



Ghid prevenție Ransomware



1. Măsuri preventive

- Creați o copie de rezervă a tuturor datelor importante pe suporturi portabile, (ex. USB-flash, hard extern), păstrați dispozitivul dat într-un loc sigur. Repetați periodic procedura pentru a păstra datele actualizate.
- Evitați deschiderea atașamentelor la e-mail care au la sfârșit extensia de ".exe" sau ".scr" și provin de la expeditori necunoscuți sau a căror identitate nu poate fi verificată.
- Configurați sistemul Windows să vă arate extensiile tuturor fișierelor. În cazul în care un fișier este numit "image.jpg.exe", majoritatea calculatoarelor Windows îl vor afișa ca "image.jpg". O bună parte din utilizatori, prin urmare, se vor gândi că acesta este o imagine inofensivă, chiar dacă în realitate fișierul este un program executabil. Pentru a preveni astfel de cazuri intrați în setările mapei (Folder Options > View) și debifați opțiunea «Hide extensions for known file types»;
- Aveți în vedere că este periculos să deschideți orice atașament, chiar și documentele Microsoft Word și PDF pot conține viruși. În cazul în care Dvs. totuși doriți să deschideți documentul:
 - a. Dacă este posibil contactați expeditorul email-lui prin telefon sau în oricare alt mod;
 - b. Asigurați-vă că Sistemul de operare al calculatorului Dvs. și baza de date a antivirusului este actualizată. Iar pentru verificarea unui fișier suspect încărcați acesta pe site-ul online de verificare <https://www.virustotal.com/>;
 - c. Asigurați-vă că sunt activate opțiunile de vizualizarea securizată a documentelor. Pentru Microsoft Office 2010 și versiuni mai noi, asigurați-vă că, în (File > Options > Trust Center > Trust Center Settings > Protected View) a fost activată opțiunea de program "Protected View". Pentru Adobe Reader, asigurați-vă că în program (Edit > Preferences > Security (Enhanced) > Sandbox Protections) a fost bifat "Enable Protected Mode at startup", iar opțiunea «Protected View» este instalată în «All files»;
 - d. De asemenea, dacă există posibilitate, deschideți fișierele suspecte într-un mediu virtual (de exemplu **VMware Player**).
- Verificați sistematic actualizările pentru sistemul de operare și antivirusul folosit. De multe ori malware-ul folosește vulnerabilitățile softului învechit pentru a penetra calculatorul Dvs, din acest considerent instalarea ultimelor actualizări va minimiza semnificativ riscul infectării.
- Nu utilizați contul de administrator în mod regulat când lucrați la calculator, astfel se va împiedica extinderea virusului în sistemul de operare în cazul infectării;
- Utilizați Windows Group sau Local Policy Editor pentru a crea politici de restricționare ce blochează rularea fișierelor de tip .exe când se află în anumite locații. Pentru mai multe informații privind configurarea restricțiilor (Software Restriction Policies), puteți consulta articolele de la Microsoft: [http://technet.microsoft.com/en-us/library/cc786941\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc786941(v=ws.10).aspx)

2. Identificare Ransomware

Dacă identificați că ați fost infectat cu Ransomware, ar trebui să executați imediat o scanare completă cu un program anti-virus sau anti-malware;

Din nefericire, în cele mai multe cazuri, infectarea nu este observată de utilizatori decât după afișarea mesajului de „ransom”, fișierele fiind deja criptate în acest moment. Procesul de scanare rămâne util, deoarece acesta va găsi și înlătura malware-ul din sistem;

Deconectați calculator de la rețeaua locală pentru a opri infectarea cu virus a resurselor disponibile în această rețea, spre exemplu fișierele comune sau discurile de rețea.

3. Măsuri post incident

Copii de rezervă. Prima opțiune este de a vă recupera datele dintr-un back-up recent al acestora;

Software pentru recuperarea datelor. În mai multe cazuri Ransomware-ul realizează o copie a fișierului valid, o criptează, după care șterge fișierul original. Într-o astfel de situație, utilizatorul victimă poate încerca să își recupereze fișierele cu ajutorul unor programe special dezvoltate pentru recuperarea datelor. Două astfel de instrumente sunt: **R-Studio** și **Photorec**.

Copii Shadow Volumes. În cazul în care aveți opțiunea de System Restore activată, sistemul de operare Windows va realiza imagini instantanee ale datelor – shadow copy snapshots – care pot fi utile pentru recuperarea datelor din acel moment de timp.

Metode de recuperare a datelor din ShadowVolume Copies

A. Windows Previous Versions

Pentru recuperarea fișierelor individuale urmați pașii de mai jos:

- Click-dreapta pe fișierul de interes;
- Properties;
- Selectați tab-ul PreviousVersions;
- Selectați versiunea fișierului pe care doriți să o recuperați;
- Selectați funcția Copy pentru recuperarea fișierului ales și alegeți directorul destinație sau
- Selectați operația Restore pentru recuperarea fișierului și înlocuirea celui curent.

B. Shadow Explorer

- Descărcați și instalați utilitarului Shadow Explorer
<http://www.shadowexplorer.com/downloads.html>;
- Deschideți Shadow Explorer și selectați din meniul drop-down din partea stângă a ferestrei partiția disponibilă la un moment de timp specificat pentru a efectua recuperarea de fișiere;
- Click-dreapta pe oricare fișier sau director criptat și alegeți opțiunea **Export** pentru a selecta locația în care doriți să se stocheze datele recuperate;

4. Eliminarea Ransomware de pe calculatorul Dvs

Pentru asistență, contactați administratorul de sistem, pentru a:

1. Formata hard disk-urile (cu eliminarea secțiunii "MBR");
2. Reinstala (sistemul de operare, Office, antivirus, etc) software-ul necesar;
3. Instalarea celor mai recente actualizări.
 - Copiați datele recuperate în calculator;
 - Scațați sistemul cu ajutorul unui antivirus.