SIGURANȚA ONLINE.RO

#sigurantaonline

STOP MALWARE

Siguranța ta online depinde de tine

sigurantaonline.ro

O campanie inițiată de:

POLIȚIA ROMÂNĂ

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

Microsoft

BITDEFENDER SENTINEL

ATTACK SIMULATOR

Susținută de:

#DREPTUL LA BANKING

SIGURANȚA ONLINE.RO

Ghid privind combaterea amenințărilor informatice de tip „RANSOMWARE”

1 DESPRE RANSOMWARE

Ransomware-ul este un tip de malware (software malițios) care folosește criptare pentru a face inaccesibile fișierele sau chiar întregul sistem informatic infectat, până când utilizatorul legitim al acestuia plătește o sumă de bani (ransom) în schimbul deblocării.

Atacurile de tip ransomware pot viza orice computer, fie că este vorba de un computer de acasă, un dispozitiv mobil sau computere ori servere dintr-o rețea a unei companii sau alte entități, inclusiv instituții guvernamentale.

Ransomware-ul este una dintre cele mai dăunătoare forme de malware, întrucât produce pagube financiare directe, iar de cele mai multe ori fișierele criptate de anumite variante de ransomware nu pot fi deblocate.

Pentru a îngreuna procesul de recuperare a fișierelor, ransomware-urile blochează accesul la fișiere (documente, fotografii, muzică, video etc.) prin criptarea asimetrică a acestora. Aceasta este criptografia, care folosește o pereche de chei pentru a cripta și decripta un fișier.

Perechea de chei public-privată este generată în mod unic de către atacator pentru victimă, iar cheia privată, folosită pentru a decripta fișierele, este stocată pe serverul atacatorului. Atacatorul pune cheia privată la dispoziția victimei numai după ce răscumpărarea este plătită, deși, așa cum s-a văzut în campaniile recente de ransomware, acest lucru nu se întâmplă mereu, cheia privată nefiind mereu pusă la dispoziția victimei, chiar dacă răscumpărarea a fost plătită. Fără acces la cheia privată, este aproape imposibil să decriptezi fișierele blocate în urma unui atac ransomware.

Există multe variante de ransomware. Adesea, ransomware-ul (și alte programe malware) sunt distribuite prin campanii de tip phishing prin e-mail sau prin atacuri direcționate. Programele malware au nevoie de un vector de atac pentru ajunge pe computerul victimei. După ce ajunge pe sisteme, malware-ul rămâne în acestea până când sarcina este îndeplinită sau atât timp cât atacatorul dorește să își mențină prezența în rețeaua respectivă, iar computerul nu este curățat.

Cum și de ce se răspândește ransomware-ul?

Atacurile ransomware și variantele acestuia evoluează rapid pentru a contracara tehnologiile preventive din mai multe motive:

- Disponibilitate ușoară a kit-urilor de malware care pot fi utilizate pentru a crea noi mostre de malware la cerere
- Utilizarea unor interpreți generici cunoscuți si de bună calitate pentru a crea ransomware pe mai multe platforme (de exemplu, Ransom32 utilizează Node.js cu payload în JavaScript)
- Utilizarea de noi tehnici, cum ar fi criptarea discului complet în locul unor fișiere selectate
- În ultimii ani, atacatorii nici măcar nu trebuie să fie cunoscători de tehnologie. Au apărut piețe online de ransomware, oferind tulpini de malware oricărui potențial infractor cibernetic și generând profit suplimentar pentru autorii de malware, care cer adesea o parte din veniturile obținute din răscumpărare.

Având în vedere evoluția acestui tip de amenințare, atât prin prisma activității DNSC, dar ținând cont și de cele mai recente studii ale companiilor de securitate cibernetică, ne putem aștepta ca și în acest an 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, Directoratul Național de Securitate Cibernetică – DNSC 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

DNSC 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-uri pentru datele stocate/prelucrate cu ajutorul sistemelor informatice. Astfel, chiar dacă accesul la date este blocat de către o variantă de ransomware, datele dumneavoastră vor putea fi restaurate rapid, iar daunele provocate vor fi minime.

IMPORTANT! Pentru copia de siguranță (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.

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 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 sau din mesaje nesolicitate, venite din surse necunoscute.

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 sistemului 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 pentru descărcarea / actualizarea de software!

8. Utilizați soluții de securitate eficiente și actualizate

O măsură absolut necesară pentru prevenirea infecțiilor cu diferite tipuri de malware o reprezintă utilizarea unei (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 DSNC 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.

Următoarele recomandări se adresează companiilor în vederea prevenirii infecțiilor cu diferite forme de malware, în special ransomware:

- **Igiena credențialelor:** Practicarea unei bune igiene a credențialelor poate ajuta la prevenirea atacurilor cu forță brută, la atenuarea efectelor furtului de credențiale și la reducerea riscului de acces neautorizat la rețea.
- **Principiul celui mai mic privilegiu:** Principiul celui mai mic privilegiu se recomandă a fi aplicat în cadrul companiilor. Acesta este un concept de securitate în care utilizatorilor, programelor și proceselor li se acordă doar privilegiile minime necesare pentru a-și îndeplini sarcinile.
- **Instruirea angajaților:** Deoarece ransomware-ul se răspândește frecvent prin acțiuni inițiate de utilizator (”veriga slabă”, cum se arată mai sus), angajații companiilor trebuie să fie convinși să urmeze cursurile periodice de securitate cibernetică oferite de companie (aceste instruiri ar trebui să pună accent pe phishing, atașamente de e-mail rău intenționate și alte tactici de inginerie socială).
- **Autentificare multifactor (MFA):** MFA ar trebui să fie aplicată ori de câte ori este posibil pentru a reduce riscul accesului neautorizat.
- **Examinarea regulată a Active Directory:** Personalul IT ar trebui să examineze în mod regulat Active Directory (AD) pentru a localiza și închide deschiderile existente, cum ar fi conturile compromise, care au adesea privilegii administrative și sunt o țintă populară pentru atacatorii care doresc să obțină acces în diverse sisteme.
- **Segregarea rețelei:** Segregarea eficientă a rețelei este esențială pentru limitarea incidentelor și reducerea la minimum a întreruperii afacerii în general.

- **Acces securizat de la distanță:** Accesul de la distanță ar trebui să fie disponibil numai prin VPN folosind VPN cu MFA și limitat doar la utilizatorii care au nevoie de acesta pentru a-și face munca.
- **Evitați BYOD (Bring Your Own Device):** Implementarea și aplicarea strictă a protocoalelor de securitate pe dispozitivele personale ale angajaților este extrem de dificilă. În mod ideal, companiile ar trebui să furnizeze dispozitive și hardware dedicate și să descurajeze angajații să folosească dispozitivele personale pentru sarcini legate de muncă.
- **PowerShell:** PowerShell este unul dintre cele mai comune instrumente utilizate de diverse versiuni de ransomware pentru a se deplasa lateral într-o rețea țintă și ar trebui dezinstalat dacă este posibil. Dacă este necesar PowerShell, acesta trebuie monitorizat îndeaproape prin intermediul sistemelor de detectare și răspuns la nivelul end-point-urilor. Personalul IT ar trebui să fie conștient de fiecare script PowerShell care rulează pe end-point-uri.
- **Asigurare de securitate cibernetică:** Companiile ar trebui să aibă asigurare de securitate cibernetică și să se asigure că aceasta va ajuta la atenuarea impactului și în cazul unui incident de tip ransomware.
- **Planurile de răspuns la incident:** Companiile ar trebui sa aibă planuri de răspuns pentru diverse tipuri de incidente care ar trebui testate în mod regulat pentru a se asigura că angajații responsabili sunt familiarizați cu procesele de securitate și înțeleg exact ce trebuie să facă în cazul unei infectări. De asemenea, testarea ajută companiile să identifice și să remedieze deficiențele din lanțul de răspuns. Cel mai nepotrivit moment pentru o companie pentru a încerca să stabilească ce să facă într-un atac ransomware este chiar în timpul unui atac ransomware real.

3 MĂSURI DE ERADICARE ȘI LIMITARE A EFECTELOR

În eventualitatea infectării cu ransomware, DNSC vă recomandă implementarea următoarelor 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.), deconectați 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. *[Important pentru companii]* Dezactivați task-urile aferente mentenanței

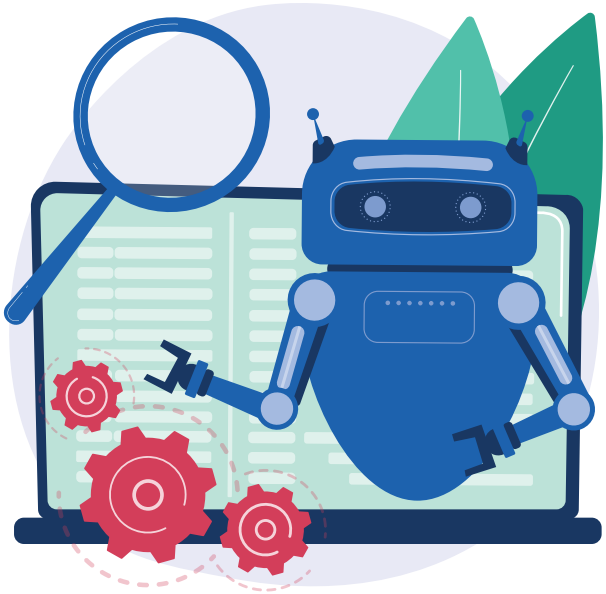
Personalul IT ar trebui să dezactiveze imediat sarcinile automate de mentenanță, cum ar fi eliminarea temporară a fișierelor și rotația jurnalelor pe sistemele afectate, deoarece aceste sarcini pot interfera cu fișierele care pot fi utile anchetatorilor și echipelor de criminalistică.

De exemplu, jurnalele de fișiere pot conține indicii valoroase cu privire la punctul inițial de infecție, în timp ce unele variante de ransomware prost programate pot stoca informații importante (cum ar fi cheile de criptare) în fișierele temporare.

3. *[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.



4. 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. 3), vă recomandăm să-l opriți imediat pentru a limita cât mai mult numărul fișierelor criptate.

5. *[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.

6. 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) deoarece decriptarea gratuită ar putea fi posibilă în viitor.

Au existat cazuri în care autoritățile de aplicare a legii au reținut autorii de ransomware și serverele C&C (comandă și control) care au fost găsite, ceea ce a dus la distribuirea cheilor de decriptare și a permis victimelor să-și recupereze datele gratuit. În plus, o serie de grupuri de ransomware – inclusiv Shade, TeslaCrypt și CrySis, printre altele – au distribuit de bunăvoie chei de decriptare după ce și-au oprit operațiunile.

7. Restaurați fișierele compromise

Cea mai simplă metodă de recuperare a fișierelor afectate de ransomware este restaurarea acestora din 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 (copiile) de HDD (realizate conform pct. 5), 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.

8. 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. 7, vă recomandăm să nu încercați dezinfectarea acestora și să utilizați alte HDD-uri pentru re-instalarea sistemului de operare.

9. Raportați incidentul către DNSC

DNSC vă recomandă să raportați incidentele de securitate cibernetică, inclusiv infecțiile cu ransomware, la adresa de email alerts@dnsc.ro, sau la numărul de urgență 1911, beneficiind astfel de suport tehnic și indicații de rezolvare a incidentelor și/sau limitare a efectelor acestora.

4 CUM SĂ NU RĂSPUNZI LA UN ATAC RANSOMWARE

Gestionarea incorectă a unui incident ransomware poate împiedica eforturile de recuperare, poate pune în pericol datele și poate duce la plata inutilă de către victime a răscumpărărilor. În urma unui atac ransomware, următoarele greșeli ar trebui evitate:

- **NU reporniți dispozitivele afectate**

  Ar trebui să se evite repornirea dispozitivelor care au fost afectate de ransomware. Multe tulpini de ransomware vor detecta încercările de a reporni și vor penaliza victimele corupând instalarea Windows a dispozitivului, astfel încât sistemul să nu pornească din nou, în timp ce altele pot începe să șteargă fișierele criptate la întâmplare. Infamul ransomware Jigsaw, care a fost prolific în 2016, a șters aleatoriu 1.000 de fișiere criptate de fiecare dată când un dispozitiv infectat a fost repornit.

  Repornirea sistemului poate împiedica, de asemenea, eforturile criminalistice. Repornirea șterge memoria mașinii care, după cum s-a menționat mai devreme, poate conține indicii care pot fi utile anchetatorilor. În schimb, sistemele afectate ar trebui puse în stare de hibernare, prin aceasta stare toate datele din memorie sunt scrise într-un fișier de referință de pe hard diskul dispozitivului, care poate fi apoi folosit pentru analize viitoare.

- **NU conectați dispozitive de stocare externe la sistemele infectate**

  Multe familii de ransomware vizează în mod intenționat dispozitivele de stocare și sistemele de rezervă. Ca atare, dispozitivele de stocare externe și sistemele de rezervă nu trebuie conectate (fizic sau prin acces la rețea) la sistemele infectate până când infecția a fost eliminată.

  Nu este întotdeauna evident că rulează ransomware. Din păcate, au existat multe cazuri în care companiile au început procesul de recuperare fără să-și dea seama că ransomware-ul este încă prezent pe sistemul lor, ceea ce a dus la criptarea cu ransomware a sistemele lor de rezervă și a dispozitivelor de stocare.

- **NU plătiți imediat răscumpărarea**

  Deși perspectiva unei perioade de nefuncționare și o potențială pierdere a reputației poate fi descurajantă, victima nu ar trebui să plătească imediat răscumpărarea. Există întotdeauna alte opțiuni, iar acestea ar trebui explorate în întregime înainte de a recurge la plata răscumpărării. Mai mult, nu există garanții că, odată plătită răscumpărarea, se vor decripta fișierele, iar, în cazul anumitor grupări care operează ransomware, furnizarea de mijloace bănești poate fi considerată un act ilegal în sine (de pildă, în cazul grupărilor teroriste).

- **NU comunicați în rețeaua afectată**

  În timpul recuperării, victimele ar trebui să presupună că atacatorii au încă acces la rețeaua compromisă și, prin urmare, pot fi capabili să intercepteze orice comunicații care sunt trimise și primite prin rețea.

- **NU ștergeți fișiere**

  Fișierele nu trebuie șterse din sistemele criptate decât dacă un specialist în recuperare ransomware a recomandat să se facă acest lucru. Nu numai că fișierele criptate sunt utile pentru analizele criminalistice, dar unele familii de ransomware stochează chei de criptare în fișierele criptate - dacă fișierele sunt șterse, decriptorul nu va funcționa.

  În mod similar, notele de răscumpărare nu trebuie niciodată șterse. Unele familii de ransomware, cum ar fi DoppelPaymer și BitPaymer, creează o notă de răscumpărare pentru fiecare fișier pe care îl criptează, care conține cheia codificată și criptată necesară pentru decriptare. Dacă o notă de răscumpărare este ștearsă, fișierul corespunzător nu poate fi decriptat.

- **NU aveți încredere în autorii de ransomware**

  În ciuda faptului că încearcă din ce în ce mai mult să adopte o fațadă de profesionalism, autorii de ransomware sunt răufăcători care nu se simt obligați să respecte niciun acord sau cod de etică. Victima nu trebuie să creadă nicio informație furnizată de grupurile de ransomware, inclusiv informațiile din nota de răscumpărare (cum ar fi tulpina de ransomware) și nici să aibă încredere că plata răscumpărării va duce la recuperarea datelor criptate.

  Victimele ar trebui să aibă în vedere faptul că atacatorii ar putea să nu ofere un decriptor după plată și că instrumentele de decriptare furnizate de atacator pot fi defecte și/sau pot deteriora datele criptate.

5 BIBLIOGRAFIE

1. https://www.us-cert.gov/ncas/alerts/TA14-295A
2. http://www.symantec.com/connect/blogs/ransomware-how-stay-safe
3. https://www.welivesecurity.com/2013/12/12/11-things-you-can-do-to-protect-against-ransomware-including-cryptolocker/
4. https://support.microsoft.com/ro-ro/windows/proteja%C8%9Bi-v%C4%83-pc-ul-de-ransomware-08ed68a7-939f-726c-7e84-a72ba92c01c3
5. https://dnsc.ro/citeste/ransomware-ul-ctb-locker
6. https://dnsc.ro/citeste/teslacrypt-si-alte-campanii-ransomware-pentru-care-exista-solutii-de-recuperare-a-fisierelor-criptate


#sigurantaonline