Malicious Process Detection v2

July 8, 2012 at 10:45am CDT
Dave Breslin [dbreslin]

Confidential: The following report contains confidential information. Do not distribute, email, fax, or transfer via any electronic mechanism unless it has been approved by the recipient company’s security policy. All copies and backups of this document should be saved on protected storage at all times. Do not share any of the information contained within this report with anyone unless they are authorized to view the information. Violating any of the previous instructions is grounds for termination.
# Table of Contents

## Summary

1

## Malicious Software Detection

- 10.100.0.13 ................................................................. 3
- 10.100.0.50 ................................................................. 5
- 10.110.0.52 ................................................................. 7
- 10.120.0.68 ................................................................. 9
- 172.16.2.11 ................................................................. 11
- 172.16.2.12 ................................................................. 13
- 172.16.2.50 ................................................................. 14
- 172.16.2.76 ................................................................. 17

## Potentially Unwanted Software

- 10.100.0.51 ................................................................. 20
- 10.110.0.67 ................................................................. 21
- 172.16.2.9 ................................................................. 23
- 172.16.2.81 ................................................................. 24
- 192.168.1.43 .............................................................. 25
Summary

7 Day Historical Trending

Plugin Summary

<table>
<thead>
<tr>
<th>Plugin</th>
<th>Total</th>
<th>Severity</th>
<th>Plugin Name</th>
<th>Family</th>
</tr>
</thead>
<tbody>
<tr>
<td>59275</td>
<td>8</td>
<td>Critical</td>
<td>Malicious Process Detection</td>
<td>Windows</td>
</tr>
<tr>
<td>59641</td>
<td>5</td>
<td>Info</td>
<td>Malicious Process Detection: Potentially unwanted software</td>
<td>Windows</td>
</tr>
</tbody>
</table>
Malicious Software Detection

Location Summary

<table>
<thead>
<tr>
<th>Asset</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distribution Center 2</td>
<td>4</td>
</tr>
<tr>
<td>HQ 1st Floor</td>
<td>2</td>
</tr>
<tr>
<td>HQ 2nd Floor</td>
<td>1</td>
</tr>
<tr>
<td>HQ 3rd Floor</td>
<td>1</td>
</tr>
<tr>
<td>Distribution Center 4</td>
<td>0</td>
</tr>
<tr>
<td>Distribution Center 3</td>
<td>0</td>
</tr>
<tr>
<td>HQ Wireless</td>
<td>0</td>
</tr>
<tr>
<td>Distribution Center 1</td>
<td>0</td>
</tr>
<tr>
<td>HQ Mgmt</td>
<td>0</td>
</tr>
</tbody>
</table>

Hosts Summary

<table>
<thead>
<tr>
<th>IP Address</th>
<th>NetBIOS Name</th>
<th>DNS Name</th>
<th>MAC Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.100.0.13</td>
<td>ITSDEPT\DT1010</td>
<td>dt1010.itsdept.com</td>
<td>08:00:27:81:f3:25</td>
</tr>
<tr>
<td>10.100.0.50</td>
<td>ITSDEPT\DT1042</td>
<td>dt1042.itsdept.com</td>
<td>08:00:27:ed:bf:fd</td>
</tr>
<tr>
<td>10.110.0.52</td>
<td>ITSDEPT\DT1044</td>
<td>dt1044.itsdept.com</td>
<td>08:00:27:06:8a:89</td>
</tr>
<tr>
<td>10.120.0.68</td>
<td>ITSDEPT\DT1056</td>
<td>dt1056.itsdept.com</td>
<td>08:00:27:f5:1b:89</td>
</tr>
<tr>
<td>172.16.2.11</td>
<td>ITSDEPT\DT3019</td>
<td>dt3019.itsdept.com</td>
<td>08:00:27:9e:0c:ee</td>
</tr>
<tr>
<td>172.16.2.12</td>
<td>ITSDEPT\DT3008</td>
<td>dt3008.itsdept.com</td>
<td>08:00:27:c3:c1:c4</td>
</tr>
<tr>
<td>172.16.2.50</td>
<td>ITSDEPT\DT3007</td>
<td>dt3007.itsdept.com</td>
<td>08:00:27:b3:5d:36</td>
</tr>
<tr>
<td>172.16.2.76</td>
<td>ITSDEPT\LT1007</td>
<td>lt1007.itsdept.com</td>
<td>00:26:18:6b:4c:2e</td>
</tr>
</tbody>
</table>
### 10.100.0.13

<table>
<thead>
<tr>
<th>NetBIOS Name: ITSDEPT\DT1010</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vulnerabilities:</strong> Critical: 14, High: 167, Medium: 42, Low: 4, Info: 82</td>
</tr>
<tr>
<td><strong>MAC Address:</strong> 08:00:27:81:f3:25</td>
</tr>
<tr>
<td><strong>DNS Name:</strong> dt1010.itsdept.com</td>
</tr>
<tr>
<td><strong>Last Scan:</strong> Jul 7, 2012 @ 6:38PM</td>
</tr>
</tbody>
</table>

**Host Details**

<table>
<thead>
<tr>
<th>Plugin</th>
<th>Plugin Name</th>
<th>Severity</th>
<th>Family</th>
</tr>
</thead>
<tbody>
<tr>
<td>59275</td>
<td>Malicious Process Detection</td>
<td>Critical</td>
<td>Windows</td>
</tr>
</tbody>
</table>

**Synopsis:** Nessus detected malicious processes on the remote host.

**Description:** The md5sum of one or more running process on the remote Windows host matches known malware.

**Solution:** n/a

**Risk Factor:** Critical

**CVSS Base Score:** 10.0

**CVSS Vector:** CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

**Plugin Output:** E48382BDC5867F05B82A2A6EB4E4E483 matches a known malware md5sum.

File Path: C:\Users\me\Local Settings\Temp\MSDCSC\msdcsc.exe

Associated PID(s) during check: 4080

The following are some of the tested AntiVirus products that consider this executable to be malware:

- Avast
- AVG
- BitDefender
- CA
- ClamAV
- DrWeb
- EsetNOD32
- Fortinet
- F-Prot
- McAfee
- Microsoft
- Panda
- Sophos
- Symantec

Number of AVs reporting malware: 22

Number of AVs tested: 25

For more information visit https://malwaredb.nessus.org/malware/470a52b5dda910c8bf52a9c4671a2562
<table>
<thead>
<tr>
<th><strong>Plugin Publication Date</strong></th>
<th>2012/04/12</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Plugin Modification Date</strong></td>
<td>2012/06/20</td>
</tr>
<tr>
<td><strong>Plugin Type</strong></td>
<td>local</td>
</tr>
<tr>
<td><strong>Source File</strong></td>
<td>wmi_malware_scan.nbin</td>
</tr>
</tbody>
</table>
## Host Details

<table>
<thead>
<tr>
<th>Plugin</th>
<th>Plugin Name</th>
<th>Severity</th>
<th>Family</th>
</tr>
</thead>
<tbody>
<tr>
<td>59275</td>
<td>Malicious Process Detection</td>
<td>Critical</td>
<td>Windows</td>
</tr>
</tbody>
</table>

**Synopsis:** Nessus detected malicious processes on the remote host.

**Description:** The md5sum of one or more running process on the remote Windows host matches known malware.

**Solution:** n/a

**Risk Factor:** Critical

**CVSS Base Score:** 10.0

**CVSS Vector:** CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

**Plugin Output:** C3F625470FD98AB3740F9F465529BBAA matches a known malware md5sum.

File Path : C:\Documents and Settings\me\Application Data\3 2\rundll32.exe
Associated PID(s) during check : 1636

The following are some of the tested AntiVirus products that consider this executable to be malware:
- Avast
- AVG
- BitDefender
- EsetNOD32
- Fortinet
- McAfee
- Microsoft
- Panda
- Sophos
- TrendMicro

Number of AVs reporting malware : 17

Number of AVs tested : 25

For more information visit https://malwaredb.nessus.org/malware/8ded19e53ae581f517bce38f7858b424
<table>
<thead>
<tr>
<th><strong>Plugin Type</strong></th>
<th>local</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Source File</strong></td>
<td>wmi_malware_scan.nbin</td>
</tr>
</tbody>
</table>
10.110.0.52

NetBIOS Name: ITSDEPT\DT1044
MAC Address: 08:00:27:06:8a:89
DNS Name: dt1044.itsdept.com
Last Scan: Jul 7, 2012 @ 6:38PM

Host Details

<table>
<thead>
<tr>
<th>Plugin</th>
<th>Plugin Name</th>
<th>Severity</th>
<th>Family</th>
</tr>
</thead>
<tbody>
<tr>
<td>59275</td>
<td>Malicious Process Detection</td>
<td>Critical</td>
<td>Windows</td>
</tr>
</tbody>
</table>

**Synopsis:** Nessus detected malicious processes on the remote host.

**Description:** The md5sum of one or more running process on the remote Windows host matches known malware.

**Solution:** n/a

**Risk Factor:** Critical

**CVSS Base Score:** 10.0

**CVSS Vector:** CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

**Plugin Output:** 01747A59613EC771CA1DEE0AE5FF2CCD matches a known malware md5sum.

File Path : C:\WINDOWS\system32\DNFchzna.exe
Associated PID(s) during check : 448

The following are some of the tested AntiVirus products that consider this executable to be malware:
Avast
AVG
BitDefender
ClamAV
DrWeb
EsetNOD32
Fortinet
F-Prot
McAfee
Microsoft
Panda
Sophos
Symantec
TrendMicro

Number of AVs reporting malware : 22
Number of AVs tested : 25

For more information visit https://malwaredb.nessus.org/malware/3bef5302e7467756583c75658edf49d1
Plugin Publication Date: 2012/04/12

Plugin Modification Date: 2012/06/20

Plugin Type: local

Source File: wmi_malware_scan.nbin
### Host Details

<table>
<thead>
<tr>
<th>Plugin</th>
<th>Plugin Name</th>
<th>Severity</th>
<th>Family</th>
</tr>
</thead>
<tbody>
<tr>
<td>59275</td>
<td>Malicious Process Detection</td>
<td>Critical</td>
<td>Windows</td>
</tr>
</tbody>
</table>

**Synopsis:** Nessus detected malicious processes on the remote host.

**Description:** The md5sum of one or more running process on the remote Windows host matches known malware.

**Solution:** n/a

**Risk Factor:** Critical

**CVSS Base Score:** 10.0

**CVSS Vector:** CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

**Plugin Output:** 55E37EE6B4B6A2B059110BFFFA0E4F6 matches a known malware md5sum.

File Path : C:\WINDOWS\Temp\Instalar.exe
Associated PID(s) during check : 2728

The following are some of the tested AntiVirus products that consider this executable to be malware:
- Avast
- AVG
- BitDefender
- EsetNOD32
- Fortinet
- McAfee
- Microsoft
- Panda
- Sophos

Number of AVs reporting malware : 18

Number of AVs tested : 25

For more information visit [https://malwaredb.nessus.org/malware/6d485ae32df53c0ba0bafef00199e5aa](https://malwaredb.nessus.org/malware/6d485ae32df53c0ba0bafef00199e5aa)

**Plugin Publication Date:** 2012/04/12

**Plugin Modification Date:** 2012/06/20
<table>
<thead>
<tr>
<th><strong>Plugin Type</strong></th>
<th>local</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Source File</strong></td>
<td>wmi_malware_scan.nbin</td>
</tr>
</tbody>
</table>
### Host Details

<table>
<thead>
<tr>
<th>Plugin</th>
<th>Plugin Name</th>
<th>Severity</th>
<th>Family</th>
</tr>
</thead>
<tbody>
<tr>
<td>59275</td>
<td>Malicious Process</td>
<td>Critical</td>
<td>Windows</td>
</tr>
<tr>
<td></td>
<td>Detection</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Synopsis:** Nessus detected malicious processes on the remote host.

**Description:** The md5sum of one or more running process on the remote Windows host matches known malware.

**Solution:** n/a

**Risk Factor:** Critical

**CVSS Base Score:** 10.0

**CVSS Vector:** CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

**Plugin Output:** 784440B32CD0B9852FFC2233A0B1965E matches a known malware md5sum.

File Path : C:\WINDOWS\Temp\Tim_Video032MPG.exe
Associated PID(s) during check : 1236

The following are some of the tested AntiVirus products that consider this executable to be malware:

- Avast
- AVG
- BitDefender
- CA
- ClamAV
- EsetNOD32
- Fortinet
- F-Prot
- McAfee
- Microsoft
- Panda
- Sophos
- Symantec

Number of AVs reporting malware : 21

Number of AVs tested : 25

For more information visit https://malwaredb.nessus.org/malware/d2447bd2a24edf75274dcda59a7ebbee
| **Plugin Publication Date**: | 2012/04/12 |
| **Plugin Modification Date**: | 2012/06/20 |
| **Plugin Type**: | local |
| **Source File**: | wmi_malware_scan.nbin |
172.16.2.12

NetBIOS Name: ITSDEPT\DT3008
MAC Address: 08:00:27:c3:c1:c4
DNS Name: dt3008.itsdept.com
Last Scan: Jul 7, 2012 @ 7:46PM

Host Details

<table>
<thead>
<tr>
<th>Plugin</th>
<th>Plugin Name</th>
<th>Severity</th>
<th>Family</th>
</tr>
</thead>
<tbody>
<tr>
<td>59275</td>
<td>Malicious Process Detection</td>
<td>Critical</td>
<td>Windows</td>
</tr>
</tbody>
</table>

**Synopsis:** Nessus detected malicious processes on the remote host.

**Description:** The md5sum of one or more running process on the remote Windows host matches known malware.

**Solution:** n/a

**Risk Factor:** Critical

**CVSS Base Score:** 10.0

**CVSS Vector:** CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

**Plugin Output:** 721B12891C014F321A3D9BE3CF55CF79 matches a known malware md5sum.

File Path: C:\WINDOWS\Temp\xtrail.exe
Associated PID(s) during check: 1100

The following are some of the tested AntiVirus products that consider this executable to be malware:

- Avast
- AVG
- F-Prot
- McAfee
- Panda

Number of AVs reporting malware: 10
Number of AVs tested: 25

For more information visit https://malwaredb.nessus.org/malware/bb288b932ac50b62903fd6b6c55c8a67

**Plugin Publication Date:** 2012/04/12

**Plugin Modification Date:** 2012/06/20

**Plugin Type:** local

**Source File:** wmi_malware_scan.nbin
172.16.2.50

<table>
<thead>
<tr>
<th>NetBIOS Name:</th>
<th>ITSDEPT\DT3007</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address:</td>
<td>08:00:27:b3:5d:36</td>
</tr>
<tr>
<td>DNS Name:</td>
<td>dt3007.itsdept.com</td>
</tr>
<tr>
<td>Last Scan:</td>
<td>Jul 7, 2012 @ 7:46PM</td>
</tr>
</tbody>
</table>

### Host Details

<table>
<thead>
<tr>
<th>Plugin</th>
<th>Plugin Name</th>
<th>Severity</th>
<th>Family</th>
</tr>
</thead>
<tbody>
<tr>
<td>59275</td>
<td>Malicious Process Detection</td>
<td>Critical</td>
<td>Windows</td>
</tr>
</tbody>
</table>

**Synopsis:** Nessus detected malicious processes on the remote host.

**Description:** The md5sum of one or more running process on the remote Windows host matches known malware.

**Solution:** n/a

**Risk Factor:** Critical

**CVSS Base Score:** 10.0

**CVSS Vector:** CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

**Plugin Output:** 6587DE0EC07A141D7F4713D04E3EC5E0 matches a known malware md5sum.

File Path: C:\Program Files\Common Files\Service\svchost.exe

Associated PID(s) during check: 2396

The following are some of the tested AntiVirus products that consider this executable to be malware:

- Avast
- AVG
- BitDefender
- EsetNOD32
- Fortinet
- McAfee
- Microsoft
- Panda
- Symantec
- TrendMicro

Number of AVs reporting malware: 18

Number of AVs tested: 24

For more information visit https://malwaredb.nessus.org/malware/6041e2052d279aa39fc0a7bf431245aa

6587DE0EC07A141D7F4713D04E3EC5E0 matches a known malware md5sum.

File Path: C:\Program Files\Common Files\Service\explorer.exe

Associated PID(s) during check: 2420
The following are some of the tested AntiVirus products that consider this executable to be malware:
Avast
AVG
BitDefender
EsetNOD32
Fortinet
McAfee
Microsoft
Panda
Symantec
TrendMicro

Number of AVs reporting malware : 18
Number of AVs tested : 24

For more information visit https://malwaredb.nessus.org/malware/6041e2052d279aa39fc0a7bf43f245aa

7BBEAC45BF4111AA9C2B8D8894B3D1B0 matches a known malware md5sum.
File Path : C:\Documents and Settings\me\Local Settings\Temp\explorer.exe
Associated PID(s) during check : 2608

The following are some of the tested AntiVirus products that consider this executable to be malware:
BitDefender
EsetNOD32
McAfee
Sophos

Number of AVs reporting malware : 8
Number of AVs tested : 25

For more information visit https://malwaredb.nessus.org/malware/02dbbf4b80e634b7e4a5a5f8d4438f5f

7BBEAC45BF4111AA9C2B8D8894B3D1B0 matches a known malware md5sum.
File Path : C:\Documents and Settings\me\Local Settings\Temp\IEXPLORE.EXE
Associated PID(s) during check : 3096

The following are some of the tested AntiVirus products that consider this executable to be malware:
BitDefender
EsetNOD32
McAfee
Sophos

Number of AVs reporting malware : 8
Number of AVs tested : 25

For more information visit https://malwaredb.nessus.org/malware/02dbbf4b80e634b7e4a5a5f8d4438f5f

**Plugin Publication Date**: 2012/04/12

**Plugin Modification Date**: 2012/06/20

**Plugin Type**: local
Source File: wmi_malware_scan.nbin
172.16.2.76

NetBIOS Name: ITSDEPT\LT1007
MAC Address: 00:26:18:6b:4c:2e
DNS Name: lt1007.itsdept.com
Last Scan: Jul 7, 2012 @ 7:45PM

Host Details

<table>
<thead>
<tr>
<th>Plugin</th>
<th>Plugin Name</th>
<th>Severity</th>
<th>Family</th>
</tr>
</thead>
<tbody>
<tr>
<td>59275</td>
<td>Malicious Process Detection</td>
<td>Critical</td>
<td>Windows</td>
</tr>
</tbody>
</table>

**Synopsis:** Nessus detected malicious processes on the remote host.

**Description:** The md5sum of one or more running process on the remote Windows host matches known malware.

**Solution:** n/a

**Risk Factor:** Critical

**CVSS Base Score:** 10.0

**CVSS Vector:** CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

**Plugin Output:** 330C31FD07122AD7F2D7D0FC863D9ED7 matches a known malware md5sum.

File Path: C:\WINDOWS\extext271437t.exe
Associated PID(s) during check: 2224

The following are some of the tested AntiVirus products that consider this executable to be malware:
- Avast
- AVG
- BitDefender
- CA
- ClamAV
- DrWeb
- EsetNOD32
- Fortinet
- F-Prot
- McAfee
- Microsoft
- Panda
- Sophos
- Symantec
- TrendMicro

Number of AVs reporting malware: 25
Number of AVs tested: 25

For more information visit https://malwaredb.nessus.org/malware/0fd342fbd57e701ef6de78ad9317f84e
8DA481ACB7CE2508F68071DA569CE84A matches a known malware md5sum.
File Path : C:\Documents and Settings\me\Local Settings\Temp\QvodSetupPlus3.exe
Associated PID(s) during check : 1320

The following are some of the tested AntiVirus products that consider this executable to be malware:
Avast
F-Prot
McAfee
Symantec
TrendMicro

Number of AVs reporting malware : 11
Number of AVs tested : 25

For more information visit https://malwaredb.nessus.org/malware/aa7765ab21c86db7b1b6538cdc9ad9e

330C31FD07122AD7F2D7D0FC863D9ED7 matches a known malware md5sum.
File Path : C:\WINDOWS\extext261437t.exe
Associated PID(s) during check : 364

The following are some of the tested AntiVirus products that consider this executable to be malware:
Avast
AVG
BitDefender
CA
ClamAV
DrWeb
EsetNOD32
Fortinet
F-Prot
McAfee
Microsoft
Panda
Sophos
Symantec
TrendMicro

Number of AVs reporting malware : 25
Number of AVs tested : 25

For more information visit https://malwaredb.nessus.org/malware/0fd342fbd57e701ef6de78ad9317f84e

**Plugin Publication Date:** 2012/04/12

**Plugin Modification Date:** 2012/06/20

**Plugin Type:** local

**Source File:** wmi_malware_scan.nbin
## Potentially Unwanted Software

### Location Summary

<table>
<thead>
<tr>
<th>Asset</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distribution Center 2</td>
<td>2</td>
</tr>
<tr>
<td>Distribution Center 3</td>
<td>0</td>
</tr>
<tr>
<td>Distribution Center 4</td>
<td>0</td>
</tr>
<tr>
<td>Distribution Center 1</td>
<td>0</td>
</tr>
<tr>
<td>HQ 3rd Floor</td>
<td>0</td>
</tr>
<tr>
<td>HQ Wireless</td>
<td>1</td>
</tr>
<tr>
<td>HQ Mgmt</td>
<td>0</td>
</tr>
<tr>
<td>HQ 2nd Floor</td>
<td>1</td>
</tr>
<tr>
<td>HQ 1st Floor</td>
<td>1</td>
</tr>
</tbody>
</table>

### Hosts Summary

<table>
<thead>
<tr>
<th>IP Address</th>
<th>NetBIOS Name</th>
<th>DNS Name</th>
<th>MAC Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.100.0.51</td>
<td>ITSDEPT\DT1043</td>
<td>dt1043.itsdept.com</td>
<td>08:00:27:16:ce:92</td>
</tr>
<tr>
<td>10.110.0.67</td>
<td>ITSDEPT\DT1050</td>
<td>dt1050.itsdept.com</td>
<td>08:00:27:98:b2:7d</td>
</tr>
<tr>
<td>172.16.2.9</td>
<td>ITSDEPT\DT3005</td>
<td>dt3005.itsdept.com</td>
<td>08:00:27:ac:c6:4d</td>
</tr>
<tr>
<td>172.16.2.81</td>
<td>ITSDEPT\LT1009</td>
<td>lt1009.itsdept.com</td>
<td>00:26:18:02:cd:bf</td>
</tr>
<tr>
<td>192.168.1.43</td>
<td>ITSDEPT\LT1003</td>
<td>lt1003.itsdept.com</td>
<td>00:25:d3:2d:0c:00</td>
</tr>
</tbody>
</table>
**10.100.0.51**

**NetBIOS Name:** ITSDEPT\DT1043  
**Vulnerabilities:** Critical: 13, High: 169, Medium: 42, Low: 4, Info: 86  
**MAC Address:** 08:00:27:16:ce:92  
**DNS Name:** dt1043.itsdept.com  
**Last Scan:** Jul 7, 2012 @ 6:38PM

<table>
<thead>
<tr>
<th>Plugin</th>
<th>Plugin Name</th>
<th>Severity</th>
<th>Family</th>
</tr>
</thead>
<tbody>
<tr>
<td>59641</td>
<td>Malicious Process Detection: Potentially unwanted software</td>
<td>Info</td>
<td>Windows</td>
</tr>
</tbody>
</table>

**Synopsis:** Nessus detected potentially unwanted processes on the remote host.

**Description:** The md5sum of one or more running process on the remote Windows host matches software known to violate some corporate policies. Verify that the remote processes are authorized in your environment.

**Solution:** Deinstall the remote software if it does not match your security policy.

**Risk Factor:** None

**Plugin Output:** 3E7321E4314D8ED97FDCC3836C7FC63A matches a known malware md5sum.

File Path: C:\Documents and Settings\me\Local Settings\Temp\CSM7.tmp  
Associated PID(s) during check: 304,484,876,144,288

The following are some of the tested AntiVirus products that consider this executable to be malware:  
AVG  
ClamAV  
DrWeb  
EsetNOD32

Number of AVs reporting malware: 5  
Number of AVs tested: 25  
For more information visit https://malwaredb.nessus.org/malware/58eb876106e2a58120f536ef781e720

**Plugin Publication Date:** 2012/06/21  
**Plugin Modification Date:** 2012/06/21  
**Plugin Type:** local  
**Source File:** wmi_unwanted_software.nbin
**10.110.0.67**

**NetBIOS Name:** ITSDEPT\DT1050  
**Vulnerabilities:** Critical: 13, High: 168, Medium: 42, Low: 4, Info: 80  
**MAC Address:** 08:00:27:98:b2:7d  
**DNS Name:** dt1050.itsdept.com  
**Last Scan:** Jul 7, 2012 @ 6:38PM

### Host Details

<table>
<thead>
<tr>
<th>Plugin</th>
<th>Plugin Name</th>
<th>Severity</th>
<th>Family</th>
</tr>
</thead>
<tbody>
<tr>
<td>59641</td>
<td>Malicious Process Detection: Potentially unwanted software</td>
<td>Info</td>
<td>Windows</td>
</tr>
</tbody>
</table>

**Synopsis:** Nessus detected potentially unwanted processes on the remote host.

**Description:** The md5sum of one or more running process on the remote Windows host matches software known to violate some corporate policies. Verify that the remote processes are authorized in your environment.

**Solution:** Deinstall the remote software if it does not match your security policy.

**Risk Factor:** None

**Plugin Output:** 32CD193036184BC50555ADD61132708E matches a known malware md5sum.  
File Path : C:\Documents and Settings\me\Local Settings\Application Data\zudztzhdrz.exe  
Associated PID(s) during check : 1140

The following are some of the tested AntiVirus products that consider this executable to be malware:

- Avast
- AVG
- BitDefender
- EsetNOD32
- Fortinet
- McAfee
- Microsoft
- Panda
- Sophos
- Symantec

**Number of AVs reporting malware :** 15  
**Number of AVs tested :** 25

For more information visit https://malwaredb.nessus.org/malware/1ce113fa9954167dc186c9e436bde711

**Plugin Publication Date:** 2012/06/21  
**Plugin Modification Date:** 2012/06/21  
**Plugin Type:** local

---

**Potentially Unwanted Software**

---

**Tenable Network Security**
Source File: wmi_unwanted_software.nbin
172.16.2.9

NetBIOS Name: ITSDEPT\DT3005
MAC Address: 08:00:27:ac:c6:4d
DNS Name: dt3005.itsdept.com
Last Scan: Jul 7, 2012 @ 7:46PM

Host Details

<table>
<thead>
<tr>
<th>Plugin</th>
<th>Plugin Name</th>
<th>Severity</th>
<th>Family</th>
</tr>
</thead>
<tbody>
<tr>
<td>59641</td>
<td>Malicious Process Detection: Potentially unwanted software</td>
<td>Info</td>
<td>Windows</td>
</tr>
</tbody>
</table>

**Synopsis:** Nessus detected potentially unwanted processes on the remote host.

**Description:** The md5sum of one or more running process on the remote Windows host matches software known to violate some corporate policies. Verify that the remote processes are authorized in your environment.

**Solution:** Deinstall the remote software if it does not match your security policy.

**Risk Factor:** None

**Plugin Output:** 3E7321E4314D8ED97FDDC3836C7FC63A matches a known malware md5sum.

File Path : C:\Documents and Settings\me\Local Settings\Temp\CSMD.tmp
Associated PID(s) during check : 440

The following are some of the tested AntiVirus products that consider this executable to be malware:
- AVG
- ClamAV
- DrWeb
- EsetNOD32

Number of AVs reporting malware : 5
Number of AVs tested : 25

For more information visit https://malwaredb.nessus.org/malware/58eb876106e2a58120f53c6ef781e720

**Plugin Publication Date:** 2012/06/21

**Plugin Modification Date:** 2012/06/21

**Plugin Type:** local

**Source File:** wmi_unwanted_software.nbin
172.16.2.81

NetBIOS Name: ITSDEPT\LT1009
MAC Address: 00:26:18:02:cd:bf
DNS Name: lt1009.itsdept.com
Last Scan: Jul 7, 2012 @ 7:45PM

Host Details

<table>
<thead>
<tr>
<th>Plugin</th>
<th>Plugin Name</th>
<th>Severity</th>
<th>Family</th>
</tr>
</thead>
<tbody>
<tr>
<td>59641</td>
<td>Malicious Process Detection: Potentially unwanted software</td>
<td>Info</td>
<td>Windows</td>
</tr>
</tbody>
</table>

**Synopsis**: Nessus detected potentially unwanted processes on the remote host.

**Description**: The md5sum of one or more running process on the remote Windows host matches software known to violate some corporate policies. Verify that the remote processes are authorized in your environment.

**Solution**: Deinstall the remote software if it does not match your security policy.

**Risk Factor**: None

**Plugin Output**: 3E7321E4314D8ED97FDDC3836C7FC63A matches a known malware md5sum.

File Path: C:\Documents and Settings\me\Local Settings\Temp\CSMC.tmp
Associated PID(s) during check: 1668,1356

The following are some of the tested AntiVirus products that consider this executable to be malware:
AVG
ClamAV
DrWeb
EsetNOD32

Number of AVs reporting malware: 5
Number of AVs tested: 25
For more information visit https://malwaredb.nessus.org/malware/58eb876106e2a58120f53c6ef781e720

**Plugin Publication Date**: 2012/06/21

**Plugin Modification Date**: 2012/06/21

**Plugin Type**: local

**Source File**: wmi_unwanted_software.nbin
192.168.1.43

**NetBIOS Name:** ITSDEPT\LT1003  
**Vulnerabilities:** Critical: 13, High: 207, Medium: 44, Low: 4, Info: 96  
**MAC Address:** 00:25:d3:2d:0c:00  
**DNS Name:** lt1003.itsdept.com  
**Last Scan:** Jul 7, 2012 @ 6:59PM

**Host Details**

<table>
<thead>
<tr>
<th>Plugin</th>
<th>Plugin Name</th>
<th>Severity</th>
<th>Family</th>
</tr>
</thead>
<tbody>
<tr>
<td>59641</td>
<td>Malicious Process Detection: Potentially unwanted software</td>
<td>Info</td>
<td>Windows</td>
</tr>
</tbody>
</table>

**Synopsis:** Nessus detected potentially unwanted processes on the remote host.

**Description:** The md5sum of one or more running process on the remote Windows host matches software known to violate some corporate policies. Verify that the remote processes are authorized in your environment.

**Solution:** Deinstall the remote software if it does not match your security policy.

**Risk Factor:** None

**Plugin Output:** 3E7321E4314D8ED97FDDC3836C7FC63A matches a known malware md5sum.

- File Path: C:\Documents and Settings\me\Local Settings\Temp\CSME.tmp
- Associated PID(s) during check: 1672, 2832

The following are some of the tested AntiVirus products that consider this executable to be malware:
- AVG
- ClamAV
- DrWeb
- EsetNOD32

Number of AVs reporting malware: 5

Number of AVs tested: 25

For more information visit https://malwaredb.nessus.org/malware/58eb876106e2a58120f53c6ef781e720

**Plugin Publication Date:** 2012/06/21  
**Plugin Modification Date:** 2012/06/21  
**Plugin Type:** local  
**Source File:** wmi_unwanted_software.nbin