RSA CONFERENCE 2020

SECURITY OPERATIONS CENTER FINDINGS REPORT

Published by

RSA CISCO

Written by
Neil R. Wyler, Jessica Bair and Percy Tucker

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 RSA Security LLC ("RSA") 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:
  "Free wireless is available in select Conference areas. Connect to SSID: .RSACONFERENCE (subject ..... to terms and conditions). Important! The .RSACONFERENCE wireless network available at the Moscone Center is an open, unsecured 5 GHz network. NOTE: 2.4 GHz is no longer supported at RSA Conference. RSA and Cisco AMP Threat Grid will be using data from the network for an educational demonstration on a working SOC, we strongly recommend that you use appropriate security measures (e.g., utilizing a VPN connection, installing a personal firewall, updating security patches, turning off your wireless adapter when not in use, disabling ad-hoc (peer-to-peer) capabilities on your device)."
- Additionally, RSA Conference advised attendees of the educational SOC on its website: https://www.rsaconference.com/usa/the-experience/conference-tips (see Tab 2 titled On-Site Tips and Tricks), 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.

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 RSAC SOC

The RSAC SOC team deployed the RSA NetWitness® Platform that included the RSA NetWitness Logs, RSA NetWitness Network and RSA NetWitness Orchestrator components for evolved SIEM capabilities, and Cisco Threat Grid, Cisco Threat Response with Talos Intelligence, Cisco Firepower Threat Defense IDS and Cisco Umbrella.®

RSA NetWitness Network collects all the raw network traffic from a switch port analyzer (SPAN) from the Moscone Center network, adds 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, RSA NetWitness Network checks a community anti-virus (AV) lookup, some static analysis and its own network intelligence. RSA NetWitness Orchestrator powered by ThreatConnect then sends the files to Threat Grid for dynamic malware analysis.

Threat Grid 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 Threat Grid, 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.

Threat Grid 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 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.

Cisco Umbrella provided visibility into DNS activity, with default security blocking turned off. We also use Cisco Threat Response, which integrates threat intelligence from the Cisco Talos intelligence team and other sources.

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

.

THE STATISTICS

During our outbrief for the RSAC SOC Findings session, attendees requested more statistics. The RSAC SOC team tried their best to provide more statistics and refined context and granularity.

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, February 24, 2020, and collected traffic through Thursday, February 27, 2020, at 4 p.m. There were 187,301,858 sessions during this period. This was 2.5 times the amount of traffic collected from RSAC 2019. This corresponds to a bandwidth utilization in 2020 of 1.3 Gbps vs. 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 2020, the SOC saw a stable amount of encrypted traffic, at 78 percent, the same as RSAC 2019. 55,029,102 of the 70,440,998 sessions were encrypted. Although there was more traffic in 2020, it maintained 78% encryption.

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 RSA NetWitness Network, Cisco Firepower or Cisco Threat Grid 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. RSA NetWitness Network and Cisco Threat Grid 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 96,361 cleartext passwords from 2,178 unique accounts. This is 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.

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. 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. During the many RSAC SOC tours when the cleartext username and password subject was presented, several people came up and asked questions about major online email providers. 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?

Cleartext Credentials RSA

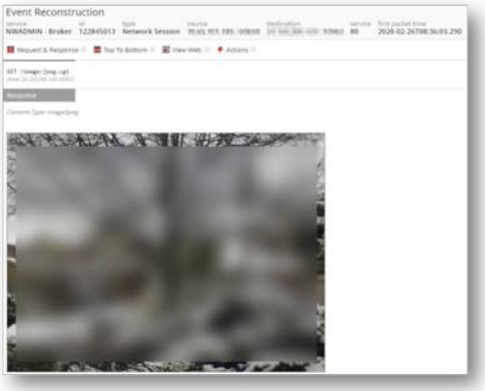
Observed	Username	Password Strength / Time to Crack		Service
1 minute, 41 seconds ago	h**********	Very Weak	less than a second	HTTP
1 minute, 47 seconds ago	s**********@[redacted].com	Weak	38 minutes	POP3
3 minutes, 1 second ago	l**********@loveyougrifter.com	Very Weak	10 seconds	HTTP
3 minutes, 58 seconds ago	t********	Weak	3 hours	HTTP
4 minutes, 23 seconds ago	a**********@[redacted].com	Strong	15 years	IMAP2
5 minutes, 59 seconds ago	b**********@[redacted].com	Very Strong	centuries	IMAP2
5 minutes, 59 seconds ago	b**********@[redacted].com	Very Strong	centuries	IMAP2
6 minutes, 56 seconds ago	a**********@[redacted]	Very Strong	centuries	IMAP2
6 minutes, 58 seconds ago	a**********@[redacted]	Very Strong	centuries	IMAP2

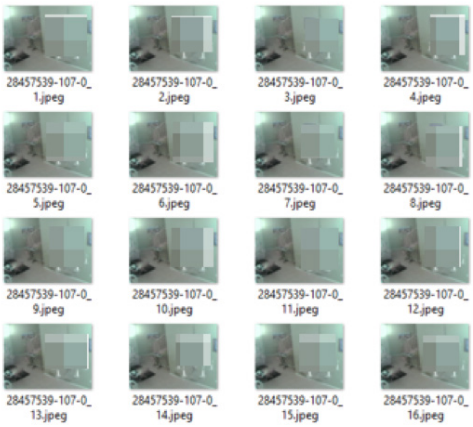
The image above is very interesting and explains the dilemma quite easily. This was written by an RSAC SOC team member to pull data from RSA NetWitness Network. The columns indicate the obfuscated username, password strength, estimated time to crack the password and the protocol used. Does anything stand out?

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 2020 saw the return of video feeds over port 80 from home security devices. Four 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. Two to three 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 images of video feeds that were traversing the RSAC wireless network in the clear.





Ring has been in the news lately regarding the security around their products. The image below is from a Ring device, but has nothing to do with the product's security protocols. In this case, an attendee decided to share a video clip with someone while on the .RSACONFERENCE network. This removed the security protocols between the device and app, and the shared footage was sent in cleartext.

Mobile Devices and the Apps We Love!

In all four years of the RSAC SOC, SOC team members have reported to attendees the security risks of mobile applications. Every year we see traffic that we probably should not from mobile devices on the network. This problem is more difficult to help remediate than cleartext username and passwords because the data is all over the place. Some apps have strong authentication and bleed data, some apps give away everything and some apps just tell us where you are.

The Case Against Wi-Fi Assist

It was discovered that a cellular provider that allows Wi-Fi-assisted services did not offer Wi-Fi-assisted security. Devices on this network that routed SMS/MMS traffic over Wi-Fi instead of the cellular network were in cleartext. We could join you for breakfast as indicated in the image below or challenge you to a step challenge from the image below that. The moral of the story, and an "aha" moment for all, is that text messages should be private. They should also be secure. The RSAC SOC team was horrified to see this traffic, but also felt it was very important to educate.

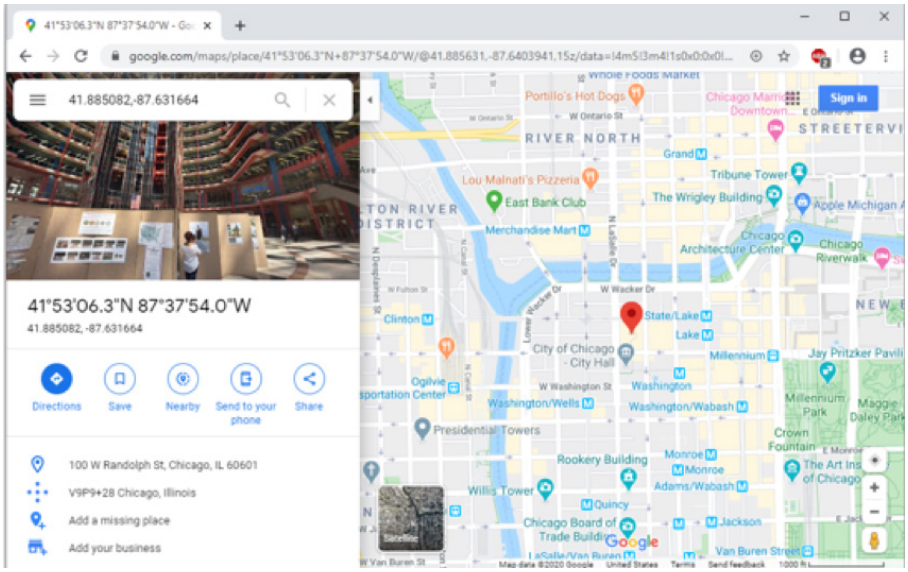
```
TYPE=PLMN.□□□□□□□□□Your message has been sent..□.³□application/smil.□0.smil..K□%..application/smil.□
123_1.smil.□êÀ"<123_1.smil>.*
□□123_1.smil.□123_1.smil.<smil><head><layout><root-layout/>
<region id="Text" top="70%" left="0%" height="30%" width="100%" fit="scroll"/>
<region id="Image" top="0%" left="0%" height="70%" width="100%" fit="meet"/>
</layout>
</head>
<body><par dur="10s"><text src="text_01.txt" region="Text"/>
</par>
</body>
</smil>
@:.□□ê□text_01.txt.À"<text_01.txt>.*.□□text_01.txt.□□□text_01.txt.hope ya'll had good evenings. at m west
eating breakfast.
```

```
TYPE=PLMN.□□□□□□□□□Your message has been sent..□.³□application/smil.□<smil>..F□□.application/smil.□ê□
smil.smil.À"<smil.smil>.□smil.smil.*.□□smil.smil.<smil><head><layout><root-layout width="1848px"
height="1080px"/>
<region id="Text" left="0" top="972" width="1848px" height="108px" fit="meet"/>
</layout>
</head>
<body><par dur="5000ms"><text src="cid:text_01.txt" region="Text"/>
</par>
</body>
</smil>
>E.□□ê□text_01.txt.À"<text_01.txt>.□text_01.txt.*.□□text_01.txt.It makes sense to pace yourself Mary. You have
done a LOT of walking
```

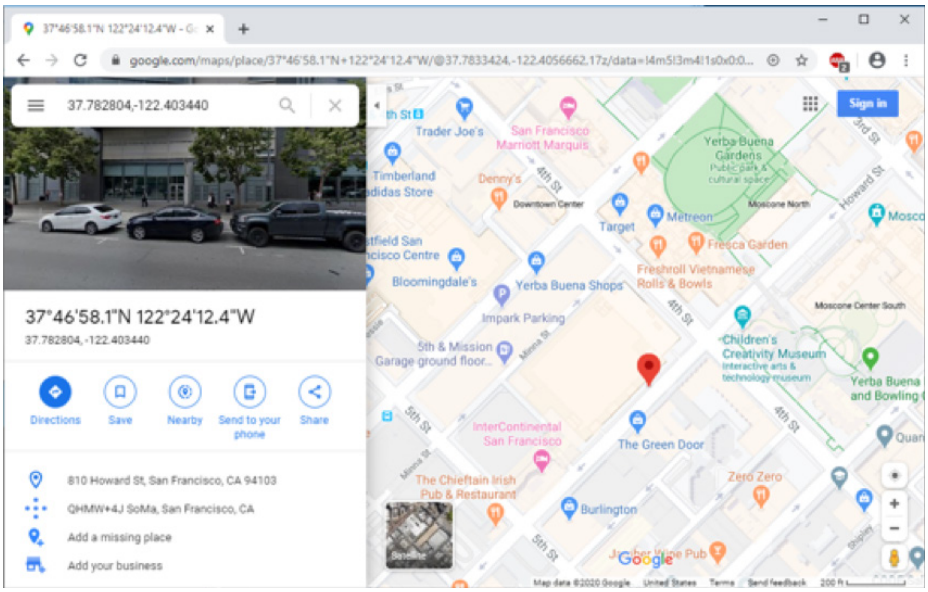
Location! Location! Location!

More mobile application lessons learned revolve around location, both past and present. Below we can see an application from an iPhone application that provides no identifiable user information, but provides GPS coordinates in cleartext.

The interesting thing here is that the GPS coordinates collected in this app contain both last location and current location. Placing these coordinates into a search engine clearly shows this attendee was last in Chicago…

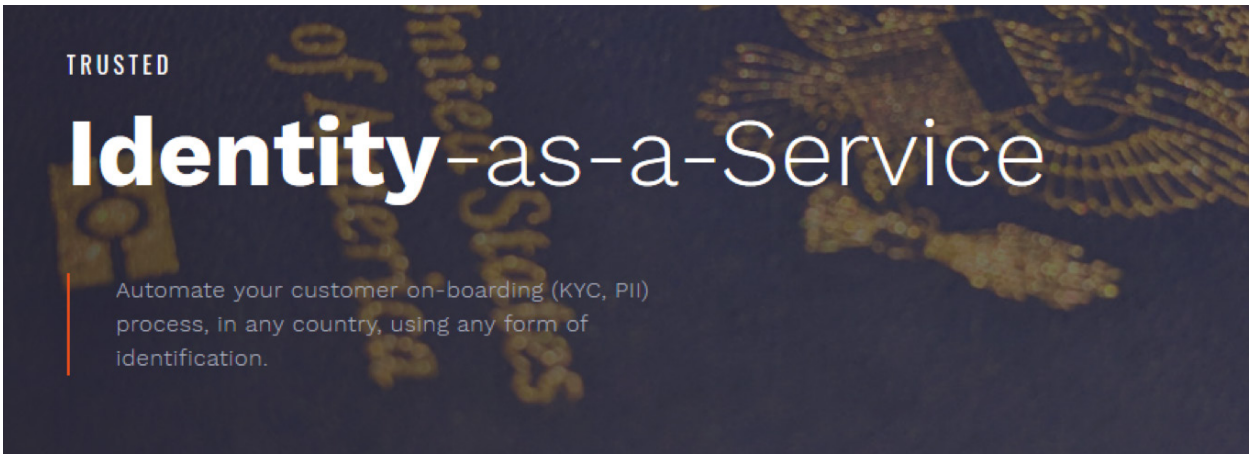


…and then in San Francisco attending the RSA Conference.



Stories from the Expo Floor

There are a lot of stories this year from the expo floor. In theory, booths on the floor should have ethernet drops to their location, which would place them outside of the .RSACONFERENCE network. However there were some vendors on the expo floor utilizing the .RSACONFERENCE wireless network. Brand identity, recognition and trust are huge. The cost of attending a conference such as this, as well as the costs associated with a booth, personnel and demos, provide the backdrop for our stories from the expo floor. Demos may be demos, but I think you will question some of the practices below in terms of whether exploitation of these insecurities could be very costly.



Insecurity as a Service

Identity is a pretty important piece of data in the cybersecurity world. If a company is a cloud-based provider of identities and markets the word "Trusted" as part of its product or brand, then perhaps they should follow standard security practices and know what information is traversing the network instead of just what is displayed on a monitor.

```
password = 'p@ssw0rd!'
```

First of all, your credentials should not be in cleartext and use a fairly common password.

Network Event Details | Text Packet File Email Web

Download PCAP

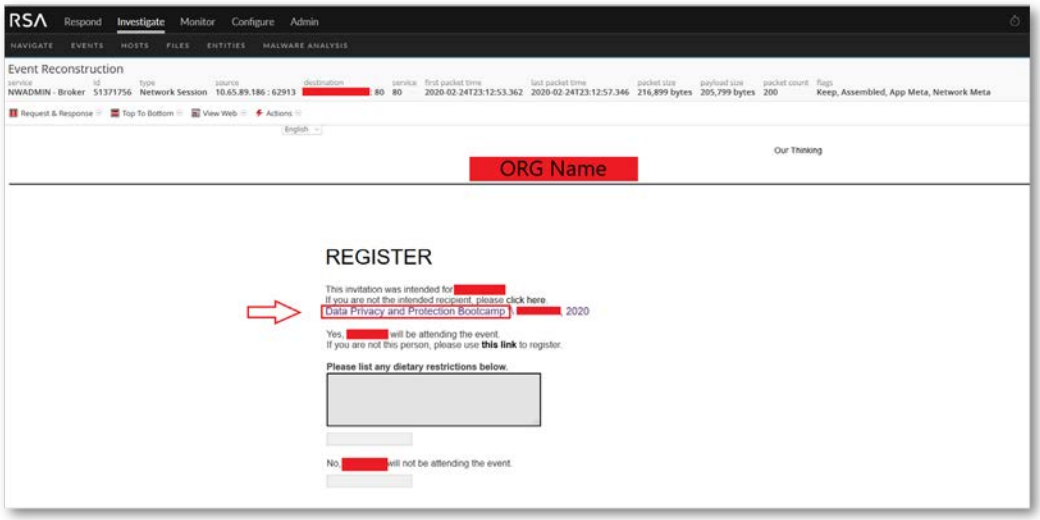
NW SERVICE	SESSION ID	SOURCE IP:PORT	DESTINATION
NWADMIN - Broker	56301806	10.65.13.61 :54533	[redacted] :80
LAST PACKET TIME	**CALCULATED PACKET SIZE**	**CALCULATED PAYLOAD SIZE**	**CALCULATED**
02/25/2020 00:20:35	63002 bytes	58983 bytes	70

REQUEST

```
Host: [redacted]
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
DNT: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/79.0.3945.130 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,a
/signed-exchange;v=b3;q=0.9
Referer: http:/[redacted]Login
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,de;q=0.8,da;q=0.7
Cookie: ASP.NET_SessionId=hbhp2ncm2t4nigmb2wjishn1
```

Showing 3%

And you should probably be using a secure protocol. In effect, the URL and login credentials are being broadcast in cleartext using HTTP. Now, ponder for a moment the implications as we share more tales from the expo floor.



The image above shows another vendor from the expo floor. Clearly this is from a booth kiosk where attendees can sign up for their "Data Privacy and Protection Bootcamp." Perhaps registering for a data privacy and protection bootcamp from a vendor that is not keeping your information private or protected isn't really a good idea.

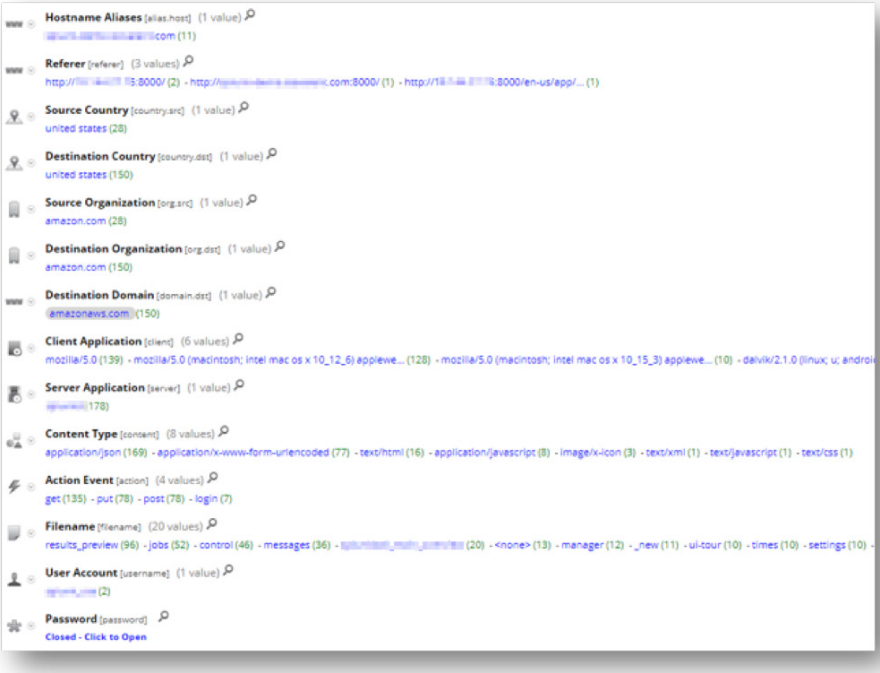
GDPR

More cleartext traffic from the expo floor: This example shows a couple of things that are anecdotal. The fact that a vendor with a booth is utilizing email over an insecure protocol is frightening. This email covers a lot of activity around meetings and booth activity. The contradictory part is towards the bottom, where text below the signature indicates that the company is "committed to ensuring your data privacy. For more information please visit our privacy notice to view our commitment to the GDPR."

ed at 11:30 AM is open. We can switch. Still at your booth?

> On Feb 24, 2020, at 4:28 PM, [redacted] wrote:
>
> .
> Hi [redacted],
>
> [redacted] has a last minute conflict during this time. Would you be able to move this meeting to Wed 2/26 at 11:30am - 12pm PT at the [redacted] booth?
>
> Respectfully,
>
> [redacted]
> <image001.png>
>
> Phone: +1.[redacted] ext 7012
> [redacted]
> [redacted]
>
> Connect with Us:
> LinkedIn | Twitter | Facebook
>
>
>
> -----Original Appointment-----
> From: [redacted]
> Sent: Wednesday, January 22, 2020 1:59 PM
> To: [redacted]
> Cc: [redacted]
> Subject: [redacted] at RSA
> When: Tuesday, February 25, 2020 5:45 PM-6:15 PM (UTC-07:00) Arizona.
> Where: Booth [redacted]
>
> Description
>
>
> [redacted], enables clients to accelerate growth and achieve best in class positions in growth, innovation and leadership. The
the generation, evaluation and implementation of powerful growth strategies. [redacted] leverages over 50 years of experience in partnering with Global 1000 com
> To join our [redacted], please visit http://www.[redacted].com.
>
> [redacted] is committed to ensuring your data privacy. For more information please visit our privacy notice to view [redacted] commitment to the GDPR
>
> Email Disclaimer

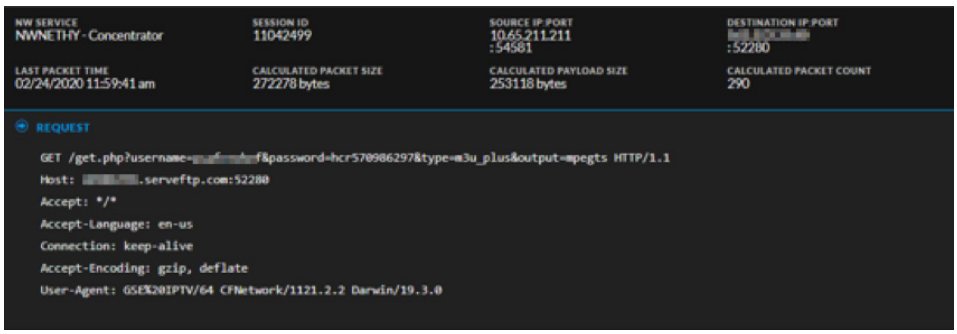
Once again we urge you to comprehend the power of identifying cleartext communication and the implications it can have for your brand, reputation, customers and overall intended experience as a vendor on the expo floor.



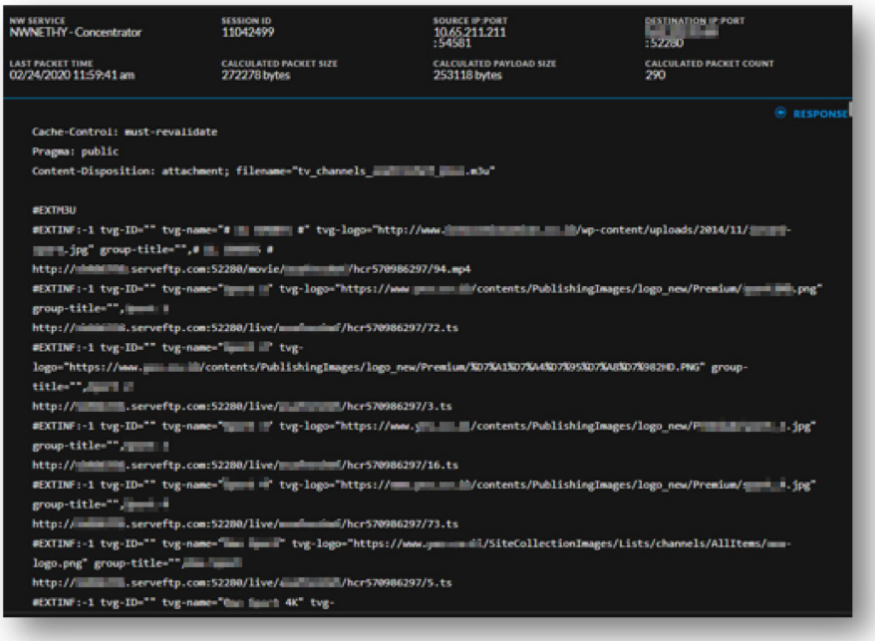
Above we see a very large security vendor performing demos on the expo floor in cleartext. What if, in the busiest moment, your organization was locked out of your very own demo while having a large audience of prospects and customers ready to see your excellent demo? Failed login? Account locked out? User doesn't exist? Utilizing insecure protocols means anyone can see this traffic, and anyone could login. They could even create new credentials or change the existing credentials, prohibiting you from executing your live demo.

Booth Blues

The RSAC SOC Team discovered several Internet Protocol Televisions (IPTV) that were joined to the .RSACONFERENCE network. You can probably guess what is coming next: Below are images of these devices with their credentials in cleartext.



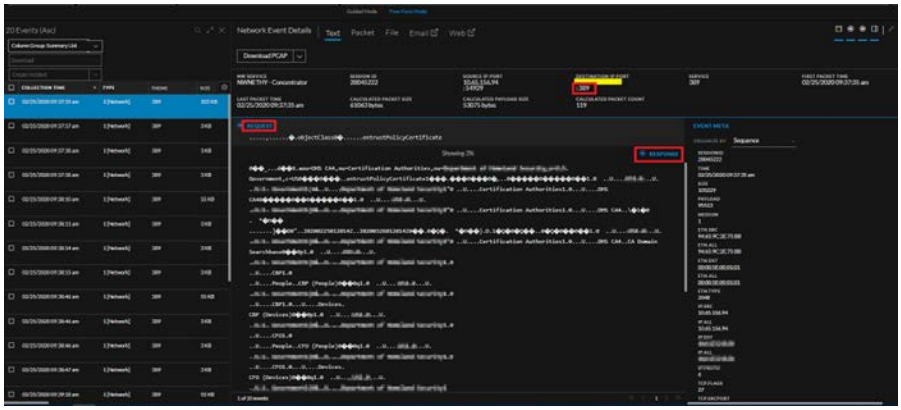
The image below shows the content to be displayed, and where to navigate and get to that content. If you look closely, the protocol to retrieve the content uses SSL, yet the device itself is using cleartext. Anyone on the network would have had the ability to remotely display any content because of the lack of security of a display.

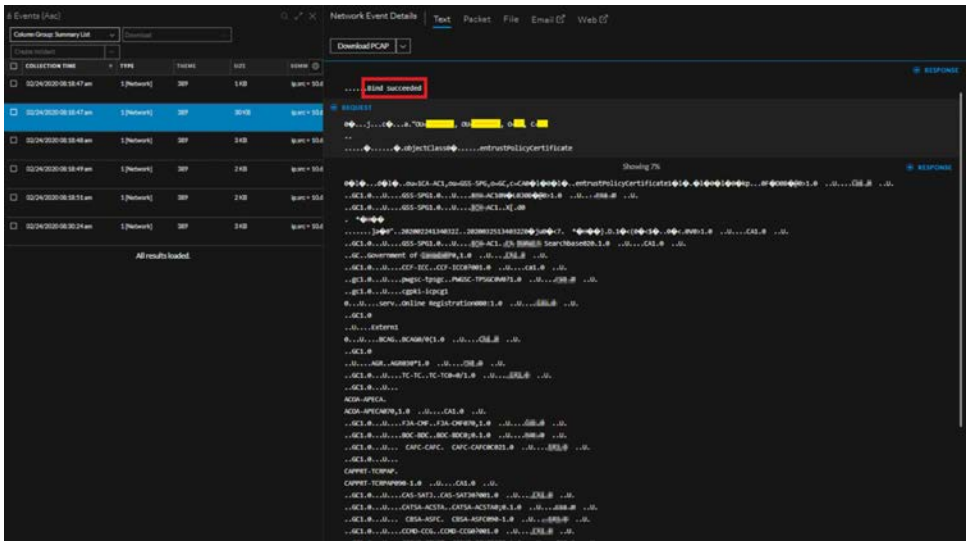


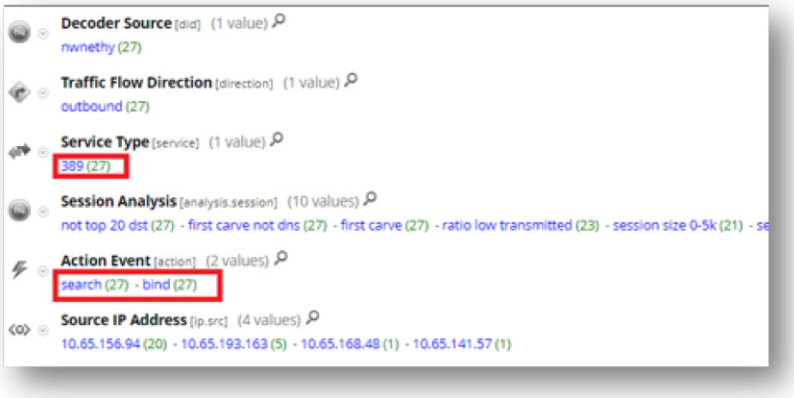
Some organizations are overlooking many security issues that could have an adverse impact on the ability to execute.

Outlaw Countries

In this example we see two government entities (different governments) that are binding to their LDAP infrastructure in cleartext. Governments tend to be large entities, but allowing this type of misconfiguration or lack of secure protocols is a risk when information about the organization can easily be viewed by others on a typical wireless network.

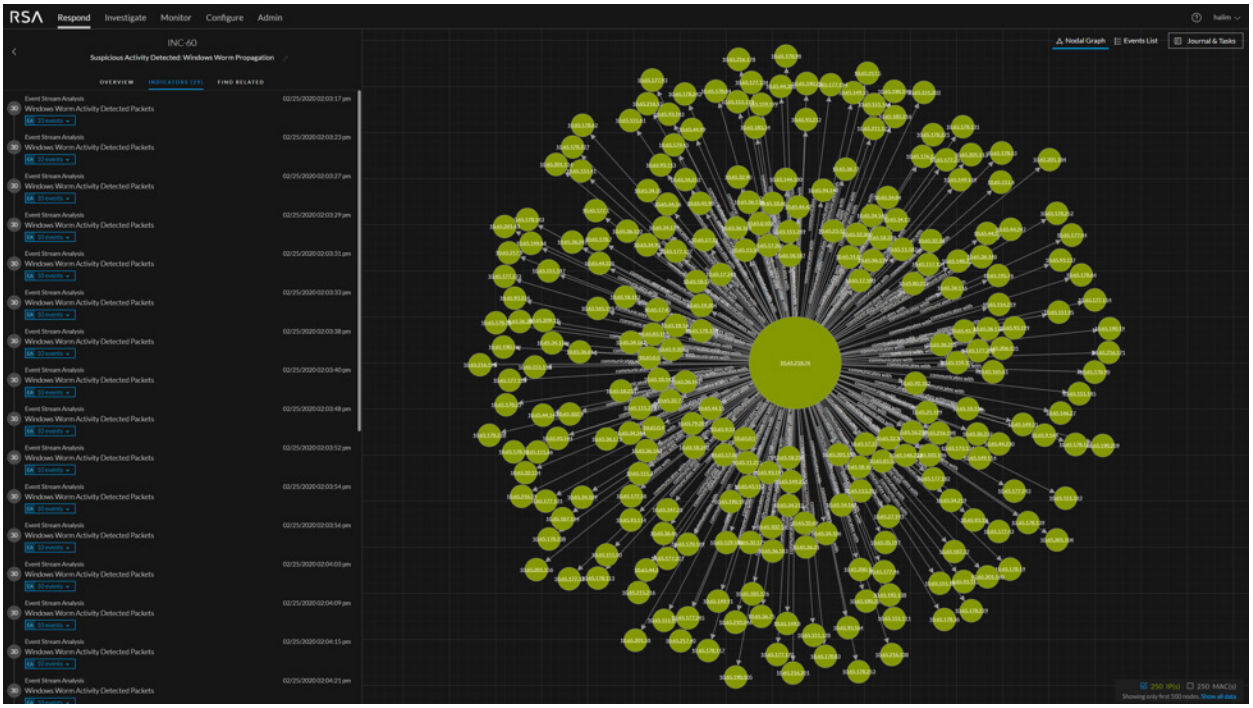






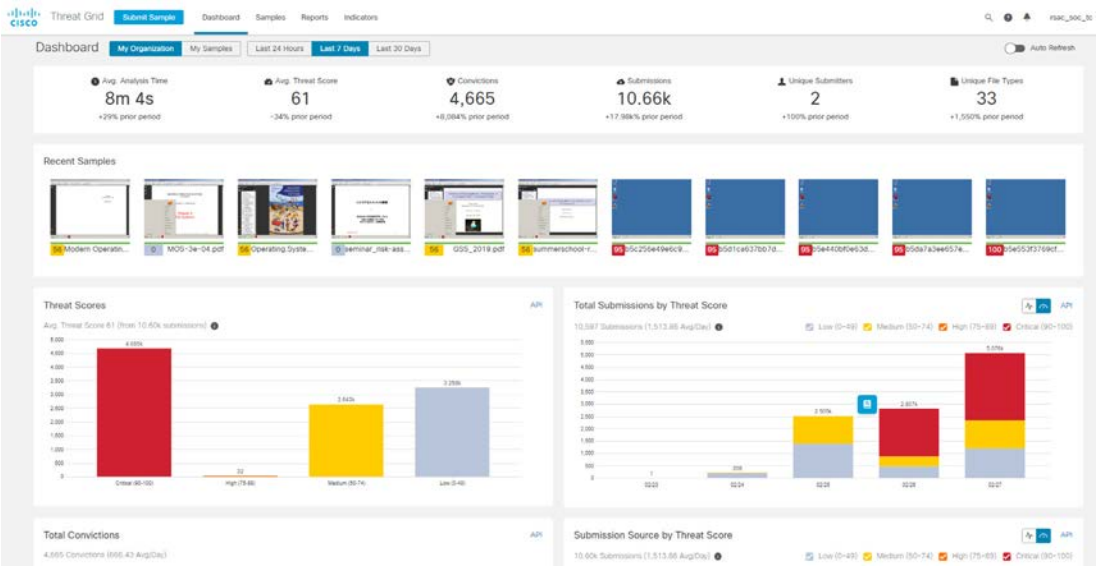
Worm or Noisy Scanner?

During the second day of the conference an RSAC SOC analyst detected a host that joined the .RSACONFERENCE wireless network and immediately began to scan for openings on ports 139 and 445. Due to the lack of host isolation, this behavior yielded multiple successful connections to other hosts, and as the analyst continued to monitor the situation, they were surprised by the boldness of the user, as there appeared to be no attempt made at controlling the speed or stealthiness of their attempted connections. As the analyst continued to monitor the situation, and investigated the traffic further, they were able to determine that this wasn't the activity of a brazen attacker, but in fact was just a MacBook joining the network and looking for shared drives. The image below quickly illustrates how often another device said "I'm sharing a drive, here you go!" You'll see our MacBook in the center of the cluster with each smaller circle showing a responsive, and in many cases oversharing, host. This type of example shows us we need to be careful with how we're configuring our network share access, because you don't have to be a sophisticated attacker to gain access. Sometimes you just have to ask.

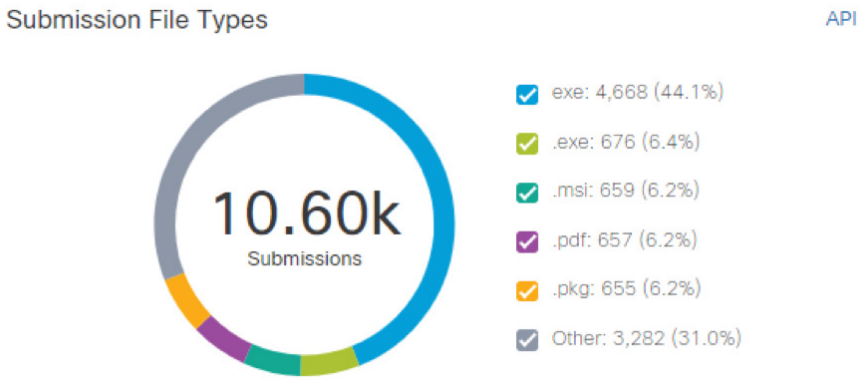

RSA
Respond
Investigate
Monitor
Configure
Admin
INC-60
Suspicious Activity Detected: Windows Worm Propagation
OVERVIEW
INDICATORS (29)
FIND RELATED
Nodal Graph
Events List
Journal & Tasks

MALWARE ANALYSIS

The RSAC SOC team sent over 10,000 potentially malicious files to Threat Grid via RSA NetWitness Network for automated behavioral analysis.



The breakdown of major file types is as follows.



Malicious Behavior

On the third full day of the conference, an attendee downloaded over 4,600 malware samples on the open network, up from about 1,000-2,000 samples in previous years. The files were sent to Threat Grid for dynamic malware analysis.

Certain types of malware require user activity to launch, such as clicking a confirmation box in the UI. To emulate a user automatically during sample analysis, Threat Grid 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.

Malware has exploited these basic differences for years. However, Threat Grid has seen a marked increase in sample submissions that require a series of user actions for the delivery mechanism to succeed. Specifically, the malware samples checking for evidence of a real user system vs. an automated system has moved from the payload to the delivery mechanism. Malware authors have taken a step back and are attempting to ensure that the first stage of their malware is delivered properly.

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

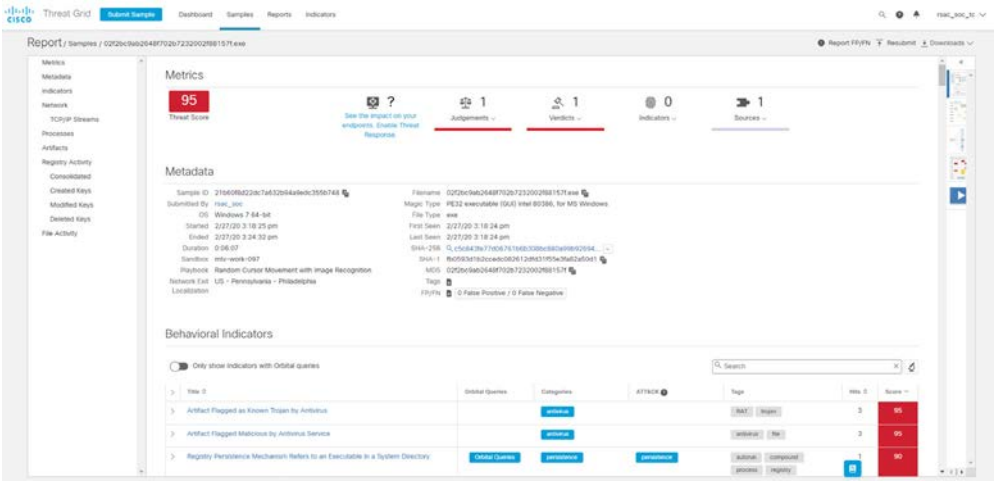
Some of the more common examples of user behavior expected by malware include:

- Close Active Window
- Conduct Active Window Change
- Open Embedded Object in Word
- Random Cursor Movements with Image Recognition
- Visit Website with Internet Explorer

Threat Grid user emulation playbooks perform these common user functions. Playbooks are available from a dropdown menu in the portal UI sample submission dialog and through the API submissions, such as with RSA NetWitness Network. The RSAC SOC team submitted files to Threat Grid with the default playbook of Random Cursor Movements with Image Recognition.

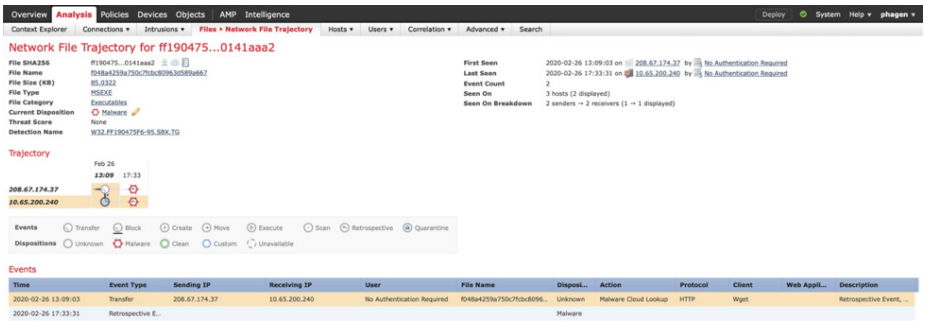
One example malware sample we saw that required user interaction used a sex chat lure to install a Trojan. The lure was observed in the thumbnails across the top of the Threat Grid display in the SOC, allowing a visual of what was occurring in the virtual machine. An RSAC SOC analyst was able to click into the virtual machine to interact with the sample in the Threat Grid Glovebox, without the risk of viral infection. Once the "Click Here to Live Sex!" button was clicked, a Trojan installed in the background, as a stream of sexually explicit chat scrolled on the screen.

The analysis of the behavior determined a Threat Score of 95 out of a possible of 100.



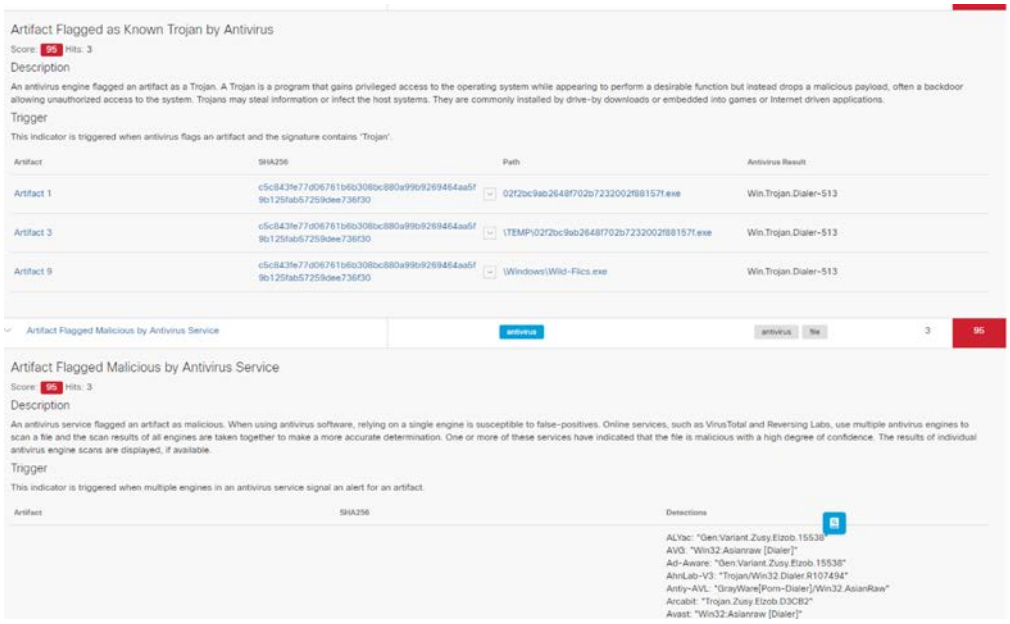
Samples with a Threat Score of 90 or above are marked as malicious (by hash value) in the global Cisco Talos Intelligence database, to provide near real-time worldwide protection. No other metadata or organization information is included with the hash value and Threat Score, for automated, anonymous intelligence sharing with all Cisco Security products and third-party technology partners that integrate with Cisco Threat Response and the upcoming Cisco SecureX.

An example of this was seen in the Firepower Management Console, where one of the sample files was unknown to Talos Intelligence at the time of downloading on the network. After the Threat Grid conviction, there was a retrospective alert of the malware in the SOC. In a production environment, the sample file's trajectory in the networks would be tracked and visualized. Also, an integrated endpoint protection would quarantine the malicious file and isolate the device.

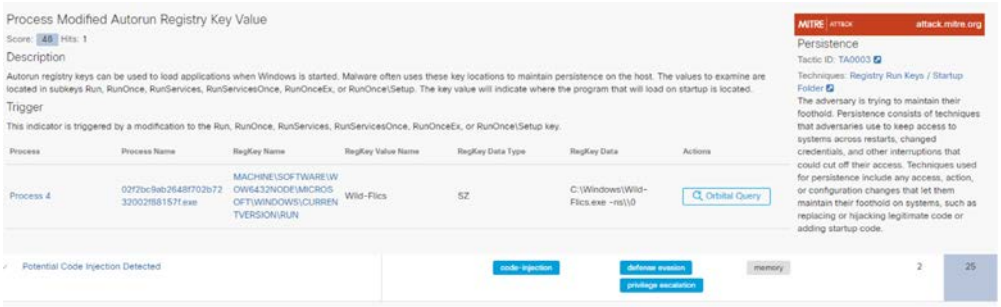


In the Black Hat NOC, the security team owns the infrastructure, so a captive portal alert, through the Palo Alto Networks firewall, is used to alert attendees when malware or cryptomining is seen on their device, or plain text passwords are utilized. The RSAC SOC has the ability to send an alert email through RSA NetWitness Orchestrator to attendees who exhibit the same behavior. Straw polls of participants in the public tours and Friday sessions indicate that many RSAC attendees would like to know if malware, command-and-control, or cryptomining traffic was seen communicating with their device and/or if they were using cleartext passwords. This proposed capability and action is under review with the RSAC organizers.

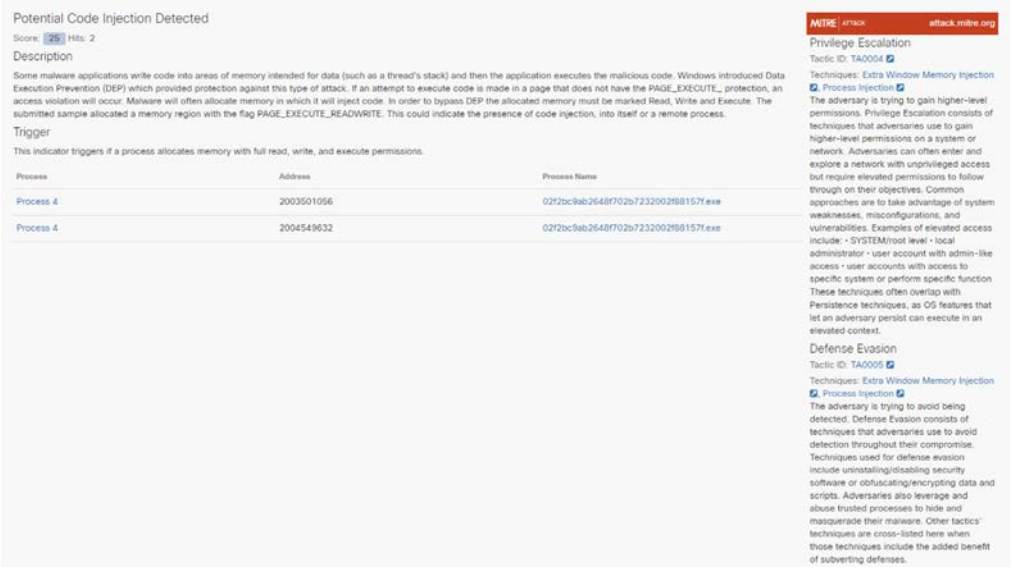
Continuing the analysis of the behavior of the above sample, we determined it was a variant of the AsianRaw Dialer Trojan.



Some of the malicious behavior included a persistence mechanism in the registry.



Also, malicious behavior included injecting code into memory.



Potential Code Injection Detected

Score: 25 Hits: 2

Description

Some malware applications write code into areas of memory intended for data (such as a thread's stack) and then the application executes the malicious code. Windows introduced Data Execution Prevention (DEP) which provided protection against this type of attack. If an attempt to execute code is made in a page that does not have the PAGE_EXECUTE_ protection, an access violation will occur. Malware will often allocate memory in which it will inject code. In order to bypass DEP the allocated memory must be marked Read, Write and Execute. The submitted sample allocated a memory region with the flag PAGE_EXECUTE_READWRITE. This could indicate the presence of code injection, into itself or a remote process.

Trigger

This indicator triggers if a process allocates memory with full read, write, and execute permissions.

Process	Address	Process Name
Process 4	2003501056	02f2bc9ab2648f702b7232002f88157f.exe
Process 4	2004549632	02f2bc9ab2648f702b7232002f88157f.exe

MITRE ATTACK attack.mitre.org

Privilege Escalation

Tactic ID: TA0004

Techniques: Extra Window Memory Injection, Process Injection

The adversary is trying to gain higher-level permissions. Privilege Escalation consists of techniques that adversaries use to gain higher-level permissions on a system or network. Adversaries can often enter and explore a network with unprivileged access but require elevated permissions to follow through on their objectives. Common approaches are to take advantage of system weaknesses, misconfigurations, and vulnerabilities. Examples of elevated access include: • SYSTEM/root level • local administrator • user account with admin-like access • user accounts with access to specific system or perform specific function These techniques often overlap with Persistence techniques, as OS features that let an adversary persist can execute in an elevated context.

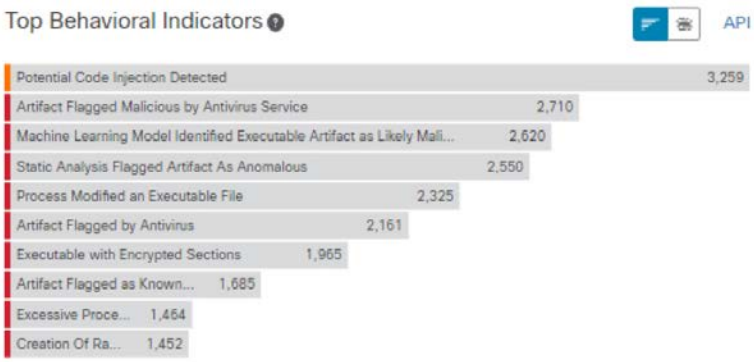
Defense Evasion

Tactic ID: TA0005

Techniques: Extra Window Memory Injection, Process Injection

The adversary is trying to avoid being detected. Defense Evasion consists of techniques that adversaries use to avoid detection throughout their compromise. Techniques used for defense evasion include uninstalling/disabling security software or obfuscating/encrypting data and scripts. Adversaries also leverage and abuse trusted processes to hide and masquerade their malware. Other tactics' techniques are cross-listed here when those techniques include the added benefit of subverting defenses.

Potential Code Injection Detected into memory was the most observed behavior, just as it was in 2019. It was closely followed again by the behavioral indicator that combines machine learning from the analysis of the common characteristics of millions of known malware samples, with the presence of artifacts previously known to be associated with malware. It is easy to create a new hash value for a malware sample. It is a lot more work to redesign how it operates and its dependencies on other files or its core functionality. Below are the top malicious behaviors observed at RSAC 2020.



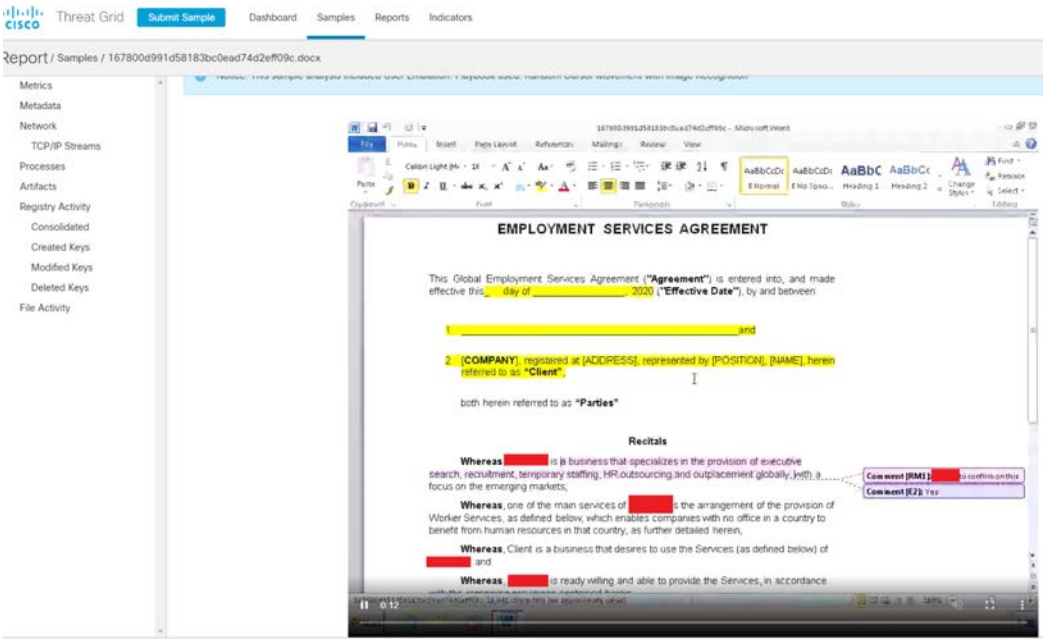
The malware sample also made an attempt at sandbox detection. Because there is no .dll, hook or other presence in the Threat Grid virtual environment (an "outside, looking in" approach to analysis), the sample did not detect the analysis and executed as programmed.

Everything an Attacker Needs for Spear Phishing Lures

This year the RSA SOC continues to see major data privacy concerns via attachments in unencrypted email traffic or downloads/uploads without HTTPS. These files were visible as they streamed through RSA NetWitness Network.

We saw dozens of invoices, billing statements and confidential business proposals. Each could be used by an attacker sniffing the public network to craft a custom spear phishing lure. They had legitimate business and financial information such as the email addresses of the sender/receiver, account information, billing address and the types of products/services the email recipient expected to receive.

RSAC is also a great place for job hunting, networking and recruiting, which are all confidential by nature.



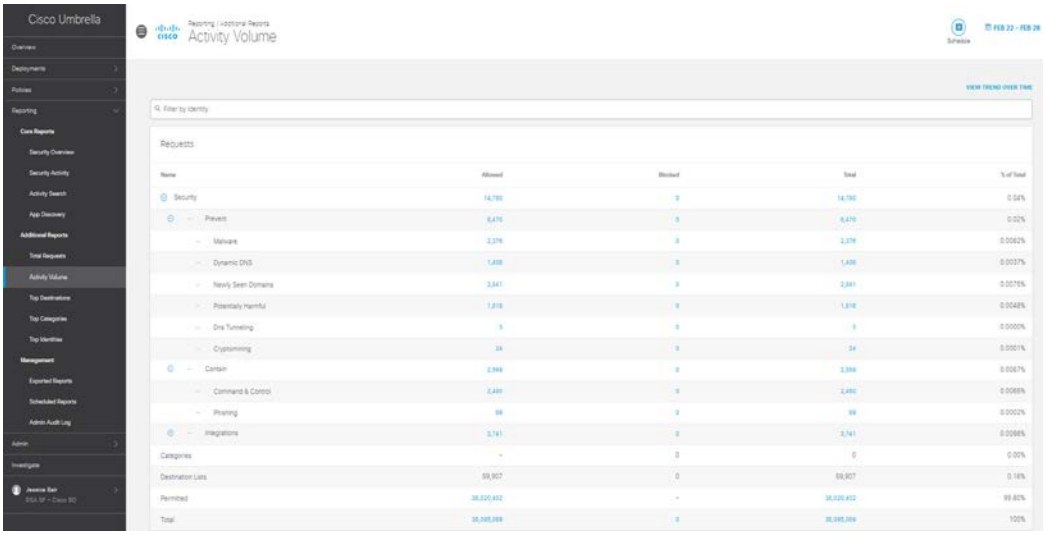
Last year, we saw the resume of a CISO candidate emailed in the clear; in 2020, the trend continued with resumes sent insecurely.

DOMAIN NAME SERVER (DNS)

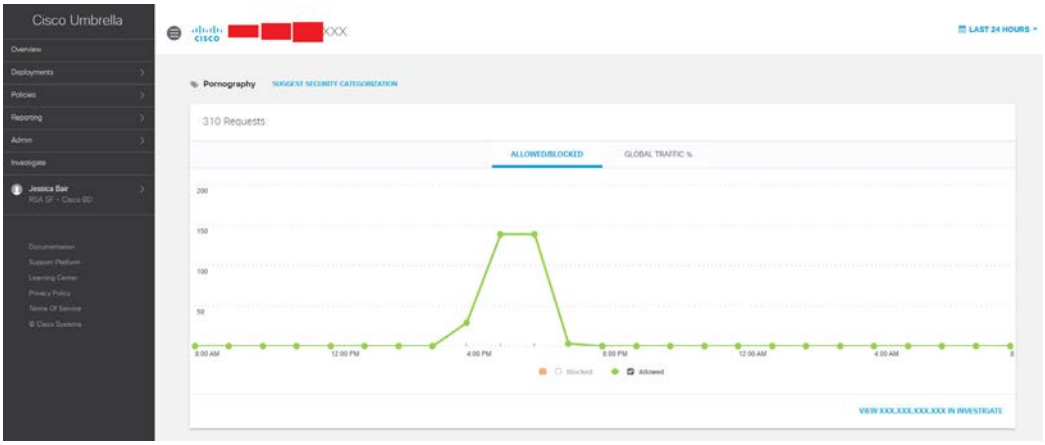
The SOC had complete DNS visibility in 2020, thanks to the support of the Moscone Center agreeing to change their DNS to Cisco Umbrella.

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 more than 37 million DNS requests over the week, of which several thousand would have been blocked for security. 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.

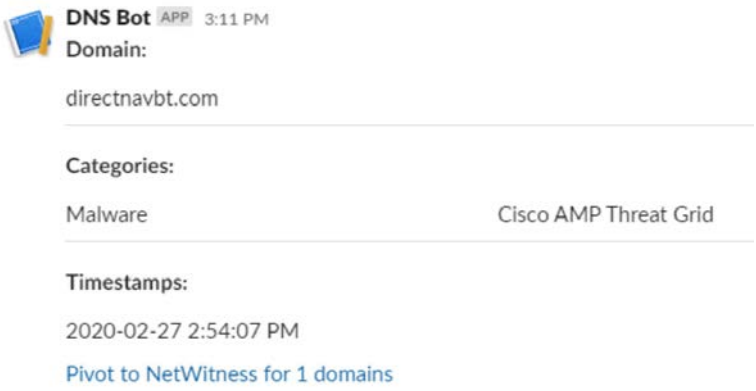


Domains also could have been blocked for content, such as pornography, terrorism-related, hate/discrimination or other such categories. Again, no blocking occurred, which gave rise to somewhat interesting behavior when an attendee spent the opening reception connecting hundreds of times to a new adult portal, and then promptly left the venue.



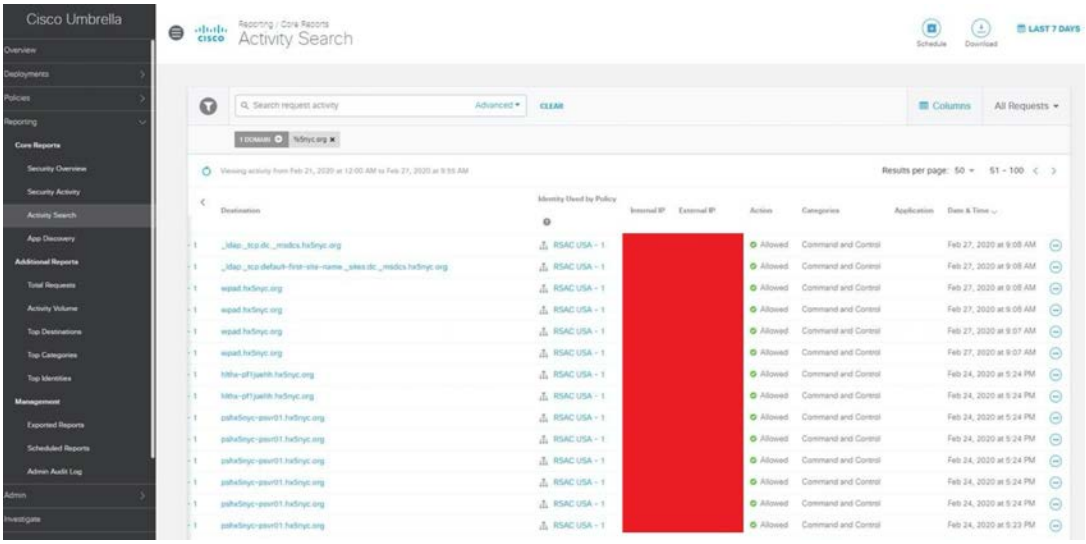
Automate, Automate

Every year, the RSAC SOC team finds more ways to improve efficacy. This year, a Cisco analyst created an automated workflow using the new Cisco Umbrella APIs to extract over 400 unique domains that would have been blocked by Cisco Umbrella as malicious. These were then shared in Slack with the RSA NetWitness Network analysts, with a link to aid in determining in RSA NetWitness Network if the connection was successful and a payload was downloaded.

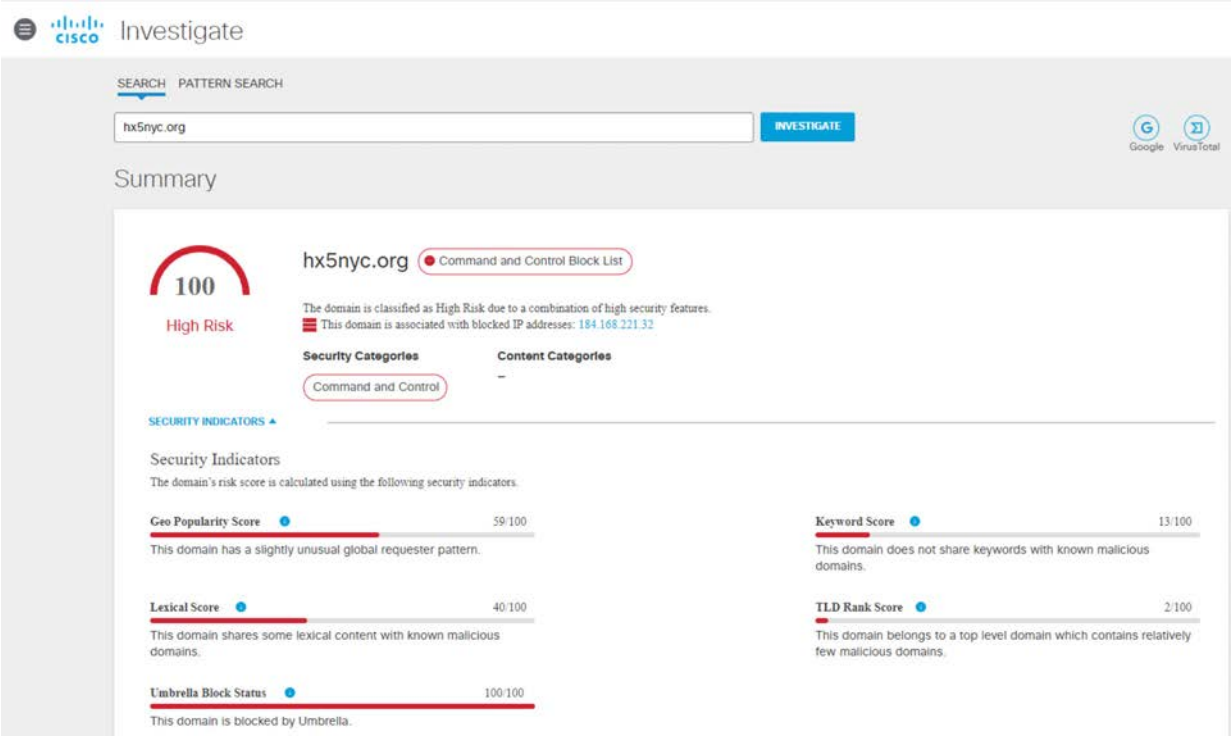


Command and Control

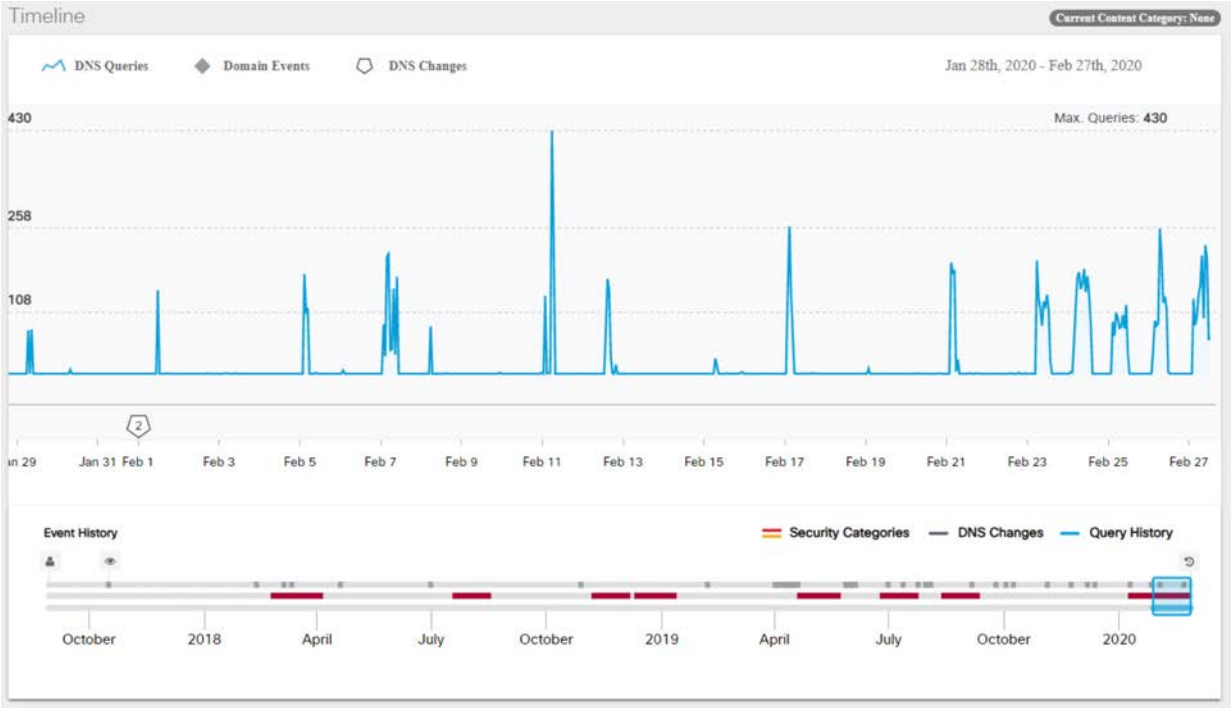
We observed a real-world command-and-control incident, where a device inside the Moscone Center, which was not attached to the wireless network, was communicating with a malicious domain and many subdomains. More than 2,000 DNS requests were made to the domains over Sunday, Monday and Thursday.



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

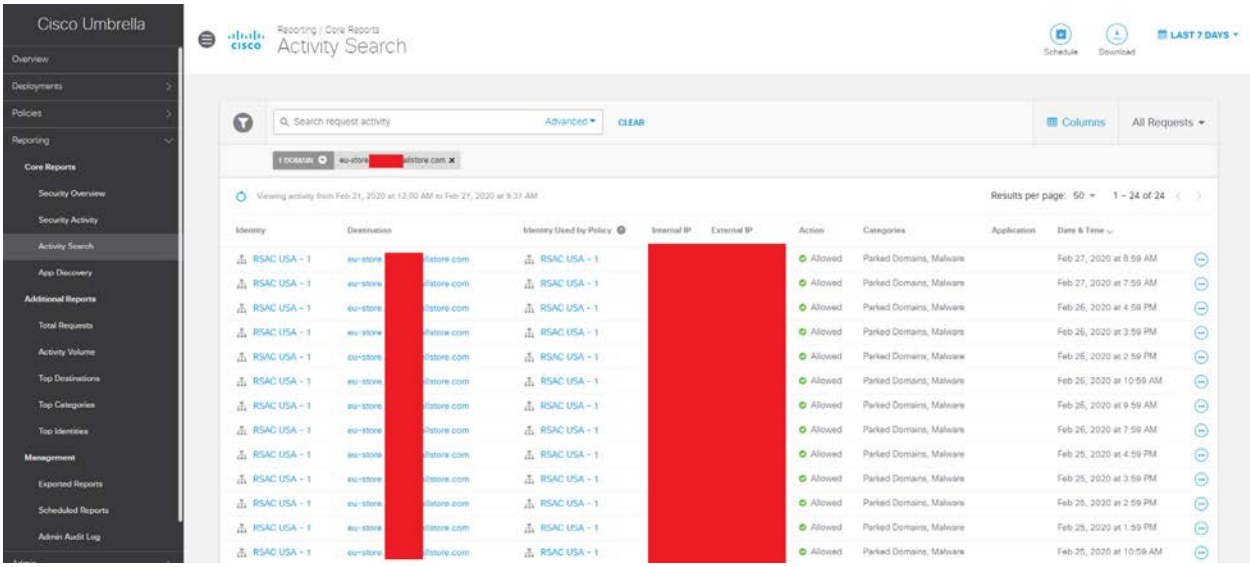


We were also able to see the frequency of global queries, of which the traffic from the Moscone Center was a part. With this intelligence, we alerted the Moscone Center NOC for action deemed appropriate.

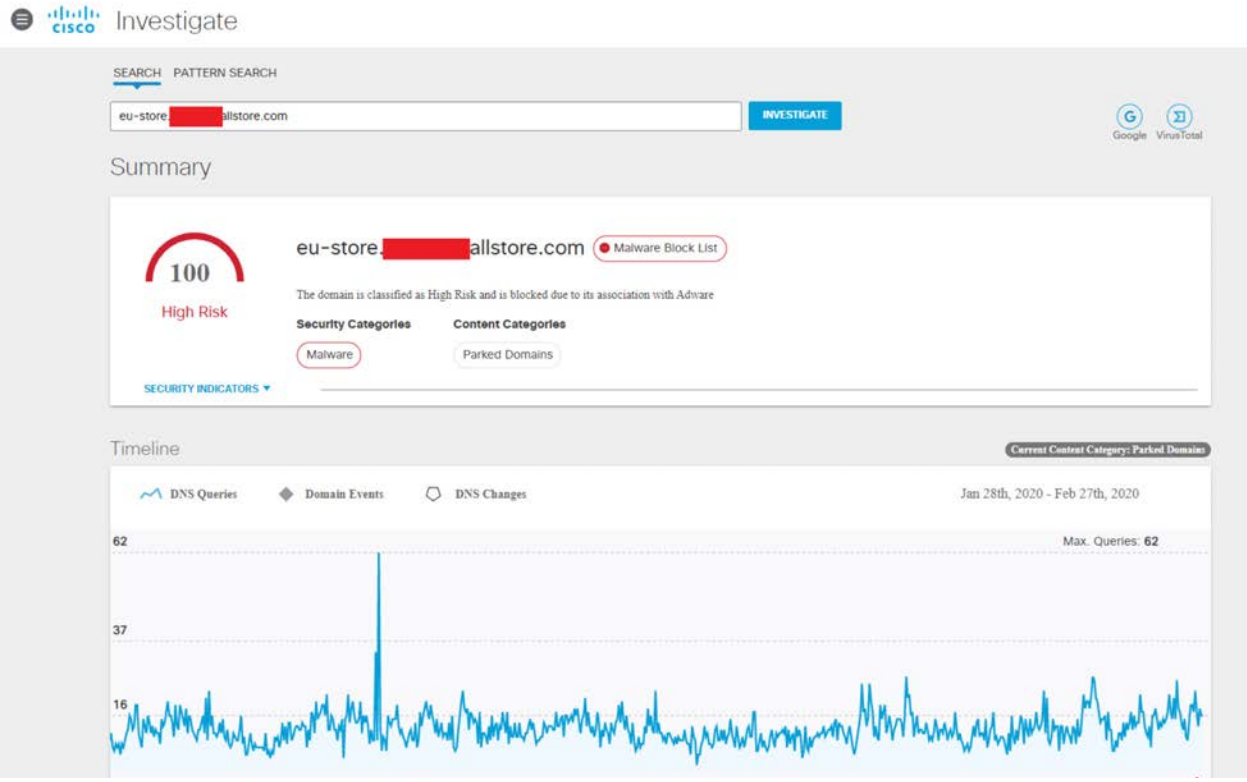


Phishing Domain

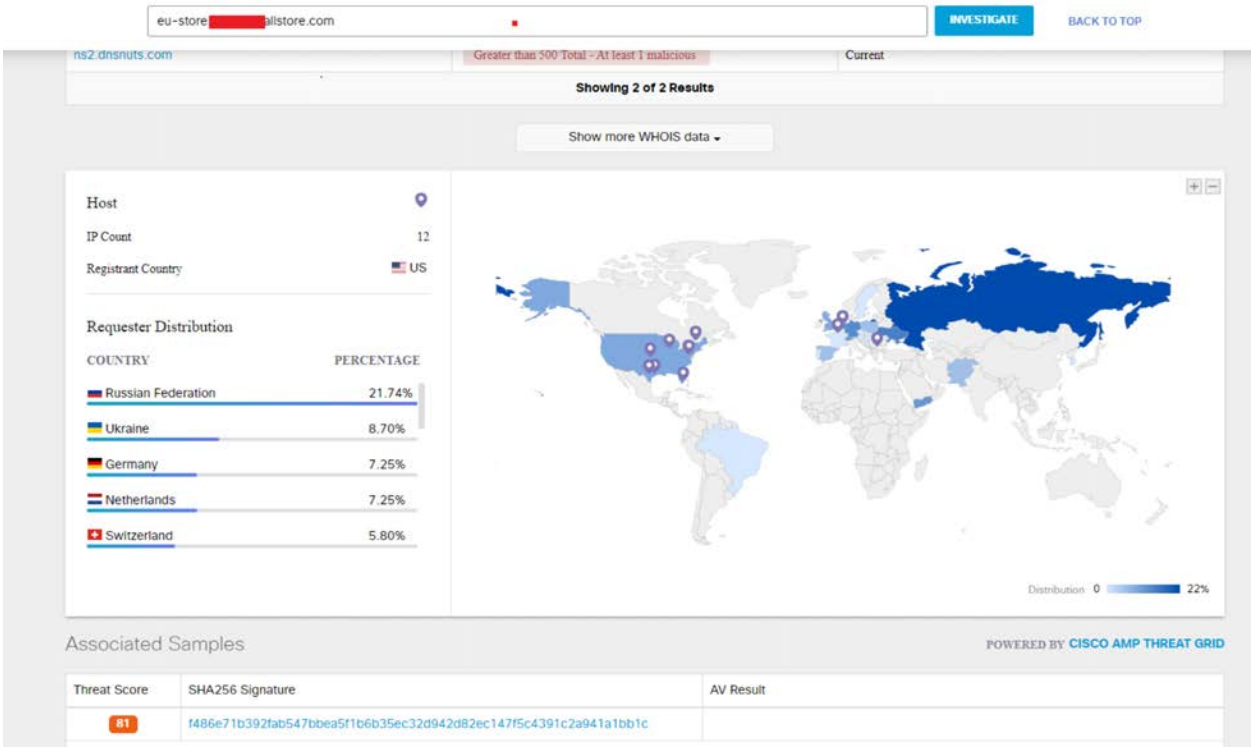
In another incident, we observed a device on the wireless network beaconing out every hour to a malicious, parked domain designed to emulate an e-store in the European Union for a global mobile device manufacturer. The morning after the first observation, representatives of the manufacturer attending RSAC had a tour scheduled at the SOC and we showed them the DNS traffic.



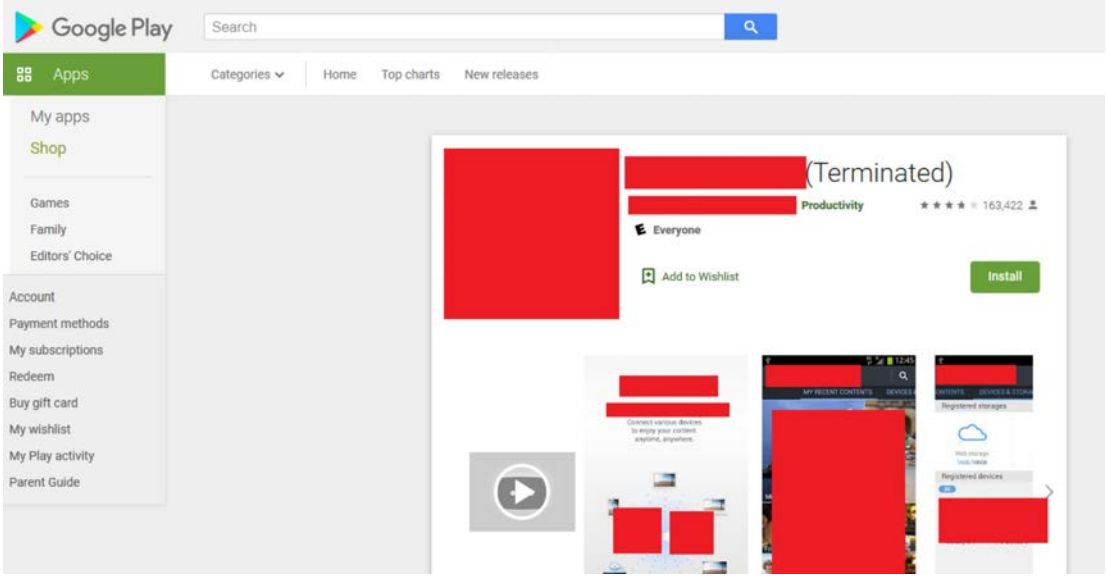
The domain would have been blocked by default for serving adware. We were able to show the manufacturer's team the extent of the global queries.



We were also able to show the global distribution, with most coming from the Russian Federation and Ukraine.

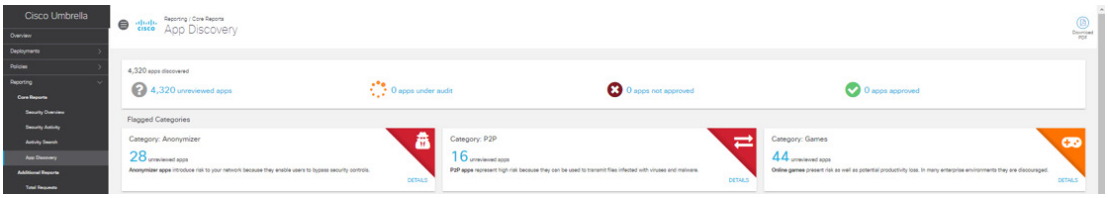


The RSA NetWitness Network analyst team was able to confirm this was an Android device utilizing a terminated app where a user was apparently tricked into pointing at the fake e-store. All of this was shared with the manufacturer representatives for their awareness and intelligence.

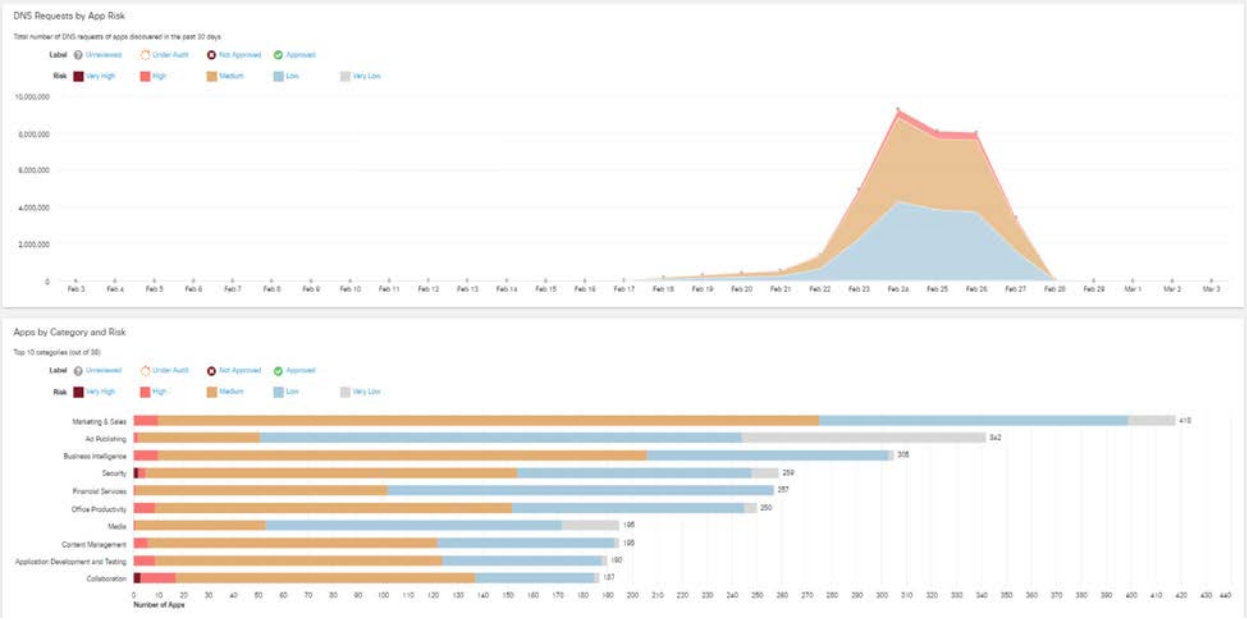


Apps, Apps and more Apps

Over 4,000 applications were identified by the DNS queries at RSAC 2020.



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.



INTRUSION DETECTION

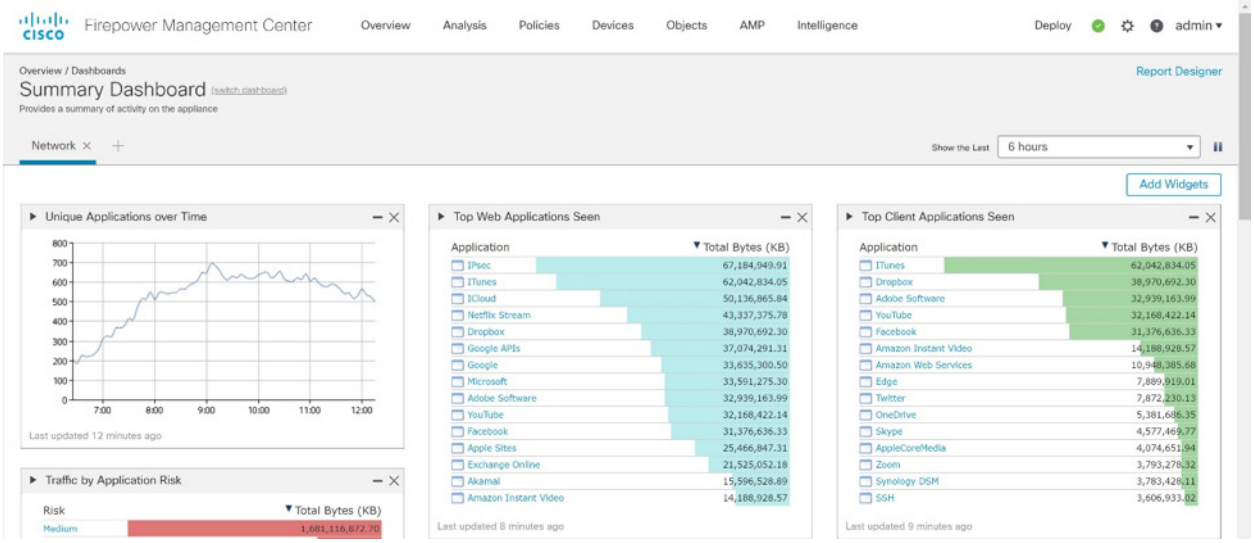
A Cisco Next-Generation Firewall 4110 appliance, running Firepower Threat Defense software, was set up as the perimeter IDS device. The IDS inspected all wireless guest traffic from event attendees, configured in monitor-only mode. Firepower offers breach detection, threat discovery and security automation.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

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.

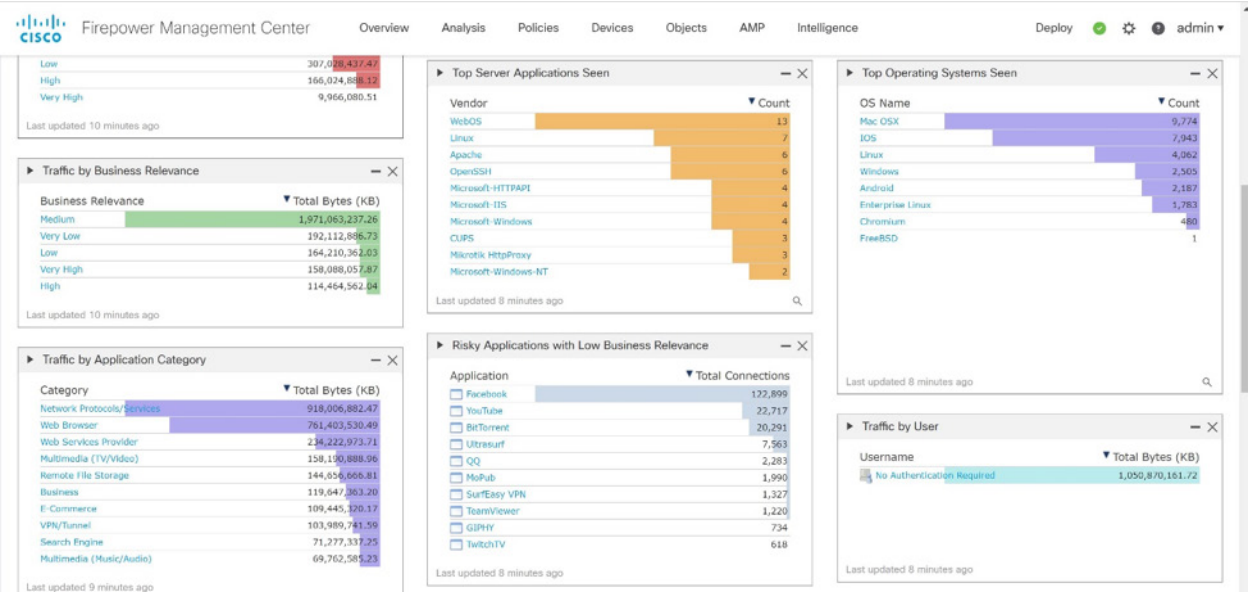


CISCO FMC - TOP DISCOVERED APPLICATIONS

The top operating systems seen in the network were Apple iOS and Mac OS. Apple operating systems usually comprise about 25 percent of the global normal daily use of PC/mobile users. However, RSAC takes place in the San Francisco area and most of the 2020 attendees were from the United States, which explains the relatively large numbers of Apple operating system users. For events in Asia or Western Europe, we usually see the operating system count centered around Microsoft Windows devices and Android phones.

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.



CISCO FMC - TOP OPERATING SYSTEMS AND RISKY APPLICATIONS

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.

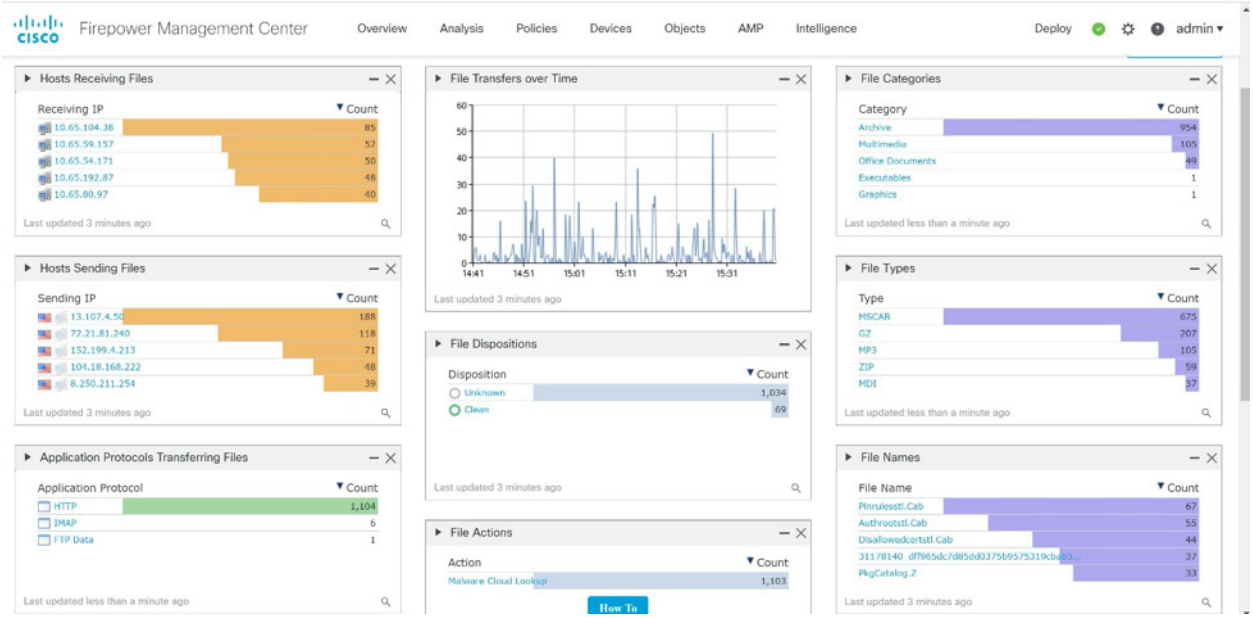
File Transfers

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:

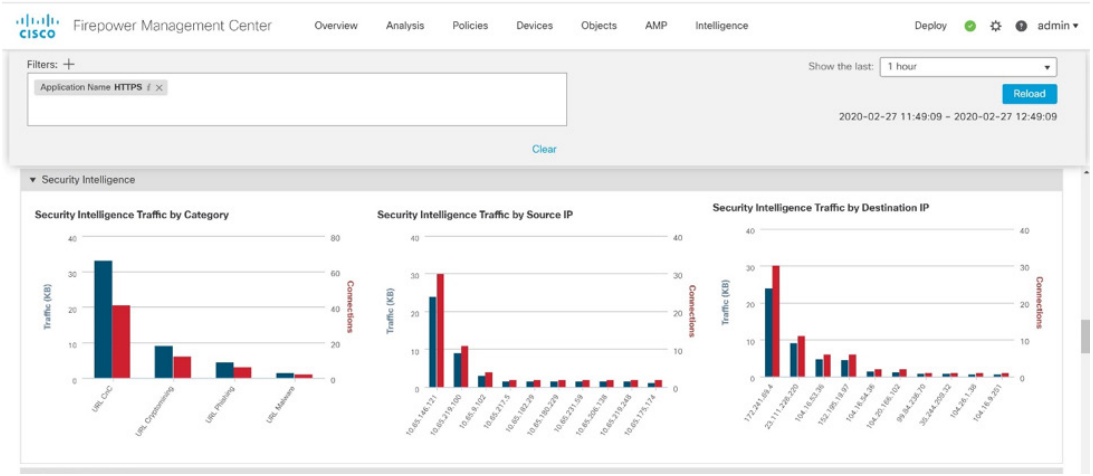
- User education covering email security (what to click and what to not click.)
- Target analysis: Is the company network being targeted specifically with these files?

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 Advanced Malware Protection Cloud Lookup and Talos Intelligence integration.



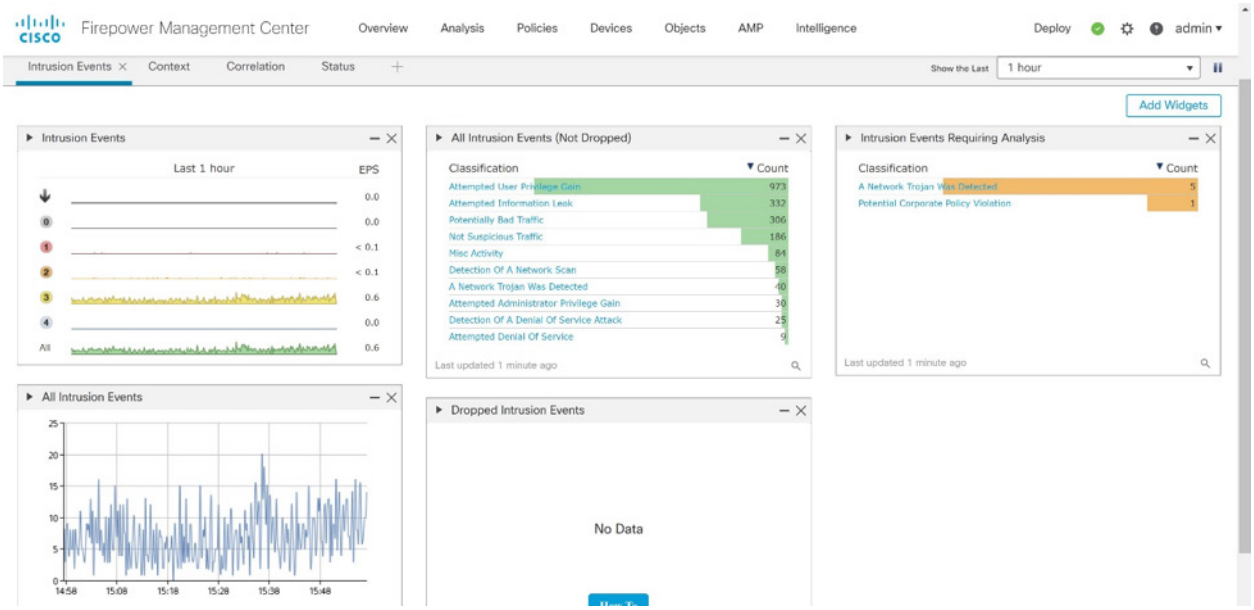
Intrusion Information

During the conference, several intrusion events were recorded by Firepower. Automated event analysis correlated threat events with contextual endpoint 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. For the RSAC SOC team, this helped cut through the noise and focus attention to save precious time.



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.



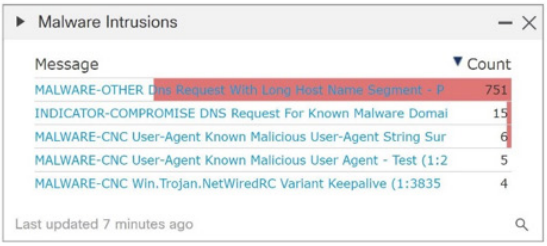
Malware Threats

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

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 ".TG Threat Grid" 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.

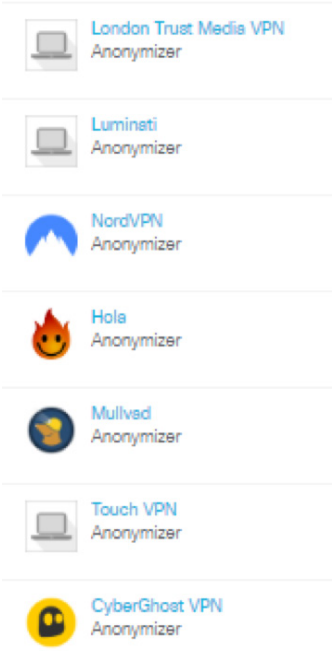
Command-and-control events remain the top type of intrusion events at RSAC in 2020. Command-and-control communications are also used extensively for doing quiet cryptomining in the background of infected devices.



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.

From a metrics perspective, 28 anonymizers were used by those who chose to conceal their information via VPN. The following are the top seven anonymizers at RSAC 2020.



Although we captured more traffic in 2020, the percentage of encrypted traffic remained the same at 78 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 2021!

ACKNOWLEDGEMENTS

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

RSA Staff

Percy Tucker

Neil Wyler

Joshua Randall

Alessio Alfonso

David Nicholson

Ben Prescott

Brandon Barton

Halim Abouzeid

James Pope

Kelly Ahlers

Cisco Staff

Jessica Bair

Michael Auger

Harneet Sigh Virk

Per Hagen

Thanks to ITSP Magazine for taking a tour of the SOC and sharing some of the 2020 findings: https://www.itspmagazine.com/rsa-conference-coverage-posts/what-happened-in-the-soc-at-rsa-conference-2020-a-conversation-with-jessica-bair-and-neil-wyler