



AUGUST 9-10, 2023

BRIEFINGS

I WATCHED YOU ROLL THE DIE: UNPARALLELED RDP MONITORING REVEAL ATTACKERS TRADECRAFT

Olivier Bilodeau & Andr anne Bergeron, GoSecure

DISCLAIMER: DUNGEONS AND DRAGONS NERDINESS



Andréanne Bergeron

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

Olivier Bilodeau

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

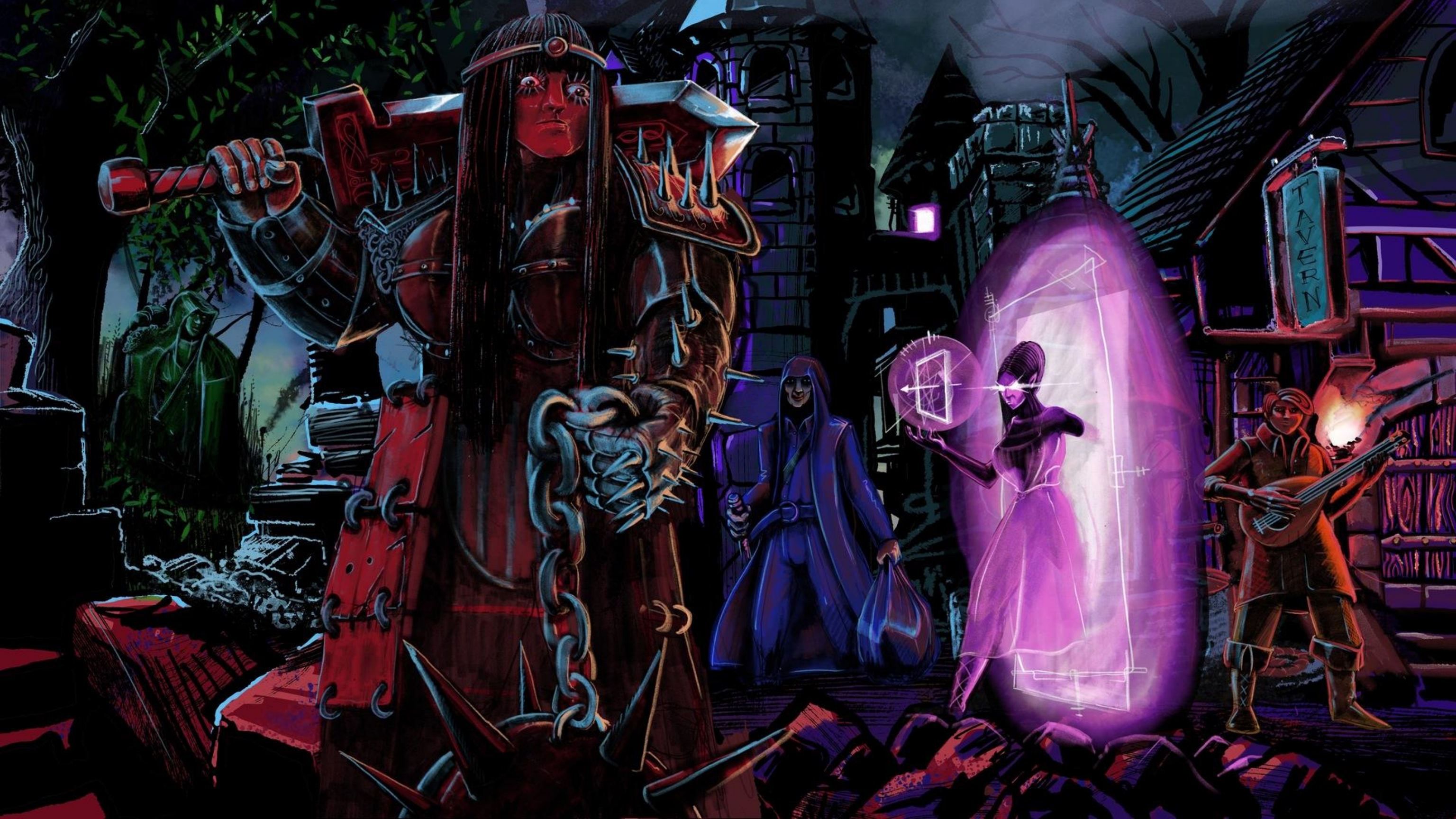




THE QUEST

- RDP Interception Explained
- 5 Attacker Classes
 - Rangers, Thieves, Barbarians, Wizards and Bards
- The Arsenal they use
- Some Memorable Session Highlights



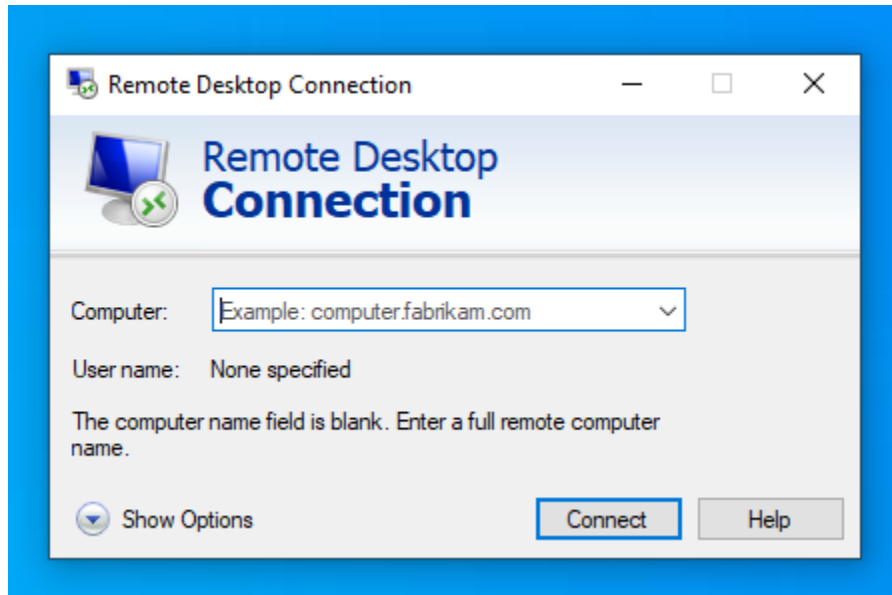




- Ransomware is a problem, RDP is an important factor
- Let's Leverage Unparalleled RDP Capture Depth



REMOTE DESKTOP PROTOCOL



my-server.gosec.co - Remote Desktop Connection

Server Manager

Server Manager ▶ Local Server

Dashboard

Local Server

All Servers

File and Storage Services ▶

PROPERTIES
For EC2AMAZ-6IS509J

Computer name	EC2AMAZ-6IS509J	Last installed updates	5/19/2017 8:36 PM
Workgroup	WORKGROUP	Windows Update	Never check for up
		Last checked for updates	5/19/2017 8:36 PM
Windows Firewall	Public: On	Windows Defender	Disabled
Remote management	Disabled	Feedback & Diagnostics	Settings
Remote Desktop	Enabled	IE Enhanced Security Configuration	On
NIC Teaming	Disabled	Time zone	(UTC) Coordinated
Ethernet	IPv4 address assigned by DHCP, IPv6 enabled	Product ID	00376-40000-0000
Operating system version	Microsoft Windows Server 2016 Datacenter	Processors	Intel(R) Xeon(R) CP
Hardware information	Xen HVM domU	Installed memory (RAM)	1 GB
		Total disk space	30 GB

EVENTS
All events | 2 total

Server Name	ID	Severity	Source	Log	Date and Time
EC2AMAZ-6IS509J	10016	Error	Microsoft-Windows-DistributedCOM	System	3/24/2022 5:25:18 PM
EC2AMAZ-6IS509J	10016	Error	Microsoft-Windows-DistributedCOM	System	3/24/2022 5:24:18 PM

5:17 PM
3/25/2022



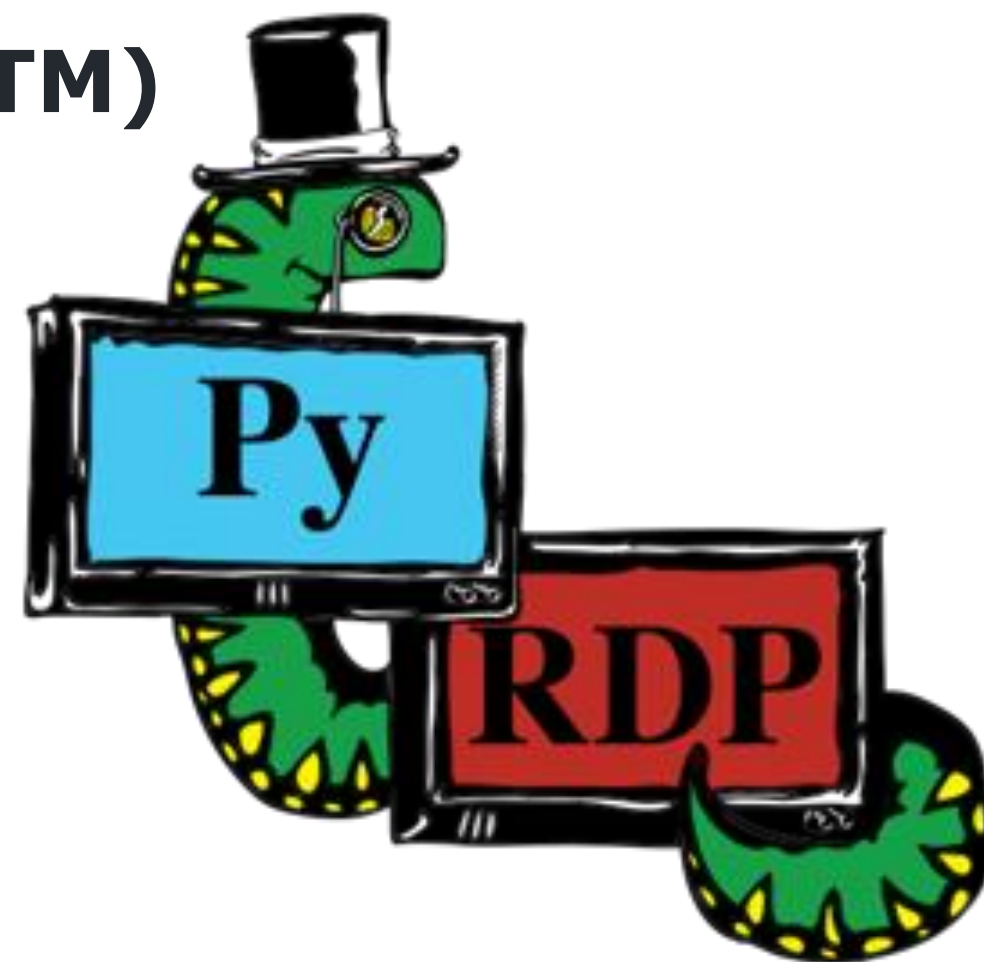
4 years in development

RDP Monster-in-the-Middle (MITM)

- RDP Interception
- Records Everything
- RDP Tampering Engine

RDP Player

- Real-time viewing and takeover
- Replay of previous captures



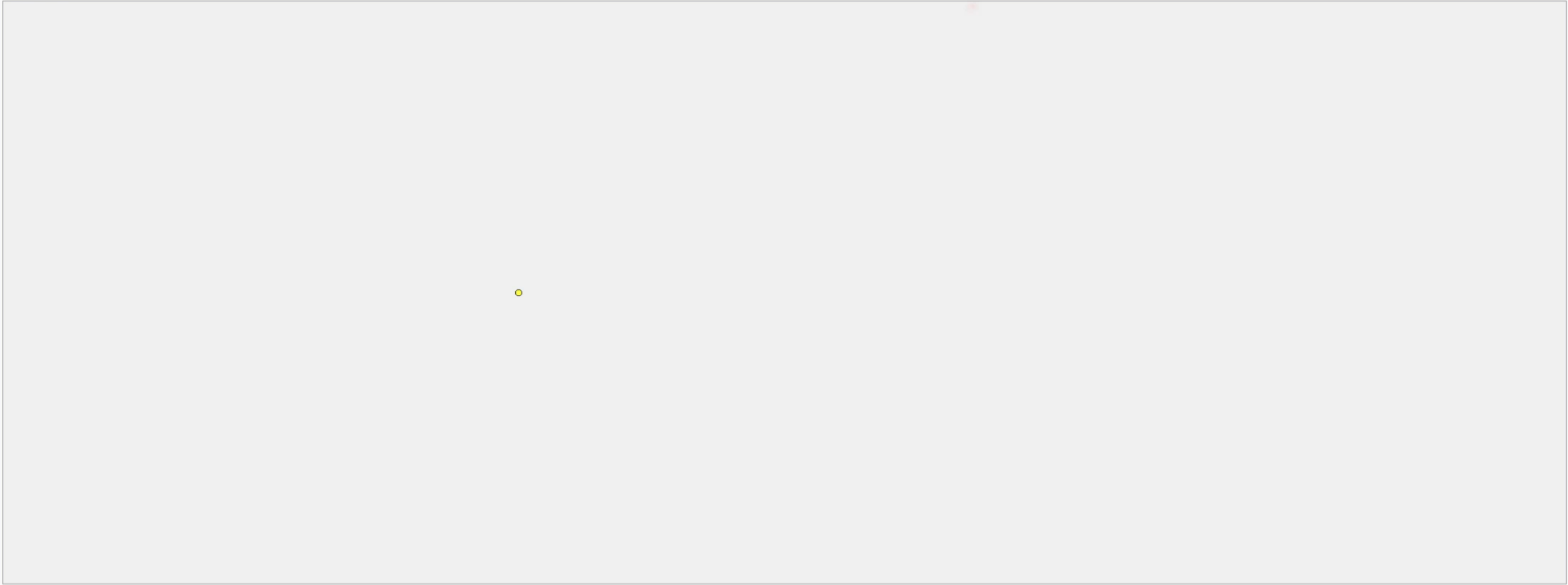
THE PYRDP CRYSTAL BALL





Speed: 1x Scale to window

Play



HOST: HOMER

USERNAME: administrator
PASSWORD: admin
DOMAIN:

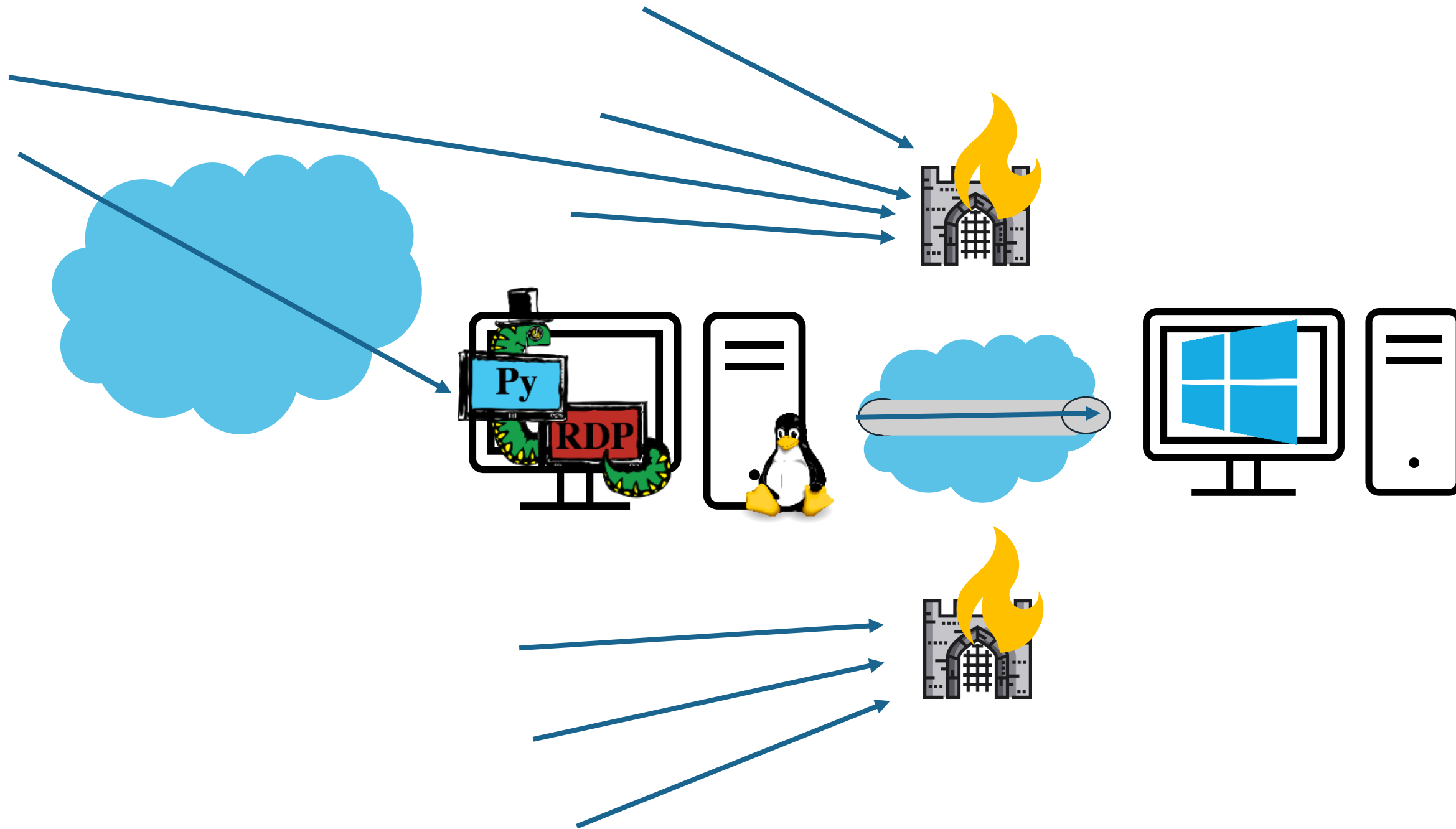


BASICALLY, SURVEILLANCE CAMERAS FOR RDP SYSTEMS



RDP HONEYPOT WITH PYRDP

Science!

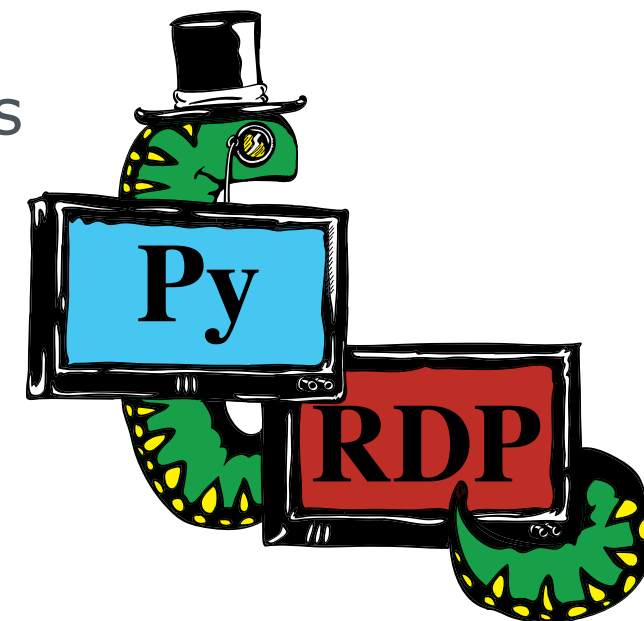


Source Code / Documentation

- <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

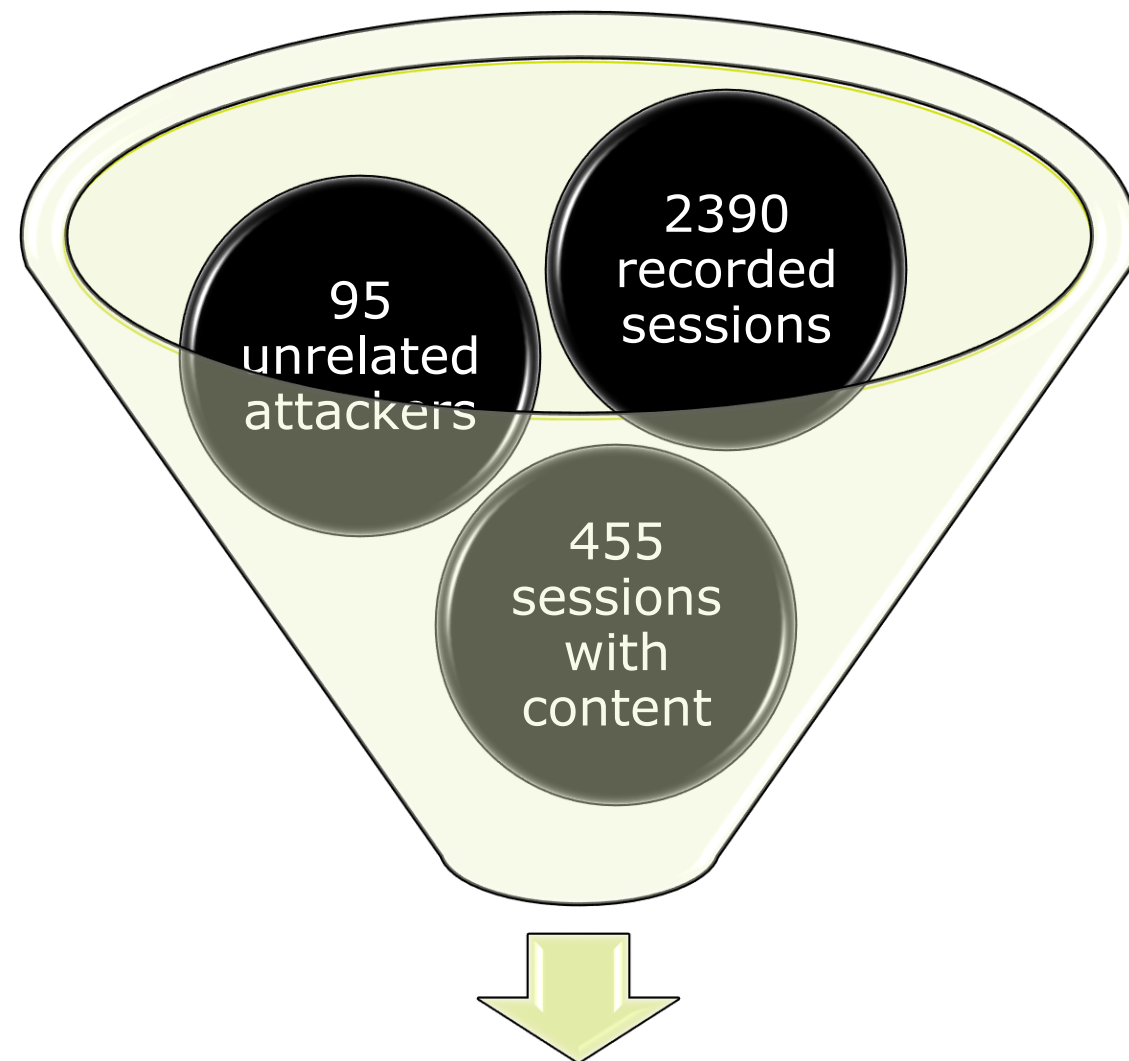
- [Introduction Blog Post](#)
- [NorthSec 2019 Talk](#)
- [BlackHat Arsenal 2019](#)
- [Blog: PyRDP on Autopilot](#)
- [DerbyCon 2019 \(Video\)](#)
- [DEFCON 28 Demo Labs](#)
- [Blog: Announcing PyRDP 1.0](#)
- [1.0 released at SecTor 2020](#)
- [BlackHat Arsenal 2021](#)
- [Purple RDP: Red and Blue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





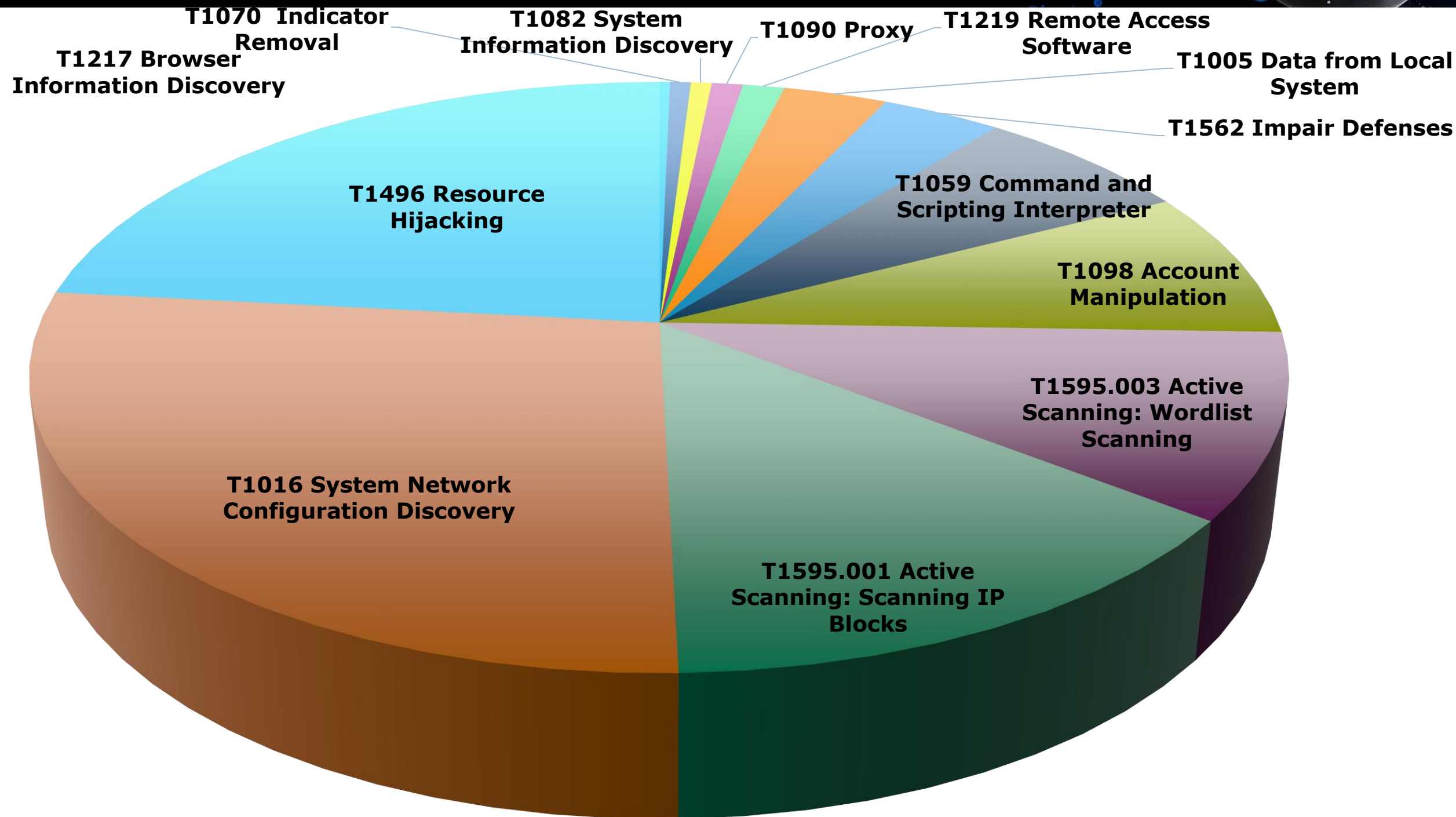
WELCOME TO THE
DUNGEON,
ADVENTURERS

 Around 100 hours
of videos analysed



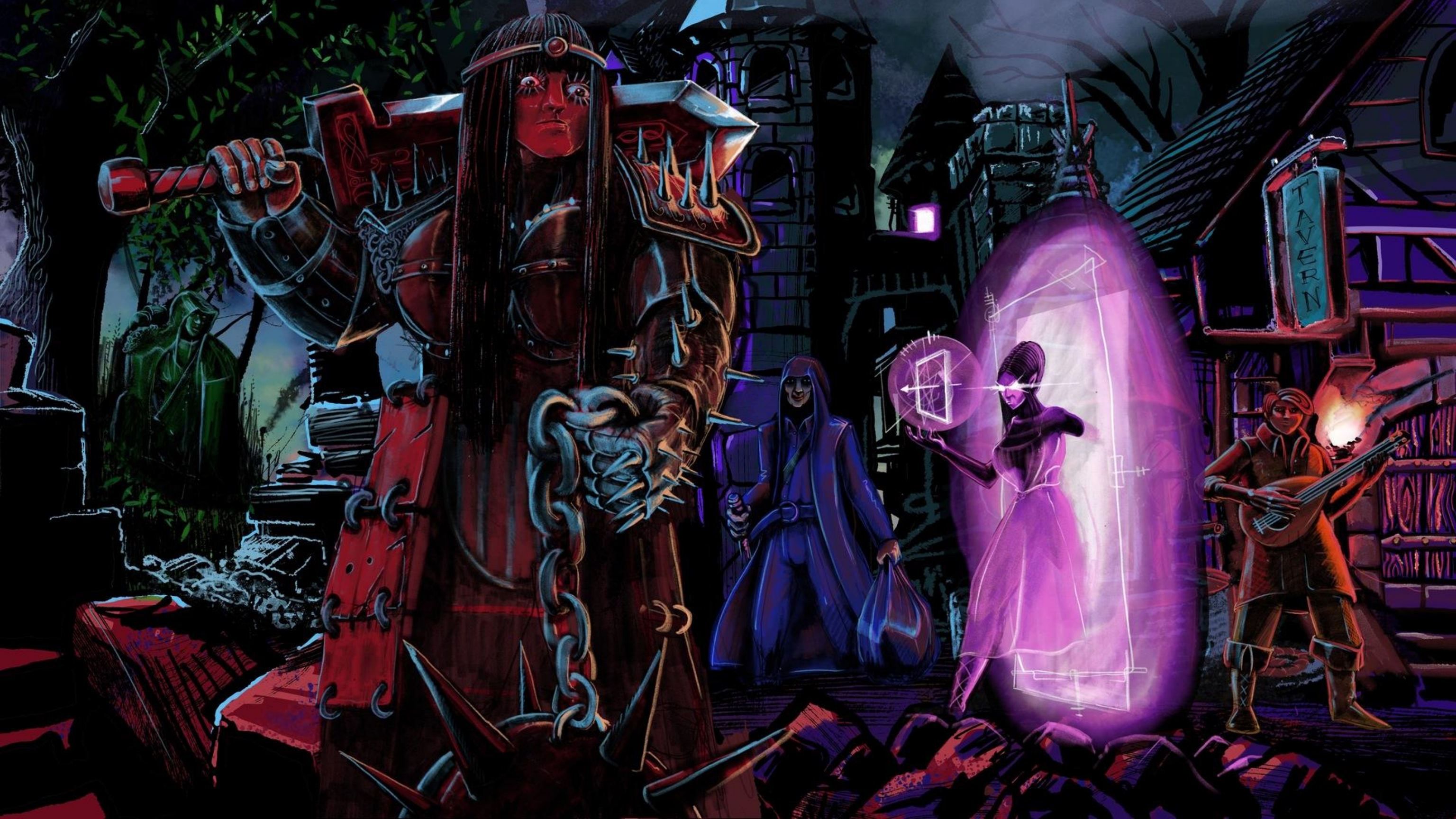
339 sessions of interest

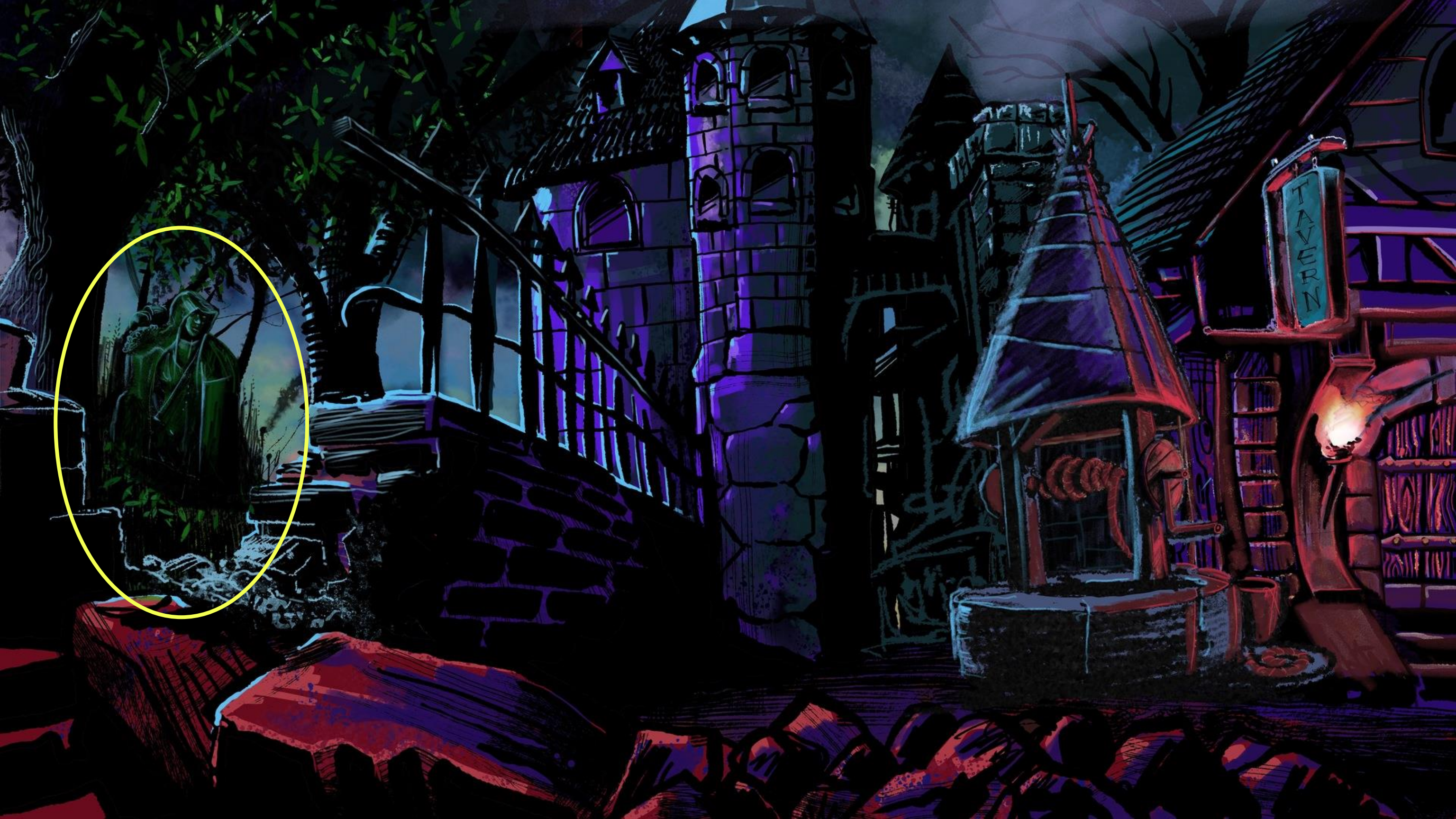
ATT&CK INDICATORS



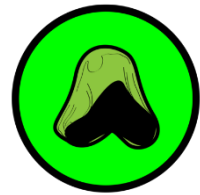


CHARACTERIZING ATTACKERS' D&D STYLE





TAVERN



RANGERS

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





Recycle Bin

EC2 Feedback

EC2 Micros...

Word

Hostname: EC2AMAZ-3IJ15JO
Instance ID: i-01312d4a89eeced55
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







THIEVES

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





THIEVES IN ACTION

Traffmonetizer

app.traffmonetizer.com/sign-in?_gl=1...

TRAFFMONETIZER

Log In

Email

Password

Forgot password

Log In

or use

G

You don't have an account? [Register Here](#)

[Terms of Service](#) | [Privacy Policy](#)

Chat with us

Privacy - Terms



Recycle Bin



EC2 Feedback



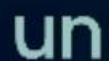
EC2 Microsoft Windows G...



Google Chrome



xmrig



unMineable Miner (M...



unMineable Miner (MFI)



ChromeSetup

Hostname: EC2AMAZ-OJK3L78

Instance ID: i-049df4c0b0dfa528c

236.56

31.32.40

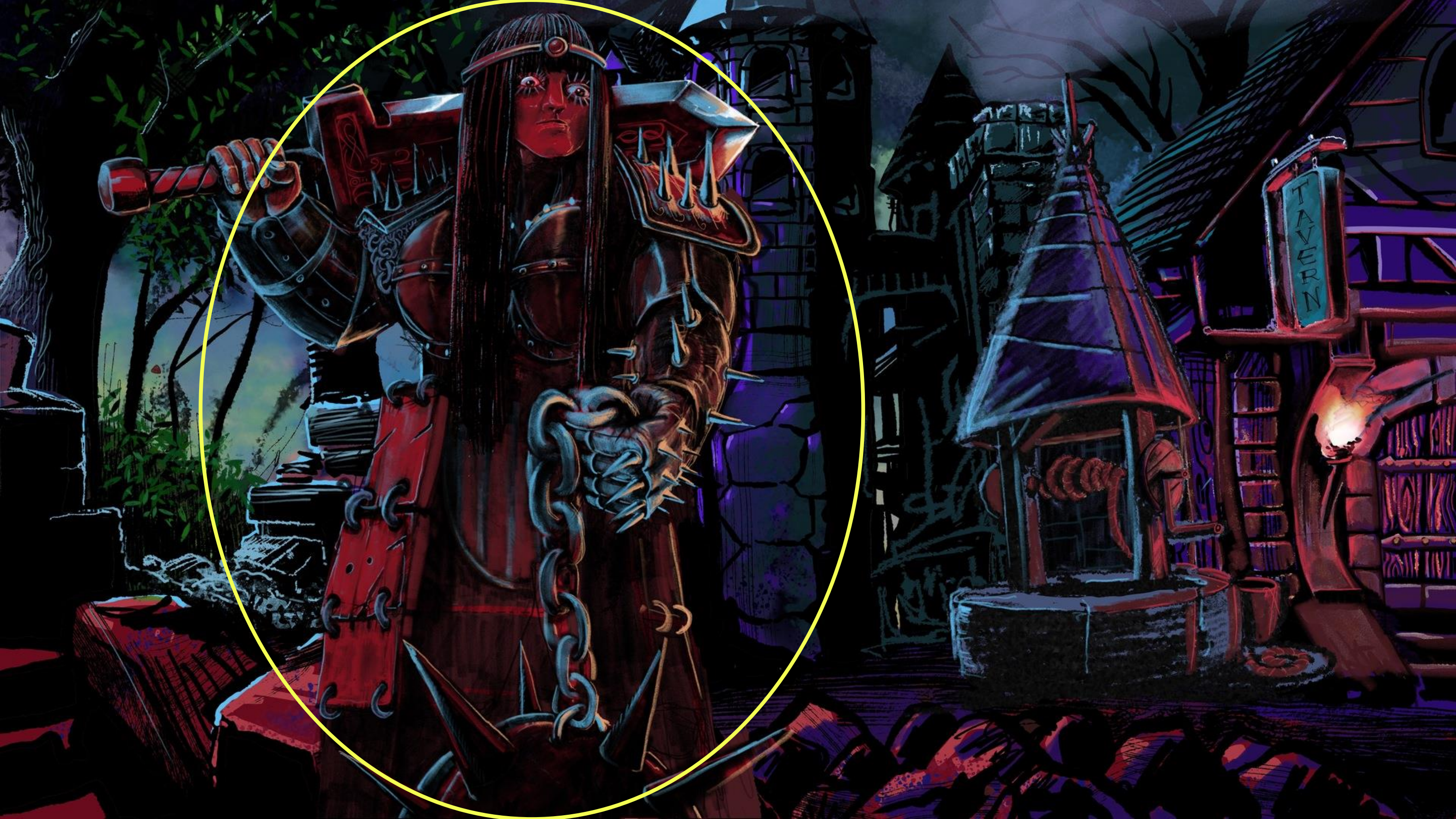
e

w to Moderate

File Explorer window titled "xmrig-6.18.0" showing the directory path: resources > miners > win32 > xmrig-6.18.0. The window contains a table of files and a tooltip for the selected file, WinRing0x64.sys.

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_ghostrider_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



TAVERN



BARBARIANS

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





The screenshot displays a Windows desktop with the following elements:

- Internet Explorer Browser:** Opened to a resource page titled "Internet Explorer Enhanced Security Configuration is enabled".
- File Explorer:** Opened to the path "This PC > Downloads > MasScan > MasScan". It shows a list of files and folders:

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

The status bar at the bottom of the File Explorer window indicates "11 items" and "1 item selected 423 KB".

- Terminal Window:** Located on the right side of the screen, displaying system information for an EC2 instance:

```
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
```






WIZARDS

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





Recycle Bin

EC2 Feedback

EC2 Micros...

mstsc - Shortcut

Remote Desktop Connection

Remote Desktop Connection

Computer: Examplecomputer.fabrikam.com

User name: None specified

The computer name field is blank. Enter a full remote computer name.

Show Options Connect Help

Hostname: EC2AMAZ-LTPPV2V
Instance ID: i-0b2165a3133c1e072
Public IPv4 Address: 18.212.55.169
Private IPv4 Address: 172.31.58.159
Instance Size: t2.micro
Availability Zone: us-east-1d
Architecture: AMD64
Total Memory: 1024 MB
Network Performance: Low to Mod

4:37 PM
8/18/2022





TAVEN





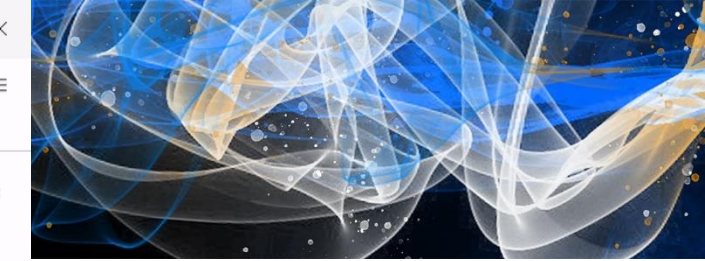
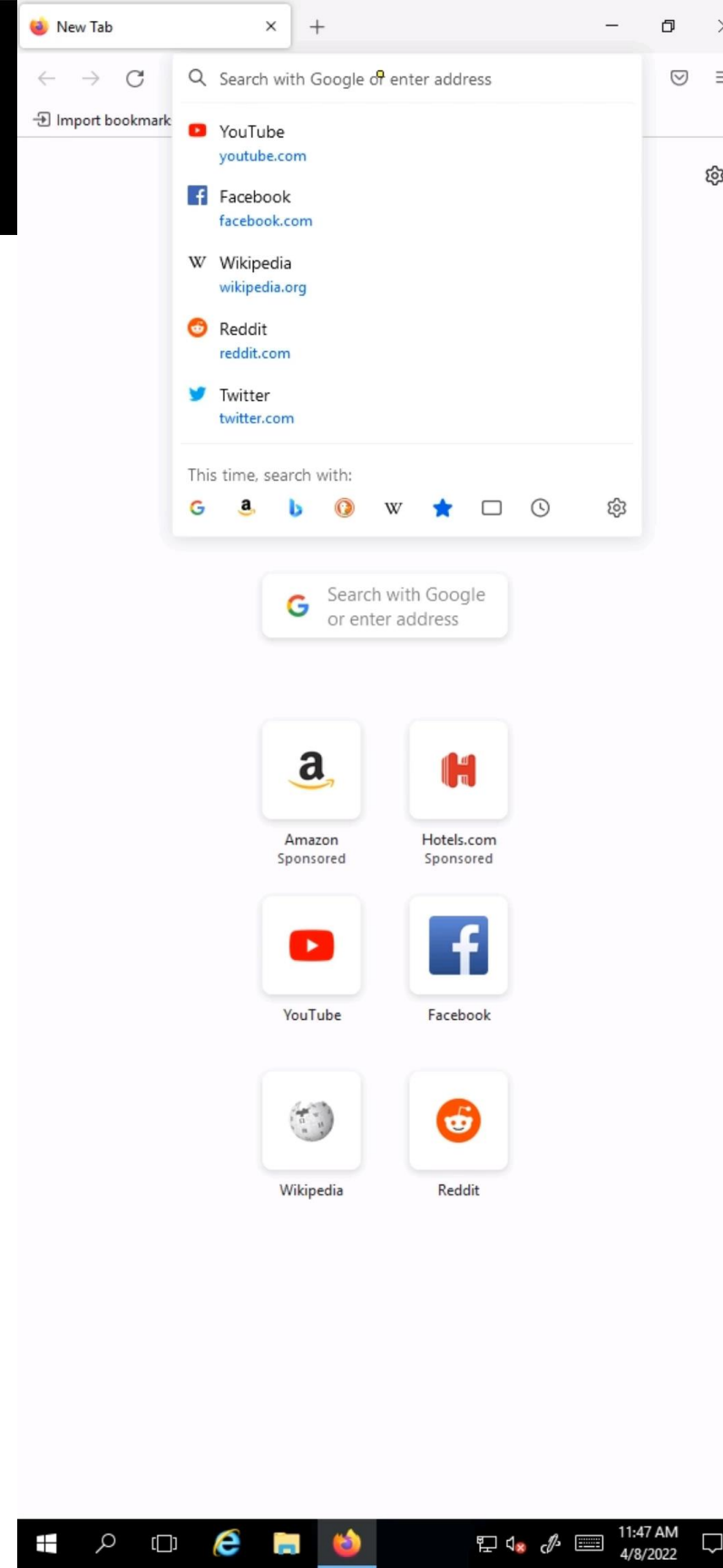
BARDS

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





BARDS IN ACTION

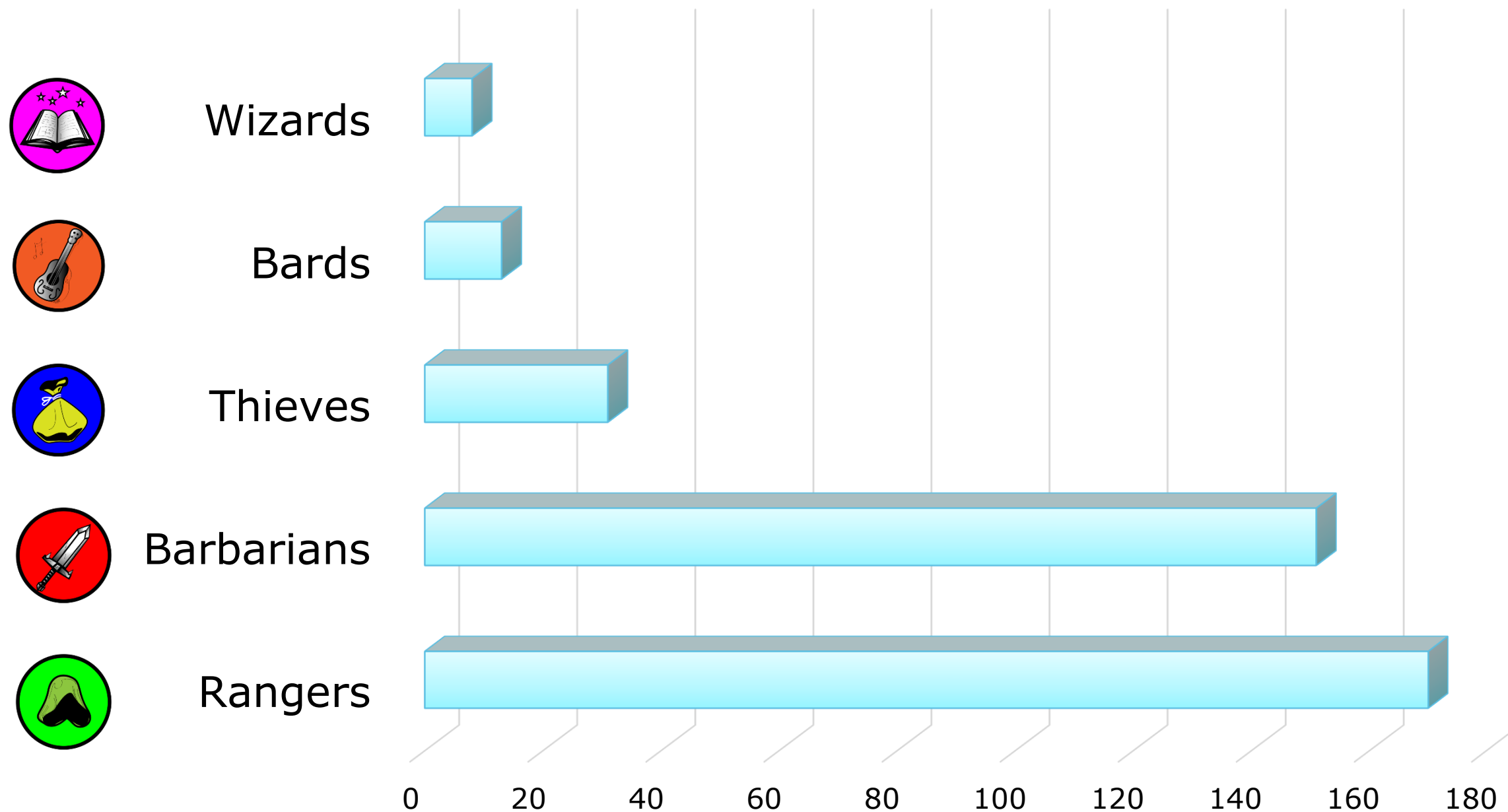




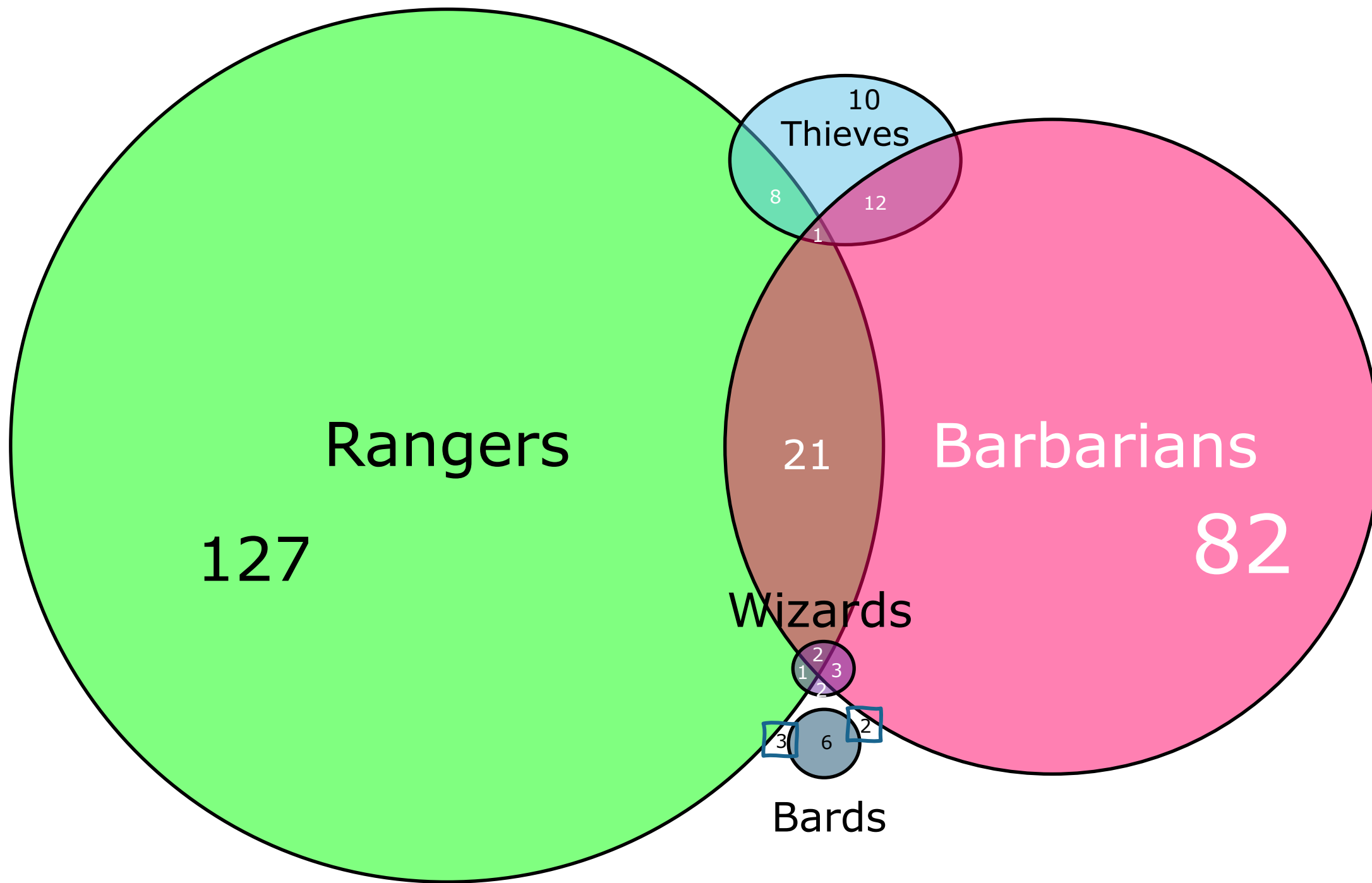
WHY P⊕RN?

Internet censorship → Ban on pornography

Number of RDP sessions associated with the profiles



ATTACKERS' OVERLAP





ATTACKERS' WEAPONRY



USED BY



ATT&CK

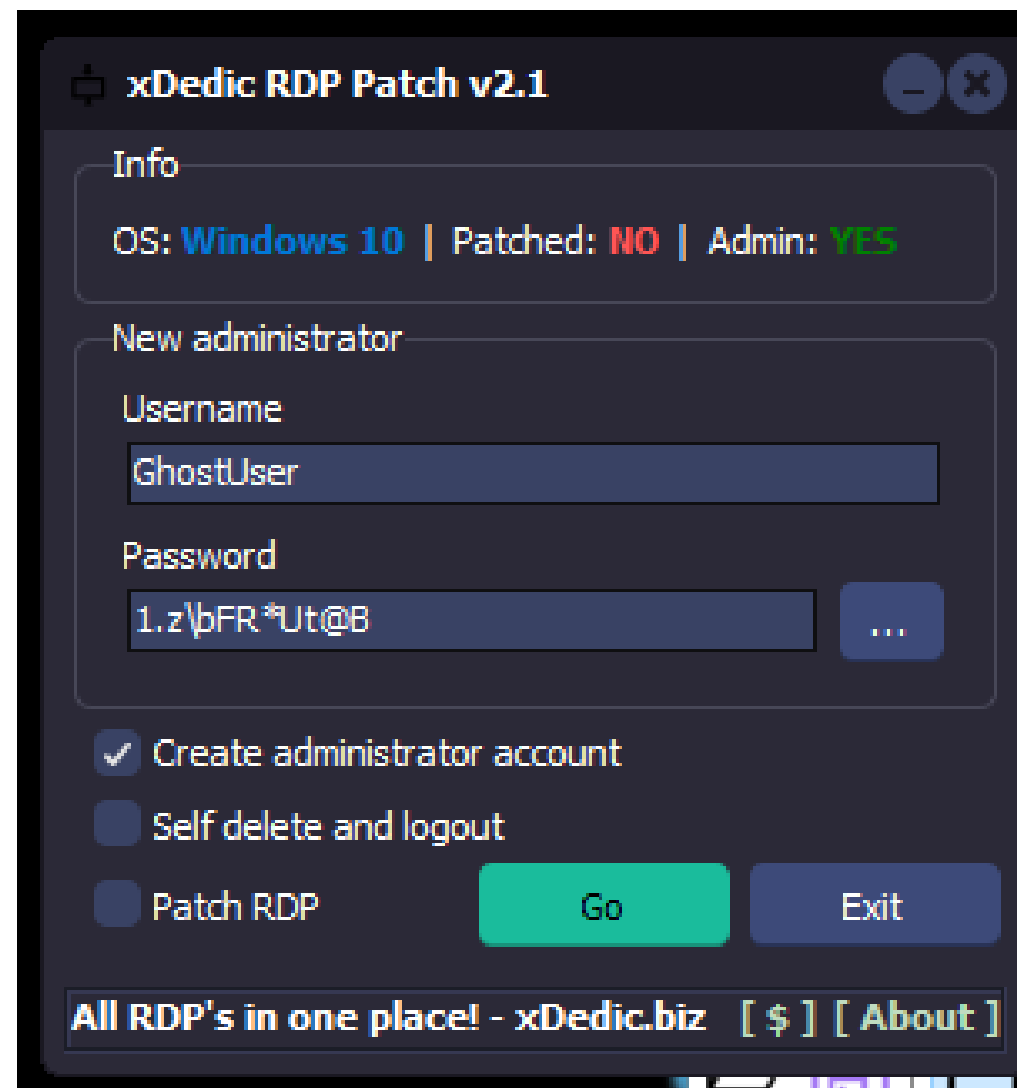
- T1098
- T1136.001
- T1543
- T1562.004
- T1556
- T1078

daddc833bffcade36b432b21046487b2
9dcd2a162d91b503334a52caee9c1fd2

SHA256-HASH

- Persistence mechanism
- Removes restrictions on non-server Windows
- Group taken down but tool still exists

DESCRIPTION



USED BY



ATT&CK

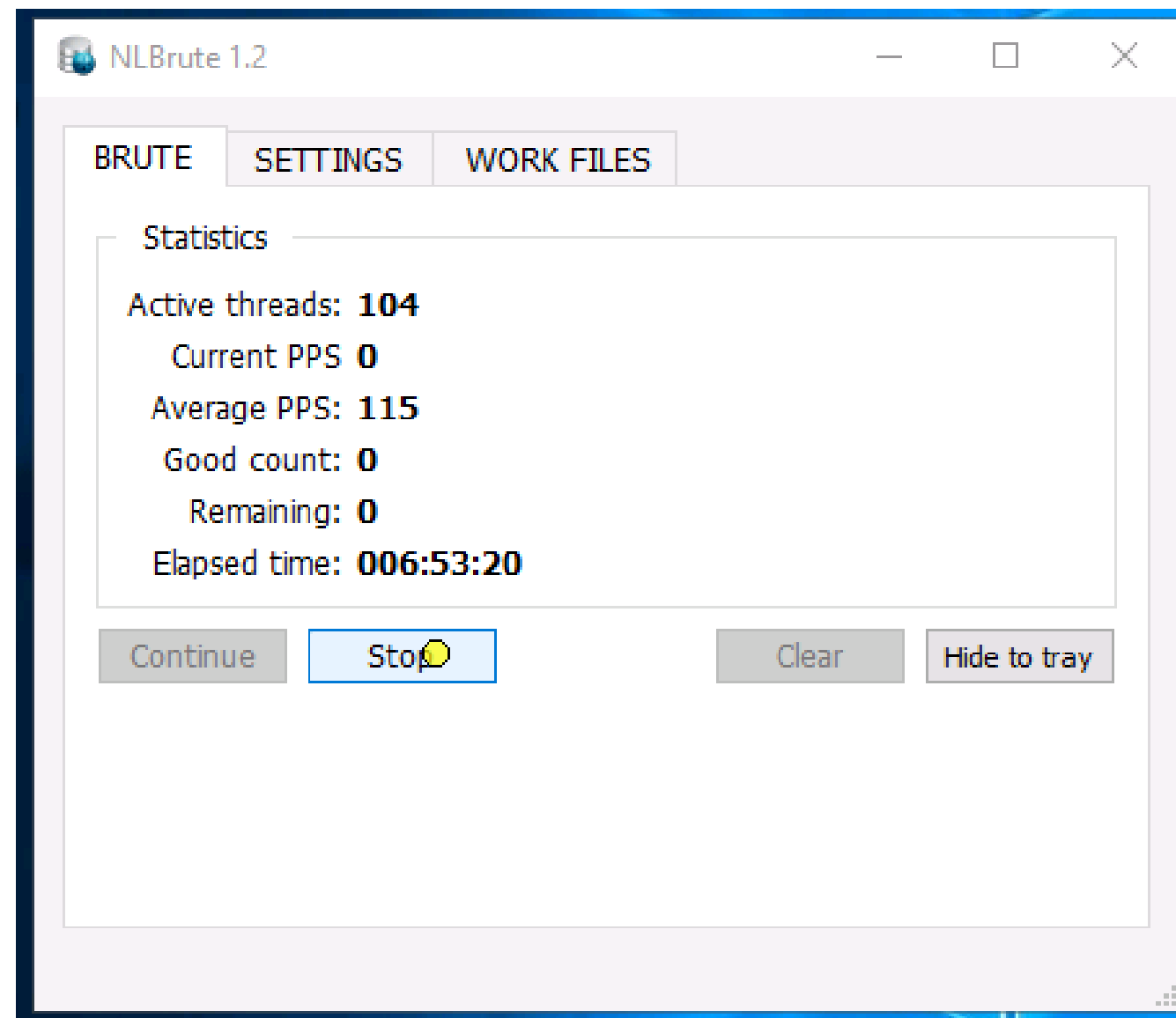
- T1133
- T1078
- T1595
- T1110

- 4e0060e367f024dae16928f3adffa79ea0ff85ac595125b3e769efc02a58af
- 1250abd2ac13d7febd8b62e8d5ec4db15ec43ff88dd2ad10ba85130869d800be
- 5187c0f887003f72bd676d0d1149c5cbcc1a69258b4bb660473dcbc170b41f0f

SHA256-HASH

- Multi-threaded brute-forcing tool dedicated to RDP
- Russian author arrested and extradited to the USA on Feb 23rd, 2023

DESCRIPTION



USED BY



ATT&CK

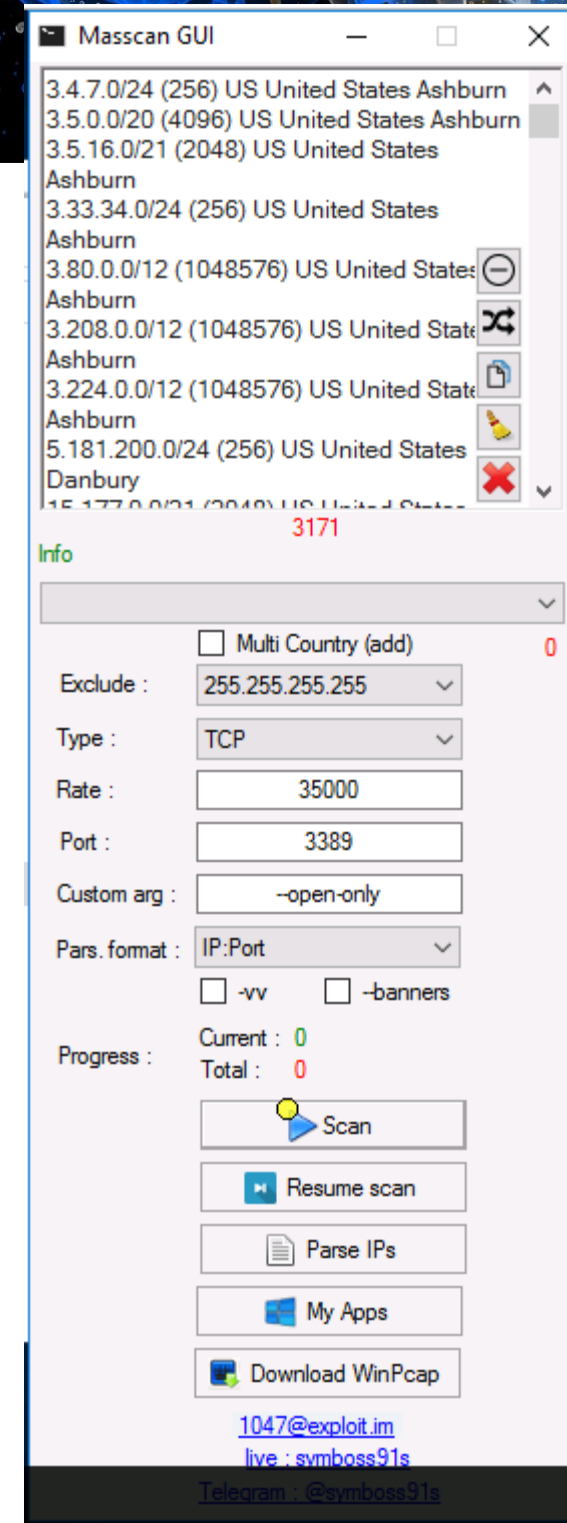
- T1133
- T1078
- T1595
- T1110

- de903a297afc249bb7d68fef6c885a4c945d740a487fe3e9144a8499a7094131
- f7f2af6f4dd9d0af03e6af3aba685969ec9ed22295055882e571bef3e96bbc4e

SHA256-HASH

- Well known tool, they use GUI wrappers
- Advanced Mode variant

DESCRIPTION





USED BY



ATT&CK

- T1595.001
- T1090
- T1119
- T0814
- T1110.004
- T1071.001

TODO

SHA256-HASH

- Proxy-first scriptable Web “testing”
- Pre-made configuration kits
- Clearly little legitimate use

DESCRIPTION

SilverBullet 1.0.0

Runner Proxies Wordlists Configs Hits DB Tools Plugins Settings Help Supporters

Start: 1 Bots: 1

Prog: 0 / 0 (0%) Prox: DEF ON OFF

Id	Data	Proxy	Status	Time	Data	Proxy	Type	Capture
----	------	-------	--------	------	------	-------	------	---------

Select CFG: None Select List: None

Runner initialized successfully!

DATA: Total: 0 Hits: 0 Custom: 0 Bad: 0 Retries: 0 To Check: 0 OCR Rate: 0%

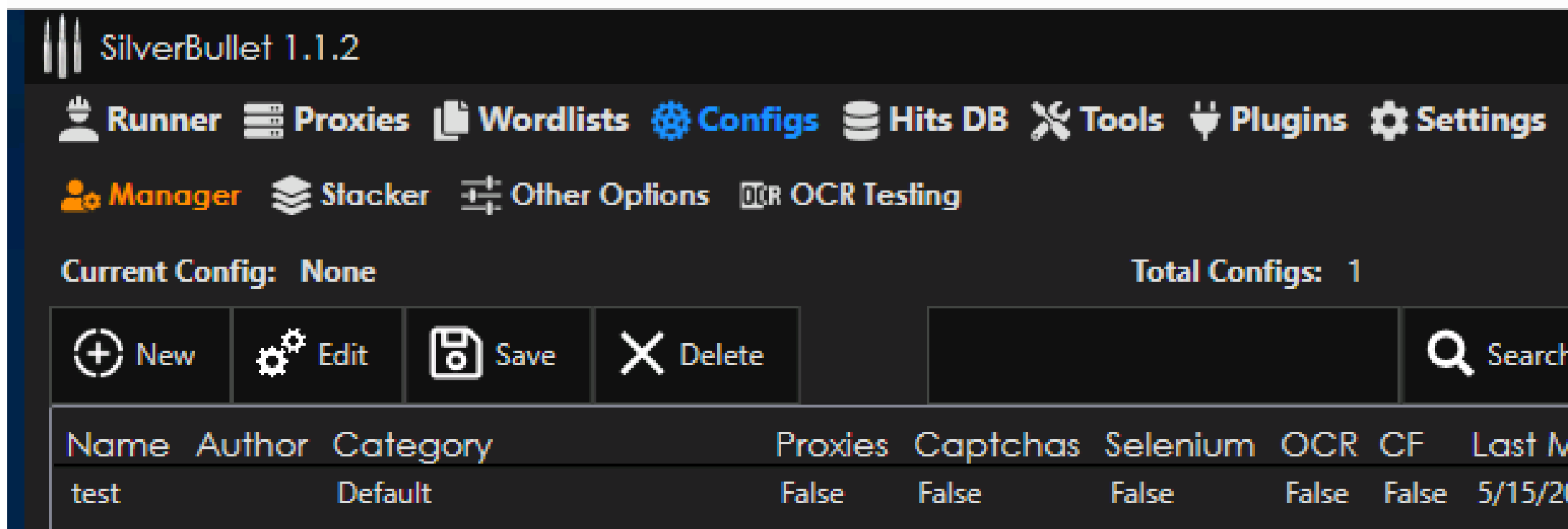
PROXIES: Total: 0 Alive: 0 Banned: 0 Bad: 0 CPM: 0 Credit: \$0

0 days 00 : 00 : 00 Unknown time left



From their website:

*OpenBullet is a webtesting suite that allows to perform requests towards a target webapp and offers a lot of tools to work with the results. This software can be used for **scraping** and **parsing data**, automated **pentesting**, unit testing through **selenium** and much more.*



SilverBullet 1.1.2

Runner Proxies Wordlists **Configs** Hits DB Tools Plugins Settings

Manager Stacker Other Options OCR OCR Testing

Current Config: None Total Configs: 1

+ New Edit Save Delete Search

Name	Author	Category	Proxies	Captchas	Selenium	OCR	CF	Last M
test		Default	False	False	False	False	False	5/15/20



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.*



**"for research
purposes only"**

cybercrime

hacking tools

WINDOWS DEFENDER REMOVE SCRIPT



USED BY



ATT&CK

- T1562
- T1518

5809c8109a48980fef1f216cc37e6aba
78cab7a75414e2687f263a539f033908

SHA256-HASH

- Leverages "install_wim_tweak.exe"
- Unhides Microsoft OS packages
- Removes Defender

DESCRIPTION

C:\Windows\system32\cmd.exe

```
-----Registry Tweak Tool v1.4.7.0-----  
-----for Windows 6.x-----  
-----Created by Michal Wnuowski-----  
-----Concept by Aviv00@msfn / lite8@MDL-----  
-----Modified by Legolash2o-----  
  
MountPath : Online  
  
-----Starting-----  
Writing to Log (Packages.txt) 3875/38750K  
-----Ending-----  
  
-----Registry Tweak Tool v1.4.7.0-----  
-----for Windows 6.x-----  
-----Created by Michal Wnuowski-----  
-----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 sucessfully.  
Removing 'Packages'... 41/44_
```


DCONTROL (AKA DEFENDERCONTROL)

USED BY



ATT&CK

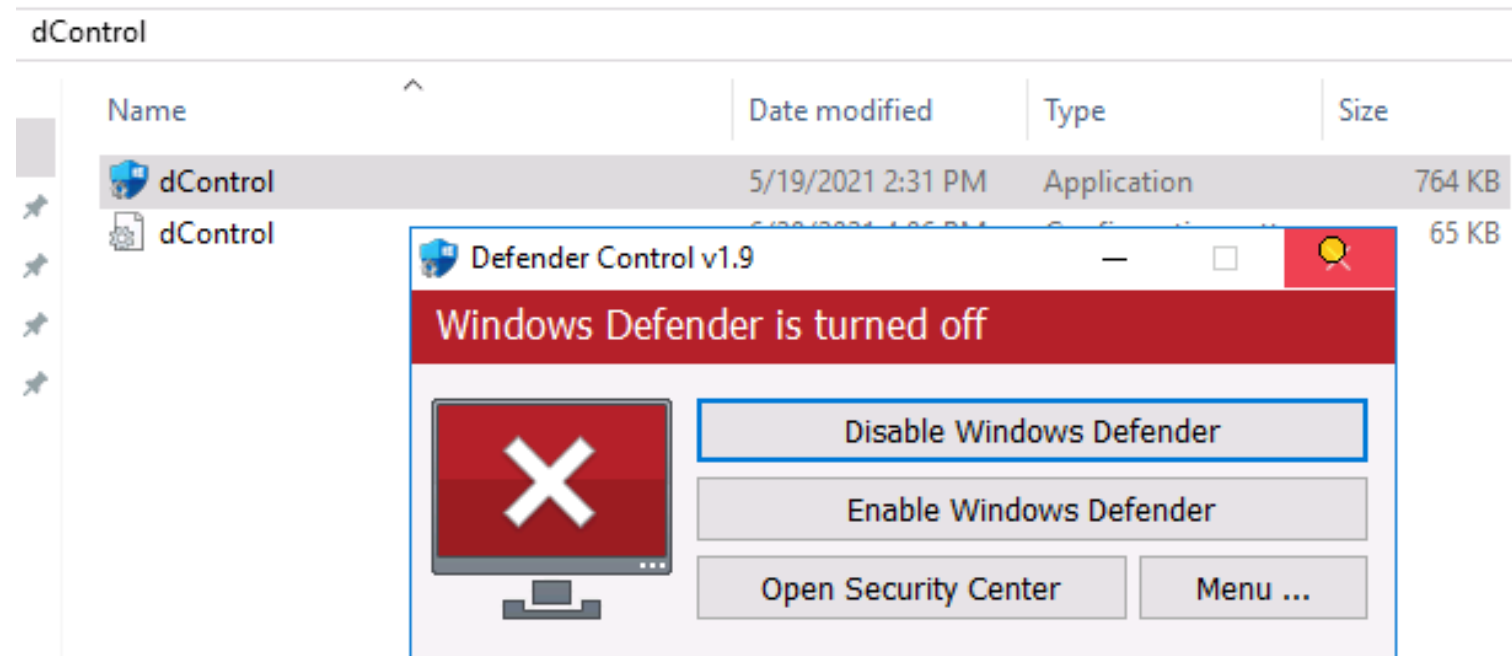
- T1562
- T1518

6606d759667fbdfaa46241db7ffb4839
d2c47b88a20120446f41e916cad77d0b

SHA256-HASH

- Disables Defender and unload its driver
- Documented by [The DFIR Report](#)

DESCRIPTION



USED BY



ATT&CK

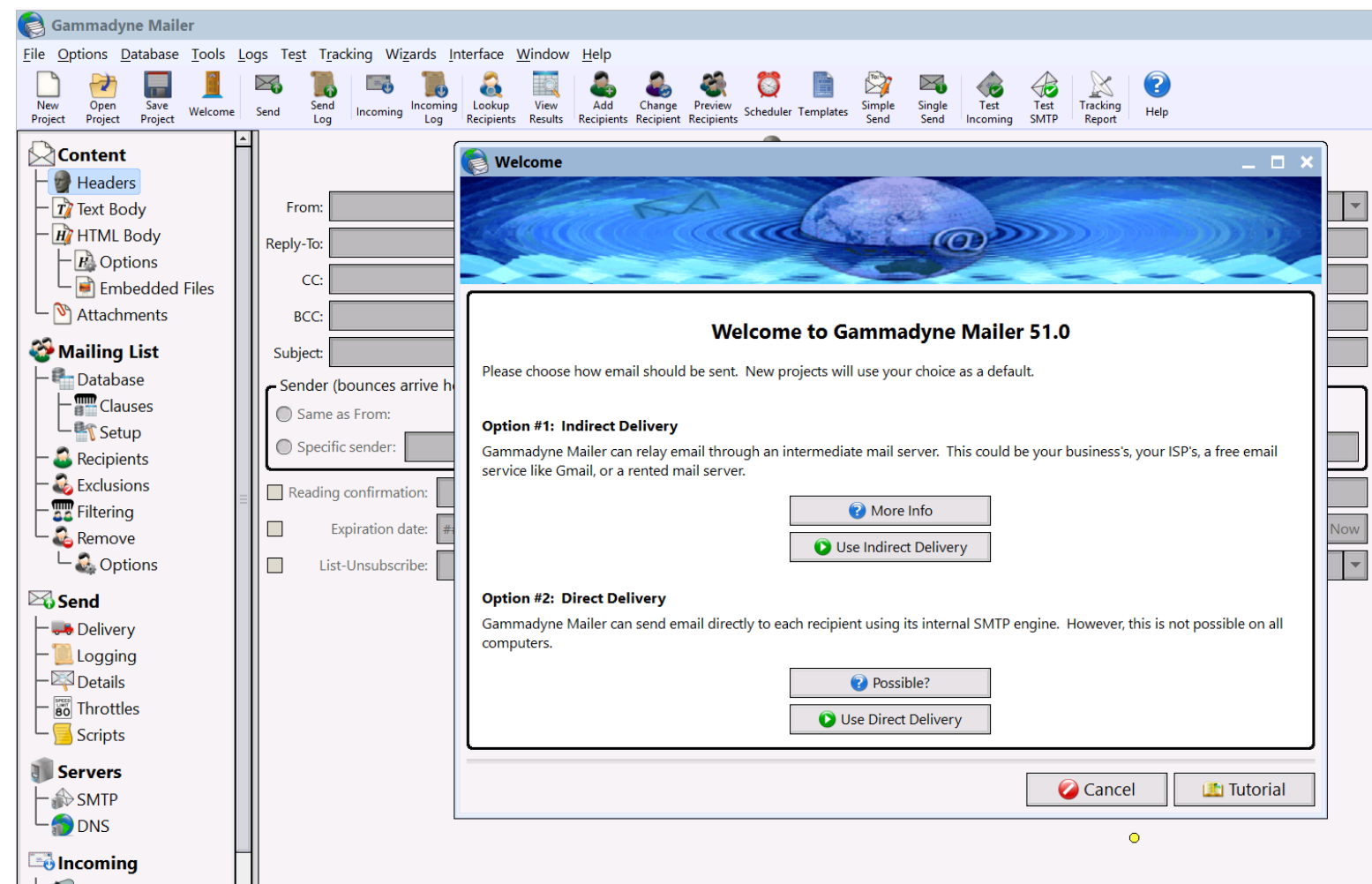
- T1598
- T1566

1883b2ab48321bdf58de973063f5a700
cfd4f39bd3b483efe314cc514ec777e3

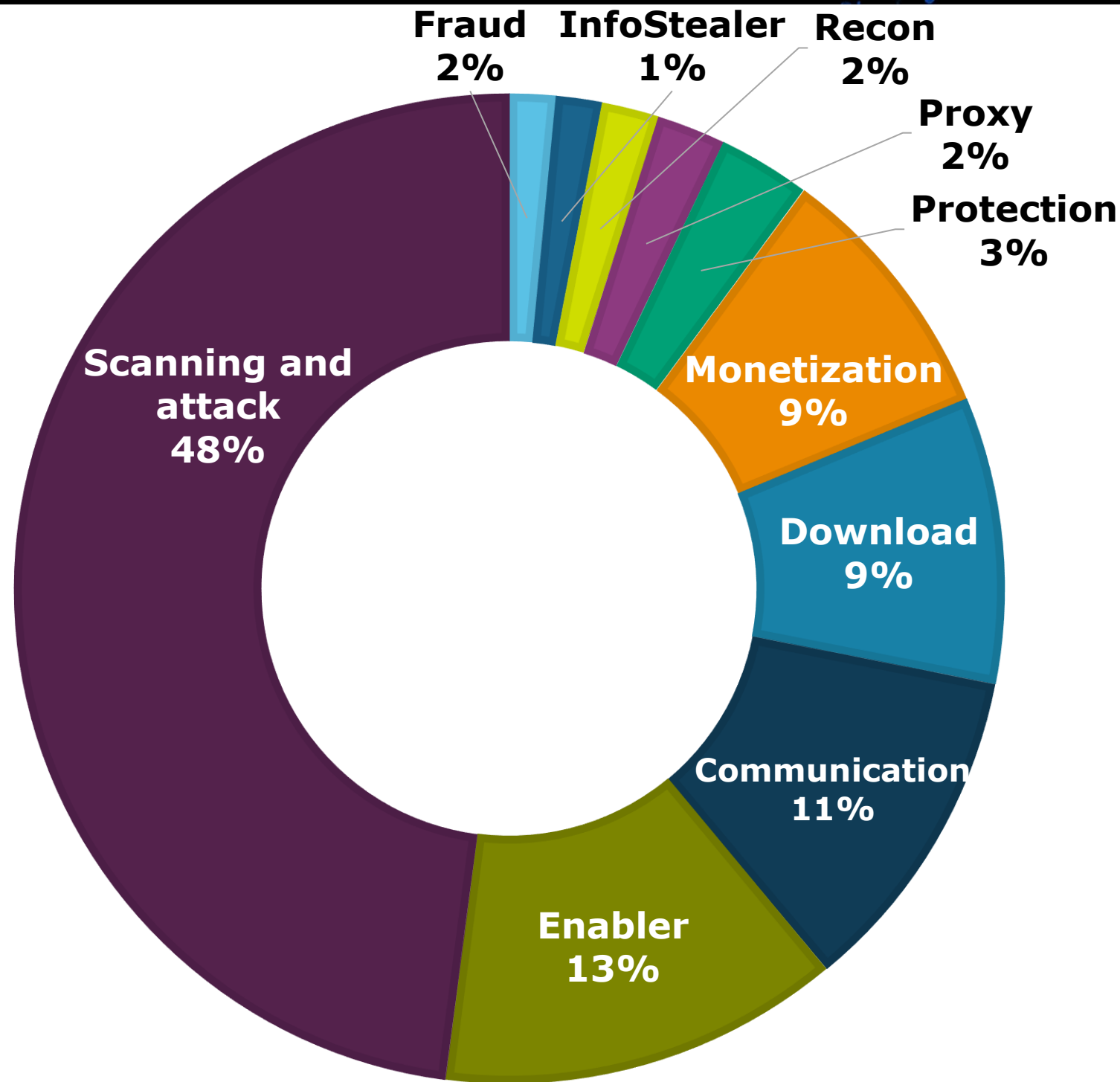
SHA256-HASH

Phishing, spearphishing and spamming
tool

DESCRIPTION



TOOL CLASSIFICATION BY OBJECTIVES



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



CRYSTAL BALL

Showing a Range of Attackers' Skills
(or lack thereof) at Work



Play

فضای رایگان آپلود فایل و آپلود عکس - PicoFile.com

NLBrute 1.2.zip

7,846 KB

لینک کوتاه جهت راحتی شما برای به یاد آوری لینک دانلود:
yon.ir/nlbrute12

با اپلیکیشن همراه من برنده 207 شو

لینک دانلود

<https://s6.picofile.com/d/8266183492/228df8aa-3e7e-4fac>

دانلود فایل

هدیه مخصوص دکتر آرام
www.Aramgroup.ir

هشدار: مسئولیت فایل آپلود شده بر عهده کاربر آپلودکننده می‌باشد، لطفا در

بلندترین شب سال
ارزانترین اینترنت سال
ADSL+ ورودیه جشنواره

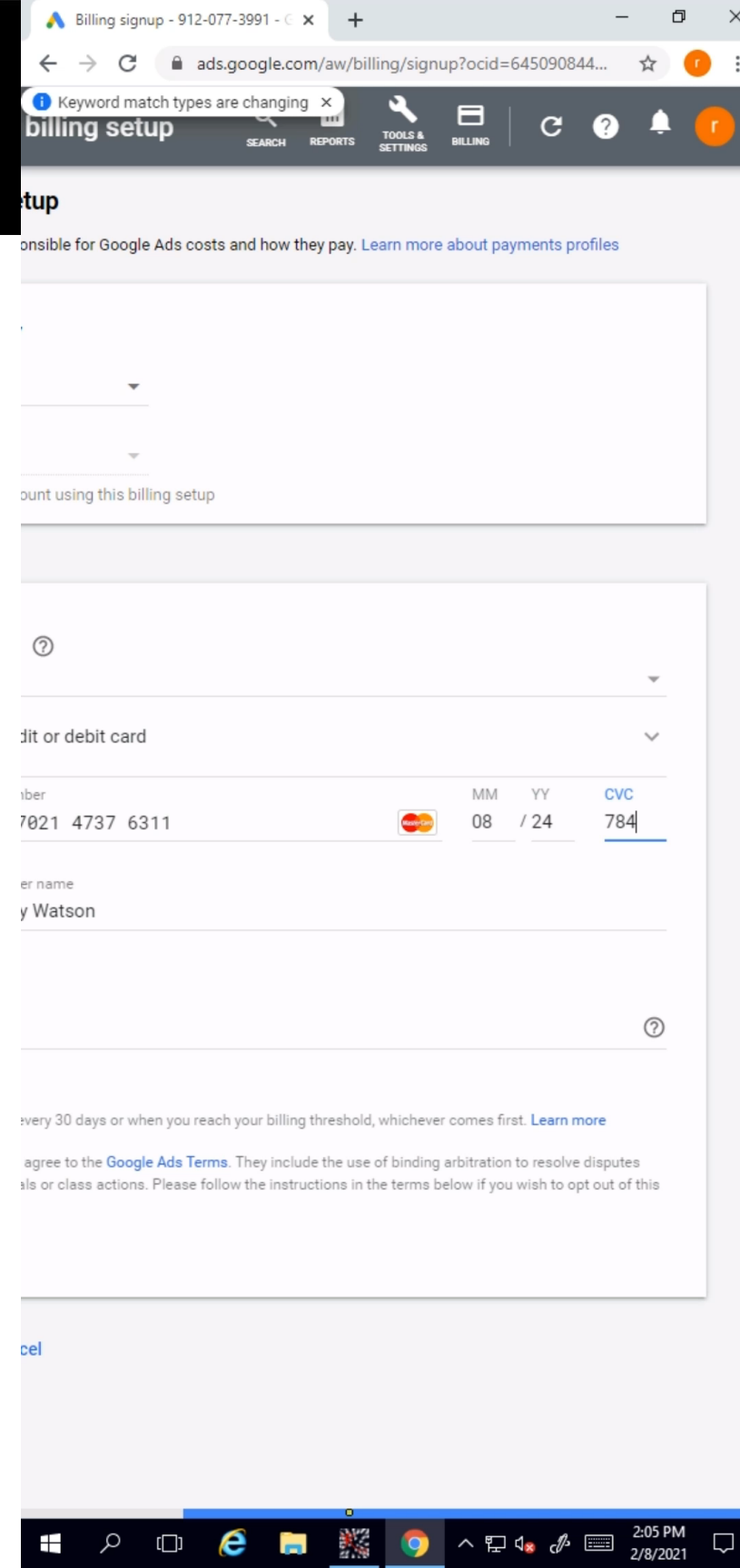
طرح تور نانو پیشگامان
اینترنت پرسرعت ADSL
۷۰۰ مگ | ۳ ماهه | ۹۹,۰۰۰ تومان دریافت سرویس

خرید بک لینک روانشناس خوب نمایشی

CLIPBOARD DATA:

CLIPBOARD DATA: لماذا حذف منہ جميع التطبيقات ❤️

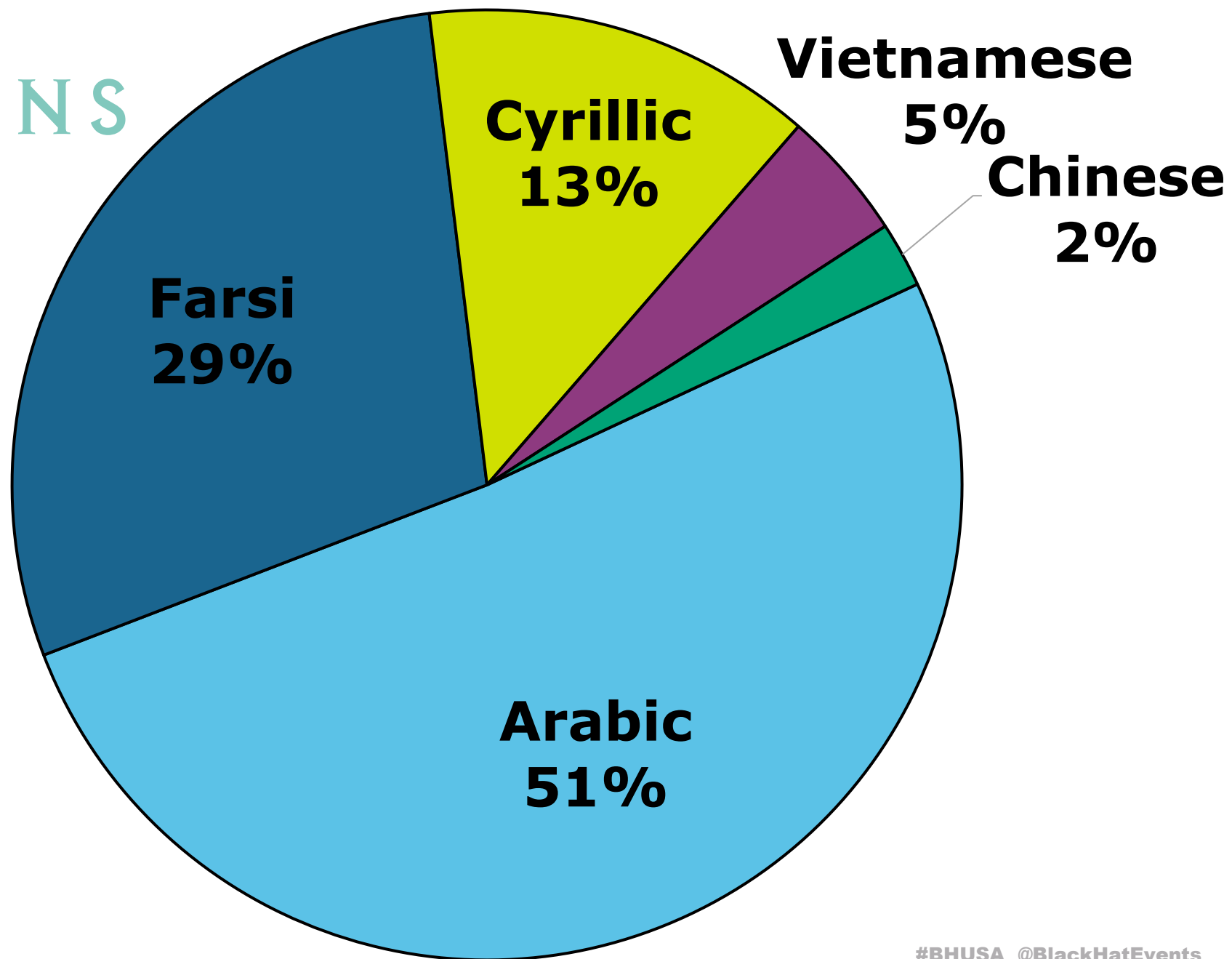
SOME ATTACKERS
DO NOT SPEAK
ENGLISH



OUR TOOL IS GREAT FOR INTEL



ALPHABET FOUND IN SESSIONS



N=45

END GAME XP AND TREASURE

The Take-Aways



THE PARTY





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

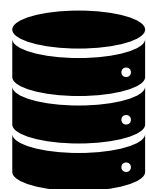
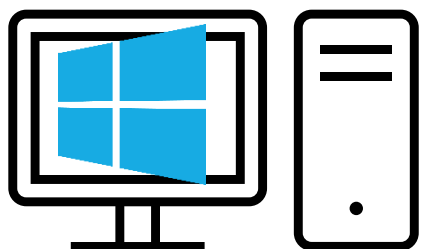
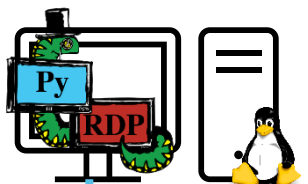
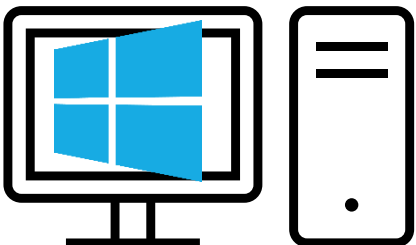
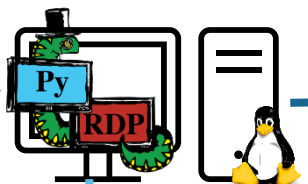
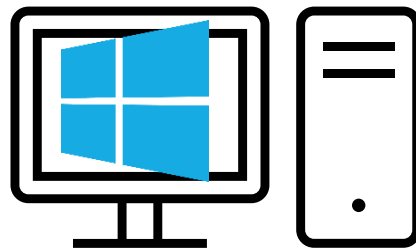
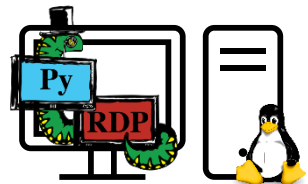
Law Enforcement: Lawfully intercept the RDP environments used by ransomware groups.

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

Honeynet Plan

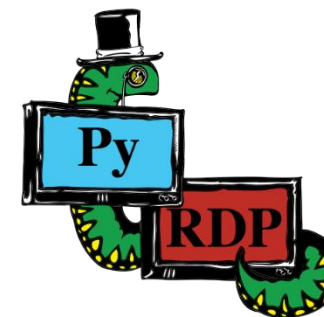


Cloud (several providers)



RabbitMQ

Science!



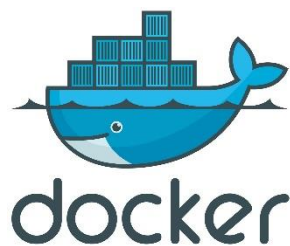
elastic



fluentd



RCLONE





PyRDP is open source

Now, our FQ RDP capture
parser 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 | aJ | client_build: 19041
0x20      44 45 53 | DES | 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 | | keyboard_function_key: 12
0x50      0c | . | ime_file_name: raw bits
0x60 | |
* |until 0x95.7 (64)
0x90      01 ca 01 | ... | code_data: raw bits
0xa0 06 ad 06 63 34 64 63 38 64 | . ..c 4 d c 8 d
* |until 0xf7.7 (98)
```




See you at the

THANK YOU! QUESTIONS?

Andréanne Bergeron

abergeron@gosecure.net

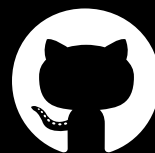


Olivier Bilodeau

obilodeau@gosecure.net
[@obilodeau](#)

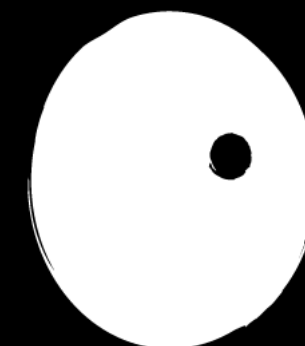


<https://gosecure.net/blog/>



<https://nsec.io>

Artwork



jeremie@tunghat.ca

#BHUSA @BlackHatEvents

