

This is a report from a file uploaded to our Sandbox. The data from our Sandbox has recently been updated to remove benign files and data, you will not see a list of all open ports or running processes, instead we are only listing those processes and files that are directly relevant to the binary (malware) that was uploaded on our website. We hope this make our reports easier to read and more useful to you.

We welcome your comments and suggestions; please send them to the email address above.

Report Contains Output Reference to file: **d3445d70f7016f477bd7b7cc36a82bf8**

MD5 Hash: **d3445d70f7016f477bd7b7cc36a82bf8**

Creates Files	Sniffer Capability	Botnet Activity	Beacons Out/Download Capable	Malware Downloaded	Key Logging Capability	Opens Listening Port	Creates SMTP Traffic	Modifies MBR	SQL Attack	FTP Remote Access	Attempts lateral connection	ADS
YES	NO	NO	YES	YES	NO	NO	NO	NO	NO	NO	YES	NO

Files created on the File System - Count: 126

[Back To Top](#)

File Name:	_desktop.ini
File Path:	66efb8b2b247d4683951f893d9055a
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	66efb8b2b247d4683951f893d9055a/update
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	\$\$a1.tmp
File Path:	Documents and Settings/Administrator/Local Settings/Temp
MD5 Hash:	d41d8cd98f00b204e9800998ecf8427e
SSDeep Hash:	3::
File Name:	\$\$a2.tmp
File Path:	Documents and Settings/Administrator/Local Settings/Temp
MD5 Hash:	d41d8cd98f00b204e9800998ecf8427e
SSDeep Hash:	3::
File Name:	\$\$a3.tmp
File Path:	Documents and Settings/Administrator/Local Settings/Temp
MD5 Hash:	d41d8cd98f00b204e9800998ecf8427e
SSDeep Hash:	3::
File Name:	\$\$a4.tmp
File Path:	Documents and Settings/Administrator/Local Settings/Temp
MD5 Hash:	d41d8cd98f00b204e9800998ecf8427e
SSDeep Hash:	3::
File Name:	\$\$a5.tmp
File Path:	Documents and Settings/Administrator/Local Settings/Temp
MD5 Hash:	d41d8cd98f00b204e9800998ecf8427e
SSDeep Hash:	3::
File Name:	\$\$a6.tmp
File Path:	Documents and Settings/Administrator/Local Settings/Temp
MD5 Hash:	d41d8cd98f00b204e9800998ecf8427e
SSDeep Hash:	3::
File Name:	\$\$a7.tmp
File Path:	Documents and Settings/Administrator/Local Settings/Temp
MD5 Hash:	d41d8cd98f00b204e9800998ecf8427e
SSDeep Hash:	3::

Files created on the File System - Count: 126

[Back To Top](#)

File Name:	\$\$a8.tmp
File Path:	Documents and Settings/Administrator/Local Settings/Temp
MD5 Hash:	d41d8cd98f00b204e9800998ecf8427e
SSDeep Hash:	3::
File Name:	_desktop.ini
File Path:	MSOCache/All Users
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	MSOCache/All Users/{90120000-0010-0409-0000-0000000FF1CE}-C
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	MSOCache/All Users/{90120000-0016-0409-0000-0000000FF1CE}-C
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	MSOCache/All Users/{90120000-0018-0409-0000-0000000FF1CE}-C
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	MSOCache/All Users/{90120000-0019-0409-0000-0000000FF1CE}-C
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	MSOCache/All Users/{90120000-001A-0409-0000-0000000FF1CE}-C
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	MSOCache/All Users/{90120000-001B-0409-0000-0000000FF1CE}-C
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	MSOCache/All Users/{90120000-002C-0409-0000-0000000FF1CE}-C/Proof.en
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	MSOCache/All Users/{90120000-002C-0409-0000-0000000FF1CE}-C/Proof.es
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	MSOCache/All Users/{90120000-002C-0409-0000-0000000FF1CE}-C/Proof.fr
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	MSOCache/All Users/{90120000-002C-0409-0000-0000000FF1CE}-C
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e

Files created on the File System - Count: 126

[Back To Top](#)

File Name:	_desktop.ini
File Path:	MSOCache/All Users/{90120000-0044-0409-0000-0000000FF1CE}-C
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	MSOCache/All Users/{90120000-00A1-0409-0000-0000000FF1CE}-C
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	MSOCache/All Users/{90120000-0114-0409-0000-0000000FF1CE}-C/Groove.en-us
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	MSOCache/All Users/{90120000-0114-0409-0000-0000000FF1CE}-C
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	MSOCache/All Users/{90120000-0115-0409-0000-0000000FF1CE}-C/1033
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	MSOCache/All Users/{90120000-0115-0409-0000-0000000FF1CE}-C
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	MSOCache/All Users/{90120000-0117-0409-0000-0000000FF1CE}-C/Access.en-us
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	MSOCache/All Users/{90120000-0117-0409-0000-0000000FF1CE}-C
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	MSOCache
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Adobe Help Viewer/1.0/Resources
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Adobe Help Viewer/1.0/Resources/en
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e

Files created on the File System - Count: 126

[Back To Top](#)

File Name:	_desktop.ini
File Path:	Program Files/Adobe/Adobe Help Viewer/1.0
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Adobe Help Viewer
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/EsI
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/Reader/AIR
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/Reader/AMT
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/Reader/BeyondReader/ENU/Onramp
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/Reader/BeyondReader/ENU
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/Reader/BeyondReader
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/Reader/Browser
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/Reader/HowTo/ENU/Images
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/Reader/HowTo/ENU
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/Reader/HowTo
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e

Files created on the File System - Count: 126

[Back To Top](#)

File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/Reader/IDTemplates/ENU
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/Reader/IDTemplates
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/Reader/Javascrpts
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/Reader/Legal
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/Reader/Legal/en_US
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/Reader/Optional
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/Reader/SPPlugins
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/Reader/Tracker
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/Reader
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/Reader/adobe_epic
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/Reader/adobe_epic/eula
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/Reader/adobe_epic/eula/en_US
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e

Files created on the File System - Count: 126

[Back To Top](#)

File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/Reader/plug_ins/AcroForm/PMP
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/Reader/plug_ins/AcroForm
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/Reader/plug_ins/Annotations/Stamps/ENU
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/Reader/plug_ins/Annotations/Stamps
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/Reader/plug_ins/Annotations
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/Reader/plug_ins/ImageViewer
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/Reader/plug_ins/ImageViewer/en_US
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/Reader/plug_ins/Multimedia/MPP
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/Reader/plug_ins/Multimedia
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/Reader/plug_ins/VDKHome/ENU
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/Reader/plug_ins/VDKHome
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/Reader/plug_ins
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e

Files created on the File System - Count: 126

[Back To Top](#)

File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/Reader/plug_ins3d
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/Reader/plug_ins3d/prc
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/Resource/Font/PFM
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/Resource/Font
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/Resource/Linguistics/LanguageNames
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/Resource/Linguistics/Providers/Proximity
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/Resource/Linguistics/Providers
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/Resource/Linguistics
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/Resource
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/Setup Files
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0/Setup Files/{AC76BA86-7AD7-1033-7B44-A81300000003}
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Adobe/Reader 8.0
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e

Files created on the File System - Count: 126

[Back To Top](#)

File Name: _desktop.ini
File Path: Program Files/Adobe
MD5 Hash: 2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash: 3:vdPc:e

File Name: _desktop.ini
File Path: Program Files/MSBuild
MD5 Hash: 2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash: 3:vdPc:e

File Name: _desktop.ini
File Path: Program Files/Microsoft Visual Studio/COMMON/IDE/IDE98
MD5 Hash: 2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash: 3:vdPc:e

File Name: _desktop.ini
File Path: Program Files/Microsoft Visual Studio/COMMON/IDE
MD5 Hash: 2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash: 3:vdPc:e

File Name: _desktop.ini
File Path: Program Files/Microsoft Visual Studio/COMMON
MD5 Hash: 2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash: 3:vdPc:e

File Name: _desktop.ini
File Path: Program Files/Microsoft Visual Studio
MD5 Hash: 2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash: 3:vdPc:e

File Name: _desktop.ini
File Path: Program Files/Microsoft Works/1033
MD5 Hash: 2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash: 3:vdPc:e

File Name: _desktop.ini
File Path: Program Files/Microsoft Works
MD5 Hash: 2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash: 3:vdPc:e

File Name: _desktop.ini
File Path: Program Files/Mozilla Firefox
MD5 Hash: 2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash: 3:vdPc:e

File Name: _desktop.ini
File Path: Program Files/Mozilla Firefox/chrome
MD5 Hash: 2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash: 3:vdPc:e

File Name: _desktop.ini
File Path: Program Files/Mozilla Firefox/components
MD5 Hash: 2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash: 3:vdPc:e

File Name: _desktop.ini
File Path: Program Files/Mozilla Firefox/defaults
MD5 Hash: 2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash: 3:vdPc:e

Files created on the File System - Count: 126

[Back To Top](#)

File Name:	_desktop.ini
File Path:	Program Files/Mozilla Firefox/defaults/autoconfig
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Mozilla Firefox/defaults/pref
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Mozilla Firefox/defaults/profile
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Mozilla Firefox/defaults/profile/chrome
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Mozilla Firefox/dictionaries
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Mozilla Firefox/extensions
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Mozilla Firefox/extensions/{972ce4c6-7e08-4474-a285-3208198ce6fd}
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Mozilla Firefox/greprefs
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Mozilla Firefox/modules
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Mozilla Firefox/plugins
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Mozilla Firefox/res
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Mozilla Firefox/res/dtd
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e

Files created on the File System - Count: 126

[Back To Top](#)

File Name:	_desktop.ini
File Path:	Program Files/Mozilla Firefox/res/entityTables
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Mozilla Firefox/res/fonts
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Mozilla Firefox/res/html
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Mozilla Firefox/searchplugins
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Mozilla Firefox/uninstall
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Online Services
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Uninstall Information
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Windows Media Connect 2
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/Windows Resource Kits
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Program Files/xerox
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e

Files created on the File System - Count: 126

[Back To Top](#)

File Name:	_desktop.ini
File Path:	Program Files/xerox/nwwia
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	RECYCLER/S-1-5-21-448539723-2000478354-725345543-500
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	RECYCLER
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	_desktop.ini
File Path:	Temp
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e
File Name:	Logo1_.exe
File Path:	WINDOWS
MD5 Hash:	11dee9bc8c56ae41cc125812a14bfc55
SSDeep Hash:	384:Nbbz8Enn1Gt5M0zhIV/DZ3KZp7JcTO4yf9Knuf2MqlUV2V9wVfUnfRqOzGOnJh:p8816GVRu1yK9fMnJG2V9dHS8
File Name:	rundl132.exe
File Path:	WINDOWS
MD5 Hash:	11dee9bc8c56ae41cc125812a14bfc55
SSDeep Hash:	384:Nbbz8Enn1Gt5M0zhIV/DZ3KZp7JcTO4yf9Knuf2MqlUV2V9wVfUnfRqOzGOnJh:p8816GVRu1yK9fMnJG2V9dHS8
File Name:	rundl132.exe
File Path:	WINDOWS/uninstall
MD5 Hash:	07ca21f67e556f03c6c6f07790444a6a
SSDeep Hash:	1536:YbaHK3QJSiOR3Rmb2neRKQAShIFroVDNVXC2lkDxKFn/Ny:YbaHK3QJSi/B9RVAnqVXVkdxy
File Name:	vDll.dll
File Path:	WINDOWS
MD5 Hash:	98213641aaca1e7fa88a4ea77a2975ef
SSDeep Hash:	384:YJxz0C6Evq+1EtQ2tdl9Fs55mJBg1Uv8fd4thLctXm3z5GZC:jC6SqdSYQ+n4litthLij5GI
File Name:	_desktop.ini
File Path:	_desktop.ini
MD5 Hash:	2da77ef26b8b2204e2d5641f9f1cc3d5
SSDeep Hash:	3:vdPc:e

Files which were modified on the File System with the corresponding MD5SUM and Path - Count: 144

File Name:	update.exe
File Path:	66efb8b2b247d4683951f893d9055a/update
MD5 Hash:	5fb12ac1cd4c88a8a6de9a034eb6b070
File Name:	NTUSER.DAT
File Path:	Documents and Settings/Administrator
MD5 Hash:	9d37b7902d2b56615e3332b04bd291c3
File Name:	NTUSER.DAT
File Path:	Documents and Settings/LocalService
MD5 Hash:	c5fbbc211489139a31984f8caba61a8a

Files which were modified on the File System with the corresponding MD5SUM and Path - Count: 144

File Name:	NTUSER.DAT
File Path:	Documents and Settings/NetworkService
MD5 Hash:	1a9358403d5f91673ffc687a5369f492
File Name:	DW20.EXE
File Path:	MSOCache/All Users/{90120000-0115-0409-0000-0000000FF1CE}-C
MD5 Hash:	9af660514f865fcb14c6af858cc737a6
File Name:	dwtrig20.exe
File Path:	MSOCache/All Users/{90120000-0115-0409-0000-0000000FF1CE}-C
MD5 Hash:	a9729f2b8a9669ba72f79259ac0428f5
File Name:	ose.exe
File Path:	MSOCache/All Users/{91120000-0030-0000-0000-0000000FF1CE}-C
MD5 Hash:	1818b21c3db7e27ea39abbb599716257
File Name:	setup.exe
File Path:	MSOCache/All Users/{91120000-0030-0000-0000-0000000FF1CE}-C
MD5 Hash:	6b07a2645f75b0f5f9cf6b8f25e60fe0
File Name:	ahv.exe
File Path:	Program Files/Adobe/Adobe Help Viewer/1.0
MD5 Hash:	7f6b8481c1f6158bb708f207c7943ffa
File Name:	AcroRd32.exe
File Path:	Program Files/Adobe/Reader 8.0/Reader
MD5 Hash:	3acb5e48f090357296e1b1cec27d797a
File Name:	AcroRd32Info.exe
File Path:	Program Files/Adobe/Reader 8.0/Reader
MD5 Hash:	c1e121ddd1a3e32c0f6f899a9ab7ef71
File Name:	AdobeCollabSync.exe
File Path:	Program Files/Adobe/Reader 8.0/Reader
MD5 Hash:	89f752d246779a408dca017034d32a40
File Name:	AdobeUpdateCheck.exe
File Path:	Program Files/Adobe/Reader 8.0/Reader
MD5 Hash:	18aae5deb9f7154adf71f0dd18497bf6
File Name:	PDFPrevHndlrShim.exe
File Path:	Program Files/Adobe/Reader 8.0/Reader
MD5 Hash:	2637916fc5459c3f31201222babfdea1
File Name:	Setup.exe
File Path:	Program Files/Adobe/Reader 8.0/Setup Files/{AC76BA86-7AD7-1033-7B44-A81300000003}
MD5 Hash:	322c3eefcb37c5047257510e17acc49c
File Name:	crashreporter.exe
File Path:	Program Files/Mozilla Firefox
MD5 Hash:	ac2421a12e863e5b673e237439e4f4aa
File Name:	firefox.exe
File Path:	Program Files/Mozilla Firefox
MD5 Hash:	f0e82f90b0cee3c1ee02c2f0fe2612b9

Files which were modified on the File System with the corresponding MD5SUM and Path - Count: 144

File Name:	helper.exe
File Path:	Program Files/Mozilla Firefox/uninstall
MD5 Hash:	c052093c1447cb1c4f9bb49bbc703918
File Name:	updater.exe
File Path:	Program Files/Mozilla Firefox
MD5 Hash:	9f2af68ebf14c393de4853ebb9666937
File Name:	wmccds.exe
File Path:	Program Files/Windows Media Connect 2
MD5 Hash:	633d26fbadc4b424e80dbbeead8de2d0
File Name:	WMCCFG.exe
File Path:	Program Files/Windows Media Connect 2
MD5 Hash:	633d26fbadc4b424e80dbbeead8de2d0
File Name:	adlb.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	b0d987858a8a27c26e52e1cd4f16d3c6
File Name:	atmarp.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	fc187b050a664daa361f6e6b0cee00ab
File Name:	atmlane.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	ad28985ecdbb049e463bd3cc91201fde
File Name:	autoexnt.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	dfe6536ec12b0027633306a7f0079022
File Name:	cdburn.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	7fea2d24a845c69c0fe582641536a014
File Name:	cepsetup.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	5b9e2f3ce318962bd97d28c5c592bcb4
File Name:	chklnks.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	ce186084952f6d39f5c6e55dc4588e04
File Name:	chknic.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	97c51aa92852bc94af00a20efddc5046
File Name:	cleanspl.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	d258be60f19e6c9277352aee282d5f3b
File Name:	clearmem.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	10dd31168a648e3a9f0d23bde77c19a8

Files which were modified on the File System with the corresponding MD5SUM and Path - Count: 144

File Name:	dh.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	f1c5a0e0278f0163766421a821b57663
File Name:	diskraid.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	103c555e5151a53bb8a4dcdace6b49c
File Name:	diskuse.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	6db9144190afb3c474ff98c0b437d019
File Name:	dnsdiag.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	cddea59796f744077f60108d265ec764
File Name:	dvdburn.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	f8a1e7efa8e385dac5f1e0f4567b3407
File Name:	empty.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	85301c8e820b2786f0c39ea8bb743eea
File Name:	eventcombmt.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	fd881ce69ca8f2e8b42d4dd2ee23a624
File Name:	fcsetup.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	36a8058c3f3533ce0c511fc804368b70
File Name:	getcm.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	0090d9fe5270796e8032c0f9068af5f2
File Name:	linkd.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	94e02200891941fc769d054080becbc6
File Name:	linkspeed.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	1711ed8bd4e96b1835cd5c908641195b
File Name:	list.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	cd1e4d39d048041c070b2fd6e1529456
File Name:	lockoutstatus.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	10ee1af4812be133fc6ee864c9d9c9ef
File Name:	logtime.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	462387c70486fe16fa92e91036941a40

Files which were modified on the File System with the corresponding MD5SUM and Path - Count: 144

File Name:	lsreport.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	9bee560dfbb23a01712f161907139dc2
File Name:	lsview.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	db91715d149b0b6bf7f5d1daa02e3f98
File Name:	mcast.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	6091f819b479b3b2aeaac1dea850bc3f
File Name:	memmonitor.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	0d6b18488bb1f745b3df96b314b3feca
File Name:	memtriage.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	5dcf89b6c1f84958f39c4e94a23d815e
File Name:	mibcc.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	780a6850c70f19847a5277e31d684ed0
File Name:	moveuser.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	af4005abeb5ce29214d608ef4cac483f
File Name:	printdriverinfo.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	51c09e98b9c5c099520665c7a6c7f130
File Name:	qgrep.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	37ad36bb34e0471483cc64db83654a5b
File Name:	qtcp.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	3c771634ed000e387b9b3f62e163f72a
File Name:	rassrvmon.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	9551e8c51791f265cb25e36cbf582557
File Name:	rcontrolad.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	1124d1cc3c088264e0dc64921eab6bd8
File Name:	regini.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	069a77742e879862860a81229bb0600d
File Name:	showperf.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	ab73e4070219dd0dc8eb711fe4c8fbfd

Files which were modified on the File System with the corresponding MD5SUM and Path - Count: 144

File Name:	showpriv.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	d3a2555c28db6a937289dfa603fd0c67
File Name:	sonar.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	8d97b9a4a6759bc0da7569d4c511972c
File Name:	splinfo.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	a89dbfab198c993bebe34a3aad888002
File Name:	srvany.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	4a95fbbd014f5b260a6d6b94a62c3d3e
File Name:	srvcheck.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	76556381c17fb04c14a4c8626794e4f9
File Name:	srvinfo.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	6da09b5d778985ad8d29da425c94d02a
File Name:	srvmgr.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	0b7f40a6c59f31a02951d72ec6b82d2d
File Name:	ssdformat.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	549ca07b2dd6ec5a1281872b3a7a0a3c
File Name:	subinacl.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	94941c12b665dbfe56a41bbd6bbbc105
File Name:	tail.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	4cbdc397c56363c0a2edc41a56eb1e12
File Name:	tccom.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	6efcbd7f9524d1dd556844edec3e4d32
File Name:	tcmon.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	e91f88c68b78e6ff64b8227a8ffbc6b
File Name:	timeit.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	f2e645db913f9f2527bdcf48ed712659
File Name:	timezone.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	66e444436913b5e7254e4f8702ee849d

Files which were modified on the File System with the corresponding MD5SUM and Path - Count: 144

File Name:	tsctst.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	0b84a3ef174e5adb03225cfa337cc361
File Name:	tsscalling.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	c86470a379e732001a5fa5bdbbcad68f
File Name:	uddiconfig.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	f4ee257a7fa3ec16d0cbf19b2907d9de
File Name:	uddidataexport.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	491c776d922e03a9c10f6a64a9963ba5
File Name:	usrmgr.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	e011210ef389d0fa539a9e2732f89233
File Name:	vadump.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	9b5c8828acd9119855821493e7421032
File Name:	vfi.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	3358fc090ed17b0b2844b1edcd7fd47d
File Name:	volperf.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	edbe56bdfb8f0d3a0ea2358d328fd399
File Name:	volrest.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	0fe5e266aa2c76e3316feecf7298a69e
File Name:	vrfydsk.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	4fd6f25e003081927a70fea70ef2b591
File Name:	winhttpcertcfg.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	61c924f008f95131cf2a3169bda22047
File Name:	winhttptracecfg.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	6a84f61be9f25b6f36e48130a0dbbc2e
File Name:	winpolicies.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	d6349d9b75890028c2371ff09636f74f
File Name:	gpmonitor.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	7d995dc589f2c36dcbef81e8476cf3b5

Files which were modified on the File System with the corresponding MD5SUM and Path - Count: 144

File Name: mqcast.exe
 File Path: Program Files/Windows Resource Kits/Tools
 MD5 Hash: 130770e10537bf916af20a1116b635ad

File Name: regview.exe
 File Path: Program Files/Windows Resource Kits/Tools
 MD5 Hash: 15d0b2f556289b2f7a5dee51ce977b0d

File Name: showacls.exe
 File Path: Program Files/Windows Resource Kits/Tools
 MD5 Hash: 2b8fa3e7975dd7205f8b0fdf2a16857a

File Name: uddicatschemeeditor.exe
 File Path: Program Files/Windows Resource Kits/Tools
 MD5 Hash: 7d0e0e992d593cd42c1ba70957668878

File Name: clusterrecovery.exe
 File Path: Program Files/Windows Resource Kits/Tools
 MD5 Hash: 226391c095de404927f623f5a1326be9

File Name: compress.exe
 File Path: Program Files/Windows Resource Kits/Tools
 MD5 Hash: c5b32cda1a8bef4962a13714071e57c3

File Name: confdisk.exe
 File Path: Program Files/Windows Resource Kits/Tools
 MD5 Hash: 1fbd4d5680c7459a560cbc93f03c77aa

File Name: consume.exe
 File Path: Program Files/Windows Resource Kits/Tools
 MD5 Hash: 3d4b66d7e54613ee3be85be81b7d1b34

File Name: creatfil.exe
 File Path: Program Files/Windows Resource Kits/Tools
 MD5 Hash: c011eb5e797d02fef24676f8c77ad9a6

File Name: csccmd.exe
 File Path: Program Files/Windows Resource Kits/Tools
 MD5 Hash: 11e87c259fb2aa07514d1fd8617fd337

File Name: custreasonedit.exe
 File Path: Program Files/Windows Resource Kits/Tools
 MD5 Hash: c05f5ecd1577d43cc9eab4cc0179e2c8

File Name: delprof.exe
 File Path: Program Files/Windows Resource Kits/Tools
 MD5 Hash: 49793954798eb9e466e3d9dd64fc3b49

File Name: gpoutil.exe
 File Path: Program Files/Windows Resource Kits/Tools
 MD5 Hash: 589809451bca7dbad2f9a48b2757c6e1

File Name: hlscan.exe
 File Path: Program Files/Windows Resource Kits/Tools
 MD5 Hash: dbe4cca0baa81d7fc5bf8ef9e2c22575

Files which were modified on the File System with the corresponding MD5SUM and Path - Count: 144

File Name:	ifiltst.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	25d680322b30fc79a7638fced5d25980
File Name:	ifmember.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	5ae5196287d5c2953880f1f9c3d1bb8a
File Name:	iniman.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	0604c4dff915de4d342f88a4d514a282
File Name:	instcm.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	4fc5e4a0f4bb2976fd8c373b1a1c7ea9
File Name:	instext.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	269498bf15623ddd6e6391d9aec6ced
File Name:	instsrv.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	eccddbdc4b9248b3cf63d7af03a4a17
File Name:	intfiltr.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	b76f2d2efdca4f99a7a5fd302a305a53
File Name:	kerbtray.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	2969b4cbe93e715c7b691c7b69524898
File Name:	kernrate.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	6bda05dd069ead2643aaf335a553b034
File Name:	klist.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	6fbefbd0d1aaa594d7ee57e9b9f79106
File Name:	krt.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	a58eaa913024b8557aa10bab37757ccd
File Name:	mqcatch.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	793734b24e031db2f0bc7daa48d86d91
File Name:	nlsinfo.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	c08e85c3211d9e2464fe06b5fa43a061
File Name:	now.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	33932780cce43286f97e3bf93c74c994

Files which were modified on the File System with the corresponding MD5SUM and Path - Count: 144

File Name:	ntimer.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	a1aae9b6ea89c7d595c882ebf6408fd0
File Name:	ntrights.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	adbf48b7fa206cdf37ad799fe4ca2074
File Name:	oh.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	bb3075c9d8ad3b8dae378cad561f7bc7
File Name:	oleview.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	0b8c7aabf9b0ea9b7672c7ae502e9e81
File Name:	pathman.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	acfa343ff9eb8eae2ef83e49720ad283
File Name:	permcoppy.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	7af672a35304c00f4b0b6a1f7f1c8f84
File Name:	perms.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	c3f45ef7b7d5a31c2e18a541ea7b3598
File Name:	pfmon.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	6ad80e023002398518e859e45b92114a
File Name:	pmon.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	2194ae2d8090761dc4a3f27c3af023b2
File Name:	remapkey.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	2cfb7c792883509525cd4e0ff2b188d5
File Name:	reportgen.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	5b03db7dd53e8718c5c46f6aa5852544
File Name:	robocopy.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	ac29a767c1e047fd581be8c04262474c
File Name:	rpccfg.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	87c1f4f7a23d2b72e2f7d15f0095bd3e
File Name:	rpccdump.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	d4598b75a4928c6752abb92bc7245dd2

Files which were modified on the File System with the corresponding MD5SUM and Path - Count: 144

File Name:	rpping.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	6e2de59325b9e3b545d16a02c1f76896
File Name:	rpingc.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	18f1773bcd1c52f5a4416ebc47d8aa5f
File Name:	rpings.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	d7f8b7aae7e728c8c95c88164b38d1a2
File Name:	rqc.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	26f34da1762ac2db210d28edf5d06fbc
File Name:	rqs.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	1ed172b277e3d70883957e75af9b6422
File Name:	setprinter.exe
File Path:	Program Files/Windows Resource Kits/Tools
MD5 Hash:	317e7367c46e1692b3e2ea2adc9ad480
File Name:	AppEvent.Evt
File Path:	WINDOWS/system32/config
MD5 Hash:	7cea37707c737cb955ee015a8562d1c8
File Name:	default
File Path:	WINDOWS/system32/config
MD5 Hash:	2cd9473b424af590b642d2e6eece8cbe
File Name:	SAM
File Path:	WINDOWS/system32/config
MD5 Hash:	b90640f5f62f990395c22a7dfc3cf5c0
File Name:	SECURITY
File Path:	WINDOWS/system32/config
MD5 Hash:	afb5a4e235a963a24b674b1790734cb1
File Name:	software
File Path:	WINDOWS/system32/config
MD5 Hash:	f7b28fee7476b60b08d10fb3bca6e5ef
File Name:	SysEvent.Evt
File Path:	WINDOWS/system32/config
MD5 Hash:	e2f9a27d341f8044af9fd9d8d1f24503
File Name:	system
File Path:	WINDOWS/system32/config
MD5 Hash:	da9e5fc613ab64bb07bdd2214fcde362
File Name:	Preferred
File Path:	WINDOWS/system32/Microsoft/Protect/S-1-5-18/User
MD5 Hash:	8518ce7ca92a1aef6df1e50ccfc62c80

Files which were modified on the File System with the corresponding MD5SUM and Path - Count: 144

File Name: wbemess.io_
 File Path: WINDOWS/system32/wbem/Logs
 MD5 Hash: 20e5cdc44b6ff3471cd05bab398c74e3

Potentially Malicious Files which were downloaded from the Internet - Count: 5

[Back To Top](#)

File Name: dlgt.txt
 File Path: sysdl
 MD5 Hash: 904dae96fd1838174357de4db68efab2
 SSDeep Hash: 192:GIUTPrjCy+6IVoWN6tGRA6Z9urHR2Ib2toukNK376EOBGC9DQmIHufmpslcgal8:GIUTPr7R+6IKWN6tGRA6Z9urHRb2quV

File Name: dlz.txt
 File Path: sysdl
 MD5 Hash: f902ffb6653fb742c7e8919e4e5da22c
 SSDeep Hash: 192:GIUTPrjCy+6IVoWN6tGRA6Z9urHRXlB2toukNK376EOBGC9DQmIHufmpslcgal2:GIUTPr7R+6IKWN6tGRA6Z9urHRYb2quH

File Name: dlzt.txt
 File Path: sysdl
 MD5 Hash: 4e88e7c293fba032094afe5f45f92798
 SSDeep Hash: 192:GIXTPrjCy+6IVoWN6tGRA6Z9urHRU1no5P01RYnyZMnBuBGC9N3JSr7YU3pslcK:GIXTPr7R+6IKWN6tGRA6Z9urHRQoh01d

File Name: dlms.txt
 File Path: sysdl
 MD5 Hash: 32686539e7a1ada24d00778e983ab751
 SSDeep Hash: 384:GIZTPr7R+6IKWN6tGRA6Z9urHRy70e3+3Xvsiib2/zFubA+nFt2HbD8J+l2zQbJi:GSSNuHUnSLEkIO7DW33Vpgv

File Name: frame.aspx?u=http:%2F%2Fsearchportal.information.com? a_id=1637&domainname=wowchian.com&adultfilter=off&popunder=off&r=2&adi=100
 File Path: frame.aspx?u=http:%2F%2Fsearchportal.information.com? a_id=1637&domainname=wowchian.com&adultfilter=off&popunder=off&r=2&adi=100
 MD5 Hash: 7aba5ae2f84990331dce1f3e14499021
 SSDeep Hash: 12:FMQ9K45gzLOVnqP2GaSEXVXMM0fOrEXqr0+YWn3RIou:6D45qOVqP2bSuB0lv0naSn

New Open Sockets in Memory - Count: 1

[Back To Top](#)

Pid	Port	Proto
4	1029	6

New Connections in Memory - Count: 20

[Back To Top](#)

LocalIpPort	RemoteIpPort	Pid
10.10.10.7:1057	10.10.10.1:139	4
10.10.10.7:1054	10.10.10.1:445	4
10.10.10.7:1056	10.10.10.1:445	4
10.10.10.7:1046	10.10.10.1:445	4
10.10.10.7:1055	10.10.10.1:139	4
10.10.10.7:1057	10.10.10.1:139	4
10.10.10.7:1054	10.10.10.1:445	4
10.10.10.7:1056	10.10.10.1:445	4
10.10.10.7:1046	10.10.10.1:445	4
10.10.10.7:1055	10.10.10.1:139	4
10.10.10.7:1057	10.10.10.1:139	4
10.10.10.7:1054	10.10.10.1:445	4
10.10.10.7:1056	10.10.10.1:445	4
10.10.10.7:1046	10.10.10.1:445	4
10.10.10.7:1055	10.10.10.1:139	4
10.10.10.7:1057	10.10.10.1:139	4
10.10.10.7:1054	10.10.10.1:445	4
10.10.10.7:1056	10.10.10.1:445	4
10.10.10.7:1046	10.10.10.1:445	4
10.10.10.7:1055	10.10.10.1:139	4
10.10.10.7:1057	10.10.10.1:139	4
10.10.10.7:1054	10.10.10.1:445	4
10.10.10.7:1056	10.10.10.1:445	4
10.10.10.7:1046	10.10.10.1:445	4
10.10.10.7:1055	10.10.10.1:139	4

New Opened files which were contained within Memory - Count: 6

[Back To Top](#)

Data

File \AsyncConnectHlp
 File \Documents and Settings\Administrator\Cookies\index.dat
 File \Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Portable Devices
 File \Documents and Settings\Administrator\Local Settings\History\History.IE5\index.dat
 File \Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\index.dat
 File \System Volume Information_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}\RP16\change.log

Strings Command executed on Processes contained within Memory - Count: 5

[Back To Top](#)

Data

true
 CSendMail
 SendMail
 net stop "Kingssoft AntiVirus Service"
 |rdr|\plug_ins\sendmail.api

Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 9

[Back To Top](#)

Data

www.wowchian.com/sysdl/dfz.txt
www.wowchian.com/sysdl/dlgt.txt
www.wowchian.com/sysdl/dlms.txt
www.wowchian.com/sysdl/dlzt.txt
www.wowchian.com
/sysdl/dfz.txt
/sysdl/dlgt.txt
/sysdl/dlms.txt
/sysdl/dlzt.txt

Malicious SMB Traffic - Count: 216

[Back To Top](#)

Data

Connection from 10.10.10.7
4 bytes received
00 00 00 85
Netbios Session packet detected
Processing netbios packet with length 133
133 bytes received
ff 53 4d 42 72 00 00 00 00 18 53 c8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 ff fe 00 00 00 00 00 62 00 02 50 43 20 4e 45 54 57 4f 52 4b 20 50
52 4f 47 52 41 4d 20 31 2e 30 00 02 4c 41 4e 4d 41 4e 31 2e 30 00 02 57
69 6e 64 6f 77 73 20 66 6f 72 20 57 6f 72 6b 67 72 6f 75 70 73 20 33 2e
31 61 00 02 4c 4d 31 2e 32 58 30 30 32 00 02 4c 41 4e 4d 41 4e 32 2e 31
00 02 4e 54 20 4c 4d 20 30 2e 31 32 00
SMB Header detected
SMB Negotiate Protocol Request Detected (0x72)
Possible HOD exploit in progress
Sending SMB session response
4 bytes received
00 00 00 ca
Netbios Session packet detected
Processing netbios packet with length 202
202 bytes received
ff 53 4d 42 73 00 00 00 00 18 07 c8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 ff fe 00 00 40 00 0c ff 00 ca 00 04 41 32 00 00 00 00 00 00 00 00 28
00 00 00 00 00 d4 00 00 a0 8f 00 4e 54 4c 4d 53 53 50 00 01 00 00 00 97
82 08 e2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 05 01 28 0a 00
00 00 0f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 32 00 30 00
30 00 32 00 20 00 53 00 65 00 72 00 76 00 69 00 63 00 65 00 20 00 50 00
61 00 63 00 6b 00 20 00 32 00 20 00 32 00 36 00 30 00 30 00 00 00 57 00
69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 32 00 30 00 30 00 32 00 20 00
35 00 2e 00 31 00 00 00 00 00
SMB Header detected
SMB Session Setup AndX Request Detected (0x73)
NTLMSSP_NEGOTIATE message detected
Sending SMB session response
Connection timed out
Connection from 10.10.10.7
4 bytes received
00 00 00 85
Netbios Session packet detected
Processing netbios packet with length 133

Malicious SMB Traffic - Count: 216

[Back To Top](#)

133 bytes received
ff 53 4d 42 72 00 00 00 00 18 53 c8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 ff fe 00 00 00 00 00 62 00 02 50 43 20 4e 45 54 57 4f 52 4b 20 50
52 4f 47 52 41 4d 20 31 2e 30 00 02 4c 41 4e 4d 41 4e 31 2e 30 00 02 57
69 6e 64 6f 77 73 20 66 6f 72 20 57 6f 72 6b 67 72 6f 75 70 73 20 33 2e
31 61 00 02 4c 4d 31 2e 32 58 30 30 32 00 02 4c 41 4e 4d 41 4e 32 2e 31
00 02 4e 54 20 4c 4d 20 30 2e 31 32 00

SMB Header detected
SMB Negotiate Protocol Request Detected (0x72)

Possible HOD exploit in progress
Sending SMB session response

4 bytes received
00 00 00 ca

Netbios Session packet detected
Processing netbios packet with length 202

202 bytes received
ff 53 4d 42 73 00 00 00 00 18 07 c8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 ff fe 00 00 40 00 0c ff 00 ca 00 04 41 32 00 00 00 00 00 00 00 00 00 28
00 00 00 00 00 d4 00 00 a0 8f 00 4e 54 4c 4d 53 53 50 00 01 00 00 00 97
82 08 e2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 05 01 28 0a 00
00 00 0f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 32 00 30 00
30 00 32 00 20 00 53 00 65 00 72 00 76 00 69 00 63 00 65 00 20 00 50 00
61 00 63 00 6b 00 20 00 32 00 20 00 32 00 36 00 30 00 30 00 00 00 57 00
69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 32 00 30 00 30 00 32 00 20 00
35 00 2e 00 31 00 00 00 00 00

SMB Header detected
SMB Session Setup AndX Request Detected (0x73)

NLMSSP_NEGOTIATE message detected
Sending SMB session response

Connection timed out
Connection from 10.10.10.7

4 bytes received
00 00 00 85

Netbios Session packet detected
Processing netbios packet with length 133

133 bytes received
ff 53 4d 42 72 00 00 00 00 18 53 c8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 ff fe 00 00 00 00 00 62 00 02 50 43 20 4e 45 54 57 4f 52 4b 20 50
52 4f 47 52 41 4d 20 31 2e 30 00 02 4c 41 4e 4d 41 4e 31 2e 30 00 02 57
69 6e 64 6f 77 73 20 66 6f 72 20 57 6f 72 6b 67 72 6f 75 70 73 20 33 2e
31 61 00 02 4c 4d 31 2e 32 58 30 30 32 00 02 4c 41 4e 4d 41 4e 32 2e 31
00 02 4e 54 20 4c 4d 20 30 2e 31 32 00

SMB Header detected
SMB Negotiate Protocol Request Detected (0x72)

Possible HOD exploit in progress
Sending SMB session response

4 bytes received
00 00 00 ca

Netbios Session packet detected
Processing netbios packet with length 202

202 bytes received
ff 53 4d 42 73 00 00 00 00 18 07 c8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 ff fe 00 00 40 00 0c ff 00 ca 00 04 41 32 00 00 00 00 00 00 00 00 00 28
00 00 00 00 00 d4 00 00 a0 8f 00 4e 54 4c 4d 53 53 50 00 01 00 00 00 97
82 08 e2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 05 01 28 0a 00
00 00 0f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 32 00 30 00

Malicious SMB Traffic - Count: 216

[Back To Top](#)

30 00 32 00 20 00 53 00 65 00 72 00 76 00 69 00 63 00 65 00 20 00 50 00
61 00 63 00 6b 00 20 00 32 00 20 00 32 00 36 00 30 00 30 00 00 00 57 00
69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 32 00 30 00 30 00 32 00 20 00
35 00 2e 00 31 00 00 00 00 00

SMB Header detected

SMB Session Setup AndX Request Detected (0x73)

NTLMSSP_NEGOTIATE message detected

Sending SMB session response

Connection timed out

Connection from 10.10.10.7

4 bytes received

00 00 00 85

Netbios Session packet detected

Processing netbios packet with length 133

133 bytes received

ff 53 4d 42 72 00 00 00 00 18 53 c8 00 00 00 00 00 00 00 00 00 00 00 00
00 00 ff fe 00 00 00 00 00 62 00 02 50 43 20 4e 45 54 57 4f 52 4b 20 50
52 4f 47 52 41 4d 20 31 2e 30 00 02 4c 41 4e 4d 41 4e 31 2e 30 00 02 57
69 6e 64 6f 77 73 20 66 6f 72 20 57 6f 72 6b 67 72 6f 75 70 73 20 33 2e
31 61 00 02 4c 4d 31 2e 32 58 30 30 32 00 02 4c 41 4e 4d 41 4e 32 2e 31
00 02 4e 54 20 4c 4d 20 30 2e 31 32 00

SMB Header detected

SMB Negotiate Protocol Request Detected (0x72)

Possible HOD exploit in progress

Sending SMB session response

4 bytes received

00 00 00 ca

Netbios Session packet detected

Processing netbios packet with length 202

202 bytes received

ff 53 4d 42 73 00 00 00 00 18 07 c8 00 00 00 00 00 00 00 00 00 00 00 00
00 00 ff fe 00 00 40 00 0c ff 00 ca 00 04 41 32 00 00 00 00 00 00 00 00 28
00 00 00 00 00 d4 00 00 a0 8f 00 4e 54 4c 4d 53 53 50 00 01 00 00 00 97
82 08 e2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 05 01 28 0a 00
00 00 0f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 32 00 30 00
30 00 32 00 20 00 53 00 65 00 72 00 76 00 69 00 63 00 65 00 20 00 50 00
61 00 63 00 6b 00 20 00 32 00 20 00 32 00 36 00 30 00 30 00 00 00 57 00
69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 32 00 30 00 30 00 32 00 20 00
35 00 2e 00 31 00 00 00 00 00

SMB Header detected

SMB Session Setup AndX Request Detected (0x73)

NTLMSSP_NEGOTIATE message detected

Sending SMB session response

Connection timed out

Connection from 10.10.10.7

4 bytes received

00 00 00 85

Netbios Session packet detected

Processing netbios packet with length 133

133 bytes received

ff 53 4d 42 72 00 00 00 00 18 53 c8 00 00 00 00 00 00 00 00 00 00 00 00
00 00 ff fe 00 00 00 00 00 62 00 02 50 43 20 4e 45 54 57 4f 52 4b 20 50
52 4f 47 52 41 4d 20 31 2e 30 00 02 4c 41 4e 4d 41 4e 31 2e 30 00 02 57
69 6e 64 6f 77 73 20 66 6f 72 20 57 6f 72 6b 67 72 6f 75 70 73 20 33 2e
31 61 00 02 4c 4d 31 2e 32 58 30 30 32 00 02 4c 41 4e 4d 41 4e 32 2e 31
00 02 4e 54 20 4c 4d 20 30 2e 31 32 00

Malicious SMB Traffic - Count: 216

[Back To Top](#)

Connection timed out

Potentially Malicious Changes in System Registry File - Count: 2

[Back To Top](#)

Data

[system\ControlSet001\Services\Eventlog\Application\Microsoft H.323 Telephony Service Provider]
"EventMessageFile"="C:\\WINDOWS\\System32\\h323.tsp"

Potentially Malicious Changes in Software Registry File - Count: 36

[Back To Top](#)

Data

@="hpqdst Document"
@="ole32.dll"
@="C:\\WINDOWS\\system32\\d3445d70f7016f477bd7b7cc36a82bf8"
@="hpqdstcp.Document"
[software\\Classes\\hpqdstcp.Document]
@="hpqdst Document"
[software\\Classes\\hpqdstcp.Document\\CLSID]
@="IDualUSDs"
"Version"="1.0"
@="IDualDestComp"
"Version"="1.0"
@="IDualDestConfig2"
"Version"="1.0"
@="IDualUSD2"
"Version"="1.0"
@="IDualDestConfig"
"Version"="1.0"
@="IUSD"
"Version"="1.0"
@="IDestConfig"
"Version"="1.0"
@="IDualUSD"
"Version"="1.0"
@="IDestComp"
"Version"="1.0"
@="IUSDs"
"Version"="1.0"
@="Hewlett-Packard CUE Destination Objects 1.0"
@="C:\\WINDOWS\\system32\\d3445d70f7016f477bd7b7cc36a82bf8"
@="0"
@=""
[software\\Microsoft\\DownloadManager]
"load"="C:\\WINDOWS\\uninstall\\rundl132.exe"
[software\\Soft]
[software\\Soft\\DownloadWWW]
"auto"="1"

Potentially Malicious Changes in NTUSER.DAT File - Count: 4

[Back To Top](#)

Data

```
[NTUSER\Software\Local AppWizard-Generated Applications]
[NTUSER\Software\Local AppWizard-Generated Applications\DestComp]
[NTUSER\Software\Local AppWizard-Generated Applications\DestComp\Settings]
"load"="C:\WINDOWS\rundl132.exe"
```

This is an automated report provided free of charge, it was generated in part by a custom script and utilizes the following tools: the Reusable Malware Analysis Net (Truman*) server, Norton Anti-Virus, Malwarebytes Anti-malware*, Sysinternals Tools, Ngrep, Tcpdump, Sed Editor, Awk, Volatile Systems Volatility Framework, SSdeep, MD5sum, MS Office and Adobe Acrobat . If you would like a full forensic examination that would tell you more about how the malware was placed on the system and if additional malicious applications are still there please contact us. In some cases we can determine if data was exfiltrated, but data from your other network devices is sometimes necessary. (example: firewalls and IDS)

* TRUMAN: Authored by Mr. Joe Stewart under the General Public License.

* VirusTotal is a service developed by Hispasec Sistemas that analyzes suspicious files and URLs enabling the identification of viruses, worms, trojans and other kinds of malicious content detected by antivirus engines and web analysis toolbars.

* Ngrep: Authored by Jordan Ritter Norton Anti Virus: Product of Symantec Corp.

* Malwarebytes Anti-Malware, Product fo Malwarebytes Corporation Windows Sysinterals Tools, Sysinternals was created in 1996 by Mark Russinovich and Bryce Cogswell to host their advanced system utilities and technical information. Microsoft acquired Sysinternals in July, 2006

* Virus Total checks multiple AV products, here is a list of all the AV applications and versions they are currently using. If our report does not show an AV application above, it did not hit on the binary submitted.