

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: **487f7ced5d59d89e21578190a146459d**

MD5 Hash: **487f7ced5d59d89e21578190a146459d**

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	NO	YES	YES	YES	NO	NO	NO	NO	NO

Files created on the File System - Count: 10

[Back To Top](#)

File Name:	index.dat
File Path:	Documents and Settings/Administrator/Local Settings/History/History.IE5/MSHist012008090920080910
MD5 Hash:	e7654a70f6e720f73270d6533289c017
SSDeep Hash:	6:qjyxXKdSG17v3skc/FB1NEeF1XnOqjhqQ6Wv3skTlxFB1NEeF1X4U:qjRr1bwhdhJda8vDhd
File Name:	Incom_.jpg.lnk
File Path:	Documents and Settings/Administrator/Recent
MD5 Hash:	3fa5cf325273c54112622bbe0751fdc7
SSDeep Hash:	12:8m2eHnPsoQ5ECBiYrNBPIBalbHjAwOw2ef8ber420wMS5rZIMS5ru:8mQEVgGIPAB5ef8bel0lBU
File Name:	system32.lnk
File Path:	Documents and Settings/Administrator/Recent
MD5 Hash:	76708ce9ebacdcd189cb3516fe5486f7
SSDeep Hash:	12:8TScN8oQ5ECBiYrWjAeU2er420wMRrZIMRru:8TWEV/Ae9eI0jK8
File Name:	kt32.atm
File Path:	WINDOWS
MD5 Hash:	9a4d7e30e1780a7806b9547f7f822c4a
SSDeep Hash:	24:hWtseeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeY:hWT
File Name:	services.exe
File Path:	WINDOWS
MD5 Hash:	e20e5add430f5001486389beee4bb1b
SSDeep Hash:	6144:mRqmp+amNOGokzLyM9tsLaitQo6tzOKkzlt8gKyfjxR9D2j4ynjD:WqmpplpGoGL3etQoMiXM8gxf/Sj4ynjD
File Name:	sservice.exe
File Path:	WINDOWS/system
MD5 Hash:	e20e5add430f5001486389beee4bb1b
SSDeep Hash:	6144:mRqmp+amNOGokzLyM9tsLaitQo6tzOKkzlt8gKyfjxR9D2j4ynjD:WqmpplpGoGL3etQoMiXM8gxf/Sj4ynjD
File Name:	fservice.exe
File Path:	WINDOWS/system32
MD5 Hash:	e20e5add430f5001486389beee4bb1b
SSDeep Hash:	6144:mRqmp+amNOGokzLyM9tsLaitQo6tzOKkzlt8gKyfjxR9D2j4ynjD:WqmpplpGoGL3etQoMiXM8gxf/Sj4ynjD
File Name:	Incom_.jpg
File Path:	WINDOWS/system32
MD5 Hash:	ad894c815059f46a95308507492eb4ee
SSDeep Hash:	1536:JP7DVJlCjFTByqpQ91QSHQ7o5K6dpMPW0dc4+PixH/1YDB3XL1:RVJ+jFTFQvQGQso6dKx61Pixf1aL1
File Name:	reginv.dll
File Path:	WINDOWS/system32
MD5 Hash:	562e0d01d6571fa2251a1e9f54c6cc69
SSDeep Hash:	384:nqqS78pWkPT5NGqu1mIwVtCj7y6bWHAgtNoUo3GFa:nqNmvt5JOCj7IWHAEiUo

Files created on the File System - Count: 10

[Back To Top](#)

File Name:	winkey.dll
File Path:	WINDOWS/system32
MD5 Hash:	b4c72da9fd1a0dcb0698b7da97daa0cd
SSDeep Hash:	384:NIYOgP RBTLClIt5dtahAxvr6+S9Pfu7n5:NIZEXL3t5dtrnx+deV

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

File Name:	index.dat
File Path:	Documents and Settings/Administrator/Local Settings/History/History.IE5
MD5 Hash:	da8c753f214b3d01221c5784b8ec34ba
File Name:	index.dat
File Path:	Documents and Settings/Administrator/Local Settings/Temporary Internet Files/Content.IE5
MD5 Hash:	5c25972269aad0190abfc726848d8a65
File Name:	NTUSER.DAT
File Path:	Documents and Settings/Administrator
MD5 Hash:	cc42e8613fa018a7a49d2711224b88aa
File Name:	NTUSER.DAT
File Path:	Documents and Settings/LocalService
MD5 Hash:	79d767f504dec24be89f15704dc8f21f
File Name:	NTUSER.DAT
File Path:	Documents and Settings/NetworkService
MD5 Hash:	eb44a170c46f1e39e327e03eb594e9c1
File Name:	AppEvent.Evt
File Path:	WINDOWS/system32/config
MD5 Hash:	acda90370144054a79d30dc2e2a1ddb6
File Name:	default
File Path:	WINDOWS/system32/config
MD5 Hash:	9d8ad6a941dce6383171e2cbdf1fe848
File Name:	SAM
File Path:	WINDOWS/system32/config
MD5 Hash:	315efe6a72112823c3fca2c7a6188c1b
File Name:	SECURITY
File Path:	WINDOWS/system32/config
MD5 Hash:	0e4c13b732ef9f3e4211ea3b226dca6b
File Name:	software
File Path:	WINDOWS/system32/config
MD5 Hash:	f77516056db375cca9e62f80c195cef6
File Name:	SysEvent.Evt
File Path:	WINDOWS/system32/config
MD5 Hash:	8d02915d3f824686098b7078a05d1c55
File Name:	system
File Path:	WINDOWS/system32/config
MD5 Hash:	e3a3adaf3fd87f14e7e2b2969e66727b

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

File Name: wbmess.lo_
 File Path: WINDOWS/system32/wbem/Logs
 MD5 Hash: b8e4d071edb3fc82e62dc9f8215472e3

New Open and/or Listening Ports (MPORT) - Count: 4

[Back To Top](#)

Protocol	LocalIpPort	RemotepPort	Service	Status
0.0.0.0:5110	TCP	0.0.0.0:6202	LISTENING	services.exe:1496
0.0.0.0:51100	TCP	0.0.0.0:10360	LISTENING	services.exe:1496
0.0.0.0:5112	TCP	0.0.0.0:2165	LISTENING	services.exe:1496
10.10.10.7:1041	TCP	4.3.2.36:25	ESTABLISHED	services.exe:1496

New Open Sockets in Memory - Count: 4

[Back To Top](#)

Pid	Port	Proto
1496	5112	6
1496	51100	6
1496	5110	6
1496	1041	6

New Processes in Memory - Count: 1

[Back To Top](#)

Pid	PPid	Name
1496	1736	services.exe

New Connections in Memory - Count: 3

[Back To Top](#)

LocalIpPort	RemotepPort	Pid
10.10.10.7:1041	4.3.2.36:25	1496
10.10.10.7:1041	4.3.2.36:25	1496
10.10.10.7:1041	4.3.2.36:25	1496

New Opened files which were contained within Memory - Count: 9

[Back To Top](#)

Data

File \AsyncConnectHlp
File \AsyncSelectHlp
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\MSHist012008090920080910\index.dat
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 \WINDOWS\WinSxS\x86_Microsoft.Windows.GdiPlus_6595b64144ccf1df_1.0.2600.2180_x-ww_522f9f82
File \WINDOWS\services.exe

Strings Command executed on Processes contained within Memory - Count: 206

[Back To Top](#)

Data

true
1 ftp ftp
FtpSrvT (c) 1999-2000 F. Piette V1.02
TFtpCtrlSocket (c) 1998-2000 F. Piette V1.06
TFtpServer (c) 1998-2000 F. Piette V1.08
TFtpSrvDataSessionConnectedEvent
220 ICS FTP Server ready.
220 Welcom to ProRat Ftp Server
220-ICS FTP Server ready
.;tj
@\$xp\$16Ftpsrv@FtpSrv__3
@\$xp\$17Ftpsrv@TFtpServer
@\$xp\$17Ftpsrv@TFtpString
@\$xp\$18Ftpsvrc@TFtpOption
@\$xp\$19Ftpsvrc@TFtpCmdType
@\$xp\$19Ftpsvrc@TFtpOptions
@\$xp\$21Ftpsvrc@TCommandEvent
@\$xp\$21Ftpsvrc@TDisplayEvent
@\$xp\$21Ftpsvrc@TFtpCtrlState
@\$xp\$22Ftpsvrc@TFtpCtrlSocket
@\$xp\$25Ftpsrv@FtpServerException
@\$xp\$25Ftpsrv@TFtpSrvCommandProc
@\$xp\$26Ftpsrv@TFtpCtrlSocketClass
@\$xp\$30Ftpsrv@TFtpSrvCommandTableItem
@\$xp\$31Ftpsrv@TFtpSrvAuthenticateEvent
@\$xp\$31Ftpsrv@TFtpSrvRetrDataSentEvent
@\$xp\$31Ftpsrv@TFtpSrvValidateXferEvent
@\$xp\$31Ftpsvrc@EFtpCtrlSocketException
@\$xp\$32Ftpsrv@TFtpSrvClientCommandEvent
@\$xp\$32Ftpsrv@TFtpSrvClientConnectEvent
@\$xp\$32Ftpsrv@TFtpSrvDataAvailableEvent
@\$xp\$33Ftpsrv@TFtpSrvAnswerToClientEvent
@\$xp\$33Ftpsrv@TFtpSrvBuildDirectoryEvent
@\$xp\$34Ftpsrv@TFtpSrvChangeDirectoryEvent
@\$xp\$39Ftpsrv@TFtpSrvDataSessionConnectedEvent
@Ftpsrv@CopyRight
@Ftpsrv@Finalization\$qqr
@Ftpsrv@FtpServerException@
@Ftpsrv@Register\$qqr
@Ftpsrv@TFtpServer@

Strings Command executed on Processes contained within Memory - Count: 206

[Back To Top](#)

@Ftpsrv@TftpServer@\$bctr\$qqrp18Classes@TComponent
@Ftpsrv@TftpServer@\$bdtr\$qqrv
@Ftpsrv@TftpServer@ClientCommand\$qqrp14System@TObjectpci
@Ftpsrv@TftpServer@ClientDataSent\$qqrp14System@TObjectus
@Ftpsrv@TftpServer@ClientPassiveSessionAvailable\$qqrp14System@TObjectus
@Ftpsrv@TftpServer@ClientRetrDataSent\$qqrp14System@TObjectus
@Ftpsrv@TftpServer@ClientRetrSessionClosed\$qqrp14System@TObjectus
@Ftpsrv@TftpServer@ClientRetrSessionConnected\$qqrp14System@TObjectus
@Ftpsrv@TftpServer@ClientSessionClosed\$qqrp14System@TObjectus
@Ftpsrv@TftpServer@ClientStorDataAvailable\$qqrp14System@TObjectus
@Ftpsrv@TftpServer@ClientStorSessionClosed\$qqrp14System@TObjectus
@Ftpsrv@TftpServer@ClientStorSessionConnected\$qqrp14System@TObjectus
@Ftpsrv@TftpServer@DisconnectAll\$qqrv
@Ftpsrv@TftpServer@GetActive\$qqrv
@Ftpsrv@TftpServer@GetClientCount\$qqrv
@Ftpsrv@TftpServer@Notification\$qqrp18Classes@TComponent18Classes@TOperation
@Ftpsrv@TftpServer@SendNextDataChunk\$qqrp22Ftpsvr@TftpCtrlSocketp16Wsocket@TWSocket
@Ftpsrv@TftpServer@ServSocketSessionAvailable\$qqrp14System@TObjectus
@Ftpsrv@TftpServer@ServSocketStateChange\$qqrp14System@TObject20Wsocket@TSocketStatet2
@Ftpsrv@TftpServer@SetActive\$qqro
@Ftpsrv@TftpServer@Start\$qqrv
@Ftpsrv@TftpServer@StartSendData\$qqrp22Ftpsvr@TftpCtrlSocket
@Ftpsrv@TftpServer@Stop\$qqrv
@Ftpsrv@TftpServer@TriggerAuthenticate\$qqrp22Ftpsvr@TftpCtrlSocket17System@AnsiStringt2ro
@Ftpsrv@TftpServer@TriggerChangeDirectory\$qqrp22Ftpsvr@TftpCtrlSocket17System@AnsiStringro
@Ftpsrv@TftpServer@TriggerClientConnect\$qqrp22Ftpsvr@TftpCtrlSocketus
@Ftpsrv@TftpServer@TriggerClientDisconnect\$qqrp22Ftpsvr@TftpCtrlSocketus
@Ftpsrv@TftpServer@TriggerMakeDirectory\$qqrp22Ftpsvr@TftpCtrlSocket17System@AnsiStringro
@Ftpsrv@TftpServer@TriggerRetrDataSent\$qqrp22Ftpsvr@TftpCtrlSocketp16Wsocket@TWSocketus
@Ftpsrv@TftpServer@TriggerRetrSessionClosed\$qqrp22Ftpsvr@TftpCtrlSocketp16Wsocket@TWSocketus
@Ftpsrv@TftpServer@TriggerRetrSessionConnected\$qqrp22Ftpsvr@TftpCtrlSocketp16Wsocket@TWSocketus
@Ftpsrv@TftpServer@TriggerServerStart\$qqrv
@Ftpsrv@TftpServer@TriggerServerStop\$qqrv
@Ftpsrv@TftpServer@TriggerStorDataAvailable\$qqrp22Ftpsvr@TftpCtrlSocketp16Wsocket@TWSocketpci
@Ftpsrv@TftpServer@TriggerStorSessionClosed\$qqrp22Ftpsvr@TftpCtrlSocketp16Wsocket@TWSocketus
@Ftpsrv@TftpServer@TriggerStorSessionConnected\$qqrp22Ftpsvr@TftpCtrlSocketp16Wsocket@TWSocketus
@Ftpsrv@TftpServer@WMFtpSrvAbortTransfer\$qqrr17Messages@TMessage
@Ftpsrv@TftpServer@WMFtpSrvClientClosed\$qqrr17Messages@TMessage
@Ftpsrv@TftpServer@WMFtpSrvCloseData\$qqrr17Messages@TMessage
@Ftpsrv@TftpServer@WMFtpSrvCloseRequest\$qqrr17Messages@TMessage
@Ftpsrv@TftpServer@WndProc\$qqrr17Messages@TMessage
@Ftpsrv@initialization\$qqrv
@Ftpsvr@CopyRight
@Ftpsvr@EFtpCtrlSocketException@
@Ftpsvr@Finalization\$qqrv
@Ftpsvr@IsUNC\$qqr17System@AnsiString
@Ftpsvr@PatchIE5\$qqrr17System@AnsiString
@Ftpsvr@TftpCtrlSocket@
@Ftpsvr@TftpCtrlSocket@\$bctr\$qqrp18Classes@TComponent
@Ftpsvr@TftpCtrlSocket@\$bdtr\$qqrv
@Ftpsvr@TftpCtrlSocket@Dup\$qqri
@Ftpsvr@TftpCtrlSocket@GetPeerAddr\$qqrv
@Ftpsvr@TftpCtrlSocket@SendAnswer\$qqr17System@AnsiString
@Ftpsvr@TftpCtrlSocket@SetAbortingTransfer\$qqro
@Ftpsvr@TftpCtrlSocket@SetDirectory\$qqr17System@AnsiString
@Ftpsvr@TftpCtrlSocket@SetRcvSize\$qqri
@Ftpsvr@TftpCtrlSocket@StartConnection\$qqrv

Strings Command executed on Processes contained within Memory - Count: 206

[Back To Top](#)

@FtpSrvC@TFtpCtrlSocket@TriggerCommand\$qqrpci
@FtpSrvC@TFtpCtrlSocket@TriggerDataAvailable\$qqrus
@FtpSrvC@TFtpCtrlSocket@TriggerSessionConnected\$qqrus
@FtpSrvC@initialization\$qqrv
@FtpSrvT@CopyRight
@FtpSrvT@FileUtcStr\$qqr17System@AnsiString
@FtpSrvT@Finalization\$qqrv
@FtpSrvT@initialization\$qqrv
@Smtpprot@TCustomSmtplibClient@Mail\$qqrv
@Smtpprot@TCustomSmtplibClient@MailFrom\$qqrv
@Smtpprot@TCustomSmtplibClient@SetMailMessage\$qqrp16Classes@TStrings
@Smtpprot@TSmtplibCli@PrepareEMail\$qqrv
@Smtpprot@TSmtplibCli@SetEMailFiles\$qqrp16Classes@TStrings
@Smtpprot@TSyncSmtplibCli@MailFromSync\$qqrv
@Smtpprot@TSyncSmtplibCli@MailSync\$qqrv
EFtpCtrlSocketExceptionD_D
EFtpCtrlSocketException`_D
EmailFiles
FtpServer1
FtpServer1Authenticate
FtpServer1ChangeDirectory
FtpServer2
FtpServer2Authenticate
FtpServerException
FtpSrv
FtpSrvC
FtpState
GET /friendship/email_thank_you.php?
folder_id=18984&fms_count=0&nick_name=Pro_Rat&user_email=Pro_Rat@yahoo.com&user_uin=&friend_nickname=&friend_contact=
Host: www.icq.com
Kisses_Mcafee
MAIL FROM:
MAIL FROM:<
Mail
MailMessage
Mail_atm=i/ri`l3118Ainul`hm/bnl
ProRat@Yahoo.Com
Referer: http://www.icq.com/friendship/pages/send_by_email_18984.php
TFtpCmdType
TFtpCtrlSocket
TFtpCtrlState
TFtpOption
TFtpOptions
TFtpServer
TFtpSrvAnswerToClientEvent
TFtpSrvAuthenticateEvent
TFtpSrvBuildDirectoryEvent
TFtpSrvChangeDirectoryEvent
TFtpSrvClientCommandEvent
TFtpSrvClientConnectEvent
TFtpSrvCommandProc
TFtpSrvCommandTableItem
TFtpSrvDataAvailableEvent
TFtpSrvRetrDataSentEvent
TFtpSrvValidateXferEvent
TFtpString
TFtpString@

Strings Command executed on Processes contained within Memory - Count: 206

[Back To Top](#)

\CuteFTP\smdata.dat
\CuteFTP\tree.dat
\GlobalSCAPE\CuteFTP Pro\2.0\sm.dat
\GlobalSCAPE\CuteFTP Pro\3.0\sm.dat
\GlobalSCAPE\CuteFTP Pro\6.0\sm.dat
\GlobalSCAPE\CuteFTP Pro\sm.dat
\GlobalSCAPE\CuteFTP\5.0\sm.dat
\GlobalSCAPE\CuteFTP\cutftp32.exe
\GlobalSCAPE\CuteFTP\sm.dat
\GlobalSCAPE\CuteFTP\smdata.dat
\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Ratings\Default\http://www.rsac.org/ratingsv01.html
aku.edu.tr
ankara.edu.tr
atauni.edu.tr
ege.edu.tr
ftp-data
ftpcABOR
ftpcAPPE
ftpcCDUP
ftpcCWD
ftpcDELE
ftpcInvalid
ftpcLIST
ftpcMDTM
ftpcMKD
ftpcNLST
ftpcNOOP
ftpcPASS
ftpcPORT
ftpcPWD
ftpcQUIT
ftpcREST
ftpcRETR
ftpcRMD
ftpcRNFR
ftpcRNT0
ftpcSIZE
ftpcSTOR
ftpcSTRU
ftpcSYST
ftpcTYPE
ftpcUNC
ftpcUSER
ftpcWaitingAnswer
ftpcWaitingPassword ftpcReady
ftpcWaitingUserCode
ftpcXPWD
smtpFctMailFrom
smtpMail
smtpMailFrom
www.icq.com
|rdr|\plug_ins\sendmail.api

Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 3

[Back To Top](#)

Data

hotmail.com
hotmail.commail
mail.hotmail.com

Malicious SMTP Traffic - Count: 29

[Back To Top](#)

Data

Connection from 10.10.10.7
HELO ProRat
AIL FROM:
RCPT TO:
DATA
From: "ProRat V1.9:Fix-10"
To: h.sham2009@hotmail.com
Subject: ProRat [victim Online]
Sender: Microsoft Outlook Express 6.00.2800.1158
ime-Version: 1.0
Content-Type: text/plain
Date: Tue, 9 Sep 2008 15:46:10 -0700
[ProRat V1.9:Fix-10]
Victim is Online.
IP Address(es) :
10.10.10.7
Port :5110
Password :123456
Victim name :victim
User name :Administrator
Computer Name :BADKARMA
Date :9/9/2008
Time :3:46:10 PM
.
QUIT
end of mail session

Potentially Malicious Changes in System Registry File - Count: 3

[Back To Top](#)

Data

"Group"=""
"DependOnGroup"=hex(7):00
"Group"=""

Potentially Malicious Changes in Software Registry File - Count: 5

[Back To Top](#)

Data

```
"StubPath"="C:\\WINDOWS\\system\\sservice.exe"  
[software\\Microsoft\\Windows\\CurrentVersion\\policies\\Explorer]  
[software\\Microsoft\\Windows\\CurrentVersion\\policies\\Explorer\\Run]  
"DirectX For Microsoft Windows"="C:\\WINDOWS\\system32\\fservice.exe"  
"Shell"="Explorer.exe C:\\WINDOWS\\system32\\fservice.exe"
```

Potentially Malicious Changes in NTUSER.DAT File - Count: 27

[Back To Top](#)

Data

```
[NTUSER\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\FileExts\\.jpg\\OpenWithList]  
[NTUSER\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\RecentDocs]  
[NTUSER\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\RecentDocs\\.jpg]  
[NTUSER\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\RecentDocs\\Folder]  
[NTUSER\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\5.0\\Cache\\Extensible Cache\\MSHist012008090920080910]  
"CachePrefix"=":2008090920080910: "  
"C:\\WINDOWS\\System32\\shimgvw.dll"="Windows Picture and Fax Viewer"  
"C:\\WINDOWS\\system32\\lncom.exe"="lncom"  
[NTUSER\\Software\\Microsoft\\Windows NT Script Host]  
[NTUSER\\Software\\Microsoft\\Windows NT Script Host\\Microsoft DxDiag]  
[NTUSER\\Software\\Microsoft\\Windows NT Script Host\\Microsoft DxDiag\\WinSettings]  
"Bulas"="1"  
"FW_KILL"="1"  
"XP_FW_Disable"="1"  
"XP_SYS_Recovery"="1"  
"ICQ_UIN"=""  
"ICQ_UIN2"=""  
"Kurban_Ismi"="whbuhl"  
"Mail"="i\\r\\l3118Ainul\\hm\\bni"  
"Online_List"=""  
"Port"="4001"  
"Sifre"="032547"  
"Hata"=""  
"KSil"="1"  
"LanNotifie"=""  
"Tport"="0"  
"ServerVersionInt"="19"
```

Keylogger - Count: 1

[Back To Top](#)

Data

```
WINDOWS\\ktd32.atm
```

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.

* Ngrsp: 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.