

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: **a.exe**

MD5 Hash: **12402d59a38b8b84342fadbd202468bd**

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
NO	NO	YES	YES	NO	NO	YES	NO	NO	NO	NO	NO	NO

Anti-Virus Tool	Result
McAfee	Generic VB.b
NOD32	a variant of Win32/Injector.EX
F-Prot	W32/VBTrojan.10!Maximus
a-squared	Riskware.Win32.Vbinder!IK
TrendMicro-HouseCall	WORM_AUTORUN.HBF
ClamAV	Trojan.Inject-3367
BitDefender	Gen:Trojan.Heur.um0@saryOfki
Comodo	Heur.Suspicious
F-Secure	Gen:Trojan.Heur.um0@saryOfki
DrWeb	BackDoor.Poison.686
AntiVir	TR/Dropper.Gen
TrendMicro	WORM_AUTORUN.HBF
McAfee-GW-Edition	Generic VB.b
Sophos	Mal/VB-BL
Authentium	W32/VBTrojan.10!Maximus
Jiangmin	Trojan/Inject.ilo
Antiy-AVL	Trojan/Win32.Inject.gen
Symantec	Trojan Horse
Microsoft	VirTool:Win32/VBInject.gen!AN
ViRobot	Trojan.Win32.Inject.36864.O
GData	Gen:Trojan.Heur.um0@saryOfki
VBA32	Trojan.VB.Motil
Sunbelt	Trojan.Win32.Generic!SB.0
PCTools	Trojan.Generic
Ikarus	VirTool.Win32.Vbinder
AVG	VB.ITP
Panda	Trj/CI.A
Avast5	Win32:Trojan-gen

VirusTotal link for: [12402d59a38b8b84342fadbd202468bd](https://www.virustotal.com/file/12402d59a38b8b84342fadbd202468bd/analysis/)

**Files which were modified on the File System with the corresponding MD5SUM and Path - Count: 11**

File Name: NTUSER.DAT  
 File Path: Documents and Settings/Administrator  
 MD5 Hash: 7cfecff09113082088fe011b42d2750

**Files which were modified on the File System with the corresponding MD5SUM and Path - Count: 11**

File Name:	NTUSER.DAT
File Path:	Documents and Settings/LocalService
MD5 Hash:	6b40c46f9e7b293df5c91e02291b41a6
File Name:	NTUSER.DAT
File Path:	Documents and Settings/NetworkService
MD5 Hash:	d9d9afc7f217a1cc01b406e2c55e1baa
File Name:	AppEvent.Evt
File Path:	WINDOWS/system32/config
MD5 Hash:	00f8fb7d27fb72c26a60b0419980b74f
File Name:	default
File Path:	WINDOWS/system32/config
MD5 Hash:	33088a8817c10bf8e8dca95ebe47e19c
File Name:	SAM
File Path:	WINDOWS/system32/config
MD5 Hash:	63fd2088cc09130d4331bf311f99bb72
File Name:	SECURITY
File Path:	WINDOWS/system32/config
MD5 Hash:	38051907fa4343f4b73616cec2f3a673
File Name:	software
File Path:	WINDOWS/system32/config
MD5 Hash:	d39950214b4b61a9a4e2063a4ae55899
File Name:	SysEvent.Evt
File Path:	WINDOWS/system32/config
MD5 Hash:	1d4dc168541875b404d74980ed2fe01c
File Name:	system
File Path:	WINDOWS/system32/config
MD5 Hash:	2234e4bbc00604bbf635326e06b6db16
File Name:	Preferred
File Path:	WINDOWS/system32/Microsoft/Protect/S-1-5-18/User
MD5 Hash:	6455a3217bdb7c4a3d8ab87204242c8b

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

[Back To Top](#)

Protocol	LocalPort	RemotePort	Service	Status
0.0.0.0:113	TCP	0.0.0.0:2256	LISTENING	a.exe:1016
10.10.10.7:1037	TCP	4.3.2.201:6667	ESTABLISHED	a.exe:1016

**New Open Sockets in Memory - Count: 2**

[Back To Top](#)

Pid	Port	Proto
1016	113	6
1016	1037	6

**New Processes in Memory - Count: 1**

[Back To Top](#)

Pid	PPid	Name
1016	996	a.exe

**New Connections in Memory - Count: 1**

[Back To Top](#)

LocalIpPort	RemotelpPort	Pid
10.10.10.7:1037	4.3.2.201:6667	1016

**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 \EVENTLOG  
 File \System Volume Information\tracking.log

**Strings Command executed on Processes contained within Memory - Count: 21**

[Back To Top](#)

**Data**

true  
 NetShareAdd  
 NetShareDel  
 NetShareEnum  
 [01-25-2019 00:12:03] [MAIN]: Connected to deathshadowz.no-ip.org.  
 [SOCKS4]: Error: Failed to connect to target, returned: <%d>.  
 [TFTP]  
 [TFTP]: Already running.  
 [TFTP]: Error: socket() failed, returned: <%d>.  
 [TFTP]: Failed to start server thread, error: <%d>.  
 [TFTP]: Failed to start server, error: <%d>.  
 [VISIT]: Failed to connect to HTTP server.  
 deathshadowz.no-ip.org  
 email  
 ftp.exe  
 hadowz.no-ip.org.  
 mail  
 ftp.exe -i get  
 tftpserver  
 tftpstop  
 |rdrr|\plug\_ins\sendmail.api

### Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 1

[Back To Top](#)

#### Data

deathshadowz.no-ip.org

### Malicious BotNet Traffic - Count: 7

[Back To Top](#)

#### Data

Connection from 10.10.10.7  
PASS server1  
NICK n-174700  
USER voxacsi 0 0 :n-174700  
USERHOST n-174700  
ODE n-174700 -x+B  
JOIN #LASER server1

### Potentially Malicious Changes in System Registry File - Count: 11

[Back To Top](#)

#### Data

```
[system\ControlSet001\Services\Eventlog\Application\Microsoft H.323 Telephony Service Provider]
"EventMessageFile"="C:\\WINDOWS\\System32\\h323.tsp"
"DhcpNameServer"="10.10.10.1"
"DhcpDomain"="company.com"
"DhcpSubnetMask"="255.255.255.0"
"DhcpServer"="10.10.10.1"
"IPAutoconfigurationAddress"="0.0.0.0"
"DhcpNameServer"="10.10.10.1"
"DhcpDomain"="company.com"
"DhcpSubnetMask"="255.255.255.0"
"DhcpServer"="10.10.10.1"
```

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 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.