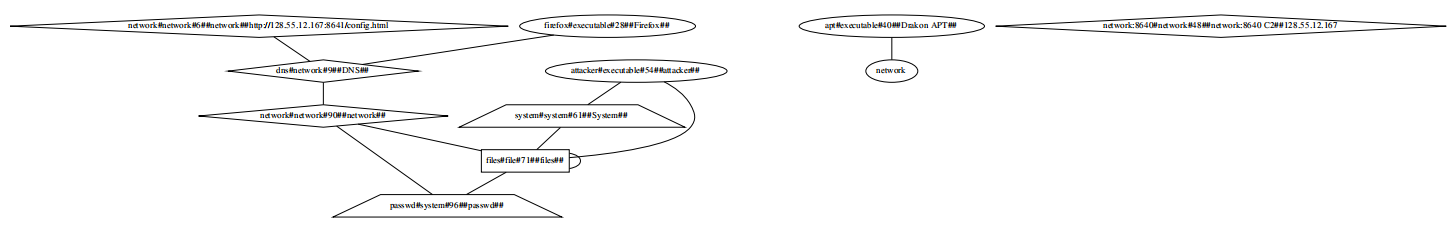
# 3. Firefox DNS Drakon APT

The attack started by browsing to *http://128.55.12.167:8641/config.html*, selecting DNS, entering hostname *Xx--ls8h.com*, file 938527054, and clicking the Visit button. This triggered the Firefox backdoor to connect out via DNS to *XX--ls8h.com*. Drakon APT was downloaded and executed and connected to *128.55.12.167:8640* for C2. The attacker escalated privileges using the new File System Filter Driver, which looks for processes opening specific files which don’t exist and elevates them. Once SYSTEM, the attacker exfil’ed the host and network files as well as a passwd file in the home directory.

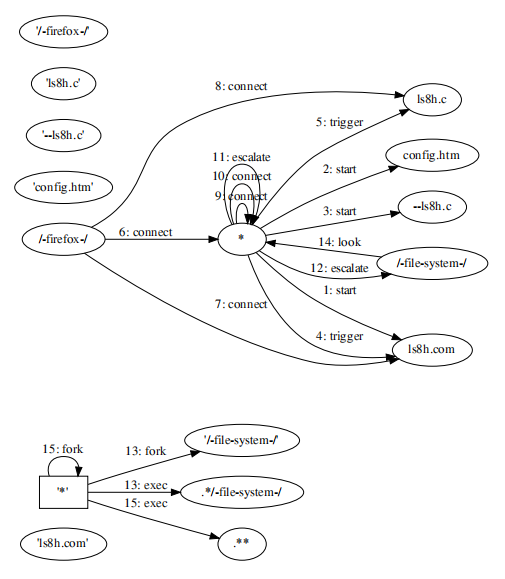
1. T1003 - OS Credential Dumping
2. T1005 - Data from Local System
3. T1059 - Command and Scripting Interpreter (8),
4. T1105 - Ingress Tool Transfer,
5. T1566 - Phsihing (T1189 - Drive-by-Compromise),
6. T1204 - User Execution,
7. T1041 - Exfiltration Over C2 Channel (T1071 - Application Layer Protocol, T1573 - Encrypted Channel (2))
8. T1218 - Signed Binary Proxy Execution (11)
9. {'T1003': ['files#file#71', 'attacker#executable#54', 'passwd#system#96', 'network#network#90'], - OS Credential Dumping (8)
10. 'T1005': ['attacker#executable#54', 'files#file#71', 'passwd#system#96', 'network#network#90', - Data from Local System'network#network#90'],
11. 'T1041': ['attacker#executable#54', 'network#network#90', 'files#file#71', 'files#file#71', 'passwd#system#96'],
12. 'T1059': ['attacker#executable#54', 'passwd#system#96', 'passwd#system#96', 'files#file#71', 'network#network#90', 'files#file#71'],
13. 'T1070': ['attacker#executable#54', 'passwd#system#96', 'network#network#90', 'files#file#71'], - Indicator Removal on Host (6)
14. 'T1071': ['attacker#executable#54', 'network#network#90', 'network#network#90', 'files#file#71'],
15. 'T1082': ['attacker#executable#54', 'passwd#system#96', 'files#file#71', 'network#network#90'], - System Information Discovery
16. 'T1083': ['files#file#71', 'attacker#executable#54', 'network#network#90', 'passwd#system#96', 'network#network#90'], - File and Directory Discovery
17. 'T1105': ['files#file#71', 'network#network#90', 'attacker#executable#54', 'passwd#system#96'],
18. 'T1106': ['files#file#71', 'attacker#executable#54', 'attacker#executable#54', 'passwd#system#96'], - Native API
19. 'T1204': ['attacker#executable#54', 'network#network#90', 'files#file#71'],
20. 'T1218': ['attacker#executable#54', 'files#file#71', 'passwd#system#96'],
21. 'T1550': ['attacker#executable#54', 'files#file#71', 'network#network#90'], - Use Alternate Authentication Material
22. 'T1566': ['network#network#90', 'files#file#71', 'attacker#executable#54', 'files#file#71'],
23. 'T1571': ['attacker#executable#54', 'network#network#90', 'files#file#71'],
24. 'T1573': ['attacker#executable#54', 'network#network#90', 'files#file#71']}



TTPDrill

T1151 (T1036/006 - Masquerading: Space after Filename), T1023 (T1547/009 - Boot or Logon Autostart Execution: Shortcut Modification), T1497 - Virtualization/Sandbox Evasion, T1055 -Process Injection , T1138 (T1546/011 - Event Triggered Execution: Application Shimming), T1184(T1563/001 - Remote Service Session Hijacking: SSH Hijacking), T1076(T1021/001 - Remote Services: Remote Desktop Protocol), T1177(T1547/008 - Boot or Logon Autostart Execution: LSASS Driver), T1192(T1566/002 - Phishing: Spearphishing Link), T1090 - Proxy, T1086(T1059/001 - Command and Scripting Interpreter: PowerShell), T1132 - Data Encoding, T1139(T1552/003 -Unsecured Credentials: Bash History), T1014 - Tootkit, T1145(T1552/004 - Unsecured Credentials: Private Keys), T1083 - File and Directory Discovery, T1005 - Data from Local System, T1158(T1564/001 -Hide Artifacts: Hidden Files and Directories), T1145(T1552/004 - Unsecured Credentials: Private Keys)

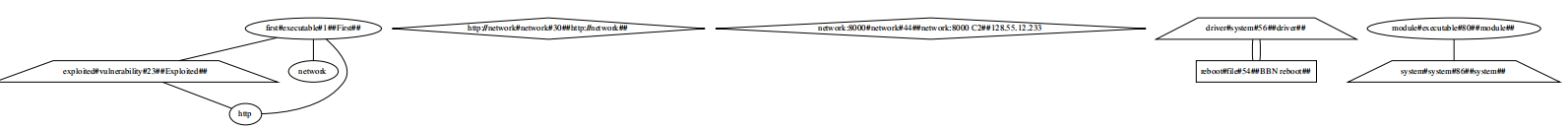
1. T1151(T1036/006) - Masquerading: Space after Filename)
2. T1023(T1547/009) - Boot or Logon Autostart Execution: Shortcut Modification)
3. T1497 - Virtualization/Sandbox Evasion
4. T1055 -Process Injection
5. T1138(T1546/011) - Event Triggered Execution: Application Shimming)
6. T1184(T1563/001) - Remote Service Session Hijacking: SSH Hijacking)
7. T1076(T1021/001) - Remote Services: Remote Desktop Protocol)
8. T1177(T1547/008) - Boot or Logon Autostart Execution: LSASS Driver)
9. T1192(T1566/002) - Phishing: Spearphishing Link)
10. T1090 - Proxy
11. T1086(T1059/001) - Command and Scripting Interpreter: PowerShell)
12. T1132 - Data Encoding
13. T1139(T1552/003 -Unsecured Credentials: Bash History)
14. T1014 - Tootkit
15. T1145(T1552/004) - Unsecured Credentials: Private Keys)
16. T1083 - File and Directory Discovery
17. T1005 - Data from Local System
18. T1158(T1564/001 -Hide Artifacts: Hidden Files and Directories)
19. T1145(T1552/004) - Unsecured Credentials: Private Keys)



# 4. Firefox Drakon APT Elevate Copykatz

First attacked ta51-pivot-2 and deployed OC2, allowing us to run our attack from within the target network. Exploited Firefox backdoor by again browsing to *http://128.55.12.233*. Loader Drakon was executed in Firefox memory and connected out to *128.55.12.233:8000* and *128.55.12.233:443* for C2. After the BBN reboot, driver was disabled, and we would now be able to use privilege escalation via our perfmon driver. We loaded the copykatz module to recon data from the system.

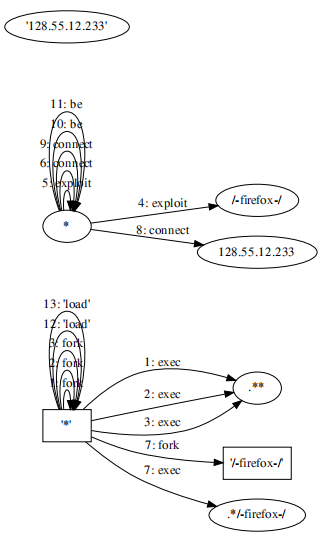
1. T1189 - Drive-by-Compromise
2. Command & Control
3. T1082 - System Information Discovery (1.86)
4. {'T1059': ['firefox#executable#38', 'exploited#vulnerability#23', 'network:443#network#46'],
5. 'T1071': ['firefox#executable#38', 'network:443#network#46', 'http://network#network#30', 'exploited#vulnerability#23'],
6. 'T1566': ['http://network#network#30', 'firefox#executable#38', 'exploited#vulnerability#23'],
7. 'T1573': ['firefox#executable#38', 'network:443#network#46']}



TTPDrill

T1017, T1055, T1201, T1134, T1138, T1068, T1212, T1204, T1003, T1186, T1181, T1177, T1014, T1206, T1050, T1175, T1055, T1215, T1013, T1117

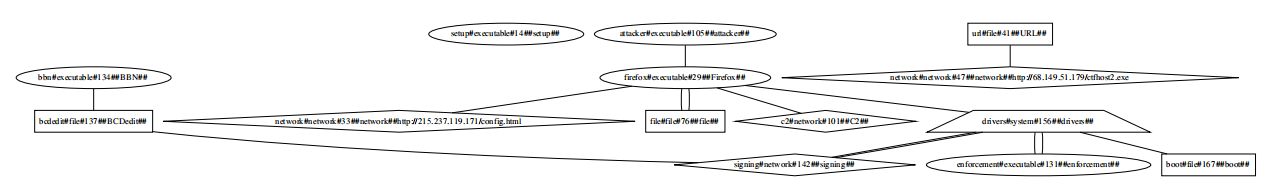
1. T1003
2. T1013(T1547/010) - Boot or Logon Autostart Execution: Port Monitors
3. T1014
4. T1017(T1072) - Software Deployment Tools
5. T1050(T1543/003) - Create or Modify System Process: Windows Service
6. T1055
7. T1068 - Exploitation for Privilege Escalation
8. T1117(T1218/010)
9. T1134 - Access Token Manipulation
10. T1138
11. T1175(1021/003, T1559/001) - Component Object Model and Distributed COM
12. T1177
13. T1181(T1055/011) - Process Injection: Extra Window Memory Injection
14. T1186(T1055/013) - Process Injection: Process Doppelgänging
15. T1201 - Password Policy Discovery
16. T1204 - User Execution
17. T1206(T1548/003) - Abuse Elevation Control Mechanism: Sudo and Sudo Caching
18. T1212 - Exploitation for Credential Access
19. T1215(T1547/006) - Boot or Logon Autostart Execution: Kernel Modules and Extensions



# 5. Firefox BITS Micro APT

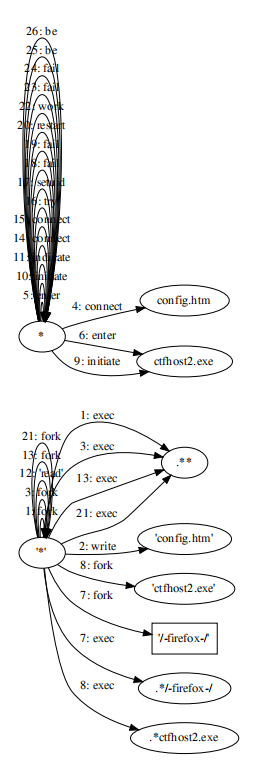
Benign activity ran for most of the morning while the tools were being setup for the day. The activity was modified so the hosts would open Firefox and browse to *http://215.237.119.171/config.html*. The simulated host then entered URL for BITS Micro APT as *http://68.149.51.179/ctfhost2.exe*. We used the exploited Firefox backdoor to initiate download of *ctfhost2.exe* via the Background Intelligent Transfer Service (BITS). Our server indicated the file was successfully downloaded using the BITS protocol, and soon after Micro APT was executed on the target and connected out to *113.165.213.253:80* for C2. The attacker tried to elevate using a few different drivers, but it failed once again due to the computer having been restarted without disabling driver signature enforcement. BBN tried using BCDedit to permanently disable driver signing, but it did not seem to work during the engagement as the drivers failed to work unless driver signing was explicitly disabled during boot.

1. T1189 - Drive-by-Compromise (T1566 - Phishing)
2. T1105 - Ingress Tool Transfer
3. T1218 - Signed Binary Proxy Execution (11)
4. Command & Control
5. {'T1041': ['firefox#executable#54', 'signing#network#142', 'bcdedit#file#137', 'bcdedit#file#137', 'driver#system#129'],
6. 'T1053': ['firefox#executable#54', 'driver#system#129', 'signing#network#142', 'bcdedit#file#137'],
7. 'T1059': ['firefox#executable#54', 'driver#system#129', 'driver#system#129', 'bcdedit#file#137', 'signing#network#142', 'bcdedit#file#137'],
8. 'T1071': ['firefox#executable#54', 'signing#network#142', 'signing#network#142', 'bcdedit#file#137'],
9. 'T1082': ['firefox#executable#54', 'driver#system#129', 'bcdedit#file#137', 'signing#network#142'],
10. 'T1105': ['bcdedit#file#137', 'signing#network#142', 'firefox#executable#54', 'driver#system#129'],
11. 'T1218': ['firefox#executable#54', 'bcdedit#file#137', 'driver#system#129'],
12. 'T1566': ['signing#network#142', 'bcdedit#file#137', 'firefox#executable#54', 'bcdedit#file#137'],
13. 'T1573': ['firefox#executable#54', 'signing#network#142', 'bcdedit#file#137']}



TTPDrill

T1497, T1207, T1003, T1023, T1155, T1055, T1195, T1046, T1117, T1197, T1138, T1015, T1186, T1077, T1086, T1192, T1177, T1014, T1089, T1206



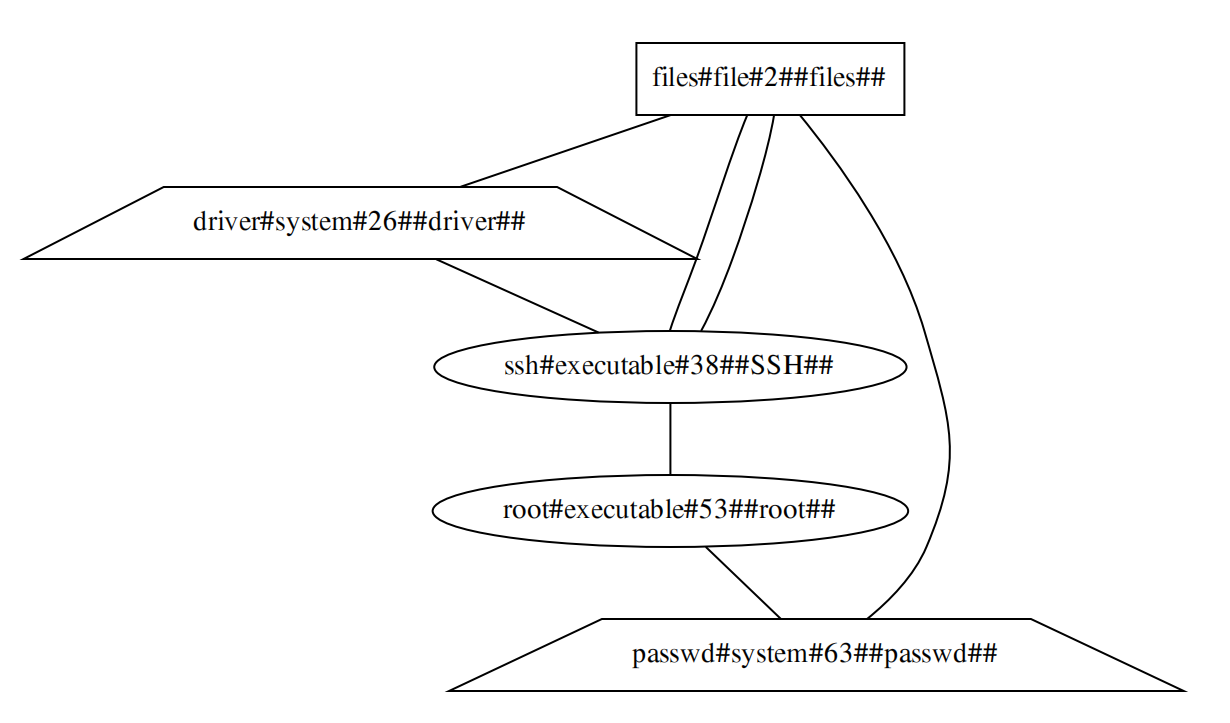
Diagram

Description automatically generated with medium confidence

# 6. SSH BinFmt-Elevate

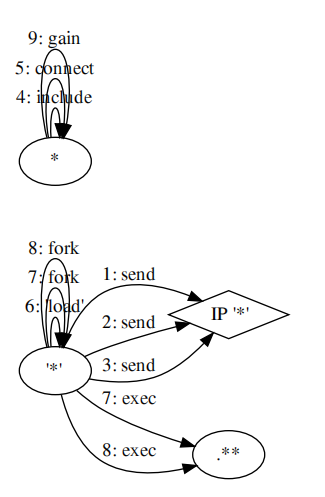
Copied files via SCP and connected via SSH from the ta1-pivot-2 host. Sent files to the target included the privilege escalation driver load\_helper and an elevate client. Connected to target using SSH with stolen credentials. Loaded the driver, and used it to gain root privileges. As root, exfil’d */etc/passwd*, */etc/shadow*, and the admin’s home directory Documents files.

1. T1003 - OS Credential Dumping
2. T1005 - Data from Local System
3. T1218 - Signed Binary Proxy Execution (11)
4. Command & Control
5. {'T1003': ['files#file#2', 'root#executable#53', 'passwd#system#63'],
6. 'T1005': ['root#executable#53', 'files#file#2', 'passwd#system#63'],
7. 'T1053': ['root#executable#53', 'passwd#system#63', 'files#file#2'],
8. 'T1059': ['root#executable#53', 'passwd#system#63', 'passwd#system#63', 'files#file#2', 'files#file#2'],
9. 'T1070': ['root#executable#53', 'passwd#system#63', 'files#file#2'],
10. 'T1071': ['root#executable#53', 'files#file#2'],
11. 'T1082': ['root#executable#53', 'passwd#system#63', 'files#file#2'],
12. 'T1105': ['files#file#2', 'root#executable#53', 'passwd#system#63'],
13. 'T1218': ['root#executable#53', 'files#file#2', 'passwd#system#63']}



TTPDrill

T1105, T1074, T1145, T1014, T1119, T1138, T1175, T1177, T1164, T1110, T1076, T1078, T1174, T1098, T1195, T1212, T1083, T1137, T1158, T1145, T1020



Diagram, timeline

Description automatically generated

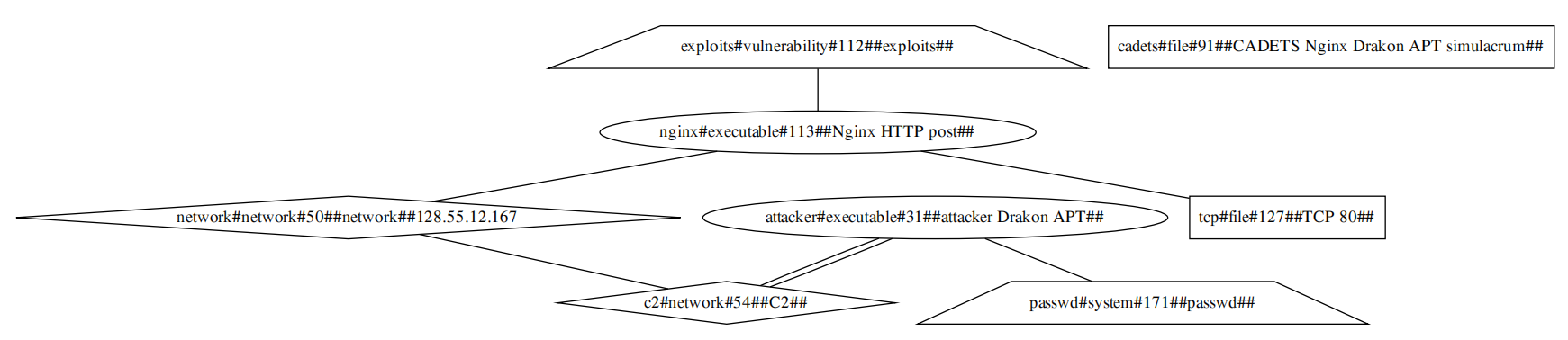
# 7. Nginx Drakon APT

The attacker first tried to attack from an outside host, using *98.23.182.25:80* to download Drakon APT and *108.192.100.31:80* for C2. That failed, though, so the attacker switched to ta1-pivot-2 for the attack C2. The malformed HTTP POST was sent from *128.55.12.167* and resulted in C2 to *128.55.12.233:80*. The attacker then repeated the same attack against ta1-cadets-1, exfil’ing */etc/password* from both hosts. The connections were both left open for later.

The CADETS hosts were both attacked in succession using the Nginx Drakon APT simulacrum.

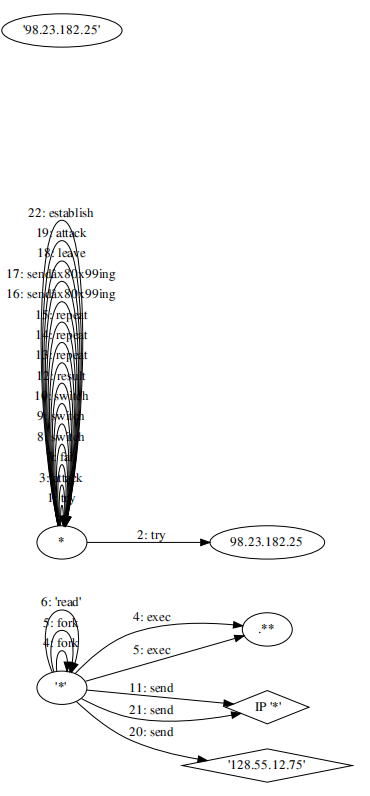
For the attack against CADETS the exploits Nginx by simulation of remote code execution on the listening port of the webserver TCP 80. A malicious HTTP post is sent to *128.55.12.75:80* and *128.55.12.51:80* respectively. The callback is established to C2 and the following commands are sent to gather intellignece on the host environment: hostname, whoami, cat */etc/passwd*, whoami, and hostname.

1. T1003 - OS Credential Dumping
2. T1005 - Data from Local System
3. T1599 - Phishing (T1204 - User Execution)
4. T1059 - Command and Scripting Interpreter (8)
5. T1068 - Exploitation for Privilege Escalation
6. T1105 - Ingress Tool Transfer
7. Command & Control
8. {'T1003': ['tcp#file#127', 'nginx#executable#113', 'passwd#system#171', 'network#network#50'],
9. 'T1005': ['nginx#executable#113', 'tcp#file#127', 'passwd#system#171', 'c2#network#54', 'c2#network#54'],
10. 'T1041': ['nginx#executable#113', 'network#network#50', 'tcp#file#127', 'tcp#file#127', 'passwd#system#171'],
11. 'T1059': ['nginx#executable#113', 'passwd#system#171', 'passwd#system#171', 'exploits#vulnerability#112', 'tcp#file#127', 'network#network#50', 'tcp#file#127'],
12. 'T1068': ['exploits#vulnerability#112', 'nginx#executable#113', 'tcp#file#127', 'passwd#system#171'],
13. 'T1070': ['nginx#executable#113', 'passwd#system#171', 'network#network#50', 'tcp#file#127'],
14. 'T1071': ['nginx#executable#113', 'network#network#50', 'c2#network#54', 'tcp#file#127', 'exploits#vulnerability#112'],
15. 'T1082': ['nginx#executable#113', 'passwd#system#171', 'tcp#file#127', 'network#network#50'],
16. 'T1083': ['tcp#file#127', 'nginx#executable#113', 'network#network#50', 'passwd#system#171', 'network#network#50'],
17. 'T1105': ['tcp#file#127', 'network#network#50', 'nginx#executable#113', 'passwd#system#171'],
18. 'T1203': ['exploits#vulnerability#112', 'tcp#file#127', 'nginx#executable#113'],
19. 'T1204': ['nginx#executable#113', 'c2#network#54', 'tcp#file#127'],
20. 'T1218': ['nginx#executable#113', 'tcp#file#127', 'passwd#system#171'],
21. 'T1550': ['nginx#executable#113', 'tcp#file#127', 'c2#network#54'],
22. 'T1566': ['c2#network#54', 'tcp#file#127', 'nginx#executable#113', 'tcp#file#127', 'exploits#vulnerability#112'],
23. 'T1571': ['nginx#executable#113', 'network#network#50', 'tcp#file#127'],
24. 'T1573': ['nginx#executable#113', 'network#network#50', 'tcp#file#127']}



TTPDrill

T1192, T1027, T1086, T1192, T1046, T1201, T1132, T1043, T1095, T1094, T1185, T1201, T1104, T1083, T1217, T1184, T1076, T1077, T1036, T1126, T1083, T1497, T1205, T1110, T1210, T1204, T1189, T1048, T1088, T1176, T1181, T1018, T1501, T1071, T1191, T1092



Diagram

Description automatically generated

# 8. Frankenstein Campaign

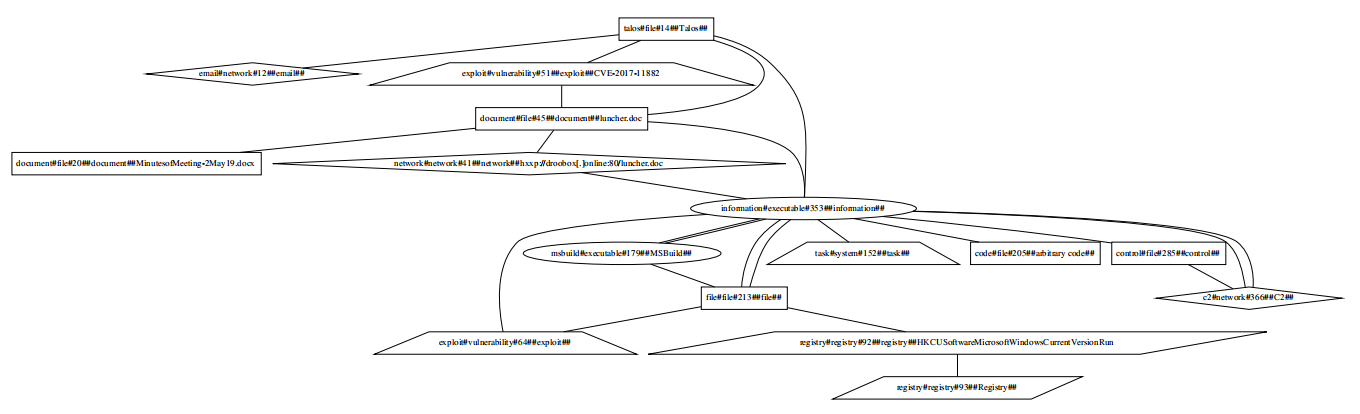
The threat actors sent the trojanized Microsoft Word documents, probably via email. Talos discovered a document named *MinutesofMeeting-2May19.docx*. Once the victim opens the document, it fetches a remove template from the actor-controlled website, *hxxp://droobox[.]online:80/luncher.doc*. Once the *luncher.doc* was downloaded, it used *CVE-2017-11882*, to execute code on the victim's machine. After the exploit, the file would write a series of base64-encoded PowerShell commands that acted as a stager and set up persistence by adding it to the *HKCU\Software\Microsoft\Windows\CurrentVersion\Run* Registry key.

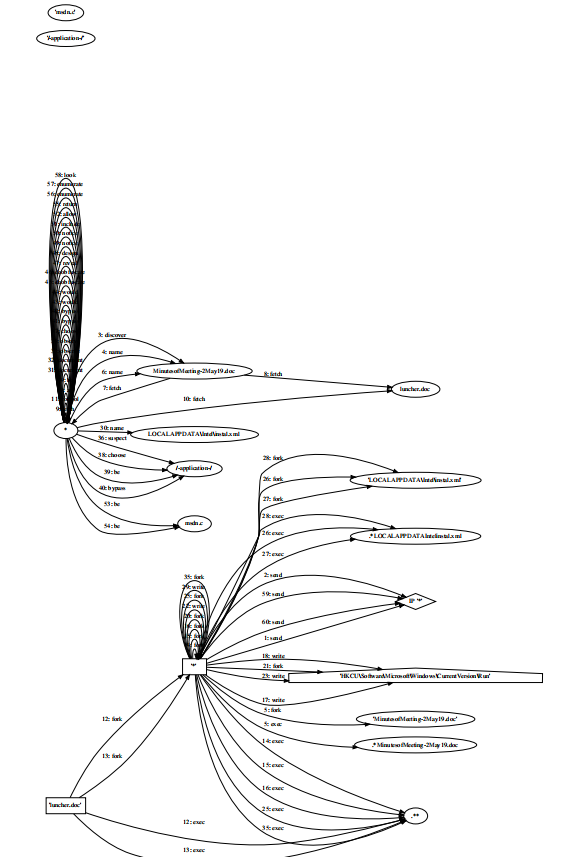
Once the evasion checks were complete, the threat actors used MSbuild to execute an actor-created file named "*LOCALAPPDATA\Intel\instal.xml*". Based on lexical analysis, we assess with high confidence that this component of the macro script was based on an open-source project called "MSBuild-inline-task." While this technique was previously documented last year, it has rarely been observed being used in operations. Talos suspects the adversary chose MSBuild because it is a signed Microsoft binary, meaning that it can bypass application whitelisting controls on the host when being used to execute arbitrary code.

Once the "*instal.xml*" file began execution, it would deobfuscate the base64-encoded commands. This revealed a stager, or a small script designed to obtain an additional payload. While analyzing this stager, we noticed some similarities to the "Get-Data" function of the FruityC2 PowerShell agent. One notable difference is that this particular stager included functionality that allowed the stager to communicate with the command and control (C2) via an encrypted RC4 byte stream. In this sample, the threat actors' C2 server was the domain *msdn[.]cloud*.

the C2 would return a string of characters. Once the string was RC4 decrypted, it launched a PowerShell Empire agent. The PowerShell script would attempt to enumerate the host to look for certain information. Once the aforementioned information was obtained, it was sent back to the threat actor's C2.

1. T1005 - Data from Local System
2. T1566 - Phishing,
3. T1204 - User Execution,
4. T1105 - Ingress Tool Transfer,
5. T1218 - Signed Binary Proxy Execution
6. T1203 - Exploitation for Client Execution (T1068 - Exploitation for Privilege Escalation) ,
7. T1547 - Boot Autostart (T1012 - Query Registry),
8. T1041 - Exfiltration Over C2 Channel (T1071 - Application Layer Protocol, T1218 - Signed Binary Proxy Execution (11), T1573 - Encrypted Channel (2)),
9. T1059 - Command and Scripting Interpreter (8)
10. {'T1005': ['msbuild#executable#179', 'document#file#45', 'task#system#152', 'email#network#12', 'email#network#12'],
11. 'T1041': ['msbuild#executable#179', 'network#network#41', 'document#file#45', 'document#file#45', 'task#system#152'],
12. 'T1059': ['msbuild#executable#179', 'task#system#152', 'task#system#152', 'exploit#vulnerability#64', 'document#file#45', 'network#network#41', 'document#file#45', 'registry#registry#93'],
13. 'T1068': ['exploit#vulnerability#64', 'msbuild#executable#179', 'code#file#205', 'task#system#152'],
14. 'T1070': ['msbuild#executable#179', 'task#system#152', 'network#network#41', 'registry#registry#93', 'code#file#205'],
15. 'T1071': ['msbuild#executable#179', 'network#network#41', 'email#network#12', 'document#file#45', 'exploit#vulnerability#64'],
16. 'T1105': ['document#file#45', 'network#network#41', 'msbuild#executable#179', 'task#system#152'],
17. 'T1203': ['exploit#vulnerability#64', 'document#file#45', 'msbuild#executable#179'],
18. 'T1218': ['msbuild#executable#179', 'registry#registry#93', 'document#file#45', 'task#system#152'],
19. 'T1566': ['email#network#12', 'document#file#45', 'msbuild#executable#179', 'document#file#45', 'exploit#vulnerability#64'],
20. 'T1571': ['msbuild#executable#179', 'network#network#41', 'document#file#45'],
21. 'T1573': ['msbuild#executable#179', 'network#network#41', 'document#file#45']}



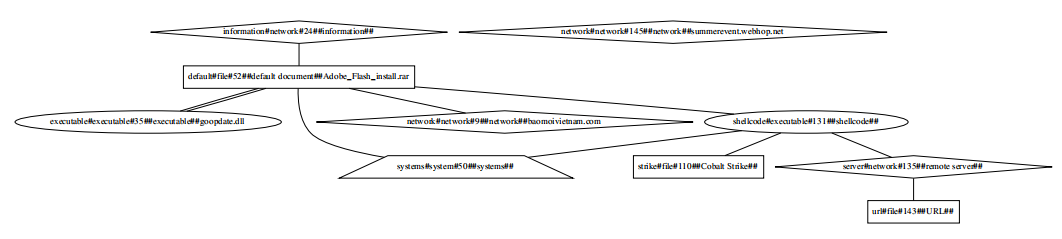


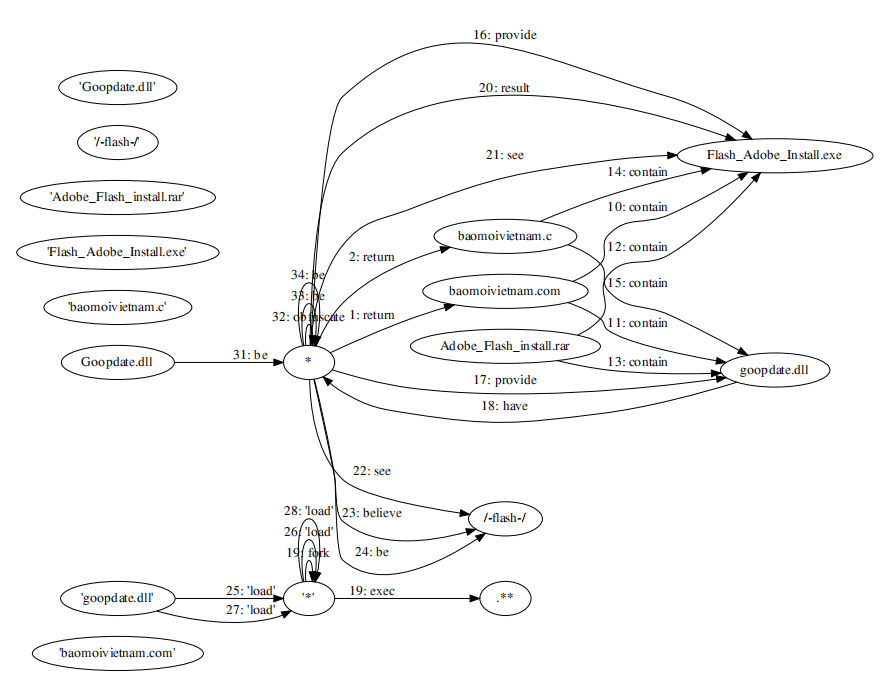
# 9. OceanLotus (APT32) Campaign

The *Adobe\_Flash\_install.rar* archive that was returned from the *baomoivietnam.com* website contained the files *Flash\_Adobe\_Install.exe* and *goopdate.dll*. The table below provides some basic information on all three of these files.

The file *goopdate.dll* has the hidden file attribute set and will not show in Windows Explorer on systems using default settings. This results in the user seeing only the *Flash\_Adobe\_Install.exe* file to execute in order to install what they believe to be an update to Flash Player. When run, it will automatically load *goopdate.dll* due to search order hijacking. *Goopdate.dll* is a highly obfuscated loader whose ultimate purpose is to load a Cobalt Strike stager into memory and then execute it. The Cobalt Strike stager will simply try to download and execute a shellcode from a remote server, in this case using the following URL: *summerevent.webhop.net/QuUA*

1. T1005 - Data from Local System
2. T1105 - Ingress Tool Transfer,
3. T1218 - Signed Binary Proxy Execution,
4. T1574 - Hijack Execution Flow, (1.14)
5. {'T1005': ['shellcode#executable#131', 'url#file#143', 'systems#system#50', 'information#network#24', 'information#network#24'],
6. 'T1059': ['executable#executable#35', 'systems#system#50', 'systems#system#50', 'url#file#143', 'information#network#24', 'url#file#143'],
7. 'T1105': ['file#file#2', network#network#9', 'executable#executable#35', 'systems#system#50'],
8. 'T1218': ['executable#executable#35', ''file#file#2', 'systems#system#50']}





# 10. Cobalt Campaign

All observed attacks start with an email message, containing either a malicious attachment or a URL which leads to the first stage of the attack. The text of the emails is likely taken from legitimate email, such as mailing lists that targeted organizations may be subscribed to. Below are three examples, with the first one purporting to be sent by the European Banking Federation and is using a newly registered domain for the spoofed sender email address. The attachment is a malicious PDF file that entices the user to click on a URL to download and open a weaponized RTF file containing exploits for *CVE-2017-11882*, *CVE-2017-8570* and *CVE-2018-8174*. The final payload is a JScript backdoor also known as More\_eggs that allows the attacker to control the affected system remotely.

Notable applications used in these attacks are cmstp and msxsl. The Microsoft Connection Manager Profile Installer (*cmstp.exe*) is a command-line program used to install Connection Manager service profiles. Cmstp accepts an installation information file (INF) as a parameter and installs a service profile leveraged for remote access connections. A malicious INF file can be supplied as a parameter to download and execute remote code. Cmstp may also be used to load and execute COM scriptlets (SCT files) from remote servers.

Microsoft allows developers to create COM+ objects in script code stored in an XML document, a so-called scriptlet file. Although it is common to use JScript or VBScript, as they are available in Windows by default, a scriptlet can contain COM+ objects implemented in other languages, including Perl and Python, which would be fully functional if the respective interpreters are installed.

To bypass AppLocker and launching script code within a scriptlet, the attacker includes the malicious code within an XML script tag placed within the registration tag of the scriptlet file and calls cmstp with appropriate parameters.

An earlier part of the second stage is implemented as an encrypted JScript scriptlet which eventually drops a randomly named COM server DLL binary with a .txt filename extension, for example, *9242.txt*, in the user's home folder and registers the server using the *regsvr32.exe* utility.The dropper contains an encrypted data blob that is decrypted and written to the disk. The dropper then launches the next stage of the attack by starting PowerShell, msxsl or *cmstp.exe* as described above.

The PowerShell chain is launched from an obfuscated JScript scriptlet previously downloaded from the command and control (C2) server and launched using *cmstp.exe*. The first PowerShell stage is a simple downloader that downloads the next PowerShell stage and launches a child instance of *powershell.exe* using the downloaded, randomly named script as the argument. The downloaded PowerShell script code is obfuscated in several layers before the last layer is reached. The last layer loads shellcode into memory and creates a thread within the PowerShell interpreter process space.

On the PowerShell side of the infection chain, the downloaded final payload is a Cobalt Strike beacon, which provides the attacker with rich backdoor functionality.

1. T1566 - Phishing
2. T1105 - Ingress Tool Transfer
3. T1203 - Exploitation for Client Execution
4. T1204 - User Execution
5. T1218 - Signed Binary Proxy Execution
6. Command & Control
7. T1059 - Command and Scripting Interpreter (8)
8. {'T1059': ['com#executable#223', 'system#system#136', 'system#system#136', 'exploits#vulnerability#109', 'control#file#448', 'servers#network#231', 'control#file#448'],
9. 'T1070': ['com#executable#223', 'system#system#136', 'servers#network#231', 'control#file#448'],
10. 'T1071': ['com#executable#223', 'servers#network#231', 'servers#network#231', 'control#file#448', 'exploits#vulnerability#109'],
11. 'T1105': ['control#file#448', 'servers#network#231', 'com#executable#223', 'system#system#136'],
12. 'T1203': ['exploits#vulnerability#109', 'control#file#448', 'com#executable#223'],
13. 'T1204': ['com#executable#223', 'servers#network#231', 'control#file#448'],
14. 'T1218': ['com#executable#223', 'control#file#448', 'system#system#136'],
15. 'T1566': ['servers#network#231', 'control#file#448', 'com#executable#223', 'control#file#448', 'exploits#vulnerability#109'],
16. 'T1571': ['com#executable#223', 'servers#network#231', 'control#file#448'],
17. 'T1573': ['com#executable#223', 'servers#network#231', 'control#file#448']}

