

# RSA® Conference 2022

San Francisco & Digital | June 6 – 9

## TRANSFORM



SESSION ID: MASH-R05

## EXPOSURE: The 3rd Annual RSAC SOC Report

**Steve Fink**

Regional VP  
NetWitness  
@InfoSecFink

**Jessica Bair Oppenheimer**

Director, Technical Alliances  
Cisco Secure  
@jessicambair

**Dave Glover**

Principal System Engineer  
NetWitness  
@rsa\_logfather

# Disclaimer

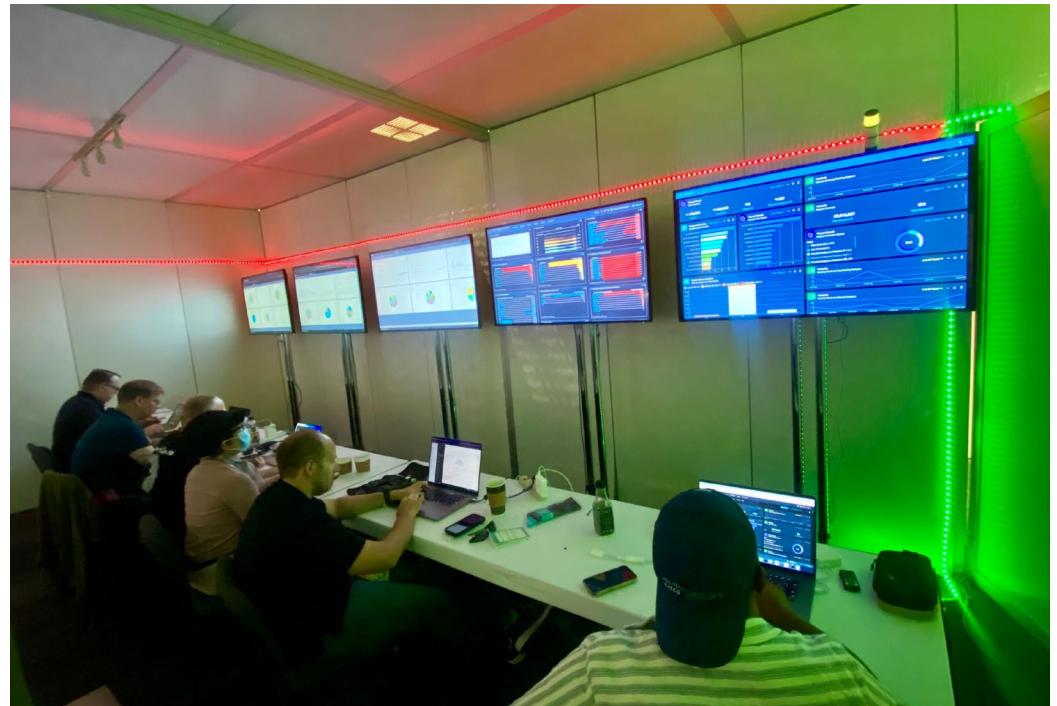
Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

©2022 RSA Conference LLC or its affiliates. The RSA Conference logo and other trademarks are proprietary. All rights reserved.



# RSAC SOC



- 7 Years Running
- 10 Tours: 20-50 people each
- Countless “Private” Tours
- Multiple Press Interviews
- Annual Findings Report
- Conference Span/TAP
- NetWitness Platform XDR
- NetWitness Orchestrator
- Cisco SecureX XDR
- Cisco Secure Malware Analytics/Threat Grid
- Cisco Umbrella DNS
- Cisco Secure Firewall – Intrusion Detection
- Cisco Talos Intelligence
- IBM X-Force Exchange
- alphaMountain.ai
- Recorded Future

# The Team

- 5 NetWitness Analysts
- 9 Cisco Analysts
- 1 IBM Threat Hunter



# The Dashboards

The screenshot displays the RSA Threat Hunting Dashboard interface, which includes several interconnected dashboards:

- Threat Category**: Shows session count trends over the past 24 hours.
- Indicators of Compromise (IOC)**: Displays a bar chart of top user agents and behaviors of compromise, along with detailed tables for each category.
- Top User Agents (100)**: A bar chart showing session counts for various user agents, last updated at 10:55:11 am.
- Top Behaviors of Compromise (10)**: A donut chart showing session counts for behaviors like suspicious TCP beaconing and large outbound data transfers, last updated at 10:55:07 am.
- Top Destinations (25)**: A donut chart showing session counts for various destination domains, last updated at 10:55:07 am.
- Top IOCs (21)**: A donut chart showing session counts for indicators of compromise, last updated at 10:55:07 am.
- Top Risky Files (25)**: A donut chart showing session counts for risky files, last updated at 10:55:08 am.

Below these dashboards are detailed tables for each category:

- ALL CLIENT KEYS**: List of client keys and their session counts.
- BEHAVIORS OF COMPROMISE**: List of behaviors and their session counts.
- DESTINATION DOMAIN**: List of destination domains and their session counts.
- INDICATORS OF COMPROMISE**: List of indicators of compromise and their session counts.
- FILENAME**: List of filenames and their session counts.

The bottom of the dashboard features a navigation bar with icons for back, forward, and search, as well as a URL field showing <https://10.40.12>.

# More Dashboards!!!

**SecureX Dashboard**

**Enabled Integrations:**

- \*Secure Firewall
- \*Secure Malware Analytics
- \*Umbrella

**RSAC SOC:**

**\*Secure Malware Analytics Threat Scores** Last 7 Days

Low (0-49) (422) Medium (50-74) (25) High (75-89) (8) Critical (90-100) (3)

**\*Secure Malware Analytics Total Submissions by Result** Last 7 Days

Complete (169) Innocuous (2) Archive Unknown Password (1) Archive Not Contain Supported (260) Filetype Not Supported (26)

**\*Secure Malware Analytics Total Submissions by Threat Score** Last 7 Days

Low (0-49) (422) Medium (50-74) (25) High (75-89) (8) Critical (90-100) (3)

**\*Umbrella Security Blocks by Cryptomining Category** Last 7 Days

**\*Umbrella Request Summary** Last 7 Days

26,301,669 Total Requests 0 Total Blocked

**\*Umbrella Security Blocks by Phishing Category** Last 7 Days

**\*Secure Firewall Incident Promotion Reason** Last 7 Days

Items

- Talos Disposition (356)
- User Promoted (6)
- Security Intelligence Category: IP (232)
- Security Intelligence Category: DNS (0)
- Security Intelligence Category: URL (182)
- Intrusion Rules Category (1)
- Malware Threat Score (0)

**\*Secure Firewall Talos IP Reputation** Last 7 Days

Reputation	Count
Poor	357
Questionable	14,420
Neutral	9,111
Favorable	42
Good	61,930

**\*Secure Firewall Event Summary** Last 7 Days

Event Type	Count
Total	143,308
Intrusion	142,864
Malware	0
Security Intelligence	444

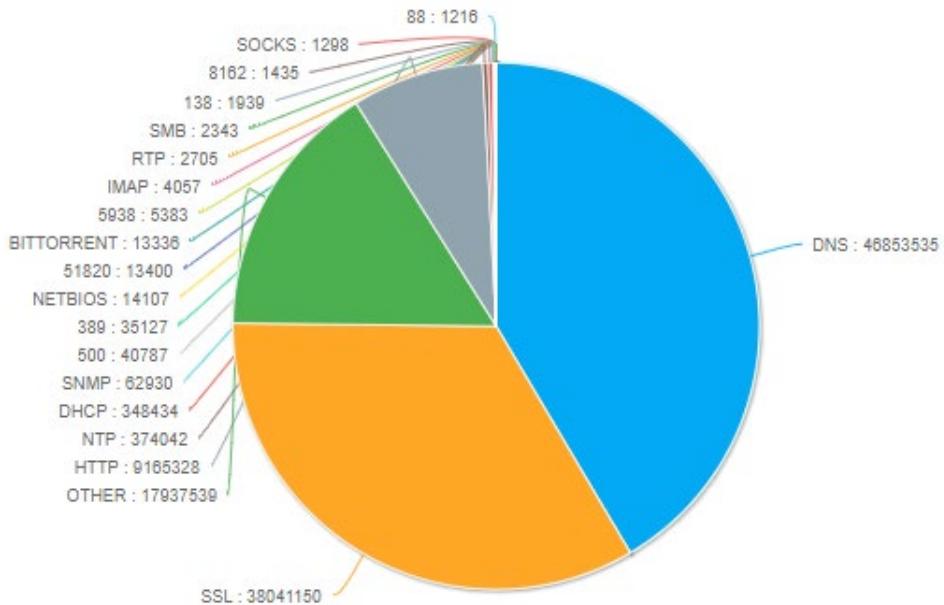
**Censys** Add Learn More

**Cisco Defense Orchestrator**

**SecureX Home**

# The Stats

- Total Packets Captured: 11.8 Billion
- Total Logs Captured: 108 Million
- Total Sessions: 187,301,858
- 13,253 Unique Devices
- 7.39 TB of packet data
- 508 GB of log data
- Peak Bandwidth Usage: 1.35Gbps
  - Similar to 2020
- ~46 Million DNS Requests
- ~80% Encrypted Traffic
- ~20% Mayhem



# It's Raining Passwords



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*****@webhealthnetwork.com	Weak	38 minutes	POP3
3 minutes, 1 second ago	*****@loveyourgrifter.com	Very Weak	10 seconds	HTTP
3 minutes, 58 seconds ago	t*****	Weak	3 hours	HTTP
4 minutes, 23 seconds ago	a*****@nimbus-berlin.com	Strong	15 years	IMAP2
5 minutes, 59 seconds ago	b*****@itswired.com	Very Strong	centuries	IMAP2
5 minutes, 59 seconds ago	b*****@itswired.com	Very Strong	centuries	IMAP2
6 minutes, 56 seconds ago	a*****@fscs.xyz	Very Strong	centuries	IMAP2
6 minutes, 58 seconds ago	a*****@fscs.xyz	Very Strong	centuries	IMAP2
-	-	Weak	24 hours	POP3
5 minutes, 46 seconds ago	n*****	Strong	4 years	POP3
5 minutes, 46 seconds ago	n*****	Weak	2 hours	POP3
6 minutes, 3 seconds ago	d*****@rcn.com	Weak	5 hours	IMAP2
6 minutes, 9 seconds ago	p*****@terra.com.br	OK	2 months	POP3
6 minutes, 20 seconds ago	d*****@rcn.com	Weak	5 hours	IMAP2
6 minutes, 38 seconds ago	d*****@rcn.com	Weak	5 hours	IMAP2
-	-	Weak	24 hours	IMAP2

2022

55,525 - Cleartext Passwords  
2,210 - Unique Accounts

2020

96,361 - Cleartext Passwords  
2,178 - Unique Accounts

# Umbrella Total Requests ~32m (~37m in 2020)

Reporting / Additional Reports

 Activity Volume

**FILTERS**

**TRAFFIC TYPE**

All

DNS

Web

IP-Layer Enforcement

Name	Allowed	Blocked
Security	12,651	0
Prevent	7,033	0
Malware	381	0
Dynamic DNS	4,245	0
Newly Seen Domains	1,936	0
Potentially Harmful	381	0
DNS Tunneling	39	0
Cryptomining	51	0
Contain	520	0
Integrations	5,098	0
Categories	-	0
Categories (Legacy)	-	0
Destination Lists	97,647	0
Permitted	32,953,106	0
Total	33,063,404	0

2022 |

# Block or not to Block, that is the Question

**SecureX | Threat Response**   **Investigate**   **Snapshots**   **Incidents**   **Intelligence**

#   Timeline   Jessica Bair

Add to Investigation ...   New Investigation   Snapshots ...   1 of 1 enrichments complete   Fit to Screen 3 Panel Layout

1 Target   1 Investigated   0 Omitted   4 Related   3 Indicators   9 Modules

Graph   Dispositions: All   Types: All   Selectors: All   Mode: Expanded   Target Filtering: None   Showing 5 nodes

Target Network 586981670

Suspicious URL http://amazonon...

Malicious Domain amazonon.ca.jp....

Malicious IP 204.44.66.6

Suspicious URL https://amazno...

Results

Details   Threat Context

1 TARGET

- 586981670   Network

1 INVESTIGATED

- amazonon.ca.jp.ce...   Malicious Domain   8 Sightings in My Environment

0 OMITTED

4 RELATED

- 204.44.66.6   Malicious IP Address
- http://amazonon.ca.j...   Suspicious URL
- https://amaznon.ca...   Suspicious URL
- 10.65.140.127

Judgements (4)   Verdicts (4)   Sightings (27)   Indicators (3)

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

Search data   Sort by  
Find ...   Start Time Newest

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

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

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

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

Sightings

My Environment (8)   Global (27)

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

■ Malicious ■ Suspicious ■ Common ■ Unknown ■ Clean ■ Targets

Distribution   0   93%

# Awards

#1 App: Office365

#1 Chat: WhatsApp

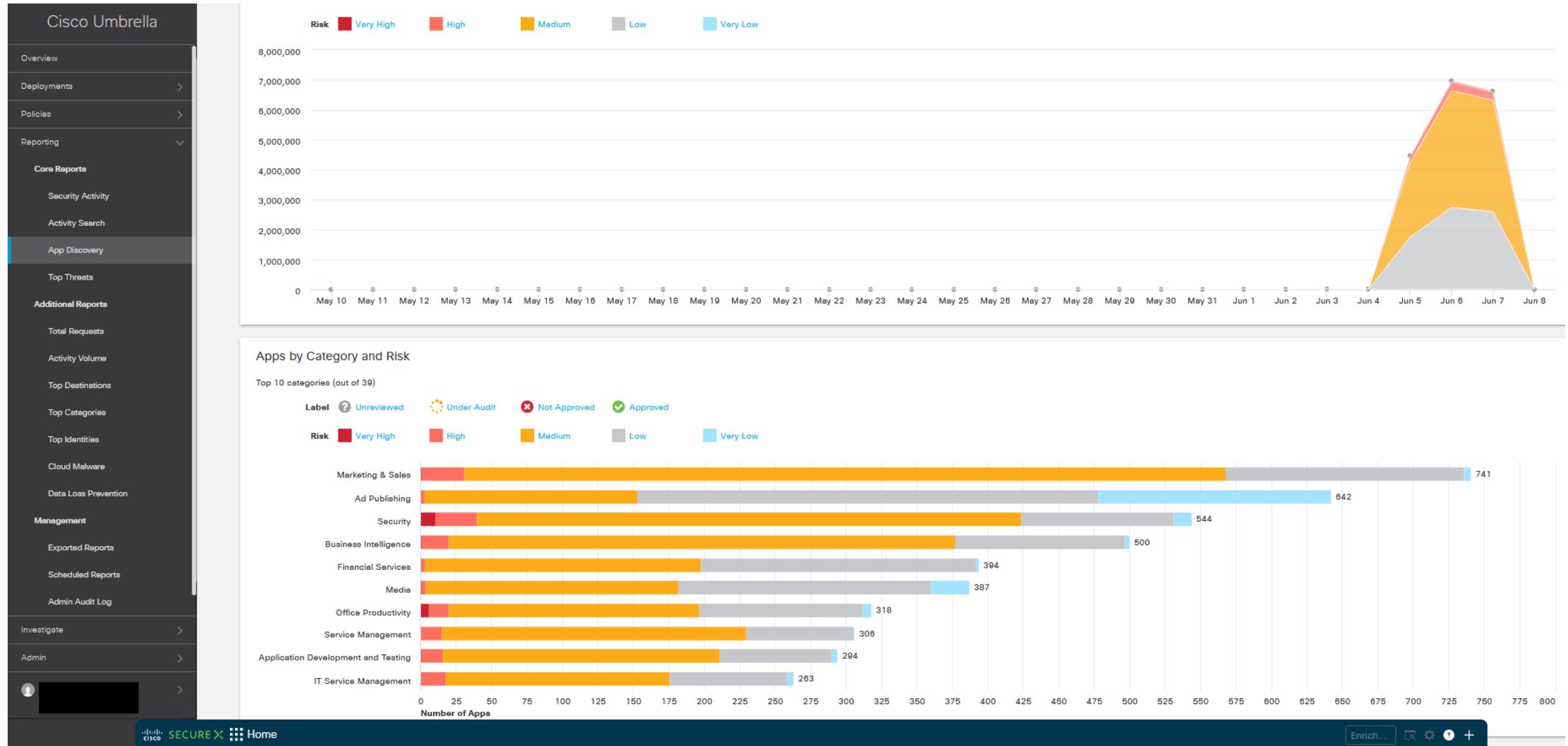
#1 Cryptomining: NiceHash

#1 Dating: grindr

#1 Porn: xvideos



# DNS App Discovery - Over 7K Applications (~4K in 2020)



# Firewall: Firepower Intrusion Detection



# Stranger Pings

Malicious IP 212.102.39.81

190 Related ▾

13 Indicators ▾

9 Modules ▾

Results

Details Threat Context

138.199.18.71 Malicious IP Address

146.70.10.17 Malicious IP Address

146.70.11.23 Malicious IP Address

154.13.1.34 Malicious IP Address

**154.16.105.147** Malicious IP Address

Verdicts (5)

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

Search data Sort by Find ... Start Time Newest

**Malicious**

Module: Recorded Future Expiration: 2022-07-08T23:30:11.000Z [JSON](#)

Module: \*Umbrella Expiration: 2022-07-08T23:29:45.747Z [JSON](#)

**Suspicious**

Module: alphaMountain.ai Threat Intelligence Expiration: Expired 2022-06-09T07:29:44.032Z [JSON](#)

Module: IBM X-Force Exchange Expiration: 2022-07-08T23:29:44.000Z [JSON](#)

Medium 365

# RSA® Conference 2022

## Story time

### Tales from the SOC



# Can you hear me now?!?

Facebook Old Reader Yahoo Mail Gmail SFgate KRON4 Weather Underground OctoPrint BoardGameGeek

RSA Investigate Respond Users Hosts Files Dashboard Reports

Threat - Malware Indicators Dashboard | Add Row

Threat Categories

Past 24 hours

SESSION COUNT

Last Refreshed at : 04:54 PM

Malware Activity DNS

Past 24 hours

10.65.77.111 : 1

10.65.5.122 : 1

10.65.103.54 : 1

10.65.159.55 : 1212

10.65.40.47 : 973

10.65.238.76 : 944

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

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

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

Help Refresh streams Inaudible streams Analyze Prepare Filter Export Close

Wireshark · RTP Player

[00: 05: 10.250] - Speaker 1  
Oh well, go away. Tomorrow morning we fly, say at 14:15 to 21:00.

Legend:

- Jitter Drops (Red circle)
- Wrong Timestamps (Blue diamond)
- Inserted Silence (Yellow triangle)

Play | Source Address | Source Port | Destination Address | Destination Port | SSRC | Setup Frame | Packets | Time Span (s) | SR (Hz) | PR (Hz) | Payloads

L	206.15.10.11	27076	10.65.159.55	23556	0xc84	SETUP 33387	20567	13676.97 - 14...	8000	8000	g711U
R	10.65.10.11	23556	206.15.10.11	27076	0xc84	SETUP 33391	20556	13677.01 - 140...	8000	8000	g711U

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

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

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

Help Refresh streams Inaudible streams Analyze Prepare Filter Export Close

# How are things back home? Laundry Day?

Event Reconstruction													
service	id	type	source	destination	service	first packet time	last packet time	packet size	payload size	packet count	flags		
NW-HU - Broker	123399301	Network Session	10.65.10.10:5000	82.65.10.10:5000	80	2022-06-08T16:27:22.731	2022-06-08T16:27:23.567	67,878 bytes	62,374 bytes	82	Keep, Assembled, App Meta, Network Meta		

 Request & Response  Top To Bottom  View Web  Actions

## Request

GET /SurveillanceStation.SnapShot&version=1&method=GetPushServSnapshot&supportNotiEncrypt=true&snapshotId=207498\_sid=2T7BhMeSSZTzdJElY\_rPEQ0r6Fa2qLDbUSNFQkUfpz09uSYQ2m7R3QaF0pkDlhwHvnIk1k957aOPHwkd0ZIEE  
(host: 82.65.5000)

## Response

*Content-Type: image/jpeg*

2022-06-08 18:27:37



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

# Internet of Pets...I mean Things

RSA Investigate Respond Users Hosts Files Dashboard Reports

NAVIGATE LEGACY EVENTS EVENTS MALWARE ANALYSIS

Event Reconstruction

service	id	type	source	destination	service	first packet time	last packet time	packet size	payload size	packet count	flags
NW-PKH - Concentrator	104743931	Network Session	10.65.1.1 : 65329	47.254.196.8088 : 80		2022-06-07T14:50:08.096	2022-06-07T14:50:11.356	6,602 bytes	4,236 bytes	35	Keep, Assembled, App Meta, Network Meta

Request & Response Top To Bottom View Web Actions

**Request**

```
GET /_Server/server.php?cmd=random&userid=123456@gmail.com&platform=mail&appn=123456
(host: 47.254.44.196:8088)
```

**Response**

```
Content-Type: text/html

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

**Request**

```
GET /_Server/server.php?cmd=login&platform=mail&userid=123456@gmail.com&passwd=123456&appn=123456
(host: 47.254.44.196:8088)
```

**Response**

```
Content-Type: text/html

{"cmd":1003, "code":20000, "msg":[{"devid":"XK8XXG186SN1FW7V111A", "devusr":"admin", "devpw":"123456"}, {"devconn":"p2p", "devchnl":"0", "devstream":"main", "dealias":"Dog Camera", "devtype":"pack", "unitype":"LSD01", "tzsec:"", "location:"", "sndeffect":"yes", "petid":"61ad791d27a4c2d070e7cd47735f075"}]}
```

**Request**

```
GET /_Server/server.php?cmd=iconname&platform=mail&userid=123456@gmail.com&petid=61ad791d27a4c2d070e7cd47735f075&appn=123456
(host: 47.254.44.196:8088)
```

# Help! I need a Medic!

## Certificado de Seguro de [REDACTED]

Nombre y Domicilio del Contratante [REDACTED] . DE R.L. DE C.V.			Póliza No. M09 [REDACTED]	Certificado No. [REDACTED] 18
Nombre del asegurado Titular: [REDACTED]			Subgrupo 004	
Sexo:	Estado Civil:	Fecha de Nacimiento:	Fecha de Ingreso a la colectividad asegurada	Vigencia de la póliza
MASCULINO	NO APLICA	Día Mes Año [REDACTED]	Día Mes Año 04 04 2022	Desde las 12:00 hrs. Hasta las 12:00 hrs. Día Mes Año 04 04 2023

## RELACION DE ASEGURADOS

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

## Características del Seguro Contratado Características del plan

TIPO DE PLAN CONTRATADO  
SUMA ASEGURADA  
SUMA ASEGURADA INTERNACIONAL GERENTES  
DEDUCIBLE  
COASEGURO  
HONORARIOS QUIRURGICOS  
TRE01  
EMERGENCIA EN EL EXTRANJERO ZONA " B "  
DERECHO DE CONVERSIÓN  
ASISTENCIA INTEGRAL

EJECUTIVO  
50,000 U. M. A. M  
300,000.00 DLLS.  
4 U. M. A. M  
10%  
G. U. A. [REDACTED]

AMPARADA  
AMPARADO  
AMPARADA

Network Event Details | Text **Packet** File Host Email Web ↗

Download PCAP ▾  DISPLAY COMPRESSED PAYLOADS

**REQUEST**

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

Showing 6%

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

# Chewing through email...



311 Park Place Blvd  
Ste 400  
Clearwater, FL 33759  
United States  
[www.isc2.org](http://www.isc2.org)  
[membersupport@isc2.org](mailto:membersupport@isc2.org)  
[www.isc2.org/contactus](http://www.isc2.org/contactus)

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

## Description

06/06/2022 15:30 - 06/07/2022 15:29 | ip.dst = 129.159. [REDACTED] | : = 'firepower' [REDACTED]

Network Event Details | Text | Packet | File | Host | Email | Web

**SUBJECT** Re: Have you been playing Wordle?

> ADDITIONAL HEADER DETAILS

4/6

On Wed, Jan 26, 2022, 14:16 [REDACTED] > wrote:  
There's only one per day. You will like this. Read the rules, and you'll start to get it after the first few. The word of the day is the same for everyone.

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

--

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

TO [REDACTED]  
**SUBJECT** You've got a money request

11 of 54 events

# Spear Phishing, Anyone?

## Emergency Connectivity Fund FCC Form 471

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

### Authorized Person

**Title:** Chief Technology Officer

**Name:** [REDACTED]

**Phone:** [REDACTED] 687-[REDACTED]

**Email:** [REDACTED].org

**Address:** [REDACTED]

**Employer:** [REDACTED] SCHOOL DISTRICT [REDACTED]

### Certified Timestamp

13-May-2022 20:15:04 EDT

which funding is sought

The equipment and services the school, library, or consortium purchases or will purchase using Emergency Connectivity Fund support will be used primarily for educational purposes and will not be sold, resold, or transferred in consideration for money or any other thing of value, except as allowed by ## 54.1713.

	Total Student Count	Urban or Rural
[REDACTED]	1286	Urban

# How do you make iPhone email insecure?!?

Filter Events > X

Meta Group Ordering

All Event Categorization Keys ec.all

All User Keys user.all

All Hostname Keys host.all

All Client Keys (1) client.all

iphone mail (19f77) (1)

All Port Keys port.all

All Domain Keys domain.all

All Email Address Keys email.all

client.all

Highlight All Match Case Match Diacritics Whole Words 1 of 1 match

Network Event Details | Text | Packet | File | Host | Email **Email** | Web

**EXPAND ALL EMAILS**

FROM [REDACTED]@icloud.com>

TO [REDACTED]terra.com.br>

REPLY TO [REDACTED]icloud.com>

SUBJECT Foto

ATTACHMENTS (1)  
IMG\_0691.jpg

ADDITIONAL HEADER DETAILS

AUTHENTICATION- mail-cmgw-in05-mia.tpn.terra.com; dkim=pass header.d=icloud.com header.b=Imt3POWW

RESULTS

CONTENT- 7bit

TRANSFER-

ENCODING

CONTENT-TYPE multipart/mixed; boundary=Apple-Mail-B1E00298-D71B-4C70-962C-1C1B524BE075

DKIM-SIGNATURE v=1; a=rsa-sha256; c=relaxed/relaxed; d=icloud.com; s=1a1hai; t=1654728329; bh=ZCAzrpkGoOr7meAnzDPIQ5QJ3wj; h=Content-Type:From:Mime-Version:Date:Subject:Message-Id:To; b=Imt3P0WW EhJQQhjGlvTKzlijAEI9rbChoON8rpwww+IEQOe0Sc4n0nTQ4jXZ3CPv+cJYjt4VXM4HdoUJVkr9Y4cjQB/wU+TsNnCOFpFMog7X Ph55eCuVLatmvaDGOL0RgL2mMuyTAWiZuMANWYJDxrqozbhYkBh3zo11VpPEAFrk8g/UhitZKnEXI3Plzdtgv4QtWWmLWdUNjfeOpBBTPCaG3o61wiLYAqPZbTRRI/ht3v7

1 of 1 events



**Important!** The wireless network available at the Moscone Center is an open, unsecured 5 GHz network.

Also note that this year, NetWitness and Cisco Systems will be using data from the Moscone Wireless Network for an educational demonstration on a working SOC. We strongly recommend that you use appropriate security measures, such as utilizing a VPN connection, installing a personal firewall and keeping your operating system up-to-date with security patches. We recommend turning off your wireless adapter when not in use and ensuring ad-hoc (peer-to-peer) capabilities are disabled on your device.



“Apply” Slide