RSA CONFERENCE 2020 SECURITY OPERATIONS CENTER FINDINGS REPORT

Published by



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

CONTENTS

Disclaimer	3
The Network	4
Technology Used in the RSAC SOC	5
The Stats	6
The Data	7
Encrypted vs. Unencrypted	7
Cleartext Usernames and Passwords	7
Cleartext Usernames and Passwords: SNMP	7
Cleartext Usernames and Passwords: POP3/IMAP2/HTTP	8
Cleartext Usernames and Passwords: Password Security, Protocol Insecurity	8
Who's Watching the Watchers?	
Mobile Devices and the Apps We Love!	
Location! Location! Location!	
More GPS (NSFW) Three's a Crowd?	
Insecurity as a Service	
GDPR	
Booth Blues	
Outlaw Countries	
Worm or Noisy Scanner?	
Malware Analysis	
Malicious Behavior	
Everything an Attacker Needs for Spear Phishing Lures	
Domain Name Server (DNS)	
Automate, Automate	
Command and Control	
Phishing Domain	
Apps, Apps and more Apps	
Intrusion Detection	
Discovered Applications	
File Transfers	
Intrusion Information	
Malware Threats	
Conclusion	
Acknowledgements	
RSA Staff	
Cisco Staff	

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: <u>https://www.</u> <u>rsaconference.com/usa/the-experience/conference-tips</u> (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.

NOTE: This report was prepared as a summary of the RSA Conference educational SOC exercise. Dell, EMC, 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 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 builtin 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.



RSA

.......

CISCO

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****** @com	Weak 38 minutes	POP3
3 minutes, 1 second ago	@loveyougrifter.com	Very Weak 10 seconds	HTTP
3 minutes, 58 seconds ago	t	Weak 3 hours	HTTP
4 minutes, 23 seconds ago	a******com	Strong 15 years	IMAP2
5 minutes, 59 seconds ago	b*************************************	Very Strong centuries	IMAP2
5 minutes, 59 seconds ago	b****** @itemation com	Very Strong centuries	IMAP2
6 minutes, 56 seconds ago	a********@fillingt	Very Strong centuries	IMAP2
6 minutes, 58 seconds ago	a**********@Billion and	Very Strong centuries	IMAP2

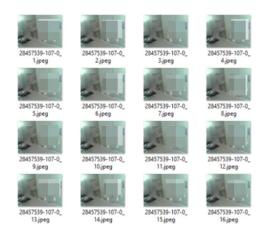
The image above is very interesting and explains the dilemma quite easily. This was written by an RSAC SOC team member to pull data from RSA NetWitness Network. The columns indicate the obfuscated username, password strength, estimated time to crack the password and the protocol used. Does anything stand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

Event Reconstr	Unction Server Server Server Mark 195 00688 (19 10000000 1000 10000 10000 10000 1000000
E Repuest & Response	🕴 🧮 Tag Ta Battan 🗉 🗮 Vee Web 🗄 🔸 Adlans 🗄
107 ringering ogl	
Response .	
Committy in majorited	
10047424	
1-2	
\$	and the second se
2	and the second se
1000	and the second sec
-	
	and the second second second
	*
	and the second se
	A STATISTICS AND A STATIS



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.

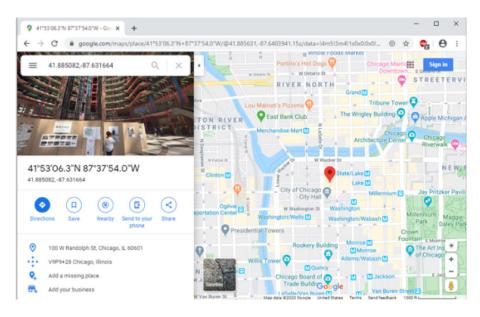


Location! Location! Location!

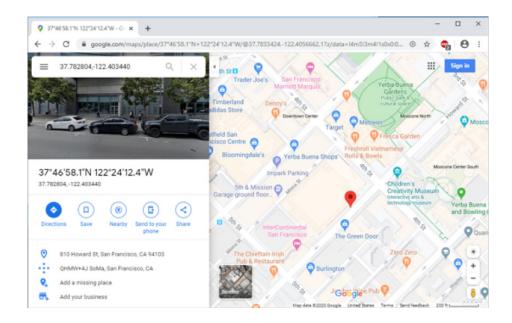
More mobile application lessons learned revolve around location, both past and present. Below we can see an application from an iPhone application that provides no identifiable user information, but provides GPS coordinates in cleartext.

NW SERVICE NWNETHY - Concentrator	SESSION ID 1689594 CALCULATED PACKET SIZE	SOURCE IP-PORT 10.65.178.178 :57152 CALCULATED PAYLOAD SIZE	DESTINATION IP-PORT 80 CALCULATED PACKET COUNT
02/24/2020 08:23:40 am	3559 bytes	2489 bytes	16
REQUEST			
"account_id" : 9933			
}			
}			
Ъ			
"name" : "hand three building t	••*		
}•			
"id" : "74F82128-9CFE-427C-9	CDF-B8B2B4CCBCAD",		
"device" : {			
"ifa" : "F0EDAD00-9018-4F18-	MFC-5A89F7EA321A",		
"osv" : "12.4.5",			
"let" : 1,			
"dpimd5" : "318b183cecbd5015	9b76e371eea896dd",		
"dpidsha1" : "a5a81f9743fa5f	fb4ce4aee7243484447b289188",		
"connectiontype" : 2,			
"os" : "105",			
"geo" : {			
"lat" : "37.782804",			
"long" : "-122.403440",			
"type" : 1			
} ,			
"ip" : "int int int, int,			
"make" : "Apple",			
	; CPU iPhone OS 12_4_5 like Mac OS	X) AppleWebKit\/605.1.15 (KHTML, 1	ike Gecko) Mobile\/15E148*,
"model" : "iPhone"			

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...

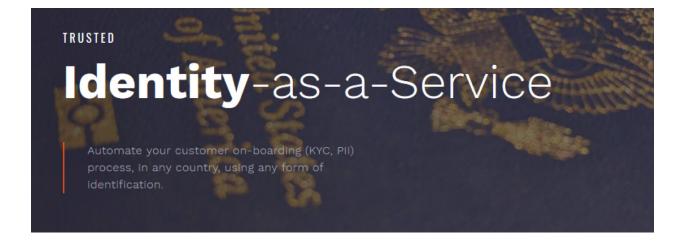


...and then in San Francisco attending the RSA Conference.



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 En	nail 岱 Web 岱	
	Download PCAP V			
	NW SERVICE NWADMIN - Broker	SESSION ID 56301806	SOURCE IP:PORT 10.65.13.61	DESTINATIO
	INVVAL/MIIN - BLOKEI	30301000	: 54533	:80
3:	LAST PACKET TIME 02/25/2020 00:20:35	CALCULATED PACKET SIZE 63002 bytes	calculated payload size 58983 bytes	CALCULATED
в				
	Host:			
3	Connection: keep-al:	ive		
	Cache-Control: max-a	age=0		
1	Upgrade-Insecure-Re	quests: 1		
	DNT: 1			
	User-Agent: Mozilla,	/5.0 (Windows NT 10.0; Win64;	x64) AppleWebKit/537.36 (KHTML	., like Gecko)
	Chrome/79.0.3945.13	0 Safari/537.36		
	Accept: text/html,a	pplication/xhtml+xml,applicati	on/xml;q=0.9,image/webp,image/	/apng,*/*;q=0.8,a
	/signed-exchange;v=	b3;q=0.9		
	Referer: http:/		Login	
	Accept-Encoding: gz:	ip, deflate		
	Accept-Language: en	-US,en;q=0.9,de;q=0.8,da;q=0.7		
	Cookie: ASP.NET_Ses	sionId-hbhp2ncm2t4nigmb2wjishn	1	
			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.

RSA Respond Investigate Monitor Configure Adm	in .	ø
NAVIGATE EVENTS HOSTS FILES ENTITIES MALWARE		
Event Reconstruction	athudon service first pucket time but packet time pucket time policet currt. Rep 10 80 2020-02.24723125.342 2020-02.24723125.7346 216,999 bytes 205,799 bytes 205 Keep, Assembled, App Meta, Network Meta	
🔢 Request & Response 🗧 🗮 Top To Bottom 😑 📷 View Web 😑 🗲 Actions 👳		
(ingle)	ORG Name	
	This invitation was intended for 1000000000000000000000000000000000000	

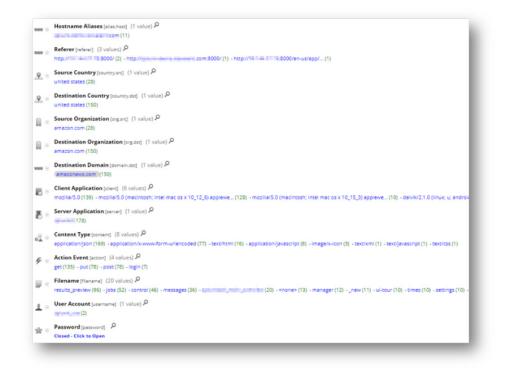
The image above shows another vendor from the expo floor. Clearly this is from a booth kiosk where attendees can sign up for their "Data Privacy and Protection Bootcamp." Perhaps registering for a data privacy and protection bootcamp from a vendor that is not keeping your information private or protected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

ing Percenters.	
1 (Berl (1)) - 1 (B	
On Feb 24, 2020, at 4:25 PH,	ingune mini aggregitera nen wote:
H THEY.	
	uring this time. Would you be able to move this meeting to Wed 2/26 at 11:100am - 12pm PT at the booth?
Respectfully,	
<inage001.png></inage001.png>	
Phone: +1	
ner. liere. are	
Connect with Us: LinkedIn Twitter Facebook	
Linkeoin Twitter Pacebook	
Original Appointment	and contrast is believe over an electronic con-
Sent: Wednesday, January 22, 2020	1:59 PK
	THE VERY COLUMN FRAMEWORK WAS ADDRESS.
Subject: at RSA	terit teritolivat 4 billion, land orbitalization interiority to billion
	5:45 PH-6:15 PH (UTC-07:00) Arizona.
Description	
he generation, evaluation and imple	months immune, enables clients to accelerate growth and achieve best in class positions in growth, innovation and leadersh mentation of powerful growth strategies.
To join our prost more than a pl	lease visit http://www
ined & mellion is committed to a	ensuring your data privacy. For more information please visit our privacy notice to view when a solution is commitment to th
Email Disclaimer	

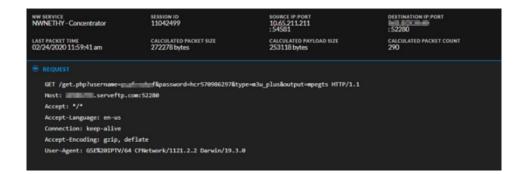
Once again we urge you to comprehend the power of identifying cleartext communication and the implications it can have for your brand, reputation, customers and overall intended experience as a vendor on the expo floor.



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.

NW SERVICE NWNETHY - Concentrator	SESSION ID 11042499	SOURCE IP-PORT 10.65.211.211 :54581	DESTINATION IP PORT						
LAST PACKET TIME 02/24/2020 11:59:41 am	CALCULATED PACKET SIZE 272278 bytes	CALCULATED PAYLOAD SIZE 253118 bytes	CALCULATED PACKET COUNT 290						
			RESPONSE						
Cache-Control: must-revalid	ate								
Pragma: public									
Content-Disposition: attach	ment; filename="tv_channels_m	an a							
#EXTH3U									
#EXTINF:-1 tvg-ID="" tvg-na	ne="# # tvg-logo="	http://www.incoming.com/incoming.com/wp	-content/uploads/2014/11/						
jpg" group-title="",#	10. INVESTIG								
http://www.serveftp.co	n:52280/movie/ /hcr5	78986297/94.mp4							
#EXTINF:-1 tvg-ID="" tvg-na	e-"Inter tyg-logo-"https:/	//www p=========/contents/Publishing	Images/logo_new/Premium/:png"						
group-title="", mmmin #									
http://www.serveftp.com	n:52280/live//hcr57	0986297/72.ts							
#EXTINF:-1 tvg-ID="" tvg-na	ee-"iiiiii iP tvg-								
logo="https://www.	/contents/PublishingImages/lo	go_new/Premium/%07%A1%07%A4%07%95%0	7%A8%D7%982HD.PNG* group-						
title-", Maril #									
http://	n:52288/live//hcr57	0986297/3.ts							
#EXTINF:-1 tvg-ID="" tvg-na	ne-"	//www.g /contents/Publishing	Images/logo_new/P						
group-title="",									
http://diministration.serveftp.com	n:52280/live//hcr57	0986297/16.ts							
#EXTINF:-1 tvg-ID="" tvg-na	me-" tvg-logo-"https:	// M/contents/Publishing	[Images/logo_new/Premium/seriesjpg"						
group-title="",									
http://	n:52280/live/mmilmini/hcr57	0986297/73.ts							
#EXTINF:-1 tvg-ID-"" tvg-na	ne-"im immi" tvg-logo-"http	s://www.pumil/SiteCollectionIma	ges/Lists/channels/AllItems/mum-						
logo.png" group-title=""	- Sector								
http://serveftp.co	n:52200/live/	0986297/5.ts							
#EXTINF:-1 tyg-ID="" tyg-name="@nu hunch 4K" tyg-									

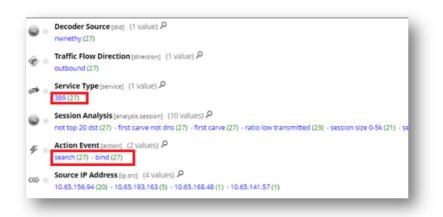
Some organizations are overlooking many security issues that could have an adverse impact on the ability to execute.

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.

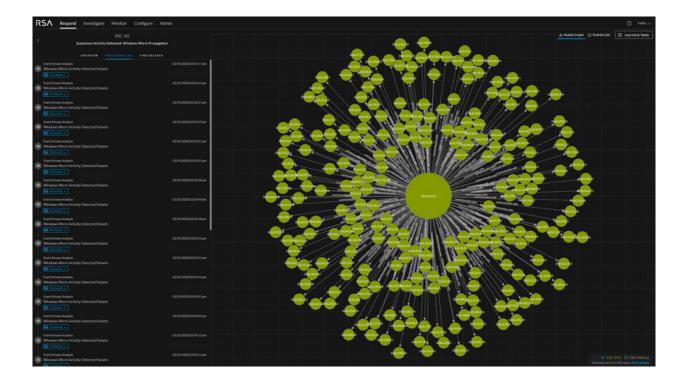
to Events (Asc) Orientonia temayola Decent				Network Event Details	hat Packet File Email				
Constitute Test				NVNETHY Concentrator	303009.10 29004().222	1000812.07.0081 30.63,156,94 134929	Contraction of cont	Servers Serv	00/25/2009/09/37/35 am
				03/25/2020/04/37/35 are	Courter Alleb Packed State \$3063 bytes	CALCULATED NETHOND NETH S2075 bythis	Condition and an internal of Coloneal \$19		
0 00050000003737am	17enwil	-	248	•	nsiteetmattelligCertifica			ENCOLORED.	
0015760091738am	1740441		348			Syning 26		Internet Million	
0.0010100000000000000000000000000000000	1 (helenstij		348	Deveraged, 1-02066661	•••	en-logaritant of Hamilton's Sources en energy (Control of Sources) High's		1146 30/05/000007.07.25.44 418 30007	
eelentronation 🗆	1/envot(sine					901.01 901.02	
C 0215/2000/07.0011 ##	(Persont)		14					1 176.10C H465.KC2E71.00	
0 0035/00800/0036 (#)****	s(retrest)		348	Searchbautitettat.e		ingers	Hart. C	1194.412 Seali RC20(75.00) ETNERT	
C 0015/200008/2013 ##	17454010		348		lejn ee ngt.e .uma.au.			THE ALL THE ALL TRACES OF ALL	
0005/000007846ae	t/wheel					ingal e		Etherhold 2004 winds 1000 Made	
0 00252680938464	1/mont			OP (beites)000014		ingt.e		Print Die Per Print Statis Statie	
C 0275/200007364636	()envol(lagenderigt.e	198.0		BARDED DATA	
D 0005/0000000000	()etert(10				aritesine 4	
	()where the			U.S. Second St.J		net.		27	

					Network Event Details Text Packet File Email 0 Web 0	
Colume Group: Summary List						
					Deveload PCAP ~	
	1116					
00/24/2020/08:58:47 with	1 (Methods)			BINC+ 20.6	Blad secreted	
□ 0094200981847am	1(Noteent)	-	- 2010	6 HC + 108	● maxes ● ••••••••••••••••••••••••••••••••••••	
0 0024900000048484	1.Network)	**	10	NUME - 204	 	
0 02242030983847#	1 Petersk)		248	\$1.00C = 10.6	Storing 75	
0 00042030085855.em	1[Network]			\$1.0°C + 55.0	00180010005590.0.0.005590.000.0000000000	
D 0224202083024am	1(Network)		348	¥1.0×€ * 10.4	- ***** 	
					UNELS AUTOURS DECOMPOSED AUTOURS AUTOUS DESIGNATION	



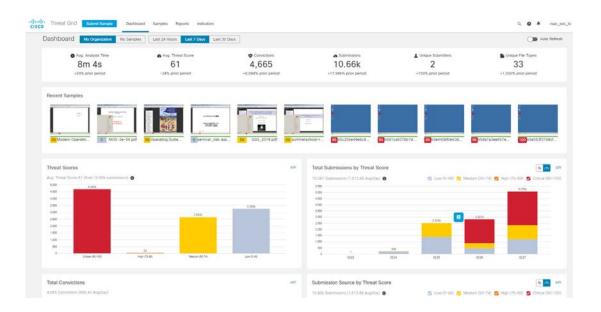
Worm or Noisy Scanner?

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.

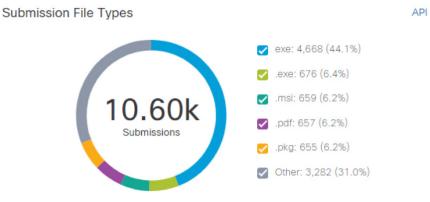


MALWARE ANALYSIS

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.

eport / serveres / coroco	102048/702672320021881571.exe					•	P Report FByRN	F Resident 🛓	Down
Methis Mataking indicating status 100pt Elevania Processes Artifacts Regimp Activity Controllation Created Keys Demons Keys Pile Activity	Metrics 95 Treat Score	See the impact on your encourse. Examine These Response	다 1 Jetyment -	g. 1 Veden -	0 iedicators -	⇒ 1 Bourse -			
	Surger C 2146/882267482394848940558274 Dearment Pr reak, pre O 9 Worksong 244-36 Sameral 2207203.31 20 pre Control 2207203.31 20 pre Samera warman con Particular 214 20 press Maximum Samera warman con Particular 214 20 press Maximum Isamitania Behavioral Indicators	Magic Type File Type Pirst Seen Last Seen SH4-258 SH4-258 SH4-15 accombion MIGS Tagi	exe 2/27/20 3:18:24.pm 2/27/20 3:18:24.pm 0, c5c8439:7100676100 8x0593418/2xx4600261 0250x58x0626468702632	ni 80386, for MS Windows					1
	Only show indicatory with Orbital queries					9, Seath		×	
	> Yms 2		Ordinal Querres	Categories	ATTACK	Tage		Scare -	
	> Artifact Plagged as Known Trojan by Antivitus			artistus -		(BAT) Buger	3	-	
	> Artifact Flagged Malcious by Arthmus Service			-		(seea) [84]		95	
	> Registry Persistence Mechaeisri Refericts an Ese	cutable in a flystern Directory.	Ototal Queens	Jacantone -	perastence	autonal compound process reports		90	

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.

Overview Analysis	Policies Devi	ces Objects AMP	Intelligence							y 🗢 Sy	stem Help +	phagen +
Context Explorer Co	nnections * Int	rusions * Files + Netv	vork File Trajectory H	osts • Users • Correlation •	Advanced • Search	1						
Network File Tr	ajectory for	ff190475014	1aaa2									
File Name File Size (KB) File Type File Category Current Disposition Threat Score	f1904750141aaa2 t048a4259a750c7tcb 85.0322 MSEXE Executables © Malware & None W32.FF190475F6-95	c80963d589a667			First Seen Last Seen Event Count Seen On Seen On Breakdown	2020-02-26 17: 2 3 hosts (2 displ	09:03 on 208.67.174. 33:31 on 200 10.65.200.2 ayed) seceivers (1 → 1 displayed	40 by 🕌 <u>No Ar</u>				
Trajectory 208.67.174.37	Feb 26 13:09 17:33											
10.65.200.240	0 0											
Events O Trans	fer <u></u> Block	⊙ Create ⊙ Move	(▷ Execute ○ Scan	Retrospective Quarantine								
Dispositions O Unker	own 🙀 Malware	O Clean O Custom	C) Unavailable									
Events												
Time	Event Type	Sending IP	Receiving IP	User	File Name	Disposi	Action	Protocol	Client	Web Appli	Descriptio	n
2020-02-26 13:09:03	Transfer	208.67.174.37	10.65.200.240	No Authentication Required	f048a4259a750c7fcbc809f	5 Unknown	Malware Cloud Lookup	HTTP	Wget		Retrospecti	ve Event,
2020-02-26 17:33:31	Retrospective I	L				Malware						

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.

	ojan by Antivirus				
core 95 Hits: 3					
escription					
	s a Trojan. A Trojan is a program that gains privileged access tem. Trojans may steal information or infect the host systems				
rigger					
his indicator is triggered when antiviru	flags an artifact and the signature contains 'Trojan'.				
Inifact	SHA256	Path		Antivirus Result	
Artifact 1	c5c843fe77d06761b6b308bc880x99b9 9b125fab57259dee736f30	169464aa51 🔄 0212	c9ab2648f702b7232002f88157f.exe	Win.Trojan.Dialer-513	
Artifact 3	c5c843fe77d06761b6b308bc880a99b9 9b125fab67259dee736f30	169464aa6f	P102f2bc9ab2648f702b7232002f88167f.exe	Win Trojan Dialer-513	
Artifact 9	c5c843fe77d06761b6b308bc880x99b9 9b125fab57259dee736f30	169464aa5f [3] Win	dows/Wild-Files.exe	Win Trojan Dialer-513	
Artifact Flagged Malicious by Antivi	a Service	antiv		artive.s Ne	3
Artifact Flagged Malicious by	Antivinie Sanúca				
	Antivirus Service				
NOW DE Hits 2					
core 95 Hits 3 Description					
lescription n antivirus service flagged an artifact a can a file and the scan results of all en	s malicious. When using antivirus software, rehying on a sing pres are taken together to make a more accurate determinat variable.				
escription n antivirus service flagged an artifact a can a file and the scan results of all en itivirus engine scans are displayed, if r	ines are taken together to make a more accurate determinat				
lescription n entivirus service flagged an artifact a can a file and the scan results of all en thivirus engine scans are displayed, if a rigger	ines are taken together to make a more accurate determinat				
Description in antivirus service flagged an artifact a can a file and the scan results of all en itbivirus engine scans are displayed, if a rigger	gines are taken together to make a more accurate determinat variable.				

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

Score: 40 Hits: 1 Description	ed Autorun Registry Key	, 10000					MIRE amore Persistence Tactic ID: TA0003	attack mitre or
located in subkeys R. Trigger	can be used to load application: m, RunOnce, RunServices, RunS ered by a modification to the Run	ervicesOnce, RunOnceEx, i	or RunOnce\Setup. The	key value will indicate whe	re the program that will load		Techniques: Registry Folder The adversary is tryin foothold. Persistence that adversaries use to	g to maintain their consists of technique
Process	Process Name	RegKey Name	Regiliery Value Name	RegKey Data Type	ny. RegKey Data	Actions	systems across restar credentials, and other	ts, changed interruptions that
Process 4	02f2bc9eb2648f702b72 32002f88157feae	MACHINE\SOFTWARE\W OW6432NODE\MICROS OFT\WINDOWS\CURREN TVERSION\RUN	Wild-Flics	sz	C:\Windows\Wild- Flics.exe -ns\\0	Q, Ortsital Query	 could cut off their acc for persistence includ or configuration chang maintain their footbole replacing or hijacking adding startup code. 	e any access, action, ges that let them I on systems, such as

Also, malicious behavior included injecting code into memory.

Potential Code Injection Del	ected		MITRE ATTACK attack mitre or
core: 25 Hits 2			Privilege Escalation
Description			Tactic ID: TA0004 🖾
xecution Prevention (DEP) which prov occess violation will occur. Malware wi ubmitted sample allocated a memory	ided protection against this type of attack. If an attempt to execu II often allocate memory in which it will inject code. In order to b	a) and then the application executes the malicious code. Windows introduced Data de code is made in a page that does not have the PAGE_EXECUTE_ protection, an ypass DEP the allocated memory must be marked Read, Write and Execute. The dicate the presence of code injection, into itself or a remote process.	Techniques: Extra Window Memory Injection Process Injection The adversary is trying to gain higher-level permissions. Privilege Escalation consists techniques that adversaries use to gain
ngger			higher-level permissions on a system or
his indicator triggers if a process allo	cates memory with full read, write, and execute permissions.		network. Adversaries can often enter and explore a network with unprivileged access
Yocasa	Address	Process Name	but require elevated permissions to follow
Process 4	2003501056	0212bc9ab2648f702b7232002f88167f.exe	 through on their objectives. Common approaches are to take advantage of syste weaknesses, misconfigurations, and
Process 4	2004549632	02f2bc9ab2640f702b7232002f88157f.exe	vulnerabilities. Examples of elevated acces
			These techniques often overlap with Persistence techniques, as OS features tha let an adversary persist can execute in an elevated context.
			Defense Evasion Tactic ID: TA0005
			Technique: Erta Window Memory Heidel © Process Repetion @ The adversary is trying to avoid being detected. Determine basissin consists of techniques that adversaries use to avoid detection throughout their components. Techniques used for defines evasion include unimating/isolabiling security software or cohacating/encrypting data as chrotia. Adversaries also fereings and abuse finulated processes to table and down funded processists to their adver- techniques include the added benefit of subwriting definese.

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.

Top Behavioral Indicators	•				🚩 🕷 🛛 API
Potential Code Injection Detected					3,259
Artifact Flagged Malicious by Antivirus Se	rvice			2,710	
Machine Learning Model Identified Execut	able Artifact	t as Likely	/ Mali	2,620	
Static Analysis Flagged Artifact As Anome	lous			2,550	
Process Modified an Executable File			2,325		
Artifact Flagged by Antivirus		2,161			
Executable with Encrypted Sections	1,965				
Artifact Flagged as Known 1,685					
Excessive Proce 1,464					
Creation Of Ra 1,452					

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.

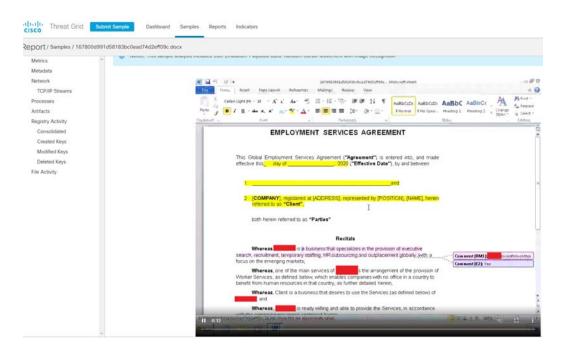
Process Checked for Softio	DE		MITRE atmox	attack.mitre.or
Score: 66 Hits: 1			Discovery	State State State
Description			Tactic ID: TA0007	
A process attempted to open a conne the presence of Soft/CE as a means o	ction to the SoftiCE drivers. SoftiCE is a kernel-mode debugger for Windows, o f anti-analysis.	often used as a reverse-engineering tool. Malware may do this to detect	Techniques: Virtualizati	lion/Sandbox Evasion
Trigger			The adversary is trying environment. Discovery	
This indicator is triggered when a file	handle for one of the SoftICE drivers is requested.		techniques an adversa	ry may use to gain
Process	Process Name	Path	knowledge about the s network. These technic	ques help adversarie
Process 4	02f2bc9ab2648f702b7232002f88157f.exe	ntice	observe the environme themselves before dec	
			They also allow advers they can control and w entry point in order to i benefit their current ob operating system tools toward this post-comp gathering objective.	what's around their discover how it could bjective. Native s are often used

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.

	Crice Activity Volume				Sametrie
Deskyments)					
	· · · · · · · · · · · · · · · · · · ·				VIEW CHENG CHEN THE
esting	Q, Fitter by sportsy				
Core Reports	Feouetts				
	repres				
Security Activity		Alassed	Bulad	Test	3. of Tax
Activity Search	 Becumy 	14,700		14,190	0.04%
App Discowy	0 - Peven	eans	(6	8,476	0.021
Additional Reports	- What	2,176		3,376	0.00629
Trui Pagaiere	- Dynamic DNS	LIB		1,408	0.0037
	- Nervly Seen Domaina	2,541		2,841	0.0078
Top Destinations	 Potentally namba 	1248		1.010	0.0048
Top Categories	- Dra Turneling	(K)		1	a 5000
Top Identities	- Oyeamong	24		36	0.0007
Managarant .	0 - Ceter	2,344		2,000	8.00671
Equited liquits	- Command & Control	2,488	1	1.00	0.0069
Scheduler Reports	- Provid				8.00021
Admin Auditing	e - inspatore	2.741	1	8/41	0.0044
	Camportes			0	0.00
***	Destructor Lans	59,907	0	68,907	0.141
Annual fait 1 RSA.07 - Date 10	Permitted	36,520,402		36,420,412	10.42
	Trui.	26.201.000		20.001.000	100

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.

Cisco Umbrella		LAST 24 HOURS
	Pernography Sincest Michael Action	
	Pernography мижеля молети саптосния саптосния на политика и п Политика и политика и по Политика и политика и Политика и политика и политик Политика и политика и политик	
Reporting >	310 Réquests	
	ALLOWTOBLOCKED GLODAL TRAFFIC %	
Jessica Bair PEA SF - Conta BD	28	
	10	
	100 million (100 m	
	107.44 U00.FM 400.FM 107.FM 10.64M 400.AM	
	a los nos contra contra contra contra contra contra contra contra contra	
	VEW XXXXXX	KOLXXX IN INVESTIGATE

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.

DNS Bot APP 3:11 PM Domain: directnavbt.com	
Categories:	
Malware	Cisco AMP Threat Grid
Timestamps:	
2020-02-27 2:54:07 PM	
Pivot to NetWitness for 1 domains	
	Domain: directnavbt.com Categories: Malware Timestamps: 2020-02-27 2:54:07 PM

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.

Cisco Umbrella		Record / Core Records								(±) =	LAST7D
inlev /	- cisco	 Activity Search 							Schedule	Download	
ploymenta >											
cen >	0	Q. Search request activity	Advanced *	CLEAR					Colu	minis All Red	uests -
oring 🖂 🖂	-										
ura Reporta		тосных О Теблусана ж									
Security Overview	0	Vening activity from Feb 21, 2020 at 12:00 AM to Feb 27, 2020 at 8:55 A	M						tesuits per page:	50 = 51 - 100	< >
Security Activity				Identity Used by Policy							
Activity Search	< C	Destination		0	Innertal SP	External IP	Acteo	Categories	Application 0	lame & Time 👃	
Age Discovery	- 1	Joleo _stop dc _mudos hušnýc org		A RSAC USA - 1			a Allowed	Command and Control	1	eb 27, 2020 at 9:08	AM ()
AStinnal Reports	14	Jdap _sca default-first-stie-name _steas dc _middes hidinye org		A REACUSA - 1			· Aloued	Command and Conimal	1	ев 27, 2029 м 9:08	AM G
Total Requests	24	wpad hidopt.org		A RSACUSA - 1			o Allowed	Command and Control	F	wb 27, 2020 at 0.08	AM 🕞
Activity Volume	-1	sepad hidinys org		A READUSA - 1			Allowed	Command and Control	F	eb 27, 2010 at 5.08	M @
Top Destructions	-1	wpad heSinyc org		A READUSA - 1			o Allowed	Convenient and Control	F	eb 27, 2020 at 9.07	AM Θ
Top Categories	-1	wpatch days org		A RSAC USA - 1			O Allowed	Command and Control		eb 27, 2020 st 9:07	*** 🕞
Top Identifies	1	hithe-offguelik hallow, org		IL REACUSA - 1			o Aloved	Command and Control	1	eb 24, 2020 # 5:24	PM (
	- 1	Nithe-off puells hedrec ang		A REAC USA - 1			O Aloned	Command and Control	F	et 24, 2020 # 5 24	PM G
Exported Reports	- 1	psha5oyc-psw01.hv0nyc.org		A RSAC USA - 1			O Allowed	Command and Corect	8	eb 24, 2020 xt 5:24	PM Θ
Scheduled Reports	-1	pabadaye-paur01.hadaye.arg		A REACUSA - 1			O Allowed	Command and Control	1	eb 24, 2020 at 5/24	PM 🕞
Adres Auto Log	- t	pshuSeyc-peur01.huSeyc.org		A RSAC USA - 1			& Aloxed	Command and Control	1	eb 24, 2020 at 5/24	PM Θ
	-1	path-diaye-payr01.hdsnyt.org		A REACUSA - 1			6 Allowed	Command and Control	4	wb 34, 2020 at 5:24	PM Θ
	- 1	pshkSeyc-peer01.hkSnyc.org		A RSAC USA - 1			O Allowed	Command and Control	5	eti 24, 2020 at 5/24	PM Θ
	11	pstikSeyc-psvr01 habryc.org		A RSACUSA - 1			6 Allowed	Command and Control	5	eb 24, 2020 at 5:23	PM 🕞

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

Investigate			
SEARCH PATTERN SEARCH			
hx5nyc.org		INVESTIGATE	Google VirusTotal
Summary			
100 High Risk ■ The da ■ The da	Command and Control Block List emain is classified as High Risk due to a combination of high security features. is domain is associated with blocked IP addresses: 184 168 221.32 rtty Categories Content Categories mmand and Control		
The domain's risk score is calculated u	sung the following security indicators. 59/100	Keyword Score	13/100
This domain has a slightly unusua	111.1110.	This domain does not share keywords domains.	
Lexical Score	40/100	TLD Rank Score	2/100
This domain shares some lexical domains.	content with known malicious	This domain belongs to a top level don few malicious domains.	nain which contains relatively
Umbrella Block Status 🛛 💿	100/100		
This domain is blocked by Umbre	ila.		

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

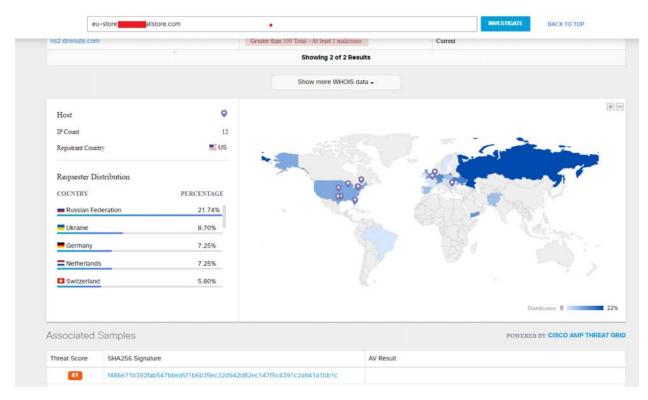
In another incident, we observed a device on the wireless network beaconing out every hour to a malicious, parked domain designed to emulate an e-store in the European Union for a global mobile device manufacturer. The morning after the first observation, representatives of the manufacturer attending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

	e disco Activ	ity Search					Schedule Download	
ploymenta >								
	Q Q 5000	h request activity	Advanced * CLE	AR			Columns All	Requests +
Core Reports	1 DOMAIN	eu-atore alistere com x						
Security Overview	O Versing activity (Inum Feb 21, 2020 at 12.00 AM m Feb 27, 3	MA 12:6 m 0.27 AM				Results per page: 50 = 1 - 24 d	of 24
Security Activity	Identity	Demoution	Infeating Used by Policy	Internal IP External IP	Action	Categories	Application Date & Time	
	A RSAC USA - 1	su-store	A RSAC USA - 1		O Allowed	Parked Domains, Malware	Feb 27, 2020 at 8:59	AM 💮
App Discovery	A RSAC USA - 1	eu-store affatore com	A READ USA - 1		© Allowed	Parked Domains, Malware	Feb 27, 2020 at 7:59	
Additional Reports	盖 RSAC USA - 1	eu-store distore.com	A RSAC USA - 1		O Allowed	Parked Comains, Malware	Feb 26, 2020 at 4.59	PM 👄
Total Requests	# R5AC 05A - 1	eu-store allatine com	A RSAC USA - 1		O Allowed	Parked Domains, Malware	Feb 26, 2020 at 3:59	
Activity Volume	击 RSAC USA + 1	eu-store, elistore.com	A RSAC USA - 1		O Allowed	Parked Domerne, Malware	Feb 25, 2020 at 2 59	PM 😐
Top Destinations	# RSAC USA - 1	eu-store	A RSAC USA - 1		O Allowed	Parked Domains, Malware	Feb 26, 2020 at 10:50	MA 0
Top Cetegories	A RSAC USA - 1	eu-store distore.com	A READ USA - 1		O Allowed	Parked Domains, Malware	Feb 26, 2020 int 9.59	AM 💮
Top Identities	AL RSAC USA + 1	eu-store Patore com	A REAC USA + 1		O Allowed	Packed Domains, Malware	Feb 26, 2020 at 7:59	AM 🕞
Menagement	di RSAC USA - 1	au-store distore com	A RSAC USA - 1		O Allowed	Parked Dombins, Malware	Feb 25, 2020 at 4.59	РМ 🕞
Exported Reports	A RSAC USA + 1	eu-store Bitom com	击 RSAC USA - 1		O Ahowed	Parked Domains, Mahvare	Feb 25, 2020 at 3:59	PM 😑
Scheduled Reports	A RSAC USA - 1	eu-store allstore.com	A RSAC USA - 1		O Allowed	Parked Domains, Malwais	Feb 25, 2020 at 2.59	РМ 💮
Admin Audit Log	曲 RSAC USA - 1	eu-store distore com	A RSAD USA - 1		O Allowed	Parked Domains, Malware	Feb 26, 2020 of 1.59	РМ 💮
The bill enders	A RSAC USA - 1	eu-store, allstore.com	A RSAC USA - 1		· Allowed	Parked Domains, Malware	Feb 25, 2020 at 10:59	9.AM 😐

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.

	re.com	ESTIGATE
Summary		
	eu-store.	
100 N	The domain is classified as High Risk and is blocked due to its association with Adware	
High Risk	Security Categories Content Categories	
SECURITY INDICATOR	Malware Parked Domains	
Time		
Timeline		Current Content Category: P
M DNS Queries	Domain Events ONS Changes	Jan 28th, 2020 - Feb 27th, 2020
62		Max. Queries:
37		

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.

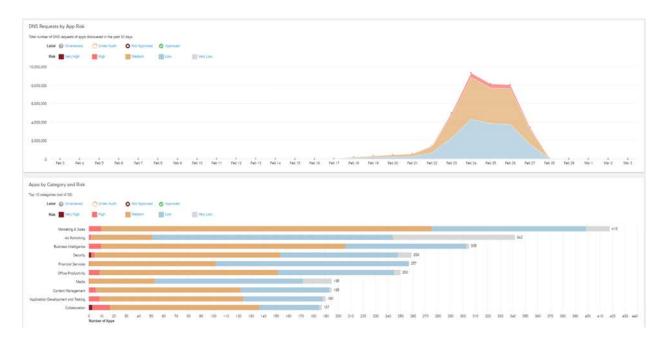
88 Apps	Ontenning	A ferrer	Tan abasta	Manusalasaa			
# Apps	Categories 🗸	Home	Top charts	New releases			
My apps							
Shop					100		
						(Termir	nated)
Games						Productivity	* * * * = 163,422 🚊
Family					E Everyone		
Editors' Choice							Contraction of the
ccount					Add to Wish	hlist	Install
ayment methods							
ty subscriptions							
edeem							Q 2245
uy gift card						MY RECENT CONTENTS	
ly wishlist					Concern various devices to enjoy your content anytime, anywhere		\square
ly Play activity				\sim			Web (torage head, heads
arent Guide					-		Tegateled devices
						-	

Apps, Apps and more Apps

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

Cisco Umbrella	e decring (Con Reports case App Discovery				0
	4,320 apps discovered				
Reporting V	4,320 unreviewed apps	0 apps under audit	(R) 0 apps not approved	O apps approved	
	Flagged Categories				
	and the first sector of the first sector.				
	Category: Anonymizer	Category: P2P	2	Category: Games	. 000
	28 unreviewed appa	16 unreviewed apps		44 unwiewed apps	
Additional Reports	Anonymizer apps introduce risk to your network because they enable users to by		cause they can be used to transmit files infected with viruses and maiware.	Online games present risk as well as potential productivity loss. In many enterprise environments they are discouraged.	
		DETALS	DETALS		DETAILS

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

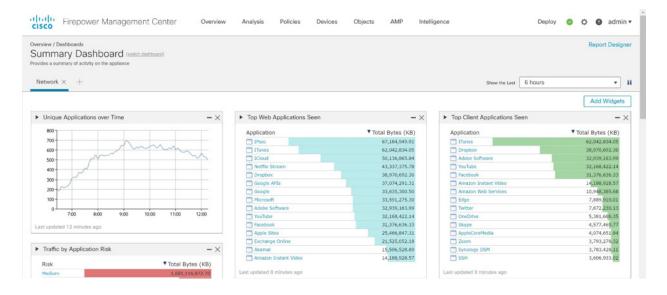
A Cisco Next-Generation Firewall 4110 appliance, running Firepower Threat Defense software, was set up as the perimeter IDS device. The IDS inspected all wireless guest traffic from event attendees, configured in monitor-only mode. Firepower offers breach detection, threat discovery and security automation. 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.





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.

	307,0 <mark>28,437.47</mark>	Top Server Applications Seen	- ×	Top Operating Systems Seen	- 2
High	166,024,88 <mark>8.12</mark>	rop ourrer reprice ourres occit	- ^	rop operating ofsterns over	
Very High	9,966,080.51	Vendor	Count	OS Name	Count
ast updated 10 minutes ago		WebOS	13	Mac OSX	9,774
		Linux	7	IOS	7,943
		Apache	6	Linux	4,062
Traffic by Business Relevance	- ×	OpenSSH	6	Windows	2,505
		Microsoft-HTTPAPI	4	Android	2,187
Business Relevance	Total Bytes (KB)	Microsoft-IIS	4	Enterprise Linux	1,783
Medium	1,971,063,237.26	Microsoft-Windows	4	Chromium	480
Very Low	192,112,886.73	CUP5	3	FreeBSD	1
Low	164,210,362.03	Mikrotik HitpProxy	3		
Very High	158,088,057.87	Microsoft-Windows-NT	2		
High	114,464,562.04	Last updated 8 minutes ago	Q		
ast updated 10 minutes ago		 Risky Applications with Low Business 	s Relevance — X		
Traffic by Application Category	- ×				
Traffic by Application Category		Application	Total Connections	Last updated 8 minutes ago	c
Traffic by Application Category Category	- × ▼ Total Bytes (KB) 918.006.882.47	Application	▼ Total Connections 122,899	Last updated 8 minutes ago	c
Traffic by Application Category	▼ Total Bytes (KB)	Application Facebook YouTube	▼ Total Connections 122,899 22,717		
Traffic by Application Category Category Network Protocols/Schribes	▼ Total Bytes (KB) 918,006,882.47	Application Facebook VolTube BitTorrent	▼ Total Connections 122,899 22,717 20,291	Last updated 8 minutes ago Traffic by User	
Traffic by Application Category Category Network Protocols/Services Web Browser	▼ Total Bytes (KB) 918,006,882.47 761,403,530.49	Application Facebook YouTube BitTorrent Uttresurf	▼ Total Connections 122,899 22,717 20,291 7,563		⊂ Total Bytes (KB)
Traffic by Application Category Category Network Protocols/Services Web Browser Web Services Provider Multimedia (TV/Mdec)	▼ Total Bytes (KB) 918,006,882.47 761,403,530.49 234,222,973.71	Application Freebook YouTube BitTorrent Uttresunt QQ	▼ Total Connections 122,899 22,717 20,291 7,563 2,283	 Traffic by User 	-
Traffic by Application Category Category Network Protocols/Services Web Browser Web Services Provider Multimedia (TV/Video) Remote Tills Storage	Total Bytes (KB) 918,006,882.47 761,403,530.49 214,222,973.71 158,130,888.96	Application Freebook VouTube BitTorend Utresurt QQ Mol-ub	▼ Total Connections 122,899 22,717 20,291 7,563 2,283 1,990	 Traffic by User Username 	Total Bytes (KB)
Traffic by Application Category Category Network Protocols/Services Web Browser Web Services Provider	▼ Total Bytes (KB) 918,006,882.47 761,403,530.49 214,222,973.71 159,190,888.96 144,656,666.81	Application Freebook YouTube BitTorrent Uttresunt QQ	▼ Total Connections 122,899 22,717 20,291 7,563 2,283 1,990 1,327	 Traffic by User Username 	Total Bytes (KB)
Traffic by Application Category Category Network Protocols/Services Web Brovices Web Brovices Provider Multimedia (YV/Video) Remote File Storage Business	 Total Bytes (KB) 918,006,882.47 761,403,530.49 214,222,973.71 159,150,880.96 144,659,606.81 119,647,363.20 	Application Frochook YouTube BriTorrent Utarsurf QQ MoPub SuffExy VPN	▼ Total Connections 122,899 22,717 20,291 7,563 2,283 1,990	 Traffic by User Username 	Total Bytes (KB)

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.

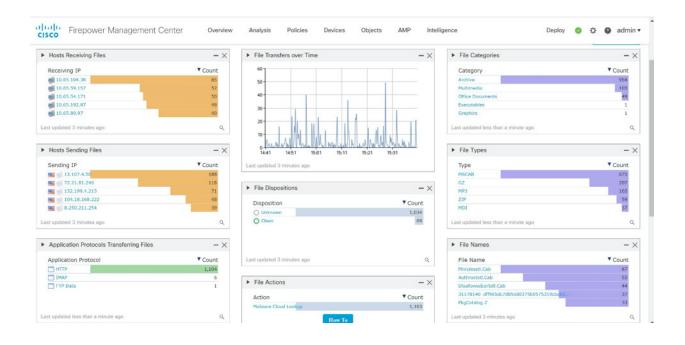
File Transfers

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.

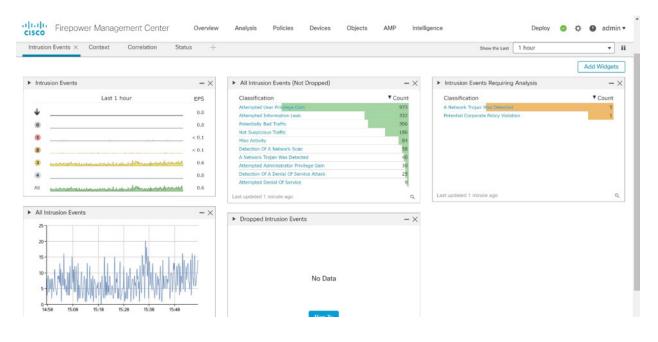


Intrusion Information

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.

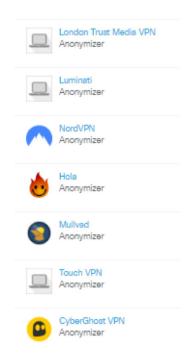
Command-and-control events remain the top type of intrusion events at RSAC in 2020. Command-andcontrol communications are also used extensively for doing quiet cryptomining in the background of infected devices.

Malware Threats	- ×	 Malware Intrusions 	-
Detection Name	▼ Count	Message	▼ Count
W32.01A092C611-100.SBX.TG	1	MALWARE-OTHER Ins Request With Long Host Name Segment - P	751
W32.1BCD17DB4D-95 SBX.TG	1	INDICATOR-COMPROMISE DNS Request For Known Malware Domai	15
W32.3A4EB6706B-95.SBX.TG	1	MALWARE-CNC User-Agent Known Malicious User-Agent String Sur	6
W32.432665F4D1-95.5BX.TG	1	MALWARE-CNC User-Agent Known Malicious User Agent - Test (1:2	5
W32.465DB4BDF4-95.56X.TG	1	MALWARE-CNC Win.Trojan.NetWiredRC Variant Keepalive (1:3835	4
ast updated less than a minute ago	Q	Last updated 7 minutes ago	c

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: <u>https://www.</u> itspmagazine.com/rsa-conference-coverage-posts/what-happened-in-the-soc-at-rsa-conference-2020-aconversation-with-jessica-bair-and-neil-wyler



RSA

©2020 Dell Inc. or its subsidiaries. All rights reserved. RSA and the RSA logo, are registered trademarks or trademarks of Dell Inc. or its subsidiaries in the United States and other countries. All other trademarks are the property of their respective owners. RSA believes the information in this document is accurate. The information is subject to change without notice. Published in the USA 5/20 H 18325

cisco.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)