security response

W97M.Dotor.A@mm

Discovered on: June 24, 2002
Last Updated on: June 25, 2002 09:15:18 AM PDT

print document email document

threat assessment | technical details | recommendations | removal instructions

W97M.Dotor.A@mm is a macro virus that drops a Windows executable and disables Microsoft Word macro security. The macro virus infects when you open an infected document.

Variants: W32.Dotor.A@mm
Type: Macro, Worm
Infection Length: One VBA Module
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 25, 2002
• Virus Definitions (LiveUpdate™) **	June 26, 2002

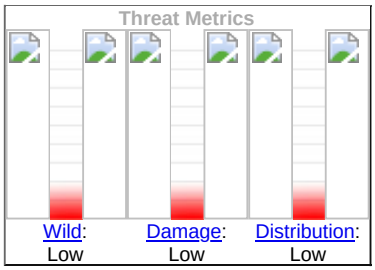
* Intelligent Updater virus definitions are released daily, but require manual download and installation. Click here to download manually.

** 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: Infects Word documents on opening
  - Modifies files: Infects Word documents on opening

technical details

When W97M.Dotor.A@mm runs, it does the following:

It creates \%Windows%\Doctor.exe. This file is detected as W32.Dotor.A@mm.

NOTE: %Windows% is a variable. The worm locates the Windows folder (by default this is C:\Windows or C:\Winnt) and copies itself to that location.

It adds the value

```
DocTor      \%Windows%\Doctor.exe /newrun
```

to the registry key

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion
```

so that Doctor.exe runs when you start Windows.

The macro virus also disables Microsoft Word macro security by setting the value data of `Level` to `1`.

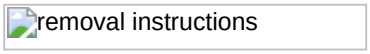
in one of these registry keys:

```
HKEY_CURRENT_USER\Software\Microsoft\Office\10.0\Word\Security
HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security
```

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.



1. Update the virus definitions, and run a full system scan. Repair all files that Norton AntiVirus (NAV) detects as W97M.Dotor.A@mm, and delete files that NAV detects as W32.Dotor.A@mm.
2. Delete the value

   `DocTor`

   from the registry key

   `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion`

3. Restore the Microsoft Word macro security settings.

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

To scan with Norton AntiVirus and delete or repair 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.Dotor.A@mm.
5. Repair all files that NAV detects as W97M.Dotor.A@mm.

To remove the value from the registry:

CAUTION: Symantec strongly recommends that you back up the registry before you make any changes to it. Incorrect changes to the registry can result in permanent data loss or corrupted files. Modify only the keys that are specified. Read the document How to make a backup of the Windows registry for instructions.

1. Click Start, and click Run. The Run dialog box appears.
2. Type `regedit` and then click OK. The Registry Editor opens.
3. Navigate to the following key:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion
```

4. In the right pane, delete the following value:

```
DocTor
```

5. Click Registry, and click Exit.

To restore the Microsoft Word macro security settings:

1. Click the Tools menu.
2. Point to Macro.
3. Click Security.
4. Click the desired security level, and click OK.

Write-up by: Douglas Knowles