Agenţia de Administrare a Reţelei Naţionale de Informatică pentru Educaţie şi Cercetare
RoCSIRT – RoEduNet CSIRT
Str. Mendeleev 21-25, Sector 1, 010362
Bucuresti – Romania
www.csirt.ro
Tel./Fax: +40-21-3171174

Raport tehnic - DNSChanger

Data: 14 Noiembrie 2011

1. Scop

Acest document pune la dispoziția utilizatorilor informații despre detectarea şi eliminarea malware-ului DNSChanger. Acest document a fost scris cu scopul de a ajuta la detectarea şi eliminarea DNSChanger.

2. Despre document

Acest document este o adaptare a documentului original al cărui autor este CCIRC[1]. Versiunea originală a acestui document, este disponibilă (în limba engleză) la adresa: http://www.publicsafety.gc.ca/prg/em/ccirc/2011/in11-002-eng.aspx

3. DNSChanger

DNSChanger este un malware ce redirectează traficul unui utilizator către servere DNS aflate sub controlul infractorilor cibernetici, în locul celor legitime furnizate de către Furnizorul de Servicii Internet (ISP). DNSChanger schimbă setările DNS ale staţiei de lucru şi acolo unde este posibil, folosind nume de utilizator şi parole implicite, poate schimba configuraţia DNS a routerului, afectând astfel traficul tuturor staţiilor din reţeaua locală, indiferent dacă sunt sau nu infectate cu DNSChanger.

Analiza infrastructurii asociate cu DNSChanger a dus la descoperirea de malware cunoscut de către comunitatea antivirus ca TDSS, Alureon, Tidserv sau TDL4. Acest malware are capacitatea de a se sustrage detecţiei şi este rezistent la încercările de ştergere, aceste caracterisitici ale sale fiind în mod regulat actualizate şi schimbate de către autorii săi. Malware-ul schimbă un număr de chei din registrul Microsoft Windows astfel încât să fie sigur că va reporni de fiecare dată când staţia de lucru este pornită. Una din versiuni infectează chiar o zonă de pe disc, numită MBR (Master Boot Record). Această zonă de pe disc este în mod normal prima care este citită de un calculator înainte de a încărca sistemul de operare. Din acest motiv, infectarea MBR necesită intervenţii non-triviale pentru a putea fi curăţată.

4. Acţiuni

4.1. Detectarea

Pentru a putea determina dacă calculatorul a fost infectat cu o variantă de DNS Changer, un utilizator trebuie să urmeze paşii de mai jos:

1. Identificarea setărilor DNS

   a. Windows
   i. Deschideţi meniul de start
   ii. Selectaţi Run
   iii. Tipăriţi: cmd.exe [si apasati ENTER]
   iv. În fereastra nou deschisă scrieţi urmatoarea comandă: ipconfig /all [şi apăsaţi ENTER]

[1] http://www.publicsafety.gc.ca

v. Cautați în informațiile furnizate liniile ce conțin "DNS Servers". De obicei acestea sunt 2 sau 3 adrese IP. Notați aceste adrese IP.

b. Apple

i. Mergeți în System Preferences
ii. Selectați Network
iii. Selectați conexiunea folosită pentru acces la Internet (uzual AirPort sau Ethernet)
iv. Selectați Advanced
v. Selectați tab-ul DNS
vi. Notati adresele IP.

c. Router propriu

Malware-ul DNSChanger este de asemenea capabil să schimbe setările DNS a anumitor routere de tip SOHO (Small Office Home Office) cum ar fi: Linksys, D-Link, Netgear și Cisco, dacă numele de utilizator și parola sunt cele implicite. Pentru a depista dacă setările DNS ale routerului dvs au fost schimbate consultați manualul routerului, secțiunea "Servere DNS". În cazul în care serverele DNS utilizate sunt în intervalul de adrese IP de mai jos, unul din calculatoarele conectate la routerul dvs este infectat cu DNSChanger.

2. Verificarea adreselor IP

Verificați dacă adresele IP ale serverelor DNS pe care le-ați notat, sunt în intervalul de adrese IP de mai jos, comparând numerele de la stanga la dreapta. **Dacă adresele IP nu încep cu**:

- 85.255.*.*
- 67.210.*.*
- 93.188.*.*
- 77.67.*.*
- 213.209.*.*
- 64.28.*.*

atunci calculatorul dvs nu a fost infectat de nici una din variantele malware-ului DNS Changer.

4.2. Repararea

În afară de redirectarea traficului web al utilizatorilor către site-uri modificate, DNSChanger poate de asemenea afecta instalarea actualizărilor de securitate la nivelul sistemului de operare și al antivirusilor. Acest fapt ridică semnificativ riscul ca stația de lucru să fie de asemenea vulnerabilă la infectarea cu un alt malware. Utilizatorii care au motive să creadă că stația de lucru poate fi infectată trebuie să contacteze departamentul IT. Înainte de a se încerca repararea stației de lucru, este recomandată copierea fișierelor importante precum: documente, fotografii sau orice alte fișiere, pe medii externe de stocare (discuri externe, CD, DVD). Odată copiate, fișierele nu vor fi considerate de încredere până când nu vor fi scanate cu un antivirus recunoscut, ce are toate actualizările făcute. Următoarele articole pot fi de folos în procesul de recuperare:

1. În cazul unei stații de lucru neinfectate, se poate consulta ghidul CCIRC TR11-001: http://www.publicsafety.gc.ca/prg/em/ccirc/2011/tr11-001-eng.aspx
2. Resurse și utilitare despre TDSS/tidserv/TDL4/Alureon:
   2.1. Analiză tehnică a malware-ului similar:
      2.1.1. http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Trojan:Win32/Alureon.DX
      2.1.2. http://isc.sans.edu/diary.html?storyid=5390
      2.1.3. http://go.eset.com/us/resources/white-papers/The_Evolution_of_TDL.pdf
   2.2. Utilitare (trebuie utilizate conform instrucțiunilor producătorului):
      2.2.1. TDSSKiller: http://support.kaspersky.com/faq/?qid=208280684
      2.2.2. fixmbr, Microsoft Recovery Console: http://support.microsoft.com/kb/314058
      2.2.3. Microsoft MSRT: http://support.microsoft.com/kb/890830
      2.2.4. FixTDSS: http://www.symantec.com/security_response/writeup.jsp?docid=2010-090608-3309-99
      2.2.5. McAfee Stinger: http://www.mcafee.com/us/downloads/free-tools/stinger.aspx
      2.2.6. Trend Micro Housecall: http://housecall.trendmicro.com

5. Despre RoCSIRT

RoEduNet CSIRT (RoCSIRT), a fost înființat ca serviciu operativ în cadrul Agenției ARNIEC / RoEduNet în decembrie 2008. Scopul primar al RoCSIRT este protejarea instituțiilor conectate la rețeaua RoEduNet prin intermediul serviciilor preventive și a celor reactive. O descriere amănunțită a serviciilor oferite de către RoCSIRT, este disponibilă în Documentul de Descriere a Serviciilor[2] disponibil pe site-ul RoCSIRT[3].

[2] https://www.csirt.ro/sites/default/files/RoCSIRT%20Service%20Definition%20-%201.02.pdf

[3] http://www.csirt.ro/