

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: **cvert.exe**

MD5 Hash: **fa42f8951b666352c1880aeb30c95df4**

SSDeep Hash: **6144:TmU2Ap/D2grP/Y9xBZa7B8shM3WRZ1ZSTdUHn:CU31rP/u+CseGRZ+ZST6**

File Description: **PE32 executable for MS Windows (GUI) Intel 80386 32-bit, Mono/.Net assembly**

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	YES	NO	NO	NO	NO	NO	YES

**** The following files are Malicious files associated with the cvert.exe, Download at your own Risk ****

- Apache.tar
- CreatedFiles.tar
- MBR.img
- ModifiedFiles.tar
- sandnet.pcap

FTP Link: <ftp://anonymous@68.15.186.23/fa42f8951b666352c1880aeb30c95df4/>

Anti-Virus Tool	Result
nProtect	Trojan/W32.Jorik.258048.C
McAfee	Artemis!FA42F8951B66
NOD32	Win32/Vnfraye.A
Symantec	Trojan Horse
Kaspersky	Trojan.Win32.Jorik.Vernet.id
BitDefender	Gen:Variant.Buzy.4059
Emsisoft	Win32.SuspectCrc!IK
Comodo	TrojWare.Win32.JorikVernet.ID
F-Secure	Gen:Variant.Buzy.4059
DrWeb	Trojan.Siggen3.10279
VIPRE	Trojan.Win32.Generic!BT
AntiVir	TR/Buzy.4059
McAfee-GW-Edition	Artemis!FA42F8951B66
Sophos	Troj/Buzy-A
Jiangmin	TrojanDropper.MSIL.gyf
Microsoft	Trojan:Win32/Dusvext.B
GData	Gen:Variant.Buzy.4059
AhnLab-V3	Trojan/Win32.Jorik
Ikarus	Win32.SuspectCrc
AVG	Dropper.Generic_c.LFE
Panda	Trj/CI.A

VirusTotal link for: [fa42f8951b666352c1880aeb30c95df4](https://www.virustotal.com/#/file-urls/analyze?url=fa42f8951b666352c1880aeb30c95df4)

File Name: winkept.exe
 File Path: Documents and Settings/Administrator/Application Data
 MD5 Hash: 3d7d2e825c63ff501e896cf008c70d75
 SSDeep Hash: 1536:AbFzR3Xtd5+QVwfD56ac4N1RG4ELxWHZMQTcGziDwW8XZ1S:Ab3PWTcCRGHVcMrFDwW8XZ1S

File Name: iexplorer.exe
 File Path: Documents and Settings/Administrator/Local Settings/Temp
 MD5 Hash: 3d7d2e825c63ff501e896cf008c70d75
 SSDeep Hash: 1536:AbFzR3Xtd5+QVwfD56ac4N1RG4ELxWHZMQTcGziDwW8XZ1S:Ab3PWTcCRGHVcMrFDwW8XZ1S

File Name: jProtect.exe
 File Path: Documents and Settings/Administrator/Local Settings/Temp
 MD5 Hash: fa42f8951b666352c1880aeb30c95df4
 SSDeep Hash: 6144:TmU2Ap/D2grP/Y9xBZa7B8shM3WRZ11ZSTdUHn:CU31rP/u+CseGRZ+ZST6

File Name: oQulNsUBP.exe
 File Path: Documents and Settings/Administrator/Local Settings/Temp
 MD5 Hash: 5a3867587244ddf3ed51cc4cba5af272
 SSDeep Hash: 96:OLVnA8eujChkMqCweQVwK2yMoUtCd5cE2xYInIYJnLLPL0KffvL/zz8LbRv1r5Rh:OLZE6OVwe9Zj4OV0nIYJLLLTzGnxH

File Name: cvert.exe
 File Path: Temp
 MD5 Hash: fa42f8951b666352c1880aeb30c95df4
 SSDeep Hash: 6144:TmU2Ap/D2grP/Y9xBZa7B8shM3WRZ11ZSTdUHn:CU31rP/u+CseGRZ+ZST6

Created Files Verified as Malicious - Count: 2

[Back To Top](#)

This output is generated from hashes corresponding with the files created on the operating system, being submitted to the website <http://www.team-cymru.org> for analysis, as to whether they are known bad binaries.

Md5 Hash	Date Submitted to Cymru.org	Detection %(Likelihood file is malicious)
fa42f8951b666352c1880aeb30c95df4	1316856662	23
fa42f8951b666352c1880aeb30c95df4	1316856662	23

Files which were modified on the File System with the corresponding MD5SUM and Path - Count: 12

File Name: NTUSER.DAT
 File Path: Documents and Settings/Administrator
 MD5 Hash: 60879a8d72b67a2501edf96d475b0a3f

File Name: NTUSER.DAT
 File Path: Documents and Settings/LocalService
 MD5 Hash: 8d6e342d2abdd497392a3849d948ed07

File Name: NTUSER.DAT
 File Path: Documents and Settings/NetworkService
 MD5 Hash: af9efe9dab858669f20f4590c6c7c466

File Name: AppEvent.Evt
 File Path: WINDOWS/system32/config
 MD5 Hash: 8ef02bb898515951320a1994e49a37de

File Name: default
 File Path: WINDOWS/system32/config
 MD5 Hash: f19bb21227f734256b21c8fc2074e6ab

Files which were modified on the File System with the corresponding MD5SUM and Path - Count: 12

File Name:	SAM
File Path:	WINDOWS/system32/config
MD5 Hash:	4cbd1dc2bd0d2375a977f132e074009f
File Name:	SECURITY
File Path:	WINDOWS/system32/config
MD5 Hash:	7e4ad93623a7bc4f442f961a1fa8d282
File Name:	software
File Path:	WINDOWS/system32/config
MD5 Hash:	0b1715adeb9c890256162726bc9ffe8d
File Name:	SysEvent.Evt
File Path:	WINDOWS/system32/config
MD5 Hash:	94f51662c0f0aea48f1e17721f042000
File Name:	system
File Path:	WINDOWS/system32/config
MD5 Hash:	c51bfd419fd22fed725c15551546ab6a
File Name:	Preferred
File Path:	WINDOWS/system32/Microsoft/Protect/S-1-5-18/User
MD5 Hash:	f7086bf5075fce82eec92909cb8218ac
File Name:	ngen_service.log
File Path:	WINDOWS/Microsoft.NET/Framework/v2.0.50727
MD5 Hash:	4b5e8a92b9edec47eb0de6351010fb82

Alternate Data Streams which were created on the File System - Count: 2

[Back To Top](#)

Data
 /Documents and Settings\Administrator\Local Settings\Temp\oQuiNsUBP.exe:
 ZONE.identifier: Alternate Data Stream Size in KB 27

Potentially Malicious Files which were downloaded from the Internet - Count: 2

[Back To Top](#)

File Name:	tasks.php?uid={18ab1ac0-200b-11df-aa92-806d6172696f-534043512}
File Path:	legendsfoo
MD5 Hash:	d41d8cd98f00b204e9800998ecf8427e
SSDeep Hash:	3::
File Name:	index.html
File Path:	index.html
MD5 Hash:	2bfdb0405fff4e83036f397d2be4b01e
SSDeep Hash:	384:UtE43HAmAPx/TLdG182wwWkJkVGI/aV88u9L+Tdfha4L:U3HYpXLLDg182wwWkJkVGIIB9L+RfhPL

New Open and/or Listening Ports (MPORT) - Count: 1

[Back To Top](#)

Protocol	LocalIpPort	RemoteIpPort	Service	Status
10.10.10.7:1045	TCP	4.3.2.196:80	CLOSE_WAIT	iexplorer.exe:3416

New Open Sockets in Memory - Count: 1

[Back To Top](#)

Pid	Port	Proto
3416	1046	6

New Processes in Memory - Count: 1

[Back To Top](#)

Pid	PPid	Name
3416	3400	iexplorer.exe

New Connections in Memory - Count: 19

[Back To Top](#)

LocalIpPort	RemoteIpPort	Pid
10.10.10.7:1041	4.3.2.196:80	3416
10.10.10.7:1039	4.3.2.196:80	3416
10.10.10.7:1038	4.3.2.196:80	3416
10.10.10.7:1046	4.3.2.196:80	3416
10.10.10.7:1040	4.3.2.196:80	3416
10.10.10.7:1041	4.3.2.196:80	3416
10.10.10.7:1046	4.3.2.196:80	3416
10.10.10.7:1039	4.3.2.196:80	3416
10.10.10.7:1038	4.3.2.196:80	3416
10.10.10.7:1041	4.3.2.196:80	3416
10.10.10.7:1040	4.3.2.196:80	3416
10.10.10.7:1046	4.3.2.196:80	3416
10.10.10.7:1039	4.3.2.196:80	3416
10.10.10.7:1038	4.3.2.196:80	3416
10.10.10.7:1041	4.3.2.196:80	3416
10.10.10.7:1046	4.3.2.196:80	3416
10.10.10.7:1040	4.3.2.196:80	3416
10.10.10.7:1046	4.3.2.196:80	3416
10.10.10.7:1046	4.3.2.196:80	3416

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

[Back To Top](#)

Data
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}\RP19\change.log
File \WINDOWS\Temp\Perflib_Perfdata_77c.dat

Strings Command executed on Processes contained within Memory - Count: 2

[Back To Top](#)

Data

http://
https://

Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 6

[Back To Top](#)

Data

/legendsfoo/tasks.php?uid={18ab1ac0-200b-11df-aa92-806d6172696f-534043512}www.tinyschats.com
www.tinyschats.com/legendsfoo/tasks.php?uid={18ab1ac0-200b-11df-aa92-806d6172696f-534043512}
www.tinyschats.comwww.tinyschats.com
www.tinyschats.com
/legendsfoo/adduser.php?uid={18ab1ac0-200b-11df-aa92-806d6172696f-53404
/legendsfoo/tasks.php?uid={18ab1ac0-200b-11df-aa92-806d6172696f-5340435

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

[Back To Top](#)

Data

[NTUSER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run]
"nvsc32"="C:\\Documents and Settings\\Administrator\\Local Settings\\Temp\\oQuINsUBP.exe"
"jProtector"="C:\\Documents and Settings\\Administrator\\Application Data\\winkept.exe"
"C:\\Documents and Settings\\Administrator\\Local Settings\\Temp\\oQuINsUBP.exe"=" "

If you are interested in your own Sandbox, contact our sales staff @ 1-(888) 256-7425 | Email: sales@netscty.com

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
- 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)

Credits:

- 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 of Malwarebytes Corporation Windows Sysinternals 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.