

# What You Need To Know About the Ransomware Economy



Steve Allison  
Field CISO

[s.allison@cdw.com](mailto:s.allison@cdw.com)



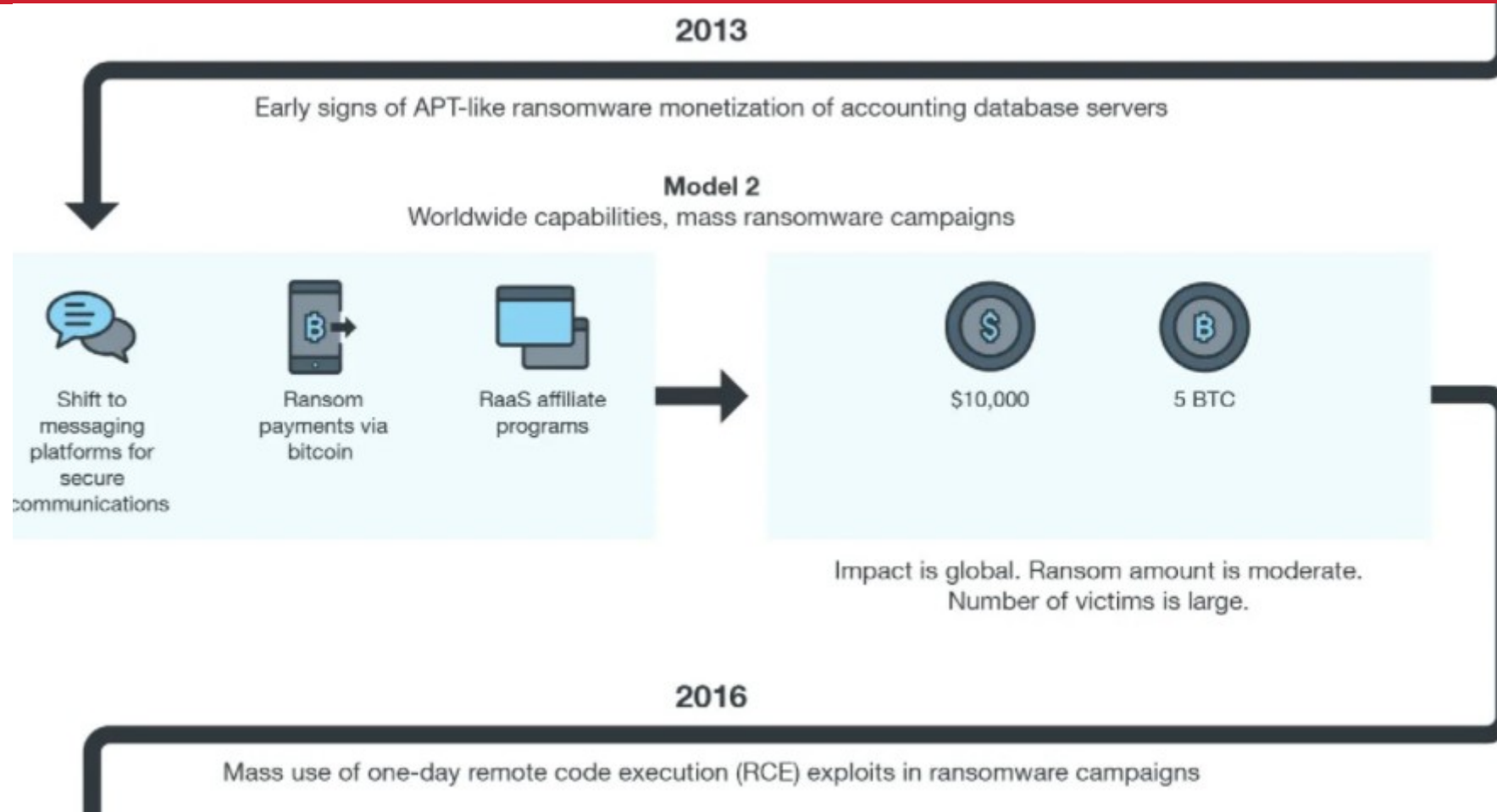
# QUICK INTRODUCTION

- **Field CISO with CDW**
- **10 years of USAF Intelligence Operations specializing in Cyber Warfare.**
- **Global Head of Threat, Vulnerability, and Investigation Management at DPWN / DHL.**
- **Americas Regional Head of Information Security and Compliance at T-Systems**
- **Cyber Security Strategist (Healthcare/Fed/Corp) - Symantec / Trend Micro**
- **Security Consultant with Paragnet**

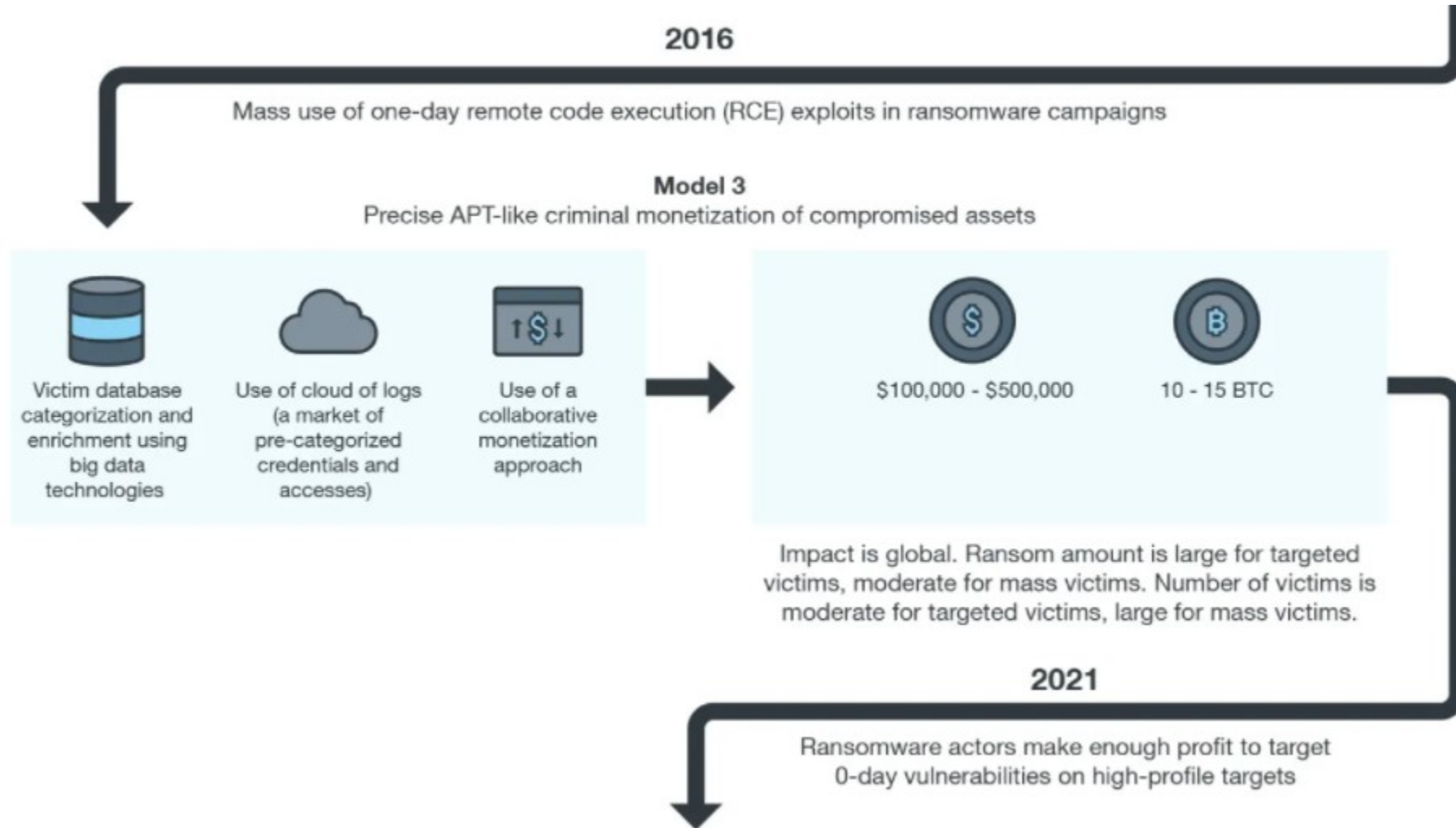
# LIFE OF A CISO IN A SINGLE PICTURE



# RANSOMWARE – BRIEF HISTORY



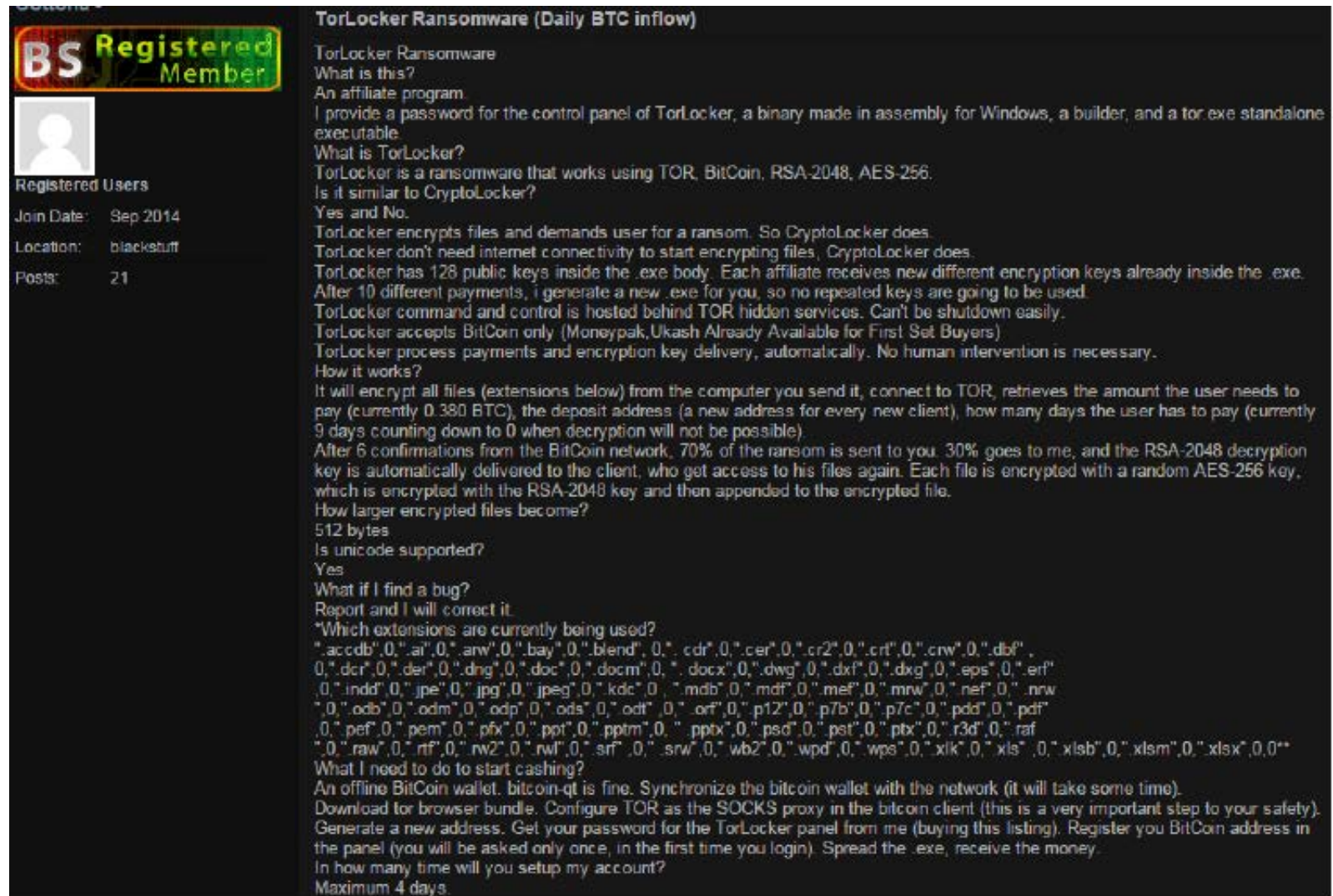
# RANSOMWARE – BRIEF HISTORY



# RANSOMWARE AS A SERVICE

Malware developers creating malware “kits” in exchange for a percentage of the profits.

Keeps the developers beyond an arm’s length



The screenshot shows a forum post on a dark background. At the top left, there is a profile for a user named 'BS Registered Member' with a join date of 'Sep 2014', location 'blackstuff', and 21 posts. The main title of the post is 'TorLocker Ransomware (Daily BTC inflow)'. The text of the post describes an affiliate program for TorLocker ransomware, detailing its operation, payment methods (BitCoin), and a list of file extensions it targets. The list of extensions includes: .accdb, .ai, .arw, .bay, .blend, .cdr, .cer, .cr2, .crt, .crw, .dbf, .dcr, .der, .dng, .doc, .docm, .docx, .dwg, .dxf, .dxd, .eps, .erf, .indd, .jpe, .jpg, .jpeg, .kdc, .mdb, .mdf, .mef, .mrw, .nef, .nrw, .odb, .odm, .odp, .ods, .odt, .orf, .p12, .p7b, .p7c, .pdd, .pdf, .pef, .pem, .pfx, .ppt, .pptm, .pptx, .psd, .pst, .ptx, .r3d, .raf, .raw, .rtf, .rw2, .rwl, .srf, .srw, .wb2, .wpd, .wps, .xlk, .xls, .xlsx, .xlsm, .xlsx\*. The post also includes instructions on how to use the ransomware, such as downloading a BitCoin wallet, configuring TOR, and generating a new address.

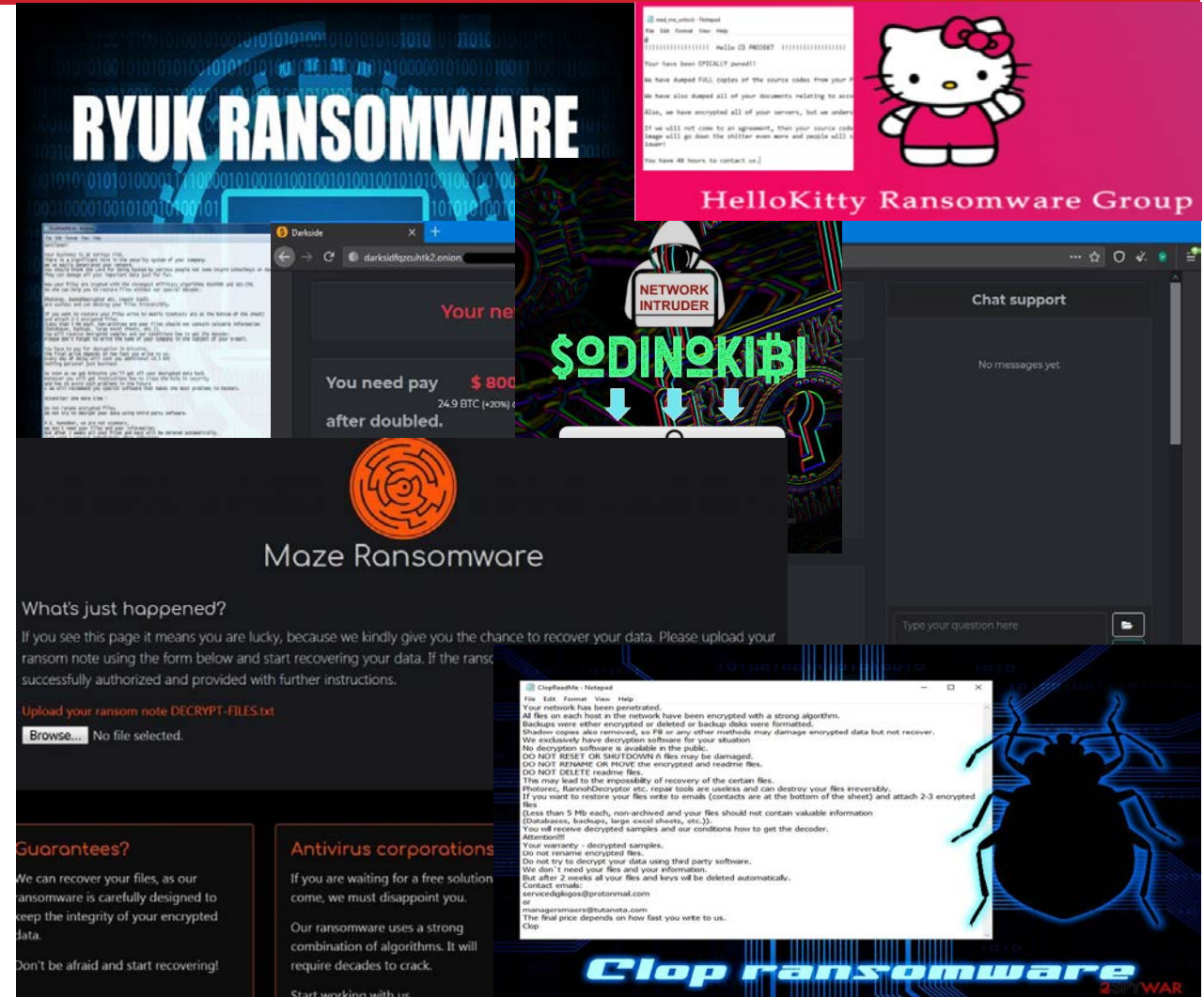
“In part, we are all connected to gandrevil, blackside, mazegreggor, lockbit, etc., because we are adverts [affiliates]...

There is no rebranding or a mix of talents because we have no direct relation to these partnership programs. Let’s just say: “We borrowed their advantages and eliminated their disadvantages.”

-Alphv/BlackCat Operator in 2022 interview with Recorded Future

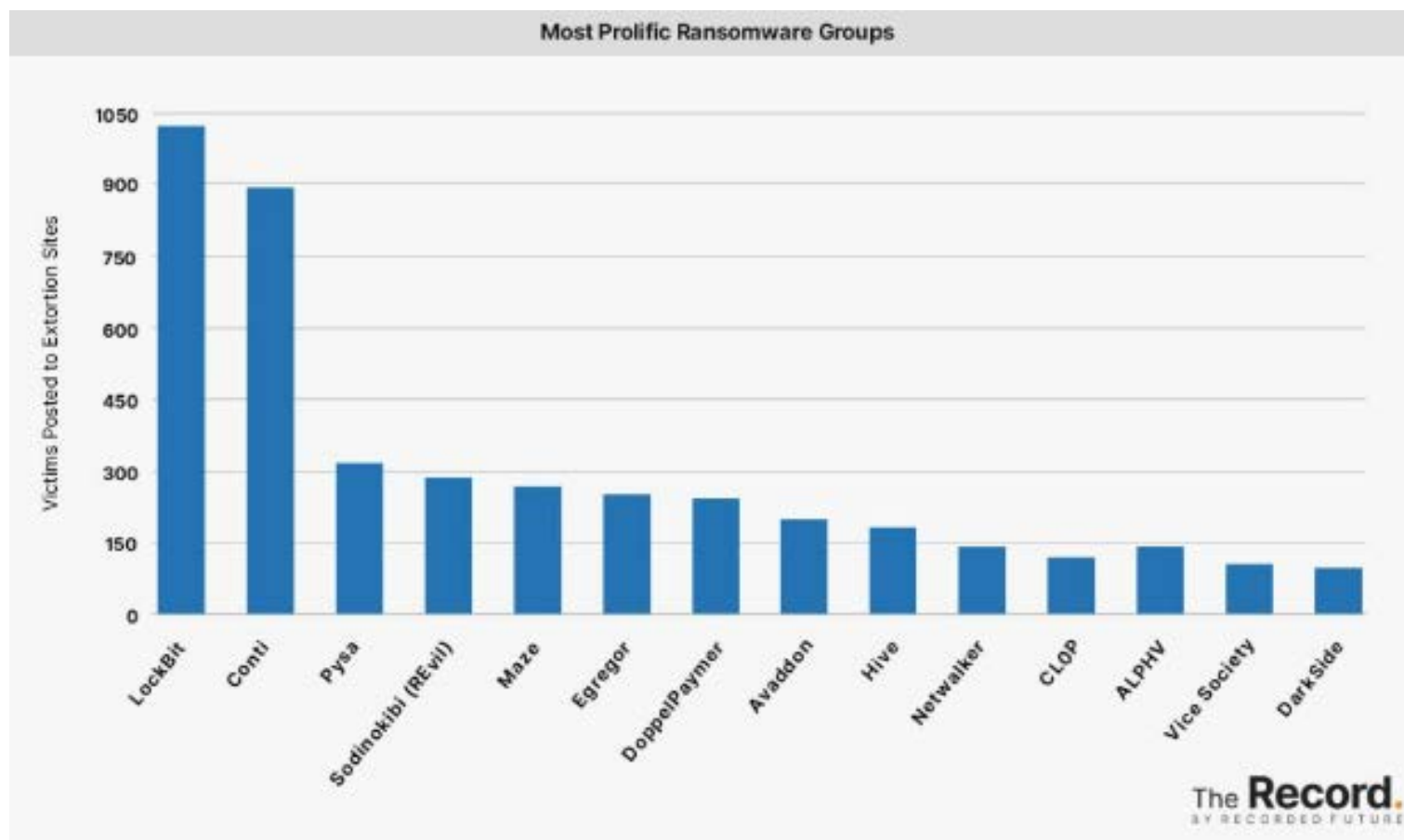
# CURRENT EXTORTION LANDSCAPE

- Multi-Extortion is the new norm **86%** of Ransomware Attacks Involved the Threat to Leak Exfiltrated Data (+5% From Q1 2021)
- The primary extortion channels include data encryption / lockout and data disclosure via “name and shame” websites
- At the Beginning of 2020 there were four (4) main ransomware variants leveraging blended extortion techniques. **Sodinokibi, DoppiePaymer, Ryuk, The Maze.** Now there are dozens of variants and groups utilizing multi-extortion techniques.
- This marriage of crypto and data extortion along with pandemic related phishing scams, targeting at-home workers and increased remote access with reduced security controls has led to a surge in ransomware attacks and costs





# MOST PROLIFIC RANSOMWARE GROUPS Q3 2022

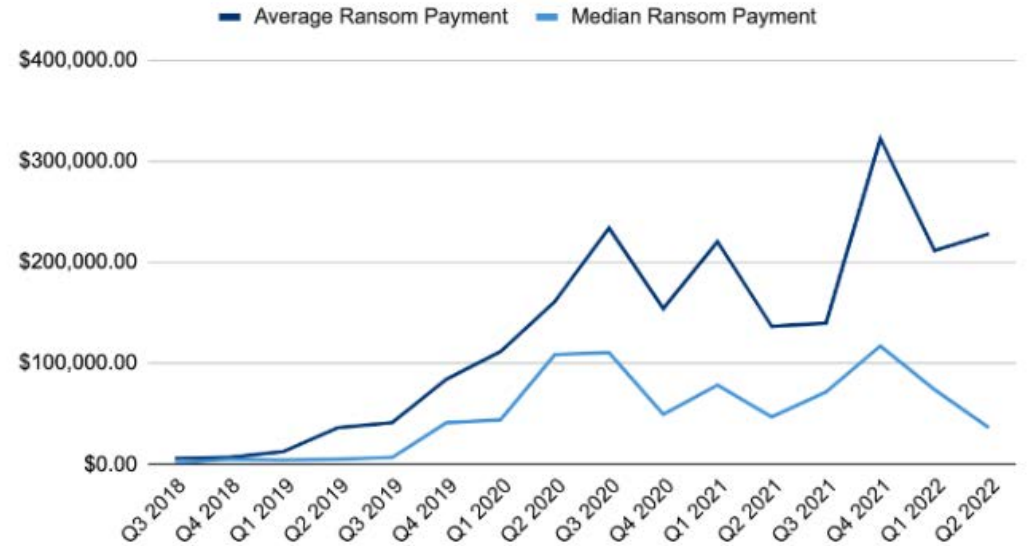


# INCREASED RANSOM COSTS

- The average ransom payment for a mid-size enterprise organizations in the 1000-5000 employee range is over **\$1 million**
- The Ransom Economy is set to exceed **\$1.4 billion** in the U.S. in 2022.
- Victims average **12-23 days of downtime** from Ransomware attacks. Which drives the total cost estimate to **\$9.3 billion** in the US alone.
- Average ransom for all attacks worldwide has more than **tripled since 2018**



Ransom Payments By Quarter



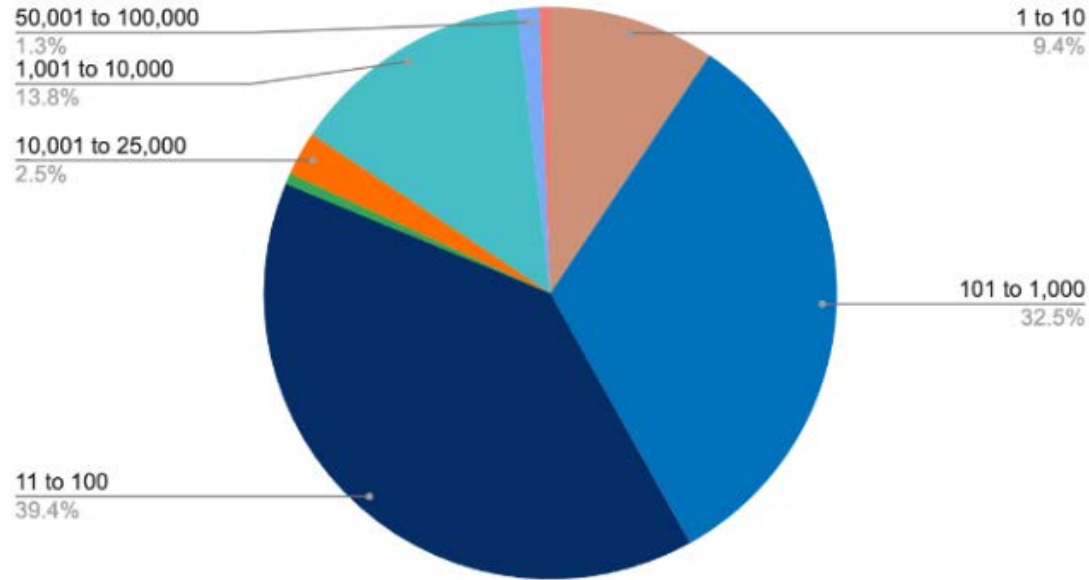
Average Ransom Payment Q1 2022

**\$228,125**

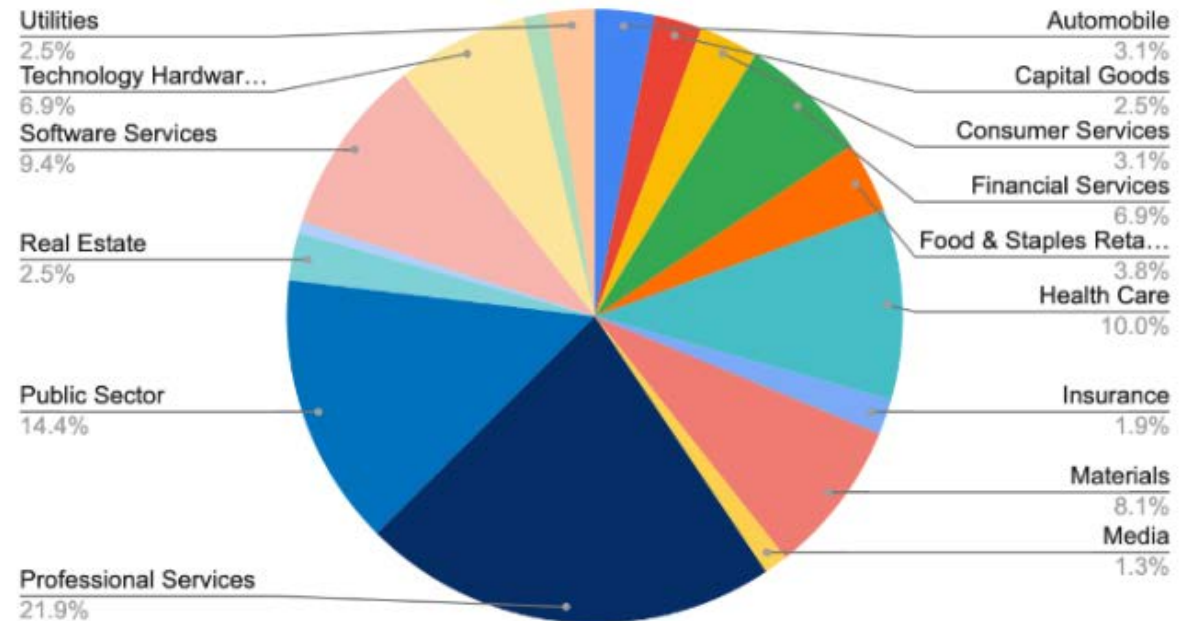
+8% from Q1 2021

# EXTORTION TARGETS

## Ransomware Impacted Companies by Size (Employee Count)



## Industries Impacted by Ransomware Q2 2022

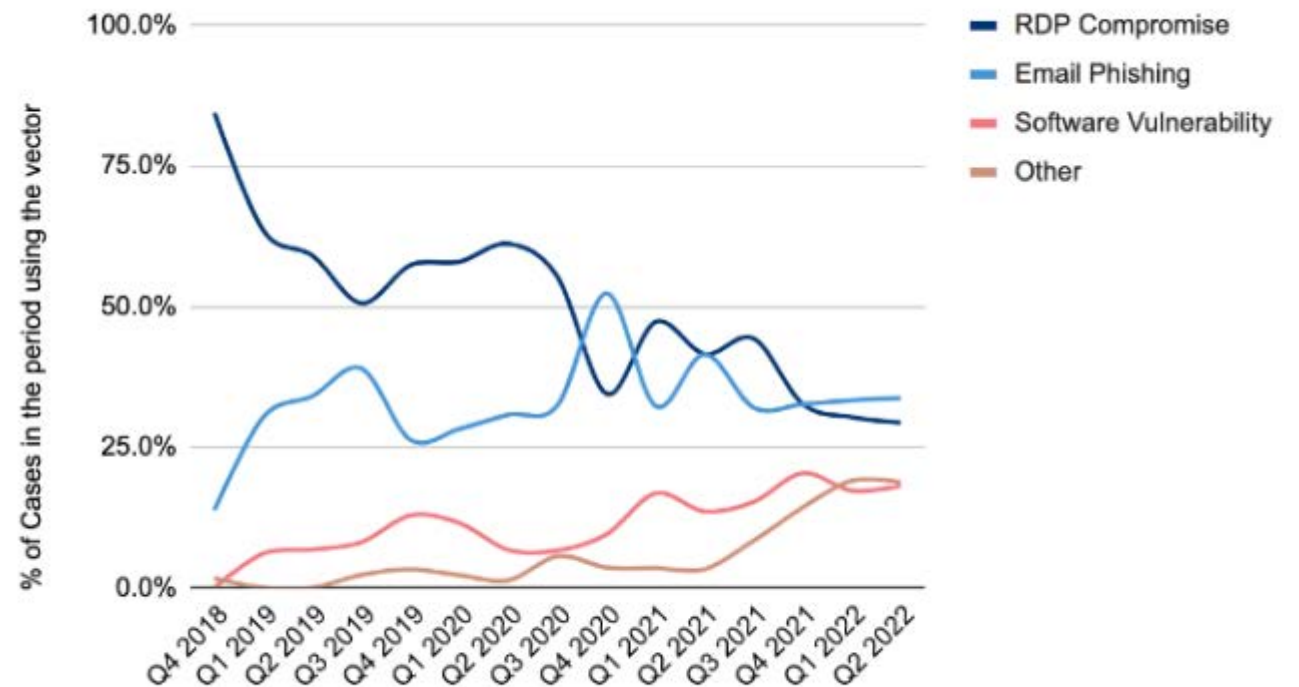


# RANSOMWARE ATTACK VECTORS AND MITRE ATT&CK TTPS OBSERVED IN Q2 2022

Notable shifts in attack vectors during the quarter involved the rise of the 'other' category which includes social engineering and direct compromising of insiders, along with a few other methods.

The social engineering attacks differ from phishing in that they are highly targeted and typically involve some priming or grooming of a target employee, before they are coaxed into allowing an attacker to gain a foothold into the network

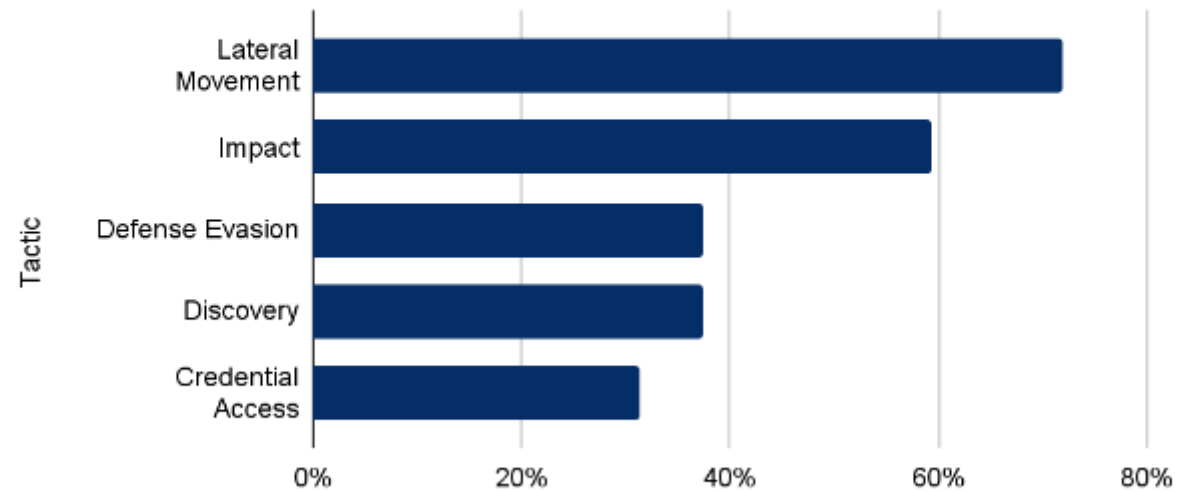
Ransomware Attack Vectors



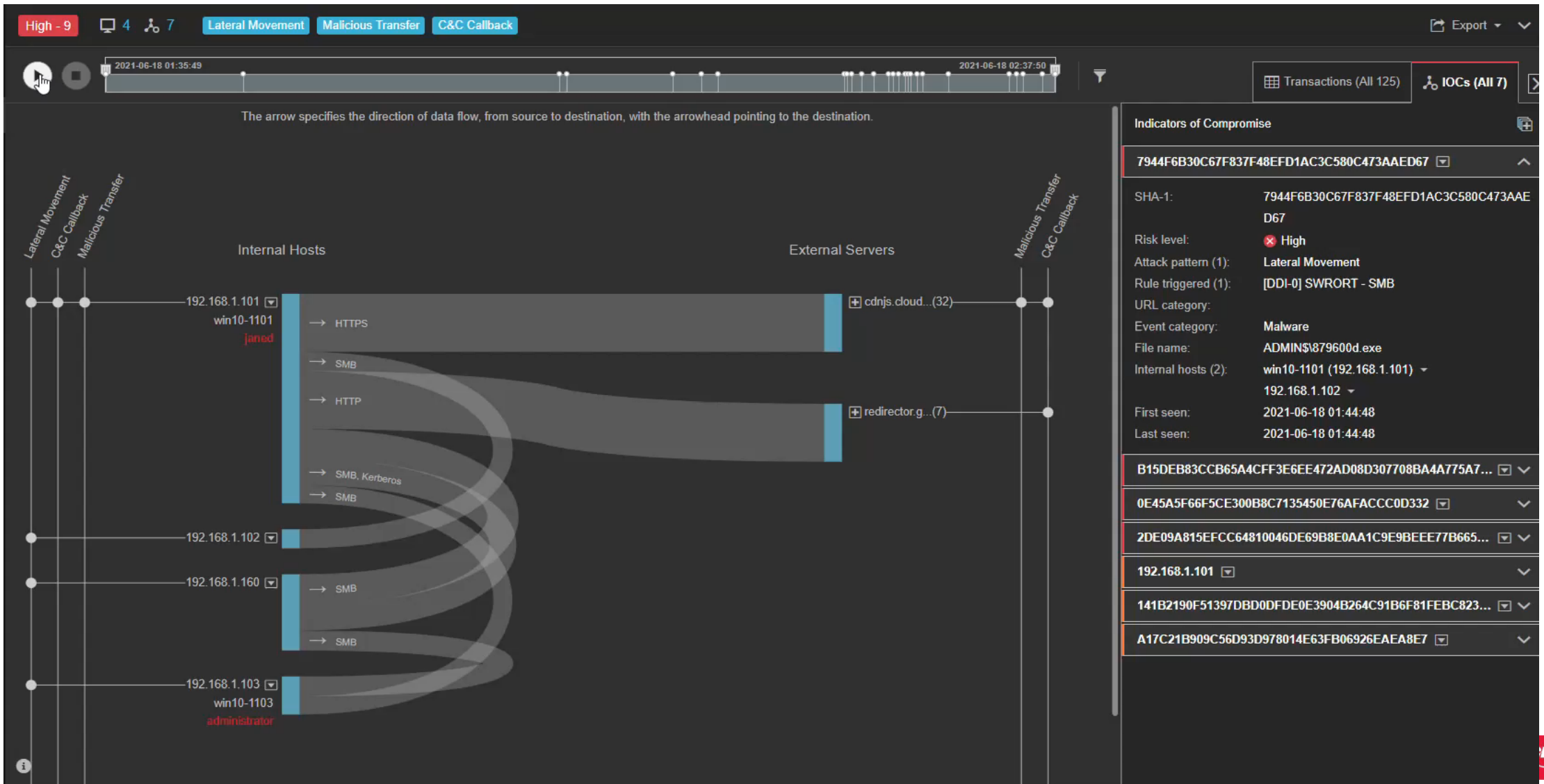
# EXTORTION TACTICS

Top MITRE ATT&CK TTPs observed in Q1 2022

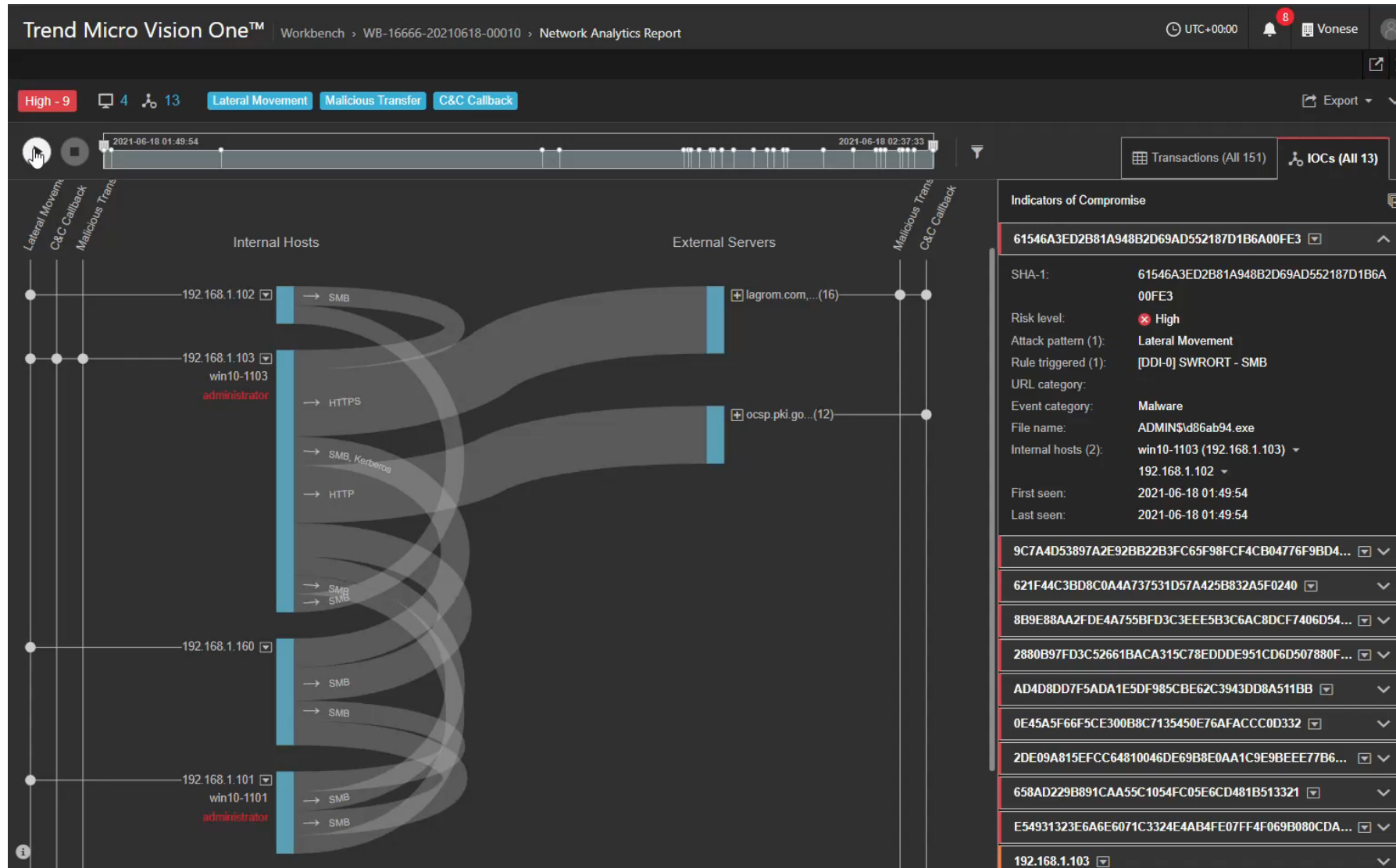
% of Cases vs. Observed Tactic



# WHAT AN ATTACK LOOKS LIKE



# WHAT AN ATTACK LOOKS LIKE



IN THE NEWS !!!





# LAPSUS\$

Lapsus\$ is a recently discovered cyber threat group (2020).

- They have not brought overly sophisticated tools to an attack but have been successful regardless.
- They have been effective, but also unprofessional and careless:
- Tactics, techniques and procedures range from simple to moderately complex.
- They have successfully targeted several high-profile organizations to completion.
- Due to the diversity of their techniques, there is no single set of effective defenses or mitigations.
- Possibly a group of teenagers and young adults.
- They utilize “big game hunting” methods – the targeting of large firms.



# LAPSUS\$

- High Profile Victims
- "New" TTPS
  - Pay for Access
  - Max Data Exfill w/ Low Dwell Time
  - Skilled with Social Media
- Teens?

“Nation states have typically wanted longer, more strategic access; ransomware groups want large lateral movement. LAPSUS\$ doesn't care, it's more about, 'What can these 2-3 accounts get me in the next 6 hours?' We haven't optimized to defend that.” -Anonymous CXO via Krebsonsecurity

LAPSUS\$

We hacked NVIDIA,

The hack is kinda public atm, and here's our announcement,

We were into nvidia systems for about a week, we fastly escalated to admin of a lot of systems.

We grabbed 1TB of data,  
We grabbed the most important stuff, schematics, driver, firmware, etc...

We are still waiting for nvidia to contact us.  
We are also selling a full LHR V2 (GA102-GA104) -> we hope it will soon be removed by nvidia

If NVIDIA doesn't contact us, we will take actions.

Please note: We are not state sponsored and we are not in politics AT ALL.

Btw NVIDIA tried but failed, we have all the data.

We also have documentation, private tools and SDKs, and everything about falcon, we know what is valuable, nvidia, please contact us.  
Can mail us @ [nvidia\\_chats@protonmail.com](mailto:nvidia_chats@protonmail.com)

7560 edited 7:08 PM



192 co

Earning opportunity for a mobile carrier employee ~ \$20000+

11/24/2021, 8:16:40 PM

My name is Alex.

I am looking for insiders/employees at either ATT, Verizon or T-Mobile

I can offer you upwards of \$20000 a week to do some \\*inside jobs\\* at either ATT, Verizon or T-Mobile for me. - these tasks are low risk for you and me..... plus you will get paid insanely well by me. - the jobs will involve Sim-Swapping 1 or 2 customers a week.... you won't even be noticed!!!

You can contact me on Telegram, my username is whitedoxbin [<https://t.me/whitedoxbin>](<https://t.me/whitedoxbin>)

[<https://telegram.org/>](<https://telegram.org/>) we can discuss further on Telegram or email. If you are interested. This is a great opportunity for me and you!

LAPSUS\$

We recruit employees/insider at the following!!!!

Reply

- Any company providing Telecommunications (Claro, Telefonica, ATT, and other similar)
- Large software/gaming corporations (Microsoft, Apple, EA, IBM, and other similar)
- Callcenter/BPM (Atento, Teleperformance, and other similar)
- Server hosts (OVH, Locaweb, and other similar)

**TO NOTE: WE ARE NOT LOOKING FOR DATA, WE ARE LOOKING FOR THE EMPLOYEE TO PROVIDE US A VPN OR CITRIX TO THE NETWORK, or some anydesk**

If you are not sure if you are needed then send a DM and we will respond!!!!

If you are not a employee here but have access such as VPN or VDI then we are still interested!!

You will be paid if you would like. Contact us to discuss that

@lapsusjobs

837 37.2K 2:37 PM

# LAPSUS\$

First Identified in 2020

Common tactics/techniques/procedures (TTPs):

- Credential theft
- Multi-factor authentication bypass
- Social engineering (especially phone-based)
- Managed service provider compromise
- SIM-swapping
- Accessing personal email accounts of employees of target organizations
- Bribing employees, suppliers, or business partners of target organizations for credentials and multifactor authentication approval
- Self-injection into ongoing crisis-communication calls of their targets



# LAPSUS\$ VICTIMS

- UBER
- Brazilian Ministry of Health
- Nvidia
- Samsung
- Ubisoft
- Vodafone
- Microsoft
- LG
- Okta
- Globant
- CISCO
- OKTA



# LAPSUS\$ RECRUITING

LAPSUS\$

Reply

**We recruit employees/insider at the following!!!!**

- Any company providing Telecommunications (Claro, Telefonica, ATT, and other similar)
- Large software/gaming corporations (Microsoft, Apple, EA, IBM, and other similar)
- Callcenter/BPM (Atento, Teleperformance, and other similar)
- Server hosts (OVH, Locaweb, and other similar)

**TO NOTE: WE ARE NOT LOOKING FOR DATA, WE ARE LOOKING FOR THE EMPLOYEE TO PROVIDE US A VPN OR CITRIX TO THE NETWORK, or some anydesk**

If you are not sure if you are needed then send a DM and we will respond!!!!

If you are not a employee here but have access such as VPN or VDI then we are still interested!!

You will be paid if you would like. Contact us to discuss that

@lapsusjobs

← 837 👁 37.2K ⭐ 2:37 PM

# LAPSUS\$: NO HONOR AMONGST THEIVES

- London police announced on March 25, 2022, that they arrested seven alleged members of Lapsus\$ Ages ranging from 16 to 21
- 16-year-old from Oxford is alleged to be the leader, having amassed \$14 million
  - AKA “White” or “Breachbase” (also WhiteDoxbin?)
  - Such a skilled hacker that investigators initially believed the activity was automated
- What led to this?
  - WhiteDoxbin purchased a site called Doxbin in 2021, which is a public forum used to post personal information on targets.
  - Doxbin was not administered very well, and the community of users expressed their discontent.
  - WhiteDoxbin sold Doxbin back to its original owner for a significant loss but leaked a lot of private data associated with the site’s members.
  - These members responded by doxxing WhiteDoxbin, up to and including publishing a video of where he allegedly lived as revenge.
- Ironically, members of a doxxing site who were frustrated because their information was leaked in turn leaking information about the site’s owner/administrator, is what ultimately led to the arrests.



# LAPSUS\$: WRAP-UP

- While law enforcement has begun pressuring the group and even arresting some alleged members, operations continue.
- Other members will very likely continue to operate under the Lapsus\$ banner or as part of another group.
- The geographic diversity of this group will make them especially difficult to permanently quash.
- The diversity of their tactics, and their lack of reliance of specific malware variants, make them very difficult to detect or stop.



# MITIGATION TECHNIQUES/STEPS

- Timely OS and software patching
  - Why are we still talking about this?
- Disable remote access/RDP ports if not being used
- Audit/Remove Admin privs
- Network segmentation
- Scan for open listening ports and disable SMBv1
- Implement Application whitelisting
- Monitor Active Directory and local admin groups changes
- Maintain only the most up-to-date version of Powershell
- Have a solution that sees events based on IoCs rather than just malware related.



# MITIGATION TECHNIQUES/STEPS

- Awareness Training, test/scold/retrain, repeat, keep repeating
- Robust email security platform (disable links, remove suspicious attachments, etc.)
- Ensure endpoint protection can auto-update and is effective against ransomware
- Multi Factor Authentication and strong passwords
- Backups air gapped and protected offline
- Plan, TEST, and implement a data recovery plan.
  - TEST again.... Especially recovery.....

## Official Guidance

- Do not pay ransoms
- Ransom payments almost always violate U.S Federal regulations against payments to sanctioned entities.

## Unofficial Guidance

- Extortion Payments should be decided on a case-by-case basis by Executive Leadership, Legal Counsel, Breach Coach, IR Firm and Broker and only after they understanding the risks
- If you choose to pay ransoms, DO NOT include ransom payment specifics in your written Incident Response Plan. Including plans to setup cryptocurrency wallets or retain a ransom broker.

# PARTNER BROKERS

**“Recovery companies we work with only simplify the process. They have their own personal discounts that can vary between 20-40% and the entire recovery process takes no more than 24 hours from the moment of the first contact.”** - Darkside operator

● Support

22 Sep, 12:56 PM [NY time]

Judging by your public statements, you are not shy about talking about it. Do you still need a key? Or can we delete it and upload your data and the source code to the soilmap?

22 Sep, 14:27 PM [NY time]

Victim

We do not care. You will not receive payment. Delete key and go away.

● Support

22 Sep, 14:33 PM [NY time]

due to the fact that coveware has distributed a file-encryptor in this chat there are a lot of people not involved in solving the problem. in order to continue the dialogue, you will need to provide your corporate email to go through the verification procedure and receive a new unique chat link

● Support

22 Sep, 14:36 PM [NY time]

First of all - you violated our data recovery guidelines and decided to use the services of a company called coveware, which is blocked in all ransomware groups, so we will not provide you with any discounts or concessions. Secondly - assuming that you are not interested in getting a decryptor, we started loading all your stolen data, including the source codes from fleet, dispatch, soilmap, aws-cli and much more (about 10 gigabytes) into a CDN to prepare the publication. Thirdly - if negotiations are entered by coveware, we will be ready to lose money, delete keys and block chats, so we recommend that you should contact another data recovery company that we have trusted, or pay by yourself. P.S. also we encrypted the soilmap again and we observe that the entire virtual infrastructure was never restored, and recuva software did not bring any results. We are waiting for feedback on when you are ready to pay for fixing the rate.

22 Sep, 14:42 PM [NY time]

Victim

The only thing we violated was your mother.

22 Sep, 14:50 PM [NY time]

Victim

Hello Sons, My mother's menu consisted of two choices: Take it or leave it! No payment for you! No free bitcoin anymore, Enough is Enough. You can stick your ransomware in your ass.



# THE CYBERSECURITY WORLD

## My Favorite quotes

- “Because that is how we’ve always done it.”
- “What is the second-best option?”
- “I need Admin rights to do my job.”
- “If WE haven’t been attacked, why do we need that?”
- “I didn’t go to a non-work-related website.”
- “I didn’t open any attachments.”

And my favorite of all time:

- “What do we need to do to make sure this never happens.....  
Again.” -- Every CIO I’ve ever talked to (post incident).



# FINAL THOUGHTS

- Have a roadmap for the future Cyber Security architecture
- Work with your security partner to establish that roadmap
- Incident based spending comes fast.....
  - .....and ends just as fast.

# Questions???

**Steve Allison**  
**Field CISO**  
s.allison@cdw.com