Amenințările de tip RANSOMWARE

Aurelian Mircea Grigore, Membru activ în ISACA Romania și Membru Colaborator al ANSSI

Toma Cîmpeanu, CEO Asociația Națională pentru Securitatea Sistemelor Informatice

Programele malware pot exista într-o varietate de forme, cum ar fi key loggers, viruși, viermi, troieni, ransomware, spyware, adware și botnet-uri, pentru a numi doar câteva. Programele malware pot fi încorporate în tipuri diferite de fișiere, și pot fi activate prin simpla accesare a unui fișier rău intenționat sau a link-ului dintr-un e-mail. Aceste programe pot fi „plantate", în mod intenționat sau accidental, pe site-uri web. De asemenea, programele malware pot fi răspândite prin intermediul unui software de comunicații (e-mail, chat etc), unor suporturi de memorie mobile (unități de stocare USB, CD-uri, dischete), wireless, prin dispozitive mobile infectate, precum și prin însăși o rețea compromisă.

Programele malware exploatează punctele slabe și vulnerabilitățile sistemelor software la nivelul sistemului de operare (OS), aplicațiilor, utilitarelor software, dar și la niveluri hardware (ex. chip-uri de calculator). Complexitatea software-ului oferă un avantaj pentru cei care dezvoltă malware, astfel programele malware sofisticate și utilizatorii acestora, pot ascunde activitățile lor și își pot acoperi urmele prin furnizarea de adrese false, redirecționarea traficului, ștergerea activităților lor (de exemplu, ștergerea fișierelor și a informațiilor din fișierele jurnal), „plantând" informații false sau lucrând în afara țării care în care se desfășoară activitatea rău intenționată. Aplicațiile malware polimorfe își schimbă semnăturile (ex. nume de fișiere și locații) și/sau indicatorii de compromitere, astfel încât software-ul antivirus nu poate identifica componentele programului pentru a le elimina. Unele tipuri de malware fac foarte dificilă eliminarea, deoarece acestea se pot ascunde prin modificarea setărilor de fișiere și permisiuni de directoare. În unele cazuri, programele malware par a fi eliminate, dar apoi se vor reinstala după repornire.

Fenomenul malware a crescut de la evenimente pur și simplu deranjante la software și sisteme care pot compromite computerele guvernamentale, pot captura informații de acces sau pot fura banii unui individ. Cei care controlează programe malware pot obține informații personale și financiare, pot afecta companiile și instituțiile financiare, amenințând mijloacele de trai ale oamenilor și averea personală.

Dezvoltatorii de malware au creat aplicații pentru a controla alte programe periculoase sau rețele de calculatoare infectate. Au apărut astfel rețele de calculatoare/terminale infectate de tip botnet controlate prin intermediul unor centre de comandă și control (C & C).

Unele dintre utilizările unui bot sau botnet includ:

- Rularea unui atac distribuit denial-of-service (DDoS), care poate trimite fluxuri mari de pachete User Datagram Protocol (UDP), cereri Internet Message Protocol Control (ICMP) sau Transmission Control Protocol (TCP) sync requests
- Infectarea altor computere dintr-o rețea prin preluarea controlului complet al unei mașini victimă
- Utilizarea și partajarea de cantități mari de lățime de bandă în rândul comunităților hacker-ilor
- Instalarea unui backdoor pentru a menține accesul după o exploatare cu succes
- Găzduirea datelor ilegale pe un sistem făcându-l parte a unei rețele de partajare de informații ilegale (software sau filme piratate)

Pentru a infecta sau a compromite un sistem informatic, un atac cibernetic trece prin trei faze:

1 **Pre-compromiterea** - Această etapă constă din:
   a. Recunoașterea țintei sau a victimei
   b. Personalizarea programelor malware pentru provocarea de daune, obținerea de date și spionarea țintei
   c. Stabilirea unui mijloc de acces

2 **Compromiterea** - În această etapă, sistemul țintă este exploatat în avantajul atacatorului (hacker) și, ulterior, malware-ul este instalat pe sistemele vulnerabile.

3 **Post-compromiterea** - Odată compromise sistemele vulnerabile ale rețelei, atacatorul stabilește un centru de C & C pentru a direcționa atacurile cibernetice viitoare.

Infractorii cibernetici nu folosesc numai programe malware pentru a avea acces la informații proprietare, sensibile si personale, ci aplică și tehnici de tip „piggyback" pentru:

- Capturarea informațiilor de acces on-line banking
- Transmiterea de surse și destinații Internet Protocol (IP) și liste de e-mail
- Manipularea site-urilor de jocuri de noroc online, în avantajul lor
- Monitorizarea practicilor neadecvate de actualizare a sistemelor
- Studierea de obiceiuri și rutine de navigare ale țintei
- Capturarea activităților de navigare pe mobil ale țintei
- Studierea rețelelor sociale și site-urilor de mesagerie

Practicile neadecvate de programare si timpul au permis infractorilor cibernetici să devină organizați și fiind conștienți că nu toată lumea dispune de cea mai bună securitate, au inceput să vizeze persoanele mai puțin pregătite.

Evoluția Ransomware

Utilizarea instrumentelor ransomware de către infractorii cibernetici și rezultatele înregistrate au condus la dezvoltarea şi diversificarea acestora. Pe parcursul ultimelor câteva luni, cercetatorii au raportat, pentru prima dată, **un ransomware capabil să cripteze fișierele fără conexiune la Internet**, nefiind necesară comunicarea cu serverele lor C & C pentru procesul de criptare.

Printre noile instrumente se remarcă ***Locky*** ransomware, al cărui mod de operare se aseamănă cu troianul bancar ***Dridex***, precum și o versiune nouă a ***CTB-Locker*** care atacă serverele de web. CTB-Locker, vizează site-uri web WordPress, criptează fișierele și-i cere proprietarului site-ului răscumpărarea acestora.

În plus, ofertele ***RaaS*** (Ransom-as-a-Service) sunt din ce în ce mai populare pe site-urile închise DeepWeb și forumuri Darknet. Aceste servicii permit potențialilor atacatori crearea cu ușurință de variante ransomware, profiturile fiind obținute din viitoarele infecții de succes. Recent, a fost identificat un nou RaaS „botezat" ***Cerber*** ransomware, care este oferit pe un forum subteran din Rusia. Anterior acestuia a fost ***ORx-Locker***, oferit ca un serviciu prin intermediul unei platforme găzduite pe un ***.onion server***.

Ransomware-ul se răspândește putând lua forme noi, inclusiv tradiționalele link-uri de e-mail sau site-uri web de phishing.

Utilizarea JavaScript în Ransomware

Cercetătorii in securitate au descoperit o noua variantă a RaaS - ransomware-as-a-service: ***Ransom32***. Spre deosebire de altele, inclusiv ***Tox*** și ***FAKIN***, aceasta dezvoltare este oarecum diferită, deoarece folosește un framework JavaScript numit NW.js. Computerworld a semnalat această evoluție la începutul lunii ianuarie.

Ransom32 solicită ca victimele sa efectueze plata în termen de 4 zile, altfel, în termen de o săptamână, întregul hard disk va fi distrus.

Bio - Aurelian Mircea Grigore

Aurelian Mircea Grigore activează de 15 ani în domeniul securității cibernetice, cu o experiență acumulată pe parcursul evoluției profesionale. A ocupat funcții de administrator de sistem, specialist în tehnologii de securitate, consultant în Securitate informatică, auditor de sisteme informaționale si a dezvoltat servicii de securitate cibernetică pentru infrastructurile critice, sisteme de control industrial și SCADA precum și pentru sectoarele public, bancar și IMM.
A participat la traducerea și adaptarea de standarde de securitate în cadrul ASRO, este membru activ în ISACA Romania și Membru Colaborator al ANSSI.
A colaborat cu fundația CAESAR și TaskForce AMCHAM pentru promovarea securității cibernetice.

Bio - Toma Cîmpeanu

Toma Cîmpeanu a absolvit ca șef de promoție facultatea de matematică și facultatea de automatizări și calculatoare, are doctoratul și un master în sisteme de coordonare și control, precum și un MBA cu o universitate britanică. În ultimii 15 ani a ocupat poziții de conducere în companii de stat și private cum ar fi SN Radiocomunicații, TAROM, Informatica Feroviară, grupul SCOP Computers, eSign România sau TotalSoft. De asemenea, a fost Secretar de Stat în Ministerul pentru Societatea Informațională, reprezentantul României și membru al Board-ului ENISA, Președinte al Agenției pentru Serviciile Societății Informaționale și Vicepreședinte al Centrului Național "România Digitală". Și-a legat numele de strategia eRomânia, sistemul național eLicitație și Punctul de Contact Unic al României. Toma Cîmpeanu a activat în domeniul academic la Universitatea din Craiova și a condus operațiunile Institutului de Management și Dezvoltare Durabilă, singura organizație românească care a coordonat la nivel global un grup de lucru al ONU. Din 2015, Toma Cîmpeanu este CEO al Asociației Naționale pentru Securitatea Sistemelor Informatice.

Problema rezidă în faptul că NW.js este un framework legitim, ceea ce face chiar mai dificil ca Ransom32 să fie adăugat la soluții de detectare a programelor malware bazate pe semnături, jucătorii din piața de securitate raportând că mulți dintre ei nu au avut o acoperire mare de detecție pentru primele câteva săptămâni după ce software-ul a fost descoperit.

Ransomware continuă să crească

Atacurile ransomware și amenințările avansate aferente au crescut în număr și rafinament în ultimul an. Variantele anterioare ransomware au suferit o scădere de 10 până la 30 la sută a profitului în cazul în care acestea au fost folosite de către infractori, în timp ce Ransom32 urcă la 25 la sută.

Până în prezent, Ransom32 a fost observat doar infectând PC-uri Windows, dar nu se așteaptă să rămână limitat la Windows pentru foarte mult timp, infractorii cibernetici generând pachete pentru Linux sau Mac pentru a-şi extinde spectrul de acțiune.

Cerber Ransomware - Nou, dar matur

Un nou ransomware criptografic, numit ***Cerber*** de creatorii săi, a început recent să vizeze utilizatorii de Windows.

Comportamentul Cerber este asemănător cu majoritatea ransomware:

- Codează o largă varietate de fișiere de sistem (inclusiv share-uri Windows și de rețea) cu criptare AES-256, și adaugă extensia .cerber
- Evită infectarea utilizatorilor în majoritatea statelor post-Sovietice
- Prezintă note de răscumpărare cu instrucțiuni privind modul de efectuare a plății (acesta solicită inițial 1,24 Bitcoin), și oferă posibilitatea de a decripta un fișier ca un demonstrație de bună-credință.

Un alt lucru interesant este faptul că Cerber nu este propagat de către dezvoltatorii săi. În schimb, ei oferă aceasta «ca serviciu» vizitatorilor unui forum subteran închis din Rusia. Până în prezent, victimele nu au nicio modalitate de a-și decripta ei înșiși fișierele, astfel încât acestea fie plătesc prețul și **speră** că infractorii le vor trimite cheia de decriptare, sau se resemnează și renunță la fișierele respective pentru totdeauna.

KeRanger - Noul ransomware vizează pentru prima dată Mac-urile

Hackerii au infectat Mac-uri cu ***KeRanger*** ransomware printr-o copie contaminată Transmission, un program popular pentru transferul de date prin intermediul rețelei de partajare de fișiere peer-to-peer BitTorrent.

KeRanger, care blochează datele de pe Mac-uri, făcându-le inaccesibile utilizatorilor, a fost descărcat de aproximativ 6500 de ori înainte ca Apple si dezvoltatorii sa fie capabili să-l contracareze.

Mai mult, experții în securitate cibernetică au declarat că în perioada următoare se așteaptă la o creştere a atacurilor pe Mac-uri.

Distribuția ransomware

Cea mai mare parte a vectorilor de distribuție de variante ransomware implică ingineria socială. De exemplu, sunt utilizate mesajele de poștă electronică, inclusiv fișiere Office rău intenționate, mesajele de tip spam cu linkuri malițioase sau campanii de publicitatea dăunătoare care exploatează site-uri WordPress vulnerabile sau site-uri Joomla cu cod malițios încorporat. Distribuirea profită de asemenea, de avantajul comenzilor macro și kit-urilor de exploatare (exploit kits), cum ar fi Nuclear sau Angler. Uneori sunt exploatate vulnerabilitățile browser-ului sau certificatele digitale furate.

Manipularea atacurilor Ransomware

Un val recent de atacuri ransomware a fost observat la nivel global, cu un număr mare de infecții raportate în Statele Unite ale Americii, Marea Britanie, Germania și Israel. Atacatorii nu par a avea un obiectiv specific, țintele fiind foarte diverse: spitale, instituții financiare și companii, şi neputându-se identifica o industrie vizată preponderent.

În continuare, gasiti sugestiile noastre privind acțiunile recomandate pentru a evita atacurile de tip ransomware, precum și modul de acțiune în cazul după infectări:

Apărați organizația împotriva potențialelor amenințări

- Instruirea angajaților dumneavoastră - deoarece componenta umană este cea mai slabă verigă din securitatea cibernetică organizațională și majoritatea cazurilor implică inginerie socială asupra unora dintre angajați. Stabiliți reguli privind utilizarea sistemelor companiei și descrieți cum arată mesajele de phishing.
- Creșterea gradului de conștientizare în ceea ce privește acceptarea fișierelor care sosesc prin intermediul mesajelor de e-mail - instruiți angajații dumneavoastră să nu deschidă fișiere suspecte sau fișiere trimise de expeditori necunoscuți. Luați în considerare punerea în aplicare a unei politici organizaționale privind abordarea unor astfel de fișiere. Vă recomandăm blocarea sau izolarea fișierelor cu următoarele extensii: js (JavaScript), jar (Java), bat (Batch file), exe (executable file), cpl (Control Panel), scr (Screensaver), com (COM file) and pif (Program Information file).
- Dezactivați script-urile Macro care rulează pe fișiere Office trimise prin e-mail - in ultimele luni, au fost raportate mai multe cazuri de atacuri ransomware care utilizează acest vector. De obicei, comenzile Macro sunt dezactivate în mod implicit și nu recomandăm să le permiteți activarea. In plus, vă sugerăm să utilizați software-ul Office Viewer pentru a deschide fișiere Word și Excelpentru care nu este necesară editarea.
- Limitarea privilegiilor de utilizator și monitorizarea în mod constant a stațiilor de lucru - gestionarea atentă a privilegiilor de utilizator și a privilegiilor de administrator poate ajuta la evitarea răspândirii ransomware în rețeaua organizației. Mai mult decât atât, monitorizarea activității asupra

stațiilor de lucru va fi utilă pentru depistarea timpurie a oricărei infecții și blocarea înmulțirii către alte sisteme și resurse de rețea.

- Creați reguli care blochează programele de executare din dosarele AppData / LocalAppData. Mai multe variante ale ransomware-ului sunt executate din aceste directoare, inclusiv CryptoLocker. Prin urmare, crearea unor astfel de norme poate reduce riscul de criptare în mod semnificativ.
- Păstrați sistemele dvs. actualizate - în multe cazuri, hackerii profita de sisteme învechite pentru a se infiltra în rețea. Prin urmare, actualizările frecvente ale sistemelor organizaționale și implementarea patch-urilor de securitate publicate pot reduce în mod semnificativ șansele de infecție.
- Utilizați un software terț dedicat pentru a face față amenințării. De exemplu, AppLocker pentru Windows, care este inclus în sistemul de operare, ajută la combaterea malware. Vă recomandăm contactarea unui furnizor de securitate organizațională și luarea în considerare a soluțiilor oferite.

Acțiuni de urmat dacă sunteți infectat

- Restaurarea fișierelor - unele instrumente ransomware crează o copie a fișierului, o criptează și apoi șterge fișierul original. În cazul în care ștergerea se realizează prin intermediul funcțiilor de ștergere din sistemului de operare, există o șansă de a restabili fișierele, deoarece, în majoritatea cazurilor, sistemul de operare nu suprascrie imediat fișerele.
- Decriptarea fișierelor criptate - decriptarea va fi posibilă dacă au fost infectate cu unul dintre următoarele trei tipuri ransomware: Bitcryptor, CoinVault sau Linux.Encoder.1. Prin urmare, detectarea exactă a genului de ransomware care a atacat PC-ul este crucială.
- Efectuați back-up pentru fișiere pe un dispozitiv de stocare separat în mod regulat - cele mai bune practici pentru a evita daunele produse de un atac ransomware este de a efectua back-up pentru toate fișierele importante pe un dispozitiv de stocare deconectat de la rețeaua organizațională, deoarece unele variante ransomware sunt capabile de a cripta fișierele stocate pe dispozitive conectate. De exemplu, cercetătorii au raportat recent un ransomware care criptează fișierele stocate pe folderul Cloud Sync.
- Dacă este detectat ransomware în organizație, deconectați imediat echipamentul infectat de la rețea. Nu încercați să eliminați malware-ul și nu reporniți sistemul înainte de a identifica varianta de ransomware. În unele cazuri, efectuarea uneia dintre aceste acțiuni vor face decriptarea imposibilă, chiar și dacă se plăteşte răscumpărarea. ■

ANSSI - Partener editorial permanent Cybersecurity Trends

Asociația Națională pentru Securitatea Sistemelor Informatice (ANSSI) a fost înființată în anul 2012 ca un liant între sectorul public și mediul de afaceri, pentru promovarea practicilor de succes și facilitarea unei schimbări culturale în domeniul securității informației. Identificarea și sesizarea factorilor cu competențe administrative în cazul eventualelor deficiențe de pe piața IT, precum și pentru coagularea unor forme de parteneriat public-privat care să conducă la creșterea eficienței si operaționalității sistemelor informatice implementate în România au fost preocupări constante ale asociației. ANSSI este o organizație neguvernamentală, nonprofit, profesională și independentă. Ea reunește 40 de membri, companii cu aproximativ 20000 de angajați, reprezentând 25% din totalul salariaților din industria privată de IT și comunicații. Membrii ANSSI, prin spectrul larg și diversitatea de capabilități tehnico-profesionale deținute, formează un grup reprezentativ la nivel sectorial, ale cărui teme de interes reflectă fidel preocupările generale ale domeniului.

ANSSI s-a implicat activ, organizând singur sau împreună cu alte autorități, instituții sau ambasade, conferințe și simpozioane naționale dar și internaționale, în domenii conexe, cum ar fi comunicațiile electronice, soluțiile și sistemele de e-guvernare și e-administrație, accesarea instrumentelor structurale, dezvoltarea profesională sau standardele ocupaționale, în care componenta de securitate tehnologică și de infrastructură IT au constituit preocuparea centrală.