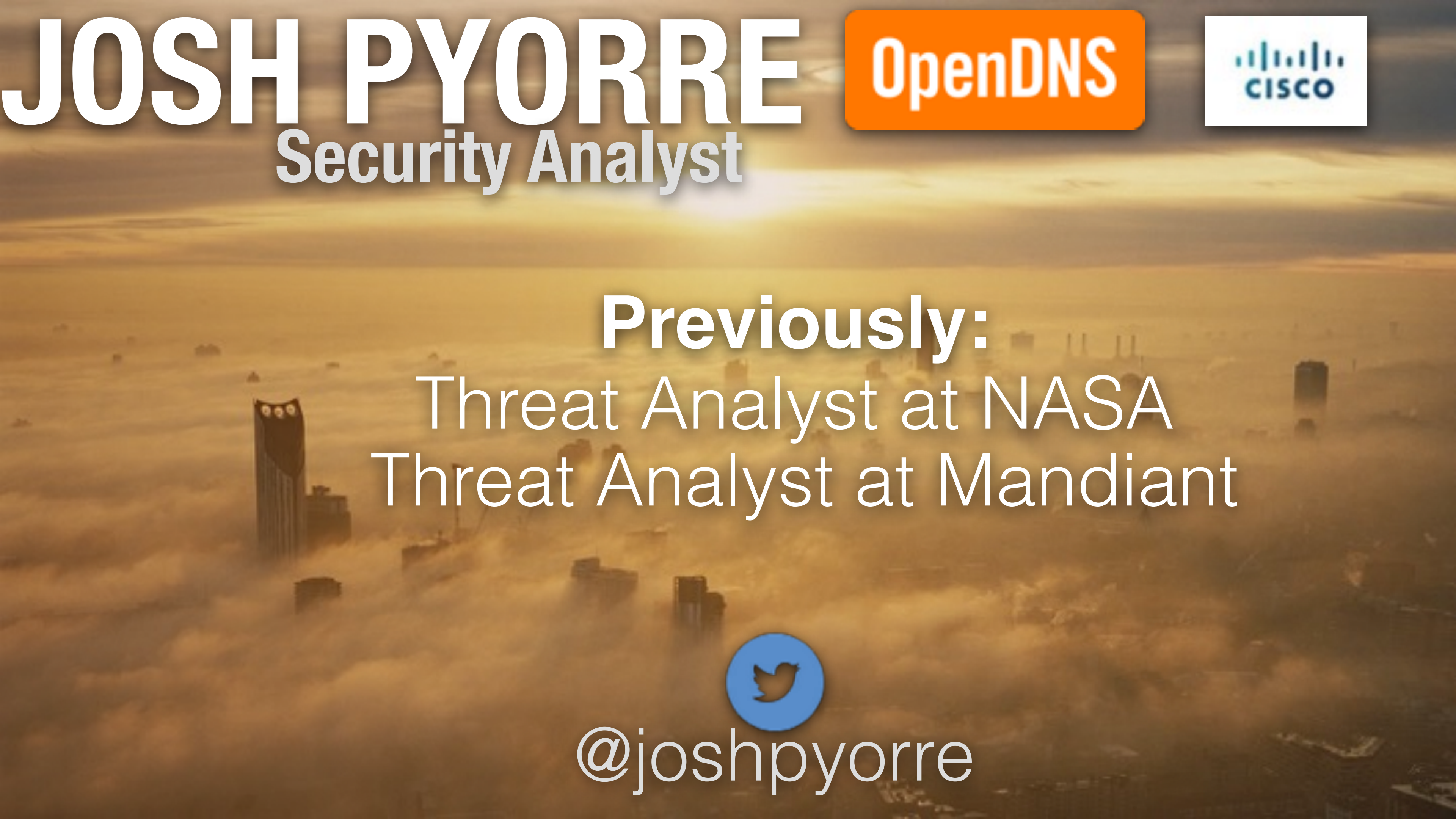
The Modern SOC

Adapting to how we work

Josh Pyorre



JOSH PYORRE

OpenDNS

cisco

Security Analyst

Previously:

Threat Analyst at NASA

Threat Analyst at Mandiant

@joshpyorre

rootaccesspodcast.com

A closer look at the notable stories inside Information Security and why they matter.

I have a podcast!

The Modern SOC

Adapting the Security Operations model to how we work.

- The Classic SOC Model
- SOC as a Service
- The Security Landscape
- Gaps
- **Adapting to Now**

Security Operations Center

Overview

Purpose

Monitoring, Detection and Reporting

Risk Assessment

Threat Intel

Vulnerability Mitigation

Overview

What the SOC Protects

- Data
- PII
- Users, from themselves…
- Systems

The SOC

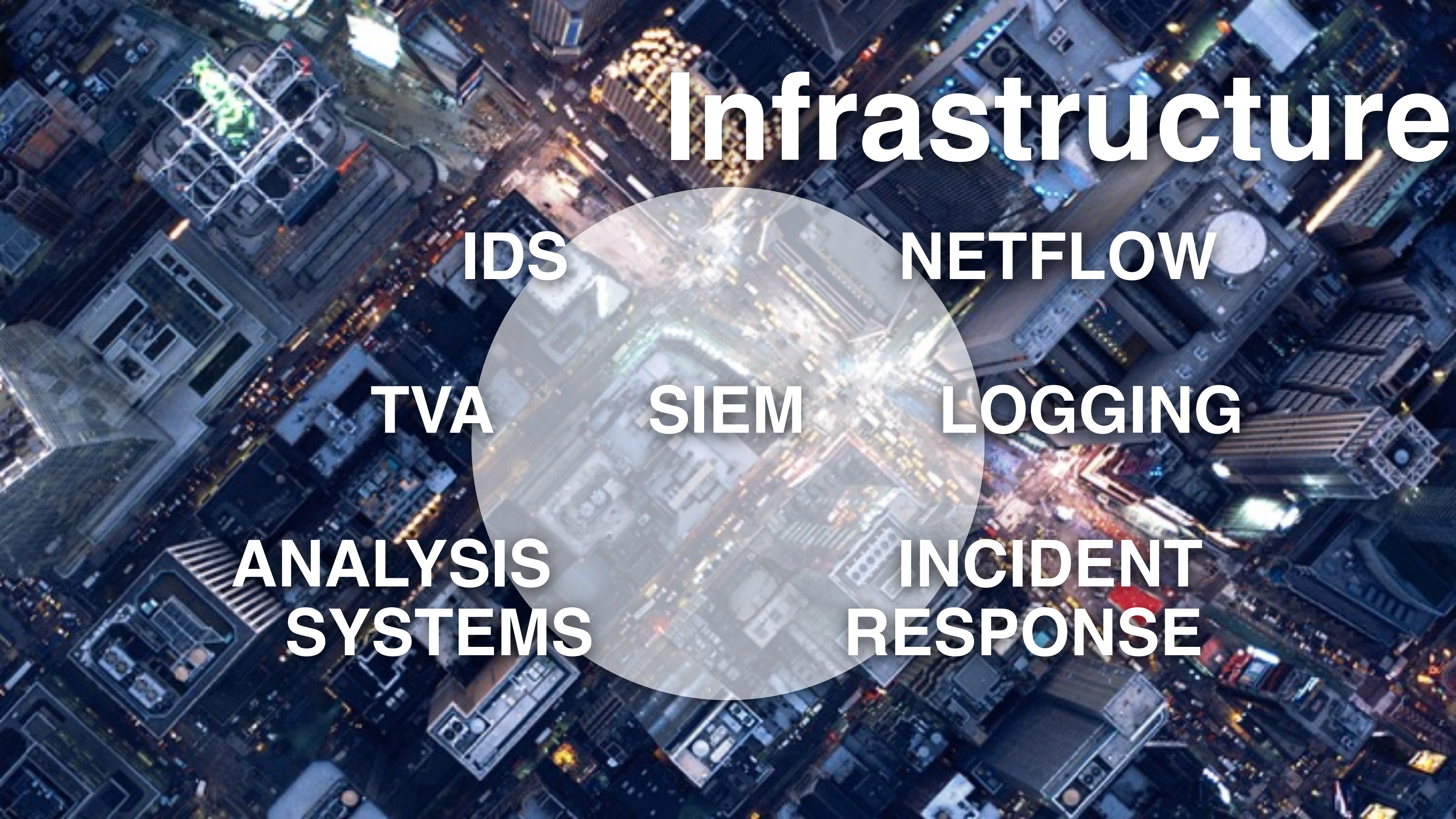
General workflow

- Collect
  - IDS Alerts, Logs, Network Flow
- Organize
  - Sinkhole, Databases, Categorization, Inventory, Log Aggregation
- Analyze
  - Anomalies, Alerts, patterns
- Report
  - Stats, Communication, contact levels, consistent info
- **Incident Response**
  - Your customers

The Classic Model

Infrastructure

Infrastructure



IDS

NETFLOW

TVA

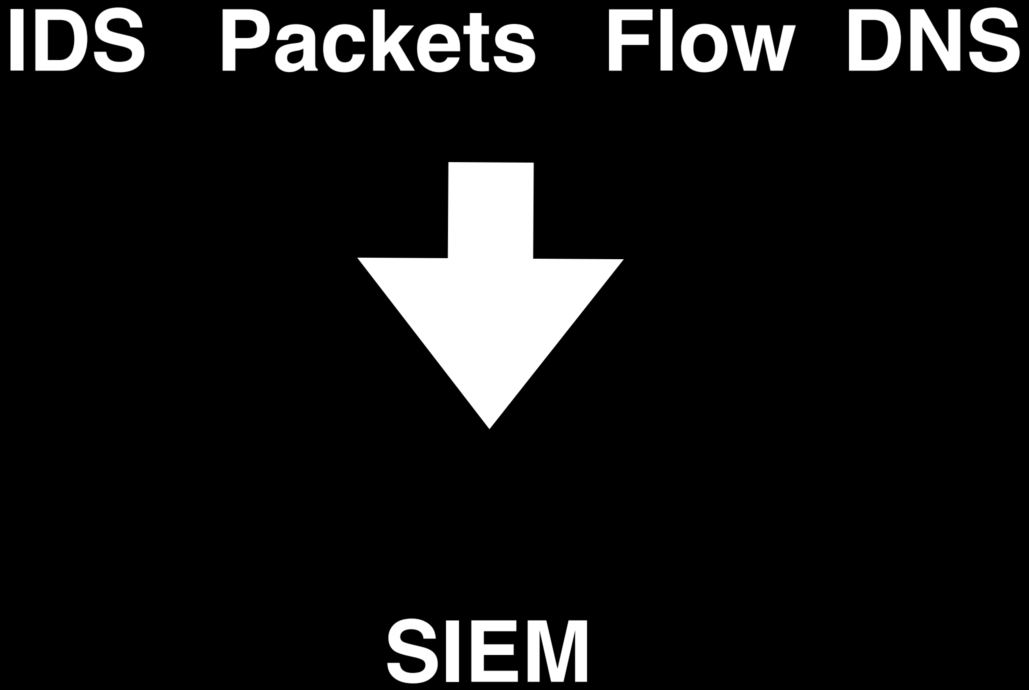
SIEM

LOGGING

ANALYSIS SYSTEMS

INCIDENT RESPONSE

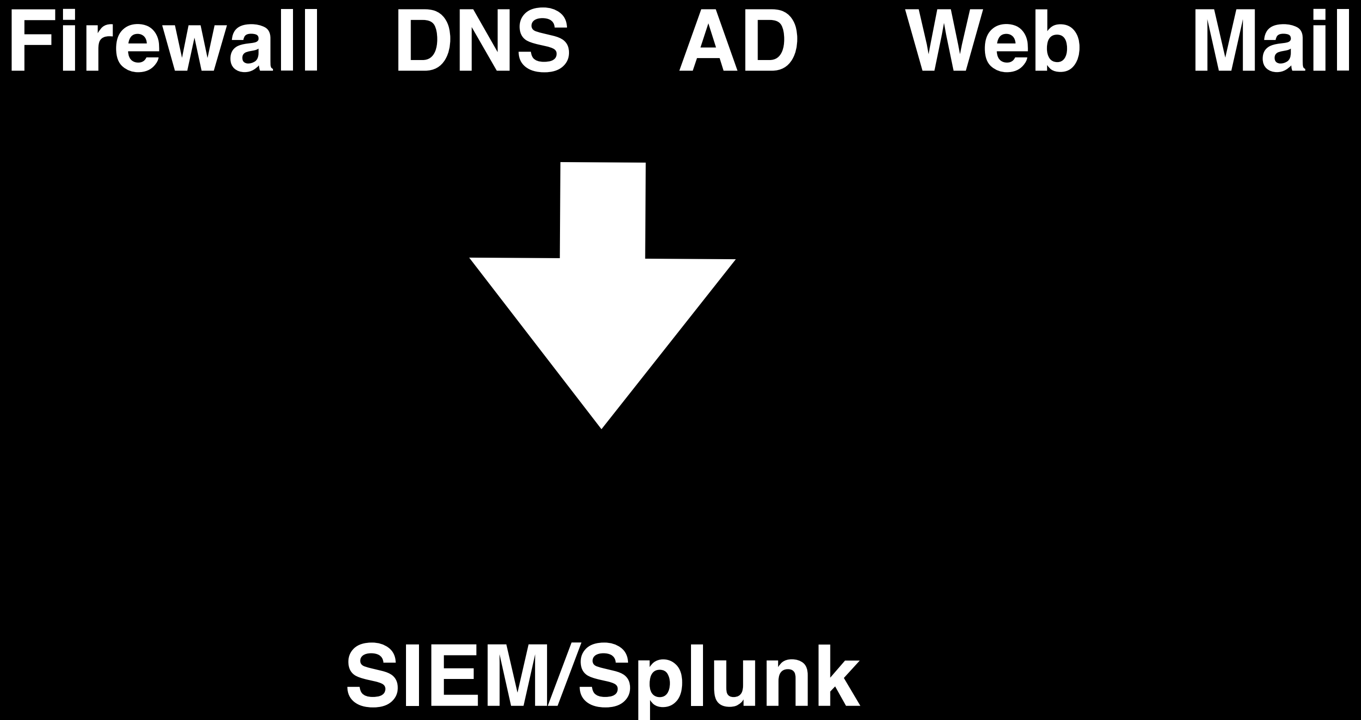
Network



IDS Packets Flow DNS

SIEM

Log Aggregation



Firewall DNS AD Web Mail

SIEM/Splunk

Email

Flow Attachments Phishing

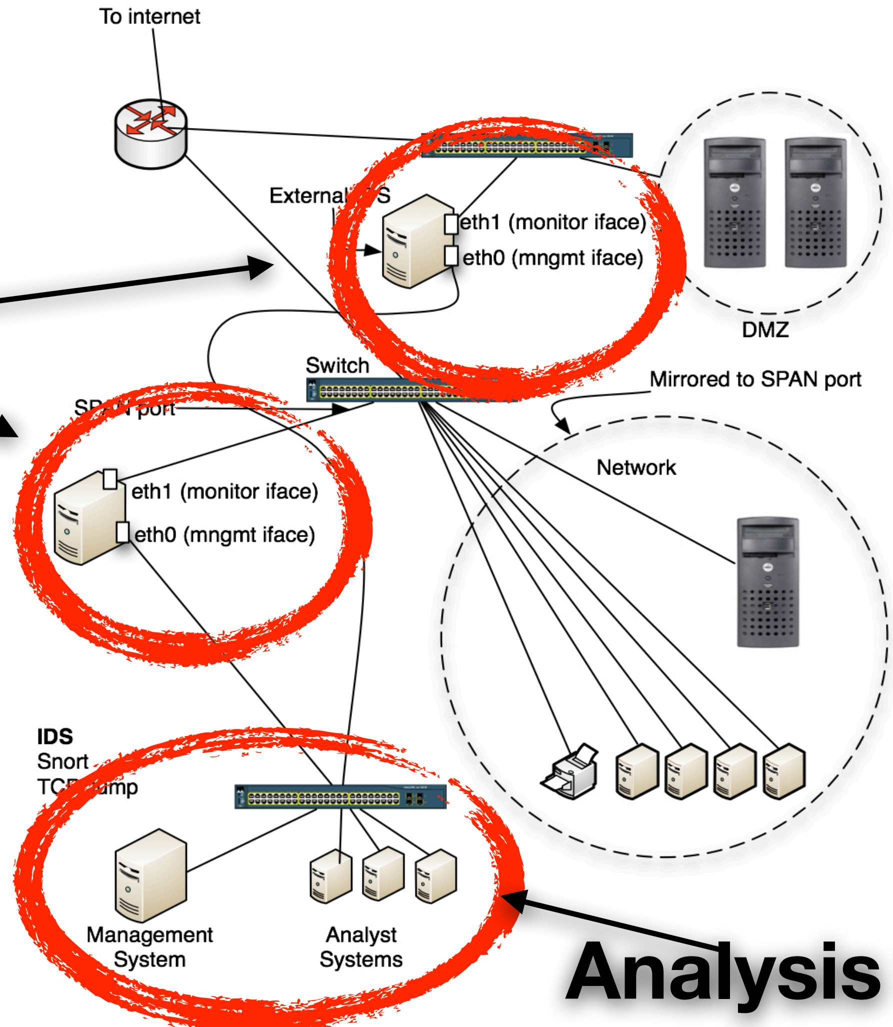
↓

SIEM

Infrastructure

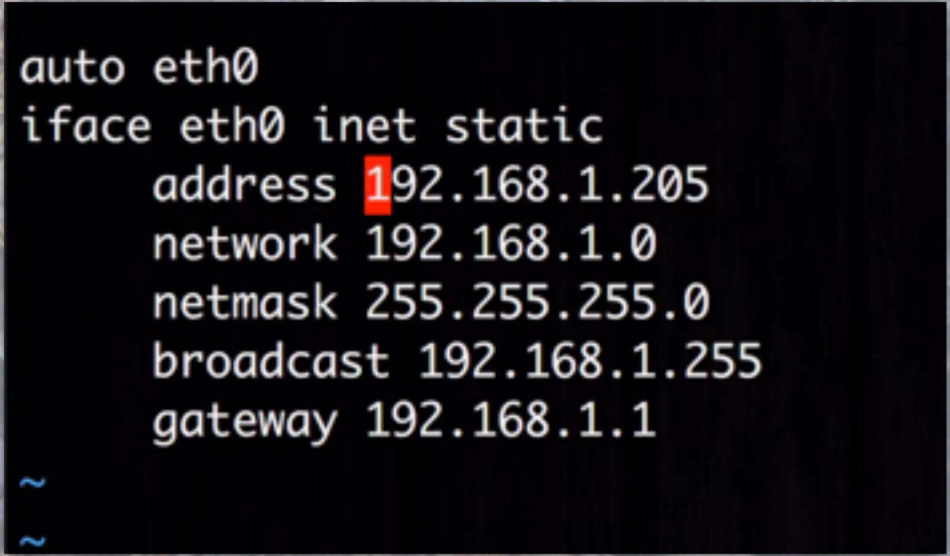
The Classic Model

IDS



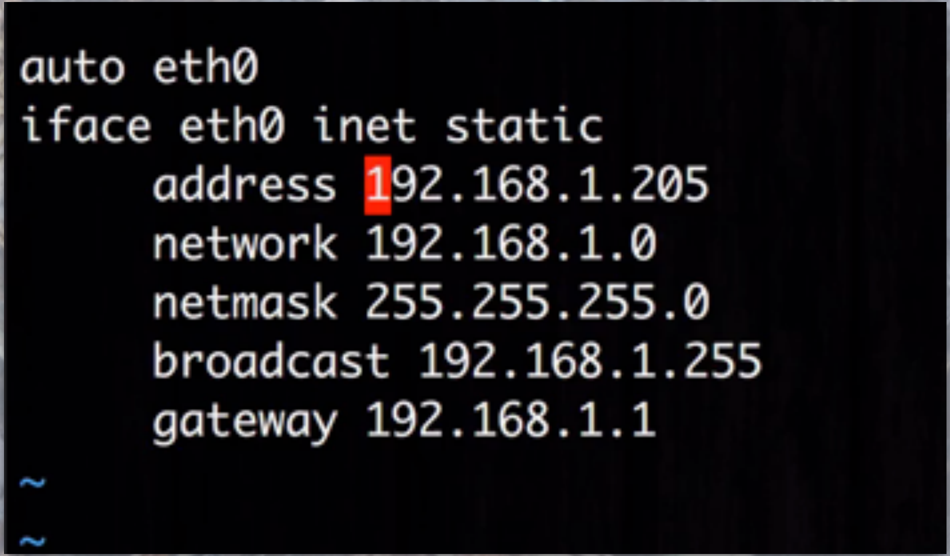
Analysis Systems

Don’t give the Interface an IP address



```
auto eth0
iface eth0 inet static
        address 192.168.1.205
        network 192.168.1.0
        netmask 255.255.255.0
        broadcast 192.168.1.255
        gateway 192.168.1.1

~
~
```

Don’t give the Interface an IP address



```
auto eth0
iface eth0 inet static
        address 192.168.1.205
        network 192.168.1.0
        netmask 255.255.255.0
        broadcast 192.168.1.255
        gateway 192.168.1.1
~
~
```

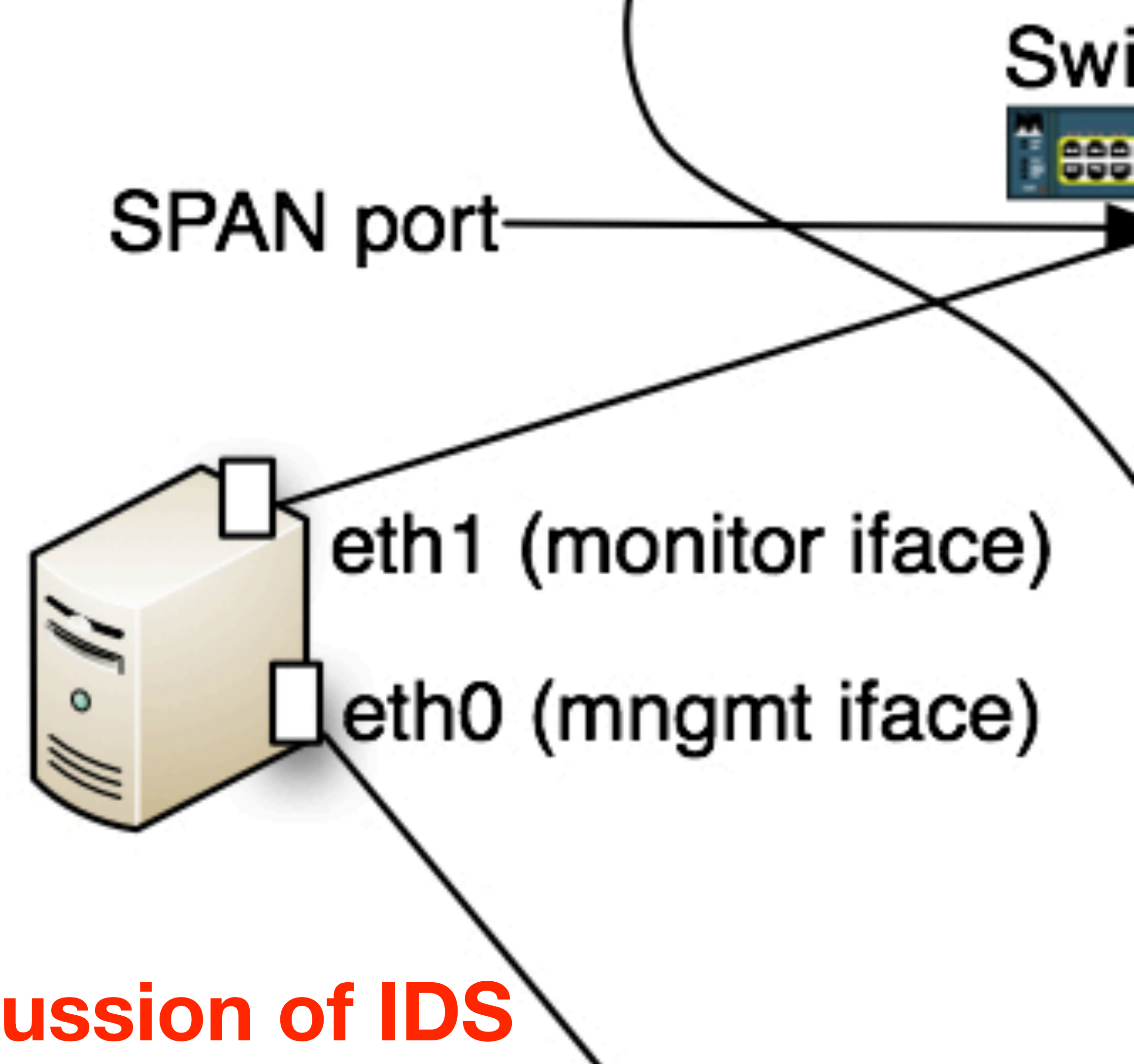
Can still respond to protocols below IP stack

Cut pin one (orange/white)

Solder a 23 pF capacitor

Infrastructure

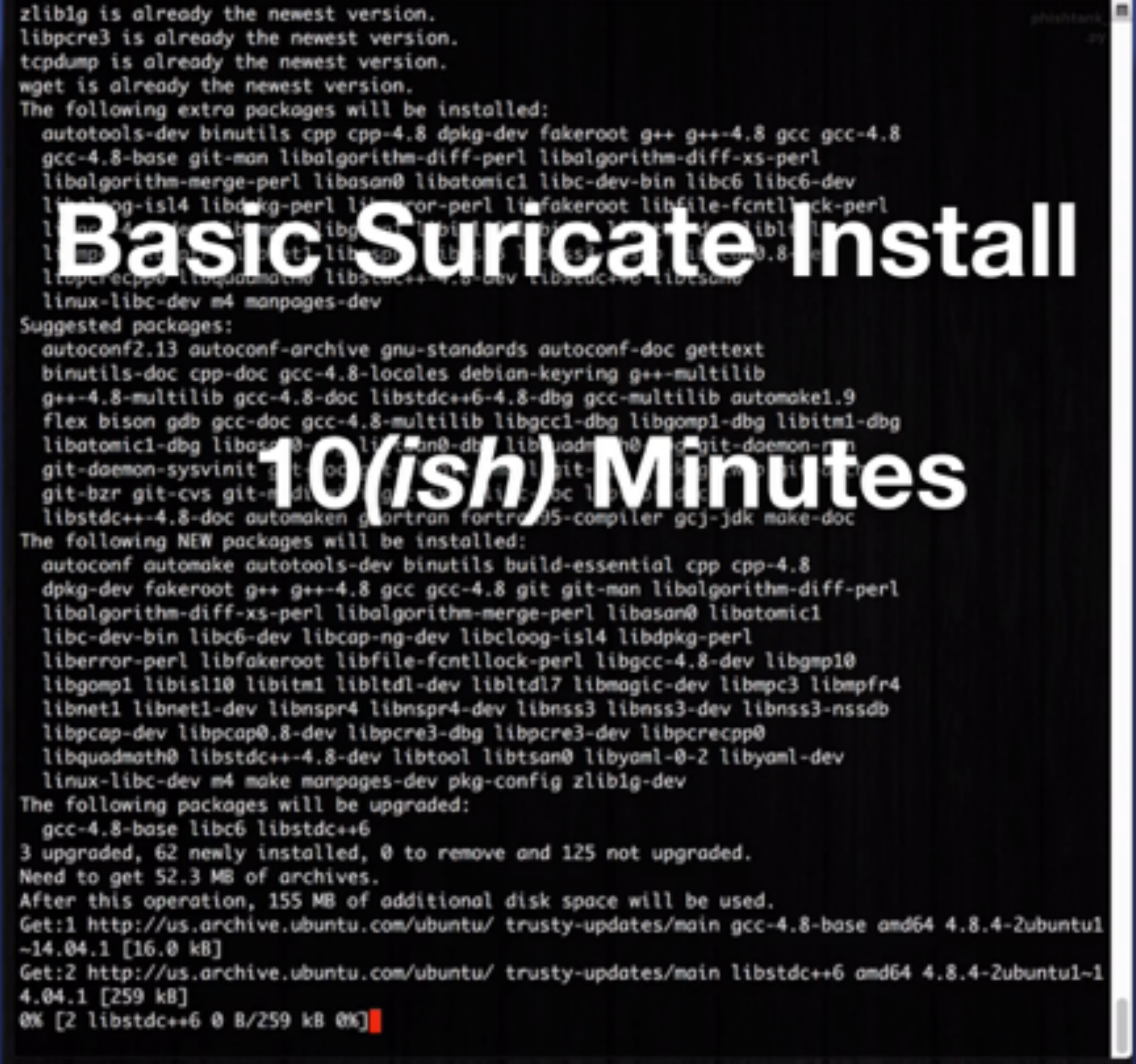
The Classic Model



A discussion of IDS

Basic Suricate Install

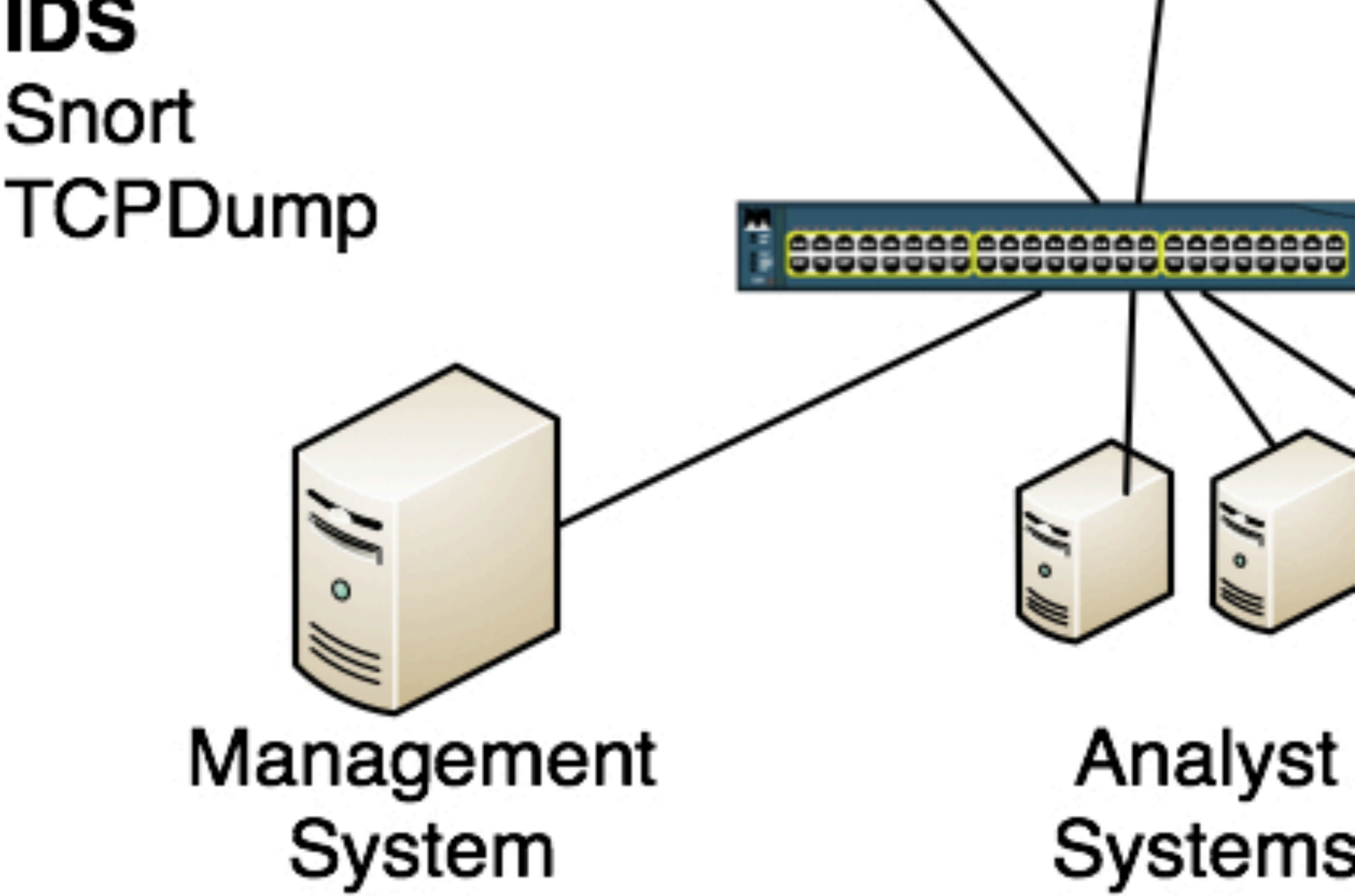
10(*ish*) Minutes



```
zlib1g is already the newest version.
libpcre3 is already the newest version.
tcpdump is already the newest version.
wget is already the newest version.
The following extra packages will be installed:
  autotools-dev binutils cpp cpp-4.8 dpkg-dev fakeroot g++ g++-4.8 gcc gcc-4.8
  gcc-4.8-base git-man libalgorithm-diff-perl libalgorithm-diff-xs-perl
  libalgorithm-merge-perl libasan0 libatomic1 libc-dev-bin libc6 libc6-dev
  libcloog-isl4 libdpkg-perl liberror-perl libfakeroot libfile-fcntllock-perl
  [illegible]
  [illegible]
  libpcrecpp0 libquadmath0 libstdc++-4.8-dev libstdc++6 libtsan0
  linux-libc-dev m4 manpages-dev
Suggested packages:
  autoconf2.13 autoconf-archive gnu-standards autoconf-doc gettext
  binutils-doc cpp-doc gcc-4.8-locales debian-keyring g++-multilib
  g++-4.8-multilib gcc-4.8-doc libstdc++6-4.8-dbg gcc-multilib automake1.9
  flex bison gdb gcc-doc gcc-4.8-multilib libgcc1-dbg libgomp1-dbg libitm1-dbg
  libatomic1-dbg libasan0-[illegible] libtsan0-dbg libquadmath0-dbg git-daemon-run
  git-daemon-sysvinit [illegible]
  git-bzr git-cvs git-[illegible]
  libstdc++-4.8-doc automaken gfortran fortran95-compiler gcj-jdk make-doc
The following NEW packages will be installed:
  autoconf automake autotools-dev binutils build-essential cpp cpp-4.8
  dpkg-dev fakeroot g++ g++-4.8 gcc gcc-4.8 git git-man libalgorithm-diff-perl
  libalgorithm-diff-xs-perl libalgorithm-merge-perl libasan0 libatomic1
  libc-dev-bin libc6-dev libcap-ng-dev libcloog-isl4 libdpkg-perl
  liberror-perl libfakeroot libfile-fcntllock-perl libgcc-4.8-dev libgmp10
  libgomp1 libisl10 libitm1 libltdl-dev libltdl7 libmagic-dev libmpc3 libmpfr4
  libnet1 libnet1-dev libnspr4 libnspr4-dev libnss3 libnss3-dev libnss3-nssdb
  libpcap-dev libpcap0.8-dev libpcre3-dbg libpcre3-dev libpcrecpp0
  libquadmath0 libstdc++-4.8-dev libtool libtsan0 libyaml-0-2 libyaml-dev
  linux-libc-dev m4 make manpages-dev pkg-config zlib1g-dev
The following packages will be upgraded:
  gcc-4.8-base libc6 libstdc++6
3 upgraded, 62 newly installed, 0 to remove and 125 not upgraded.
Need to get 52.3 MB of archives.
After this operation, 155 MB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu/ trusty-updates/main gcc-4.8-base amd64 4.8.4-2ubuntu1
~14.04.1 [16.0 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu/ trusty-updates/main libstdc++6 amd64 4.8.4-2ubuntu1~1
4.04.1 [259 kB]
0% [2 libstdc++6 0 B/259 kB 0%]
```

Infrastructure

The Classic Model



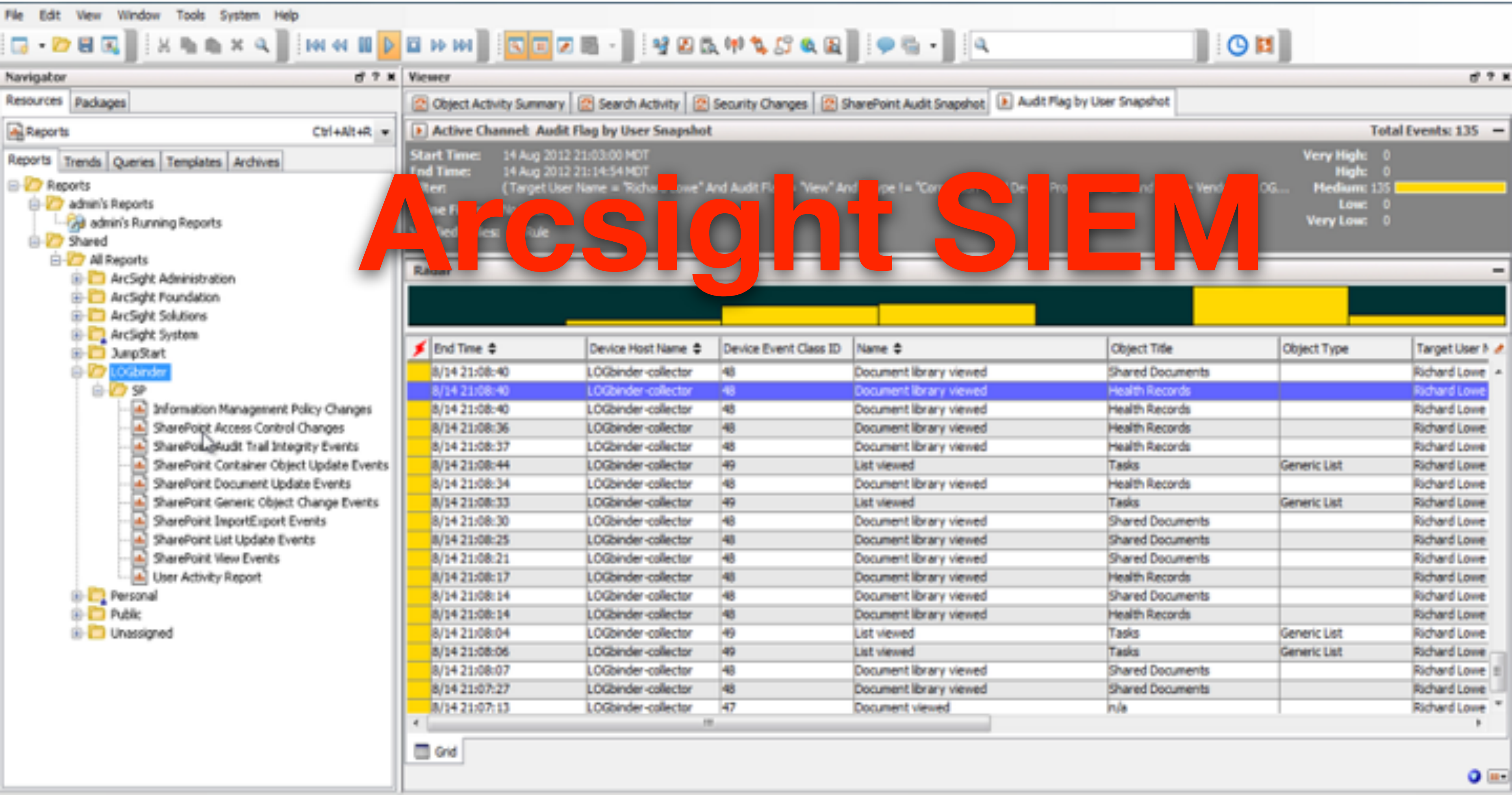
IDS
Snort
TCPDump

Management System

Analyst Systems

Looking at the Management System

Arcsight SIEM



Active Channel: Audit Flag by User Snapshot

Total Events: 135

Start Time: 14 Aug 2012 21:03:00 MDT

End Time: 14 Aug 2012 21:14:54 MDT

Very High: 0

High: 0

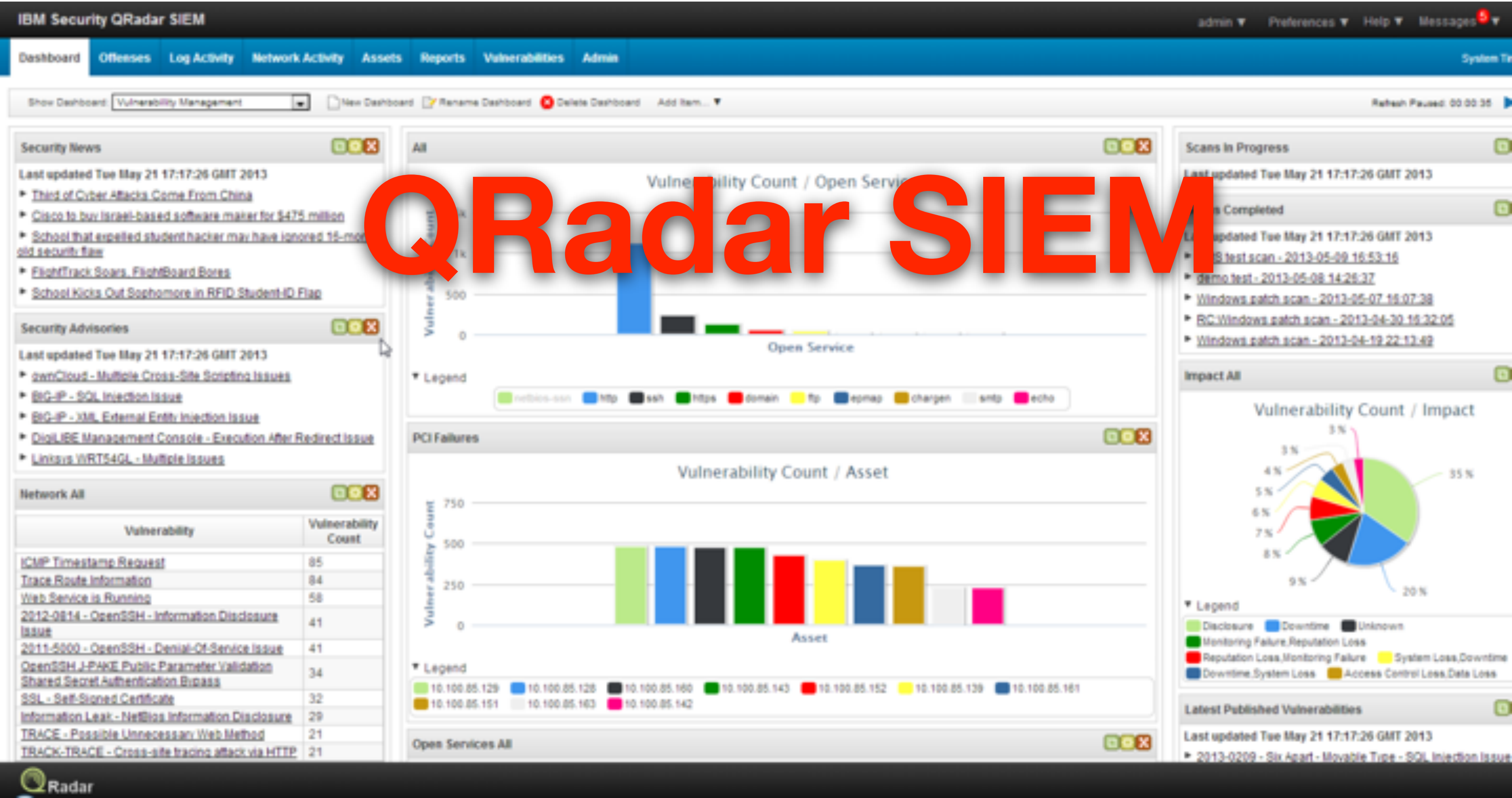
Medium: 135

Low: 0

Very Low: 0

End Time	Device Host Name	Device Event Class ID	Name	Object Title	Object Type	Target User N
8/14 21:08:40	LOGbinder-collector	48	Document library viewed	Shared Documents		Richard Lowe
8/14 21:08:40	LOGbinder-collector	48	Document library viewed	Health Records		Richard Lowe
8/14 21:08:40	LOGbinder-collector	48	Document library viewed	Health Records		Richard Lowe
8/14 21:08:36	LOGbinder-collector	48	Document library viewed	Health Records		Richard Lowe
8/14 21:08:37	LOGbinder-collector	48	Document library viewed	Health Records		Richard Lowe
8/14 21:08:44	LOGbinder-collector	49	List viewed	Tasks	Generic List	Richard Lowe
8/14 21:08:34	LOGbinder-collector	48	Document library viewed	Health Records		Richard Lowe
8/14 21:08:33	LOGbinder-collector	49	List viewed	Tasks	Generic List	Richard Lowe
8/14 21:08:30	LOGbinder-collector	48	Document library viewed	Shared Documents		Richard Lowe
8/14 21:08:25	LOGbinder-collector	48	Document library viewed	Shared Documents		Richard Lowe
8/14 21:08:21	LOGbinder-collector	48	Document library viewed	Shared Documents		Richard Lowe
8/14 21:08:17	LOGbinder-collector	48	Document library viewed	Health Records		Richard Lowe
8/14 21:08:14	LOGbinder-collector	48	Document library viewed	Shared Documents		Richard Lowe
8/14 21:08:14	LOGbinder-collector	48	Document library viewed	Health Records		Richard Lowe
8/14 21:08:04	LOGbinder-collector	49	List viewed	Tasks	Generic List	Richard Lowe
8/14 21:08:06	LOGbinder-collector	49	List viewed	Tasks	Generic List	Richard Lowe
8/14 21:08:07	LOGbinder-collector	48	Document library viewed	Shared Documents		Richard Lowe
8/14 21:07:27	LOGbinder-collector	48	Document library viewed	Shared Documents		Richard Lowe
8/14 21:07:13	LOGbinder-collector	47	Document viewed	n/a		Richard Lowe

QRadar SIEM



Show Dashboard: Vulnerability Management

Refresh Paused: 00:00:35

Security News

Last updated Tue May 21 17:17:26 GMT 2013

- Third of Cyber Attacks Come From China
- Cisco to buy Israel-based software maker for $475 million
- School that expelled student hacker may have ignored 15-mo old security flaw
- FlightTrack Soars, FlightBoard Bores
- School Kicks Out Sophomore in RFID Student-ID Flap

Security Advisories

Last updated Tue May 21 17:17:26 GMT 2013

- ownCloud - Multiple Cross-Site Scripting Issues
- BIG-IP - SQL Injection Issue
- BIG-IP - XML External Entity Injection Issue
- DigiLIBE Management Console - Execution After Redirect Issue
- Linksys WRT54GL - Multiple Issues

Network All

Vulnerability	Vulnerability Count
ICMP Timestamp Request	85
Trace Route Information	84
Web Service is Running	58
2012-0814 - OpenSSH - Information Disclosure Issue	41
2011-5000 - OpenSSH - Denial-Of-Service Issue	41
OpenSSH J-PAKE Public Parameter Validation Shared Secret Authentication Bypass	34
SSL - Self-Signed Certificate	32
Information Leak - NetBios Information Disclosure	29
TRACE - Possible Unnecessary Web Method	21
TRACK-TRACE - Cross-site tracing attack via HTTP	21

All

PCI Failures

Open Services All

Scans In Progress

Last updated Tue May 21 17:17:26 GMT 2013

s Completed

updated Tue May 21 17:17:26 GMT 2013

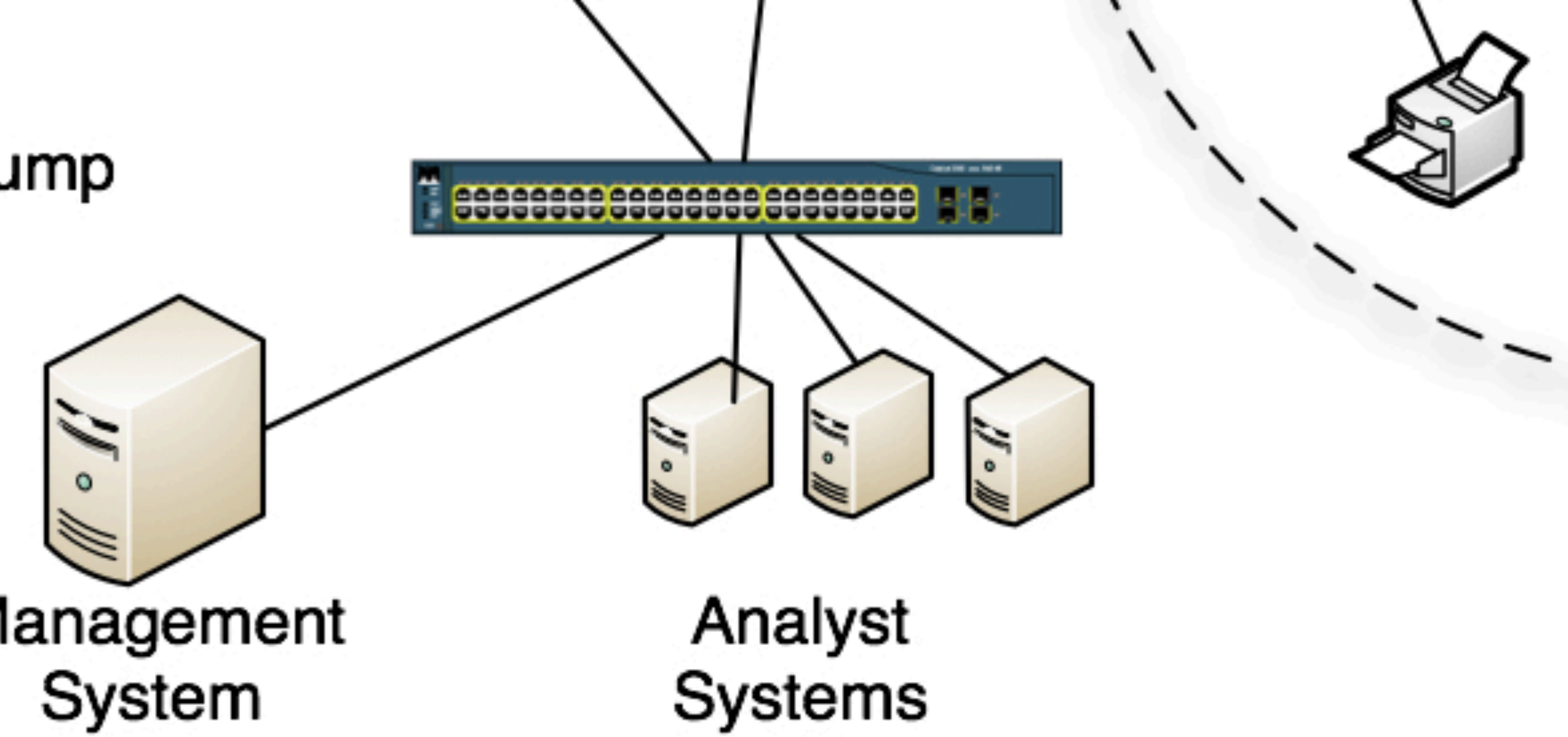
- S test scan - 2013-05-09 16:53:16
- demo test - 2013-05-08 14:26:37
- Windows patch scan - 2013-05-07 16:07:38
- RC:Windows patch scan - 2013-04-30 16:32:05
- Windows patch scan - 2013-04-19 22:13:49

Impact All

Latest Published Vulnerabilities

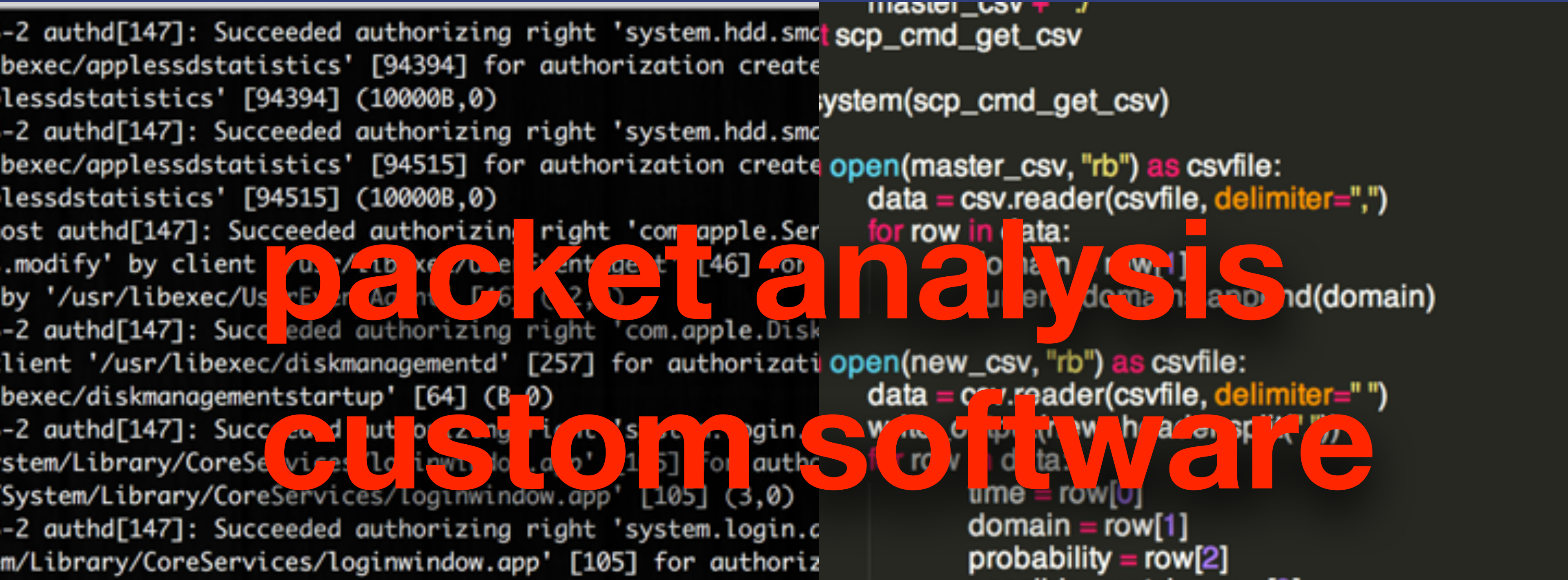
Last updated Tue May 21 17:17:26 GMT 2013

- 2013-0209 - Six Apart - Movable Type - SQL Injection Issue



Looking at the Analysis Systems

Analysis Software



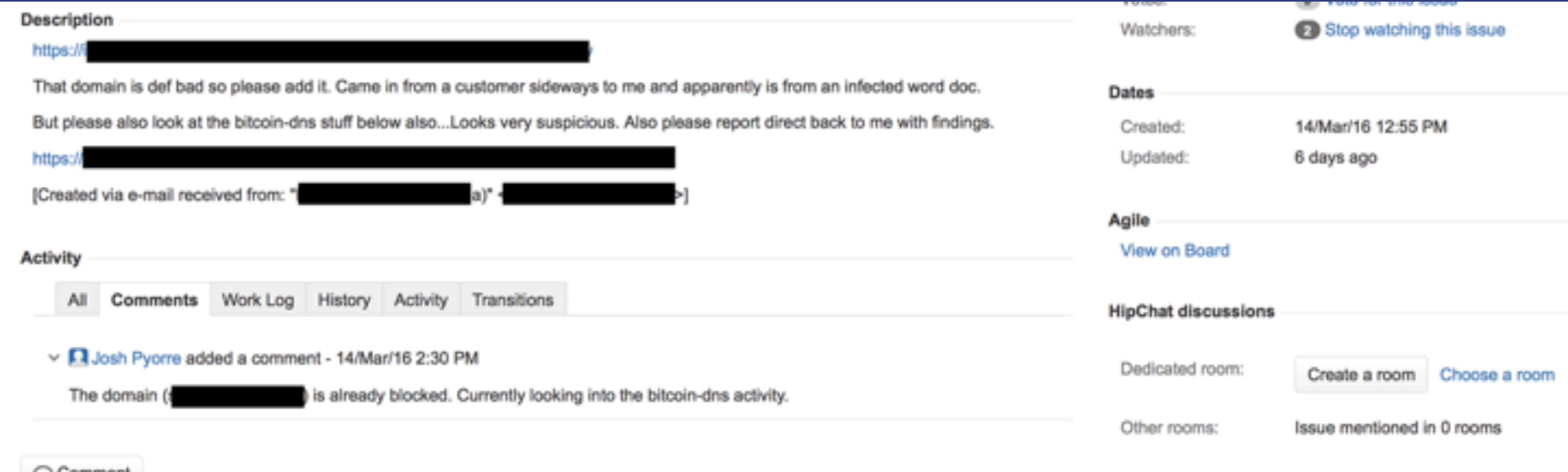
```
-2 authd[147]: Succeeded authorizing right 'system.hdd.smc
bexec/applessdstatistics' [94394] for authorization create
lessdstatistics' [94394] (10000B,0)
-2 authd[147]: Succeeded authorizing right 'system.hdd.smc
bexec/applessdstatistics' [94515] for authorization create
lessdstatistics' [94515] (10000B,0)
ost authd[147]: Succeeded authorizing right 'com.apple.Ser
.modify' by client '/usr/libexec/UserEventAgent' [46] for
by '/usr/libexec/UserEventAgent' [46] (2,0)
-2 authd[147]: Succeeded authorizing right 'com.apple.Disk
lient '/usr/libexec/diskmanagementd' [257] for authorizati
bexec/diskmanagementstartup' [64] (B,0)
-2 authd[147]: Succeeded authorizing right 'system.login.
stem/Library/CoreServices/loginwindow.app' [105] for autho
System/Library/CoreServices/loginwindow.app' [105] (3,0)
-2 authd[147]: Succeeded authorizing right 'system.login.c
m/Library/CoreServices/loginwindow.app' [105] for authoriz
```

```
    master_csv + "./"
t scp_cmd_get_csv

ystem(scp_cmd_get_csv)

open(master_csv, "rb") as csvfile:
    data = csv.reader(csvfile, delimiter=",")
    for row in data:
        domain = row[1]
        current_domains.append(domain)

open(new_csv, "rb") as csvfile:
    data = csv.reader(csvfile, delimiter=" ")
    [illegible](new_header.split(","))
    for row in data:
            time = row[0]
            domain = row[1]
            probability = row[2]
```

packet analysis

custom software

Ticketing



Description

https://[redacted]

That domain is def bad so please add it. Came in from a customer sideways to me and apparently is from an infected word doc.

But please also look at the bitcoin-dns stuff below also...Looks very suspicious. Also please report direct back to me with findings.

https://[redacted]

[Created via e-mail received from: "[redacted]a)" <[redacted]>]

Activity

Josh Pyorre added a comment - 14/Mar/16 2:30 PM

The domain ([redacted]) is already blocked. Currently looking into the bitcoin-dns activity.

Watchers: 2

Dates

Created: 14/Mar/16 12:55 PM

Updated: 6 days ago

Agile

HipChat discussions

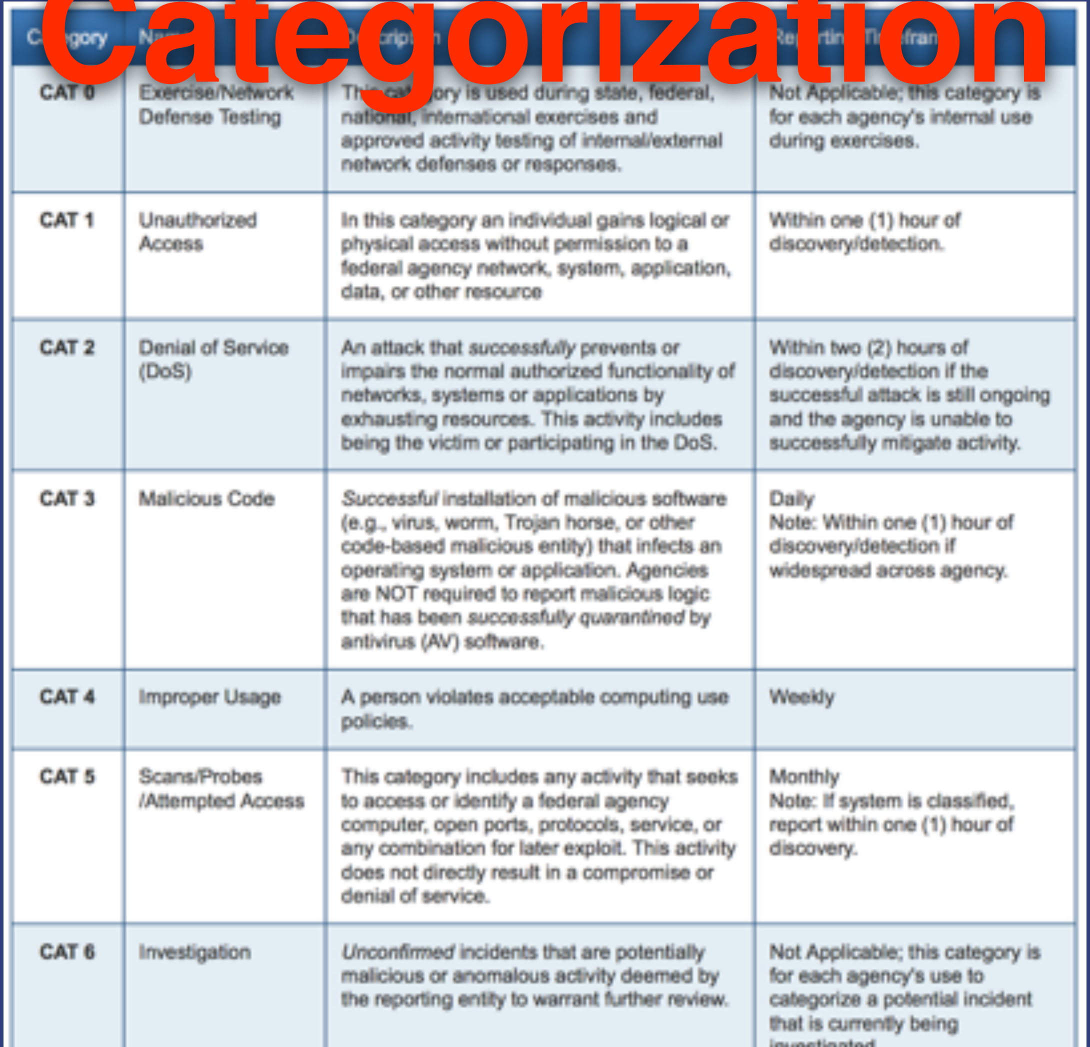
Dedicated room:

Other rooms: Issue mentioned in 0 rooms

The Classic Model

Operations

Categorization



Category	Name	Description	Reporting Timeframe
CAT 0	Exercise/Network Defense Testing	This category is used during state, federal, national, international exercises and approved activity testing of internal/external network defenses or responses.	Not Applicable; this category is for each agency's internal use during exercises.
CAT 1	Unauthorized Access	In this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource	Within one (1) hour of discovery/detection.
CAT 2	Denial of Service (DoS)	An attack that *successfully* prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.	Within two (2) hours of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate activity.
CAT 3	Malicious Code	*Successful* installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are NOT required to report malicious logic that has been *successfully quarantined* by antivirus (AV) software.	Daily Note: Within one (1) hour of discovery/detection if widespread across agency.
CAT 4	Improper Usage	A person violates acceptable computing use policies.	Weekly
CAT 5	Scans/Probes /Attempted Access	This category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.	Monthly Note: If system is classified, report within one (1) hour of discovery.
CAT 6	Investigation	*Unconfirmed* incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.	Not Applicable; this category is for each agency's use to categorize a potential incident that is currently being investigated

The Classic Model

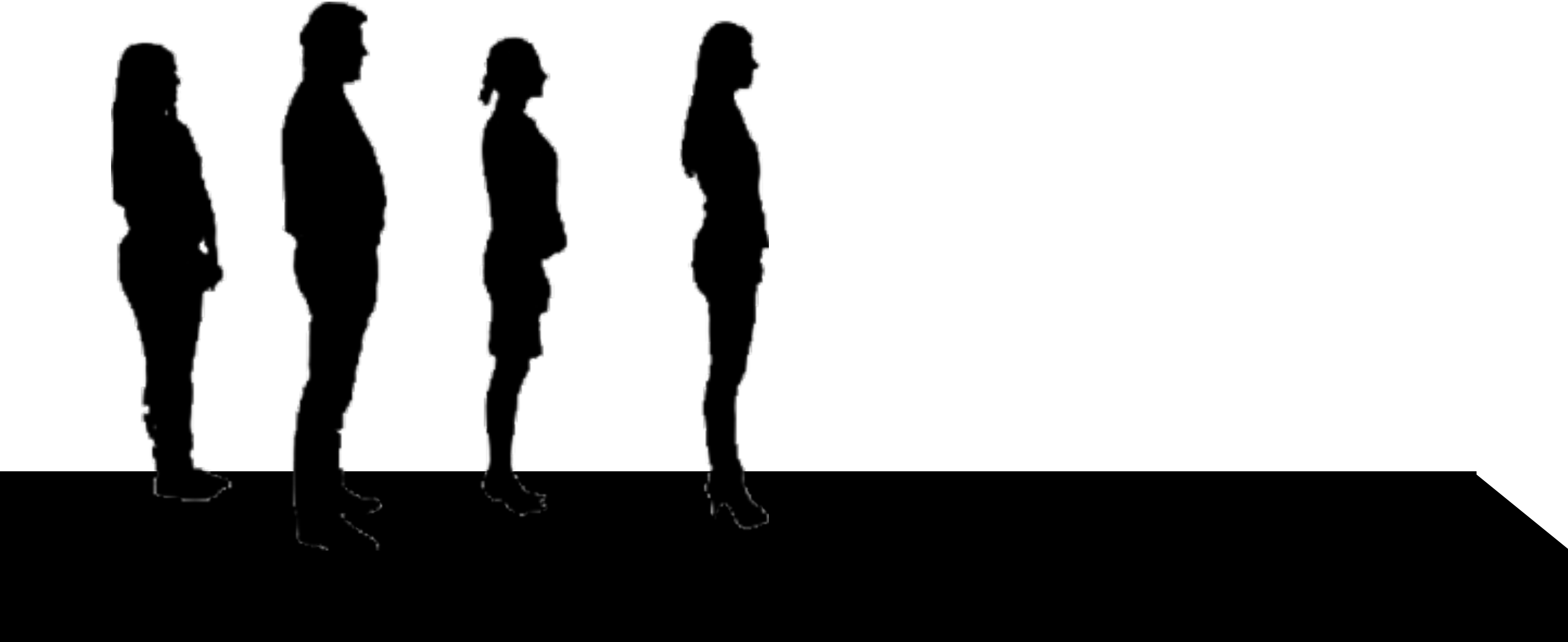
People

The People

SYSTEM ADMINISTRATORS!

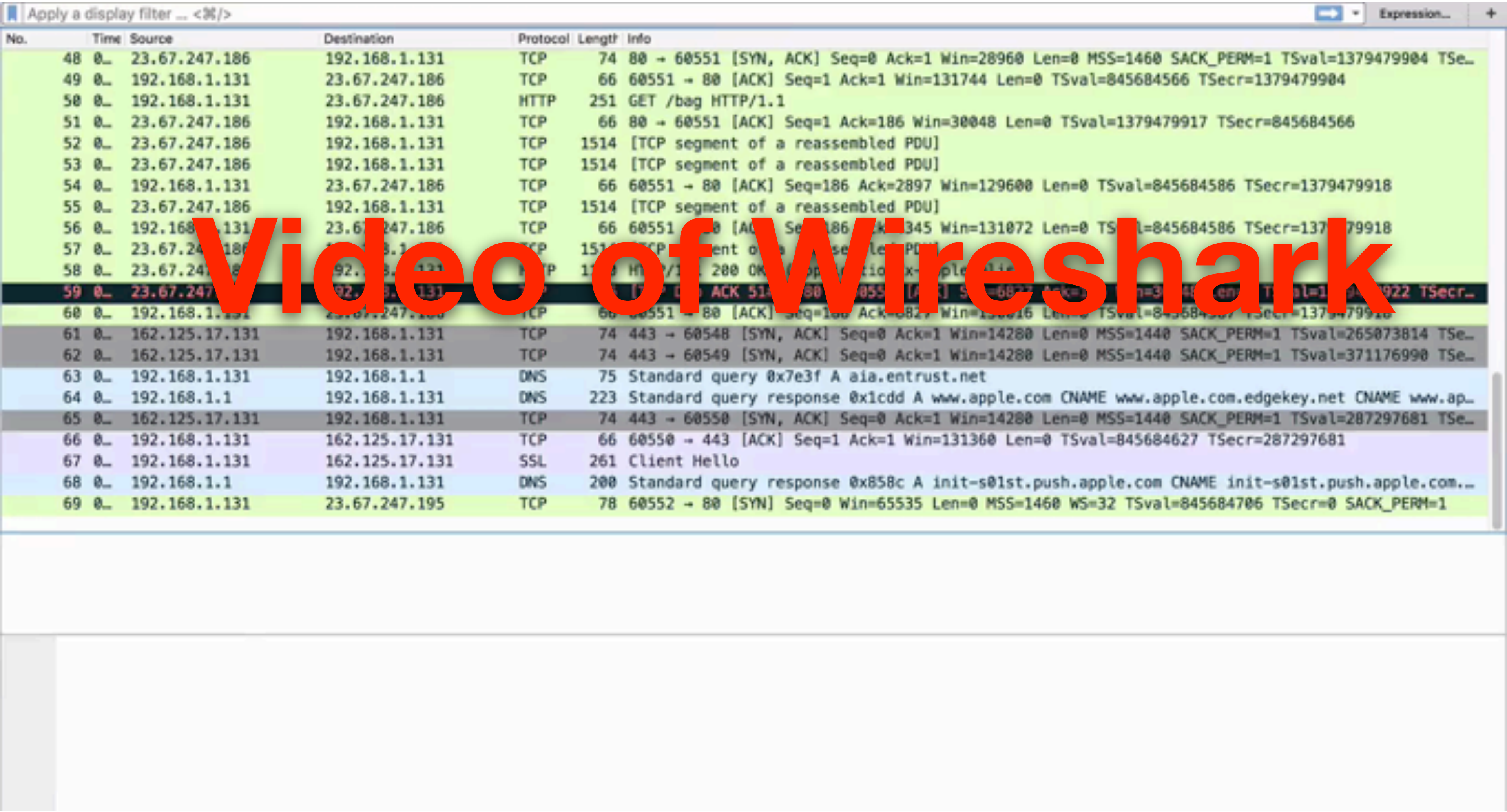
The People

ANALYSTS!



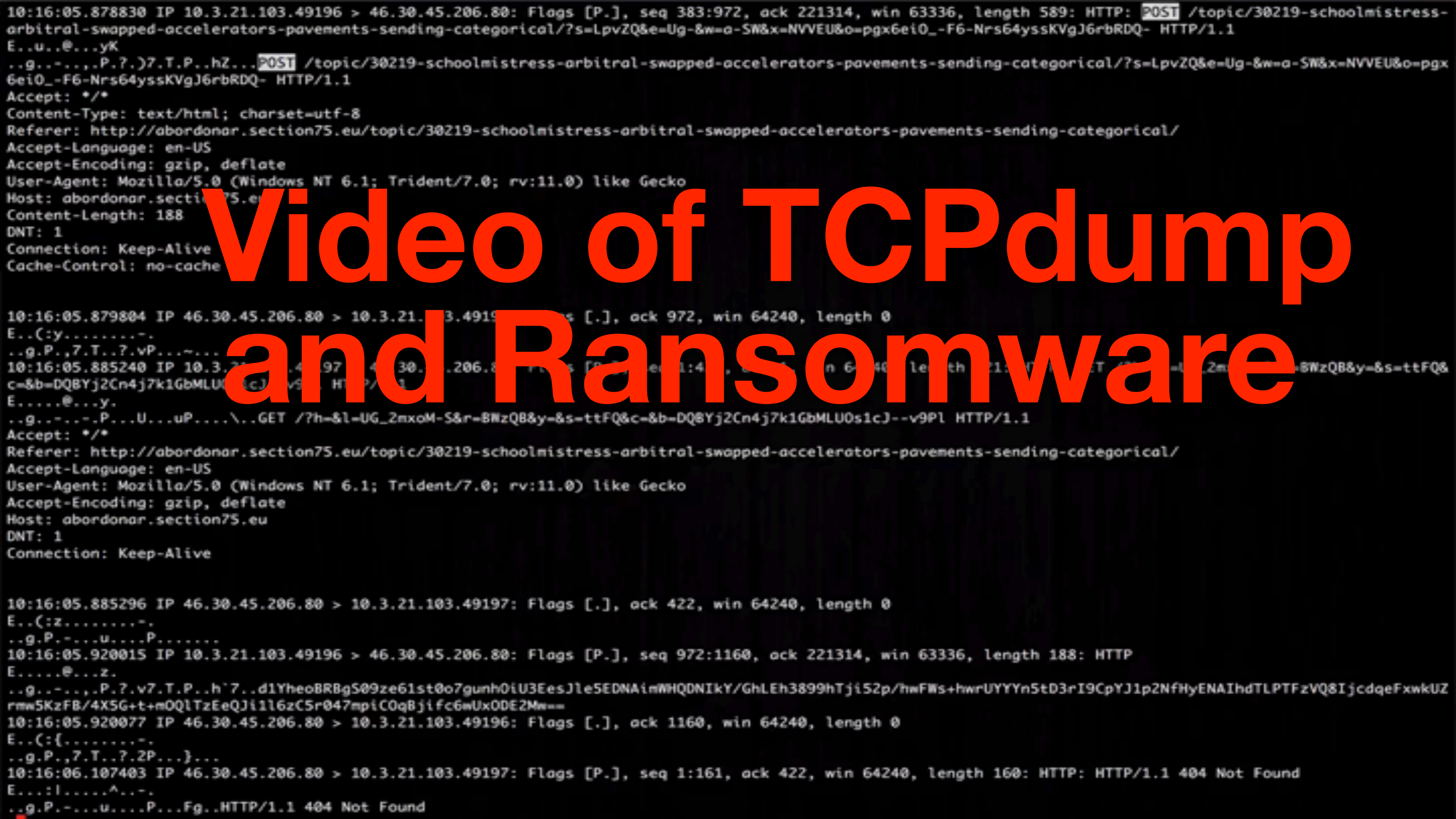
The People

Video of Wireshark



```
No.      Time Source           Destination       Protocol Length Info
    48 0…  23.67.247.186    192.168.1.131     TCP        74 80 → 60551 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=1379479904 TSe…
    49 0…  192.168.1.131    23.67.247.186     TCP        66 60551 → 80 [ACK] Seq=1 Ack=1 Win=131744 Len=0 TSval=845684566 TSecr=1379479904
    50 0…  192.168.1.131    23.67.247.186     HTTP      251 GET /bag HTTP/1.1
    51 0…  23.67.247.186    192.168.1.131     TCP        66 80 → 60551 [ACK] Seq=1 Ack=186 Win=30048 Len=0 TSval=1379479917 TSecr=845684566
    52 0…  23.67.247.186    192.168.1.131     TCP      1514 [TCP segment of a reassembled PDU]
    53 0…  23.67.247.186    192.168.1.131     TCP      1514 [TCP segment of a reassembled PDU]
    54 0…  192.168.1.131    23.67.247.186     TCP        66 60551 → 80 [ACK] Seq=186 Ack=2897 Win=129600 Len=0 TSval=845684586 TSecr=1379479918
    55 0…  23.67.247.186    192.168.1.131     TCP      1514 [TCP segment of a reassembled PDU]
    56 0…  192.168[illegible].131    23.6[illegible]47.186     TCP        66 60551 [illegible] [AC[illegible] Se[illegible]186 [illegible]345 Win=131072 Len=0 TS[illegible]l=845684586 TSecr=137[illegible]79918
    57 0…  23.67.24[illegible]18[illegible]    [illegible]     [illegible]CP      151[illegible] [illegible]CP [illegible]ent o[illegible] [illegible]se[illegible]le[illegible] PDU[illegible]
    58 0…  23.67.24[illegible]    [illegible]92.[illegible].131     [illegible]TP      1[illegible] H[illegible]P/1[illegible] 200 OK [illegible]p[illegible]tio[illegible] x-[illegible]ple[illegible]li[illegible]
    59 0…  23.67.247[illegible]    [illegible]92.[illegible]131     T[illegible]      [illegible] [T[illegible] D[illegible] ACK 51[illegible] 80 [illegible]055[illegible] [A[illegible]] S[illegible]=682[illegible] [illegible]922 TSecr…
    60 0…  192.168.1.[illegible]    [illegible]247.[illegible]     [illegible]CP        6[illegible] [illegible]551 → 80 [ACK] [illegible]eq=1[illegible] Ack=682[illegible] Win=1[illegible]16 [illegible] TSval=84[illegible] [illegible]=137[illegible]79918
    61 0…  162.125.17.131   192.168.1.131     TCP        74 443 → 60548 [SYN, ACK] Seq=0 Ack=1 Win=14280 Len=0 MSS=1440 SACK_PERM=1 TSval=265073814 TSe…
    62 0…  162.125.17.131   192.168.1.131     TCP        74 443 → 60549 [SYN, ACK] Seq=0 Ack=1 Win=14280 Len=0 MSS=1440 SACK_PERM=1 TSval=371176990 TSe…
    63 0…  192.168.1.131    192.168.1.1       DNS        75 Standard query 0x7e3f A aia.entrust.net
    64 0…  192.168.1.1      192.168.1.131     DNS       223 Standard query response 0x1cdd A www.apple.com CNAME www.apple.com.edgekey.net CNAME www.ap…
    65 0…  162.125.17.131   192.168.1.131     TCP        74 443 → 60550 [SYN, ACK] Seq=0 Ack=1 Win=14280 Len=0 MSS=1440 SACK_PERM=1 TSval=287297681 TSe…
    66 0…  192.168.1.131    162.125.17.131    TCP        66 60550 → 443 [ACK] Seq=1 Ack=1 Win=131360 Len=0 TSval=845684627 TSecr=287297681
    67 0…  192.168.1.131    162.125.17.131    SSL       261 Client Hello
    68 0…  192.168.1.1      192.168.1.131     DNS       200 Standard query response 0x858c A init-s01st.push.apple.com CNAME init-s01st.push.apple.com…
    69 0…  192.168.1.131    23.67.247.195     TCP        78 60552 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=845684706 TSecr=0 SACK_PERM=1
```

Video of TCPdump and Ransomware



```
10:16:05.878830 IP 10.3.21.103.49196 > 46.30.45.206.80: Flags [P.], seq 383:972, ack 221314, win 63336, length 589: HTTP: POST /topic/30219-schoolmistress-
arbitral-swapped-accelerators-pavements-sending-categorical/?s=LpvZQ&e=Ug-&w=a-SW&x=NVVEU&o=pgx6eiO_-F6-Nrs64yssKVgJ6rbRDQ- HTTP/1.1
E..u..@...yK
..g..-..,.P.?.)7.T.P..hZ...POST /topic/30219-schoolmistress-arbitral-swapped-accelerators-pavements-sending-categorical/?s=LpvZQ&e=Ug-&w=a-SW&x=NVVEU&o=pgx
6eiO_-F6-Nrs64yssKVgJ6rbRDQ- HTTP/1.1
Accept: */*
Content-Type: text/html; charset=utf-8
Referer: http://abordonar.section75.eu/topic/30219-schoolmistress-arbitral-swapped-accelerators-pavements-sending-categorical/
Accept-Language: en-US
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
Host: abordonar.secti 75.e
Content-Length: 188
DNT: 1
Connection: Keep-Alive
Cache-Control: no-cache


10:16:05.879804 IP 46.30.45.206.80 > 10.3.21. 3.4919  s [.], ack 972, win 64240, length 0
E..(:y........-.
..g.P.,7.T..?.vP...~...
10:16:05.885240 IP 10.3.  .4 97  4 30.  .206.   s [P   e  1:4 ,    n 6  40  le  th  21:     ET /    =U  2m    BWzQB&y=&s=ttFQ&
c=&b=DQBYj2Cn4j7k1GbMLU  cJ  v9  HT P/  1
E.....@...y.
..g..-..-.P...U...uP....\..GET /?h=&l=UG_2mxoM-S&r=BWzQB&y=&s=ttFQ&c=&b=DQBYj2Cn4j7k1GbMLUOs1cJ--v9Pl HTTP/1.1
Accept: */*
Referer: http://abordonar.section75.eu/topic/30219-schoolmistress-arbitral-swapped-accelerators-pavements-sending-categorical/
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: abordonar.section75.eu
DNT: 1
Connection: Keep-Alive


10:16:05.885296 IP 46.30.45.206.80 > 10.3.21.103.49197: Flags [.], ack 422, win 64240, length 0
E..(:z........-.
..g.P.-...u....P.......
10:16:05.920015 IP 10.3.21.103.49196 > 46.30.45.206.80: Flags [P.], seq 972:1160, ack 221314, win 63336, length 188: HTTP
E.....@...z.
..g..-..,.P.?.v7.T.P..h`7..d1YheoBRBgS09ze61st0o7gunhOiU3EesJle5EDNAimWHQDNIkY/GhLEh3899hTji52p/hwFWs+hwrUYYYn5tD3rI9CpYJ1p2NfHyENAIhdTLPTFzVQ8IjcdqeFxwkUZ
rmw5KzFB/4X5G+t+mOQlTzEeQJi1l6zC5r047mpiCOqBjifc6wUxODEZMw==
10:16:05.920077 IP 46.30.45.206.80 > 10.3.21.103.49196: Flags [.], ack 1160, win 64240, length 0
E..(:{........-.
..g.P.,7.T..?.2P...}...
10:16:06.107403 IP 46.30.45.206.80 > 10.3.21.103.49197: Flags [P.], seq 1:161, ack 422, win 64240, length 160: HTTP: HTTP/1.1 404 Not Found
E...:|.....^..-.
..g.P.-...u....P...Fg..HTTP/1.1 404 Not Found
```

Analyst Workflow

- Analyze
- Categorize
- Malware on System
- Alert the IR team
- Move on

Threat Analysts

- Investigate phishing
- Analyze Malware
  - Writing new rules/updating existing rules
- Read a lot
- Programmers
- Thought leaders
  - Speak at conferences
  - Write blog posts

Threat Intel Sources

- Passive DNS
- Honeypots
- Hunting
- Third parties

Video of useless Threat Map often seen in SOCs

ATTACK ORIGINS

#		COUNTRY
[illegible]		China
[illegible]		United States
[illegible]		Mil/Gov
[illegible]		Germany
[illegible]		Russia
[illegible]		Taiwan
[illegible]		Netherlands
[illegible]		Turkey
[illegible]		Japan
[illegible]		France

ATTACK TARGETS

#		COUNTRY
[illegible]		United States
[illegible]		Philippines
[illegible]		Russia
[illegible]		Taiwan
[illegible]		France
[illegible]		Netherlands
[illegible]		Mil/Gov
[illegible]		Poland
[illegible]		South Korea
6		Germany

ATTACK TYPES

#		SERVICE	PORT
[illegible]	●	telnet	23
[illegible]	●	http-alt	8080
[illegible]	●	domain	53
[illegible]	●	ms-wbt-server	3389
[illegible]	●	unknown	[illegible]
[illegible]	●	ssh	22
[illegible]	●	http	80
[illegible]	●	ms-sql-s	1433

LIVE ATTACKS

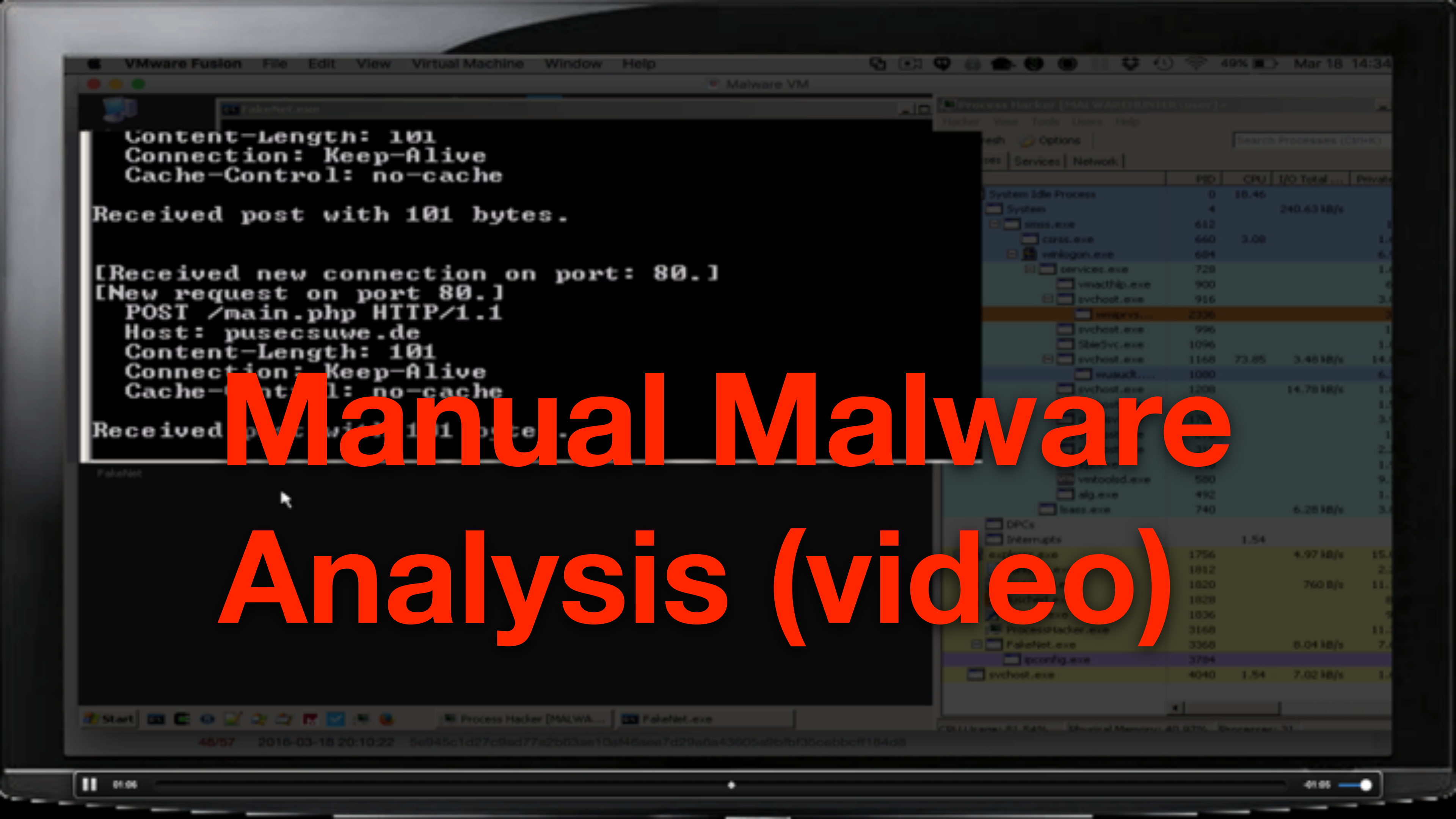
	ATTACKER			TARGET	TYPE	
TIMESTAMP	ORGANIZATION	LOCATION	IP	LOCATION	SERVICE	PORT
2015-02-19 00:00:00.25	H1 DC Infrastructure	unknown, Russia	[illegible]	unknown, Russia	[illegible]	[illegible]
2015-02-19 00:00:00.25	H1 DC Infrastructure	unknown, Russia	[illegible]	unknown, Russia	[illegible]	1
2015-02-19 00:00:00.26	H1 DC Infrastructure	unknown, Russia	[illegible]	unknown, Russia	[illegible]	1
2015-02-19 00:00:00.26	H1 DC Infrastructure	unknown, Russia	[illegible]	unknown, Russia	[illegible]	1
2015-02-19 00:00:00.26	H1 DC Infrastructure	unknown, Russia	[illegible]	unknown, Russia	[illegible]	1
2015-02-19 00:00:00.34	N/A	unknown, Japan	203.83.240.112	Saint Louis, United	unknown	52508
2015-02-19 00:00:00.49	Chinanet Jiangsu Province	Changzhou, China	61.160.224.129	Medina, United States	[illegible]	873
2015-02-19 00:00:00.80	[illegible]	Tønsberg, Norway	[illegible]	Englewood, United	unknown	[illegible]

threat map

analysis tools

threat platforms

terminal



```
  Content-Length: 101
  Connection: Keep-Alive
  Cache-Control: no-cache

Received post with 101 bytes.


[Received new connection on port: 80.]
[New request on port 80.]
  POST /main.php HTTP/1.1
  Host: pusecsuwe.de
  Content-Length: 101
  Connection: Keep-Alive
  Cache-Control: no-cache

Received post with 101 bytes.
```

Manual Malware Analysis (video)

SOC as a Service

SOC as a Service

Install their boxes

They watch your network

They alert you when there’s a problem

They manage all that SOC stuff

SOC as a Service?

What’s their response time?

How do they innovate?

You aren’t their only customer

The Security Landscape

The Security Landscape

We are working everywhere

Everyone brings their own devices

It can never happen to us

Malware is the best way into a network.

APT is over-hyped - just stop the big thing

The Modern SOC

Some of the gaps

- Cloud Services
- Behavioral Analysis
- BYOD
- **Too much manual stuff**

Risk Assessment

What are you protecting?

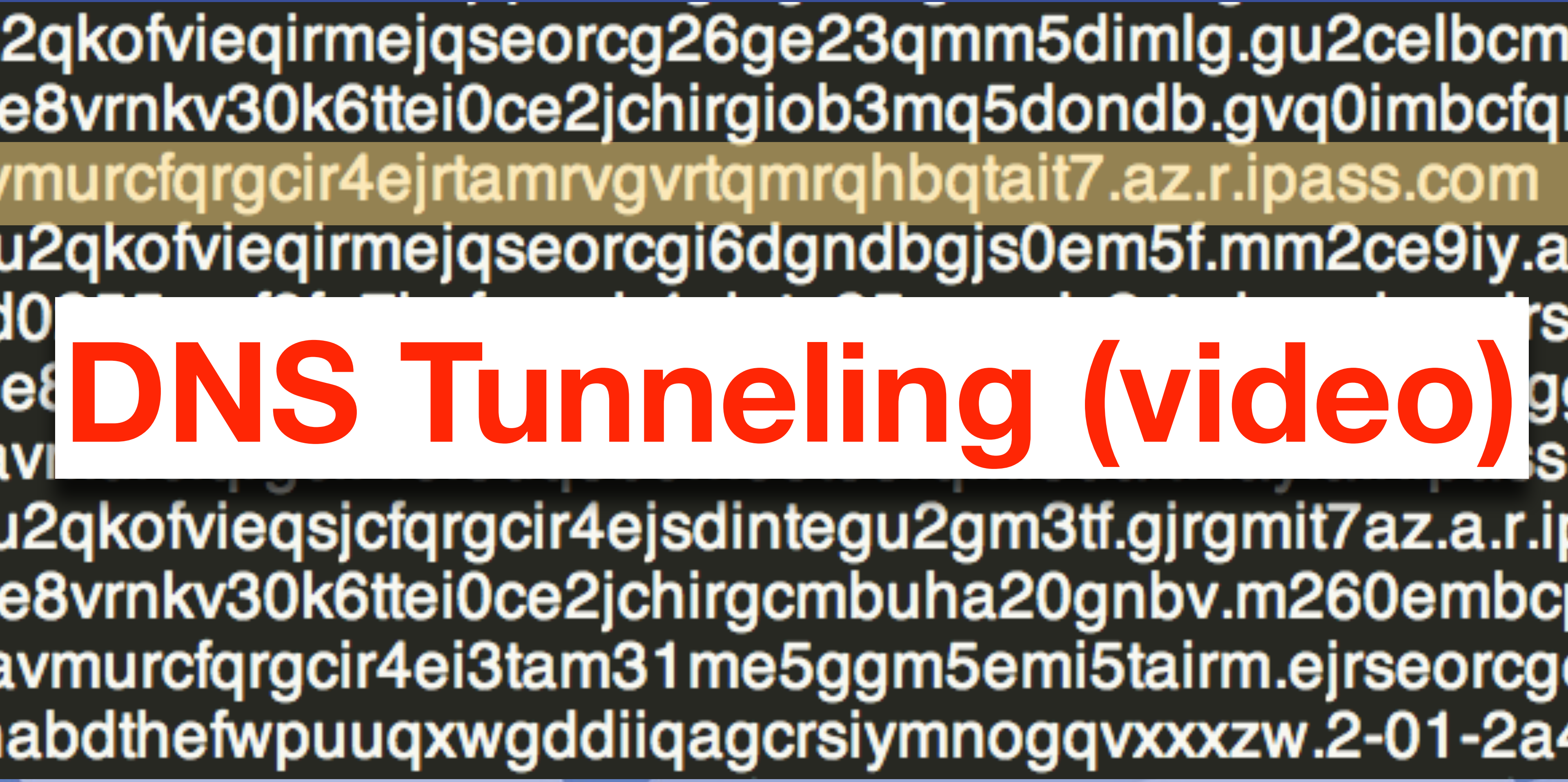
- Depends on industry
- Depends on what you’re running
    - Inventory lists
- Are networks segregated?
    - guest, VPN, Internal

Adapting to Now

DNS

- DGA's
  - Complex domains, generated by malware
- Typosquatting
  - wellsfarg0[.]com, Vistaprint
- **Known Bad**
  - Third party, Hunting
- **Covert Tunneling**
  - Next slide…

DNS Tunneling (video)



```
2qkofvieqirmejqseorcg26ge23qmm5dimlg.gu2celbcm
e8vrnkv30k6ttei0ce2jchirgiob3mq5dondb.gvq0imbcfq
vmurcfqrgcir4ejrtamrvgvrtqmrqhbqtait7.az.r.ipass.com
u2qkofvieqirmejqseorcgi6dgndbgjs0em5f.mm2ce9iy.a
u2qkofvieqsjcfqrgcir4ejsdintegu2gm3tf.gjrgmit7az.a.r.ip
e8vrnkv30k6ttei0ce2jchirgcmbuha20gnbv.m260embcp
avmurcfqrgcir4ei3tam31me5ggm5emi5tairm.ejrseorcg
abdthefwpuuqxwgddiiqagcrsiymnogqvxxxzw.2-01-2a
```

EMAIL

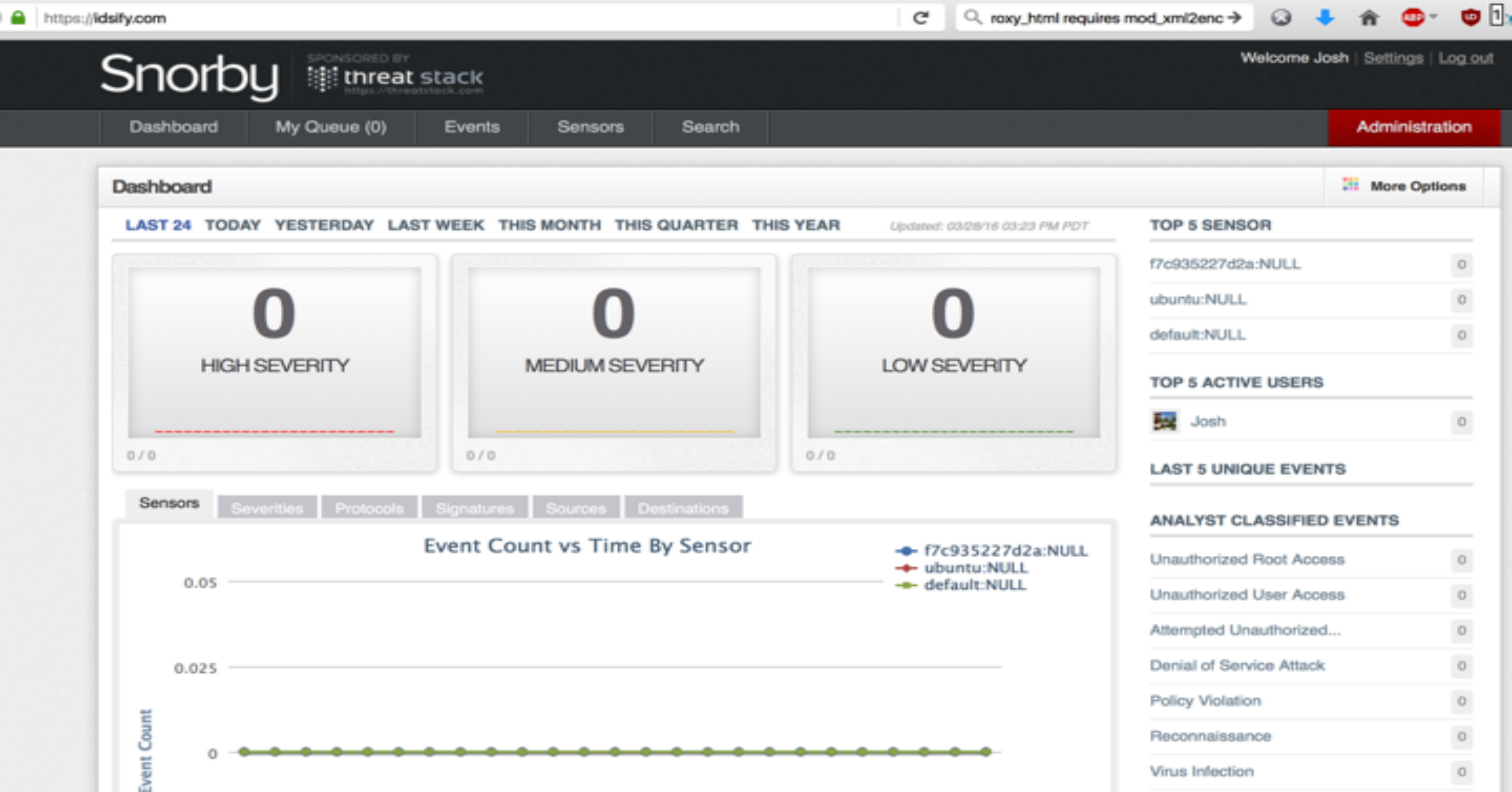
- Attachments
  exe's or other unusual items
- **Headers**
  Analyze from vs first 'received by'

BEHAVIOR

- Training
  - TRAINING!!!!!
- **Anomalies**
  - Visits to somewhere different

Management System

Snorby (web based)



TOP 5 SENSOR	
f7c935227d2a:NULL	0
ubuntu:NULL	0
default:NULL	0

TOP 5 ACTIVE USERS	
Josh	0

LAST 5 UNIQUE EVENTS

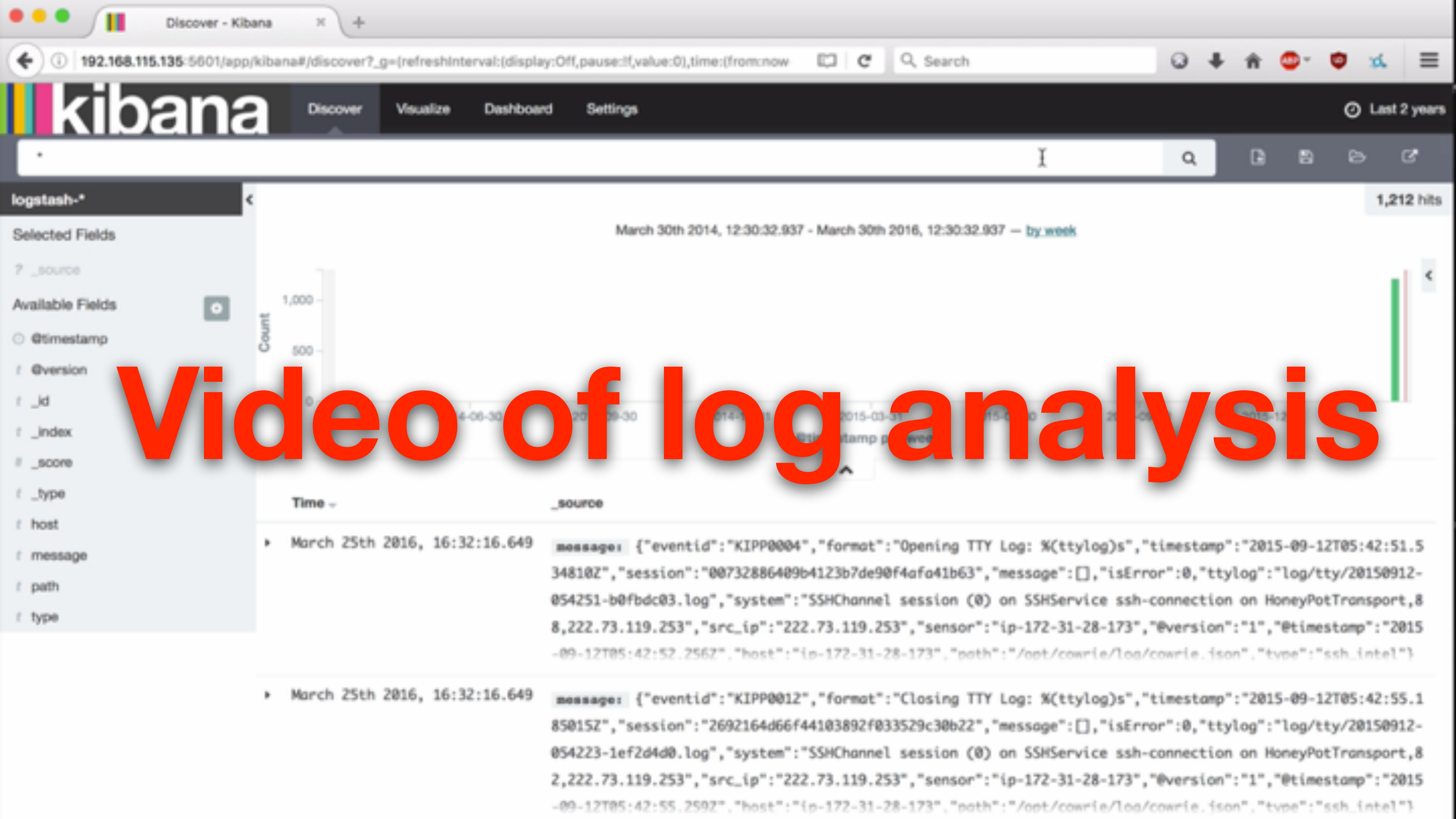
ANALYST CLASSIFIED EVENTS	
Unauthorized Root Access	0
Unauthorized User Access	0
Attempted Unauthorized...	0
Denial of Service Attack	0
Policy Violation	0
Reconnaissance	0
Virus Infection	0

Management System

Snorby (web based)

ELK (Log Aggregation)

Video of log analysis



```
March 25th 2016, 16:32:16.649  message: {"eventid":"KIPP0004","format":"Opening TTY Log: %(ttylog)s","timestamp":"2015-09-12T05:42:51.5
                               34810Z","session":"00732886409b4123b7de90f4afa41b63","message":[],"isError":0,"ttylog":"log/tty/20150912-
                               054251-b0fbdc03.log","system":"SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,8
                               8,222.73.119.253","src_ip":"222.73.119.253","sensor":"ip-172-31-28-173","@version":"1","@timestamp":"2015
                               -09-12T05:42:52.256Z","host":"ip-172-31-28-173","path":"/opt/cowrie/log/cowrie.json","type":"ssh_intel"}

March 25th 2016, 16:32:16.649  message: {"eventid":"KIPP0012","format":"Closing TTY Log: %(ttylog)s","timestamp":"2015-09-12T05:42:55.1
                               85015Z","session":"2692164d66f44103892f033529c30b22","message":[],"isError":0,"ttylog":"log/tty/20150912-
                               054223-1ef2d4d0.log","system":"SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,8
                               2,222.73.119.253","src_ip":"222.73.119.253","sensor":"ip-172-31-28-173","@version":"1","@timestamp":"2015
                               -09-12T05:42:55.259Z","host":"ip-172-31-28-173","path":"/opt/cowrie/log/cowrie.json","type":"ssh_intel"}
```

Building Systems for Adaptability

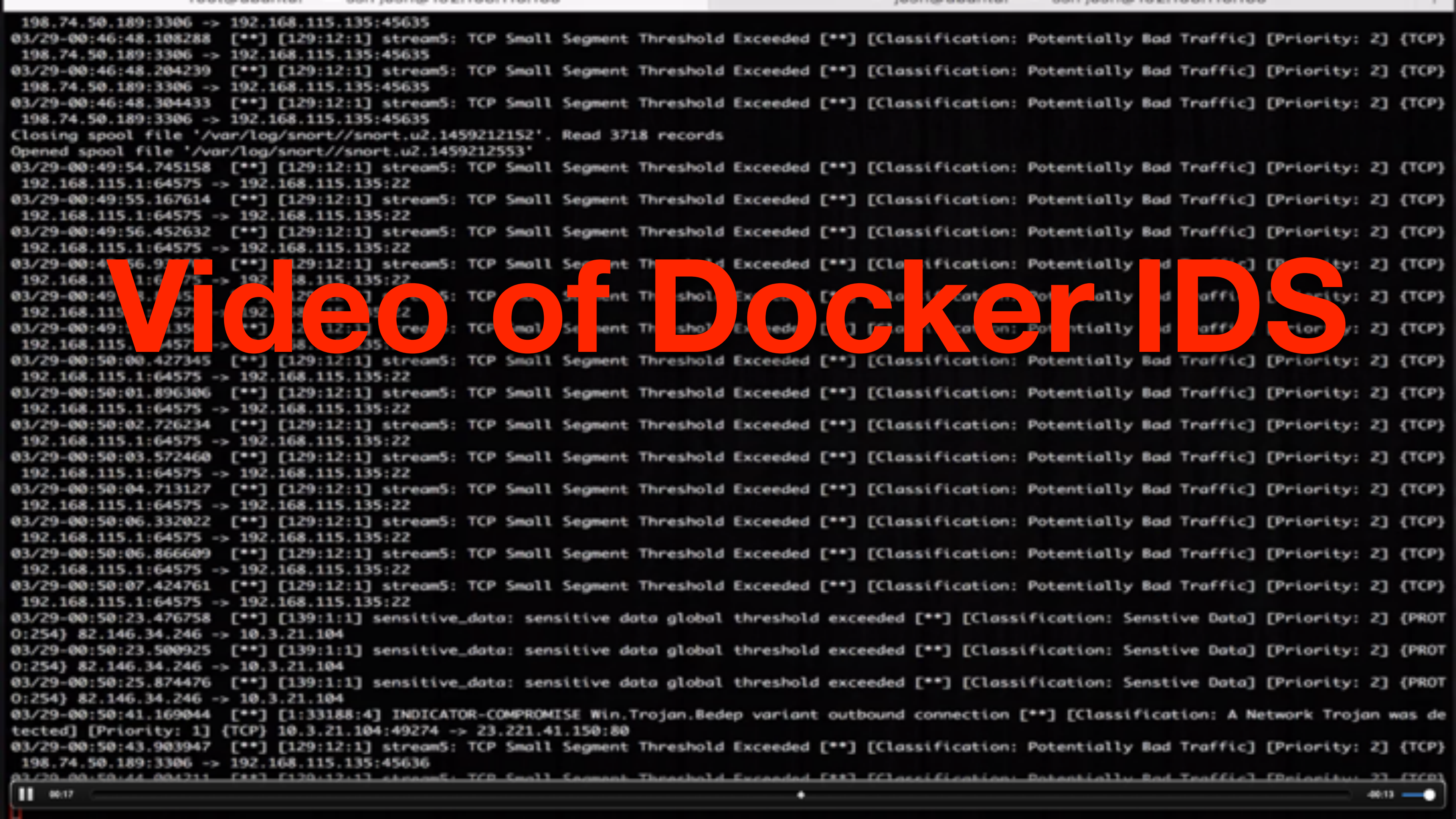
- Compartmentalized systems for quick deployment
  - One configuration file
  - Central ruleset
  - Purpose driven, one use

- IDS on every device
- Deploy as many as needed, really fast

```
josh@ubuntu:~$ docker run -it -p 80:80 --net=host jpyorre/snortbase
```

Video of Docker IDS

Video of Docker IDS



```
 198.74.50.189:3306 -> 192.168.115.135:45635
03/29-00:46:48.108288  [**] [129:12:1] stream5: TCP Small Segment Threshold Exceeded [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP}
 198.74.50.189:3306 -> 192.168.115.135:45635
03/29-00:46:48.204239  [**] [129:12:1] stream5: TCP Small Segment Threshold Exceeded [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP}
 198.74.50.189:3306 -> 192.168.115.135:45635
03/29-00:46:48.304433  [**] [129:12:1] stream5: TCP Small Segment Threshold Exceeded [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP}
 198.74.50.189:3306 -> 192.168.115.135:45635
Closing spool file '/var/log/snort//snort.u2.1459212152'. Read 3718 records
Opened spool file '/var/log/snort//snort.u2.1459212553'
03/29-00:49:54.745158  [**] [129:12:1] stream5: TCP Small Segment Threshold Exceeded [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP}
 192.168.115.1:64575 -> 192.168.115.135:22
03/29-00:49:55.167614  [**] [129:12:1] stream5: TCP Small Segment Threshold Exceeded [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP}
 192.168.115.1:64575 -> 192.168.115.135:22
03/29-00:49:56.452632  [**] [129:12:1] stream5: TCP Small Segment Threshold Exceeded [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP}
 192.168.115.1:64575 -> 192.168.115.135:22
03/29-00:4[illegible]56.9[illegible]  [**] [illegible]29:12:1] stream5: TCP Small Se[illegible]nt Th[illegible] Exceeded [**] [Cla[illegible]ification: Potentially [illegible] [illegible]ty: 2] {TCP}
 192.168.1[illegible]1:6[illegible]75 -> 192.[illegible]8.115.135:22
03/29-00:49[illegible] [illegible]: TCP [illegible] S[illegible]nt Th[illegible]shol[illegible] Ex[illegible] [illegible] [illegible]ally [illegible]d [illegible]affi[illegible] [illegible]ity: 2] {TCP}
 192.168.115[illegible]57[illegible] [illegible]22
03/29-00:49:[illegible]135[illegible]*] [illegible]12:1] [illegible]re[illegible]: TCP [illegible]mal[illegible] Se[illegible]ment Th[illegible]shol[illegible] [illegible]ede[illegible] [illegible]] [Cla[illegible]ca[illegible]on: Pot[illegible]ntially [illegible]d [illegible]affi[illegible] [illegible]rior[illegible]: 2] {TCP}
 192.168.115.[illegible]457[illegible] -> [illegible]8.[illegible]135:[illegible]
03/29-00:50:00.427345  [**] [129:12:1] stream5: TCP Small Segment Threshold Exceeded [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP}
 192.168.115.1:64575 -> 192.168.115.135:22
03/29-00:50:01.896306  [**] [129:12:1] stream5: TCP Small Segment Threshold Exceeded [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP}
 192.168.115.1:64575 -> 192.168.115.135:22
03/29-00:50:02.726234  [**] [129:12:1] stream5: TCP Small Segment Threshold Exceeded [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP}
 192.168.115.1:64575 -> 192.168.115.135:22
03/29-00:50:03.572460  [**] [129:12:1] stream5: TCP Small Segment Threshold Exceeded [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP}
 192.168.115.1:64575 -> 192.168.115.135:22
03/29-00:50:04.713127  [**] [129:12:1] stream5: TCP Small Segment Threshold Exceeded [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP}
 192.168.115.1:64575 -> 192.168.115.135:22
03/29-00:50:06.332022  [**] [129:12:1] stream5: TCP Small Segment Threshold Exceeded [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP}
 192.168.115.1:64575 -> 192.168.115.135:22
03/29-00:50:06.866609  [**] [129:12:1] stream5: TCP Small Segment Threshold Exceeded [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP}
 192.168.115.1:64575 -> 192.168.115.135:22
03/29-00:50:07.424761  [**] [129:12:1] stream5: TCP Small Segment Threshold Exceeded [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP}
 192.168.115.1:64575 -> 192.168.115.135:22
03/29-00:50:23.476758  [**] [139:1:1] sensitive_data: sensitive data global threshold exceeded [**] [Classification: Senstive Data] [Priority: 2] {PROT
O:254} 82.146.34.246 -> 10.3.21.104
03/29-00:50:23.500925  [**] [139:1:1] sensitive_data: sensitive data global threshold exceeded [**] [Classification: Senstive Data] [Priority: 2] {PROT
O:254} 82.146.34.246 -> 10.3.21.104
03/29-00:50:25.874476  [**] [139:1:1] sensitive_data: sensitive data global threshold exceeded [**] [Classification: Senstive Data] [Priority: 2] {PROT
O:254} 82.146.34.246 -> 10.3.21.104
03/29-00:50:41.169044  [**] [1:33188:4] INDICATOR-COMPROMISE Win.Trojan.Bedep variant outbound connection [**] [Classification: A Network Trojan was de
tected] [Priority: 1] {TCP} 10.3.21.104:49274 -> 23.221.41.150:80
03/29-00:50:43.903947  [**] [129:12:1] stream5: TCP Small Segment Threshold Exceeded [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP}
 198.74.50.189:3306 -> 192.168.115.135:45636
```

Cloud Services

We work fast, setting up devices and services quickly.

Cloud IDS

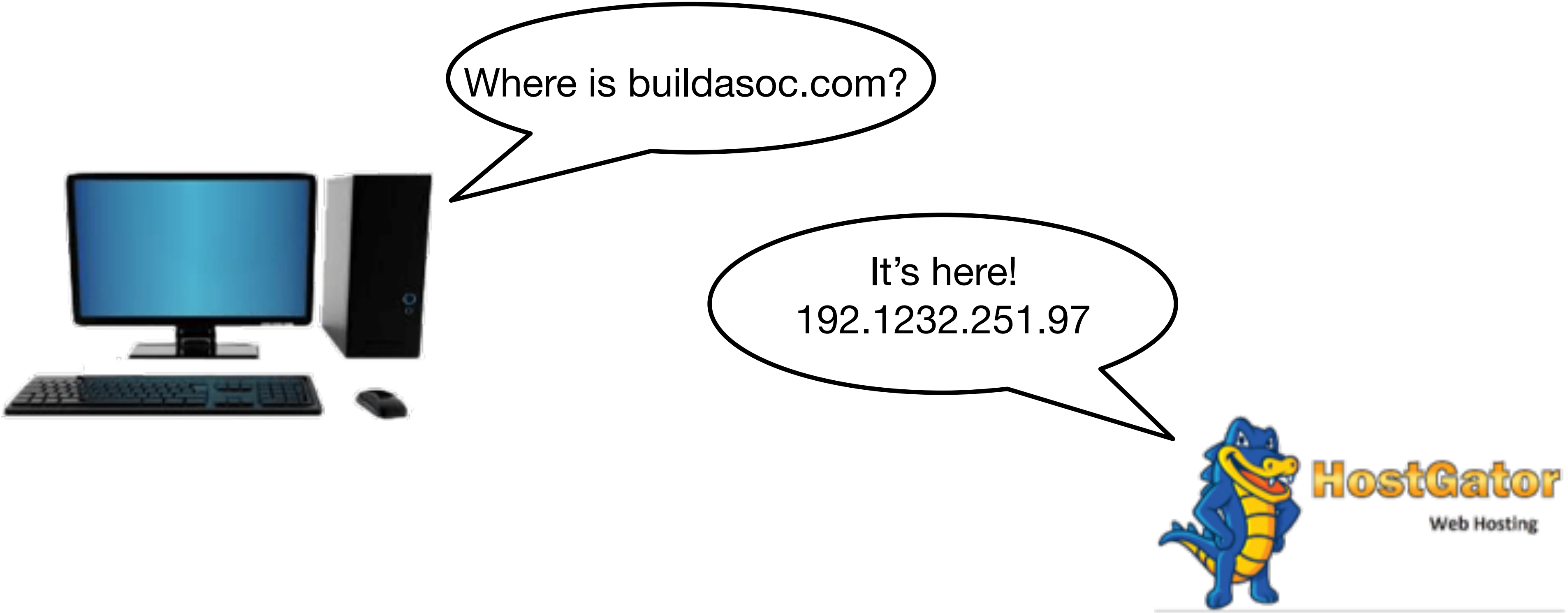
Looking at an unmonitored site

Where is buildasoc.com?

Go ask:

ns155.hostgator.com
ns156.hostgator.com

Normal DNS

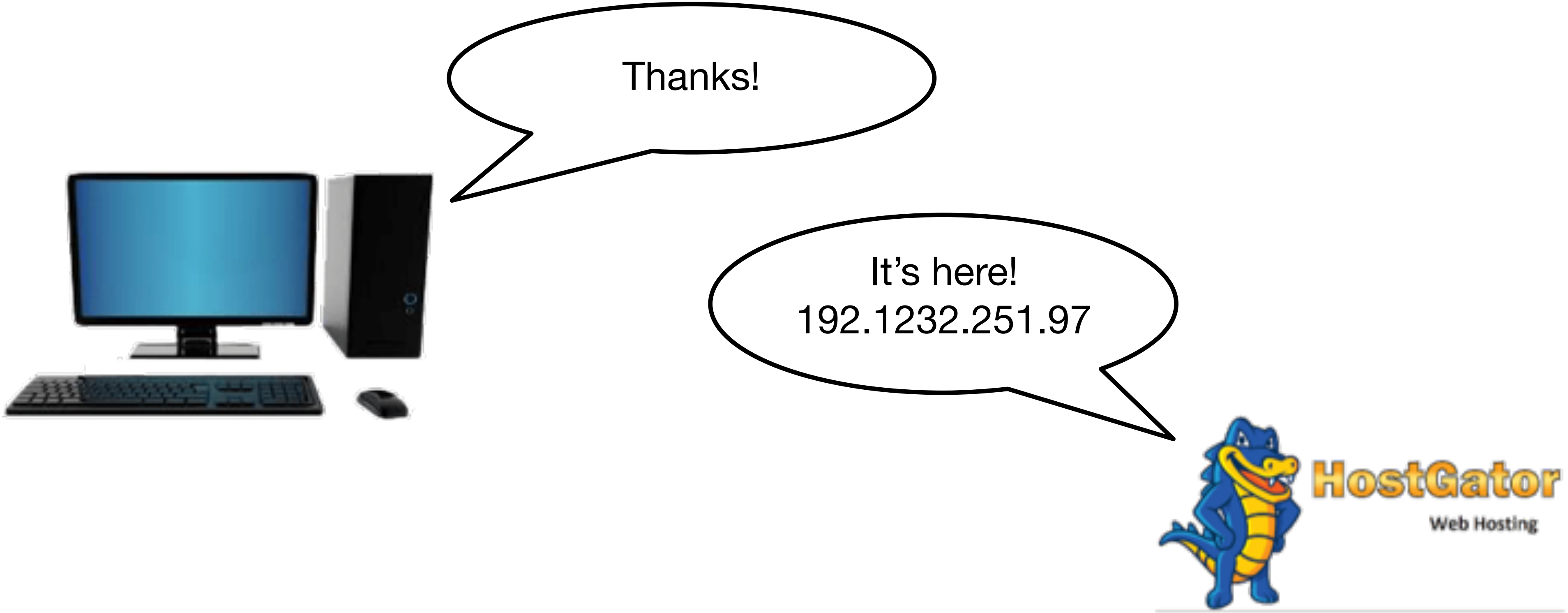


Where is buildasoc.com?

It’s here!
192.1232.251.97

ns1.hostgator.com
ns2.hostgator.com

Normal DNS



ns155.hostgator.com
ns156.hostgator.com

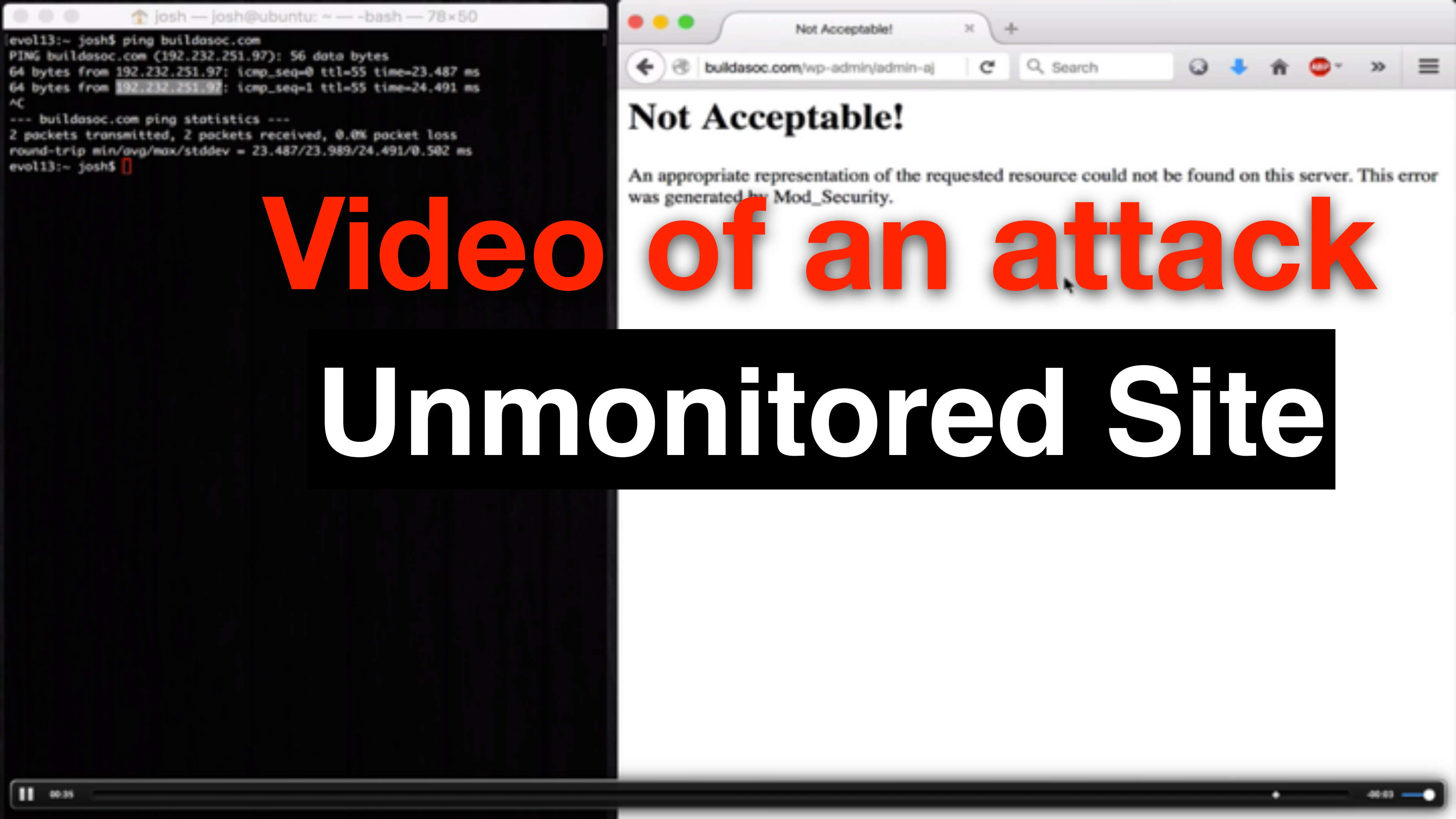
Normal DNS

buildasoc – SOC Building!
buildasoc.com
Search
buildasoc
SHOW ME

Normal DNS

Video of an attack

Unmonitored Site



josh — josh@ubuntu: ~ — -bash — 78×50

```
evol13:~ josh$ ping buildasoc.com
PING buildasoc.com (192.232.251.97): 56 data bytes
64 bytes from 192.232.251.97: icmp_seq=0 ttl=55 time=23.487 ms
64 bytes from 192.232.251.97: icmp_seq=1 ttl=55 time=24.491 ms
^C
--- buildasoc.com ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 23.487/23.989/24.491/0.502 ms
evol13:~ josh$ 
```

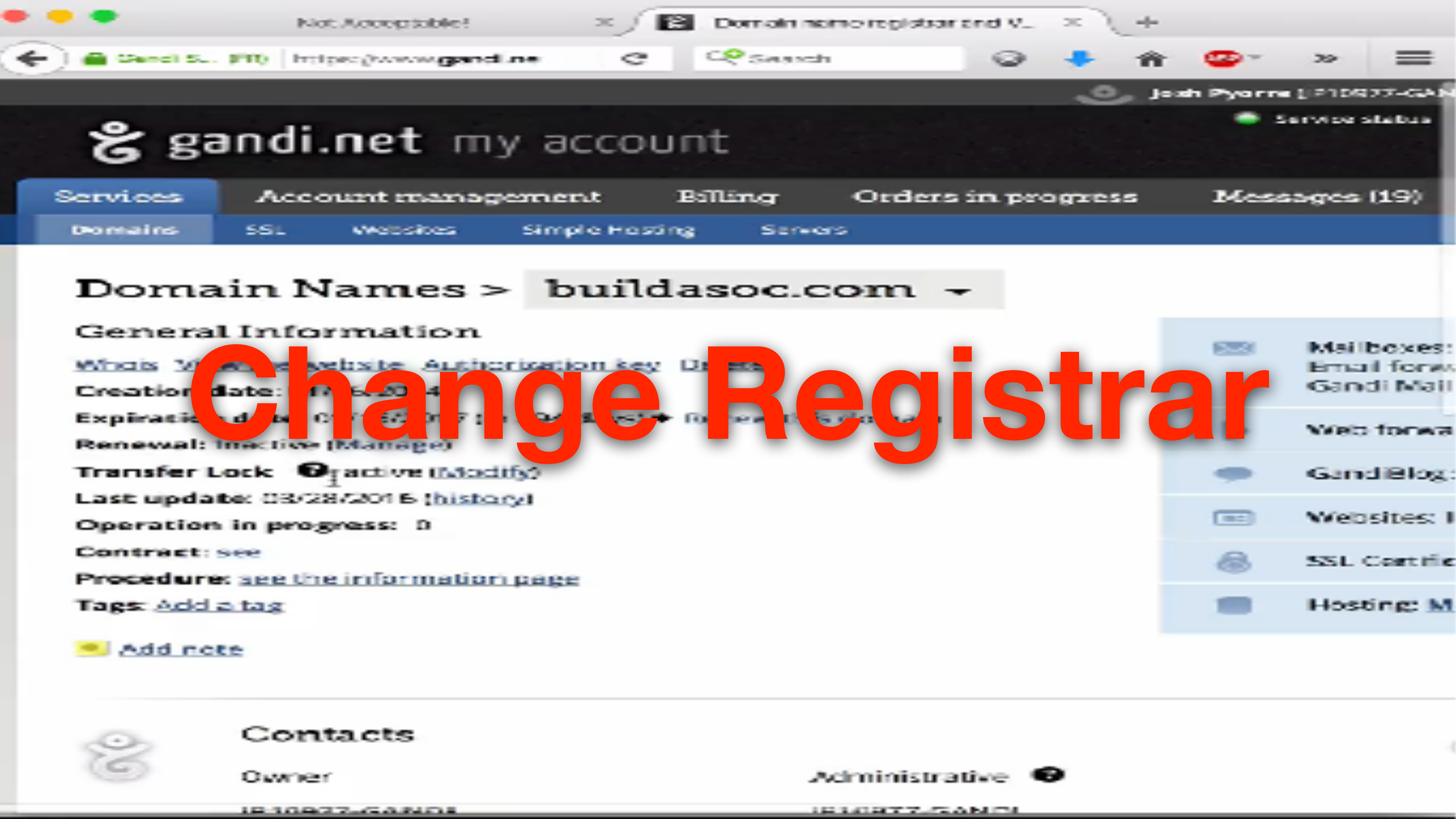
Not Acceptable!
buildasoc.com/wp-admin/admin-aj
Search

Not Acceptable!

An appropriate representation of the requested resource could not be found on this server. This error was generated by Mod_Security.

Adding an IDS

Change Registrar



Domain Names > buildasoc.com

General Information

Creation date: [illegible]

Expiration date: [illegible]

Renewal: Inactive (Manage)

Transfer Lock: active (Modify)

Last update: 03/28/2016 (history)

Operation in progress: 0

Contract: see

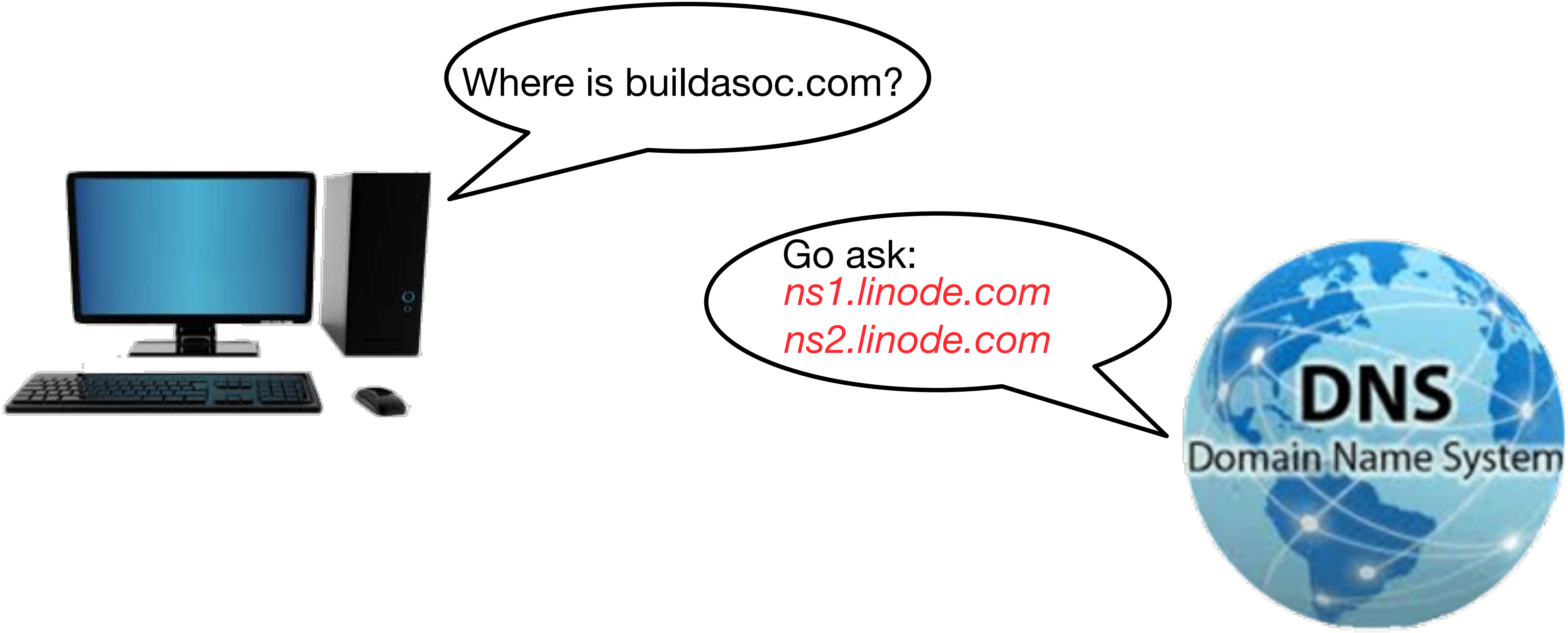
Procedure: see the information page

Tags: Add a tag

Contacts

Owner

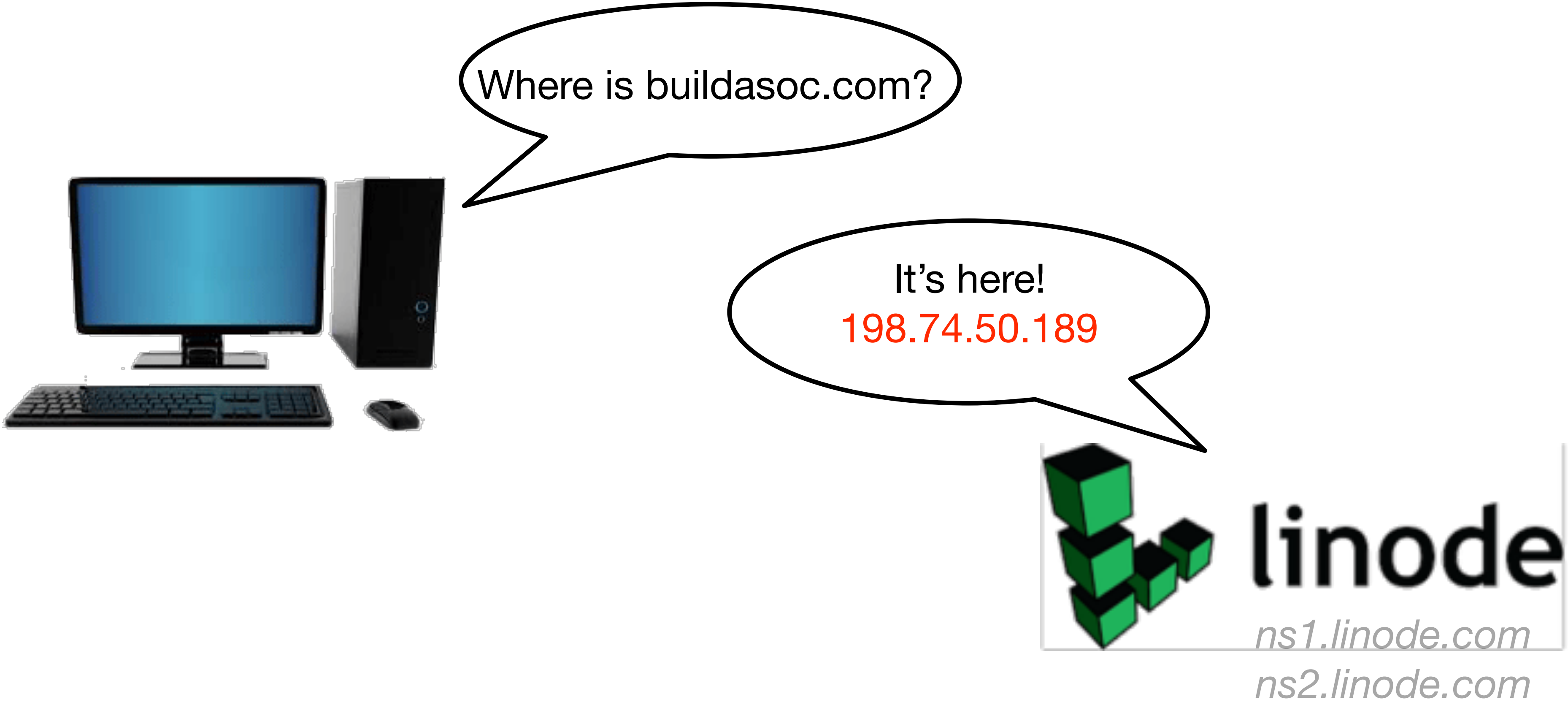
Administrative



Where is buildasoc.com?

Go ask:
ns1.linode.com
ns2.linode.com

Modified DNS



Where is buildasoc.com?

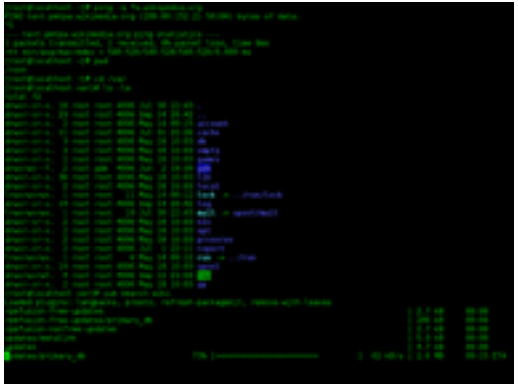
It’s here!
198.74.50.189

ns1.linode.com
ns2.linode.com

Modified DNS

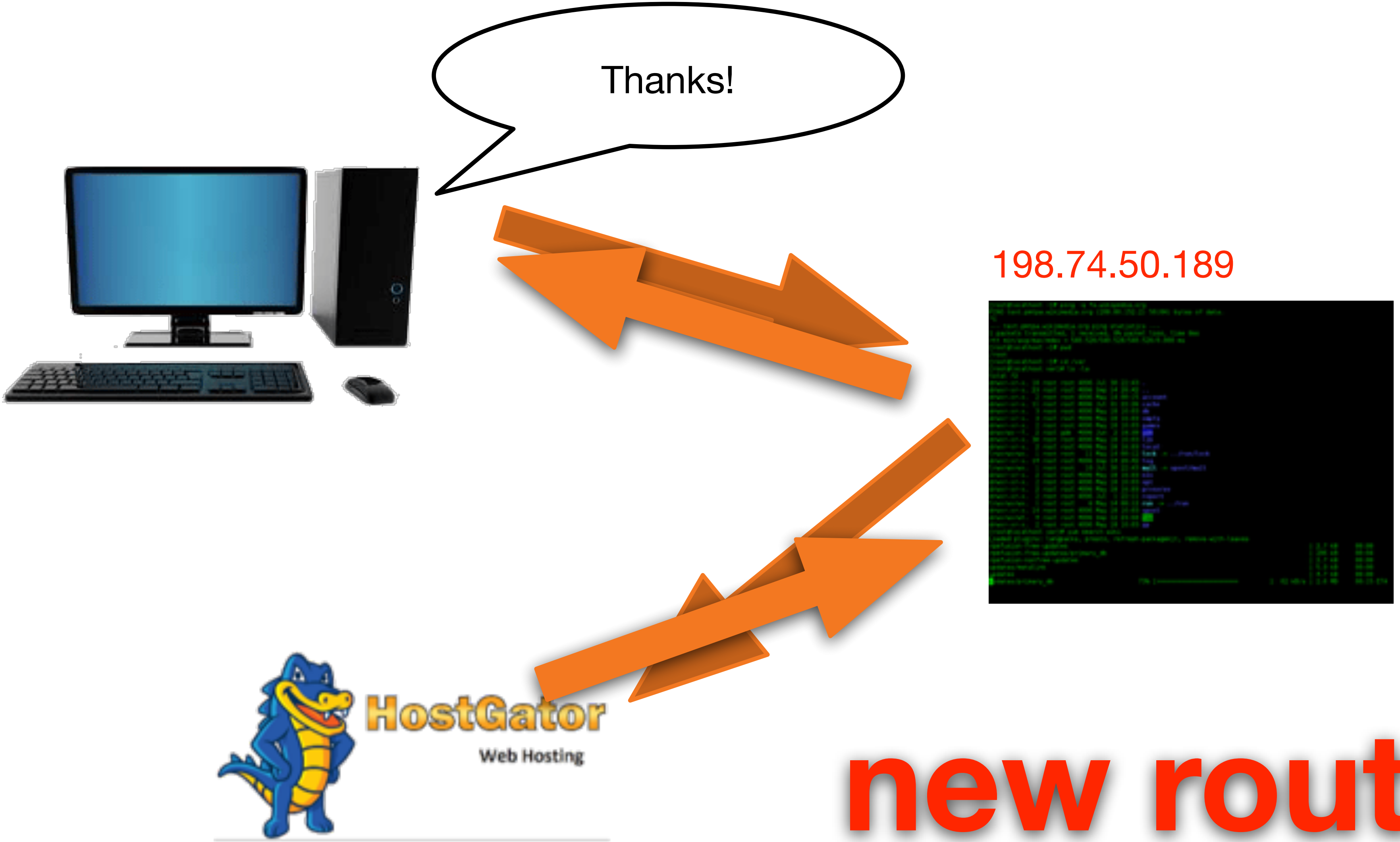
Where is buildasoc.com?

198.74.50.189



Linux system, running docker/IDS/proxy

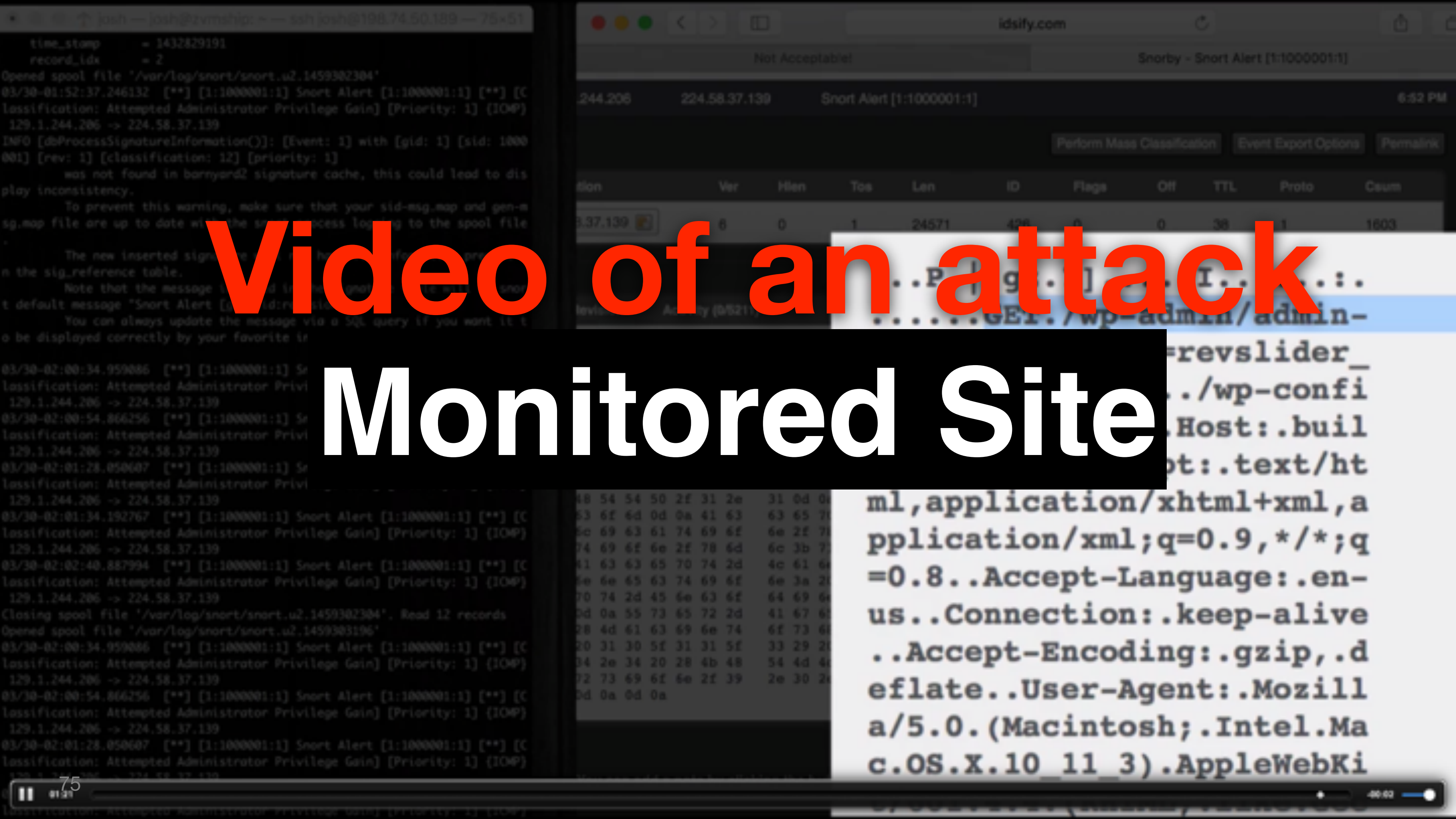
Modified DNS



new route

User sees the site as normal

Modified DNS



Video of an attack

Monitored Site

josh — josh@zvmship: ~ — ssh josh@198.74.50.189 — 75×51
idsify.com
Not Acceptable!
Snorby - Snort Alert [1:1000001:1]
Perform Mass Classification
Event Export Options
Permalink

```
    time_stamp        = 1432829191
    record_idx        = 2
Opened spool file '/var/log/snort/snort.u2.1459302304'
03/30-01:52:37.246132  [**] [1:1000001:1] Snort Alert [1:1000001:1] [**] [C
lassification: Attempted Administrator Privilege Gain] [Priority: 1] {ICMP}
 129.1.244.206 -> 224.58.37.139
INFO [dbProcessSignatureInformation()]: [Event: 1] with [gid: 1] [sid: 1000
001] [rev: 1] [classification: 12] [priority: 1]
        was not found in barnyard2 signature cache, this could lead to dis
play inconsistency.
        To prevent this warning, make sure that your sid-msg.map and gen-m
sg.map file are up to date with the snort process logging to the spool file
.
        The new inserted signature
n the sig_reference table.
        Note that the message
t default message "Snort Alert [
        You can always update the message via a SQL query if you want it t
o be displayed correctly by your favorite in

03/30-02:00:34.959086  [**] [1:1000001:1] Sn
lassification: Attempted Administrator Privi
 129.1.244.206 -> 224.58.37.139
03/30-02:00:54.866256  [**] [1:1000001:1] Sn
lassification: Attempted Administrator Privi
 129.1.244.206 -> 224.58.37.139
03/30-02:01:28.050607  [**] [1:1000001:1] Sn
lassification: Attempted Administrator Privi
 129.1.244.206 -> 224.58.37.139
03/30-02:01:34.192767  [**] [1:1000001:1] Snort Alert [1:1000001:1] [**] [C
lassification: Attempted Administrator Privilege Gain] [Priority: 1] {ICMP}
 129.1.244.206 -> 224.58.37.139
03/30-02:02:40.887994  [**] [1:1000001:1] Snort Alert [1:1000001:1] [**] [C
lassification: Attempted Administrator Privilege Gain] [Priority: 1] {ICMP}
 129.1.244.206 -> 224.58.37.139
Closing spool file '/var/log/snort/snort.u2.1459302304'. Read 12 records
Opened spool file '/var/log/snort/snort.u2.1459303196'
03/30-02:00:34.959086  [**] [1:1000001:1] Snort Alert [1:1000001:1] [**] [C
lassification: Attempted Administrator Privilege Gain] [Priority: 1] {ICMP}
 129.1.244.206 -> 224.58.37.139
03/30-02:00:54.866256  [**] [1:1000001:1] Snort Alert [1:1000001:1] [**] [C
lassification: Attempted Administrator Privilege Gain] [Priority: 1] {ICMP}
 129.1.244.206 -> 224.58.37.139
03/30-02:01:28.050607  [**] [1:1000001:1] Snort Alert [1:1000001:1] [**] [C
lassification: Attempted Administrator Privilege Gain] [Priority: 1] {ICMP}
```

```
.244.206    224.58.37.139    Snort Alert [1:1000001:1]    6:52 PM

tion    Ver  Hlen  Tos  Len    ID   Flags  Off  TTL  Proto  Csum
.37.139  6    0     1   24571  428  0      0    38   1      1603
```

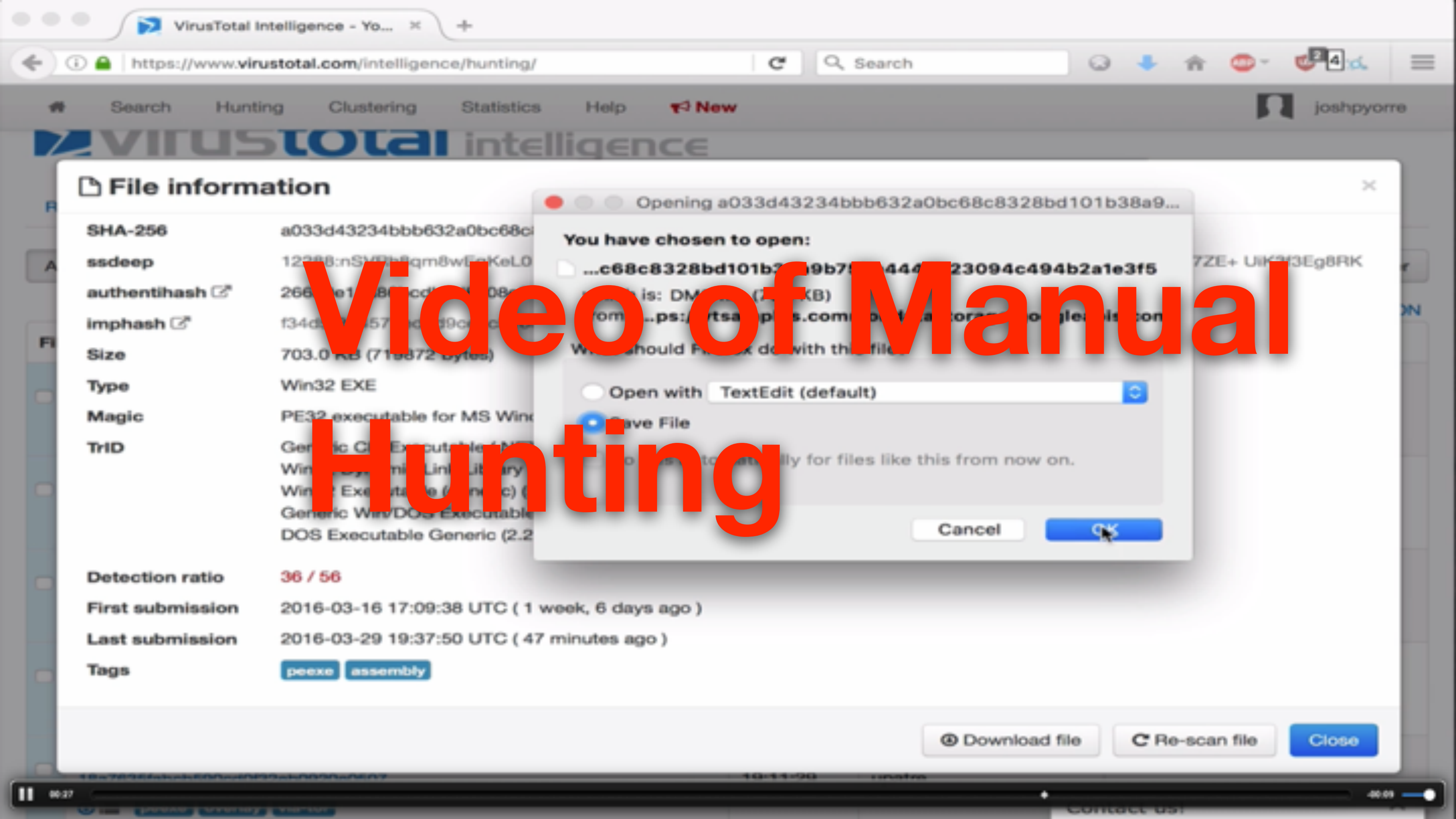
```
..P|g..]...I.....:.
.......GET./wp-admin/admin-
                 =revslider_
                 ../wp-confi
                 .Host:.buil
                 pt:.text/ht
ml,application/xhtml+xml,a
pplication/xml;q=0.9,*/*;q
=0.8..Accept-Language:.en-
us..Connection:.keep-alive
..Accept-Encoding:.gzip,.d
eflate..User-Agent:.Mozill
a/5.0.(Macintosh;.Intel.Ma
c.OS.X.10_11_3).AppleWebKi
```

Threat Analysis

..or predicting the future

Let’s talk about Automation

Video of Manual Hunting



VirusTotal Intelligence - Yo...
https://www.virustotal.com/intelligence/hunting/
Search
Search
Hunting
Clustering
Statistics
Help
New
joshpyorre
virustotal intelligence

File information

SHA-256 a033d43234bbb632a0bc68c

ssdeep 12288:nS...qm8w...KeL0 ...7ZE+ Ui...3Eg8RK

authentihash 266...e1...8...cd...08

imphash f34d...57...89c

Size 703.0 KB (719872 bytes)

Type Win32 EXE

Magic PE32 executable for MS Win

TrID Ge...ic CIL Executable ...
Win... Linl... Lib...ry
Win... Exe...table (...ic) (
Generic Win/DOS Executable
DOS Executable Generic (2.2

Detection ratio 36 / 56

First submission 2016-03-16 17:09:38 UTC (1 week, 6 days ago)

Last submission 2016-03-29 19:37:50 UTC (47 minutes ago)

Tags peexe assembly

Opening a033d43234bbb632a0bc68c8328bd101b38a9...

You have chosen to open:

...c68c8328bd101b3...9b7...444...23094c494b2a1e3f5

which is: DM... (7...KB)

from: ...ps://...tsa...p...s.com...o...a...tora...oogleapis.com

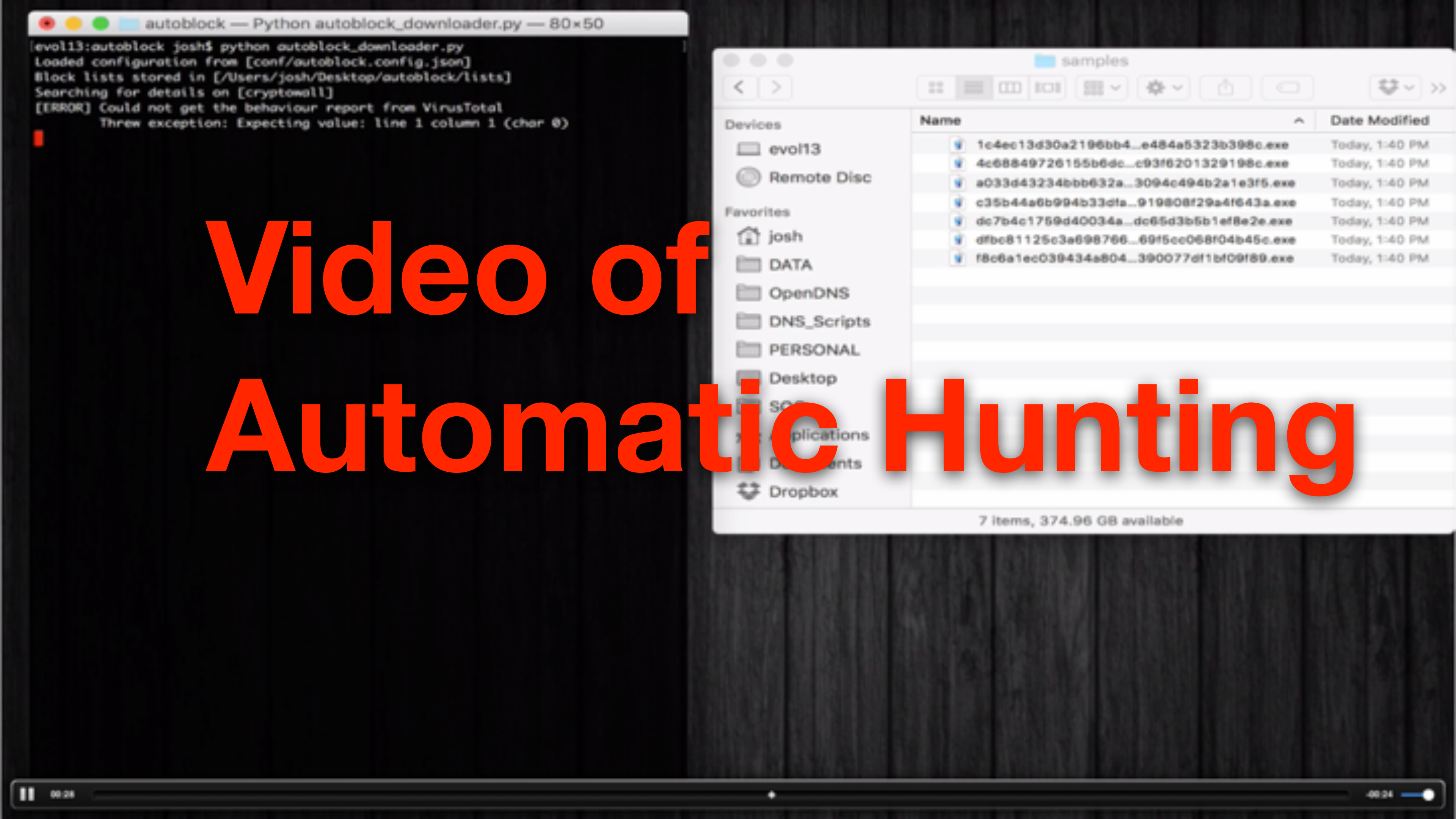
What should Firefox do with this file?

○ Open with TextEdit (default)

● Save File

Do this automatically for files like this from now on.

Video of Automatic Hunting



autoblock — Python autoblock_downloader.py — 80×50

```
evol13:autoblock josh$ python autoblock_downloader.py
 Loaded configuration from [conf/autoblock.config.json]
 Block lists stored in [/Users/josh/Desktop/autoblock/lists]
 Searching for details on [cryptowall]
 [ERROR] Could not get the behaviour report from VirusTotal
         Threw exception: Expecting value: line 1 column 1 (char 0)
```

samples

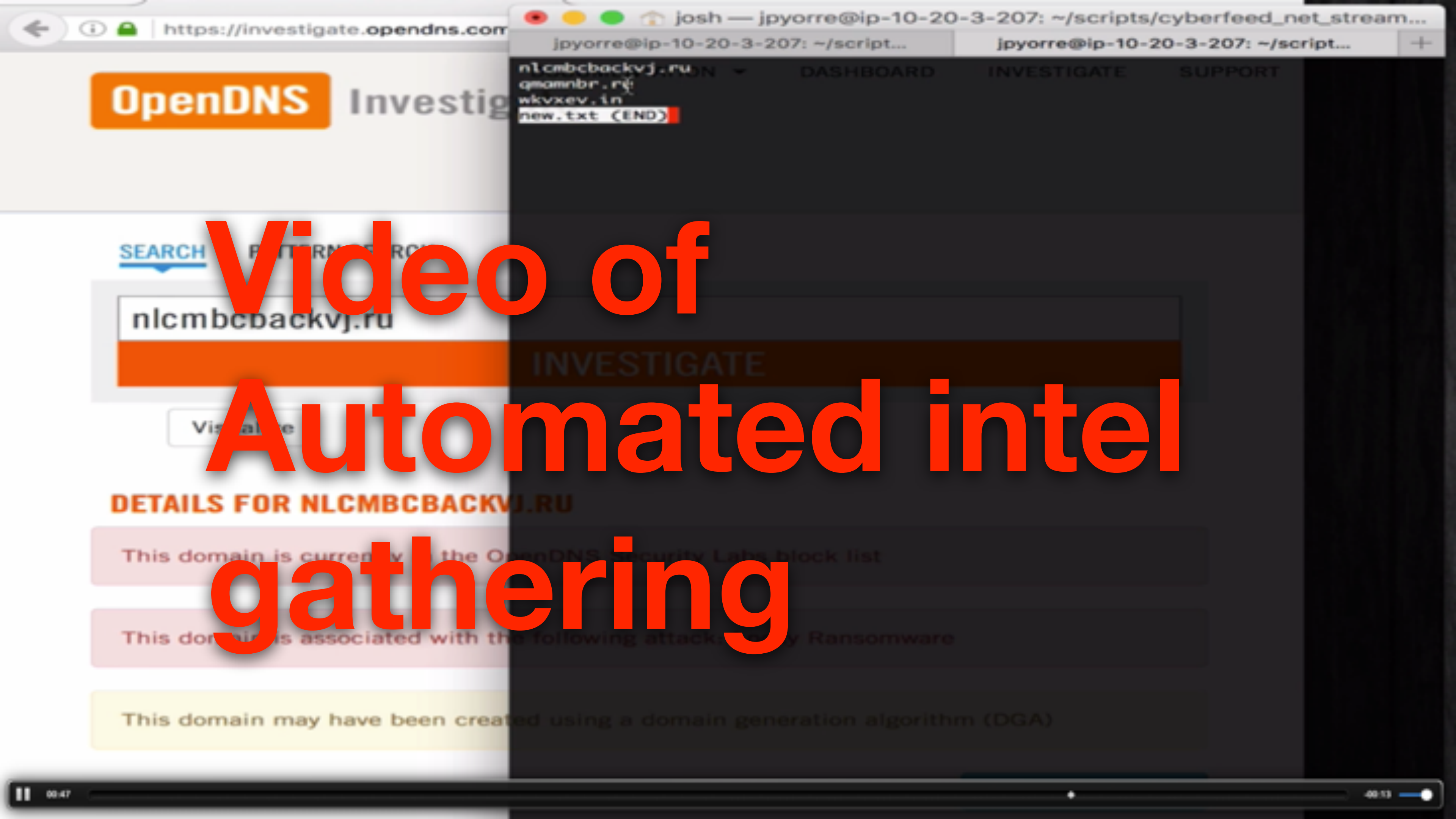
Name	Date Modified
1c4ec13d30a2196bb4...e484a5323b398c.exe	Today, 1:40 PM
4c68849726155b6dc...c93f620132919 8c.exe	Today, 1:40 PM
a033d43234bbb632a...3094c494b2a1e3f5.exe	Today, 1:40 PM
c35b44a6b994b33dfa...919808f29a4f643a.exe	Today, 1:40 PM
dc7b4c1759d40034a...dc65d3b5b1ef8e2e.exe	Today, 1:40 PM
dfbc81125c3a698766...69f5cc068f04b45c.exe	Today, 1:40 PM
f8c6a1ec039434a804...390077df1bf09f89.exe	Today, 1:40 PM

7 items, 374.96 GB available

Automatic Analysis

- Sending to Threat Services / Providing
- Sending to Cuckoo or malwr.com
- **Scraping Sites**

Video of Automated intel gathering



```
josh — jpyorre@ip-10-20-3-207: ~/scripts/cyberfeed_net_stream...
nlcmbcbackvj.ru
qmomnbr.ru
wkvxev.in
new.txt (END)
```

https://investigate.opendns.com

OpenDNS Investigate

nlcmbcbackvj.ru

DETAILS FOR NLCMBCBACKVJ.RU

This domain is currently in the OpenDNS Security Labs block list

This domain is associated with the following attacks: Locky Ransomware

This domain may have been created using a domain generation algorithm (DGA)

jpyorre@cisco.com

jpyorre@opendns.com

@joshpyorre

rootaccesspodcast.com