov alebo zákazníkov obetí, ktoré nezaplatili výkupné. Kybernetickí zločinci informujú partnerov/zákazníkov obete, že v rámci ransomvérového útoku získali prístup k ich citlivým údajom, a navrhnú im zatlačiť na obeť útoku, aby výkupné zaplatila, a tak zabránila zverejneniu týchto údajov. V niektorých prípadoch dokonca útočníci požadujú platbu od týchto partnerov/zákazníkov.

V posledných rokoch došlo k posunu od útokov na veľký počet náhodných ľudí a požadovania len malého výkupného smerom k cielenému prístupu, v rámci ktorého sa požaduje oveľa väčšie výkupné od menšej skupiny obetí. Táto skupina má dostatok finančných prostriedkov a jej členovia si nemôžu dovoliť stratiť prístup k svojim údajom alebo kontrolu nad nimi.

Titulky z roku 2021 o významných cieľoch ransomvérových útokov:

- *Ransomvérový útok skupiny REvil na spoločnosť Kaseya v čase, keď opravovala zero-day zraniteľnosť*
- *Útok ransomvérom skupiny REvil na amerického dodávateľa jadrových zbraní*
- *Ransomvérový útok na írske zdravotníctvo – hackeri žiadajú 20 miliónov dolárov*
- *Kybernetický útok vyradil z prevádzky palivové potrubie v USA*
- *ADATA terčom ransomvérového útoku skupiny Ragnar Locker*
- *Útok ransomvérom zapríčinil odstávku online služieb mesta Tulsa*

Po pozornom preskúmaní týchto útokov je zrejmé, že obete pochádzajú z verejného aj súkromného sektora v rôznych odvetviach. Žiadne odvetvie nie je imúnne proti cielenému ransomvéru, a hoci nejde o technicky najkomplexnejšiu hrozbu, ochrana pred ňou je stredobodom záujmu mnohých bezpečnostných tímov.

RANSOMVÉR JE VEĽKÝ BIZNIS

Nikto naozaj nevie, koľko autori ransomvéru zarábajú. *Podľa prieskumu spoločnosti Group-IB* o aktuálnej situácii v odvetví sa priemerné požadované výkupné pohybuje vo výške okolo 170 000 dolárov. Autori prieskumu však dodávajú, že niektoré skupiny majú tú drzosť žiadať aj desiatky miliónov dolárov, napr. skupina Sodinokibi (tiež známa ako REvil) požadovala od každej zo spoločností Acer a Quanta 50 miliónov dolárov. Ďalšie zaujímavé čísla:

- podľa správy agentúry ENISA o ransomvéri sa v roku 2019 na zaplatenie výkupného minulo celkovo 10 miliárd eur,
- podľa FBI bolo skupine Ryuk *v rokoch 2013 – 2019 vyplatených 144 miliónov dolárov,*
- podľa autorov ransomvéru Sodinokibi bol ich zisk v roku 2020 100 miliónov dolárov (môže však ísť o prehnané číslo),
- podľa spoločnosti AdvIntel bolo skupine Ryuk *v roku 2020 vyplatených 150 miliónov dolárov,*
- v roku 2021 spoločnosť CNA Financial zaplatila pri útoku ransomvérom Phoenix Locker doteraz najvyššie jednorazové výkupné *40 miliónov dolárov,*
- v roku 2021 bolo skupine Darkside vyplatených 17,5 milióna dolárov ešte pred tým, ako sa po útoku na spoločnosť Colonial Pipeline „stiahla",
- podľa odhadov spoločnosti Chainanalysis sa *v roku 2020 na zaplatenie výkupného minulo 350 miliónov dolárov,*
- po útoku ransomvérom Sodinokibi na aplikáciu Kaseya VSA v roku 2021 požadovali útočníci 70 miliónov dolárov za univerzálny dešifrovač.

PSYCHOLOGICKÝ ASPEKT RANSOMVÉRU

Ransomvér využíva ako svoju hlavnú taktiku nátlak, a hoci existuje mnoho metód, najväčšou hrozbou, ktorú predstavuje, je zašifrovanie dôležitých údajov a zabránenie prístupu k nim. Údaje, či už osobné, pracovné alebo patriace do kategórie duševného vlastníctva, sú v každom prípade citlivé a cenné.

Situácia je o to horšia, keď môže dôjsť k poškodeniu dobrého mena jednotlivcov alebo organizácií, obchodným výpadkom alebo dokonca právnym a finančným sankciám. Riziko takýchto škôd sa ešte zvýšilo v dôsledku nového trendu, tzv. doxingu, ktorý využívajú viaceré ransomvérové gangy. Útočníci vtedy hľadajú v systémoch obetí citlivé údaje, ktoré potom hrozia zverejniť, ak obete okrem výkupného nezaplatia aj ďalší poplatok. Ide o typ dvojitého vydierania. Gang Maze, ktorý v novembri 2019 odštartoval trend doxingu, dokonca vylepšil svoj pôvodný prístup a vytvoril si vlastnú ilegálnu stránku s uniknutými údajmi, čím obetiam sťažil ich stiahnutie z obehu.

Po nátlaku, ktorý spravidla narastá, zvykne nasledovať manipulácia. Obete sú často svedkami toho, ako sú zasiahnuté viaceré aspekty ich digitálnych kontaktných bodov, od útokov DDoS na ich webové stránky až po nepríjemné prejavy prítomnosti zločincov v sieti. Niektoré z týchto útokov zahŕňajú aj metódy, ktorých účelom je vyvolať šok, ako napríklad *intenzívny útok na tlačiarne*, pri ktorom sa viacerým tlačiarňam v sieti prikáže vytlačiť žiadosť o výkupné, čo ohrozuje schopnosť manažmentu mať pod kontrolou internú a externú komunikáciu o incidente. Nátlak môže byť vyvíjaný aj priamejšou formou, napríklad získaním prístupu k údajom zákazníkov danej firmy a ich následným kontaktovaním, prípadne dokonca *obvolávaním*, ďalším ohrozovaním a verejným prenasledovaním obetí, zatiaľ čo IT oddelenia sa snažia zmierniť dôsledky útoku.

To sú len niektoré z typických aktivít, ktoré sprevádzajú dnešné ransomvérové kampane. Jednoducho povedané, ransomvér môže nešťastný incident s malvérom premeniť na psychologickú vojnu, ktorej cieľom je prinútiť obete konať proti ich vôli a záujmom. Zatiaľ čo pri fyzických únosoch zločinci zvyčajne začínajú vyvíjať nátlak, až keď majú nejaké eso v rukáve (hoci neskôr im môžu dôjsť možnosti), kybernetickí zločinci majú k dispozícii ešte širšiu škálu metód, ktoré môžu použiť na získanie prevahy a zmarenie akejkoľvek nádeje na bezproblémové vyriešenie situácie.

Na dosiahnutie svojich zlých úmyslov využívajú kybernetickí zločinci veľké množstvo metód, ktoré im potenciálne umožňujú získať vzdialený prístup, monitorovať aktivity svojich obetí a potom na ne vyvíjať chirurgicky presný nátlak. To dokazuje, akú veľkú moc môžu získať nad údajmi, sieťami, kontinuitou podnikania a reputáciou svojich obetí. Zdrojom týchto útokov totiž nemusí byť len prispôsobený malvér, zero-day zraniteľnosti alebo dlhodobé kampane pretrvávajúcich hrozieb. Môžu byť jednoducho výsledkom zlých bezpečnostných postupov zamestnancov, nevhodnej konfigurácie RDP či iných nástrojov vzdialeného prístupu alebo nedostatkov v postupoch a procesoch vo vašej organizácii, ako aj u poskytovateľov služieb alebo iných subjektov v dodávateľskom reťazci.

TECHNICKÝ ASPEKT RANSOMVÉRU

Hoci nám ransomvér znepríjemňuje život už viac ako desať rokov, v období intenzívnejšieho využívania digitálnych technológií, ktoré priniesla pandémia COVID-19, sa rozšíril ešte viac. Rýchlo sa ukázala jasná spojitosť medzi lockdownami v dôsledku pandémie COVID-19 a phishingovými e-mailami, ktoré často zneužívali aktuálne obavy z negatívnych vplyvov pandémie na podnikanie a zo stratených príležitostí.

Ďalším prejavom tohto fenoménu bola náhla práca zamestnancov z domu a ich (často úplne prvý) prístup k interným systémom a službám spoločnosti cez Remote Desktop Protocol (RDP). Ten sa stal mimoriadne obľúbeným vektorom na doručenie ransomvéru. Keďže v niektorých prípadoch je používanie RDP naviazané na práva správcu, popri mnohých iných bezpečnostných problémoch sa môže v sieti objaviť aj ransomvér.

Takisto vidíme, že používanie ransomvéru ako nástroja digitálnej kriminality do veľkej miery závisí od ambícií a rozsahu. Menej skúsení útočníci môžu amatérsky kódovať nedokonalé škodlivé skripty, ktoré prostredníctvom spamu zasiahnu veľmi obmedzený počet obetí. Iní môžu skúšať šťastie šírením škodlivého kódu (vrátane ransomvéru) prostredníctvom nástrojov na sťahovanie alebo botnetov. Ambicióznejší útočníci môžu zaplatiť poplatok za použitie plne vyladeného ransomvérového produktu a nasadiť ho s cieľom dosiahnuť osobný zisk, čím sa stanú partnermi vývojárov ransomvéru v rámci obchodného modelu ransomvéru ako služby (RaaS).

Pokročilí zločinci využívajúci systémy RaaS často najskôr zneužijú zraniteľnosti na získanie prístupu k počítaču, následne sa laterálne presunú na server a ďalej do širšej siete a až neskôr sa rozhodnú použiť ransomvér. Ak majú tieto gangy dostatok prostriedkov, môžu si kúpiť zero-day exploity alebo si dokonca vyvinúť vlastné, čo im umožní obísť mnohé typy technológií na proaktívne zmiernenie rizík. A napokon, či už vďaka šťastiu, zručnostiam alebo značným investíciám do ľudských a finančných zdrojov, *môžu útočníci zaútočiť na dodávateľský reťazec a získať tak prístup k celým IT ekosystémom*. Napríklad ovládnutím obľúbených platforiem poskytovateľov spravovaných služieb (MSP) a nástrojov na zvýšenie produktivity môžu útočníci vo veľkom rozsahu šíriť ransomvér vo viacerých sieťach (a teda aj organizáciách). Využitie útoku na dodávateľský reťazec na nasadenie ransomvéru je ďalším obávaným scenárom, s ktorým sa podniky musia vyrovnať.

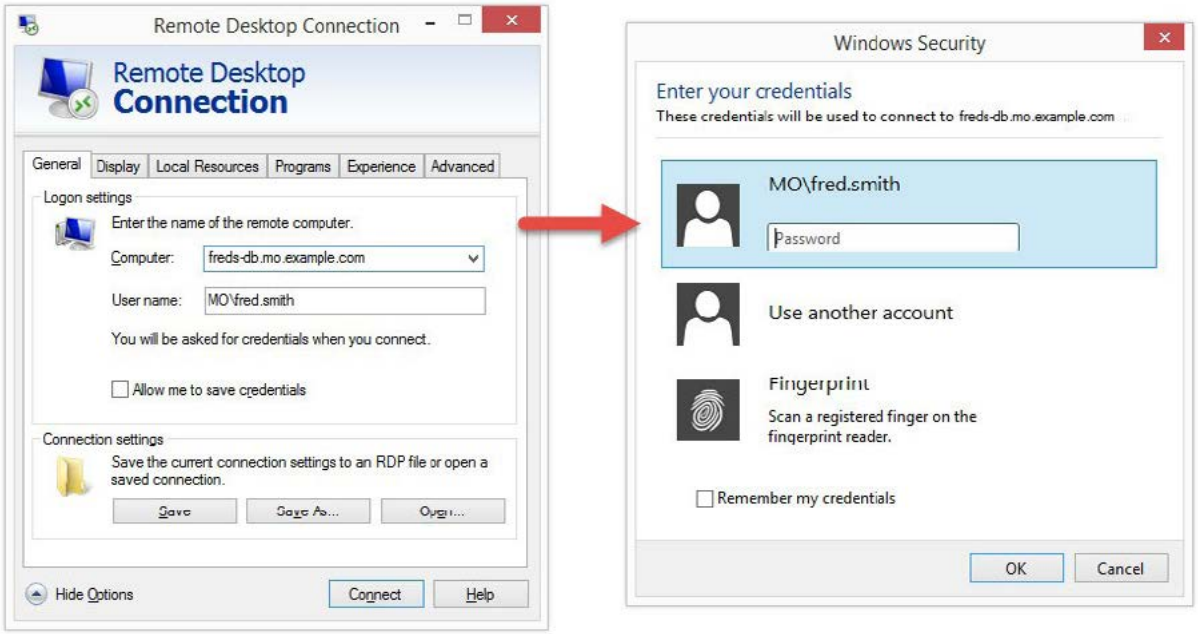
Uvedomenie si čoraz väčšej rozmanitosti prístupov a rýchlosti, s akou sa ransomvér môže vyvíjať, je rozhodujúce pre pochopenie celkového zabezpečenia potrebného na zabránenie výpadkom v podnikaní. Tempo inovácií v oblasti ransomvéru je rýchle. Príkladom je situácia, keď si výskumníci *všimli*, že ransomvér Sodinokibi (tiež známy ako REvil) bez povšimnutia šifroval súbory v núdzovom režime počítača, pričom bolo potrebné dodatočné prihlásenie používateľa. *V priebehu mesiaca* bola táto nová schopnosť vylepšená o zmenu prihlasovacieho hesla podľa výberu útočníka a o konfiguráciu počítača na automatický reštart a prihlásenie do núdzového režimu, čo z neho urobilo životaschopný vektor pre rozsiahlu kampaň.

Pozornosť ransomvérových gangov upútali aj ukladacie zariadenia pripojené k sieti (NAS), ktoré sa bežne používajú na zdieľanie súborov a vytváranie záloh. V roku 2021 výrobca týchto zariadení QNAP *upozornil* svojich zákazníkov, že ransomvér eCh0raix napáda ich zariadenia NAS, najmä tie so slabými heslami. Z telemetrie spoločnosti ESET v štvrtom štvrťroku 2020 vyplýva, že eCh0raix bol najčastejšie používaným ransomvérom zameraným na zariadenia NAS.

ÚTOK RANSOMVÉROM CEZ RDP

Koncové zariadenie RDP je zariadenie so systémom Windows, na ktorom je spustený softvér Remote Desktop Protocol (RDP) umožňujúci prístup k tomuto zariadeniu cez sieť, napríklad cez internet. RDP umožňuje vzdialený prístup k zariadeniam organizácie so systémom Windows, ako keby boli ich klávesnice a obrazovky na vašom stole. Nasadenie RDP môže mať viacero výhod – od správy zariadení zamestnancov alebo riešenia problémov s nimi až po poskytovanie centralizovaných zdrojov, ako sú stolové počítače, na ktorých môžu bežať náročné pracovné úlohy, aplikácie alebo databázy.

Firemné systémy, ku ktorým zamestnanci potrebujú vzdialený prístup, musia mať povolené RDP a v ideálnom prípade aj nastavený prístup k platforme prostredníctvom dvojúrovňového overovania. Zamestnanci sa potom k týmto systémom pripájajú pomocou softvéru RDP, napríklad zo svojich notebookov. Po zadaní sieťovej adresy vzdialeného systému sa klientsky softvér pripojí na určený port vzdialeného systému (predvolený port pre RDP je 3389, ale možno ho zmeniť). Vzdialený systém zobrazí prihlasovaciu obrazovku s požiadavkou na zadanie prihlasovacieho mena a hesla. Na obrázku 1 môžete vidieť, ako to vyzerá v systéme Windows.



Obrázok 1 // Prihlasovacia obrazovka RDP

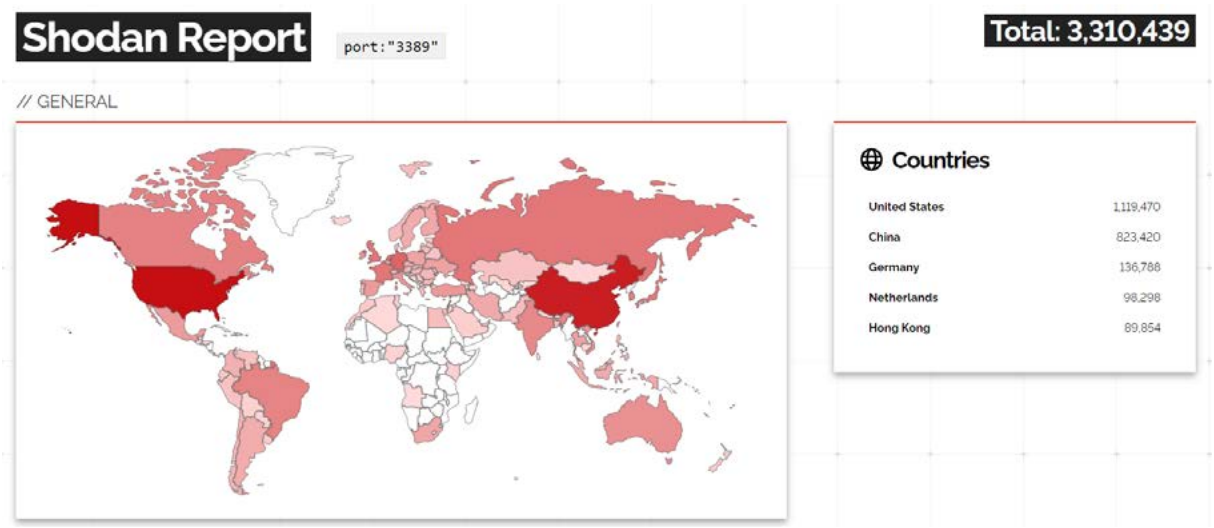
Organizácie používajú RDP dvoma hlavnými spôsobmi:

1. Prvým je správa programov bežiacich na serveri, ako sú webové stránky alebo back-endová databáza. V tomto prípade najjednoduchšia konfigurácia spočíva v tom, že správca systému otvorí port 3389 a povolí prístup zvonku, aby umožnil vzdialenú správu.
2. Druhým spôsobom používania RDP je umožnenie vzdialeného prístupu k firemným stolovým alebo virtuálnym počítačom, ktoré majú prístup k prostriedkom nedostupným mimo firemnej siete. Prístup k takýmto systémom prostredníctvom RDP znamená, že nie je potrebné priamo sprístupniť citlivé interné servery cez internet. Takisto je možné, že stolové počítače v kancelárii majú mimoriadny výpočtový výkon potrebný na mnohé procesy alebo drahý špecializovaný softvér, ktorý zamestnanci potrebujú na vykonávanie niektorých (alebo v niektorých prípadoch väčšiny) svojich úloh. Keď sa na to využíva internet, port 3389 je často otvorený, aby umožňoval prístup zvonku.

Pre kriminálnikov je jednoduché nájsť systémy dostupné zvonku a následne ich zneužiť na škodlivé účely, pretože:

- zraniteľné systémy RDP sa dajú ľahko nájsť,
- útočníci môžu ľahko preniknúť do systémov RDP so zlou konfiguráciou,
- mnohé systémy RDP majú slabú konfiguráciu,
- nástroje a techniky na zvýšenie úrovne oprávnení a získanie práv správcu v napadnutých systémoch RDP sú všeobecne známe a dostupné.

Systémy s RDP možno identifikovať pomocou špecializovaných vyhľadávačov, ako je napríklad *Shodan*, ktoré neustále prehľadávajú internet a zhromažďujú informácie o pripojených zariadeniach. Podľa platformy Shodan bolo k 15. júnu 2021 na internete viac ako 3 milióny systémov s otvoreným portom 3389 (na filtrované vyhľadávanie cez Shodan sa môže vyžadovať registrácia). Ako vidno na obrázku 2 s rozhraním Shodan, viac ako milión týchto systémov bolo v USA.



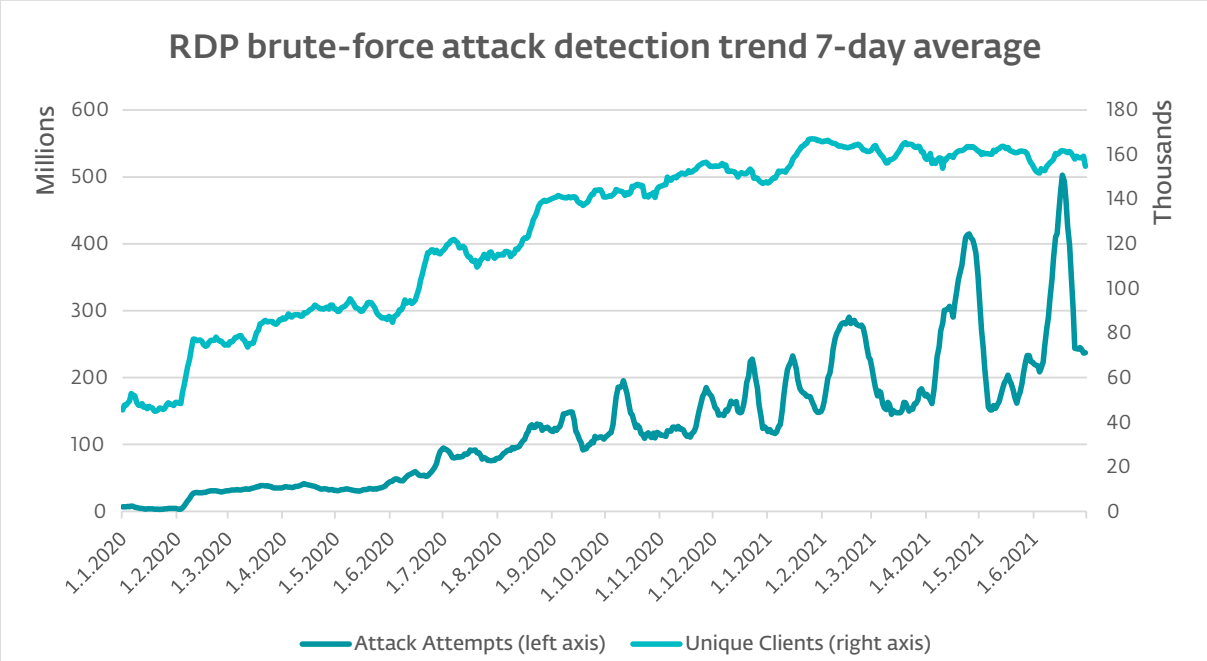
Obrázok 2 // Viac ako 3 milióny systémov na internete používajú port 3389 (zdroj: Shodan)

Pri *inom dopyte* sa zase zistilo, že na viac ako 2,7 milióna počítačov je explicitne spustený protokol RDP. Pre útočníka sú všetky tieto počítače potenciálnym cieľom, na ktorý by sa mohol zamerať. Pri prihlasovaní do systému RDP sa zvyčajne vyžaduje používateľské meno a heslo. Útočníci môžu tieto údaje prekvapivo ľahko uhádnuť a mnohým sa to aj podarí.

Útočníci, ktorí majú dostatok finančných prostriedkov, si to môžu ešte viac uľahčiť a prístup ku kompromitovaným systémom RDP si jednoducho kúpiť. Takéto prihlasovacie údaje sú k dispozícii na dark webe. Upozorňujeme, že šírenie ransomvéru nie je jediným dôvodom na nákup hacknutých prihlasovacích údajov RDP. Kompromitovaný systém RDP možno využiť aj na odosielanie spamu, hosťovanie malvéru, prelamovanie hesiel, ťažbu kryptomien a celý rad ďalších činností, pri ktorých je žiaduca anonymita, no atribúcia nie (napríklad podvodné nákupy a pranie špinavých peňazí).

Ak sa na vzdialený prístup k zariadeniu vyžaduje len používateľské meno a heslo, útočník, ktorý si takéto koncové zariadenie vybral za svoj cieľ, môže prihlasovacie údaje opakovane skúšať uhádnuť. Ak to robí vo veľkom a využíva databázu hodnoverných prihlasovacích údajov, ide o útok hrubou silou. V prípade absencie akéhokoľvek mechanizmu na obmedzenie mnohonásobných nesprávnych pokusov môžu byť takéto útoky veľmi účinné a dokonca viesť k napadnutiu celej siete.

Telemetria spoločnosti ESET potvrdzuje, že RDP je jedným z najobľúbenejších vektorov útoku, pričom od januára 2020 do júna 2021 bolo zachytených viac ako 71 miliárd detekcií. K najvýraznejšiemu nárastu došlo v prvej polovici roka 2020 a v roku 2021 boli zase zaznamenané doposiaľ najvyššie hodnoty. V prvom polroku 2021 zaznamenala spoločnosť ESET v porovnaní s prvým polrokom 2020 šesťnásobný nárast počtu detegovaných útokov hrubou silou namierených proti RDP.



Obrázok 3 // Vývoj pokusov o pripojenie k RDP a jedinečných klientov od januára 2020 do júna 2021, sedemdňový kĺzavý priemer

Získanie neoprávneného prístupu k zariadeniam s RDP z internetu si môže vyžadovať viac úsilia než šírenie ransomvéru cez e-mail, avšak vektor RDP ponúka útočníkom značné výhody, ako napríklad možnosť zneužiť legitímny prístup, vyhnúť sa ochrane koncového zariadenia a rýchlo kompromitovať viacero systémov (alebo dokonca celú sieť) v rámci jednej organizácie.

> „Útoky cez RDP môžu uniknúť mnohým detekčným metódam, čo znamená menej metrík a slabšiu informovanosť o hrozbách."

Napríklad každá organizácia s kvalitným programom informačnej bezpečnosti odhalí a zablokuje ransomvér vložený do súboru priloženého k prichádzajúcemu e-mailu. Takéto incidenty sú zvyčajne zaznamenané a nahlásené programami na ochranu koncových zariadení, pričom dodávatelia takýchto programov vytvárajú z týchto hlásení anonymizované súhrnné štatistiky o trendoch v oblasti hrozieb.

To isté často platí aj o snahe oklamať používateľov, aby navštívili škodlivé webové stránky, ktoré šíria ransomvér. Ak však útočník s oprávneniami správcu systému pred nasadením ransomvéru vypne na napadnutom serveri softvér na ochranu koncových zariadení, môže tento útok uniknúť typickým metrikám malvéru.

Laterálny pohyb a využívanie dostupných prostriedkov

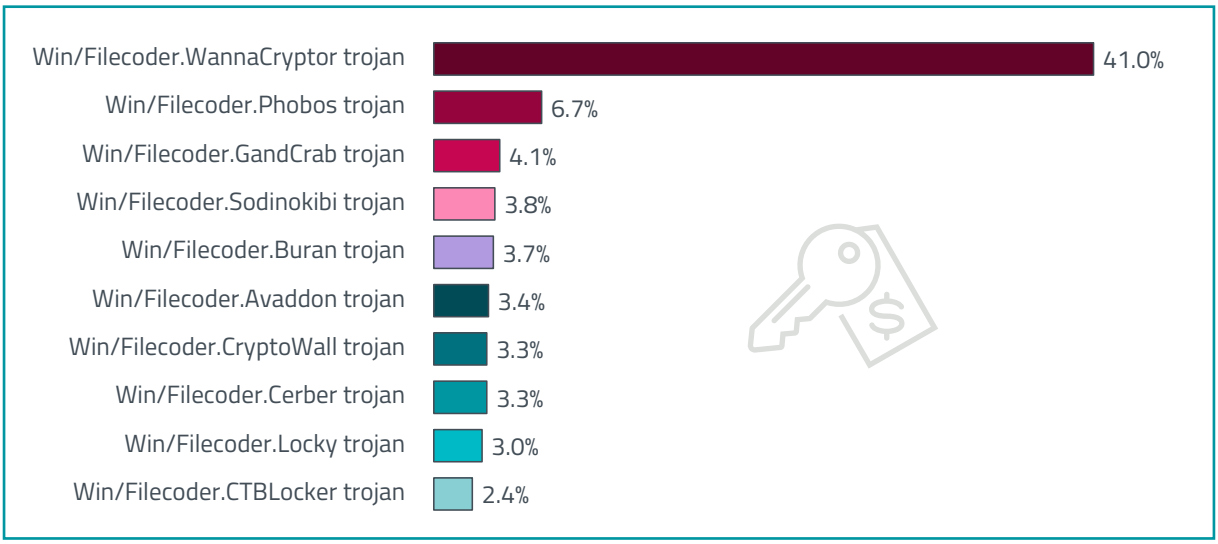
Pre ransomvérového útočníka môže kompromitovaný systém RDP znamenať oveľa viac ako len vymáhanie peňazí za dešifrovanie súborov v napadnutom počítači. Platí to najmä vtedy, ak sa daný systém môže stať vstupnou bránou do celej siete zariadení, čo môže útočníkovi umožniť rozsiahle šifrovanie alebo krádež dôležitých údajov. Práve toto sa stalo v mnohých známych prípadoch spomínaných vyššie, pričom techniky uplatňované pri tomto type útoku nie sú žiadnym tajomstvom.

Po získaní vzdialeného prístupu sa útočník bude chcieť dozvedieť viac o napadnutom počítači a vyhodnotí jeho potenciál na zneužitie, a to aj tak, že zmapuje jeho pripojenia k iným systémom. Ak prístup nezískal s prihlasovacími údajmi správcu, môže použiť niekoľko techník, vďaka ktorým svoje oprávnenia povýši na úroveň správcu. Ak je v systéme nainštalované bezpečnostné riešenie na ochranu koncových zariadení, ktoré môže vypnúť používateľ s oprávneniami správcu, útočník tak pravdepodobne urobí. Po posúdení potenciálu systému na zneužitie tak môže útočník ľahšie stiahnuť ďalší softvér. Upozorňujeme, že činnosti opísané v nasledujúcom texte ako vykonávané „útočníkom" nemusí vykonávať osoba sediaca pri klávesnici, ale softvér slúžiaci na automatizáciu jednotlivých aspektov útoku.

Niektorí útočníci sa pokúsia zaviesť do systému čo najmenej škodlivého kódu, aby minimalizovali šancu na odhalenie. Namiesto toho využijú na hlbší prienik do siete dostupné prostriedky, a teda legitímny softvér, ktorý často používajú skutoční správcovia systému, a dokonca aj štandardné nástroje nainštalované so základným operačným systémom. Napríklad PsExec a Windows Management Instrumentation Command-line (WMIC) sa často zneužívajú na šírenie infekcie naprieč napadnutými sieťami (tzv. laterálny pohyb). Na spustenie týchto programov existujú opodstatnené dôvody, a preto môže byť detekcia ich zneužitia útočníkom náročná, hoci nie nemožná. Ďalšie informácie o tom, ako ich odhaliť, sú k dispozícii v časti o nástrojoch na detekciu a reakciu na útoky na koncové zariadenia (EDR).

Termín laterálny pohyb označuje stratégiu preniknutia do jedného systému a jeho následného využitia na kompromitáciu ďalších zariadení, ku ktorým sa dá dostať z tohto systému. Útočníci môžu napríklad použiť kompromitované prihlasovacie údaje, zaútočiť na server, ktorý sa v cieľovej organizácii ani nenachádza, a využiť jeho pripojenie k hlavnej infraštruktúre na doručenie ransomvéru.

Okrem dostupných prostriedkov *môžu útočníci pri útokoch ransomvérom využiť aj neopravené zraniteľnosti v legitímnom softvéri systému*. Azda jedným z najtypickejších príkladov bol ransomvér WannaCryptor, ktorý sa šíril prostredníctvom *exploitu EternalBlue* zneužívajúceho mimoriadne závažnú zraniteľnosť v implementácii protokolu Server Message Block v systémoch Microsoft. Napriek tomu, že bezpečnostné záplaty boli verejne dostupné približne dva mesiace pred kampaňou WannaCryptor spustenou 12. mája 2017, útočníci aj tak našli a kompromitovali viac ako 200 000 zraniteľných počítačov. Infikované zariadenia dokonca aj v posledných fázach šírenia ransomvéru naďalej predstavovali hrozbu, keďže používatelia mohli napríklad nevedomky priniesť kompromitované notebooky do zóny, ktorú správcovia považovali za bezpečnú.



Obrázok 4 // Desať najčastejších rodín ransomvéru v prvej tretine roka 2021 (% detekcií ransomvéru).
Štyri roky po ničivom útoku z roku 2017 patrí WannaCryptor stále medzi najčastejšie detegované rodiny ransomvéru v reálnom prostredí (zdroj údajov: *Správa spoločnosti ESET o bezpečnostných hrozbách za prvú tretinu roka 2021*)

Samozrejme, je možné, že v niektorých prípadoch sa prvým miestom kontaktu útočníka s organizáciou stane server s nejakou dôležitou databázou. Vtedy sa oportunistický zločinec môže rozhodnúť ušetriť si čas a námahu a zvolí si prístup s rýchlym účinkom – jednoducho ukradne údaje, zašifruje súbory používané daným serverom a bude požadovať výkupné. Vytrvalosť však prináša svoje ovocie, takže mnohí autori ransomvérov budú pravdepodobne pátrať ďalej aj po odcudzení údajov a pred ich zašifrovaním, len aby sa uistili, že majú dostatočné páky.

Obrana proti útokom ransomvérom cez RDP

Systémy s RDP je možné chrániť pred neoprávneným prístupom, a tak zabrániť zločincom zneužiť tento čoraz obľúbenejší vektor útoku, či už na šírenie ransomvéru, alebo nejaký ďalší neoprávnený prístup k systému. Táto časť dokumentu je venovaná obranným stratégiám, ale podrobnejší zoznam spôsobov ochrany pred ransomvérom je uvedený v časti *Zabezpečenie RDP pred ransomvérom*.

Samozrejme, vaša organizácia už môže mať zavedené politiky týkajúce sa zabezpečenia vzdialeného prístupu. Môžete mať vytvorené pravidlá, podľa ktorých musí byť každý prístup k RDP smerovaný cez VPN (virtuálnu súkromnú sieť), zabezpečený viacúrovňovým overovaním a obmedzený na konkrétne roly, ako aj konkrétne systémy, ktoré sú bezpečne nakonfigurované, okamžite chránené bezpečnostnými záplatami, neustále monitorované, vhodne chránené firewallom a pravidelne zálohované.

No aj keď máte zavedené takéto pravidlá alebo pracujete na ich zavedení, samotné pravidlá nezabezpečia, že váš vzdialený prístup nebude hacknutý. Stále sa musíte uistiť, že všetci tieto pravidlá dodržiavajú, a zároveň musíte byť pripravení zvládnuť útok, ktorý sa napriek týmto pravidlám nejakým spôsobom podarí uskutočniť.

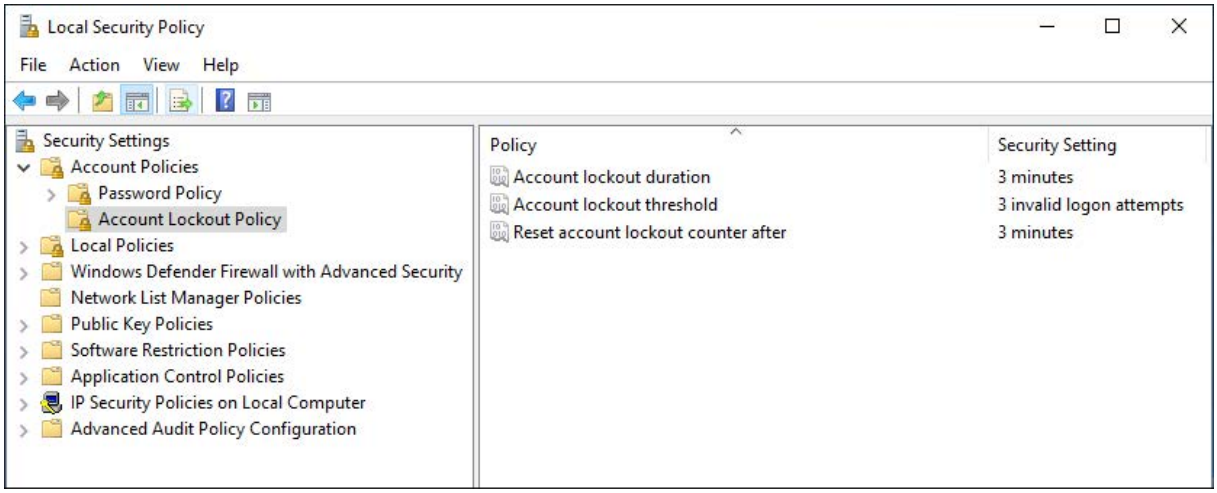
Prvým základným krokom pri obrane proti útokom ransomvérom cez RDP je inventarizácia vašich aktív pripojených k internetu. Tvrdenie, že nemôžete chrániť systém, ak neviete o jeho existencii, môže znieť pochopiteľne, ale na základe našich vyšetrovaní nie je nasledujúci scenár až taký nezvyčajný: pri útoku na organizáciu je zneužité aktívum pripojené k internetu, o ktorom bezpečnostní pracovníci organizácie až do útoku nevedeli.

Musíte zaviesť procesy, ktoré zabezpečia, aby sa to vo vašej organizácii nestalo. Napríklad dodávateľ alebo zamestnanec by nemali mať možnosť pripojiť fyzický alebo virtuálny server k firemnej sieti a internetu, pokiaľ tento server nie je bezpečne nakonfigurovaný; konfigurácia musí prebehnúť pred uvedením servera do prevádzky, najmä ak na ňom beží RDP s kontom správcu domény.

Po dokončení inventarizácie aktív pripojených k internetu je potrebné zdokumentovať, ktoré z nich majú povolený vzdialený prístup, a potom rozhodnúť, či je tento prístup potrebný. Ak je potrebný, pre účty s takýmto prístupom vyžadujte dlhé heslá. Aké dlhé? Heslá s aspoň 15 znakmi sa môžu zdať príliš dlhé, ale ak sa používajú *prístupové frázy*, dajú sa ľahko zapamätať. Okrem toho sa na heslá s takouto dĺžkou nemusia vzťahovať pravidlá komplexnosti, ktoré podľa výskumov majú tendenciu nútiť ľudí k nevhodným postupom pri vytváraní hesiel. Po nastavení prísnych požiadaviek na dĺžku hesla pre účty určte, či je možné obmedziť tieto systémy na internú sieť a pristupovať k nim vzdialene pomocou firemnej siete VPN.

Ak systém musí byť prístupný z verejného internetu prostredníctvom RDP a používanie VPN nie je možné, nainštalujte aspoň viacúrovňové overovanie, aby ste sa pri ochrane nespoliehali len na heslá. Uistite sa však, že nepoužívate viacúrovňové overovanie na báze SMS. Zločinci poznajú veľa spôsobov, ako prekaziť overovanie cez SMS (tieto techniky často vyvíjajú autori malvéru zameraného na zákazníkov európskych bánk, kde sa viacúrovňové overovanie na báze SMS používa už mnoho rokov na potvrdzovanie bankových transakcií).

Ak ste nútení spoliehať sa na heslá, pretože viacúrovňové overovanie nie je k dispozícii (prípadne z dôvodu krátkozrakej rozpočtovej politiky), aspoň zabráňte potenciálnym narušiteľom v opakovaných pokusoch o uhádnutie prihlasovacích údajov. Nastavte limit troch neplatných pokusov o prihlásenie, po ktorých sa počas stanoveného obdobia (napríklad tri minúty) nerozpozná žiadny ďalší pokus o prihlásenie. Na obrázku 3 môžete vidieť, ako to vyzerá v systéme Windows.



Obrázok 5 // Politika uzamknutia účtu

Môžete tiež zmeniť načúvací port RDP z 3389 na iný, aby bolo pre útočníkov o niečo ťažšie nájsť prístupné počítače. Dá sa to urobiť prostredníctvom systémových nastavení, ale budete musieť zmeniť aj pravidlá firewallu, aby vyhovovali určenému portu. Majte na pamäti, že ide len o zabezpečenie vychádzajúce z neznalosti útočníka (tzv. security by obscurity) a nemali by ste sa spoliehať, že tým zaistíte bezpečnosť systémov RDP (ďalšie podrobnosti nájdete v časti *Zabezpečenie RDP pred ransomvérom*).

V prípade všetkých vzdialene prístupných zariadení by sa mali sprísniť nastavenia a opraviť zraniteľnosti. Okrem identifikácie a odstránenia všetkých bezpečnostných zraniteľností by ste sa mali takisto uistiť, že všetky nepodstatné služby a komponenty sú odstránené alebo vypnuté a že nastavenia sú nakonfigurované na zaistenie maximálnej ochrany.

Napríklad v systémoch Windows môžete pomocou politík obmedzenia softvéru (SRP) zabrániť spúšťaniu súborov z priečinkov, ako sú AppData a LocalAppData, ktoré niekedy zneužíva malvér. Pomocou nástroja AppLocker môžete tiež určiť, ktoré aplikácie a súbory môžu zamestnanci spúšťať na svojich počítačoch. Samozrejme, poslednou líniou obrany proti ransomvéru zameranému na RDP je komplexný a osvedčený systém zálohovania a obnovy. Keďže zálohovanie je kľúčom k tomu, ako zvládnuť útok ransomvérom bez ohľadu na jeho vektor, budeme sa mu venovať po preskúmaní ďalších troch vektorov – e-mailu, dodávateľského reťazca a bezpečnostných zraniteľností.

Poznámka na okraj: druhé miesto hneď po RDP patrí protokolu SMB

Protokol SMB (Server Message Block), ktorý sa používa najmä na zdieľanie súborov a tlačiarní vo firemných sieťach, sa tiež často zneužíva ako vzdialená služba, cez ktorú môže do siete preniknúť ransomvér. V prvej tretine roka 2021 technológie ESET *zablokovali* 335 miliónov útokov hrubou silou na verejne prístupné služby SMB. Hoci ide o 50 % pokles v porovnaní s poslednou tretinou roka 2020, útoky cez SMB zostávajú významnou hrozbou. Aj ransomvér WannaCryptor (tiež známy ako WannaCry), ktorý v danom období roka 2021 tvoril 41 % detekcií ransomvéru, sa šíri zneužívaním zraniteľného protokolu SMBv1.

Na ochranu pred hrozbami zameranými na protokol SMB postupujte podľa týchto odporúčaní:

- *Vypnite SMBv1 a SMBv2*, no nezabudnite, že je potrebné postarať sa o všetky existujúce závislosti na týchto zastaraných verziách.
- Prejdite na najnovšiu verziu protokolu SMB, čo je v súčasnosti SMBv3.

- Pomocou nastavení skupinovej politiky zabezpečte, aby sa medzi hostiteľmi a doménovými radičmi vyžadovalo podpisovanie protokolu SMB s cieľom zabrániť opakovaným útokom na sieť.
- Zablokujte porty TCP 445 a 139 a porty UDP 137 a 138 pred internetovou komunikáciou. Tým sa zabráni, aby boli všetky verzie protokolu SMB prístupné mimo vašej siete.

Zabezpečenie RDP pred ransomvérom

Zvážte tieto stratégie a techniky:

1. **Zdokumentujte problém**
   Uistite sa, že ľudia, ktorí majú na starosti zabezpečenie, vedia o všetkých aktívach vašej organizácie pripojených k internetu. Majte zavedený proces, vďaka ktorému sa nezabudne ani na nové zariadenia.
2. **Obmedzte sprístupnené aktíva**
   Uistite sa, že žiadne digitálne aktíva nie sú vzdialene prístupné priamo z internetu, pokiaľ neboli schválené na používanie týmto spôsobom a vhodne nakonfigurované. Pouvažujte nad tým, prečo nemôžu byť aktíva sprístupnené cez VPN. Vypnite RDP vždy, keď nie je potrebné (v týchto článkoch sa dozviete, ako postupovať v rôznych verziách systému Microsoft Windows: *Server 2019*, *Server 2016*, *Server 2008/R2*, *Windows 10*, *Windows 8*, *Windows 7*).
3. **Chráňte sprístupnené aktíva**
   Ak bezpodmienečne musíte používať RDP bez VPN, uistite sa, že vykonáte čo najviac z nasledujúcich krokov:

a. Pravidelne meňte heslo k používateľskému účtu, ku ktorému sa pripájate na vzdialenom počítači. Uistite sa, že ste zmenili predvolené heslo, ktoré sa pre cloudové inštancie niekedy generuje automaticky.
b. Vynucujte komplexné heslá (povinná by mala byť dlhá prístupová fráza obsahujúca aspoň 15 znakov bez slovných spojení, ktoré sa týkajú firmy, názvov produktov alebo používateľov).
c. Nastavte prah uzamknutia účtu na zablokovanie vzdialeného prístupu po niekoľkých po sebe idúcich neúspešných pokusoch o prihlásenie.

   Nastavením počítača, aby po niekoľkých nesprávnych pokusoch na určitý čas uzamkol účet, zablokujete útočníkov, ktorí používajú automatizované nástroje na hádanie hesiel (útok hrubou silou). Ak chcete nastaviť politiku uzamknutia účtu v systéme Windows, postupujte takto:

   Prejdite do ponuky Štart --> Programy --> Nástroje na správu --> Lokálna politika zabezpečenia.

   V sekcii Politika kont --> Politika uzamknutia účtu nastavte hodnoty pre všetky tri možnosti (odporúčame tri neplatné pokusy s trojminútovým trvaním uzamknutia účtu).
d. Otestujte a nasaďte bezpečnostné záplaty pre všetky známe zraniteľnosti a uistite sa, že medzi opravenými chybami sú aj tie najčastejšie zraniteľnosti, ako napríklad BlueKeep a EternalBlue. V prípade, že počítač nie je možné zabezpečiť pred zraniteľnosťou, naplánujte jeho včasnú výmenu.
e. Pomocou overovania na úrovni siete môžete zvýšiť bezpečnosť hostiteľa relácie vzdialenej plochy tým, že pred vytvorením relácie budete od používateľa vyžadovať overenie voči serveru hostiteľa relácie vzdialenej plochy.

f. Zmeňte predvolený port pre RDP 3389. Upozorňujeme však, že ide len o zabezpečenie vychádzajúce z neznalosti útočníka (tzv. security by obscurity), a preto by nemalo byť jediným opatrením, ktoré prijmete.

   Ak chcete zmeniť port, upravte nasledujúcu hodnotu registra (VAROVANIE: neskúšajte to, ak nie ste oboznámení s databázou Registry systému Windows a protokolom TCP/IP): HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\PortNumber.

g. Obmedzte, ktoré verejné IP adresy sa môžu pripojiť cez RDP. Táto úloha môže byť náročná, ak vzdialení používatelia nemajú statické IP adresy (napríklad pri cestovaní alebo práci z domu).

h. Používajte viac ako jeden faktor overenia. Máte tri možnosti: faktor, ktorý poznáte, napríklad používateľské mená a heslá; faktor, ktorý je vám vlastný, napríklad odtlačok prsta alebo hlasový odtlačok; faktor, ktorý vlastníte, napríklad telefón, ktorý môže prijímať jednorazové prístupové kódy alebo spustiť overovaciu aplikáciu, ktorá vám takýto kód vygeneruje.

   Ak však ako druhý faktor používate kódy zasielané do telefónu, vyhnite sa SMS kódom, pretože zločinci už v minulosti prekazili overenie cez SMS (ako je opísané v *tomto článku*). Existujú dobré riešenia na viacúrovňové overovanie, ktoré využívajú rozšírenosť telefónov, ale nekomunikujú prostredníctvom SMS (napríklad *ESET Secure Authentication*). Sprísnite povolenia a oprávnenia používateľov. Zakážte spúšťanie súborov z priečinkov AppData a LocalAppData. Zablokujte spúšťanie z podadresára Temp (predvolene je súčasťou stromu AppData). Zablokujte spúšťanie spustiteľných súborov z pracovných adresárov rôznych komprimačných nástrojov (napríklad WinZip alebo 7-Zip). Okrem toho, ak máte dobrý produkt na ochranu koncových zariadení, môžete vytvoriť pravidlá HIPS, ktorými povolíte, aby sa v počítači predvolene spúšťali len určité aplikácie a všetky ostatné boli blokované.

i. Pri prístupe k serverom cez lokálne účty s právami správcu by sa mali používať jedinečné heslá (napr. s využitím nástroja LAPS alebo účinnej služby na správu hesiel). Zároveň odporúčame, aby prístupové práva k serverom mala iba obmedzená skupina používateľov. Obmedzením počtu používateľov s povoleným prístupom sa zredukujú aj možné miesta útokov na dané servery.

j. Ak je to možné, pre pripojenia klienta RDP nastavte „vysokú" úroveň šifrovania. V opačnom prípade použite pre pripojenia čo najvyššiu dostupnú úroveň šifrovania.

k. Nainštalujte bránu VPN na sprostredkovanie všetkých externých pripojení cez RDP, ktoré neprichádzajú z vašej lokálnej siete.

l. Produkt na ochranu koncových zariadení zabezpečte heslom, aby ste zabránili neoprávnenej zmene nastavení, vypnutiu ochrany alebo dokonca odinštalovaniu produktu (použite však iné heslo ako to, ktoré slúži na prihlásenie cez RDP).

m. Zapnite *blokovanie zneužití* v bezpečnostnom softvéri na koncových zariadeniach. Ide o *technológiu* určenú na detekciu anomálií, ktorá monitoruje správanie často zneužívaných aplikácií.

n. Izolujte od siete akýkoľvek nezabezpečený počítač, ktorý musí byť prístupný z internetu prostredníctvom RDP.

o. V prípade, že všetci vaši zamestnanci a dodávatelia pôsobia v rovnakej krajine alebo v niekoľkých vybraných krajinách, zvážte možnosť blokovať prístup z vylúčených krajín zavedením blokovania geografických IP adries na bráne VPN. Takto zablokujete pripojenia útočníkov z cudziny.

ÚTOK RANSOMVÉROM CEZ E-MAIL

Každý skúsený bezpečnostný expert vám povie, že hrozby pre informačné systémy sa kumulujú. Ak sa napríklad niektorí zločinci rozhodnú využiť ako vektor útoku ransomvérom servery s povoleným vzdialeným prístupom, neznamená to, že ostatné vektory môžete ignorovať. Niektorí zločinci stále využívajú e-mailové prílohy na inštaláciu malvéru, ktorý slúži ako počiatočná fáza kompromitácie. Tá sa potom končí útokom ransomvérom.

Tento vektor môžu použiť na doručenie nástrojov na sťahovanie, ktoré nainštalujú malvér do počítača príjemcu e-mailu, alebo na prienik do sieťového počítača v rámci organizácie. Takýto prienik do počítača môže byť prvým krokom pri pokuse o krádež cenných údajov, zašifrovanie súborov v celej organizácii a následné požadovanie vysokého výkupného, ako to často býva v prípade cielených útokov ransomvérom cez RDP.

E-mail je jedným z hlavných vektorov útoku najmä pre botnety, ako sú Trickbot, Qbot a Dridex, ktoré bežne používajú dokumenty Microsoft Office so škodlivými makrami na počiatočný prienik a následné doručenie ransomvéru. Takúto súčinnosť sme mohli doteraz vidieť medzi týmito botnetmi a ransomvérom: *Emotet*, Qbot, *Trickbot*, *Ryuk* a Conti; *Dridex* a FriedEx (tiež známy ako BitPaymer); *Nemucod*, *Avaddon*, Dridex, Ursnif a Trickbot; *SmokeLoader, Zloader*, LockBit a Crysis.

Orgány činné v trestnom konaní na začiatku roka 2021 zneškodnili *Emotet*, čo viedlo k veľmi výraznému poklesu šírenia nástrojov na sťahovanie cez e-mail. Dôsledky kampaní malvéru Emotet, a to pred jeho zneškodnením aj po ňom, sú opísané v *správe o bezpečnostných hrozbách ESET za prvú tretinu roka 2021*, v *správe o bezpečnostných hrozbách ESET za štvrtý štvrťrok 2020* a v *správe o bezpečnostných hrozbách ESET za tretí štvrťrok 2020*.

Napriek výraznému poklesu šírenia nástrojov na sťahovanie zostávajú útočníci využívajúci kompromitované makrá hlavnou e-mailovou hrozbou aj v roku 2021. V januári sa dokonca zvýšil počet e-mailov doručujúcich škodlivé dokumenty balíka Office, ktoré inštalovali nástroje na sťahovanie Dridex a Emotet. V októbri 2020 sme boli svedkami pokusu o zneškodnenie ďalšieho populárneho botnetu *Trickbot*, ale zdá sa, že naša radosť bola predčasná, pretože jeho autori už v januári 2021 spustili *novú phishingovú kampaň* zameranú na právnické a poisťovacie spoločnosti v Severnej Amerike. V budúcnosti bude teda zrejme potrebné vynaložiť ďalšie úsilie, aby sme sa botnetu Trickbot nadobro zbavili.

Pokiaľ ide o ochranu vašej organizácie pred útokmi ransomvérom cez e-mail, prvou líniou obrany je filtrovanie všetkých prichádzajúcich e-mailov, či neobsahujú spam a phishingové správy. Na takéto filtrovanie existovalo niekoľko dobrých dôvodov dávno predtým, ako sa e-mail začal využívať na šírenie ransomvéru, takže mnohé organizácie už majú zavedené základné filtrovanie spamu a detekciu phishingu.

V rámci ochrany môžete zájsť ešte ďalej a blokovať všetky typy príloh, ktoré vaša firma bežne neočakáva, že dostane e-mailom. Vhodnosť tejto stratégie však bude závisieť od druhu podnikania a môže si vyžadovať zmenu niektorých pracovných návykov. Ak si napríklad zamestnanci zvyknú posielať cez e-mail tabuľky programu Excel a dokumenty programu Word, organizácia možno bude musieť najskôr zaviesť bezpečné riešenie na zdieľanie súborov alebo rámec spolupráce a následne zaistiť jeho používanie zamestnancami. Až potom bude môcť striktne implementovať prísnejšie filtrovanie e-mailových príloh.

Uistite sa, že na všetkých koncových zariadeniach je nainštalovaný kvalitný softvér na ochranu koncových zariadení (EPP), ktorý zabráni zamestnancom pristupovať na webové stránky, o ktorých je známe, že sú hostiteľmi malvéru. Môžete využiť aj ďalšiu vrstvu ochrany v podobe filtrovania webového obsahu. Okrem blokovania škodlivých webových lokalít môže filtrovanie webového obsahu zabrániť zamestnancom navštevovať webové stránky, ktoré sa považujú za nevhodné na pracovné účely.

Vaše riešenie na ochranu koncových zariadení by malo byť spravované centrálne, aby sa mohli vynucovať príslušné bezpečnostné politiky, ako napríklad obmedzenie možnosti vypnúť ochranu koncového zariadenia alebo vložiť/pripojiť vymeniteľné médiá. Uistite sa, že na všetkých koncových zariadeniach je nainštalovaná najnovšia verzia produktu a úspešne načítava aktualizácie. Ak má váš produkt na ochranu koncových zariadení cloudovú súčasť, uistite sa, že je zapnutá, pretože umožňuje ešte rýchlejšie reagovať na nové hrozby. ESET tento cloudový komponent nazýva *ESET LiveGrid®* a v niektorých produktoch *ESET Dynamic Threat Defense*.

Včasnou a komplexnou inštaláciou bezpečnostných záplat pre operačné systémy a aplikácie zabránite prieniku ransomvéru prostredníctvom e-mailových príloh alebo neúmyselne stiahnutých súborov. Užitočná môže byť aj bezpečná konfigurácia. Zvážte napríklad použitie skupinovej politiky na úplné vypnutie makier Microsoft Office. Obmedzíte tým možné miesta útokov ransomvérom, hoci toto opatrenie nemusí byť uskutočniteľné, ak sa v rámci pracovných postupov organizácie využívajú makrá.

V súčasnosti už niet pochýb o tom, že bezpečnosť je spoločnou zodpovednosťou, preto sa uistite, že vaše školenie pre zamestnancov o kybernetickej bezpečnosti je aktuálne a odráža najnovšie trendy v oblasti hrozieb.

Zamestnancom jasne povedzte, že by mali podozrivé správy a prílohy okamžite nahlásiť technickej podpore alebo bezpečnostnému tímu. Okrem toho, že takýmto včasným varovaním sa zabráni škodám alebo sa aspoň obmedzia, organizácii to pomôže vyladiť filtre nevyžiadanej pošty a obsahu a posilniť firewally a iné ochranné prostriedky.

ÚTOK RANSOMVÉROM CEZ DODÁVATEĽSKÝ REŤAZEC

Vektorom útoku ransomvérom, ktorý si v súčasnosti zaslúži zvýšenú pozornosť, je dodávateľský reťazec softvéru. Riziká v dodávateľskom reťazci softvéru sa rovnako ako ransomvér datujú do minulého storočia. V časoch, keď sa počítačové vírusy šírili najmä prostredníctvom počítačových diskov, ktoré predstavovali hlavný spôsob, akým ľudia získavali softvér, sa malvér niekedy dostal na produkčné disky alebo disky so skúšobnými verziami programov, ktoré sa distribuovali spolu s časopismi o počítačoch.

V roku 2017 spoločnosť ESET *zistila*, že zločinci používali legitímny účtovný softvér na *šírenie malvéru NotPetya/DiskCoder.C*. Útočníci prenikli na aktualizačné servery softvérovej spoločnosti a pridali do legitímnych aktualizačných súborov aplikácie svoj vlastný kód. Keď používatelia účtovného softvéru klikli na inštaláciu aktualizácií programu, súčasne s nimi nainštalovali aj backdoor malvéru, čím otvorili cestu najničivejšiemu kybernetickému útoku v histórii. Prvou líniou obrany proti takémuto útoku je dobrý produkt na ochranu koncových zariadení s podporou nástrojov EDR.

Vzhľadom na komplexnosť dôsledkov týchto útokov a ich následné nevyhnutné zmiernenie sú výskumníci a správcovia zabezpečenia v strehu. *Dňa 2. júla 2021 došlo v súvislosti so softvérom spoločnosti Kaseya na správu IT služieb pre MSP k sérii udalostí*, ktoré vykazovali vlastnosti ransomvérového útoku na dodávateľský reťazec využívajúceho trójskeho koňa Win32/Filecoder.Sodinokibi.N. Následné vyšetrovanie ukázalo, že incident bol založený na zneužití zero-day zraniteľnosti, avšak už len zmienka o dodávateľskom reťazci vyvolala rýchlu reakciu. Spoločnosť Kaseya rýchlo určila prioritné incidenty a odoslala oznámenia potenciálne zasiahnutým firmám s odporúčaním okamžite vypnúť potenciálne napadnuté lokálne servery VSA.

O rastúcej intenzite útokov na dodávateľský reťazec svedčí aj počet *publikovaných* výskumných článkov spoločnosti ESET o prípadoch, pri ktorých bol použitý tento vektor útoku. Medzi novembrom 2020 a februárom 2021 len spoločnosť ESET zachytila štyri prípady útokov na dodávateľský reťazec, čo je veľmi vysoký počet v porovnaní s predchádzajúcimi rokmi.

Obrana proti tomuto typu útoku zahŕňa inštaláciu bezpečnostných záplat, používanie softvéru na ochranu koncových zariadení, využívanie *riešení EDR* a vzdelávanie používateľov o nevyžiadaných e-mailoch, ktoré ich nabádajú k návšteve neznámych webových stránok.

ÚTOK RANSOMVÉROM PROSTREDNÍCTVOM ZNEUŽITIA ZRANITEĽNOSTÍ

Hoci kybernetickí zločinci môžu využívať známe aj neznáme zraniteľnosti, zneužívanie zero-day zraniteľností je vo všeobecnosti doménou APT skupín a štátom sponzorovaných útočníkov. Napriek hrozbe, ktorú predstavujú zero-day zraniteľnosti, aj známe bezpečnostné zraniteľnosti môžu spôsobovať správcom zabezpečenia, výskumníkom a majiteľom firiem viac než dosť starostí.

Príkladom je skutočnosť, že takmer všetci dodávatelia bezpečnostných riešení stále detegujú exploit EternalBlue (2017) a jeho mnohé varianty, ako aj pokračujúce zneužívanie zraniteľnosti založené na protokole zdieľania súborov SMBv1 v systémoch Microsoft. Príčinou dlhej životnosti zraniteľností a hrozieb, ako je WannaCryptor (tiež známy ako WannaCry), sú zvyčajne nedostatočné aktualizácie a zlá správa bezpečnostných záplat vo firmách a inštitúciách.

Súčasne s rastúcou komplexnosťou hrozieb sa objavili nové nástroje na boj proti modernejším hrozbám, ktoré hľadajú zraniteľnosti v produktoch a zaisťujú dôkladnú správu bezpečnostných záplat, čím predstavujú ďalšiu technickú záťaž.

Obrovský nárast používania siete VPN vo firmách aj na osobnú potrebu a závislosť od nej bije do očí. V tejto súvislosti sa v mysli vynoria dva prípady, keď boli v službách VPN spoločností *Pulse Secure* a *Fortinet* identifikované zraniteľnosti, ktoré umožnili šírenie ransomvéru medzi zákazníkmi. Používanie

VPN vo veľkých inštitúciách a podnikoch je síce veľmi účinné, ale zároveň prináša ďalšiu zodpovednosť, pokiaľ ide o aktualizácie produktu podľa potreby. Toto zameranie na včasné aktualizácie by malo byť sprevádzané používaním viacúrovňového overovania pri prihlasovaní do príslušných služieb VPN. V prípade podozrenia zo zneužitia prihlasovacích údajov by mali organizácie pristúpiť ku komplexnému obnoveniu účtov.

Tieto výzvy sa odzrkadľujú aj v celosvetovom náraste využívania veľkých platforiem produktivity a spolupráce. V marci 2021 vypukol medzi útočníkmi, poprednými dodávateľmi softvéru a širším odvetvím kybernetickej bezpečnosti ošiaľ, keď sa zistilo, že spoločnosť Microsoft urýchlene vydala núdzové aktualizácie na riešenie štyroch zero-day zraniteľností ovplyvňujúcich Microsoft Exchange Server vo verziách 2013, 2016 a 2019. Následne sa zistilo, že útočníci využívali tieto zraniteľnosti v reálnom prostredí na prístup k lokálnym Exchange serverom, čo im umožnilo kradnúť e-maily, sťahovať údaje a zneužívať počítače s malvérom na dlhodobý prístup do sietí obetí.

Pri tomto rozsiahlom incidente boli *Exchange servery v konečnom dôsledku napadnuté najmenej desiatimi skupinami APT*. Výskumníci spoločnosti ESET sa okamžite zamerali na to, koľko organizácií by útočníci mohli presondovať a infiltrovať s cieľom pripraviť si cestu pre budúce útoky vrátane ransomvéru. Aký by bol pravdepodobný mechanizmus? Po preniknutí na Microsoft Exchange Server by mali útočníci privilegovaný prístup k spoločnosti, možno aj práva správcu, a potom by mohli včas naplánovať nadchádzajúci útok.

Ako už bolo uvedené v časti o útokoch na dodávateľský reťazec, *útok* ransomvérom na aplikáciu Kaseya VSA zasiahol viac ako 50 poskytovateľov spravovaných služieb s dosahom na vyše 1 000 koncových zákazníkov. Útočníci využili niekoľko zero-day zraniteľností vrátane CVE-2021-30116 na kompromitáciu softvéru na IT správu Kaseya VSA, ktorý je obľúbeným nástrojom poskytovateľov spravovaných služieb. Útočníci tvrdili, že napadli viac ako milión systémov, čo však môže byť prehnané. Telemetria spoločnosti ESET odhalila obete v 17 krajinách vrátane Spojeného kráľovstva, Južnej Afriky, Kanady, Nemecka a Spojených štátov amerických.

Hoci sa nepotvrdili prvé náznaky, že problémy spoločnosti Kaseya spôsobil útok na dodávateľský reťazec, zero-day útok tohto druhu je veľmi vážny a skutočne mal dosah aj na dodávateľský reťazec. Stručne povedané, vzhľadom na popularitu systémov Kaseya boli ovplyvnené aj podniky iba okrajovo spojené s platformou VSA pre poskytovateľov spravovaných služieb. Od 2. júla zatvoril škandinávsky reťazec supermarketov Coop približne 500 predajní, pretože sprostredkovateľ platieb tretej strany a *dodávateľ ich pokladničného/POS systému* využíval práve systémy hosťované spoločnosťou Kaseya. Takže hoci spoločnosť Coop nebola priamou obeťou, tento incident mal na ňu značný dosah vzhľadom na jej závislosť od inej služby, ktorá bola odstavená v dôsledku útoku na spoločnosť Kaseya.

IT správcovia, vedúci pracovníci z oblasti kybernetických hrozieb a informačnej bezpečnosti a vrcholoví manažéri by mali venovať pozornosť rozsahu a dôsledkom oboch incidentov (Microsoft Exchange aj Kaseya), aby vnímali prostredie hrozieb a vplyv ransomvéru na podnikanie z novej perspektívy. Ďalšie informácie nájdete vo verejných správach o niektorých z najčastejšie spomínaných zraniteľností:

- *Kaseya VSA,*
- *Pulse Connect Secure,*
- *Citrix Hypervisor,*
- *Fortinet VPN,*
- Microsoft Exchange Server – prečítajte si článok v našej najnovšej *správe o bezpečnostných hrozbách*,
- *Citrix Application Delivery Controller a Gateway,*
- *Microsoft Office Common Controls,*
- *Windows Win32k,*
- *Accellion File Transfer Appliance.*

CLOUD A SEGMENTÁCIA

Ak ransomvér prenikne do vašej organizácie (bez ohľadu na použitý vektor útoku), existuje veľká šanca, že sa pokúsi rozšíriť na čo najviac počítačov, čo môže mať vplyv na všetky firemné operácie. Obmedzenie počtu počítačov, na ktoré môže mať útočník dosah z jedného vstupného bodu, má teda v rámci obrannej stratégie jednoznačne veľké výhody. Existuje niekoľko prístupov k zavedeniu takejto stratégie, najmä segmentácia siete.

Diskusia o architektúre siete nie je predmetom tohto dokumentu, no rozdelenie širokej a ľahko preniknuteľnej „plochej" siete do segmentov môže byť náročné a nákladné (zaujímavý pohľad ponúka táto *správa spoločnosti KPMG*). Každá organizácia však musí poznať silné a slabé stránky svojej súčasnej sieťovej architektúry z hľadiska bezpečnosti. Toto poznanie môže zlepšiť jednoduchý audit založený na rozhovore, pri ktorom sa budú klásť otázky ako „Môžem sa dostať odtiaľto tam?" alebo „Čo bráni niekomu dostať sa odtiaľ sem?".

Pokiaľ ide o architektúru systému, v posledných rokoch je obľúbenou stratégiou presun údajov do cloudu. Cloud však neposkytuje automatickú imunitu proti ransomvérovým útokom (hoci menej svedomití dodávatelia sa snažia vytvoriť dojem, že cloud je synonymom bezpečnosti). V skutočnosti sa cloud vďaka nízkym nákladom a relatívnej jednoduchosti, s akou možno v cloude vytvoriť nové servery a pripojiť ich k zvyšku digitálnej infraštruktúry organizácie, stal živnou pôdou pre zločincov. Je zrejmé, že každé použitie cloudu ktoroukoľvek časťou organizácie musí byť riadne autorizované a bezpečne nakonfigurované. Rovnako ako na všetky ostatné systémy, aj na tie v cloude sa musí uplatňovať vhodný režim zálohovania a obnovy.

BEZPEČNOSTNÉ ZÁPLATY A ZÁLOHOVANIE AKO OBRANA PROTI RANSOMVÉRU

Bezpečnostné záplaty a zálohovanie sú dva aspekty prevádzky a správy systémov, ktoré zohrávajú dôležitú úlohu pri obrane proti útoku ransomvérom. Oprava systémov pomocou bezpečnostných záplat uzatvára potenciálne cesty útoku a môže zabrániť preniknutiu ransomvéru do vašej organizácie alebo, v prípade úspešného útoku, zmierniť škody, ktoré môže spôsobiť.

Samozrejme, ako už vie každý správca systému, oprava môže byť oveľa komplikovanejšia, než sa zdá. Bezpečnostné záplaty a aktualizácie sa musia pred nasadením otestovať. Niektoré firemné systémy môžu mať softvérové závislosti, ktoré sa prechodom na najnovšiu verziu aplikácie alebo operačného systému zrušia. Vysoká cena za to, že ransomvér prenikne do vašej siete, však odôvodňuje úsilie riešiť problémy a dodržiavať režim okamžitých a dôsledných opráv s cieľom zabrániť ransomvéru dostať sa do siete.

Často sa hovorí, že ak ransomvér prenikne do vašej organizácie – či už prostredníctvom RDP, e-mailu, dodávateľského reťazca softvéru alebo človeka zvnútra, komplexný a riadne spravovaný program zálohovania a obnovy je dôležitým obranným mechanizmom a má zásadný význam pre vaše úsilie obnoviť systémy.

Na tomto tvrdení je veľa pravdy a existuje mnoho dobrých dôvodov, prečo takýto program zaviesť, ale nezabúdajte, že niektoré útoky ransomvérom prebiehajú dlhší čas, počas ktorého môže dôjsť aj k jeho zálohovaniu, čo ohrozuje možnosť bezproblémového obnovenia. Zálohovanie preto nie je obranou, ktorú stačí len nastaviť a o viac sa nestarať, ale je potrebné ho monitorovať a spravovať, pričom proces obnovy sa musí pravidelne testovať.

V súčasnosti existuje viac možností zálohovania a obnovy ako kedysi, najmä cloudové úložisko, či už vzdialené, lokálne alebo hybridné. Existuje však aj viac údajov, ktoré treba zálohovať, a to z viacerých miest. Pokiaľ nemáte vytvorenú komplexnú stratégiu zálohovania, vždy je tu šanca, že šíritelia ransomvéru nájdu to jedno zariadenie, ktoré ste nezálohovali.

Podľa odborníkov na zálohovanie zo spoločnosti Xopero, ktorá je členom *ESET Technologickej aliancie*, komplexná záloha zahŕňa údaje a stav systému na všetkých koncových zariadeniach, serveroch, e-mailových schránkach, sieťových diskoch, mobilných zariadeniach a virtuálnych počítačoch.

Podrobná diskusia o firemnej stratégii zálohovania a obnovy nie je predmetom tohto informačného dokumentu, ale malo by byť jasné, že mať takúto stratégiu je dôležitejšie ako kedykoľvek predtým. Ransomvér je jedným z mnohých dôvodov, prečo by vaša organizácia nemala šetriť na tejto časti IT programu. Existuje však niekoľko špecifických varovaní týkajúcich sa ransomvéru. Napríklad keď je úložisko „vždy zapnuté“, jeho obsah môže byť zraniteľný voči ransomvéru rovnako ako lokálne či iné úložisko pripojené k sieti.

Ak chcete zabrániť preniknutiu ransomvéru, vyberte si vzdialené úložisko, ktoré:

- nie je bežne a trvalo online,
- chráni zálohované údaje pred automatickou a tichou úpravou alebo prepísaním malvérom, keď je vzdialené zariadenie online,
- chráni predchádzajúce generácie zálohovaných údajov pred kompromitáciou, takže aj keď sa niečo stane s najnovšou zálohou, môžete získať späť aspoň niektoré údaje vrátane skorších verzií aktuálnych údajov, a
- chráni zákazníka tým, že stanovuje právne/zmluvné povinnosti poskytovateľa v prípade, že tento ukončí svoju činnosť a podobne.

Pri archivácii údajov nepodceňujte ani užitočnosť médií na jednorazový zápis. Súbory uložené na médiách, ktoré sa nedajú prepisovať, sú imúnne proti útokom ransomvérom.

Samozrejme, existuje mnoho ďalších dôvodov, prečo vaša organizácia potrebuje program zálohovania a obnovy, napríklad na obnovenie údajov po požiari, povodni, víchrici atď.

REAKCIA NA ÚTOK RANSOMVÉROM

Okrem budovania obrany proti ransomvéru musí byť každá organizácia pripravená reagovať na akýkoľvek útok, ktorému sa podarí preniknúť cez túto obranu. Základom tejto prípravy je aktualizácia bezpečnostných politík spoločnosti tak, aby zahŕňali ransomvér. Musíte spresniť, ako by mali zamestnanci na všetkých úrovniach reagovať na požiadavky ransomvéru. Uistite sa, že vaše politiky odpovedajú na tieto otázky:

- Komu majú zamestnanci nahlásiť podozrenie na ransomvér?
- Aké sú zásady spoločnosti, pokiaľ ide o platenie výkupného pri útoku ransomvérom?
- Kto je oprávnený zaplatiť výkupné alebo o ňom vyjednávať? Politiky by mali byť vytvorené tak, aby sa zabránilo
  nasledujúcim problémom:
  - zamestnanci nenahlasujú podozrenie na ransomvér, pretože sa obávajú trestu,
  - správcovia siete zaplatia výkupné, pretože je to jednoduchšie ako obnoviť systémy zo záloh,
  - neoprávnené zverejňovanie informácií o skutočných útokoch ransomvérom alebo podozreniach na ne.
- Aké kroky je organizácia povinná podniknúť v prípade úniku údajov?
- Aké sú zásady spoločnosti, pokiaľ ide o vypnutie napadnutých počítačov? Kto prijíma toto rozhodnutie? Vypnutím počítačov odstránite potenciálne dôkazy uložené v pamäti a môže sa to považovať za porušenie predpisov.

Po aktualizácii politík informačnej bezpečnosti tak, aby pokrývali aj ransomvérové útoky, sa musíte uistiť, že vaše programy na zvyšovanie povedomia o bezpečnosti a školenia zamestnancov zahŕňajú náležité informácie o ransomvéri.

Takisto by ste sa mali uistiť, že pre prípad útoku ransomvérom máte pripravené plány obnovy po strate dát či zlyhaní systémov a reakcie na krízové situácie/incidenty. Nižšie uvádzame prehľad oblastí, ktorý musí váš plán reakcie pokrývať:

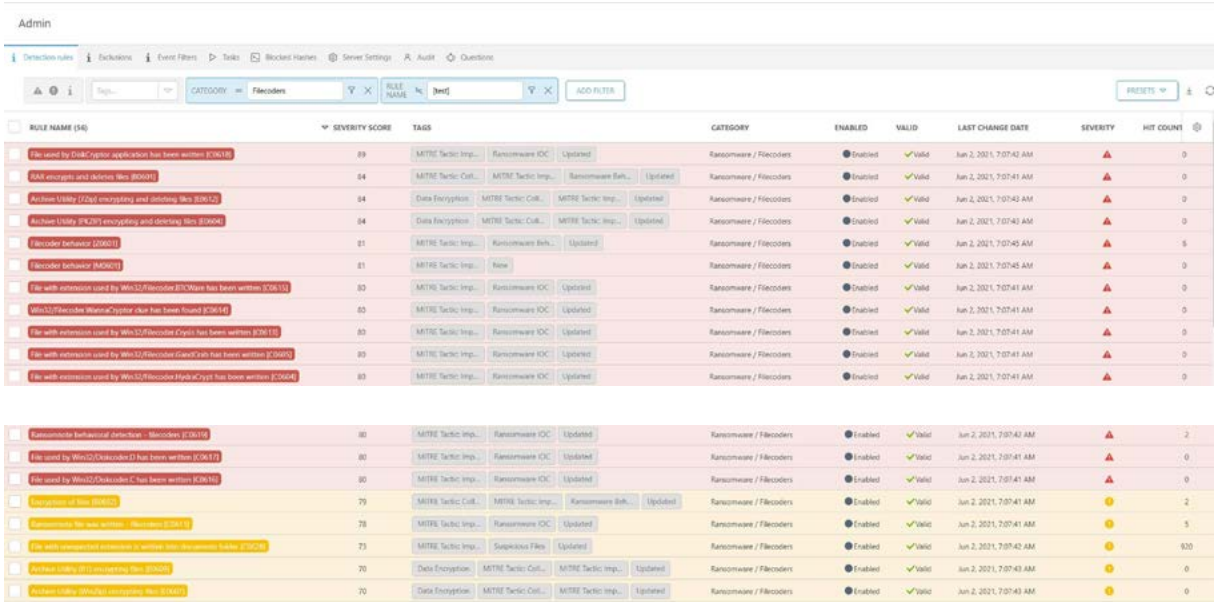
- Pri prvých príznakoch útoku informujte určený personál.
- Izolujte a analyzujte zasiahnuté počítače.
- Vypnite napájanie: ak napadnuté počítače nie je možné izolovať, vytvorte obraz systému a pamäte a potom ich vypnite, aby ste zabránili ďalšiemu šíreniu ransomvéru.
- Po potvrdení útoku zalarmujte tím pre riešenie incidentov/krízových situácií.
- Upozornite právneho poradcu.
- Kontaktujte dodávateľov, ktorí by vám vedeli pomôcť.
- Pripomeňte zamestnancom politiky týkajúce sa tlače a sociálnych médií.
- Posúďte rozsah útoku a špecifiká ransomvéru (napr. či je k dispozícii kľúč).
- Kontaktujte orgány presadzovania práva.
- Pripravte vyhlásenie.
- Ak boli súbory zašifrované, zistite, či ich možno obnoviť zo zálohy.
- Priebežne informujte zamestnancov o stave.
- V prípade potreby aktivujte plán na zabezpečenie kontinuity podnikania.
- Zhromaždite príslušné protokoly a možné indikátory kompromitácie, ako sú binárne súbory, požiadavky na výkupné, IP adresy, položky databázy Registry alebo iné súbory.
- Zdokumentujte počiatočné vyšetrovanie útoku a kroky prijaté na nápravu.

Odporúčame mať v príručke krízového plánovania aspoň jeden scenár útoku ransomvérom a prejsť si ho v rámci simulačných cvičení s príslušnými zamestnancami vrátane vedúcich pracovníkov. Môžete tak odhaliť nedostatky v plánoch zálohovania a obnovy a pomôže vám to predvídať dôsledky v prípade, že z dôvodu zašifrovaných systémov nebudete mať prístup k základným službám (e-mail, telefóny VoIP, prístup na internet).

DETEKCIA A REAKCIA NA ÚTOKY NA KONCOVÉ ZARIADENIA (EDR)

Existuje jedna kategória bezpečnostného softvéru, ktorá môže pomôcť obmedziť vplyv útokov ransomvérom a posilniť reakciu na ne: nástroje na detekciu a reakciu na útoky na koncové zariadenia, skrátene EDR. Nástroje EDR, ktoré sú dostupné buď ako súbor interne vyvinutých nástrojov, alebo ako integrovaný bezpečnostný produkt, možno využiť pri manuálnom vyhľadávaní hrozieb vo vašich sieťach, ako aj automatizácii širokej škály obranných opatrení.

Na obrázku 6 môžete vidieť niekoľko pravidiel EDR súvisiacich s ransomvérom, ktoré slúžia na to, aby boli bezpečnostní pracovníci upozornení na podozrivú aktivitu (tento konkrétny nástroj EDR je *ESET Enterprise Inspector*).



Obrázok 6 // Riadiaci panel nástroja ESET Enterprise Inspector s pravidlami súvisiacimi s ransomvérom

Nástroj EDR dokáže monitorovať všetky firemné koncové zariadenia na prítomnosť anomálií a podozrivých aktivít, ako je napríklad zmena prípon súborov, ktorá je typická pre útok ransomvérom. Váš bezpečnostný tím by určite chcel byť upozornený na prítomnosť útočných nástrojov, ako je Mimikatz, ktorý je určený na krádež prihlasovacích údajov používateľov z pamäte, alebo Cobalt Strike Beacon, ktorý útočníci často používajú na preniknutie do systému a vzdialené vykonávanie príkazov.

Včasné varovné signály narušenia môžu byť zakódované do pravidiel a výstrah. Tie sa dajú priebežne spresňovať na základe čerstvých údajov zo zdrojov informácií o hrozbách, ako sú zoznamy indikátorov kompromitácie (IOC). Dobrý nástroj EDR bude mať pravidlá, ktoré operátorovi umožnia nájsť kompromitované systémy okamžite po spustení pravidla, izolovať ich a potom diagnostikovať problém vrátane vrátenia histórie príkazov, ktoré vykonali napadnuté systémy. Vďaka týmto funkciám môže nástroj EDR zvýšiť schopnosť vášho bezpečnostného tímu zabrániť útokom, reagovať na ne a vykonávať forenznú analýzu po útoku.

PÁR SLOV O PLATENÍ VÝKUPNÉHO

Tie slová sú: nerobte to. Prečo? Pretože *zaplatiť zločincovi, ktorý zašifroval vaše súbory, znamená*:

- potvrdiť účinnosť obchodného modelu použitého pri zločine,
- podporovať ďalšiu trestnú činnosť,
- umožniť ransomvérovým gangom skúmať zero-day zraniteľnosti a vyvíjať nové exploity,
- možnosť stať sa terčom budúcich útokov a ďalšieho vymáhania peňazí.

Okrem toho zaplatenie výkupného zločincom, ktorí zašifrovali vaše súbory, v žiadnom prípade nezaručuje, že dostanete dešifrovací kľúč; koniec koncov, nemôžete ich predsa dať na súd alebo nahlásiť obchodnej inšpekcii. Existuje mnoho dôvodov, prečo ani po zaplatení nemusíte získať svoje súbory späť:

- niektoré údaje sa mohli pri šifrovaní poškodiť, a preto sa nedajú obnoviť,
- nástroj na dešifrovanie môže byť dodaný spolu s iným malvérom, nemusí fungovať správne alebo je dešifrovanie oveľa pomalšie ako obnovenie zo záloh,
- existuje mnoho spôsobov, ako môže proces poskytnutia dešifrovacieho kľúča zlyhať,
- útočník koná so zlým úmyslom a *nemá v pláne poskytnúť dešifrovacie kľúče*.

Tieto informácie by mali byť dostatočné na to, aby organizácie odradili od platenia výkupného. Aby sme však tomuto odporúčaniu dodali väčšiu váhu, uvádzame aj, čo o platení výkupného *hovorí* FBI: „Zaplatenie výkupného nezaručuje organizácii, že dostane svoje údaje späť – zaznamenali sme prípady, keď organizácie po zaplatení výkupného nikdy nedostali dešifrovací kľúč. Zaplatenie výkupného nielenže dodá súčasným kybernetickým zločincom odvahu, aby sa zamerali na ďalšie organizácie, ale motivuje aj ostatných zločincov, aby sa zapájali do takýchto nelegálnych činností. A napokon, zaplatením výkupného môže organizácia neúmyselne financovať inú *nezákonnú činnosť týchto zločincov*."

Zdá sa, že v praxi existujú dva argumenty pre zaplatenie výkupného, pričom prvým je, že firma „nemôže obnoviť zašifrované informácie zo záloh". Dôvodom môže byť to, že zálohy neexistujú, alebo ak existujú, tak sú neúplné alebo nejakým spôsobom poškodené. Môžu však existovať alternatívy k zaplateniu výkupného. Takže skôr ako sa rozhodnete poslať útočníkom peniaze, overte si u svojho dodávateľa bezpečnostného softvéru: a) či nejde o jednu zo zriedkavých situácií, keď je k dispozícii nástroj na dešifrovanie, ktorý umožňuje obnovu údajov bez zaplatenia výkupného; a b) či nejde o variant ransomvéru, o ktorom je známe, že po zaplatení výkupného nebudú alebo nemôžu byť údaje obnovené.

Druhým častým argumentom pre zaplatenie výkupného je, že „je to lacnejšie ako obnovenie zo záloh". Ak sa počíta len čas a práca, potom toto tvrdenie môže byť technicky správne. Avšak zaplatenie výkupného je napriek tomu veľkou chybou, a to z dôvodov uvedených vyššie, najmä: nemožnosť spoľahnúť sa na prísľub, že údaje budú dešifrované, pravdepodobnosť ďalšieho útoku po prvej platbe (predsa len nemáte do činenia so slušnými občanmi dodržiavajúcimi zákony) a podporovanie trestného konania, čím zvyšujete pravdepodobnosť ďalších útokov aj na ostatných.

Možno ste počuli, že niektorí šíritelia ransomvéru ponúkajú obetiam dôkaz, že dešifrovanie funguje. To sa síce stáva, ale môže to viesť k ešte väčším problémom. Predpokladajme, že útočníci si od vás nechajú poslať zašifrovaný súbor, ktorý potom dešifrujú a pošlú vám ho späť ako dôkaz dobrej vôle – nielenže ste práve osobám s pochybnou morálkou uľahčili zverejnenie obsahu tohto súboru, ale navyše ste sa v prípade, že by boli v týchto údajoch obsiahnuté akékoľvek osobné informácie, pravdepodobne dopustili trestného činu podľa jedného alebo viacerých prísnych vnútroštátnych a regionálnych zákonov o ochrane osobných údajov.

Majte tiež na pamäti, že odstránenie aktívneho ransomvéru pomocou bezpečnostného softvéru nie je v žiadnom prípade to isté ako obnovenie údajov. Ak odstránite ransomvér a následne sa rozhodnete zaplatiť výkupné, údaje už nemusí byť možné obnoviť ani v spolupráci so zločincami, pretože dešifrovací mechanizmus býva často súčasťou malvéru. Inými slovami, ak sa rozhodnete zaplatiť, postupujte opatrne.

BUDÚCNOSŤ RANSOMVÉRU

Požadovanie peňazí za obnovenie prístupu k systémom a údajom je útokom na aspekt dostupnosti z klasickej bezpečnostnej trojice CIA – confidentiality (dôvernosť), integrity (integrita) a availability (dostupnosť). Ransomvér v podstate využíva závislosť organizácie od technológií, takže čím viac sú od nich organizácie závislé, tým väčší priestor má ransomvér k dispozícii. To znamená, že môžeme očakávať, že ransomvér v budúcnosti nepoľaví a bude sa vyvíjať (ak nedôjde k nepredvídaným zmenám v globálnej politike a ekonomike).

Na základe našich skúseností so škodlivým kódom od konca 80. rokov môžeme povedať, že hrozby malvéru majú tendenciu vyvíjať sa takto:

- v novej technológii sa objavia zraniteľnosti a diskutuje sa o jej potenciáli zneužitia na kriminálne účely,
- začína sa úsilie o nápravu a zmiernenie týchto zraniteľností,
- pokusy o zneužívanie najnovších technológií na kriminálne účely sú spočiatku zriedkavé, pretože zločincom prinášajú ľahko zarobené peniaze osvedčené stratégie,
- ak nedôjde k rozsiahlemu trestnému zneužitiu, v úsilí o nápravu a zmiernenie sa postupne poľavuje,
- nakoniec zločinci zistia, že táto „nová" technológia je pripravená na zneužitie,
- objaví sa nový trend v oblasti malvéru.

Medzi príklady patria distribuované útoky odmietnutia služby (DDoS), ktoré využívajú zariadenia na sledovanie pripojené k internetu (Mirai) a malvér zacielený na router (VPNFilter). Pokiaľ ide o ransomvér, prudký nárast v zavádzaní slabo zabezpečených zariadení internetu vecí (IoT) vytvára živnú pôdu pre budúce útoky, rovnako ako rastúce využívanie priemyselných riadiacich systémov pripojených k internetu, inteligentných budov a vozidiel vrátane autonómnych vozidiel (pozri článok *RoT: ransomvér vecí* a webový seminár *Temná stránka ransomvéru*).

Ak pokles výnosov z tradičnejšej kybernetickej kriminality privedie zločincov k využívaniu nových schém, je pravdepodobných niekoľko scenárov. Malvér na routeroch by mohol potenciálne obmedziť alebo zablokovať komunikáciu, pokiaľ nezaplatíte poplatok, a v prípade pokusu o odstránenie malvéru by mohol hroziť zablokovaním routera alebo odhalením obsahu komunikácie.

Diaľkové uzamykanie vozidiel, domov a budov by sa mohlo zneužiť na vydieranie. Manipulácia so systémami na automatizáciu budov, ktoré dokážu ovládať prístup do budov, kúrenie, vetranie a klimatizáciu, by mohla byť základom vydieračských schém, pričom *náznaky takéhoto konania vidíme už teraz*. Pokiaľ ide o komerčné roboty, uskutočniteľnosť útokov ransomvérom na ne už bola preukázaná.

Tieto scenáre súvisiace s vyvíjajúcim sa ransomvérom majú pre podniky mnohonásobné dôsledky. Odporúčajú sa tieto reakcie:

- Začnite sa vo svojej stratégii riadenia rizík a plánovaní zameriavať na tieto potenciálne hrozby.
- Začnite sa už teraz zaoberať aktívami, za ktoré možno požadovať výkupné: zariadenia IoT, routery SOHO, roboty, riadiace systémy, autonómne systémy.
- Sledujte správy o bezpečnostných zraniteľnostiach súvisiacich s týmito aktívami.
- Majte prehľad o bezpečnostných záplatách a aktualizáciách firmvéru pre tieto aktíva.
- Izolujte zariadenia IoT a ďalšie nové technológie od produkčných sietí.

ZÁVER

Z údajov, techník a reálnych prípadov v tomto dokumente vyplýva, že ransomvér sa skutočne stal kybernetickou hrozbou súčasnosti. Jeho vzostup možno z veľkej časti pripísať vývoju techniky dvojitého vydierania (alebo doxingu), ktorej priekopníkom bol v roku 2019 dnes už neexistujúci gang Maze. Členovia tejto neslávne známej ransomvérovej skupiny nielenže zašifrovali svojim obetiam zariadenia, ale ukradli im aj ich najcennejšie a najcitlivejšie údaje a vyhrážali sa ich zverejnením.

Ostatní autori ransomvéru sa nimi čoskoro inšpirovali a ďalej stavali na tomto účinnom dvojitom vydieraní. Zaviedli nové metódy, ktoré sa zameriavali nielen na údaje obetí, ale aj na ich webové stránky, zamestnancov, obchodných partnerov a zákazníkov, čím sa zvyšoval tlak, a teda aj ochota zaplatiť.

Ransomvérové gangy využili chaos a neistotu, ktoré priniesla pandémia, a začali hrubou silou prenikať do sietí cez RDP, ktorý sa nakoniec stal jedným z hlavných vektorov útoku. *Malspamové* kampane doručujúce škodlivé makrá, nebezpečné odkazy a binárne súbory botnetov však nezmizli a okrem miliárd pokusov o uhádnutie hesiel boli potenciálne obete vystavené aj intenzívnym útokom.

Vzhľadom na zvýšenú účinnosť techník vydierania a nové distribučné kanály sa odhaduje, že na účtoch týchto technicky zdatných kybernetických zločincov skončili stovky miliónov dolárov, čo im umožnilo vybudovať obchodný model ransomvéru ako služby a získať množstvo nových partnerov. Niektoré gangy, oslobodené od „špinavej práce“, začali získavať zero-day zraniteľnosti a kupovať ukradnuté prihlasovacie údaje, čím ďalej rozširovali okruh potenciálnych obetí.

Rastúci počet ransomvérových incidentov nepriamo spojených s útokmi na dodávateľský reťazec predstavuje ďalší znepokojujúci trend, ktorý môže naznačovať, akým smerom sa budú tieto gangy uberať v budúcnosti.

Keďže ransomvérovým gangom zvyčajne nechýbajú peniaze, ambície ani odhodlanie, je nevyhnutné, aby sa každý odborník v oblasti IT a bezpečnosti poučil z odstrašujúcich príbehov a analýz, o ktorých denne informujú médiá. Od začiatku roka 2020 sa opakovane ukázalo, že vynútené politiky, správna konfigurácia a silné heslá v kombinácii s viacúrovňovým overovaním môžu byť rozhodujúce v boji proti ransomvéru. Mnohé z incidentov uvedených v tomto dokumente takisto zdôraznili dôležitosť včasného nasadenia bezpečnostných záplat, keďže známe zraniteľnosti patria medzi hlavné vektory týchto gangov.

Na obranu pred zero-day zraniteľnosťami, botnetmi, spamom šíriacim malvér (malspam) a inými technicky pokročilejšími technikami sú potrebné ďalšie bezpečnostné technológie: viacvrstvové riešenie na ochranu koncových zariadení, ktoré dokáže odhaliť a blokovať prichádzajúce hrozby v e-mailoch, odkazoch, RDP a iných sieťových protokoloch, a nástroje na detekciu a reakciu na útoky na koncové zariadenia, ktoré monitorujú, identifikujú a izolujú anomálie a náznaky škodlivej činnosti vo firemnej infraštruktúre.

Nové technológie, hoci sú pre spoločnosť prínosom, ponúkajú kybernetickým zločincom čoraz viac príležitostí na útok. Dúfajme, že tento dokument, v ktorom vysvetľujeme, akú vážnu hrozbu predstavuje ransomvér a ako sa proti nemu brániť, pomôže zaistiť spoločnosti tieto prínosy a zároveň minimalizovať škody spôsobené útočníkmi.

O SPOLOČNOSTI ESET

Už viac ako 30 rokov spoločnosť ESET® vyvíja popredný softvér a služby zamerané na IT bezpečnosť a ochranu podnikov, kritickej infraštruktúry a domácností z celého sveta pred čoraz sofistikovanejšími digitálnymi hrozbami. V rámci širokej škály riešení zameraných na ochranu koncových a mobilných zariadení, šifrovanie či viacúrovňové overovanie prináša ESET svojim zákazníkom vysokovýkonné a zároveň jednoducho použiteľné produkty, ktoré chránia používateľov bez zbytočného rušenia 24 hodín denne, pričom ochranné mechanizmy sa aktualizujú v reálnom čase, aby boli používatelia vždy v bezpečí a bola zaistená plynulá prevádzka firmy. Keďže hrozby sa neustále vyvíjajú, na svojom vývoji musí pracovať aj spoločnosť zameraná na IT bezpečnosť, ktorá chce napomáhať k bezpečnému používaniu technológií. Na tomto cieli a podpore lepšej spoločnej budúcnosti pracuje spoločnosť ESET prostredníctvom svojich centier výskumu a vývoja v rôznych kútoch sveta. Viac informácií nájdete na stránke www.eset.sk, prípadne nás môžete sledovať na sociálnych sieťach *LinkedIn*, *Facebook* a *Twitter*.

Digital Security
Progress. Protected.