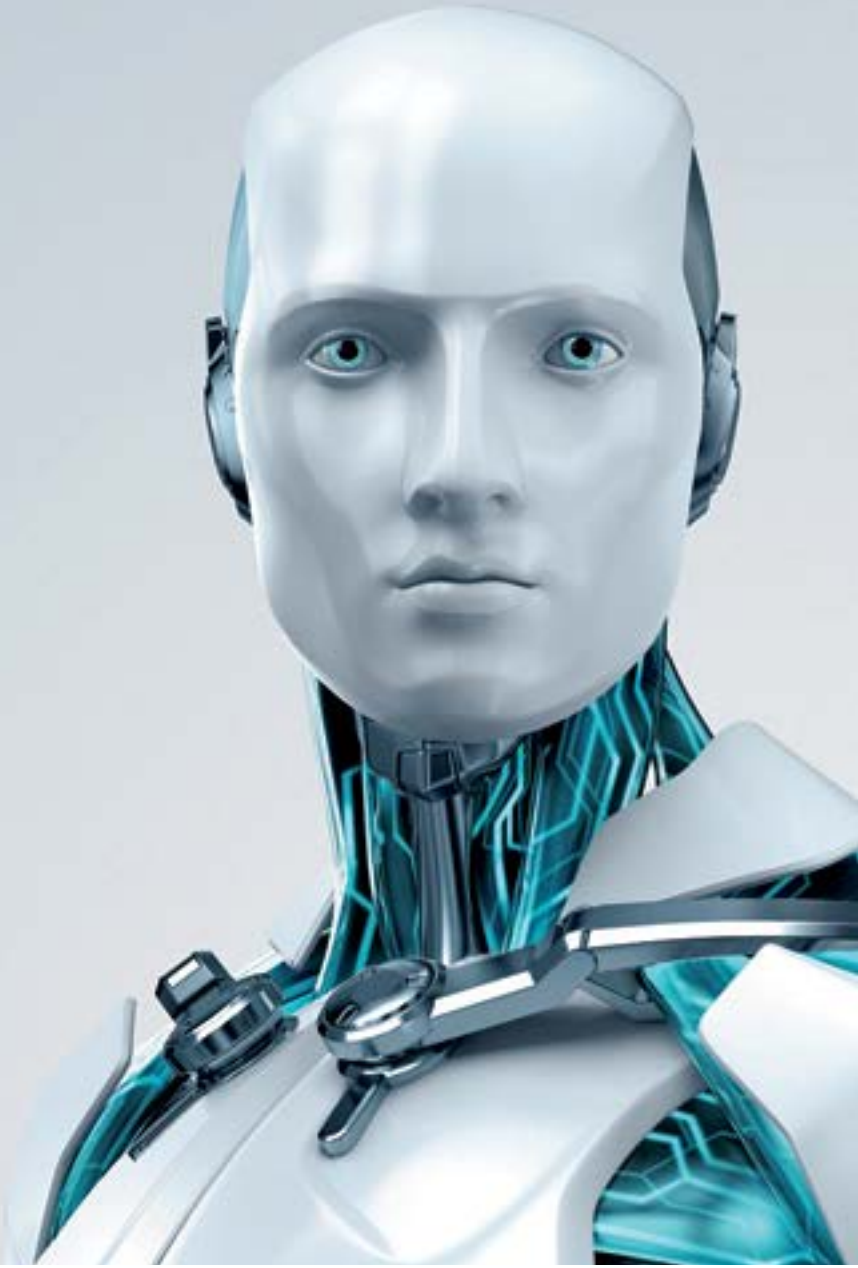
Tehnologia ESET

Abordarea multi-stratificată și eficiența ei



Versiunea documentului:
1.0

Autori:
Jakub Debski, Head of Core Technology Development
Juraj Malcho, Chief Research Officer
Peter Stancik, Security Researcher

CONȚINUT

OBIECTIVE

În acest document, vom rezuma modurile în care ESET utilizează tehnologii pe mai multe niveluri pentru a îmbunătăți capacitățile de bază ale antivirusului. Realizăm acest lucru explicând ce straturi sunt implicate în rezolvarea problemelor specifice și ce beneficii sunt oferite utilizatorului.

DE CE ANTIVIRUSUL ESTE ȘI NU ESTE MORT

Majoritatea companiilor antivirus s-au dezvoltat datorită dorinței de a ajuta oamenii care au probleme în privința virușilor sau codurilor malware, iar tehnologia a evoluat pentru a combate mulțimea de amenințări pe care vendorii de securitate au început să le adreseze. Astăzi, antivirusul este perceput ca un bun de larg consum, iar securitatea este un subiect care rezonează cu toată lumea, chiar dacă utilizatorii înțeleg sau nu, ce înseamnă cu adevărat. Recent, am observat o creștere de noi companii, auto-intitulate "de următoare generație". Acestea în special, au puțină experiență în dezvoltarea soluțiilor anti-malware, dar promovează în mod agresiv produsele lor ca fiind "inovative", desființând în același timp companiile fondate mai demult, numindu-le "dinozauri". Ca în cazul vânzărilor, multe dintre mesajele lor de brand sunt derizorii și, în mod ironic, capacitatea lor de detecție se bazează în mare parte pe un motor de detectare terț de la un vendor cunoscut, deoarece foarte puține dintre zecile de soluții de acum, prezente pe piață, au experiența sau capacitatea de a permite să își dezvolte propria tehnologie nucleu de detecție. Tehnologiile ESET sunt brevetate și au fost dezvoltate de specialiștii noștri.

Antivirusul nu este mort. Totuși, simpla detecție a semnăturilor statice care - conform noilor veniți - compromite eficiența industriei anti-malware reprezintă numai o componentă redusă a mecanismului tehnologic complex prin care produsele de securitate moderne adresează noile amenințări.

AMENINȚĂRI MULTIPLE, PROTECȚIE PE MAI MULTE NIVELURI

Companiile anti-malware, fondate în trecut, care activează astăzi și-au menținut cota de piață prin creșterea vitezei de reacție la amenințările actuale. Aceste amenințări nu sunt statice iar evoluția lor nu s-a oprit la începutul anilor 2000. Pericolele de azi nu mai pot fi combătute în mod eficient doar cu ajutorul tehnologiei realizate în anii 1990. Lupta împotriva malware-ului modern, este un joc de șoarecele cu pisica în care ne confruntăm cu echipe de indivizi rău intenționați calificați și (financiar) motivați. Astfel încât, companiile de securitate au nevoie să-și îmbunătățească produsele în mod constant, atât activ cât și proactiv, pentru a oferi soluții eficiente, adăugând straturi diferite, prin care programele malware moderne pot fi detectate și / sau blocate. Un singur punct de protecție sau o singură metodă de apărare nu este, pur și simplu, de ajuns. Acesta este unul dintre motivele pentru care ESET a evoluat de la un furnizor de soluții antivirus într-o companie de securitate IT.

AMENINȚĂRI MULTIPLE, PLATFORME MULTIPLE

Sistemele de operare Microsoft nu sunt singurele platforme pe care rulează codurile malware în zilele noastre. Câmpul de luptă se schimbă rapid, deoarece atacatorii încearcă să preia controlul asupra platformelor și a proceselor neexplorate anterior.

- Orice pârghie tehnologică ce poate fi controlată pentru a induce activități malițioase poate fi exploatată de infractori.
- Orice care rulează coduri executabile pentru a procesa datele externe poate fi potențial deturnat de către secvențele malware.

Serverele Linux au reprezentat o țintă majoră pentru atacatori (*Operațiunea Windigo, Linux/Mumblehard*), Mac-urile care rulează OS X au constituit cea mai mare rețea de botneți dintotdeauna (*OSX/Flashback)*, telefoanele mobile sunt ținte comune (*Hesperbot*) și atacă prin routere devenind serioase amenințări (*Linux/Moose*). Rootkit-urile ajung din ce în ce mai aproape de hardware (atacuri ale firmware-ului sau *UEFI rootkit*), iar virtualizarea deschide noi posibilități de atac (Bluepill, VM nu recunosc toate vulnerabilitățile). De asemenea, navigatoarele web și alte aplicații au devenit la fel de complexe precum sistemele de operare, iar mecanismul lor de script este folosit, de obicei, în scopuri malițioase (*Win32/Theola*).

VECTORI DIFERIȚI DE DISTRIBUȚIE

Din punct de vedere istoric, primul cod malware a apărut ca un proces de auto-replicare, la început în cadrul sistemelor iar mai apoi a evoluat ca metodă de infectare a fișierelor și /sau infectare a discurilor, răspândindu-se de la PC la PC. Deoarece utilizarea internetului a devenit aproape universală, numărul de moduri de distribuire a malware-ului a crescut enorm. Obiectele periculoase pot fi trimise și prin e-mail ca atașamente sau link-uri, descărcate din pagini web, prin script-uri din documente, partajate pe dispozitive mobile, instalate la distanță profitând de autorizările ușoare și parolele slabe, executate prin intermediul exploit-urilor sau instalate de către utilizatorii finali păcăliți prin tehnici de inginerie socială.

DESIGNUL MALWARE

Epoca în care malware-ul era scris în principal de către adolescenți ca o glumă sau pentru a se da mari a trecut demult. În zilele noastre, malware-ului este scris cu scopul de a genera bani sau de a fura informații, cantități importante de bani fiind investite în dezvoltarea lui atât de către infractori cât și de guverne.

În speranța de a face detectarea mult mai dificilă, codul malware este scris în diferite limbaje de programare, folosind diferite compilatoare și limbi diverse. Codul este mascat și protejat cu ajutorul software-ului personalizat pentru a face detectarea si analiza mai greu de realizat. Codul este introdus în procesele curate pentru a evita monitorizarea bazată pe comportament - care este proiectată să detecteze activități suspecte - și să împiedice îndepărtarea, asigurându-se astfel persistența lui în sistem. Scripturile sunt folosite pentru a evita tehnicile de control a aplicațiilor iar malware-ul care se execută "numai în memorie" evită securitatea bazată pe analiza fișierelor.

Pentru a trece nevăzuți, infractorii invadează internetul cu mii de variante ale malware-ului lor. O altă metodă constă în distribuirea către un număr mic de ținte pentru a evita atragerea atenției companiilor de securitate. Pentru a evita detectarea, componentele software curate sunt utilizate în mod abuziv sau sunt folosite coduri dăunătoare semnate prin utilizarea certificatelor furate de la companii legitime, astfel încât codul neautorizat este mai greu de observat.

De asemenea, la nivel de rețea, malware-ul utilizează mai puțin serverele hardcoded de comandă și de control (C & C) pentru a trimite instrucțiuni și de a primi date de la sistemele compromise. Controlul decentralizat al botneților folosind rețeaua peer-to-peer este cel utilizat în mod obișnuit, iar comunicarea criptată face identificarea atacurilor mult mai greu de realizat. Algoritmii generatori de domenii reduc eficacitatea de detecție bazată pe blocarea URL-urilor cunoscute. Atacatorilor preiau controlul asupra site-urilor legitime, care au o reputație bună și chiar servicii de publicitate legale sunt folosite pentru a servi conținutul malițios.

Există mai multe modalități prin care atacatorii pot evita detectarea, astfel încât o soluție simplă, cu un singur strat nu este suficientă pentru a asigura protecția. La ESET considerăm că în mod constant, în timp real, o protecție pe mai multe niveluri este necesară pentru a asigura cel mai înalt nivel de securitate.

BENEFICIILE TEHNOLOGIEI NUCLEU ESET

Motorul de scanare ESET este în centrul produselor noastre și, în timp ce tehnologia de bază a fost moștenită de la "antivirusul de stil vechi", acesta a fost extins foarte mult și îmbunătățit și este în mod constant în curs de dezvoltare pentru a acoperi amenințările moderne.

Scopul motorului de scanare este de a identifica malware-ul și de a lua decizii automatizate cu privire la probabilitatea de a fi un cod rău intenționat.

Timp de mulți ani, performanța ESET s-a bazat pe algoritmi inteligenți și coduri de asamblare realizate manual pentru a depăși blocajele de performanță cauzate de analiza de cod profundă, implicată de tehnologia Sandbox integrată în produs. Cu toate acestea, am îmbunătățit această abordare. Acum, pentru performanțe maxime, folosim traducerea binară împreună cu emulare interpretată.

Cu ajutorul sandboxing-ului integrat trebuie să se imite diferite componente hardware și software pentru a fi executat un program într-un mediu virtualizat. Aceste componente pot include memoria, sistemul de fișiere, API-uri ale sistemului de operare și CPU (unitate centrală de procesare).

În trecut, CPU-ul a fost emulat folosind codul de asamblare personalizat
Cu toate acestea, a fost în "codul interpretat", ceea ce înseamnă că fiecare instrucțiune unică a trebuit să fie emulată separat. Cu traducerea binară se execută instrucțiuni emulate în mod nativ pe un procesor real. Această acțiune este de multe ori mai rapidă, mai ales în cazul buclelor din cod: introducerea buclelor multiple este o tehnică nativă de protecție pentru toate executabilele, acolo unde au fost aplicate măsuri pentru a le proteja de analiza produselor de securitate și cercetătorilor.

Produsele ESET analizează sute de formate de fișiere diferite (executabile, asistenți de instalare, scripturi, arhive, documente și bytecodes), pentru a detecta cu precizie componentele dăunătoare încorporate.

Figura de mai jos prezintă diferitele tehnologii ESET de nucleu și o aproximare a momentului și modul în care acestea pot detecta și / sau bloca o amenințare în timpul ciclului său de viață în sistem:

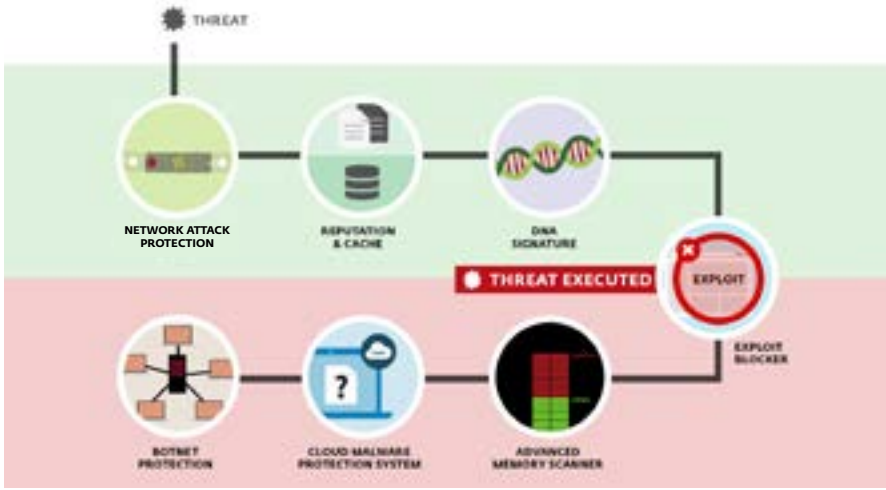


Fig. 1: Straturile de protecție ESET

PROTECȚIA LA ATAC A REȚETEI

Protecția Împotriva Atacurilor Derulate la nivelul Rețelei **este o extensie a tehnologiei firewall si îmbunătățește detectarea vulnerabilităților cunoscute la nivel de rețea**. Prin implementarea detecției pentru vulnerabilități comune în protocoalele utilizate pe scară largă, cum ar fi *SMB*, *RPC* și *RDP*, **este realizat un alt strat important de protecție** împotriva răspândirii malware-ului, a atacurilor derulate la nivel de rețea și a exploatării vulnerabilităților pentru care un patch de securitate nu a fost lansat sau propus spre implementare.

REPUTAȚIE & CACHE

În momentul inspecției unui obiect, cum ar fi un fișier sau un URL, înainte de a se produce orice scanare, produsele noastre verifică cache-ul local (și **ESET Shared Local Cache**, în cazul în care aveți ESET Endpoint Security) pentru coduri malițioase cunoscute sau elemente benigne care se află în lista albă. Acest lucru **îmbunătățește performanța de scanare**. După aceea, **ESET LiveGrid® Reputation System este interogat pentru reputația obiectului** (adică dacă obiectul a fost deja observat în altă parte și clasificat ca fiind rău intenționat sau în alt mod). Acest lucru **îmbunătățește eficiența de scanare și permite partajarea rapidă a informațiilor despre malware către clienții noștri**. Aplicarea listelor negre de URL și verificarea reputației previn ca utilizatorii să acceseze site-uri cu conținut dăunător și / sau site-uri de phishing.

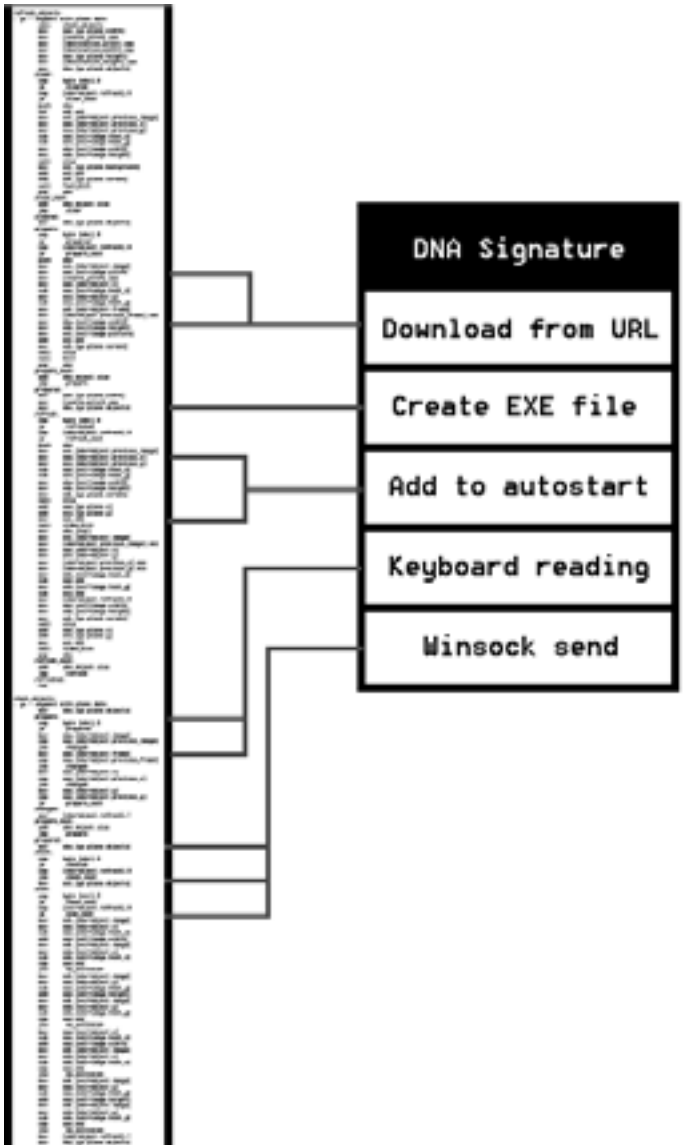
SEMNĂTURILE ADN

Tipurile de semnături variază de la hash-uri foarte specifice (utile, de exemplu, în vizarea precisă a codurilor binare malițioase, sau a anumitor versiuni de malware, în scopuri statistice sau pur și simplu pentru a da un nume de detecție mai precisă a malware-ului pe care l-am detectat euristic) și până la **Semnăturile ADN ESET** care **sunt definiții complexe ale comportamentului codurilor rău intenționate sau ale caracteristicilor malware.**

Metoda de verificare a tiparului malware, folosită de produsele antivirus mai vechi poate fi ocolită cu ușurință prin simpla modificare a codului sau utilizarea tehnicilor de disimulare. Cu toate acestea, comportamentul codurilor nu poate fi schimbat atât de ușor. Semnăturile ADN ESET sunt proiectate tocmai pentru a beneficia de acest principiu. Efectuăm o analiză profundă a codului, extrăgând "genele" care sunt responsabile pentru comportamentul său. **Astfel de gene comportamentale conțin mult mai multe informații decât indicatorii de compromitere (IOCs)** care mai sunt promovați de așa-numitele soluții "next-gen" drept o "alternativa mai bună" pentru detectarea semnăturii. Genele comportamentale ESET sunt folosite pentru a construi ADN-ul Semnăturilor, care sunt folosite pentru a evalua codul potențial suspect, indiferent dacă este găsit pe disc sau în memoria procesului de rulare.

În plus, motorul nostru de scanare extrage multe gene discriminatoare, care sunt utilizate pentru detectarea anomaliilor: orice secvență care nu arată legitim are potențialul de a fi cod malițios

În funcție de nivelul reglabil și de condițiile de potrivire, semnăturile ADN pot identifica mostre specifice cunoscute de malware, noi variante ale unei familii malware cunoscute sau chiar secvențe malware nevăzute sau necunoscute anterior, care conțin gene ce indică un comportament rău intenționat. Cu alte cuvinte, **o singură semnătură ADN, bine realizată, poate detecta zeci de**



mii de variante de malware interconectate și permite software-ului nostru antivirus să detecteze nu numai malware-ul pe care îl cunoște deja sau pe care l-a mai văzut înainte, dar, **de asemenea, noi variante, necunoscute anterior.** Mai mult decât atât, cluster-izarea automată și aplicarea algoritmilor de învățare automată pentru seturile noastre de eșantioane malware ne permit să identificăm noi gene rău intenționate și noi modele comportamentale pentru a le adăuga la sistemul de detecție al motorului nostru de scanare. Astfel de gene sunt comparate cu un set imens de liste albe pentru a ne asigura că nu este generată o detecție fals pozitivă.

EXPLOIT BLOCKER

Tehnologiile ESET protejează împotriva diferitelor tipuri de vulnerabilitate pe diferite niveluri: motorul nostru de scanare se referă la exploit-uri care apar în fișierele document malformate; Protecția Împotriva Atacurilor de Rețea vizează nivelul de comunicare; și în cele din urmă, Exploit Blocker-ul blochează procesul de exploatare în sine.

Exploit Blocker-ul monitorizează aplicațiile exploatabile în mod normal (browsere, cititoare de documente, clienți de e-mail, Flash Player, Java și altele) și în loc de a ținti doar *identificatorii CVE* **se concentrează pe tehnicile de exploatare.** Fiecare exploit este o anomalie în executarea procesului și ne uităm după anomaliile care sugerează prezența unor tehnici de exploatare. Pe măsură ce tehnologia este în curs de dezvoltare în mod constant, se adaugă noi metode de detecție, în mod regulat, pentru a acoperi noi tehnici de exploatare. Atunci când este declanșat, comportamentul procesului este analizat și, în cazul în care acesta este considerat suspect, **amenințarea poate fi imediat blocată pe aparat**, mai multe metadate referitoare la atac fiind trimise către sistemul nostru din cloud ESET LiveGrid. Aceste informații sunt prelucrate ulterior și corelate, **ceea ce ne permite să găsim amenințări necunoscute anterior și așa-numitele atacuri zero-day**, oferind laboratorului nostru informații valoroase despre noile amenințări.

Exploit Blocker-ul adaugă un alt strat de protecție, fiind cu un pas mai aproape de atacatori, prin utilizarea unei tehnologii care este complet diferită de tehnicile de detectare care se concentreaza pe analiza codului dăunător în sine.

SCANNER AVANSAT DE MEMORIE

Scannerul Avansat de Memorie este **o tehnologie unică ESET** care **abordează** în mod eficient o problemă importantă ridicată de malware-ul modern - utilizarea frecventă a **disimulării și / sau criptării.**

Aceste tactici de protecție a malware-ului, de multe ori folosite în packere run-time și dispozitive de protecție de cod, cauzează probleme pentru soluțiile de detectare care folosesc tehnici de unpacking, cum ar fi emularea sau sandboxing-ul. Mai mult decât atât, dacă verificarea se face cu ajutorul unui emulator sau unui sandbox virtual / fizic, nu există nici o garanție că, în timpul analizei malware-ul va afișa un comportament rău intenționat, care îi va permite să fie clasificat ca atare. Malware-ul poate fi disimulat în așa fel încât nu toate căile de execuție pot fi analizate; codul poate conține declanșatori condiționați, inclusiv în funcție de timp, pentru activarea proprie; și, foarte frecvent, se pot descărca noi componente în timpul vieții sale. Pentru a aborda aceste probleme, Scannerul Avansat de Memorie monitorizează comportamentul unui proces rău intenționat și îl scanează după ce îl descoperă în memorie. Acest lucru completează funcționalitatea mai tradițională de pre-execuție sau execuție de analiză de cod proactivă.

De asemenea, procesele curate pot deveni brusc rău intenționate, din cauza exploatării sau injectării de cod. Din aceste motive, efectuarea analizei o singură dată nu este de ajuns. Este necesară o monitorizare constantă, iar acesta este Scannerului Avansat de Memorie. **Ori de câte ori un proces apelează sistemul dintr-o nouă pagină executabilă, Scannerului Avansat de Memorie efectuează o analiză de cod comportamentală folosind Semnăturile ADN ESET.**

Analiza de cod este realizată nu numai pentru memoria executabilă standard, dar, de asemenea, pentru NET MSIL (Microsoft Intermediate Language) cod utilizat de către autorii malware pentru a împiedica analiza dinamică. Ca urmare a punerii în aplicare a sistemului de cache inteligent, Scannerul Avansat de Memorie nu are nici un impact și nu provoacă nici o deteriorare considerabilă a vitezei de procesare.

Scannerul Avansat de Memorie cooperează bine cu Exploit Blocker-ul. Spre deosebire de cel din urmă, Scannerul este o metodă post-execuție, ceea ce înseamnă că există riscul ca unele activități rău intenționate să fi avut loc deja. Cu toate acestea, **se implică în lanțul de protecție în ultimă instanță** în cazul în care un atacator reușește să ocolească alte straturi de protecție.

Mai mult decât atât, există o nouă tendință în malware-ul avansat: unele coduri malițioase operează acum "numai în memorie", fără a avea nevoie de componente permanente în sistemul de fișiere care pot fi detectate în mod convențional. Inițial, un astfel de malware a apărut numai pe servere, din cauza uptime-ului lor pe termen lung - deoarece sistemele de servere sunt active luni sau ani la rând, la un moment dat, procese rău intenționate ar putea rămâne în memorie pe termen nelimitat, fără a avea nevoie să supraviețuiască unui restart - dar atacurile recente asupra întreprinderilor indică o schimbare a acestei tendințe, iar noi observăm că sunt vizate, de asemenea, endpoint-urile. **Doar scanarea memoriei poate descoperi cu succes astfel de atacuri rău intenționate și ESET este pregătit pentru această nouă tendință de atac datorită Scannerului Avansat de Memorie.**

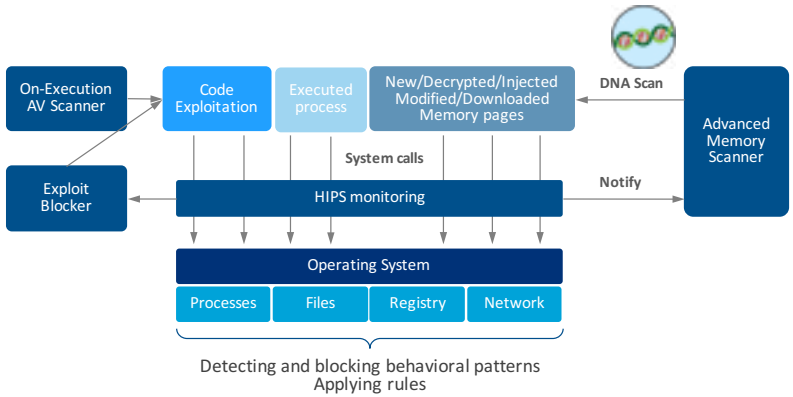
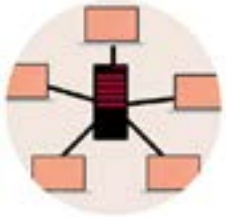


Fig.2: Modul de funcționare al detecției comportamentale ESET

SISTEM DE PROTECȚIE ÎMPOTRIVA MALWARE-ULUI BAZAT PE CLOUD

Sistemul de protecție ESET Împotriva Malware-ului bazat pe Cloud este una dintre tehnologiile ESET care se bazează pe sistemul cloud ESET LiveGrid. Aplicațiile necunoscute potențial periculoase și alte amenințări posibile sunt monitorizate și transmise către cloud-ul ESET prin sistemul de feedback ESET LiveGrid. **Probele colectate sunt supuse sandboxing-ului automat și sunt analizate comportamental,** ceea ce duce la crearea de semnături automate, dacă trăsăturile malițioase sunt confirmate. Clienții ESET sunt sincronizați cu aceste detectări automate prin intermediul sistemului de reputație ESET LiveGrid fără a fi nevoie să aștepte următoarea actualizare a bazei de semnături. Timpul de răspuns al mecanismul este de obicei sub 20 de minute, ceea ce permite detectarea eficientă a amenințărilor emergente, chiar înainte ca semnăturile regulate să fie livrate către calculatoarele utilizatorilor.



PROTECȚIE BOTNET

Un element al malware-ului, care este costisitor pentru ca autorii săi să îl schimbe ușor, este schimbarea comunicării cu serverele C & C. **Protecția Botnet ESET este recunoscută pentru detectarea cu succes a comunicării rău intenționate utilizate de botneți indetificând, în același timp, procesele ofensatoare.**

Rețeaua de Semnături ESET extinde Tehnologia de Protecție Botnet pentru a aborda problemele generale asociate cu analiza traficului de rețea. Ele **permit detectarea mai rapidă și mai flexibilă a traficului rău intenționat.** Semnăturile standard din industrie, cum ar fi Snort sau BRO permit detectarea multor atacuri, dar Rețeaua de Semnături ESET este proiectată special pentru a viza vulnerabilități de rețea, kiturile exploit și comunicarea derulată de programele malware avansate.

Capacitatea de a efectua analiza traficului de rețea pe endpoint-uri are avantaje suplimentare. Ea ne permite să identificăm exact ce proces sau modul este responsabil pentru comunicarea malțioasă, permite luare de măsuri împotriva obiectului identificat și, uneori, poate chiar aproba criptarea comunicării pentru a nu fi ocolită.

Protecție reactivă vs proactivă astăzi

În timp ce Semnăturile ADN sunt excelent pentru detectarea chiar și a unei familii întregi de malware, ele trebuie să fie distribuite utilizatorilor pentru a-i proteja. Același lucru este valabil pentru motorul de scanare, euristica sau orice schimbare care vizează noile amenințări. În zilele noastre, este necesară comunicarea cu sistemul ESET LiveGrid bazat pe cloud, pentru a asigura cel mai înalt nivel de protecție pentru mai multe motive:

- Scanarea offline este în mare parte reactivă. A fi proactiv în zilele noastre nu mai înseamnă doar a avea cele mai bune euristici din produs. Atâta vreme cât soluțiile dvs. de protecție sunt disponibile pentru un atacator, nu contează dacă utilizați semnături, euristică sau mașini care folosesc clasificarea: un autor malware poate experimenta tehnologia de detectare, modifica malware-ul până când acesta nu mai este detectat și numai atunci îl eliberează. ESET LiveGrid contra-atacă această strategie malware.
- Actualizări nu sunt în timp real. Actualizări pot fi lansate mai des și pot fi livrate către utilizatori la fiecare câteva minute. Dar poate fi făcut acest lucru mai bine? Da: ESET LiveGrid permite o protecție instantanee, prin furnizarea de informații ori de câte ori este nevoie.
- Malware-ul încearcă să funcționeze fără a fi detectat de radar. Autorii de malware, mai ales în cazul spionajului cibernetic, încearcă să evite detectarea cât mai mult timp posibil. Atacurile puternic direcționate - spre deosebire de distribuțiile în masă, cum ar fi viermii de e-mail - implementează secvențe unice de malware unui număr mic de ținte, uneori, unuia singur. Noi folosim acest lucru împotriva autorilor de malware: obiectele care nu sunt populare și nu au o reputație bună sunt presupuse a fi potențial periculoase și analizate în detaliu, fie pe endpoint, fie sunt înregistrate pentru o analiză detaliată automatizată prin intermediul sistemului nostru de feedback LiveGrid. Sistemul de Reputație ESET LiveGrid conține informații despre fișierele, origini, similitudini, certificate, URL-uri și IP-uri.

Protecție folosind ESET LiveGrid

Cel mai simplu mod de a asigura o protecție cu ajutorul unui sistem cloud este folosirea de liste negre exacte cu ajutorul hashing-ului. Acest sistem funcționează bine atât pentru fișiere cât și pentru URL-uri, dar este capabil să blocheze numai obiecte care se potrivesc exact cu hash-ul. Această limitare a dus la inventarea hashing-ului fuzzy. Hashing-ul fuzzy ia în considerare similitudinea binară a obiectelor, ca obiecte similare care au același hash sau unul asemănător.

ESET a mutat hashing-ul fuzzy la nivelul următor. Noi nu efectuăm hashing de date, ci hashing-ul comportamental descris în Semnăturile ADN. Folosind hashing-ul ADN suntem capabili să blocăm mii de variante diferite de malware instantaneu.

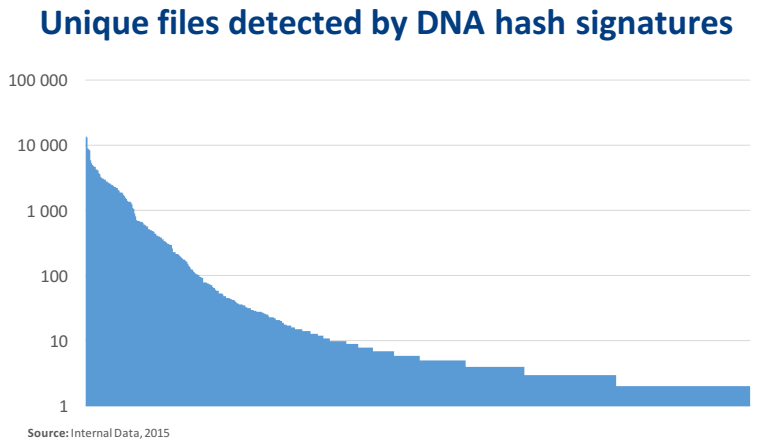


Fig.3: Numărul de fișiere unice (axa y) detectate de hash-urile ADN individuale (axa x).

Furnizarea unui sistem instantaneu de liste negre utilizatorilor nu este singurul scop al Sistemului de Protecție Împotriva Malware-ului Bazat pe Cloud. În cazul în care un utilizator decide să participe la procesul de depunere a eșantioanelor, ori de câte ori este identificat un nou eșantion cu o reputație îndoielnică acesta este trimis la ESET pentru o analiză aprofundată. Pentru a beneficia de întregul potențial al Sistemului de Protecție Împotriva Malware-ului Bazat pe Cloud, utilizatorii ar trebui să permită, de asemenea ca sistemul de feedback ESET LiveGrid să colecteze orice probe suspecte cu o reputație îndoielnică, pentru o analiză comportamentală aprofundată.

PRELUCRAREA AUTOMATĂ ȘI MANUALĂ A PROBELOR

În fiecare zi, ESET primește sute de mii de probe, care sunt prelucrate în mod automat, semi-automat și manual după pre-procesare și grupare. **Analiza automatizată este realizată prin instrumente dezvoltate intern, pe o serie de mașini virtuale și reale.** Clasificarea se realizează folosind atribute diferite extrase în timpul execuției, în conformitate cu: analiza de cod static și dinamic, cu modificările aduse sistemului de operare, cu modelele de rețea de comunicare și similitudinea cu alte mostre de malware sau cu caracteristicile ADN și informații structurale de detectare a anomaliilor.

Toate clasificatoarele automate au dezavantaje:

- **Alegerea caracteristicilor discriminatorii pentru clasificare nu poate fi automatizată** și trebuie realizată cu ajutorul cunoștințelor oamenilor care sunt experți în domeniul malware-ului.
- **Clasificatoarele bazate pe machine-learning necesită participarea experților umani** pentru a verifica intrările utilizate pentru învățare. Cu prelucrare complet automatizată, în cazul în care eșantioanele clasificate de către sistem ar fi utilizate ca intrări în sistem, un efect de bulgăre de zăpadă de la bucla de feedback pozitiv ar face rapid sistemul instabil. "Garbage in – garbage out".
- Algoritmii de învățare ai mașinii nu înțeleg datele **și chiar dacă informația este corectă din punct de vedere statistic, nu înseamnă că este validă.** De exemplu, mașina de învățare nu poate distinge noile versiuni ale software-ului curat de versiunile malformate și nu poate distinge un modul de actualizare legat de o aplicație curată de un downloader utilizat de malware, și nu poate recunoaște atunci când componentele software curate sunt folosite în scopuri rău intenționate.
- Cu sistemul de învățare automatizat al mașinii, adăugarea de noi probe la un proces de învățare poate provoca răspunsuri fals pozitive, iar eliminarea fals pozitivelor poate reduce eficiența detectării pozitivelor adevărate.
- În timp ce procesarea automată permite răspunsuri instantanee la noile amenințări cu ajutorul ESET LiveGrid, prelucrarea suplimentară a probelor de către inginerii de detectare este esențială pentru a asigura cea mai mare rată de calitate și de detecție și cel mai mic număr de rezultate fals pozitive.

Servicii de reputație

ESET LiveGrid oferă, de asemenea, reputație pentru obiecte. Noi verificăm reputația diferitelor entități, inclusiv fișiere, certificate, URL-uri și IP-uri. După cum este descris mai sus, reputația poate fi utilizată pentru a identifica noi obiecte periculoase sau surse de infecție. Există, totuși și alte utilizări.

Scanarea cu liste albe

Scanarea whitelisting este o caracteristică care reduce timpul de care motorul de scanare are nevoie pentru a inspecta un obiect. În cazul în care suntem siguri că un obiect nu a fost modificat și este curat, nu este nevoie să efectuăm o scanare totală. Acest lucru are un impact pozitiv asupra performanței și ajută produsele ESET să fie discrete. Așa cum am spus, "cel mai rapid cod este cel care nu se execută deloc". Listele albe ESET sunt în mod constant adaptate la realitatea în continuă schimbare din lumea software-ului.

Colectarea de informații

În cazul în care un utilizator decide să participe la trimiterea de statistici ESET LiveGrid, noi utilizăm aceste informații pentru urmărirea și monitorizarea amenințărilor globale. Aceste informații ne oferă date de cercetare importante pentru a lucra și **ne permite să ne concentrăm asupra celor mai urgente și problematice cazuri, să observăm tendințele malware-ului și să planificăm și să prioritizăm dezvoltarea tehnologiilor de protecție.**

DESPRE FPS ȘI IOCS

Indicatorii de compromis (IOCs) sunt percepuți ca fiind foarte importanți în securitatea corporativă actuală, dar aceștia sunt departe de a fi speciali sau avansați, chiar dacă sunt supraestimați de către furnizorii de securitate "next-gen". Imaginea de mai jos este o defalcare a IOCs-urilor cei mai predominanți, indicând pe ce sunt bazați.* După cum putem vedea, caracteristicile prezentate sunt extrem de simple: Într-un sfert dintre cazuri este vorba despre cunoscutul MD5s, nume de fișiere, etc. Aceste rezultate clarifică faptul că acest lucru nu este o metodă adecvată pentru prevenire și blocare, deși poate fi util pentru analiza de tip forensic. Este ironic faptul că unii dintre furnizorii "next-gen" care nu acceptă detecțiile pe bază de semnătură "învechite" utilizate pentru "vechiul AV" laudă IOCs atât de mult, chiar dacă acestea sunt cea mai slabă modalitate pe bază de semnături pentru a detecta fișierele sau evenimentele malware.

*Sursa datelor: IOC Bucket, aprilie 2015. IOC Bucket este o platformă gratuită, dedicată pentru a oferi comunității din domeniul securității o modalitate de a schimba informații despre amenințări.

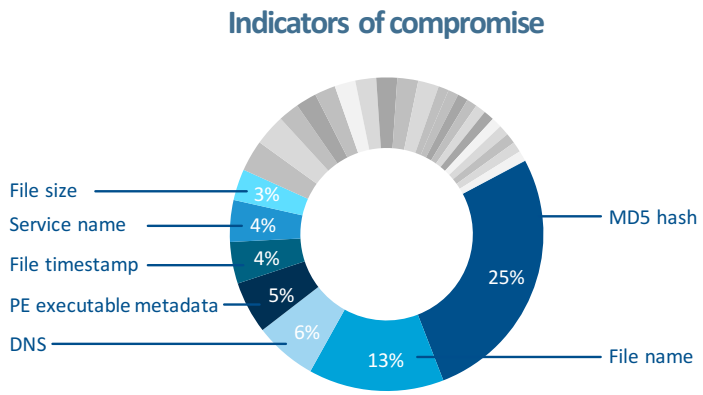


Fig.4: Analiza indicatorilor de compromis din IOC Bucket (probă aprilie 2015).

CONCLUZII

Nu există niciun glonț de argint în materie de securitate. Malware-ului de astăzi, fiind dinamic și adesea targetat, necesită o abordare pe mai multe niveluri, bazată pe tehnologii proactive și inteligente, care să ia în considerare petabytes de informații de analiză, adunați pe parcursul multor ani de către cercetătorii cu experiență. Privind în urmă cu 20 de ani, ESET a recunoscut că AV - abordarea tradițională - a fost o soluție incompletă, moment în care am început includerea tehnologiei proactive în motorul nostru de scanare și, treptat, am pus în aplicare diferite straturi de protecție pentru a lovi în diferite etape ale unui atac cibernetic în lanț.

ESET este unul dintre puținii furnizori de securitate capabili să asigure un nivel ridicat de protecție bazându-se pe mai mult de 25 de ani de cercetare. Acest lucru ne permite să fim cu un pas înaintea malware-ului, îmbunătățind în mod constant tehnologiile noastre, mergând dincolo de utilizarea semnăturilor standard, statice. Combinația noastră unică de tehnologii bazate pe endpoint și pe cloud oferă cea mai avansată modalitate de securitate împotriva malware-ului de pe piață.