

# Lotus Blossom Continues ASEAN Targeting

[community.rsa.com/community/products/netwitness/blog/2018/02/13/lotus-blossom-continues-asean-targeting](https://community.rsa.com/community/products/netwitness/blog/2018/02/13/lotus-blossom-continues-asean-targeting)

During the last weeks of January (2018), nation state actors from Lotus Blossom conducted a targeted malspam campaign against the Association of Southeast Asian Nations (ASEAN) countries. Just months after the APT32 watering hole activity against ASEAN-related websites was observed in Fall 2017, this new activity clearly indicates the association (ASEAN) clearly remains a priority collection target in the region. This new Lotus Blossom 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 [Compatibility Mode] - Microsoft Word

Table Tools

Page Layout References Mailings Review View Design Layout

Font Paragraph Styles

**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 Saifuddin 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 Ithram 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. Lt. Gen. Chansomone Chanyalath Minister of National Defence	BO Khamsy Vongkhamsoo Permanent Secretary of Defence Ministry of National Defence	Lt. Col. Phavyvanh Chamthaphomma Deputy Director-General of Foreign Relations Department Ministry of National Defence Fax: 856 21 911 728
		Y.Bhg. Dato Sri Abdul Rahim bin	Mr. Ahmad Nadari 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 malware, 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 in 'C:\Users\... Documents\admin.doc	Open System Process	explorer.exe	C:\Windows\...	explorer.exe
igss.exe		Open Browser Process	iexplore.exe	C:\Program Files (x86)\Internet Explorer\...	iexplore.exe
iexplore.exe	iexplore.exe	Write to Executable	NavShExt.dll	C:\Users\... AppData\Roaming\Microsoft\Windows\Che...	NavShExt.dll
iexplore.exe	iexplore.exe	Modify Run Key	@{f8e0d...	HKEYS-1-S-21-96073022-276150838-846734840-1110\Software\Microsoft\Windows\CurrentVersion\Run\...	@{f8e0d...
svchost.exe	svchost.exe & netsh	Open Process	EQNEDT32.EXE	C:\Program Files\Common Files\Microsoft Shared\EQUATION\...	EQNEDT32.EXE
svchost.exe	svchost.exe & DcomLaunch	Create Process	EQNEDT32.EXE	C:\Program Files\Common Files\Microsoft Shared\EQUATION\...	EQNEDT32.EXE
WINWORD.EXE	WINWORD.EXE in 'C:\Users\... Documents\admin.doc	Write to Executable	a.b	C:\Users\... \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 & netsh	Open Process	WINWORD.EXE	C:\Program Files\Microsoft Office\Office14\...	WINWORD.EXE
WINWORD.EXE	WINWORD.EXE in 'C:\Users\... Documents\admin.doc	Modify Internet Zone Settings	@{1400}	HKEYS-1-S-21-96073022-276150838-846734840-1110\Software\Microsoft\Windows\CurrentVersion\Internet Set...@1400	@{1400}
WINWORD.EXE	WINWORD.EXE in 'C:\Users\... Documents\admin.doc	Modify Internet Zone Settings	@{1030}	HKEYS-1-S-21-96073022-276150838-846734840-1110\Software\Microsoft\Windows\CurrentVersion\Internet Set...@1030	@{1030}
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	svchost.exe	C:\Windows\System32\...	svchost.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.

The dashboard shows a summary of system processes. A red circle highlights a score of 159. Below the summary is a table of processes:

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	
explorer.exe	10	0	1	Valid: Microsoft Corporation	Good	
incupdate_genuineinet.dll	10	1	2	Valid: Microsoft Windows	-	
dumpfve.sys	9	0	1	Valid: Microsoft Windows	Good	
lsasrv.exe	9	0	1	Valid: Microsoft Windows	Good	
GROOVE.EXE	9	1	1	Valid: Microsoft Corporation	Good	
spoolsv1	9	1	2	Valid: Microsoft Windows	-	
ntlsadm.exe	5	0	1	Valid: Microsoft Windows	Good	
RDPREFMP.sys	3	0	2	Valid: Microsoft Windows	Good	
System.exe	3	0	1	Valid: Microsoft Corporation	Good	

Below the process list is a 'Machine IOCs' table and a 'Tracking' log.

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

The tracking log shows events such as 'Create Process' for 'services.exe', 'Open Process' for 'lsass.exe', and 'Create Process' for 'svchost.exe'.

The 'ADVANCED DETAILS OF PROCESS' window shows the following information for EQNEDT32.EXE (PID: 3174):

- Score:** 100 out of 100 (Malicious)
- Path:** C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
- Parent process:** svchost.exe (PID: 540)
- Exitcode:** 0x00000000
- User:** admin
- MD5:** 5-1-5-21-1902019708-1900728564-155583590-1000
- RL:** MEDIUM

**Timeline:** Created at +2574, Terminated at +2777. Children: 524 instances of 'explorer.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: 88118988

**INDICATORS OF SUSPICIOUS BEHAVIOUR:**

- DANGER:**
  - Application loaded dropped or rewritten executable
  - Equation Editor starts application (CVE-2017-11882)
- WARNING:**
  - Starts Internet Explorer

**EVENTS:** A 'WRITE' event at +2391ms shows a registry change: Key: HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-10\Products\188084189E608904200000000F01FEC\Usage; Name: EquationEditorFilesInt1\_1833; Value: 1278935043.

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

Machines

935 Score Administrative Status: Last Seen Just Now

Show Whitelisted Hide Good Files Hide Valid Signatures

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

File Name	IOC Score	Risk Score (%)	Machine Count	Registry Path
NavShExt.dll	643	58	1	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run @US10D
chmsrv.exe	2	2	2	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components\{B690C445-D564-463c-AFF1-4609C530F96} @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
TPVMon.dll	1	1	1	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Monitors\ThinPrint Print Post Monitor for VMWare @Driver
7-zip.dll	1	1	1	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SP48_Extensions\Approved @{25170F69-40C1-278A-2000-000100020
vsoclib.dll	1	1	1	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog_Entries\00000000013 @P
vsoclib.dll	1	1	1	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog_Entries\00000000012 @P
vsoclib.dll	1	1	1	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog_Entries\00000000011 @P
vsoclib.dll	1	1	1	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order @ProviderOrder
vmhgfs.dll	1	1	1	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog_Entries\00000000013 @P
vsoclib.dll	1	1	1	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog_Entries\00000000013 @P
vsoclib.dll	1	1	1	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog_Entries\00000000012 @P
vmhgfs.dll	1	1	1	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order @ProviderOrder
vsoclib.dll	1	1	1	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog_Entries\00000000013 @P
vsoclib.dll	1	1	1	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog_Entries\00000000012 @P
vmhgfs.dll	1	1	1	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order @ProviderOrder
vsoclib.dll	1	1	1	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog_Entries\00000000013 @P
vsoclib.dll	1	1	1	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog_Entries\00000000012 @P
vmhgfs.dll	1	1	1	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order @ProviderOrder
vsoclib.dll	1	1	1	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog_Entries\00000000013 @P
vsoclib.dll	1	1	1	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog_Entries\00000000012 @P
vmhgfs.dll	1	1	1	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order @ProviderOrder

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

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\	ieplorex.exe	ieplorex.exe	Write to Executable	NavShExt.dll
1/29/2018 7:13:44.772 AM	C:\Program Files\Microsoft Office\Office14\	WINWORD.EXE	WINWORD.EXE /h "C:\Users\..."	Write to Executable	a.b

Machines

935 Score Administrative Status: Last Seen Just Now

Show Whitelisted Hide Good Files Hide Valid Signatures

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

File Name	IOC Score	Risk Score (%)	Signature	Machine Count	Hash Lock...	Downloaded	Full Path
NavShExt.dll	643	58	Not signed	1	-	<input checked="" type="checkbox"/>	C:\Users\...AppData\Roaming\Microsoft\Windows\Caches\NavShExt...
n.3	643	58	Not signed	1	-	<input checked="" type="checkbox"/>	C:\Users\...AppData\Local\h.3
(FLOATING CODE)	128	1	Not signed	0	-	<input type="checkbox"/>	(FLOATING CODE)
EQUEDT52.EXE	128	0	Valid: Microsoft Cooperat...	1	Good	<input type="checkbox"/>	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQUEDT52.EXE
ieabs.exe	12	0	Valid: Microsoft Windows	1	Good	<input type="checkbox"/>	C:\Windows\System32\ieabs.exe
ievhst.exe	12	0	Valid: Microsoft Windows	2	Good	<input type="checkbox"/>	C:\Windows\System32\ievhst.exe
ieplorex.exe	10	0	Valid: Microsoft Cooperat...	1	Good	<input type="checkbox"/>	C:\Program Files (x86)\Internet Explorer\ieplorex.exe
incupdate_GenuineIntel.dll	10	1	Valid: Microsoft Windows	2	-	<input type="checkbox"/>	C:\Windows\System32\incupdate_GenuineIntel.dll
dumpfve.sys	9	0	Valid: Microsoft Windows	1	Good	<input type="checkbox"/>	C:\Windows\System32\drivers\dumpfve.sys
lsservice.exe	9	0	Valid: Microsoft Windows	1	Good	<input type="checkbox"/>	C:\Windows\System32\lsservice.exe
GROOVE.EXE	9	1	Valid: Microsoft Cooperat...	1	Good	<input type="checkbox"/>	C:\Program Files\Microsoft Office\Office14\GROOVE.EXE
ntoskrnl.exe	5	0	Valid: Microsoft Windows	1	Good	<input type="checkbox"/>	C:\Windows\System32\ntoskrnl.exe
RDPREMP.sys	3	0	Valid: Microsoft Windows	2	Good	<input type="checkbox"/>	C:\Windows\System32\drivers\RDPREMP.sys
System.exe	3	0	Valid: Microsoft Cooperat...	1	Good	<input type="checkbox"/>	C:\Windows\System.exe
PEAuth.sys	3	0	Valid: Microsoft Windows	1	Good	<input type="checkbox"/>	C:\Windows\System32\drivers\PEAuth.sys
CompatTelRunner.exe	3	0	Valid: Microsoft Windows	1	Good	<input type="checkbox"/>	C:\Windows\System32\CompatTelRunner.exe
tenices.exe	3	0	Valid: Microsoft Windows	2	Good	<input type="checkbox"/>	C:\Windows\System32\tenices.exe

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

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\	ieplorex.exe	ieplorex.exe	Write to Executable	NavShExt.dll
1/29/2018 7:13:44.772 AM	C:\Program Files\Microsoft Office\Office14\	WINWORD.EXE	WINWORD.EXE /h "C:\Users\..."	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

Source: registry

First seen: +2516ms

**danger**

## 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\Roaming\Microsoft\Windows\Caches\NavShExt.dll,Setting
time:     +2516ms

```



Close

> C:\Users\admin\AppData\Local\Microsoft\Windows\Explorer\thumbcache\_1CD60.db

Download

⚠ Dropped from process

Mime: application/octet-stream

🔍 Look up on [VirusTotal](#)

Size: 617.00 b

### TrID - File Identifier

TYPE UNKNOWN

### Hashes

MDS  03C3522B1A7DFB3054ACBF3CCF79CFA6  
 SHA1  CD4E3B08CAF0C97B0769B3AB80CBAC75F8AF1212  
 SHA256  D98418834B021D7F25169FF246836AD3A113B2BF32EBC9D00A8465F6FF416F29  
 SSDEEP  12 :S+C/7+T50TxIv2LxGKdhIF083dG0v7Wxjyy/Aqz/kH2R3msR0fbd :S970/LtdhuA3w0v7Aev4/M2R3g

### HEX

```

00000000 : 60 59 A0 AC 23 59 FF 66 75 C8 F4 9D 42 A0 01 B9
00000010 : A6 E4 85 96 05 C2 7B 54 32 61 07 22 41 3E 0E 6F
00000020 : C0 54 46 7C 90 B1 C5 48 6E 90 97 16 0E 85 D1 3F
00000030 : 76 8F 39 E5 59 32 89 F5 E3 81 55 40 1E 5B 08 61
00000040 : C8 F0 0C D6 D1 2D 9F BC 89 06 D3 61 15 BA 98 07
00000050 : 8E C1 65 BF BA ED 82 D3 CB 39 16 2B 80 4A E2 0B
00000060 : 03 82 69 7B 85 8E 5B 54 40 DD 3B 5A 7F A0 97 F2
00000070 : D3 A6 C7 B2 5D 14 9A C3 59 4A 60 AE B6 8E 45 34
00000080 : E8 3E 96 70 B5 F8 2E 4E 8B 51 B5 18 81 EB 07 00
00000090 : A3 0B DE 08 77 62 20 1C 14 37 CD EB B8 88 59 BD
000000A0 : E2 3A AD 3C 11 B7 8A FA F6 96 CF 4B 42 3C 2A 32
000000B0 : 81 FD E4 CB D7 90 E9 CF 1D C0 2F FB 10 47 A3 D3
000000C0 : 9A 2A BD 16 3C 56 32 B7 6A BD 82 14 5F 68 8E 94
000000D0 : EB 4C 7A 85 86 AC B5 26 20 EB 74 05 51 86 DC C1
000000E0 : F7 09 C3 00 0D 77 09 E7 A2 AA 93 69 29 87 AC FC
000000F0 : 5B DE D4 0A 4C 65 32 B6 08 B3 3B 79 D4 9B 34 FC

```

```

`Y.-#YÿfuÊð.B..¹
|ä...Ä{T2a."A>.o
ÀTF|.±ÄHn....Ñ?
v.9âY2.õã.U@.[.a
Ëð.ÖÑ-.%..Óa.º..
.Áe¿ºí.ÓÉ9.+Já.
..i{.[T@Ý;Z..ò
Ó|Ç²]. .ÄYJ`ø¶.E4
è>.pμø.N.Qμ..ë..
£.b.wb ..7Íë_.Y%
â:.<..úö.İKB<*2
.yäËx.éİ.À/0.G£Ó
.*½.<V2.j%.._h..
ëlZ..~μ& ët.Q.ÜÁ
÷.Ä..w.ççª.i).~ü
[þÖ.Le2¶.ª;yÖ.4ü

```





alias.host = 'pdhl.info'

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

- 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)
  - tid 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.

```

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;
}

```

After our Elise infection had run for about a day, we were visited by the threat actor. While it's unclear exactly what the actor may have been looking for, our infected (sandboxed) machine was not it and the backdoor was deleted.

```
+ System
- EventData
  UtcTime      2018-01-30 00:11:20.033
  ProcessGuid  {ABD1D68A-B828-5A6F-0000-001019274000}
  ProcessId    1480
  Image        C:\Windows\SysWOW64\cmd.exe
  CommandLine  "C:\Windows\system32\cmd.exe" /c del C:\Users\██████████\AppData\Roaming\MICROS~1
              \Windows\Caches\NavShExt.dll > nul
  CurrentDirectory C:\Windows\system32\
  User         ████████████████████
  LogonGuid    {ABD1D68A-6869-5A6F-0000-0020BC7C0F00}
  LogonId      0xf7cbc
  TerminalSessionId 1
  IntegrityLevel Medium
  Hashes       SHA1=EE8CBF12D87C4D388F09B4F69BED2E91682920B5
  ParentProcessGuid {ABD1D68A-686A-5A6F-0000-0010DA051000}
```

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): d3fc69a9f2ae2c446434abfbfe1693ef0f81a5da0a7f39d27c80d85f4a49c411
- NavShExt.dll (SHA256): 6dc2a49d58dc568944fef8285ad7a03b772b9bdf1fe4bddff3f1ade3862eae79