DFRWS

DIGITAL FORENSIC RESEARCH CONFERENCE

USA 2023

# Ransomware Simulations

Hands-on Case Studies

# Our Sponsors

# $ WHOAMI

## Ali Hadi

- Associate Professor and Program Director, Computer and Digital Forensics, Champlain College
- Research Director, Leahy Center for Digital Forensics and Cybersecurity
- Co-Founder and CTO, Cyber 5W, Digital forensics Training & Consulting

@binaryz0ne

## Mariam Khader

- Assistant Professor, Computer and Digital Forensics, Champlain College
- Research Lead, Leahy Center for Digital Forensics and Cybersecurity

@maryst33d

# Workshop is Not!!!

- About reverse engineering ransomware
- About decrypting ransomed files
- How to catch threat actors (attribution)
- How to compromise networks

# Overview

- Ransomware
- Ransomware Attack Components
- Simulations
- TARIQ & RansomCare
- Detection Techniques & Recommendations

# What is Ransomware?

Ransomware (ransom software) is a type of malware that restricts access to data or a system

## Cryptographic Ransomware

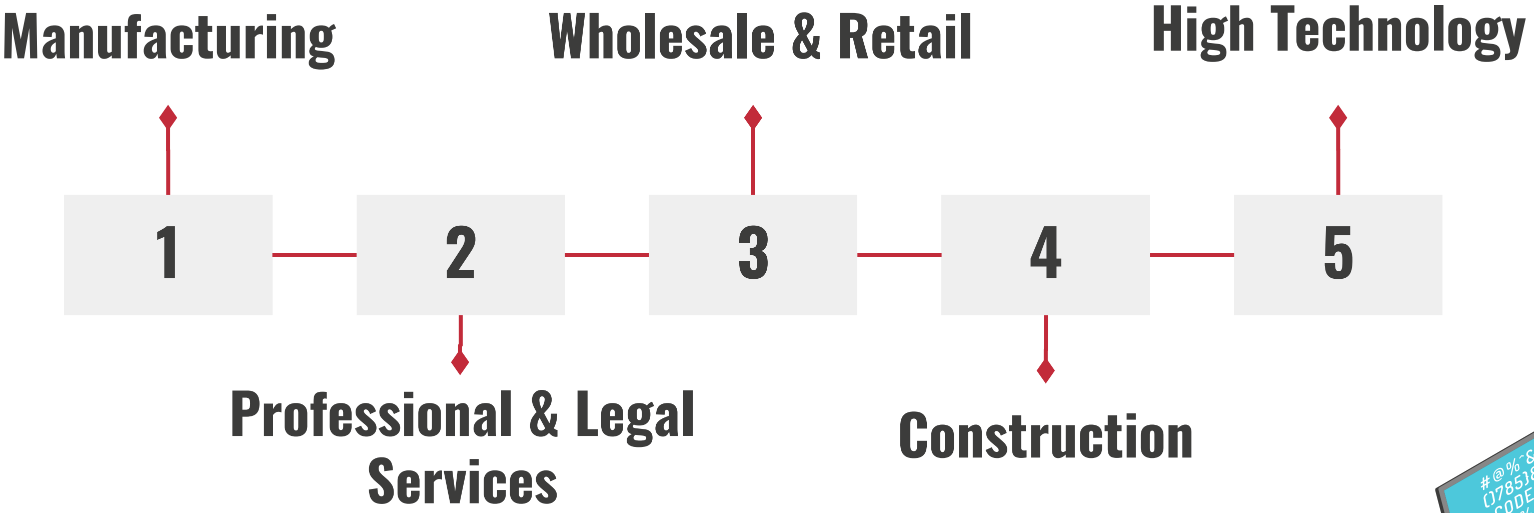
Encrypts the victim files

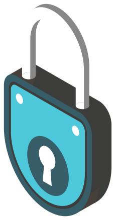
## Locker Ransomware

Prevents victims from accessing their systems

Both types of ransomware require a ransom to be paid in order to unlock the files or regain access to the system

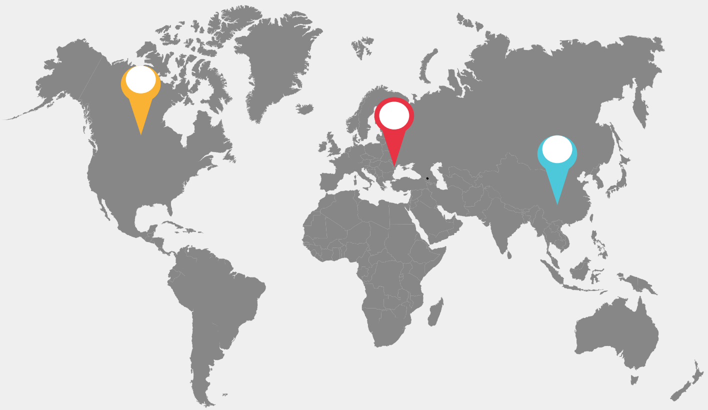
# Ransomware Stats by Industry



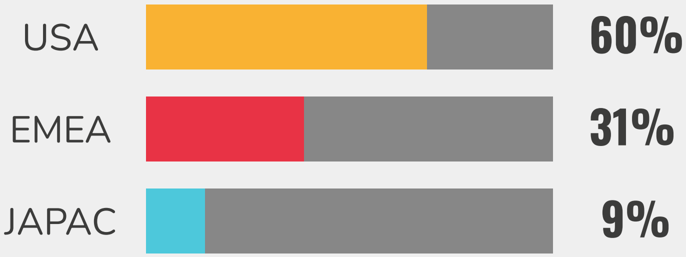


# Demographics Stats

## LOCATION



## %



## Regions

USA

EMEA

JAPAC

# 1.7 M

1.7 million ransomware attacks every day which means every second 19 ransomware attacks

# Ransomware Attacks

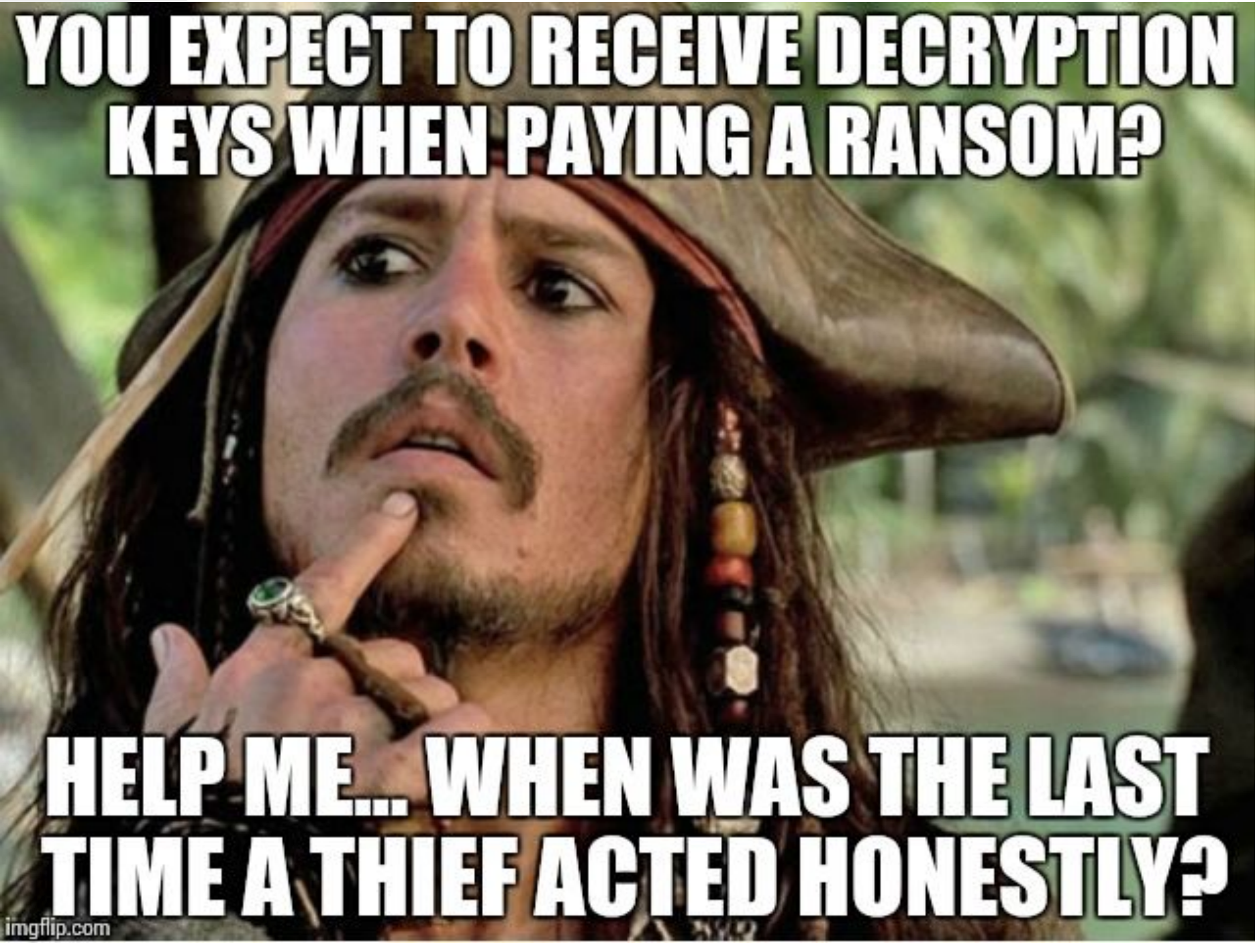
| | |
|---|---|
| 90% | Impacted ability to operate |
| 86% | Lose revenue or business |
| 97% | Infected backup repositories |

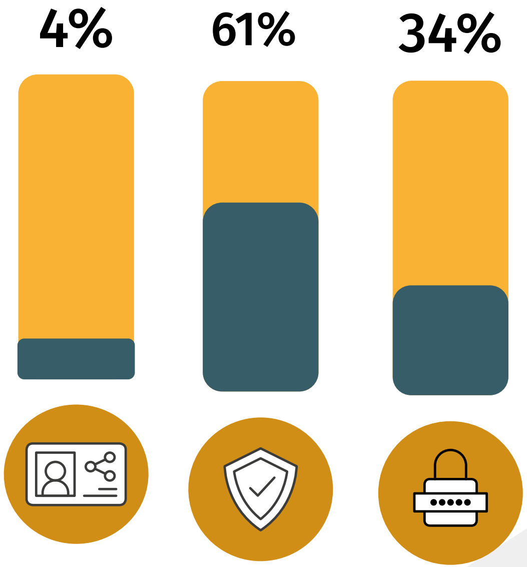
# Ransomware Payment Stats

## Payments

- Ransom demands range from $3,000 to $50M
- Ransom payments range from $3,000 to $7M
- The median demand was **$650,000**, while the median ransom payment was **$350,000**, this means a 46% decrease from the original median ransom demand

The State of Ransomware 2022


YOU EXPECT TO RECEIVE DECRYPTION KEYS WHEN PAYING A RANSOM?
HELP ME... WHEN WAS THE LAST TIME A THIEF ACTED HONESTLY?
imgflip.com


4%
61%
34%

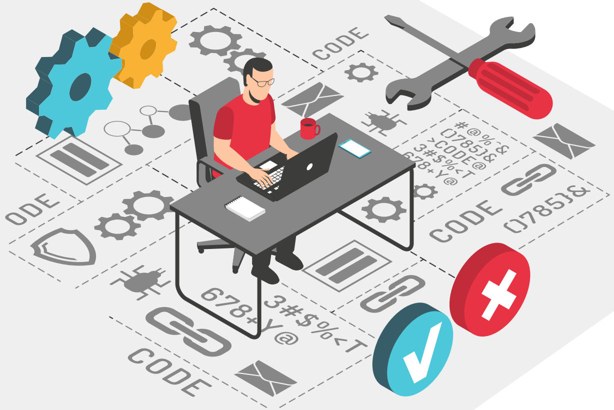
# Ransomware Groups

| year/ Group Name | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| **2021** | Conti | REvil | BlackCat | AvosLocker | Hive |
| **2022** | Black Basta | Hive | Conti | Lazarus | LockBit |
| **2023** | LockBit | Vice Society | BlackCat | Clop | Royal |

# Ransomware Malicious Behavior

| Encryption | Locking | Data Exfiltration |
|---|---|---|
| Symmetric, Asymmetric, & Hybrid | Screen, Browser, MBR | Steal Victim’s Valuable Information |

# Ransomware Types based on Target

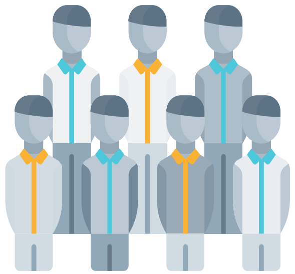


## Platforms

Ransomware targets PCs, Workstations, Mobile Devices, and IoT/CPS Devices

## Victims

Examining the characteristics of end-users and organizations that are targeted by ransomware can help in the design of effective protective measures



# Ransomware Types based on Payment Method

01

Premium-rate Text Messages

02

Pre-paid Vouchers

03

Cryptocurrencies

SO I JUST HAVE TO PAY YOU HALF A
BITCOIN TO UNLOCK MY COMPUTER?
imgflip.com

Does payment guarantee recovery?

# Ransomware Attack Components

Strong Encryption Techniques

Worm-like Capabilities

Pseudo-Anonymous Payment Methods

Ransomware as a Service (RaaS)

# Ransomware Attack Components - Cont.

## Use Shortcuts

Using an Initial Access Broker (IAB)

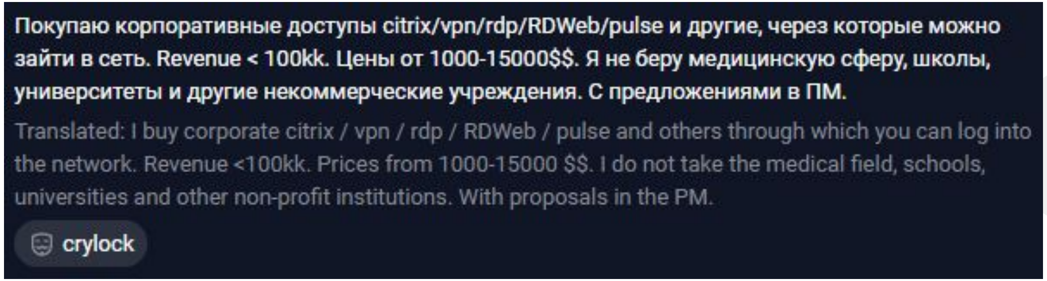
## Use Any Tricks that work

Using Anonymized Services (ex: ToR)

## Innovative

Create new variants to widen the scope of possible victims

Ransomware operators looking for IAB

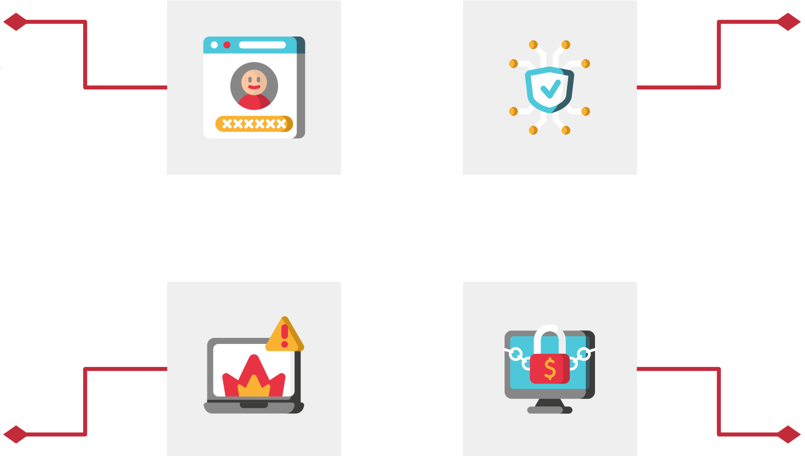


Покупаю корпоративные доступы citrix/vpn/rdp/RDWeb/pulse и другие, через которые можно зайти в сеть. Revenue < 100kk. Цены от 1000-15000$$. Я не беру медицинскую сферу, школы, университеты и другие некоммерческие учреждения. С предложениями в ПМ.

Translated: I buy corporate citrix / vpn / rdp / RDWeb / pulse and others through which you can log into the network. Revenue <100kk. Prices from 1000-15000 $$. I do not take the medical field, schools, universities and other non-profit institutions. With proposals in the PM.

crylock

# Attack Phases of Ransomware



## Infection (Initial Access)

Ransomware is delivered to the victim system

## Communication with C2

Exchange of crucial information, such as encryption keys and target system info

## Discovery & Destruction

Actual attack, encryption or locking the system

## Extortion

Ransom note explaining the payment instructions

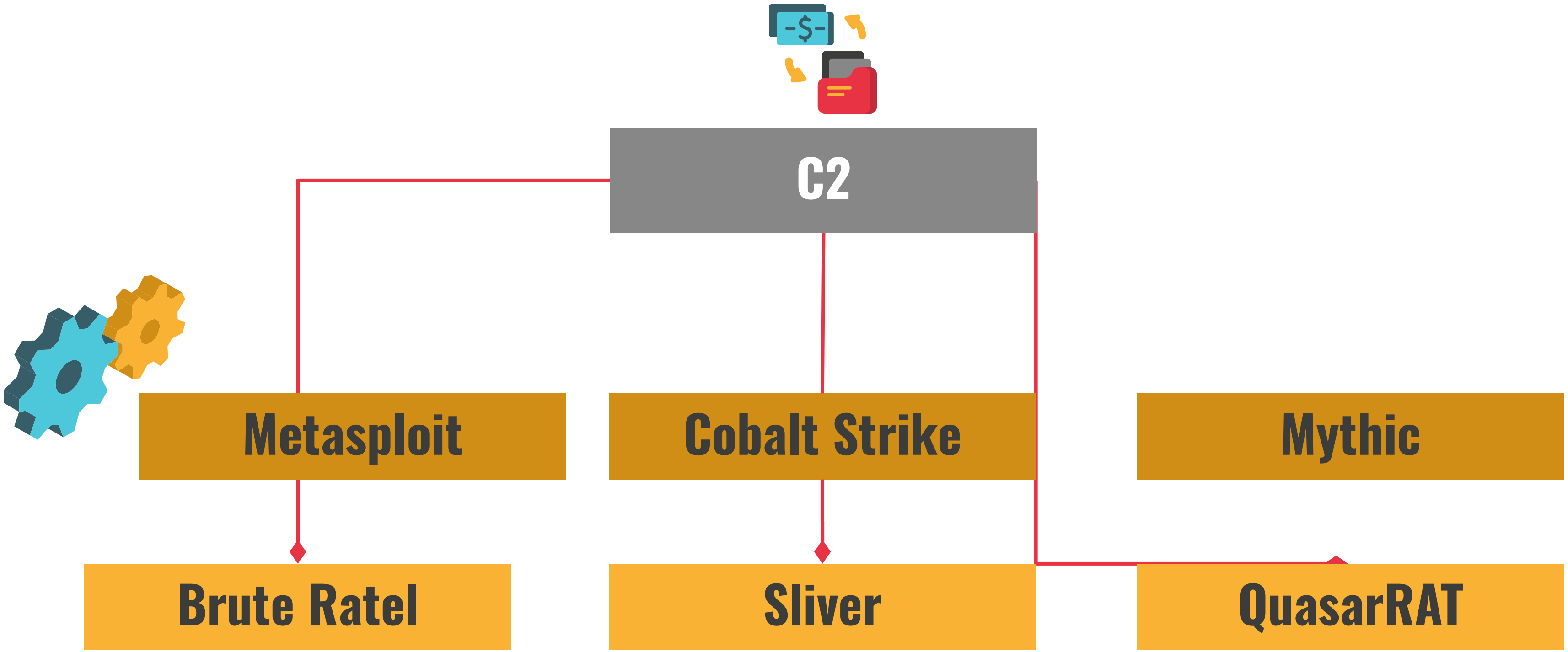
# Initial Access Methods

- Malicious Emails, SMS, & IMs (Phishing)
- Container & Compressed Files (ISO, VHD & ZIP, RAR)
- Search engine optimization (SEO) Poisoning
- Drive-by-Download (e.g. Malvertising)
- Remote Administration (e.g. RDP, RMM, etc)
- Malicious Macros
- Windows LNKs & MSI files
- Downloaders, Droppers, Stagers
- Malicious Applications
- Vulnerabilities

# Ransomware - Stagers

1. Qbot
2. Impacket
3. Gootloader
4. SocGolish
5. Mimikatz
6. Raspberry Robin
7. Cobalt Strike
8. BloodHound

# Communication with C2



C2

Metasploit

Cobalt Strike

Mythic

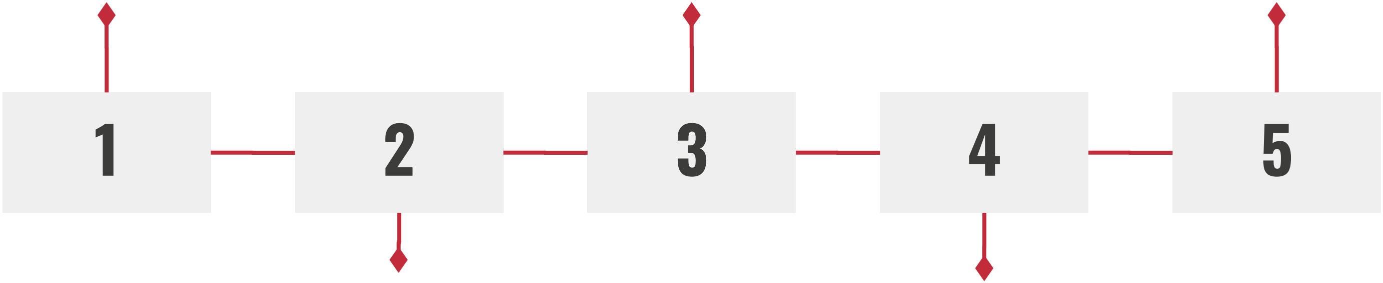
Brute Ratel

Sliver

QuasarRAT

https://www.thec2matrix.com/matrix

# Discovery & Destruction



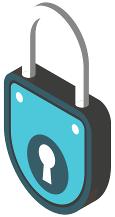
1. Enumeration of files

2. Discover existing drives, removable media, shared drives and shares

3. Delete File and Directories

4. Deletes existing backups to prevent recovery

5. Delete Volume Shadow Copies (VSC)



# Lateral Movement

Exploitation of Remote Services

Internal Spearphishing

Lateral Tool Transfer

Taint Shared Content

Remote Service Session Hijacking

Remote Services

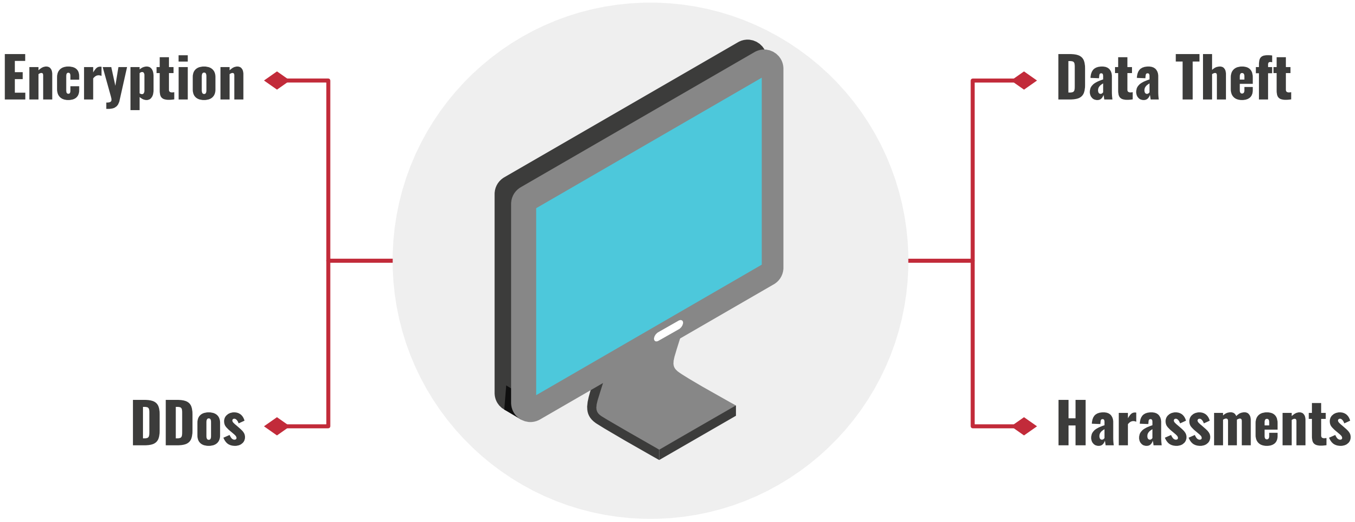
Replication Through Removable Media

Software Deployment Tools

Use Alternate Authentication Material

Why Are Backups No Longer Sufficient?

# Multi-Extortion Techniques



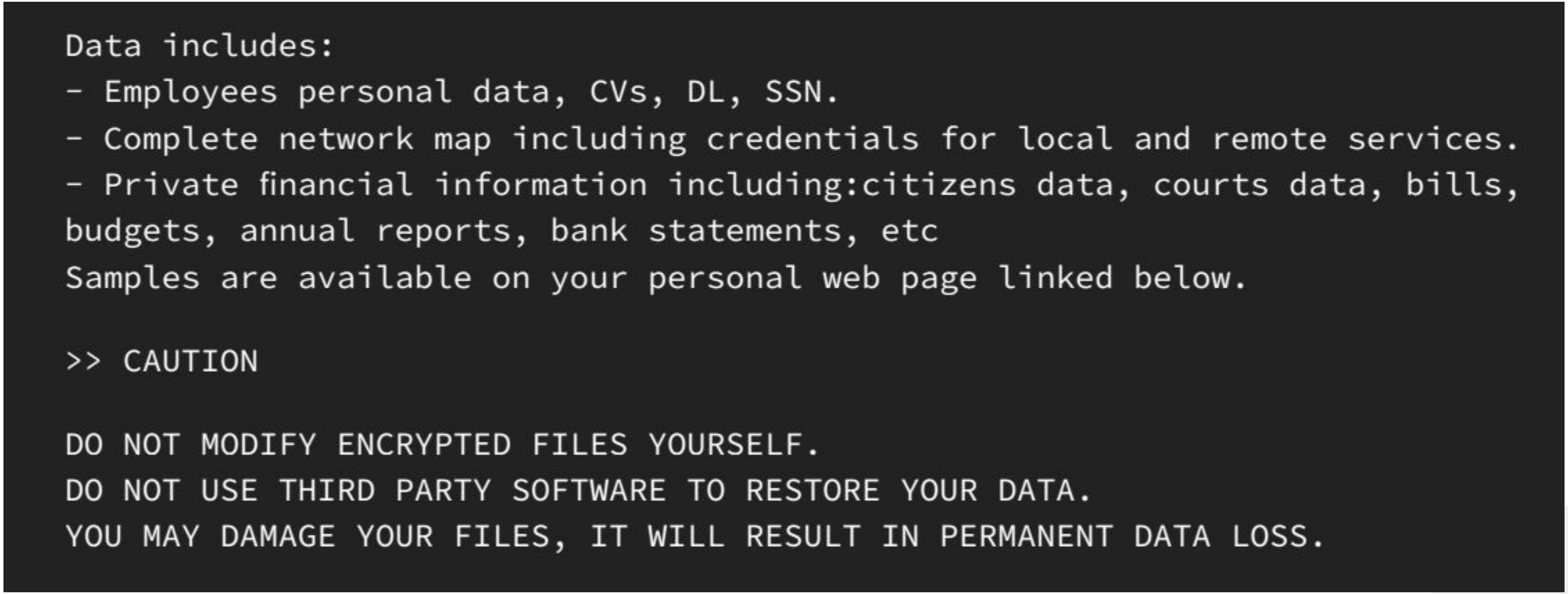
Encryption

DDos

Data Theft

Harassments

# Ransomware Notes



```
Data includes:
- Employees personal data, CVs, DL, SSN.
- Complete network map including credentials for local and remote services.
- Private financial information including:citizens data, courts data, bills,
budgets, annual reports, bank statements, etc
Samples are available on your personal web page linked below.

>> CAUTION

DO NOT MODIFY ENCRYPTED FILES YOURSELF.
DO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.
YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.
```

*BlackCat ransom note*

# Simulations

# Breach and Attack Simulation (BAS)

Involves simulating potential threat activities (tactics, techniques, and procedures) in order to assess the effectiveness of security controls in a production environment.

This way, BAS can help companies find weaknesses in their security and take action to patch them up before any cybercriminals can take advantage of them.

*In other words, ASSESS YOUR SECURITY POSTURE!*

# Ransomware BAS

## Security Posture

Assess security posture of your network against ransomware TTPs

## Phishing

Evaluate your protection measures against ransomware when employees fall victim to SE attacks

## Rollback Capability

Undo the damage done to your environment after running the attack simulation

## Level of Understanding

Helps establishing best practices to optimize your organization's resistance to ransomware attacks

CYBER5W

# TARIQ

## Adversary Simulation Framework

# Why TARIQ ?

**Plugin-Engine**

→ Uses a plugin-engine technique to load and unload new plugins at run-time extending TARIQ’s capabilities

→ Easy to interface with off-the-shelf tools by using TARIQ’s wrapper (APIs)

→ Easy to maintain and update, since everything is a separate module

# TARIQ Simulation Capabilities - Engine

1

## Memory-based

→ Memory Based Load and Unload

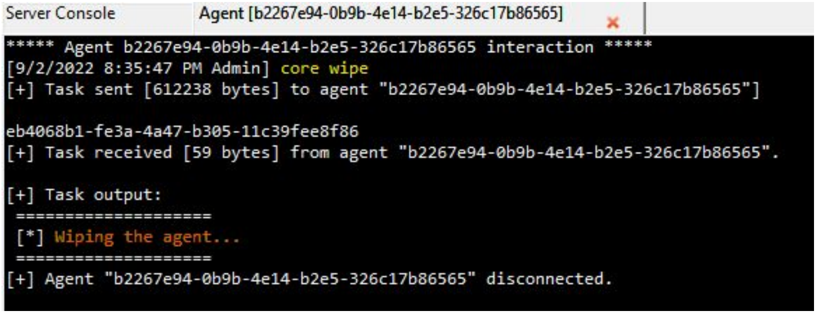
- Extend capabilities with new tools at runtime
- Wipe code from memory

2

## Core System Control

→ Interact with Target

- Retrieve victim information
- Upload/Download files
- Wipe Agent

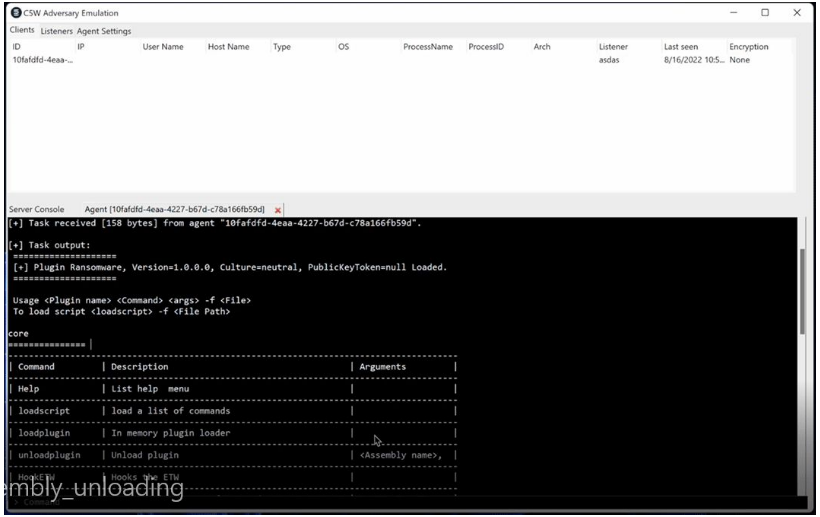


```
***** Agent b2267e94-0b9b-4e14-b2e5-326c17b86565 interaction *****
[9/2/2022 8:35:47 PM Admin] core wipe
[+] Task sent [612238 bytes] to agent "b2267e94-0b9b-4e14-b2e5-326c17b86565"]

eb4068b1-fe3a-4a47-b305-11c39fee8f86
[+] Task received [59 bytes] from agent "b2267e94-0b9b-4e14-b2e5-326c17b86565".

[+] Task output:
 ====================
 [*] Wiping the agent...
 ====================
[+] Agent "b2267e94-0b9b-4e14-b2e5-326c17b86565" disconnected.
```

# TARIQ Simulation Capabilities - Engine



| ID | IP | User Name | Host Name | Type | OS | ProcessName | ProcessID | Arch | Listener | Last seen | Encryption |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 10fafdfd-4eaa-... | | | | | | | | | asdas | 8/16/2022 10:5... | None |

```
[+] Task received [158 bytes] from agent "10fafdfd-4eaa-4227-b67d-c78a166fb59d".

[+] Task output:
 ====================
 [+] Plugin Ransomware, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null Loaded.
 ====================

 Usage <Plugin name> <Command> <args> -f <File>
 To load script <loadscript> -f <File Path>

core
=============== |
------------------------------------------------------------------------------------
| Command           | Description                                   | Arguments         |
------------------------------------------------------------------------------------
| Help              | List help  menu                               |                   |
------------------------------------------------------------------------------------
| loadscript        | load a list of commands                       |                   |
------------------------------------------------------------------------------------
| loadplugin        | In memory plugin loader                       |                   |
------------------------------------------------------------------------------------
| unloadplugin      | Unload plugin                                 | <Assembly name>,  |
------------------------------------------------------------------------------------
| HookETW           | Hooks the ETW                                 |                   |
------------------------------------------------------------------------------------
> Command
```

3

## Multi-Communication Channels

→TCP, HTTP, and DNS

4

## Multi-Crypto Methods

→ AES (128, 192, and 256),
Hybrid RSA + AES → (*Very soon*)

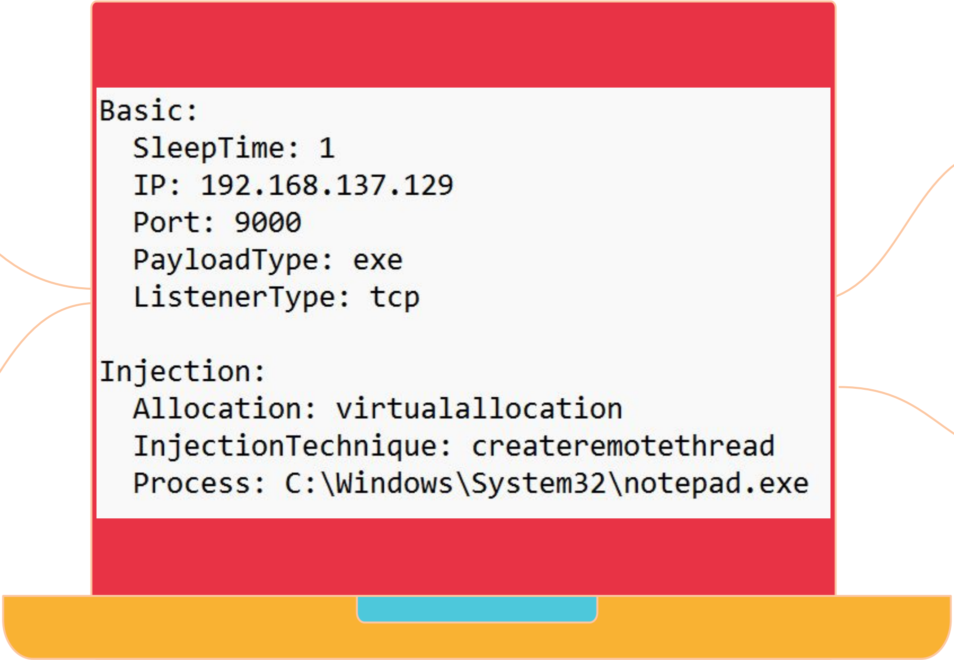
# 5 Malleable Tariq Profiles!!!

**Beaconing**

DNS & HTTP

**Custom HTTP Headers**

Server & Client



```
Basic:
  SleepTime: 1
  IP: 192.168.137.129
  Port: 9000
  PayloadType: exe
  ListenerType: tcp

Injection:
  Allocation: virtualallocation
  InjectionTechnique: createremotethread
  Process: C:\Windows\System32\notepad.exe
```

**Network Settings**

→ IP address
→ Port #
→ Type of Listener

**Misc**

→ Payload Type
→ Mutex

*Used to automate the agent's behaviour*

# TARIQ Simulation Capabilities - Engine

## Miscellaneous

6

→ Custom Loader

→ PPID Spoofing

- Capability of faking the parent process

→ ETW Hooking

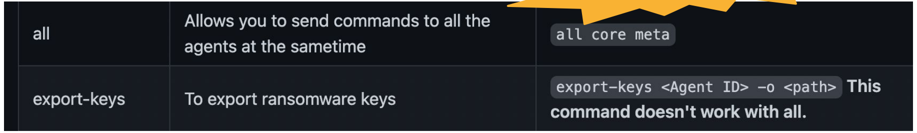
→ Create TCP or SMB Pivots

→ Mass execution

- Capability of sending instructions to all targets

→ Python Automation
(*beta phase*)

Mass Execution



| | | |
|---|---|---|
| all | Allows you to send commands to all the agents at the sametime | `all core meta` |
| export-keys | To export ransomware keys | `export-keys <Agent ID> -o <path>` This command doesn't work with all. |

# TARIQ Building Blocks - Plugins

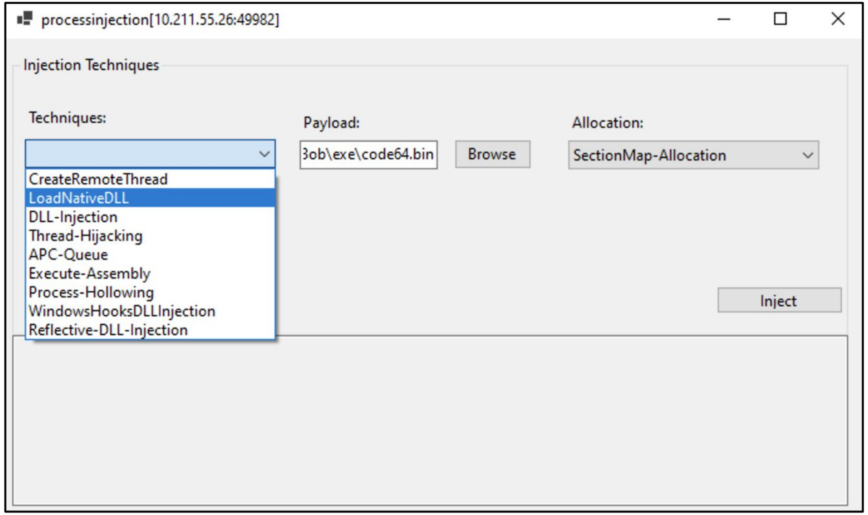
- SemiCore
  - Cmd functionality: cd, mkdir, ls, rmdir, pwd
  - Process: shell, ps, pskill, listmodules
- Persistence
  - SharPersist
- System Security Check
  - Seatbelt

- PowerShell
  - run → run PowerShell scripts
  - runcmd → run PowerShell cmd
  - wipelogs → wipe Windows Events
- Add your own!

# Process Injection - Plugin

## Multi-Injection Techniques

1. Thread Hijacking
2. APC Queue Code Injection
3. CreateRemoteThread Injection
4. DLL Injection
5. .NET Injection
6. Process Hollowing
7. Running Native DLL
8. Windows Hooks DLL Injection
9. Reflective DLL Injection
10. Shellcode Reflective DLL Injection (sRDI)



processinjection[10.211.55.26:49982]

Injection Techniques

Techniques:

Payload: 3ob\exe\code64.bin

Allocation: SectionMap-Allocation

# Why RansomCare ?...

Is a ransomware simulation plugin for our Adversary Simulation Framework...

## FILELESS

| | | |
|---|---|---|
| **Encryption / Decryption** | $ File and Directories<br>$ Targeted File Extensions | $ Send/Receive Keys<br>$ Whitelist File Extensions |
| **Inhibit System Recovery** | $ Delete Volume Shadow Copies<br>$ Delete File and Directories | $ Locate System Shares<br>$ Delete File History |
| **Miscellaneous** | $ Memory Based (process injection)<br>$ Custom Ransom Wallpaper | $ Custom Ransom Notes<br>$ Custom File Extensions |
| **Anti-X Techniques** | $ Hook the Event Tracing for Windows<br>$ Wipe Ransomware | |

# Blunders In Simulators - Thanks Unit42!

### #1 - Encrypting the files you dropped

RansomCare is an in-memory loaded module

### #2 Dropping known extensions

RansomCare provides custom file extensions

### #3 - Not deleting backups

SemiCore & PowerShell Plugins provide extra search and delete capabilities

### #4 - Context is everything

Full encryption/decryption is available to simulate the full encryption life-cycle of a ransomware

# Blunders In Simulators - Thanks Unit42!

### #5 - No command and control

RansomCare comes with a fully encrypted C2 channel

### #6 - No remote encryption and shared drives

SemiCore provides shell access, plus you can upload a new plugin to achieve that

### #7 - Only remote encryption and shared drives

SemiCore provides shell access, plus you can upload a new plugin to achieve that

### #8 - Using real ransomware, but not executing it

Helps establishing best practices to optimize your organization's resistance to ransomware attacks

# TARIQ Capabilities - MITRE

- Execution
  - PowerShell
  - Windows Command Shell
- Process Injection
- Inhibit System Recovery
  - VSS, Wiping, Shutdown/Reboot
- File and Directory Discovery
- Exfiltration
- Command and Control (C2)
- Persistence
  - SharPersist

- Ransomware
  - Data Destruction
  - Data Encrypted for Impact
  - Defacement: Internal Defacement
    - Drop note
    - Change wallpaper
- System Security Check
  - Seatbelt
- Impair Defenses
  - Indicator Blocking
  - Disable Windows Event Logging

# Simulations

## Ransomware Simulation Case Studies

# Case Study #1

| | |
|---|---|
| Testable requirement | System Logging,  Corruption Testing, and Backup Capability |
| Description | Simulating the execution of a weak ransomware. |
| Preconditions | User downloaded and ran an executable from the internet that is ransomware.<br>Note: you can use any IA method to achieve this condition. |
| Procedure | 1. Start Tariq<br>2. Generate agent<br>3. Deploy agent on target system<br>4. Upload & start ransomware plugin<br>5. Delete Volume Shadow Copies<br>6. Encrypt files<br>7. Upload Note and Wallpaper<br>8. Unload/Remove Plugin<br>9. Wipe agent |
| Expected Results (pass) | User files gets encrypted and volume shadow copies are deleted. |
| Actual Results Details of the event were understood and the moment of last | User files were copied before being encrypted so recovery is possible. Also, only volume shadow copies were deleted and not other types of backups. |
| Overall Result | Ransomware Failed to succeed in its mission. |

# Case #1 Techniques

## Process Injection

## Destruction

Deleting Volume Shadow Copies

## Encryption

Encrypting Files

## Extortion

Leaving note and changing the wallpaper

# Case Study #2

| | |
|---|---|
| Testable requirement | System Logging, Corruption Testing, and Backup Capability |
| Description | Simulating the execution of a ransomware with a special file extension and is capable of deleting volume shadow copies. |
| Preconditions | User downloaded and ran an executable from the internet that is ransomware. The user’s files are then encrypted by the ransomware |
| Procedure | 1. Start Tariq<br>2. Generate agent<br>3. Deploy agent on target system<br>4. Upload & start ransomware plugin<br>5. Change extension<br>6. Delete Volume Shadow Copies<br>7. Encrypt files<br>8. Upload Note and Wallpaper<br>9. Unload/Remove Plugin<br>10. Wipe agent |
| Expected Results (pass) | User files gets encrypted with custom file extension and volume shadows deleted |
| Actual Results Details of the event were understood and the moment of last | User files were encrypted properly so recovery is not possible. Files now have a unique file extension and volume shadow copies are deleted. |
| Overall Result | Ransomware was partially successful in its mission. |

# Case #2 Techniques

## Process Injection

## Destruction

Deleting Volume Shadow Copies

## Encryption

Encrypting Files & Change Extension

## Extortion

Leaving note and changing the wallpaper

# Case Study #3

| | |
|---|---|
| Testable requirement | System Logging,  Corruption Testing, and Backup Capability |
| Description | Simulating the execution of a ransomware with a special file extension and targets certain files. The ransomware is also capable of deleting volume shadow copies, plus file history. |
| Preconditions | User downloaded and ran an executable from the internet that is ransomware. The user's files are then encrypted by the ransomware |
| Procedure | 1. Start Tariq<br>2. Generate agent<br>3. Deploy agent on target system<br>4. Upload and Start ransomware<br>5. Change extension<br>6. Target certain files<br>7. Delete Volume Shadow Copies<br>8. Delete file history<br>9. Encrypt files<br>10. Upload Note and Wallpaper<br>11. Unload/Remove Plugin<br>12. Wipe agent |
| Expected Results (pass) | User files gets encrypted and backups deleted |
| Actual Results Details of the event were understood and the moment of last | Certain user files were encrypted properly so recovery is not possible. Encrypted files show up with a unique file extension. Both volume shadow copies and file history are deleted. |
| Overall Result | Ransomware was successful in its mission. |

# Case #3 Techniques

## Process Injection

## Destruction

Deleting Volume Shadow Copies
Delete File History

## Encryption

Encrypting Files

## Extortion

Leaving note and changing the wallpaper

Attack Simulation

# Thanks to …

## Shady Shaheen

- ★ Software Developer at Cyber 5W
  - ○ Main developer behind TARIQ
- ★ Interests: C2 Development and Malware Analysis
- ★ @Th3Hunger_

Windows Credentials
user1 / Passw0rd!

# Workshop Time

Please use the following credentials:

https://192.168.1.80
https://192.168.1.90

Check your cards for user access

😃

# Thank You For Attending!

## Any questions?

send them our way
Info [at] advemu [dot] com

# Credits & References...

Special thanks to all the people who made and released these awesome resources for free:

- Presentation template by SlidesGo
- Adam, Ideas and Blue Team Fingers, @Hexacorn
- Florian Roth, Sigma Rules and others, @cyb3rops
- Velociraptor, hayabusa, chainsaw, NirSoft, etc
- MITRE Framework, https://attack.mitre.org/techniques/
- Sorry if we missed someone!