Security Center / W32.HLLW.Doomjuice

W32.HLLW.Doomjuice

Printer Friendly Page

TECHNICAL DESCRIPTION

Discovered: February 09, 2004
Updated: February 13, 2007 12:17:10 PM
Also Known As: W32/Doomjuice.worm.a [McAfee], WORM_DOOMJUICE.A [Trend], Win32.Doomjuice.A [Computer As, Worm.Win32.Doomjuice [Kaspersk, W32/Doomjuice-A [Sophos]
Type: Worm
Systems Affected: Windows

When W32.HLLW.Doomjuice runs, it does the following:

1. Creates the mutex, "sync-Z-mtx_133," which allows only one instance of the worm to execute in memory.
2. Copies itself as %System%\intrenat.exe.

   Note: %System% is a variable. The worm locates the System folder and copies itself to that location. By default, this is C:\Windows\System (Windows 95/98/Me), C:\Winnt\System32 (Windows NT/2000), or C:\Windows\System32 (Windows XP).

3. Adds the value:

   "Gremlin" = "%System%\intrenat.exe"

   to one of the following the registry keys:
   - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
   - HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

     so that the worm runs when you start Windows.

4. Creates the file Sync-src-1.00.tbz (28,569 bytes) and copies this file to the %Windir%, %System%, %Temp%, and %UserProfile% folders, as well as to the root folder of all the fixed and remote drives. This file is a tar archive, which contains the source code of W32.Mydoom.A@mm.

   Notes:
   - %Windir% is a variable: The worm locates the Windows installation folder (by default, this is C:\Windows or C:\Winnt) and copies the archive file to that location.
   - %UserProfile% is a variable: This is C:\Documents and Settings\<current logged in user>, by default, on Windows NT/2000/XP systems.
   - %Temp% is a variable: By default, this is C:\Windows\TEMP (Windows 95/98/Me), or C:\WINNT\Temp (Windows NT/2000), or C:\Document and Settings\<current logged in user>\Local Settings\Temp (Windows XP).

5. Randomly generates IP addresses and attempts to connect to those IP addresses on TCP port 3127.

   Note: Port 3127 is the port that the backdoor component of W32.Mydoom.A@mm opened.

6. If the connection is established, the worm first sends five bytes to the remote computer. Then, it sends a copy of itself to the remote computer. The backdoor component of W32.Mydoom.A@mm will accept the file and execute it.

7. If the current system date is between February 8th and 11th, the worm launches a DoS attack against www.microsoft.com, after delaying for a random amount of time, by sending a large number of HTTP GET requests to port 80.
8. If the current system date is after February 11th, but before the end of this month, the worm immediately launches a DoS attack against www.microsoft.com.

Recommendations

Symantec Security Response encourages all users and administrators to adhere to the following basic security "best practices":

- Use a firewall to block all incoming connections from the Internet to services that should not be publicly available. By default, you should deny all incoming connections and only allow services you explicitly want to offer to the outside world.
- Enforce a password policy. Complex passwords make it difficult to crack password files on compromised computers. This helps to prevent or limit damage when a computer is compromised.
- Ensure that programs and users of the computer use the lowest level of privileges necessary to complete a task. When prompted for a root or UAC password, ensure that the program asking for administration-level access is a legitimate application.
- Disable AutoPlay to prevent the automatic launching of executable files on network and removable drives, and disconnect the drives when not required. If write access is not required, enable read-only mode if the option is available.
- Turn off file sharing if not needed. If file sharing is required, use ACLs and password protection to limit access. Disable anonymous access to shared folders. Grant access only to user accounts with strong passwords to folders that must be shared.
- Turn off and remove unnecessary services. By default, many operating systems install auxiliary services that are not critical. These services are avenues of attack. If they are removed, threats have less avenues of attack.
- If a threat exploits one or more network services, disable, or block access to, those services until a patch is applied.
- Always keep your patch levels up-to-date, especially on computers that host public services and are accessible through the firewall, such as HTTP, FTP, mail, and DNS services.
- Configure your email server to block or remove email that contains file attachments that are commonly used to spread threats, such as .vbs, .bat, .exe, .pif and .scr files.
- Isolate compromised computers quickly to prevent threats from spreading further. Perform a forensic analysis and restore the computers using trusted media.
- Train employees not to open attachments unless they are expecting them. Also, do not execute software that is downloaded from the Internet unless it has been scanned for viruses. Simply visiting a compromised Web site can cause infection if certain browser vulnerabilities are not patched.
- If Bluetooth is not required for mobile devices, it should be turned off. If you require its use, ensure that the device's visibility is set to "Hidden" so that it cannot be scanned by other Bluetooth devices. If device pairing must be used, ensure that all devices are set to "Unauthorized", requiring authorization for each connection request. Do not accept applications that are unsigned or sent from unknown sources.
- For further information on the terms used in this document, please refer to the Security Response glossary.

Writeup By: Yana Liu

© 1995–2018 Symantec Corporation

EX1020
CISCO SYSTEMS, INC. / Page 2 of 2