Črv Conficker

Ivan Verdonik
Fakulteta za gradbeništvo
Univerza v Mariboru

Uvod

- Eden najpomembnejših sploh
- Okužil več kot 10 milijonov sistemov po celem svetu
- V osnovi je izkoriščal ranljivost MS08-067
- Tekom časa od jeseni 2008 do poletja 2009 je nastalo 5 glavnih različic (A do E)
- Napisan po vseh pravilih

Kaznivi vidiki

- Ogrožanje državne varnosti (okužbe vojaških in policijskih računalnikov)
- Ogrožanje varnosti ljudi (okužbe bolniščniških računalnikov)
- Ogromna materialna škoda
- Zaenkrat še ni v rokah organiziranega kriminala
- Microsoft razpisal 250 000 $ za aretacijo avtorja

Opis glavne ranljivosti

- Varnostna napaka je v:
  - Windows API NetpwPathCanonicalize() funkciji
  - V knjižnici netapi32.dll

  Napad je izpeljan preko SMB seje na TCP vratih 445

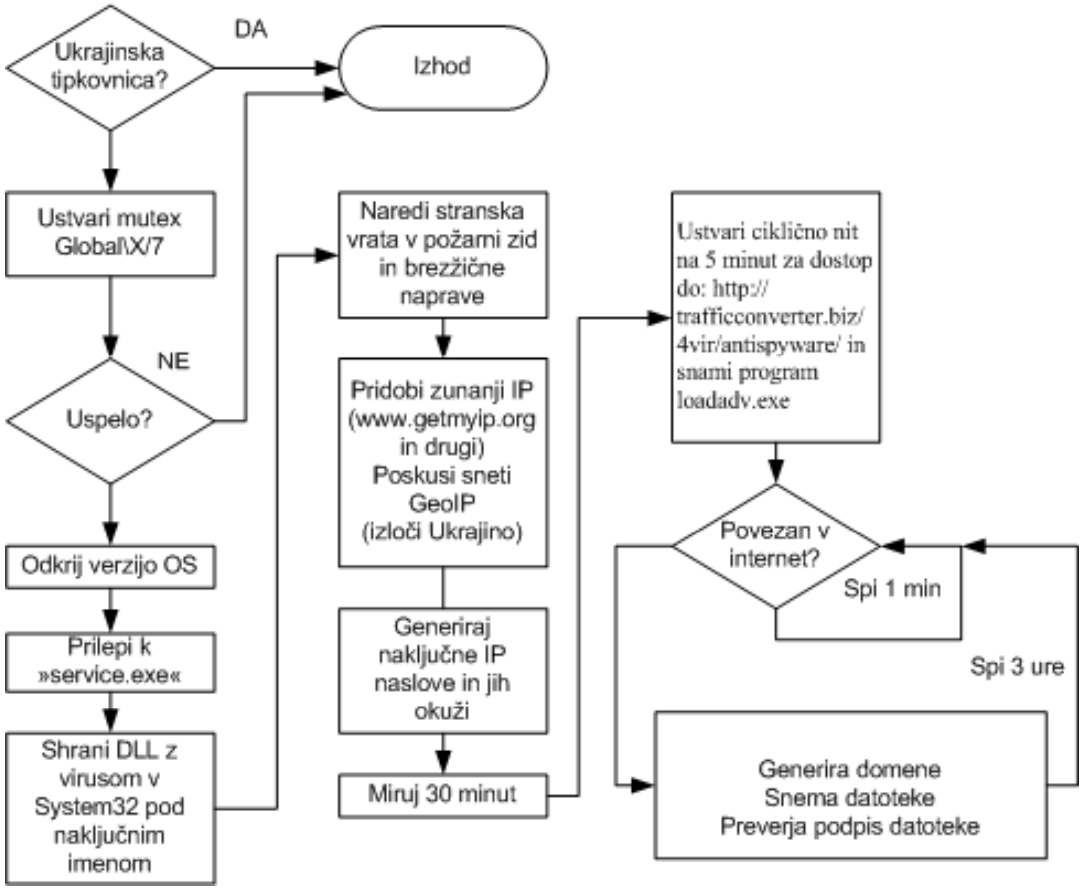
  Funkcija ima za vhod niz, v katerem je pot do vira. Ta vhod normalizira. Zaradi programske napake, lahko posebej prirejen niz preusmeri izvajanje na zlonamerno kodo, ki jo posreduje napadalec

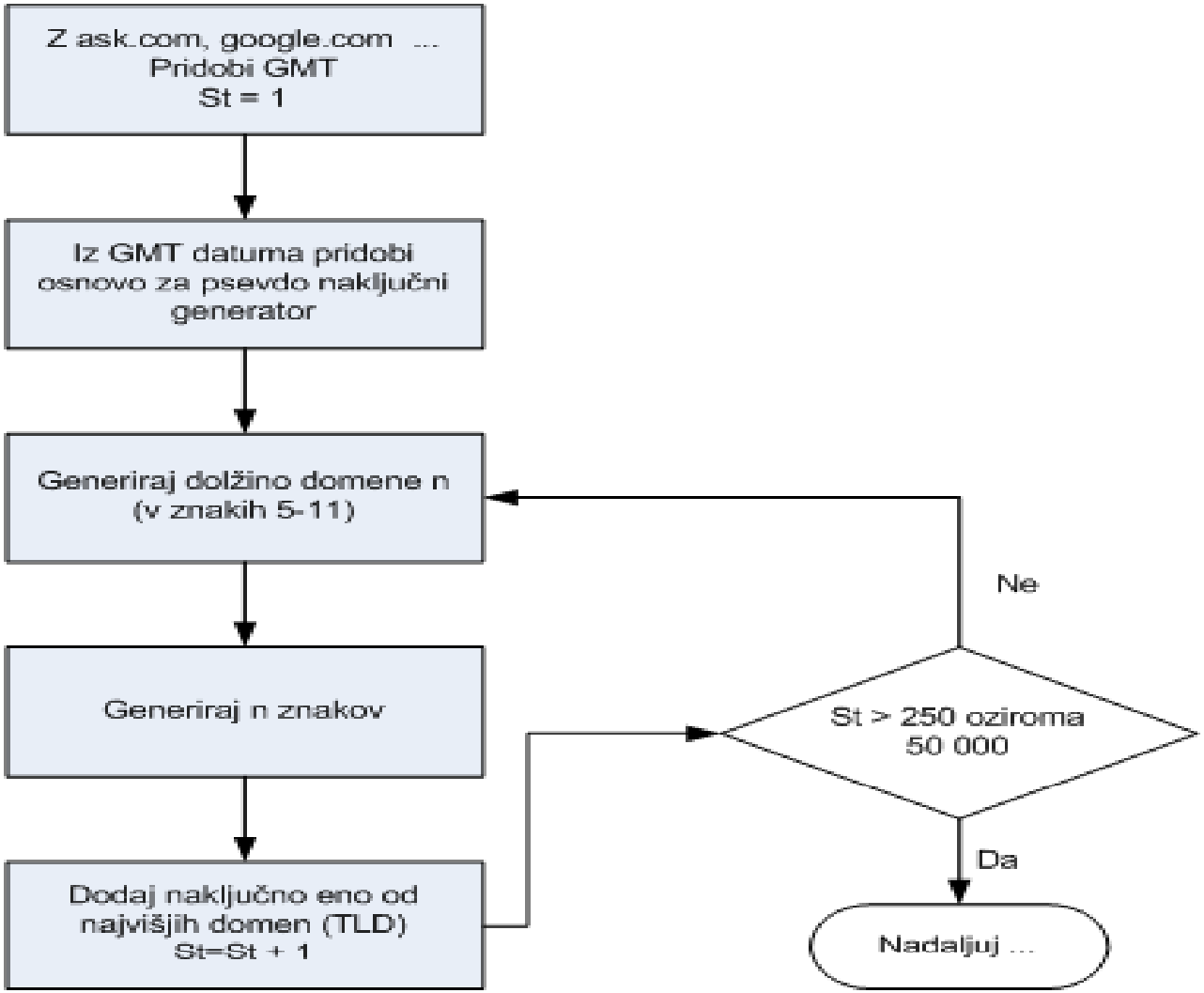
Različica A

- Okužba preko posebej prirejenega RPC klica na vrata 445 TCP
- Koda se vbrizga (inject) v services.exe
- Kopira se v sistemsko mapo, kot .dll s naključno izbranim 5-8 znakov dolgim imenom (npr. drpjxs.dll)
- Spremeni Registry, zakrpa ranljivost ...
- Se širi na naključne IP naslove

Različica A nadaljevanje

- Na “obiskanem” sistemu skuša okužiti svchost.exe (Windows Server service)
- Ustvari enostaven http strežnik na naključnih vratih, s katerim nalaga bremena
- Povezuje se s http bot master sistemom
- Na enem od vsak dan 250 generiranih URL-jev – kjer prevzema posodobitve


Ukrajinska tipkovnica?
DA
Izhod
Ustvari mutex Global\X/7
NE
Uspelo?
Odkrij verzijo OS
Prilepi k »service.exe«
Shrani DLL z virusom v System32 pod naključnim imenom
Naredi stranska vrata v požarni zid in brezžične naprave
Pridobi zunanji IP (www.getmyip.org in drugi) Poskusi sneti GeoIP (izloči Ukrajino)
Generiraj naključne IP naslove in jih okuži
Miruj 30 minut
Ustvari ciklično nit na 5 minut za dostop do: http://trafficconverter.biz/4vir/antispyware/ in snami program loadadv.exe
Povezan v internet?
Spi 1 min
Spi 3 ure
Generira domene
Snema datoteke
Preverja podpis datoteke


Z ask.com, google.com ...
Pridobi GMT
St = 1
Iz GMT datuma pridobi osnovo za psevdo naključni generator
Generiraj dolžino domene n (v znakih 5-11)
Generiraj n znakov
Dodaj naključno eno od najvišjih domen (TLD)
St=St + 1
St > 250 oziroma 50 000
Ne
Da
Nadaljuj ...

Različica B

- Znatno naprednejša
- Širjenje preko deljenih map in MS08-067
- Blokira storitve:
  - Windows Update Service (wuauserv)
  - Background Intelligent Transfer Service (BITS)
  - Windows Defender (WinDefend)
  - Windows Error Reporting Services (wersvc)
  - Error Reporting Service (ersvc)
  - Windows Security Center Service (wscsvc)

Različica B nadaljevanje

- Ni moče dostopiti do spletnih mest, z naslovi:
  virus, spyware, malware, rootkit, defender, microsoft, symantec, norton, mcafee, trendmicro, sophos, panda, etrust, drweb
  ...
- Širjenje tudi preko Microsoftovega omrežja s šibkimi gesli

Različica B nadaljevanje

- Širjenje z USB ključi in diski
- Virus v korensko mapo USB-ja (v RECYCLER) ter datoteko Autorun.inf
- Ob vključitvi se sproži Autorun in naloži virus na računalnik
- Psevdonaključno tvori URL-je na katerih nato išče posodobitve
- Omrežje je zelo obremenjeno

Različica C

- Dodatne možnosti posodabljanja
- S peer to peer metodo
- Preveri avtentičnost in veljavnost posodobitev z RSA digitalnim podpisom.
- Na ta način se ščiti pred drugimi hekerji, ki bi lahko izkoristili okužbo s Confickerjem za svoje (kriminalne) dejavnosti

Različica D

- Se več ne širi naprej
- Utrjuje pa se na že okuženih sistemih
- Ima spremenjen način posodabljanja
- Tvori 50 000 URL-jev dnevno, od tega jih obišče le 500.
- Onemogoči zagon v varnem načinu
- Vsako sekundo preveri seznam procesov in ubije vsakega, ki vsebuje določen naziv

autoruns - "Autoruns" program
avenger - kernel-mode security program
bd_rem - "bd_rem_tool_console.exe" &
"bd_rem_tool_gui.exe" programs
cfremo - Enigma Software "cfremover.exe" program
confick - taken from the name 'Conficker'
downad - taken from the name 'Downadup' alias 'Conficker'
filemon - "File Monitor" program
gmer - rootkit detection program
hotfix - security update
kb890 - Microsoft KB article, includes MSRT
kb958 - Microsoft KB article, includes MS08-067
kido - taken from the name 'Kido', another 'Conficker' alias
kill - utility used to terminate other processes
klwk - Kaspersky program
mbsa. - "Microsoft Baseline Security Analyzer" program
mrt. - "Microsoft Malicious Software Removal Tool" program
mrtstub - "Microsoft Malicious Software Removal Tool" program
ms08-06 - Microsoft Security Update MS08-067
procexp - "Process Explorer" program
procmon - "Process Monitor" program
regmon - "Registry Monitor" program
...

Različica E

- Namesti se le na sisteme že okužene z različicami B, C in D
- Še težje odstranljiva
- V splošnem se izvršljiva verzija po 3. maju 2009 sama uniči – kar je veliko presenečenje
- Ostane pa dll knjižnica

Zaščita črva

- Šifriranje: RSA elektronski podpis pri posodobitvah (tako http, kot P2P)
- Zameglitev (obfuscation): premešana v “špageti” kodo, zato še vedno nimamo povratnega inženiringa celotnega črva
- Jedrni paket (rootkit): “Kavlja” (hooking) funkcije: DnsQuery_A, DnsQuery_UTF8, DnsQuery_W

Sklep

- Zelo nevaren črv
- Okužil več kot 12 milijonov računalnikov
- Težko ga je odstraniti
- Še vedno je z njim inficirano več milijonov sistemov