Malicious Process Detection

June 19, 2012 at 6:36pm 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

## Infected Hosts

- 10.100.0.13 ................................................................. 3
- 10.100.0.50 ................................................................. 5
- 10.100.0.51 ................................................................. 9
- 10.100.0.52 ................................................................. 10
- 10.100.0.67 ................................................................. 11
- 10.100.0.68 ................................................................. 12
- 10.100.0.73 ................................................................. 14
- 10.100.0.76 ................................................................. 16
- 10.100.0.81 ................................................................. 18
- 10.106.0.9 ................................................................. 20
- 10.106.0.11 ............................................................... 22
- 10.106.0.12 ............................................................... 24
Summary

7 Day Historical Trending of Infected Hosts

Infected Host Totals by Location

<table>
<thead>
<tr>
<th>Asset</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>HQ</td>
<td>9</td>
</tr>
<tr>
<td>Levallois-Perret Office</td>
<td>3</td>
</tr>
<tr>
<td>HQ Wireless 1</td>
<td>0</td>
</tr>
<tr>
<td>HQ Wireless 2</td>
<td>0</td>
</tr>
<tr>
<td>Kilburn Office</td>
<td>0</td>
</tr>
<tr>
<td>Milton Keynes Office</td>
<td>0</td>
</tr>
</tbody>
</table>

Infected Host Totals by /24 Subnets

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.100.0.0/24</td>
<td>9</td>
</tr>
<tr>
<td>10.106.0.0/24</td>
<td>3</td>
</tr>
</tbody>
</table>
Infected Hosts

Infected 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>08:00:27:43:89:f3</td>
</tr>
<tr>
<td>10.100.0.50</td>
<td>ITSDEPT\DT1042</td>
<td>dt1042.itsdept.com</td>
<td>08:00:27:43:89:f1</td>
</tr>
<tr>
<td>10.100.0.51</td>
<td>ITSDEPT\DT1043</td>
<td>dt1043.itsdept.com</td>
<td>08:00:27:43:89:f7</td>
</tr>
<tr>
<td>10.100.0.52</td>
<td>ITSDEPT\DT1044</td>
<td>dt1044.itsdept.com</td>
<td>08:00:27:43:89:f9</td>
</tr>
<tr>
<td>10.100.0.67</td>
<td>ITSDEPT\DT1050</td>
<td>dt1050.itsdept.com</td>
<td>08:00:27:43:89:b1</td>
</tr>
<tr>
<td>10.100.0.68</td>
<td>ITSDEPT\DT1056</td>
<td>dt1056.itsdept.com</td>
<td>08:00:27:43:89:b5</td>
</tr>
<tr>
<td>10.100.0.73</td>
<td>ITSDEPT\LT1003</td>
<td>lt1003.itsdept.com</td>
<td>08:00:27:cf:2a:a7</td>
</tr>
<tr>
<td>10.100.0.76</td>
<td>ITSDEPT\LT1007</td>
<td>lt1007.itsdept.com</td>
<td>08:00:27:cf:2a:a9</td>
</tr>
<tr>
<td>10.106.0.9</td>
<td>ITSDEPT\DT3005</td>
<td>dt3005.itsdept.com</td>
<td>08:00:27:43:89:c5</td>
</tr>
<tr>
<td>10.106.0.11</td>
<td>ITSDEPT\DT3007</td>
<td>dt3007.itsdept.com</td>
<td>08:00:27:43:89:c8</td>
</tr>
<tr>
<td>10.106.0.12</td>
<td>ITSDEPT\DT3008</td>
<td>dt3008.itsdept.com</td>
<td>08:00:27:43:87:1f</td>
</tr>
</tbody>
</table>
10.100.0.13

**NetBIOS Name:** ITSDEPT\DT1010

**Vulnerabilities:** Critical: 0, High: 55, Medium: 5, Low: 3, Info: 74

**MAC Address:** 08:00:27:43:89:f3

**DNS Name:** dt1010.itsdept.com

**Last Scan:** Jun 19, 2012 @ 2:38PM

### Infected Detail

<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>High</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:** High

**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: 3632

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

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

Number of AVs reporting malware: 18

Number of AVs tested: 24

For more information visit [https://malwaredb.nessus.org/malware/d2447bd2a24edf75274dcdca59a7ebbee](https://malwaredb.nessus.org/malware/d2447bd2a24edf75274dcdca59a7ebbee)
### Plugin Information

<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>2012/06/08</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>
Infected Detail

<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>High</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**: High

**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: 1540

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: 25

For more information visit https://malwaredb.nessus.org/malware/6041e2052d279aa39fc0a7b43f245aa

6587DE0EC07A141D7F4713D04E3EC5E0 matches a known malware md5sum.

File Path: C:\Program Files\Common Files\Service\explorer.exe
<table>
<thead>
<tr>
<th>Associated PID(s) during check : 1516</th>
</tr>
</thead>
<tbody>
<tr>
<td>The following are some of the tested AntiVirus products that consider this executable to be malware:</td>
</tr>
<tr>
<td>Avast, AVG, BitDefender, EsetNOD32, Fortinet, McAfee, Microsoft, Panda, Symantec, TrendMicro</td>
</tr>
<tr>
<td>Number of AVs reporting malware : 18</td>
</tr>
<tr>
<td>Number of AVs tested : 25</td>
</tr>
<tr>
<td>For more information visit <a href="https://malwaredb.nessus.org/malware/6041e2052d279aa39fc0a7bf43f245aa">https://malwaredb.nessus.org/malware/6041e2052d279aa39fc0a7bf43f245aa</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>E81E02D1DC63642088018CF0B088C5AD matches a known malware md5sum.</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Path : C:\Documents and Settings\me\Local Settings\Temp\dd.exe</td>
</tr>
<tr>
<td>Associated PID(s) during check : 3032</td>
</tr>
<tr>
<td>The following are some of the tested AntiVirus products that consider this executable to be malware:</td>
</tr>
<tr>
<td>Avast, AVG, BitDefender, ClamAV, EsetNOD32, Fortinet, F-Prot, McAfee, Microsoft, Sophos, Symantec</td>
</tr>
<tr>
<td>Number of AVs reporting malware : 19</td>
</tr>
<tr>
<td>Number of AVs tested : 24</td>
</tr>
<tr>
<td>For more information visit <a href="https://malwaredb.nessus.org/malware/2357a8553dabef424114e704a8b6ae7b">https://malwaredb.nessus.org/malware/2357a8553dabef424114e704a8b6ae7b</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>330C31FD07122AD7F2D7D0FC863D9ED7 matches a known malware md5sum.</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Path : C:\WINDOWS\extext158812t.exe</td>
</tr>
<tr>
<td>Associated PID(s) during check : 4024</td>
</tr>
<tr>
<td>The following are some of the tested AntiVirus products that consider this executable to be malware:</td>
</tr>
<tr>
<td>Avast, AVG, BitDefender, CA, ClamAV, DrWeb, EsetNOD32, Fortinet, F-Prot</td>
</tr>
</tbody>
</table>

Infected Hosts
Malicious Process Detection

Infected Hosts

McAfee
Microsoft
Panda
Sophos
Symantec
TrendMicro

Number of AVs reporting malware : 24
Number of AVs tested : 25
For more information visit https://malwaredb.nessus.org/malware/0fd342fbd57e701ef6de78ad9317f84e

E81E02D1DC63642088018CF0B088C5AD matches a known malware md5sum.

File Path : C:\Documents and Settings\me\Local Settings\Temp\dd.exe
Associated PID(s) during check : 2632

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

Number of AVs reporting malware : 19
Number of AVs tested : 24
For more information visit https://malwaredb.nessus.org/malware/2357a8553dabef424114e704a8b6ae7b

D70939E86FB427F92FBDC367DD016ABB matches a known malware md5sum.

File Path : C:\Documents and Settings\me\Local Settings\Temp\explorer.exe
Associated PID(s) during check : 2332

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

Number of AVs reporting malware : 17
Number of AVs tested : 25
For more information visit https://malwaredb.nessus.org/malware/ac158d961604143a133982686072f204
<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>2012/06/08</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>
**10.100.0.51**

**NetBIOS Name:** ITSDEPT\DT1043  
**Vulnerabilities:** Critical: 0, High: 46, Medium: 5, Low: 3, Info: 73  
**MAC Address:** 08:00:27:43:89:f7  
**DNS Name:** dt1043.itsdept.com  
**Last Scan:** Jun 19, 2012 @ 2:38PM

---

### Infected Detail

<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>High</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:** High

**CVSS Base Score:** 10.0

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

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

- File Path: C:\Documents and Settings\me\Local Settings\Temp\CSM16.tmp
- Associated PID(s) during check: 1768,3628

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](https://malwaredb.nessus.org/malware/58eb876106e2a58120f53c6ef781e720)

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

**Plugin Modification Date:** 2012/06/08

**Plugin Type:** local

**Source File:** wmi_malware_scan.nbin
10.100.0.52

**NetBIOS Name:** ITSDEPT\DT1044  
**Vulnerabilities:** Critical: 0, High: 26, Medium: 5, Low: 3, Info: 72  
**MAC Address:** 08:00:27:43:89:f9  
**DNS Name:** dt1044.itsdept.com  
**Last Scan:** Jun 19, 2012 @ 2:38PM

### Infected Detail

<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>High</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:** High

**CVSS Base Score:** 10.0

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

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

File Path: C:\Documents and Settings\me\Local Settings\Temp\CSM7.tmp  
Associated PID(s) during check: 1668,2356

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:** 2012/04/12

**Plugin Modification Date:** 2012/06/08

**Plugin Type:** local

**Source File:** wmi_malware_scan.nbin

Infected Hosts
### Infected Detail

<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>High</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:** High

**CVSS Base Score:** 10.0

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

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

- File Path: `C:\Documents and Settings\me\Local Settings\Temp\CSM16.tmp`
- Associated PID(s) during check: 1668, 3256

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:** 2012/04/12

**Plugin Modification Date:** 2012/06/08

**Plugin Type:** local

**Source File:** wmi_malware_scan.nbin
### Infected Detail

<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>High</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**: High

**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: 3468

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: 21

Number of AVs tested: 24

For more information visit [https://malwaredb.nessus.org/malware/3bef5302e7467756583c75658edf49d1](https://malwaredb.nessus.org/malware/3bef5302e7467756583c75658edf49d1)
**Plugin Publication Date:** 2012/04/12  
**Plugin Modification Date:** 2012/06/08  
**Plugin Type:** local  
**Source File:** wmi_malware_scan.nbin
10.100.0.73

**NetBIOS Name:** ITSDEPT\LT1003  
**Vulnerabilities:** Critical: 13, High: 169, Medium: 39, Low: 3, Info: 66  
**MAC Address:** 08:00:27:cf:2a:a7  
**DNS Name:** lt1003.itsdept.com  
**Last Scan:** Jun 19, 2012 @ 2:42PM

### Infected Detail

<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>High</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:** High

**CVSS Base Score:** 10.0

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

**Plugin Output:** 55E37EE6B4BB6A2B059110BFFFA0E4F6 matches a known malware md5sum.

File Path: `C:\WINDOWS\Temp\Instalar.exe`
Associated PID(s) during check: 3072

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

Number of AVs reporting malware: 11
Number of AVs tested: 24

For more information visit https://malwaredb.nessus.org/malware/6d485ae32df53c0ba0bafe900199e5aa

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

**Plugin Modification Date:** 2012/06/08
Plugin Type: local
Source File: wmi_malware_scan.nbin
**Infected Detail**

<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>High</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:** High

**CVSS Base Score:** 10.0

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

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

File Path: `C:\Documents and Settings\me\Local Settings\Temp\CSM2D.tmp`

Associated PID(s) during check: 1644,396,196,1496

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

---

**Infected Hosts**

Tenable Network Security
Symantec

Number of AVs reporting malware : 7
Number of AVs tested : 25

For more information visit https://malwaredb.nessus.org/malware/53de19c9e78313855f9fae4ac66a021b

11033FE49E144984B82AE16CE1221CD0 matches a known malware md5sum.

File Path : C:\Documents and Settings\me\Local Settings\Temp\is-AF4HQ.tmp\rkverify.exe
Associated PID(s) during check : 1496

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

Number of AVs reporting malware : 12
Number of AVs tested : 25

For more information visit https://malwaredb.nessus.org/malware/8df8f47d7df4f55306282eb3a2129cbb

**Plugin Publication Date**: 2012/04/12
**Plugin Modification Date**: 2012/06/08
**Plugin Type**: local
**Source File**: wmi_malware_scan.nbin
Infected Hosts

10.100.0.81

**NetBIOS Name:** ITSDEPT\LT1009  
**Vulnerabilities:** Critical: 13, High: 168, Medium: 39, Low: 3, Info: 57  
**MAC Address:** 08:00:27:cf:2a:b4  
**DNS Name:** lt1009.itsdept.com  
**Last Scan:** Jun 19, 2012 @ 2:39PM

### Infected Detail

<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>High</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:** High

**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 : 1780

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](https://malwaredb.nessus.org/malware/bb288b932ac50b62903fd6b6c55c8a67)

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

**Plugin Modification Date:** 2012/06/08

**Plugin Type:** local
Source File: wmi_malware_scan.nbin
**10.106.0.9**

**NetBIOS Name:** ITSDEPT\DT3005  
**Vulnerabilities:** Critical: 1, High: 51, Medium: 16, Low: 3, Info: 72  
**MAC Address:** 08:00:27:43:89:c5  
**DNS Name:** dt3005.itsdept.com  
**Last Scan:** Jun 19, 2012 @ 2:39PM

### Infected Detail

<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>High</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:** High

**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\32\rundll32.exe  
Associated PID(s) during check: 3004

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

- Avast
- AVG
- BitDefender
- EsetNOD32
- Fortinet
- McAfee
- Sophos

Number of AVs reporting malware: 11

Number of AVs tested: 25

For more information visit https://malwaredb.nessus.org/malware/8ded19e53ae581f517bce381f858b424

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

**Plugin Modification Date:** 2012/06/08
<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>
### Infected Detail

<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>High</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:** High

**CVSS Base Score:** 10.0

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

**Plugin Output:** F1F49FB85AB029AD86C02EBECB892B12 matches a known malware md5sum.

File Path: C:\Program Files\Common Files\000309D5ce.dll
Associated PID(s) during check: 908, 1004, 2040

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

Number of AVs reporting malware: 21

Number of AVs tested: 25

For more information visit https://malwaredb.nessus.org/malware/af8d3ec25ec66e5345d3da7586c857c
Malicious Process Detection

Plugin Publication Date: 2012/04/12
Plugin Modification Date: 2012/06/08
Plugin Type: local
Source File: wmi_malware_scan.nbin
10.106.0.12

**NetBIOS Name:** ITSDEPT\DT3008

**Vulnerabilities:** Critical: 1, High: 55, Medium: 16, Low: 3, Info: 73

**MAC Address:** 08:00:27:43:87:1f

**DNS Name:** dt3008.itsdept.com

**Last Scan:** Jun 19, 2012 @ 2:39PM

---

**Infected Detail**

<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>High</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:** High

**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 : 3088

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 : 25

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

6587DE0EC07A141D7F4713D04E3EC5E0 matches a known malware md5sum.

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

---

**Infected Hosts**

Tenable Network Security
Associated PID(s) during check : 3112

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 : 25

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

E81E02D1DC63642088018CF0B088C5AD matches a known malware md5sum.

File Path : C:\Documents and Settings\me\Local Settings\Temp\ddd.exe
Associated PID(s) during check : 2064

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

Number of AVs reporting malware : 19

Number of AVs tested : 24

For more information visit https://malwaredb.nessus.org/malware/2357a8553dabef4214e704a8b6ae7b

E81E02D1DC63642088018CF0B088C5AD matches a known malware md5sum.

File Path : C:\Documents and Settings\me\Local Settings\Temp\dd.exe
Associated PID(s) during check : 4024

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

Number of AVs reporting malware: 19
Number of AVs tested: 24

For more information visit https://malwaredb.nessus.org/malware/2357a8553dabe4f24114e704a8b6ae7b

D70939E86FB427F92FBDC367DDD016ABB matches a known malware md5sum.
File Path: C:\Documents and Settings\me\Local Settings\Temp\explorer.exe
Associated PID(s) during check: 3528

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

Number of AVs reporting malware: 17
Number of AVs tested: 25

For more information visit https://malwaredb.nessus.org/malware/ac158d961604143a133982686072f204

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

**Plugin Modification Date:** 2012/06/08

**Plugin Type:** local

**Source File:** wmi_malware_scan.nbin