**SERVICIUL TEHNOLOGIA INFORMAȚIEI**
**ȘI SECURITATE CIBERNETICĂ**

# INSTRUCȚIUNEA PRIVIND COMBATEREA VIRUSULUI „CTB- LOCKER”

1. **Măsuri de întreprins pentru a preveni infectarea:**
   - Faceţi o copie de rezervă a tuturor datelor importante pe suporturi portabile, de exemplu pe un USB-flash, păstrați flash-ul într-un loc sigur. Repetați periodic procedura pentru a păstra datele actualizate;
   - Niciodată nu deschideți atașamentele la email care au la sfârșit extensia de ".exe" sau ".scr". 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:
     - Dacă este posibil contactați expeditorul email-lui prin telefon sau în oricare alt mod;
     - 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/;
     - 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»;
     - 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://support.microsoft.com/kb/310791
     http://technet.microsoft.com/en-us/library/cc786941(v=ws.10).aspx

     Locațiile folosite de acest tip de infecții sunt:

     C:<random><random>.exe

C:Users<User>AppDataLocal<random>.exe (Vista/7/8)
C:Users<User>AppDataLocal<random>.exe (Vista/7/8)
C:Documents and Settings<User>Application Data<random>.exe (XP)
C:Documents and Settings<User>Local Application Data<random>.exe (XP)
%Temp%

2. **În caz că calculatorul Dvs a fost infectat cu ”Ransomware”**
   - Dacă descoperiți că ați fost infectați cu malware-ul CTB Locker sau Critroni, ar trebui să executați imediat o scanare completă cu un program anti-virus sau anti-malware. Din nefericire, în cele mai multe cazuri, infecția nu este observată de utilizatori decât după afișarea mesajului de „ransom”, fișierele fiind 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. **Recuperarea datelor:**
   - **Copii de rezervă.** Prima opţiune este de a vă recupera datele dintr-un backup recent al acestora;
   - **Software pentru recuperarea datelor**. Aparent, CTB Locker realizează o copie a fișierului identificat ca 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 şi 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. În continuare sunt prezentate două metode de recuperare a datelor din Shadow Volume Copies:
     1) **Windows Previous Versions**. Pentru recuperarea fișierelor individuale urmaţi paşii de mai jos:
        - Click-dreapta pe fișierul de interes;
        - Properties;
        - Selectați tab-ul Previous Versions;
        - Selectați versiunea fișierului pe care doriți să o recuperați;
        - Selectați funcția Copy pentru recuperarea fișierului ales și alegeți directorul destinație sau
        - Selectaţi operaţia Restore pentru recuperarea fişierului şi înlocuirea celui curent.

     2) **Shadow Explorer**:
        - Descărcaţi şi instalaţi utilitarului Shadow Explorer http://www.shadowexplorer.com/downloads.html;
        - Deschideţi Shadow Explorer şi selectaţi din meniul drop-down din partea stângă a ferestrei partiţia disponibilă la un moment de timp specificat pentru a efectua recuperea de fişiere;
        - Click-dreapta pe oricare fişier sau director criptat şi alegeţi opţiunea Export pentru a selecta locaţia în care doriţi să se stocheze datele recuperate;

**4. Eliminarea infecției 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;
- Scanați sistemul cu ajutorul unui antivirus.