SANS @ Night

Hands on Cyber Security in the Age of the Internet of Everything

Wednesday, 21 June 2017 @ 8:15pm
Happy Solstice!

Matthew J. Harmon
GSEC, GCIH, GCIA, CISSP

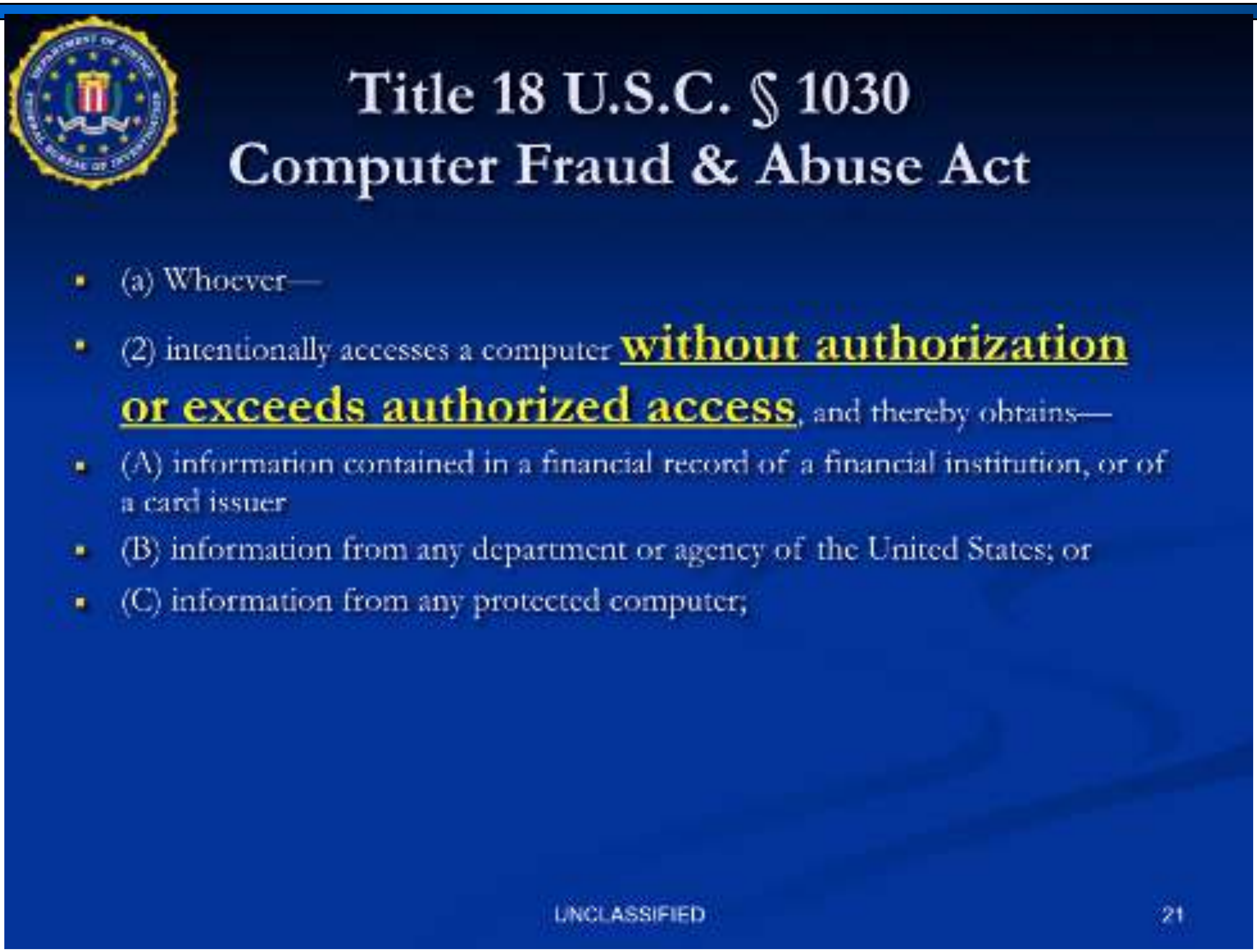
Matthew J. Harmon

- Security Consultant & Researcher for IT Risk Limited
- Instructor for SANS & Saint Paul College
- Two emergency spinal operations last year

What are we going to cover tonight?

- Legal Challenges for IoT Security Research
- Importance of routine maintenance, an analogy
- The Internet of Everything
- Smart = Exploitable, most of the time
- Establishing a known state
- Device Enumeration
- Data Enumeration

Legal Challenges



Title 18 U.S.C. § 1030
Computer Fraud & Abuse Act

- (a) Whoever—
- (2) intentionally accesses a computer **without authorization or exceeds authorized access**, and thereby obtains—
- (A) information contained in a financial record of a financial institution, or of a card issuer
- (B) information from any department or agency of the United States; or
- (C) information from any protected computer;

UNCLASSIFIED

21

Source: Minneapolis FBI Cyber Division at Saint Paul College Spring 2017

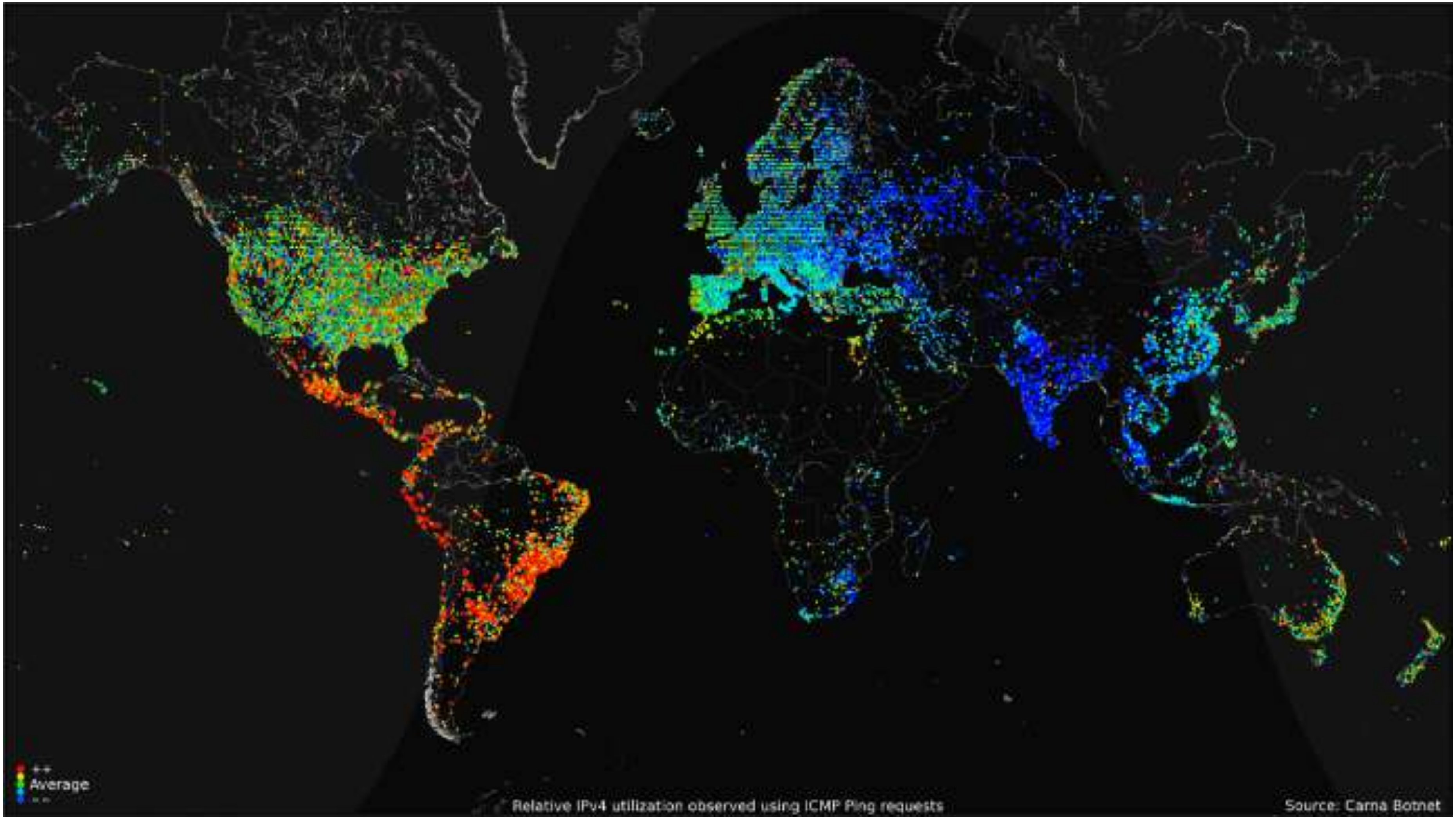
Legal Challenges (cont.)

- Patent law and reverse engineering IoT devices
- I asked a cyber lawyer, the Electronic Frontier Foundation and was basically told

These things matter not to attackers

Image: ST:TNG "A Matter of Perspective”

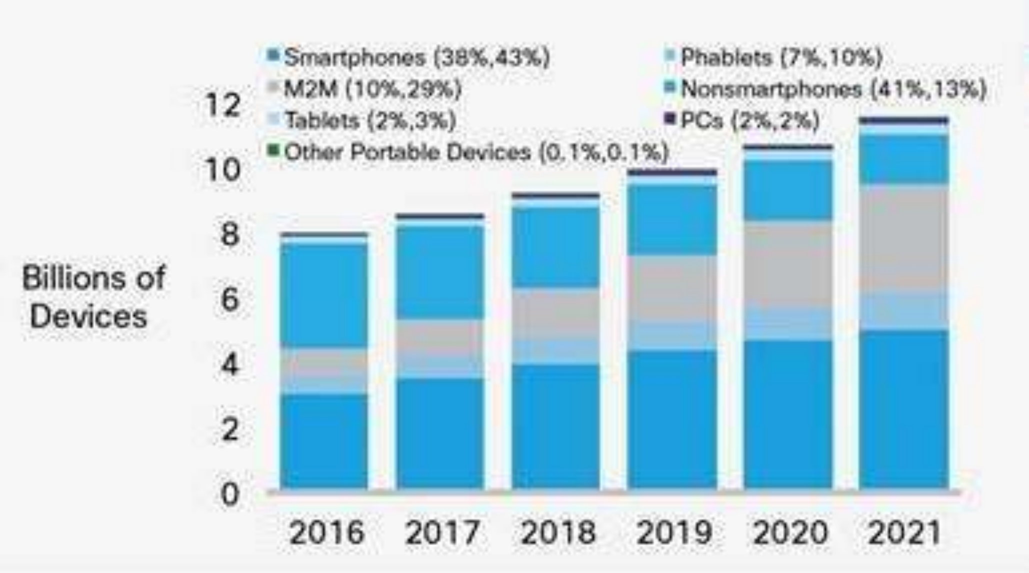
Internet Census 2012 (Carna Botnet)



Scope: 460 Million IP addresses that responded to ICMP ping requests or port scans from June and October 2012
Source: http://census2012.sourceforge.net/paper.html

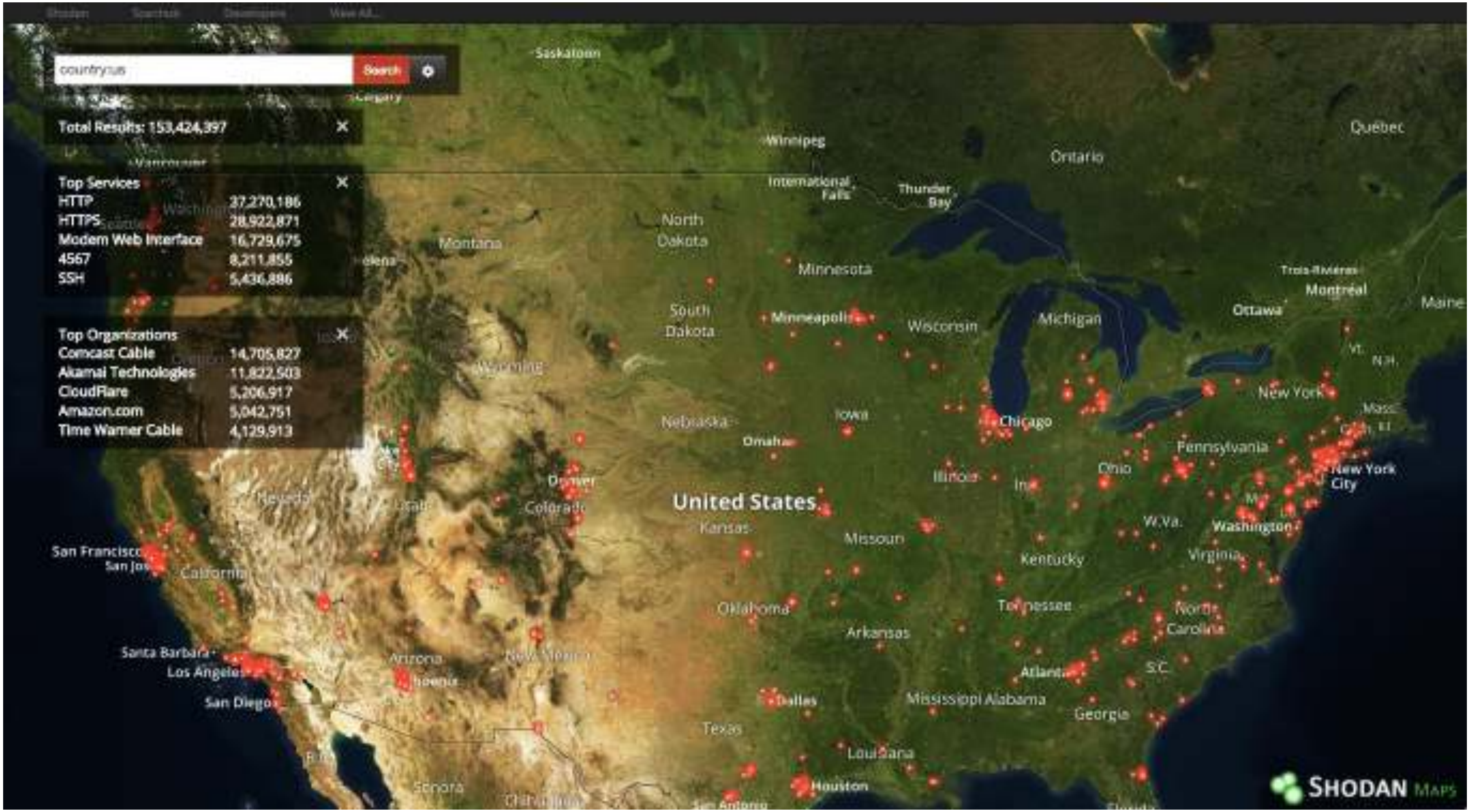
IoT Growth

- Added in 2016: ~429 million mobile/connections
- Global mobile devices and connections in 2016 grew to 8.0 billion, up from 7.6 billion in 2015.
- By 2021, ~3/4 of all devices connected will be “smart”



Source: Cisco Visual Networking Index 2017

Shodan Indexed IPs (country:us)



country:us Search

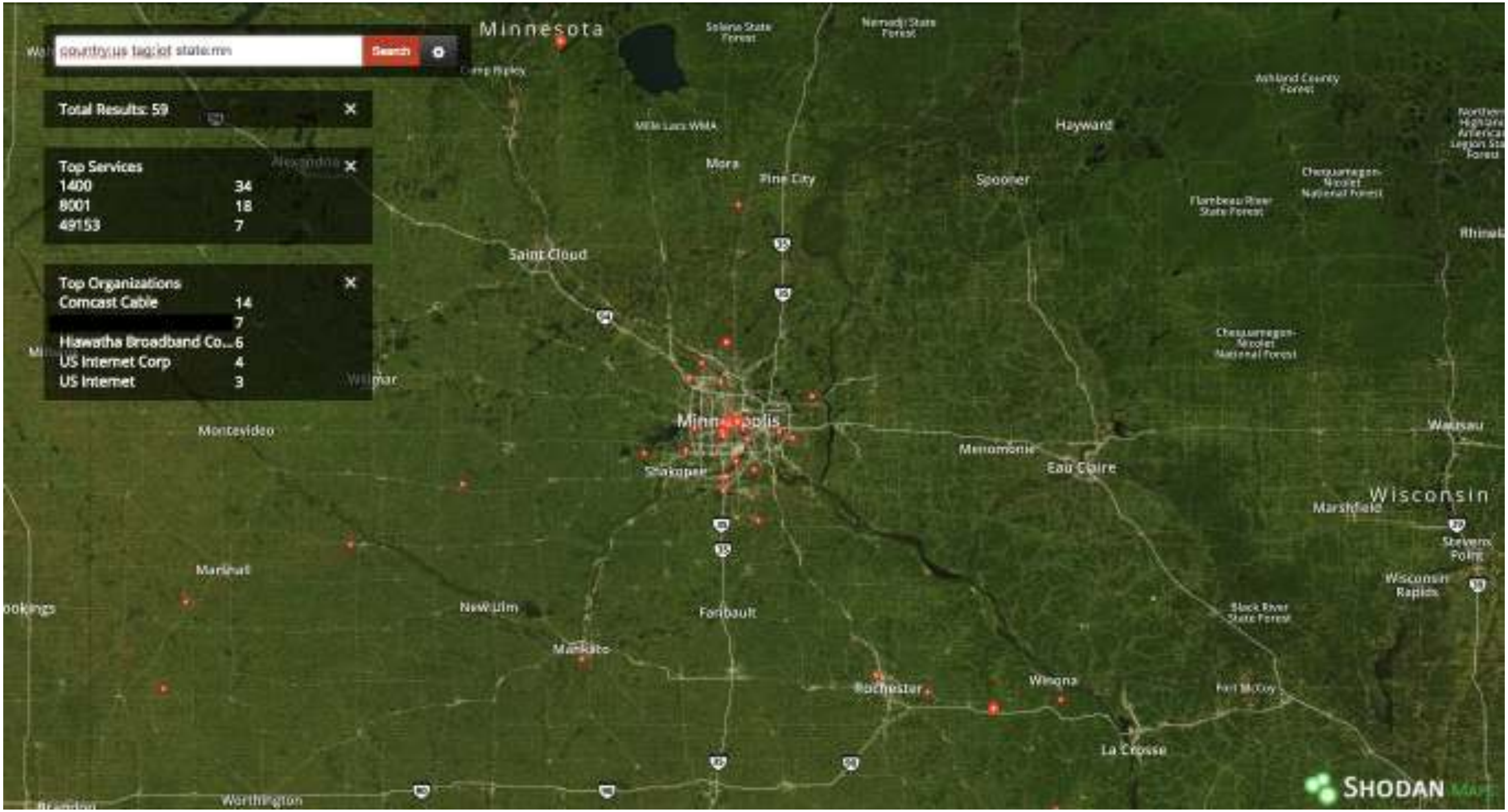
Total Results: 153,424,397

Top Services	
HTTP	37,270,186
HTTPS	28,922,871
Modem Web Interface	16,729,675
4567	8,211,855
SSH	5,436,886

Top Organizations	
Comcast Cable	14,705,827
Akamai Technologies	11,822,503
CloudFlare	5,206,917
Amazon.com	5,042,751
Time Warner Cable	4,129,913

Thanks: John C. Matherly at Shodan (@achillean)

Shodan Indexed "IoT" tagged



country:us tag:iot state:mn

Search

Total Results: 59

Top Services	
1400	34
8001	18
49153	7

Top Organizations	
Comcast Cable	14
[redacted]	7
Hiawatha Broadband Co...	6
US Internet Corp	4
US Internet	3

Thanks: John C. Matherly at Shodan (@achillean)

IoT Attack Surface (Highlights)

- Administrative Interface
  - Directory transversal (Smart Dishwasher)
  - Weak/Default Passwords ("password")
- Local Data Storage
  - Unencrypted or weakly encrypted data
  - Decomissioning
- Patches/updates
  - Transmitted in the clear
  - Eventually everything comes to an end…

Source: OWASP IoT https://www.owasp.org/index.php/IoT_Attack_Surface_Areas

IoT Attack Surface (cont)

- Firmware backdoors
    - Insecure credential storage weak recovery/reset
    - Vulnerable Services, Hardcoded Creds, privacy
- Sensors
    - Location, microphone
    - Damage
- Network Traffic
    - LAN to Internet
    - Wireless (WiFi, X/Zigbee, Bluetooth)

Source: OWASP IoT https://www.owasp.org/index.php/IoT_Attack_Surface_Areas

Some questions

- Is dishwasher's web server is patched?
- Do you know if your lightbulb is packet flooding a journalist?
- Is your camera sending mpegs to another country?
- Is your TV is sending fingerprints of movies you are watching?
- Is your refrigerator is being used as a C&C host?
- Is a nation state using your SOHO router as a monitoring point?
- Your NAS is syncing to an unk party, or have weak permissions?
- Is your board room phone recording and sending those recordings somewhere?

WHY DO WE HAVE TO ASK THESE QUESTIONS!?

In summary…

If it says "Smart",
you should read it as
"Exploitable"

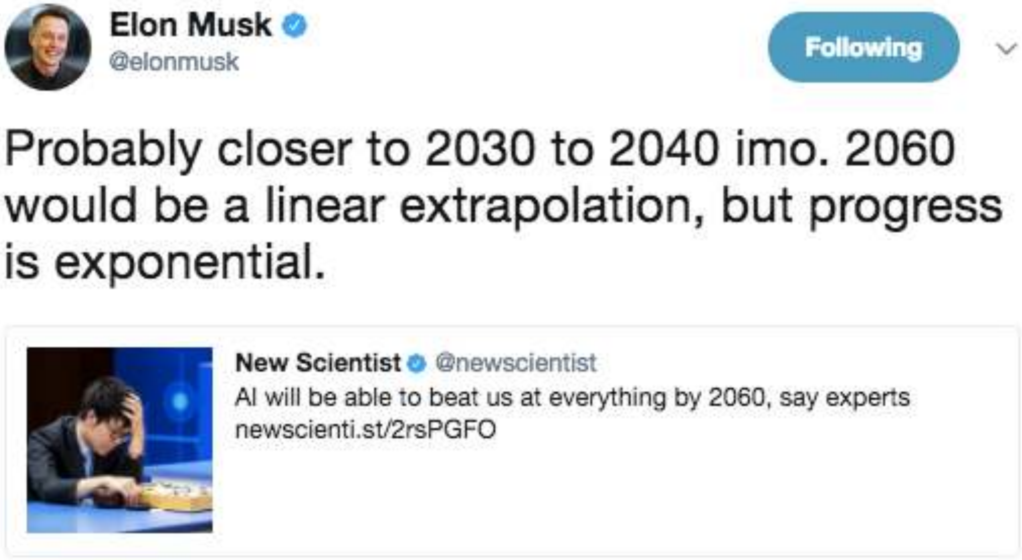
Hat Tip: Mikko Hypponen (@mikko)

IoT of today will eventually fail

- 32-bit processors and Y2k38

I'M GLAD WE'RE SWITCHING TO 64-BIT, BECAUSE I WASN'T LOOKING FORWARD TO CONVINCING PEOPLE TO CARE ABOUT THE UNIX 2038 PROBLEM.
WHAT'S THAT?
REMEMBER Y2K? THIS COULD BE EVEN *WORSE!*

- About the time AI is reaching epoch



Elon Musk
@elonmusk

Probably closer to 2030 to 2040 imo. 2060 would be a linear extrapolation, but progress is exponential.

New Scientist @newscientist
AI will be able to beat us at everything by 2060, say experts
newscienti.st/2rsPGFO

The Future of IoT

What time is it?

Hat Tip: Mikko Hypponen (@mikko)

How do we tackle this?

- Know what you’re defending
  - How to collect the data?
  - Passive, Active, or Aggressive?
  - Attackers don’t care if they tip over systems
    - We do.
    - nmap -T4 is called insane mode for a reason
    - You (probably) don’t need masscan
  - Passive takes longer, but captures more info
- Let’s use Darkstat, Bro and ntopng
- Then, we can use nmap to validate!

How do we tackle this? (cont)

- We need to take control of our local environment, at the very least have:
  - Manufacturer, Model, System Name, Location
  - Operating System, IP address/Netmask, MAC

- Identify and map our “normal” traffic profiles

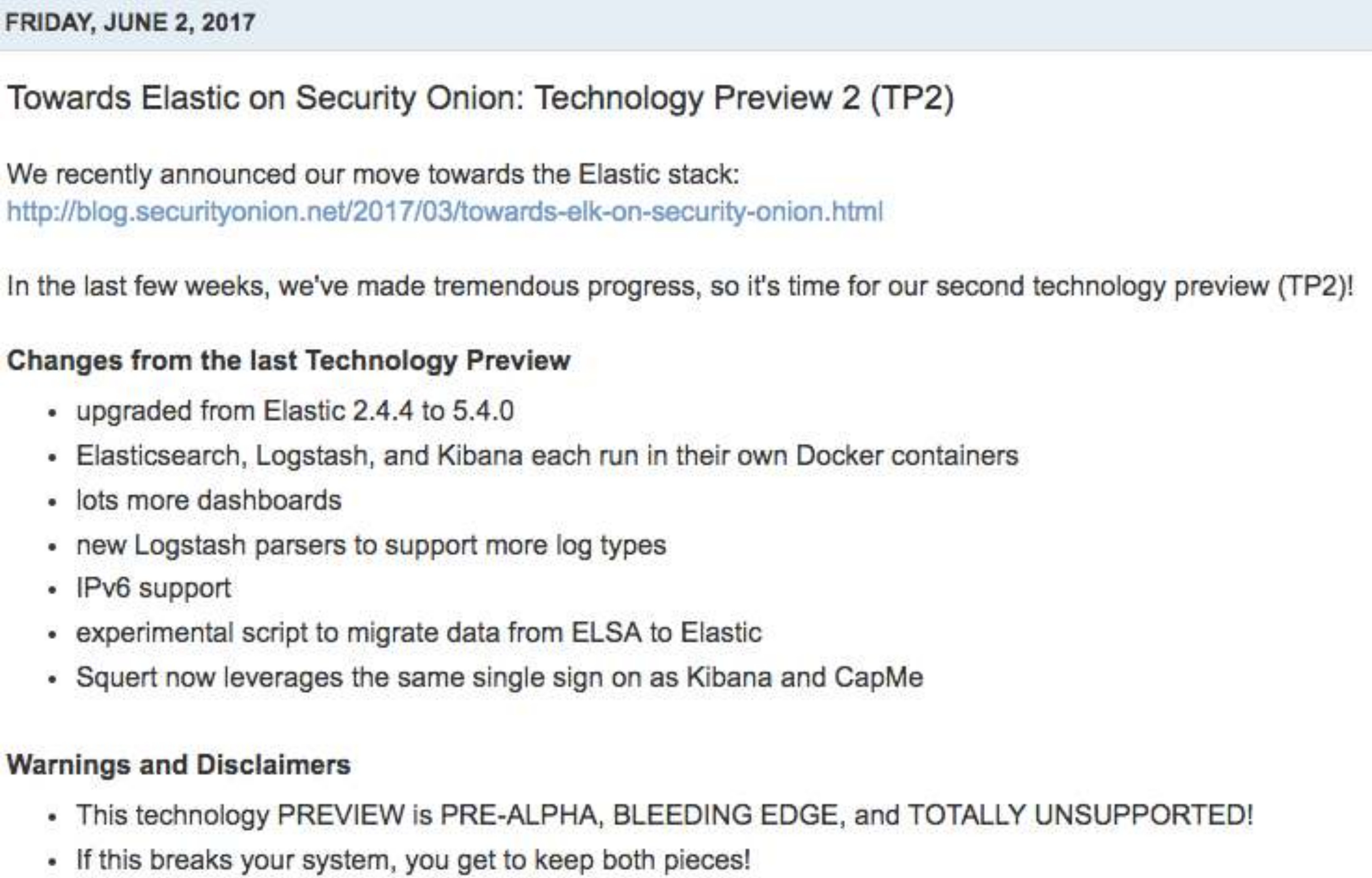
Our Do It Yourself Build Today

- Step 1
  - Install Security Onion on a 2+1 NIC box
  - Go bleeding edge, and test SO+ELK
  - http://blog.securityonion.net/2017/06/towards-elastic-on-security-onion.html
- Step 2
  - Setup a span, mirror or network tap
  - NetGear GS108E is still awesome and only $60

Do It Yourself (cont.)

- Step 3
  - Install Darkstat and ntop-NG
    - https://github.com/Security-Onion-Solutions/security-onion/wiki/DeployingNtopng
    - apt install darkstat
  - Configure Dashboards
    - https://localhost/app/kibana
- Step 4
  - Deploy OSSEC & Sysmon
    - https://github.com/SwiftOnSecurity/sysmon-config

Security Onion + Elastic



FRIDAY, JUNE 2, 2017

Towards Elastic on Security Onion: Technology Preview 2 (TP2)

We recently announced our move towards the Elastic stack:
http://blog.securityonion.net/2017/03/towards-elk-on-security-onion.html

In the last few weeks, we've made tremendous progress, so it's time for our second technology preview (TP2)!

Changes from the last Technology Preview

- upgraded from Elastic 2.4.4 to 5.4.0
- Elasticsearch, Logstash, and Kibana each run in their own Docker containers
- lots more dashboards
- new Logstash parsers to support more log types
- IPv6 support
- experimental script to migrate data from ELSA to Elastic
- Squert now leverages the same single sign on as Kibana and CapMe

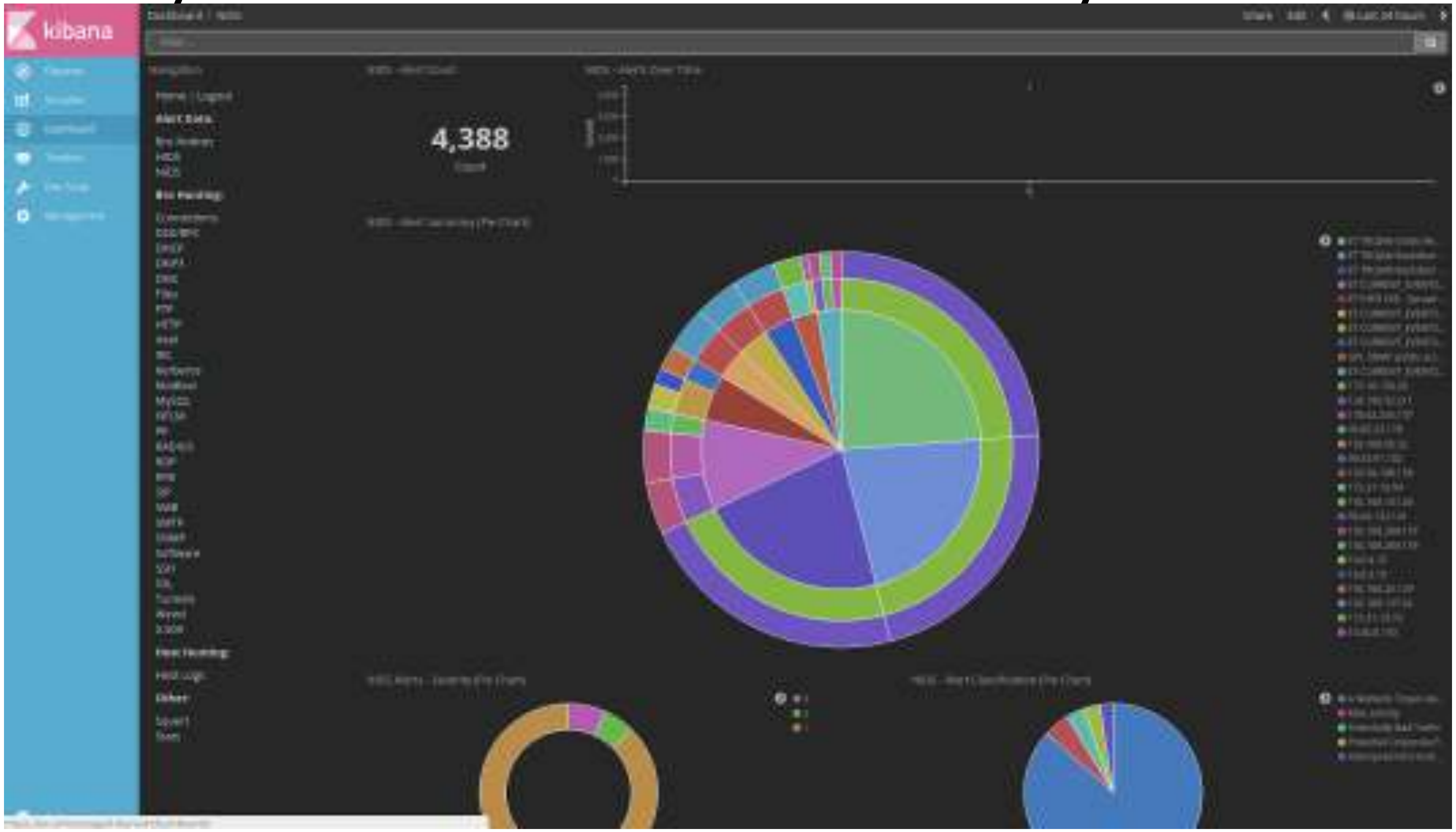
Warnings and Disclaimers

- This technology PREVIEW is PRE-ALPHA, BLEEDING EDGE, and TOTALLY UNSUPPORTED!
- If this breaks your system, you get to keep both pieces!

Source: http://blog.securityonion.net/2017/06/towards-elastic-on-security-onion.html

Taking this to the next level

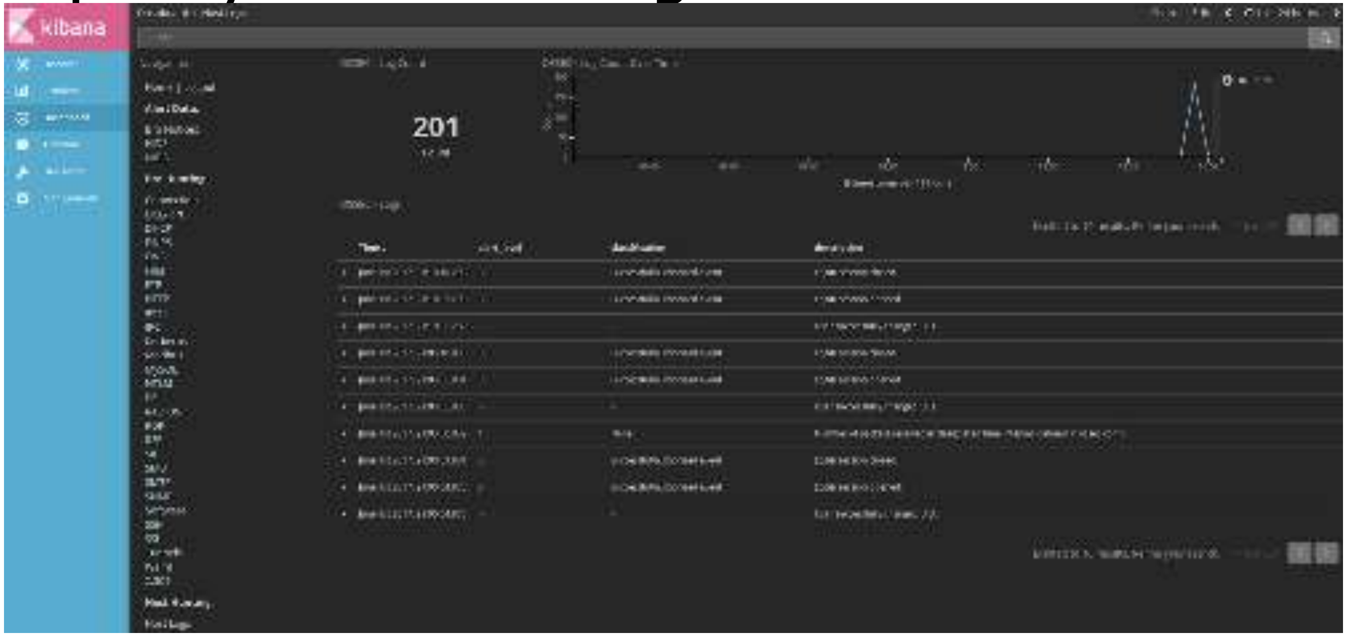
- Security Onion + ELK + OSSEC + Sysmon



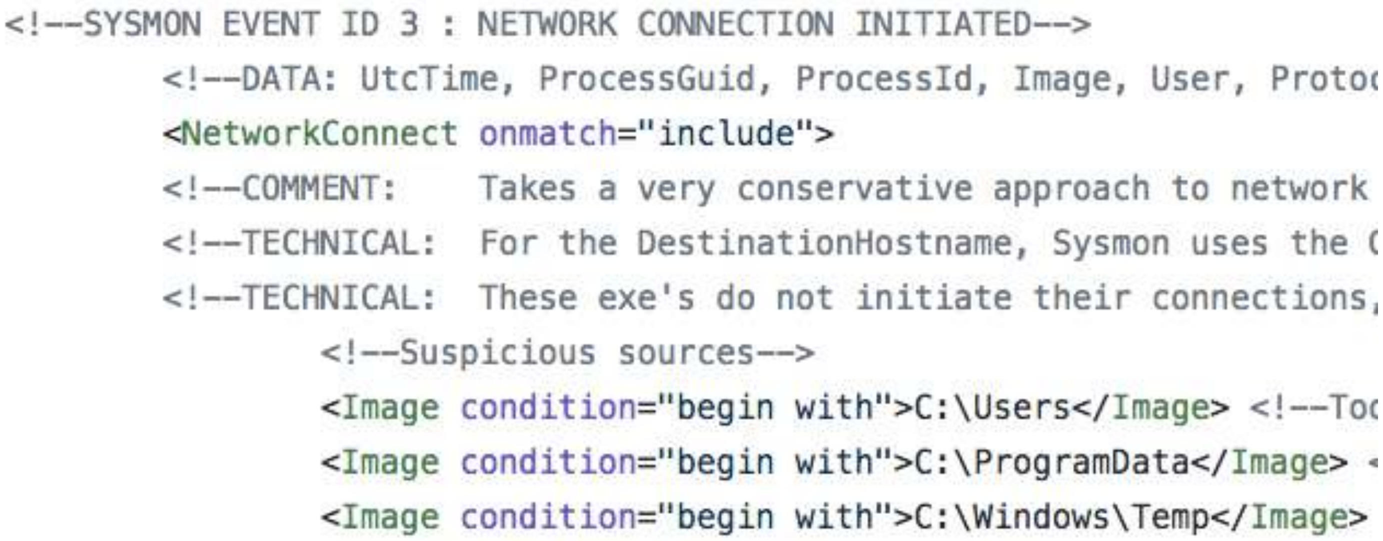
https://technet.microsoft.com/en-us/sysinternals/sysmon
References: https://github.com/Security-Onion-Solutions/security-onion/wiki/Sysmon,
Joshua Brower: https://digital-forensics.sans.org/community/papers/gcfa/sysmon-enrich-security-onions-host-level-capabilities_10612

Using Sysmon for Awesome

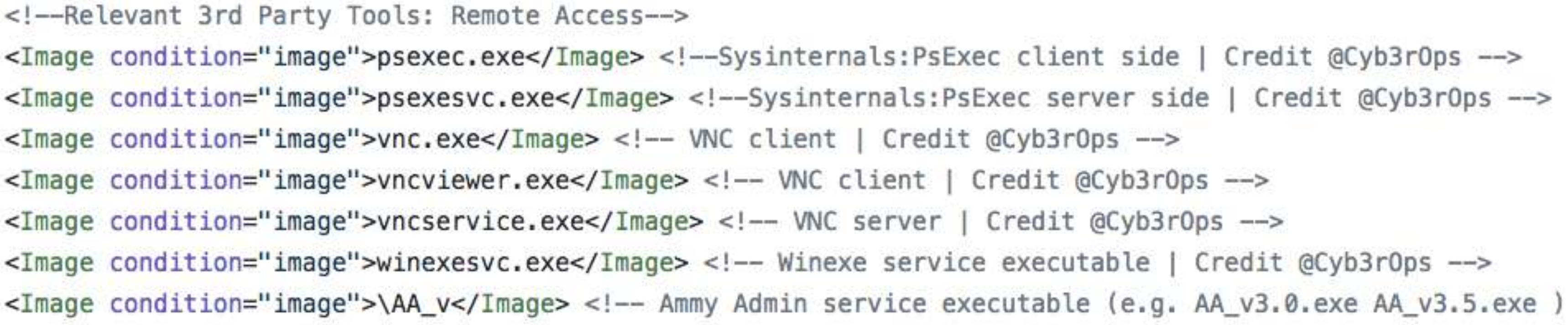
- @SwitftOnSecurity
- https://github.com/SwiftOnSecurity/sysmon-config/
- “Sysmon configuration file template with default high-quality event tracing”



Using Sysmon for Awesome



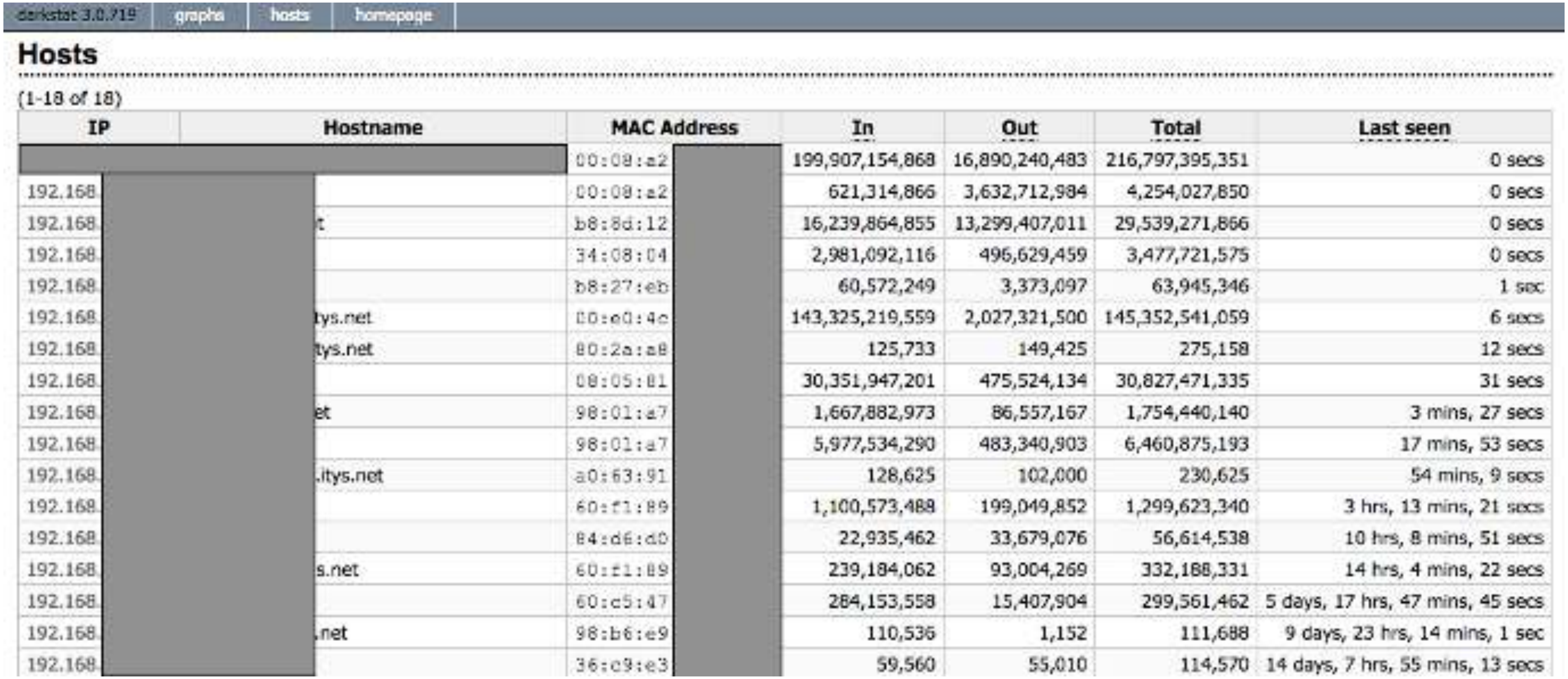
```
<!--SYSMON EVENT ID 3 : NETWORK CONNECTION INITIATED-->
        <!--DATA: UtcTime, ProcessGuid, ProcessId, Image, User, Protoc
        <NetworkConnect onmatch="include">
        <!--COMMENT:    Takes a very conservative approach to network
        <!--TECHNICAL:  For the DestinationHostname, Sysmon uses the (
        <!--TECHNICAL:  These exe's do not initiate their connections,
                <!--Suspicious sources-->
                <Image condition="begin with">C:\Users</Image> <!--Toc
                <Image condition="begin with">C:\ProgramData</Image> <
                <Image condition="begin with">C:\Windows\Temp</Image>
```



```
<!--Relevant 3rd Party Tools: Remote Access-->
<Image condition="image">psexec.exe</Image> <!--Sysinternals:PsExec client side | Credit @Cyb3rOps -->
<Image condition="image">psexesvc.exe</Image> <!--Sysinternals:PsExec server side | Credit @Cyb3rOps -->
<Image condition="image">vnc.exe</Image> <!-- VNC client | Credit @Cyb3rOps -->
<Image condition="image">vncviewer.exe</Image> <!-- VNC client | Credit @Cyb3rOps -->
<Image condition="image">vncservice.exe</Image> <!-- VNC server | Credit @Cyb3rOps -->
<Image condition="image">winexesvc.exe</Image> <!-- Winexe service executable | Credit @Cyb3rOps -->
<Image condition="image">\AA_v</Image> <!-- Ammy Admin service executable (e.g. AA_v3.0.exe AA_v3.5.exe )
```

Source: https://github.com/SwiftOnSecurity/sysmon-config/

Darkstat Passive Enumeration



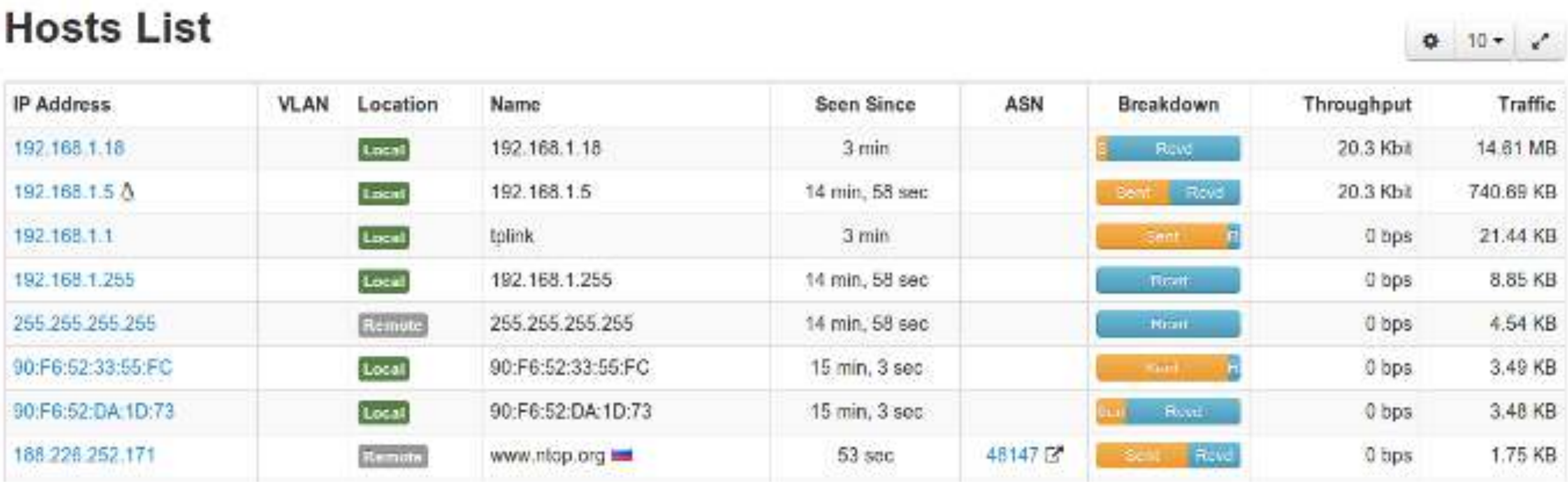
Hosts

(1-18 of 18)

IP	Hostname	MAC Address	In	Out	Total	Last seen
[redacted]	[redacted]	00:08:a2[redacted]	199,907,154,868	16,890,240,483	216,797,395,351	0 secs
192.168.[redacted]	[redacted]	00:08:a2[redacted]	621,314,866	3,632,712,984	4,254,027,850	0 secs
192.168.[redacted]	[redacted]t	b8:8d:12[redacted]	16,239,864,855	13,299,407,011	29,539,271,866	0 secs
192.168.[redacted]	[redacted]	34:08:04[redacted]	2,981,092,116	496,629,459	3,477,721,575	0 secs
192.168.[redacted]	[redacted]	b8:27:eb[redacted]	60,572,249	3,373,097	63,945,346	1 sec
192.168.[redacted]	[redacted]tys.net	00:e0:4c[redacted]	143,325,219,559	2,027,321,500	145,352,541,059	6 secs
192.168.[redacted]	[redacted]tys.net	80:2a:a8[redacted]	125,733	149,425	275,158	12 secs
192.168.[redacted]	[redacted]	08:05:81[redacted]	30,351,947,201	475,524,134	30,827,471,335	31 secs
192.168.[redacted]	[redacted]et	98:01:a7[redacted]	1,667,882,973	86,557,167	1,754,440,140	3 mins, 27 secs
192.168.[redacted]	[redacted]	98:01:a7[redacted]	5,977,534,290	483,340,903	6,460,875,193	17 mins, 53 secs
192.168.[redacted]	[redacted].itys.net	a0:63:91[redacted]	128,625	102,000	230,625	54 mins, 9 secs
192.168.[redacted]	[redacted]	60:f1:89[redacted]	1,100,573,488	199,049,852	1,299,623,340	3 hrs, 13 mins, 21 secs
192.168.[redacted]	[redacted]	84:d6:d0[redacted]	22,935,462	33,679,076	56,614,538	10 hrs, 8 mins, 51 secs
192.168.[redacted]	[redacted]s.net	60:f1:89[redacted]	239,184,062	93,004,269	332,188,331	14 hrs, 4 mins, 22 secs
192.168.[redacted]	[redacted]	60:c5:47[redacted]	284,153,558	15,407,904	299,561,462	5 days, 17 hrs, 47 mins, 45 secs
192.168.[redacted]	[redacted].net	98:b6:e9[redacted]	110,536	1,152	111,688	9 days, 23 hrs, 14 mins, 1 sec
192.168.[redacted]	[redacted]	36:c9:e3[redacted]	59,560	55,010	114,570	14 days, 7 hrs, 55 mins, 13 secs

Source: https://unix4lyfe.org/darkstat/

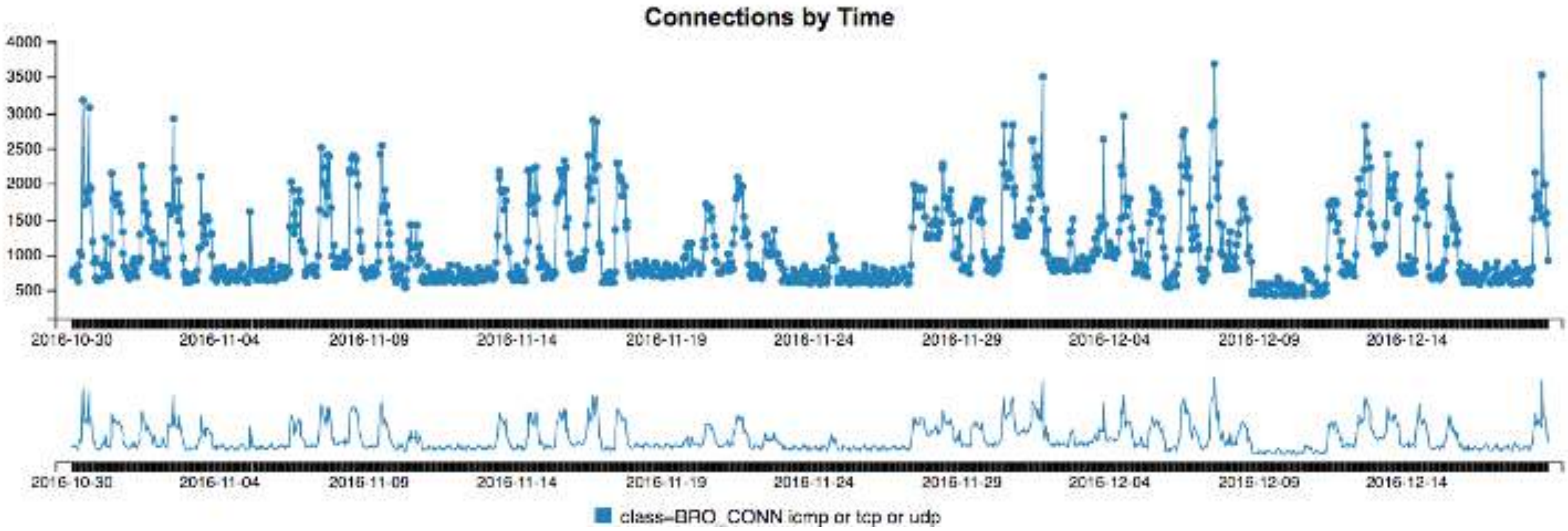
ntopng hosts

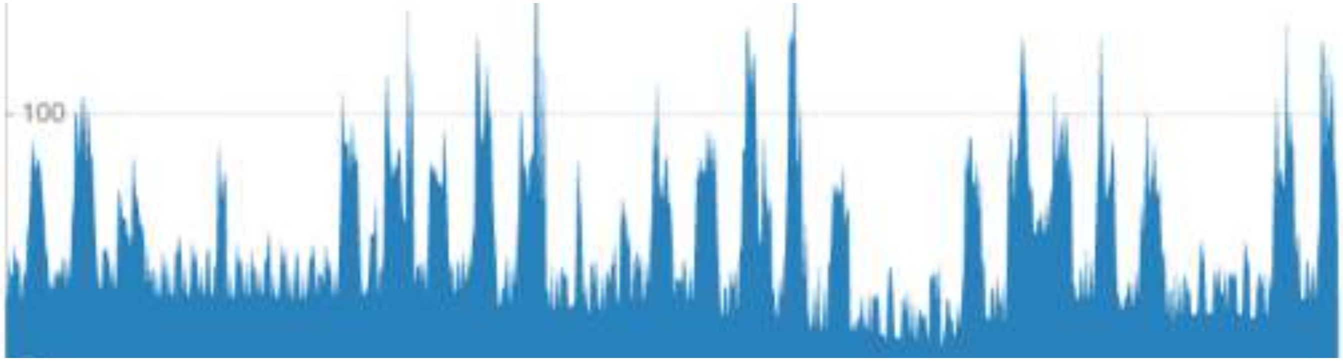


Hosts List

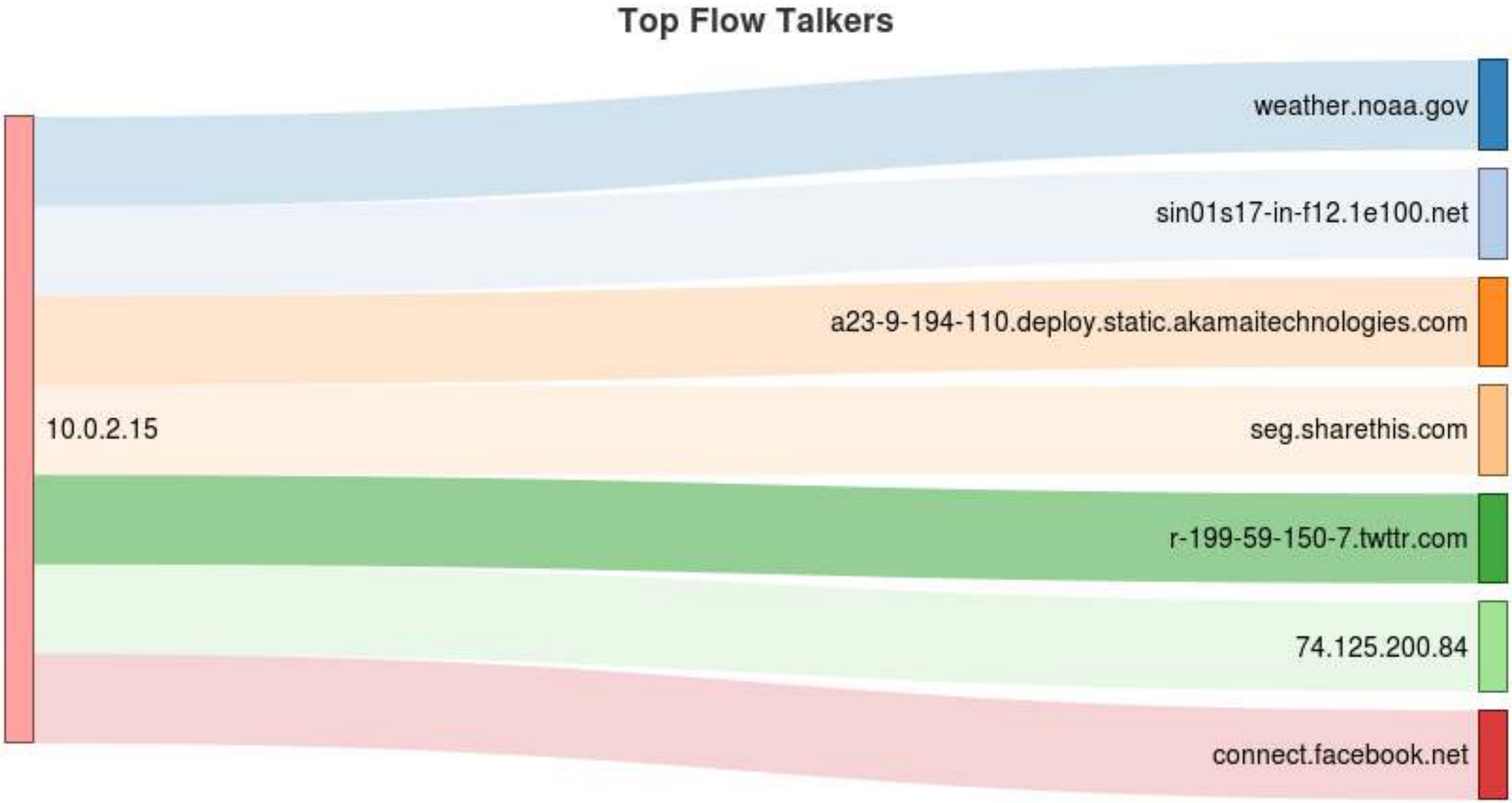
IP Address	VLAN	Location	Name	Seen Since	ASN	Breakdown	Throughput	Traffic
192.168.1.18		Local	192.168.1.18	3 min		S Rcvd	20.3 Kbit	14.61 MB
192.168.1.5		Local	192.168.1.5	14 min, 58 sec		Sent Rcvd	20.3 Kbit	740.69 KB
192.168.1.1		Local	tplink	3 min		Sent R	0 bps	21.44 KB
192.168.1.255		Local	192.168.1.255	14 min, 58 sec		Rcvd	0 bps	8.85 KB
255.255.255.255		Remote	255.255.255.255	14 min, 58 sec		Rcvd	0 bps	4.54 KB
90:F6:52:33:55:FC		Local	90:F6:52:33:55:FC	15 min, 3 sec		Sent R	0 bps	3.49 KB
90:F6:52:DA:1D:73		Local	90:F6:52:DA:1D:73	15 min, 3 sec		Sent Rcvd	0 bps	3.48 KB
188.226.252.171		Remote	www.ntop.org	53 sec	48147	Sent Rcvd	0 bps	1.75 KB

Correlating Bro & ntopng Passive Enumeration





ntopng Flow Enumeration



Source: © 2017 LinOxide

Bringing it all together

DCIM: Data center Infrastructure Management
netbox_devices.csv

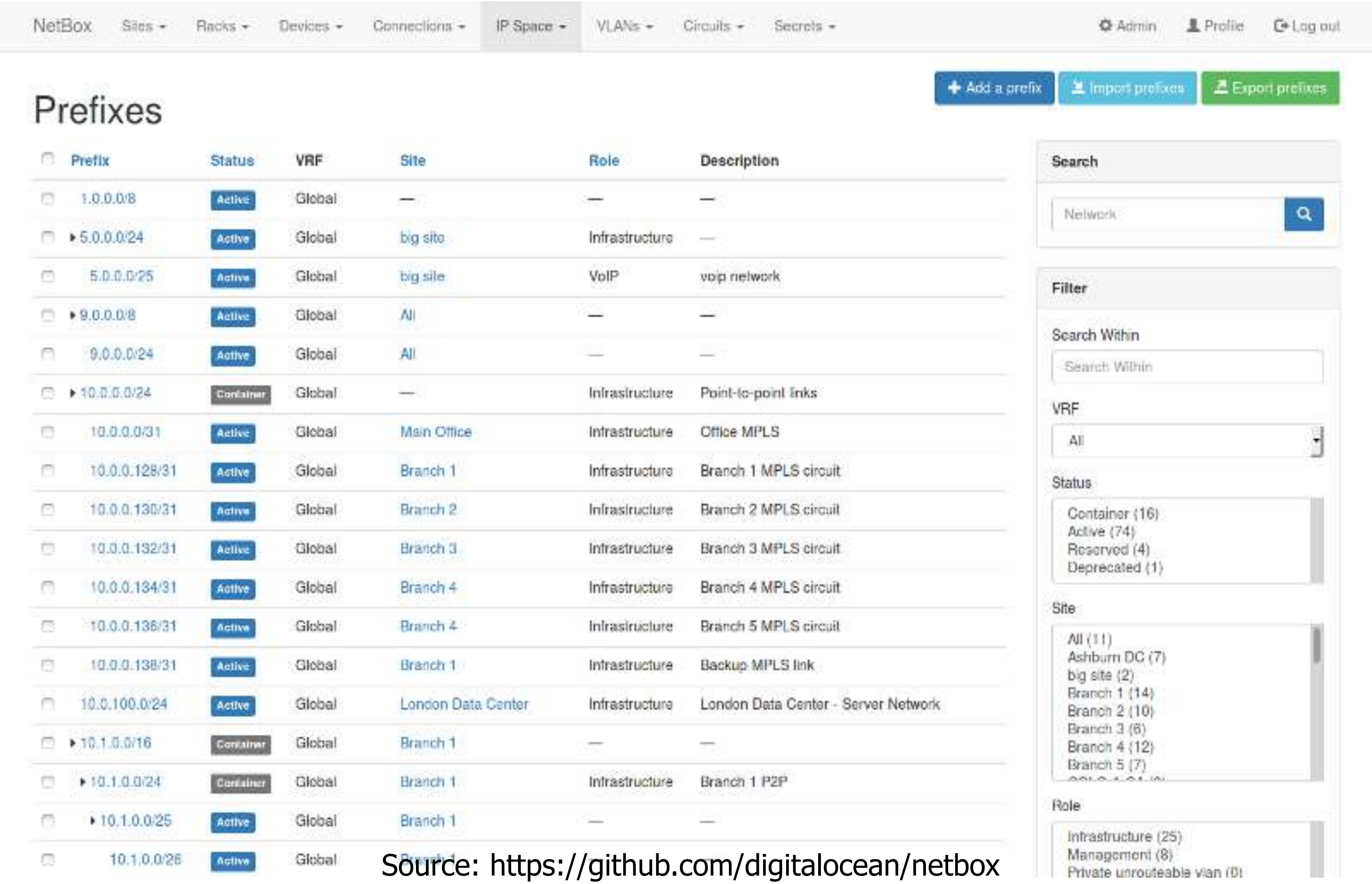
- Device Name, Device Role, Tenant
- HW Manufacturer, Model, OS, Serial Number
- Interface, Site, Rack, Position, Face

IPAM:IP address management

netbox_IP_addresses.csv

- IP Address, Device Role, Tenant
- Status, FQDN, Interface, Connected, Serial/MAC

NetBox (IPAM/DCIM)



Prefixes

□	Prefix	Status	VRF	Site	Role	Description
□	1.0.0.0/8	Active	Global	—	—	—
□	▸ 5.0.0.0/24	Active	Global	big site	Infrastructure	—
□	5.0.0.0/25	Active	Global	big site	VoIP	voip network
□	▸ 9.0.0.0/8	Active	Global	All	—	—
□	9.0.0.0/24	Active	Global	All	—	—
□	▸ 10.0.0.0/24	Container	Global	—	Infrastructure	Point-to-point links
□	10.0.0.0/31	Active	Global	Main Office	Infrastructure	Office MPLS
□	10.0.0.128/31	Active	Global	Branch 1	Infrastructure	Branch 1 MPLS circuit
□	10.0.0.130/31	Active	Global	Branch 2	Infrastructure	Branch 2 MPLS circuit
□	10.0.0.132/31	Active	Global	Branch 3	Infrastructure	Branch 3 MPLS circuit
□	10.0.0.134/31	Active	Global	Branch 4	Infrastructure	Branch 4 MPLS circuit
□	10.0.0.136/31	Active	Global	Branch 4	Infrastructure	Branch 5 MPLS circuit
□	10.0.0.138/31	Active	Global	Branch 1	Infrastructure	Backup MPLS link
□	10.0.100.0/24	Active	Global	London Data Center	Infrastructure	London Data Center - Server Network
□	▸ 10.1.0.0/16	Container	Global	Branch 1	—	—
□	▸ 10.1.0.0/24	Container	Global	Branch 1	Infrastructure	Branch 1 P2P
□	▸ 10.1.0.0/25	Active	Global	Branch 1	—	—
□	10.1.0.0/26	Active	Global	Branch 1	[illegible]	[illegible]

Search

Network

Filter

Search Within

Search Within

VRF

All

Status

Container (16)
Active (74)
Reserved (4)
Deprecated (1)

Site

All (11)
Ashburn DC (7)
big site (2)
Branch 1 (14)
Branch 2 (10)
Branch 3 (6)
Branch 4 (12)
Branch 5 (7)

Role

Infrastructure (25)
Management (8)
Private unrouteable vlan (0)

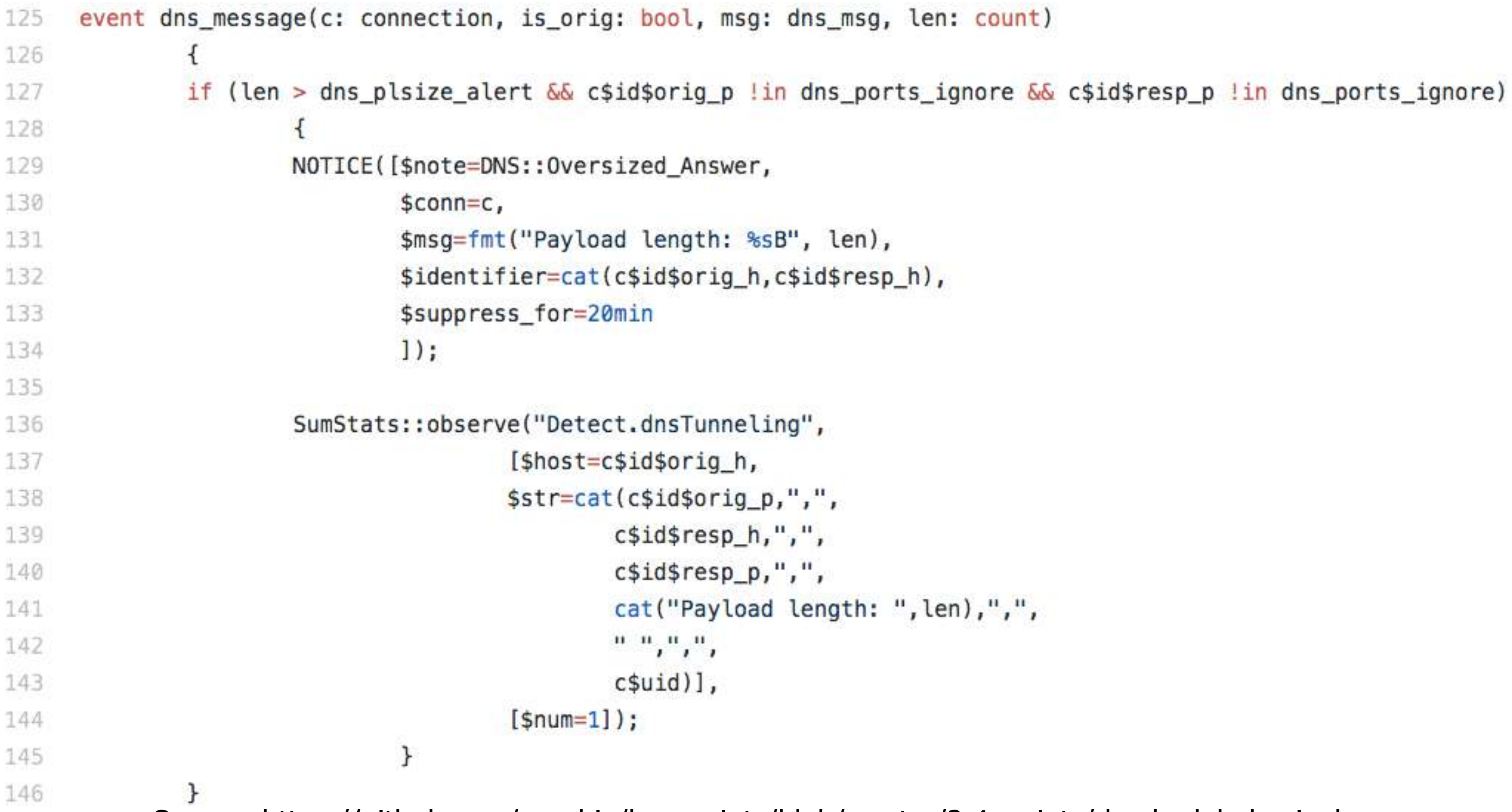
Source: https://github.com/digitalocean/netbox

Easy button

- nmap -vv -oN mynetwork.nmap 192.168.0.1/24
- https://github.com/maaaaz/nmaptocsv

```
$python nmaptocsv.py –i mynetwork.nmap /
ip–mac–fqdn–os–port–service–version
```

Bro-IDS for detecting deviant traffic

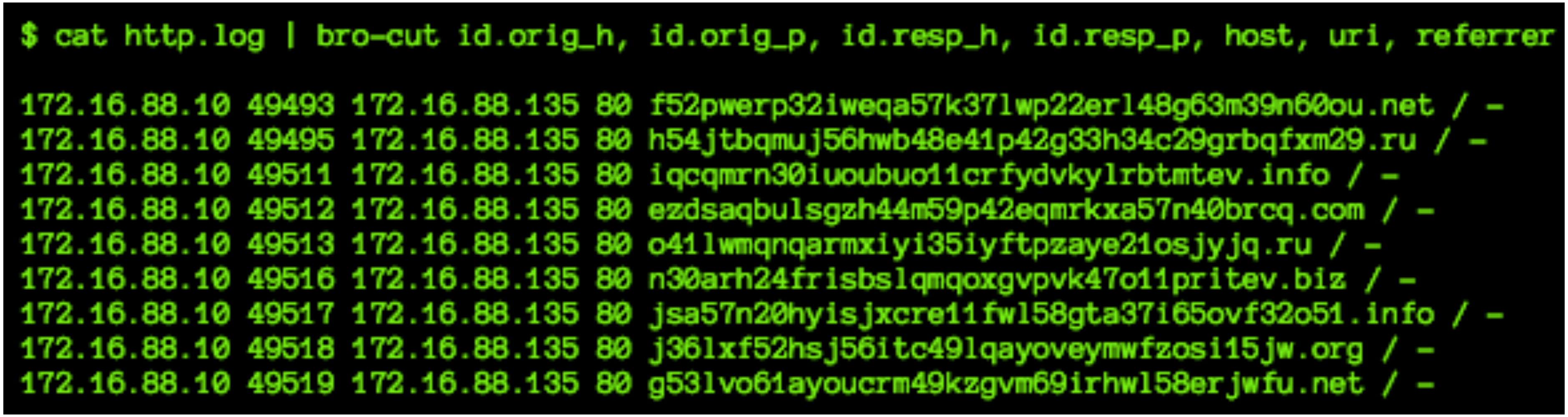


```
event dns_message(c: connection, is_orig: bool, msg: dns_msg, len: count)
        {
        if (len > dns_plsize_alert && c$id$orig_p !in dns_ports_ignore && c$id$resp_p !in dns_ports_ignore)
                {
                NOTICE([$note=DNS::Oversized_Answer,
                        $conn=c,
                        $msg=fmt("Payload length: %sB", len),
                        $identifier=cat(c$id$orig_h,c$id$resp_h),
                        $suppress_for=20min
                        ]);

                SumStats::observe("Detect.dnsTunneling",
                                [$host=c$id$orig_h,
                                $str=cat(c$id$orig_p,",",
                                        c$id$resp_h,",",
                                        c$id$resp_p,",",
                                        cat("Payload length: ",len),",",
                                        " ",",",
                                        c$uid)],
                                [$num=1]);
                        }
        }
```

Source: https://github.com/sooshie/bro-scripts/blob/master/2.4-scripts/dns-bad_behavior.bro

Interesting Domains



```
$ cat http.log | bro-cut id.orig_h, id.orig_p, id.resp_h, id.resp_p, host, uri, referrer

172.16.88.10 49493 172.16.88.135 80 f52pwerp32iweqa57k37lwp22erl48g63m39n60ou.net / -
172.16.88.10 49495 172.16.88.135 80 h54jtbqmuj56hwb48e41p42g33h34c29grbqfxm29.ru / -
172.16.88.10 49511 172.16.88.135 80 iqcqmrn30iuoubuo11crfydvkylrbtmtev.info / -
172.16.88.10 49512 172.16.88.135 80 ezdsaqbulsgzh44m59p42eqmrkxa57n40brcq.com / -
172.16.88.10 49513 172.16.88.135 80 o41lwmqnqarmxiyi35iyftpzaye21osjyjq.ru / -
172.16.88.10 49516 172.16.88.135 80 n30arh24frisbslqmqoxgvpvk47o11pritev.biz / -
172.16.88.10 49517 172.16.88.135 80 jsa57n20hyisjxcre11fwl58gta37i65ovf32o51.info / -
172.16.88.10 49518 172.16.88.135 80 j36lxf52hsj56itc49lqayoveymwfzosi15jw.org / -
172.16.88.10 49519 172.16.88.135 80 g53lvo61ayoucrm49kzgvm69irhwl58erjwfu.net / -
```

Network Forensics with Bro: https://github.com/aboutsecurity/Bro-samples
Output Source: http://blog.opensecurityresearch.com/2014/03/identifying-malware-traffic-with-bro.html
Lenny Zeltser REMnux “Toolkit for Analyzing & Reverse Engineering Malware”: https://remnux.org/

Data Enumeration

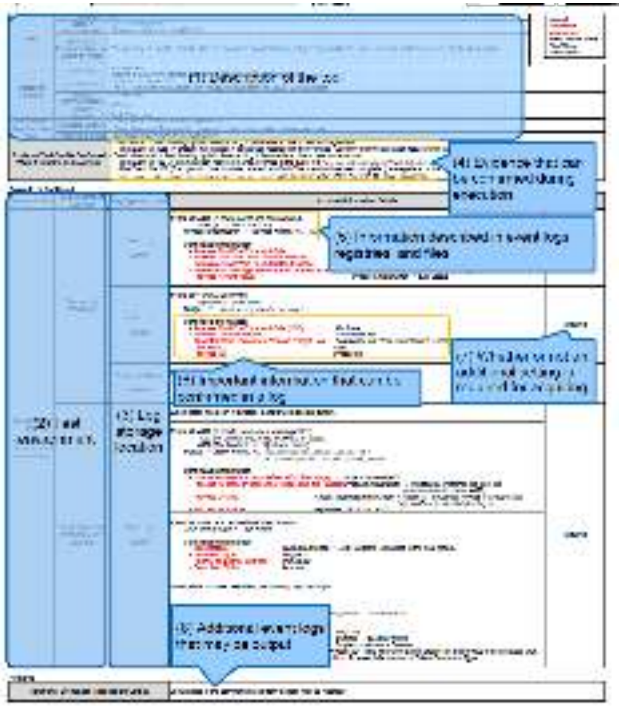
- Now that you’ve got a list of hosts and services, time to identify your data stores:
  - Start with Servers and Workstations turned Server
  - Have discussions with Third Party Vendors
  - Then address your IoT devices

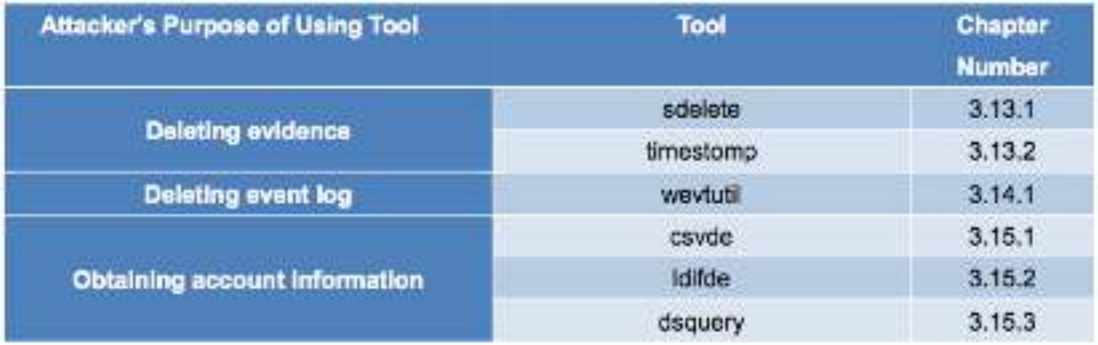
Data Enumeration (cont)

- Artifacts to collect
  - Type, Asset Unique ID, File Name, Description
  - Recipient, Data Custodian, Responsible Party
  - Primary Location, Criticality level, Classification
  - Restriction, Internal Share Loc, External Share Loc,
  - Internal Backup Loc, Off-Site Backup Loc
  - Public, Legal Restricted, Medical Restricted

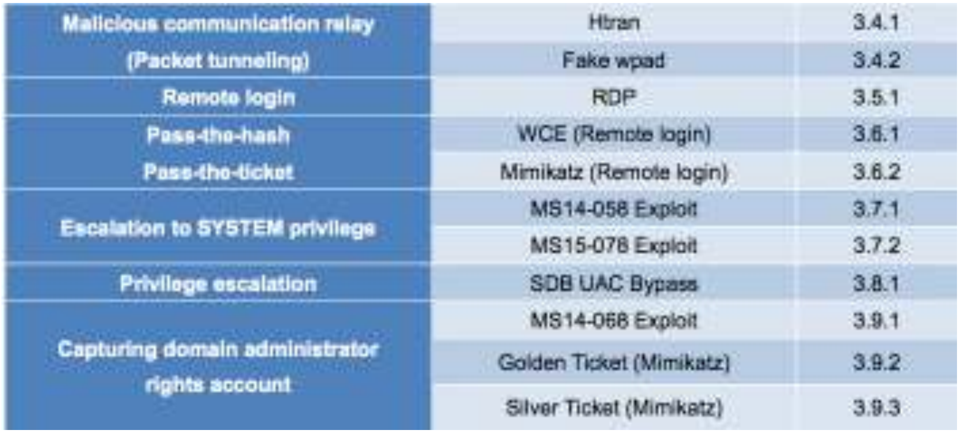
Detecting Pivots

- JPCERT Coordination Center: Detecting Lateral Movement through Tracking Event Logs





Attacker's Purpose of Using Tool	Tool	Chapter Number
Deleting evidence	sdelete	3.13.1
	timestomp	3.13.2
Deleting event log	wevtutil	3.14.1
Obtaining account information	csvde	3.15.1
	ldifde	3.15.2
	dsquery	3.15.3

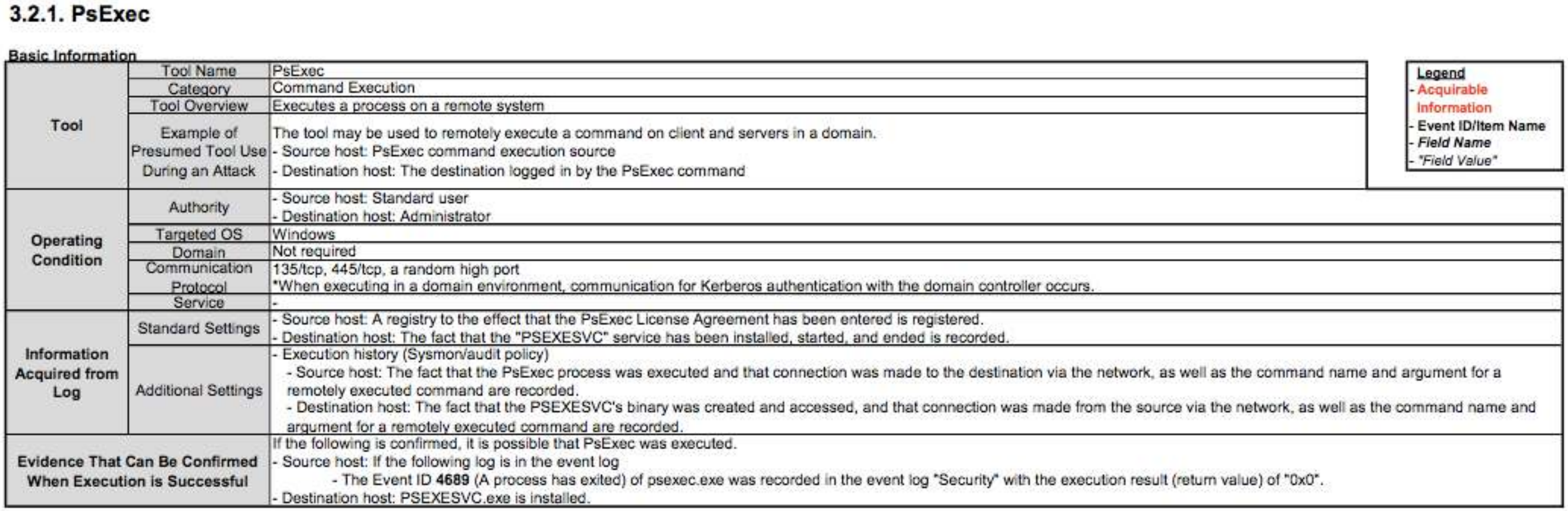


Malicious communication relay (Packet tunneling)	Htran	3.4.1
	Fake wpad	3.4.2
Remote login	RDP	3.5.1
Pass-the-hash Pass-the-ticket	WCE (Remote login)	3.6.1
	Mimikatz (Remote login)	3.6.2
Escalation to SYSTEM privilege	MS14-058 Exploit	3.7.1
	MS15-078 Exploit	3.7.2
Privilege escalation	SDB UAC Bypass	3.8.1
Capturing domain administrator rights account	MS14-068 Exploit	3.9.1
	Golden Ticket (Mimikatz)	3.9.2
	Silver Ticket (Mimikatz)	3.9.3

Source: JPCERT https://www.jpcert.or.jp/english/pub/sr/ir_research.html

Detecting PSEXEC

Detecting Lateral Movement through Tracking Event Logs



3.2.1. PsExec

Basic Information

Tool	Tool Name	PsExec
	Category	Command Execution
	Tool Overview	Executes a process on a remote system
	Example of Presumed Tool Use During an Attack	The tool may be used to remotely execute a command on client and servers in a domain. - Source host: PsExec command execution source - Destination host: The destination logged in by the PsExec command
Operating Condition	Authority	- Source host: Standard user - Destination host: Administrator
	Targeted OS	Windows
	Domain	Not required
	Communication Protocol	135/tcp, 445/tcp, a random high port *When executing in a domain environment, communication for Kerberos authentication with the domain controller occurs.
	Service	-
Information Acquired from Log	Standard Settings	- Source host: A registry to the effect that the PsExec License Agreement has been entered is registered. - Destination host: The fact that the "PSEXESVC" service has been installed, started, and ended is recorded.
	Additional Settings	- Execution history (Sysmon/audit policy) - Source host: The fact that the PsExec process was executed and that connection was made to the destination via the network, as well as the command name and argument for a remotely executed command are recorded. - Destination host: The fact that the PSEXESVC's binary was created and accessed, and that connection was made from the source via the network, as well as the command name and argument for a remotely executed command are recorded.
Evidence That Can Be Confirmed When Execution is Successful		If the following is confirmed, it is possible that PsExec was executed. - Source host: If the following log is in the event log - The Event ID **4689** (A process has exited) of psexec.exe was recorded in the event log "Security" with the execution result (return value) of "0x0". - Destination host: PSEXESVC.exe is installed.

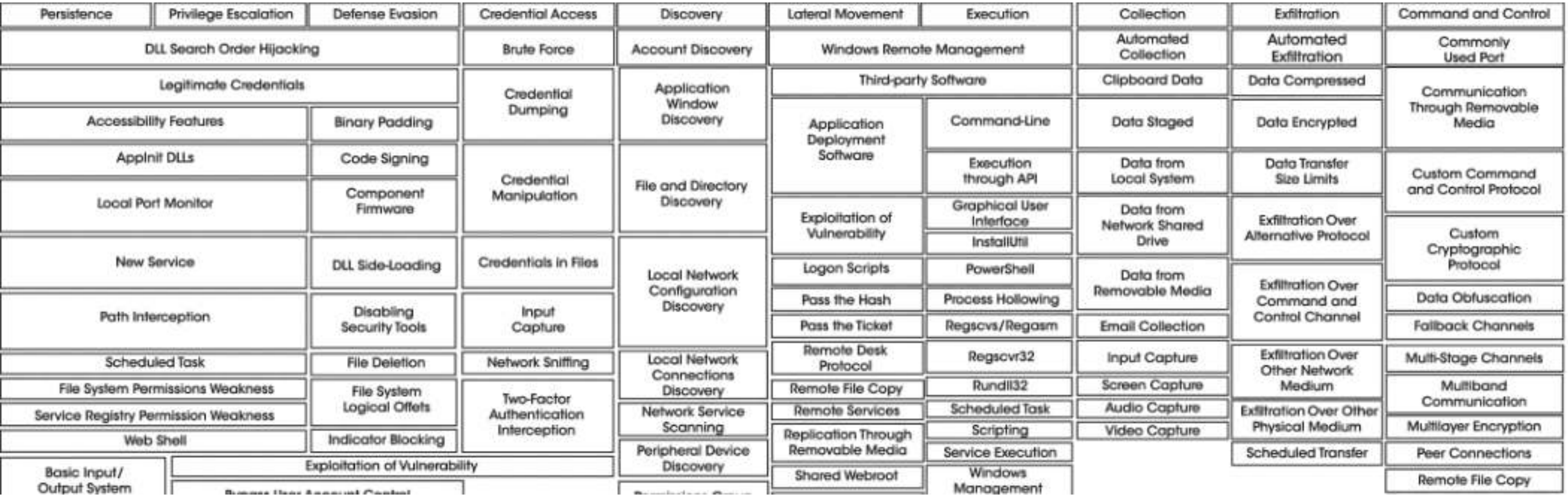
Legend
- Acquirable Information
- **Event ID/Item Name**
- ***Field Name***
- *"Field Value"*

Source: JPCERT https://www.jpcert.or.jp/english/pub/sr/ir_research.html

MITRE CAR & ATT&CK

- **C**yber **A**nalytics **R**epository
  - https://car.mitre.org/wiki/Main_Page
- **A**dversarial **T**actics, **T**echniques, **&**nd **C**ommon **K**nowledge
  - https://attack.mitre.org

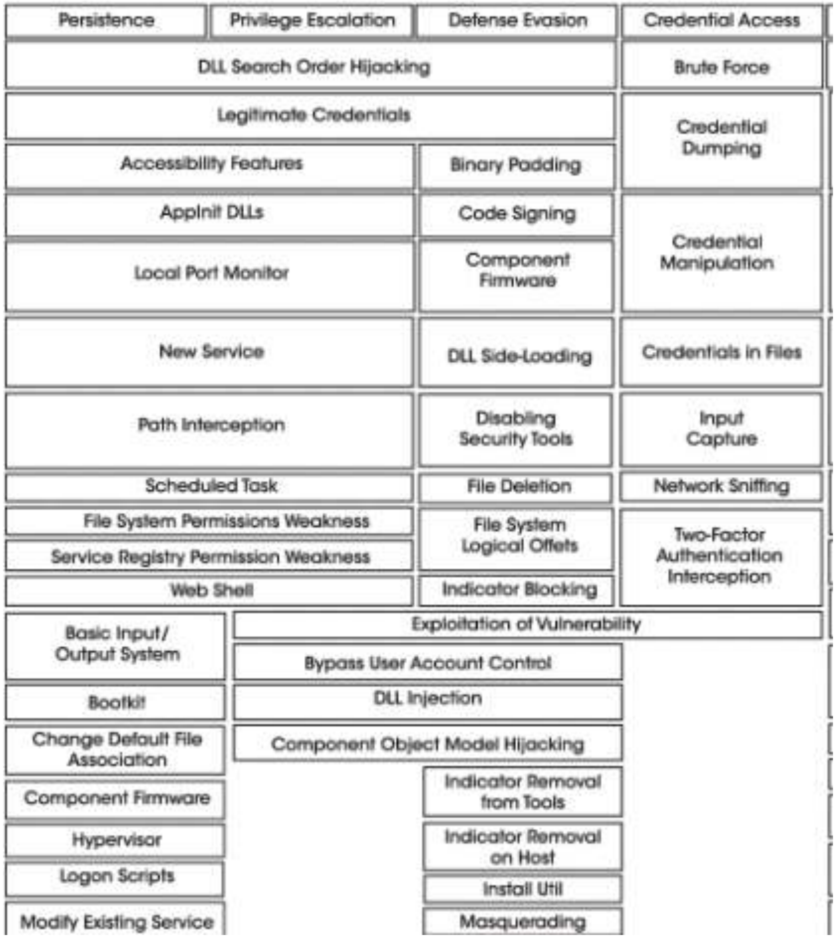
MITRE ATT&CK Matrix



Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
DLL Search Order Hijacking			Brute Force	Account Discovery	Windows Remote Management		Automated Collection	Automated Exfiltration	Commonly Used Port
Legitimate Credentials			Credential Dumping	Application Window Discovery	Third-party Software		Clipboard Data	Data Compressed	Communication Through Removable Media
Accessibility Features		Binary Padding	Credential Manipulation	File and Directory Discovery	Application Deployment Software	Command-Line	Data Staged	Data Encrypted	Custom Command and Control Protocol
AppInit DLLs		Code Signing	Credentials in Files	Local Network Configuration Discovery	Exploitation of Vulnerability	Execution through API	Data from Local System	Data Transfer Size Limits	Custom Cryptographic Protocol
Local Port Monitor		Component Firmware	Input Capture	Local Network Connections Discovery	Logon Scripts	Graphical User Interface	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	Data Obfuscation
New Service		DLL Side-Loading	Network Sniffing	Network Service Scanning	Pass the Hash	InstallUtil	Data from Removable Media	Exfiltration Over Command and Control Channel	Fallback Channels
Path Interception		Disabling Security Tools	Two-Factor Authentication Interception	Peripheral Device Discovery	Pass the Ticket	PowerShell	Email Collection	Exfiltration Over Other Network Medium	Multi-Stage Channels
Scheduled Task		File Deletion			Remote Desk Protocol	Process Hollowing	Input Capture	Exfiltration Over Other Physical Medium	Multiband Communication
File System Permissions Weakness		File System Logical Offets			Remote File Copy	Regscvs/Regasm	Screen Capture	Scheduled Transfer	Multilayer Encryption
Service Registry Permission Weakness		Indicator Blocking			Remote Services	Regscvr32	Audio Capture		Peer Connections
Web Shell					Replication Through Removable Media	Rundll32	Video Capture		Remote File Copy
Basic Input/ Output System	Exploitation of Vulnerability				Shared Webroot	Scheduled Task			
						Scripting			
						Service Execution			
						Windows Management			

Source: https://attack.mitre.org/w/images/8/87/ATTaCK_Matrix.png

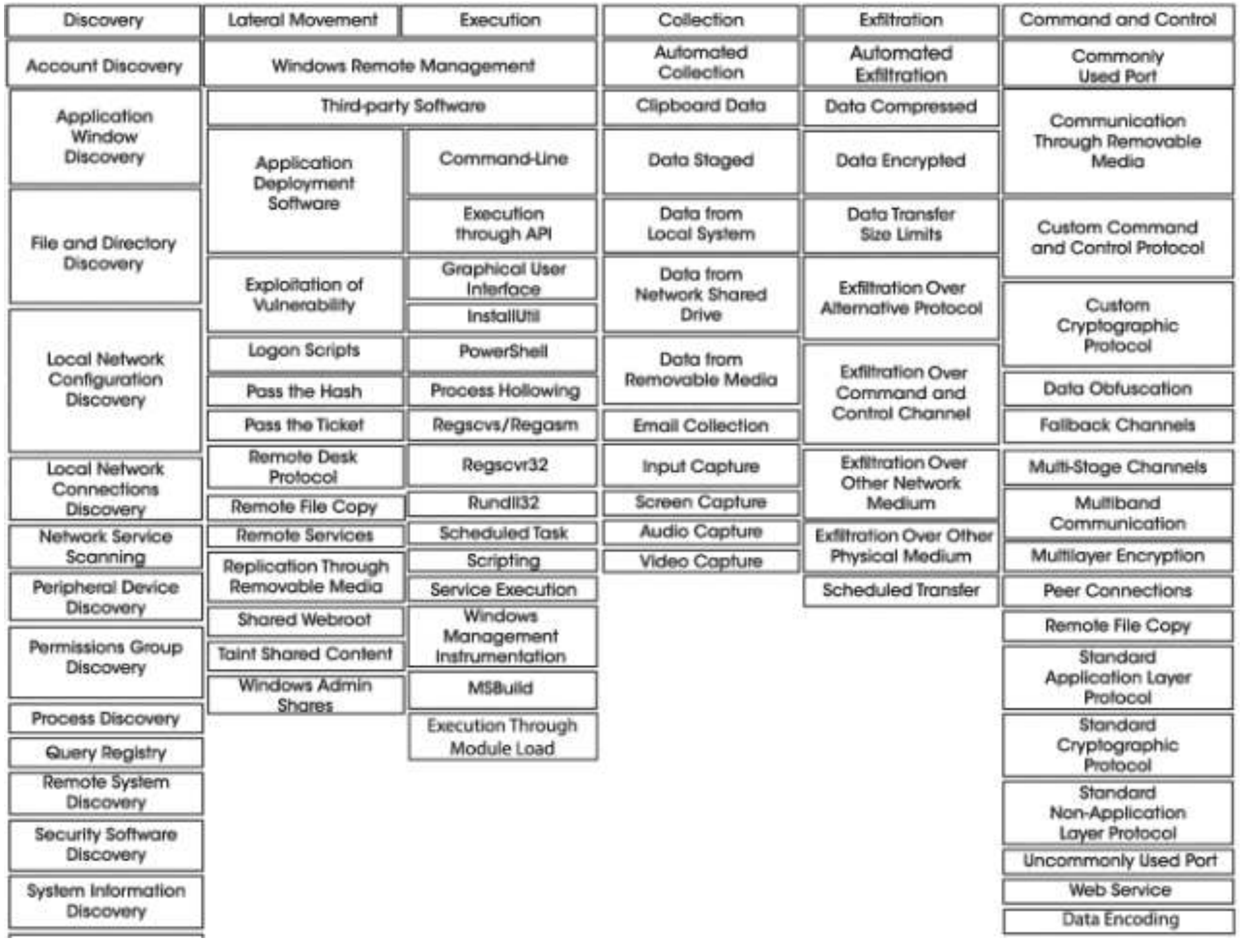
MITRE ATT&CK Matrix



Persistence	Privilege Escalation	Defense Evasion	Credential Access
DLL Search Order Hijacking			Brute Force
Legitimate Credentials			Credential Dumping
Accessibility Features		Binary Padding	
AppInit DLLs		Code Signing	Credential Manipulation
Local Port Monitor		Component Firmware	
New Service		DLL Side-Loading	Credentials in Files
Path Interception		Disabling Security Tools	Input Capture
Scheduled Task		File Deletion	Network Sniffing
File System Permissions Weakness		File System Logical Offets	Two-Factor Authentication Interception
Service Registry Permission Weakness			
Web Shell		Indicator Blocking	
Basic Input/ Output System	Exploitation of Vulnerability		
	Bypass User Account Control		
Bootkit	DLL Injection		
Change Default File Association	Component Object Model Hijacking		
Component Firmware		Indicator Removal from Tools	
Hypervisor		Indicator Removal on Host	
Logon Scripts		Install Util	
Modify Existing Service		Masquerading	

Source: https://attack.mitre.org/w/images/8/87/ATTaCK_Matrix.png

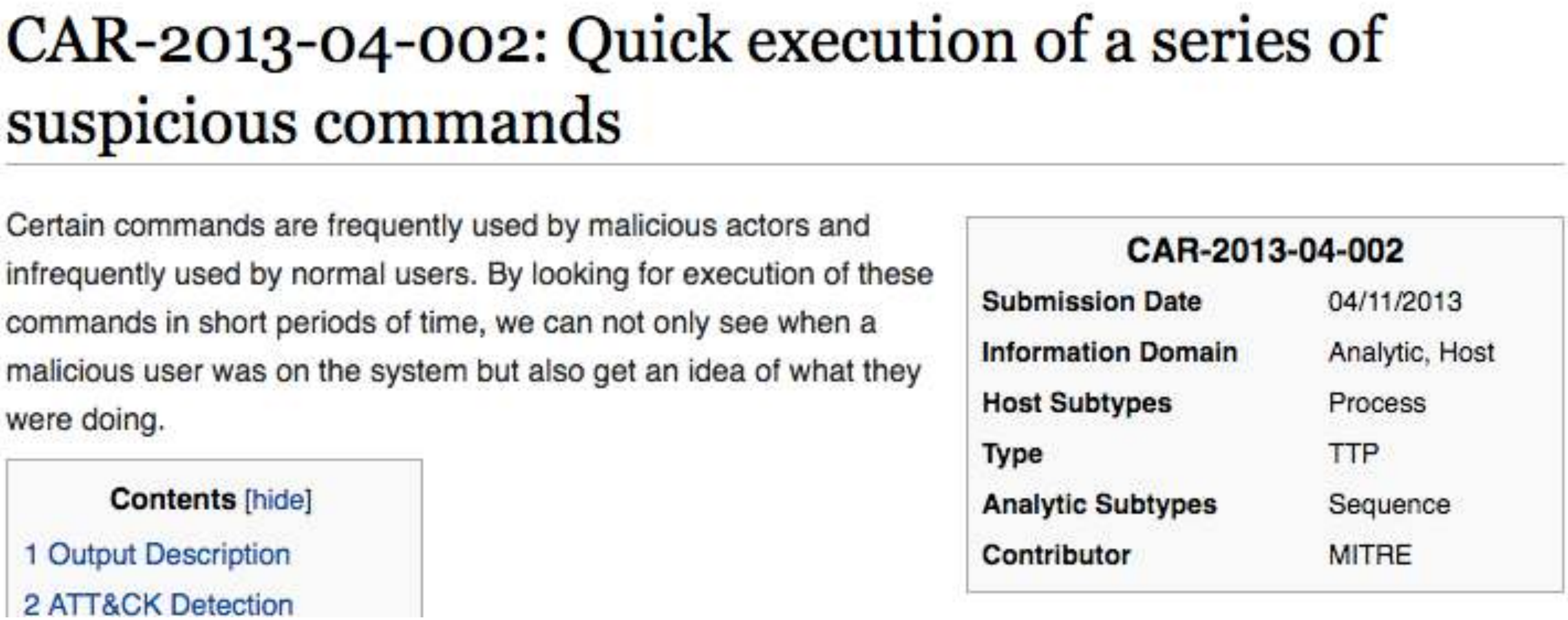
MITRE ATT&CK Matrix



Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Account Discovery	Windows Remote Management	Windows Remote Management	Automated Collection	Automated Exfiltration	Commonly Used Port
Application Window Discovery	Third-party Software	Third-party Software	Clipboard Data	Data Compressed	Communication Through Removable Media
File and Directory Discovery	Application Deployment Software	Command-Line	Data Staged	Data Encrypted	Custom Command and Control Protocol
Local Network Configuration Discovery	Exploitation of Vulnerability	Execution through API	Data from Local System	Data Transfer Size Limits	Custom Cryptographic Protocol
Local Network Connections Discovery	Logon Scripts	Graphical User Interface	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	Data Obfuscation
Network Service Scanning	Pass the Hash	InstallUtil	Data from Removable Media	Exfiltration Over Command and Control Channel	Fallback Channels
Peripheral Device Discovery	Pass the Ticket	PowerShell	Email Collection	Exfiltration Over Other Network Medium	Multi-Stage Channels
Permissions Group Discovery	Remote Desk Protocol	Process Hollowing	Input Capture	Exfiltration Over Other Physical Medium	Multiband Communication
Process Discovery	Remote File Copy	Regscvs/Regasm	Screen Capture	Scheduled Transfer	Multilayer Encryption
Query Registry	Remote Services	Regscvr32	Audio Capture		Peer Connections
Remote System Discovery	Replication Through Removable Media	Rundll32	Video Capture		Remote File Copy
Security Software Discovery	Shared Webroot	Scheduled Task			Standard Application Layer Protocol
System Information Discovery	Taint Shared Content	Scripting			Standard Cryptographic Protocol
	Windows Admin Shares	Service Execution			Standard Non-Application Layer Protocol
		Windows Management Instrumentation			Uncommonly Used Port
		MSBuild			Web Service
		Execution Through Module Load			Data Encoding

Source: https://attack.mitre.org/w/images/8/87/ATTaCK_Matrix.png

Removing the Low Hanging Fruit



CAR-2013-04-002: Quick execution of a series of suspicious commands

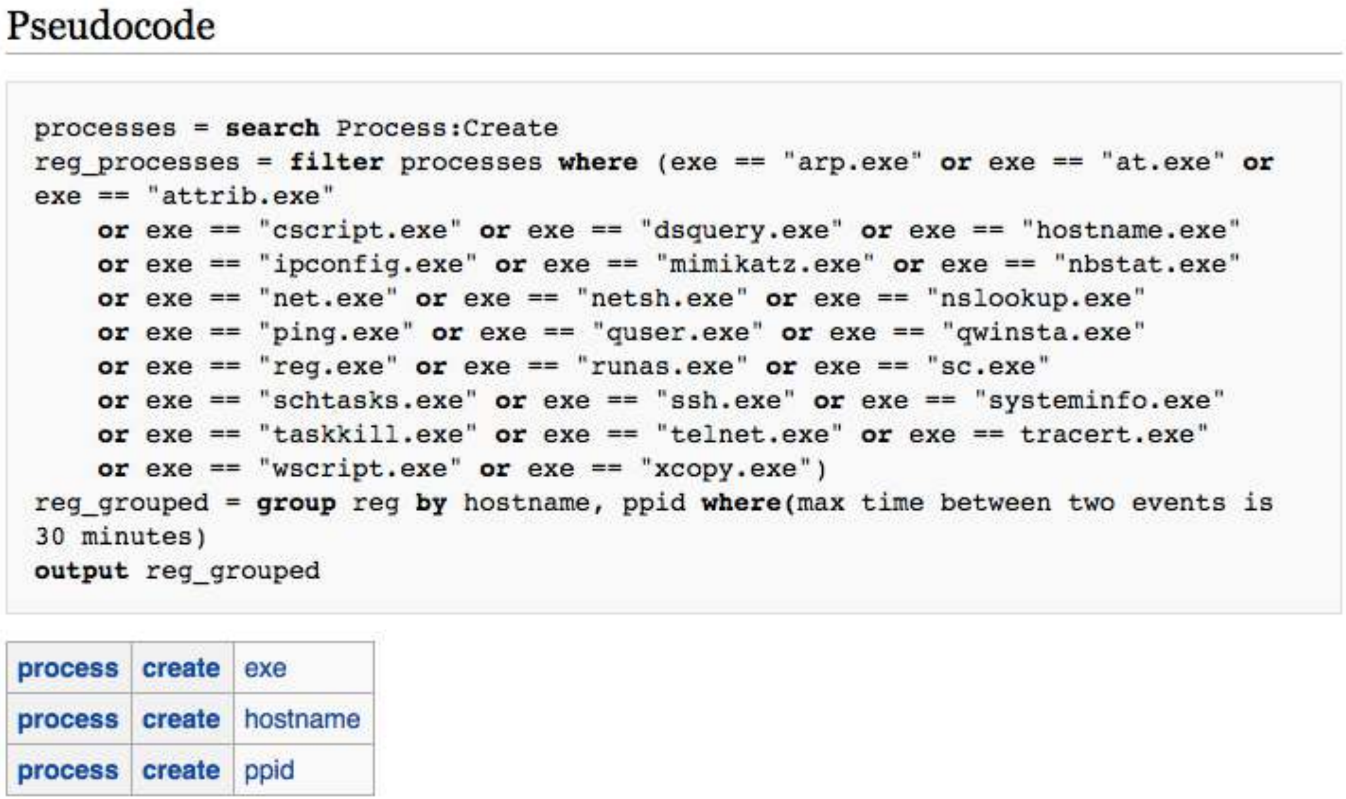
Certain commands are frequently used by malicious actors and infrequently used by normal users. By looking for execution of these commands in short periods of time, we can not only see when a malicious user was on the system but also get an idea of what they were doing.

CAR-2013-04-002	
Submission Date	04/11/2013
Information Domain	Analytic, Host
Host Subtypes	Process
Type	TTP
Analytic Subtypes	Sequence
Contributor	MITRE

Contents [hide]

Source: https://car.mitre.org/wiki/Main_Page

search Process:Create



Pseudocode

```
processes = search Process:Create
reg_processes = filter processes where (exe == "arp.exe" or exe == "at.exe" or
exe == "attrib.exe"
    or exe == "cscript.exe" or exe == "dsquery.exe" or exe == "hostname.exe"
    or exe == "ipconfig.exe" or exe == "mimikatz.exe" or exe == "nbstat.exe"
    or exe == "net.exe" or exe == "netsh.exe" or exe == "nslookup.exe"
    or exe == "ping.exe" or exe == "quser.exe" or exe == "qwinsta.exe"
    or exe == "reg.exe" or exe == "runas.exe" or exe == "sc.exe"
    or exe == "schtasks.exe" or exe == "ssh.exe" or exe == "systeminfo.exe"
    or exe == "taskkill.exe" or exe == "telnet.exe" or exe == tracert.exe"
    or exe == "wscript.exe" or exe == "xcopy.exe")
reg_grouped = group reg by hostname, ppid where(max time between two events is
30 minutes)
output reg_grouped
```

process	create	exe
process	create	hostname
process	create	ppid

Source: https://car.mitre.org/wiki/Main_Page

Removing the Low Hanging Fruit

Source: gfycat.com/HilariousSophisticatedGlowworm

The secret? Once enumerated, it’s all low hanging fruit

Thank you!

Security B-Sides MSP 2017 starts Saturday

BSidesMSP.ORG

Email mjh@itys.net
for tonights talk or
check @mjharmon
on twitter next week