RSA CONFERENCE 2022

SECURITY OPERATIONS CENTER FINDINGS REPORT

Published by

NETWITNESS

CISCO
SECURE

Written by
Steve Fink, Jessica Bair Oppenheimer and David Glover

CONTENTS

Contents

DISCLAIMER

It is important to clearly understand the role of the security operations center ("SOC") at RSA Conference ("RSAC").

- The SOC is an educational exhibit sponsored by NetWitness®, a RSA Security LLC company ("NetWitness") and Cisco Systems, Inc. ("Cisco") that monitors network activity during the course of the RSA Conference event.
- By connecting to Moscone Center WIFI or using the RSAC mobile application, all RSAC attendees (including e.g., sponsors, exhibitors, guests, employees) accepted the following terms and conditions: *"THE WIRELESS NETWORK AVAILABLE AT THE MOSCONE CENTER IS AN OPEN, UNSECURED 5 GHZ NETWORK. NETWITNESS AND CISCO SYSTEMS WILL BE USING DATA FROM THE MOSCONE WIRELESS NETWORK FOR AN EDUCATIONAL DEMONSTRATION ON A WORKING SOC. WE STRONGLY RECOMMEND THAT YOU USE APPROPRIATE SECURITY MEASURES, SUCH AS UTILIZING A VPN CONNECTION, INSTALLING A PERSONAL FIREWALL AND KEEPING YOUR OPERATING SYSTEM UP-TO-DATE WITH SECURITY PATCHES. WE RECOMMEND TURNING OFF YOUR WIRELESS ADAPTER WHEN NOT IN USE AND ENSURING AD-HOC (PEER-TO-PEER) CAPABILITIES ARE DISABLED ON YOUR DEVICE.)."*
- Additionally, RSA Conference advised attendees of the educational SOC in printed materials and onsite signage.
- The SOC is not a true security operations center. The infrastructure at the event is managed by the Moscone Center, except for Cisco Umbrella DNS, and only has a SPAN of the network traffic from the Moscone Center wireless network (named .RSACONFERENCE). There are limited log files from Cisco Firepower Threat Defense Intrusion Detection System (IDS) because it is not inline; however, the primary data is a real-time mirror of the traffic traversing the wireless network.
- The SOC goal is to use technology to educate RSAC attendees about what happens on a typical open, unsecured wireless network. The education comes in the form of SOC tours, an RSAC session and the publication of a Findings Report issued by sponsors RSA and Cisco.
- The RSAC SOC team is not part of the RSAC security team. As such, the RSAC SOC acted as an educational exercise only and was not intended to protect, mitigate or remediate any issue uncovered during the SOC educational exercise.
- "The network" is a typical network that users connect to for internet access, similar to networks in hotels, airports or coffee shops. The network used during RSAC is an open network offered by the Moscone Center.
- The findings of this report and any security issues identified relate to user activity, not the network itself.
- Data collected by the RSAC SOC has been wiped and a certificate of completion is held by RSAC.

NOTE: This report was prepared as a summary of the RSA Conference educational SOC exercise. RSA, Cisco nor any of their employees or subcontractors, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or any third party's use or the results of such use of any information, product, or process referenced or disclosed herein, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement or recommendation.

THE NETWORK

The RSACONFERENCE wireless network is a flat network with no (as in zero) host isolation. This alone is an important statement and a great starting point for understanding wireless networks and the risks associated with connecting to them. A flat network without host isolation means that anyone with an IP address can theoretically communicate to any other devices on the network. Host isolation provides a device a one-way route out to the internet, but no routes within the network. Knowing which type of network you are attaching to can be discovered by identifying your IP address and trying to ping another IP address on that network. If you get a response, you are on a network without host isolation; if you get a "request timed out" response, you are probably isolated

TECHNOLOGY USED IN THE RSACSOC

The RSAC SOC team deployed the NetWitness® Platform XDR that included the NetWitness® Network, NetWitness® Logs and NetWitness® Orchestrator components for true XDR. Along with Cisco SecureX XDR, Cisco Secure Malware Analytics (formerly Cisco Threat Grid), Cisco Talos Intelligence, Cisco Firepower Threat Defense Intrusion Detection and Cisco Umbrella®

Also, donated licenses from IBM X-Force Exchange, Recorded Future and alphaMountain.ai, along with a half dozen open-source threat intelligence.

NetWitness® Platform XDR collects all the raw network traffic from a switch port analyzer (SPAN) from the Moscone Center network, generates metadata and visually prioritizes threats occurring in real time. It inspects every network packet session for threat indicators at time of collection and enriches this data with threat intelligence and business context.

For suspicious files that might be malicious, NetWitness® Platform XDRchecks a community anti-virus (AV) lookup, some static analysis and its own network intelligence. NetWitness Orchestrator® built on ThreatConnect then sends the files to Cisco Secure Malware Analytics for dynamic malware analysis.

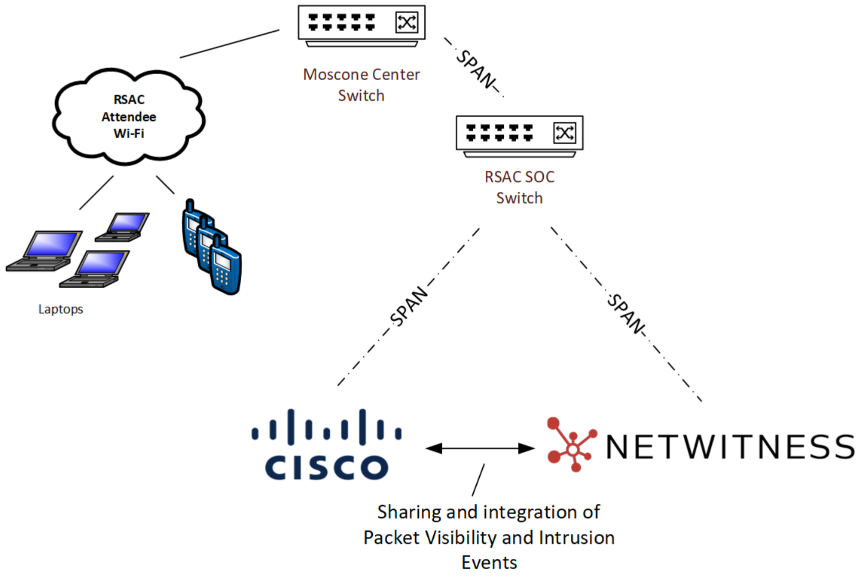
Secure Malware Analytics combines advanced sandboxing with threat intelligence in one unified solution to protect organizations from malware. It analyzes the behavior of a file against millions of samples and billions of malware artifacts. With Secure Malware Analytics, the RSAC SOC team had a global and historical view of the malware, its activity and how large a threat it posed to the RSAC network.

Secure Malware Analytics identifies key behavioral indicators of malware and their associated campaigns, which enabled the RSAC SOC team to save time by quickly prioritizing attacks with the biggest potential impact. The built- in Glovebox user interaction tool makes it possible to safely interact with samples and observe malware behavior directly.

Cisco Secure Firewall Firepower Threat Defense IDS receives the same network SPAN as RSA NetWitness® Network. The IDS inspects all wireless guest traffic from event attendees, configured in monitor-only mode. Firepower Threat Defense offers breach detection, threat discovery and security automation. Rich contextual information (such as applications, operating systems, vulnerabilities, intrusions, and transferred files) serves the SOC to help uncover threats lurking on the network. The Malware Analysis of the Secure Firewall Threat Defense also sends sample to Secure Malware Analytics for analysis.

Cisco Umbrella provided visibility into DNS activity, with default security blocking turned off. We also use Cisco SecureX XDR, which integrates threat intelligence from the Cisco Talos intelligence team and other sources, along with correlating sightings of indicators of compromise / observables from NetWitness® and the Cisco Secure Firewall / Firepower logs and Umbrella DNS queries.

Below shows a visual representation of the technology used at the RSAC SOC.



THESTATISTICS

A commonly requested RSACSOC Findings session, attendees requested more statistics. The RSAC SOC team tried their best to provide more statistics and refined context and granularity.

2022 Stats from **~19,000** attendees (down from ~39,000 in 2020)

Total packets captured: **11.8 billion** (down from 12.7 billion)

Total logs captured: **108 million** (up from 88.3 million)

Total sessions: 187.3 million

Total unique devices: 13,253
Total packets written to disk: **7.39 terabytes** (down from 8.08

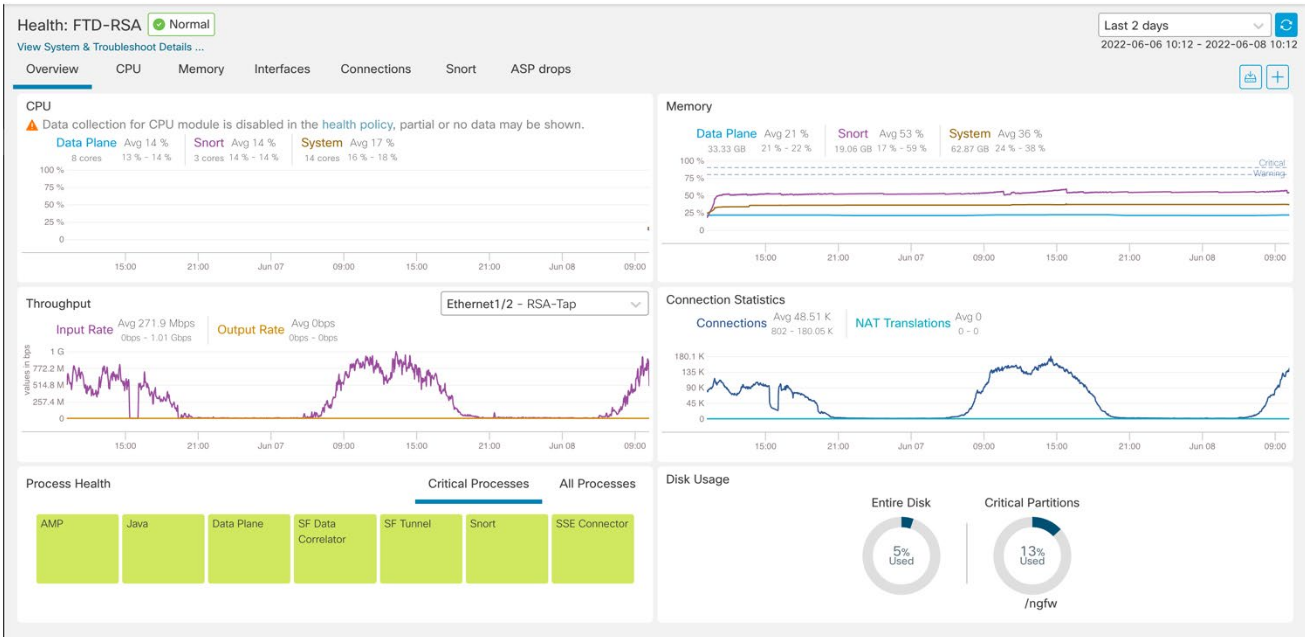
terabytes)

Total logs written to disk: 50.8 gigabytes

Peak bandwidth utilization: 1.35 Gbps (equivalent to 1.30 Gbps)

DNS Requests: **~46 million** (up from 37 million)
Totalcleartextusername/passwords: **55,525** (down from 96,361)
Unique devices/accountswithcleartextusernames/passwords: **2,210** (up from 2,178)

Total files sent for malware analysis: **570+** (down from +10,000)


Health: FTD-RSA
Normal
View System & Troubleshoot Details ...
Last 2 days
2022-06-06 10:12 - 2022-06-08 10:12
Overview
CPU
Memory
Interfaces
Connections
Snort
ASP drops
CPU
Data collection for CPU module is disabled in the health policy, partial or no data may be shown.
Data Plane Avg 14 % 8 cores 13 % - 14 %
Snort Avg 14 % 3 cores 14 % - 14 %
System Avg 17 % 14 cores 16 % - 18 %
100 %
75 %
50 %
25 %
0
15:00
21:00
Jun 07
09:00
15:00
21:00
Jun 08
09:00
Memory
Data Plane Avg 21 % 33.33 GB 21 % - 22 %
Snort Avg 53 % 19.06 GB 17 % - 59 %
System Avg 36 % 62.87 GB 24 % - 38 %
Critical
Warning
Throughput
Ethernet1/2 - RSA-Tap
Input Rate Avg 271.9 Mbps 0bps - 1.01 Gbps
Output Rate Avg 0bps 0bps - 0bps
values in bps
1 G
772.2 M
514.8 M
257.4 M
Connection Statistics
Connections Avg 48.51 K 802 - 180.05 K
NAT Translations Avg 0 0 - 0
180.1 K
135 K
90 K
45 K
Process Health
Critical Processes
All Processes
AMP
Java
Data Plane
SF Data Correlator
SF Tunnel
Snort
SSE Connector
Disk Usage
Entire Disk
5% Used
Critical Partitions
13% Used
/ngfw

2020 Stats (from ~39,000 attendees)

Total packets captured: 12.7 billion

Total logs captured: 88.3 million

Total sessions: 187.3 million

Total unique devices: 13,253

Total packets written to disk: 8.08 terabytes

Total logs written to disk: 50.52 gigabytes

Peak bandwidth utilization: 1.3 Gbps

DNS Requests: 37 million

Total cleartext username/passwords: 96,361

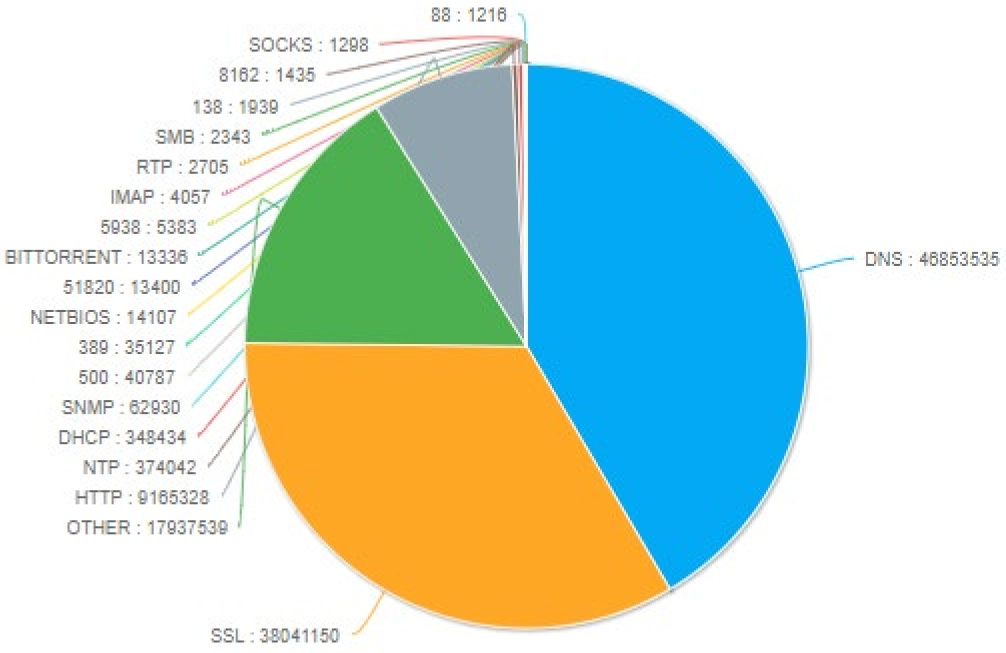
Unique devices/accounts with cleartext usernames/passwords: 2,178

Total files sent for malware analysis: 10,000+

THE DATA

The RSAC SOC started analyzing all wireless traffic on Monday, June 6, 2022, and collected traffic through Thursday, June 9, 2022, at 3p.m. There were 187,301,858 sessions during this period. Which was 2.5 times the amount of traffic collected from RSAC 2019. This corresponds to a bandwidth utilization of 1.35 Gbps vs. 2020 of 1.3 Gbps and 740 Mbps in 2019.

Historically speaking, events where this team has provided services such as in the United States and the United Kingdom, the average percentage of encrypted vs. unencrypted traffic has varied from 60-78 percent encrypted and 22-40 percent unencrypted. For RSAC 2022, the SOC saw an uptick in the amount of encrypted traffic, at 80 percent, from 78 percent in both RSAC 2019 and 2020. 55,029,102 of the 70,440,998 sessions were encrypted.



Encrypted vs. Unencrypted

Encryption of traffic is relevant because of the amount of information that RSAC attendees leak. The unencrypted traffic presents a number of threats to both individuals and organizations. A company or person does not need NetWitness® Platform XDR, Cisco Firepower or Cisco Malware Analytics to view unencrypted traffic, as any attendee, with the help of a quick internet search, can collect a subset of this data on a personal device. NetWitness and Cisco allow the RSAC SOC to collect all the data and easily analyze the top threat categories, as well as understand if any of those threats are seen by other attendees. Think of this as north-south and east-west. Encrypting traffic does not necessarily make one more secure, but it does stop individuals from giving away their credentials, and organizations from giving away corporate asset information in the clear.

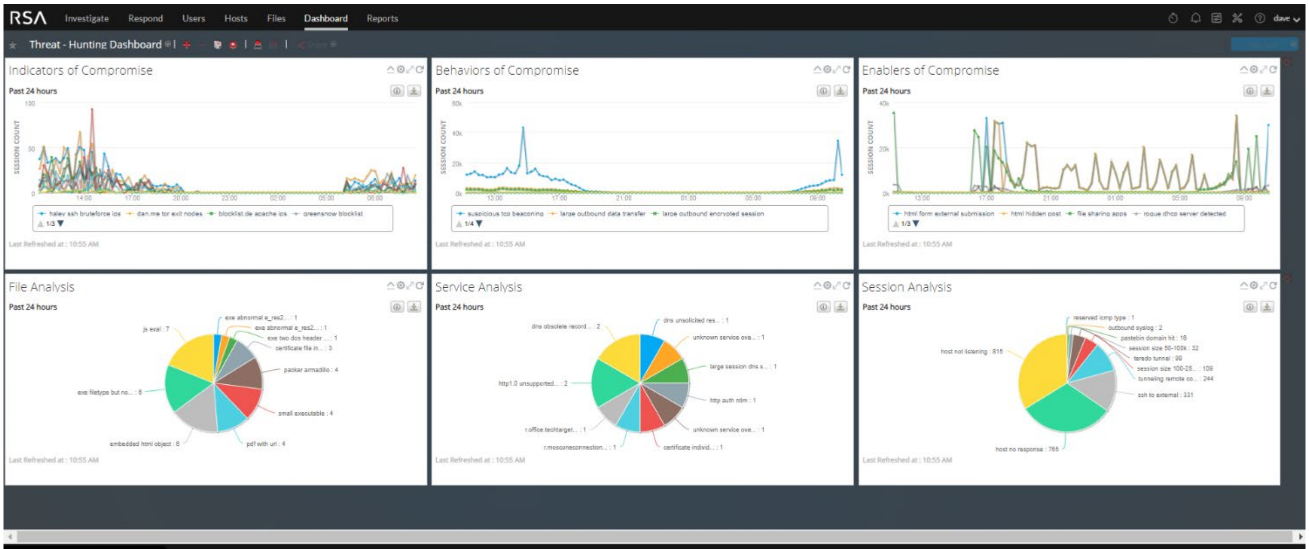
The role of the RSAC SOC around this issue is to help educate RSAC attendees about the information that is readily available on a public wireless network. In the past, we have spoken to many people on SOC tours about their mobile applications. We have seen mobile applications such as dating and home security video camera applications streaming data in the clear. Authentication to the apps was secure, but once authenticated, the data went back to an insecure transport—and we could see it all. Fortunately, many of these applications, but not all, have been secured and are now using secure protocols post-authentication to secure viewing.

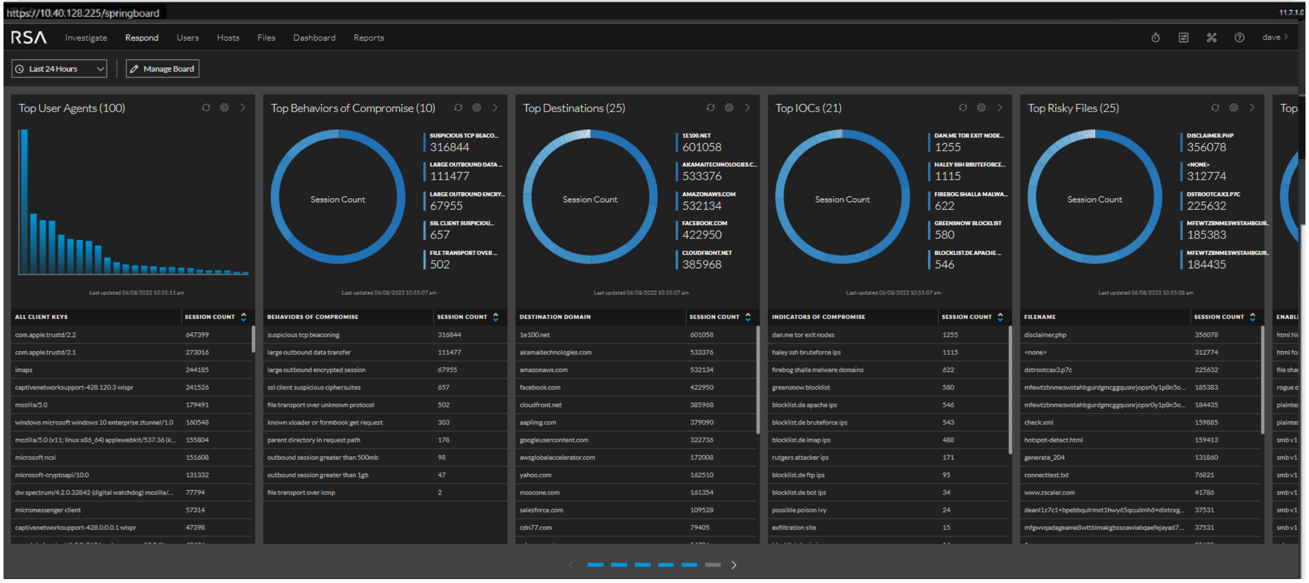
Cleartext Usernames and Passwords

Cleartext usernames and passwords continue to pose a problem. The RSAC SOC saw 55,525 cleartext passwords (down from 96,361 in 2020) from 2,210 unique accounts (up from 2,178 in 2020). Both are an improvement from 2019, when nobody on the RSAC SOC team wanted to figure out the number because it exceeded the counter that maxed out at 100,000+. There is a lot to discuss when throwing out a number this large for a four-day conference of security professionals on a public wireless network, so let's dig in.

Cleartext Usernames and Passwords: SNMP

Almost 80 percent of the 96,361 cleartext usernames and passwords came from corporate devices using older Simple Network Management Protocol (SNMP) versions 1 and 2. This is not necessarily a high-fidelity threat; however, it does leak information about the device as well as the organization it's trying to communicate with. SNMPv3 adds security to the protocol, so this is something organizations can implement to avoid prying eyes.





ALL CLIENT KEYS	SESSION COUNT
com.apple.trustd/2.2	647399
com.apple.trustd/2.1	273016
imaps	244185
captivenetworksupport-428.120.3 wispr	241526
mozilla/5.0	179491
windows microsoft windows 10 enterprise ztunnel/1.0	160548
mozilla/5.0 (x11; linux x86_64) applewebkit/537.36 (k...	155804
microsoft ncsi	151608
microsoft-cryptoapi/10.0	131332
dw spectrum/4.2.0.32842 (digital watchdog) mozilla/...	77794
micromessenger client	57314
captivenetworksupport-428.0.0.0.1 wispr	47398

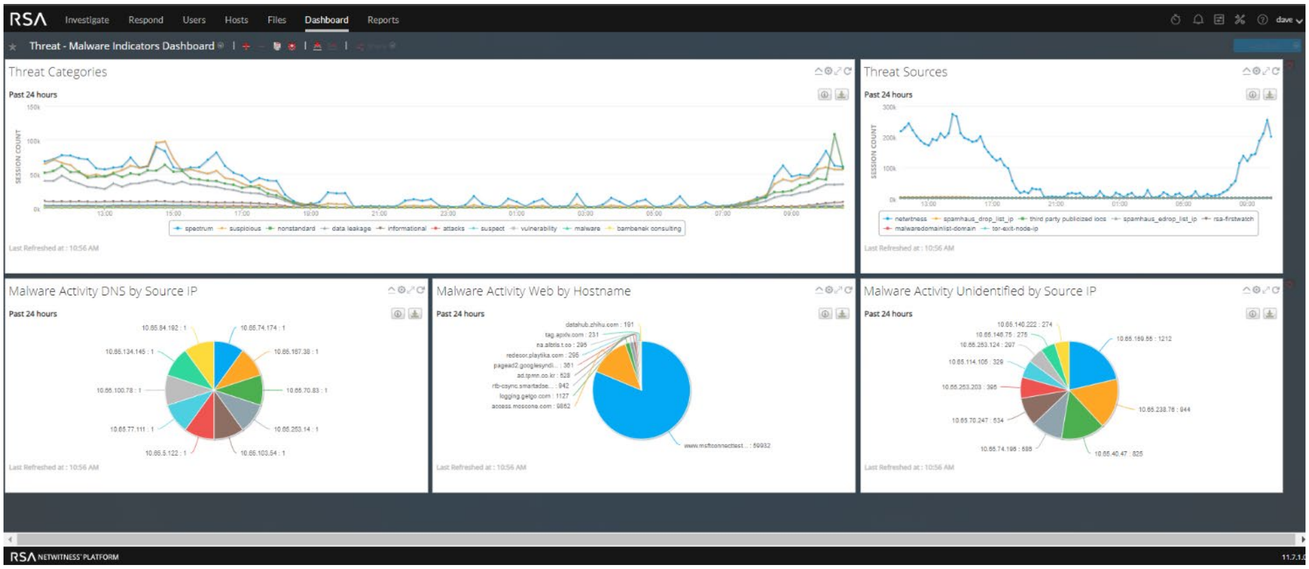
BEHAVIORS OF COMPROMISE	SESSION COUNT
suspicious tcp beaconing	316844
large outbound data transfer	111477
large outbound encrypted session	67955
ssl client suspicious ciphersuites	657
file transport over unknown protocol	502
known xloader or formbook get request	303
parent directory in request path	178
outbound session greater than 500mb	98
outbound session greater than 1gb	47
file transport over icmp	2

DESTINATION DOMAIN	SESSION COUNT
1e100.net	601058
akamaitechnologies.com	533376
amazonaws.com	532134
facebook.com	422950
cloudfront.net	385968
aaplimg.com	379090
googleusercontent.com	322736
awsglobalaccelerator.com	172008
yahoo.com	162510
moscone.com	161354
salesforce.com	109528
cdn77.com	79405

INDICATORS OF COMPROMISE	SESSION COUNT
dan.me tor exit nodes	1255
haley ssh bruteforce ips	1115
firebog shalla malware domains	622
greensnow blocklist	580
blocklist.de apache ips	546
blocklist.de bruteforce ips	543
blocklist.de imap ips	488
rutgers attacker ips	171
blocklist.de ftp ips	95
blocklist.de bot ips	34
possible poison ivy	24
exfiltration site	15

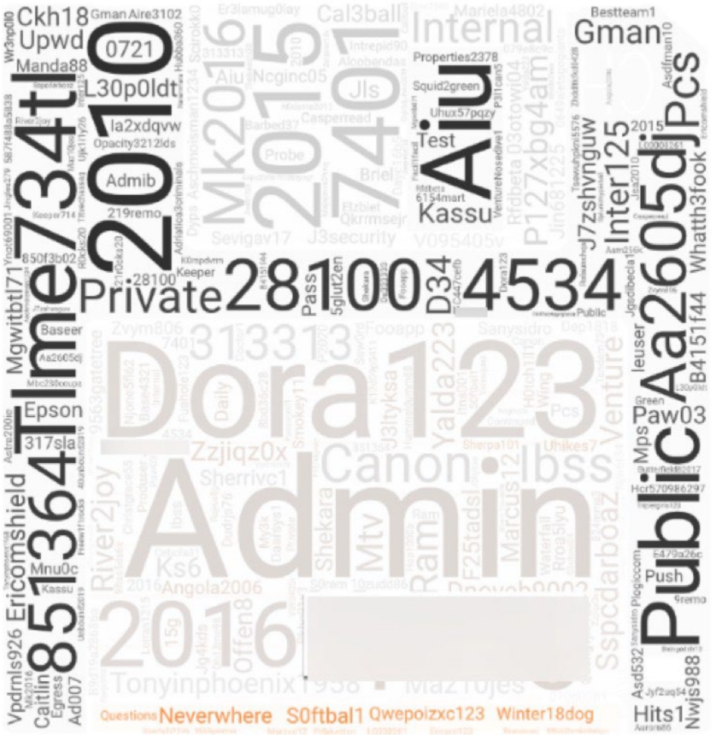
FILENAME	SESSION COUNT
disclaimer.php	356078
<none>	312774
dstrootcax3.p7c	225632
mfewtzbnmeswstahbgurdgmcggqusnrjopsr0y1p8n5o...	185383
mfewtzbnmeswstahbgurdgmcggqusnrjopsr0y1p8n5o...	184435
check.xml	159885
hotspot-detect.html	159413
generate_204	131860
connecttest.txt	76821
www.zscaler.com	41786
deanl1z7c1+bpebbqulrmxt1hwy65qcudmh6+dixtcxg...	37531
mfgwvqadageame8wttblmakgbssoawiabqaefejayad7...	37531

ENABL
html hi
html fo
file sha
rogue d
plainte
plainte
smb v1
smb v1
smb v1
smb v1
smb v1
smb v1



Cleartext Usernames and Passwords: POP3/IMAP2/HTTP

Removing SNMP from the cleartext username and password totals, we can start to focus on the attendees' security posture.



The above image is made up of actual passwords that were seen on the wireless network at RSAC in years past. Security conferences typically have many vendors displaying their wares on the expo floor. RSAC is no exception, and some of these cleartext usernames and passwords appeared to be from demo environments. Looking at other protocols, the majority of the cleartext usernames and passwords came from older protocols such as POP3, IMAP2, HTTP and FTP.

The use of POP3, IMAP2 and HTTP could provide an interesting conversation about who, what, where and why. It is difficult to send email in cleartext these days, and analyzing these incidents found similarities. Most of this traffic was to and from hosted domains. This means email services on domains that are family names or small businesses. The RSAC SOC team plans to work with RSAC to help notify those who are sending email in cleartext.

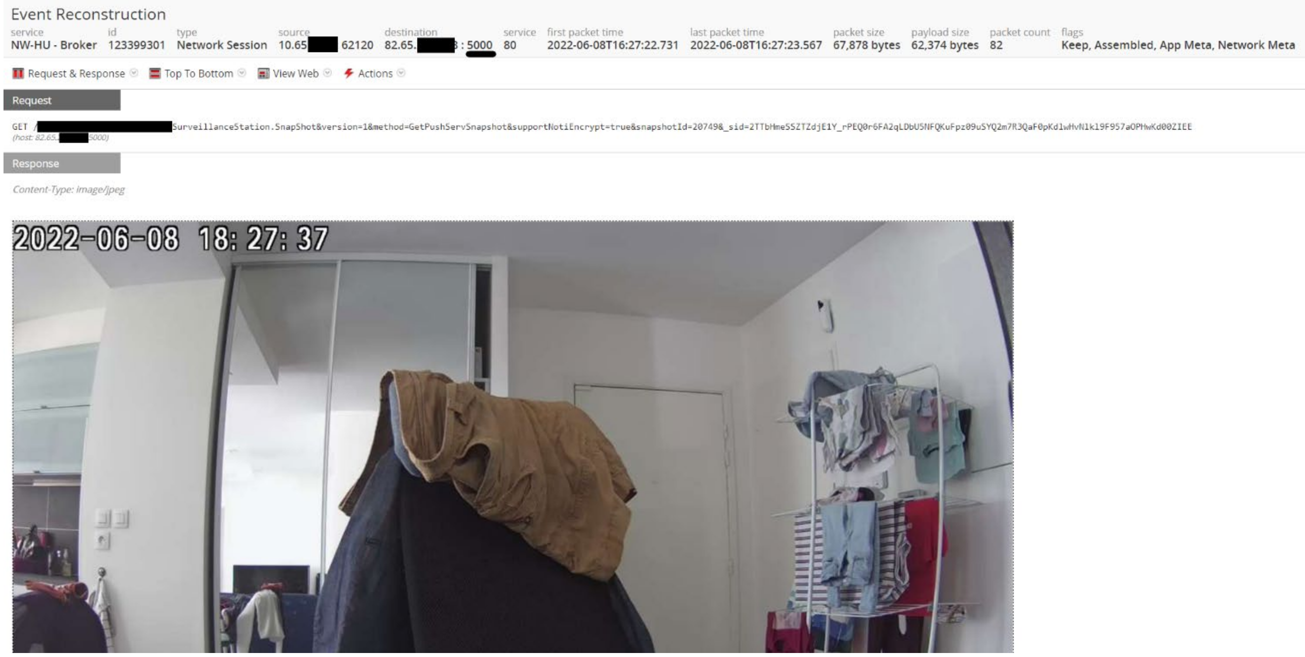
Cleartext Usernames and Passwords: Password Security, Protocol Insecurity

Further investigation into the POP3, IMAP2 and HTTP protocols raised some interesting questions about users and their lack of understanding about password strength vs. protocol. Most major online email providers use Secure Socket Layer (SSL) security, and these providers, for the most part, are not in cleartext. So, what's the issue?

Once again, within the cleartext username and password data, there were passwords that were very complex. This means the passwords were long, and they had upper- and lower-case, numeric and special characters. Password security is very important, but if we do not understand the protocols we use, our efforts in security education are wasted. The passwords are complex (red rectangles in the image above), but it doesn't matter because they were sending the data in cleartext. Ultimately, you have to understand your device and its protocols, and use strong passwords—because as strong as some of these were, they were in cleartext.

Who’s Watching the Watchers?

RSAC 2022 saw the return of video feeds over port 80 from home security devices. Six years ago, the SOC team reported that authentication to many of these apps was secure, but post-authentication, the traffic reverted to port 80 and in the clear. Four to five years ago, we noticed post-authentication traffic maintained an SSL connection, which was great. This traffic could simply indicate older equipment or a vendor that has not implemented this type of security. Below you will see various image a photo that was traversed the RSAC wireless network in the clear, along with the geo location down to three meters.



Event Reconstruction

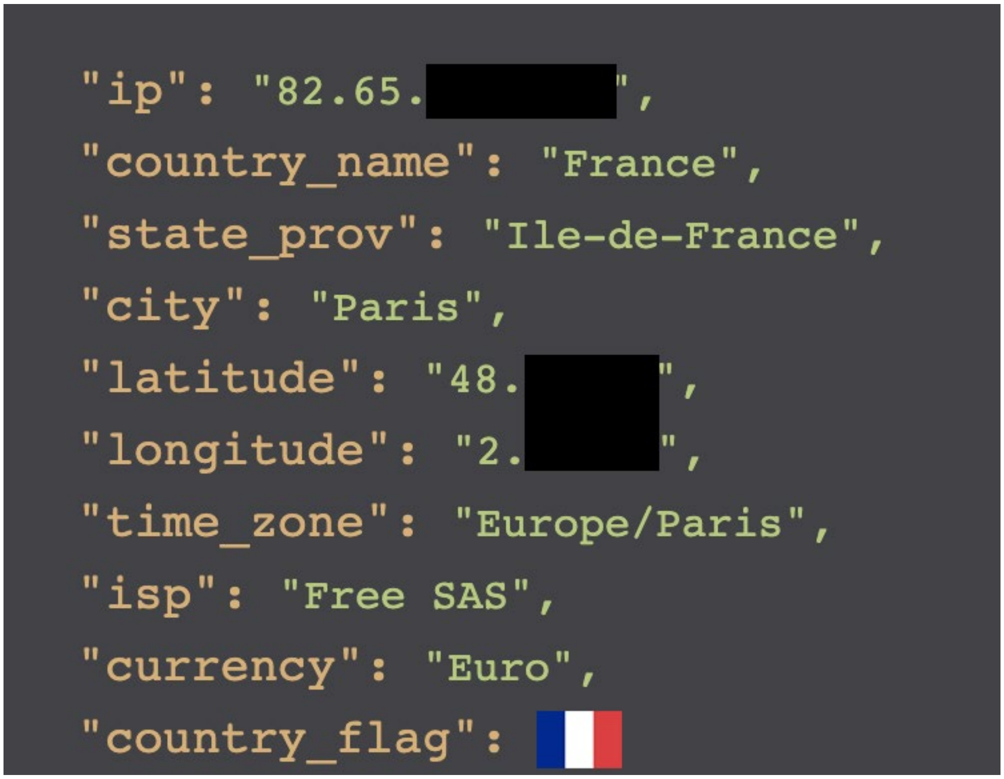
service	id	type	source	destination	service	first packet time	last packet time	packet size	payload size	packet count	flags
NW-HU - Broker	123399301	Network Session	10.65[redacted] 62120	82.65.[redacted] : 5000	80	2022-06-08T16:27:22.731	2022-06-08T16:27:23.567	67,878 bytes	62,374 bytes	82	Keep, Assembled, App Meta, Network Meta

Request

```
GET /[redacted]SurveillanceStation.SnapShot&version=1&method=GetPushServSnapshot&supportNotiEncrypt=true&snapshotId=20749&_sid=2TTbHme5SZTZdjE1Y_rPEQ0r6FA2qLDbU5NFQKuFpz09uSYQ2m7R3QaF0pKdlwHvN1k19F957aOPHwKd00ZIEE
(host: 82.65.[redacted]5000)
```

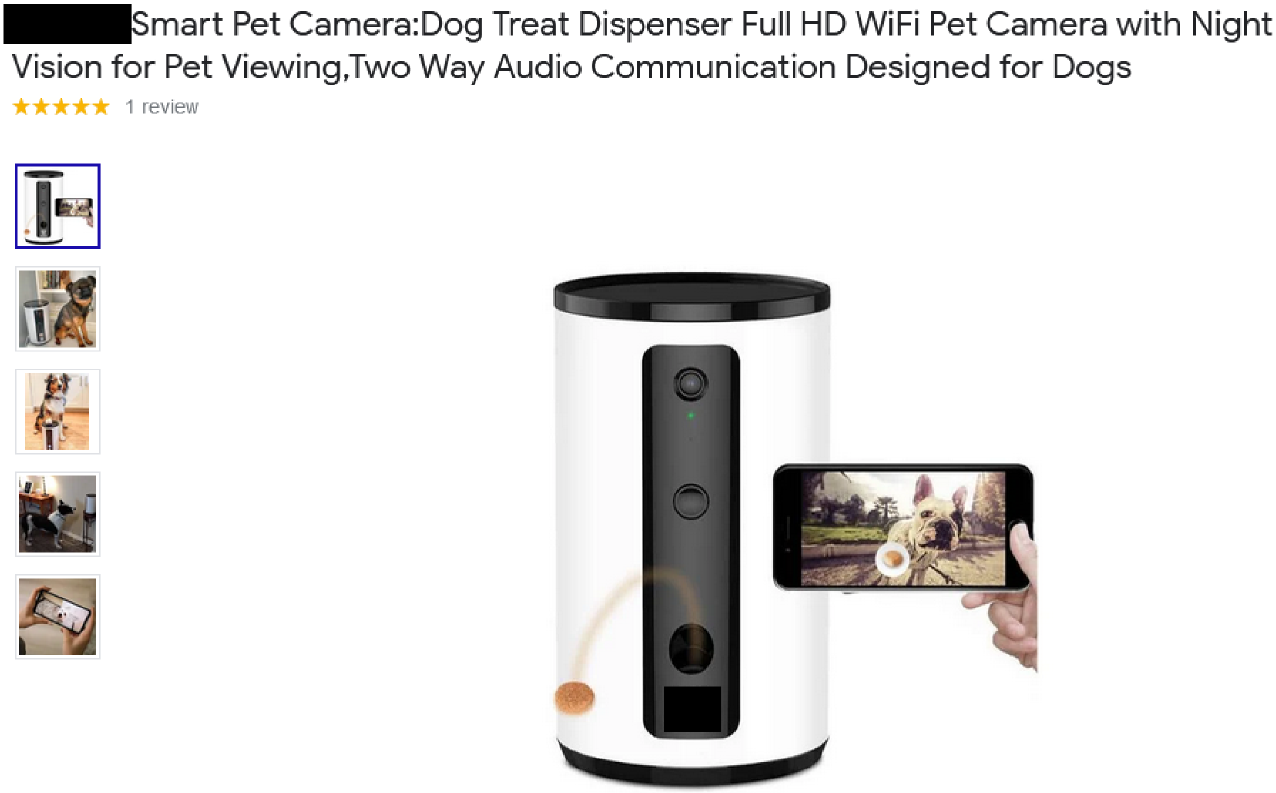
Response

Content-Type: image/jpeg



```
"ip": "82.65.[redacted]",
"country_name": "France",
"state_prov": "Ile-de-France",
"city": "Paris",
"latitude": "48.[redacted]",
"longitude": "2.[redacted]",
"time_zone": "Europe/Paris",
"isp": "Free SAS",
"currency": "Euro",
"country_flag": 🇫🇷
```

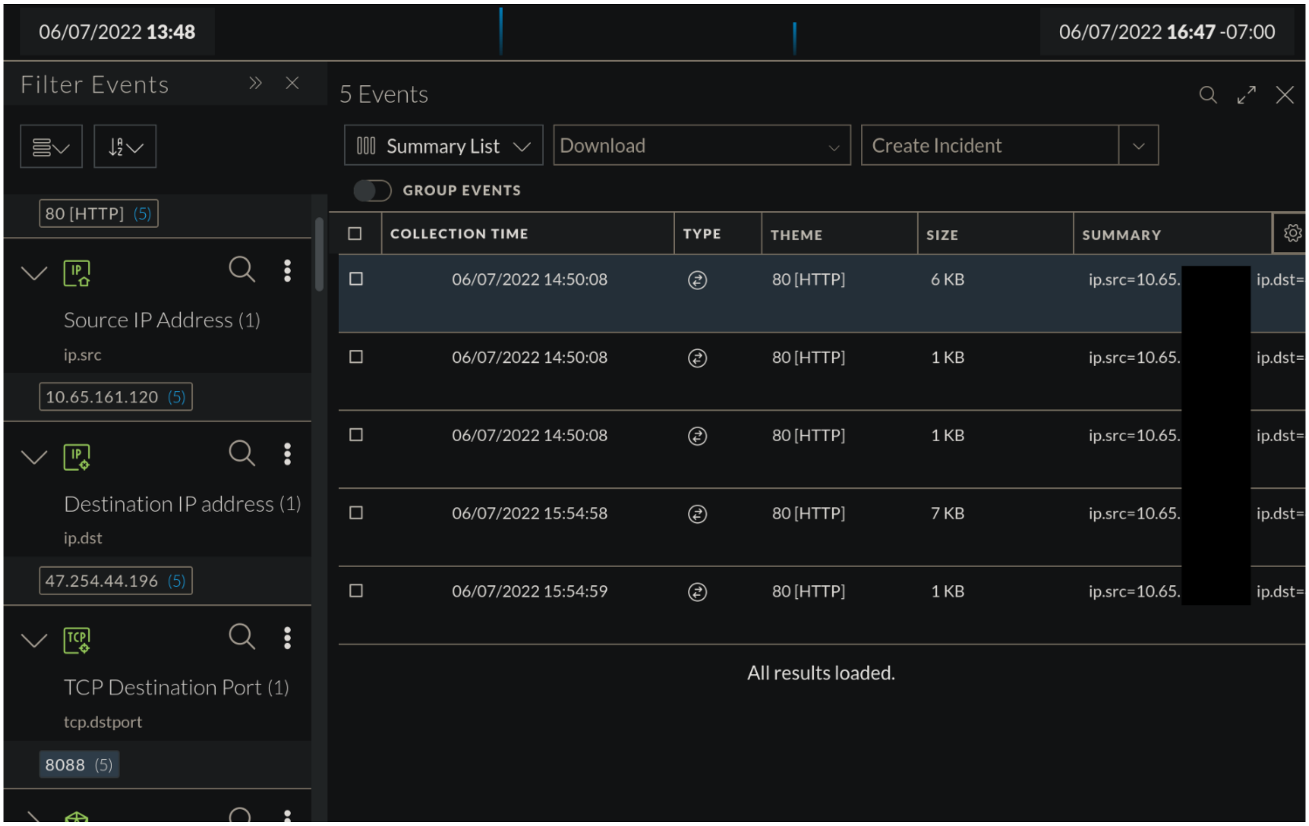
We observed a Smart Pet Camera, widely available in major online platforms and retailers, that allowed you to talk to your dog, see videos and give out treats.



[redacted] Smart Pet Camera:Dog Treat Dispenser Full HD WiFi Pet Camera with Night Vision for Pet Viewing,Two Way Audio Communication Designed for Dogs

★★★★★ 1 review

We were alerted to the traffic going over port 80.



06/07/2022 **13:48** — 06/07/2022 **16:47** -07:00

80 [HTTP] (5)

Source IP Address (1)
ip.src
10.65.161.120 (5)

Destination IP address (1)
ip.dst
47.254.44.196 (5)

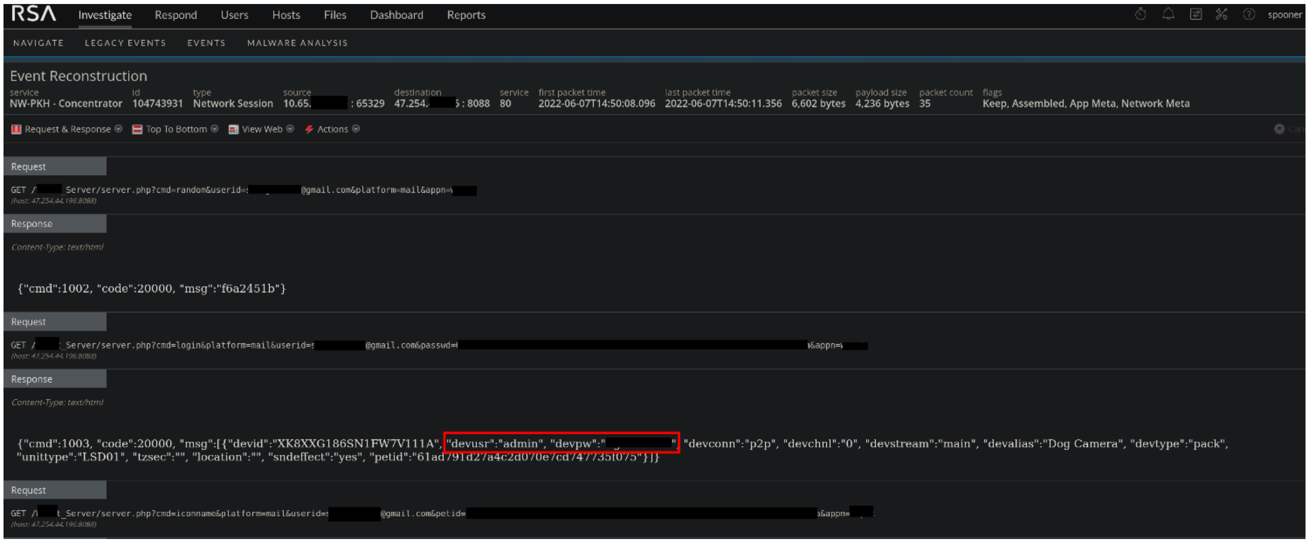
TCP Destination Port (1)
tcp.dstport
8088 (5)

5 Events

☐	COLLECTION TIME	TYPE	THEME	SIZE	SUMMARY
☐	06/07/2022 14:50:08	⇄	80 [HTTP]	6 KB	ip.src=10.65. [redacted] ip.dst=
☐	06/07/2022 14:50:08	⇄	80 [HTTP]	1 KB	ip.src=10.65. [redacted] ip.dst=
☐	06/07/2022 14:50:08	⇄	80 [HTTP]	1 KB	ip.src=10.65. [redacted] ip.dst=
☐	06/07/2022 15:54:58	⇄	80 [HTTP]	7 KB	ip.src=10.65. [redacted] ip.dst=
☐	06/07/2022 15:54:59	⇄	80 [HTTP]	1 KB	ip.src=10.65. [redacted] ip.dst=

All results loaded.

The username (full email address) was transmitted in the clear, with an encrypted password. However, the IOT device responded with the device's admin user and password in clear text.



Event Reconstruction

service	id	type	source	destination	service	first packet time	last packet time	packet size	payload size	packet count	flags
NW-PKH - Concentrator	104743931	Network Session	10.65.[redacted] : 65329	47.254.[redacted]5 : 8088	80	2022-06-07T14:50:08.096	2022-06-07T14:50:11.356	6,602 bytes	4,236 bytes	35	Keep, Assembled, App Meta, Network Meta

Request

```
GET /[redacted]_Server/server.php?cmd=random&userid=[redacted]@gmail.com&platform=mail&appn=[redacted]
(host: 47.254.44.196:8088)
```

Response

Content-Type: text/html

```
{"cmd":1002, "code":20000, "msg":"f6a2451b"}
```

Request

```
GET /[redacted]_Server/server.php?cmd=login&platform=mail&userid=[redacted]@gmail.com&passwd=[redacted]&appn=[redacted]
(host: 47.254.44.196:8088)
```

Response

Content-Type: text/html

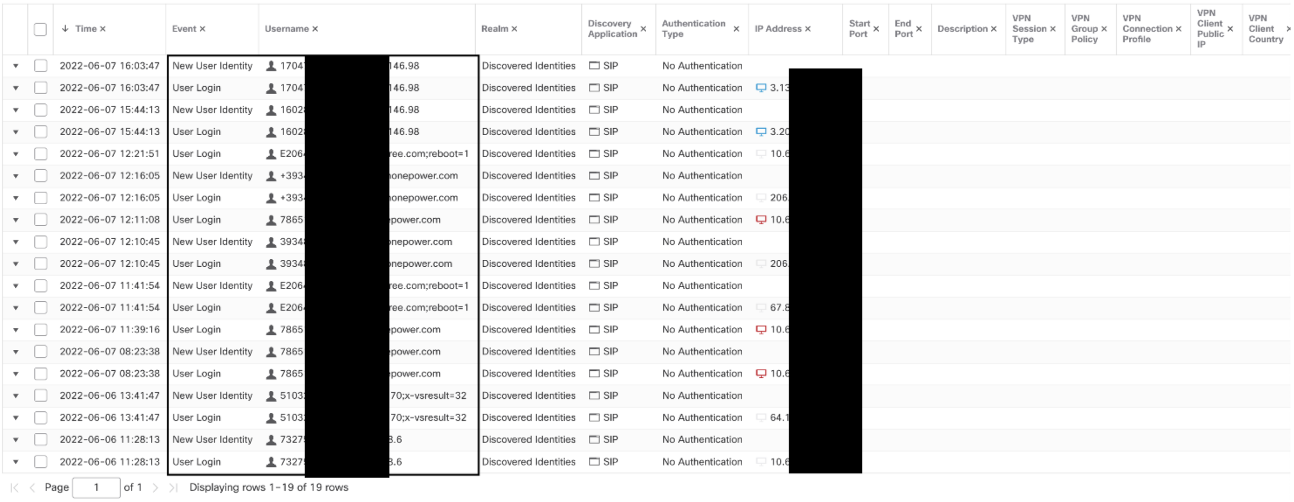
```
{"cmd":1003, "code":20000, "msg":[{"devid":"XK8XXG186SN1FW7V111A", "devusr":"admin", "devpw":"[redacted]", "devconn":"p2p", "devchnl":"0", "devstream":"main", "devalias":"Dog Camera", "devtype":"pack",
"unittype":"LSD01", "tzsec":"", "location":"", "sndeffect":"yes", "petid":"61ad791d27a4c2d070e7cd747735f075"}]}
```

Request

```
GET /[redacted]t_Server/server.php?cmd=iconname&platform=mail&userid=[redacted]@gmail.com&petid=[redacted]&appn=[redacted]
(host: 47.254.44.196:8088)
```

Voice over IP

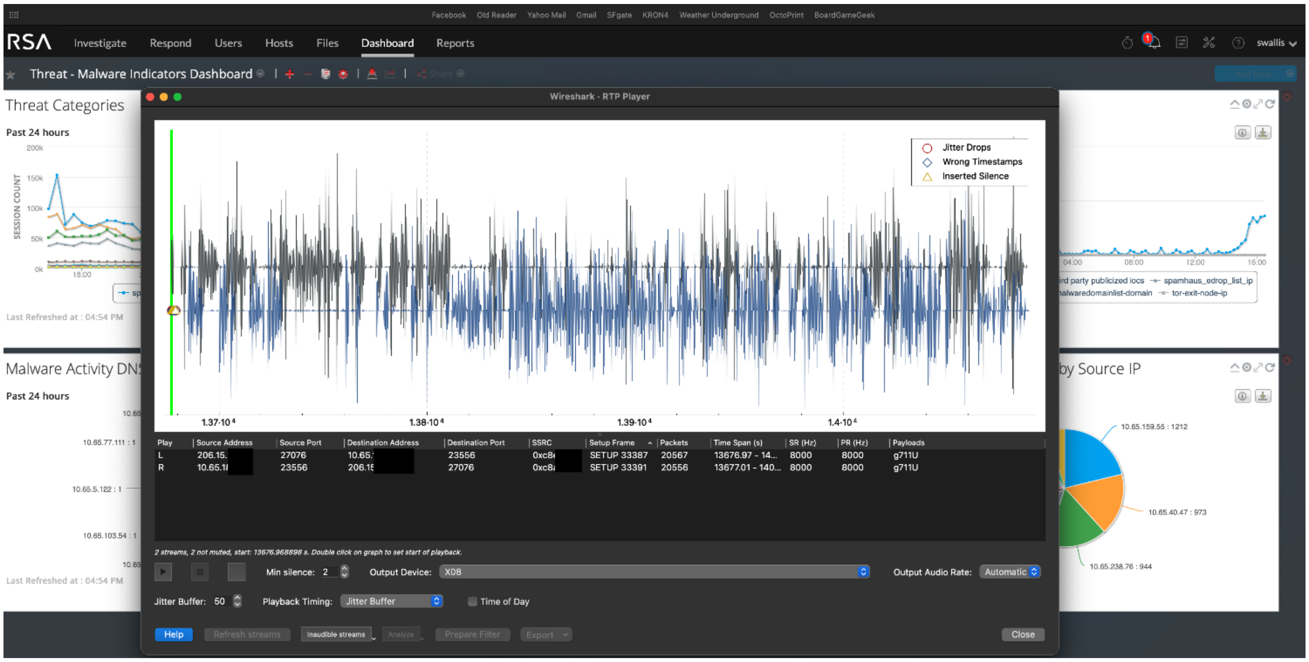
The SOC team members saw clear text Session Initiation Protocol (SIP) Control Channel (setting up audio call) under user activity in the Cisco Secure Firewall Management Center.



	☐	↓ Time ×	Event ×	Username ×	Realm ×	Discovery Application ×	Authentication Type ×	IP Address ×	Start Port ×	End Port ×	Description ×	VPN Session Type ×	VPN Group Policy ×	VPN Connection Profile ×	VPN Client Public IP ×	VPN Client Country ×
▾	☐	2022-06-07 16:03:47	New User Identity	1704[redacted]146.98	Discovered Identities	SIP	No Authentication									
▾	☐	2022-06-07 16:03:47	User Login	1704[redacted]146.98	Discovered Identities	SIP	No Authentication	3.13[redacted]								
▾	☐	2022-06-07 15:44:13	New User Identity	1602[redacted]146.98	Discovered Identities	SIP	No Authentication	[redacted]								
▾	☐	2022-06-07 15:44:13	User Login	1602[redacted]146.98	Discovered Identities	SIP	No Authentication	3.20[redacted]								
▾	☐	2022-06-07 12:21:51	User Login	E206[redacted]ree.com;reboot=1	Discovered Identities	SIP	No Authentication	10.6[redacted]								
▾	☐	2022-06-07 12:16:05	New User Identity	+393[redacted]onepower.com	Discovered Identities	SIP	No Authentication	[redacted]								
▾	☐	2022-06-07 12:16:05	User Login	+393[redacted]onepower.com	Discovered Identities	SIP	No Authentication	206[redacted]								
▾	☐	2022-06-07 12:11:08	User Login	7865[redacted]power.com	Discovered Identities	SIP	No Authentication	10.6[redacted]								
▾	☐	2022-06-07 12:10:45	New User Identity	3934[redacted]nepower.com	Discovered Identities	SIP	No Authentication	[redacted]								
▾	☐	2022-06-07 12:10:45	User Login	3934[redacted]nepower.com	Discovered Identities	SIP	No Authentication	206[redacted]								
▾	☐	2022-06-07 11:41:54	New User Identity	E206[redacted]ree.com;reboot=1	Discovered Identities	SIP	No Authentication	[redacted]								
▾	☐	2022-06-07 11:41:54	User Login	E206[redacted]ree.com;reboot=1	Discovered Identities	SIP	No Authentication	67.8[redacted]								
▾	☐	2022-06-07 11:39:16	User Login	7865[redacted]power.com	Discovered Identities	SIP	No Authentication	10.6[redacted]								
▾	☐	2022-06-07 08:23:38	New User Identity	7865[redacted]power.com	Discovered Identities	SIP	No Authentication	[redacted]								
▾	☐	2022-06-07 08:23:38	User Login	7865[redacted]power.com	Discovered Identities	SIP	No Authentication	10.6[redacted]								
▾	☐	2022-06-06 13:41:47	New User Identity	5103[redacted]70;x-vsresult=32	Discovered Identities	SIP	No Authentication	[redacted]								
▾	☐	2022-06-06 13:41:47	User Login	5103[redacted]70;x-vsresult=32	Discovered Identities	SIP	No Authentication	64.1[redacted]								
▾	☐	2022-06-06 11:28:13	New User Identity	7327[redacted]3.6	Discovered Identities	SIP	No Authentication	[redacted]								
▾	☐	2022-06-06 11:28:13	User Login	7327[redacted]3.6	Discovered Identities	SIP	No Authentication	10.6[redacted]								

Page 1 of 1 Displaying rows 1–19 of 19 rows

We could see their phone number and the connection with a SIP provider. The team correlated the time and IPs, very quickly finding the RTP/RTSP stream (Audio) using NetWitness®, decoded and was able to replay the conversations.



Play	Source Address	Source Port	Destination Address	Destination Port	SSRC	Setup Frame	Packets	Time Span (s)	SR (Hz)	PR (Hz)	Payloads
L	206.15. [redacted]	27076	10.65. [redacted]	23556	0xc8 [redacted]	SETUP 33387	20567	13676.97 - 14...	8000	8000	g711U
R	10.65.1 [redacted]	23556	206.15 [redacted]	27076	0xc8 [redacted]	SETUP 33391	20556	13677.01 - 140...	8000	8000	g711U

2 streams, 2 not muted, start: 13676.968898 s. Double click on graph to set start of playback.

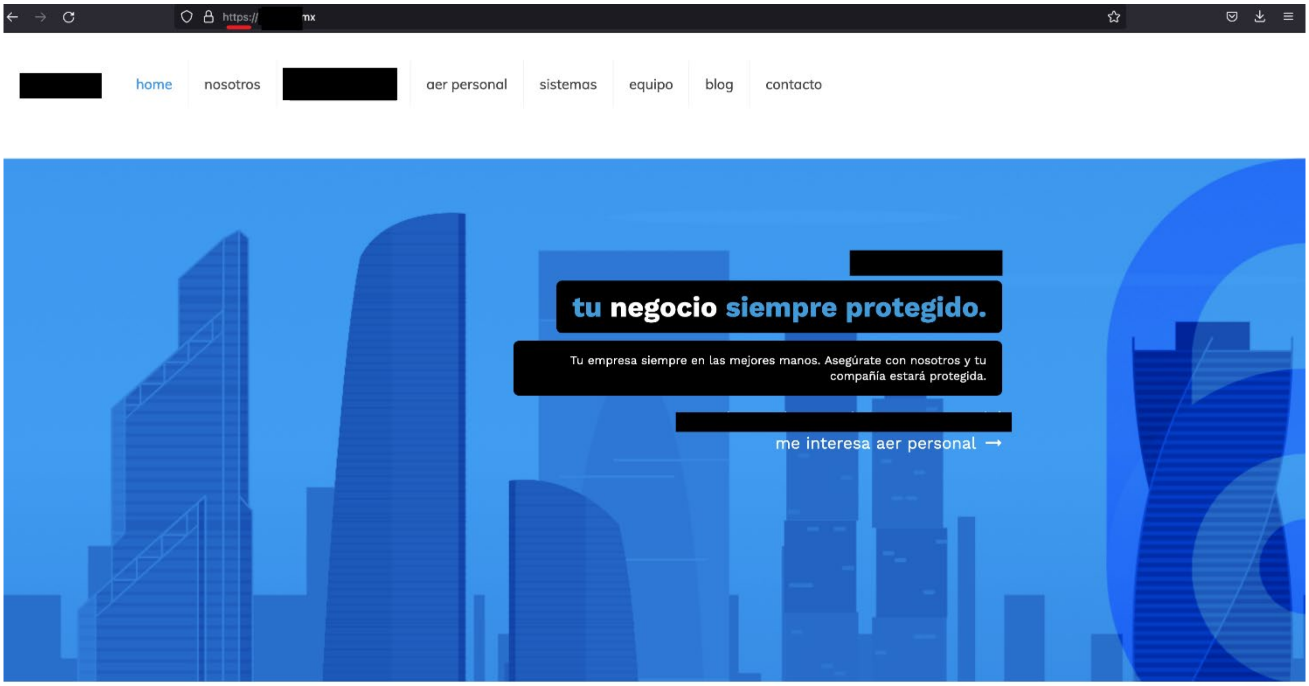
Min silence: 2 Output Device: X08 Output Audio Rate: Automatic

Jitter Buffer: 50 Playback Timing: Jitter Buffer □ Time of Day

An excerpt: [00: 05: 10.250] - Speaker 1 – “Tomorrow morning we fly, say at 14:15 to 21:00.”

HTTPS -> HTTP

We are trained as security professionals to look for the HTTPS:// in the browser bar, especially when working with private information like our health care and that of our family.



https:// [redacted] mx

[redacted] home nosotros [redacted] aer personal sistemas equipo blog contacto

[redacted]

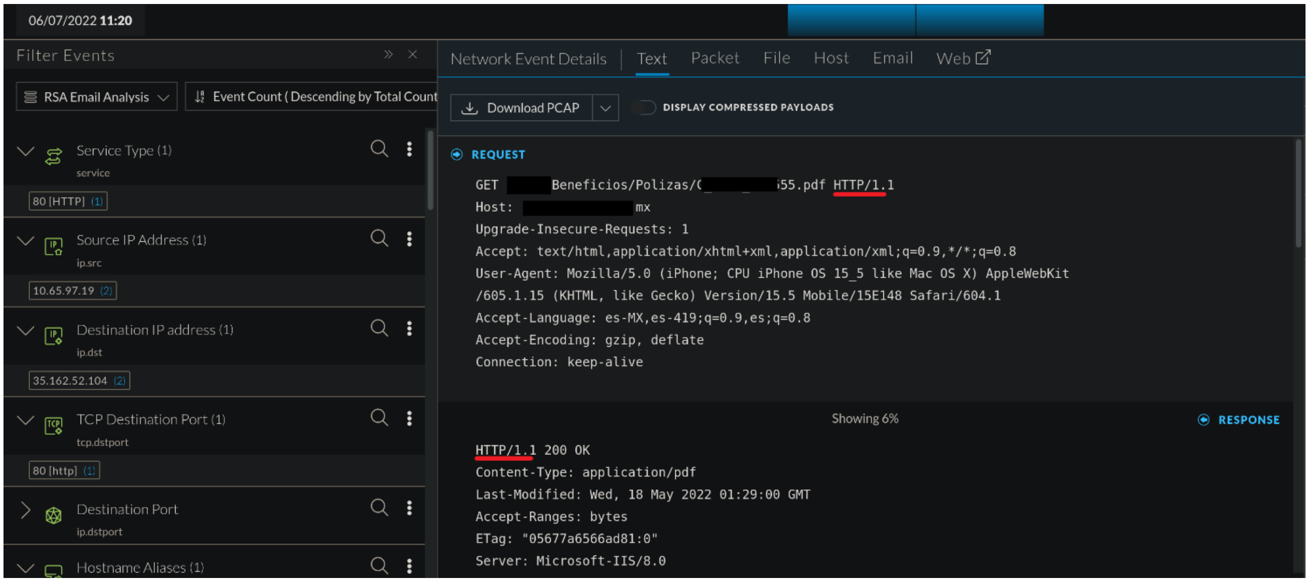
tu negocio siempre protegido.

Tu empresa siempre en las mejores manos. Asegúrate con nosotros y tu compañía estará protegida.

[redacted]

me interesa aer personal ⟶

Unfortunately, misconfigured security implementations will sometimes flip over to insecure HTTP, without warning or the user realizing. We observed a PDF downloaded to an iPhone over in secure HTTP 1.1 protocol.



Service Type (1)
service
80 [HTTP] (1)

Source IP Address (1)
ip.src
10.65.97.19 (2)

Destination IP address (1)
ip.dst
35.162.52.104 (2)

TCP Destination Port (1)
tcp.dstport
80 [http] (1)

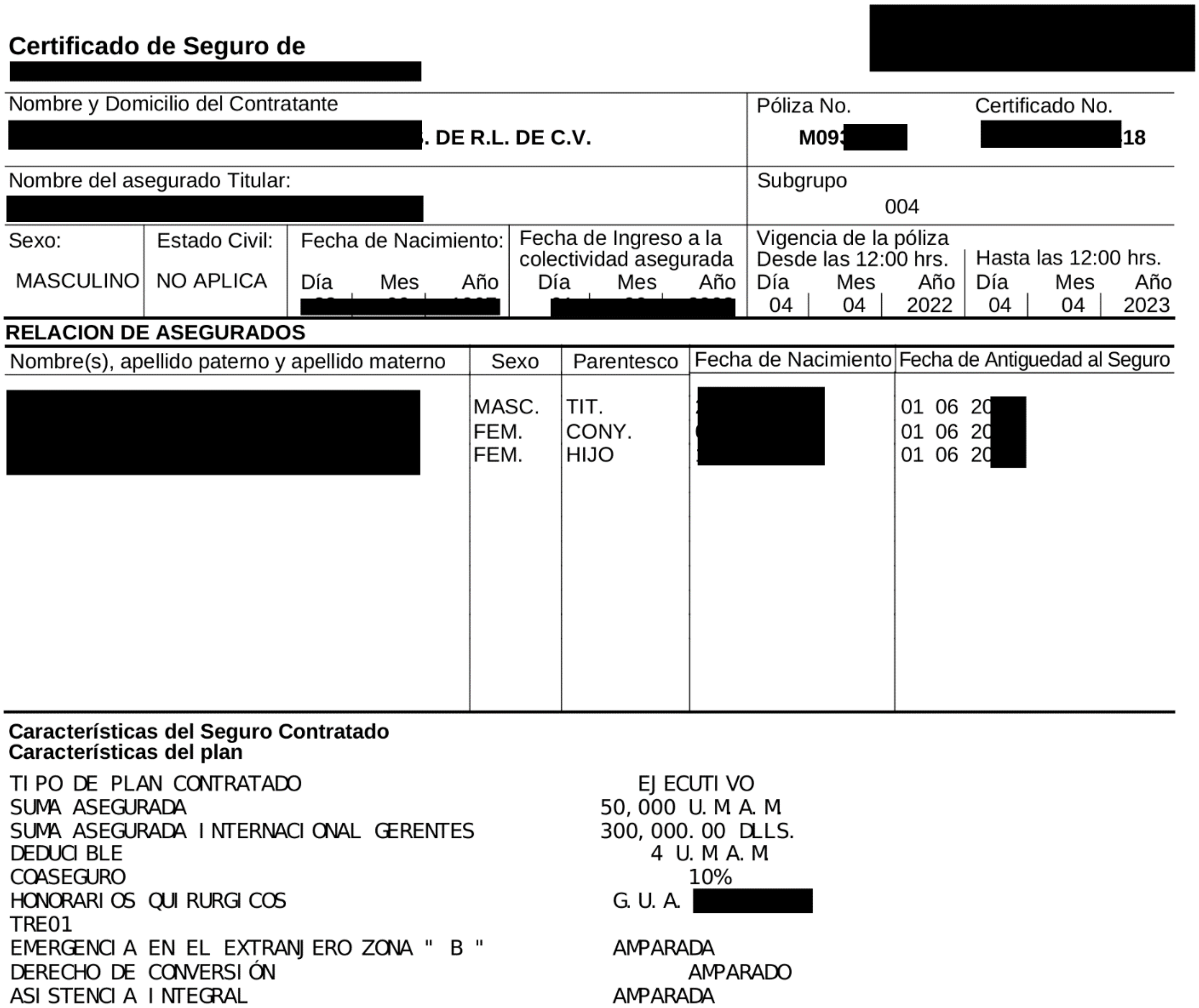
Destination Port
ip.dstport

Hostname Aliases (1)

```
GET [redacted]Beneficios/Polizas/[redacted]55.pdf HTTP/1.1
Host: [redacted]mx
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 15_5 like Mac OS X) AppleWebKit
/605.1.15 (KHTML, like Gecko) Version/15.5 Mobile/15E148 Safari/604.1
Accept-Language: es-MX,es-419;q=0.9,es;q=0.8
Accept-Encoding: gzip, deflate
Connection: keep-alive
```

```
HTTP/1.1 200 OK
Content-Type: application/pdf
Last-Modified: Wed, 18 May 2022 01:29:00 GMT
Accept-Ranges: bytes
ETag: "05677a6566ad81:0"
Server: Microsoft-IIS/8.0
```

The PDF was a certificate of insurance from a major medical insurance company, and contained the personal information of an entire family.



Certificado de Seguro de

[redacted]

[redacted]

Nombre y Domicilio del Contratante	Póliza No.	Certificado No.
[redacted]. DE R.L. DE C.V.	M09[redacted]	[redacted]18

Nombre del asegurado Titular:	Subgrupo
[redacted]	004

Sexo:	Estado Civil:	Fecha de Nacimiento:			Fecha de Ingreso a la colectividad asegurada			Vigencia de la póliza Desde las 12:00 hrs.			Hasta las 12:00 hrs.		
		Día	Mes	Año	Día	Mes	Año	Día	Mes	Año	Día	Mes	Año
MASCULINO	NO APLICA	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	04	04	2022	04	04	2023

RELACION DE ASEGURADOS

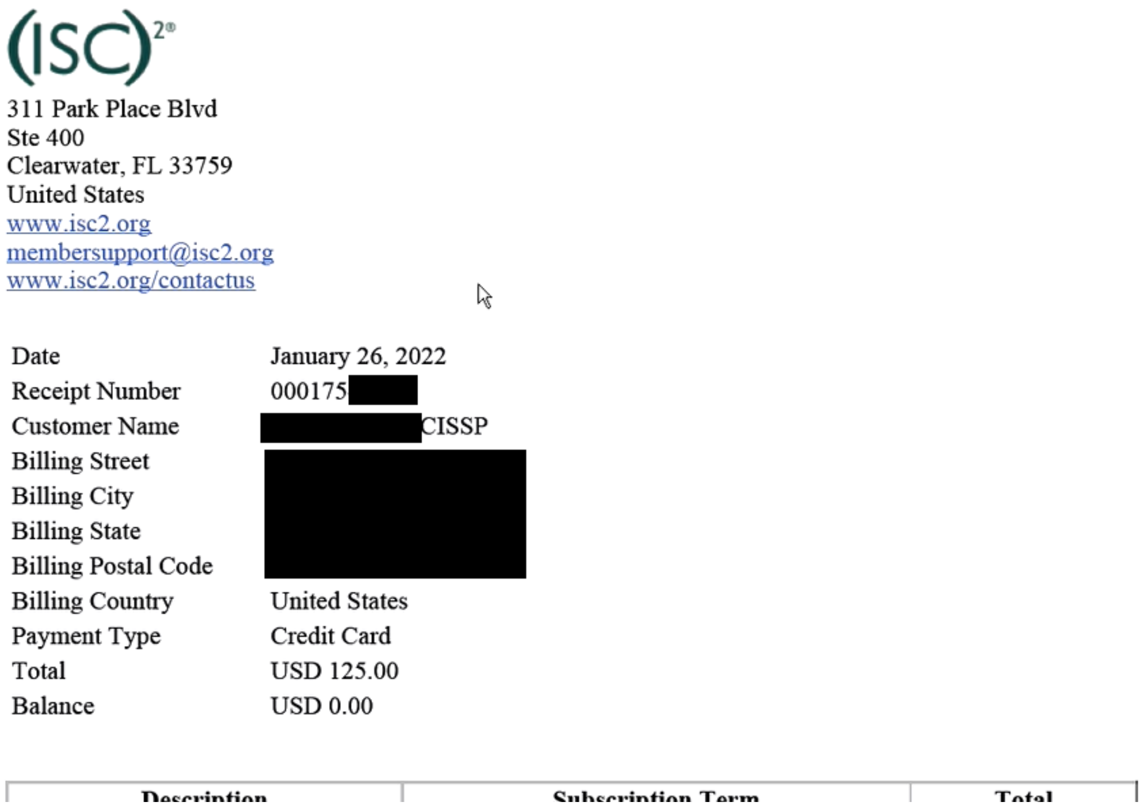
Nombre(s), apellido paterno y apellido materno	Sexo	Parentesco	Fecha de Nacimiento	Fecha de Antiguedad al Seguro
[redacted]	MASC.	TIT.	[redacted]	01 06 20[redacted]
	FEM.	CONY.	[redacted]	01 06 20[redacted]
	FEM.	HIJO	[redacted]	01 06 20[redacted]

Características del Seguro Contratado
Características del plan

TIPO DE PLAN CONTRATADO	EJECUTIVO
SUMA ASEGURADA	50,000 U.M.A.M
SUMA ASEGURADA INTERNACIONAL GERENTES	300,000.00 DLLS.
DEDUCIBLE	4 U.M.A.M
COASEGURO	10%
HONORARIOS QUIRURGICOS	G.U.A. [redacted]
TRE01	
EMERGENCIA EN EL EXTRANJERO ZONA " B "	AMPARADA
DERECHO DE CONVERSIÓN	AMPARADO
ASISTENCIA INTEGRAL	AMPARADA

POP3 – Chewing threw email

While reviewing submitted samples in Cisco Secure Malware Analytics observed a `Receipt.PDF` submitted for analysis. The name was enough to warrant a look at the video of the detonation. It was a receipt for renewal of a CISSP designation.



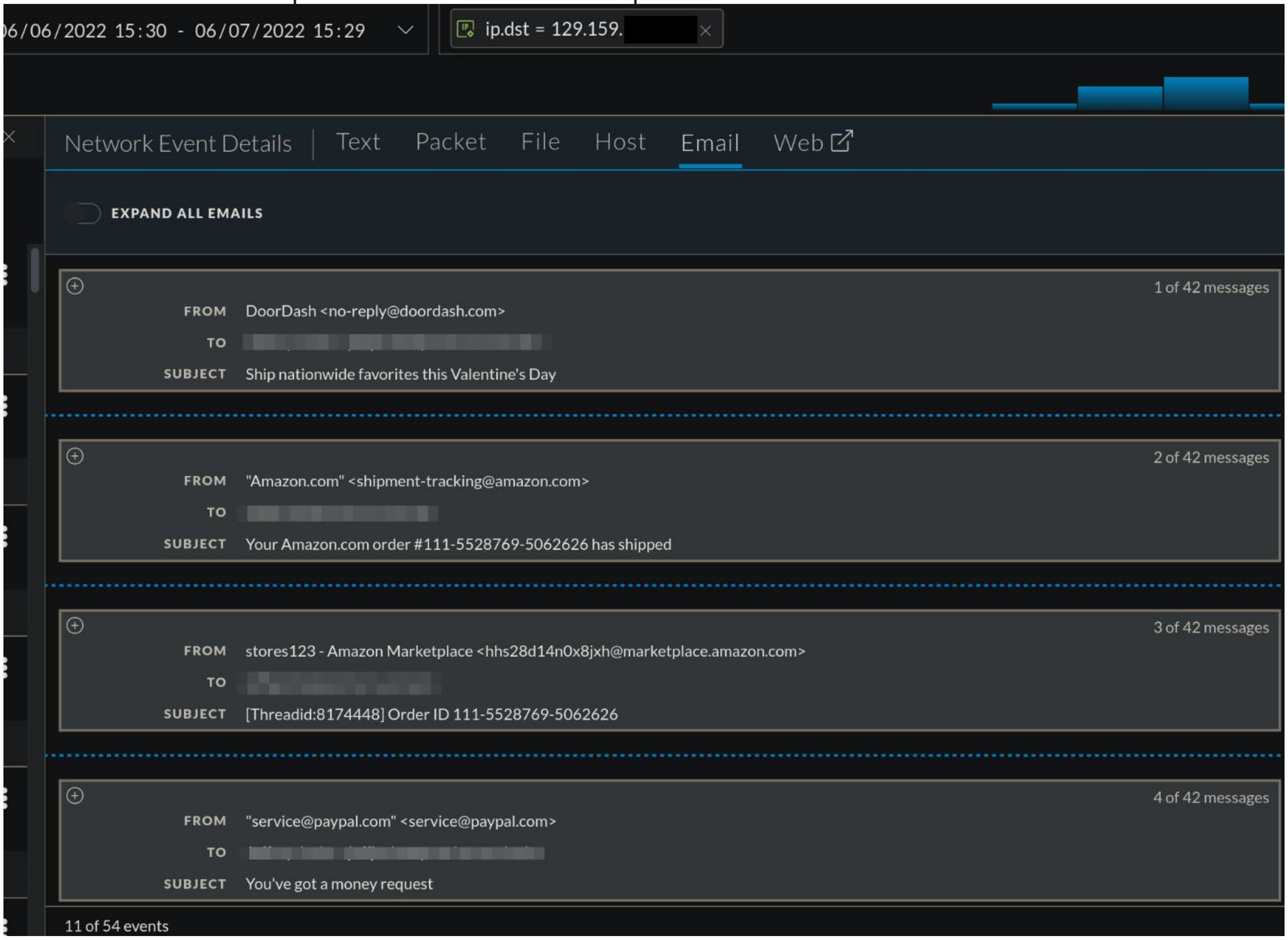
(ISC)²®

311 Park Place Blvd
Ste 400
Clearwater, FL 33759
United States
www.isc2.org
membersupport@isc2.org
www.isc2.org/contactus

Date	January 26, 2022
Receipt Number	000175[redacted]
Customer Name	[redacted]CISSP
Billing Street	[redacted]
Billing City	[redacted]
Billing State	[redacted]
Billing Postal Code	[redacted]
Billing Country	United States
Payment Type	Credit Card
Total	USD 125.00
Balance	USD 0.00

Description	Subscription Term	Total

The discovery sparked an investigation that confirmed dozens of emails from and to the person were downloaded across the open network in the unsecure protocol.



6/06/2022 15:30 - 06/07/2022 15:29

ip.dst = 129.159.[redacted]

1 of 42 messages

FROM DoorDash <no-reply@doordash.com>

TO [redacted]

SUBJECT Ship nationwide favorites this Valentine's Day

2 of 42 messages

FROM "Amazon.com" <shipment-tracking@amazon.com>

TO [redacted]

SUBJECT Your Amazon.com order #111-5528769-5062626 has shipped

3 of 42 messages

FROM stores123 - Amazon Marketplace <hhs28d14n0x8jxh@marketplace.amazon.com>

TO [redacted]

SUBJECT [Threadid:8174448] Order ID 111-5528769-5062626

4 of 42 messages

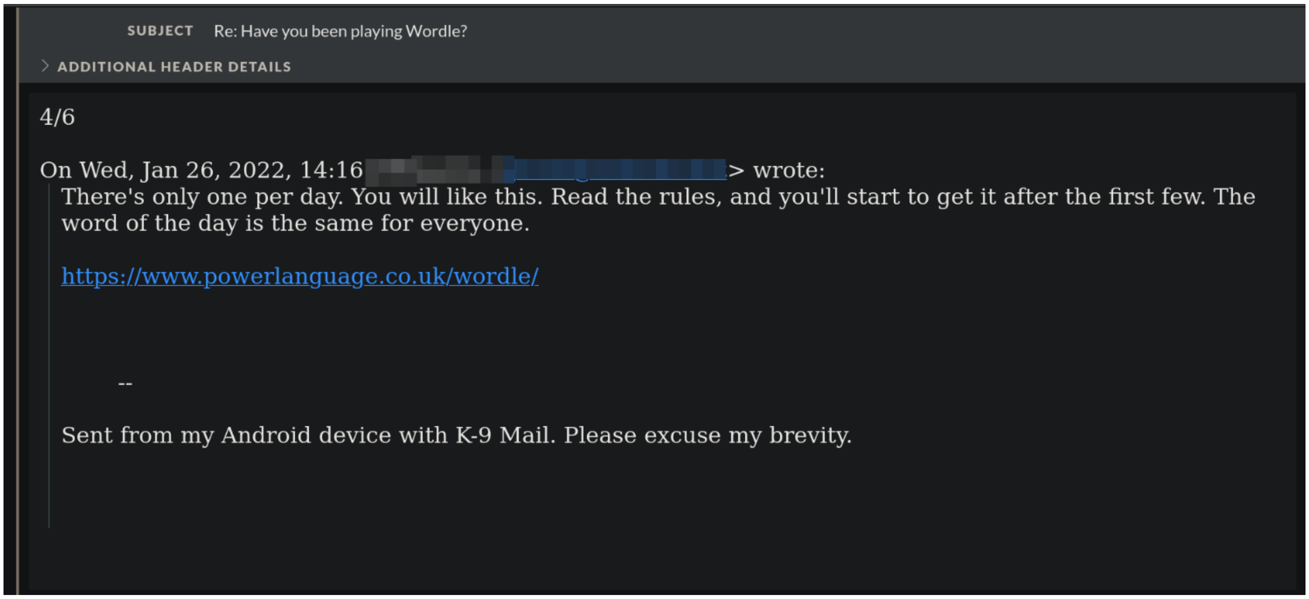
FROM "service@paypal.com" <service@paypal.com>

TO [redacted]

SUBJECT You've got a money request

11 of 54 events

A quick internet search revealed the person was a Chief Information Officer at a public corporation. One email alerted the SOC team to the email client in use: K-9, an Android based, open source email client, to help users "chew threw their email…"



SUBJECT Re: Have you been playing Wordle?

4/6

On Wed, Jan 26, 2022, 14:16 [redacted]> wrote:

There's only one per day. You will like this. Read the rules, and you'll start to get it after the first few. The word of the day is the same for everyone.

https://www.powerlanguage.co.uk/wordle/

--

Sent from my Android device with K-9 Mail. Please excuse my brevity.

Among the attachments were documents that contained the cell phone number of the person. It appeared the issue was likely a configuration problem with the email client, rather than a security flaw. The SOC lead for NetWitness® called the person on the phone, leaving a detailed message. The next day, after the 10:30am SOC tour, the person knocked on the SOC door and identified themselves as receiving the voice mail.

The SOC team showed the person the emails and attachments, and then walked them through the configuration settings for both send and receive. It was observed that the "TLS" setting was unchecked for both send and receive. Transport Layer Security (TLS) is an encryption protocol that protects Internet communications and replaced Secure Socket Layer (SSL) in 1999.

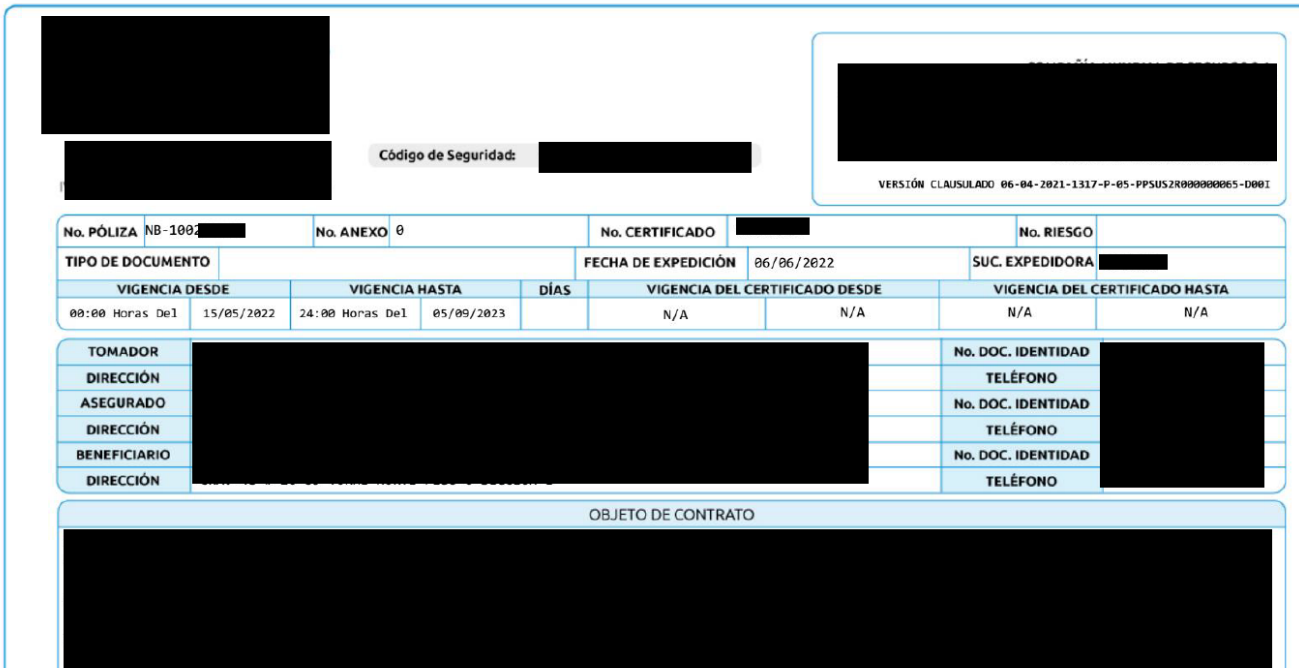
After the setting was enabled, the person confirmed they could both send and receive email. The SOC also confirmed that the emails were now encrypted and not able to be read/downloaded on the open network.

Spear Phishing Bait

In the SOC, we saw a lot of personal identifying information and business documents that could be used to craft a spear phishing campaign.

The US Department of Defense defines a spear phishing attack "...as an attempt to acquire sensitive information or access to a computer system by sending counterfeit messages that appear to be legitimate. 'Spear phishing' is a type of phishing campaign that targets a specific person or group and often will include information known to be of interest to the target, such as current events or financial documents. Like other social engineering attacks, spear phishing takes advantage of our most basic human traits, such as a desire to be helpful, provide a positive response to those in authority, a desire to respond positively to someone who shares similar tastes or views, or simple curiosity about contemporary news and events. These messages are delivered via e-mail and are designed to convince the user to open a malicious link or attachment, exposing the target to malicious software." Source:
https://www.dni.gov/files/NCSC/documents/campaign/Counterintelligence_Tips_Spearphishing.pdf

In one example, the private intranet share for a corporation was accessed and accessible over the internet. Non-disclosure agreement, contracts and business communications were all available in the clear.



[redacted]

[redacted]

Código de Seguridad: [redacted]

[redacted]

VERSIÓN CLAUSULADO 06-04-2021-1317-P-05-PPSUS2R000000065-D00I

No. PÓLIZA	NB-1002[redacted]	No. ANEXO	0	No. CERTIFICADO	[redacted]	No. RIESGO	
TIPO DE DOCUMENTO				FECHA DE EXPEDICIÓN	06/06/2022	SUC. EXPEDIDORA	[redacted]

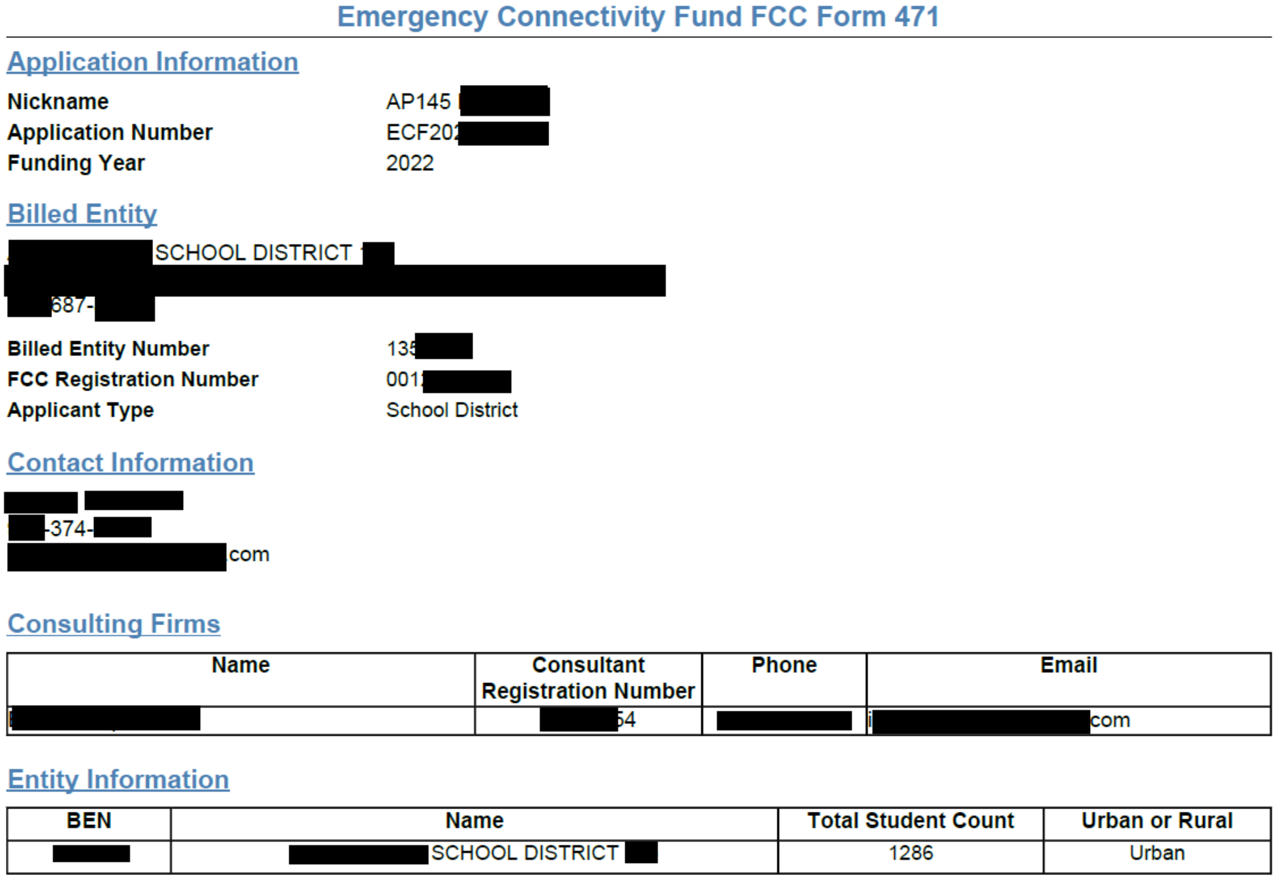
VIGENCIA DESDE		VIGENCIA HASTA		DÍAS	VIGENCIA DEL CERTIFICADO DESDE		VIGENCIA DEL CERTIFICADO HASTA	
00:00 Horas Del	15/05/2022	24:00 Horas Del	05/09/2023		N/A	N/A	N/A	N/A

TOMADOR	[redacted]	No. DOC. IDENTIDAD	[redacted]
DIRECCIÓN	[redacted]	TELÉFONO	[redacted]
ASEGURADO	[redacted]	No. DOC. IDENTIDAD	[redacted]
DIRECCIÓN	[redacted]	TELÉFONO	[redacted]
BENEFICIARIO	[redacted]	No. DOC. IDENTIDAD	[redacted]
DIRECCIÓN	[redacted]	TELÉFONO	[redacted]

OBJETO DE CONTRATO

[redacted]

We also saw other contracts and official documents, for example a funding request and information for computer equipment procurement for a school district.



Emergency Connectivity Fund FCC Form 471

Application Information

Nickname	AP145 [redacted]
Application Number	ECF20[redacted]
Funding Year	2022

Billed Entity

[redacted]SCHOOL DISTRICT [redacted]
[redacted]
[redacted]687-[redacted]

Billed Entity Number	135[redacted]
FCC Registration Number	001[redacted]
Applicant Type	School District

Contact Information

[redacted] [redacted]
[redacted]-374-[redacted]
[redacted]com

Consulting Firms

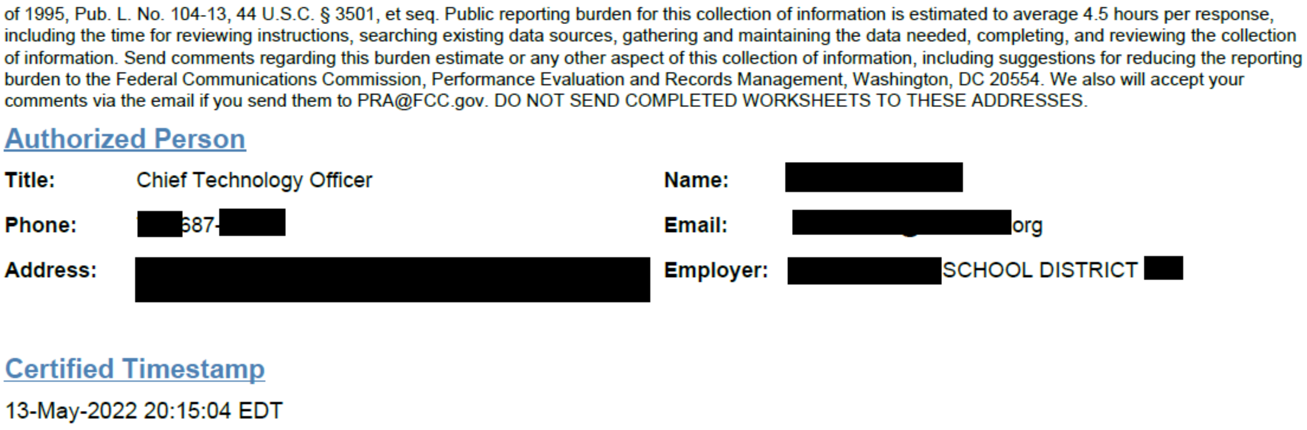
Name	Consultant Registration Number	Phone	Email
[redacted]	[redacted]54	[redacted]	i[redacted]com

Entity Information

BEN	Name	Total Student Count	Urban or Rural
[redacted]	[redacted]SCHOOL DISTRICT [redacted]	1286	Urban

The document was downloaded with a GET request from an S3 bucket.

If contained all the information needed to mount a spear phishing campaign against the school district.



of 1995, Pub. L. No. 104-13, 44 U.S.C. § 3501, et seq. Public reporting burden for this collection of information is estimated to average 4.5 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, completing, and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the reporting burden to the Federal Communications Commission, Performance Evaluation and Records Management, Washington, DC 20554. We also will accept your comments via the email if you send them to PRA@FCC.gov. DO NOT SEND COMPLETED WORKSHEETS TO THESE ADDRESSES.

Authorized Person

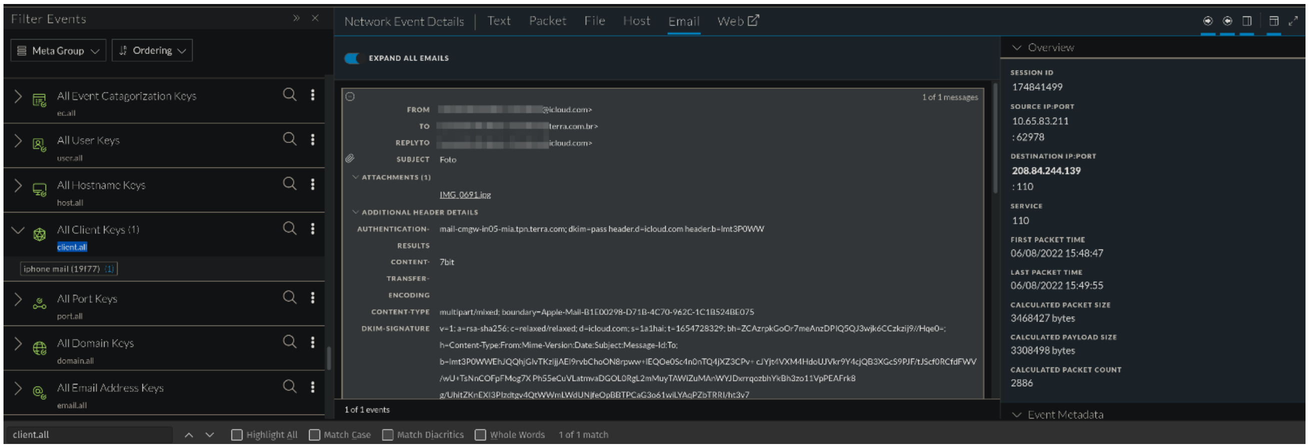
Title:	Chief Technology Officer	**Name:**	[redacted]
Phone:	[redacted]687-[redacted]	**Email:**	[redacted]org
Address:	[redacted]	**Employer:**	[redacted]SCHOOL DISTRICT [redacted]

Certified Timestamp

13-May-2022 20:15:04 EDT

How do you make iPhone email unsecure?

One thing that really stumped us in the SOC, was the observation of an emailed photo from an iPhone.



FROM [redacted]@icloud.com>
TO [redacted]terra.com.br>
REPLYTO [redacted]icloud.com>
SUBJECT Foto
ATTACHMENTS (1)
IMG_0691.jpg
ADDITIONAL HEADER DETAILS
AUTHENTICATION-RESULTS mail-cmgw-in05-mia.tpn.terra.com; dkim=pass header.d=icloud.com header.b=Imt3P0WW
CONTENT-TRANSFER-ENCODING 7bit
CONTENT-TYPE multipart/mixed; boundary=Apple-Mail-B1E00298-D71B-4C70-962C-1C1B524BE075
DKIM-SIGNATURE v=1; a=rsa-sha256; c=relaxed/relaxed; d=icloud.com; s=1a1hai; t=1654728329; bh=ZCAzrpkGoOr7meAnzDPIQ5QJ3wjk6CCzkzij9//Hqe0=;
h=Content-Type:From:Mime-Version:Date:Subject:Message-Id:To;
b=Imt3P0WWEhJQQhjGlvTKzIjjAEI9rvbChoON8rpww+IEQOe0Sc4n0nTQ4jXZ3CPv+ cJYjt4VXM4HdoUJVkr9Y4cjQB3XGcS9PJF/tJScf0RCfdFWV
/wU+TsNnCOFpFMog7X Ph55eCuVLatmvaDGOL0RgL2mMuyTAWlZuMAnWYJDxrrqozbhYkBh3zo11VpPEAFrk8
g/UhltZKnEXl3PIzdtgv4QtWWmLWdUNjfeOpBBTPCaG3o61wlLYAqPZbTRRI/ht3v7

SESSION ID
174841499
SOURCE IP:PORT
10.65.83.211
: 62978
DESTINATION IP:PORT
208.84.244.139
: 110
SERVICE
110
FIRST PACKET TIME
06/08/2022 15:48:47
LAST PACKET TIME
06/08/2022 15:49:55
CALCULATED PACKET SIZE
3468427 bytes
CALCULATED PAYLOAD SIZE
3308498 bytes
CALCULATED PACKET COUNT
2886

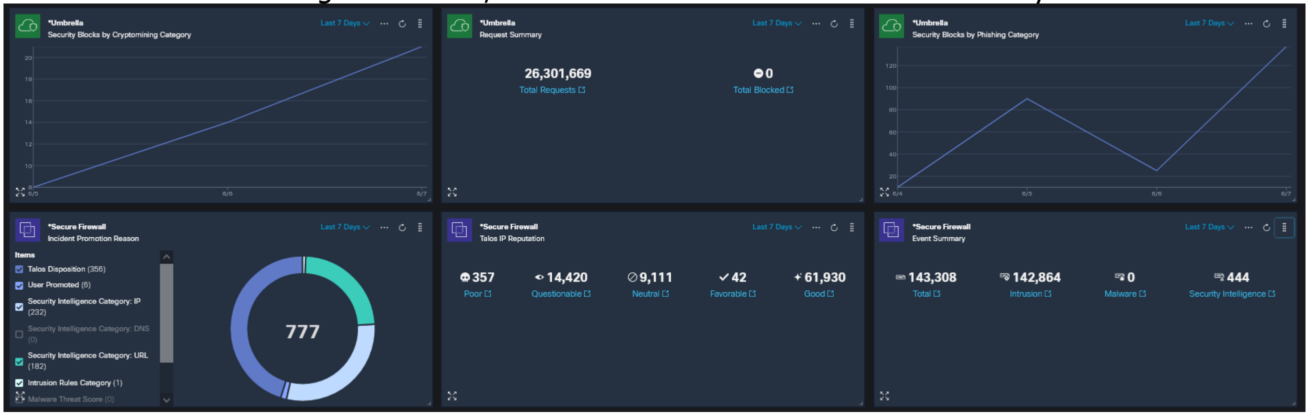
Perhaps the iOS was out of date? We could not find another scenario where an iPhone could be set to send an email in an unsecure protocol. What you do think?

Booth Blues

The RSAC SOC Team discovered several Internet Protocol Televisions (IPTV) that were joined to the RSACONFERENCE network. Some organizations are overlooking many security issues that could have an adverse impact on the ability to execute.

INTEGRATION AND THREAT HUNTING

Cisco SecureX XDR brought Umbrella, Secure Firewall and Secure Malware Analytics.



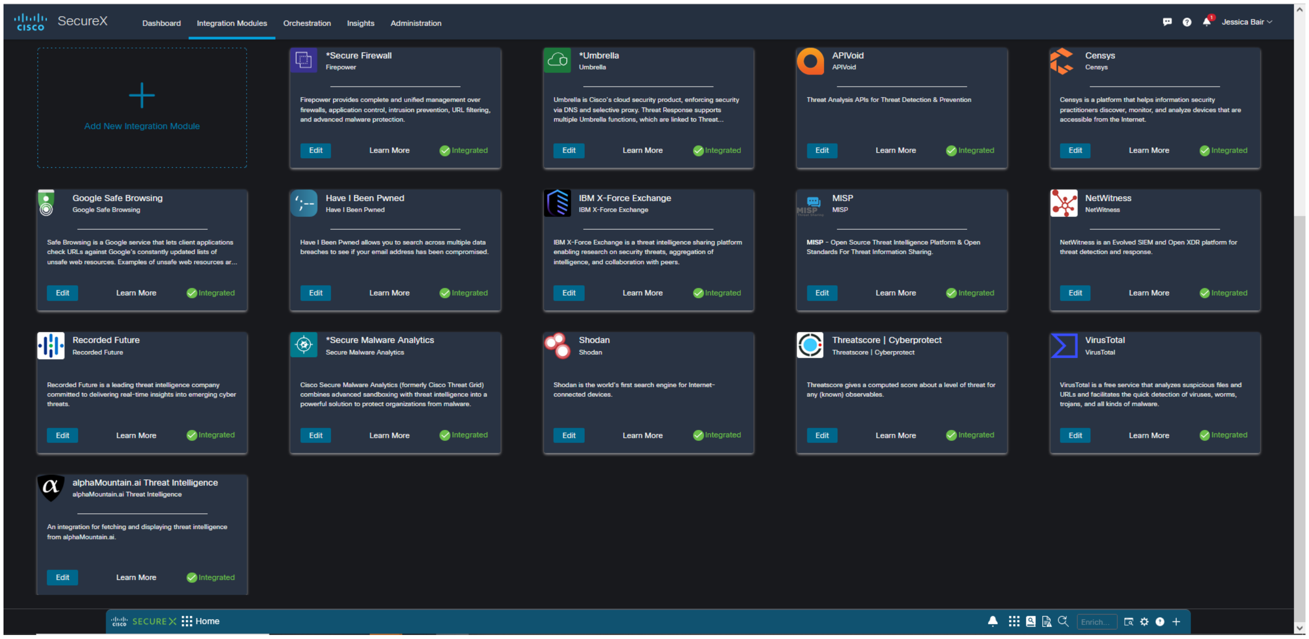
To aid in Threat Hunting, we added threat intelligence from several sources.

Cisco Secure Threat Intelligence

- SecureX threat intelligence
- Cisco Secure Endpoint's File Reputation Database
- Cisco Talos Intelligence

Donated Partner Threat Intelligence

- Recorded Future threat intelligence
- alphaMountain.ai threat intelligence



*Secure Firewall
Firepower
Firepower provides complete and unified management over firewalls, application control, intrusion prevention, URL filtering, and advanced malware protection.

*Umbrella
Umbrella
Umbrella is Cisco's cloud security product, enforcing security via DNS and selective proxy. Threat Response supports multiple Umbrella functions, which are linked to Threat...

APIVoid
APIVoid
Threat Analysis APIs for Threat Detection & Prevention

Censys
Censys
Censys is a platform that helps information security practitioners discover, monitor, and analyze devices that are accessible from the Internet.

Google Safe Browsing
Google Safe Browsing
Safe Browsing is a Google service that lets client applications check URLs against Google's constantly updated lists of unsafe web resources. Examples of unsafe web resources ar...

Have I Been Pwned
Have I Been Pwned
Have I Been Pwned allows you to search across multiple data breaches to see if your email address has been compromised.

IBM X-Force Exchange
IBM X-Force Exchange
IBM X-Force Exchange is a threat intelligence sharing platform enabling research on security threats, aggregation of intelligence, and collaboration with peers.

MISP
MISP
MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing.

NetWitness
NetWitness
NetWitness is an Evolved SIEM and Open XDR platform for threat detection and response.

Recorded Future
Recorded Future
Recorded Future is a leading threat intelligence company committed to delivering real-time insights into emerging cyber threats.

*Secure Malware Analytics
Secure Malware Analytics
Cisco Secure Malware Analytics (formerly Cisco Threat Grid) combines advanced sandboxing with threat intelligence into a powerful solution to protect organizations from malware.

Shodan
Shodan
Shodan is the world's first search engine for Internet-connected devices.

Threatscore | Cyberprotect
Threatscore | Cyberprotect
Threatscore gives a computed score about a level of threat for any (known) observables.

VirusTotal
VirusTotal
VirusTotal is a free service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

alphaMountain.ai Threat Intelligence
alphaMountain.ai Threat Intelligence
An integration for fetching and displaying threat intelligence from alphaMountain.ai.

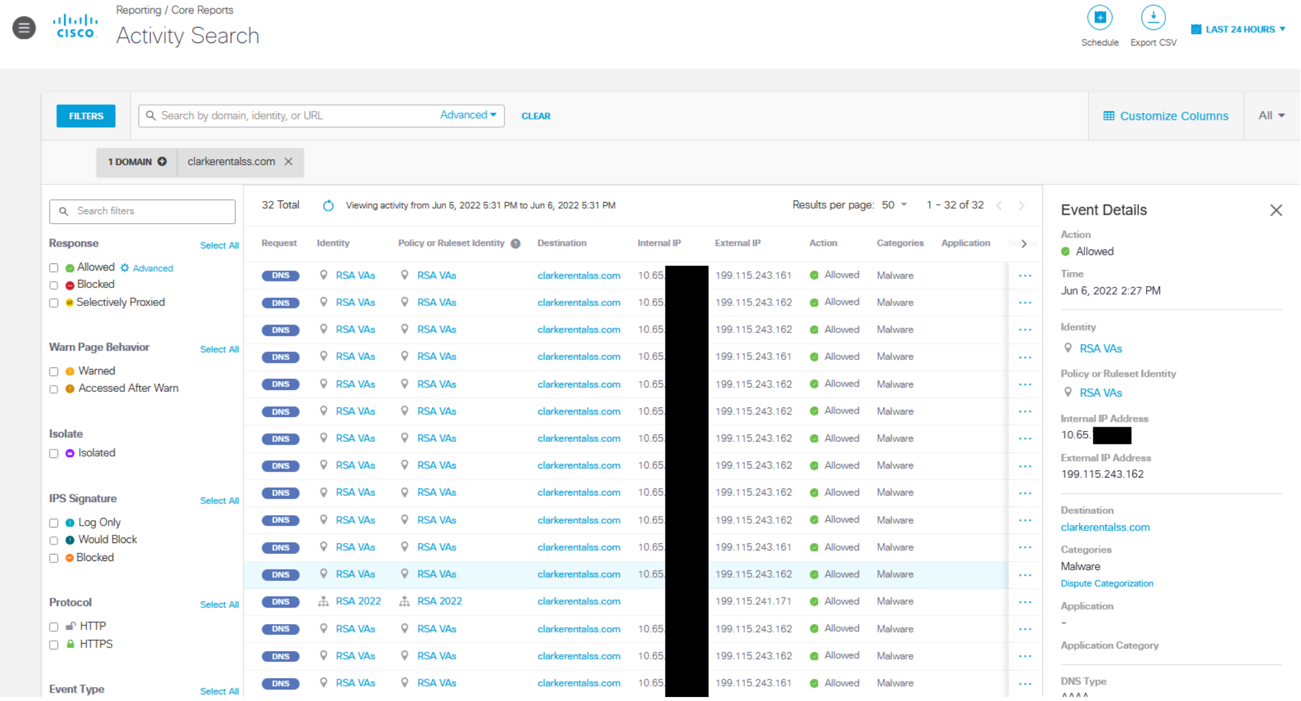
Open-Source Threat Intelligence (correlated through SecureX)

- APIVoid
- Censys
- Google Safe Browsing
- Have I Been Pwned

- IBM X-Force Exchange
- MISP
- Threatscore | Cyberprotect
- VirusTotal

We also built a custom integration with NetWitness® Logs to visualize Sightings during investigations.

The SOC team had an alert about a Domain hosting a trickbot malware in Umbrella.



Reporting / Core Reports

Activity Search

Schedule | Export CSV | LAST 24 HOURS ▾

FILTERS | Search by domain, identity, or URL | Advanced ▾ | CLEAR | Customize Columns | All ▾

1 DOMAIN ⊕ | clarkerentalss.com ✕

Search filters

Response (Select All)
□ Allowed (Advanced)
□ Blocked
□ Selectively Proxied

Warn Page Behavior (Select All)
□ Warned
□ Accessed After Warn

Isolate
□ Isolated

IPS Signature (Select All)
□ Log Only
□ Would Block
□ Blocked

Protocol (Select All)
□ HTTP
□ HTTPS

Event Type (Select All)

32 Total | Viewing activity from Jun 5, 2022 5:31 PM to Jun 6, 2022 5:31 PM | Results per page: 50 ▾ | 1 - 32 of 32

Request	Identity	Policy or Ruleset Identity	Destination	Internal IP	External IP	Action	Categories	Application
DNS	RSA VAs	RSA VAs	clarkerentalss.com	10.65.[redacted]	199.115.243.161	Allowed	Malware	
DNS	RSA VAs	RSA VAs	clarkerentalss.com	10.65.[redacted]	199.115.243.162	Allowed	Malware	
DNS	RSA VAs	RSA VAs	clarkerentalss.com	10.65.[redacted]	199.115.243.162	Allowed	Malware	
DNS	RSA VAs	RSA VAs	clarkerentalss.com	10.65.[redacted]	199.115.243.161	Allowed	Malware	
DNS	RSA VAs	RSA VAs	clarkerentalss.com	10.65.[redacted]	199.115.243.162	Allowed	Malware	
DNS	RSA VAs	RSA VAs	clarkerentalss.com	10.65.[redacted]	199.115.243.162	Allowed	Malware	
DNS	RSA VAs	RSA VAs	clarkerentalss.com	10.65.[redacted]	199.115.243.162	Allowed	Malware	
DNS	RSA VAs	RSA VAs	clarkerentalss.com	10.65.[redacted]	199.115.243.162	Allowed	Malware	
DNS	RSA VAs	RSA VAs	clarkerentalss.com	10.65.[redacted]	199.115.243.162	Allowed	Malware	
DNS	RSA VAs	RSA VAs	clarkerentalss.com	10.65.[redacted]	199.115.243.162	Allowed	Malware	
DNS	RSA VAs	RSA VAs	clarkerentalss.com	10.65.[redacted]	199.115.243.161	Allowed	Malware	
DNS	RSA VAs	RSA VAs	clarkerentalss.com	10.65.[redacted]	199.115.243.162	Allowed	Malware	
DNS	RSA 2022	RSA 2022	clarkerentalss.com	[redacted]	199.115.241.171	Allowed	Malware	
DNS	RSA VAs	RSA VAs	clarkerentalss.com	10.65.[redacted]	199.115.243.162	Allowed	Malware	
DNS	RSA VAs	RSA VAs	clarkerentalss.com	10.65.[redacted]	199.115.243.162	Allowed	Malware	
DNS	RSA VAs	RSA VAs	clarkerentalss.com	10.65.[redacted]	199.115.243.161	Allowed	Malware	

Event Details

Action: Allowed

Time: Jun 6, 2022 2:27 PM

Identity: RSA VAs

Policy or Ruleset Identity: RSA VAs

Internal IP Address: 10.65.[redacted]

External IP Address: 199.115.243.162

Destination: clarkerentalss.com

Categories: Malware

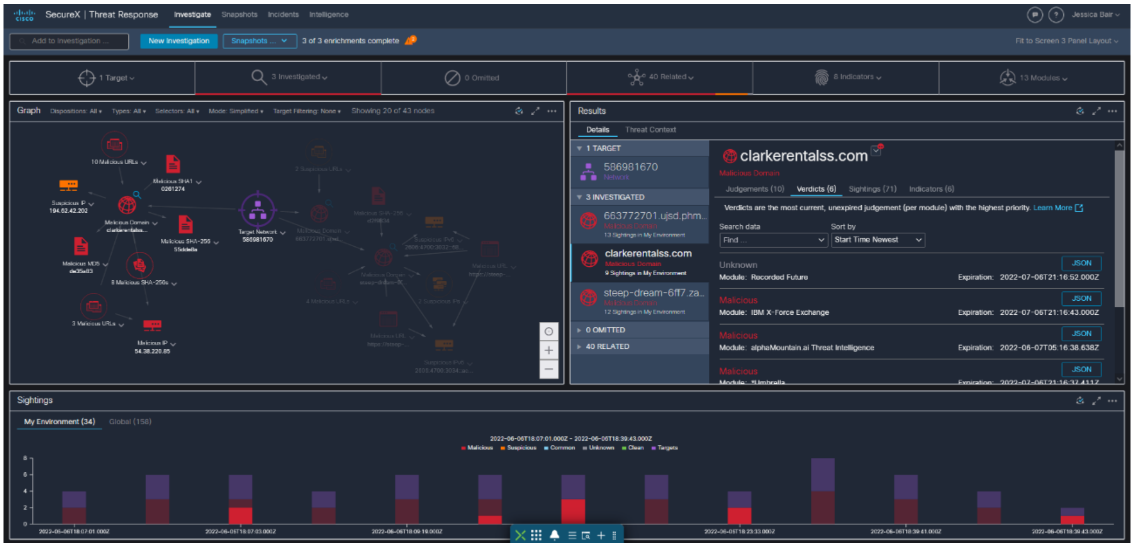
Dispute Categorization

Application: -

Application Category

DNS Type: AAAA

Investigating the domain in SecureX revealed the extent of the threat and the Sightings in the network, showing it was limited to one endpoint, and not the start of a botnet infection at the conference.



SecureX | Threat Response | Investigate | Snapshots | Incidents | Intelligence | Jessica Bair

Add to Investigation ... | New Investigation | Snapshots ... | 3 of 3 enrichments complete | Fit to Screen 3 Panel Layout

1 Target | 3 Investigated | 0 Omitted | 40 Related | 8 Indicators | 13 Modules

Graph | Dispositions: All | Types: All | Selectors: All | Mode: Simplified | Target Filtering: None | Showing 20 of 43 nodes

Results | Details | Threat Context

1 TARGET
586981670 (Network)

3 INVESTIGATED
663772701.ujsd.phm... — Malicious Domain — 13 Sightings in My Environment
clarkerentalss.com — Malicious Domain — 9 Sightings in My Environment
steep-dream-6ff7.za... — Malicious Domain — 12 Sightings in My Environment

0 OMITTED

40 RELATED

clarkerentalss.com
Malicious Domain

Judgements (10) | Verdicts (6) | Sightings (71) | Indicators (6)

Verdicts are the most current, unexpired judgement (per module) with the highest priority. Learn More

Search data: Find ... | Sort by: Start Time Newest

Unknown — Module: Recorded Future — Expiration: 2022-07-06T21:16:52.000Z — JSON

Malicious — Module: IBM X-Force Exchange — Expiration: 2022-07-06T21:16:43.000Z — JSON

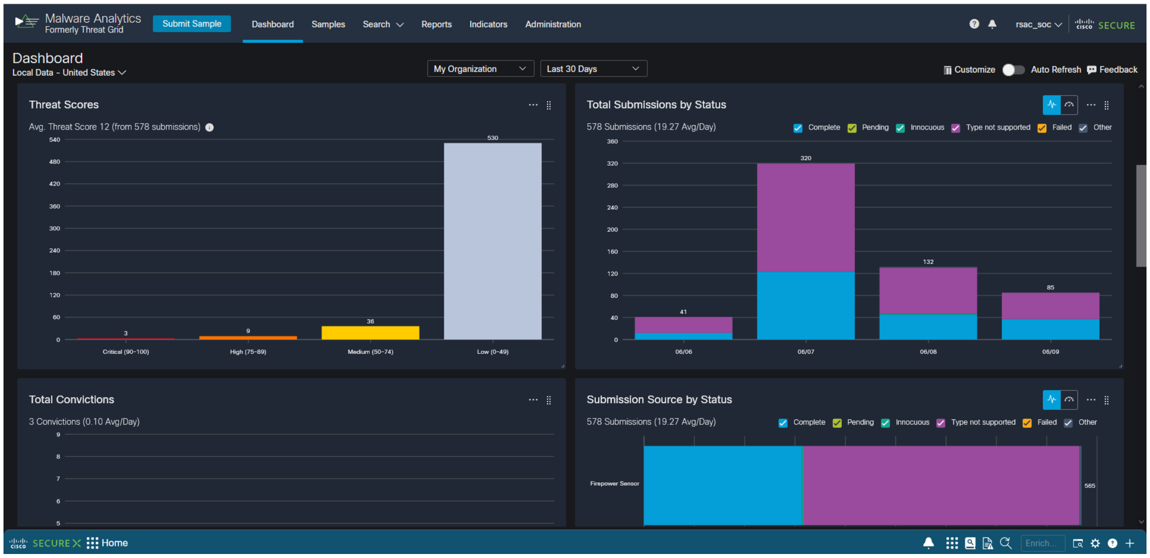
Malicious — Module: alphaMountain.ai Threat Intelligence — Expiration: 2022-06-07T05:16:38.638Z — JSON

Malicious — Module: *Umbrella — Expiration: 2022-07-06T21:16:37.411Z — JSON

Sightings | My Environment (34) | Global (158)

MALWARE ANALYSIS

The RSAC SOC team sent over 500 potentially malicious files to Secure Malware Analytics via NetWitness® Platform XDR and Secure Firewall, for automated behavioral analysis.



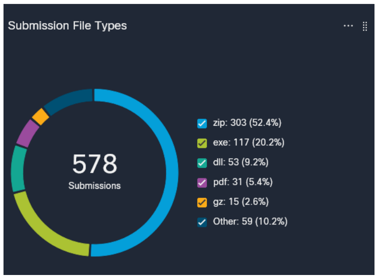
Avg. Threat Score 12 (from 578 submissions)

578 Submissions (19.27 Avg/Day)

3 Convictions (0.10 Avg/Day)

578 Submissions (19.27 Avg/Day)

The breakdown of major file types is as follows.



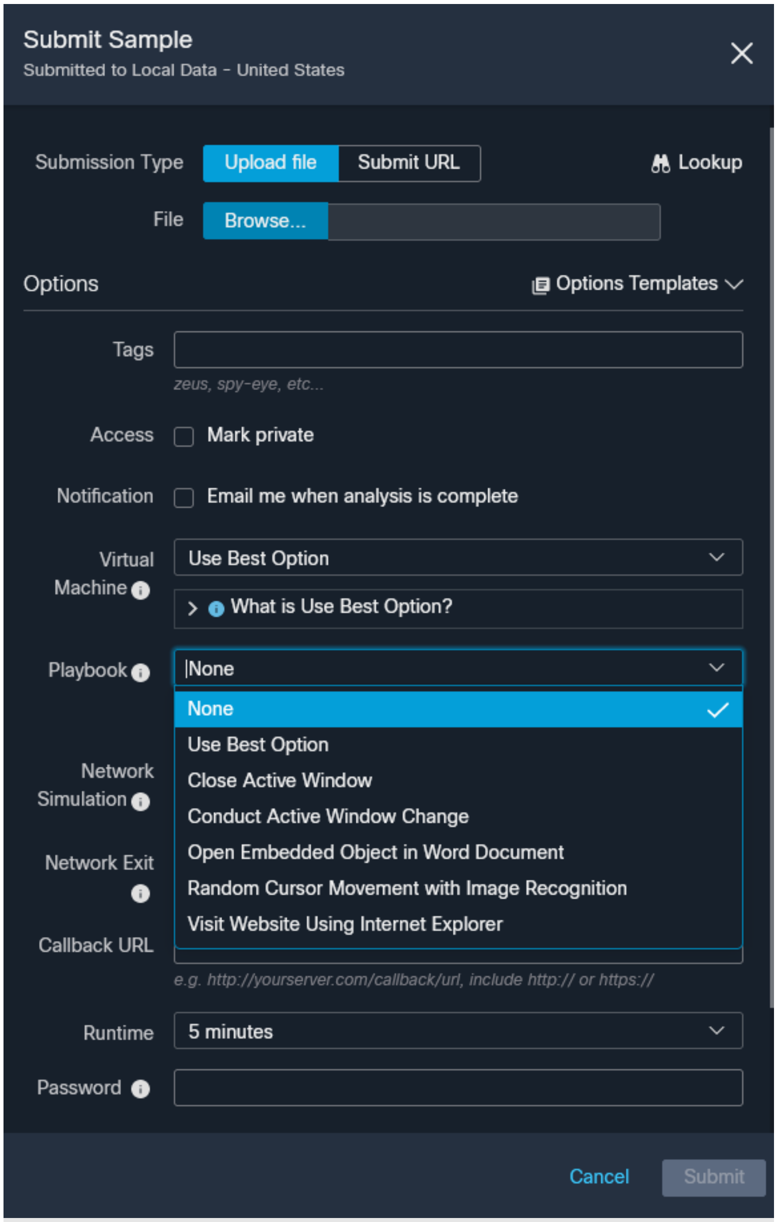
- zip: 303 (52.4%)
- exe: 117 (20.2%)
- dll: 53 (9.2%)
- pdf: 31 (5.4%)
- gz: 15 (2.6%)
- Other: 59 (10.2%)

Malicious Behavior

In 2020, on the third full day of the conference, an attendee downloaded over 4,600 malware samples on the open network. We had no such event in 2022 and most of the samples were documents or updates to applications.

To emulate a user automatically during sample analysis, Secure Malware Analytics provides user emulation through playbooks, which are pre-defined steps that simulate user activity. A system with a user present appears vastly different from an automated analysis system (i.e., a sandbox). For example, an automated system may execute a submitted sample, but never change windows or move the mouse. On the other hand, a system with a real user present will have mouse movement and window changes as the user proceeds with a task or attempts to determine why the file they just opened did nothing.

Playbooks automatically simulate user activity during sample analysis, which allows Secure Malware Analytics to behave as if a user were present and operating the keyboard and mouse during analysis.



Submit Sample

Submitted to Local Data - United States

Submission Type: Upload file

File

Options

Tags: zeus, spy-eye, etc...

Access: □ Mark private

Notification: □ Email me when analysis is complete

Virtual Machine: Use Best Option

Playbook: None

Network Simulation

Network Exit

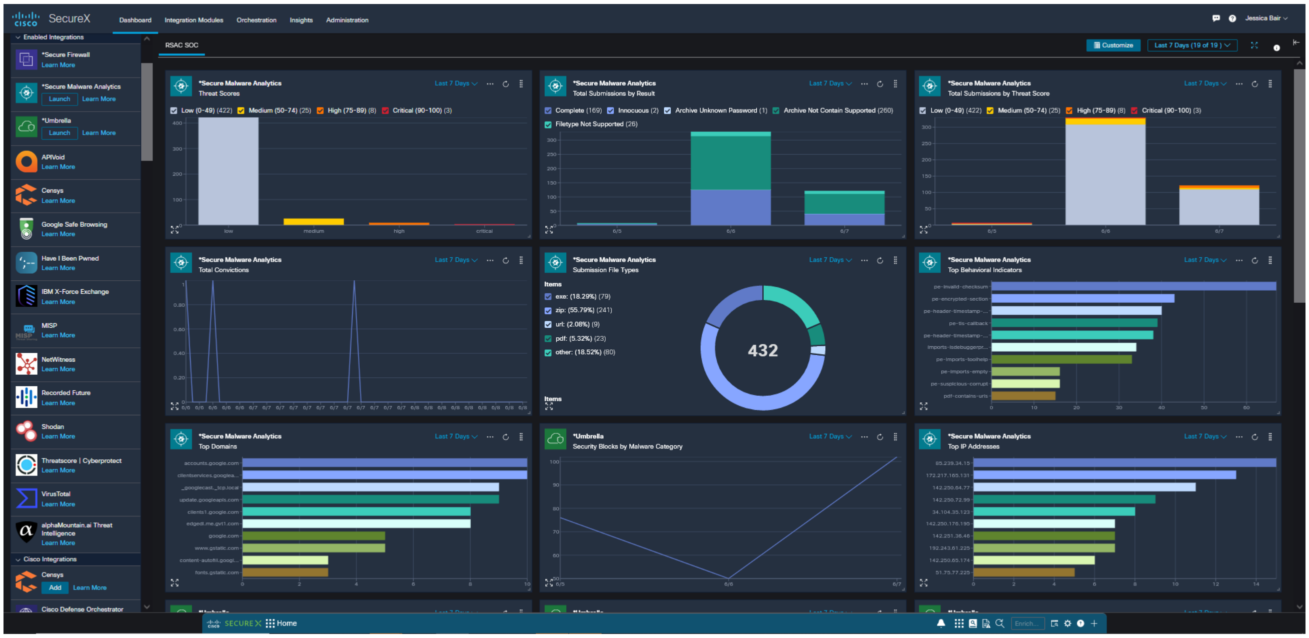
Callback URL: e.g. http://yourserver.com/callback/url, include http:// or https://

Runtime: 5 minutes

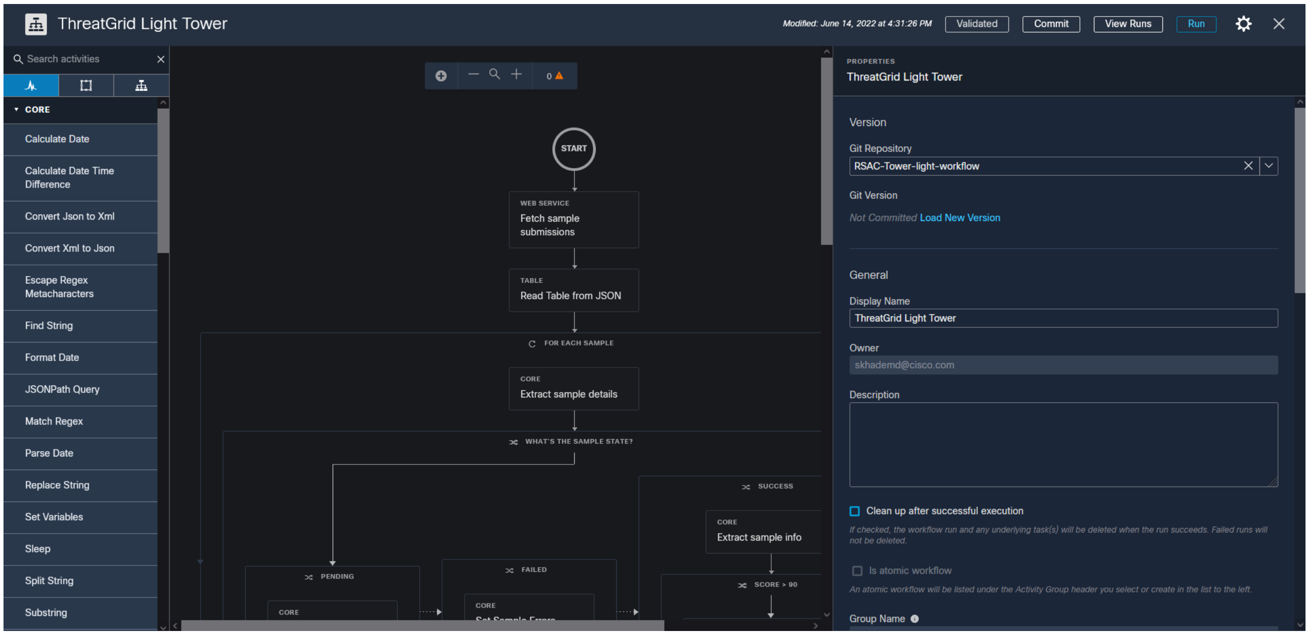
Password

Upload file
Submit URL
Lookup
Browse...
Options Templates
What is Use Best Option?
None ✓
Use Best Option
Close Active Window
Conduct Active Window Change
Open Embedded Object in Word Document
Random Cursor Movement with Image Recognition
Visit Website Using Internet Explorer
Cancel
Submit

We were able to monitor the sample submissions in the SecureX dashboard during the operations.



The team built a custom SecureX orchestration workflow to interact with Secure Malware Analytics.



ThreatGrid Light Tower

Modified: June 14, 2022 at 4:31:26 PM

Validated | Commit | View Runs | Run

Search activities

▾ CORE
- Calculate Date
- Calculate Date Time Difference
- Convert Json to Xml
- Convert Xml to Json
- Escape Regex Metacharacters
- Find String
- Format Date
- JSONPath Query
- Match Regex
- Parse Date
- Replace String
- Set Variables
- Sleep
- Split String
- Substring

START

WEB SERVICE
Fetch sample submissions

TABLE
Read Table from JSON

FOR EACH SAMPLE

CORE
Extract sample details

WHAT'S THE SAMPLE STATE?

SUCCESS

CORE
Extract sample info

SCORE > 90

PENDING

CORE

FAILED

CORE
Set Sample Errors

PROPERTIES
ThreatGrid Light Tower

Version

Git Repository: RSAC-Tower-light-workflow

Git Version: *Not Committed* Load New Version

General

Display Name: ThreatGrid Light Tower

Owner: skhademd@cisco.com

Description:

□ Clean up after successful execution

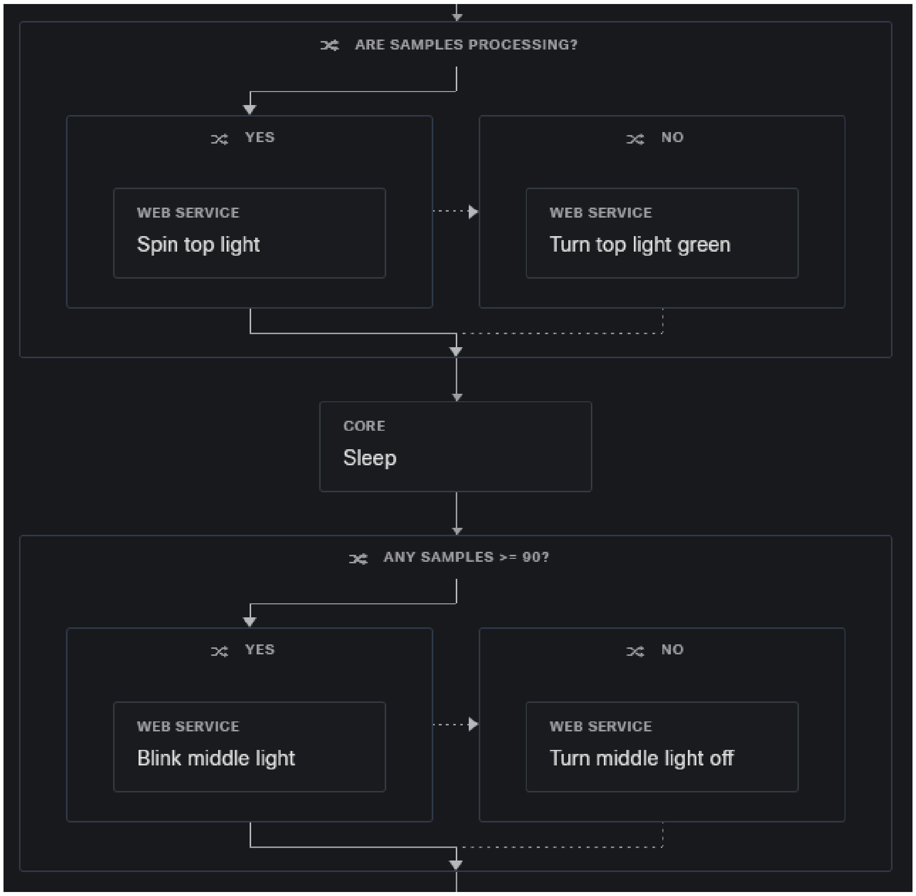
If checked, the workflow run and any underlying task(s) will be deleted when the run succeeds. Failed runs will not be deleted.

□ Is atomic workflow

An atomic workflow will be listed under the Activity Group header you select or create in the list to the left.

Group Name

The workflow caused the light to flash red when a sample had a threat score over 90 and also alert when processing samples.



The light was a welcome addition to the SOC dashboards.

DOMAIN NAME SERVER (DNS)

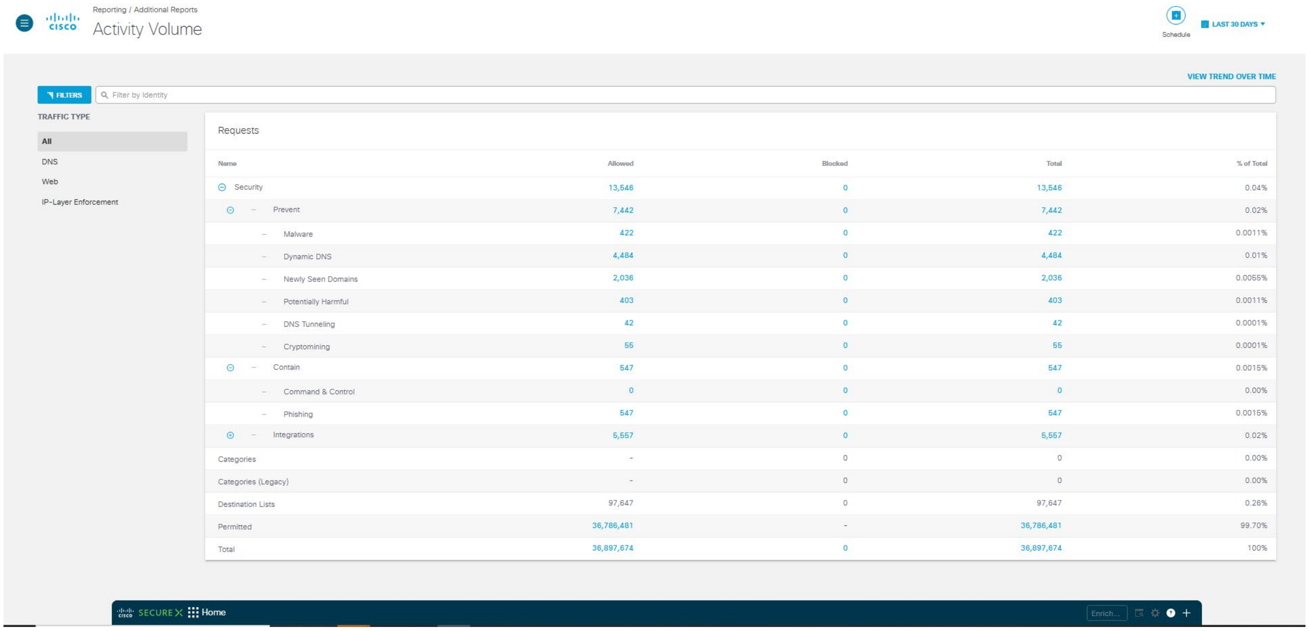
The SOC had complete DNS visibility in 2022, thanks to the support of the Moscone Center agreeing to change their DNS to Cisco Umbrella and installing an Umbrella virtual appliance in the Network Operation Center.

The default security settings for Cisco Umbrella are to block malware, command-and-control callback, and phishing attacks. All blocking was turned off for the conference network.

We saw nearly 37 million DNS requests over the week, of which several thousand would have been blocked for security.

This was almost the same number of DNS request in 2020.

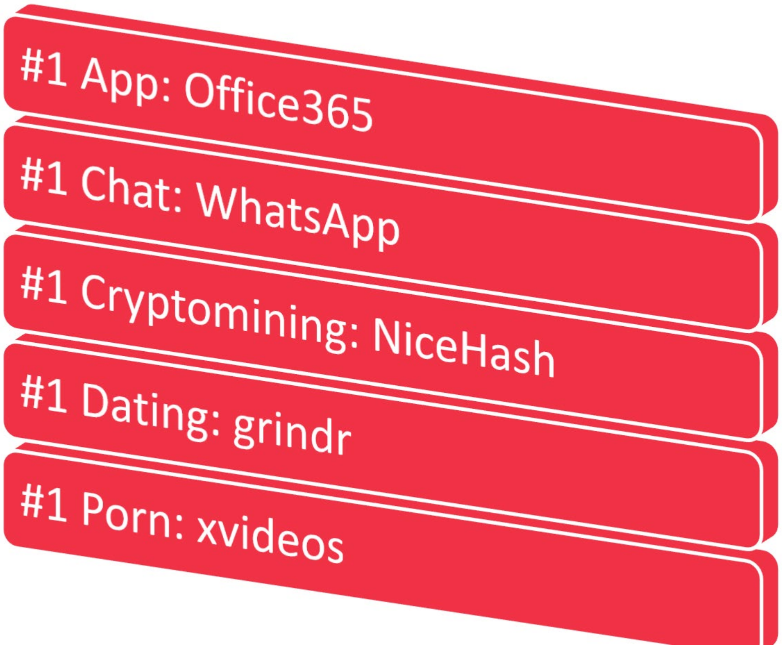
DNS is an area of the RSAC SOC, where preventive and protective measures could be taken, as in a production environment. However, we did not want to block any booth demonstrations, sessions or other training activity that relies on connecting to a malicious domain or IP address.



Requests

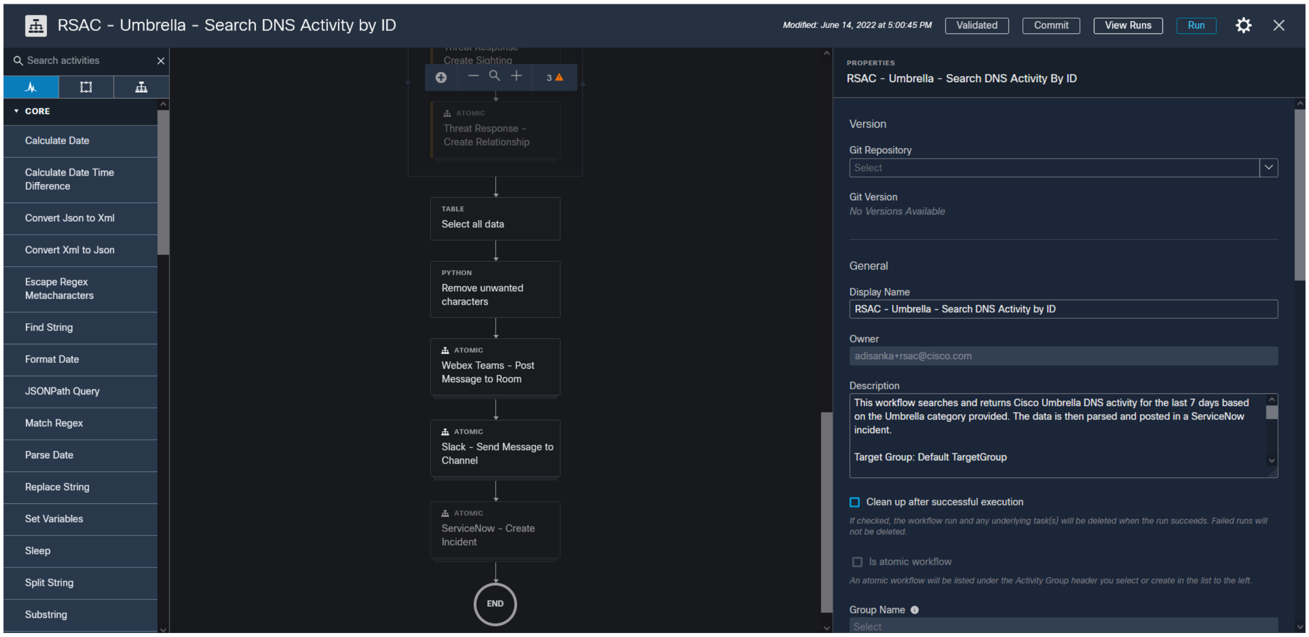
Name	Allowed	Blocked	Total	% of Total
⊖ Security	13,546	0	13,546	0.04%
⊖ – Prevent	7,442	0	7,442	0.02%
– Malware	422	0	422	0.0011%
– Dynamic DNS	4,484	0	4,484	0.01%
– Newly Seen Domains	2,036	0	2,036	0.0055%
– Potentially Harmful	403	0	403	0.0011%
– DNS Tunneling	42	0	42	0.0001%
– Cryptomining	55	0	55	0.0001%
⊖ – Contain	547	0	547	0.0015%
– Command & Control	0	0	0	0.00%
– Phishing	547	0	547	0.0015%
⊕ – Integrations	5,557	0	5,557	0.02%
Categories	-	0	0	0.00%
Categories (Legacy)	-	0	0	0.00%
Destination Lists	97,647	0	97,647	0.26%
Permitted	36,786,481	-	36,786,481	99.70%
Total	36,897,674	0	36,897,674	100%

Domains also could have been blocked for content, such as pornography, terrorism-related, hate/ discrimination or other such categories. Again, no blocking occurred and the SOC issued awards to the top domains in the SOC session on 9 June 2022.



Automate, Automate

Every year, the RSAC SOC team finds more ways to improve efficacy. This year, a Cisco analyst created an automated workflow in SecureX orchestration to post to the RSAC SOC Slack Channel and Webex space when an Umbrella security category was activated with a DNS request or a Firewall rule was triggered in Firepower IDS.


RSAC - Umbrella - Search DNS Activity by ID
Modified: June 14, 2022 at 5:00:45 PM
Validated
Commit
View Runs
Run
Search activities
CORE
Calculate Date
Calculate Date Time Difference
Convert Json to Xml
Convert Xml to Json
Escape Regex Metacharacters
Find String
Format Date
JSONPath Query
Match Regex
Parse Date
Replace String
Set Variables
Sleep
Split String
Substring
Create Sighting
3
ATOMIC
Threat Response - Create Relationship
TABLE
Select all data
PYTHON
Remove unwanted characters
ATOMIC
Webex Teams - Post Message to Room
ATOMIC
Slack - Send Message to Channel
ATOMIC
ServiceNow - Create Incident
END
PROPERTIES

RSAC - Umbrella - Search DNS Activity By ID

Version

Git Repository: Select

Git Version: *No Versions Available*

General

Display Name: RSAC - Umbrella - Search DNS Activity by ID

Owner: adisanka+rsac@cisco.com

Description: This workflow searches and returns Cisco Umbrella DNS activity for the last 7 days based on the Umbrella category provided. The data is then parsed and posted in a ServiceNow incident.

Target Group: Default TargetGroup

☐ Clean up after successful execution

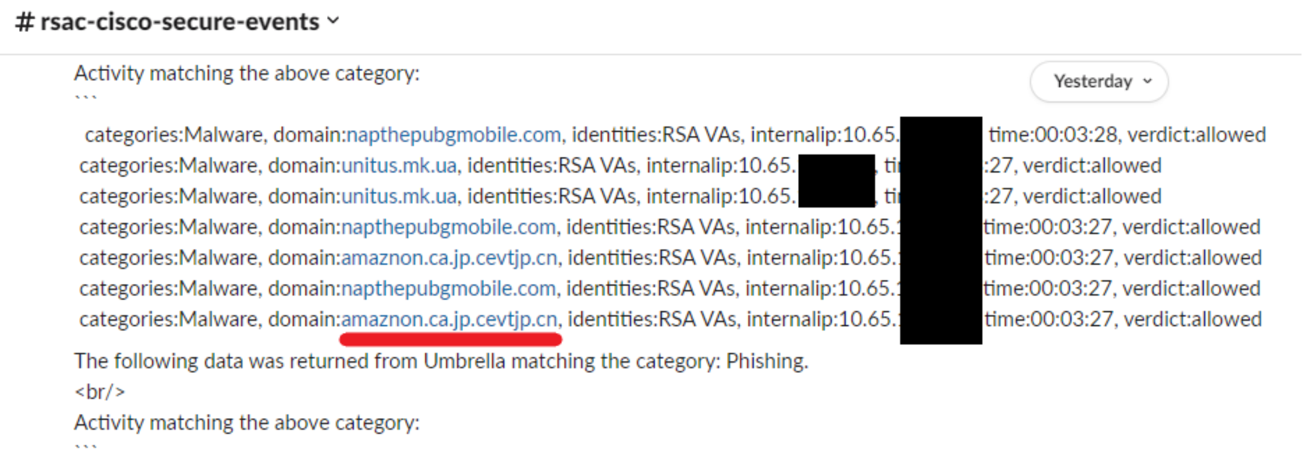
If checked, the workflow run and any underlying task(s) will be deleted when the run succeeds. Failed runs will not be deleted.

☐ Is atomic workflow

An atomic workflow will be listed under the Activity Group header you select or create in the list to the left.

Group Name: Select

One such Slack trigger was on a phishing domain, crafted to look like Amazon.com to users.

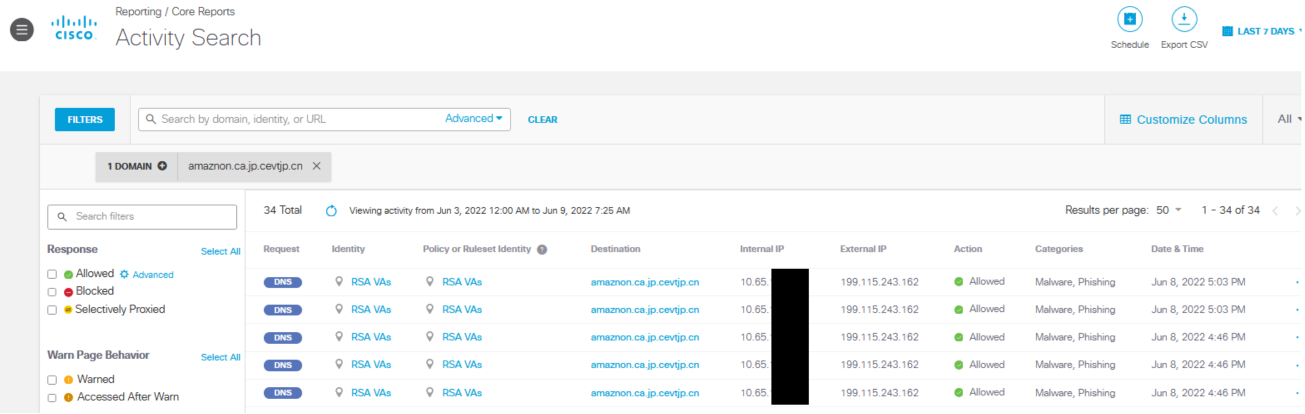
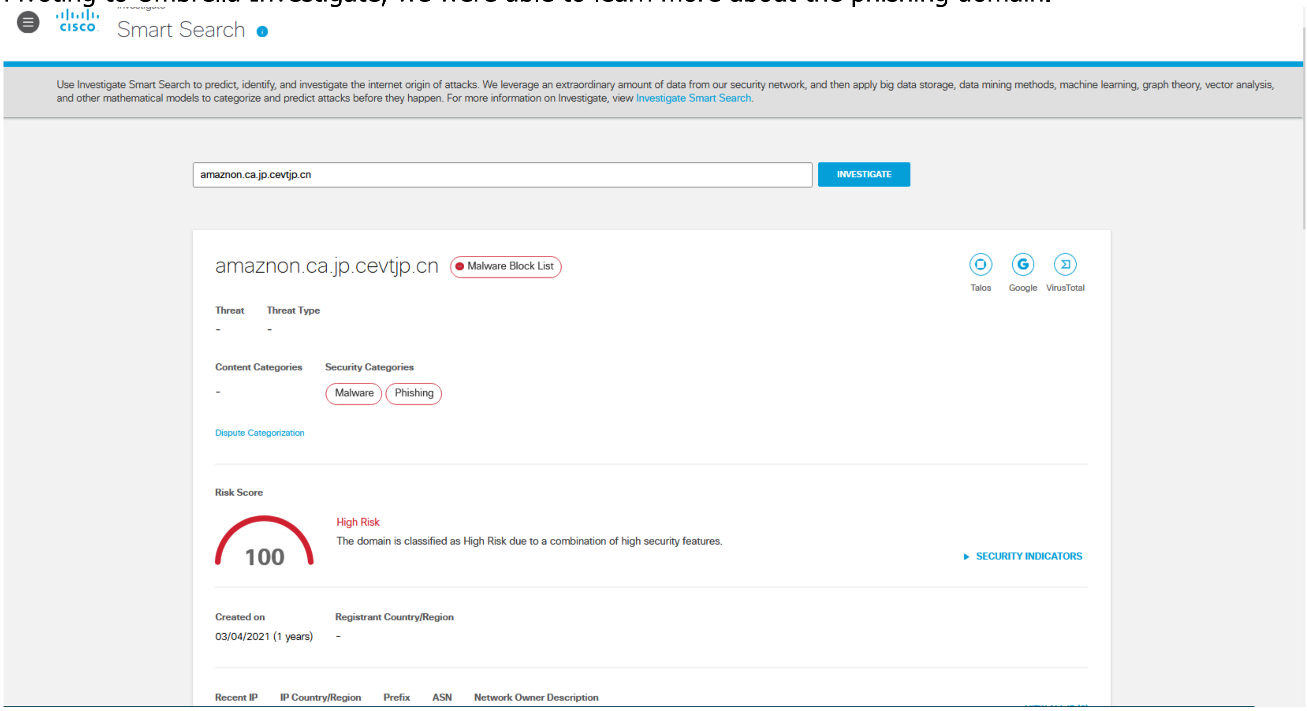


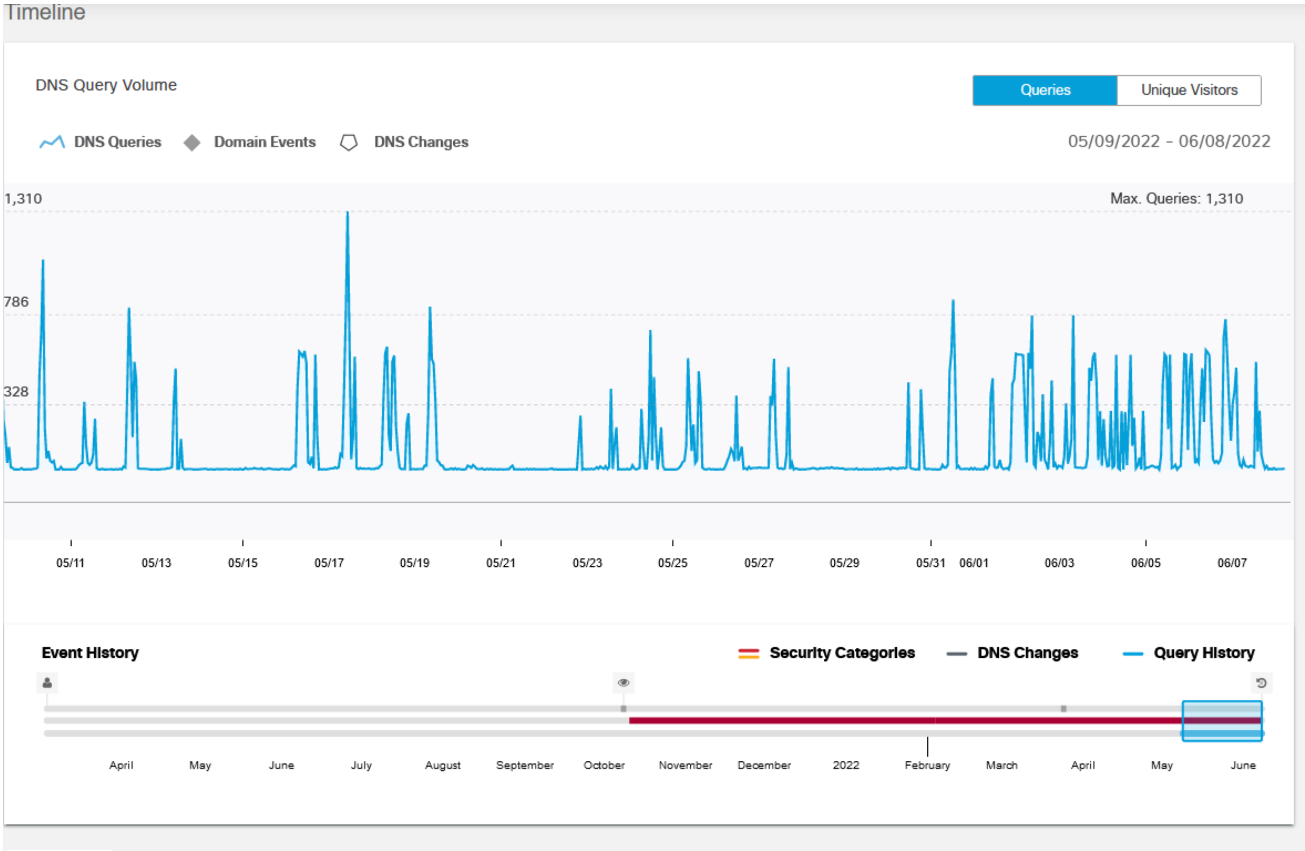
rsac-cisco-secure-events

Activity matching the above category:

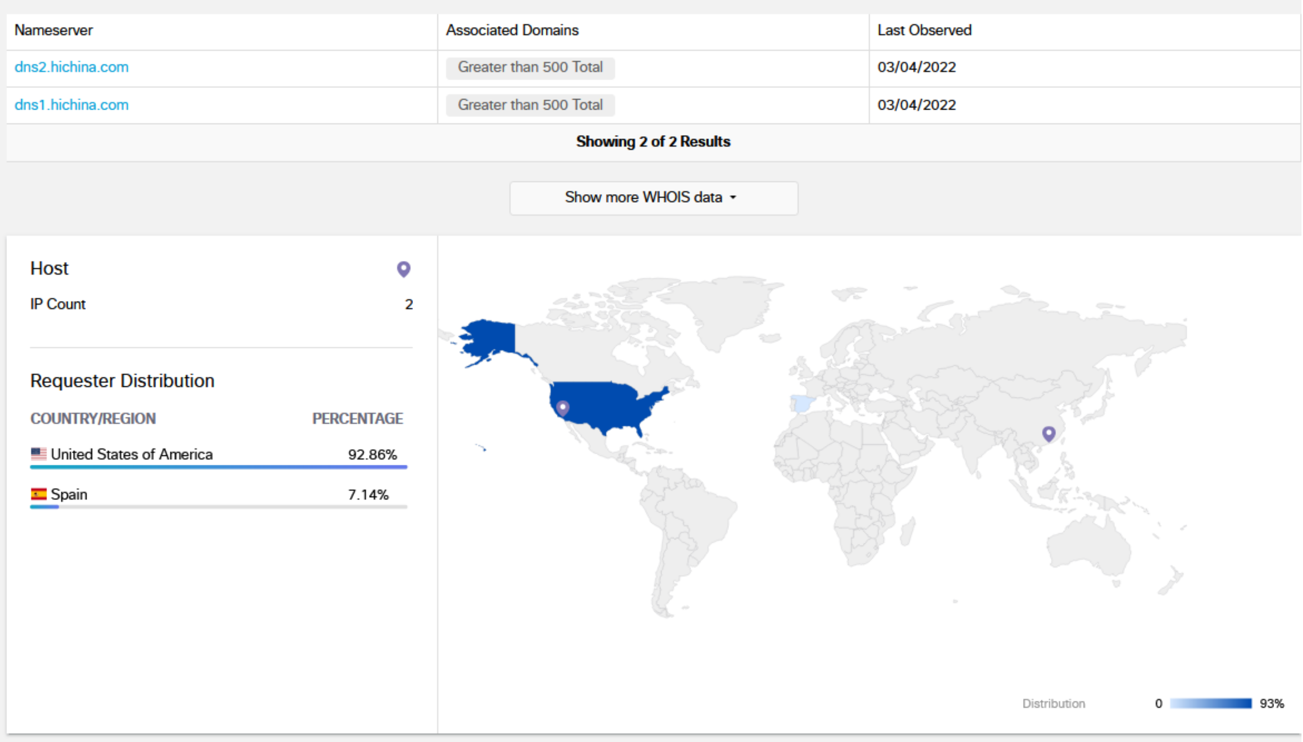
Yesterday

```
 categories:Malware, domain:napthepubgmobile.com, identities:RSA VAs, internalip:10.65.[redacted] time:00:03:28, verdict:allowed
categories:Malware, domain:unitus.mk.ua, identities:RSA VAs, internalip:10.65.[redacted] ti[redacted]:27, verdict:allowed
categories:Malware, domain:unitus.mk.ua, identities:RSA VAs, internalip:10.65.[redacted] ti[redacted]:27, verdict:allowed
categories:Malware, domain:napthepubgmobile.com, identities:RSA VAs, internalip:10.65.[redacted]time:00:03:27, verdict:allowed
categories:Malware, domain:amaznon.ca.jp.cevtjp.cn, identities:RSA VAs, internalip:10.65.[redacted]time:00:03:27, verdict:allowed
categories:Malware, domain:napthepubgmobile.com, identities:RSA VAs, internalip:10.65.[redacted]time:00:03:27, verdict:allowed
categories:Malware, domain:amaznon.ca.jp.cevtjp.cn, identities:RSA VAs, internalip:10.65.[redacted]time:00:03:27, verdict:allowed
```

The following data was returned from Umbrella matching the category: Phishing.
<br/>
Activity matching the above category:
```

Investigation identified the IP address of the user and the frequency of the DNS requests.



Reporting / Core Reports

## Activity Search

Response — Select All

- ☐ Allowed — Advanced
- ☐ Blocked
- ☐ Selectively Proxied

Warn Page Behavior — Select All

- ☐ Warned
- ☐ Accessed After Warn

34 Total — Viewing activity from Jun 3, 2022 12:00 AM to Jun 9, 2022 7:25 AM — Results per page: 50 — 1 - 34 of 34

| Request | Identity | Policy or Ruleset Identity | Destination | Internal IP | External IP | Action | Categories | Date & Time |
|---|---|---|---|---|---|---|---|---|
| DNS | RSA VAs | RSA VAs | amaznon.ca.jp.cevtjp.cn | 10.65.[redacted] | 199.115.243.162 | Allowed | Malware, Phishing | Jun 8, 2022 5:03 PM |
| DNS | RSA VAs | RSA VAs | amaznon.ca.jp.cevtjp.cn | 10.65.[redacted] | 199.115.243.162 | Allowed | Malware, Phishing | Jun 8, 2022 5:03 PM |
| DNS | RSA VAs | RSA VAs | amaznon.ca.jp.cevtjp.cn | 10.65.[redacted] | 199.115.243.162 | Allowed | Malware, Phishing | Jun 8, 2022 4:46 PM |
| DNS | RSA VAs | RSA VAs | amaznon.ca.jp.cevtjp.cn | 10.65.[redacted] | 199.115.243.162 | Allowed | Malware, Phishing | Jun 8, 2022 4:46 PM |
| DNS | RSA VAs | RSA VAs | amaznon.ca.jp.cevtjp.cn | 10.65.[redacted] | 199.115.243.162 | Allowed | Malware, Phishing | Jun 8, 2022 4:46 PM |

Pivoting to Umbrella Investigate, we were able to learn more about the phishing domain.



## Smart Search

Use Investigate Smart Search to predict, identify, and investigate the internet origin of attacks. We leverage an extraordinary amount of data from our security network, and then apply big data storage, data mining methods, machine learning, graph theory, vector analysis, and other mathematical models to categorize and predict attacks before they happen. For more information on Investigate, view Investigate Smart Search.

amaznon.ca.jp.cevtjp.cn — Malware Block List

| Threat | Threat Type |
|---|---|
| - | - |

| Content Categories | Security Categories |
|---|---|
| - | Malware, Phishing |

Risk Score

100 — High Risk

The domain is classified as High Risk due to a combination of high security features.

| Created on | Registrant Country/Region |
|---|---|
| 03/04/2021 (1 years) | - |

Recent IP — IP Country/Region — Prefix — ASN — Network Owner Description

This included the global query volume and that it was not a recently created domain.
```



The domain was registered in China and primarily targeted the USA, although also Spain.



Nameserver	Associated Domains	Last Observed
dns2.hichina.com	Greater than 500 Total	03/04/2022
dns1.hichina.com	Greater than 500 Total	03/04/2022

Showing 2 of 2 Results

Host

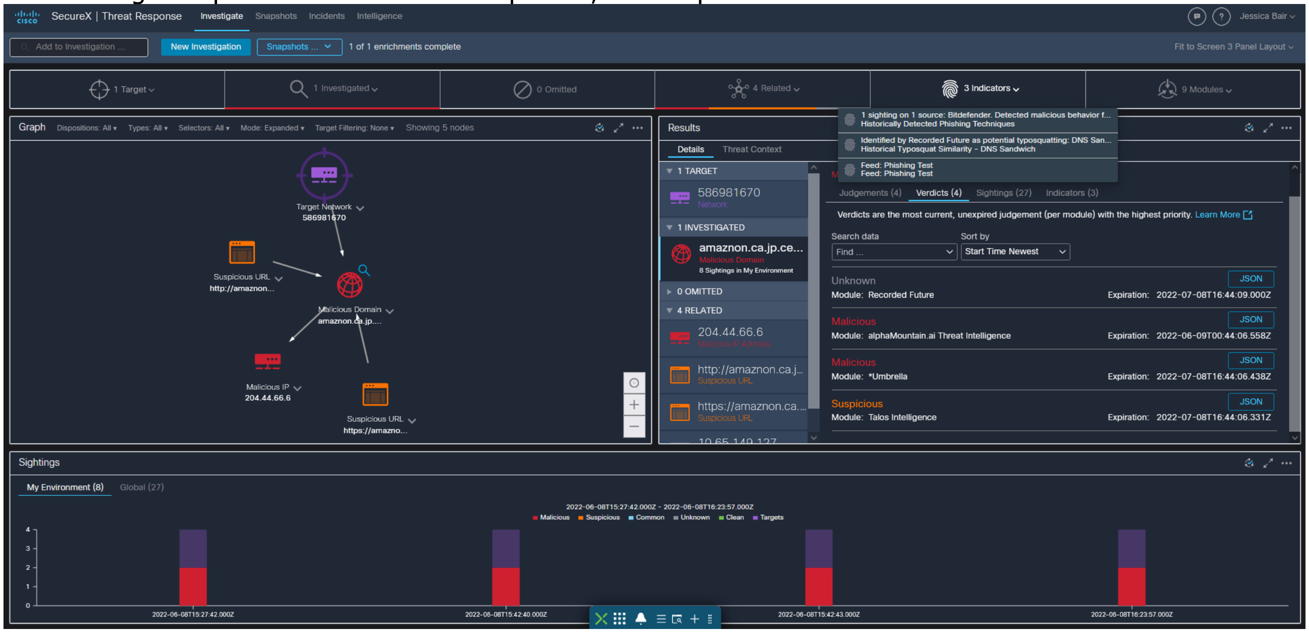
IP Count	2

Requester Distribution

COUNTRY/REGION	PERCENTAGE
United States of America	92.86%
Spain	7.14%

We dug in deeper with an investigation in SecureX threat response XDR, where we could see the threat intelligence about the domain and related artifacts.

The investigation pointed a demo in the Expo Hall, an acceptable use of the conference network.



1 of 1 enrichments complete

1 sighting on 1 source: Bitdefender. Detected malicious behavior f...
Historically Detected Phishing Techniques

Identified by Recorded Future as potential typosquatting: DNS San...
Historical Typosquat Similarity - DNS Sandwich

Feed: Phishing Test
Feed: Phishing Test

1 TARGET
586981670
Network

1 INVESTIGATED
amaznon.ca.jp.ce...
Malicious Domain
8 Sightings in My Environment

0 OMITTED

4 RELATED
204.44.66.6
Malicious IP Address
http://amaznon.ca.j...
Suspicious URL
https://amaznon.ca....
Suspicious URL
10.65.149.127

Verdicts are the most current, unexpired judgement (per module) with the highest priority. Learn More

Unknown
Module: Recorded Future Expiration: 2022-07-08T16:44:09.000Z

Malicious
Module: alphaMountain.ai Threat Intelligence Expiration: 2022-06-09T00:44:06.558Z

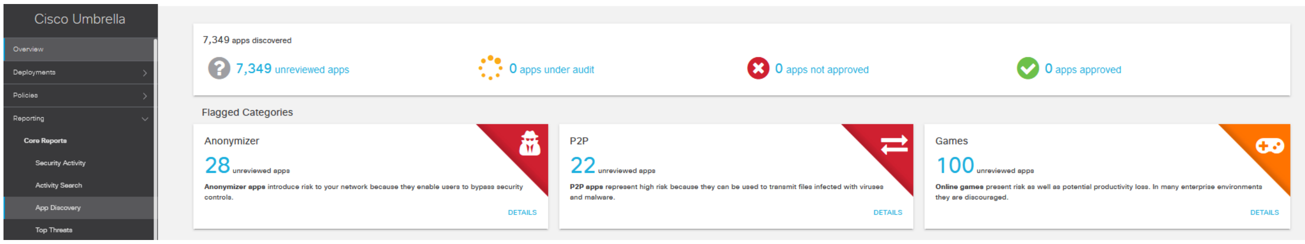
Malicious
Module: *Umbrella Expiration: 2022-07-08T16:44:06.438Z

Suspicious
Module: Talos Intelligence Expiration: 2022-07-08T16:44:06.331Z

2022-06-08T15:27:42.000Z - 2022-06-08T16:23:57.000Z

Apps, Apps and more Apps

Over 7,200 applications (up from just 4,000 applications in 2020) were identified by the DNS queries at RSAC 2020.



7,349 apps discovered

7,349 unreviewed apps | 0 apps under audit | 0 apps not approved | 0 apps approved

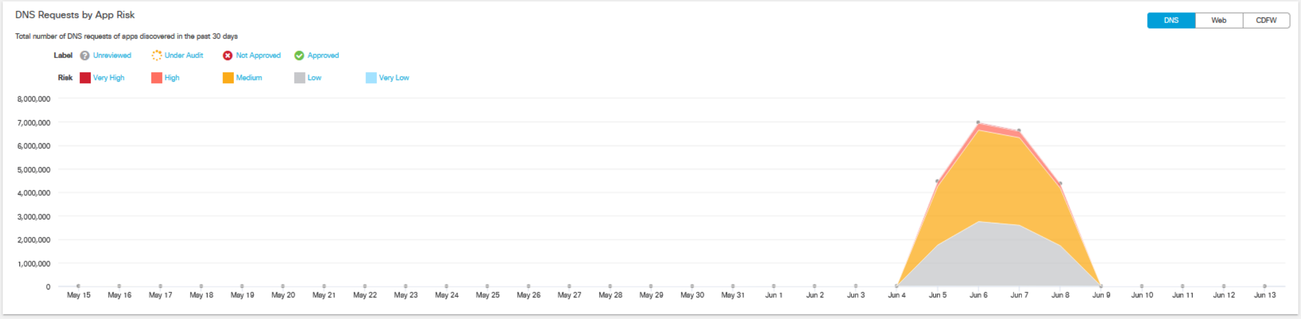
Flagged Categories

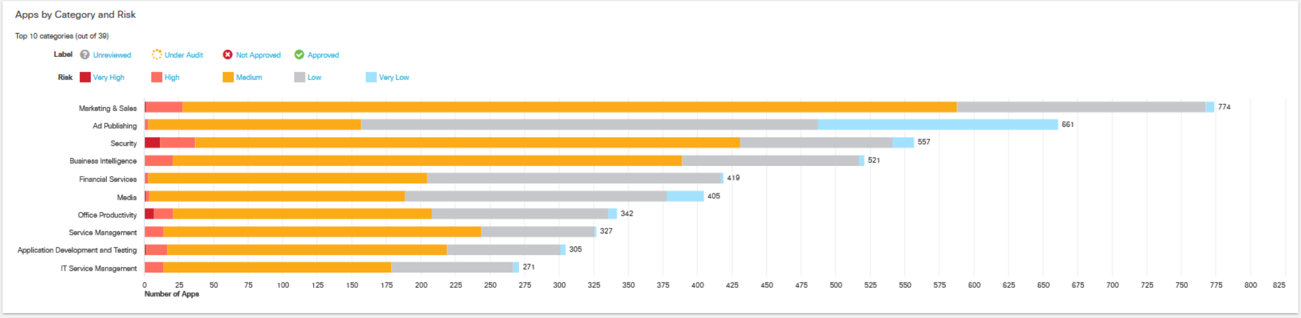
Anonymizer
28 unreviewed apps
Anonymizer apps introduce risk to your network because they enable users to bypass security controls.

P2P
22 unreviewed apps
P2P apps represent high risk because they can be used to transmit files infected with viruses and malware.

Games
100 unreviewed apps
Online games present risk as well as potential productivity loss. In many enterprise environments they are discouraged.

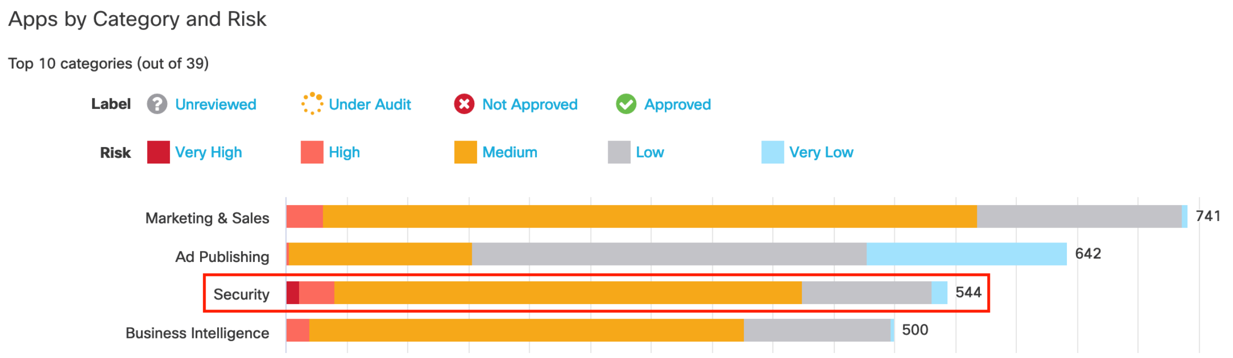
The apps were categorized by risk to an organization in a production environment. A rogue or unauthorized app could have been blocked from the conference, in the event of a major incident—again, one of the ways the SOC can be used for protection in an emergency.





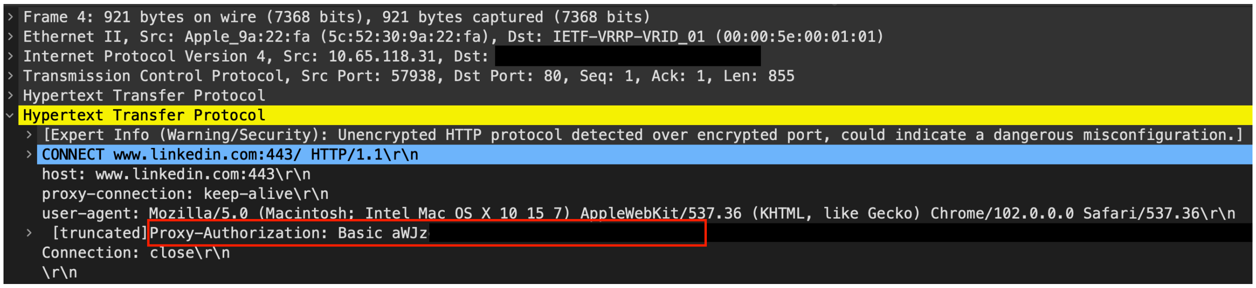
Open Web Proxy

Web security vendors abound at the RSA conference so it's not surprising to see lot of traffic from the show floor destined for cloud proxies of all kinds. We spotted thousands of instances of machines checking in with, sending traffic to, and otherwise utilizing over 500 security solutions. A Cisco Umbrella engineer on the SOC team with a history in web proxies and was naturally interested in examining how some of these solutions communicate with their cloud resources, and what might be visible to anyone listening on the local network.



Using the Umbrella dashboard to explore the DNS queries made to the "Security" app category, he immediately homed in on the domains he recognized as cloud proxy solutions. The engineer could tell by the DNS queries that some of them were requests directly to a cloud web proxy. These would be HTTP or HTTPS requests destined for the Internet but encapsulated in an HTTP CONNECT request to the cloud security solution, which would service the request to the Internet server.

Pivoting over to NetWitness® Platform XDR, he was able to search and locate the content of the requests themselves and scrutinize the headers inside.



```
› Frame 4: 921 bytes on wire (7368 bits), 921 bytes captured (7368 bits)
› Ethernet II, Src: Apple_9a:22:fa (5c:52:30:9a:22:fa), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
› Internet Protocol Version 4, Src: 10.65.118.31, Dst: [redacted]
› Transmission Control Protocol, Src Port: 57938, Dst Port: 80, Seq: 1, Ack: 1, Len: 855
› Hypertext Transfer Protocol
⌄ Hypertext Transfer Protocol
  › [Expert Info (Warning/Security): Unencrypted HTTP protocol detected over encrypted port, could indicate a dangerous misconfiguration.]
  › CONNECT www.linkedin.com:443/ HTTP/1.1\r\n
    host: www.linkedin.com:443\r\n
    proxy-connection: keep-alive\r\n
    user-agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.0.0 Safari/537.36\r\n
  ›  [truncated]Proxy-Authorization: Basic aWJz[redacted]
    Connection: close\r\n
    \r\n
```

When and explicit proxy is configured in an OS or browser, requests are encapsulated in HTTP, even those that ultimately flow over HTTPS (encrypted in a TLS tunnel). Proxies that require authentication can be configured to accept a few different methods to identify the requestor. Basic authentication is the least secure form of this flow and simply accepts a base64 encoded header containing the username and password.

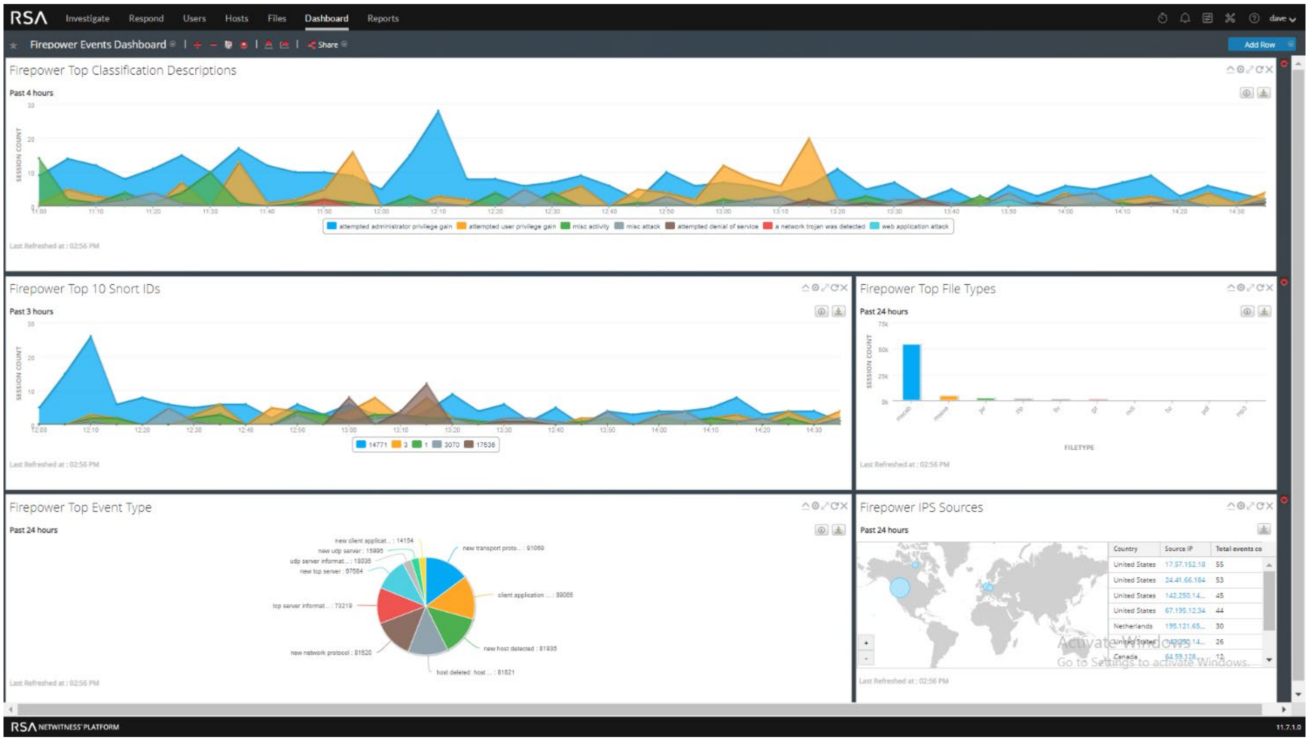
Even this can be done securely if the client utilized some form of encryption or ephemeral generation of the credentials that only the cloud proxy could validate or predict. In this case, none of that was true. By simply extracting the base64 encoded credentials, it is possible for anyone sniffing the network to browse the internet using this proxy server, authenticated as the unsuspecting attendee. There are many ways to leverage an open web proxy that a creative hacker may want to explore, should this misconfiguration be discovered.

INTRUSION DETECTION

A Secure Firewall 4110 appliance, running Firepower Threat Defense software, was set up as the perimeter IDS device. The IDS inspected all wireless guest traffic from event attendees, configured in monitor-only mode. Firepower offers breach detection, threat discovery, malware sample submission to Secure Malware Analytics and security automation. Rich contextual information (such as applications, operating systems, vulnerabilities, intrusions, and transferred files) served the SOC to help uncover threats lurking in the environment.

The Cisco team was able to complete a direct integration of event data into NetWitness® Platform XDR using the Firepower eStreamer protocol. Over 50 million+ events were sent to NetWitness® from Firepower, at an average event rate between 500-1100 events per second. This integration enables NetWitness® users to directly query Firewall data and create mash up visualizations from both data sources.

The analytic below depicts a detailed analysis of Firepower events by volume, threat category and geolocation and triggered Snort rule.


RSA
Investigate
Respond
Users
Hosts
Files
Dashboard
Reports
dave
Firepower Events Dashboard
Share
Add Row
Firepower Top Classification Descriptions
Past 4 hours
SESSION COUNT
30
20
10
0
11:00
11:10
11:20
11:30
11:40
11:50
12:00
12:10
12:20
12:30
12:40
12:50
13:00
13:10
13:20
13:30
13:40
13:50
14:00
14:10
14:20
14:30
attempted administrator privilege gain
attempted user privilege gain
misc activity
misc attack
attempted denial of service
a network trojan was detected
web application attack
Last Refreshed at : 02:56 PM
Firepower Top 10 Snort IDs
Past 3 hours
14771
3
1
3070
17536
Last Refreshed at : 02:56 PM
Firepower Top File Types
Past 24 hours
75k
50k
25k
0k
FILETYPE
Last Refreshed at : 02:56 PM
Firepower Top Event Type
Past 24 hours
new client applicat... : 14154
new udp server : 15996
udp server informat... : 18036
new tcp server : 67564
tcp server informat... : 73219
new network protocol : 81620
host deleted: host ... : 81821
new host detected : 81935
client application ... : 89065
new transport proto... : 91069
Last Refreshed at : 02:56 PM
Firepower IPS Sources
Past 24 hours
Activate Windows
Go to Settings to activate Windows.
Last Refreshed at : 02:56 PM
RSA NETWITNESS PLATFORM
11.7.1.0

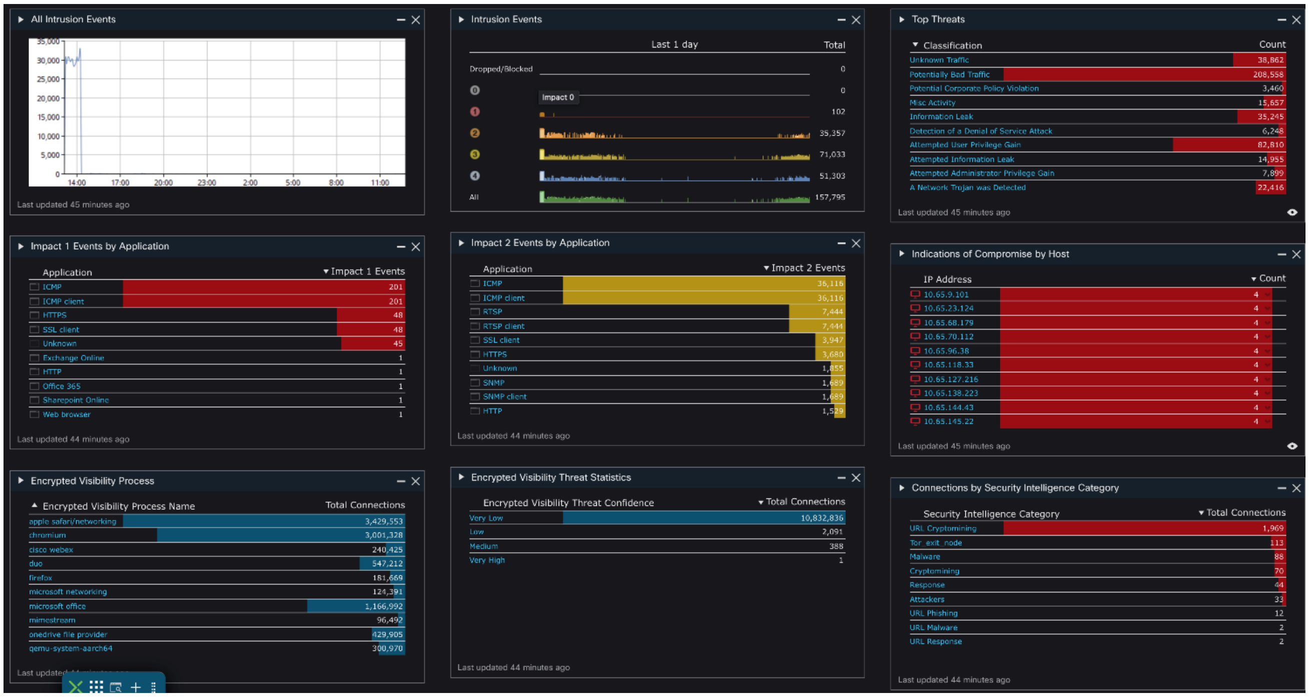
Country	Source IP	Total events co
United States	17.57.152.18	55
United States	24.41.66.184	53
United States	142.250.14...	45
United States	67.195.12.34	44
Netherlands	195.121.65...	30
United States	142.250.14...	26
Canada	64.59.128...	12

Discovered Applications

Firepower detected many popular applications in use, with Netflix, YouTube (often used for demos), iTunes updates and iPhone backups being the top applications. A lot of visitors were using the VPN to connect back to their company's network using the RSAC Wi-Fi, which explains why IPSEC is the top application.

With the increases in social media activity around the event, Facebook and Twitter were the top two social media platforms used at RSAC, for personal as well as promotional purposes.

Using personal social media and sensitive websites on public Wi-Fi, without VPN, is not recommended because of common security issues.



All Intrusion Events

Last updated 45 minutes ago

Intrusion Events

	Last 1 day	Total
Dropped/Blocked		0
0	Impact 0	0
1		102
2		35,357
3		71,033
4		51,303
All		157,795

Top Threats

▼ Classification	Count
Unknown Traffic	38,862
Potentially Bad Traffic	208,558
Potential Corporate Policy Violation	3,460
Misc Activity	15,657
Information Leak	35,245
Detection of a Denial of Service Attack	6,248
Attempted User Privilege Gain	82,810
Attempted Information Leak	14,955
Attempted Administrator Privilege Gain	7,899
A Network Trojan was Detected	22,416

Last updated 45 minutes ago

Impact 1 Events by Application

Application	▼ Impact 1 Events
ICMP	201
ICMP client	201
HTTPS	48
SSL client	48
Unknown	45
Exchange Online	1
HTTP	1
Office 365	1
Sharepoint Online	1
Web browser	1

Last updated 44 minutes ago

Impact 2 Events by Application

Application	▼ Impact 2 Events
ICMP	36,116
ICMP client	36,116
RTSP	7,444
RTSP client	7,444
SSL client	3,947
HTTPS	3,680
Unknown	1,855
SNMP	1,689
SNMP client	1,689
HTTP	1,529

Last updated 44 minutes ago

Indications of Compromise by Host

IP Address	▼ Count
10.65.9.101	4
10.65.23.124	4
10.65.68.179	4
10.65.70.112	4
10.65.96.38	4
10.65.118.33	4
10.65.127.216	4
10.65.138.223	4
10.65.144.43	4
10.65.145.22	4

Last updated 45 minutes ago

Encrypted Visibility Process

▲ Encrypted Visibility Process Name	Total Connections
apple safari/networking	3,429,553
chromium	3,001,328
cisco webex	240,425
duo	547,212
firefox	181,669
microsoft networking	124,391
microsoft office	1,166,992
mimestream	96,492
onedrive file provider	429,905
qemu-system-aarch64	300,970

Last updated

Encrypted Visibility Threat Statistics

Encrypted Visibility Threat Confidence	▼ Total Connections
Very Low	10,832,836
Low	2,091
Medium	388
Very High	1

Last updated 44 minutes ago

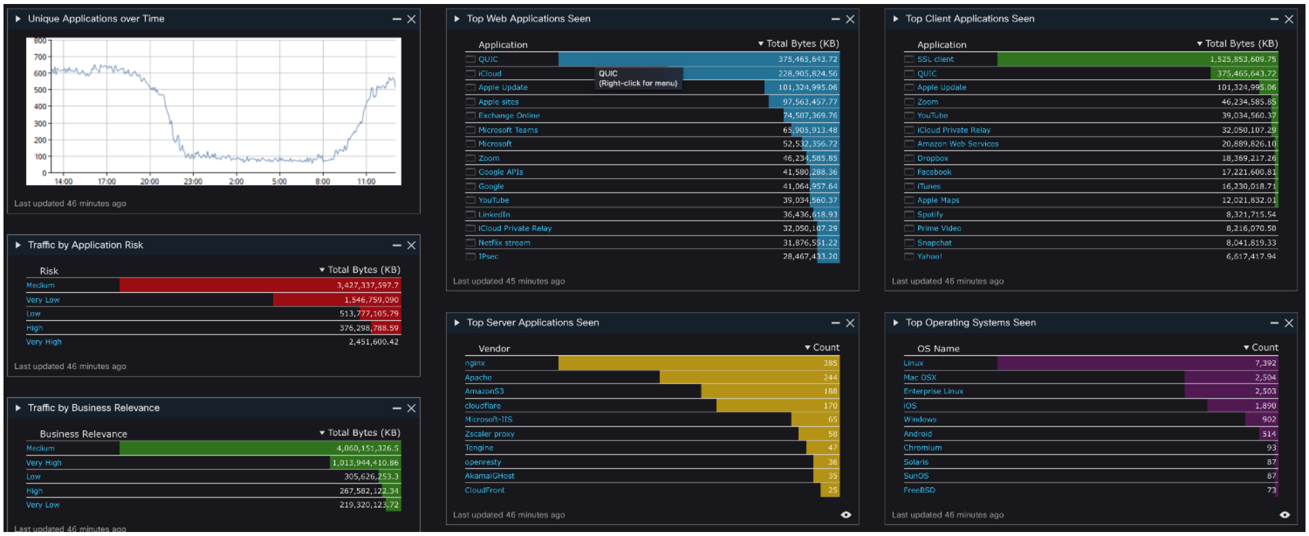
Connections by Security Intelligence Category

Security Intelligence Category	▼ Total Connections
URL Cryptomining	1,969
Tor_exit_node	113
Malware	88
Cryptomining	70
Response	44
Attackers	33
URL Phishing	12
URL Malware	2
URL Response	2

Last updated 44 minutes ago

CISCO FMC - TOP DISCOVERED APPLICATIONS

The top operating systems seen in the network were Linux and Mac OS.



Unique Applications over Time

Last updated 46 minutes ago

Traffic by Application Risk

Risk	▼ Total Bytes (KB)
Medium	3,427,337,597.7
Very Low	1,546,759,090
Low	513,777,105.79
High	376,298,788.59
Very High	2,451,600.42

Last updated 46 minutes ago

Traffic by Business Relevance

Business Relevance	▼ Total Bytes (KB)
Medium	4,060,151,326.5
Very High	1,013,944,410.86
Low	305,626,253.3
High	267,582,122.34
Very Low	219,320,123.72

Last updated 46 minutes ago

Top Web Applications Seen

Application	▼ Total Bytes (KB)
QUIC	375,465,643.72
iCloud	228,905,824.56
Apple Update	101,324,995.06
Apple sites	97,563,457.77
Exchange Online	74,507,369.76
Microsoft Teams	65,905,913.48
Microsoft	52,532,356.72
Zoom	46,234,585.85
Google APIs	41,580,288.36
Google	41,064,957.64
YouTube	39,034,560.37
LinkedIn	36,436,618.93
iCloud Private Relay	32,050,107.29
Netflix stream	31,876,551.22
IPsec	28,467,433.20

Last updated 45 minutes ago

Top Client Applications Seen

Application	▼ Total Bytes (KB)
SSL client	1,525,853,609.75
QUIC	375,465,643.72
Apple Update	101,324,995.06
Zoom	46,234,585.85
YouTube	39,034,560.37
iCloud Private Relay	32,050,107.29
Amazon Web Services	20,889,826.10
Dropbox	18,369,217.26
Facebook	17,221,600.81
iTunes	16,230,018.71
Apple Maps	12,021,832.01
Spotify	8,321,715.54
Prime Video	8,216,070.50
Snapchat	8,041,819.33
Yahoo!	6,617,417.94

Last updated 46 minutes ago

Top Server Applications Seen

Vendor	▼ Count
nginx	385
Apache	244
AmazonS3	188
cloudflare	170
Microsoft-IIS	65
Zscaler proxy	58
Tengine	47
openresty	36
AkamaiGHost	35
CloudFront	25

Last updated 46 minutes ago

Top Operating Systems Seen

OS Name	▼ Count
Linux	7,392
Mac OSX	2,504
Enterprise Linux	2,503
iOS	1,890
Windows	902
Android	514
Chromium	93
Solaris	87
SunOS	87
FreeBSD	73

Last updated 46 minutes ago

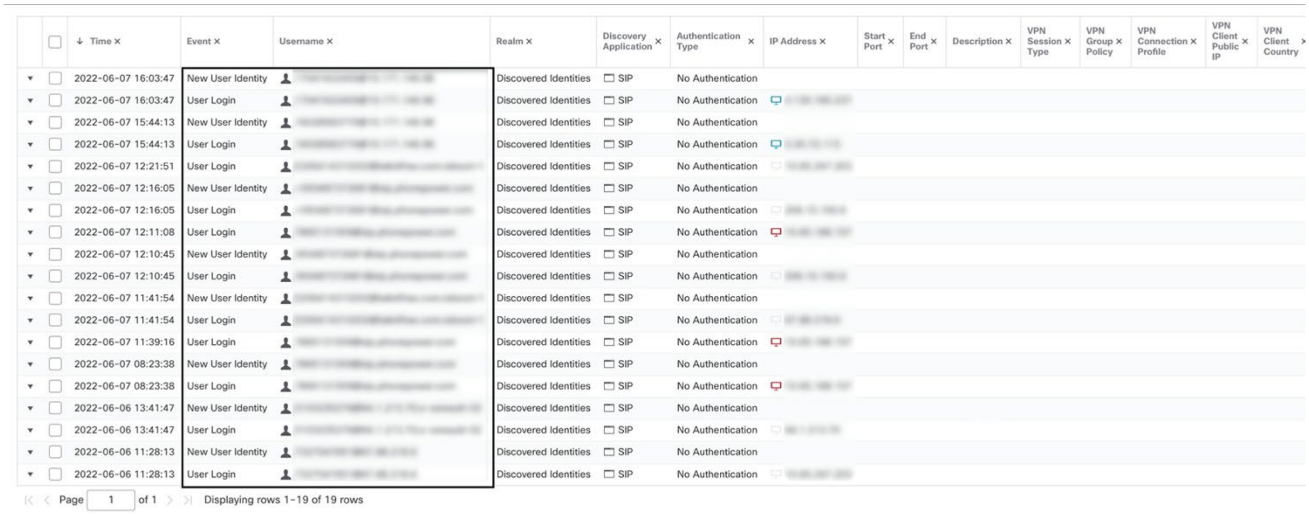
Daily OS counts also help provide a rough number of how many attended the event for that day. However, the wireless session lease was only three hours, which makes it difficult to make more precise daily OS counts. The same user connected to RSAC Wi-Fi could show multiple counts in one day. It is recommended to configure a wireless lease of more than one day to help correlate events for a user the next day.

These statistics are for a public Wi-Fi, which explains why the "Top Server Applications Seen" counts are so low.

The "Risky Applications with Low Business Relevance" count places Facebook at the top, but at events like RSAC, Facebook and other social media are often used as business promotion tools.

Discovered User Activities

Firepower detected and generated events for many user activities and their details in the network. These activity details were used to identify non-encrypted Email, VoIP (SIP) and File transfers communications and revealed user credentials and actual audio calls. All this was done in collaboration with NetWitness®. Firepower was able to provide user activity details and we were able to retrieve actual data traffic from NetWitness®.

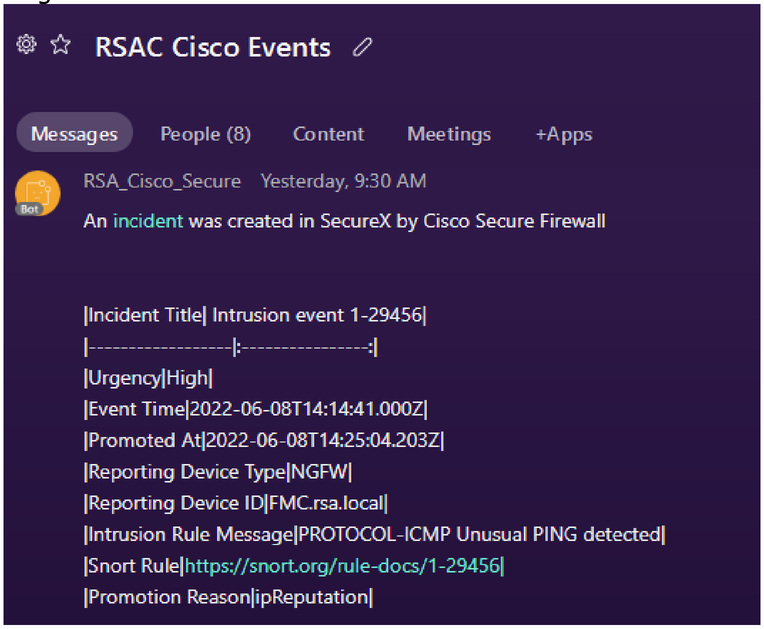


	☐	↓ Time ×	Event ×	Username ×	Realm ×	Discovery Application ×	Authentication Type ×	IP Address ×	Start Port ×	End Port ×	Description ×	VPN Session Type ×	VPN Group Policy ×	VPN Connection Profile ×	VPN Client Public IP ×	VPN Client Country ×
▾	☐	2022-06-07 16:03:47	New User Identity	[redacted]	Discovered Identities	SIP	No Authentication									
▾	☐	2022-06-07 16:03:47	User Login	[redacted]	Discovered Identities	SIP	No Authentication	[redacted]								
▾	☐	2022-06-07 15:44:13	New User Identity	[redacted]	Discovered Identities	SIP	No Authentication									
▾	☐	2022-06-07 15:44:13	User Login	[redacted]	Discovered Identities	SIP	No Authentication	[redacted]								
▾	☐	2022-06-07 12:21:51	User Login	[redacted]	Discovered Identities	SIP	No Authentication	[redacted]								
▾	☐	2022-06-07 12:16:05	New User Identity	[redacted]	Discovered Identities	SIP	No Authentication									
▾	☐	2022-06-07 12:16:05	User Login	[redacted]	Discovered Identities	SIP	No Authentication	[redacted]								
▾	☐	2022-06-07 12:11:08	User Login	[redacted]	Discovered Identities	SIP	No Authentication	[redacted]								
▾	☐	2022-06-07 12:10:45	New User Identity	[redacted]	Discovered Identities	SIP	No Authentication									
▾	☐	2022-06-07 12:10:45	User Login	[redacted]	Discovered Identities	SIP	No Authentication	[redacted]								
▾	☐	2022-06-07 11:41:54	New User Identity	[redacted]	Discovered Identities	SIP	No Authentication									
▾	☐	2022-06-07 11:41:54	User Login	[redacted]	Discovered Identities	SIP	No Authentication	[redacted]								
▾	☐	2022-06-07 11:39:16	User Login	[redacted]	Discovered Identities	SIP	No Authentication	[redacted]								
▾	☐	2022-06-07 08:23:38	New User Identity	[redacted]	Discovered Identities	SIP	No Authentication									
▾	☐	2022-06-07 08:23:38	User Login	[redacted]	Discovered Identities	SIP	No Authentication	[redacted]								
▾	☐	2022-06-06 13:41:47	New User Identity	[redacted]	Discovered Identities	SIP	No Authentication									
▾	☐	2022-06-06 13:41:47	User Login	[redacted]	Discovered Identities	SIP	No Authentication	[redacted]								
▾	☐	2022-06-06 11:28:13	New User Identity	[redacted]	Discovered Identities	SIP	No Authentication									
▾	☐	2022-06-06 11:28:13	User Login	[redacted]	Discovered Identities	SIP	No Authentication	[redacted]								

Page 1 of 1 Displaying rows 1–19 of 19 rows

Stranger Pings

In the RSAC SOC, we are always on alert for indicators that a user is attacking other users within the network or evidence that network is being used to attack the Internet. The SOC had over 365 alerts about non-standard ICMP traffic being sent to known malicious external IP addresses.

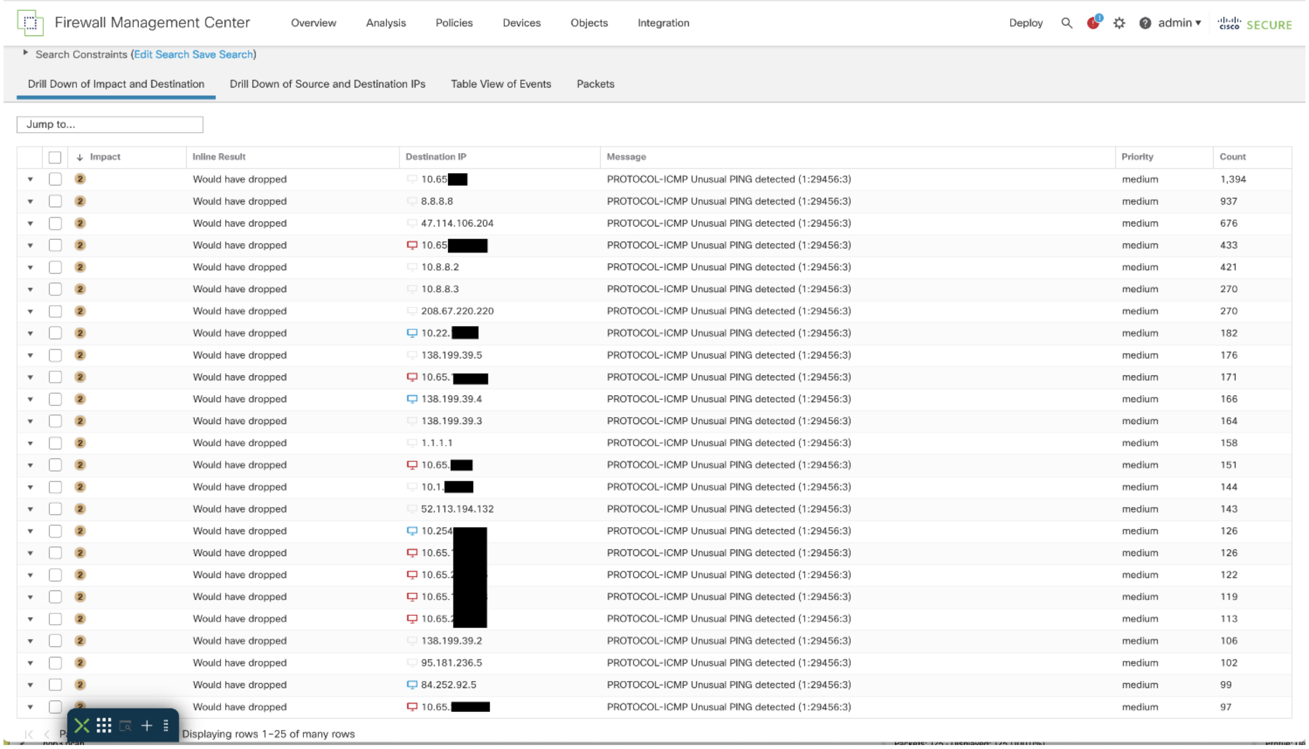


RSA_Cisco_Secure Yesterday, 9:30 AM

An incident was created in SecureX by Cisco Secure Firewall

Incident Title	Intrusion event 1-29456
Urgency	High
Event Time	2022-06-08T14:14:41.000Z
Promoted At	2022-06-08T14:25:04.203Z
Reporting Device Type	NGFW
Reporting Device ID	FMC.rsa.local
Intrusion Rule Message	PROTOCOL-ICMP Unusual PING detected
Snort Rule	https://snort.org/rule-docs/1-29456
Promotion Reason	ipReputation

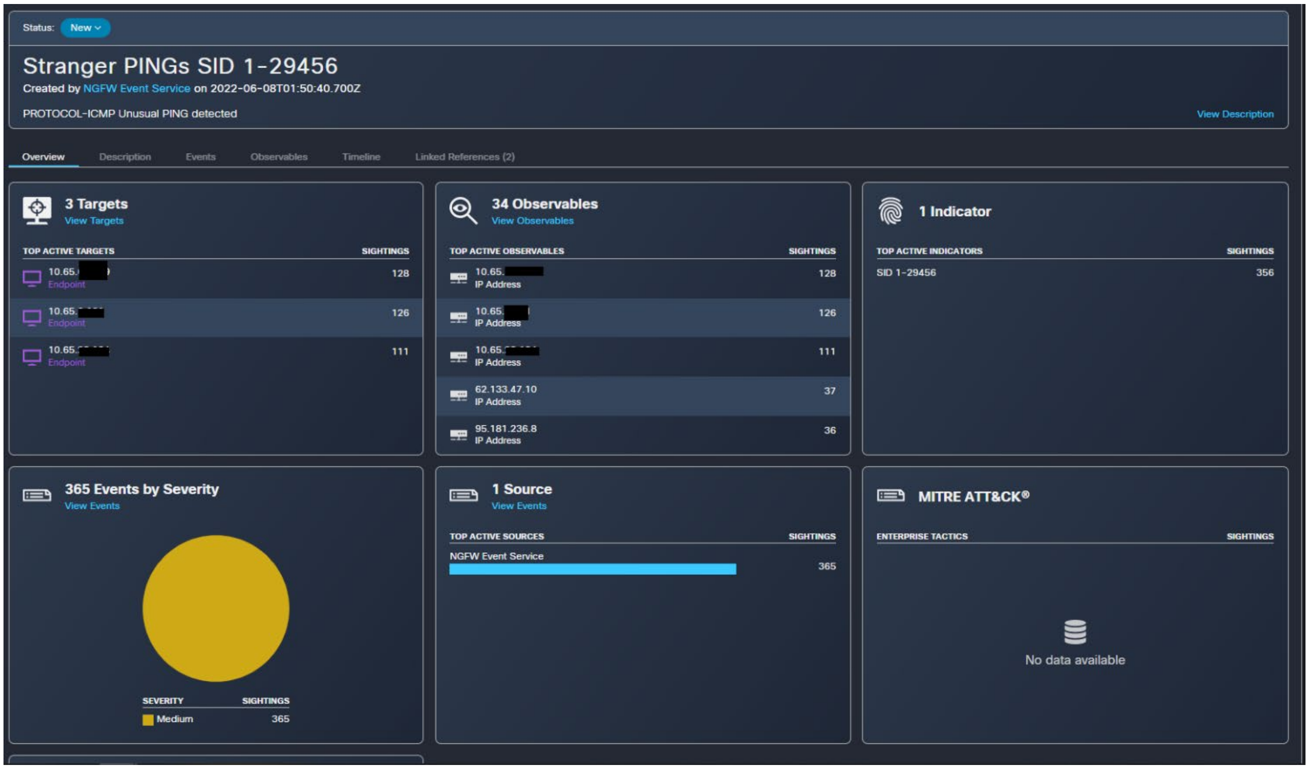
All of them involved one or more of the same three SRC IPs. These IPs had also been seen targeting internal IPs with the same malformed traffic.


Firewall Management Center
Overview
Analysis
Policies
Devices
Objects
Integration
Deploy
admin ▾
cisco SECURE
Search Constraints (Edit Search Save Search)
Drill Down of Impact and Destination
Drill Down of Source and Destination IPs
Table View of Events
Packets
Jump to...

	☐	↓ Impact	Inline Result	Destination IP	Message	Priority	Count
▼	☐	2	Would have dropped	10.65[redacted]	PROTOCOL-ICMP Unusual PING detected (1:29456:3)	medium	1,394
▼	☐	2	Would have dropped	8.8.8.8	PROTOCOL-ICMP Unusual PING detected (1:29456:3)	medium	937
▼	☐	2	Would have dropped	47.114.106.204	PROTOCOL-ICMP Unusual PING detected (1:29456:3)	medium	676
▼	☐	2	Would have dropped	10.65[redacted]	PROTOCOL-ICMP Unusual PING detected (1:29456:3)	medium	433
▼	☐	2	Would have dropped	10.8.8.2	PROTOCOL-ICMP Unusual PING detected (1:29456:3)	medium	421
▼	☐	2	Would have dropped	10.8.8.3	PROTOCOL-ICMP Unusual PING detected (1:29456:3)	medium	270
▼	☐	2	Would have dropped	208.67.220.220	PROTOCOL-ICMP Unusual PING detected (1:29456:3)	medium	270
▼	☐	2	Would have dropped	10.22.[redacted]	PROTOCOL-ICMP Unusual PING detected (1:29456:3)	medium	182
▼	☐	2	Would have dropped	138.199.39.5	PROTOCOL-ICMP Unusual PING detected (1:29456:3)	medium	176
▼	☐	2	Would have dropped	10.65.[redacted]	PROTOCOL-ICMP Unusual PING detected (1:29456:3)	medium	171
▼	☐	2	Would have dropped	138.199.39.4	PROTOCOL-ICMP Unusual PING detected (1:29456:3)	medium	166
▼	☐	2	Would have dropped	138.199.39.3	PROTOCOL-ICMP Unusual PING detected (1:29456:3)	medium	164
▼	☐	2	Would have dropped	1.1.1.1	PROTOCOL-ICMP Unusual PING detected (1:29456:3)	medium	158
▼	☐	2	Would have dropped	10.65.[redacted]	PROTOCOL-ICMP Unusual PING detected (1:29456:3)	medium	151
▼	☐	2	Would have dropped	10.1.[redacted]	PROTOCOL-ICMP Unusual PING detected (1:29456:3)	medium	144
▼	☐	2	Would have dropped	52.113.194.132	PROTOCOL-ICMP Unusual PING detected (1:29456:3)	medium	143
▼	☐	2	Would have dropped	10.254[redacted]	PROTOCOL-ICMP Unusual PING detected (1:29456:3)	medium	126
▼	☐	2	Would have dropped	10.65.[redacted]	PROTOCOL-ICMP Unusual PING detected (1:29456:3)	medium	126
▼	☐	2	Would have dropped	10.65.[redacted]	PROTOCOL-ICMP Unusual PING detected (1:29456:3)	medium	122
▼	☐	2	Would have dropped	10.65.[redacted]	PROTOCOL-ICMP Unusual PING detected (1:29456:3)	medium	119
▼	☐	2	Would have dropped	10.65.[redacted]	PROTOCOL-ICMP Unusual PING detected (1:29456:3)	medium	113
▼	☐	2	Would have dropped	138.199.39.2	PROTOCOL-ICMP Unusual PING detected (1:29456:3)	medium	106
▼	☐	2	Would have dropped	95.181.236.5	PROTOCOL-ICMP Unusual PING detected (1:29456:3)	medium	102
▼	☐	2	Would have dropped	84.252.92.5	PROTOCOL-ICMP Unusual PING detected (1:29456:3)	medium	99
▼	☐	2	Would have dropped	10.65.[redacted]	PROTOCOL-ICMP Unusual PING detected (1:29456:3)	medium	97

Displaying rows 1–25 of many rows

Investigation in SecureX revealed that many of the destination IPs for these malformed pings were contacted by two or all three of these sources.


Status: New

Stranger PINGs SID 1-29456

Created by NGFW Event Service on 2022-06-08T01:50:40.700Z

PROTOCOL-ICMP Unusual PING detected

3 Targets

TOP ACTIVE TARGETS	SIGHTINGS
10.65.[redacted] Endpoint	128
10.65.[redacted] Endpoint	126
10.65.[redacted] Endpoint	111

34 Observables

TOP ACTIVE OBSERVABLES	SIGHTINGS
10.65.[redacted] IP Address	128
10.65.[redacted] IP Address	126
10.65.[redacted] IP Address	111
62.133.47.10 IP Address	37
95.181.236.8 IP Address	36

1 Indicator

TOP ACTIVE INDICATORS	SIGHTINGS
SID 1-29456	356

365 Events by Severity

SEVERITY	SIGHTINGS
🟨 Medium	365

1 Source

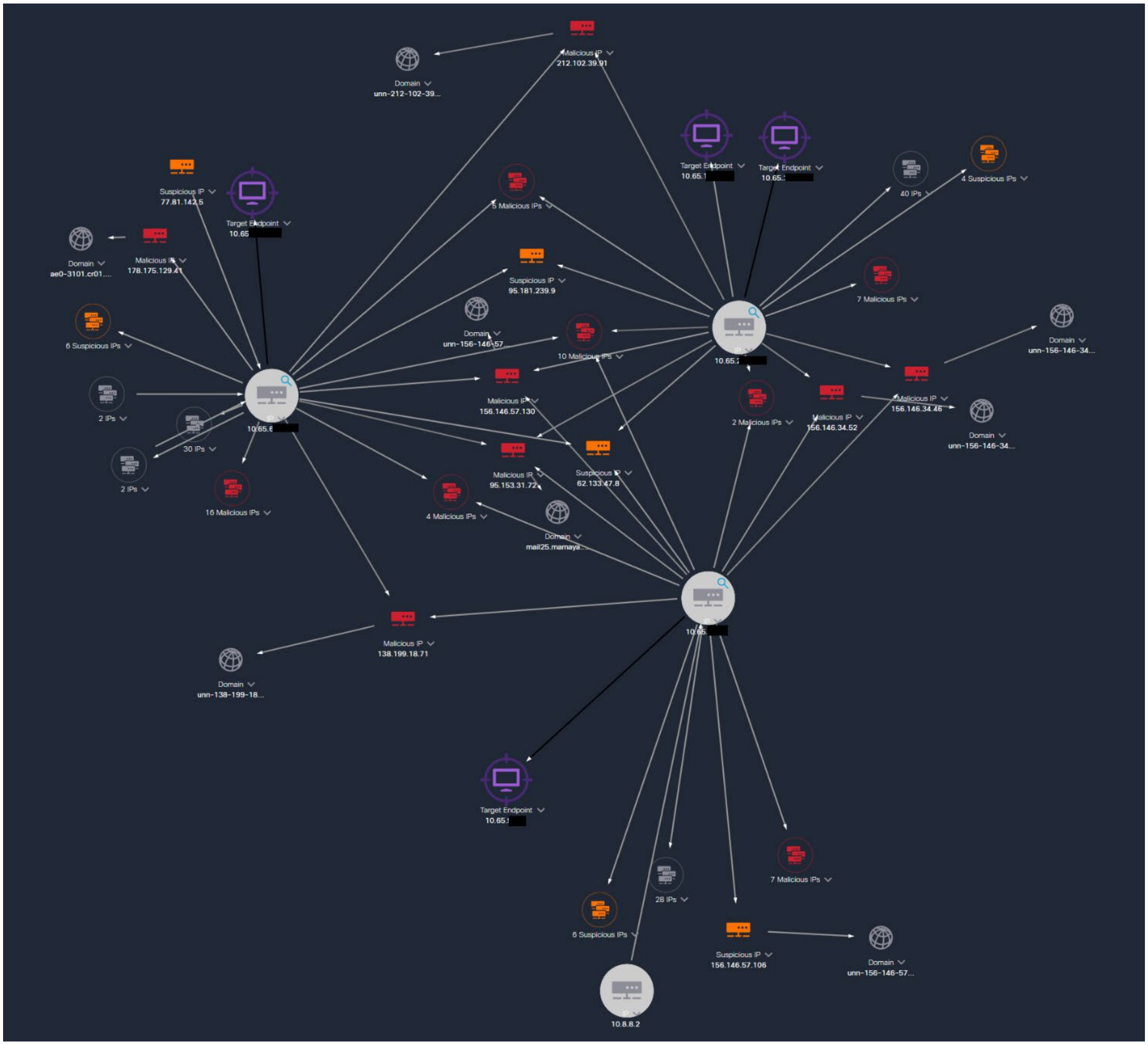
TOP ACTIVE SOURCES	SIGHTINGS
NGFW Event Service	365

MITRE ATT&CK®

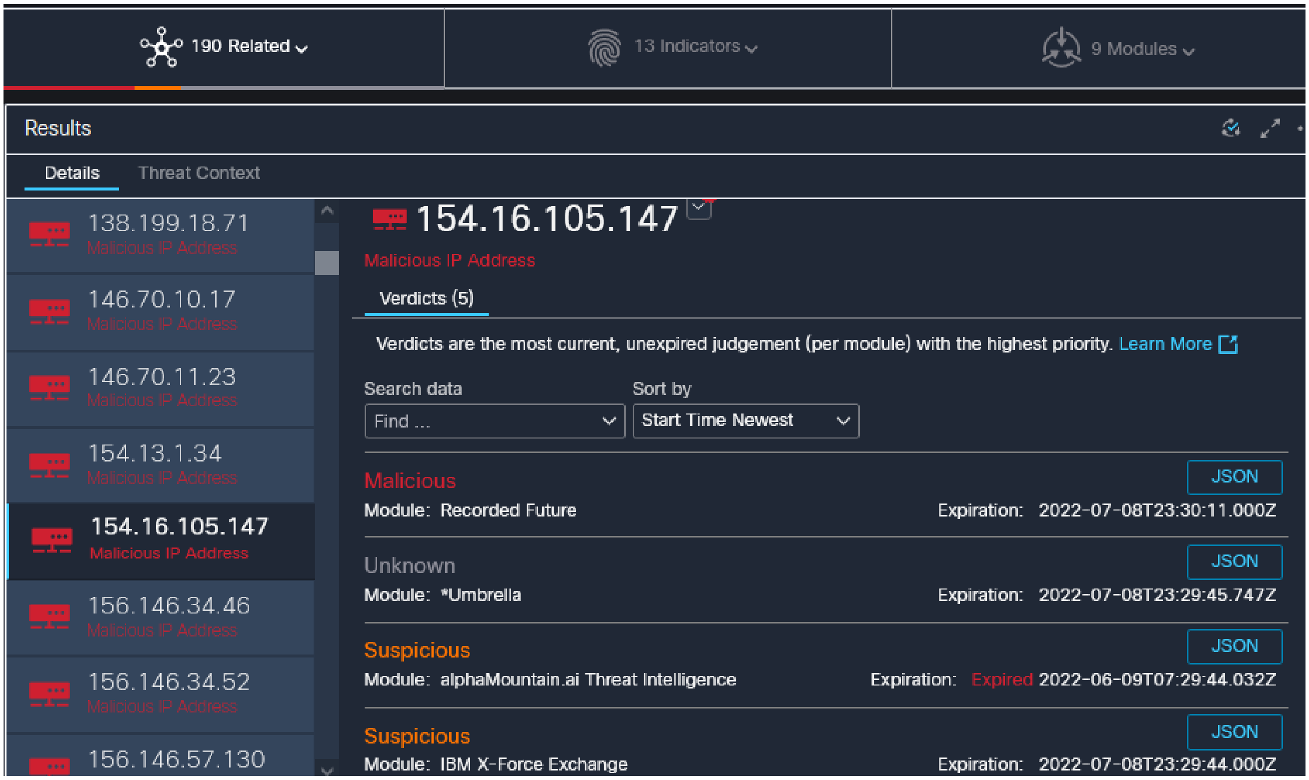
ENTERPRISE TACTICS	SIGHTINGS

No data available

Network analysis revealed that all three IPs have separate MAC addresses, so are not a single device getting new DHCP. Packet analysis revealed extra content in normally unused fields in the ICMP structure.


Malicious IP
212.102.39.91
Domain
unn-212-102-39...
Suspicious IP
77.81.142.5
Target Endpoint
10.65[redacted]
Domain
ae0-3101.cr01....
Malicious IP
178.175.129.41
6 Suspicious IPs
2 IPs
30 IPs
2 IPs
16 Malicious IPs
IP
10.65.6[redacted]
5 Malicious IPs
Suspicious IP
95.181.239.9
Domain
unn-156-146-57...
10 Malicious IPs
Malicious IP
156.146.57.130
Malicious IP
95.153.31.72
Suspicious IP
62.133.47.8
4 Malicious IPs
Domain
mail25.mamaya....
Target Endpoint
10.65.1[redacted]
Target Endpoint
10.65.[redacted]
40 IPs
4 Suspicious IPs
7 Malicious IPs
IP
10.65.2[redacted]
Domain
unn-156-146-34...
2 Malicious IPs
Malicious IP
156.146.34.52
Malicious IP
156.146.34.46
Domain
unn-156-146-34...
Malicious IP
138.199.18.71
Domain
unn-138-199-18...
IP
10.65.[redacted]
Target Endpoint
10.65.[redacted]
28 IPs
7 Malicious IPs
6 Suspicious IPs
Suspicious IP
156.146.57.106
Domain
unn-156-146-57...
IP
10.8.8.2

The investigation revealed known threat intelligence about the destinations and found over a hundred related artifacts with a dozen indicators of maliciousness.



138.199.18.71 Malicious IP Address
146.70.10.17 Malicious IP Address
146.70.11.23 Malicious IP Address
154.13.1.34 Malicious IP Address
154.16.105.147 Malicious IP Address
156.146.34.46 Malicious IP Address
156.146.34.52 Malicious IP Address
156.146.57.130

154.16.105.147

Malicious IP Address

Verdicts (5)

Verdicts are the most current, unexpired judgement (per module) with the highest priority. Learn More

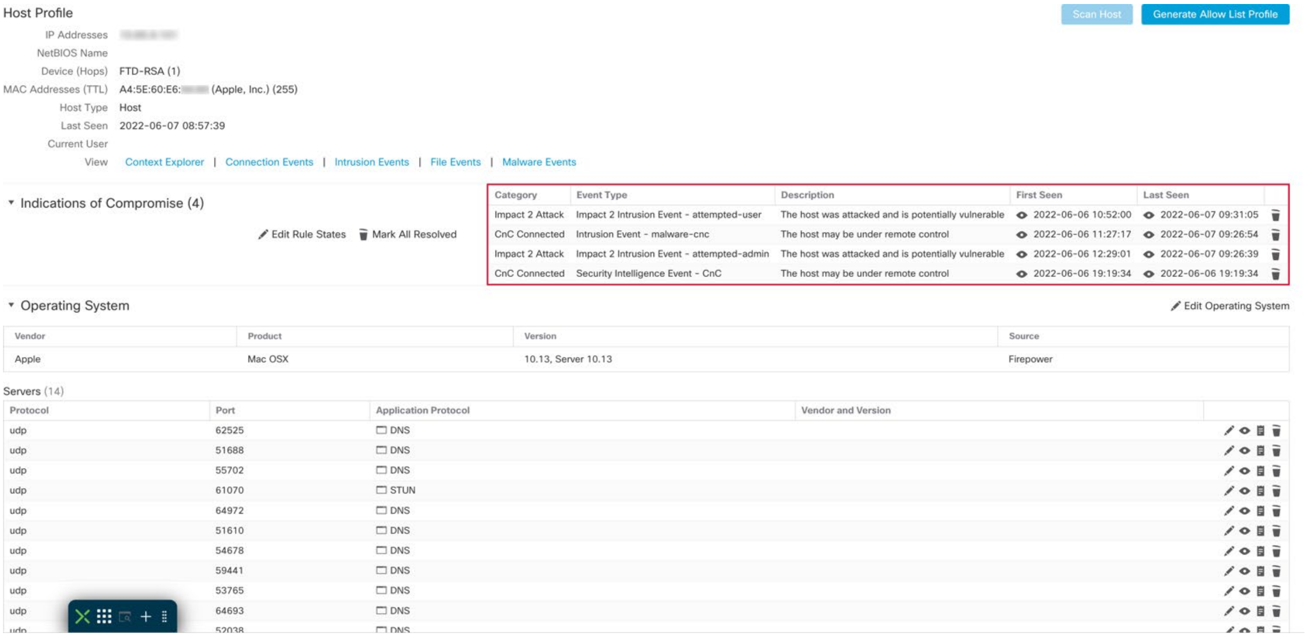
Search data: Find ...

Sort by: Start Time Newest

Verdict	Module	Expiration
Malicious	Recorded Future	2022-07-08T23:30:11.000Z
Unknown	*Umbrella	2022-07-08T23:29:45.747Z
Suspicious	alphaMountain.ai Threat Intelligence	Expired 2022-06-09T07:29:44.032Z
Suspicious	IBM X-Force Exchange	2022-07-08T23:29:44.000Z

The investigation did not indicate that the pings were part of an attack within or from the network and was closed.

Using the same notification method of Slack/Webex Teams we noticed the one of the same source IP's involved in a slew of intrusion events related to Malware and CnC. To gain contextual insights on the device we were able to pull up the host profile on the Firewall Management Center and realized this apple machine has been involved in other malicious events.



Host Profile

IP Addresses	[redacted]
NetBIOS Name	
Device (Hops)	FTD-RSA (1)
MAC Addresses (TTL)	A4:5E:60:E6:[redacted] (Apple, Inc.) (255)
Host Type	Host
Last Seen	2022-06-07 08:57:39
Current User	
View	Context Explorer | Connection Events | Intrusion Events | File Events | Malware Events

▾ Indications of Compromise (4)

Category	Event Type	Description	First Seen	Last Seen
Impact 2 Attack	Impact 2 Intrusion Event - attempted-user	The host was attacked and is potentially vulnerable	2022-06-06 10:52:00	2022-06-07 09:31:05
CnC Connected	Intrusion Event - malware-cnc	The host may be under remote control	2022-06-06 11:27:17	2022-06-07 09:26:54
Impact 2 Attack	Impact 2 Intrusion Event - attempted-admin	The host was attacked and is potentially vulnerable	2022-06-06 12:29:01	2022-06-07 09:26:39
CnC Connected	Security Intelligence Event - CnC	The host may be under remote control	2022-06-06 19:19:34	2022-06-06 19:19:34

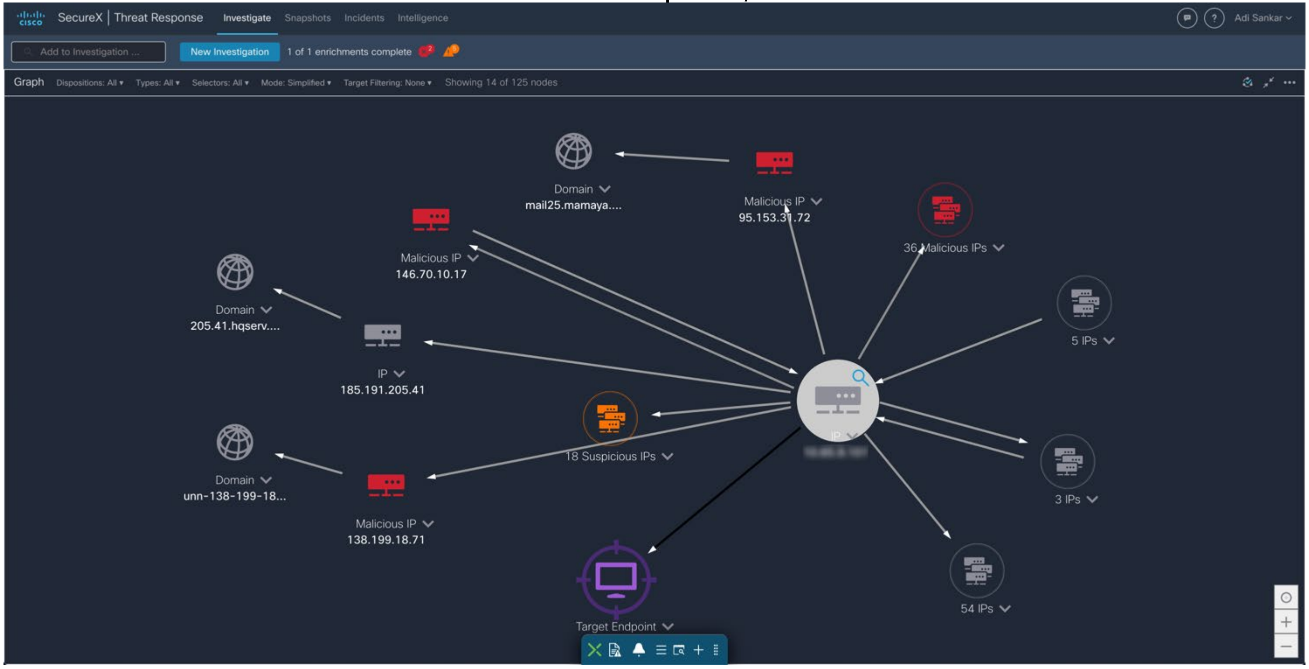
▾ Operating System

Vendor	Product	Version	Source
Apple	Mac OSX	10.13, Server 10.13	Firepower

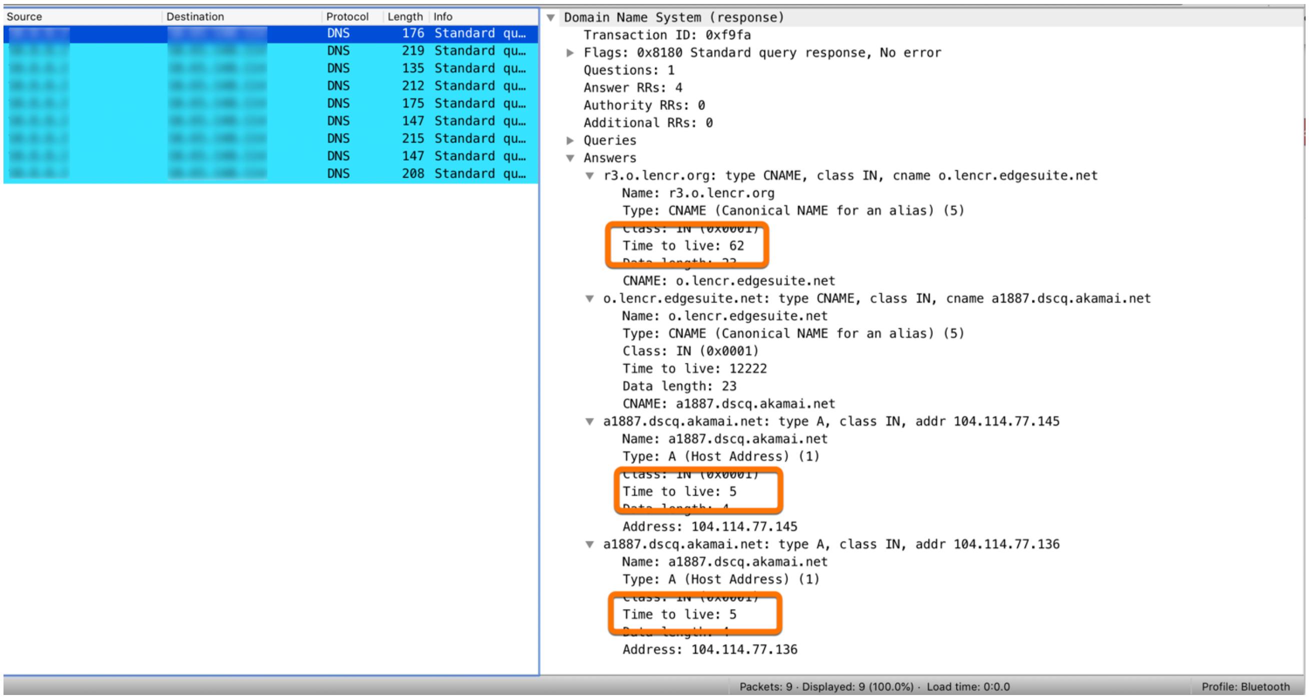
Servers (14)

Protocol	Port	Application Protocol	Vendor and Version
udp	62525	DNS	
udp	51688	DNS	
udp	55702	DNS	
udp	61070	STUN	
udp	64972	DNS	
udp	51610	DNS	
udp	54678	DNS	
udp	59441	DNS	
udp	53765	DNS	
udp	64693	DNS	
udp	52038	DNS	

To gain broader visibility of what other artifacts this machine has been involved with we conducted an investigation in SecureX threat response. After investigating we can see that this host has had bidirectional communication with a CnC server and over 50 other suspicious/malicious IP's!



Now we wanted to understand why the machine had connected to so many different IP's. Pivoting from the host profile in Firewall Management Center into some of the other events we saw massive amounts of DNS Fast Flux alerts. This is a technique used by attackers to obfuscate what their real IP is. By downloading the packet capture from the Firewall, we could see the TTL in the DNS responses was very short allowing the attackers to rotate amongst a plethora of IP's making it harder to block the malicious communication.



Source	Destination	Protocol	Length	Info
[redacted]	[redacted]	DNS	176	Standard qu…
[redacted]	[redacted]	DNS	219	Standard qu…
[redacted]	[redacted]	DNS	135	Standard qu…
[redacted]	[redacted]	DNS	212	Standard qu…
[redacted]	[redacted]	DNS	175	Standard qu…
[redacted]	[redacted]	DNS	147	Standard qu…
[redacted]	[redacted]	DNS	215	Standard qu…
[redacted]	[redacted]	DNS	147	Standard qu…
[redacted]	[redacted]	DNS	208	Standard qu…

```
▼ Domain Name System (response)
    Transaction ID: 0xf9fa
  ▶ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 4
    Authority RRs: 0
    Additional RRs: 0
  ▶ Queries
  ▼ Answers
    ▼ r3.o.lencr.org: type CNAME, class IN, cname o.lencr.edgesuite.net
        Name: r3.o.lencr.org
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 62
        Data length: 23
        CNAME: o.lencr.edgesuite.net
    ▼ o.lencr.edgesuite.net: type CNAME, class IN, cname a1887.dscq.akamai.net
        Name: o.lencr.edgesuite.net
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 12222
        Data length: 23
        CNAME: a1887.dscq.akamai.net
    ▼ a1887.dscq.akamai.net: type A, class IN, addr 104.114.77.145
        Name: a1887.dscq.akamai.net
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 5
        Data length: 4
        Address: 104.114.77.145
    ▼ a1887.dscq.akamai.net: type A, class IN, addr 104.114.77.136
        Name: a1887.dscq.akamai.net
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 5
        Data length: 4
        Address: 104.114.77.136
```

Packets: 9 · Displayed: 9 (100.0%) · Load time: 0:0.0   Profile: Bluetooth

After all the information was collected the investigation was closed under the assumption that one of the booths was conducting a demo as we continued to see these alerts from the same source IP every day.

File Transfers

File monitoring and analysis yields valuable network monitoring information, as well as providing insight into the types of users in the network. The large number of locally spread malware files indicate that someone was downloading these files locally from inside the network.

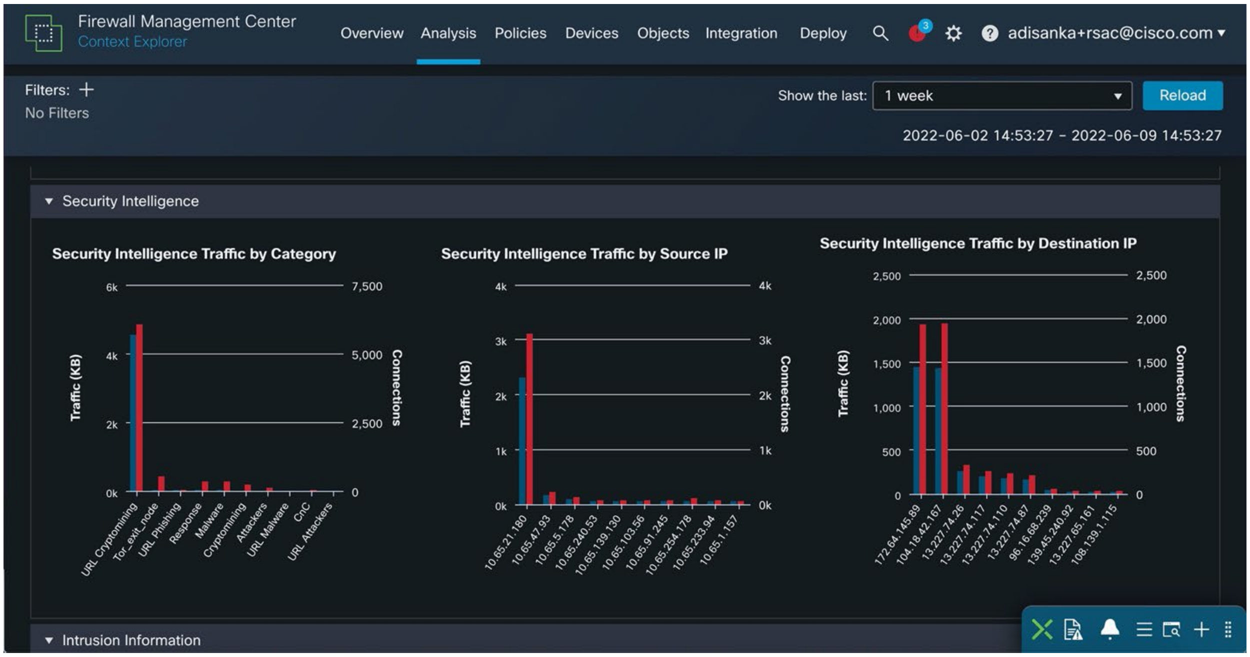
If it was not already known to the SOC who perpetrated the dump, these malware files could also provide other information such as:

- User education covering email security (what to click and what to not click.)
- Target analysis: Is the company network being targeted specifically with these files?

Returning to our RSAC findings, most malware files these days spread with HTTPS, and the RSAC SOC didn't enable any SSL decryption; this may explain why the malware/malicious files count was so low. Still, with the 22 percent of traffic being over HTTP, we were able to catch a good number of these files with the help of our Cisco Secure Cloud Lookup and Talos Intelligence integration.

Intrusion Information

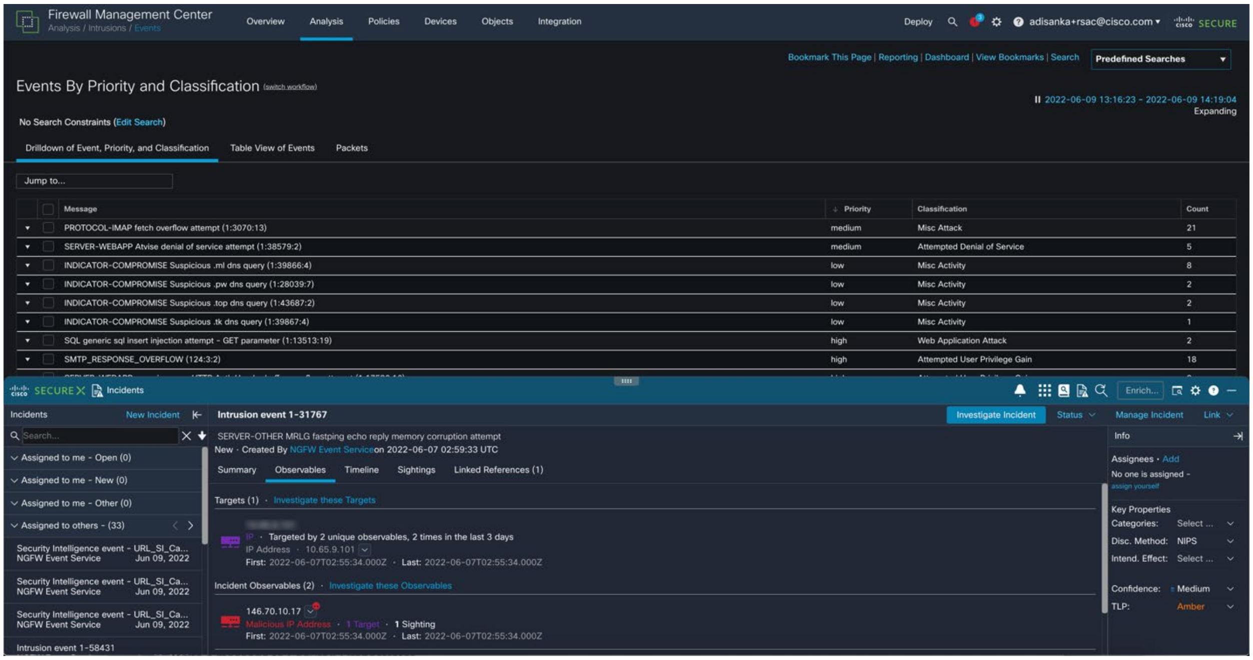
During the conference, several intrusion events were recorded by Firepower. Automated event analysis correlated threat events with contextual host profile data, to identify IPS events requiring immediate investigation. Whenever a working exploit targeted a vulnerable host on the guest network, an Impact 1 event was raised. Intrusion events with the Impact 1 flag are automatically promoted to SecureX incidents and can be investigated directly from the SecureX ribbon in FMC. For the RSAC SOC team, this helped cut through the noise and focus attention to save precious time.



Filters: No Filters

Show the last: 1 week

2022-06-02 14:53:27 - 2022-06-09 14:53:27



Events By Priority and Classification (switch workflow)

No Search Constraints (Edit Search)

2022-06-09 13:16:23 - 2022-06-09 14:19:04
Expanding

Message	Priority	Classification	Count
PROTOCOL-IMAP fetch overflow attempt (1:3070:13)	medium	Misc Attack	21
SERVER-WEBAPP Atvise denial of service attempt (1:38579:2)	medium	Attempted Denial of Service	5
INDICATOR-COMPROMISE Suspicious .ml dns query (1:39866:4)	low	Misc Activity	8
INDICATOR-COMPROMISE Suspicious .pw dns query (1:28039:7)	low	Misc Activity	2
INDICATOR-COMPROMISE Suspicious .top dns query (1:43687:2)	low	Misc Activity	2
INDICATOR-COMPROMISE Suspicious .tk dns query (1:39867:4)	low	Misc Activity	1
SQL generic sql insert injection attempt - GET parameter (1:13513:19)	high	Web Application Attack	2
SMTP_RESPONSE_OVERFLOW (124:3:2)	high	Attempted User Privilege Gain	18

Incidents

- Assigned to me - Open (0)
- Assigned to me - New (0)
- Assigned to me - Other (0)
- Assigned to others - (33)

Security Intelligence event - URL_SI_Ca...
NGFW Event Service Jun 09, 2022

Security Intelligence event - URL_SI_Ca...
NGFW Event Service Jun 09, 2022

Security Intelligence event - URL_SI_Ca...
NGFW Event Service Jun 09, 2022

Intrusion event 1-58431

Intrusion event 1-31767

SERVER-OTHER MRLG fastping echo reply memory corruption attempt
New · Created By NGFW Event Serviceon 2022-06-07 02:59:33 UTC

Targets (1) · Investigate these Targets

[redacted]
IP · Targeted by 2 unique observables, 2 times in the last 3 days
IP Address · 10.65.9.101
First: 2022-06-07T02:55:34.000Z · Last: 2022-06-07T02:55:34.000Z

Incident Observables (2) · Investigate these Observables

146.70.10.17
Malicious IP Address · 1 Target · 1 Sighting
First: 2022-06-07T02:55:34.000Z · Last: 2022-06-07T02:55:34.000Z

Info

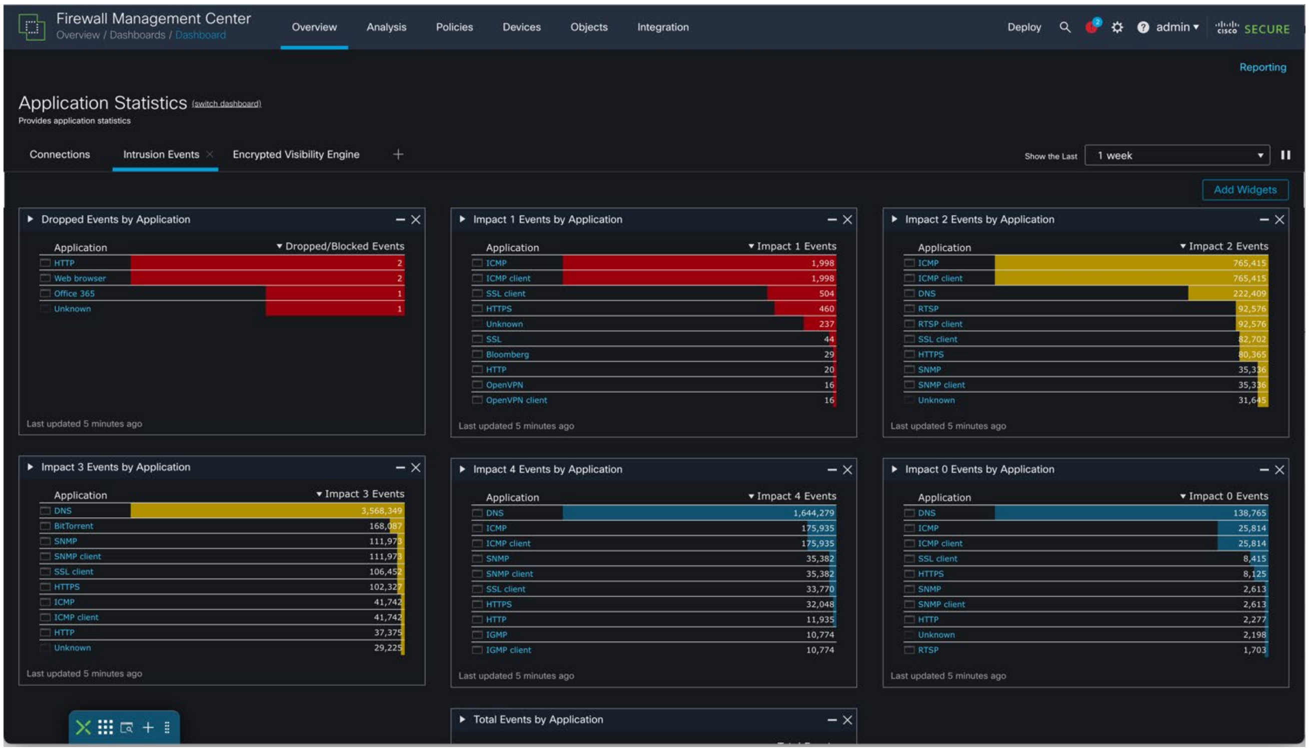
Assignees · Add
No one is assigned - assign yourself

Key Properties
Categories: Select ...
Disc. Method: NIPS
Intend. Effect: Select ...

Confidence: Medium
TLP: Amber

Many "user privilege gain" attacks were detected, which indicated an attacker was trying to gain access to demo and other networking devices. This also calls attention to why you should never use default passwords.

Multiple intrusion events were categorized as high priority.



Application Statistics (switch dashboard)
Provides application statistics

Show the Last 1 week

Dropped Events by Application

Application	Dropped/Blocked Events
HTTP	2
Web browser	2
Office 365	1
Unknown	1

Last updated 5 minutes ago

Impact 1 Events by Application

Application	Impact 1 Events
ICMP	1,998
ICMP client	1,998
SSL client	504
HTTPS	460
Unknown	237
SSL	44
Bloomberg	29
HTTP	20
OpenVPN	16
OpenVPN client	16

Last updated 5 minutes ago

Impact 2 Events by Application

Application	Impact 2 Events
ICMP	765,415
ICMP client	765,415
DNS	222,409
RTSP	92,576
RTSP client	92,576
SSL client	82,702
HTTPS	80,365
SNMP	35,336
SNMP client	35,336
Unknown	31,645

Last updated 5 minutes ago

Impact 3 Events by Application

Application	Impact 3 Events
DNS	3,568,349
BitTorrent	168,087
SNMP	111,973
SNMP client	111,973
SSL client	106,452
HTTPS	102,327
ICMP	41,742
ICMP client	41,742
HTTP	37,375
Unknown	29,225

Last updated 5 minutes ago

Impact 4 Events by Application

Application	Impact 4 Events
DNS	1,644,279
ICMP	175,935
ICMP client	175,935
SNMP	35,382
SNMP client	35,382
SSL client	33,770
HTTPS	32,048
HTTP	11,935
IGMP	10,774
IGMP client	10,774

Last updated 5 minutes ago

Impact 0 Events by Application

Application	Impact 0 Events
DNS	138,765
ICMP	25,814
ICMP client	25,814
SSL client	8,415
HTTPS	8,125
SNMP	2,613
SNMP client	2,613
HTTP	2,277
Unknown	2,198
RTSP	1,703

Last updated 5 minutes ago

Total Events by Application

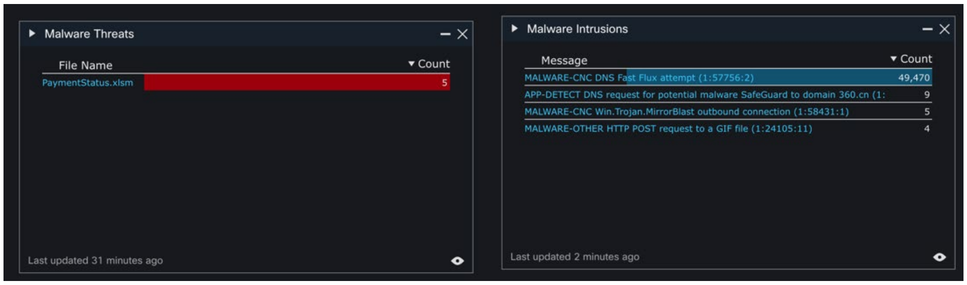
Malware Threats

Cisco Firepower Management Center (FMC) malware event dashboard showed us some serious malware intrusions, as well as threats live from the RSAC network.

Secure Malware Analytics (formerly Threat Grid) was used in a combination with the Cisco FMC to learn more details about the malware threats, reflected in the "Malware Threats" dashboard as analyzed files. Combining different security products and making them talk to each other creates a more secure and safe environment, along with the help of correlation from different products and their analysis. At times, a single tool may report a completely new "first-time-seen" file as a risk-free file. However, leveraging a combination of security tools can make it possible to dig deeper to see what is really going on.

A huge number of DNS request-based intrusions were seen in the network. Cisco Umbrella can be used along with other security devices to stop these types of attacks, as most of the DNS traffic is cleaned by Cisco Umbrella before it even enters our network/security devices or next-generation firewall devices.

Command-and-control events remain the top type of intrusion events at RSAC in 2022. Command-and-control communications are also used extensively for doing quiet cryptomining in the background of infected devices.



Malware Threats

File Name	▾ Count
PaymentStatus.xlsm	5

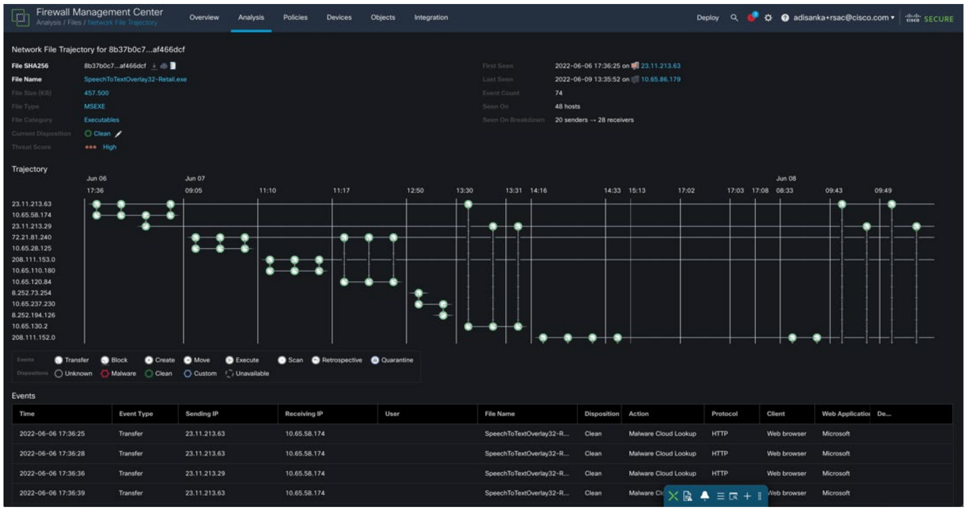
Last updated 31 minutes ago

Malware Intrusions

Message	▾ Count
MALWARE-CNC DNS Fast Flux attempt (1:57756:2)	49,470
APP-DETECT DNS request for potential malware SafeGuard to domain 360.cn (1:	9
MALWARE-CNC Win.Trojan.MirrorBlast outbound connection (1:58431:1)	5
MALWARE-OTHER HTTP POST request to a GIF file (1:24105:11)	4

Last updated 2 minutes ago

Using Firepower Management File Trajectory we are able to see which hosts are specifically targeted by mapping how the file traversed the network, identifying passing hosts on a time series graph that details potentially infected IPs and the frequency which those hosts were visited. Additionally we can see telemetry on malware signature itself, including threat score, first and last occurrences, hash signature and current disposition.



Firewall Management Center
Analysis / Files / Network File Trajectory
Overview
Analysis
Policies
Devices
Objects
Integration
Deploy
adisanka+rsac@cisco.com ▾
cisco SECURE

Network File Trajectory for 8b37b0c7...af466dcf

File SHA256	8b37b0c7...af466dcf
File Name	SpeechToTextOverlay32-Retail.exe
File Size (KB)	457.500
File Type	MSEXE
File Category	Executables
Current Disposition	○ Clean
Threat Score	●●● High
First Seen	2022-06-06 17:36:25 on 23.11.213.63
Last Seen	2022-06-09 13:35:52 on 10.65.86.179
Event Count	74
Seen On	48 hosts
Seen On Breakdown	20 senders → 28 receivers

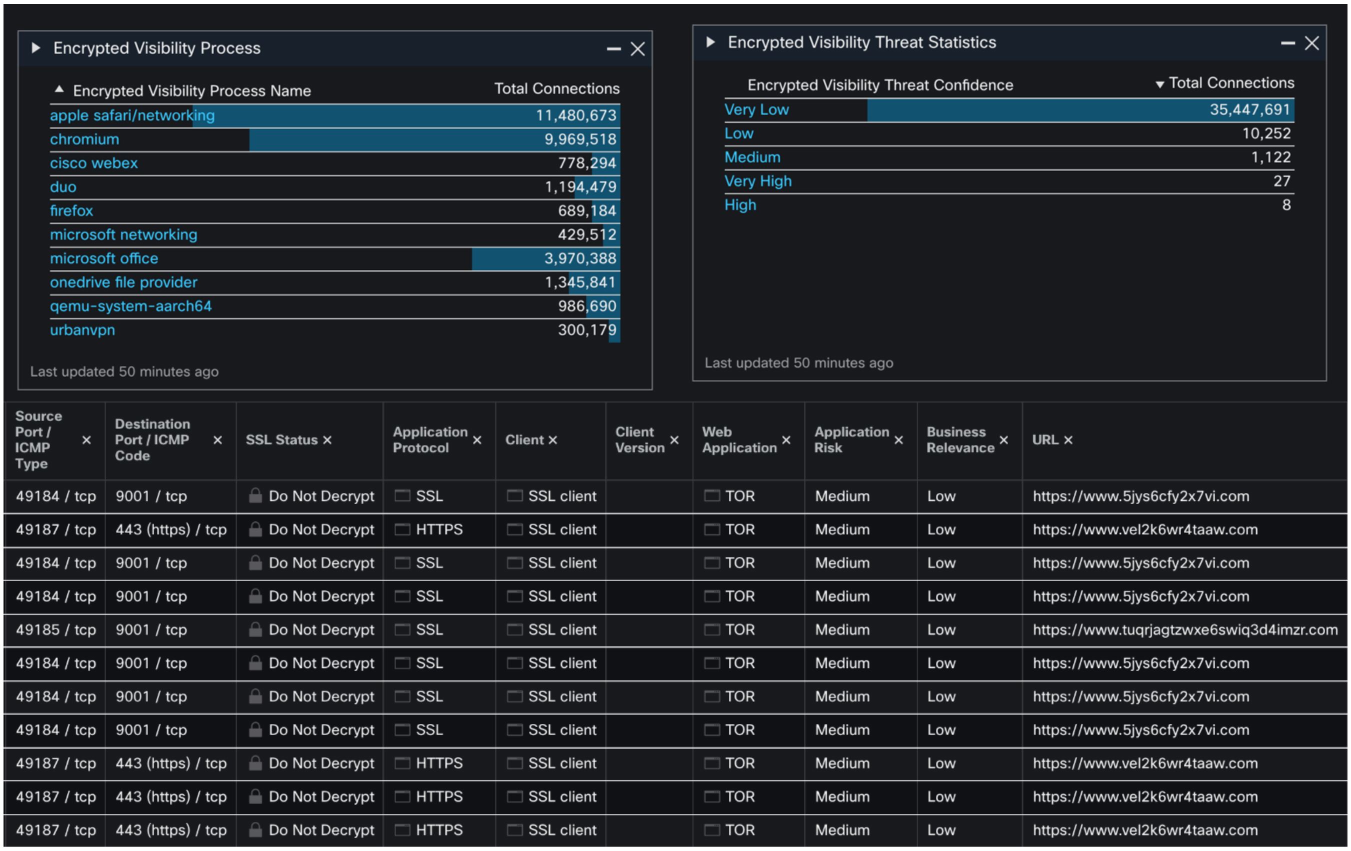
Trajectory

Events

Time	Event Type	Sending IP	Receiving IP	User	File Name	Disposition	Action	Protocol	Client	Web Applicatioı	De...
2022-06-06 17:36:25	Transfer	23.11.213.63	10.65.58.174		SpeechToTextOverlay32-R...	Clean	Malware Cloud Lookup	HTTP	Web browser	Microsoft	
2022-06-06 17:36:28	Transfer	23.11.213.63	10.65.58.174		SpeechToTextOverlay32-R...	Clean	Malware Cloud Lookup	HTTP	Web browser	Microsoft	
2022-06-06 17:36:36	Transfer	23.11.213.29	10.65.58.174		SpeechToTextOverlay32-R...	Clean	Malware Cloud Lookup	HTTP	Web browser	Microsoft	
2022-06-06 17:36:39	Transfer	23.11.213.63	10.65.58.174		SpeechToTextOverlay32-R...	Clean	Malware Cl		Web browser	Microsoft	

Firepower Encrypted Visibility Engine (EVE)

Firepower system also gained visibility into an encrypted session without needing to decrypt it using the Encrypted Visibility Engine (EVE) feature. The engine fingerprints and analyzes encrypted traffic and provides more visibility into encrypted traffic, including protocols such as TLS and QUIC and provides a list of all the applications, micro-apps and processes used within those applications. Firepower also tries to find any potential encrypted vulnerable traffic within that encrypted application traffic and assigns a Threat Confidence Score (0 –100) and categorizes them (Very Low – High). At RSA, Firepower EVE did find TOR client traffic along with URL's which had a Threat Confidence of 90 and was marked as potentially malicious communication.



Encrypted Visibility Process

Encrypted Visibility Process Name	Total Connections
apple safari/networking	11,480,673
chromium	9,969,518
cisco webex	778,294
duo	1,194,479
firefox	689,184
microsoft networking	429,512
microsoft office	3,970,388
onedrive file provider	1,345,841
qemu-system-aarch64	986,690
urbanvpn	300,179

Last updated 50 minutes ago

Encrypted Visibility Threat Statistics

Encrypted Visibility Threat Confidence	Total Connections
Very Low	35,447,691
Low	10,252
Medium	1,122
Very High	27
High	8

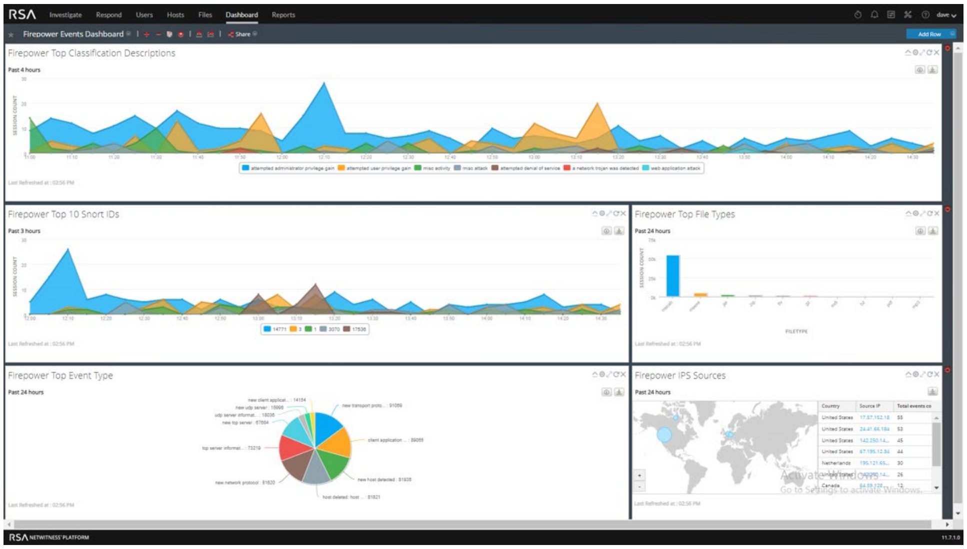
Last updated 50 minutes ago

Source Port / ICMP Type	Destination Port / ICMP Code	SSL Status	Application Protocol	Client	Client Version	Web Application	Application Risk	Business Relevance	URL
49184 / tcp	9001 / tcp	Do Not Decrypt	SSL	SSL client		TOR	Medium	Low	https://www.5jys6cfy2x7vi.com
49187 / tcp	443 (https) / tcp	Do Not Decrypt	HTTPS	SSL client		TOR	Medium	Low	https://www.vel2k6wr4taaw.com
49184 / tcp	9001 / tcp	Do Not Decrypt	SSL	SSL client		TOR	Medium	Low	https://www.5jys6cfy2x7vi.com
49184 / tcp	9001 / tcp	Do Not Decrypt	SSL	SSL client		TOR	Medium	Low	https://www.5jys6cfy2x7vi.com
49185 / tcp	9001 / tcp	Do Not Decrypt	SSL	SSL client		TOR	Medium	Low	https://www.tuqrjagtzwxe6swiq3d4imzr.com
49184 / tcp	9001 / tcp	Do Not Decrypt	SSL	SSL client		TOR	Medium	Low	https://www.5jys6cfy2x7vi.com
49184 / tcp	9001 / tcp	Do Not Decrypt	SSL	SSL client		TOR	Medium	Low	https://www.5jys6cfy2x7vi.com
49184 / tcp	9001 / tcp	Do Not Decrypt	SSL	SSL client		TOR	Medium	Low	https://www.5jys6cfy2x7vi.com
49187 / tcp	443 (https) / tcp	Do Not Decrypt	HTTPS	SSL client		TOR	Medium	Low	https://www.vel2k6wr4taaw.com
49187 / tcp	443 (https) / tcp	Do Not Decrypt	HTTPS	SSL client		TOR	Medium	Low	https://www.vel2k6wr4taaw.com
49187 / tcp	443 (https) / tcp	Do Not Decrypt	HTTPS	SSL client		TOR	Medium	Low	https://www.vel2k6wr4taaw.com

Firepower and NetWitness® Integration

The Cisco Event Streamer (also known as eStreamer) enables users to stream Firepower System events to external client applications. You can stream host, discovery, correlation, compliance white list, intrusion, user activity, file, malware, and connection data from a Management Center. This year at RSA we took the opportunity to integrate eStreamer data with NetWitness® to provide a cross check validation of events in real time.

The Cisco team was able to complete a direct integration of event data into NetWitness® using the Firepower eStreamer protocol. Over 50 million+ events were sent to NetWitness® from Firepower, at an average event rate between 500-1100 events per second. This integration enables NetWitness® users to directly query Firewall data and create mash up visualizations from both data sources which can be used to identify gaps in policy and coverage between the product lines. The analytic below was created in NetWitness® using Firepower data, and depicts a detailed analysis of events by volume, threat category and geolocation, and triggered Snort rule.


RSA
Investigate
Respond
Users
Hosts
Files
Dashboard
Reports
dave
Firepower Events Dashboard
Share
Add Row
Firepower Top Classification Descriptions
Past 4 hours
SESSION COUNT
attempted administrator privilege gain
attempted user privilege gain
misc activity
misc attack
attempted denial of service
a network trojan was detected
web application attack
Last Refreshed at : 02:56 PM
Firepower Top 10 Snort IDs
Past 3 hours
SESSION COUNT
14771
3
1
3070
17538
Last Refreshed at : 02:56 PM
Firepower Top File Types
Past 24 hours
SESSION COUNT
FILETYPE
Last Refreshed at : 02:56 PM
Firepower Top Event Type
Past 24 hours
new client applicat... : 14154
new udp server : 15996
udp server informat... : 18036
new tcp server : 67684
tcp server informat... : 73219
new network protocol : 81820
host deleted: host ... : 81821
new host detected : 81835
client application ... : 89065
new transport proto... : 91069
Last Refreshed at : 02:56 PM
Firepower IPS Sources
Past 24 hours
Last Refreshed at : 02:56 PM
Activate Windows
Go to Settings to activate Windows.
RSA NETWITNESS PLATFORM
11.7.1.0

Country	Source IP	Total events co
United States	17.57.152.18	55
United States	24.41.66.184	53
United States	142.250.14...	45
United States	67.195.12.34	44
Netherlands	195.121.65...	30
United States	142.250.14...	26
Canada	64.59.128...	12

CONCLUSION

Those who have served in the military know there is a difference between concealment and cover. This analogy relates to cleartext vs. encryption. We can all make greater strides in becoming more secure, but we need to learn to stop giving away valuable information that can only hurt us. There's a reason breaches are on the rise. We have valuable information and—based on analysis of this free public wireless network—we are giving away way too much of that information.

The percentage of encrypted traffic rose two percent to 80 percent. Encrypt, encrypt…trust but verify!

We're looking forward to monitoring traffic at next year's RSAC and reporting the results to you. The RSAC SOC team is always looking for ways to educate and assist attendees; and we will continue to explore ways to notify attendees of insecure protocols, cleartext usernames and passwords, malware and cryptomining. See you in 2023!

ACKNOWLEDGEMENTS

Thank you to the amazing engineers and analysts who made the SOC possible:

RSA Staff

Percy Tucker

Steve Fink

Bart Stump

Dave Glover

…

Cisco Staff

Jessica Bair Oppenheimer	*Cisco SOC Manager*
Ian Redden	*Team Lead & Integrations*
Aditya Sankar / Ben Greenbaum	*SecureX & Malware Analytics*
Alejo Calaoagan / Christian Clasen	*Cisco Umbrella*
Dinkar Sharma / Seyed Khadem-Djahaghi	*Cisco Secure Firewall*
Matt Vander Horst	*SecureX Orchestration*
Doug Hurd	*Partnerships*

Hardware Support
Eric Kostlan
Navin Sinha
Zohreh Khezri
Eric Goodwin
Gabe Gilligan and the amazing staff at XPO Digital!