TENABLE NETWORK SECURITY, INC.

Malicious Process Detection v2

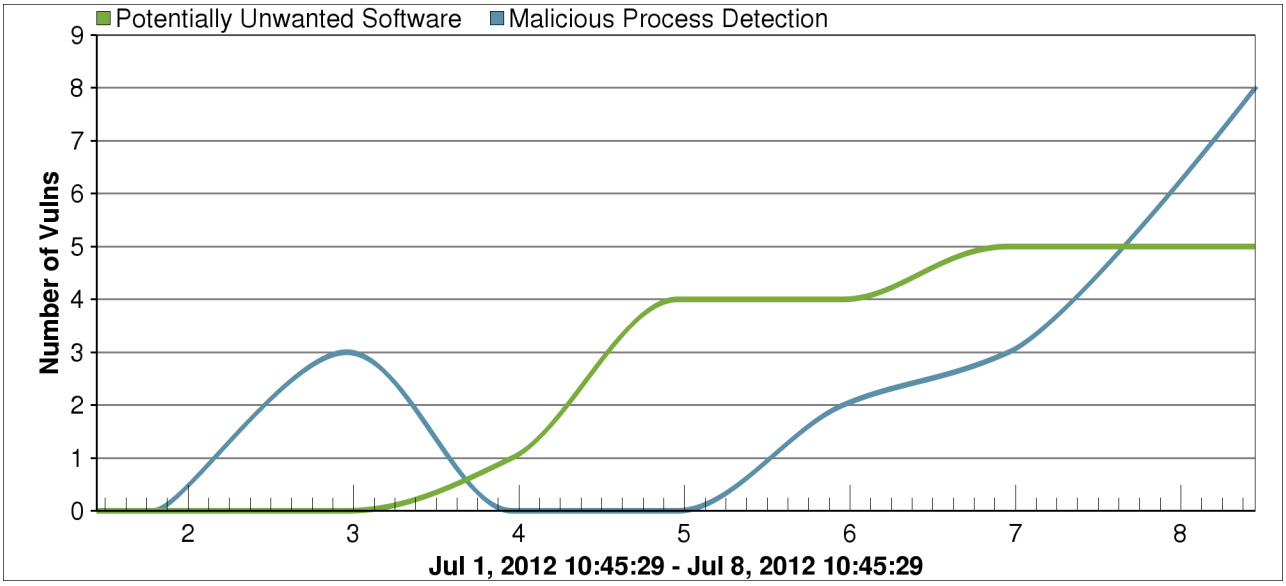
July 8, 2012 at 10:45am CDT
Dave Breslin [dbreslin]

TENABLE
Network Security®

Table of Contents

Summary

7 Day Historical Trending



Plugin Summary

Plugin	Total	Severity	Plugin Name	Family
59275	8	Critical	Malicious Process Detection	Windows
59641	5	Info	Malicious Process Detection: Potentially unwanted software	Windows

Malicious Software Detection

Location Summary

Asset	Total
Distribution Center 2	4
HQ 1st Floor	2
HQ 2nd Floor	1
HQ 3rd Floor	1
Distribution Center 4	0
Distribution Center 3	0
HQ Wireless	0
Distribution Center 1	0
HQ Mgmt	0

Hosts Summary

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

10.100.0.13

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

Host Details

Plugin	Plugin Name	Severity	Family
59275	Malicious Process Detection	Critical	Windows

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:\Documents and Settings\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

Plugin Publication Date: 2012/04/12

Plugin Modification Date: 2012/06/20

Plugin Type: local

Source File: wmi_malware_scan.nbin

10.100.0.50

NetBIOS Name: ITSDEPT\DT1042
Vulnerabilities: Critical: 14, High: 169, Medium: 42, Low: 4, Info: 79
MAC Address: 08:00:27:ed:bf:fd
DNS Name: dt1042.itsdept.com
Last Scan: Jul 7, 2012 @ 6:38PM

Host Details

Plugin	Plugin Name	Severity	Family
59275	Malicious Process Detection	Critical	Windows

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

Plugin Publication Date: 2012/04/12

Plugin Modification Date: 2012/06/20

Plugin Type: local

Source File: wmi_malware_scan.nbin

10.110.0.52

NetBIOS Name: ITSDEPT\DT1044
Vulnerabilities: Critical: 14, High: 169, Medium: 42, Low: 4, Info: 84
MAC Address: 08:00:27:06:8a:89
DNS Name: dt1044.itsdept.com
Last Scan: Jul 7, 2012 @ 6:38PM

Host Details

Plugin	Plugin Name	Severity	Family
59275	Malicious Process Detection	Critical	Windows

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

10.120.0.68

NetBIOS Name: ITSDEPT\DT1056
Vulnerabilities: Critical: 14, High: 205, Medium: 44, Low: 4, Info: 93
MAC Address: 08:00:27:f5:1b:89
DNS Name: dt1056.itsdept.com
Last Scan: Jul 7, 2012 @ 6:39PM

Host Details

Plugin	Plugin Name	Severity	Family
59275	Malicious Process Detection	Critical	Windows

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: 55E37EE6B4BB6A2B059110BFFFA0E4F6 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/6d485ae32df53c0ba0bafe900199e5aa

Plugin Publication Date: 2012/04/12

Plugin Modification Date: 2012/06/20

Plugin Type: local

Source File: wmi_malware_scan.nbin

172.16.2.11

NetBIOS Name: ITSDEPT\DT3019
Vulnerabilities: Critical: 14, High: 194, Medium: 44, Low: 4, Info: 93
MAC Address: 08:00:27:9e:0c:ee
DNS Name: dt3019.itsdept.com
Last Scan: Jul 7, 2012 @ 7:53PM

Host Details

Plugin	Plugin Name	Severity	Family
59275	Malicious Process Detection	Critical	Windows

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
Vulnerabilities: Critical: 14, High: 196, Medium: 44, Low: 4, Info: 88
MAC Address: 08:00:27:c3:c1:c4
DNS Name: dt3008.itsdept.com
Last Scan: Jul 7, 2012 @ 7:46PM

Host Details

Plugin	Plugin Name	Severity	Family
59275	Malicious Process Detection	Critical	Windows

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

NetBIOS Name: ITSDEPT\DT3007
Vulnerabilities: Critical: 14, High: 196, Medium: 44, Low: 4, Info: 92
MAC Address: 08:00:27:b3:5d:36
DNS Name: dt3007.itsdept.com
Last Scan: Jul 7, 2012 @ 7:46PM

Host Details

Plugin	Plugin Name	Severity	Family
59275	Malicious Process Detection	Critical	Windows

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/6041e2052d279aa39fc0a7bf43f245aa

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
Vulnerabilities: Critical: 14, High: 207, Medium: 44, Low: 4, Info: 191
MAC Address: 00:26:18:6b:4c:2e
DNS Name: lt1007.itsdept.com
Last Scan: Jul 7, 2012 @ 7:45PM

Host Details

Plugin	Plugin Name	Severity	Family
59275	Malicious Process Detection	Critical	Windows

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/aa7765ab21c86db7b1b6538dcdc9ad9e

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

Asset	Total
Distribution Center 2	2
Distribution Center 3	0
Distribution Center 4	0
Distribution Center 1	0
HQ 3rd Floor	0
HQ Wireless	1
HQ Mgmt	0
HQ 2nd Floor	1
HQ 1st Floor	1

Hosts Summary

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

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

Host Details

Plugin	Plugin Name	Severity	Family
59641	Malicious Process Detection: Potentially unwanted software	Info	Windows

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\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/58eb876106e2a58120f53c6ef781e720

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

Plugin	Plugin Name	Severity	Family
59641	Malicious Process Detection: Potentially unwanted software	Info	Windows

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

Source File: wmi_unwanted_software.nbin

172.16.2.9

NetBIOS Name: ITSDEPT\DT3005
Vulnerabilities: Critical: 13, High: 206, Medium: 44, Low: 4, Info: 95
MAC Address: 08:00:27:ac:c6:4d
DNS Name: dt3005.itsdept.com
Last Scan: Jul 7, 2012 @ 7:46PM

Host Details

Plugin	Plugin Name	Severity	Family
59641	Malicious Process Detection: Potentially unwanted software	Info	Windows

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
Vulnerabilities: Critical: 13, High: 210, Medium: 44, Low: 4, Info: 96
MAC Address: 00:26:18:02:cd:bf
DNS Name: lt1009.itsdept.com
Last Scan: Jul 7, 2012 @ 7:45PM

Host Details

Plugin	Plugin Name	Severity	Family
59641	Malicious Process Detection: Potentially unwanted software	Info	Windows

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

Plugin	Plugin Name	Severity	Family
59641	Malicious Process Detection: Potentially unwanted software	Info	Windows

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