W32.Gubed@mm

Discovered on: June 21, 2002
Last Updated on: June 24, 2002 07:10:58 PM PDT

print document email document

threat assessment | technical details | recommendations | removal instructions

W32.Gubed@mm is a mass-mailing worm that will send itself to all e-mail addresses it finds in htm and html files on an infected machine. This e-mail message will have the following characteristics:

Subject: Congratulations for your site
Attachment: WebMakeFullInstall.exe

The worm also drops a script that is an intended mass mailing worm that will attempt to send itself to all recipients in the Outlook Address Book, but due to bugs in the code, the worm will not perform the mass-mailing functionality. The e-mail message would have the following characteristics:
Subject: Important EMail for [recipient's name]
Attachment: start.vbs

The worm will copy itself to "%System%\DebugW32.exe". It will also create the file "start.vbs" in the startup folder. This Vbscript will search the "My Documents" folder and it's subfolders for files with extension of "vbs", and overwrite each file with "start.vbs".

The executable will copy itself five times to both the Windows and Windows System directory.

Also Known As: WORM_GUBED.A
Type: Worm
Infection Length: 12,800 bytes
Systems Affected: Windows 95, Windows 98, Windows NT, Windows 2000, Windows XP, Windows Me
Systems Not Affected: Macintosh, Unix, Linux

protection

• Virus Definitions (Intelligent Updater) *	June 24, 2002
• Virus Definitions (LiveUpdate™) **	June 26, 2002

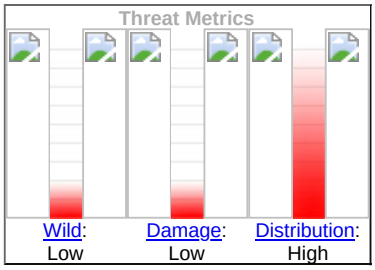
* Intelligent Updater virus definitions are released daily, but require manual download and installation. Click here to download manually.

** LiveUpdate virus definitions are usually released every Wednesday. Click here for instructions on using LiveUpdate.

threat assessment

Wild

- Number of infections: 0 - 49
- Number of sites: 0 - 2
- Geographical distribution: Low
- Threat containment: Easy
- Removal: Easy



Damage

- Payload: Attempts to send itself to all recipients in the Outlook Address Book along with sending itself to all e-mail addresses it finds in htm, html files on the infected machine.
  - Large scale e-mailing: Attempts to send itself to all recipients in the Outlook Address Book along with sending itself to all e-mail addresses it finds in htm, html files on the infected machine.

Distribution

- Subject of email: "Congratulations for your site" or "Important EMail for [recipient's name]"
- Name of attachment: WebMakeFullInstall.exe or start.vbs
- Size of attachment: 12,800 bytes or 27,255 bytes

technical details

W32.Gubed@mm is a mass-mailing worm that will send itself to all e-mail addresses it finds in the following files on an infected machine:
index.htm
index.html
index.asp
default.htm
default.html
default.asp
main.htm
main.html
main.asp
This e-mail message will have the following characteristics:
Subject: Congratulations for your site
Body: Congratulations for your site
This is a good tool to improve it.
Best Regards.
Attachment: WebMakeFullInstall.exe

The worm also drops a script that is an intended mass mailing worm that will attempt to send itself to all recipients in the Outlook Address Book, but due to bugs in the code, the worm will not perform the mass-mailing functionality. The e-mail message would have the following characteristics:
Subject: Important EMail for [recipient's name]
Body: Look at this attached file, it may be important.
Attachment: start.vbs

The worm will copy itself to "%System%\DebugW32.exe". It will set this file to start with Windows by adding the value:
"Debug"="%System%\DebugW32.exe"
to the registry key:
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

It will also create the file "%Windows%\Start Menu\Programs\StartUp\start.vbs".

This Vbscript will attempt to search the "My Documents" folder and it's subfolders for files with extension of "vbs", and overwrite each file with "start.vbs", but due to bugs in the code, the script will not perform this action.

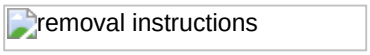
The executable will copy itself five times to both the Windows and Windows System directory. It will search for ".exe" in both folders and append on "_vbpe.exe". For example, if it finds "ACTMOVIE.EXE", it will copy itself to "ACTMOVIE.EXE_vbpe.exe". It will do this for five files in both directories.

recommendations

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

- Turn off and remove unneeded services. By default, many operating systems install auxiliary services that are not critical, such as an FTP server, telnet, and a Web server. These services are avenues of attack. If they are removed, blended threats have less avenues of attack and you have fewer services to maintain through patch updates.
- If a blended 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.
- 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.
- Configure your email server to block or remove email that contains file attachments that are commonly used to spread viruses, such as .vbs, .bat, .exe, .pif and .scr files.
- Isolate infected computers quickly to prevent further compromising your organization. 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.



To remove this worm:

1. Update the virus definitions, run a full system scan, and delete all files that are detected as W32.Gubed@mm.
2. Delete the value

```
Debug      %System%\DebugW32.exe
```

from the registry key

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

For details on how to do this, read the following instructions.

To scan with Norton AntiVirus and delete the infected files:

1. Obtain the most recent virus definitions. There are two ways to do this:
   - Run LiveUpdate, which is the easiest way to obtain virus definitions. These virus definitions have undergone full quality assurance testing by Symantec Security Response and are posted to the LiveUpdate servers one time each week (usually Wednesdays) unless there is a major virus outbreak. To determine whether definitions for this threat are available by LiveUpdate, look at the **Virus Definitions (LiveUpdate)** line at the top of this write-up.
   - Download the definitions using the Intelligent Updater. Intelligent Updater virus definitions have undergone full quality assurance testing by Symantec Security Response. They are posted on U.S. business days (Monday through Friday). They must be downloaded from the Symantec Security Response Web site and installed manually. To determine whether definitions for this threat are available by the Intelligent Updater, look at the **Virus Definitions (Intelligent Updater)** line at the top of this write-up.

     Intelligent Updater virus definitions are available here. For detailed instructions on how to download and install the Intelligent Updater virus definitions from the Symantec Security Response Web site, click here.
2. Start Norton AntiVirus (NAV), and make sure that NAV is configured to scan all files.
   - NAV Consumer products: Read the document How to configure Norton AntiVirus to scan all files.
   - NAV Enterprise products: Read the document How to verify a Symantec Corporate antivirus product is set to scan All Files.
3. Run a full system scan.
4. Delete all files that NAV detects as W32.Gubed@mm. Replace deleted files from a clean backup or reinstall them.

Write-up by: Douglas Knowles