



Nuevo gusano en Internet con categoría 4

Anexo del Comunicado VITI

TI024-SI-030504

Se ha detectado un nuevo gusano en Internet que tiene una alta capacidad para distribuirse utilizando una vulnerabilidad anunciada el día 13 de abril por Microsoft en su Boletín de Seguridad de Abril.

Este gusano ya está clasificado por Symantec con categoría 4, principalmente por el gran número de equipos que ya se encuentran afectados.

Las definiciones de virus del día 1 de Mayo, ya detectan esta nueva amenaza. Nuevamente se les recomienda actualizar sus sistemas operativos y actualizar las definiciones de su antivirus.

Este es el aviso emitido por Symantec, del cual pueden obtener mayor información y detalle para ejercer las medidas correspondientes.

Symantec Malicious Code Alert

W32.Sasser.B.Worm

MCID	2912
Discovered	5/1/2004
Origin	Unknown
Last Update	5/2/2004 7:47:20 PM
Types	Worm
Features	Encrypted, Memory Resident, Persistent
Risk	4/5 (High) Severity 4.5
Impact	2.6
Contagion Potential	6.4 Wild High
Last Change	Raised Risk Rating due to increased pervasiveness in the wild.
Aliases	W32/Sasser.worm.b

Infection Targets

- Microsoft Windows 2000 Advanced Server
- Microsoft Windows 2000 Advanced Server SP1
- Microsoft Windows 2000 Advanced Server SP2
- Microsoft Windows 2000 Advanced Server SP3
- Microsoft Windows 2000 Advanced Server SP4
- Microsoft Windows 2000 Datacenter Server
- Microsoft Windows 2000 Datacenter Server SP1
- Microsoft Windows 2000 Datacenter Server SP2
- Microsoft Windows 2000 Datacenter Server SP3
- Microsoft Windows 2000 Datacenter Server SP4
- Microsoft Windows 2000 Professional
- Microsoft Windows 2000 Professional SP1
- Microsoft Windows 2000 Professional SP2
- Microsoft Windows 2000 Professional SP3
- Microsoft Windows 2000 Professional SP4
- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Server SP1
- Microsoft Windows 2000 Server SP2
- Microsoft Windows 2000 Server SP3
- Microsoft Windows 2000 Server SP4
- Microsoft Windows XP Home
- Microsoft Windows XP Home SP1
- Microsoft Windows XP Media Center Edition
- Microsoft Windows XP Professional
- Microsoft Windows XP Professional SP1

Summary

- W32.Sasser.B.Worm is a worm that attempts to exploit the LSASS vulnerability patched in MS04-011. The worm spreads by randomly scanning IP addresses for vulnerable systems. It is similar in functionality to W32.Sasser.Worm.

Executable Types

- File / Binary / Portable Executable (PE)

Infection Vectors

- Remotely Exploitable Vulnerability

Impact

- Collateral Damage: Propagation may impact network performance and resources.
- Collateral Damage: Propagation may impact CPU and memory.

Symptoms

- Presence of the file %Windir%\avserve2.exe or files with names consisting of 4 or 5 digits followed by _up.exe (eg 74354_up.exe).
- Presence of the value "avserve2.exe"="%Windir%\avserve2.exe" in the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Large amounts of traffic on TCP port 445.
- Open TCP ports 5554 or 9996.
- Significant performance degradation.

Technical Description

When W32.Sasser.B.Worm runs, it does the following:

- Copies itself as %Windir%\avserve2.exe.
- Creates a mutex named "Jobaka3" so that only a single instance is present in memory at any time.
- Adds the value "avserve2.exe"="%Windir%\avserve2.exe" to the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run.
- Starts an FTP server on TCP port 5554. This server is used to spread the worm to other hosts.
- Attempts to connect to randomly-generated IP addresses on TCP port 445.
- If a connection is made, the worm sends shellcode to the host which may cause it to run a remote shell on TCP port 9996. The worm then uses the shell to connect back to the FTP server on port 5554 and retrieve a copy of the worm. This copy will have a name consisting of 4 or 5 digits followed by _up.exe (eg 74354_up.exe).

Mitigating Strategies

- Apply the patch for Microsoft Security Bulletin MS04-11 in order to prevent the LSASS buffer overrun exploit used by this threat.
- Use a firewall to block all incoming connections from the Internet to services that should not be publicly available.

Disinfection

- Remove the registry value "avserve2.exe"="%Windir%\avserve2.exe" from the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run.
- Restart the system.
- Remove the file %Windir%\avserve2.exe.

Variants

Variant of W32.Sasser.Worm

References

Symantec W32.Sasser.Worm

<http://securityresponse.symantec.com/avcenter/venc/data/w32.sasser.worm.html>

Computer Associates Win32.Sasser.A

<http://www3.ca.com/threatinfo/virusinfo/virus.aspx?id=39012>

F-Secure Sasser

<http://www.europe.f-secure.com/v-descs/sasser.shtml>

McAfee W32/Sasser.worm

http://vil.nai.com/vil/content/v_125007.htm

Trend Micro WORM_SASSER.A

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

ER.A

Microsoft PSS Security Response Team Alert - New Worm Sasser

<http://www.microsoft.com/technet/security/alerts/sasser.msp>

Symantec W32.Sasser.B.Worm

<http://securityresponse.symantec.com/avcenter/venc/data/w32.sasser.b.worm.html>

McAfee W32/Sasser.worm.b

http://vil.nai.com/vil/content/v_125008.htm



Change Log

2004.05.02: Raised Risk Rating due to increased pervasiveness in the wild.

2004.05.01: Initial analysis.

URL

https://alerts.symantec.com/members/display_alert.asp?AlertType=2&id=2912

For help with interpreting the meaning of any of the sections or labels in the alert, please visit:

<https://alerts.symantec.com/help/sia-users/malicious-code-alert-pdf.htm>

View public key at:

<https://alerts.symantec.com/Members/gnupg-sigkey.asp>