



FROM RDP TO D&D: UNPARALLELED REMOTE DESKTOP MONITORING REVEAL ATTACKERS' TRADECRAFT

Olivier Bilodeau, GoSecure

THIS RESEARCH IS POSSIBLE WITHOUT

Andréanne Bergeron

- Ph.D in Criminology, **Université de Montréal**
- Cybersecurity Researcher, **GoSecure**
- Co-VP Engagement and Outreach,
NorthSec
- Scientific Director, **Open-Source Research Group**



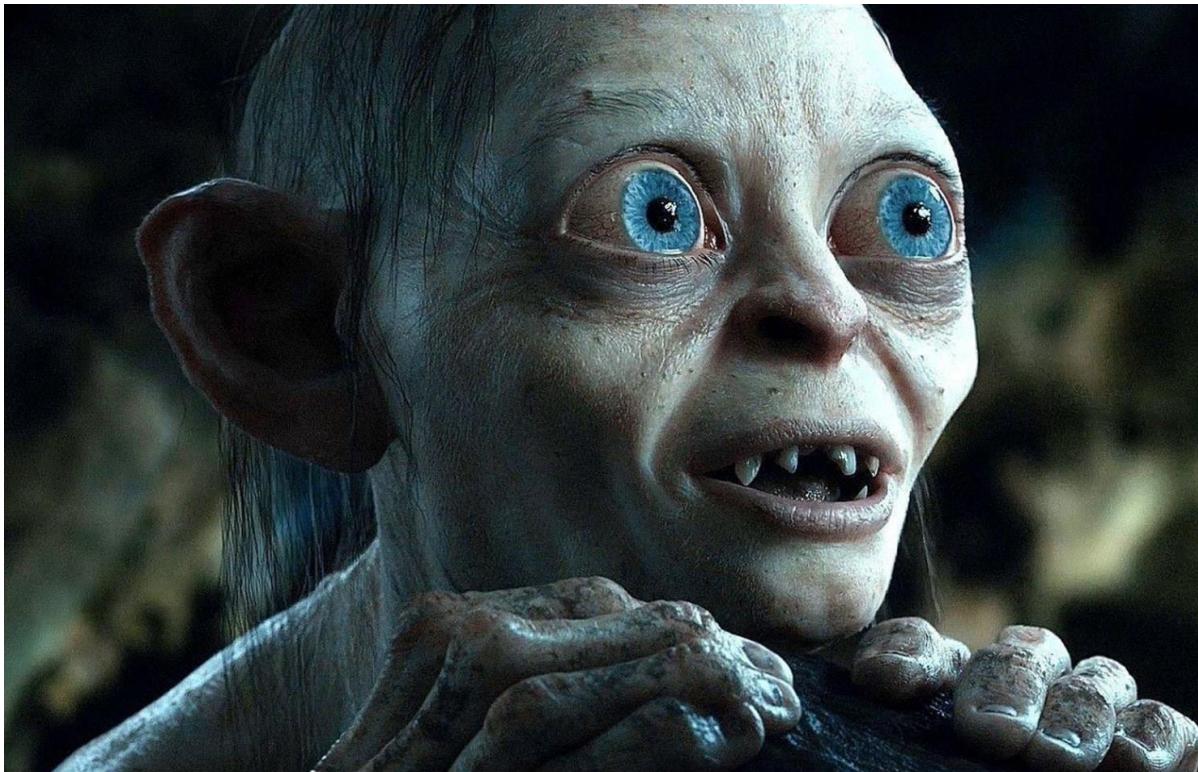
THIS RESEARCH IS POSSIBLE WITHOUT

Andréanne Bergeron

- Ph.D in Criminology, **Université de Montréal**
- Cybersecurity Researcher, **GoSecure**
- Co-VP Engagement and Outreach,
NorthSec
- Scientific Director, **Open-Source Research Group**



WHO AM I



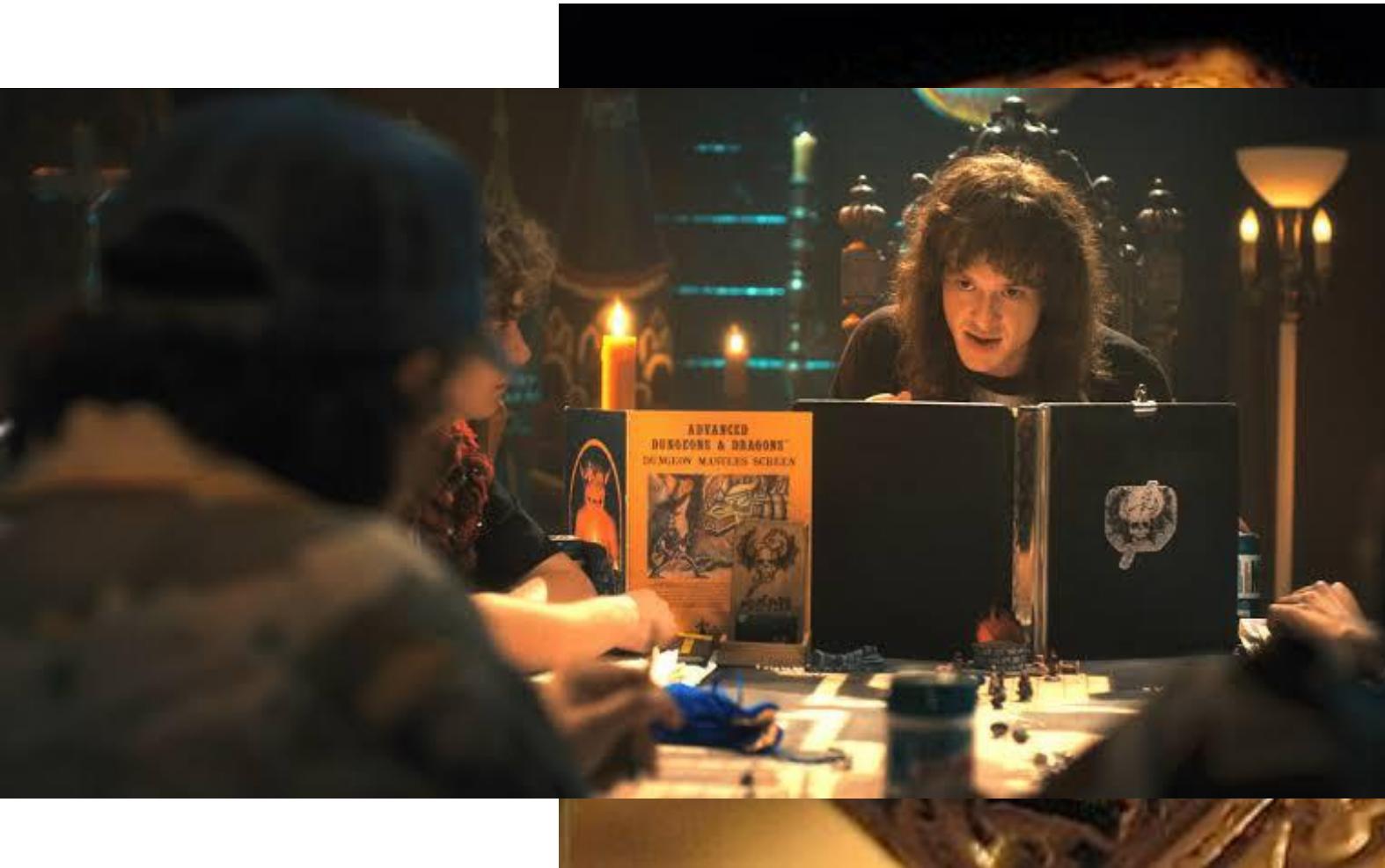
Olivier Bilodeau

- Cybersecurity Research Director, **GoSecure**
- President, **NorthSec**
 - Training sessions, Conference and CTF in Montréal
- Co-founder of **MontréHack**
 - Applied Security Workshops
- Enthusiastic Serial Speaker



DISCLAIMER: DUNGEONS AND DRAGONS NERDINESS

GOSECURE



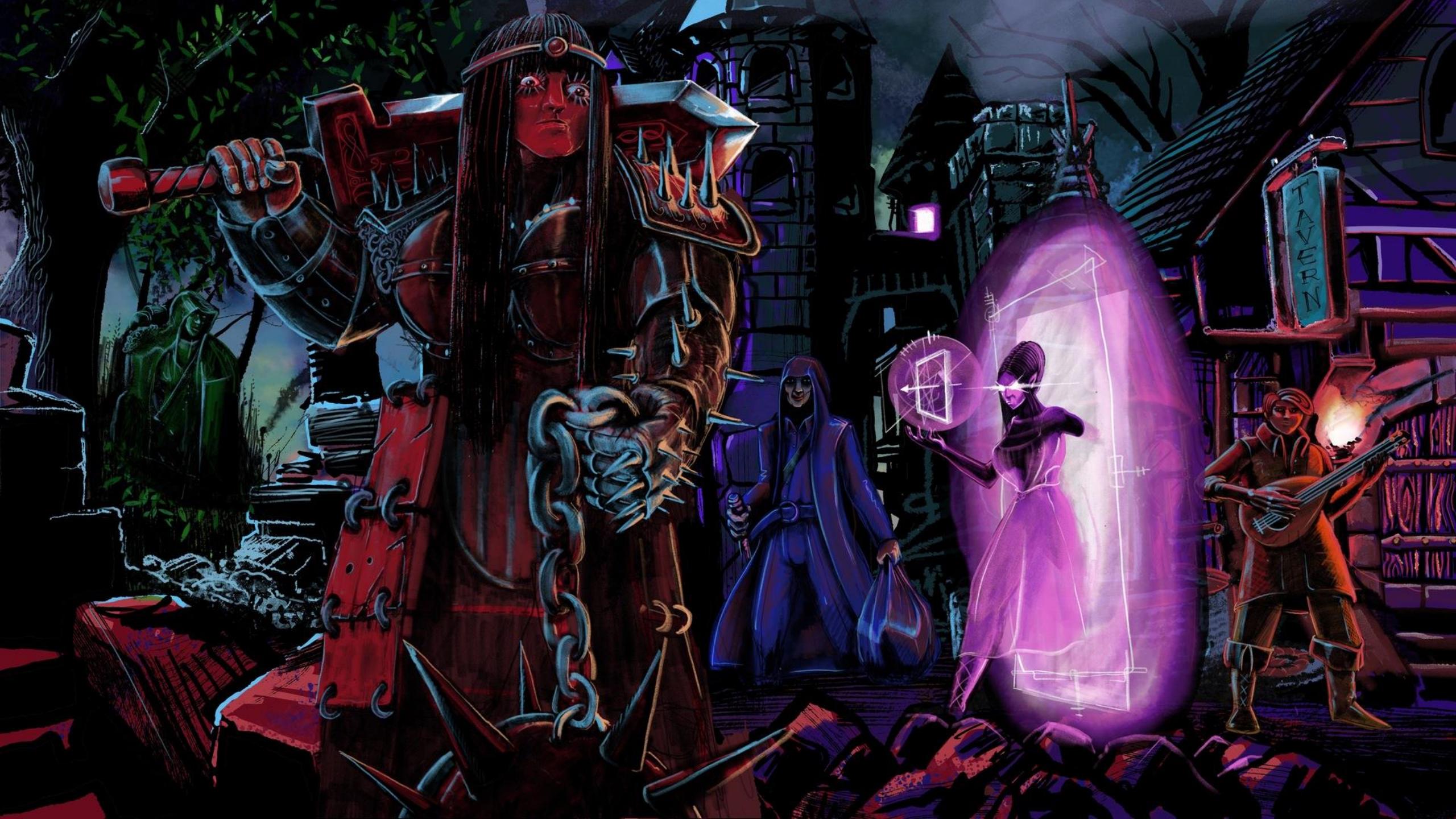


THE QUEST

THE QUEST (AGENDA)

- RDP Interception Explained
- 5 Attacker Classes
 - 190+ million events
- The Arsenal They Use
- Some Memorable Session Highlights



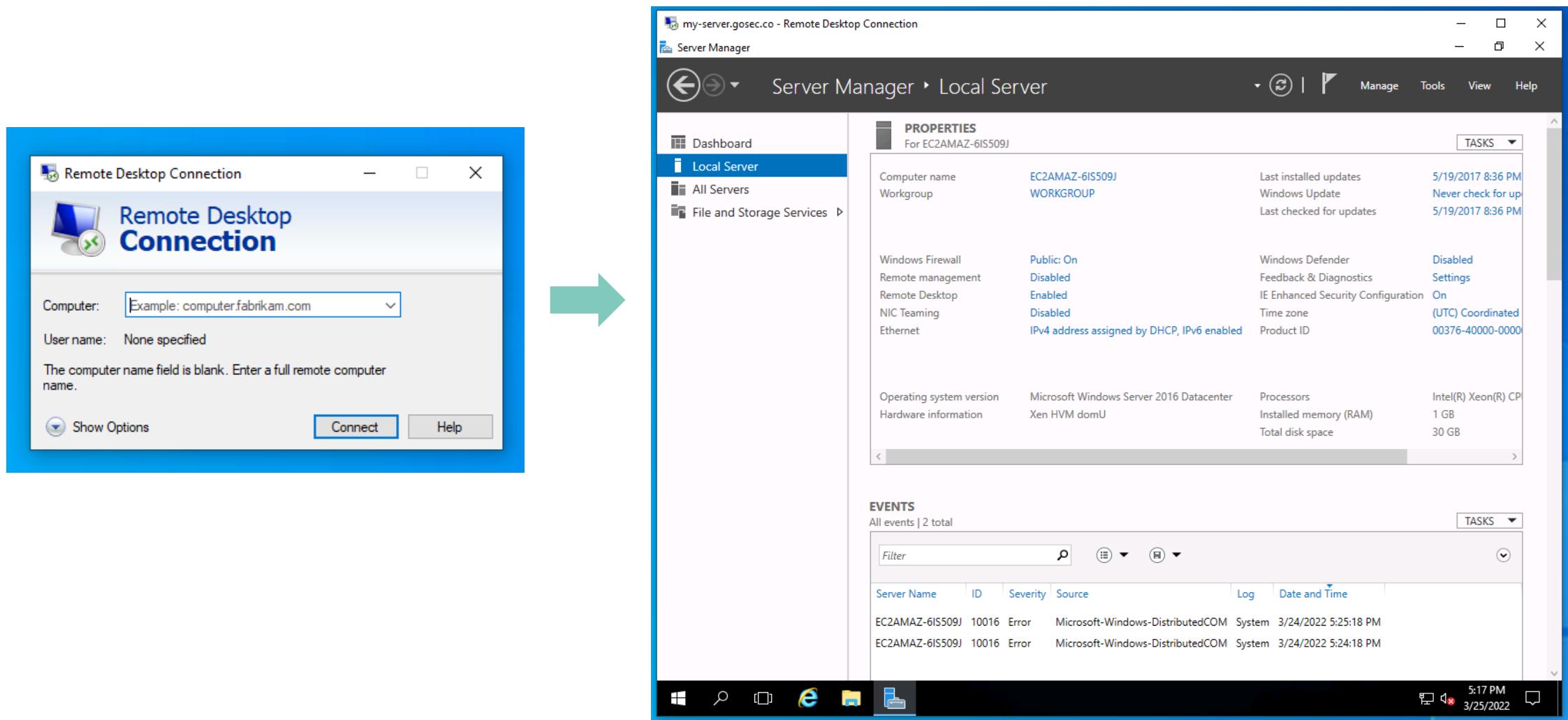


TODAY'S GAME

- RDP is targeted
- Telnet/SSH honeypots are attacked by bots
- Let's Leverage Unparalleled RDP Capture Depth



REMOTE DESKTOP PROTOCOL



PYRDP: TOOL CHARACTERISTICS

4 years in development

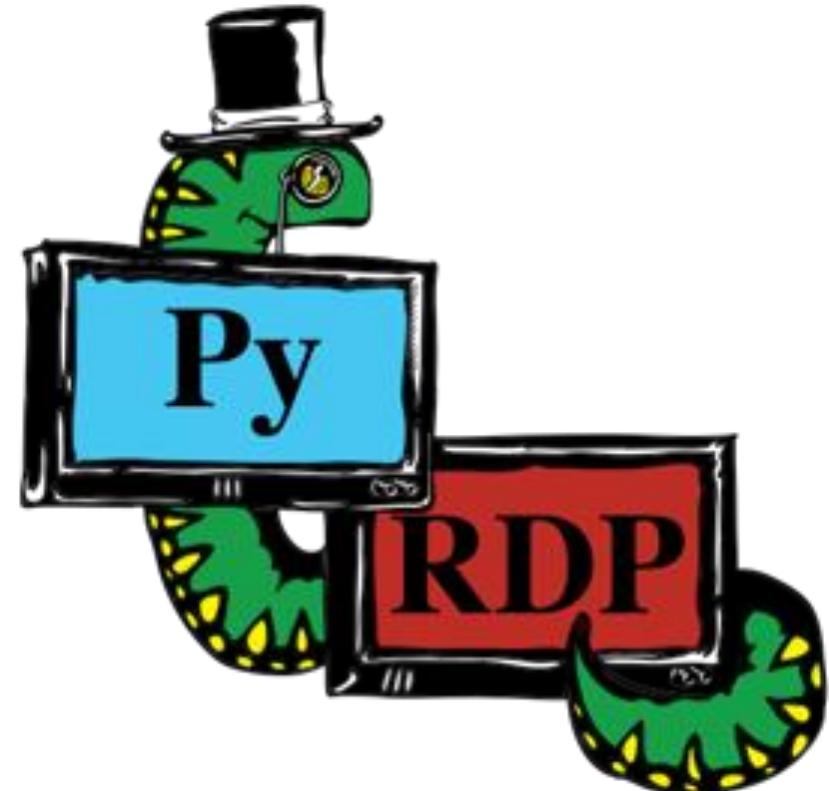
RDP Monster-in-the-Middle (MITM)



RDP Interception

Records Everything

RDP Tampering Engine



RDP Player

Real-time viewing and takeover

Replay of previous captures

THE PYRDP CRYSTAL BALL



Speed: 1x

Scale to window

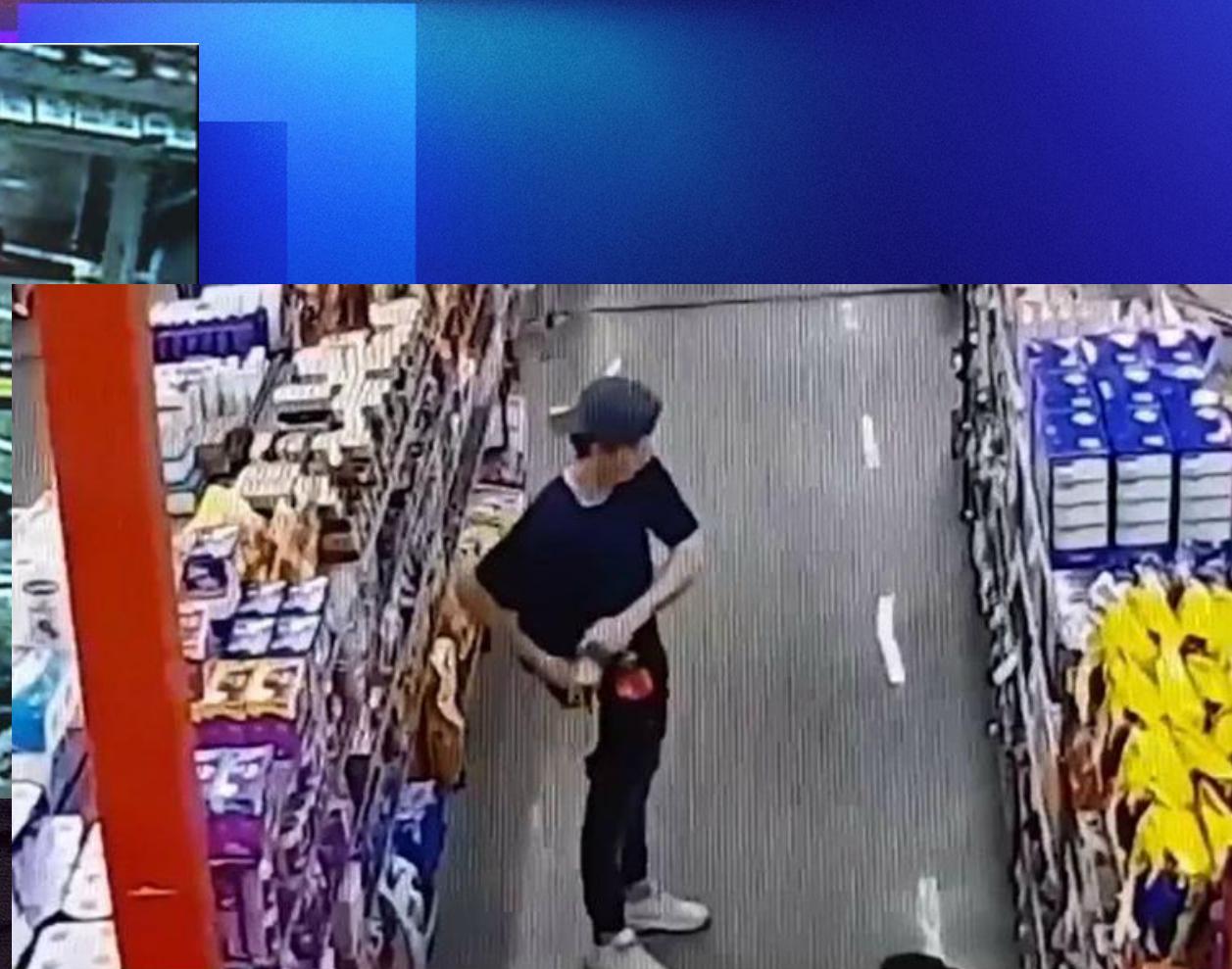
Play



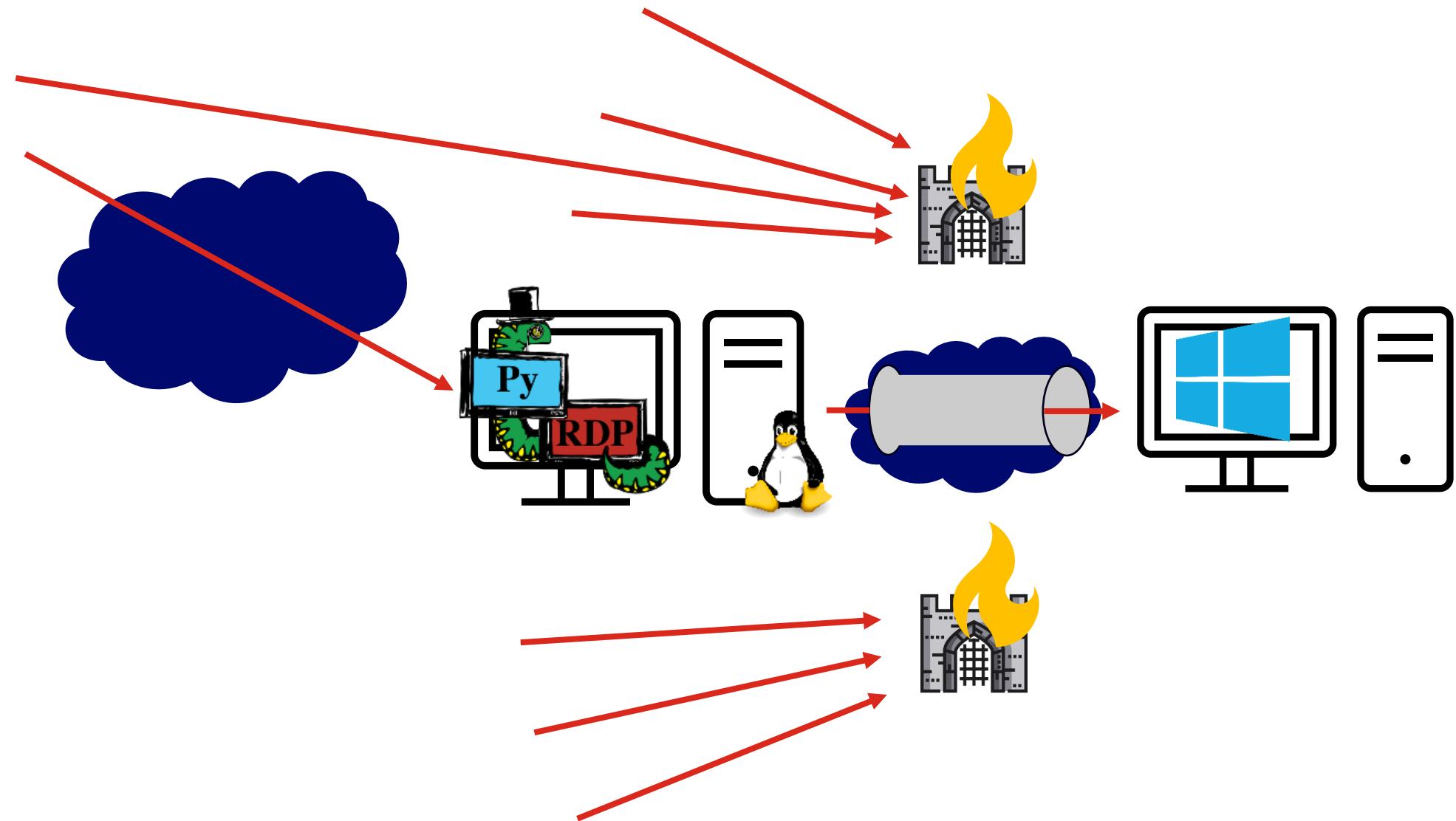
HOST: HOMER

USERNAME: administrator
PASSWORD: admin
DOMAIN:

Basically, surveillance cameras for Windows Systems



RDP HONEYPUFF WITH PYRDP



PYRDP: LEARN MORE

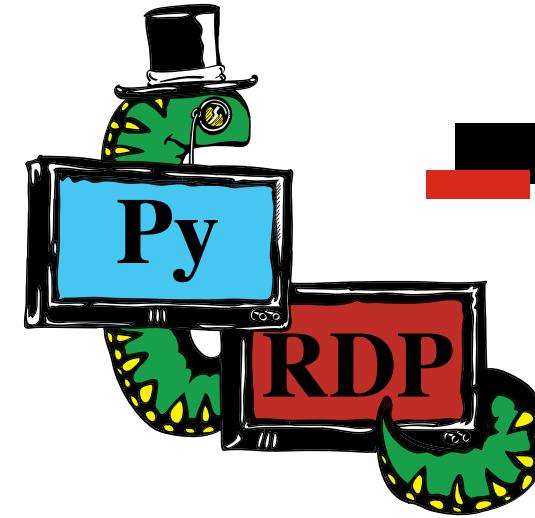


Source Code / Documentation

- <https://github.com/GoSecure/pyrdp>
- [PyRDP ReadMe](#)
- [PyRDP Transparent Proxying Guide](#)
- [Windows RDP Certificate Extraction](#)
- [RDP Connection Sequence](#)
- [RDP Basic Protocol Specification](#)

Past Presentations & Blogs

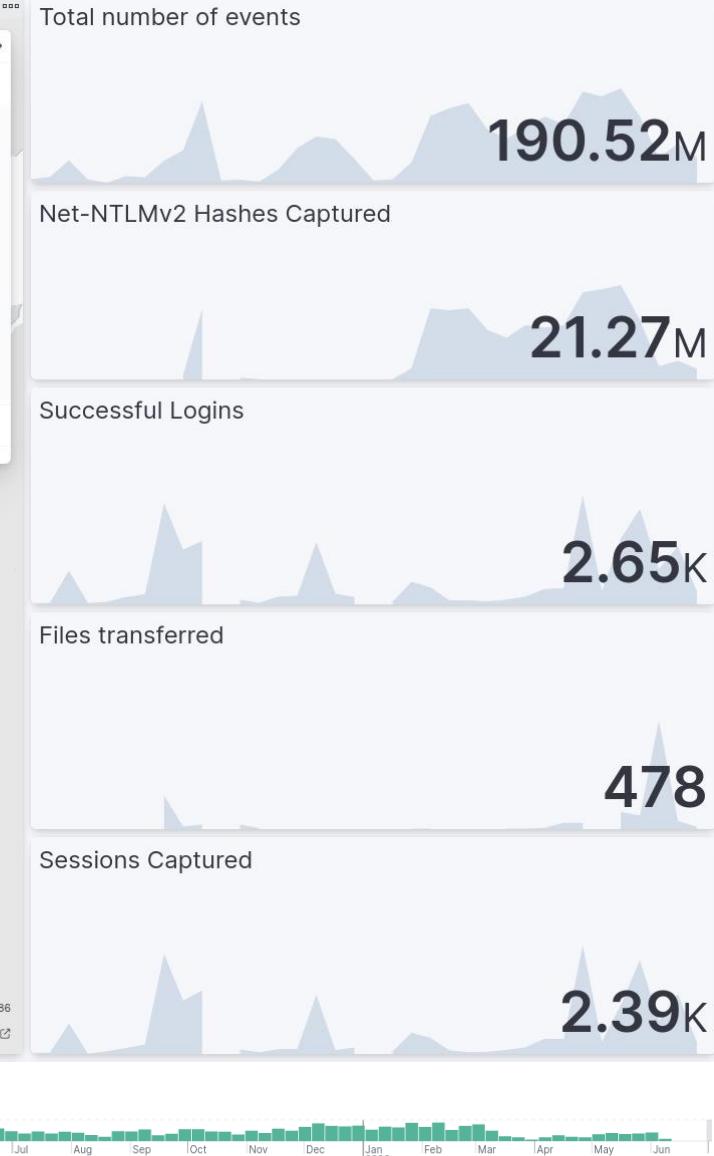
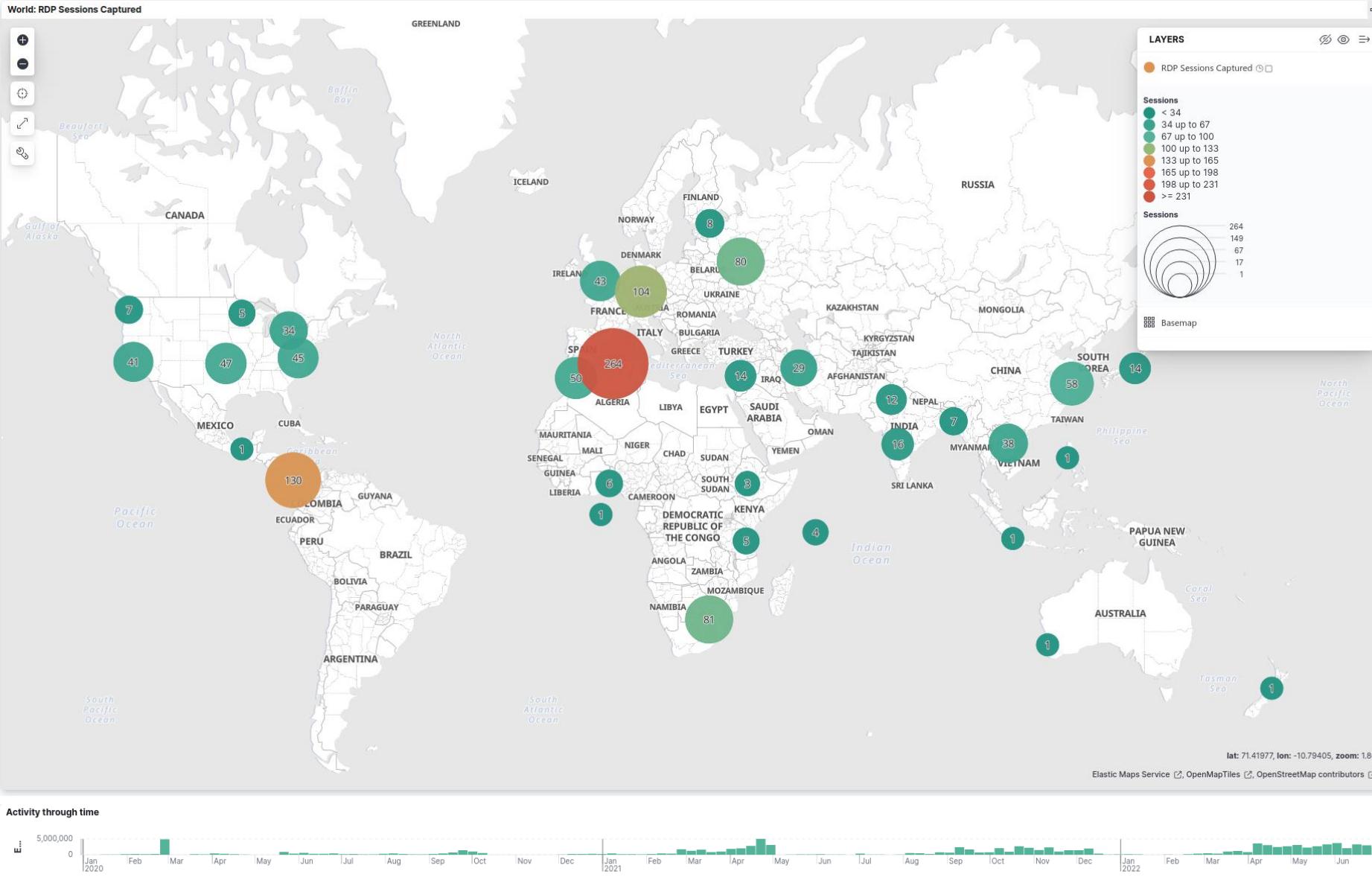
- [Introduction Blog Post](#)
- [NorthSec 2019 Talk](#)
- [BlackHat Arsenal 2019](#)
- [Blog: PyRDP on Autopilot](#)
- [DerbyCon 2019 \(Video\)](#)
- [DEFCON 28 Demo Labs](#)
- [Blog: Announcing PyRDP 1.0](#)
- [1.0 released at SecTor 2020](#)
- [BlackHat Arsenal 2021](#)
- [Purple RDP: Red and Blue Tradecraft](#)
- [Blog: 1.2 release "Rudolph Desktop Protocol"](#)





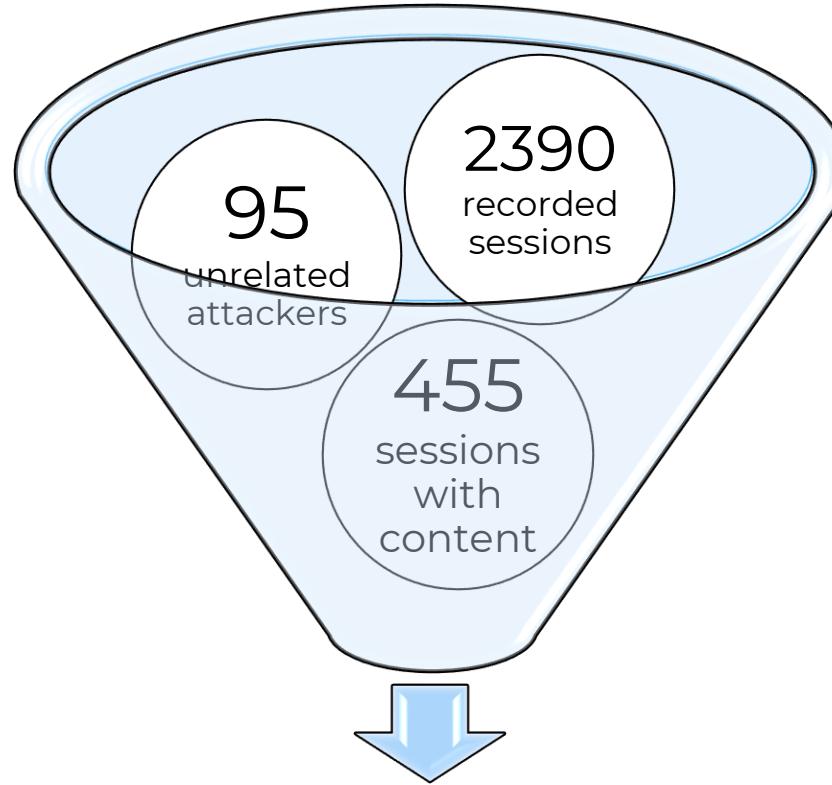
WELCOME TO THE
DUNGEON,
ADVENTURERS

COLLECTED INTELLIGENCE



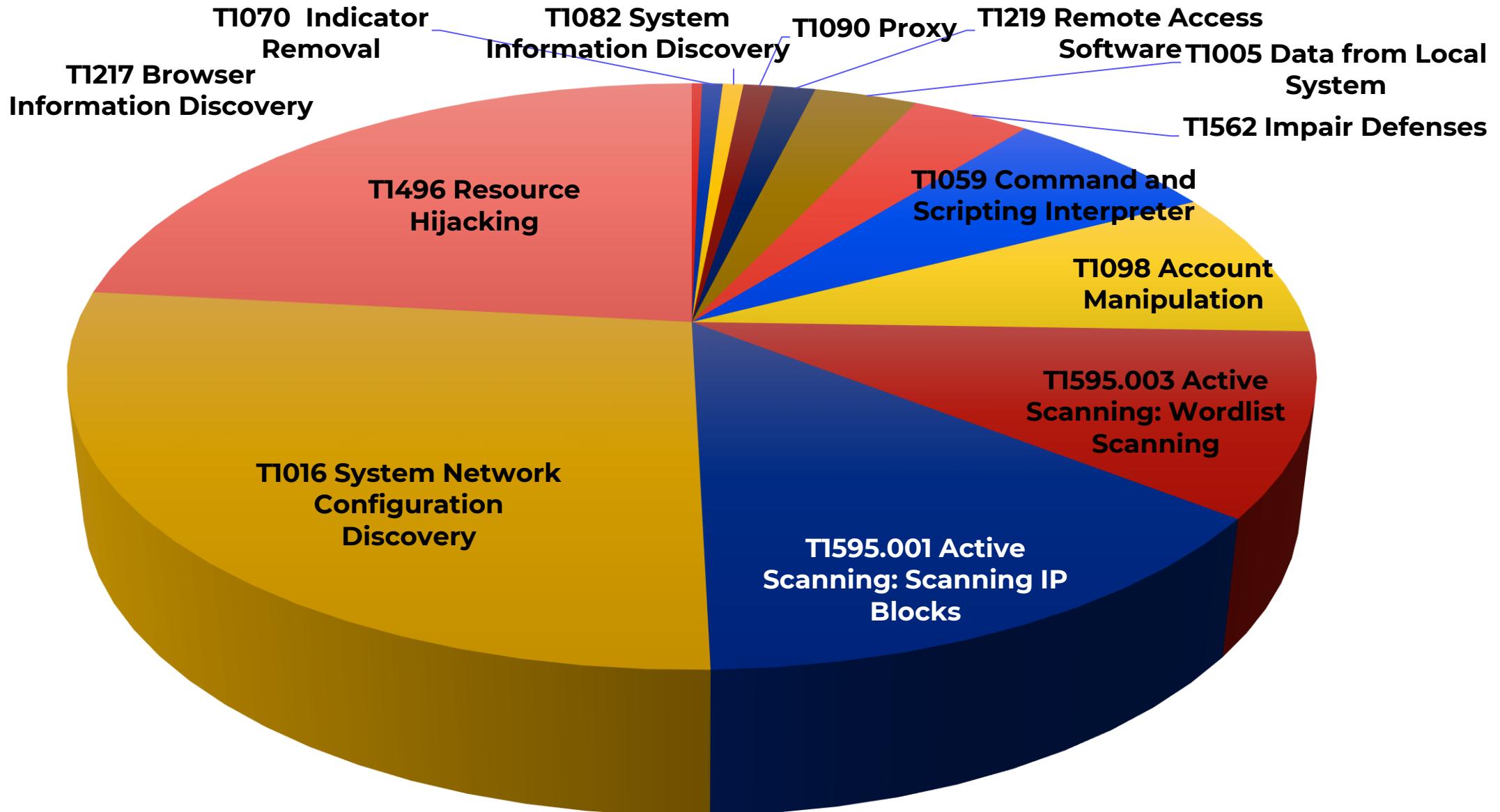
COLLECTED INTEL (CONT.)

Around 100 hours of videos analyzed



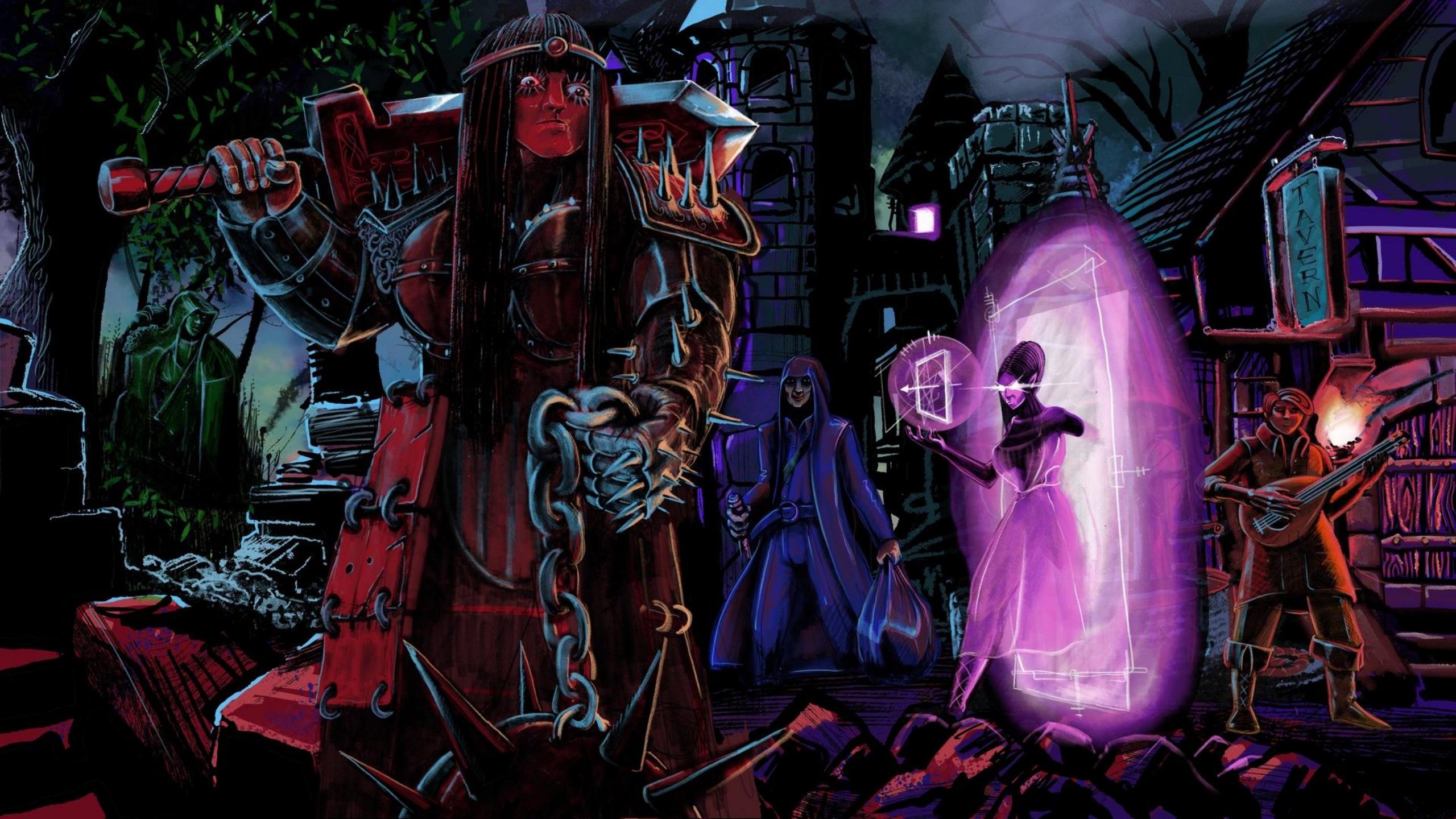
339 sessions of interest

ATT&CK INDICATORS





CHARACTERIZING ATTACKERS' D&D STYLE





RANGERS



- Explore the system
- Run reconnaissance
- Might be evaluating the system for others



RANGER IN ACTION



Hostname: EC2AMAZ-3IJ15JO
Instance ID: i-01312d4a89eecee55
Public IPv4 Address: 3.88.186.135
Private IPv4 Address: 172.31.50.210
Instance Size: t2.micro
Availability Zone: us-east-1d
Architecture: AMD64
Total Memory: 1024 MB
Network Performance: Low to Moderate

Recycle Bin

EC2 Feedback

EC2 Micros...

Word

11:41 AM
12/12/2022



THIEVES



- Monetize the RDP access
- Examples
 - Traffic generator
 - Traffmonetizer
 - Cryptominers





THIEVES IN ACTION

The screenshot shows a Microsoft Edge browser window with the following details:

- Title Bar:** Traffmonetizer
- Address Bar:** app.traffmonetizer.com/sign-in?_gl=1...
- Content Area:**
 - Logo:** Traffmonetizer logo (blue and orange stylized letters)
 - Text:** Log In
 - Fields:** Email (with user icon), Password (with lock icon)
 - Links:** Forgot password, Register Here
 - Buttons:** Log In (purple background)
 - Text:** or use
 - Icon:** Google (G) icon
 - Text:** You don't have an account? [Register Here](#)
 - Links:** [Terms of Service](#) | [Privacy Policy](#)
- Bottom Right:** Chat with us button (white speech bubble with blue icon) and a blue circular icon with a white 'G'.



Recycle Bin



EC2 Feedback

EC2 Microsoft
Windows G...Google
Chrome

xmrig

unMineable
Miner (M...)unMineable
Miner (MFI)

ChromeSetup

Hostname: EC2AMAZ-OJK3L78

Instance ID: i-049df4c0b0dfa528c

.236.56

31.32.40

RE

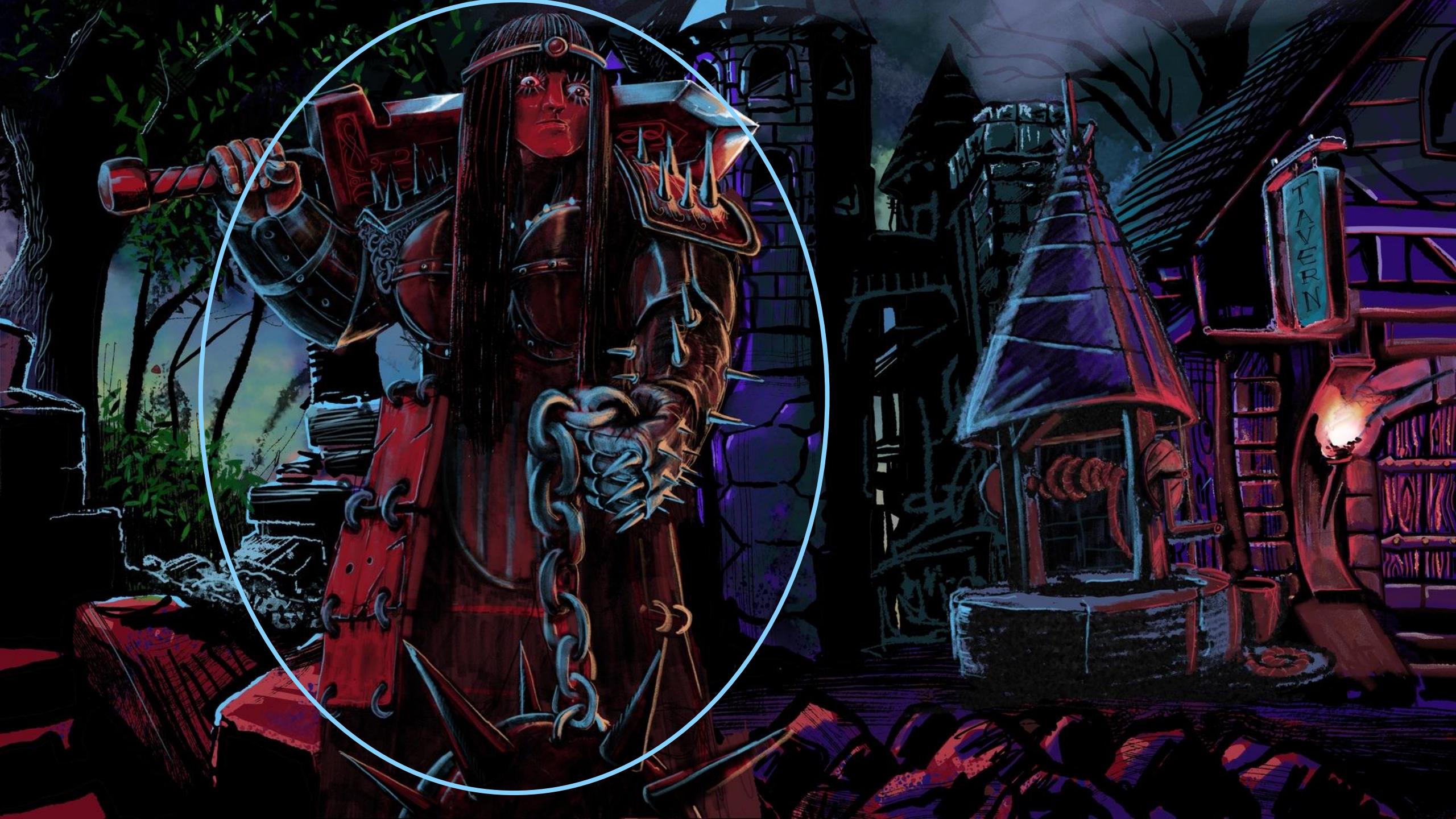
Name	Date modified	Type	Size
benchmark_1M	11/15/2022 7:31 PM	Windows Comma...	1 KB
benchmark_10M	11/15/2022 7:31 PM	Windows Comma...	1 KB
config.json	11/15/2022 7:31 PM	JSON File	3 KB
pool_mine_example	11/15/2022 7:31 PM	Windows Comma...	2 KB
rtm_ghotrider_example	11/15/2022 7:31 PM	Windows Comma...	2 KB
SHA256SUMS	11/15/2022 7:31 PM	File	1 KB
solo_mine_example	11/15/2022 7:31 PM	Windows Comma...	1 KB
start	11/15/2022 7:31 PM	Windows Comma...	1 KB
WinRing0x64.sys	11/15/2022 7:31 PM	System file	15 KB
xmrig	11/15/2022 7:31 PM	Application	8,031 KB

File description: WinRing0
Company: OpenLibSys.org
File version: 1.2.0.5
Date created: 3/6/2023 4:03 PM
Size: 14.2 KB



un

4:03 PM
3/6/2023



BARBARIANS



- Brute-force more computers
- Work with lists of IP addresses, usernames and passwords



BARBARIAN IN ACTION

Hostname: EC2AMAZ-PH85V08
Instance ID: i-07445ee7ec1a9a5f9
Public IPv4 Address: 54.237.89.231
Private IPv4 Address: 172.31.40.93
Instance Size: t2.micro
Availability Zone: us-east-1e
Architecture: AMD64
Memory: 1024 MB
Performance: Low to Moderate

Internet Explorer Enhanced Security Configuration is enabled

File Home Share View Manage Application Tools MasScan

This resource might be unsafe. See help and security settings.

File This PC Downloads MasScan MasScan

Name Date modified Type Size

Name	Date modified	Type	Size
_config	5/13/2022 4:51 AM	Configuration sett...	1 KB
exclude	5/13/2022 4:14 AM	Text Document	0 KB
Input	5/13/2022 4:51 AM	Text Document	34 KB
IPs	5/13/2022 4:51 AM	Text Document	78 KB
masscan	5/13/2022 4:14 AM	Application	233 KB
Massscan_GUI	5/13/2022 4:14 AM	Application	334 KB
msvcr100.dll	5/13/2022 4:14 AM	Application extens...	756 KB
Output	5/13/2022 4:51 AM	Text Document	150 KB
Packet.dll	5/13/2022 4:14 AM	Application extens...	95 KB
winpcap-4.13	5/13/2022 4:14 AM	Application	424 KB
wpcap.dll	5/13/2022 4:14 AM	Application extens...	220 KB

11 items 1 item selected 423 KB

5 items



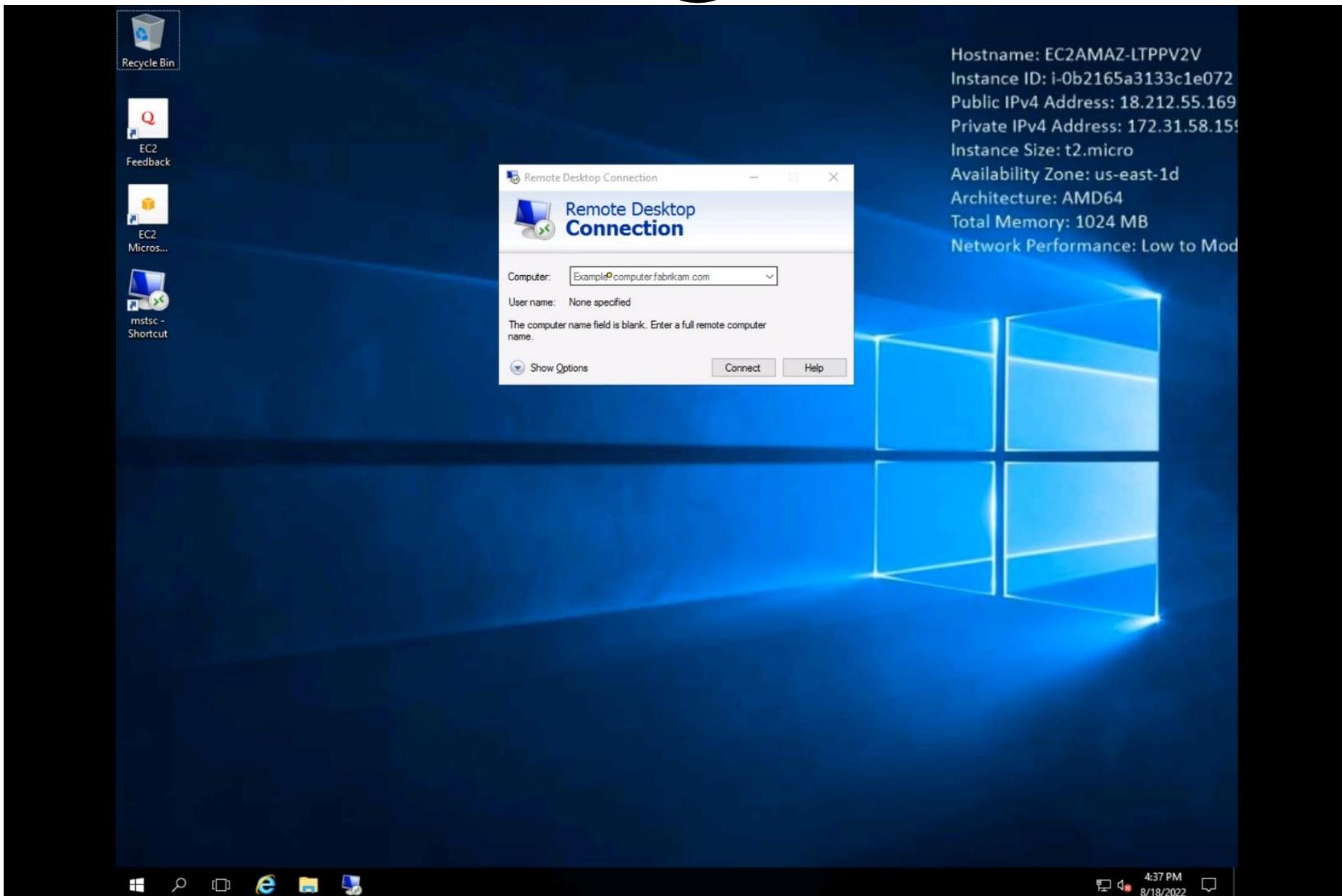
WIZARDS



- Use the RDP access as a portal to connect to other computers
- Show a high level of skill



WIZARD IN ACTION





BARDS



- No apparent hacking skills
- Examples:
 - Google searches related to hacking
 - Porn watching
 - Downloading movies
- Might have bought the access





BARDS IN ACTION

GOSECURE

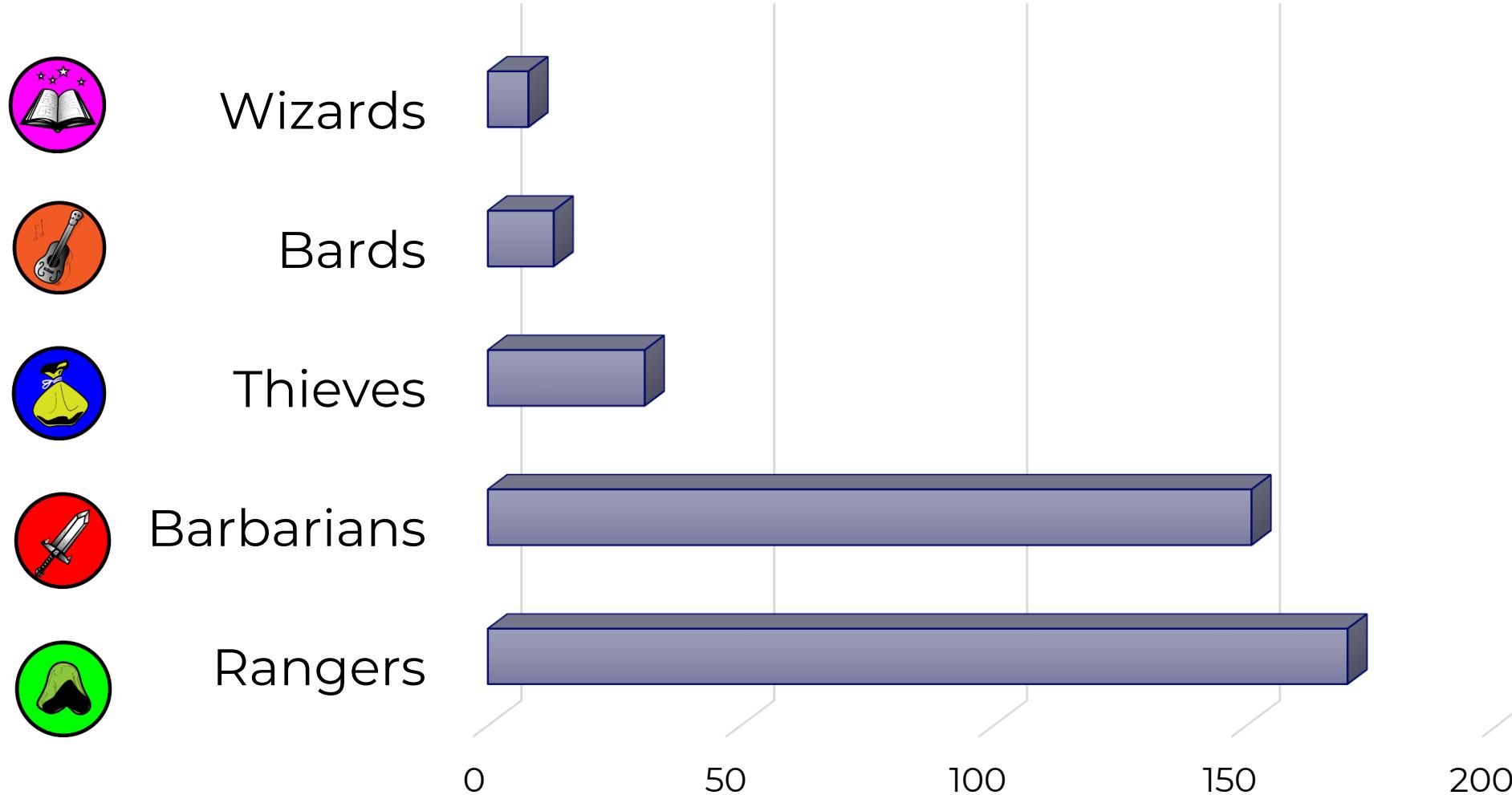


WHY PORN?

Internet censorship → Ban on pornography → RDP as a solution

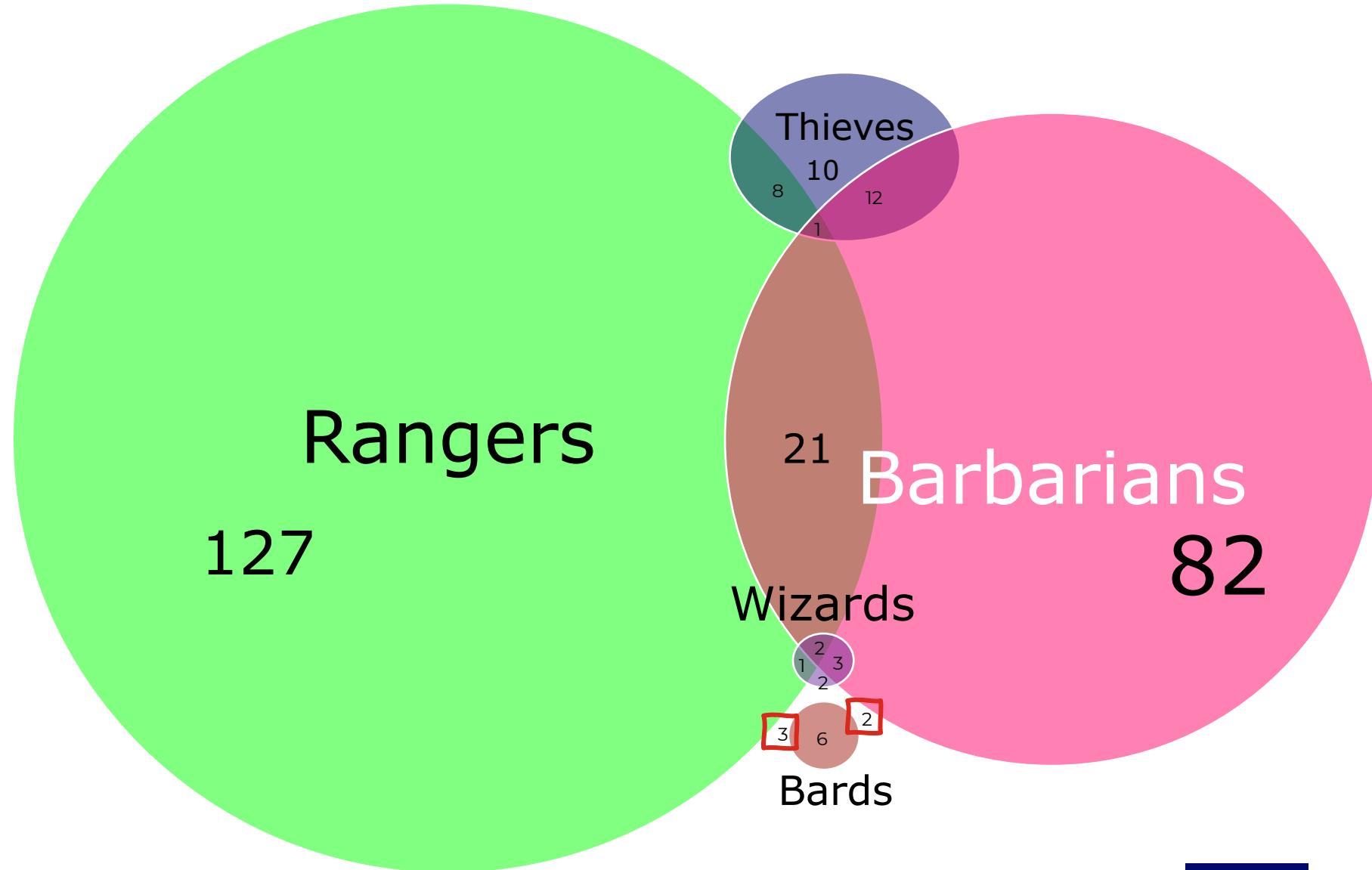
SESSIONS BY PROFILE

Number of RDP sessions associated with the profiles



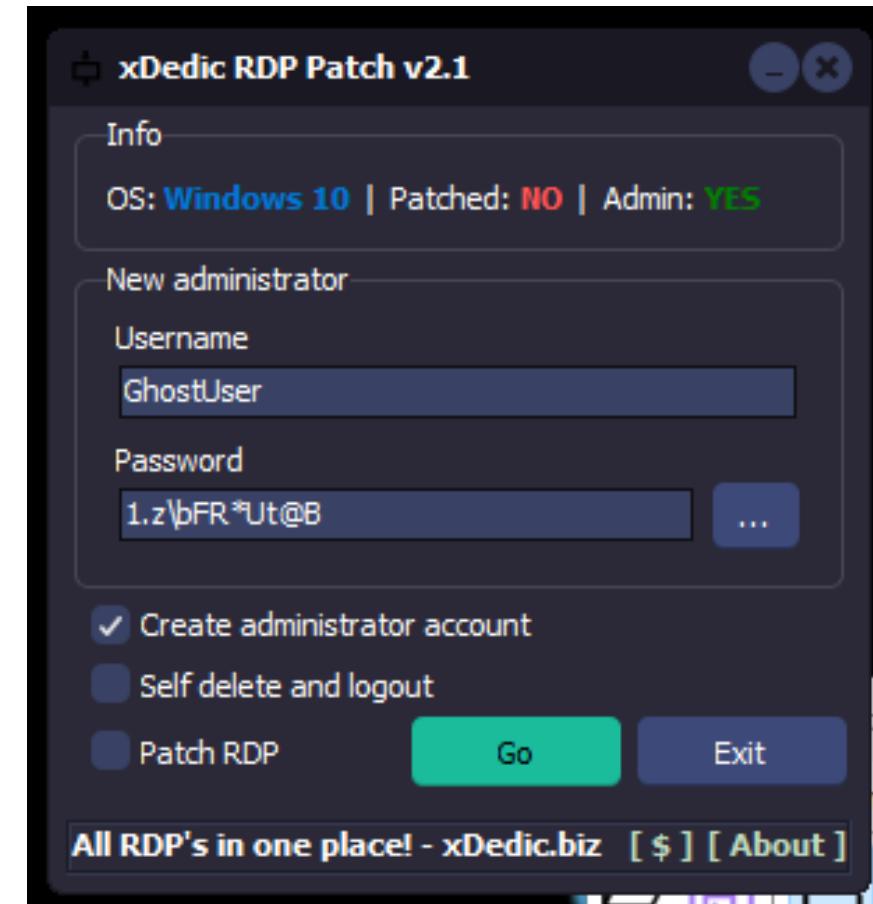
ATTACKERS' OVERLAP

GOSECURE

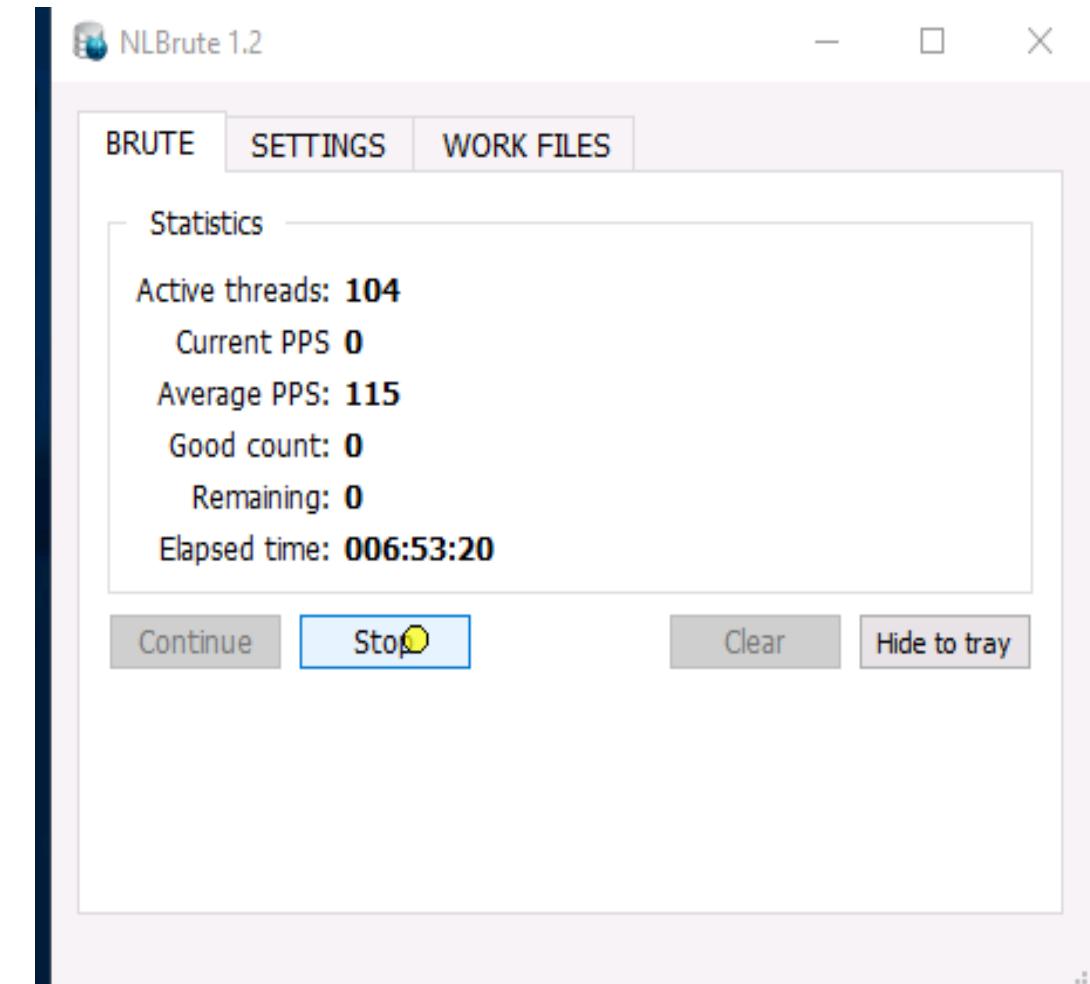


ATTACKERS' WEAPONRY

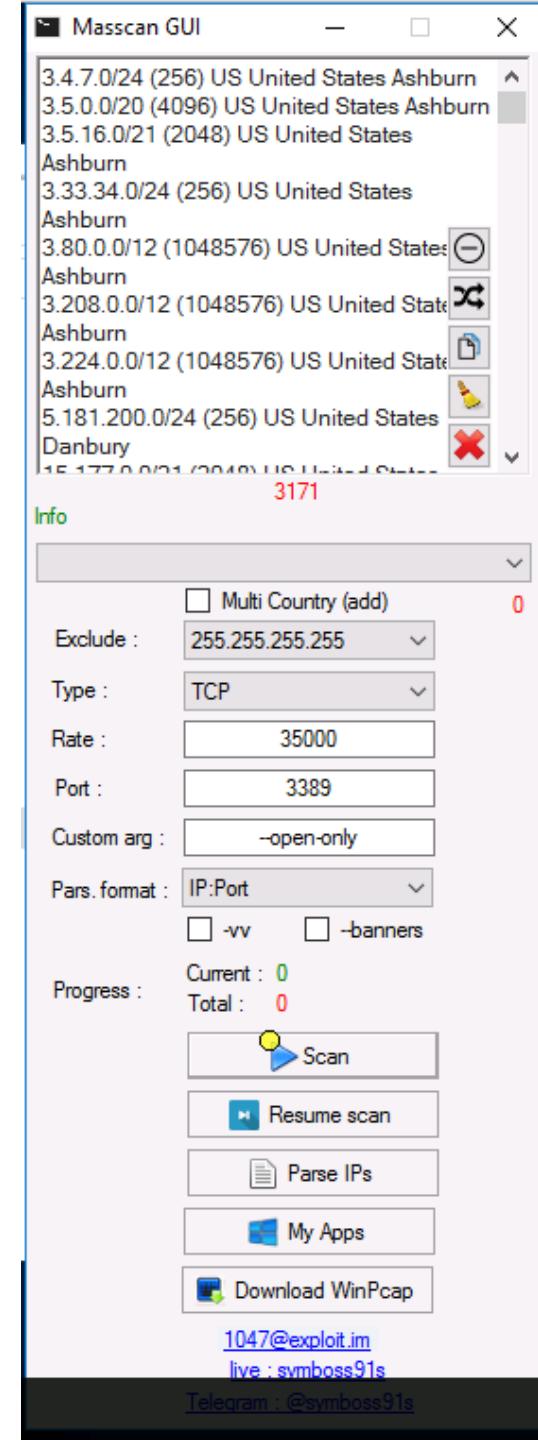
XDEDIC RDP PATCH



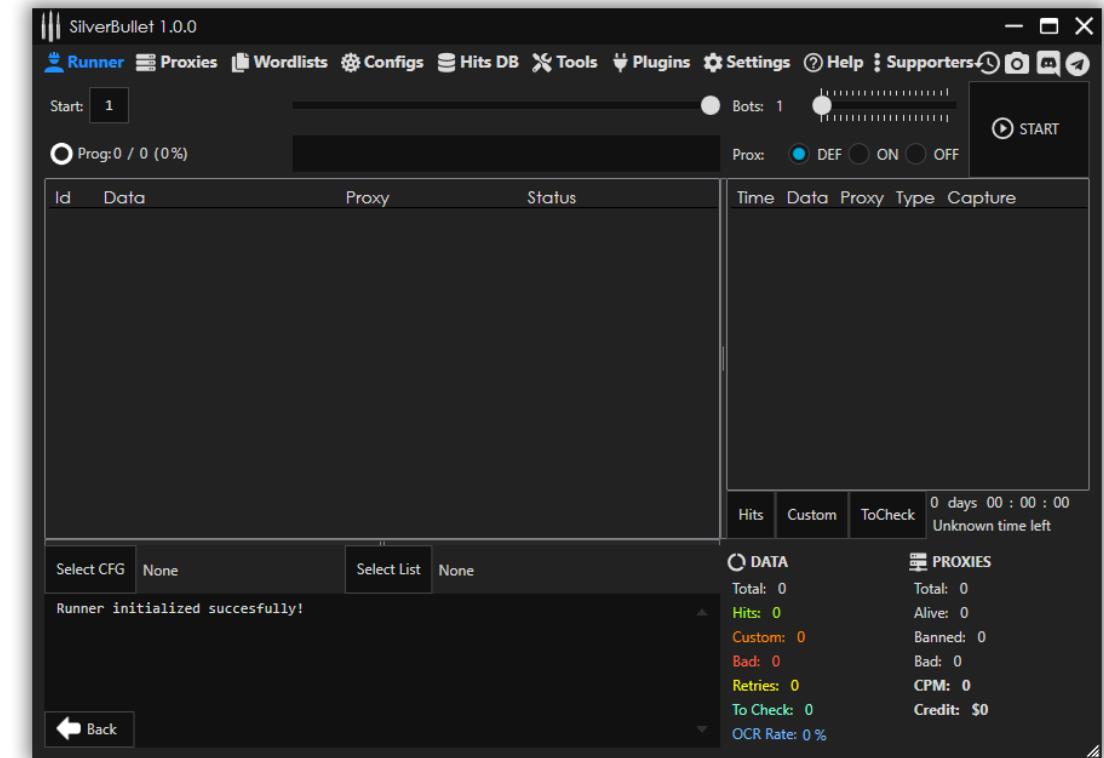
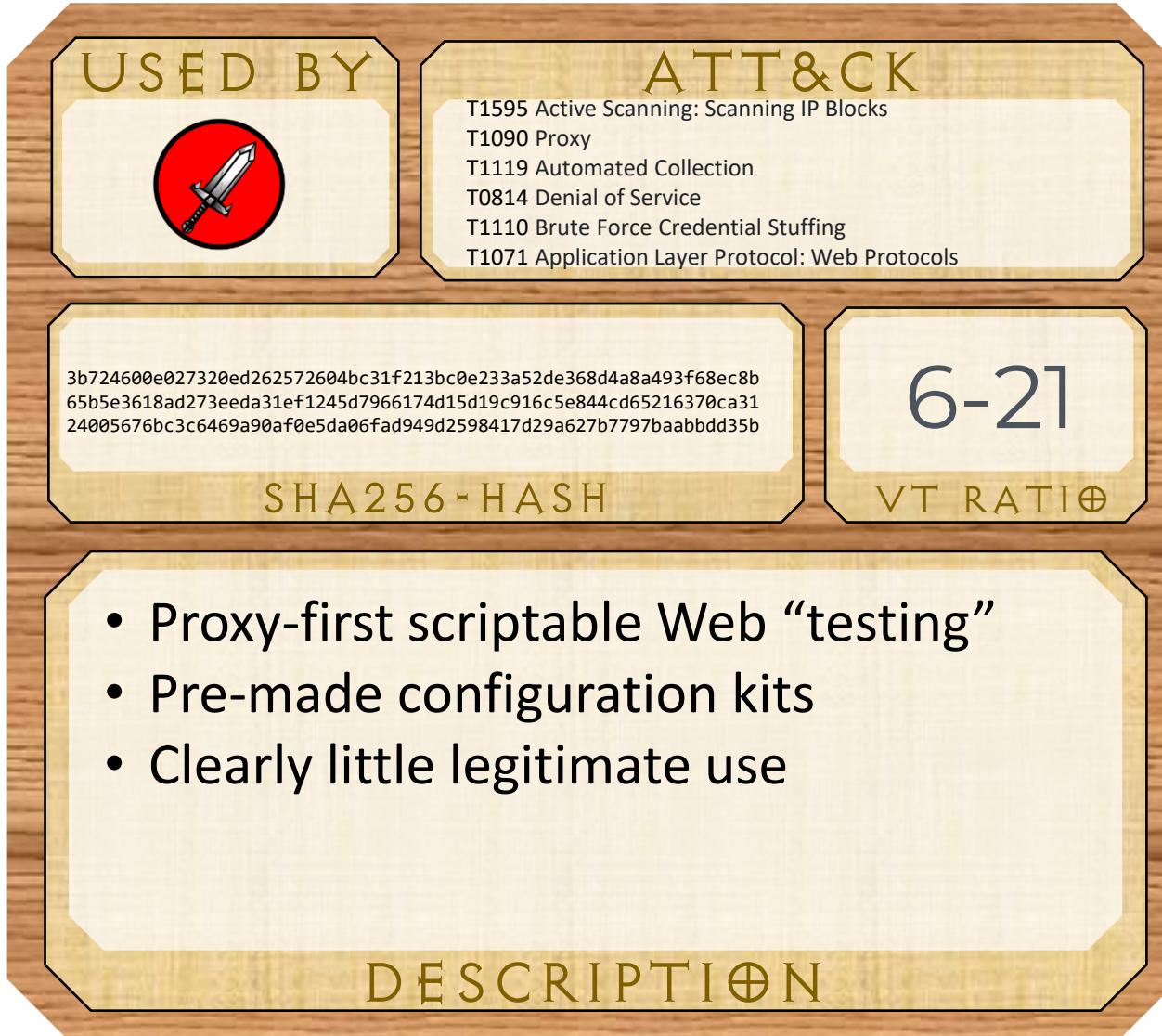
NLBRUTE



MASSCAN GUI



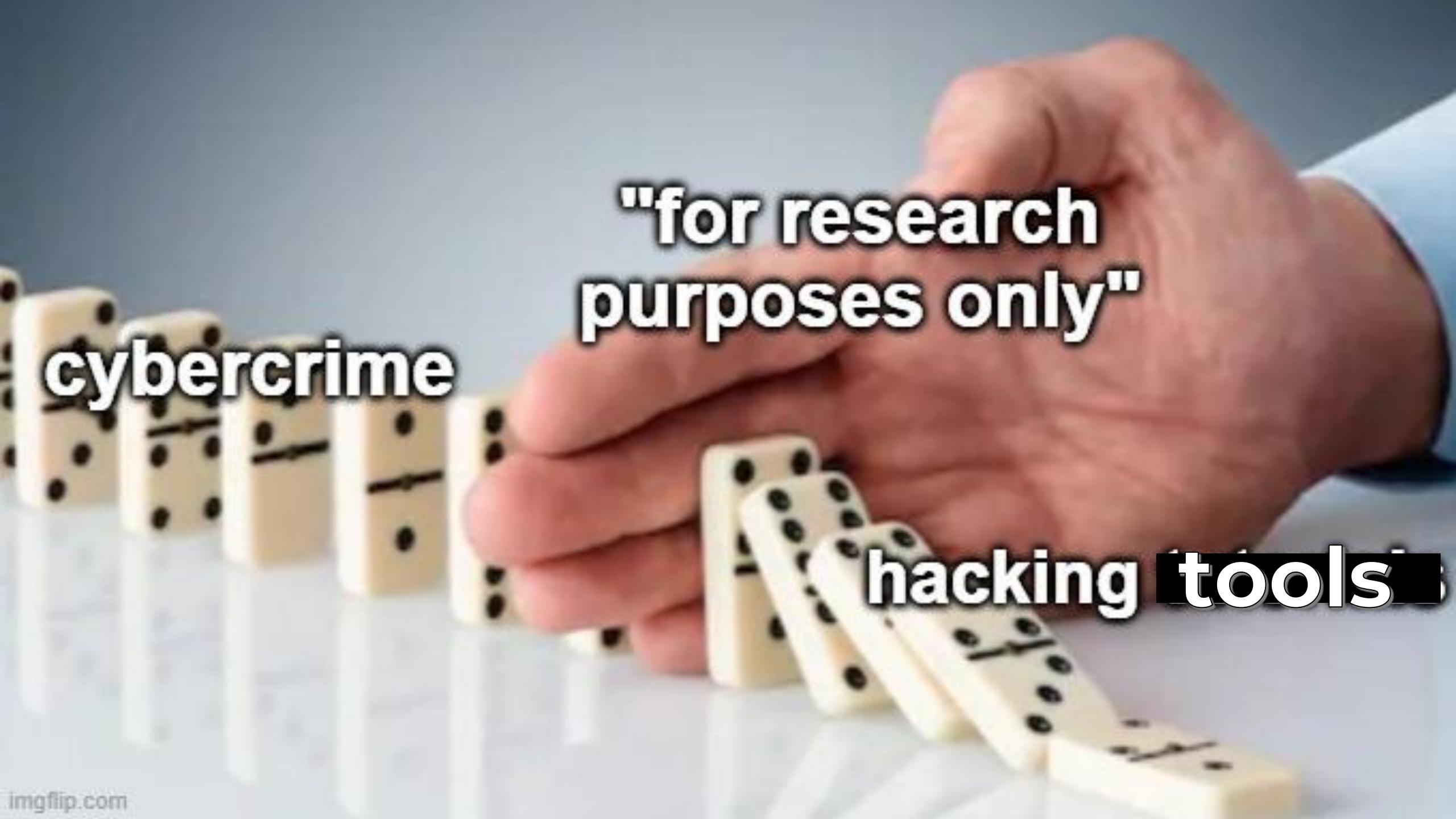
SILVERBULLET



SILVERBULLET (CONT.)

Again, on their website:

IMPORTANT! Performing (D)DoS attacks or credential stuffing on sites you do not own (or you do not have permission to test) is **illegal!** The developer will not be held responsible for improper use of this software.

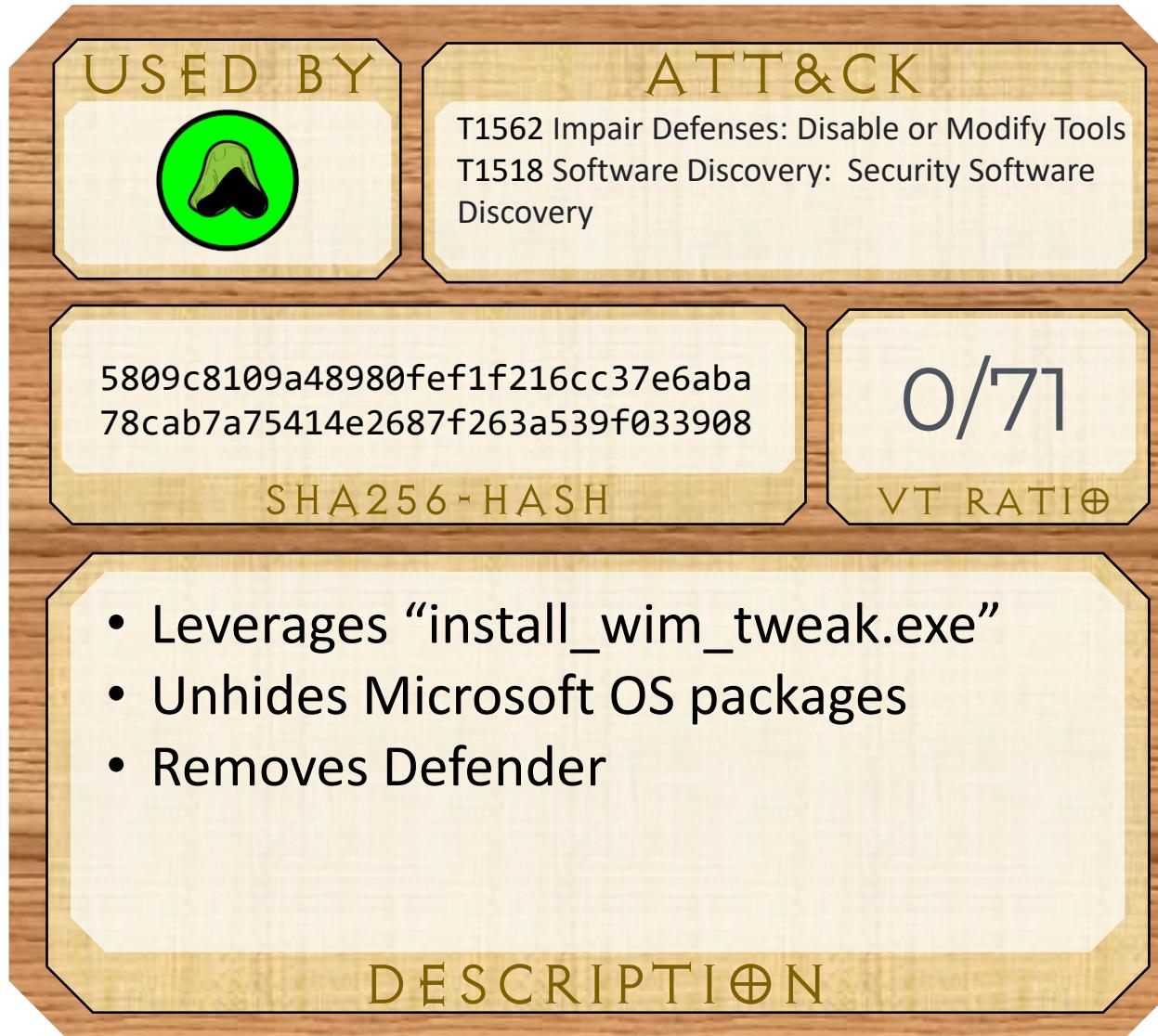
A close-up photograph of a person's hand holding several white dominoes with black pips. The dominoes are arranged horizontally, with the last one being held by the fingers and thumb, while the others are balanced on top of it. The background is a plain, light color.

cybercrime

**"for research
purposes only"**

hacking tools

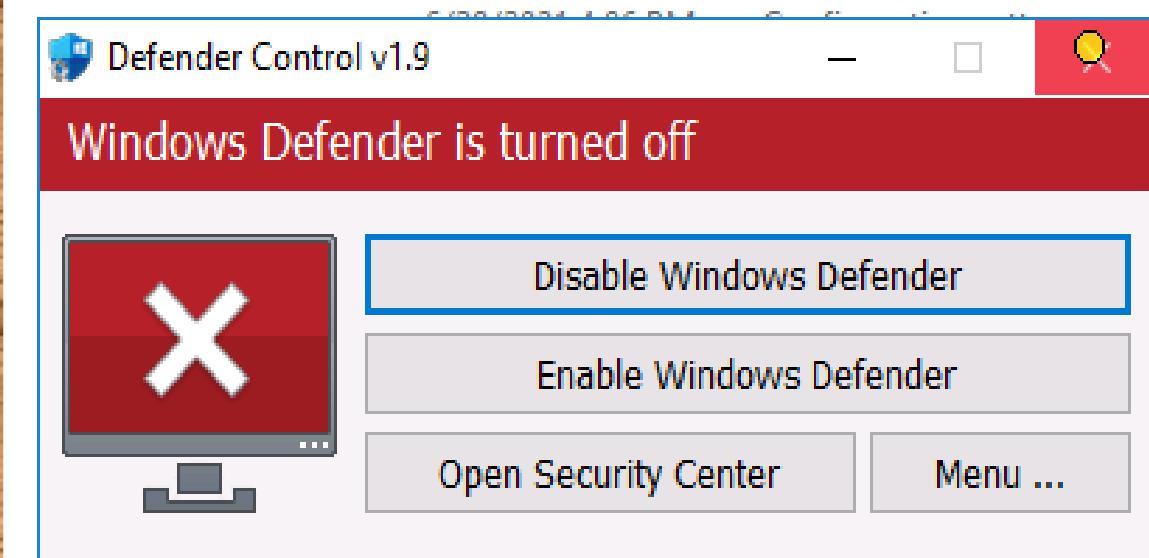
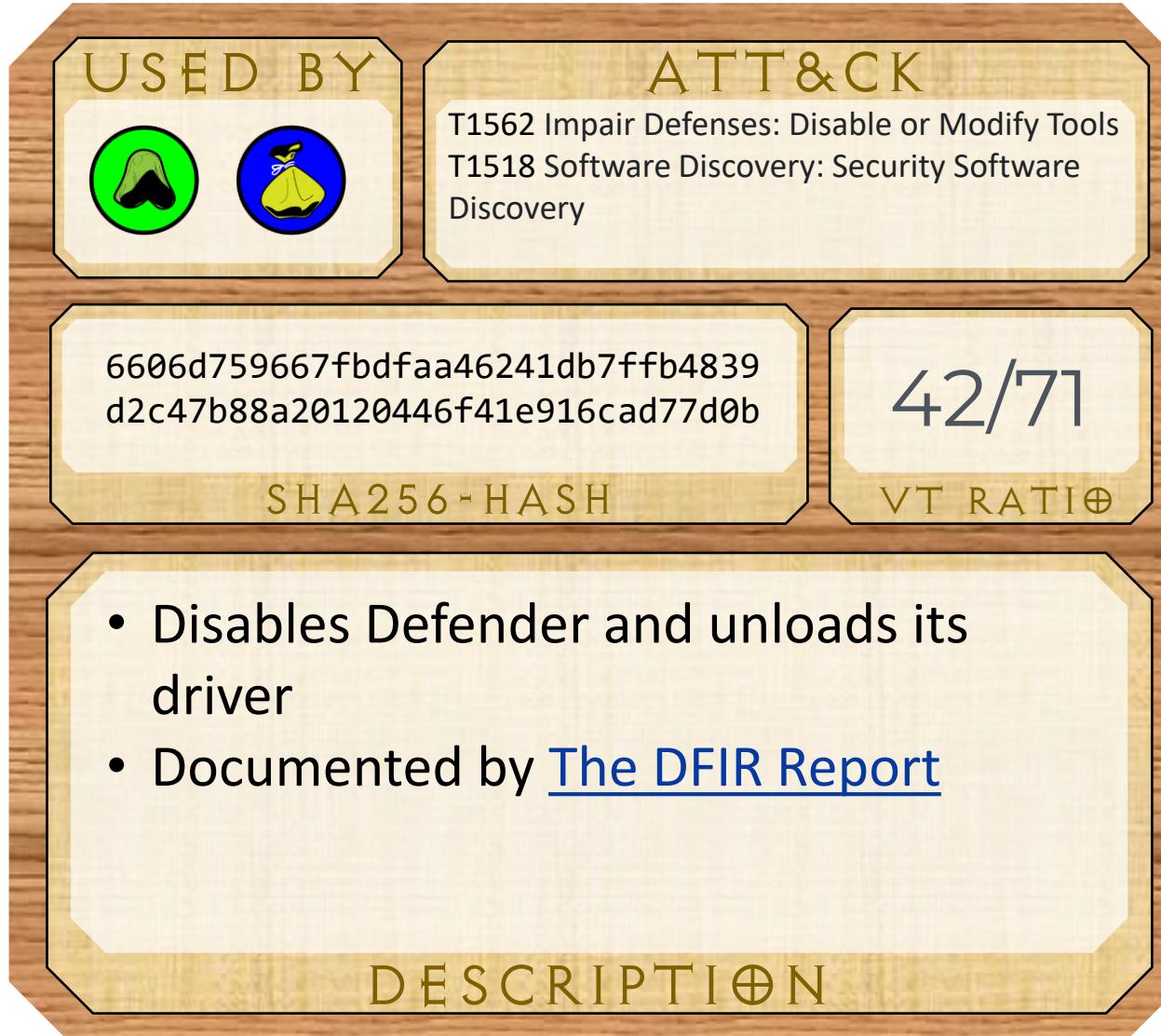
WINDOWS DEFENDER REMOVE SCRIPT



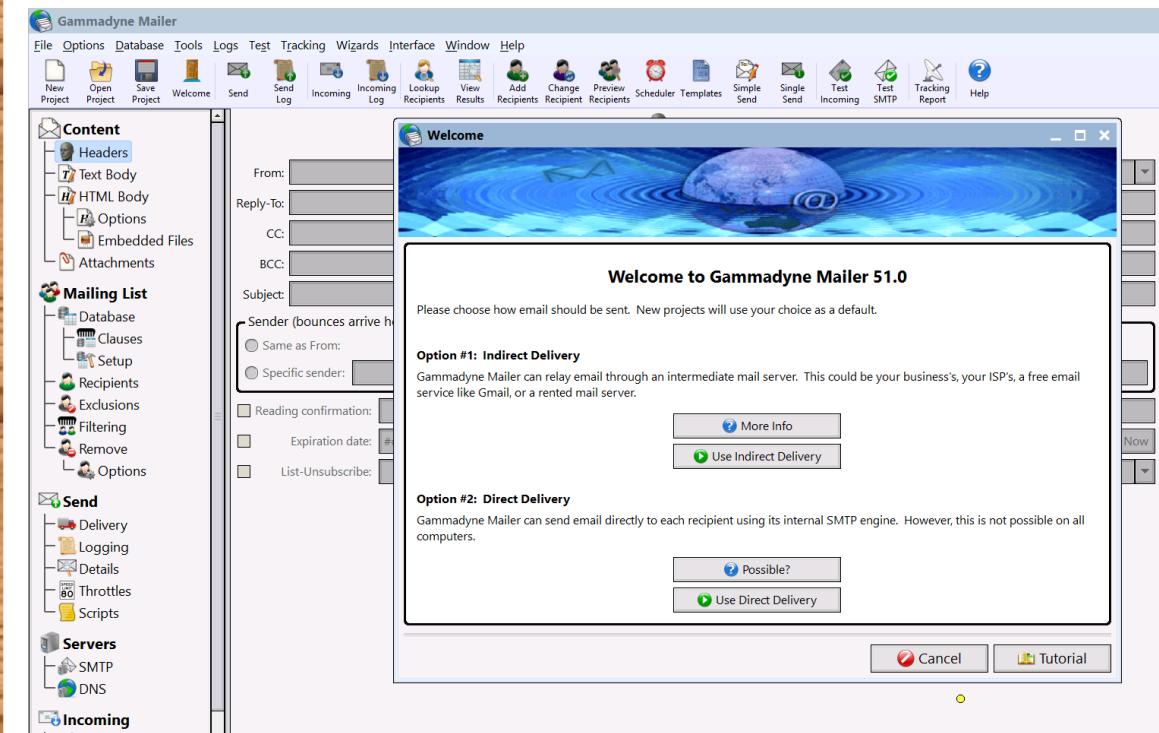
```
C:\Windows\system32\cmd.exe

-----  
Registry Tweak Tool v1.4.7.0-----  
-----for Windows 6.x-----  
-----Created by Michal Wniewski-----  
-----Concept by Aviv00@msfn / lite8@MDL-----  
-----Modified by Legolash2o-----  
  
MountPath : Online  
  
-----Starting-----  
Writing to Log (Packages.txt) 3875/3875OK  
-----Ending-----  
  
-----Registry Tweak Tool v1.4.7.0-----  
-----for Windows 6.x-----  
-----Created by Michal Wniewski-----  
-----Concept by Aviv00@msfn / lite8@MDL-----  
-----Modified by Legolash2o-----  
  
MountPath : Online  
Component : "Windows-Defender"  
  
-----Starting-----  
Taking Ownership... OK  
Editing 'Packages' subkeys 44/44OK  
Modifying registry completed successfully.  
Removing 'Packages'... 41/44
```

DCONTROL (AKA DEFENDERCONTROL)



GAMMADYNE MAILER



AND MORE...



Thieves

- XMRig (cryptominer)
- Monetizing browsers (Websidia, Netbox)
- Traffmonetizer
- WorldWind
- AlexaMaster
- Honeygain dashboard



Rangers

- Change pass one click

Miscellaneous

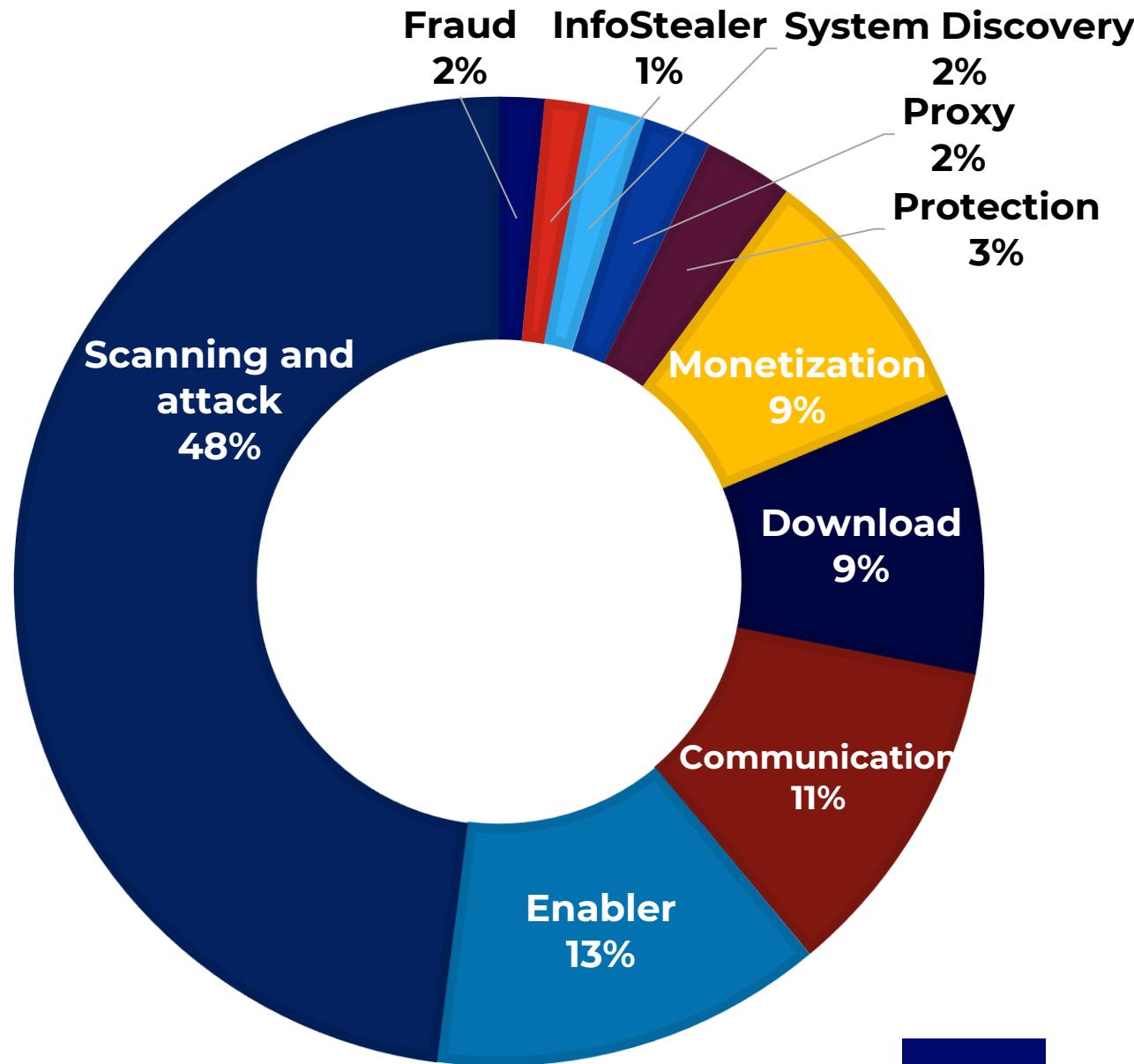
- Telegram Bot API toolkit
- IPVanish
- Time restart reloaded (Chrome extension)
- Backset



Barbarians

- KPort Scan
- NLA checker
- Mimikatz
- Advanced IP Scanner
- STORM
- OK Prog Proxy leecher
- Spotify proxyless brute checker
- Soft Perfect Scanner or netscanold
- RDP Cracked by Arman
- Brute XML

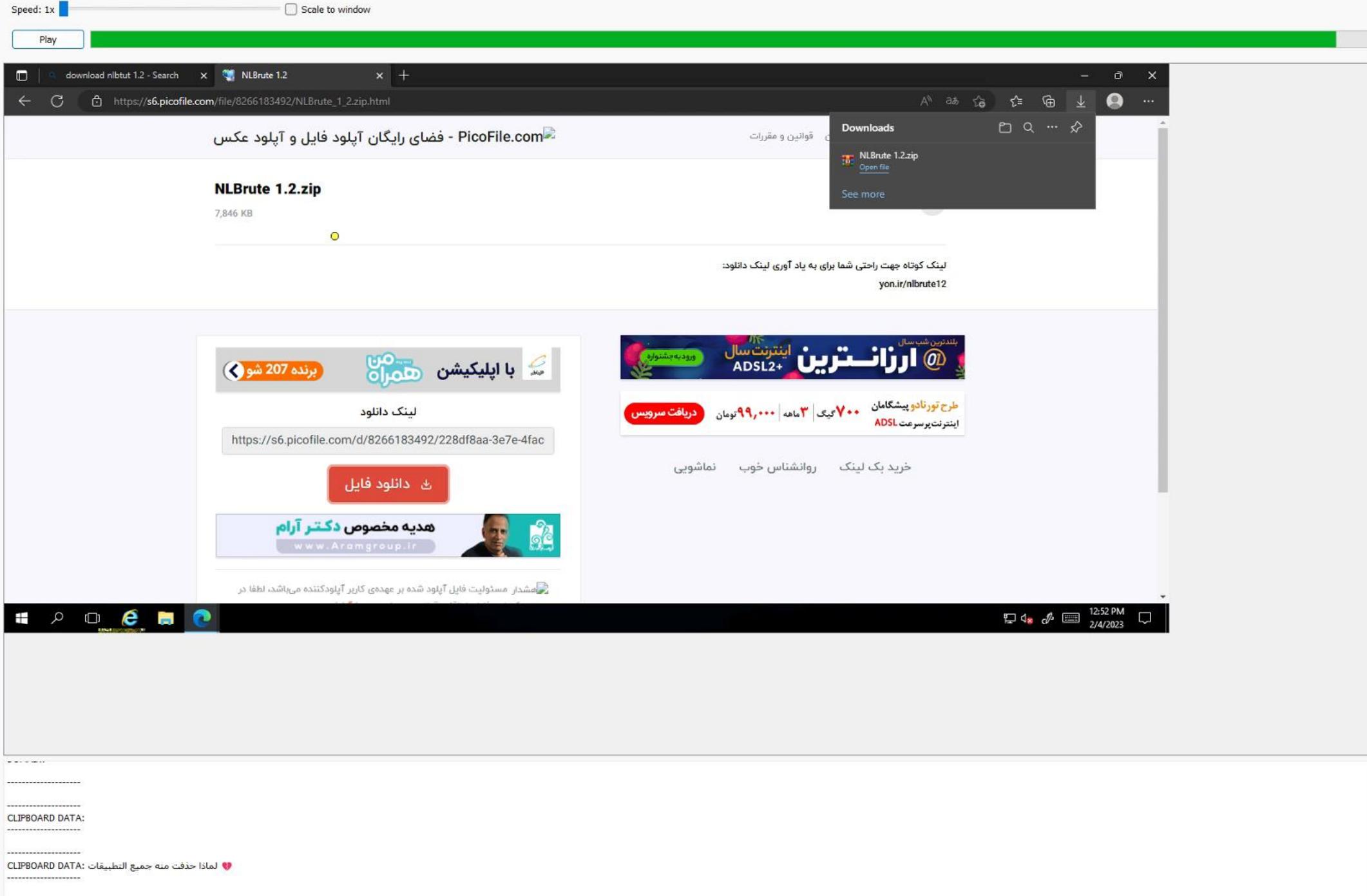
TOOL CLASSIFICATION BY OBJECTIVE



■ CRYSTAL BALL

They are humans after all



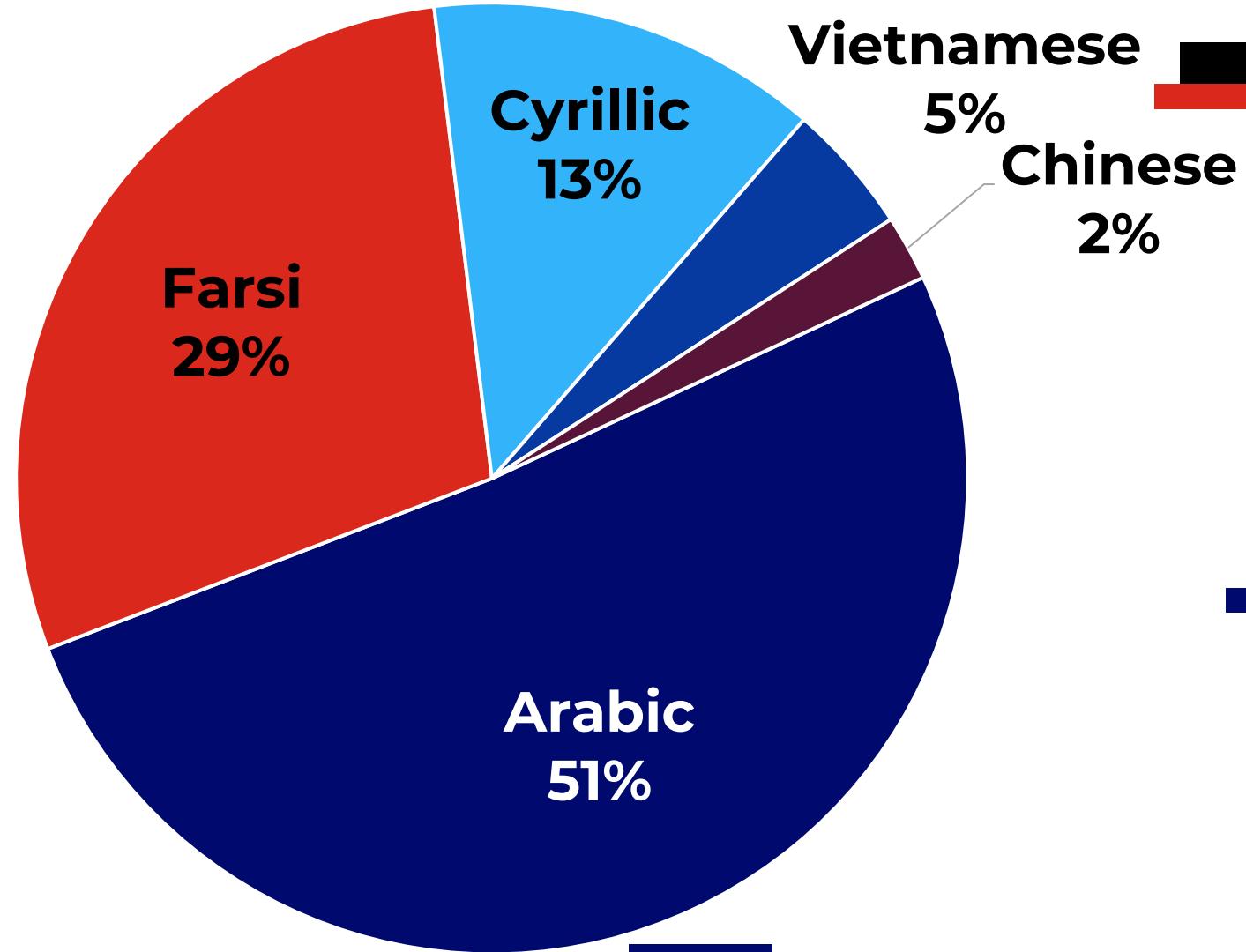


SOME ATTACKERS DO NOT SPEAK ENGLISH

The screenshot shows a Google Ads billing setup page. At the top, there's a navigation bar with links for SEARCH, REPORTS, TOOLS & SETTINGS, and BILLING. Below the navigation, there's a section about payment profiles. The main part of the screen is a form for entering payment information. It includes fields for a credit or debit card, with a sample card number (7021 4737 6311) and expiration date (08 / 24). There's also a field for the cardholder's name, which contains the text "y Watson". At the bottom of the form, there's a note about payment frequency and a link to Google Ads Terms. The status bar at the bottom of the browser window shows the time as 2:05 PM and the date as 2/8/2021.

ALPHABET FOUND IN SESSIONS

N=45



OUR TOOL IS GREAT FOR INTEL



Recycle Bin



Telegram

Google
Chrome

WinRAR

EC2
FeedbackEC2
Micros...

END GAME XP AND TREASURE

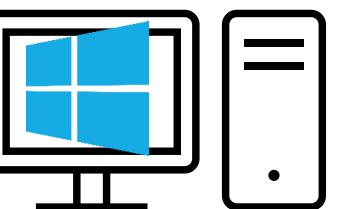
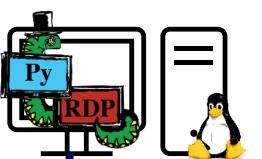
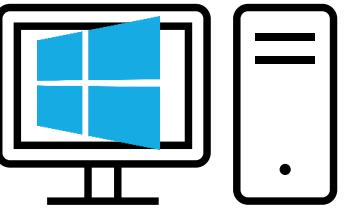
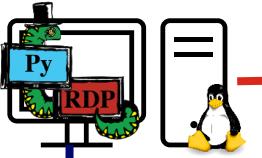
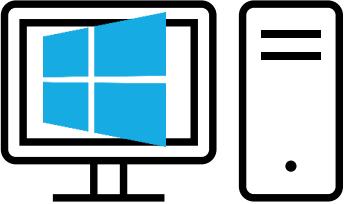
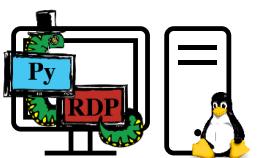
The Takeaways



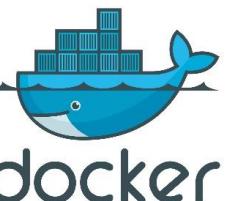
Honeynet Plan



Cloud (several providers)



RabbitMQ



docker



Terraform

Science!



elastic



fluentd



RCLONE

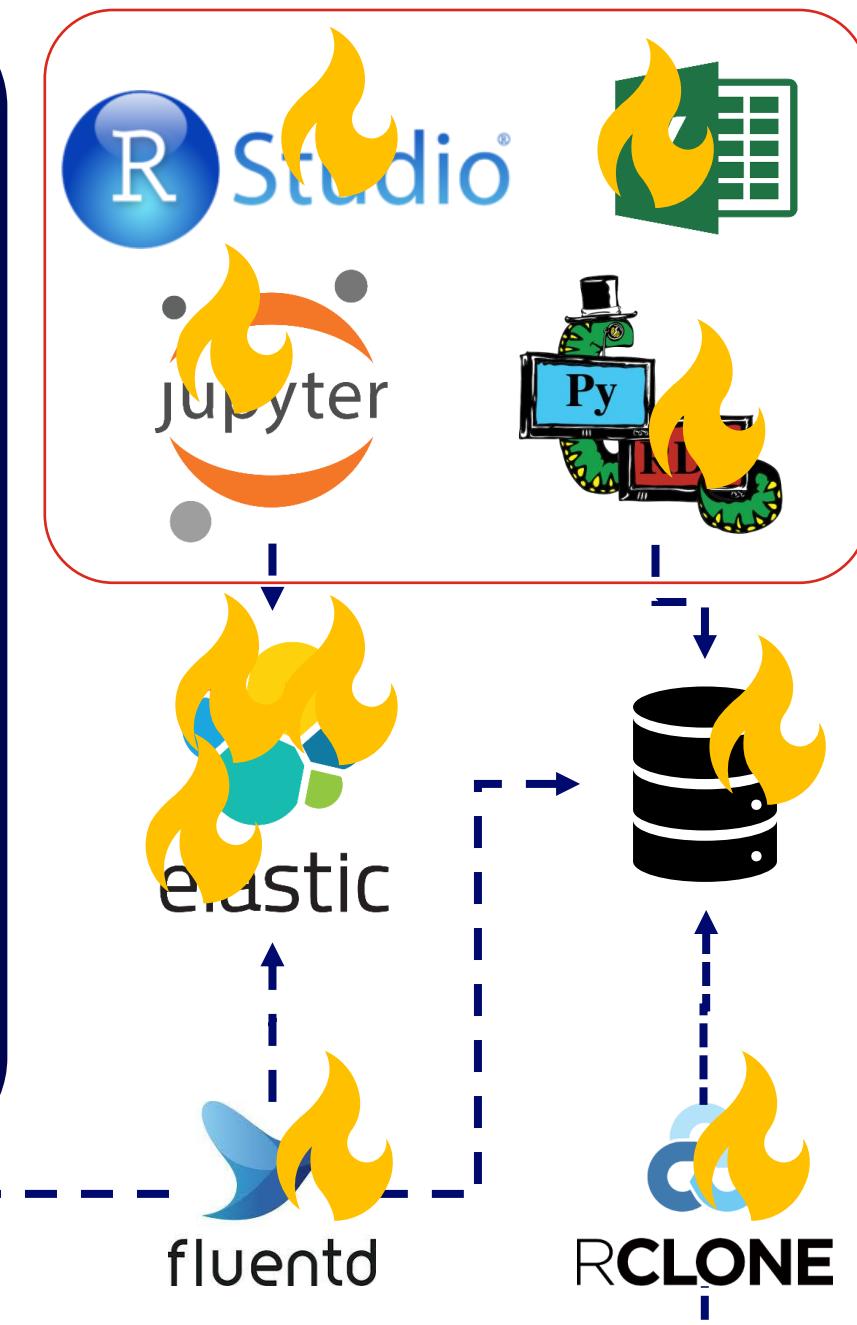
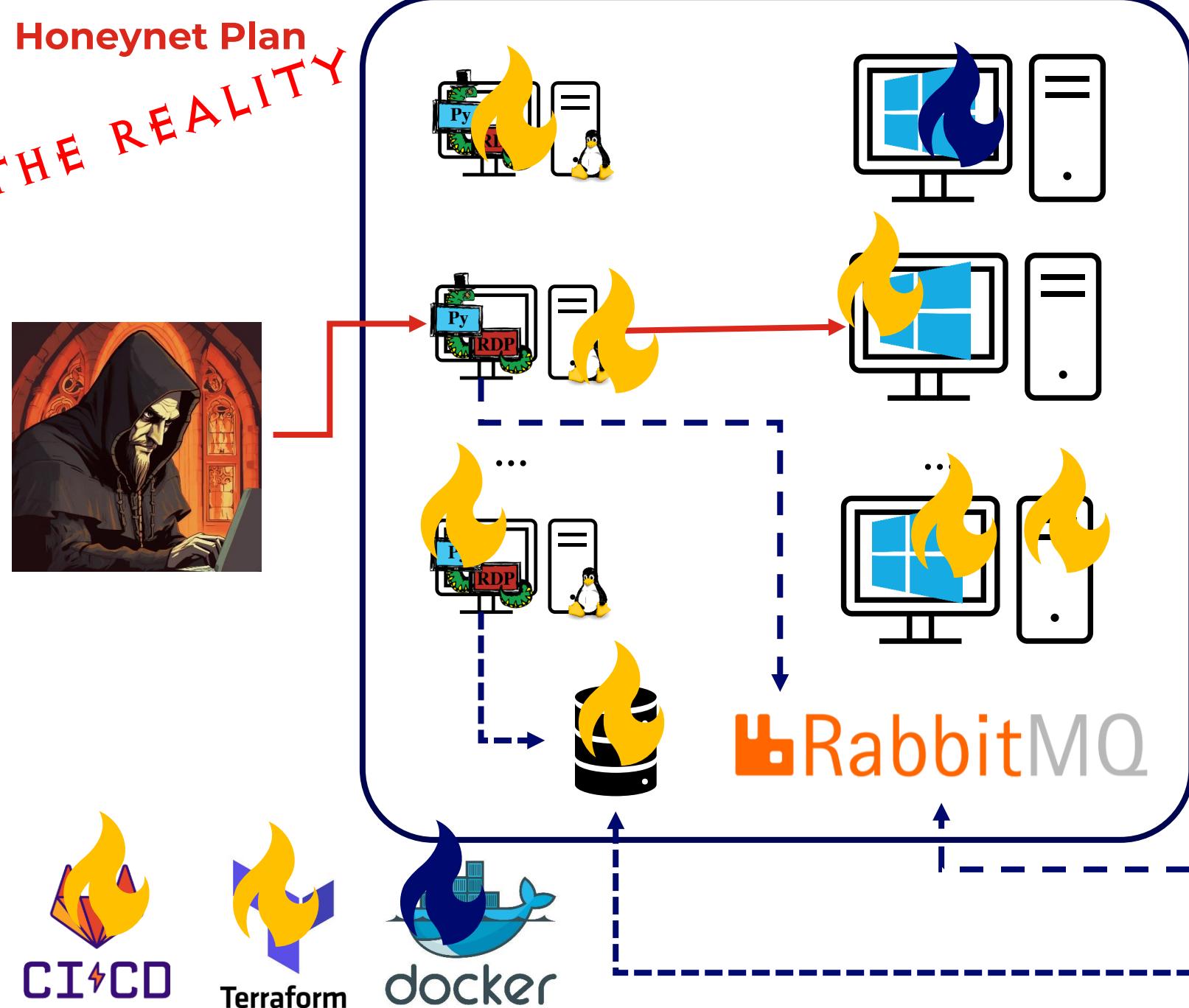
Honeynet Plan

THE REALITY



CI⁺CD

Terraform



THE PARTY



TAKEAWAYS

Researchers: RDP is ripe for attacker study

Blue Team: Consume the IOCs, roll out your own traps

Law Enforcement: Lawfully intercept the RDP environments used by ransomware groups.

If the attackers fear getting caught on camera, they will be more careful which will slow them down.

BLUE TEAM TAKEAWAYS (CONT.)

- No Internet-exposed RDP systems
- Change the Administrator username
- Prevent the use of weak passwords
- Rate-limit the connections
- Good Internet Citizen: Prevent outbound RDP in the DMZ to prevent attackers from pivoting

⊕NE MORE THING

PyRDP is open source

Now, our FQ RDP capture
parser is too!

Analysis at scale

	00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f	0123456789abcdef	.events[0].client_data{}
0x10	01 c0		header: "client_core" (49153)
0x10	ea		length: 234
0x10	0d 08		version: "rdp10_8" (524301) (RDP 10.8)
0x10	40 06		desktop_width: 1600
0x10	84 03		desktop_height: 900
0x10	01 ca		color_depth: 51713
0x20	03 aa		sas_sequence: 43523
0x20	09 04		keyboard_layout: 1033
0x20	61 4a		client_build: 19041
0x20	44 45 53		client_name: "DESKTOP-UPH091R"
0x30	4b 54 4f 50 2d 55 50 48	K T O P - U P H	
0x40	4f 39 31 52	O 9 1 R	
0x40	04	.	keyboard_type: 4
0x40			keyboard_sub_type: 0
0x50			
0x50	0c	.	keyboard_function_key: 12
0x50			ime_file_name: raw bits
0x60			
*	until 0x95.7 (64)		
0x90	01 ca 01	10	...
0xa0	06 ad 06 63 34 64 63 38 64	. . . c 4 d c 8 d	code_data: raw bits
*	until 0xf7.7 (98)		

THANK YOU! QUESTIONS?

Olivier Bilodeau

obilodeau@gosecure.net
[@obilodeau](https://www.linkedin.com/in/obilodeau)



 GoSECURE

<https://gosecure.net/blog/>



 nsec

<https://nsec.io>

See you at the



Artwork



jeremie@tunghat.ca

REFERENCES / IOC

- IoCs: <https://github.com/GoSecure/malware-ioc/>
- PyRDP:
<https://github.com/GoSecure/pyrdp/blob/master/README.md#pyrdp-lore>
- Newly open-sourced FQ PyRDP replay parser:
<https://github.com/GoSecure/fq-pyrdp/>