

MSBlast crv – šta da se učini

Aleksandar Aničić

Nakon konferencije hakera u Las Vegasu stiže nam novi virus koji je već dobio ocenu 7 u klasifikaciji ZDNet-a. Radi se o Internet "crvu" po imenu "MSBlast", takođe poznatim i pod imenom "Worm/Lovsan.A".

Kako radi crv?

Crv radi na taj način što koristi poznate sigurnosne greške (flaws) u Microsoftovim operativnim sistemima i to Windows NT, Windows 2000 i Windows XP. Ne napada Windows 9x/ME izuzev ako se ručno ne preuzme ("downloaduje") i pokrene **msblast.exe**. Kada dođe do vašeg kompjutera, momentalno počinje da koristi famozni DCOM (Distributed Component Object Model) RPC (Remote Procedure Call) interfejs. Naime, gore pomenuta napast u vidu crva ne stiže na vaš sistem kao i većina dosadašnjih "napasnika".



Ovaj "osluškuje" Internet na portu 135 i traži nezaštićene kompjutere kako bi ih "inficirao". Kada nadje "žrtvu" nastoji da iskoristi DCOM RPC buffer overflow. Tada kreira "remote root shell" na TCP portu 4444 i na njemu koristi FTP da bi "downloadovao" fajl sa imenom **msblast.exe** na inficiranu mašinu, te ga "smestio" u \windows\%system% direktorijum. MSBlast tada unosi izmene u Registrima i to na sledeći način:

```
Hkey_local_machine\software\Microsoft\Windows\CurrentVersion\ Run "windows auto update" = msblast.exe I just want to say LOVE YOU SAN!!billy gates why DO you make this possible? Stop making money and fixed your software!!"
```

Najzanimljivije je ponašanje ovog "crva" na Microsoft Windows XP operativnom sistemu. Radi tako što vam na svakih 60 do 80 sekundi jednostavno ugasi kompjuter. Jednostavno se nakon 60 sekundi dobije poruka na ekranu:

System Shutdown

This system is shutting down. Please save all work in progress and log off. Any unsaved changes will be lost. This shutdown was initiated by NT AUTHORITY\SYSTEM....

Time before shutdown: 00:00:14

Message

Windows must now restart because the Remote Procedure Call (RPC) Service terminated unexpectedly

Takođe, dovodi do Denial of Service-a (DoS) prilikom pokretanja Windows Update-a. Nezgodno, zar ne? Zato se valja zaštititi. *"Bolje sprečiti nego lečiti!"*

Šta nam je za činiti?

Pre otprilike mesec dana je Microsoft Technet objavio postojanje "flaw"-a na DCOM RPC interfejsu i pustio je "patch" (zakrpu) za ovaj "flaw". No, većina korisnika Interneta vrlo, vrlo retko ode na ovaj sajt koji lično smatram jako korisnim, naročito ljudima čiji je posao da vode računa o korporacijskim mrežama, da ne kažem za Network Administratore. Oni koji još nisu uneli ovaj "patch" evo gde mogu to učiniti zavisno od toga koji operativni sistem koriste:



<http://microsoft.com/downloads/details.aspx?FamilyId=2CC66F4E-217E-4FA7-BDBF-DF77A0B9303F&displaylang=en> za Win NT 4.0 Server

<http://microsoft.com/downloads/details.aspx?FamilyId=6C0F0160-64FA-424C-A3C1-C9FAD2DC65CA&displaylang=en> za Win NT 4.0 Terminal Server Edition

<http://microsoft.com/downloads/details.aspx?FamilyId=C8B8A846-F541-4C15-8C9F-220354449117&displaylang=en> za Win 2000

<http://microsoft.com/downloads/details.aspx?FamilyId=2354406C-C5B6-44AC-9532-3DE40F69C074&displaylang=en> za Win XP 32-bit Edition

<http://microsoft.com/downloads/details.aspx?FamilyId=1B00F5DF-4A85-488F-80E3-C347ADCC4DF1&displaylang=en> za Win XP 64-bit Edition

<http://microsoft.com/downloads/details.aspx?FamilyId=F8E0FF3A-9F4C-4061-9009-3A212458E92E&displaylang=en> za Win 2000 32-bit Edition

<http://microsoft.com/downloads/details.aspx?FamilyId=2B566973-C3F0-4EC1-995F-017E35692BC7&displaylang=en> za Win 2000 64-bit Edition

Ili jednostavno odete na www.microsoft.com/technet i naći ćete link koji je naglašen i zove se **MS03-026** pa izvolite i preuzmite lek pre nego li se inficirate. To mu dođe kao vakcina. Dakle, valja bolest sprečiti.

No, ako je neko već zakasnio (crv je prisutan na Internetu već nekoliko dana), valjalo bi da zna način kako da ovu napast ukloni sa svog kompjutera. Većina kompanija koja piše antivirus programe je već unela MSBlast u svoje baze.

Za detekciju i uklanjanje ovog virusa za korisnike McAfee-a toplo preporučujem neki od sledećih linkova, respektivno:

<http://www.networkassociates.com/us/downloads/updates/>

<http://a64.g.akamai.net/7/64/2015/2003-08-11-03-/download.nai.com/products/mcafee-avert/100547.zip>

<http://a64.g.akamai.net/7/64/2015/2003-08-11-03-/download.nai.com/products/mcafee-avert/sdat100547b.exe>

Korisnici Symantec-ovog Norton Antivirus-a treba da posete:

<http://www.symantec.com/avcenter/venc/data/w32.blaster.worm.html>

Korisnici Trend Micro usluga:

http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_MSBLAST.A

Na ovom poslednjem sajtu ćete naći detaljno uputstvo za ručno uklanjanje ovog virusa.

Pozdrav iz Vancouver-a