Welcome To The 10th Annual Hacking Conference

Dungeons and Dragons™

InfoSec Master Edition

The Institute of Internal Auditors Chicago

ISACA Chicago Chapter

Welcome To The 10th Annual Hacking Conference

Remember to check-in to this session on the app!

The Institute of Internal Auditors Chicago

ISACA Chicago Chapter

Threat Intelligence in Advanced Security Operations

Fayyaz Rajpari, Managing Partner, Intelliguards

Alex Lanstein, Chief Evangelist, StrikeReady

The Institute of Internal Auditors Chicago

ISACA Chicago Chapter

About me…

Passionate about Blue Teams, Threat Intelligence & Blockchain security.

Fayyaz Rajpari, Managing Partner @Intelliguards

23 Years in Cyber

Financial / Insurance Industry

- Security engineer
- Security Architect
- Incident responder

Tech Industry

- Technical sales (SE / SA)
- Product management (SIEM / Threat Intelligence / NDR)
- Consulting and Leadership roles

About me…

Alex Lanstein – Chief Evangelist @StrikeReady

Based in Boston, formally the "city of champions"

20 Years in Cyber

15 years at FireEye

- Started in QA (via helpdesk worker in college)
- Product came of age as APT became mainstream
- Ended career running targeted threat detection program across products and services

Meta/FB

- Countered espionage threats on platform from three south asian countries, as well as two commercial surveillance companies

Threat Intelligence

The "cyclical practice" of planning, collecting, processing, analyzing and disseminating information that poses a threat to applications and systems. Threat intelligence collects information in real-time to showcase the threat landscape for identifying threats to a computer, application or network. This information is gathered from a number of resources and compiled into a single database enabling visibility into vulnerabilities and exploits actively being used on the internet (in the wild) by threat actors.

Security Operations

A security operations center (SOC) is responsible for protecting an organization against cyber threats. SOC analysts perform round-the-clock monitoring of an organization’s network and investigate any potential security incidents.

Source: https://www.wikipedia.org/

Threat Intelligence in 2000s…

10 years later…

MITRE ATT&CK™

~15 years later to present…

Drives decisions at the executive level and ***who*** the company should be defending against and ***why***. (Ex: Curated Reports and Articles)

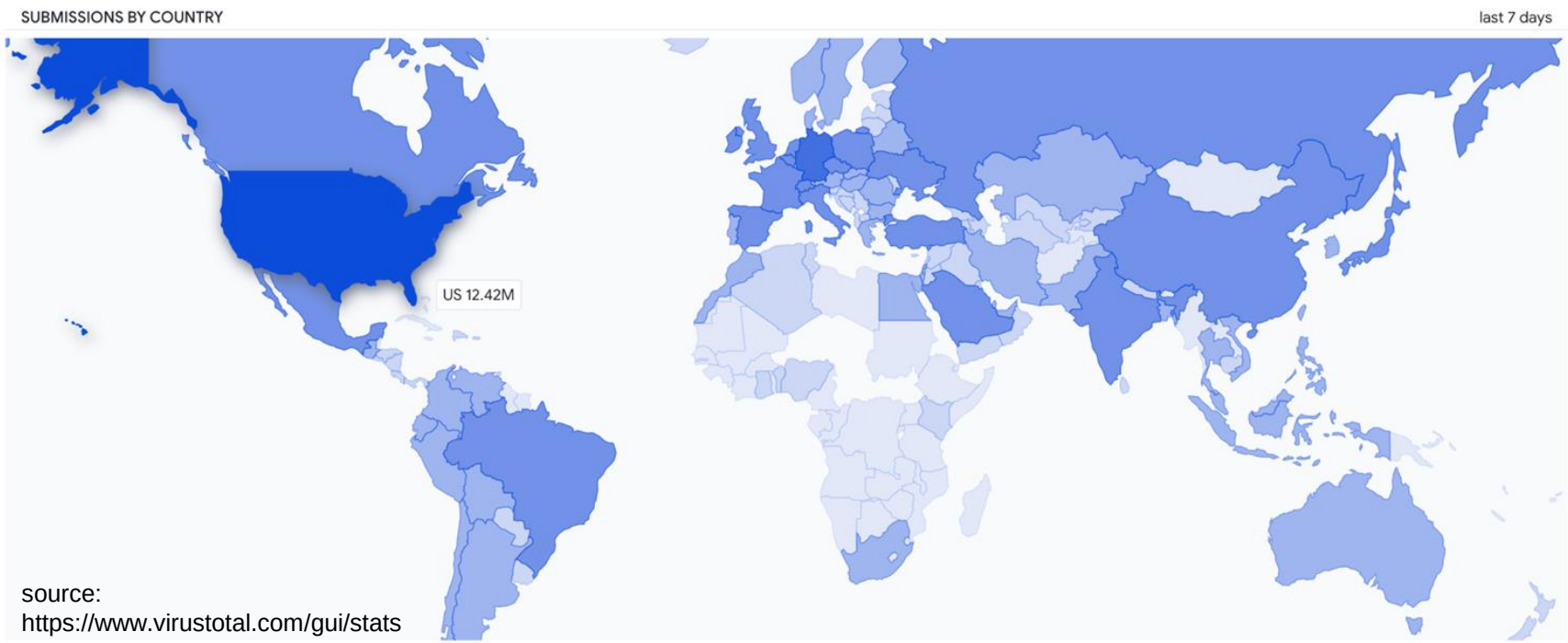
Standard operating procedures used by Adversaries for their ultimate goals and ***how*** they carry out their mission. (Ex: Tactics, Techniques, and Procedures)

Indicators of compromise and/or attack discovered and implemented directly in security controls. The ***what*** in response and prevention. (Ex: hashes, domains, ips, URLs)

Depth

Breadth

Confidence



source:
https://www.virustotal.com/gui/stats

Threat Intelligence

Mainnet

1 M

Malicious Samples

7-day daily average

Top 5 Malware Families

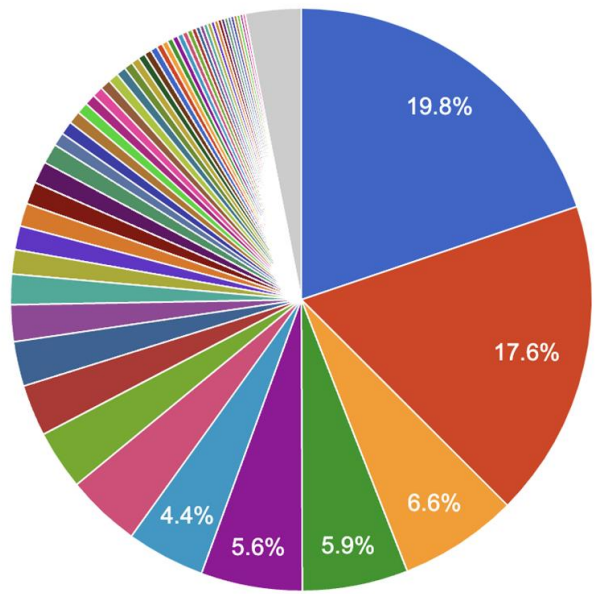
- Qukart
- Padodor
- Allaple
- PackedENT
- Ganelp

Top 5 File Types

- application/x-dosex
- text/html
- application/octet-st
- text/plain
- application/zip

source: https://www.abuseipdb.com/statistics

Reported IP Addresses By Country (Last 7 Days)



- United States of America
- China
- Brazil
- Singapore
- Korea (Republic of)
- India
- United Kingdom of Great Britain…
- Russian Federation
- Germany
- Netherlands
- Hong Kong
- Viet Nam
- Indonesia
- Japan

1/4

source: https://www.abuseipdb.com/statistics


Accuracy
Precision
Skill

ATOMIC IOCs	COMPUTED IOCs	ANALYTICS / AI
IP Addresses	File Hash Values	Curated Detections
Domain Names	Service Hashes	Automated Detections
URLs	SSH Keys	Automated Response
User Names	SSL Keys	Predictive Intelligence
Email Addresses	NTLM/Kerberos	
User Agents	JA3/JA3S	
Applications (FTP/RDP/HTTP/Other)	JA4	

If Alexa can…

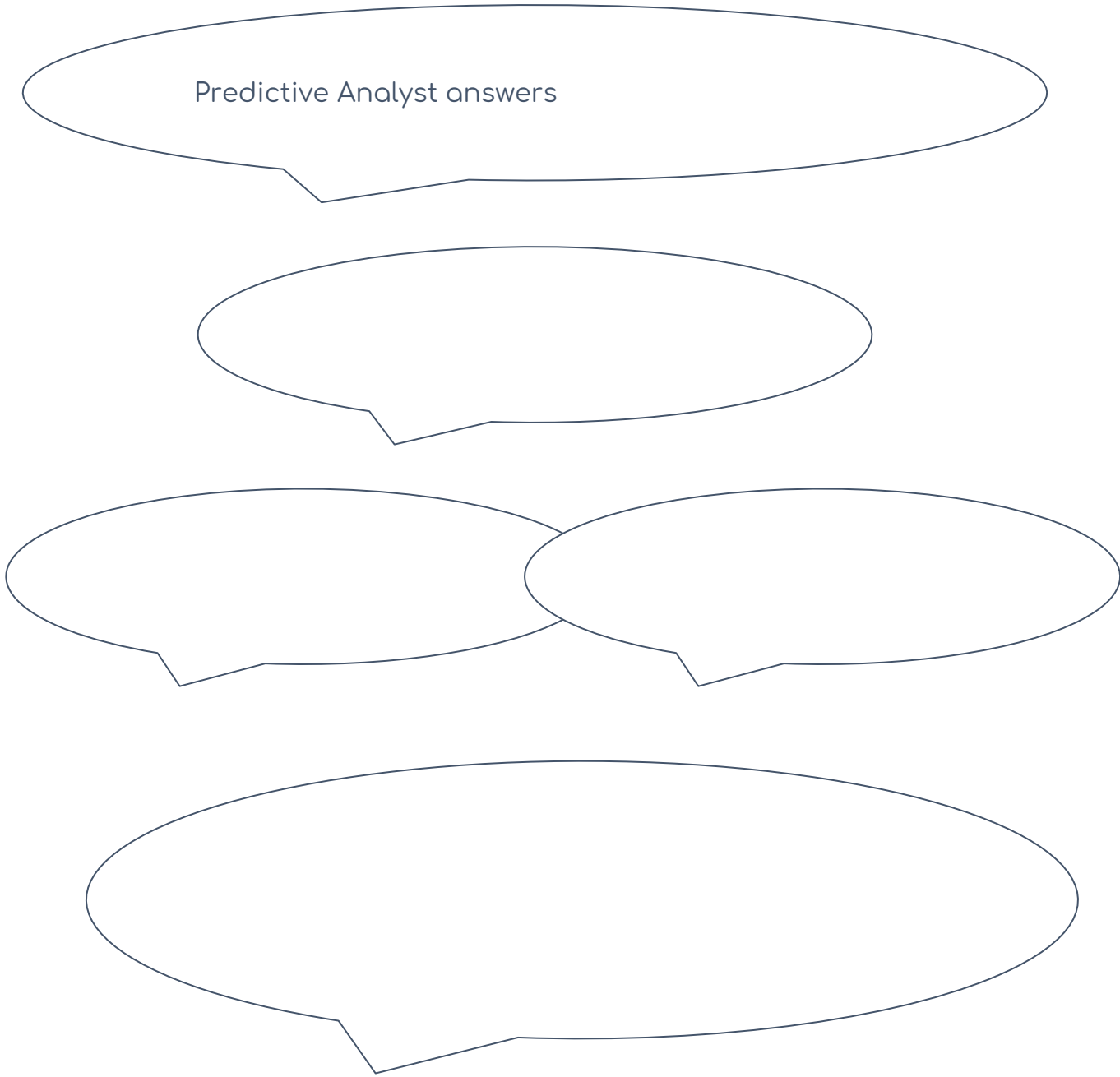
- Tell me what's on my calendar
- Turn on/off my lights, tvs, and electronics
- Order me things
- Tell me how the day is outside
- and guard my home…

All Automatically!

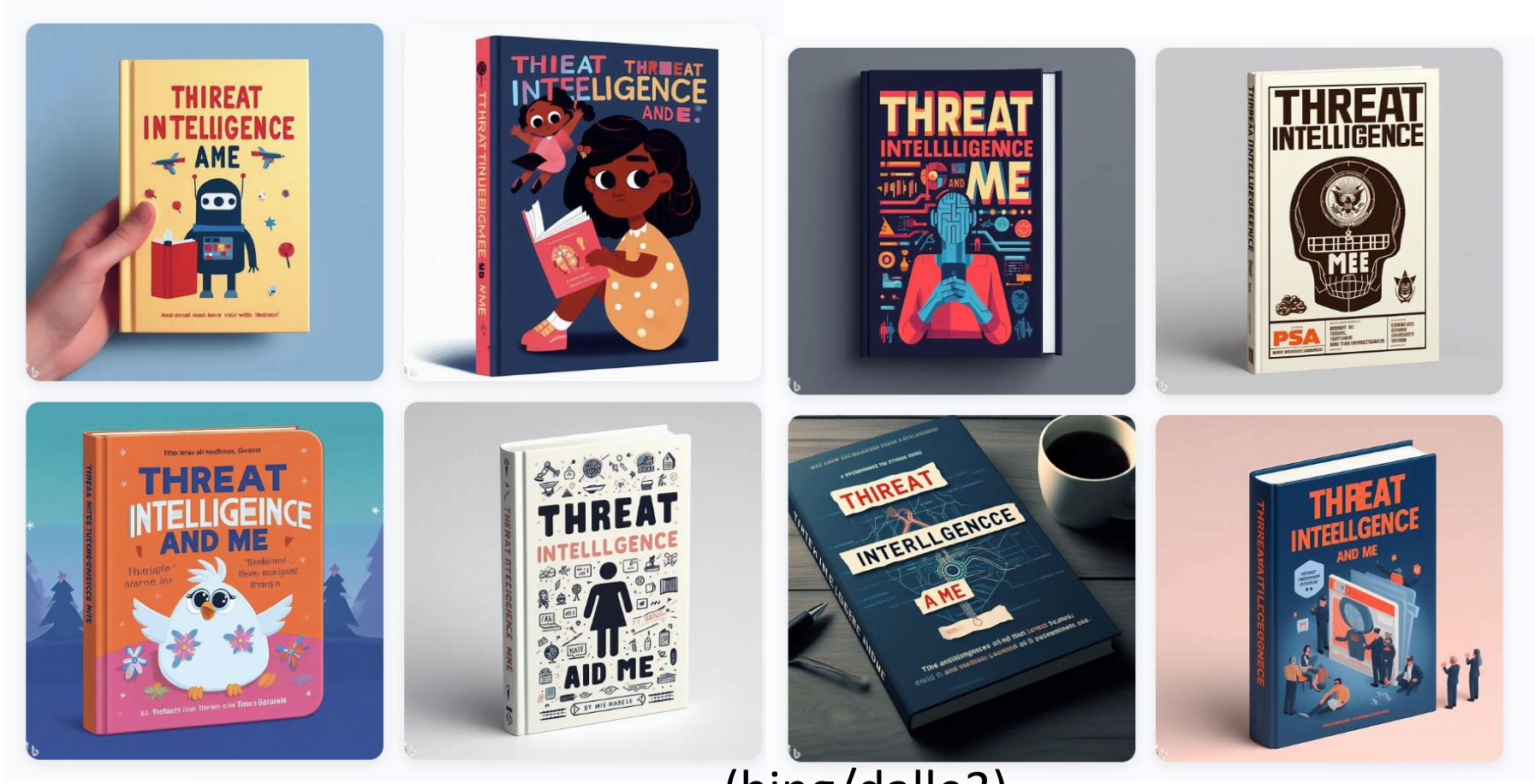
Why can't I guard my company and get answers to the hard stuff that the bad guys did or trying to do!

possible use for Alex slides?

Questions on Threat Intelligence and answers →



What does “success” look like for Threat Intelligence in a SOC?



(bing/dalle3)

Alex Lanstein
Director / Threat Research
StrikeReady

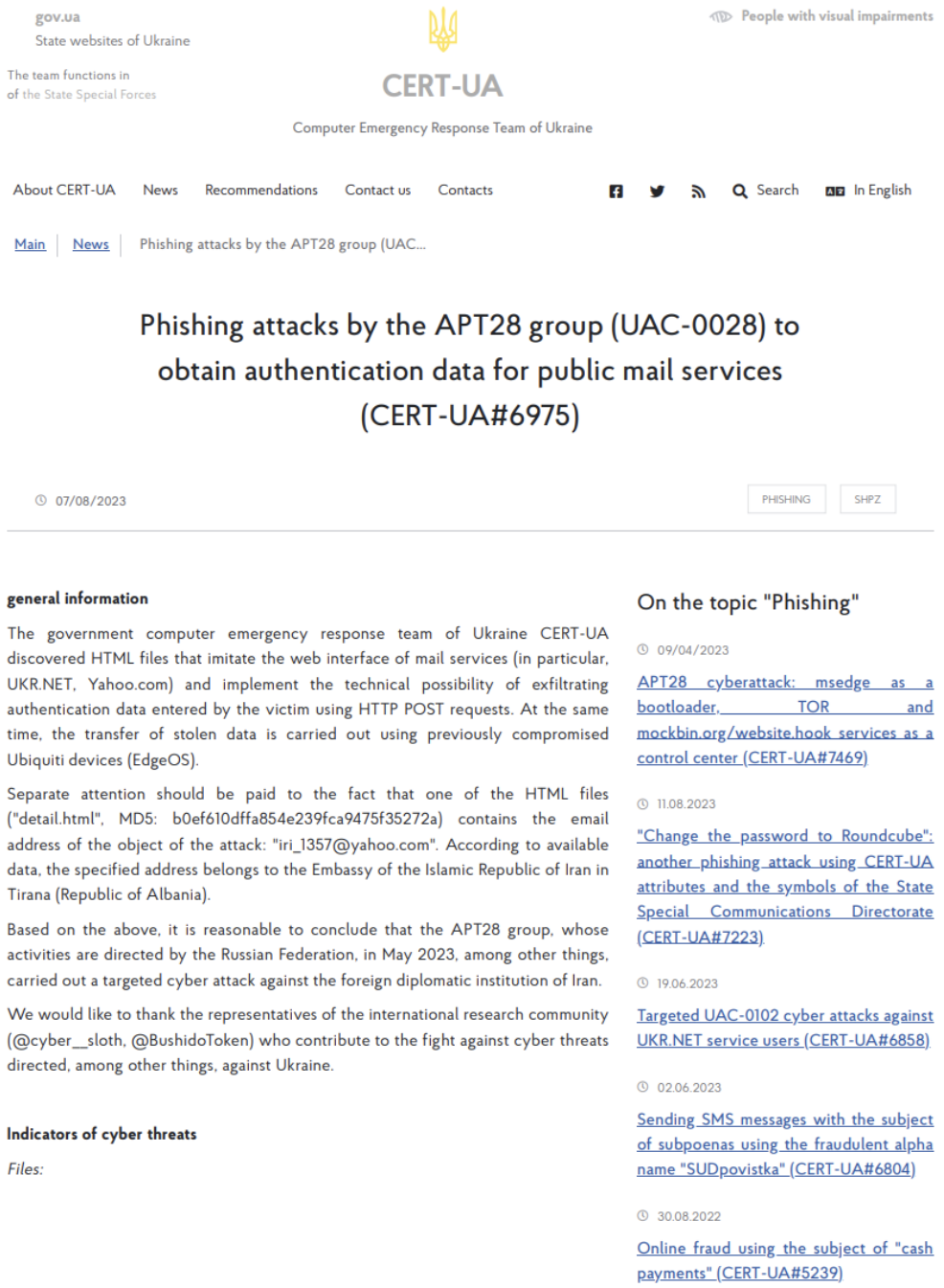
The Institute of Internal Auditors Chicago

ISACA Chicago Chapter

There are hundreds of quality intel sources who publish every day

- Government CERTs
- Security vendors
- Independent researchers
- ISACs
- And of course … paid intelligence providers

And your boss could wave any of them around the SOC



gov.ua
State websites of Ukraine

People with visual impairments

The team functions in
of the State Special Forces

CERT-UA

Computer Emergency Response Team of Ukraine

About CERT-UA | News | Recommendations | Contact us | Contacts | Search | In English

Main | News | Phishing attacks by the APT28 group (UAC...

Phishing attacks by the APT28 group (UAC-0028) to obtain authentication data for public mail services (CERT-UA#6975)

07/08/2023 PHISHING SHPZ

general information

The government computer emergency response team of Ukraine CERT-UA discovered HTML files that imitate the web interface of mail services (in particular, UKR.NET, Yahoo.com) and implement the technical possibility of exfiltrating authentication data entered by the victim using HTTP POST requests. At the same time, the transfer of stolen data is carried out using previously compromised Ubiquiti devices (EdgeOS).

Separate attention should be paid to the fact that one of the HTML files ("detail.html", MD5: b0ef610dffa854e239fca9475f35272a) contains the email address of the object of the attack: "iri_1357@yahoo.com". According to available data, the specified address belongs to the Embassy of the Islamic Republic of Iran in Tirana (Republic of Albania).

Based on the above, it is reasonable to conclude that the APT28 group, whose activities are directed by the Russian Federation, in May 2023, among other things, carried out a targeted cyber attack against the foreign diplomatic institution of Iran.

We would like to thank the representatives of the international research community (@cyber__sloth, @BushidoToken) who contribute to the fight against cyber threats directed, among other things, against Ukraine.

Indicators of cyber threats

Files:

On the topic "Phishing"

09/04/2023
APT28 cyberattack: msedge as a bootloader, TOR and mockbin.org/website.hook services as a control center (CERT-UA#7469)

11.08.2023
"Change the password to Roundcube": another phishing attack using CERT-UA attributes and the symbols of the State Special Communications Directorate (CERT-UA#7223)

19.06.2023
Targeted UAC-0102 cyber attacks against UKR.NET service users (CERT-UA#6858)

02.06.2023
Sending SMS messages with the subject of subpoenas using the fraudulent alpha name "SUDpovistka" (CERT-UA#6804)

30.08.2022
Online fraud using the subject of "cash payments" (CERT-UA#5239)

“Create an image of a boss in a security operations center waving a piece of paper”

(adobe firefly)

When your boss asks you about a report — what are they really asking?

- Did we get hit by “this thing”, and we blocked it?

- Did we got lucky this time, or were we not vulnerable because one of our layers mitigated the damage?

- If we had have gotten hit by this
  - Were we vulnerable to any part of it?
  - Would our tools have detected it?
  - If our tools detected it, would our humans have recognized this was an important detection?

Lastly, and perhaps most importantly:

> “Did we get hit by this thing, **or a close variation**, and our tools did not detect it?”

Did we get hit by “this thing”, and we blocked it?

Need to extract:

- IPs
- Domains
- Email addresses
- Hashes
- File Paths/behavior

Indicators of cyber threats

Files:

```
76dd1a509028dab3e45613f2f5b062f0 ab7d21d81de1039345f9b08d5b64b3c015ea70a15d7
4b6880d3b614548fec6426b8caea2840 8c268cf8d0bbe3ab1f25f5fdc205c14e30d78a63cc4
9ff8225ea895e8e8a9f1d768bc41ba77 47569fbf80dda804b4ea00c5678d4d98113c3b1f2e5
20d7223482ed78acedb3bd19e4b98a46 aab6b46c209305b4fef7c7bfc16cc9ada1e937ef322
80067d1c66f79910ddad67d17998851c 1c47e40a2f4dc93ed5b8253278799a4cd70890ec968
b7c7dc5d07ddd105e0c6de37967b5aa9 561ab624c7214e3b21edd97bf575d5ec0ff7da25b1a
4b6880d3b614548fec6426b8caea2840 8c268cf8d0bbe3ab1f25f5fdc205c14e30d78a63cc4
9ff8225ea895e8e8a9f1d768bc41ba77 47569fbf80dda804b4ea00c5678d4d98113c3b1f2e5
20d7223482ed78acedb3bd19e4b98a46 aab6b46c209305b4fef7c7bfc16cc9ada1e937ef322
74e07e9b83c3967578e2b8c88f7c20d1 4b4fbfb0f201d6b80f22cbf1c8d6b1fb2e1a155ce37
8718966fa7ad85b5be84655251f2a8fe 9b6b926b7089d401a6f73094167a6144dd3f6e48512
a8085a7b624d572de024e53871da49ea af4d7ad40e505d047f9df078ef3f6c7e0207c882dc9
3951e4409e66a767af53ee9a920386b9 d03373be2435af1966bfdfe51ae6d0038e4d4f3c353
```

Network:

```
arunmishra1974@portugalmail.pt
louw@seznam.cz
hXXps://mockbin[.]org/bin/%GUID%
hXXps://mockbin[.]org/bin/%GUID%/%w
hXXps://run.mocky[.]io/v3/%GUID%
hXXps://webhook[.]site/%GUID%
mockbin[.]org (Legitimate service)
mocky[.]io (Legitimate service)
run.mocky[.]io (Legitimate service)
webhook[.]site (Legitimate service)
file[.]io (Legitimate service)
ipapi[.]co (Legitimate service)
185.220.100[.]253 (Received)
173.239.196[.]198
```

Hosts:

```
%PROGRAMDATA%\l09y3n.cmd
%PROGRAMDATA%\z201qo.cmd
%PROGRAMDATA%\%GUID%.bat
%PROGRAMDATA%\%GUID%.vbs
%PROGRAMDATA%\Lotus\Data\config.ini
%PROGRAMDATA%\Lotus\service\ManagementServic
%PROGRAMDATA%\Lotus\LotusManagementNowServic
C:\Windows\System32\Tasks\Lotus\LotusManagem
C:\Windows\System32\WScript.exe %PROGRAMDATA
C:\Windows\system32\cmd.exe /c ""%TMP%\Rar$D
C:\Windows\system32\cmd.exe /c ""%PROGRAMDAT
start "" msedge --headless=new --disable-gpu
start "" msedge --headless=new --disable-gpu
powershell Compress-Archive %USERPROFILE%\Ap
powershell.exe Test-NetConnection -ComputerN
```

Did we get hit by “this thing”, and we blocked it?

Integration Stack

Endpoint	Network	Email	Intel	IAM	Cloud
Forensic	Vuln	Case	SIEM	VPN	Mgmt

Goal: search across all deployed technology to search for alerts that specifically match indicators from an intel report

Did we got lucky this time, or were we not vulnerable because we prepared?

Goal: understand systematic weaknesses that the threat actor took advantage of

CVEs

Visibility Gaps

Credential Stuffing

Embedded CVEs

Shadow IT

Unknown Systems

Would our tools have detected it? Would our humans have recognized this was an important detection?

Goal: simulate the threat

1) download a payload through your detection stack (firewall, ips, proxy, etc)
2) beacon out to c2s through your infrastructure
3) Execute payloads on a workstation running your EDR

If there aren't detections across the stack

- Triage! Tuning, Alert/log centralization, YARA, snort ...

If there are detections:

- Would a human have noticed and triaged this alert?
  - Many vendors play fast&loose with detection questions

Did we get hit by "this thing", or a variant, and we missed it?

- Did we receive any email from this sender, whether it was blocked or not? Is anyone communicating with it?
- Did any system make a request to the domain or IP? What process did it?
- Did this IP scan any of our public facing systems? Did they register for an account on any of our hosted products?
- Did we see this hash downloaded anywhere, or does this hash currently exist anywhere? (imagine the scenario where the reported hash is a top level archive)

- Did seeing this threat alert make you realize you do not have visibility in a certain segment?

Did we get hit by “this thing”, **or a variant**, and we missed it?

Void Rabisu Targets Female Political Leaders with New Slimmed-Down ROMCOM Variant

Network

URL	Description
hXXps://onedrive.live[.]com/?authkey=%21AAdO%2Di5%2DikrnuaA&id=79E2A760F4732317%21106&cid=79E2A760F4732317	OneDrive folder hosting ROMC
wplsummit.com	Fake WPL Summit 2023 page
https://mctelemetryzone.com/favicon.ico	Second stage downloader
netstaticsinformation.com	ROMCOM C&C
redditanalytics.pm	ROMCOM modules
wirelessvezion.com	Suspected ROMCOM C&C (CHECK)
budgetnews.org	ROMCOM C&C
pap-cut.com	Malware hosting
speedymarker.com	SEO domain
kayakahead.net	SEO domain

Files

SHA-256	File name	Description
4f66d6ec70a49aaddb8018af1bf859284a6a4a27eb2615c80a32d5c7c156e476	Unpublished Pictures 1-20230802T122531-002-sfx.exe	First stage
4299c16e11a725dd2ac9468c5c0aabf94ea5a90d2232810c19ba13b35b3708f9 (encrypted)	favicon.ico	Second stage
3c014d59cf22acbd062a4e2cab8cb8ede7127b6a69af9db45a7dcefde866369a (decrypted)	favicon.ico	Second stage
41e995a8554fb6e4160d0e445856221ece2117a2b030012ead9efe76611bdc14	Security.dll	Third stage
d1ca5349da287dbb13a1ea2a2982d23e6ce34ed822baee7468ce1980a4179d42	OneDriveService.dll	Third stage
83448756a4cafbfd784d36add719cffa65b912e550d3a5fd63d407201c6ff94c	pcmf-installer-23.0.5.exe	ROMCOM 3.0 c

Did we get hit by “this thing”, **or a variant**, and we missed it?

redditanalytics.pm > 79.124.78.58 > 155.94.208.147
any ANYIPV4 ANYIPV4

Monitor

Clear Filters | Total Results: 5 | Results on current page: 5

Query	Query ASN	Answer	Answer ASN	First Seen	Last Seen
redditanalytics.pm	-	79.124.78.58	201133	2023-09-19 11:56:19	2023-11-03 05:08:08
redditanalytics.pm	-	155.94.208.147	207083	2023-08-04 13:55:50	2023-09-18 12:24:35
redditanalytics.pm	-	1-you.njalla.no	-	2023-08-04 13:56:10	2023-11-03 13:35:30
redditanalytics.pm	-	2-can.njalla.in	-	2023-08-04 13:56:10	2023-11-03 13:35:30
redditanalytics.pm	-	3-get.njalla.fo	-	2023-08-04 13:56:10	2023-11-03 13:35:30
mail.uream.com	-	155.94.208.147	207083	2023-08-29 16:24:51	2023-09-29 13:58:19
uream.com	-	155.94.208.147	207083	2023-08-29 16:24:45	2023-09-29 13:57:46
www.redditanalytics.pm	-	155.94.208.147	207083	2023-08-04 13:55:49	2023-09-18 23:18:04
redditanalytics.pm	-	155.94.208.147	207083	2023-08-04 13:55:50	2023-09-18 12:24:35

Are we an "apex" SOC?

BeyondTrust Discovers Breach of Okta Support Unit

October 20, 2023

Blog

Summary

On October 2nd, 2023, the BeyondTrust security teams detected an identity-centric attack on an in-house Okta administrator account. We immediately detected and remediated the attack through our own Identity Security tools, resulting in no impact or exposure to BeyondTrust's infrastructure or to our customers. The incident was the result of Okta's support system being compromised which allowed an attacker to access sensitive files uploaded by their customers.

The incident began when BeyondTrust security teams detected an attacker trying to access an in-house Okta administrator account using a valid session cookie stolen from Okta's support system. Custom policy controls blocked the attacker's initial activity, but limitations in Okta's security model allowed them to perform a few confined actions. BeyondTrust's own Identity Security Insights tool alerted the team of the attack, and they were able to block all access and verify that that attacker did not gain access to any systems.

The initial incident response indicated a possible compromise at Okta of either someone on their support team or someone in position to access customer support-related data. We raised our concerns of a breach to Okta on October 2nd. Having received no acknowledgement from Okta of a possible breach, we persisted with escalations within Okta until October 19th when Okta security leadership notified us that they had indeed experienced a breach and we were one of their affected customers.

How Cloudflare mitigated yet another Okta compromise

10/20/2023

 Sourov Zaman  Lucas Ferreira  Kimberly Hall

 Grant Bourzikas

3 min read

On Wednesday, October 18, 2023, we discovered attacks on our system that we were able to trace back to Okta – threat actors were able to leverage an authentication token compromised at Okta to pivot into Cloudflare's Okta instance. While this was a troubling security incident, our Security Incident Response Team's (SIRT) real-time detection and prompt response enabled containment and minimized the impact to Cloudflare systems and data. We have verified that **no Cloudflare customer information or systems were impacted by this event** because of our rapid response. Okta has now released a public statement about this incident.

This is the second time Cloudflare has been impacted by a breach of Okta's systems. In March 2022, we blogged about our investigation on how a breach of Okta affected Cloudflare. In that incident, we concluded that there was no access from the threat actor to any of our systems or data – Cloudflare's use of hard keys for multi-factor authentication stopped this attack.

The key to mitigating this week's incident was our team's early detection and immediate response. In fact, we contacted Okta about the breach of their systems before they had notified us. The attacker used an open session from Okta, with Administrative privileges, and accessed our Okta instance. We were able to use our Cloudflare Zero Trust Access, Gateway, and Data Loss Prevention and our Cloudforce One threat research to validate the scope of the incident and contain it before the attacker could gain access to customer data, customer systems, or our production network. With this confidence, we were able to quickly mitigate the incident before the threat-actors were able to establish persistence.

Are we an "apex" SOC?

The Washington Post
Democracy Dies in Darkness

Chinese cyberspies, exploiting a fundamental gap in Microsoft's cloud, hacked email accounts at the Commerce and State departments, including that of Commerce Secretary Gina Raimondo — whose agency has imposed stiff export controls on Chinese technologies that Beijing has denounced as a malicious attempt to suppress its companies.

Sign up for Fact Checker, our weekly review of what's true, false or in-between in politics. →

Raimondo is the only known Cabinet-level official to have their account compromised in the targeted cyberespionage campaign, according to U.S. officials familiar with the matter, who spoke on the condition of anonymity due to the matter's sensitivity.

The breaches have been mitigated, officials said, but an FBI investigation continues.

The Microsoft vulnerability was discovered last month by the State Department. Also targeted were the email accounts of a congressional staffer, a U.S. human rights advocate and U.S. think tanks, officials and security professionals said. State and Commerce were the only two executive branch agencies known to be breached, officials said.

Microsoft mitigates China-based threat actor Storm-0558 targeting of customer email

MSRC / By MSRC / July 11, 2023 / 3 min read

UPDATE: Microsoft performed a comprehensive technical investigation into the acquisition of the Microsoft account consumer signing key, including how it was used to access enterprise email. Our technical investigation has concluded, and on September 6, 2023, we published our investigation findings.

Microsoft has released threat analysis on Storm-0558 activity here. Microsoft additionally released additional defense-in-depth security fixes to help customers improve token validation in their custom applications.

Microsoft has mitigated an attack by a China-based threat actor Microsoft tracks as Storm-0558 which targeted customer emails. Storm-0558 primarily targets government agencies in Western Europe and focuses on espionage, data theft, and credential access. Based on customer reported information on June 16, 2023, Microsoft began an investigation into anomalous mail activity. Over the next few weeks, our investigation revealed that beginning on May 15, 2023, Storm-0558 gained access to email accounts affecting approximately 25 organizations in the public cloud including government agencies as well as related consumer accounts of individuals likely associated with these organizations. They did this by using forged authentication tokens to access user email using an acquired Microsoft account (MSA) consumer signing key. **Microsoft has completed mitigation of this attack for all customers.**

Our telemetry indicates that we have successfully blocked Storm-0558 from accessing customer email using forged authentication tokens. **No customer action is required.** As with any observed nation-state actor activity, Microsoft has contacted all targeted or compromised organizations directly via their tenant admins and provided them with important information to help them investigate and respond. We continue to work closely with these organizations. **If you have not been contacted, our investigations indicate that you have not been impacted.**

Microsoft is partnering with DHS CISA and others to protect affected customers and address the issue. We continue to investigate and monitor the Storm-0558 activity.

PRODUCT

StrikeReady unifies all the elements necessary for proactive cyber defense into a single, AI-based platform.

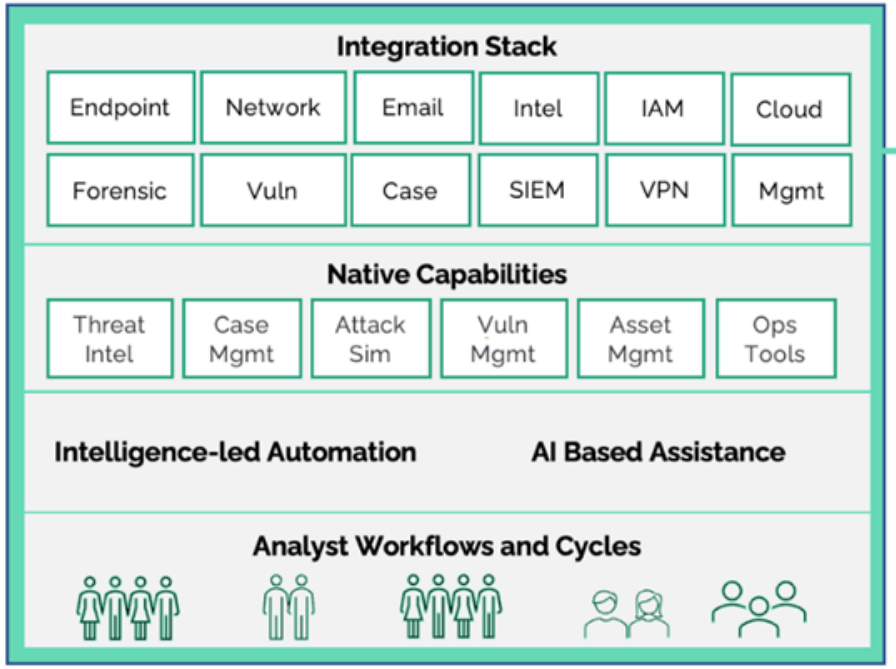
STRIKE READY

INTEGRATE

CONSOLIDATE

RECOMMEND, TRAIN & ASSIST

COMMON WORKSPACE

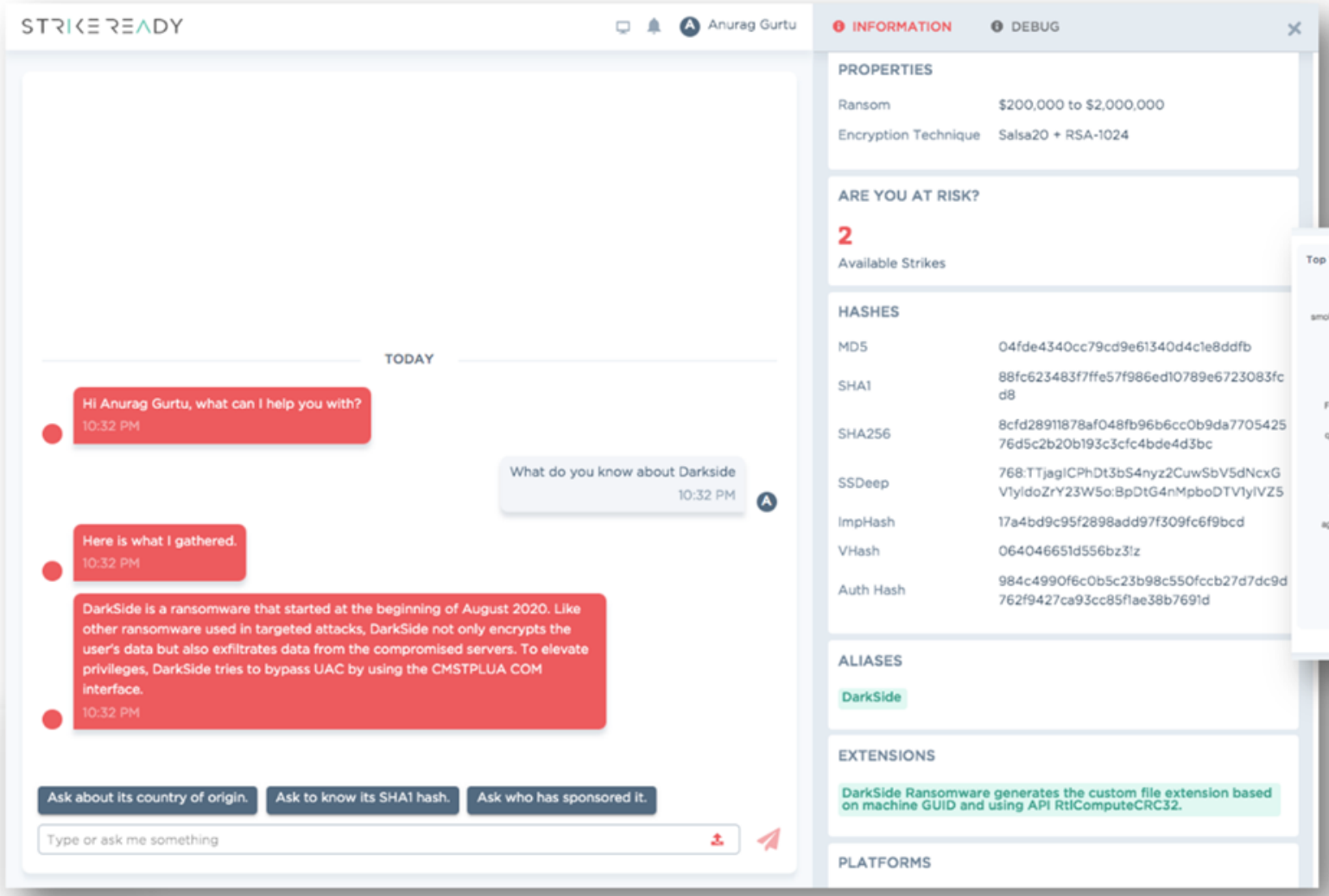


400 pre-built, security integrations

STRIKE READY

USE CASES

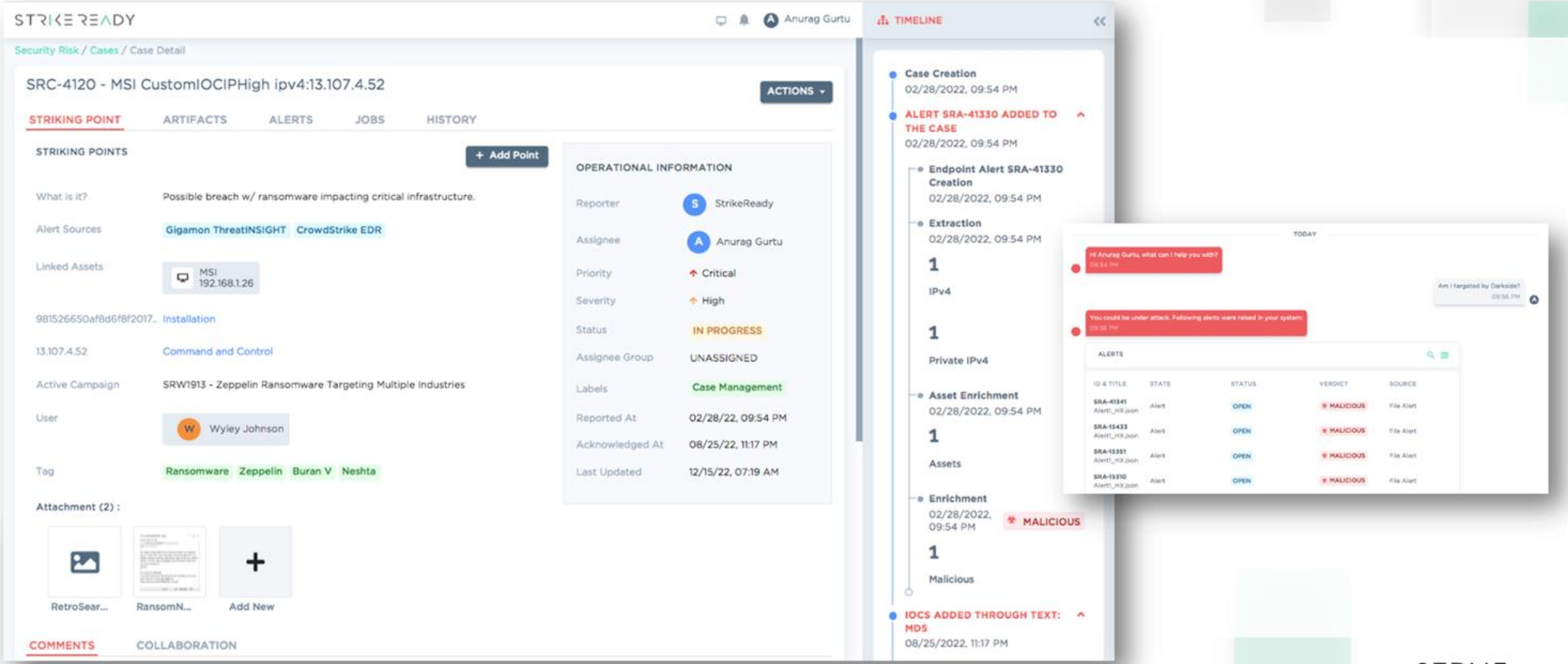
Threat Intel Analyst – Automated threat intel ingestion, prioritization & deployment



STRIKE READY

USE CASES

SOC/IR Analyst – Automated alert analysis, enrichment, triage, documentation & response



THANK YOU

https://www.linkedin.com/in/frajpari

fayyaz@intelliguards.com

https://www.linkedin.com/in/alexlanstein/

alex@strikeready.com

Welcome To The 10th Annual Hacking Conference

Remember to check-in to this session on the app!

The Institute of Internal Auditors Chicago

ISACA Chicago Chapter