

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: **1e3cb1375219b95ad3b55418b214297f.exe**

MD5 Hash: **1e3cb1375219b95ad3b55418b214297f**

SSDeep Hash: **384:arOF+qpy8YDPOfZ1xasRPOqPGe8PT2WNYOA/AVwwxOIhEtkaiY2DTsOFK/:jF+1ZDbsRPrIGOA/bEF4kaxEzFK/**

File Description: **PE32 executable for MS Windows (GUI) Intel 80386 32-bit**

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	SSL
YES	NO	NO	YES	NO	NO	YES	YES	NO	NO	YES	NO	NO	NO

**** The following files are Malicious files associated with the 1e3cb1375219b95ad3b55418b214297f.exe, Download at your own Risk ****

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

FTP Link: <ftp://anonymous@68.15.186.23/1e3cb1375219b95ad3b55418b214297f/>

Files created on the File System - Count: 4

[Back To Top](#)

File Name:	codec.exe.exe
File Path:	Documents and Settings/Administrator/Application Data
MD5 Hash:	1e3cb1375219b95ad3b55418b214297f
SSDeep Hash:	384:arOF+qpy8YDPOfZ1xasRPOqPGe8PT2WNYOA/AVwwxOIhEtkaiY2DTsOFK/:jF+1ZDbsRPrIGOA/bEF4kaxEzFK/
File Name:	~DF16EF.tmp
File Path:	Documents and Settings/Administrator/Local Settings/Temp
MD5 Hash:	27e24ad19cd0a08fb75d6fd8c2f3a877
SSDeep Hash:	48:r+ry5PnUpB/S1cYzr66NiTTTTTTTTTTTTTTTTTTT:qQ/9W60TTTTTTTTTTTTTTTTTTT
File Name:	1e3cb1375219b95ad3b55418b214297f.exe
File Path:	Temp
MD5 Hash:	1e3cb1375219b95ad3b55418b214297f
SSDeep Hash:	384:arOF+qpy8YDPOfZ1xasRPOqPGe8PT2WNYOA/AVwwxOIhEtkaiY2DTsOFK/:jF+1ZDbsRPrIGOA/bEF4kaxEzFK/
File Name:	BADKARMA.txt
File Path:	WINDOWS
MD5 Hash:	57767a4f3a1f8d10b8cbb57ccba57368
SSDeep Hash:	6:4uPcCKIB8XV6a4qQhQKpZj1g5aGoBK9BD0MRzshF484aENr+yNFp2LKCikQvMt1n:4WwIBG8NhfpZxAckPD1RO48DGNXV2gMD

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)
1e3cb1375219b95ad3b55418b214297f	1265394662	71
1e3cb1375219b95ad3b55418b214297f	1265394662	71

Files which were modified on the File System with the corresponding MD5SUM and Path - Count: 13

File Name: jusched.log
 File Path: Documents and Settings/Administrator/Local Settings/Temp
 MD5 Hash: 174edf7f2a6675f5ee776e5bdb07dc29

File Name: NTUSER.DAT
 File Path: Documents and Settings/Administrator
 MD5 Hash: 81e84e276ef9ad264d7c227d255d4018

File Name: NTUSER.DAT
 File Path: Documents and Settings/LocalService
 MD5 Hash: ff1615488221375823d4781211f51abd

File Name: NTUSER.DAT
 File Path: Documents and Settings/NetworkService
 MD5 Hash: 8f2eec89e6fc191bd2a9ad2f96b2fcfe

File Name: AppEvent.Evt
 File Path: WINDOWS/system32/config
 MD5 Hash: b685755338f53f871f757604defc9cbe

File Name: default
 File Path: WINDOWS/system32/config
 MD5 Hash: 67de4ea572024b1aa4fc014bd6ba7f4

File Name: SAM
 File Path: WINDOWS/system32/config
 MD5 Hash: 653672871c0c7b585e6b5f5e19fbd82e

File Name: SECURITY
 File Path: WINDOWS/system32/config
 MD5 Hash: 7e8050e4a209dbad429656a02ef07de3

File Name: software
 File Path: WINDOWS/system32/config
 MD5 Hash: 39b6f428121dc198bce6286ed5267042

File Name: SysEvent.Evt
 File Path: WINDOWS/system32/config
 MD5 Hash: 19f62bab86fe9d25f274700eebdd840

File Name: system
 File Path: WINDOWS/system32/config
 MD5 Hash: 76ae234ac04770be887fd0c7edfc458d

Files which were modified on the File System with the corresponding MD5SUM and Path - Count: 13

File Name:	Preferred
File Path:	WINDOWS/system32/Microsoft/Protect/S-1-5-18/User
MD5 Hash:	623b2e47e70db8137dde062ae5296a65
File Name:	ngen_service.log
File Path:	WINDOWS/Microsoft.NET/Framework/v2.0.50727
MD5 Hash:	a1b4956caf89c544974bcfb18deedbff

New Open and/or Listening Ports (MPORT) - Count: 2

Note: all 4.3.2.x IP addresses in this report belong to our sandbox [Back To Top](#)

Local IP Address: Port	Protocol	Remote IP Address: Port	Service	Status
0.0.0.0:1042	TCP	0.0.0.0:55306	LISTENING	1e3cb1375219b95ad3b55418b214297f.exe:3120
10.10.10.7:1040	TCP	4.3.2.251:21	ESTABLISHED	1e3cb1375219b95ad3b55418b214297f.exe:3120

New Open Sockets in Memory - Count: 2

[Back To Top](#)

Pid	Port	Proto
3120	1042	6
3120	1040	6

New Processes in Memory - Count: 1

[Back To Top](#)

Pid	PPid	Name
3120	3112	1e3cb1375219b95ad3b55418b214297f.exe

New Connections in Memory - Count: 1

Note: all 4.3.2.x IP addresses in this report belong to our sandbox [Back To Top](#)

Local IP: Port	Remote IP: Port	Pid
10.10.10.7:1040	4.3.2.251:21	3120

New Opened files which were contained within Memory - Count: 1

[Back To Top](#)

Data
Binary file /forensics/OutPut/1e3cb1375219b95ad3b55418b214297f--1e3cb1375219b95ad3b55418b214297f.exe-files/memopenfiles.ls matches

Strings Command executed on Processes contained within Memory - Count: 10

[Back To Top](#)

Data

FtpCreateDirectoryA
FtpDeleteFileA
FtpFindFirstFileA
FtpGetCurrentDirectoryA
FtpGetFileA
FtpPutFileA
FtpRemoveDirectoryA
FtpRenameFileA
FtpSetCurrentDirectoryA
mEmail

Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 2

[Back To Top](#)

Data

freetzi.com
smtp.live.com

Malicious FTP Traffic - Count: 16

[Back To Top](#)

Data

Connection from 10.10.10.7
USER foro-red-anime.coolpage.biz
PASS jumpers123
TYPE I
PASV
TYPE I
PORT 10,10,10,7,4,18
STOR BADKARMA - 1:29:53 AM.txt
Connection from 10.10.10.7
USER foro-red-anime.coolpage.biz
PASS jumpers123
TYPE I
PASV
TYPE I
PORT 10,10,10,7,4,22
STOR BADKARMA - 1:35:01 AM.txt

Malicious SMTP Traffic - Count: 2

[Back To Top](#)

Data

Connection from 10.10.10.7
EHLO badkarma

Potentially Malicious Changes in System Registry File - Count: 1

[Back To Top](#)

Data

"C:\\Temp\\1e3cb1375219b95ad3b55418b214297f.exe"="C:\\Temp\\1e3cb1375219b95ad3b55418b214297f.exe*:Enabled:svchost"

Potentially Malicious Changes in Software Registry File - Count: 3

[Back To Top](#)

Data

"ScheduleId"="S-1-5-21-448539723-2000478354-725345543"

[software\\Microsoft\\Tracing\\FWCFG]

"codec.exe"="C:\\Documents and Settings\\Administrator\\Application Data\\codec.exe.exe"

Potentially Malicious Changes in NTUSER.DAT File - Count: 6

[Back To Top](#)

Data

[NTUSER\\Software\\JavaSoft\\Java Update\\Policy\\JavaFX]

[NTUSER\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\FileExts\\.pl]

[NTUSER\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\FileExts\\.pl\\OpenWithProgids]

"Perl"=hex(0):

[NTUSER\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System]

"codec.exe"="C:\\Documents and Settings\\Administrator\\Application Data\\codec.exe.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.