CENTRUL NAŢIONAL DE RĂSPUNS LA INCIDENTE DE SECURITATE

CIBERNETICĂ CERT-RO

GHID
privind combaterea amenint a rilor informatice de tip „ransomware”

- Versiunea: 1.0 / Data: 15.03.2016 -

Adresă: Bd. Mareșal Averescu nr. 8-10, București, sector 1, Cod Postal: 011455, Tel: +4031-6202187, E-mail: office@cert.ro, Web: www.cert.ro

1. Despre ransomware

Ransomware-ul este un malware (software malițios) ce împiedică accesul la fișiere, sau chiar la întregul sistem informatic infectat, până la plata unei „recompense” (ransom). Astfel, ransomware-ul este una dintre cele mai supărătoare forme de malware, întrucât produce pagube financiare directe, iar de cele mai multe ori fișierele criptate de malware nu pot fi decriptate.

Pentru a îngreuna procesul de recuperare a fișierelor, ransomware-urile blochează accesul la fișiere (documente, fotografii, muzică, video etc.) prin criptarea asimetrică a acestora.

Având în vedere evoluția acestui tip de amenințare, atât prin prisma activității CERT-RO, dar ținând cont și de cele mai recente studii ale companiilor de securitate cibernetică, ne putem aștepta ca în anul 2016 tot mai mulți cetățeni, instituții și companii să fie afectate de ransomware. Din acest motiv, singurul răspuns adecvat acestei amenințări este prevenția.

În acest context, Centrul Național de Răspuns la Incidente de Securitate Cibernetică – CERT-RO recomandă utilizatorilor și organizațiilor din România să respecte următorul set minim de măsuri în scopul prevenirii infectării cu ransomware, dar și pentru diminuarea daunelor produse în eventualitatea infectării.

2. Măsuri de prevenție

CERT-RO vă recomandă implementarea următoarelor **10 măsuri de prevenire a infecțiilor cu diferite forme de malware, în special ransomware**:

1. Fiți precauți

Această recomandare este general valabilă pentru a spori securitatea sistemelor informatice pe care le utilizați/administrați. Este deja bine-cunoscut faptul că utilizatorul reprezintă veriga cea mai slabă din lanțul ce formează securitatea cibernetică, fapt pentru care majoritatea atacurilor vizează exploatarea componentei umane (social engineering, phishing, spear phishing, spam etc.). În consecință, vă recomandăm să nu accesați link-urile sau atașamentele conținute de mesajele email suspecte înainte de a verifica în prealabil sursa/legitimitatea acestora. De asemenea, o atenție sporită trebuie acordată site-urilor web pe care le accesați și surselor online pe care le utilizați pentru descărcarea sau actualizarea aplicațiilor.

2. Faceți copii de siguranță (backup) ale datelor

Cea mai eficientă metodă pentru combaterea amenințării ransomware este realizarea periodică de backup pentru datele stocate/procesate cu ajutorul sistemelor informatice. Astfel, chiar dacă accesul la date este blocat de către un ransomware, datele dumneavoastră vor putea fi restaurate rapid, iar daunele provocate vor fi minime.

IMPORTANT! Pentru backup utilizați un mediu de stocare extern care nu este conectat în permanență la sistem, altfel existând riscul ca, în cazul infectării cu ransomware, să fie criptate și fișierele de pe respectivul mediu de stocare.

Adresă: Bd. Mareșal Averescu nr. 8-10, București, sector 1, Cod Postal: 011455, Tel: +4031-6202187, E-mail: office@cert.ro,
Web: www.cert.ro

3. **Activați opțiunile de tip „System Restore”**

   În cazul sistemelor de operare Windows, vă recomandăm activarea opțiunii „System Restore” pentru toate partițiile de stocare. În cazul infectării sau cu malware sau compromiterii unor fișiere (chiar și fișiere de sistem), datele ar putea fi rapid restaurate prin aducerea sistemului la o stare anterioară. **ATENȚIE!** Nu vă bazați exclusiv pe această facilitate deoarece unele versiuni recente de ransomware șterg datele din „System Restore”.

4. **Implementați mecanisme de tip „Application Whitelisting”**

   „Application Whitelisting” presupune implementarea unui mecanism care să asigure faptul că în cadrul unui sistem informatic rulează numai software autorizat/cunoscut. Conceptul în sine nu este nou, reprezentând practic o extindere a abordării „default deny” (nu permite în mod implicit) utilizată de mult timp de soluțiile de securitate de tip firewall. În prezent, „application whitelisting” este considerată una dintre cele mai importante strategii de combatere a amenințării malware și există deja o varietate de soluții tehnice cu ajutorul cărora poate fi implementată, inclusiv de către utilizatorii casnici, mai ales în cadrul sistemelor de operare Windows unde implementarea se poate realiza utilizând uneltele deja conținute de sistemul de operare: **SRP (Software Restriction Policies)**, **AppLocker** (unealta recomandată începând cu sistemul de operare Windows 7, având același scop ca și facilitatea SRP din Group Policy).

5. **Dezactivați execuția programelor din directoare precum %AppData% și %Temp%**

   O soluție alternativă la mecanismul de tip „Application Whitelisting” (nu la fel de eficientă, însă care aduce un spor semnificativ de securitate) este blocarea execuției programelor din directoare ca **%AppData%** și **%Temp%**, prin intermediul politicii de securitate (**GPO** – Group Policy Object) sau utilizând o soluție de tip **IPS** (Intrusion Prevention Software).

6. **Afișați extensiile fișierelor**

   Unele tipuri de ransomware, precum Cryptolocker, sunt livrate sub forma unor fișiere cu extensie cunoscută (.doc, .docx, .xls, .xlsx, .txt etc.) la care se adaugă extensia „.exe”, caracteristică fișierelor executabile, rezultând extensii de forma „.docx.exe”, „.txt.exe” etc. Astfel, afișarea extensiilor fișierelor poate facilita observarea fișierelor suspicioase/malițioase. Este recomandat să nu rulați niciodată fișiere executabile venite prin email.

7. **Actualizați în permanență sistemele de operare și aplicațiile**

   Actualizarea aplicațiilor/programelor utilizate reprezintă o măsură obligatorie pentru asigurarea unui nivel de securitate ridicat al sistemul informatic. De cele mai multe ori, un software neactualizat este echivalentul unei uși deschise (backdoor) pentru infractorii din mediul cibernetic. În general producătorii de software, precum Microsoft și Adobe, publică în mod regulat actualizări (update-uri) pentru sistemele de operare și aplicații, utilizatorul având posibilitatea să configureze descărcarea și instalarea automată a acestora. Astfel, vă recomandăm să activați opțiunea pentru actualizări automate acolo unde este posibil și să aveți în vedere modalitatea cea mai eficientă pentru actualizarea celorlalte programe (verificarea periodică a versiunilor pe site-ul producătorilor).

   ATENȚIE! Deseori, programele malițioase au fost livrate sub forma unui update de software. Verificați cu atenție sursele utilizate pt. descărcarea/actualizarea de software.

Adresă: Bd. Mareșal Averescu nr. 8-10, București, sector 1, Cod Postal: 011455, Tel: +4031-6202187, E-mail: office@cert.ro, Web: www.cert.ro

8. Utilizați soluții de securitate eficiente și actualizate

O măsură absolut necesară pentru prevenirea infecțiilor cu diferite tipuri de malware o reprezintă utilizarea uneia sau mai multor soluții software de securitate eficiente și actualizate care să dispună de facilități/servicii de tip antivirus, antimalware, antispyware, antispam, firewall etc.

9. Utilizați instrumente software pentru monitorizarea fișierelor

Utilizarea de instrumente software pentru monitorizarea fișierelor (accesare, modificare, ștergere etc.) poate fi de ajutor pentru observarea rapidă a unor comportamente suspicioase în cadrul sistemelor informatice sau rețelei.

10. Manifestați atenție sporită la accesarea reclamelor web

Unele dintre versiunile de ransomware investigate de CERT-RO în ultimul timp au fost livrate prin intermediul unor reclame malițioase (malvertising) afișate pe site-uri web populare (știri, magazine online etc.). Vă recomandăm să evitați pe cât posibil accesarea reclamelor și chiar utilizarea unor instrumente software (de tip „add block") care să blocheze automat încărcarea/afișarea reclamelor.

3. Măsuri de eradicare și limitare a efectelor

În eventualitatea infectării cu ransomware, CERT-RO **vă recomandă implementarea următoarelor 8 măsuri de eradicare și limitare a afectelor ransomware**:

1. Deconectați mediile de stocare externe

Deconectați urgent toate mediile de stocare externe conectate la PC (memorie USB, card de memorie, hard disk extern etc.), de-conectați cablul de rețea și dezactivați orice alte conexiuni de rețea (WiFi, 3G etc.). Astfel se previne afectarea fișierelor stocate pe mediile de stocare externe sau celor accesibile prin rețea (network share, cloud storage etc.).

2. [Opțional]. Realizați o captură de memorie (RAM)

În cazul în care se urmărește investigarea ulterioară a incidentului și eventual încercarea de a recupera cheile de criptare utilizate de ransomware din memorie, realizați cât mai rapid o captură de memorie (RAM), înainte de oprirea PC-ului, utilizând o unealtă specializată.

ATENȚIE! Există riscul ca până la finalizarea procesului de realizare a unei capturi de memorie să fie afectate (criptate) cât mai multe fișiere (sau chiar toate). Decizia de a opri imediat PC-ul sau de a efectua mai întâi o captură de memorie trebuie luată în funcție de priorități (sunt mai importante datele sau posibilitatea efectuării unei analize ulterioare?). Spre exemplu, dacă există un backup pentru datele stocate pe PC-ul afectat, sau fișierele nu sunt considerate importante, se poate lua decizia de a efectua o captură de memorie.

Adresă: Bd. Mareșal Averescu nr. 8-10, București, sector 1, Cod Postal: 011455, Tel: +4031-6202187, E-mail: office@cert.ro,
Web: www.cert.ro

3. Opriți PC-ul (Shutdown)

În cazul în care suspectați că un PC a fost infectat cu ransomware și decideți să nu realizați o captură de memorie (conform pct. 2), vă recomandăm să-l opriți imediat pentru a limita cât mai mult numărul fișierelor criptate.

4. [Opțional] Realizați o copie (imagine) de HDD

În cazul în care se urmărește investigarea ulterioară a incidentului și eventual încercarea de a recupera o parte din fișiere cu ajutorul unor instrumente de tip „Data Recovery", realizați o copie de tip „bit cu bit" (imagine) a hard-disk-urilor afectate de ransomware, utilizând o unealtă specializată.

5. Realizați un back-up „offline" al fișierelor

Porniți PC-ul (boot) utilizând un sistem de operare care se încarcă de pe un mediu de stocare extern (CD, DVD, memorie USB etc.), majoritatea distribuțiilor moderne de Linux oferind această facilitate. Copiați pe un alt mediu de stocare toate fișierele de care aveți nevoie, inclusiv pe cele care au fost compromise (criptate).

6. Restaurați fișierele compromise

Cea mai simplă metodă de recuperare a fișierelor afectate de ransomware este restaurarea acestora din cadrul unor back-up-uri. În cazul în care astfel de back-up-uri nu sunt disponibile, vă recomandăm să încercați recuperarea fișierelor prin „System Restore" sau utilizând instrumente software specializate de recuperare date (de tip „Data Recovery").

ATENȚIE! Vă recomandăm să încercați recuperarea datelor cu uneltele software de tip „Data Recovery" numai de pe imaginile (copiille) de HDD (realizate conform pct. 4), altfel existând riscul să compromiteți șansele de reușită ale unor proceduri mai complexe ce presupun recuperarea datelor direct de pe mediile de stocare. Există soluții pentru a încerca recuperarea datelor direct de pe mediile de stocare, însă acestea necesită un nivel ridicat de expertiză și dotări tehnice speciale.

7. Dezinfectați sistemele informatice afectate

Cea mai sigură metodă prin care vă puteți asigura că sistemul informatic nu mai conține malware (sau rămășițe de malware) este re-instalarea completă a sistemului de operare, prin formatarea tuturor HDD-urilor/partițiilor în prealabil. În cazul în care acest lucru nu este posibil (spre exemplu în cazul în care se intenționează recuperarea datelor direct de pe HDD-urile afectate), vă recomandăm să utilizați una sau mai multe soluții de securitate de tip antivirus/antimalware /antispyware pentru scanarea sistemului și dezinfectare acestuia.

ATENȚIE! În cazul în care intenționați să încercați recuperarea de date de pe HDD-urile afectate, conform indicațiilor de la pct. 6, vă recomandăm să nu încercați dezinfectarea acestora și să utilizați alte HDD-uri pentru re-instalarea sistemului de operare.

8. Raportați incidentul către CERT-RO

CERT-RO vă recomandă să raportați incidentele de securitate cibernetică, inclusiv infecțiile cu ransomware, la adresa de email alerts@cert.ro, beneficiind astfel de suport tehnic și indicații de rezolvare a incidentelor si/sau limitare a efectelor acestora.

Adresă: Bd. Mareșal Averescu nr. 8-10, București, sector 1, Cod Postal: 011455, Tel: +4031-6202187, E-mail: office@cert.ro, Web: www.cert.ro

7. Bibliografie

[1]. https://www.us-cert.gov/ncas/alerts/TA14-295A ;

[2]. http://www.symantec.com/connect/blogs/ransomware-how-stay-safe ;

[3]. http://www.welivesecurity.com/2013/12/12/11-things-you-can-do-to-protect-against-ransomware-including-cryptolocker/ ;

[4]. http://blog.doctoroz.com/dr-oz-blog/protecting-yourself-against-the-threat-of-ransomware ;

[5]. https://cert.ro/citeste/ransomware-ul-ctb-locker ;

[6]. https://cert.ro/citeste/teslacrypt-si-alte-campanii-ransomware-pentru-care-exista-solutii-de-recuperare-a-fisierelor-criptate ;

Adresă: Bd. Mareșal Averescu nr. 8-10, București, sector 1, Cod Postal: 011455, Tel: +4031-6202187, E-mail: office@cert.ro,
Web: www.cert.ro