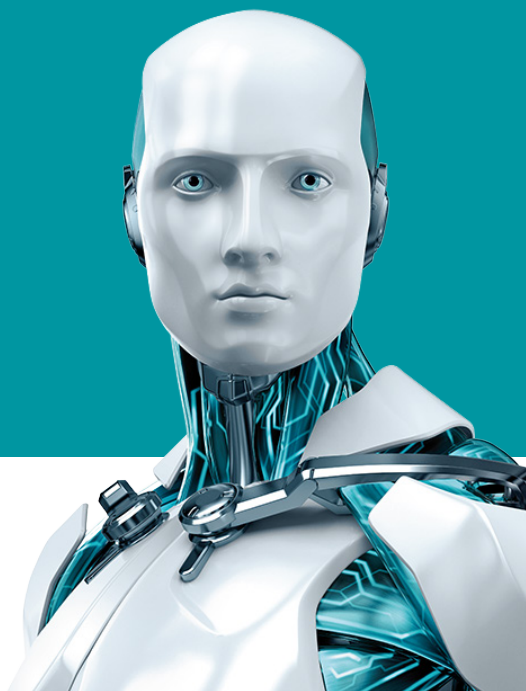
ESET vs. CRYPTO-RANSOMWARE

Ce, cum și de ce?



ENJOY SAFER TECHNOLOGY™

CUPRINS

INTRODUCERE

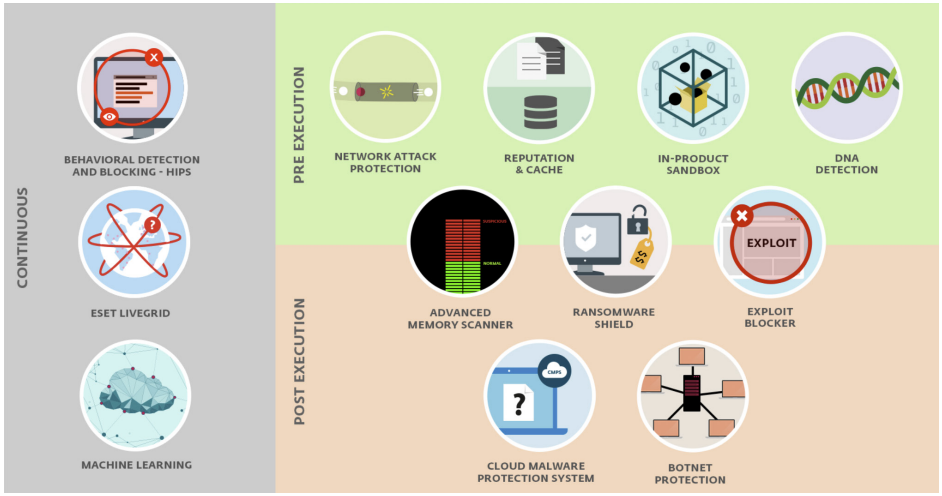
Atacurile crypto-ransomware (sau filecoderele) au evoluat continuu din 2013, atunci când a apărut secvența malware CryptoLocker. De atunci, infractorii cibernetici au colectat milioane de dolari, extorcând bani de la victime, în schimbul deblocării datelor criptate. În 2016, estimările bazate pe constatările FBI au sugerat ca ransomware-ul a generat venituri de **1 miliard de dolari pe an pentru atacatori.**

Câștigurile infractorilor cibernetici demonstrează impactul acestei tendințe exponențiale și reprezintă principalul motiv pentru care crypto-ransomware-ul a devenit malware-ul preferat de atacatori. De asemena, nu ar trebui să fie o surpriză faptul că cele mai multe campanii ransomware folosesc kituri de exploatare și e-mailuri cu inginerii sociale drept vectori de infectare, fapt ce contribuie, de asemenea, la creșterea prevalenței lor. Potrivit serviciului PhishMe "*peste 97% dintre mesajele de tip phishing livrate în 2016 conțineau ransomware...* "

ESET a monitorizat scena ransomware îndeaproape și a răspuns la evoluția rapidă a acestui tip de atac. În 2016, au existat doar câteva zile în care cercetătorii ESET nu s-au confruntat cu o nouă familie ransomware.

Totuși, deși este una dintre cele mai grave tipuri de malware „in-the-wild", este doar una dintre multele amenințări. Acest lucru înseamnă că ESET luptă împotriva lui cu ajutorul unor multiple straturi de protecție, adresând astfel orice amenințare potențială.

TOATE STRATURILE DE PROTECȚIE ACTIVE



Majoritatea atacurilor ransomware sunt blocate de *tehnologia multi-stratificată ESET* chiar înainte ca infectarea propriu-zisă cu ransomware să comunice în vreun fel cu computerele victimelor. Un bun exemplu este detectarea mesajelor de e-mail care conțin droppers, care în cele din urmă ar descărca și executa secvențele ransomware.

Un alt exemplu este detectarea încercărilor de exploatare care ar permite atacatorilor să preia controlul de la distanță asupra dispozitivelor victimelor și care, în multe cazuri, conduc la extorcare via ransomware. Funcția ESET Network Detection este proiectată să prevină astfel de tentative prin vizarea vulnerabilităților de rețea și a kiturilor de exploatare. În plus, **ESET Exploit Blocker** monitorizează procesele de funcționare ale aplicațiilor și caută anomalii în comportamentul lor. Design-ul permite soluțiilor ESET să detecteze și să blocheze exploatarea vulnerabilităților, în mod eficient chiar și a celor necunoscute anterior, așa-numitele amenințări "zero-days", care ar putea fi utilizate de către crypto-ransomware pentru a se infiltra în sistemul vizat.

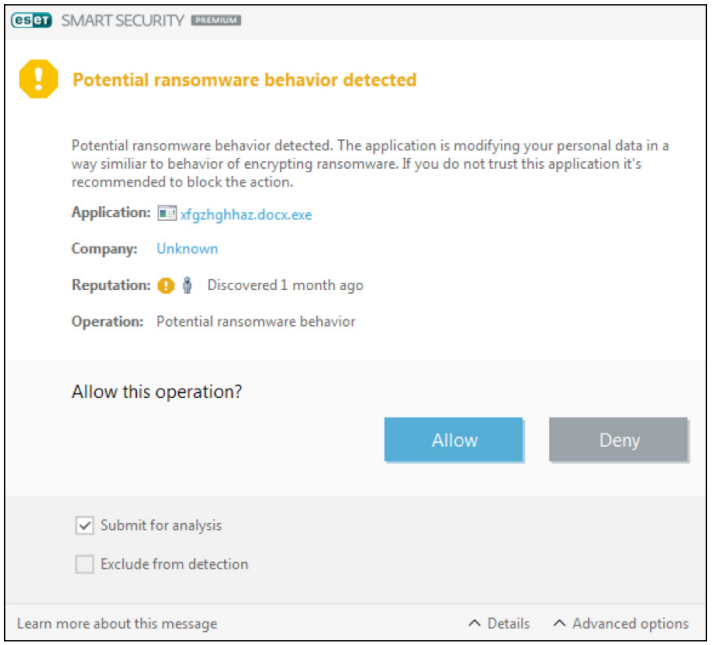
Cu scopul de a întări suplimentar protecția sistemelor utilizatorilor, **ESET Advanced Memory Scanner** este proiectat pentru a descoperi adevărata natură a proceselor puternic disimulate, detectând în mod constant secvențele crypto-ransomware înainte ca acestea să cripteze fișierele valoroase. Un astfel de malware disimulat constituie o parte semnificativă a traficului malițios de astăzi, mai ales din cauza serviciilor automatizate de reîmpachetare/disimulare disponibile pe piața neagră. Dar chiar și cel mai disimulat cod din lume, trebuie să se dezvăluie la un moment dat, pentru a fi executat. Acela este punctul în care este descoperit de Scannerul nostru Avansat de Memorie, declanșat prin sistemul ESET Host-Based Intrusion Prevention System (HIPS) la momentul potrivit.

Pe scurt, fiecare nivel al tehnologiei multi-stratificate ESET utilizează diferite mijloace pentru a lua parte la blocarea efectivă a crypto-ransomware-ului. Mai mult decât atât, metadatele din fiecare strat pot fi trimise către sistemele noastre cloud **ESET LiveGrid®** sporind inteligența algoritmilor noștri de învățare automatizată. Aceste sisteme automate, în combinație cu expertiza cercetătorilor și a inginerilor noștri, ne permit să reducem timpul de reacție față de noile amenințări emergente, la doar câteva minute.

Pentru a se apropia cât mai mult de o securitate perfectă, ESET a adăugat încă un strat de protecție pentru a aborda fenomenul ransomware.

ESET Ransomware Shield

ESET Ransomware Shield monitorizează și evaluează aplicațiile executate folosind euristica. Este configurat să detecteze și să blocheze comportamentul asemănător cu cel al ransomware-ului. Tehnologia este activată în mod implicit. Dacă ESET Ransomware Shield se declanșează în urma unei acțiuni suspecte, atunci utilizatorului i se va solicita să aprobe/interzică o acțiune de blocare.



În plus, fereastra de dialog îi permite utilizatorului să trimită aplicația suspectă pentru analiză - sau să o excludă de la detecții viitoare.

DE CE AȘA ȘI NU ALTFEL?

Printre mai multe abordări posibile pentru combaterea ransomware-ului, noi credem că abordarea noastră cu mai multe straturi este cea adecvată. Și nu e doar părerea noastră; eficacitatea sa a fost dovedită în nenumărate teste independente de către organizațiile de testare cu reputație. De exemplu, *într-un test al organizației independente SE Labs, axat pe detecția ransomware, ESET a avut o rată de detecție de 100%.* Cuvântul "reputație" este foarte important: există teste care nu aduc o valoare informațională. Unele dintre aceste teste sunt chiar înșelătoare, cum ar fi cazul așa-numitului *RanSim*.

RanSim

Acest software ar putea fi considerat un simulator, dar cu siguranță NU copiază comportamentul crypto-ransomware. Din moment ce modifică numai fișierele pe care el le-a creat, simulează de fapt doar secvențe "ransomware" care solicită o taxă pentru decriptarea propriilor documente create.

Produsele ESET nu detectează – și nu vor detecta - acest comportament ca fiind rău intenționat și astfel vor "pierde" în astfel de teste. În cazul în care ar trebui să detecteze ceva similar, implicit ar trebui să detecteze tehnici de gestionare a drepturilor digitale utilizate de platformele de distribuție digitală, cum ar fi Steam. Acestea se comportă în mod similar, prin descărcarea propriilor fișiere criptate - jocuri, în cazul Steam - și decriptarea lor la momentul potrivit.

Dar să revenim la subiectul acestei secțiuni și să discutăm de ce nu abordăm crypto-ransomware-ul în mod diferit.

Whitelisting-ul aplicațiilor nu este imbatabil

Simpla idee de introducere în liste albe a aplicațiilor benigne este prezentată de multe ori ca o metodă puternică împotriva crypto-ransomware-ului. Indiferent de sarcina de a păstra numărul de detecții fals pozitive cât mai scăzut posibil, există mai multe probleme care trebuie adresate.

Cazurile problematice includ, de exemplu, crypto-ransomware-ul care se injectează într-un proces care aparține unei aplicații din lista albă. Sau când unele dintre aplicațiile din lista albă ar putea fi interpretatori, cum ar fi wscript, autoIt sau cmd, în cazul cărora ar putea fi o provocare permiterea executării lor, deoarece codul pe care trebuie să-l interpreteze ar putea fi dăunător.

Acest lucru este menționat pentru cazurile în care o aplicație legitimă, care este capabilă să cripteze fișiere (ex. un arhivator) este utilizat în mod abuziv pentru criptarea acestora. Acest lucru nu înseamnă că introducerea în liste albe nu are sens. Contribuie la detecția globală pe care o oferă ESET. Cu toate acestea, fără alte straturi de protecție, detecția ar fi semnificativ mai slabă.

Shadow Copy este util, dar nu și împotriva crypto-ransomware

Shadow Copy este o tehnologie care permite extragerea manuală sau automată a copiilor de back-up, instantanee ale fișierelor de pe calculator sau ale volumelor, chiar și atunci când acestea sunt în uz. Cu toate acestea, există unele situații de luat în considerare înainte de a încerca să folosiți această metodă ca o soluție de preluare a datelor după un atac crypto-ransomware.

În primul rând, ar trebui să fie luată în considerare degradarea potențială a performanței legate de crearea și stocarea copiilor shadow. În al doilea rând, copiile shadow pot fi șterse sau criptate de ransomware dacă nu sunt protejate. Mai mult decât atât, dacă ransomware-ul începe să cripteze în mod repetat fișierele, memoria buffer dedicată stocării modificărilor fișierelor și-ar putea atinge limita. Și cel mai important, nu trebuie să uităm despre ransomware-ul disk-encrypting (cum ar fi *Petya*), împotriva cărora copiile shadow ar fi complet inutile.

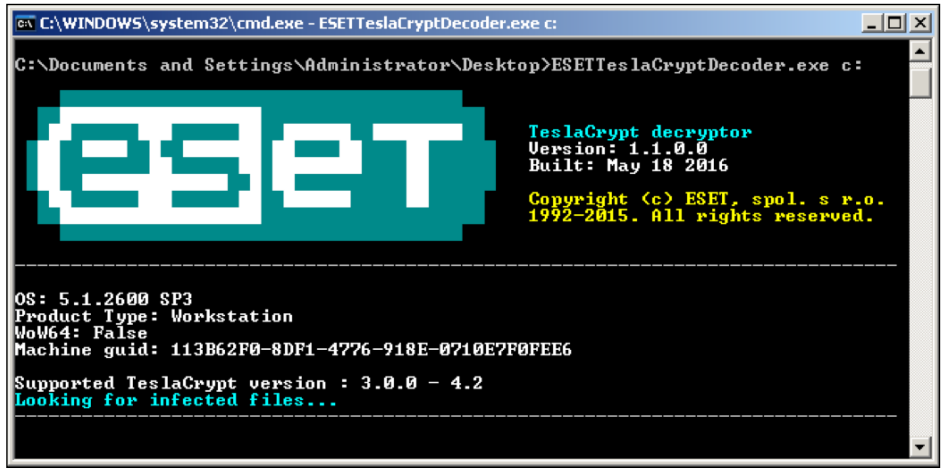
De ce nu un rollback, în ultimă instanță?

Există, în mod evident, beneficii pentru a avea o funcție de rollback implementată direct într-o soluție de securitate. Testăm și evaluăm în mod continuu impactul global al unei astfel de soluții și ar putea fi pusă în aplicare în viitor. În acest moment, analizele noastre sugerează că abordarea actuală - cu accentul în principal pe măsurile proactive - oferă rezultate optime.

ALTE MODALITĂȚI PRIN CARE ESET COMBATE RANSOMWARE-UL

La ESET știm că lupta împotriva malware-ului, mai ales împotriva tipurilor malițioase precum crypto-ransomware, trebuie să meargă dincolo de soluțiile noastre de securitate standard și de tehnologia implementată în cadrul acestora. Din acest motiv, cercetătorii noștri analizează constant oportunitățile care pot fi exploatate pentru a stopa operațiunile infractorilor cibernetici.

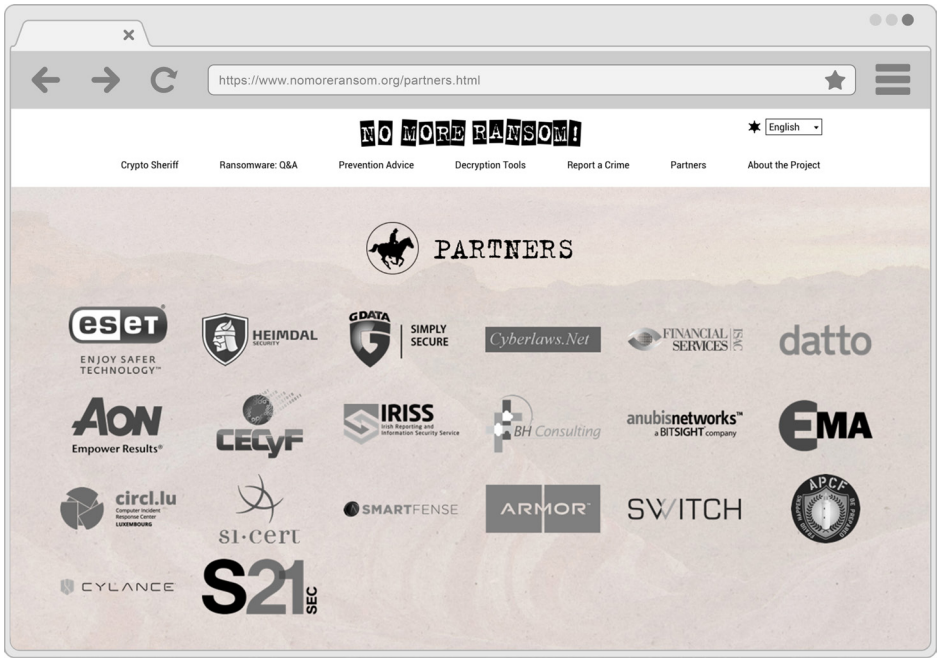
În cazul crypto-ransomware, acest lucru presupune identificarea unor erori în implementarea acestuia sau a lacunelor din infrastructura criminalilor cibernetici. Adoptăm orice oportunitate de a crea programe de decriptare pentru ransomware, care să îi ajute pe cei care au căzut victime să-și obțină datele înapoi. În cele mai multe cazuri, dezvoltăm programe de decriptare adaptate unor cazuri specifice victimei, deoarece, de obicei, există mai multe variabile specifice sistemului care trebuie luate în considerare. Cu toate acestea, ori de câte ori este posibil, vom crea astfel de programe de decriptare și le vom furniza în mod gratuit publicului. Programul nostru de decriptare pentru TeslaCrypt, care a fost descărcat de peste 100 000 de ori, este un astfel de caz.



Similar cu abordarea proactivă pe care o oferă produsele noastre, comunicăm în mod proactiv rezultatele cercetării noastre despre crypto-ransomware, realizate în centrele de cercetare ESET

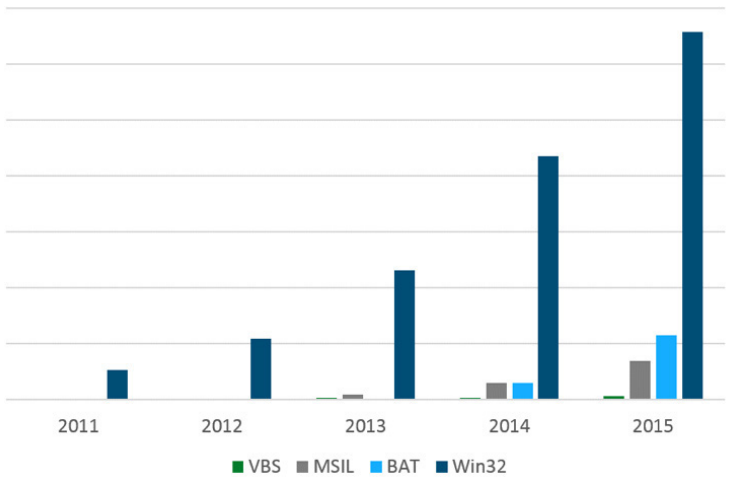
Lansăm în mod frecvent comunicate de presă privind cercetările noi derulate și rapoarte despre crypto-ransomware pe blog-ul nostru regional *www.blog.eset.ro* sau global *www.welivesecurity.com* și suntem prezenți la numeroase conferințe internaționale.

Noi împărtășim descoperirile noastre cu cercetători din întreaga lume, fie că lucrează pentru cei mai mari competitori sau pentru entitățile de aplicare a legii cum ar fi FBI. Suntem una dintre primele companii private care a devenit un partener al proiectului "*No more ransom*" iar aceasta este una dintre multiplele metode prin care ESET și-a dovedit dedicarea în lupta împotriva crypto-ransomware-ului.



FOCUS PE PETYA CRYPTO-RANSOMWARE

ESET a acoperit anterior evoluția *crypto-ransomware-ului* evidențiind importanța tot mai mare a acestuia. Numărul de familii, variante și platforme vizate au crescut semnificativ începând cu 2011.



Numărul de programe ransomware de criptare a fișierelor Windows în perioada 2011-2015

Petya a adoptat o abordare diferită de cea a altor coduri crypto-ransomware. În loc să cripteze fișierele în mod individual, viza sistemul de fișiere. Obiectivul era *master boot record* (MBR), care este responsabil de încărcarea sistemului de operare.

Atunci când Petya este executat, acesta pornește un atac în două etape, menit să cripteze MBR-ul. Acest proces de criptare al MBR începe prin modificarea MBR pentru a cauza un *BSOD* și care să repornească sistemul. Acesta afișează apoi un ecran *CHKDSK* fals în timp ce execută criptarea MBR și, în final, repornește sistemul. Când se întâmplă acest lucru, este afișat un ecran intermitent cu un craniu și un mesaj de răscumpărare.

Evoluția ecranelor de tip Petya și a mesajelor de răscumpărare (variantele inițiale roșii și mai recente, verzi și galbene)

Deși acest mesaj este, fără îndoială, înspăimântător, este totuși posibilă anularea daunelor cauzate, din cauza mai multor defecte în felul în care Petya se ocupă de criptare.

Dezvoltatorii Petya au comis o eroare de implementare în nucleul Salsa20, care reduce nivelul de securitate al criptării. Doar jumătate din cheie este aplicată, ceea ce o reduce de la 92 de biți la 46 de biți de securitate, care este posibil să se rupă în câteva secunde folosind forța brută.

Cu toate acestea, ultima versiune a ransomware-ului nu mai are aceste defecte, deoarece acestea au fost reperate și fixate de către operatorii malware.

RECOMANDĂRI FUNDAMENTALE PENTRU PROTEJAREA DATELOR PERSONALE ÎMPOTRIVA RANSOMWARE

Ransomware-ul este doar o altă familie de malware. Singura diferență este că vă vizează fișierele - deci pe lângă toate eforturile pe care le depuneți pentru a fi protejați (vectorii de atac sunt de cele mai multe ori e-mailurile și kiturile de exploatare), trebuie să dispuneți de o politică de back-up implementată eficient ceea ce înseamnă să aveți capacitatea de a restaura rapid datele. Soluțiile de tip Journaling solicită resurse CPU/disk și nu doriți să le folosiți când apare o problemă de tip ransomware (fiind deja mult prea târziu). Pentru a limita vectorii de atac:

1. Configurați corect endpoint-urile și software-ul de securitate.
2. Actualizați și implementați patch-urile sistemului de operare și ale software-ului în mod regulat. Ransomware-ul exploatează în mod frecvent vulnerabilitățile cunoscute. Acordați o atenție deosebită browserelor de internet în această privință.
3. Soluțiile de securitate pentru endpoint-uri și perimetru sunt o necesitate, iar acestea trebuie să fie configurate în mod corespunzător pentru a fi capabile să utilizeze setul complet de caracteristici oferit, cum ar fi detecțiile rapide bazate pe cloud.
4. Utilizați capabilitățile pe care sistemul de operare vi le oferă pentru a-l securiza:
   - eliminați posibilitatea de a rula codul untrusted cu AppLocker sau cu Software Restriction Policie;
   - dezactivați scriptingul în sistemele de operare și browsere web;
   - dezactivați servicii inutile, cum ar fi RDP;
   - setați ca sistemul de operare să afișeze extensiile fișierelor;
   - luați în considerare implementarea unui serviciu de System Restore;
   - luați în considerare dezactivarea Windows Script Host;
   - setați funcția "Open with ..." pentru extensiile care de cele mai multe ori sunt folosite pentru infectare cu un reader (cum ar fi Notepad), mai degrabă decât cu un program de interpretare;
   - blocați executarea aplicațiilor din %LocalAppData% și %AppData%;
5. Dezactivați accesul inutil la share-urile din rețea.
6. Nu utilizați serverele similar unui sistem desktop standard (ex. pentru navigarea pe internet).


ENJOY SAFER TECHNOLOGY™