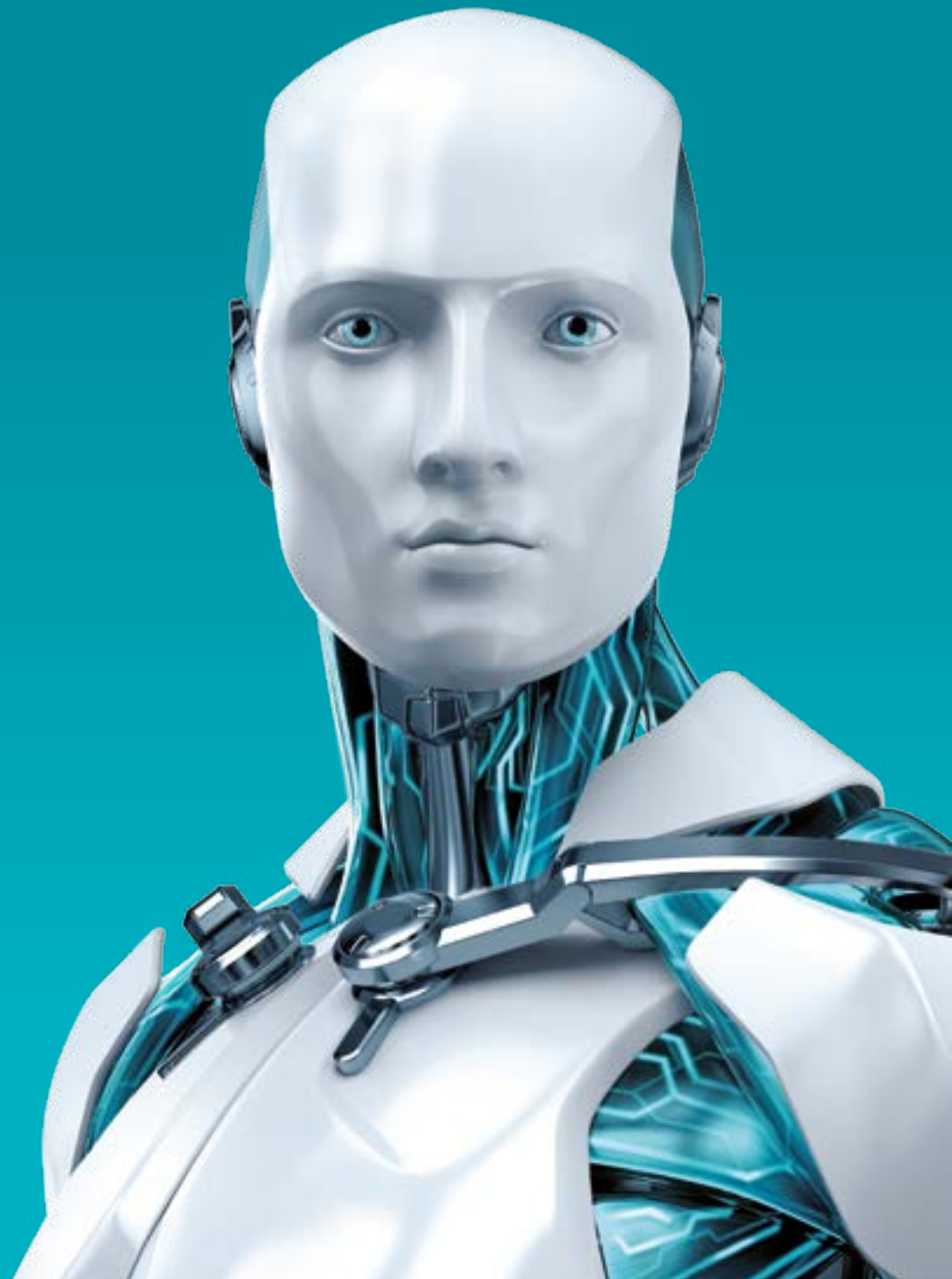
Filecodery

[Ransomware]

Dvojitá prevencia a liečba



UŽÍVAJTE SI BEZPEČNEJŠIE TECHNOLÓGIE™

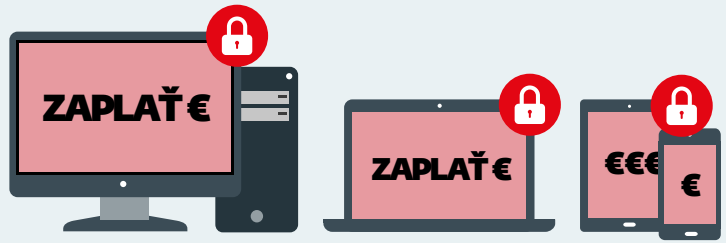
Obsah

Úvod

Filecodery sú kategóriou ransomwaru, ktorá pri infekcii zašifruje obsah zariadenia a za jeho odblokovanie požaduje výkupné. Vo firme alebo organizácii sa dokáže rozšíriť do niekoľkých zariadení a takýmto spôsobom spomalí alebo zablokuje jej štandardný chod. Niektoré Filecodery sa totiž dokážu šíriť už aj ako červy. Pred infekciou týmto typom škodlivého kódu sa však dá účinne brániť. Keďže ESET zaznamenal v poslednom období viacero prípadov úspešných útokov na Slovensku, rozhodli sme sa vytvoriť tento komplexný návod vysvetľujúci, ako sa pred infekciou chrániť a aké sú možnosti jej liečby.

Účinná prevencia

Rovnako ako pri vašom zdraví platí, že prevencia je lacnejšia, než samotný liečba. Pri Filecoderoch je totiž vysoká pravdepodobnosť, že sa ich nezbavíte a stratíte tým pádom všetky informácie uložené na infikovanom zariadení alebo na sieťových diskoch prístupných užívateľovi infikovaného zariadenia. Pamätajte, že útočníci môžu používať rovnako kvalitné šifrovanie ako banky snažiace sa ochrániť finančné transakcie svojich klientov.



Ransomware je typ škodlivého softvéru, ktorý dokáže uzamknúť vaše zariadenie a k súborom v ňom sa správa ako k rukojemníkom.

Malware je častokrát šírený e-mailom alebo drive-by-downloadom z kompromitovaných webstránok. Po dokončení svojej záškodnej činnosti vygeneruje ransomware správu s oznamom, aby ste zaplatili.

Prejdite na vyššiu verziu vašej ESET ochrany

V posledných mesiacoch sa nám stalo, že ESET poprosili o konzultáciu ohľadom infekcie Filecoderom aj spoločnosti, ktoré dlhodobo využívali našu ochranu. Pri analýze sme však zistili, že používali aj niekoľko rokov starú verziu bezpečnostného softvéru, napríklad verziu 3 alebo verziu 4. Prípadne, že neboli chránené všetky zariadenia v sieti. Všetkým zákazníkom preto odporúčame prechod na najnovšiu šiestu generáciu našich riešení pre firmy, ktorá obsahuje technológie ako Pokročilú kontrolu pamäte a Exploit Blocker. Tieto novo navrhnuté ESET algoritmy posilňujú ochranu proti vírusom, ktoré boli navrhnuté tak, aby sa vyhýbali odhaleniu bezpečnostným softvérom napríklad aj použitím šifrovania.

Ak ste majiteľom platnej licencie na ESET riešenia, prechod na novšiu verziu je ich súčasťou a je teda bezplatný.

V prípade, že by bol vo vašom firemnom prostredí prechod na šiestu generáciu ESET ochrany výrazným zásahom do plánovanej práce IT oddelenia, prípadne máte tento upgrade naplánovaný na neskoršie obdobie, prejdite aspoň na piatu generáciu, ktorá je technicky podobná štvrtej a tretej, obsahuje však aj ESET Live Grid a boli do nej spätne pridané špeciálne ochranné technológie ako Pokročilá kontrola pamäte a Exploit Blocker.

Návod ako prejsť na najnovšiu verziu ESET Endpoint riešení nájdete na našom webe v článku: *Ako môžem vzdialene inštalovať na klientske počítače pomocou ESET Remote Administrator? (6.x)*

Informáciu o ESETom poskytovanej platenej službe Pomoc pri inštalácii nájdete na webe: *ESET Inštalačná služba*

Návod ako zapnúť ESET Live Grid v Endpoint riešeniach nájdete v článku: *ESET Live Grid – čo to je a ako ho povolím*

Povoľte ESET Live Grid

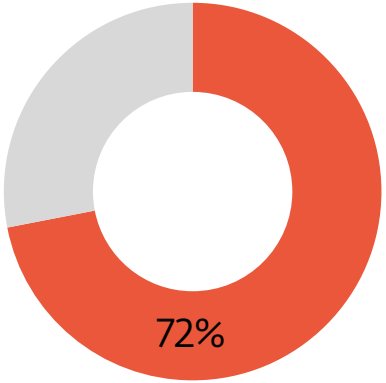
Každý deň vyjde niekoľko nových variantov alebo rovnakého šifrovacieho malwaru. Niekoľkokrát denne pridávame do aktualizácií vírusovej databázy novo vyskytujúce mutácie. Doplnenie tejto informácie do vírusovej databázy však trvá niekoľko hodín, niektoré mutácie šifrovacieho malwaru majú preto vyššiu šancu infikovať váš systém. Ak však máte vo svojej ESET ochrane zapnutú funkciu ESET Live Grid, dokáže na novo vzniknuté hrozby reagovať oveľa skôr, a to v priebehu len niekoľkých minút. Ide o veľmi podstatnú ochrannú zložku nášho softvéru, všetkým zákazníkom preto odporúčame mať túto funkciu zapnutú.

Live Grid dokáže v porovnaní s aktualizáciou vírusovej databázy oveľa skôr označiť škodlivý súbor. Niektoré procesy, napríklad sťahovanie spustiteľného súboru zo siete, dokážu v našom programe vyvolať okamžitú otázku na Live Grid, či je tento súbor bezpečný. Taktiež efektívnejšie distribuuje informácie o blokovaných škodlivých linkách a nemusí čakať na informáciu z aktualizácie vírusovej databázy.

Taktiež agresívnejšie blokuje procesy Filecoderov. Ak podľa whitelistingu daný proces nie je bezpečný, okamžite ho zablokuje. Napríklad ak sa nejaký proces snaží zmazať zálohu, čo sa pokúšajú robiť aj Filecodery. Je dôležité podotknúť, že Live Grid nám zasiela hashe podozrivých súborov, nikdy však ich obsah. Vaše súkromie tým pádom nenarušuje. Defaultne sa na diagnostiku nezasielajú súbory *.doc/docx, *.rtf, *.xls/xlsx,* .dbf, *.mdb, *.sxw, *.sxc, *.dot, *.xlt, *.ppt, *.pot, *.pps.

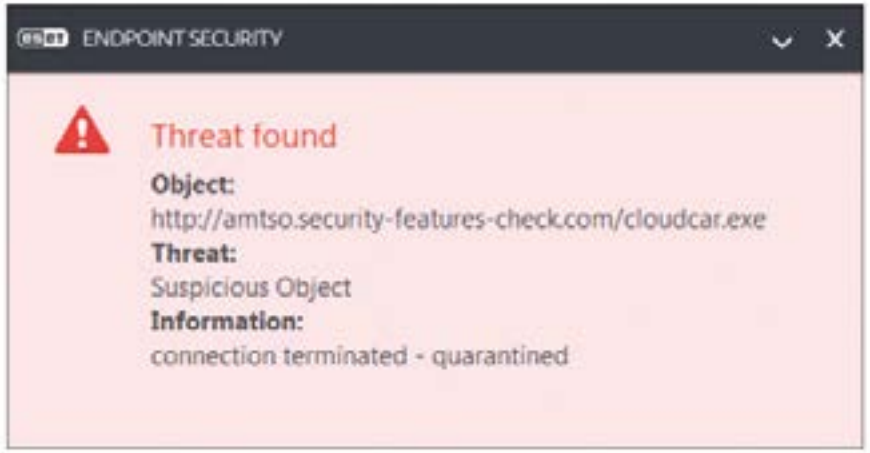
Po zapnutí ESET Live Gridu overte, či naozaj funguje správne. Je totiž možné, že váš vlastný firemný firewall zablokuje komunikáciu Live Gridu. Pre otestovanie prejdite na túto stránku renomovanej organizácie AMTSO, ktorej je ESET členom:

http://www.amtso.org/feature-settings-check-cloud-lookups/



Percentuálne vyjadrenie počtu infikovaných zákazníkov, ktorí nemali zapnutý ESET Live Grid.

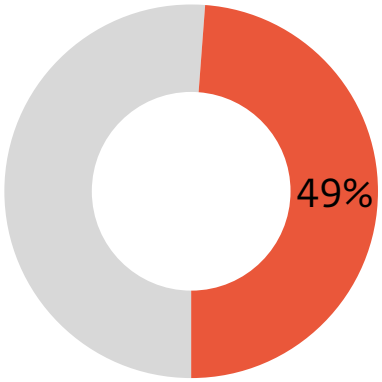
Následne kliknite na odkaz „Download the CloudCar Testfile" a stiahnite testovací súbor *cloudcar.exe*. Ak ESET Live Grid funguje správne, sťahovaný súbor sa otvorí na internetových serveroch ESET a na základe spätne získaných informácií bude zablokovaný. Nebude uložený do počítača. Zároveň sa na monitore zobrazí upozornenie o zablokovaní hrozby:



Neopomínajte aktualizácie programov a operačného systému

Okrem vypnutého Live Gridu majú Filecodermi infikované zariadenia ďalšiu častú spoločnú vlastnosť: ich operačným systémom je Windows XP. Microsoft tomuto systému od 8. apríla 2014 neposkytuje aktualizácie, jeho zabezpečenie je tým pádom zastaralé. Pokiaľ preto nemáte závažný dôvod na zotrvanie pri Windows XP, prejdite na novšiu verziu operačného systému, na ktorý Microsoft stále vytvára bezpečnostné záplaty. Napriek tomu, že ESET bude Windows XP podporovať minimálne do roku 2017, nepovažujeme používanie tohto operačného systému za najbezpečnejšiu voľbu.

Určite nezabúdajte pravidelne aktualizovať aj ostatný softvér používaný vo vašej firme alebo organizácii, akým je napríklad balíček Microsoft Office, PDF čítačky a internetové prehliadače.



Percentuálne vyjadrenie počtu infikovaných zákazníkov, ktorí používali Windows XP.

Zálohovanie

Ak by ste chceli dostať tip na jedinú zaručenú vec, ktorá dokáže vyhrať nad Filecodermi, bude to určite zálohovanie. Ak sa váš zamestnanec stane obeťou takéhoto malwaru, možno stratí dokumenty, na ktorých pracoval v deň útoku, všetky zvyšné však budete vedieť obnoviť. Pamätajte, že Filecodery dokážu zašifrovať aj všetky namapované disky. Taktiež akékoľvek pripojené externé pamäťové jednotky ako napríklad USB kľúče alebo akékoľvek sieťové alebo cloudové súborové úložiská alebo pripojené disky, ktoré ste namapovali. Potrebujete si teda vytvoriť pravidelné zálohovacie návyky, či už to bude zálohovanie na externé disky alebo využijete zálohovaciu službu. Pamätajte však, že sa musia automaticky odpájať od zariadenia, ak práve nezálohujú. Inak hrozí, že aj ich zašifruje Filecoder.

Zobrazte skryté súborové prípony

Filecoder sa k vám môže dostať v súbore, ktorý je pomenovaný napríklad príponou .PDF.EXE, počíta teda s nechcenou pomocou Windowsu, ktorý defaultne ukrýva známe súborové prípony. Nezaškolený zamestnanec môže dostať správu s prílohou Nove_nastavenie_platov.pdf, v skutočnosti to však môže byť spustiteľný súbor **Nove_nastavenie_platov.pdf.exe**.

Filtrujte .EXE súbory v e-mailoch

Ak má váš gatewayový mail skener schopnosť filtrovať súbory podľa prípon, nastavte ho tak, aby odmietal e-maily s .EXE príponami, alebo aj správy so súbormi, ktoré majú dve súborové prípony, z ktorých posledná je .EXE (konkrétne „*.*.EXE“). Okrem spustiteľných súborov vám odporúčame zablokovať aj typy súborov ako *.BAT, *.CMD, *.SCR a *.JS. Ak si vaši zamestnanci naozaj potrebujú posielať takéto súbory a vy ich v správach chcete blokovať, môžu ich prijímať alebo posielať zazipované (samozrejme chránené heslom). Stretli sme sa však aj s prípadmi, kedy útočníci posielajú svojej obeti archív (napríklad .RAR, .ZIP alebo .7Z), v ktorom sa nachádza javascriptový súbor (.JS). Obeť si myslí, že po jeho otvorení sa nič nestane. Pravdou však je, že sa do zariadenia buď stiahne a spustí Filecoder zo servera alebo ho daný javascript stiahne na disk z archívu a následne spustí.

Znefunkčnite spustenie súborov v priečinkoch AppData/LocalAppData

V nastaveniach Windowsu (alebo ak používate Intrusion Prevention Software) môžete zamietnuť správanie, ktoré je špecifické pre Filecodery. A to je spúšťanie súborov v priečinkoch App Data alebo Local App Data. Ak máte legitímny dôvod na to, aby sa vám nejaký program spúšťal v App Data, budete mu musieť vytvoriť výnimku z tohto pravidla.

Nezapínajte zbytočne RDP

Škodlivý softvér Filecoder často pristupuje k cieľovým počítačom prostredníctvom protokolu RDP (Remote Desktop Protocol) – RDP je utilita v systéme Microsoft Windows, ktorá umožňuje iným používateľom pristúpiť na diaľku k vášmu počítaču. Ak nepotrebujete túto utilitu, môžete ju vypnúť. Týmto si ochránite počítač pred škodlivým softvérom Filecoder a ostatnými hrozbami, ktoré využívajú protokol RDP.

Minimalizujte riziko vírusového útoku: Venujte sa zamestnancom

Nevypínajte User Account Control (UAC). Neotvárajte podozrivé prílohy ako fax, faktúru, potvrdenku, ktoré majú podozrivý názov alebo tie, ktoré ste nečakali vôbec. Venujte sa vzdelávaniu zamestnancov, obzvlášť tých, ktorí často dostávajú správy z externého prostredia, ktoré môžu obsahovať rôzne prílohy, napríklad personálne a finančné oddelenie. V pravidelných intervaloch môžete uskutočňovať bezpečnostné školenia a kvízy, na ktorých môžete nenúteným spôsobom informovať zamestnancov o tom, akými rôznymi spôsobmi môžu nechtiac infikovať firemné (alebo aj svoje súkromné) zariadenie. Taktiež zamestnancov informujte o postupe čo robiť, ak si všimnú podozrivé správanie na svojom zariadení alebo priamo infekciu.

Viac tipov ako zvýšiť ochranu vašej siete nájdete na našom webe v článku: *Čo mám spraviť, ak chcem minimalizovať riziko vírusového útoku?*

Ich automatickou reakciou pri zbadaní niečoho podozrivého by malo byť okamžité kontaktovanie vášho IT oddelenia a nahlásenie tohto bezpečnostného incidentu.

ESET zároveň poskytuje prostredníctvom divízie ESET Services platené služby v oblasti vzdelávania a šírenia povedomia o informačnej bezpečnosti. Viac informácií je dostupných na stránke: *Školenia*

V prípade Filecoderov máme podozrenie, že zneužívajú makrá v MS Word. Zamestnancovi príde do poštovej schránky správa s prílohou MS Word, ktorá sa otvorí v chránenom zobrazení (Protected View). Samotný dokument však v tomto zobrazení môže obsahovať informáciu, že na zobrazenie celého dokumentu musí používateľ dokumentu povoliť úpravy, čím v ňom spustí makrá. Ich vlastnosťou však je, že sa vedia pripojiť na internet a sťahovať z neho súbory. Informujte o tejto taktike útočníkov svojich zamestnancov. Pri otvorení podozrivej prílohy, ktorá sa zamestnanca snaží naviesť k tomu, aby v dokumente povolil úpravy, by mali kontaktovať vaše IT oddelenie.

AKO SA OCHRÁNIŤ

PRED INFEKCIOU

1. ***Zálohujte*** svoje dáta
2. ***Zobrazte*** skryté súborové prípony defaultne skryté Windowsom
3. ***Filtrujte*** spustiteľné súbory (.exe) v e-mailoch
4. Používajte dôveryhodný ***bezpečnostný softvér***
5. ***Aktualizujte*** svoj softvér
6. ***Vypnite*** Remote Desktop Protocol

AK MÁTE PODOZRENIE

1. ***Odpojte*** sa od internetu a siete
2. Vo Windowse použite ***systém obnovy***
3. Zmeňte čas v ***BIOSe*** na minulosť
4. A obzvlášť: ***neplaťte!***

Firemné zariadenie je infikované, čo mám robiť?

Zariadenie okamžite odpojte od internetu a siete

Ak vy alebo niekto z vašich zamestnancov spustí na svojom zariadení podozrivý súbor alebo si všimne, že niektoré uložené súbory sa zrazu nedajú otvoriť alebo sa vám zobrazí priamo Filecoderová obrazovka, okamžite zariadenie odpojte od internetu, firemnej siete a aj elektrickej siete. Ak budete jednať rýchlo je možné, že zastavíte komunikáciu malwaru s C&C serverom ešte predtým, než dokončí šifrovanie obsahu zariadenia. Zašifrovanie celého obsahu zariadenia totiž istý čas trvá. Máte teda šancu celý proces zastaviť. Táto technika nie je stopercentná ale odpojiť zariadenie od internetu a siete je lepšie, než nespraviť nič.

Kontaktujte technickú podporu ESET, ktorej služby sú súčasťou vašej ESET licencie

V prípade, že vám Filecoder naozaj zašifroval zariadenie a nemáte jeho zálohu, kontaktujte technickú podporu spoločnosti ESET.

Nezabudnite pripojiť aj výstup z ESET Log Collectora a niekoľko vzoriek zašifrovaných súborov, ideálne súborov MS Office v počte okolo päť kusov.

Ak zariadenie ešte nie je kompletne zašifrované, spojte sa s technickou podporou v pracovných dňoch v čase od **8:00 do 18:30 telefonicky na čísle 02/322 44 444**

Ak je zariadenie zašifrované, vyplňte online ticket *na stránke technickej podpory*.

Ak je rozsah vašej licencie viac než 100PC, do jedného až dvoch pracovných dní po predchádzajúcom vyplnení online ticketu sa vám ozvú naši špecialisti a vyžiadajú si viac informácií o priebehu infekcie. Následne sa interne v spolupráci s Virus Labom pokúšame zistiť, či dokážeme obsah zašifrovaného zariadenia sprístupniť. Pamätajte však, že tvorcovia Filecoderov svoje techniky a útoky neustále zlepšujú a je stále ťažšie prelomiť ich šifrovanie. Šifrovanie je technologický štandard, používajú ho banky, chráni vaše údaje i financie. Je preto nemožné dešifrovať všetko a ihneď. Ak by to niekto dokázal, ohrozil by zabezpečenie finančných inštitúcií, webových obchodov a mnohých ďalších internetových služieb. Práve preto je infekcia Filecoderom taká nebezpečná. Nikto vám totiž nemôže zaručiť, že sa opäť dostanete k svojim súborom.

Ako získate výstup z ESET Log Collectora zistíte v článku: *Ako použijem nástroj ESET Log Collector*

Viac informácií o platenej službe ESET Technická podpora Premium môžete nájsť na stránke: *Technická podpora*

V šifrovaní používanom Filecodermi preto hľadáme chyby, ktoré nám pomôžu dešifrovať obsah napadnutého zariadenia. V prípade, že sme úspešní a tvorca Filecodera naozaj spravil chybu, dodáme vám **na mieru vytvorený dešifrovací nástroj aj s návodom na použitie**. Takýmto spôsobom dokážeme dešifrovať asi jednu pätinu rôznych druhov Filecoderov. Tento proces však môže trvať niekoľko týždňov a v závislosti od zručnosti autora škodlivého softvéru nemusí byť vôbec úspešný.

Ak používate služby ESET Technickej podpory Premium, naši špecialisti sú vám k dispozícii 24 hodín denne 365 dní v roku.

Myslite aj na firemné android zariadenia

Rôzne formy Filecoderov sa šíria aj na mobilné Android zariadenia. ESET zaznamenal malware, ktorý blokoval obrazovku zariadenia, zašifroval obsah zariadenia alebo dokonca zmenil PIN kód do mobilu alebo smartfónu. Ak ho zariadenie nastavené nemalo, malware ho vybral sám. Aj v týchto prípadoch pýtajú výkupné za odblokovanie.

V prípade nerootovaných zariadení, ktoré nie sú chránené bezpečnostnou aplikáciou, neexistuje okrem obnovenia továrenských nastavení (Factory Reset) jednoduchý spôsob, ako napríklad zmeniť na zariadení PIN. Výsledkom toho je však strata údajov uložených na zariadení.

Androidový malware sa väčšinou šíri cez neoficiálne obchody s aplikáciami, cez warez fóra alebo torrenty. Sľubujú zaujímavé funkcie, ktoré obeť nalákajú na inštaláciu. V mnohých prípadoch však svoju funkciu neplnia. Administrátorské povolenia môžu získať tak, že sa maskujú ako inštalácia záplaty. V mnohých prípadoch však útočníkom stačia menej sofistikované taktiky. Spoliehajú sa na to, že používateľ jednoducho klikne „OK“ na čokoľvek, čo mu mobil zobrazí.

Aj mobil alebo smartfón je však vašim firemným majetkom. Zamestnanci by s nimi mali podľa toho zaobchádzať a rovnako ako nemajú možnosť inštalovať čokoľvek na svoj firemný počítač, nemali by mať možnosť robiť to na svojom firemnom mobilnom zariadení. A aj v tomto prípade by ste ich mali informovať o zásadách bezpečného používania:

- Zakážte na firemných mobilných zariadeniach používanie aplikácií, ktoré nepochádzajú z oficiálnych digitálnych obchodov Google Play a Amazon Appstore. Napriek tomu, že Google Play nie je 100-percentne očistený od škodlivého kódu, má silné ochranné mechanizmy určené na zabezpečenie používateľov.
- Sťahujte aplikácie len od dôveryhodných vývojárov a vždy si pri nich čítajte hodnotenia a komentáre od používateľov. Podvodné správanie záškodných aplikácií si používatelia všimnú veľmi rýchlo. Taktiež si vezmite minútu času na to, aby ste skontrolovali, aké povolenia od vás aplikácia pri inštalácii vyžaduje.
- Nepodceňujte potrebu antivírusovej ochrany svojho Android zariadenia. Ak ste existujúcim zákazníkom spoločnosti ESET, bezpečnostnú aplikáciu *ESET Endpoint Security pre Android* môžete získať za výhodnejšiu cenu, alebo dokonca sú už v cene bezpečnostných balíkov ESET Business Solutions, medzi ktoré patria:
  – *ESET Endpoint Protection Standard*
  – *ESET Endpoint Protection Advanced*
  – *ESET Secure Business*
  – *ESET Secure Enterprise*

Zaplatiť útočníkom? Neodporúčame

Útočníci po zašifrovaní obsahu zariadenia vyžadujú od svojej obete poplatok za dešifrovanie. Silno odporúčame toto výkupné neplatiť. Zaplatenie vám síce môže prinavrátiť dáta, poznáme však mnoho prípadov, v ktorých dešifrovací kľúč vôbec nefungoval alebo v ktorých nebol úspešný pri dešifrovaní všetkých súborov. Aj útočníci sú totiž omylní a nemusí sa im podariť dešifrovať súbor, ktorý sami zašifrovali. Malware autori okrem toho samozrejme nepraktizujú legálny biznis. Nemajú žiadnu právnu povinnosť spraviť to, čo vám v žiadosti o výkupné sľubujú. Nemáte tiež záruku, že po odšifrovaní zariadenia vám ho o niekoľko dní opäť nezašifrujú.

V niektorých prípadoch si obete myslia, že pomôže prestavenie BIOS hodín na čas pred útokom. Jediným dôsledkom tohto úkonu však môže byť zmena výhražnej správy od útočníkov, ktorá sa môže v priebehu času meniť a v ktorej sa môže postupne zvyšovať suma za poskytnutie dešifrovacieho kľúča.

IT komunitu veľmi prekvapilo vyjadrenie Josepha Bonavolanta, špeciálneho agenta americkej FBI, ktorý na bezpečnostnom summite v Bostone povedal: „Aby som bol úprimný, často ľuďom odporúčame, aby jednoducho zaplatili výkupné. Pretože Ransomware je naozaj taký kvalitný." Odporúčanie FBI je totiž v ostrom rozpore s pozíciou bezpečnostnej komunity, ktorá si myslí, že zaplatenie výkupného by nemalo byť akceptované. V ESETe považujeme za veľmi nešťastné, že zaplatenie výkupného bolo postavené nad alternatívu kvalitnej prevencie, ktorú spomíname v tomto dokumente.

Europol označil Ransomware, ktorý je jedným z druhov Filecodera, vo svojom hodnotení „Organized Crime Threat" za najväčšiu hrozbu. FBI zase povedala, že od apríla 2014 do júna 2015 dostala takmer tisíc sťažností súvisiacich s CryptoWallom. Ide o jeden z najaktívnejších Ransomwarov, straty s ním spojené stáli americké firmy a jednotlivcov okolo 18 miliónov dolárov. Podľa výsledku panelovej diskusie Georgetown „Law's Cybercrime 2020: Budúcnosť digitálnej kriminality a vyšetrovania" uskutočnenej v decembri 2014, Ransomware predstavuje budúcnosť spotrebiteľskej kyberkriminality.

Ransomware a Filecodery sú bezpochyby na vzostupe. Napriek tomu predstavujú len zlomok hrozieb, ktorým musia čeliť firmy a organizácie. Práve preto je myšlienka „v najhoršom prípade teda zaplatím" taká chybná. Výkupné by ste nemali považovať za špeciálnu formu bezpečnostného auditu. Pamätajte tiež na to, že v hre nie je len výška výkupného ale aj vaše dáta a dôvera vašich zákazníkov.

www.eset.sk