



Tales FROM

THE

black hat®

NOC



\$ whoami

- 6 yr. IT before InfoSec (not counting HS or College)
- 2 yr. InfoSec Team Lead @ Medline Industries
- 2 yr. Solutions Engineer @ LightCyber
- 2 yr. Solutions Engineer Specialist @ Palo Alto Networks
- 4.5 yr. Solutions Engineer @ Corelight
- 1 yr. Tech Marketing Engineer @ Corelight

Plus:

- 2 yr. Threat Hunter in the Black Hat Conference NOC



Mark Overholser



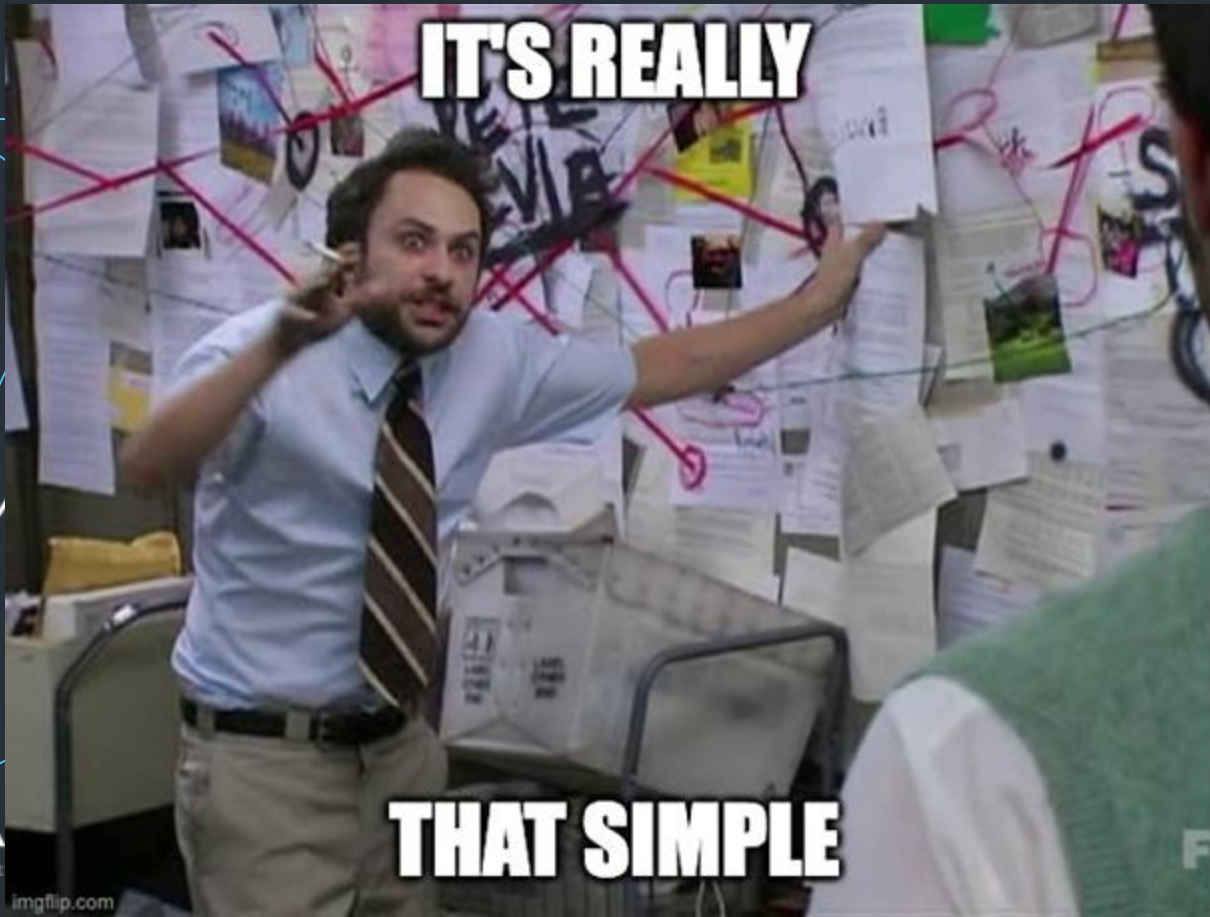
The Black Hat conference NOC partners



ARISTA

LUMEN®





IT'S REALLY

THAT SIMPLE

syslog



imgflip.com

CISCO Meraki

TALOS
Recorded Future
Pulsedive Community
CyberGrine
SHODAN
VIRUSTOTAL
THREATSCORE®
opivoid

threat intelligence



network visibility




User Protection Suite



The digital display features a vibrant, geometric, crystalline background with blue and red tones. The text on the display includes:

- black hat** NETWORK OPERATIONS CENTER
- Network Analytics and Detection Provider
- corelight**
- At the bottom left, there is a small logo for **Black Hat**.

 corelight

 MSP





WORLD TOUR 2023
METADAT
WITH SPECIAL GUESTS
ATTACK • COMMAND AND CONTROL • DATA EXFILTRATION •
DATA BREACH • DATA BREACH INVESTIGATION • DATA BREACH
USER EXECUTION • PROCESS INJECTION • RDP •
BRUTE FORCE • DISCOVERY • SYSTEM HARDWARE

Subnets services stats

45m

#Monitored subnets	#Monitored IPs	Distinct services	Monitored subnets
7	385	25	Cisco DNS AP/Switch Mgmt Show Management RegistrationWifi NOC Wired NOC WiFi ETS/Production/Streaming

Services per IP Address

source_ip	services
10.10.10.11	ssl ntp dns dhcp
10.10.10.12	ntp dns dhcp
10.10.10.13	ntp dns dhcp
10.10.10.14	ntp vxlan dns dhcp
10.10.10.15	ssl ntp dhcp
10.10.10.16	ntp dns dhcp
10.10.10.17	ntp dns dhcp
10.10.10.18	ntp dns dhcp
10.10.10.19	ntp vxlan dns dhcp
10.10.10.20	ntp dns dhcp
10.10.10.21	ntp dns dhcp
10.10.10.22	ntp dns dhcp
10.10.10.23	ntp vxlan dns dhcp
10.10.10.24	ntp vxlan dns dhcp
10.10.10.25	ntp dns dhcp
10.10.10.251	ssl ntp dns
10.10.10.252	ssl ntp dns
10.10.10.253	ssl ntp dns
10.10.10.254	ssl ntp dns
10.10.10.26	ntp dns dhcp
10.10.10.27	ntp dns dhcp
10.10.10.28	ntp vxlan dns dhcp
10.10.10.29	ntp dns dhcp
10.10.10.3	ssl ntp dns
10.10.10.30	ntp dns dhcp
10.10.10.31	ntp dns dhcp
10.10.10.32	ssl ntp dns dhcp
10.10.10.33	ssl ntp dns dhcp
10.10.10.34	ssl ntp http dns dhcp
10.10.10.35	ssl ntp http dns dhcp
10.10.10.36	ssl ntp dns dhcp
10.10.10.37	ssl ntp dns dhcp
10.10.10.38	ssl ntp dns dhcp
10.10.10.39	ssl ntp dns dhcp

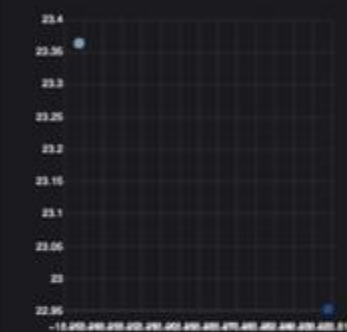
AP/Switch Mgmt

15m



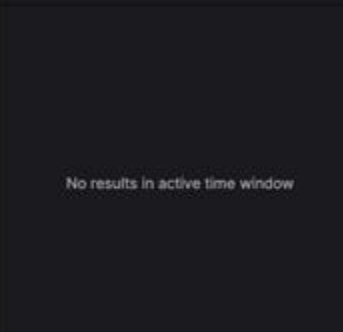
Cisco DNS

15m



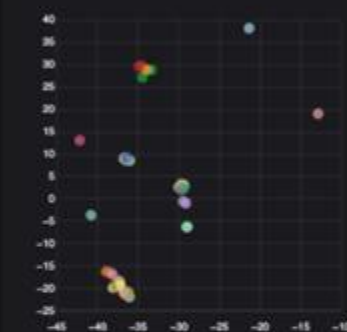
GlobalProtect VPN

15m



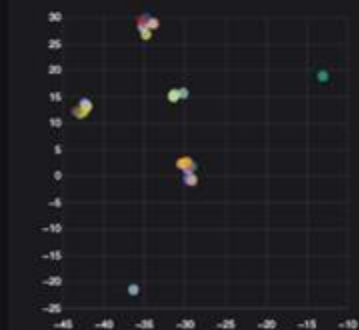
NOC WIFI

15m



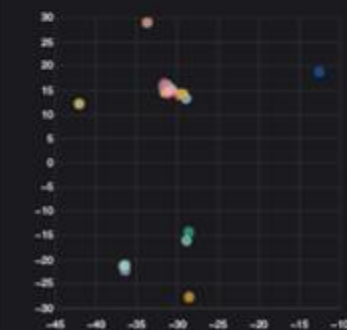
NOC Wired

15m



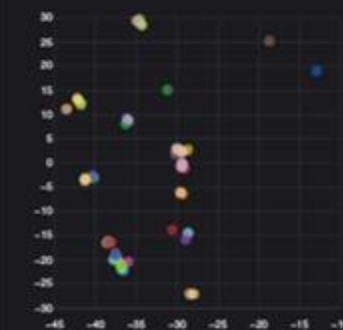
RegistrationWifi

15m



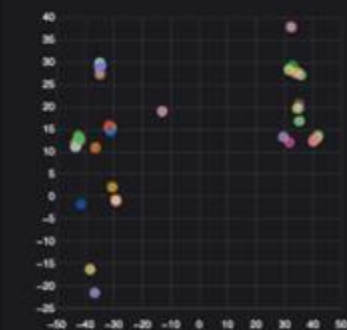
Show Management

15m



ETS/Production/Streaming

15m



Tales FROM
THE



NO

C

Open-source roots

zeek



Tales FROM
THE

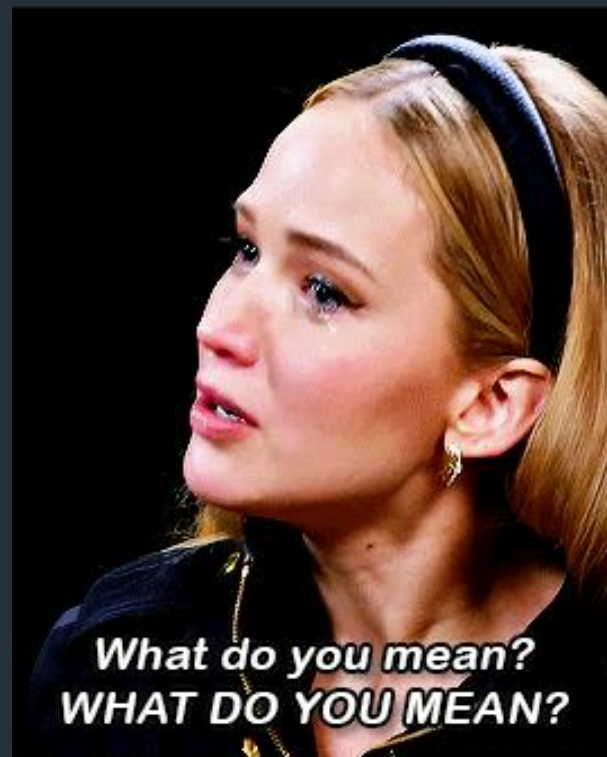


NO
C

Amazon shrugged

host	server_headers	_count ↑
ocsp.rootca1.amazontrust.com	Server: "\ (ツ) /"	1673
ocsp.rootg2.amazontrust.com	Server: "\ (ツ) /"	503
ocsp.rootca3.amazontrust.com	Server: "\ (ツ) /"	73
ocsp.rootg2.amazontrust.com:80	Server: "\ (ツ) /"	2
ocsp.rootca4.amazontrust.com	Server: "\ (ツ) /"	2
ocsp.rootca1.amazontrust.com:80	Server: "\ (ツ) /"	2

— _ (ツ) _ /



Tales FROM
THE


black hat[®]

NO

C

Pentesters gonna pentest

Tales FROM
THE



NO
C

Living in syn-ology


```
General_WiFi      192.168.241.93  http://[redacted].synology.me:5000/webapi/query.cgi
Content-Type:application/x-www-form-urlencoded
Content-Length:50
Host:[redacted].synology.me:5000
Connection:Keep-Alive
Accept-Encoding:gzip
Cookie: id=[redacted]
User-Agent:Synology-DS_file_4.17.1_rv:588_SM-69868
```

If you select Synology as the service provider, you can configure the following settings:

- **Get a certificate from Let's Encrypt and set it as default** Tick the checkbox to apply a Let's Encrypt SSL certificate for your Synology DDNS and set it as the default certificate for DSM. However, if an SSL certificate is already matched for your DDNS hostname, the checkbox will be disabled. For more information on the SSL certificate, please refer to [this article](#).

```
cerberus@[redacted] zeek_output % ls
conn.log          files.log          http.log           packet_filter.log
extract_files     heic               mp4                reporter.log
cerberus@[redacted] zeek_output % file heic/*
heic/extract-1701853095.994659-HTTP-FaeE1YewTXchExTpe.heic: ISO Media, HEIF Image HEVC Main or Main Still Picture Profile
heic/extract-1701860860.583039-HTTP-FzXbTl4AhDzGHgoujh.heic: ISO Media, HEIF Image HEVC Main or Main Still Picture Profile
heic/extract-1701862798.988648-HTTP-F6FfUkiaNGXPfwp4g.heic: ISO Media, HEIF Image HEVC Main or Main Still Picture Profile
heic/extract-1701862800.589052-HTTP-FYbjn93H54VZu4IX9.heic: ISO Media, HEIF Image HEVC Main or Main Still Picture Profile
heic/extract-1701862802.002174-HTTP-Fk90UH2cKljogkNo8.heic: ISO Media, HEIF Image HEVC Main or Main Still Picture Profile
heic/extract-1701862894.675585-HTTP-FwMBUA2JXqgGP5dSfI.heic: ISO Media, HEIF Image HEVC Main or Main Still Picture Profile
heic/extract-1701863023.68998-HTTP-FwGq42141QJT9SMcGj.heic: ISO Media, HEIF Image HEVC Main or Main Still Picture Profile
cerberus@[redacted] zeek_output % file mp4/*
mp4/extract-1701853097.844574-HTTP-FN2gll0Tchks3lB09.mp4: ISO Media, MP4 v2 [ISO 14496-14]
```



Information [Show Less](#)

Created	Today, 09:21
Modified	Today, 09:21
Last opened	Today, 09:24
Content created	Yesterday, 08:00
Dimensions	3024 x 4032
Resolution	72 x 72
Color space	RGB
Color profile	sRGB IEC61966-2.1
Device make	samsung
Device model	SM-G986B
Aperture value	1.69
Exposure time	1/50
Focal length	5.4 mm
ISO speed	640
Flash	No
F number	f/1.8
Exposure program	Normal
Metering mode	Center-weighted average
White balance	Auto
Content Creator	G986BXXSIHWJD
Longitude	0° 4' 17.392" W
Latitude	51° 30' 42.39" N

Tags

Add Tags...

Tales FROM
THE




NO

C

A vpn that doesn't understand what p stands for

host	user_agent	post_body	url
218.	MGUARD_APP_API	[{"action": "CYCLE_UPDATE_POLICY", "auditLogDesc": "auditLogDesc", "companyId": "CompanyID", "deviceId": "110", "deviceId": "110"}]	/api/insertAuditLog.js
218.	MGUARD_APP_API	[{"action": "CYCLE_UPDATE_POSITION", "auditLogDesc": "auditLogDesc", "companyId": "CompanyID", "deviceId": "110", "deviceId": "110"}]	/api/insertAuditLog.js
218.	MGUARD_APP_API	[{"action": "CYCLE_UPDATE_POSITION", "auditLogDesc": "auditLogDesc", "companyId": "CompanyID", "deviceId": "110", "deviceId": "110"}]	/api/insertAuditLog.js
218.	MGUARD_APP_API	[{"action": "CYCLE_UPDATE_POSITION", "auditLogDesc": "auditLogDesc", "companyId": "CompanyID", "deviceId": "110", "deviceId": "110"}]	/api/insertAuditLog.js
218.	MGUARD_APP_API	[{"action": "CYCLE_UPDATE_POSITION", "auditLogDesc": "auditLogDesc", "companyId": "CompanyID", "deviceId": "110", "deviceId": "110"}]	/api/insertAuditLog.js
218.	MGUARD_APP_API	[{"action": "CYCLE_UPDATE_POSITION", "auditLogDesc": "auditLogDesc", "companyId": "CompanyID", "deviceId": "110", "deviceId": "110"}]	/api/insertAuditLog.js

1.283904249943263,103.8590548066



1°17'02.1"N 103°51'32.6"E
1.283904, 103.859055

Directions
Save
Nearby
Send to phone
Share


#02

7VM5+HJ7 Singapore

Add a missing place

Add your business

Add a label



Tales FROM
THE



NO
C

DOH!

id.resp_h	host	uri
47.246.2.191	httpdns.alicdn.com	/multi_httpdns_resolve?host_key=vdn5-1.vzuu.com;vdn.vzuu.com;vdn6-1.vzuu.com&qtype=all
47.246.2.192	httpdns.alicdn.com	/multi_httpdns_resolve?host_key=vdn.vzuu.com;vdn5-1.vzuu.com;vdn6-1.vzuu.com&qtype=all
47.246.2.192	httpdns.alicdn.com	/multi_httpdns_resolve?host_key=vdn5-1.vzuu.com;vdn.vzuu.com;vdn6-1.vzuu.com&qtype=all
47.246.2.191	httpdns.alicdn.com	/multi_httpdns_resolve?host_key=vdn.vzuu.com;vdn5-1.vzuu.com;vdn6-1.vzuu.com&qtype=all
59.111.211.11	httpdns.yunxindns.com	/httpdns/v2/d?domain=im-web.zeekrlife.com
59.111.211.11	httpdns.yunxindns.com	/httpdns/v2/d?domain=statistic.live.126.net

This *looks like* DOH...

But DOH is *supposed to* be over HTTPS!

Sanity check?

Yep, it works.

```
> ; curl -sH "ThisIsNotEncrypted" 'http://httpdns.c.cdnhwc2.com/dns/live?num=5&domain=google.com&qtype=ADDRS' \
> | jq .
{
  "content": [
    {
      "domain": "google.com",
      "ipv4": [
        "156.59.151.147",
        "156.59.151.144",
        "156.59.151.145",
        "156.59.151.146",
        "156.59.151.19"
      ],
      "ipv6": []
    }
  ],
  "clientIp": " ",
  "qtype": "ADDRS",
  "ttl": 60
}
```


Tales FROM
THE



NO

C

It came from behind the podium!

List Table

Score	Alert Category	Entity	Alert Type	#Alerts
6	ET MALWARE TraderTraitor CnC Domain in DNS Lookup (canolagroove .com)	192.168.0.50	Suricata	22
6	ET MALWARE Observed DNS Query to UNC3890 Domain (office365update .live)	192.168.0.50	Suricata	41
6	ET MALWARE Observed DNS Query to UNC3890 Domain (rnfacebook .com)	192.168.0.50	Suricata	12
6	ET MALWARE TraderTraitor CnC Domain in DNS Lookup (primerosauxiliosperu .com)	192.168.0.50	Suricata	16
6	ET MALWARE TraderTraitor CnC Domain in DNS Lookup (alwaysckain .com)	192.168.0.50	Suricata	21
6	ET MALWARE Mallox Ransomware CnC Domain (whyers .io) in DNS Lookup	192.168.0.50	Suricata	24
6	ET MALWARE TraderTraitor CnC Domain in DNS Lookup (centos-repos .org)	192.168.0.50	Suricata	11
6	ET MALWARE TraderTraitor CnC Domain in DNS Lookup (reggedrobin .com)	192.168.0.50	Suricata	9
6	ET MALWARE TraderTraitor CnC Domain in DNS Lookup (centos-pkg .org)	192.168.0.50	Suricata	12
6	ET MALWARE TraderTraitor CnC Domain in DNS Lookup (toyourownbeat .com)	192.168.0.50	Suricata	12
6	ET MALWARE TraderTraitor CnC Domain in DNS Lookup (datadog-cloud .com)	192.168.0.50	Suricata	9
6	ET MALWARE TraderTraitor CnC Domain in DNS Lookup (nomadpkg .com)	192.168.0.50	Suricata	9
6	ET MALWARE TraderTraitor CnC Domain in DNS Lookup (datadog-graph .com)	192.168.0.50	Suricata	12
6	ET MALWARE TraderTraitor CnC Domain in DNS Lookup (launchruse .com)	192.168.0.50	Suricata	9
6	ET MALWARE TraderTraitor CnC Domain in DNS Lookup (nomadpkgs .com)	192.168.0.50	Suricata	9



America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Search

Topics ▾

Spotlight

Resources & Tools ▾

News & Events ▾

Careers ▾

About ▾

[Home](#) / [News & Events](#) / [Cybersecurity Advisories](#) / [Cybersecurity Advisory](#)

CYBERSECURITY ADVISORY

TraderTraitor: North Korean State-Sponsored APT Targets Blockchain Companies

Last Revised: April 20, 2022

Alert Code: AA22-108A

Tales FROM
THE



NO

C

SOME EDR are authorized C2

1 2 3 4 5

Number of distinct alert signatures

6

Suricata alert signatures

signature	_count
ET_INFO_WinHttp_AutoProxy_Request_wpad.dat_Possible_BadTunnel	77
ET_INFO_TLS_Handshake_Failure	6
ET_HUNTING_Suspicious_POST_With_Reference_to_WINDOWS_Folder_Possible_Malware_Infection	4
ET_INFO_EXE - Served_Attached_HTTP	2
ET_INFO_Packed_Executable_Download	2
ET_SCAN_Behavioral_Unusual_Port_135_traffic_Potential_Scan_or_Infection	1

Top Resp Countries



!_resp_geoentity



Number of distinct entities

6

Top Entities

Source	Destination	Severity	Signature	Category	_count
192.168.1.1	192.168.1.2	Low	ET_INFO_WinHttp_AutoProxy_Request_wpad.dat_Possible_BadTunnel	Generic_Protocol_Command_Decode	47
192.168.1.1	121.1.1.1	Low	ET_INFO_WinHttp_AutoProxy_Request_wpad.dat_Possible_BadTunnel	Generic_Protocol_Command_Decode	38
192.168.1.1	143.1.1.1	Medium	ET_INFO_TLS_Handshake_Failure	Potentially_Bad_Traffic	4
192.168.1.1	121.1.1.1	High	ET_HUNTING_Suspicious_POST_With_Reference_to_WINDOWS_Folder_Possible_Malware_Infection	A_Network_Trojan_was_detected	2
192.168.1.1	143.1.1.1	Medium	ET_INFO_TLS_Handshake_Failure	Potentially_Bad_Traffic	2
192.168.1.1	282.1.1.1	High	ET_HUNTING_Suspicious_POST_With_Reference_to_WINDOWS_Folder_Possible_Malware_Infection	A_Network_Trojan_was_detected	2
192.168.1.1	34.1.1.1	Low	ET_INFO_EXE - Served_Attached_HTTP	Misc_activity	2
192.168.1.1	34.1.1.1	Low	ET_INFO_Packed_Executable_Download	Misc_activity	2
192.168.1.1	121.1.1.1	Low	ET_SCAN_Behavioral_Unusual_Port_135_traffic_Potential_Scan_or_Infection	Misc_activity	1

MAC	Source	Dest	Host	URI	Post Body
9c...	192...	221...	nive...	/edr/telemetry?CustomerId=1	{ "ComponentId" : 117553, "DateCheckedFrom" : 1681715868933, "DateCheckedTo" : 168172268933,
9c...	192...	282...	nive...	/edr/telemetry?CustomerId=1	{ "ComponentId" : 117553, "DateCheckedFrom" : 1681715868933, "DateCheckedTo" : 168172268933,

Customer telemetry...

Who knew that EDR stood for "Everything Disseminated in Real-time"?

```

E...x8...@...y...%T...q...P...Y...POST /edr/telemetry?CustomerId=1 HTTP/1.1
Content-Type: application/octet-stream
Accept: application/octet-stream
Content-Length: 258123
Connection: Keep-Alive
Host: nive...

{
  "ComponentId" : 117553,
  "DateCheckedFrom" : 1681715868933,
  "DateCheckedTo" : 168172268933,
  "Message" :
  {
    "CommandLine" :
    {
      {
        "id" : 16768,
        "string" : "taskhostw.exe SYSTEM"
      },
      {
        "id" : 12868,
        "string" : "\"C:\\Program Files (x86)\\Google\\Update\\GoogleUpdate.exe\" /ua /installsource scheduler"
      },
      {
        "id" : 13521,
        "string" : "\"C:\\Program Files (x86)\\Microsoft\\EdgeUpdate\\MicrosoftEdgeUpdate.exe\" /ua /installsource sch"
      },
      {
        "id" : 6643168,
        "string" : "\"C:\\Program Files (x86)\\DesktopCentral_Agent\\bin\\dcagentupgrader.exe\" Task"
      },
      {
        "id" : 9885780,
        "string" : "C:\\WINDOWS\\system32\\Upfc.exe /launchtype periodic /cv fW6v2+NCxkG1Fk3Gaj2Avw.8"
      },
      {
        "id" : 5993238,
        "string" : "C:\\WINDOWS\\system32\\wbem\\screens.exe -Embedding"
      },
      {
        "id" : 2189,
        "string" : "\\?\\C:\\WINDOWS\\system32\\conhost.exe &ffffff -ForceV1"
      }
    }
  }
}

```


Tales FROM
THE



NO
C

IN SSHAMBLES



runZERO

RESEARCH

BLACK HAT BRIEFINGS

Secure Shells in **Shambles**

HD MOORE | ROB KING | AUGUST 7, 2024

sshamble

SSHamble is a research tool for SSH implementations that includes:

- Interesting attacks against authentication
- Post-session authentication attacks
- Pre-authentication state transitions
- Authentication timing analysis
- Post-session enumeration

This project is a work-in-progress and likely to change quickly.

You can reach our team via research@runZero.com.

<https://SSHamble.com/>

Timeline

4:00-4:30pm
5:15pm
5:35pm
5:50pm
6:00pm



ells in
ing traffic
cluding ady collected
ned multiple g the fingerprint
firmed that IP

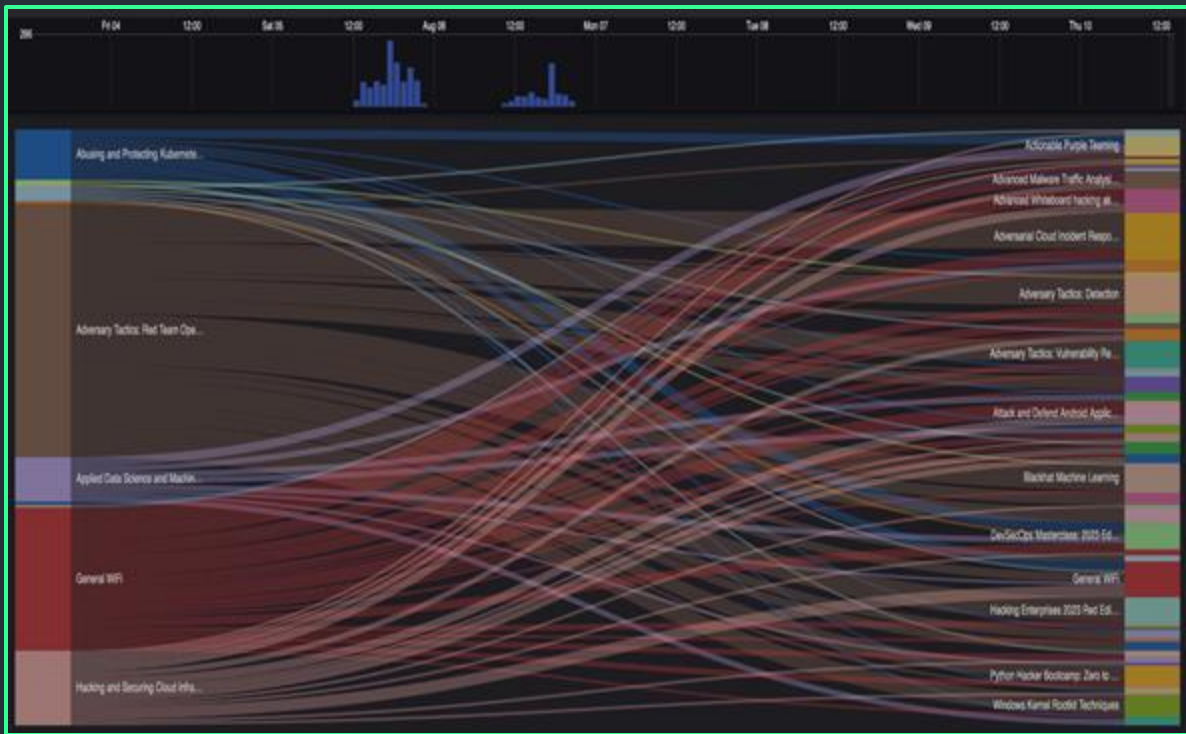
Tales FROM
THE



NO

C

Multicast DNS Misadventures



Remember when I said we isolated networks effectively?

Well, we didn't.

***Responder.py** has entered the chat*





Tales FROM

THE

black hat®

NOC

