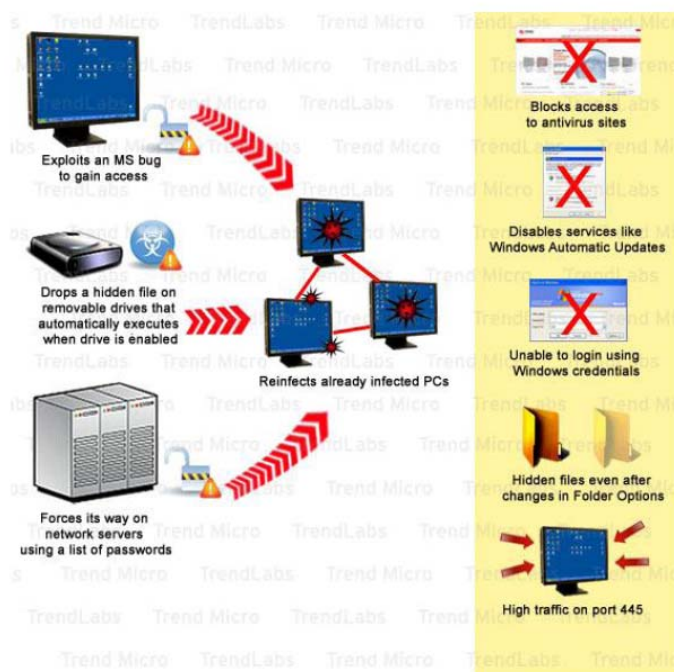




WORM_DOWNAD.KK

Best Practices and Security Recommendation



Worm_Downad.KK aka Conflicker may be downloaded and dropped from remote sites by other malwares. It may be downloaded unknowingly by an unsuspecting user when visiting malicious websites. It then registers itself as a system service to ensure its automatic execution at system start-up.

This worm connects to time servers to determine the current date. It then generates random strings based on the current date and uses certain domain extension to add to this random string for the generated websites. This worm may generate up to 50,000 random url based on the given strings. At the same time, it connects to 500 random generated URL's at a time.

More information is made available via visiting this link:

http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?vName=WORM_DOWNAD.KK&Vsect=T.

Be protected from the Exploit - Patch Security Vulnerability MS08-067

Discovery Date: Oct 23, 2008

Risk: Critical

Affected Software:

- Microsoft Windows 2000 Service Pack 4
- Microsoft Windows Server 2003 Service Pack 1
- Microsoft Windows Server 2003 Service Pack 2
- Microsoft Windows Server 2003 with SP1 for Itanium-based Systems
- Microsoft Windows Server 2003 with SP2 for Itanium-based Systems
- Microsoft Windows Server 2003 x64 Edition
- Microsoft Windows Server 2003 x64 Edition Service Pack 2
- Microsoft Windows XP Professional x64 Edition

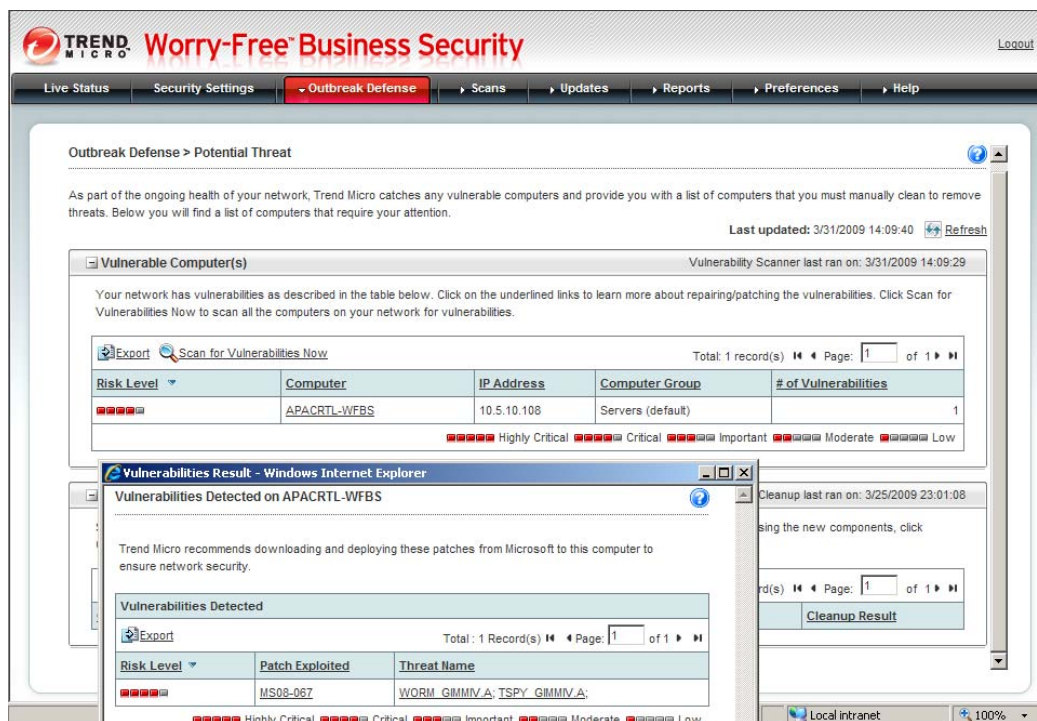
- Microsoft Windows XP Professional x64 Edition Service Pack 2
- Microsoft Windows XP Service Pack 2
- Microsoft Windows XP Service Pack 3
- Windows Server 2008 for 32-bit Systems
- Windows Server 2008 for Itanium-based Systems
- Windows Server 2008 for x64-based Systems
- Windows Vista
- Windows Vista Service Pack 1
- Windows Vista x64 Edition
- Windows Vista x64 Edition Service Pack 1

Description:

This security update resolves a reported vulnerability in the Server service. This vulnerability could allow remote code execution if an affected system received a specially-crafted RPC request. This vulnerability may be used by malicious users in the crafting of a wormable exploit such as the WORM_DOWNAD.KK.

Trend Micro Solutions:

1. **Vulnerability Assessment** – Trend Micro Control Manager for Enterprise and Worry Free Business Security for SMB has this built in feature that detects software vulnerability that can be exploited. Vulnerability Assessment does not scan for a particular malware but rather it checks the preventive measures that can be exploited by malware writers to assess the likelihood that these would be attacked by a particular malware. Minimum for Vulnerability Assessment Pattern is 94.
 - a. **Worry Free Business Security** – Checking of vulnerable machines can be done via going to Outbreak Defense > Potential Threat. There is also an option to Schedule Vulnerability Assessment via Outbreak Defense > Settings > Vulnerability Assessment.



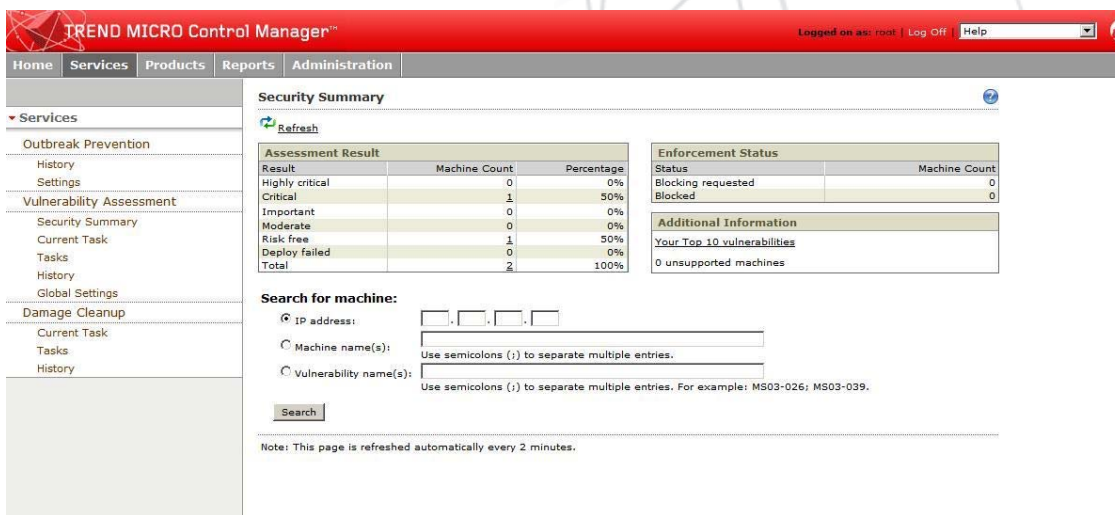
The screenshot displays the 'Outbreak Defense > Potential Threat' section of the Trend Micro Worry-Free Business Security interface. It shows a table of vulnerable computers with the following data:

Risk Level	Computer	IP Address	Computer Group	# of Vulnerabilities
Highly Critical	APACRTL-WFBS	10.5.10.108	Servers (default)	1

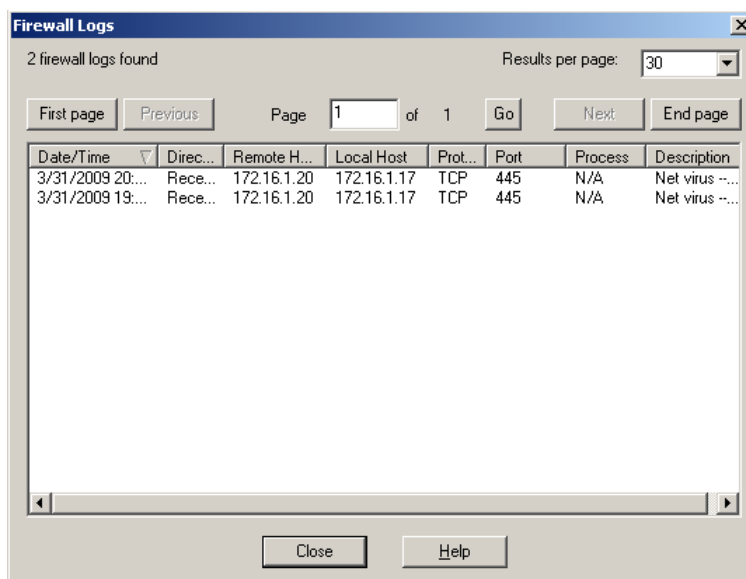
Below this, a 'Vulnerabilities Result - Windows Internet Explorer' window is open, showing details for 'Vulnerabilities Detected on APACRTL-WFBS'. It lists a vulnerability with the following details:

Risk Level	Patch Exploited	Threat Name
Highly Critical	MS08-067	WORM_GIMMVA; TSPY_GIMMVA;

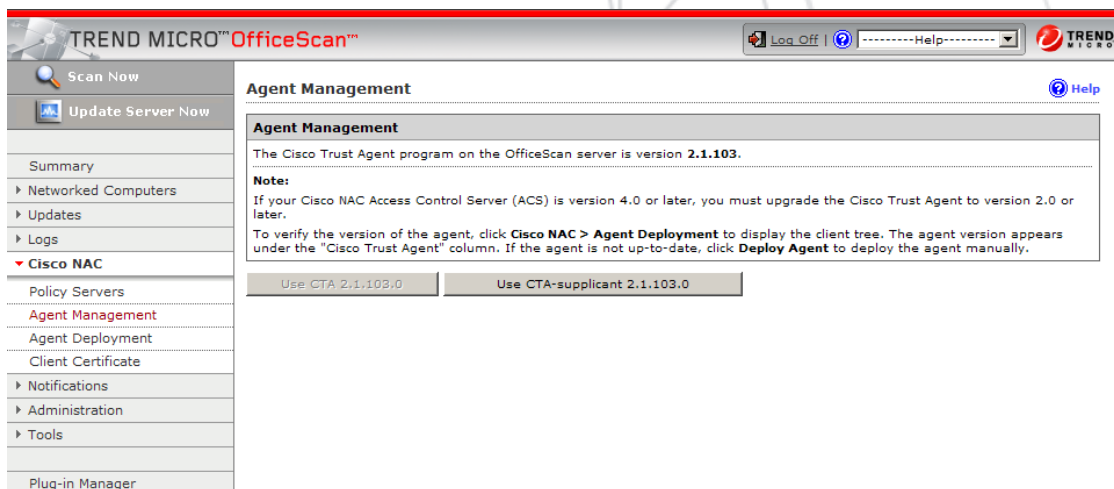
- b. **Trend Micro Control Manager** – To check for vulnerable machines click on Services > Vulnerability Assessment >Task. Create a new task that will allow Vulnerability Scanning of the entire network. Note that if it's the first time to use this feature an Active X applet prompt will be seen asking to install a library file called DCSselectTarget.cab.



- Intrusion Defense Firewall** – A plug-in firewall for OfficeScan that adds additional protection and acts as the intrusion defense system that enables you to create and enforce security policies that protect sensitive data, applications, computers or network segments. More information is made available on this link: <http://www.trendmicro.com/download/product.asp?productid=84>.
- Client Firewall** – This firewall module acts as the host firewall that helps protect machines from attacks by setting the firewall policies to monitor, evaluate and block incoming and outgoing traffic using IDS and network virus scanning. Minimum requirement for the Network Virus Pattern is 10273. Once there is a WORM_DOWNAD.KK infection and there are unpatched machines on the network there will be a high traffic on port 445 on the firewall logs and you will see the unpatched machine as Remote Host attacking the said machine as Local Host. Please see sample screenshot below:

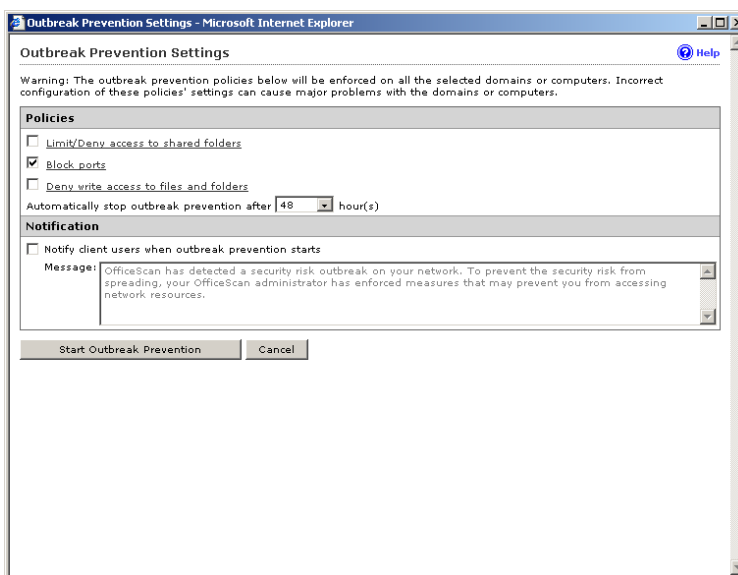


- Network Virus Wall** – An outbreak prevention appliance strategically placed on the network layer that acts as the NAC device that helps organizations to stop network viruses and block high-threat vulnerabilities during outbreaks and does cleanup of infection sources including unprotected devices as they enter the network. It separates an infected or unprotected machine from the rest of the healthy systems to prohibit spreading of the infection. This can be an alternative for a NAC compliant device such as Cisco NAC which works with OfficeScan as seen on screenshot below:

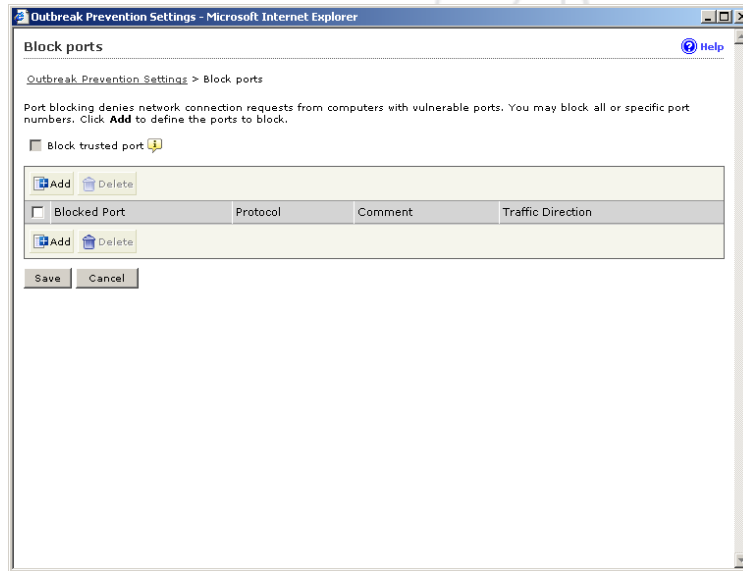


- Trend Micro Outbreak Prevention Policy** – Internally, you can use the Trend Micro solution firewalls mentioned above to block TCP ports 139 and 445 or use Outbreak Prevention Policies to help protect the network from network-based attempts to exploit this vulnerability. To use Outbreak Prevention Feature click on Network Computers > Outbreak Prevention > Start Outbreak Prevention.

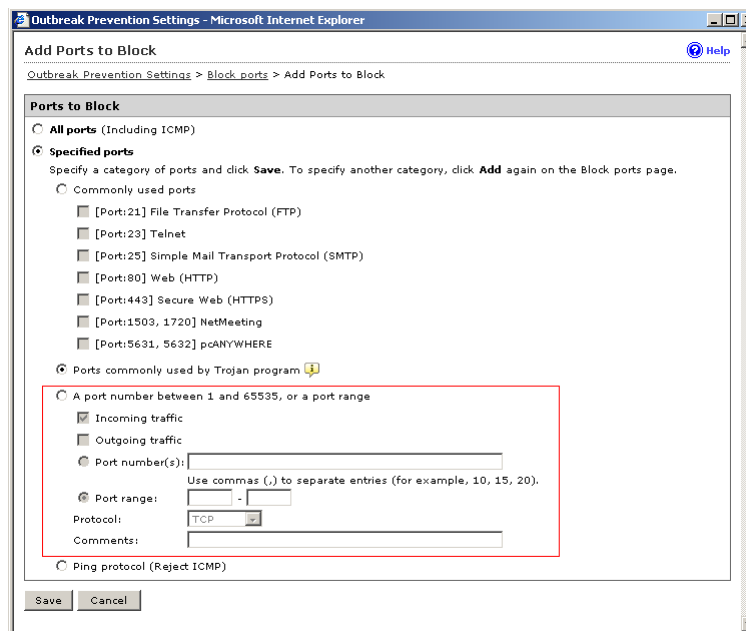
To Configure **Block ports** click on **Block Ports** from Outbreak Prevention Settings as seen on screenshot below:



Click on Add to create a port blocking rule as seen on the screenshot below:



Under the Add Ports to Block section choose the option *A port number between 1 and 65536* as seen on the screenshot below and input manually TCP ports 139 and 445:



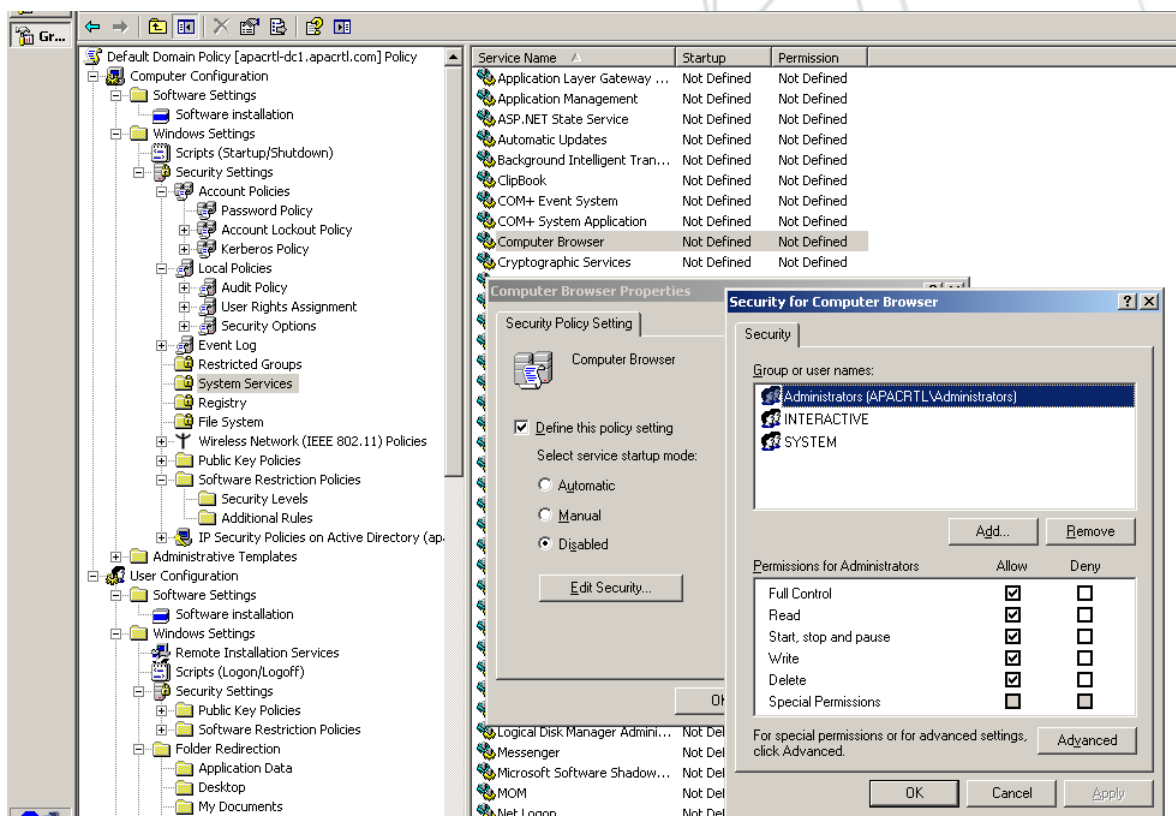
Alternative Solution:

In the absence of the above mentioned Trend Micro Solutions, to address the Vulnerability exploits you can download and install the Microsoft Baseline Security Analyzer. You may download the said tool from this link: <http://technet.microsoft.com/en-us/security/cc184923.aspx>.

The MBSA has the capability to scan a single or multiple machines on the network. Aside from providing information on the

missing hotfixes that are not installed, it also provides information on Security weaknesses such as weak password accounts, etc. In the absence of Trend Micro firewall solutions or Outbreak Prevention Policy you may use host based or personal firewalls like Windows Firewall.

Disabling the *Computer Browser* and *Server service* on the affected systems will help protect systems from remote attempts to exploit this vulnerability. You may configure this from the Domain's GPO as seen below:



Additionally, it is recommended to block TCP ports 139 and 445 at the edge or gateway firewall, as these ports are used to initiate a connection with the affected component. Blocking all unsolicited inbound communication from the Internet may help prevent attacks that use other ports.

Download the patch manually from this link: <http://www.microsoft.com/downloads/details.aspx?familyid=0D5F9B6E-9265-44B9-A376-2067B73D6A03&displaylang=en>.

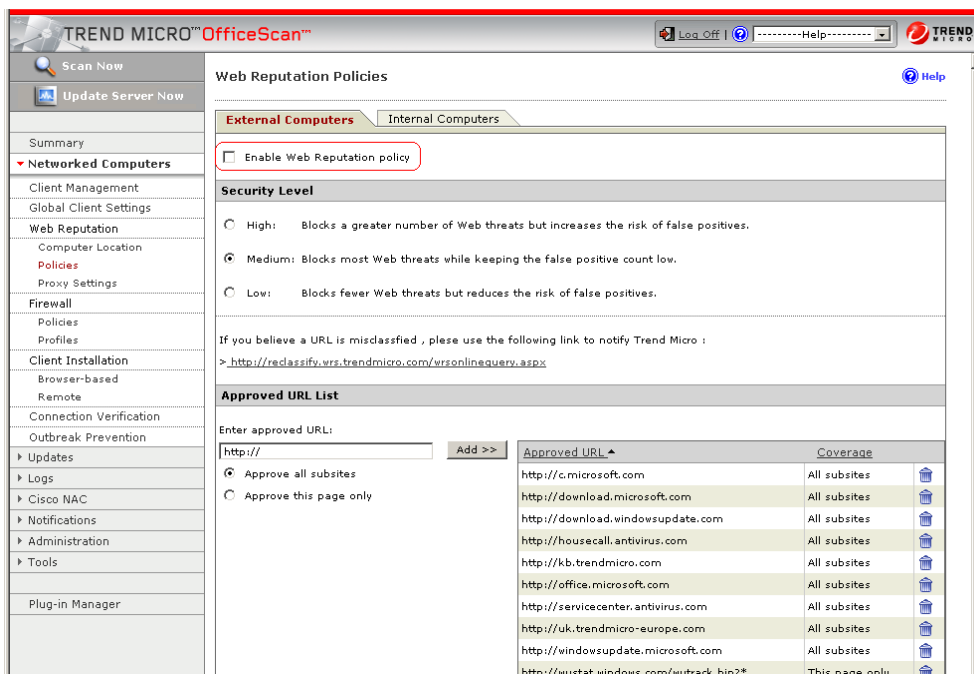
Since this malware blocks access to security sites, you may use these steps to help correct this and get the much needed security updates. Kindly follow this link for details:

<http://esupport.trendmicro.com/pages/How-to-restore-access-to-Trend-Micro-and-other-security-sites-that-have-been-blocked-by-malware-infections.aspx>

Enabling Web Threat Protection

Web Threat Protection is available on Trend Micro products Officescan 8.0, Worry Free Business Suite 5.0/5.1, InterScan Gateway Security Appliance and InterScan Web Security Suite line of products. It's highly recommended that this feature be enabled to protect non-suspecting users from visiting malicious sites.

This feature of OfficeScan 8.0 allows mobile computers to connect to multiple outside networks which extends Web threat protection to these roaming machines even when they are disconnect from the company's network. Web Reputation policies ensure client computer protection regardless of the location.



Web Reputation policies dictate whether Officescan will block or allow access to a Web site. This is useful for WORM_DOWNAD.KK since it generates 50,000 urls per day, which at anytime can unload a payload once it connects to those sites. Please see sample queries being made by the malware:

No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.16.1.20	172.16.1.255	NBNS	Name query NB VGAVTZXBSCZ.COM<00>
2	0.078170	172.16.1.20	172.16.1.255	NBNS	Name query NB HLXEHGX.NET<00>
3	0.078220	172.16.1.20	172.16.1.255	NBNS	Name query NB SREVVY.NET<00>
4	0.562767	172.16.1.20	172.16.1.255	NBNS	Name query NB LEORWX.NET<00>
5	0.750030	172.16.1.20	172.16.1.255	NBNS	Name query NB VGAVTZXBSCZ.COM<00>
6	0.828081	172.16.1.20	172.16.1.255	NBNS	Name query NB HLXEHGX.NET<00>
7	0.828094	172.16.1.20	172.16.1.255	NBNS	Name query NB SREVVY.NET<00>
8	0.994322	172.16.1.20	172.16.1.255	NBNS	Name query NB PQOSQWRX.COM<00>

These URL's are blocked automatically by Trend Micro's Web Threat Protection. But if you are not using this feature you can manually import the generated list to your HTTP filtering solutions. Download a free tool from this link:
ftp://apac-rtl.servftp.com/solutions/tools/WORM_DOWNAD.KK%20Solutions/downatool2_01.zip.

Use the following credentials:

Username: rtl
Password: rtlpattern
Archive Password: wormdownad

Additional Tools for Troubleshooting WORM_DOWNAD.KK can be downloaded from this link:
ftp://apac-rtl.servftp.com/solutions/tools/WORM_DOWNAD.KK%20Solutions/WORM_DOWNAD.KK_Solutions.zip

Use the following credentials:

Username: rtl
Password: rtlpattern
Archive Password: trendmicro

NOTE: This doesn't include the specialized Sysclean for WORM_DOWNAD.KK and TMImmune that will help protect the uninfected machines from infection Solutions. This can be requested from Trend Micro Technical Support.

Preventing WORM_DOWNAD from spreading by using Group Policy

Disclaimer:

This procedure does not remove the WORM_DOWNAD malware from the system. This procedure only stops the spread of the malware. You should use the provided Trend Micro Solutions to remove the malware from the system.

Create a new policy that applies to all computers in a specific organizational unit (OU), site, or domain, as required in your environment.

To do this, follow these steps:

1. Set the policy to remove write permissions to the following registry subkey:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Svchost

This prevents the random named malware service from being created in the netsvcs registry value.

To do this, follow these steps:

1. Open the Group Policy Management Console (GPMC).
2. Create a new Group Policy object (GPO). Give it any name that you want.
3. Open the new GPO, and then move to the following folder:
Computer Configuration\Windows Settings\Security Settings\Registry
4. Right-click **Registry**, and then click **Add Key**.

5. In the **Select Registry Key** dialog box, expand **Machine**, and then move to the following folder:
Software\Microsoft\Windows NT\CurrentVersion\Svchost
 6. Click **OK**.
 7. In the dialog box that opens, click to clear the **Full Control** check box for both **Administrators** and **System**.
 8. Click **OK**.
 9. In the **Add Object** dialog box, click **Replace existing permissions on all subkeys with inheritable permissions**.
 10. Click **OK**.
-
2. Set the policy to remove write permissions to the %windir%\tasks folder. This prevents the WORM_DOWNAD.AD from creating the Scheduled Tasks that can re-infect the system.
To do this, follow these steps:
 1. In the same GPO that you created earlier, move to the following folder:
Computer Configuration\Windows Settings\Security Settings\File System
 2. Right-click File System and then click Add File.
 3. In the **Add a file or folder** dialog box, browse to the %windir%\Tasks folder. Make sure that **Tasks** is highlighted and listed in the **Folder:** dialog box.
 4. Click **OK**.
 5. In the dialog box that opens, click to clear the check boxes for **Full Control**, **Modify** and **Write** for both **Administrators** and **System**.
 6. Click **OK**.
 7. In the **Add Object** dialog box, click **Replace existing permissions on all subkeys with inheritable permissions**.
 8. Click **OK**.

Set AutoPlay (Autorun) features to disabled. This keeps the WORM_DOWNAD from spreading by using the AutoPlay features that are built into Windows.

To do this, follow these steps:

In the same GPO that you created earlier, move to one of the following folders:

For a Windows Server 2003 domain, move to the following folder:

Computer Configuration\Administrative Templates\System

For a Windows 2008 domain, move to the following folder:

Computer Configuration\Administrative Templates\Windows Components\Autoplay Policies

9. Open the **Turn off Autoplay** policy
10. In the **Turn off Autoplay** dialog box, click **Enabled**.
11. In the drop-down menu, click **All drives**.
12. Click **OK**.

For OfficeScan 8 you can also use the Device Access Control referencing the link below:
<http://esupport.trendmicro.com/pages/Access-control-on-external-device.aspx>.

For OfficeScan 10 please use the link below:

<http://esupport.trendmicro.com/pages/Using-Device-Access-Control-to-protect-your-computer-against-Autorun-malware.aspx>

3. Disable the local administrator account. This blocks the WORM_DOWNAD.AD from using the brute force password attack against the administrator account on the system.

Note: Do not follow this step if you link the GPO to the domain controller's OU because you could disable the domain administrator account. If you have to do this on the domain controllers, create a separate GPO that does not link the GPO to the domain controller's OU, and then link the new separate GPO to the domain controller's OU. To do this, follow these steps:

1. In the same GPO that you created earlier, move to the following folder:
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options
2. Open **Accounts: Administrator account status**.
3. In the **Accounts: Administrator account status** dialog box, click to select the **Define this policy** check box.
4. Click **Disabled**.
5. Click **OK**
4. Close the Group Policy Management Console.
5. Link the newly created GPO to the location that you want it to apply to.
6. Allow for enough time for Group Policy to update to all computers. Generally, Group Policy replication takes five minutes to replicate to each domain controller, and then 90 minutes to replicate to the rest of the systems. However, more time may be required, depending on the environment.
7. After the Group Policy has propagated, clean the network using the recommended Trend Micro Solutions.