

The Blaster Worm: Then and Now

Oleh :

Kasiman Peranginangin
peranginanginkasiman@yahoo.com

*Dipublikasikan dan didedikasikan
untuk perkembangan pendidikan di Indonesia melalui*

MateriKuliah.Com

Lisensi Pemakaian Artikel:

*Seluruh artikel di **MateriKuliah.Com** dapat digunakan, dimodifikasi dan disebarakan secara bebas untuk tujuan bukan komersial (nonprofit), dengan syarat tidak menghapus atau merubah atribut Penulis. Hak Atas Kekayaan Intelektual setiap artikel di **MateriKuliah.Com** adalah milik Penulis masing-masing, dan mereka bersedia membagikan karya mereka semata-mata untuk perkembangan pendidikan di Indonesia. **MateriKuliah.Com** sangat berterima kasih untuk setiap artikel yang sudah Penulis kirimkan.*

Pendahuluan

Pada tahun 2003 Blaster worm menginfeksi sedikitnya 100.000 sistem Microsoft Windows dan jutaan biaya dibutuhkan untuk memperbaikinya. Kendati usaha untuk membersihkan dilakukan, suatu anti worm dan suatu tool untuk membasminya, worm tersebut tetap saja menyebar. Aktivitas worm tersebut memberi pengertian yang sangat mendalam dalam evolusi worm Internet.

Worm.Win32.Lovesan.a ([Kaspersky Lab](#)) juga dikenal sebagai:

- W32/Blaster.worm.a ([McAfee](#)),
- W32.Blaster.Worm ([Symantec](#)),
- Win32.HLLW.LoveSan.based ([Doctor Web](#)),
- W32/Blaster-A ([Sophos](#)),
- Win32/Msblast.A ([RAV](#)),
- WORM_MSBLAST.A ([Trend Micro](#)),
- Worm/Lovsan.A ([H+BEDV](#)),
- W32/Msblast.A ([FRISK](#)),
- Win32:Blaster ([ALWIL](#)),
- Worm/Lovsan.A ([Grisoft](#)),
- Win32.Msblast.A ([SOFTWIN](#)),
- Worm.Blaster.A ([ClamAV](#)),
- W32/Blaster ([Panda](#)),
- Win32/Lovsan.A ([Eset](#))

yang ditulis dengan bahasa C dan Compiler LCC.

Worm yang dikenal dengan nama W32/Blaster.A dan banyak varian lainnya dengan nama Welchia atau Nachi yang menyebar menggunakan celah keamanan pada RPC DCOM BUFFER OVERFLOW. Worm W32/Blaster.A ini pada hari pertama pemunculannya langsung menempati peringkat pertama sebagai worm yang paling banyak terdeteksi menyebar di internet dimana kegiatan yang dilakukan worm ini yang terdeteksi oleh wormwatch.com adalah menscan port 135: Kalau dihitung mundur ke beberapa hari pada akhir bulan Juli 2003 ada laporan bahwa ada celah keamanan pada para

pemakai Microsoft Windows NT 4.0 & Terminal Services Edition, Microsoft Windows 2000, Microsoft Windows XP, dan Microsoft Windows Server 2003. Para penyusup dapat memasuki komputer yang terhubung dalam sebuah jaringan Internet. Pada tanggal 18 Agustus 2003 Welchia atau Nachi worm juga memanfaatkan celah yang sama dengan Blaster untuk melakukan penyebaran.

Celah keamanan pada Windows adalah **Distributed Component Object Model (DCOM) Remote Procedure Call (RPC)** interface. Celah keamanan ini sangat berbahaya dan mengancam pengguna versi Windows tersebut di atas karena para penyusup dapat melakukan:

- Instalasi Program,
- Melihat, merubah dan menghapus data, dan
- Membuat user baru dengan hak akses full pada komputer yang belum di-*patch*.

Sistem Yang Diserang

- Microsoft Windows NT 4.0
- Microsoft Windows 2000
- Microsoft Windows XP
- Microsoft Windows Server 2003

Metode Distribusi

Pertama-tama worm ini akan memindai seluruh subnet untuk membuka port 135, kemudian ia akan memindai secara random dan yang dipilih pertama kali adalah class B subnets (255.255.0.0). Jika sebuah port 135 terbuka ditemukan, seorang penyusup akan menggunakan celah keamanan yang ada untuk melakukan segala sesuatu pada komputer yang terinfeksi seperti komputer miliknya pribadi. Jika semuanya diasumsikan sukses dapat dijalankan dan ia mencoba untuk menghubungkan (connect) port 4444 dari

komputer yang terinfeksi. Ini dilakukan setelah virus ini membuat file **CMD.EXE** sebagai remote shell yang disembunyikan sehingga dapat memantau pada TCP port 4444.

Setelah tersambung, worm ini akan memerintahkan komputer kita untuk mendownload sebuah file yang bernama **MSBLAST.EXE** dengan ukuran 6,176 byte, dikemas dengan menggunakan UPX, jika di-*uncompress* besarnya 11.296 byte. Hasil download tersebut diletakkan pada direktori **Windows\System32**.

Proses download ini menggunakan FTP service dengan menjalankan sebuah file **TFTP.EXE** (*Trivial File Transfer Protocol*) pada UDP port 69. Kemudian mengirimkan sebuah perintah untuk menjalankan file **MSBLAST.EXE** tersebut pada komputer yang terinfeksi. Sebagai catatan file **TFTP.EXE** adalah sebuah utility yang terdapat pada Windows 2000/XP terletak pada **C:\WINNT\System32\TFTP.EXE**. Worm ini mampu mencari terus menerus (jika terkoneksi ke Internet) secara bersamaan ke lebih kurang 20 komputer yang belum di-*patch*. Kalau calon korbannya tidak diketahui sistem operasi apa yang dipakai, virus ini akan mengira-ngira. Ada kurang lebih 80% kesempatan akan dicoba untuk menyerang Windows XP, dan selebihnya 20% untuk Windows 2000. Jika perkiraan dari virus ini tidak benar dan komputer tersebut ada celah keamanan yang dapat ditembus, maka proses dari file **SVCHOST.EXE** yang terletak pada direktori **C:\WINDOWS\System32\svchost.exe** pada target sebuah komputer akan *crash*.

Sistem komputer akan menjadi tidak stabil, tetapi penginfeksian terhadap komputer akan gagal. Ketika **SVCHOST.EXE** *crash*, sebuah pesan akan ditampilkan pada sistem operasi Windows 2000 dan Windows XP. Untuk sistem operasi Windows XP secara **otomatis akan reboot** pada point ini.

Jika virus ini dalam memperkirakan sebuah sistem operasi berhasil mendapatkannya dan komputer tersebut memang dapat ditembus, maka ia akan langsung menginfeksi komputer tersebut. Jika worm disconnects dari komputer yang terinfeksi, proses koneksi **SCVHOST.EXE** akan *exit*. Pada sistem operasi Windows XP, ini dimungkinkan karena komputer akan **reboot**, kemudian sebuah pesan akan ditampilkan.

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

Cara kerja dari worm ini cukup unik. Setelah dijalankan virus ini akan membuat sebuah *value* dalam file *registry* sehingga akan selalu dijalankan jika komputer booting.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\windows auto update="msblast.exe"

Kemudian virus ini akan menscan dengan menggunakan metode algorithm dalam pencarian sebuah alamat IP. Ini dilakukan secara random untuk nilai-nilai angka yang akan didapatkan. Kita ketahui bahwa struktur dari sebuah *IP address* adalah A.B.C.D dimana nilai-nilai yang digunakan adalah :

A dari 0 sampai 255

B dari 0 sampai 255

C dari 0 sampai 255

D selalu 0

Mulai dari tanggal 16 Agustus 2003 komputer yang terinfeksi dengan Lovsan akan mengirimkan secara besar-besaran sebuah paket ke **windowsupdate.com**. ukuran paket tersebut hanya sebesar 40 byte yang dikirimkan dengan interval 20 millisecond ke port 80. Ini maksudnya akan menyebabkan sebuah **Distributed Denial-of-Service (DDoS)** menyerang website tersebut dengan cepatnya, yang pada akhirnya web site tersebut akan hang.

Worm ini mengandung sebuah teks (**yang tidak ditampilkan**):

```
I just want to say LOVE YOU SAN!!  
billy gates why do you make this possible ? Stop making  
money and fix your software!!
```

Bagaimana cara membasminya

- Install Service pack yang terbaru jika belum pernah menginstallnya pada masing-masing komputer sesuai dengan sistem operasinya.

- Install / memperbaharui DCOM sesuai dengan sistem operasi yang diinstall pada komputer.
- Scan komputer dengan menggunakan update yang terakhir dari antivirus yang gunakan.
- Hapus value yang telah dibuat oleh virus tersebut :

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\windows auto update="msblast.exe"

- Memblok akses ke TCP port 4444 pada firewall, dan memblok port di bawah ini :
 - TCP Port 135, "DCOM RPC"
 - UDP Port 69, "TFTP"
 - 69/UDP
 - 135/TCP
 - 135/UDP
 - 139/TCP
 - 139/UDP
 - 445/TCP
 - 445/UDP
 - 593/TCP
 - 4444/TCP

Michael Bailey is a graduate student and program manager at the University of Michigan, and a former director of engineering at Arbor Networks. His research interests include the security and availability of complex distributed systems. Bailey has a BS in computer science from the University of Illinois at Urbana-Champaign and an MS in computer science from DePaul University. Contact him at mibailey@umich.edu.

Evan Cooke is a PhD candidate at the University of Michigan and a lead researcher on the Internet Motion Sensor (IMS) project. His research interests include network security, large-scale Internet measurement, and distributed systems. Cooke has BS degrees in electrical engineering, computer science, and psychology from the University of Wisconsin and an MS in computer science from the University of Michigan. Contact him at emcooke@umich.edu.

Farnam Jahanian is a professor of electrical engineering and computer science at the University of Michigan and cofounder of Arbor Networks. His research interests include distributed computing, network security, and network architectures. Jahanian has an MS and a PhD in computer science from the University of Texas at Austin. Contact him at farnam@umich.edu.

David Watson is a postdoctoral research fellow at the University of Michigan. His research interests include network routing protocols and network infrastructure security. Watson has a BS in computer science from Carnegie Mellon University, and an MSE and PhD in computer science from the University of Michigan. Contact him at dwatson@umich.edu.

Jose Nazario is a software and security engineer at Arbor Networks. His research interests include worm detection techniques, distributed denial-of-service activity, and large-scale Internet measurements. Nazario has a BA in biology from Luther College and a PhD in biochemistry from Case Western Reserve University. He is the author of *Defense and Detection Strategies Against Internet Worms* (Artech House, 2003). Contact him at jose@arbor.net.

BIOGRAFI PENULIS



Kasiman Peranginangin. Lahir di Ujung Deleng Tanah Karo, 17 Juli 1968. Menamatkan SMU di SMU Perguruan Nasional Khalsa, Medan pada tahun 1988. Menyelesaikan program S1 pada jurusan Teknik Informatika di Institut Sains dan Teknologi T.D Pardede, Medan pada tahun 1994. Bekerja sebagai Dosen di AMIK MBP Medan. Saat ini sedang menyelesaikan program S2 pada jurusan Ilmu Komputer di Universitas Gadjah Mada Yogyakarta. Kompetensi inti adalah pada bidang Software Engineering, Jaringan Komputer dan Web Engineering

Berpengalaman sebagai engineer dan konsultan dalam bidang yang berhubungan dengan Ilmu Komputer dan Teknologi Informasi, khususnya tentang bahasa pemrograman, sistem operasi, jaringan komputer, administrasi server, aplikasi database, dan pemrograman berbasis web.

Selain tema itu juga memiliki minat dalam tema yang berhubungan dengan leadership, self improvement.

Informasi lebih lanjut tentang penulis ini bisa didapat melalui:

Email : peranginanginkasiman@yahoo.com

YM : kprans

Referensi Utama:

<http://www.computer.org/security/> (akses 21 Desember 2005)

Reference Tambahan:

http://en.wikipedia.org/wiki/Blaster_worm (akses 30 Desember 2005)

<http://www.viruslist.com/en/index.html> (akses 21 Desember 2005)

<http://www.cert.org/advisories/CA-2003-20.html> (akses 21 Desember 2005)

<http://www.angr.smu.edu/~tchen> (akses 21 Desember 2005)

<http://www.punten.com> (akses 21 Desember 2005)