GENERAL DYNAMICS
Fidelis Cybersecurity Solutions

www.fidelissecurity.com

www.threatgeek.com

@FidSecSys

+1800.652.4020

Fidelis Threat Advisory #1009

"njRAT" Uncovered

June 28, 2013

Document Status: FINAL
Last Revised: 2013-06-28

Executive Summary

In the past thirty days (30) an increase attack activity has been observed using the "njRAT" malware. This remote access trojan (RAT) has capabilities to log keystrokes, access the victim's camera, steal credentials stored in browsers, open a reverse shell, upload/download files, view the victim's desktop, perform process, file, and registry manipulations, and capabilities to let the attacker update, uninstall, restart, close, disconnect the RAT and rename its campaign ID. Through the Command & Control (CnC) server software, the attacker has capabilities to create and configure the malware to spread through USB drives.

"njRAT" is currently leveraged by advanced threat actors in the Middle East, in particular when delivered via HTTP (i.e. Phishing attack or Drive-by download). It has also been observed that attackers are delivering "njRAT" embedded in other applications (i.e. L517 v.0.994 Word List Generator), and compressed with EZIRIZ .NET Reactor/.NET protector. Obfuscation with the use of compressors or protectors is a technique used by attackers to prevent detection by network-based and host-based security defenses.

We have observed the majority of the attacks leveraging "njRAT" to be against organizations based in or focused on the Middle East region in the government, telecom, and energy sectors. However as this is a publicly available tool it can be attained and deployed with ease regardless of location or industry.

During the analysis of "njRAT", it was observed that some of the top antivirus vendors were not currently detecting some variants of this threat.

Some of the file names of carrier files or njRAT samples observed were: L517 v0.994.exe, RealUpgrade.exe, password hotmail cracker 2013.exe, elisa.exe, Crack All Games.exe, fresh cc

cvv all info 2013_txt.scr, spoolsv.exe, Hack Origin Game's.exe, Authorization form may - 2013 - 115444.scr, and Authorization.exe.

This document will provide detailed information about the njRAT's functionality, file system indicators, network indicators, some of the campaign IDs observed, MD5 hashes, and domains. It will also go over a detailed analysis of one of the malware variants.

Threat Overview

The "njRAT" is a robust remote access trojan that once it reaches and infects the end-point, allows the attacker to have full control over the Victim system. With this access, the attacker can start scanning other systems in the victim network to perform lateral movement.

We will start this section by performing analysis on the following "njRAT" sample:

- Filename: Authorization.exe
- MD5: 1d3baedd747f6f9bf92c81eb9f63b34b

The "Authorization.exe" njRAT malware was embedded and dropped in the victim system by the following file: "Authorization form may - 2013 - 115444.scr" (MD5: 63781fe1932e612c6c29225d25515111).

The next section (Indicators & Mitigation Strategies), will provide information about other variants of the malware obtained.

Summary

The "**Authorization.exe**" malware sample was created with version **V.0.5** of this RAT. The njRAT application was developed with VB.NET (Visual Basic .NET).

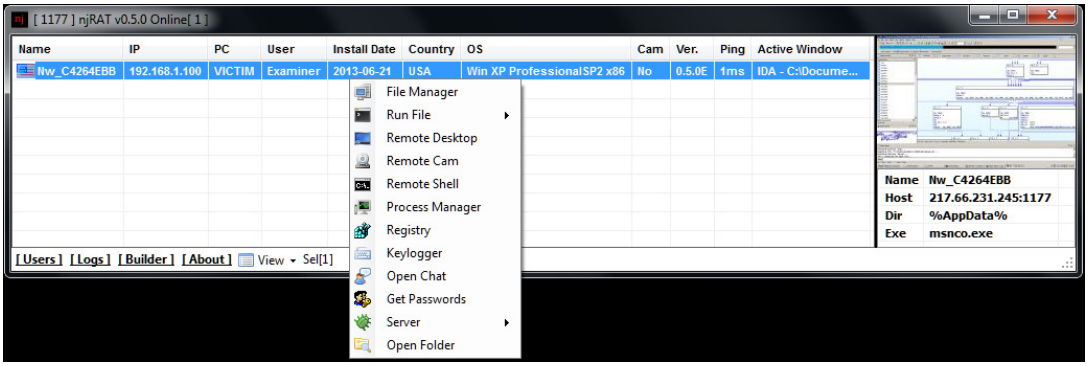
When the malware connects to the Command & Control (CnC) server, the attacker is able to perform the following actions from the njRAT CnC server GUI:

- Open a 'File Manager' window to manipulate files
  - This window allows the attacker to Upload & Download, Run, Delete, Edit, Rename, Copy, Cut, Paste, and Empty files.
  - The window also allows the attacks to create new folders in the Victim system
- Open a 'Run File' window
  - This window allows the attacker to upload a file, or provide a link to a file to run in the Victim system
- Open a 'Remote Desktop' window
  - When selected, it opens a live window of the Victim's user desktop
- Open a 'Remote Cam' window
  - This window allows the attacker to obtain access to the Victim's system camera to see the Victim user

- Open a 'Remote Shell' window
  - This window opens a reverse shell window and allow the attacker to perform all the activities possible from the command prompt
- Open a 'Process Manager' window
  - This window allows the attacker to Refresh the process list, Kill processes, Suspend processes, Resume processes
- Open a 'Registry' window
  - This window allows the attacker manipulate the Victim's system registry (edit, delete, create keys and values)
- Open a 'Keylogger' window
  - When this option is selected, the keylogger file is automatically uploaded from the Victim system into the attacker's machine
- Open a 'Get Passwords' window
  - This window appears to collect all the passwords stored by the browser (User, Password, URL, App). At the moment of writing this report, the functionality was not confirmed. When the option is selected, the malware searches Mozilla Firefox, Google Chrome, Opera directories.
- Open a 'Server' window
  - This window allows the attacker to Update, Uninstall, Restart, Close, Disconnect, or Rename the malware running in the Victim system
- Open an 'Open Folder' window
  - This window open the local folder in the attackers machine in which the artifacts collected through the "njRAT" GUI are stored in his/her system
- Open a 'Builder' Window
  - This window allows the attacker to build new Clients to be deployed to Victims or used in attack campaigns. Some of the options in this builders allows the attacker to configure:

    - C2 node IP
    - C2 node port
    - Vic Tim Name (Looks like this could be used to identify the attack campaign)
    - Malware name (when it makes a copies itself)
    - Directory to make a copy of the malware when it is executed
    - Capabilities to spread via USB
    - Select the malware icon
    - Protect the malware process
    - Stub Randomization

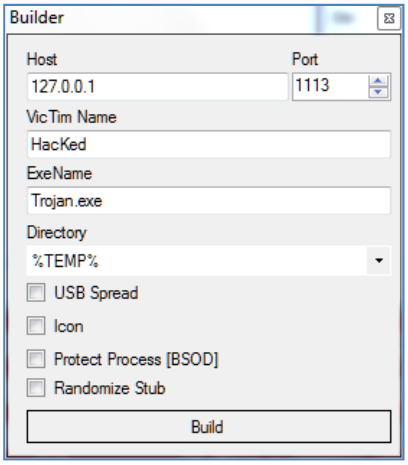
The following is a screenshot of the "njRAT" v.0.5 CnC GUI when a Victim system connects to it:



The following "About" information was observed in this version (0.5.0) of the C2 server software found online:

Project	: njRat
Verison	: 0.5.0
Coded By	: njq8
FireFox Stealer	: DarkSel
Paltalk Stealer	: pr0t0fag
Chrome Stealer	: RockingWithTheBest
Opera Stealer	: Black-Blood, KingCobra
MySite	: http://xnjq8x.com

The following screenshot shows the Builder interface and default parameters:



The "**Authorization.exe**" malware has keylogger functionality. It stores the logged keystrokes in the following file: "[CWD]**.tmp**". When the malware is dropped by the "**Authorization form may - 2013 - 115444.scr**" carrier file, the logged keystrokes are stored in: "C:\Extracted**.tmp**".

The IP address used by the Command & Control (C2) node appears to be under an IP range owned by: "Palestinian Internet Services, P. O. BOX 5111 Gaza City, Palestine".

Variants of this malware have been observed by the community since at least 2012. The malware appears to be known by the community as: njRAT, MSIL/Bladabindi, and Backdoor.LV.

When the "**Authorization.exe**" malware is executed it:

- Creates a copy of itself in the following locations:
  - %APPDATA%**msnco.exe**
  - C:\Documents and Settings\%USERNAME%\Start Menu\Programs\Startup**b6554e5bcfef391ff7a7ffda58092e10.exe**

- Tries to open the following file: [CWD]\ **Authorization.exe.config**

- Entrenches in the system for persistence in the following registry locations:
  - `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\b6554e5bcfef391ff7a7ffda58092e10`
  - `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\b6554e5bcfef391ff7a7ffda58092e10`

Makes the following modifications to the registry to bypass the Windows Firewall:

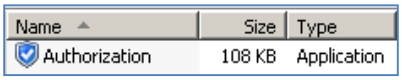
- Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List*[%APPDATA%]*\msnco.exe
- Value: *[%APPDATA%]*\msnco.exe:*:Enabled:msnco.exe

- Beacons to the following C2 node over TCP port **1177**: "**217.66.231.245**"

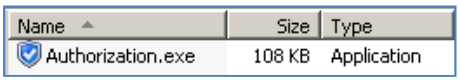
The attacker tries to make sure the malware will run in the system by making the second copy into the above mentioned directory (C:\Documents and Settings\%USERNAME%\Start Menu\Programs\Startup**b6554e5bcfef391ff7a7ffda58092e10.exe**)

- This causes the malware to execute again when the system is rebooted and re-starts the infection in the system. Once the system is infected again, it will beacon to the C2 node.

The attacker tries to trick the user by using different icons for the malware. Various samples were observed with MS Word and PDF icons. The following is a screenshot of how the file will look like to a normal user:



When the system is configured to show file extensions, the EXE extension is now revealed:



When the malware connects to the C2 node, it will send information about the victim system, malware version, open windows, etc. The following is the network traffic observed:

```
lv|'|'|TndfQzQyNjRFQkI=|'|'|VICTIM|'|'|Examiner|'|'|2013-06-21|'|'|USA|'|'|Win XP ProfessionalSP2
x86|'|'|No|'|'|0.5.0E|'|'|..|'|'|Y3B0YnRfUHJvY2Vzc19SZWdpc3RyeV9GaWxlX0luZm8ubG9nIC0gTm90ZXB
hZA==|'|'|[endof]act|'|'|
Y3B0YnRfUHJvY2Vzc19SZWdpc3RyeV9GaWxlX0luZm8ubG9nIC0gTm90ZXBhZA== [endof]
```

The following table provides information of some of the fields observed in the network traffic:

Field	Information
TndfQzQyNjRFQkI=	Base64 encoded data. The decoded data reveals the following string: "**Nw_C4264EBB**". It appears that the string before the "_" (**Nw**) can be used by the attacker to identify the attack campaign. This is configured through the "njRAT" builder GUI. The second portion ("**C4264EBB**") is the Volume Serial Number of the victim system
VICTIM	Computer name
Examiner	Username
2013-06-21	Date Modified attribute of the malware. This date will match the first time the file is created in the victim system
USA	System locale
Win XP ProfessionalSP2 x86	Operating System Information
No	Report if the system has a camera
0.5.0E	Malware version
Y3B0YnRfUHJvY2Vzc19SZWdpc3RyeV9GaWxlX0luZm8ubG9nIC0gTm90ZXBhZA==	Base64 encoded data. The decoded data reveals the following string: "cptbt_Process_Registry_File_Info.log - Notepad". In this case, the decoded string is just information about an open window used by the examiner to capture system activity

Information sent by the attacker on opened windows in the system could inform him/her of his malware being analyzed and allowed to connect to the C2 node. For example, if Wireshark, Filemon, Regmon, and IDA are opened in the system when the analyst executes the malware, this will quickly let the attacker know that someone is performing reverse engineering of his malicious code.

The following WHOIS information was found related to the C2 node (**217.66.231.245**):

inetnum:	217.66.228.0 - 217.66.231.255
netname:	AV_FXD_RA
descr:	AV_FXD_RA
country:	PS
admin-c:	HT1472-RIPE
tech-c:	WK4085-RIPE
status:	Assigned PA
mnt-by:	Palnet-mnt
source:	RIPE # Filtered
person:	Hadara Tech
address:	RaMallah
phone:	+97022403434
nic-hdl:	HT1472-RIPE
mnt-by:	palnet-MNT
source:	RIPE # Filtered
person:	Walid Kassab
address:	**Palestinian Internet Services**
address:	**P. O. BOX 5111 Gaza City, Palestine**
phone:	+972 8 284 3197
fax-no:	+972 8 284 3187
nic-hdl:	WK4085-RIPE
mnt-by:	PIS-MNTNER
source:	RIPE # Filtered
% Information related to '217.66.224.0/20 AS15975'	
route:	217.66.224.0/20
descr:	PALNET-NET
origin:	AS15975
remarks:	removed cross-nfy: MND1-RIPE
remarks:	removed cross-mnt: PALNET-MNT
mnt-by:	PALNET-MNT
source:	RIPE # Filtered

The "**Authorization.exe**" variant in this report appears to have been available at some point through the following URL: "**hxxp://bongdacongdong.vn/authorization.exe**". The domain currently resolves to the following IP address: "**112.213.89.144**", but at some point, the domain was associated with the following IP address: "**31.170.165.90**".

The following information was found at Virustotal for "**31.170.165.90**":

- Passive DNS replication

  The following domains resolved to the given IP address:

  2013-04-18 abilkart.p.ht
  2013-04-22 alexis.id1945.com
  2013-04-27 aw.nation-sim.net
  2013-06-04 bongdacongdong.vn
  2013-04-11 cs-viewer.ru
  2013-06-26 dota2mail.hol.es
  2013-05-07 download.mikroonur.tk
  2013-06-27 express.vv.si
  2013-04-16 forumteam.ru
  2013-04-25 hs.nation-sim.net

- Latest detected URLs

  Latest URLs hosted in this IP address detected by at least one URL scanner or malicious URL dataset:

  3/38 2013-06-09 08:16:23 hxxp://www.saldo-dobrado.id1945.com/sodexo2013/dobro.htm
  2/38 2013-06-05 15:15:03 hxxp://yandload.besaba.com/
  3/38 2013-06-04 02:08:18 hxxp://bongdacongdong.vn/authorization.exe
  4/38 2013-05-30 21:34:09 hxxp://yandload.besaba.com/index.php?f=rubinrot.exe
  5/39 2013-05-24 17:36:28 hxxp://indonesiancode.p.ht/
  2/36 2013-05-10 04:50:52 hxxp://yandload.besaba.com/index.php%3F
  2/37 2013-04-30 05:06:15 hxxp://yandload.besaba.com/index.php%5B%2A%2Aqmark%2A%2A%5D
  2/37 2013-04-29 22:23:55 hxxp://php6.besaba.com/install_flashplayer11x32_mssd_aih.exe
  2/36 2013-04-27 09:14:33 hxxp://aw.nation-sim.net/ips_kernel/sabre/Sabre/DAV/FS/option.php
  1/36 2013-04-22 21:56:09 hxxp//alexis.id1945.com/

- First submission:

  2013-05-28 at 00:12:24

"Authorization.exe" File Information

```
File Name:  Authorization.exe
File Size:  110080 bytes
MD5:        1d3baedd747f6f9bf92c81eb9f63b34b
SHA1:       328c12ba3e6e99e63968b066455b7575e7ee862b
PE Time:    0x5197ACE1 [Sat May 18 16:31:29 2013 UTC]
PEID Sig:   Microsoft Visual C# / Basic .NET
PEID Sig:   Microsoft Visual Studio .NET
Sections (4):
  Name      Entropy  MD5
  .text     5.09     dd1ed0314f376bad9786d08b53796a67
  .sdata    7.99     f92654e72b03e352178cad42896f9662
  .rsrc     5.65     03e4e092203078e7957cd7c164240f3d
  .reloc    0.08     3f2e9251bcd17a2cb17e9202d1b100d3
```

Antivirus Hits

AV Tool	Common Name
Kaspersky	Trojan.MSIL.Zapchast.zlg
AntiVir	TR/MSIL.Zapchast.zlg
Avast	Win32:Malware-gen
AVG	Generic33.AHLZ
BitDefender	Trojan.GenericKDV.1013622
F-Secure	Trojan.GenericKDV.1013622
Fortinet	W32/Zapchast.ZLG!tr
McAfee	RDN/Generic.grp!ep
Microsoft	Trojan:Win32/Comitsproc
Norman	Troj_Generic.LRVVH
Sophos	Mal/Generic-S
Symantec	WS.Reputation.1
TrendMicro	TROJ_GEN.RCCCDF5
VIPRE	Trojan.Win32.Generic!BT

Process artifacts

The following processes were started when the "**Authorization.exe**" malware was executed:

- C:\Windows\System32\netsh.exe
- %APPDATA%\msnco.exe

File system artifacts

The following files were created when the "**Authorization.exe**" malware was executed:

- %APPDATA%\msnco.exe
- C:\WINDOWS\Prefetch\AUTHORIZATION.EXE-0AD199D6.pf
- C:\Documents and Settings\%USERNAME%\Start Menu\Programs\Startup\b6554e5bcfef391ff7a7ffda58092e10.exe
- C:\WINDOWS\Prefetch\NETSH.EXE-085CFFDE.pf
- C:\WINDOWS\Prefetch\MSNCO.EXE-1616CBE8.pf
- [CWD] \.tmp (or when created by the original dropper: "C:\Extracted\.tmp")

Registry artifacts

The following registry values were set by the "**Authorization.exe**" malware when it was executed:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\b6554e5bcfef391ff7a7ffda58092e10 [Value: "[*%APPDATA%*]\msnco.exe" ..]
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\b6554e5bcfef391ff7a7ffda58092e10 [Value: "[*%APPDATA%*]\msnco.exe" ..]
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List\ *[%APPDATA%]*\msnco.exe [Value: *[%APPDATA%]*\msnco.exe:*:Enabled:msnco.exe]

Network artifacts

Domain/IP	Port	Encrypted/Encoded
217.66.231.245	1177	Some data is Base64 encoded

Indicators & Mitigation Strategies:

The following three (3) tables will provide information about some of the malware observed to be njRAT itself or carrier files that once executed dropped njRAT in the victim system. The first table contains the MD5 hash , size, domain, port, njRat version, and campaign ID. The second table contains information about the file system artifacts (kelogger file location, files created). The third table contains information about registry key entrenchment for persistence. Then, a list of network indicators will be provided to assist network defenders with the creation of signatures to be deployed to the sensors.

Table 1: MD5 hash, size, domain/IP, port, njRat version, and campaign ID

Note: The Campaing ID named "HacKed" is the default string in the njRAT Builder interface.

MD5	Size (bytes)	Domain/IP	Port	Version	Campaign ID
2013385034e5c8dfbbe47958fd821ca0	441344	dr-vip.no-ip.org	1177	0.5.0E	شيعى جديد
7c42d2426c51318f5947a92bf23e1686	839101	mp3.servemp3.com	9632	0.5.0E	رجه النفيعي_
a6da3b63981e345e1c3cd58c6e3dc7fc	123904	mp3.servemp3.com	9632	0.5.0E	رجه النفيعي_
e1471b169d6b4049d757bb705877d329	233984	kyfen.dyndns.biz	288	0.5.0E	~صليلي~
1d3baedd747f6f9bf92c81eb9f63b34b	790235	217.66.231.245	1177	0.5.0E	Nw
a669c0da6309a930af16381b18ba2f9d	26624	ksadxxd24.no-ip.org	80	0.3.6	شخصـــي تلغيـــم
5fcb5282da1a2a0f053051c8da1686ef	30208	xxsniper.no-ip.biz	81	0.3.5	sniper jordan
3b99f596b36ece7b6add78e3b14a3b17	295640	mohammad3badi.zapto.org	120	0.5.0E	26-3-2013
79dce17498e1997264346b162b09bde8	40960	naif.no-ip.org	1177	0.4.1a	2013
3ad5fded9d7fdf1c2f6102f4874b2d52	79360	wolblid.zapto.org	1177	0.5.0E	VictimO
fc96a7e27b1d3dab715b2732d5c86f80	977408	m3333m.no-ip.org	1177	0.3.6	NEW XXX
60f1b8980d109a556922d5000ae02010	1230848	zackhaviland.no-ip.org	1177	0.5.0E	leak
92ee1fb5df21d8cfafa2b02b6a25bd3b	26624	alitatat.no-ip.org	1177	0.3.6	IRAQ
2164c555f9f23dca54e76b94b1747480	59392	kurdkalar11.zapto.org	1177	0.5.0E	HacKed_By_XF
a98b4c99f64315aac9dd992593830f35	44544	kurdkalar11.zapto.org	1177	0.5.0E	HacKed_By_XF
7e34abdd10c5c763291e69a886452849	50688	hack-badone.no-ip.biz	1177	0.5.0E	HacKed By Badone
29daad42dafffab5e0f1f96d620e7392	96256	special.no-ip.biz	1500	0.5.0E	HacKed
4168543695513f767ba44997ebd71431	244736	nasr23200.no-ip.org	1177	0.5.0E	HacKed

fb671c8735461809534813b818d193f4	187904	wisam77.no-ip.biz	1177	0.5.0E	HacKed
2bf859ea02ae3340cd66eb5e46b1a704	75264	hassoon03.no-ip.info	1177	0.5.0E	HacKed
24cc5b811a7f9591e7f2cb9a818be104	314880	samirsamir.hopto.org	1177	0.5.0E	HacKed
11b79281a25da1b798574f667c56898b	428032	gdsg.no-ip.org	1199	0.5.0E	HacKed
2cdbbe5045bed2031a1fc77c3e30e719	583747	Saman70.no-ip.org	1177	0.5.0E	HacKed
f6b4a2be06fc3ba4bb02d1bcbea328fe	95232	Saman70.no-ip.org	1177	0.5.0E	HacKed

Table 2: MD5 hash, File system artifacts

Note: The copy of njRAT created with the filename "Trojan.exe", is the default filename string in the njRAT Builder interface. The Keylogger file location referred to as "[CWD]\.tmp", refers to the location from which the original malware is executed. It was observed that this was used when the malware was embedded in a legitimate looking application, and the kelogger files get created in the directory of that application (i.e. C:\Program Files\Facebook\QuadAtom\.tmp).

MD5	Keylogger File	Created Malware
2013385034e5c8dfbbe47958fd821ca0	%APPDATA%\ja33kk.exe.tmp	%APPDATA%\ja33kk.exe C:\Documents and Settings\%USERNAME%\Start Menu\Programs\Startup\9758a8dfbe15a00f55a11c8306f80da1.exe
7c42d2426c51318f5947a92bf23e1686	[CWD]\.tmp	%USERPROFILE%\RealUpgrade.exe C:\Documents and Settings\%USERNAME%\Start Menu\Programs\Startup\d30ac691925b853d59f2822ae7a67c94.exe (MD5: a6da3b63981e345e1c3cd58c6e3dc7fc, Size: 123904)
a6da3b63981e345e1c3cd58c6e3dc7fc	[CWD]\.tmp	%USERPROFILE%\RealUpgrade.exe C:\Documents and Settings\%USERNAME%\Start Menu\Programs\Startup\d30ac691925b853d59f2822ae7a67c94.exe
e1471b169d6b4049d757bb705877d329	[CWD]\.tmp	%TEMP%\java.exe C:\Documents and Settings\%USERNAME%\Start Menu\Programs\Startup\d2be3e6d11846430c067fc874a79f583.exe

1d3baedd747f6f9bf92c81eb9f63b34b	C:\Extracted\.tmp [CWD]\.tmp	%APPDATA%\msnco.exe C:\Documents and Settings\%USERNAME%\Start Menu\Programs\Startup\b6554e5bcfef391ff7a7ffda58092e10.exe
a669c0da6309a930af16381b18ba2f9d	%TEMP%\Trojan.exe.tmp	%TEMP%\Trojan.exe C:\Documents and Settings\Examiner\Start Menu\Programs\Startup\5cd8f17f4086744065eb0992a09e05a2.exe
5fcb5282da1a2a0f053051c8da1686ef	%TEMP%\Trojan.exe.log	%TEMP%\Trojan.exe C:\Documents and Settings\Examiner\Start Menu\Programs\Startup\5cd8f17f4086744065eb0992a09e05a2.exe
3b99f596b36ece7b6add78e3b14a3b17	[CWD]\.tmp	%TEMP%\mohd.exe C:\Documents and Settings\%USERNAME%\Start Menu\Programs\Startup\2635ef5d1f5dc1ac753feb21f019d8e4.exe
79dce17498e1997264346b162b09bde8	%APPDATA%\Trojan.exe.tmp	%APPDATA%\Trojan.exe C:\Documents and Settings\%USERNAME%\Start Menu\Programs\Startup\8515eb34d8f9de5af815466e9715b3e5.exe
3ad5fded9d7fdf1c2f6102f4874b2d52	%TEMP%\trojen.exe.tmp	%TEMP%\trojen.exe C:\Documents and Settings\%USERNAME%\Start Menu\Programs\Startup\49afcb0bd0c44cd98007157d78e8394a.exe
fc96a7e27b1d3dab715b2732d5c86f80	%TEMP%\Trojan.exe.tmp	%TEMP%\Trojan.exe C:\Documents and Settings\%USERNAME%\Start Menu\Programs\Startup\5cd8f17f4086744065eb0992a09e05a2.exe
60f1b8980d109a556922d5000ae02010	%TEMP%\file.exe.tmp	%TEMP%\file.exe C:\Documents and Settings\%USERNAME%\Start Menu\Programs\Startup\1052b8e9071d5b658c32c84c463014f5.exe
92ee1fb5df21d8cfafa2b02b6a25bd3b	%APPDATA%\Trojan.exe.tmp	%APPDATA%\Trojan.exe C:\Documents and Settings\Examiner\Start Menu\Programs\Startup\8515eb34d8f9de5af815466e9715b3e5.exe
2164c555f9f23dca54e76b94b1747480	%TEMP%\scvhost.exe.tmp	%TEMP%\scvhost.exe C:\Documents and Settings\%USERNAME%\Start Menu\Programs\Startup\8cff24636d2a58810bd5cdc8cb1b8987.exe %TEMP%\1.exe (MD5: a98b4c99f64315aac9dd992593830f35. Size: 44544)

		%TEMP%\2.exe
a98b4c99f64315aac9dd992593830f35	%TEMP%\scvhost.exe.tmp	%TEMP%\scvhost.exe C:\Documents and Settings\%USERNAME%\Start Menu\Programs\Startup\8cff24636d2a58810bd5cdc8cb1b8987.exe %TEMP%\1.exe (MD5: a98b4c99f64315aac9dd992593830f35. Size: 44544) %TEMP%\2.exe (MD5: a98b4c99f64315aac9dd992593830f35)
7e34abdd10c5c763291e69a886452849	%TEMP%\system.exe.tmp	%TEMP%\system.exe C:\Documents and Settings\%USERNAME%\Start Menu\Programs\Startup\12ce4e06a81e8d54fd01d9b762f1b1bb.exe
29daad42dafffab5e0f1f96d620e7392	[CWD]\.tmp	%TEMP%\Trojan.exe C:\Documents and Settings\%USERNAME%\Start Menu\Programs\Startup\5cd8f17f4086744065eb0992a09e05a2.exe
4168543695513f767ba44997ebd71431	[CWD]\.tmp	%TEMP%\Trojan.exe C:\Documents and Settings\%USERNAME%\Start Menu\Programs\Startup\5cd8f17f4086744065eb0992a09e05a2.exe
fb671c8735461809534813b818d193f4	%TEMP%\wsmlol.exe.tmp	%TEMP%\wsmlol.exe C:\Documents and Settings\%USERNAME%\Start Menu\Programs\Startup\191530b485fd6f0420e2c6bff7f0dbd7.exe
2bf859ea02ae3340cd66eb5e46b1a704	[CWD]\.tmp	%TEMP%\Trojan.exe C:\Documents and Settings\%USERNAME%\Start Menu\Programs\Startup\5cd8f17f4086744065eb0992a09e05a2.exe
24cc5b811a7f9591e7f2cb9a818be104	%APPDATA%\spoolsv.exe.tmp	%APPDATA%\spoolsv.exe (MD5: 24cc5b811a7f9591e7f2cb9a818be104, size: 314880) C:\Documents and Settings\%USERNAME%\Start Menu\Programs\Startup\28a9e392f74a71da2b5285754eb1baca.exe
11b79281a25da1b798574f667c56898b	%TEMP%\Win7.exe.tmp	%TEMP%\Win7.exe C:\Documents and Settings\%USERNAME%\Start Menu\Programs\Startup\614ef891df302ed5efa9b06422720faf.exe
2cdbbe5045bed2031a1fc77c3e30e719	C:\Program Files\Facebook\QuadAtom\.tmp	%TEMP%\Trojan.exe (MD5: f6b4a2be06fc3ba4bb02d1bcbea328fe, Size: 95232) C:\Documents and Settings\%USERNAME%\Start Menu\Programs\Startup\5cd8f17f4086744065eb0992a09e05a2.exe

f6b4a2be06fc3ba4bb02d1bcbea328fe	[CWD]\.tmp, or C:\Program Files\Facebook\QuadAtom\ .tmp	%TEMP%\Trojan.exe C:\Documents and Settings\%USERNAME%\Start Menu\Programs\Startup\5cd8f17f4086744065eb0992a09e05a2 .exe

Table 3: MD5 hash, Registry artifacts

MD5	Registry Entrenchment
2013385034e5c8dfbbe47958fd821ca0	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\9758a8dfbe15a00f55a11c8306f80da1 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\9758a8dfbe15a00f55a11c8306f80da1
7c42d2426c51318f5947a92bf23e1686	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\d30ac691925b853d59f2822ae7a67c94 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\d30ac691925b853d59f2822ae7a67c94
a6da3b63981e345e1c3cd58c6e3dc7fc	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\d30ac691925b853d59f2822ae7a67c94 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\d30ac691925b853d59f2822ae7a67c94
e1471b169d6b4049d757bb705877d329	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\d2be3e6d11846430c067fc874a79f583 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\d2be3e6d11846430c067fc874a79f583
1d3baedd747f6f9bf92c81eb9f63b34b	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\b6554e5bcfef391ff7a7ffda58092e10 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\b6554e5bcfef391ff7a7ffda58092e10
a669c0da6309a930af16381b18ba2f9d	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\5cd8f17f4086744065eb0992a09e05a2 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\5cd8f17f4086744065eb0992a09e05a2
5fcb5282da1a2a0f053051c8da1686ef	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\5cd8f17f4086744065eb0992a09e05a2 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\5cd8f17f4086744065eb0992a09e05a2
3b99f596b36ece7b6add78e3b14a3b17	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\2635ef5d1f5dc1ac753feb21f019d8e4 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\2635ef5d1f5dc1ac753feb21f019d8e4
79dce17498e1997264346b162b09bde8	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\8515eb34d8f9de5af815466e9715b3e5 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\8515eb34d8f9de5af815466e9715b3e5
3ad5fded9d7fdf1c2f6102f4874b2d52	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\49afcb0bd0c44cd98007157d78e8394a

	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\49afcb0bd0c44cd98007157d78e8394a
fc96a7e27b1d3dab715b2732d5c86f80	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\5cd8f17f4086744065eb0992a09e05a2 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\5cd8f17f4086744065eb0992a09e05a2
60f1b8980d109a556922d5000ae02010	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\1052b8e9071d5b658c32c84c463014f5 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\1052b8e9071d5b658c32c84c463014f5
92ee1fb5df21d8cfafa2b02b6a25bd3b	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\8515eb34d8f9de5af815466e9715b3e5 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\8515eb34d8f9de5af815466e9715b3e5
2164c555f9f23dca54e76b94b1747480	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\8cff24636d2a58810bd5cdc8cb1b8987 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\8cff24636d2a58810bd5cdc8cb1b8987
a98b4c99f64315aac9dd992593830f35	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\8cff24636d2a58810bd5cdc8cb1b8987 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\8cff24636d2a58810bd5cdc8cb1b8987
7e34abdd10c5c763291e69a886452849	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\12ce4e06a81e8d54fd01d9b762f1b1bb HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\12ce4e06a81e8d54fd01d9b762f1b1bb
29daad42dafffab5e0f1f96d620e7392	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\5cd8f17f4086744065eb0992a09e05a2 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\5cd8f17f4086744065eb0992a09e05a2
4168543695513f767ba44997ebd71431	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\5cd8f17f4086744065eb0992a09e05a2 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\5cd8f17f4086744065eb0992a09e05a2
fb671c8735461809534813b818d193f4	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\191530b485fd6f0420e2c6bff7f0dbd7 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\191530b485fd6f0420e2c6bff7f0dbd7
2bf859ea02ae3340cd66eb5e46b1a704	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\5cd8f17f4086744065eb0992a09e05a2 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\5cd8f17f408

	6744065eb0992a09e05a2
24cc5b811a7f9591e7f2cb9a818be104	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\28a9e392f74a71da2b5285754eb1baca HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\28a9e392f74a71da2b5285754eb1baca
11b79281a25da1b798574f667c56898b	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\614ef891df302ed5efa9b06422720faf HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\614ef891df302ed5efa9b06422720faf
2cdbbe5045bed2031a1fc77c3e30e719	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\5cd8f17f4086744065eb0992a09e05a2 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\5cd8f17f4086744065eb0992a09e05a2
f6b4a2be06fc3ba4bb02d1bcbea328fe	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\5cd8f17f4086744065eb0992a09e05a2 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\5cd8f17f4086744065eb0992a09e05a2

The following will present the network traffic observed when different options were selected from the "njRAT" C2 server GUI (YELLOW = Data sent by C2. TURQUOISE = Response from Victim). These artifacts will hopefully assist the research community with generation of network signatures to detect this threat:

- File Manager window

  In this case, the "C:\" directory of the Victim system was browsed and a folder named "njRAT_Directory_Created" was created in it.

  Main network traffic indicators of C2 activity through its "File Manager" window:

  - "**FM|'|'|**"
  - "**nd|'|'|**"
    New directory to be created

FM|'|'|217.66.231.100:1264|'|'|~[endof]~[endof]FM|'|'|217.66.231.100:1264|'|'|!|'|'|QzpcO0ZpeGVk|'|'|QzpcRG9jdW1lbnRzIGFuZCBTZXR0aW5nc1xFeGFtaW5lclxEZXNrdG9wXDs=|'|'|QzpcRG9jdW1lbnRzIGFuZCBTZXR0aW5nc1xFeGFtaW5lclxNeSBEb2N1bWVudHNcOw==|'|'|QzpcRG9jdW1lbnRzIGFuZCBTZXR0aW5nc1xFeGFtaW5lclw7|'|'|QzpcRG9jdW1lbnRzIGFuZCBTZXR0aW5nc1xFeGFtaW5lclxTdGFydCBNZW51XFByb2dyYW1zXFN0YXJ0dXBcOw==|'|'|QzpcUHJvZ3JhbSBGaWxlc1w7|'|'|XDs=|'|'|QzpcV0lORE9XU1w7|'|'|QzpcV0lORE9XU1xzeXN0ZW0zMlw7|'|'|QzpcRG9jdW1lbnRzIGFuZCBTZXR0aW5nc1xFeGFtaW5lclxBcHBsaWNhdGlvbiBEYXRhXDs=|'|'|QzpcRE9DVU1FfjFcRXhhbWluZXJcTE9DQUxTfjFcVGVtcFw7[endof]|'|'|Qzpc[endof]FM|'|'|217.66.231.100:1264|'|'|@|'|'|Qzpc|'|'|RG9jdW1lbnRzIGFuZCBTZXR0aW5ncw==;TGli;TVNPQ2FjaGU=;UERGU3RyZWFtRHVtcGVy;UGVybA==;UHJvZ3JhbSBGaWxlcw==;UHI0aG9uMjU=;UHI0aG9uMjY=;UHI0aG9uMjc=;UkVDWUNMRVI=;UnVieTE5Mw==;U3IzdGVtIFZvbHVtZSBJbmZvcm1hdGlvbg==;dGxz;V0lORE9XUw==;ezkzNjI4OTA2LUE2QUltNENFNC1BQzhCLUI0MkYwRThCRTc5N30=;[endof]@|'|'|Qzpc[endof]

FM|'|'|217.66.231.100:1264|'|'|#|'|'|Qzpc|'|'|LnJuZDsxMDI0;QVVUT0VYRUMuQkFUOzA=;Ym9vdC5pbmk7MjEx;Q09ORklHLlNZUzsw;SU8uU1lTOzA=;TVNET1MuU1lTOzA=;TlRERVRFQ1QuQ09NOzQ3NTY0;bnRsZHI7MjUwMDMy;cGFnZWZpbGUuc3lzOzgwNTMwNjM2OA==;VklSVFBBUlQuREFUOzI1MTY1ODI0;[endof]P[endof]P[endof]P[endof]P[endof]nd|'|'|QzpcbmpSQVRfRGlyZWN0b3J5X0NyZWF0ZWQ=[endof]

217.66.231.100 = Victim's IP.

The following table provides information about some of the encoded data which is files and directories in the folder browsed.

Encoded Data	Decoded Data
QzpcO0ZpeGVk	C:\;Fixed
QzpcRG9jdW1lbnRzIGFuZCBTZXR0aW5nc1xFeGFtaW5lclxEZXNrdG9wXDs=	C:\Documents and Settings\Examiner\Desktop\;
QzpcRG9jdW1lbnRzIGFuZCBTZXR0aW5nc1xFeGFtaW5lclw7	C:\Documents and Settings\Examiner\;
QzpcRG9jdW1lbnRzIGFuZCBTZXR0aW5nc1xFeGFtaW5lclxTdGFydCBNZW51XFByb2dyYW1zXFN0YXJ0dXBcOw==	C:\Documents and Settings\Examiner\Start Menu\Programs\Startup\;
bnRsZHI7MjUwMDMy;cGFnZWZpbGUuc3lzOzgwNTMwNjM2OA==	ntldr;250032
TlRERVRFQ1QuQ09NOzQ3NTY0	NTDETECT.COM;47564
TVNET1MuU1lTOzA=	MSDOS.SYS;0
ezkzNjI4OTA2LUE2QUItNENFNC1BQzhCLUI0MkYwRThCRTc5N30=	{93628906-A6AB-4CE4-AC8B-B42F0E8BE797}
cGFnZWZpbGUuc3lzOzgwNTMwNjM2OA==	pagefile.sys;805306368
QzpcbmpSQVRfRGlyZWN0b3J5X0NyZWF0ZWQ=	**C:\njRAT_Directory_Created**

- Run File -> From Disk window

  Main network traffic indicator of C2 activity through its "RunFile->From Disk" window: "**rn|'|'|**"

P[endof]P[endof]rn|'|'|.exe|'|'|H4sIAAAAAAAAEAO29B2AcSZYlJi9tynt/SvVK1+B0oQiAYBMk2JBAEOzBiM3mkuwdaUcjKasqgcplVmVdZhZAzO2dvPfee++9995777ujudTif33/8/XGZkAWz2zkrayZ4hgKrIHz9+fB8/Ir74qT/p1/i1f41f49f4dej///f//Wv8Gn/XryHP76k/Nz3/G/3/N/ld/p7f5Nf4237sn/9d/65f8/k//7u+mRdNuqqrizpbpNNsuazadJKn
---------- TRUNCATED BY EXAMINER ----------
5S17Md7HuM1Q7/a37Hs/NrYH0I2Moa+JJXr93oJ9xrq33+GrQavkPtn9PfF9zSzDGwu6BVa7Tpf5b+Gn81/X+P3gXI0w+k6O9JEvRrEq8I/EJxNmNfDuA+5p/4fJ/W4H9N4lesH8+oL1DRn++U/uuO+xHTN3ynS+UhGj/9NcB3P0k91BGu/DV+jd+NPdM3PKNYMy/pp88XP/br/E2/Dv/y/9Ln/wHcuiMpAIwAAAA=[endof]bla[endof]act|'|'|QmluVGV4dCAzLjAuMw==[endof]P[endof]P[endof]

In this case, an application called BinText (bintext.exe) was selected in the Attacker's Machine. This application was executed in the Victim's machine. The Victim system responded with the name of the new window opened:

Encoded Data	Decoded Data
QmluVGV4dCAzLjAuMw==	BinText 3.0.3

The other portion of the traffic between the text "TRUNCATED BY THE EXAMINER" is the encoded executable (BinText) uploaded to the Victim system.

- Remote Desktop window

  Main network traffic indicators of C2 activity through its "Remote Desktop" window:
  - "**sc~|'|'|**"
  - "**scPK|'|'|**"

sc~|'|'|217.66.231.100:1264|'|'|1269|'|'|885[endof]!|'|'|217.66.231.100:1306|'|'|1269|'|'|885|'|'|0[endof]**scPK|'|'|**217.66.231
.100:1306|'|'|1269,885|'|'|0,0,/9j/4AAQSkZJRgABAQEAYABgAAD/2wBDABQODxIPDRQSEBIXFRQYHjIhHhwcHj0sLi
QySUBMS0dARkVQWnNiUFVtVkVGZIhlbXd7gYKBTmCNl4x9lnN+gXz/2wBDARUXFx4aHjshITt8U0ZTfHx8fHx8fHx8f
Hx8fHx8fHx8fHx8fHx8fHx8fHx8fHx8fHx8fHx8fHx8fHz/wAARCACxBPUDAS
-- TRUNCATED BY EXAMINER --
pP7Q8P/APPlbf8AfkUXDQ4miu2/tHw9/wA+Vr/35FH9peHv+fO1/wC/IpgcTRXbDUPD7EBbK1JPAAhHNTvLpEZw+lRq
eOttjrRqwOCorvVk0hxldJjYbtmRbfxen1pxOlqSG0dQR1za9KLMDgKK7yebR7XH2nS4oc9PMttufzqD+0vD3/Pna/8Afk
UAcVRXbf2l4e/587X/AL8ik/tLw9/z52v/AH5FAHFUV239o+Hv+fO1/wC/Ipf7Q8Pn/Ixtv+/IpAcRRXb/AG7QP+fG2/78inR3
ehyuEj06B3Y4CrACTRcDhqK7xpdlWMyNpUYQcljbcD8aie+0GPG+wtl3AMMwAZB6GmBxFFdt/aXh7/nztf8AvyKP7S8
Pf8+dr/35FAHE0

- Remote Cam window

  Main network traffic indicators of C2 activity through its "Remote Cam" window:
  - "**CAM|'|'|**"
  - "**USB Video Device[endof]**"

CAM|'|'|192.168.1.100:1260|'|'|~|'|'|**USB Video
Device[endof]**!|'|'|0|'|'|220,160[endof]CAM|'|'|192.168.1.100:1260|'|'|!|'|'|![endof]!|'|'|0|'|'|220,160[endof]CAM|'|'|192.168.1.
100:1260|'|'|!|'|'|![endof]!|'|'|0|'|'|220,160[endof]CAM|'|'|192.168.1.100:1260|'|'|!|'|'|![endof]!|'|'|0|'|'|220,160[endof]CAM|'|'|192
.168.1.100:1260|'|'|!|'|'|![endof]!|'|'|0|'|'|220,160[endof]CAM|'|'|192.168.1.100:1260|'|'|!|'|'|![endof]!|'|'|0|'|'|220,160[endof]CA
M|'|'|192.168.1.100:1260|'|'|!|'|'|![endof]!|'|'|0|'|'|220,160[endof]CAM|'|'|192.168.1.100:1260|'|'|!|'|'|![endof]!|'|'|0|'|'|220,160[en
dof]CAM|'|'|192.168.1.100:1260|'|'|!|'|'|![endof]!|'|'|0|'|'|220,160[endof]CAM|'|'|192.168.1.100:1260|'|'|!|'|'|![endof]!|'|'|0|'|'|220,
160[endof]CAM|'|'|192.168.1.100:1260|'|'|!|'|'|![endof]!|'|'|0|'|'|220,160[endof]CAM|'|'|192.168.1.100:1260|'|'|!|'|'|![endof]!|'|'|0
|'|'|220,160[endof]CAM|'|'|192.168.1.100:1260|'|'|!|'|'|![endof]!|'|'|0|'|'|220,160[endof]CAM|'|'|192.168.1.100:1260|'|'|!|'|'|![end
of]!|'|'|0|'|'|220,160[endof]CAM|'|'|192.168.1.100:1260|'|'|!|'|'|![endof]!|'|'|0|'|'|220,160[endof]CAM|'|'|192.168.1.100:1260|'|'|!|
'|'|![endof]!|'|'|0|'|'|220,160[endof]CAM|'|'|192.168.1.100:1260|'|'|!|'|'|/9j/4AAQSkZJRgABAQEAIQAgAAD/2wBDAAgGBgcG
BQgHBwcJCQgKDBQNDAsLDBkSEw8UHRofHh0aHBwgJC4nICIsIxwcKDcpLDAxNDQ0Hyc5PTgyPC4zNDL/2wBDAQ
kJCQwLDBgNDRgyIRwhMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjL/wAARCACgANwDASIA
AhEBAxEB/8QAHwAAAQUBAQEBAQEAAAAAAAAAAAECAwQFBgcICQoL/8QAtRAAAgEDAwIEAwUFBAQAAAF9AQ

IDAAQRBRIhMUEGE1FhByJxFDKBkaEII0KxwRVS0fAkM2JyggkKFhcYGRolJicoKSo0NTY3ODk6Q0RFRkdISUpTVFV
WV1hZWmNkZWZnaGlqc3R1dnd4eXqDhIWGh4iJipKTlJWWl5iZmqKjpKWmp6ipqrKztLW2t7i5usLDxMXGx8jJytLT1NX
W19jZ2uHi4+Tl5ufo6erx8vP09fb3+Pn6/8QAHwEAAwEBAQEBAQEBAQAAAAAAAAECAwQFBgcICQoL/8QAtREAAgE
CBAQDBAcFBAQAAQJ3AAECAxEEBSExBhJBUQdhcRMiMoEIFEKRobHBCSMzUvAVYnLRChYkNOEl8RcYGRomJy
gpKjU2Nzg5OkNERUZHSElKU1RVVldYWVpjZGVmZ2hpanN0dXZ3eHl6goOEhYaHiImKk
---------- TRUNCATED BY EXAMINER ----------
+FBPy5B5pgJ368DtSYIFLkk9OtHbvmmFxD1pnGelOJ460BSRnP6UAnY//9k=[endof]!|'|'|0|'|'|220,160[endof]

- Remote Shell winodow

  Main network traffic indicator of C2 activity through its "Remote Shell" window: "**rs|'|'|**"

  The following command was executed through the reverse shell: "dir C:\"

rss[endof]rss[endof]**rs**|'|'|TWljcm9zb2Z0IFdpbmRvd3MgWFAgW1ZlcnNpb24gNS4xLjI2MDBd[endof]**rs**|'|'|KEMpIENvcHlyaWdodCAxOTg1LTIwMDEgTWljcm9zb2Z0IENvcnAu[endof]rs|'|'|[endof]P[endof]P[endof]**rs**|'|'|ZGlyIEM6XA==[endof]rs|'|'|QzpcRG9jdW1lbnRzIGFuZCBTZXR0aW5nc1xFeGFtaW5lclxEZXNrdG9wXEdEPmRpciBDOlw=[endof]rs|'|'|IFZvbHVtZSBpbiBkcml2ZSBDIGhhcyBubyBsYWJlbC4=[endof]rs|'|'|IFZvbHVtZSBTZXJpYWwgTnVtYmVyIGlzIEM0MjYtNEVCQg==[endof]rs|'|'|[endof]rs|'|'|IERpcmVjdG9yeSBvZiBDOlw=[endof]rs|'|'|[endof]rs|'|'|MDQvMDIvMjAxMiAgMDM6MjkgUE0gICAgICAgICAgICAgICAgICAgMSwwMjQgLnJuZA==[endof]rs|'|'|MDIvMjcvMjAxMiAgMDk6MTIgQU0gICAgICAgICAgICAgICAgICAgDAgQVVUT0VYRUMuQkFU[endof]rs|'|'|MDIvMjcvMjAxMiAgMDk6MTIgQU0gICAgICAgICAgICAgICAgICAgDAgQ09ORklHLINZUw==[endof]rs|'|'|MDcvMDkvMjAxMiAgMDQ6MjUgUE0gICAgPERJUj4gICAgICAgICAgICAgRG9jdW1lbnRzIGFuZCBTZXR0aW5ncw==[endof]rs|'|'|MDgvMDgvMjAxMiAgMDQ6MjIgUE0gICAgPERJUj4gICAgICAgICAgICAgTGli[endof]rs|'|'|MDQvMDIvMjAxMiAgMDM6MjYgUE0gICAgPERJUj4gICAgICAgICAgICAgUERGU3RyZWFtRHVtcGVy[endof]rs|'|'|MDQvMDIvMjAxMiAgMDM6MzUgUE0gICAgPERJUj4gICAgICAgICAgICAgUGVybA==[endof]rs|'|'|MDYvMDIvMjAxMyAgMTA6NDMgQU0gICAgPERJUj4gICAgICAgICAgICAgUHJvZ3JhbSBGaWxlcw==[endof]rs|'|'|MDgvMDkvMjAxMiAgMDc6MjAgUE0gICAgPERJUj4gICAgICAgICAgICAgUHl0aG9uMjU=[endof]rs|'|'|MDgvMDkvMjAxMiAgMDc6MTkgUE0gICAgPERJUj4gICAgICAgICAgICAgUHl0aG9uMjY=[endof]rs|'|'|MDgvMDkvMjAxMiAgMDc6MTkgUE0gICAgPERJUj4gICAgICAgICAgICAgUHl0aG9uMjc=[endof]rs|'|'|MDgvMTUvMjAxMiAgMDI6MjIgUE0gICAgPERJUj4gICAgICAgICAgICAgUnVieTE5Mw==[endof]rs|'|'|MDQvMTUvMjAxMyAgMDU6NDAgUE0gICAgPERJUj4gICAgICAgICAgICAgdGxz[endof]rs|'|'|MDMvMDYvMjAxMiAgMDE6MzQgUE0gICAgICAgIDI1LDE2NSw4MjQgVklSVFBBUlQuREFU[endof]rs|'|'|MDYvMDIvMjAxMyAgMTA6NDMgQU0gICAgPERJUj4gICAgICAgICAgICAgV0lORE9XUw==[endof]rs|'|'|MDYvMDIvMjAxMyAgMTA6NDMgQU0gICAgPERJUj4gICAgICAgICAgICAgezkzNjI4OTA2LUE2QUItNENFNC1BQzhCLUI0MkYwRThCRTc5N30=[endof]rs|'|'|ICAgICAgICAgICAgICAgICAgNCBGaWxlKHMpICAgICAyNSwxNjYsODQ4IGJ5dGVz[endof]rs|'|'|ICAgICAgICAgICAgICAxMiBEaXlocykgIDI0LDAxMywyMjUsOTg0IGJ5dGVzIGZyZWU=[endof]rs|'|'|[endof]rsc[endof]**rs**|'|'|QzpcRG9jdW1lbnRzIGFuZCBTZXR0aW5nc1xFeGFtaW5lclxEZXNrdG9wXEdEPg==[endof]rsc[endof]

Encoded Data	Decoded Data
TWljcm9zb2Z0IFdpbmRvd3MgWFAgW1ZlcnNpb24gNS4xLjI2MDBd	Microsoft Windows XP [Version 5.1.2600]
KEMpIENvcHlyaWdodCAxOTg1LTIwMDEgTWljcm9zb2Z0IENvcnAu	(C) Copyright 1985-2001 Microsoft Corp.
ZGlyIEM6XA==	**dir C:**
QzpcRG9jdW1lbnRzIGFuZCBTZXR0aW5nc1xFeGFtaW5lclxEZXNrdG9wXEdEPmRpciBDOlw=	C:\Documents and Settings\Examiner\Desktop\GD>dir C:\

IFZvbHVtZSBpbiBkcml2ZSBDIGhhcyBubyBsYWJlbC4=	Volume in drive C has no label.
IFZvbHVtZSBTZXJpYWwgTnVtYmVyIGlzIEM0MjYtNEVCQg==	Volume Serial Number is **C426-4EBB**
IERpcmVjdG9yeSBvZiBDOlw=	Directory of C:\
MDQvMDIvMjAxMiAgMDM6MjkgUE0gICAgICAgICAgICAgMSwwMjQgLnJuZA==	04/02/2012 03:29 PM 1,024 .rnd
MDIvMjcvMjAxMiAgMDk6MTIgQU0gICAgICAgICAgICAgICAgIDAgQVVUT0VYRUMuQkFU	02/27/2012 09:12 AM 0 AUTOEXEC.BAT
MDIvMjcvMjAxMiAgMDk6MTIgQU0gICAgICAgICAgICAgICAgIDAgQ09ORklHLlNZUw==	02/27/2012 09:12 AM 0 CONFIG.SYS

Basically, the response from the directory listing (date, time, file size, and file name) is sent back to the attacker in Base64 encoded format.

- Process Manager window

Main network traffic indicator of C2 activity through its "Process Manager" window:

- Process listing: "**proc|'|'|**"
- Killing a process: "**k|'|'|*[Process_ID]***"

proc|'|'|217.66.231.100:1185|'|'|pid|'|'|2396[endof]~[endof]**proc|'|'|**217.66.231.100:1185|'|'|~|'|'|33[endof]proc|'|'|217.66.231.100:1185|'|'|!|'|'|C:\WINDOWS\system32\svchost.exe,976|'|'|C:\WINDOWS\Explorer.EXE,1804|'|'|C:\Program Files\VMware\VMware Tools\vmacthlp.exe,960|'|'|C:\Program Files\Common Files\Microsoft Shared\VS7DEBUG\MDM.EXE,336|'|'|C:\WINDOWS\System32\svchost.exe,1144|'|'|C:\Program Files\VMware\VMware Tools\TPAutoConnSvc.exe,1492|'|'|**C:\WINDOWS\system32\notepad.exe,1396**|'|'|C:\WINDOWS\system32\lsass.exe,776|'|'|C:\Program Files\VMware\VMware Tools\TPAutoConnect.exe,2560|'|'|C:\DOCUME~1\Examiner\LOCALS~1\Temp\ahbornad.exe,2396|'|'|C:\WINDOWS\system32\notepad.exe,416|'|'|C:\WINDOWS\system32\services.exe,764|'|'|C:\Program Files\VMware\VMware Tools\vmtoolsd.exe,656|'|'|C:\WINDOWS\system32\svchost.exe,160|'|'|C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\WPF\WPFFontCache_v0400.exe,2896|'|'|C:\WINDOWS\system32\svchost.exe,1024|'|'|C:\WINDOWS\system32\cmd.exe,540|'|'|C:\WINDOWS\system32\smss.exe,572|'|'|C:\WINDOWS\system32\wscntfy.exe,2264|'|'|C:\WINDOWS\system32\ctfmon.exe,1992|'|'|C:\Program Files\Symantec\Norton Ghost 2003\GhostStartTrayApp.exe,1904|'|'|C:\WINDOWS\system32\spoolsv.exe,1544|'|'|C:\Program Files\VMware\VMware Tools\vmtoolsd.exe,1896|'|'|C:\Program Files\Symantec\Norton Ghost 2003\GhostStartService.exe,300|'|'|C:\WINDOWS\system32\svchost.exe,1316|'|'|C:\Program Files\VMware\VMware Tools\VMwareTray.exe,1888|'|'|\??\C:\WINDOWS\system32\csrss.exe,640|'|'|C:\WINDOWS\system32\rundll32.exe,1880|'|'|\??\C:\WINDOWS\system32\winlogon.exe,720|'|'|System,4|'|'|Idle,0|'|'|C:\WINDOWS\system32\svchost.exe,1252|'|'|C:\WINDOWS\System32\alg.exe,1872[endof]P[endof]P[endof]**k|'|'|1396**[endof]proc|'|'|217.66.231.100:1185|'|'|**RM|'|'|1396**[endof]

In the above case, the Process Listing window opened in the Attacker's VM was used to kill a process in the Victim VM. Process information:

- Process path: **C:\WINDOWS\system32\notepad.exe**
- Process ID: **1396**

- Registry window

  In this case, the Registry window opened in the Attacker's VM was used to browse to the 'HKLM\Software\Microsost\Windows\CurrentVersion\Run' location in the victim system.

  Main network traffic indicator of C2 activity through its "Registry" window: "**RG|'|'|~|'|'|**"

P[endof]P[endof]RG|'|'|~|'|'|HKEY_LOCAL_MACHINE\[endof]RG|'|'|~|'|'|HKEY_LOCAL_MACHINE\|'|'|HARDWARE|'|'|SAM|'|'|SECURITY|'|'|SOFTWARE|'|'|SYSTEM|'|'|[endof]RG|'|'|~|'|'|HKEY_LOCAL_MACHINE\SOFTWARE\[endof]RG|'|'|~|'|'|HKEY_LOCAL_MACHINE\SOFTWARE\|'|'|7-Zip|'|'|ActiveState|'|'|Adobe|'|'|AT&T Research Labs|'|'|C07ft5Y|'|'|Classes|'|'|Clients|'|'|Cygwin|'|'|Gemplus|'|'|Immunity Inc|'|'|JetBrains|'|'|L&H|'|'|Macromedia|'|'|Microsoft|'|'|MozillaPlugins|'|'|Notepad++|'|'|NSIS_stunnel|'|'|ODBC|'|'|oreas|'|'|Perl|'|'|Policies|'|'|Program Groups|'|'|Python|'|'|Red Gate|'|'|RegisteredApplications|'|'|RubyInstaller|'|'|Schlumberger|'|'|Secure|'|'|Symantec|'|'|ThinPrint|'|'|VMware, Inc.|'|'|Windows 3.1 Migration Status|'|'|WinPcap|'|'|{167F5D73-87FF-4f15-8EBD-C502337D7B34}|'|'|[endof]RG|'|'|~|'|'|HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\[endof]RG|'|'|~|'|'|HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\|'|'|.NETFramework|'|'|Active Setup|'|'|AD7Metrics|'|'|ADs|'|'|Advanced INF Setup|'|'|ALG|'|'|ASP.NET|'|'|AudioCompressionManager|'|'|BidInterface|'|'|COM3|'|'|Command Processor|'|'|Conferencing|'|'|Cryptography|'|'|CTF|'|'|DataAccess|'|'|DataFactory|'|'|DevDiv|'|'|DeviceManager|'|'|Dfrg|'|'|Direct3D|'|'|DirectDraw|'|'|DirectInput|'|'|DirectMusic|'|'|DirectPlay|'|'|DirectPlay8|'|'|DirectPlayNATHelp|'|'|DirectX|'|'|Driver Signing|'|'|DRM|'|'|DrWatson|'|'|EAPOL|'|'|EnterpriseCertificates|'|'|ESENT|'|'|EventSystem|'|'|Exchange|'|'|Fusion|'|'|HTMLHelp|'|'|IE Setup|'|'|IE4|'|'|Ieak|'|'|IMAPI|'|'|IMEJP|'|'|IMEKR|'|'|IMEMIP|'|'|Intelligent Search|'|'|Internet Account Manager|'|'|Internet Connection Wizard|'|'|Internet Domains|'|'|Internet Explorer|'|'|IPSec|'|'|Jet|'|'|Machine Debug Manager|'|'|MediaPlayer|'|'|MessengerService|'|'|Microsoft Reference|'|'|MM20|'|'|MMC|'|'|MMCIsForIE|'|'|Mobile|'|'|Mr. Enigma|'|'|MSBuild|'|'|MSDAIPP|'|'|MSDTC|'|'|MSLicensing|'|'|MSMQ|'|'|MSNInstaller|'|'|MSOSOAP|'|'|MSXML 6.0 Parser and SDK|'|'|MSXML60|'|'|Multimedia|'|'|NET Framework AU|'|'|NET Framework Setup|'|'|NetDDE|'|'|NetSh|'|'|NetShow|'|'|Non-Driver Signing|'|'|ODBC|'|'|Office|'|'|Ole|'|'|Outlook Express|'|'|PCHealth|'|'|Ras|'|'|RAS AutoDial|'|'|Remote Desktop|'|'|Router|'|'|Rpc|'|'|Schedule+|'|'|SchedulingAgent|'|'|Secure|'|'|Security Center|'|'|Shared|'|'|Shared Tools|'|'|Shared Tools Location|'|'|SmartCard|'|'|Speech|'|'|SQMClient|'|'|SystemCertificates|'|'|Tcpip|'|'|TelnetServer|'|'|Terminal Server Client|'|'|TIP Shared|'|'|Tracing|'|'|Transaction Server|'|'|TShoot|'|'|Tuning Spaces|'|'|Updates|'|'|UPnP Device Host|'|'|VBA|'|'|VisualStudio|'|'|WAB|'|'|WBEM|'|'|Web Folders|'|'|Web Service Providers|'|'|Windows|'|'|Windows Imaging Component|'|'|Windows Media Device Manager|'|'|Windows Messaging Subsystem|'|'|Windows NT|'|'|Windows Script Host|'|'|Windows Scripting Host|'|'|Wisp|'|'|Works|'|'|WSE|'|'|WZCSVC|'|'|[endof]P[endof]P[endof]RG|'|'|~|'|'|HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\[endof]RG|'|'|~|'|'|HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\|'|'|CurrentVersion|'|'|Help|'|'|HTML Help|'|'|ITStorage|'|'|Shell|'|'|Windows Error Reporting|'|'|[endof]RG|'|'|~|'|'|HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\[endof]RG|'|'|~|'|'|HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\|'|'|App Management|'|'|App Paths|'|'|Applets|'|'|Control Panel|'|'|Controls Folder|'|'|CSCSettings|'|'|DateTime|'|'|Dynamic Directory|'|'|Explorer|'|'|Extensions|'|'|Group Policy|'|'|H323TSP|'|'|Hints|'|'|IME|'|'|Installer|'|'|Internet Settings|'|'|IntlRun|'|'|IPConfTSP|'|'|MS-DOS Emulation|'|'|Nls|'|'|OptimalLayout|'|'|PhotoPropertyHandler|'|'|policies|'|'|PreviewHandlers|'|'|PropertySystem|'|'|Reinstall|'|'|Reliability|'|'|Run|'|'|RunOnce|'|'|RunOnceEx|'|'|Setup|'|'|SharedDlls|'|'|Shell Extensions|'|'|ShellCompatibility|'|'|ShellScrap|'|'|ShellServiceObjectDelayLoad|'|'|SideBySide|'|'|SMDEn|'|'|StillImage|'|'|Syncmgr|'|'|Telephony|'|'|ThemeManager|'|'|Themes|'|'|Uninstall|'|'|URL|'|'|WebCheck|'|'|WindowsUpdate|'|'|DevicePath/ExpandString/C:\WINDOWS\inf|'|'|MediaPathUnexpanded/ExpandString/C:\WINDOWS\Media|'|'|SM_GamesName/String/Games|'|'|SM_ConfigureProgramsName/String/Set Program Access and Defaults|'|'|ProgramFilesDir/String/C:\Program Files|'|'|CommonFilesDir/String/C:\Program Files\Common Files|'|'|ProductId/String/76487-018-7438105-22214|'|'|WallPaperDir/ExpandString/C:\WINDOWS\Web\Wallpaper|'|'|MediaPath/String/C:\WINDOWS\Media|'|'|ProgramFilesPath/ExpandString/C:\Program Files|'|'|SM_AccessoriesName/String/Accessories|'|'|PF_AccessoriesName/String/Accessories|'|'|[endof]RG|'|'|~|'|'|HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\[endof]RG|'|'|~|'|'|HKEY_LOCAL_MACHIN

E\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\|'|'|OptionalComponents|'|'|BluetoothAuthenticationAgent/String/rundll32.exe bthprops.cpl,,BluetoothAuthenticationAgent|'|'|VMware Tools/String/"C:\Program Files\VMware\VMware Tools\VMwareTray.exe"|'|'|VMware User Process/String/"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr|'|'|GhostStartTrayApp/String/C:\Program Files\Symantec\Norton Ghost 2003\GhostStartTrayApp.exe|'|'|IMJPMIG8.1/String/"C:\WINDOWS\IME\imjp8_1\IMJPMIG.EXE" /Spoil /RemAdvDef /Migration32|'|'|IMEKRMIG6.1/String/C:\WINDOWS\ime\imkr6_1\IMEKRMIG.EXE|'|'|MSPY2002/String/C:\WINDOWS\system32\IME\PINTLGNT\ImScInst.exe /SYNC|'|'|PHIME2002ASync/String/C:\WINDOWS\system32\IME\TINTLGNT\TINTSETP.EXE /SYNC|'|'|PHIME2002A/String/C:\WINDOWS\system32\IME\TINTLGNT\TINTSETP.EXE /IMEName|'|'|Adobe Reader Speed Launcher/String/"C:\Program Files\Adobe\Reader 9.0\Reader\Reader_sl.exe"|'|'|**0954e473c171a53f80142346107acfb3/String/"C:\Documents and Settings\Examiner\Local Settings\Temp\ahbornad.exe" ..**|'|'|[endof]P[endof]P[endof]P[endof]P[endof]

- Keylogger window

  Main network traffic indicator of C2 activity through its "Keylogger" window: "**kl|'|'|**"

kl[endof]kl|'|'|DQoBMTMvMDYvMDYgV0lOV09SRCBEb2N1bWVudDEgLSBNaWNyb3NvZnQgV29yZAENCkhlbGxvIFdvcmxkIQ0KATEzLzA2LzA2IFdJTldPUkQgRG9jdW1lbnQxIC0gTWljcm9zb2Z0IFdvcmQBDQp0ZXN0DQoBMTMvMDYvMDYgbm90ZXBhZCBVbnRpdGxlZCAtIE5vdGVwYWQBDQpFeHBsb3JlciBwYXNzd29yZDogMTIzNDU1W0JhY2tdNg0KATEzLzA2LzA2IG5vdGVwYWQgVW50aXRsZWQgLSBOb3RlcGFkAQ0KYXNkZmQ=[endof]P[endof]P[endof]

The encoded data sent by the Victim system was the keystrokes collected into the keylogger file in the Victim. The data decodes to:

Encoded Data	Decoded Data
DQoBMTMvMDYvMDYgV0lOV09SRCBEb2N1bWVudDEgLSBNaWNyb3NvZnQgV29yZAENCkhlbGxvIFdvcmxkIQ0KATEzLzA2LzA2IFdJTldPUkQgRG9jdW1lbnQxIC0gTWljcm9zb2Z0IFdvcmQBDQp0ZXN0DQoBMTMvMDYvMDYgbm90ZXBhZCBVbnRpdGxlZCAtIE5vdGVwYWQBDQpFeHBsb3JlciBwYXNzd29yZDogMTIzNDU1W0JhY2tdNg0KATEzLzA2LzA2IG5vdGVwYWQgVW50aXRsZWQgLSBOb3RlcGFkAQ0KYXNkZmQ=	13/06/06 WINWORD Document1 - Microsoft WordHello World! 13/06/06 WINWORD Document1 - Microsoft Word test 13/06/06 notepad Untitled - Notepad Explorer password: 123455[Back]6 13/06/06 notepad Untitled - Notepad asdfd

- Get Passwords window

  Main potential network traffic indicators of C2 activity through its "Get Passwords" window:
  - "**ret**|'|'|"
  - "**pl**|'|'|"

```
ret|'|'|682dfec8c66a0de6f1475ca73c462a69|'|'|([endof]bla[endof]pl|'|'|682dfec8c66a0de6f1475ca73c462a69|'|'|0[endo
f]ret|'|'|682dfec8c66a0de6f1475ca73c462a69|'|'|KiAqICogKiAqICogKiAqICogKiA=[endof]
```

The Fidelis Take

Fidelis XPS sensors detect the "njRAT" malware variants and domains observed throughout this report.

Fidelis XPS sensors detected the NJC242.exe/njRAT malware as "Trojan.Win32.Jorik.Agent.rkp". Fidelis XPS is capable of detecting this threat regardless of delivery method employed by the Threat Actors responsible. Fidelis XPS can detect and alert on executables such as the "njRAT" malware multiple layers deep inside of archive files (i.e. ZIP), or even XOR'ed inside of a weaponized MS Office document or Adobe PDF File. The Fidelis Threat Research and Network Forensics and Incident Response teams will continue to actively monitor the ever-evolving threat landscape for the latest threats to our customers' network security.