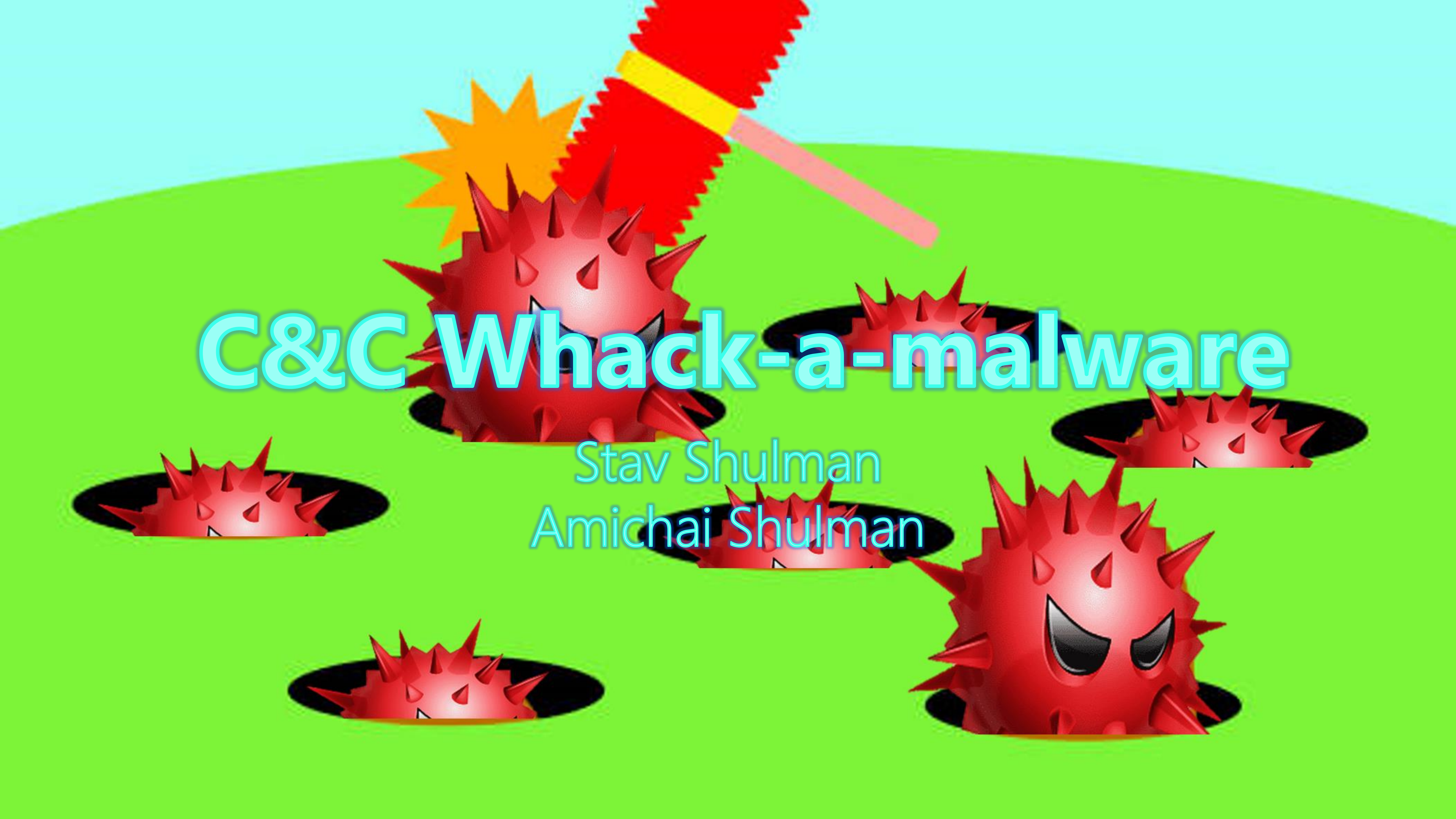
C&C Whack-a-malware

Stav Shulman
Amichai Shulman

BlueHat IL 2023



C&C Whack-a-malware

Stav Shulman
Amichai Shulman

Agenda

- Motivation
- A (short) introduction to botnets and how to fight them
- Building an uber resilient botnet
- Further research
- Conclusions

Why Botnets?

- Cyber crime in scale relies on large and functioning botnets
- Threat actors must continuously build and maintain these networks to support their ops
- Different groups and personas specialize in building this kind of infrastructure and these type of infection chains
- A robust and resilient botnet is key to the success or failure of an opperation

Motivation

- Neutralizing the botnet == destroy the operation
- Can a botnet survive “neutralizing”?
- Can a resilient botnet be cost effective?
- Can a father and daughter team survive joint research?

Basic Botnet Infrastructure

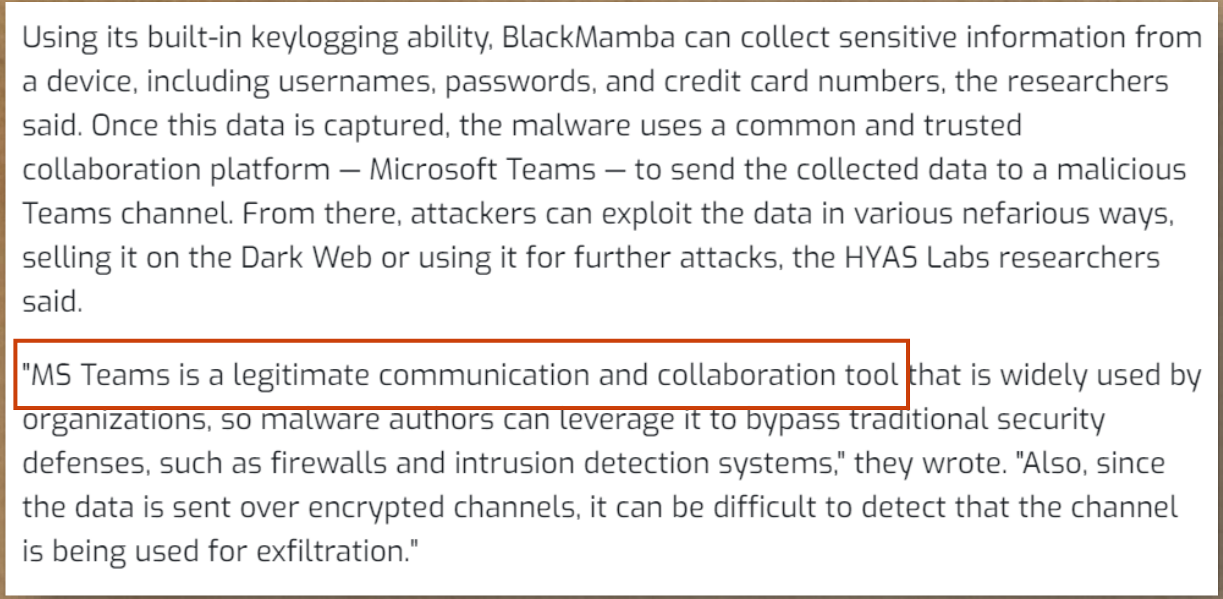
- Manually maintain a domain name pool
  - Acquire dedicated domain names
  - Abuse compromised servers
- Deliver initial domain name list to target
  - Hard coded inside the malicious binary
  - Dedicated configuration file
- Periodically update domain name list
  - Through one of the functioning domains

Mid-level Practices

- DGA
- Name generation mechanism is embedded inside the malware distribution
- Automatically register new domains as they are required

Advanced Practices

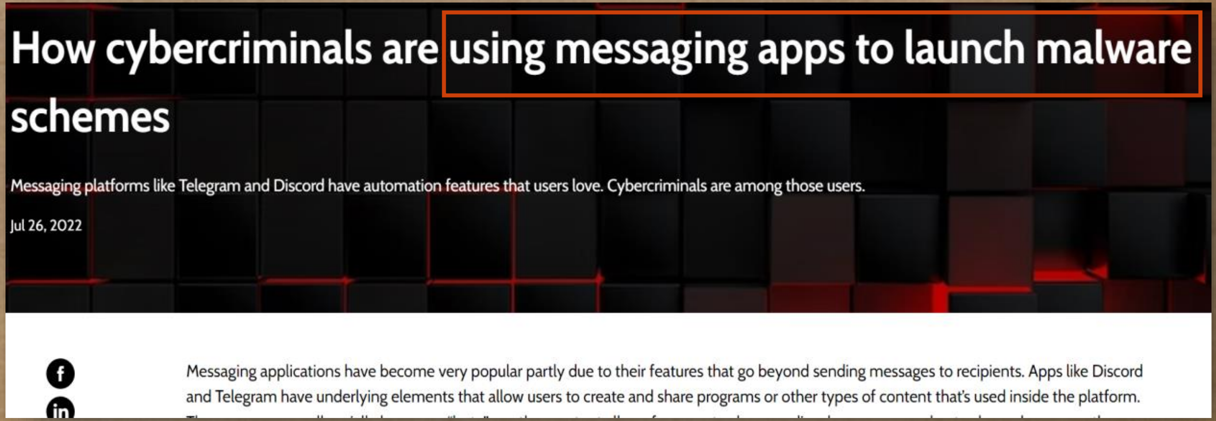
- Usage of dedicated social networking profiles
  - o Facebook, Twitter, Instagram
- Cloud based file sharing services
  - o Dropbox, Google Drive
- Communication over “legit” services and tools



Using its built-in keylogging ability, BlackMamba can collect sensitive information from a device, including usernames, passwords, and credit card numbers, the researchers said. Once this data is captured, the malware uses a common and trusted collaboration platform — Microsoft Teams — to send the collected data to a malicious Teams channel. From there, attackers can exploit the data in various nefarious ways, selling it on the Dark Web or using it for further attacks, the HYAS Labs researchers said.

"MS Teams is a legitimate communication and collaboration tool that is widely used by organizations, so malware authors can leverage it to bypass traditional security defenses, such as firewalls and intrusion detection systems," they wrote. "Also, since the data is sent over encrypted channels, it can be difficult to detect that the channel is being used for exfiltration."

Darkreading - AI-Powered 'BlackMamba' Keylogging Attack Evades Modern EDR Security



How cybercriminals are using messaging apps to launch malware schemes

Messaging platforms like Telegram and Discord have automation features that users love. Cybercriminals are among those users.

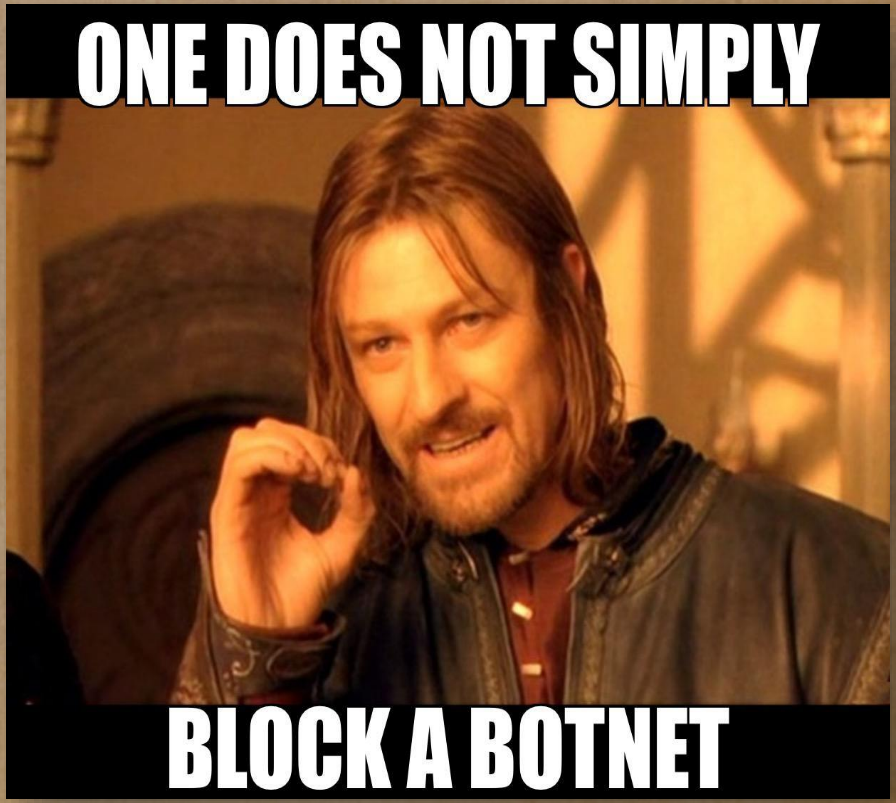
Jul 26, 2022

Messaging applications have become very popular partly due to their features that go beyond sending messages to recipients. Apps like Discord and Telegram have underlying elements that allow users to create and share programs or other types of content that's used inside the platform.

Intel471 - How cybercriminals are using messaging apps to launch malware schemes

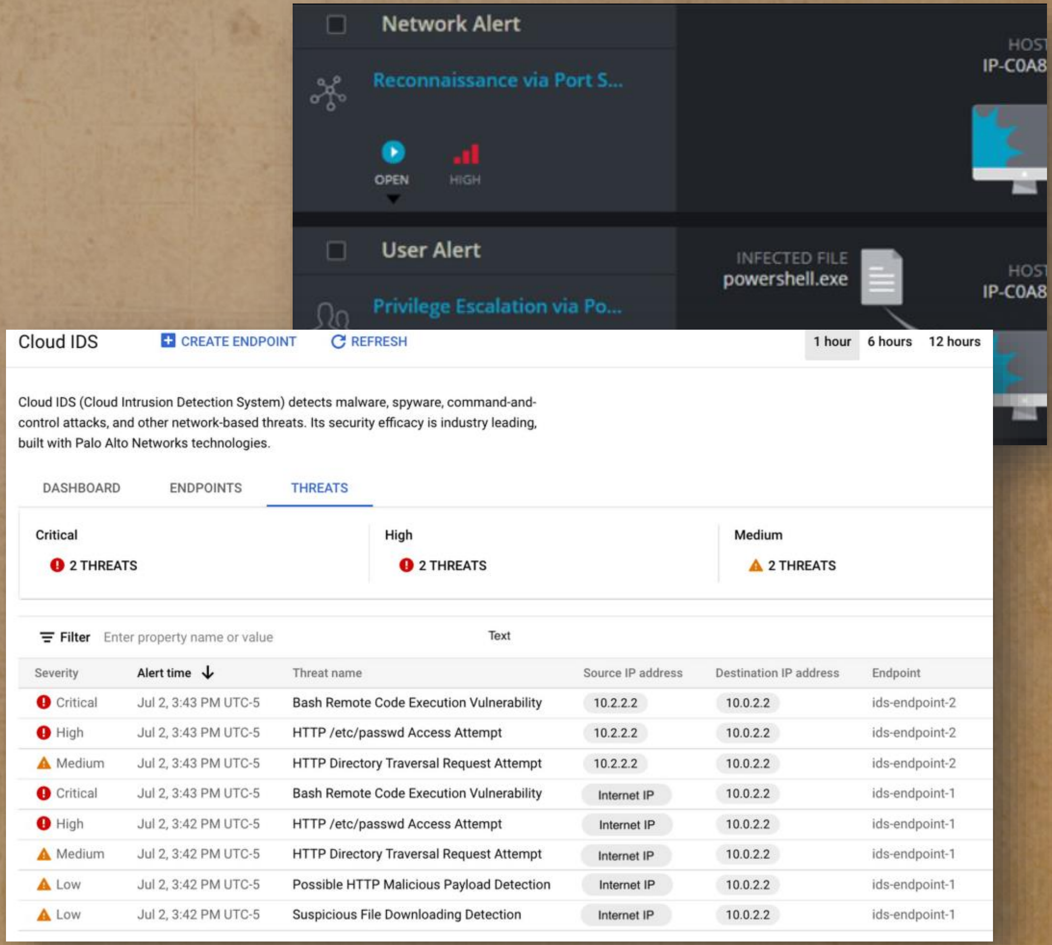
Tearing Down a Botnet

- Identify active resources
- Analyze captured samples
- Threat data enrichment
- Respond



Identify Active Resources

- Network anomalies
  - Nonstandard ports
  - Large packets
  - Strange domain names
- EDR alerts
  - Processes using unusual communication channel
- IDS alerts



Cloud IDS (Cloud Intrusion Detection System) detects malware, spyware, command-and-control attacks, and other network-based threats. Its security efficacy is industry leading, built with Palo Alto Networks technologies.

Critical	High	Medium
2 THREATS	2 THREATS	2 THREATS

Severity	Alert time ↓	Threat name	Source IP address	Destination IP address	Endpoint
Critical	Jul 2, 3:43 PM UTC-5	Bash Remote Code Execution Vulnerability	10.2.2.2	10.0.2.2	ids-endpoint-2
High	Jul 2, 3:43 PM UTC-5	HTTP /etc/passwd Access Attempt	10.2.2.2	10.0.2.2	ids-endpoint-2
Medium	Jul 2, 3:43 PM UTC-5	HTTP Directory Traversal Request Attempt	10.2.2.2	10.0.2.2	ids-endpoint-2
Critical	Jul 2, 3:43 PM UTC-5	Bash Remote Code Execution Vulnerability	Internet IP	10.0.2.2	ids-endpoint-1
High	Jul 2, 3:42 PM UTC-5	HTTP /etc/passwd Access Attempt	Internet IP	10.0.2.2	ids-endpoint-1
Medium	Jul 2, 3:42 PM UTC-5	HTTP Directory Traversal Request Attempt	Internet IP	10.0.2.2	ids-endpoint-1
Low	Jul 2, 3:42 PM UTC-5	Possible HTTP Malicious Payload Detection	Internet IP	10.0.2.2	ids-endpoint-1
Low	Jul 2, 3:42 PM UTC-5	Suspicious File Downloading Detection	Internet IP	10.0.2.2	ids-endpoint-1

Analyze Captured Samples

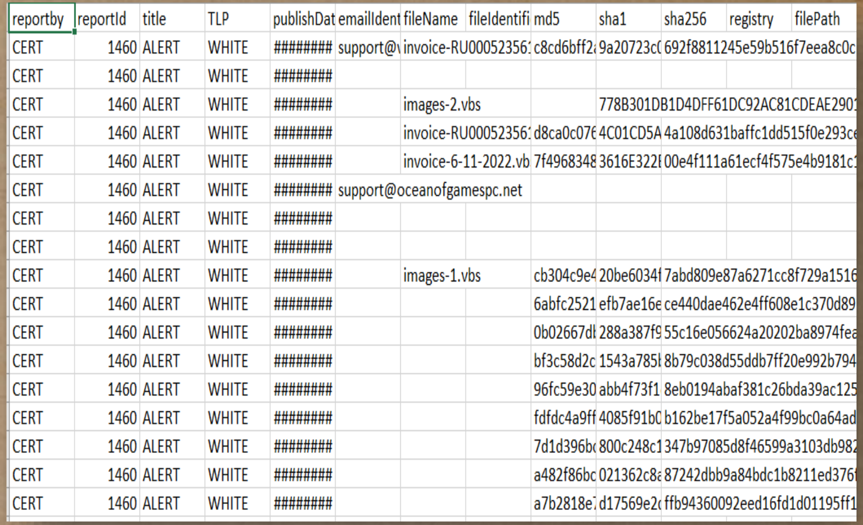
- Static analysis
- Dynamic analysis
- Extract more resources / algorithms

Threat Data Enrichment

- Identify domain registration patterns
- Detect distinct paths and content on hacked servers
- Identification of certificates

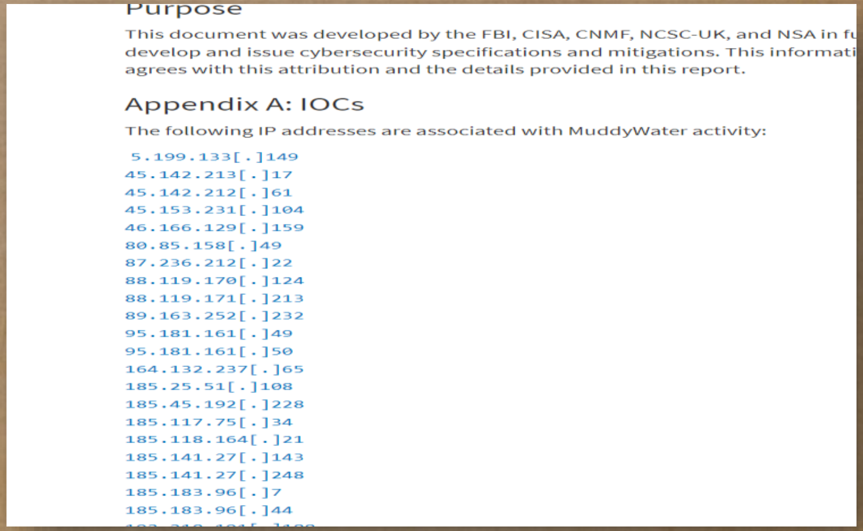
Respond

- IOC - Denylisting of network resources
  - Domain names
  - URI paths
  - URI parameters
- Sink-holes
  - Take over domain names
  - Take over unprotected C&C servers
- Removal (client and server)
  - Remove (or ban) accounts
  - Identify all infected hosts



reportby	reportId	title	TLP	publishDat	emailIdent	fileName	fileIdentifi	md5	sha1	sha256	registry	filePath
CERT	1460	ALERT	WHITE	########	support@v	invoice-RU00052356		c8cd6bff2a	9a20723c(	692f8811245e59b516f7eea8c0c		
CERT	1460	ALERT	WHITE	########								
CERT	1460	ALERT	WHITE	########		images-2.vbs			778B301DB1D4DFF61DC92AC81CDEAE2901			
CERT	1460	ALERT	WHITE	########		invoice-RU00052356		d8ca0c076	4C01CD5A	4a108d631baffc1dd515f0e293ce		
CERT	1460	ALERT	WHITE	########		invoice-6-11-2022.vb		7f4968348	3616E322I	00e4f111a61ecf4f575e4b9181c1		
CERT	1460	ALERT	WHITE	########	support@oceanofgamespc.net							
CERT	1460	ALERT	WHITE	########								
CERT	1460	ALERT	WHITE	########								
CERT	1460	ALERT	WHITE	########		images-1.vbs		cb304c9e4	20be6034f	7abd809e87a6271cc8f729a1516		
CERT	1460	ALERT	WHITE	########				6abfc2521	efb7ae16e	ce440dae462e4ff608e1c370d89		
CERT	1460	ALERT	WHITE	########				0b02667dl	288a387f9	55c16e056624a20202ba8974fea		
CERT	1460	ALERT	WHITE	########				bf3c58d2c	1543a785l	8b79c038d55ddb7ff20e992b794		
CERT	1460	ALERT	WHITE	########				96fc59e30	abb4f73f1	8eb0194abaf381c26bda39ac125		
CERT	1460	ALERT	WHITE	########				fdfdc4a9ff	4085f91b0	b162be17f5a052a4f99bc0a64ad		
CERT	1460	ALERT	WHITE	########				7d1d396b(	800c248c1	347b97085d8f46599a3103db982		
CERT	1460	ALERT	WHITE	########				a482f86bc	021362c8a	87242dbb9a84bdc1b8211ed376		
CERT	1460	ALERT	WHITE	########				a7b2818e7	d17569e2(	ffb94360092eed16fd1d01195ff1		

CERT IL: alert_1460c



Purpose

This document was developed by the FBI, CISA, CNMF, NCSC-UK, and NSA in fu develop and issue cybersecurity specifications and mitigations. This informati agrees with this attribution and the details provided in this report.

Appendix A: IOCs

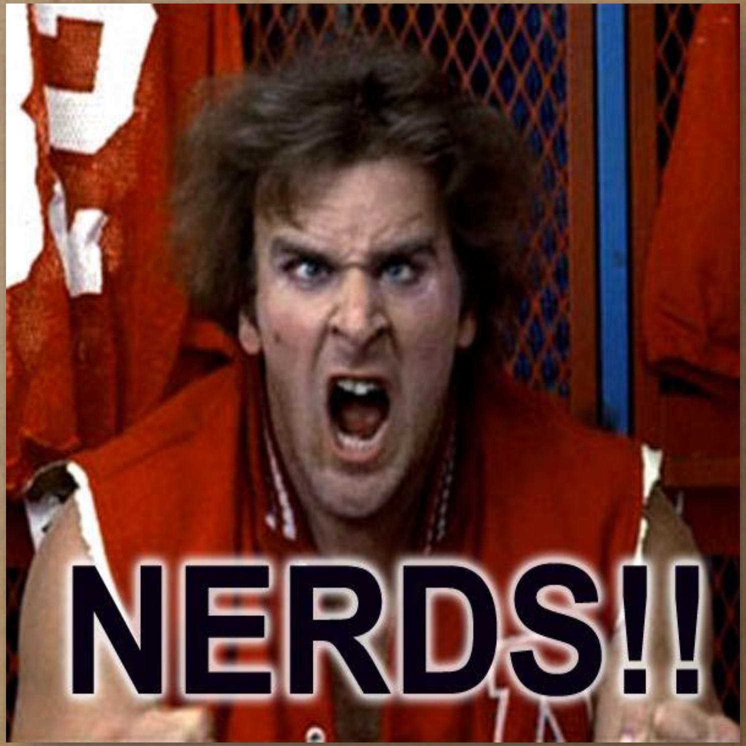
The following IP addresses are associated with MuddyWater activity:

```
 5.199.133[.]149
45.142.213[.]17
45.142.212[.]61
45.153.231[.]104
46.166.129[.]159
80.85.158[.]49
87.236.212[.]22
88.119.170[.]124
88.119.171[.]213
89.163.252[.]232
95.181.161[.]49
95.181.161[.]50
164.132.237[.]65
185.25.51[.]108
185.45.192[.]228
185.117.75[.]34
185.118.164[.]21
185.141.27[.]143
185.141.27[.]248
185.183.96[.]7
185.183.96[.]44
```

CISA: Alert (AA22-055A)

Researchers are Winning!

- Domain registration is expensive at scale
- Domain registration is traceable at scale
- New account registration for Google / Dropbox / etc. is very labor intensive and does not scale
- Network traffic uniquely identified and blocked



Researchers are Winning!

- When a sample is captured, further registration of similar samples is denied
- When IOCs are put in place, existing bots can no longer communicate with the botnet
- When servers are taken down, the new botnet infrastructure will not be able to communicate with existing bots

Researchers Lose to State Sponsored Actors

- Resource overflow
  - Endless budget
  - Abundance of HC
- Defy gravity
  - Create identities and resources at a gigantic scale

Power to the People!

- Creating a botnet infrastructure for your everyday hacker
- Rely on public infrastructure
- Indistinguishable from legitimate traffic
- Individual bots never die
- Cheap!

Not the Right Way

- Block Chain based infrastructure
    - Noisy and expensive

- Individual bots register to a service
    - Complex
    - Way too expensive
- Off brand services
    - Easily identified and blocked

Maybe the Right Way

Discord

Trello

- Single account used for distributing individual accounts
- Find a service with lax registration process (e.g. accepts ProtonMail)
- Initial sample contains credentials of a bootstrap account
- Backend generates a pool of individual accounts
- Upon infection a bot communicates through the bootstrap account to receive an individual account

Maybe Not?

Pros

- Two-way communication
- Bots survive a takedown of the bootstrap account
- Bots can survive a takedown of their individual account

Cons

- Sample must be replaced if bootstrap account is taken down
- Account creation is still a hassle
- Botnet is vulnerable to account exhaustion attack

When you don’t know something just Google it!

Epiphany

- Bots do not know the **C&C**
- Bots know how to **SEARCH** for the **C&C**
- Bots know a **C&C** when they **C** one
- **SEARCH** terms are always **legit**… Right?

A Guide to Becoming a Malware Lord

Gather your minions

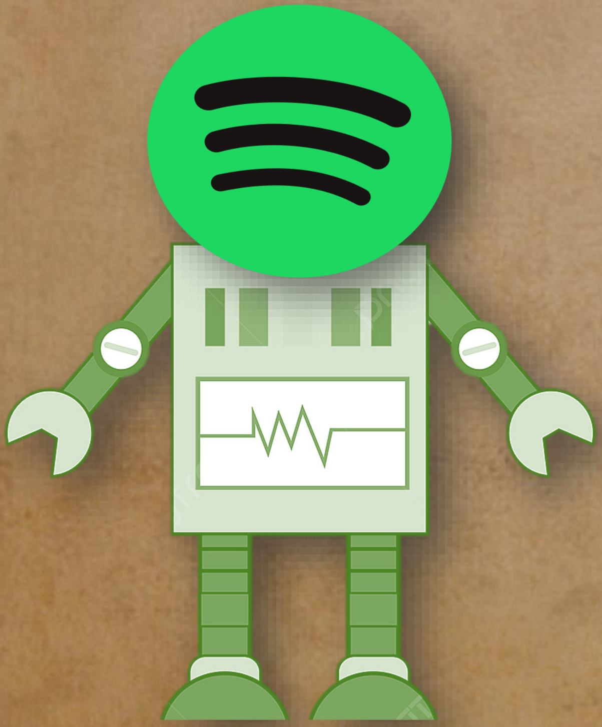
Build a weapon

Steal the moon

A Guide to Becoming a Malware Lord

- A service that supports anonymous data consumption
- Offers a flexible and diverse search functionality
- Content creation may require a registered account but content itself is not scrutinized

Introducing....



SPOTBOT!

SPOTBOT

- Media can be consumed anonymously
- Anonymous media search by arbitrary keywords
- Podcast content is not scrutinized (neither for copyright nor offensive content)

The Right to Free Speech

- Podcasts are easy to deliver through Spotify
- Use Castos to build Podcasts and upload episodes (19USD/month)
- Use podcasters.spotify.com to start publishing

Listen to Me!

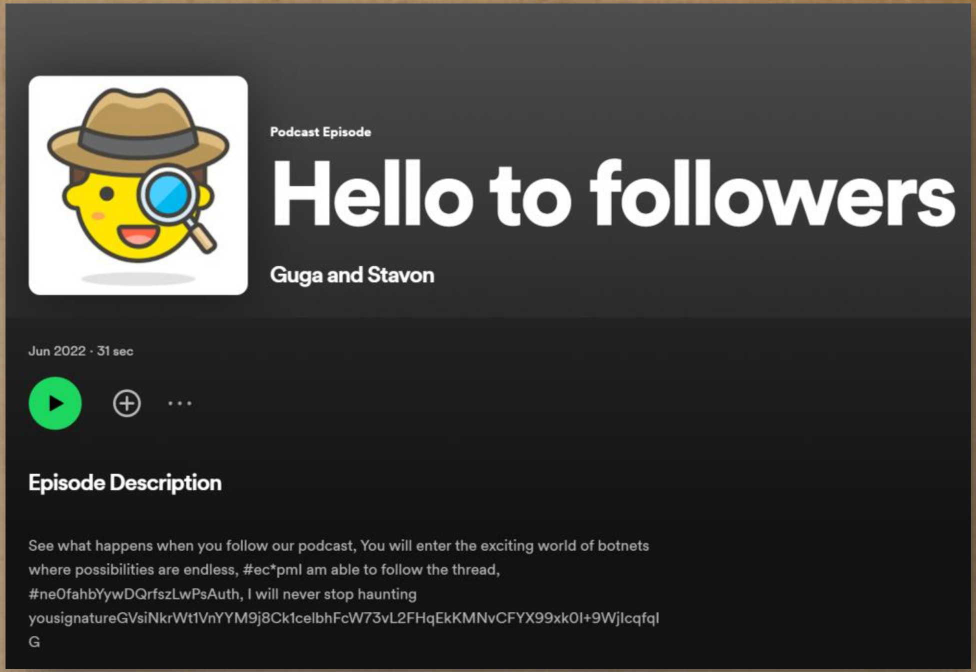
- Data can be encoded into the audio stream, or the image associated with the episode
  - Files are transformed when uploaded to Spotify
  - Data must be encoded / decoded using OCR or audio modulation
- Short data messages can be text encoded within episode description
  - Short commands
  - URL for downloads
  - ID of another Spotify object
  - DSA signature size is 64B (90 chars)

Making Initial Contact

- Search Spotify podcasts for some set keywords
  - Keywords are packaged into malware distribution
  - Keywords refer to podcast name
- Filter episodes by keywords in their description
- A digital signature is included in the description
  - Bots cannot be sink-holed

Data encoding

- The episode contains commands / data
- ID of the next episode to retrieve can be included in a command
- Retrieve an episode
    - https://open.spotify.com/episode/0jud9pWI80eK4zMopVUy0q



Podcast Episode

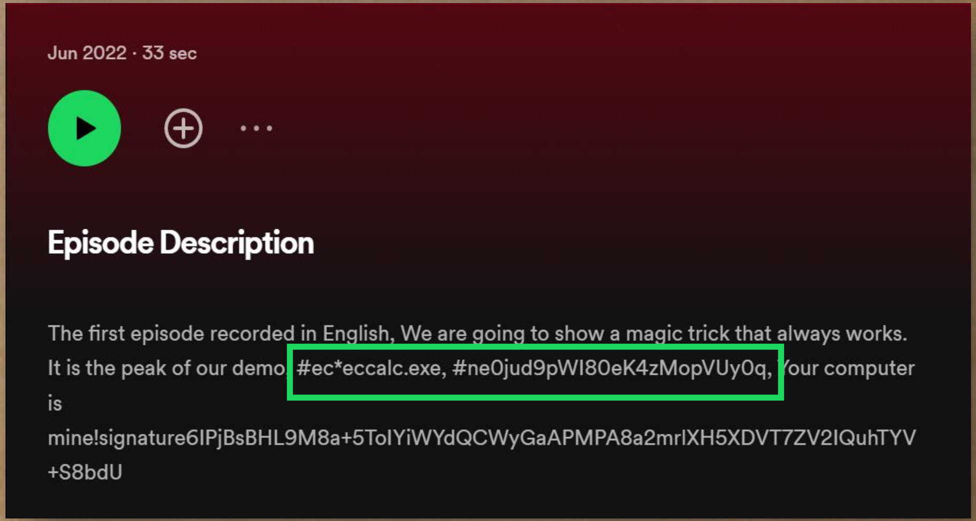
Hello to followers

Guga and Stavon

Jun 2022 · 31 sec

Episode Description

See what happens when you follow our podcast, You will enter the exciting world of botnets where possibilities are endless, #ec*pml am able to follow the thread, #ne0fahbYywDQrfszLwPsAuth, I will never stop haunting yousignatureGVsiNkrWt1VnYYM9j8Ck1celbhFcW73vL2FHqEkKMNvCFYX99xk0I+9WjIcqfqIG



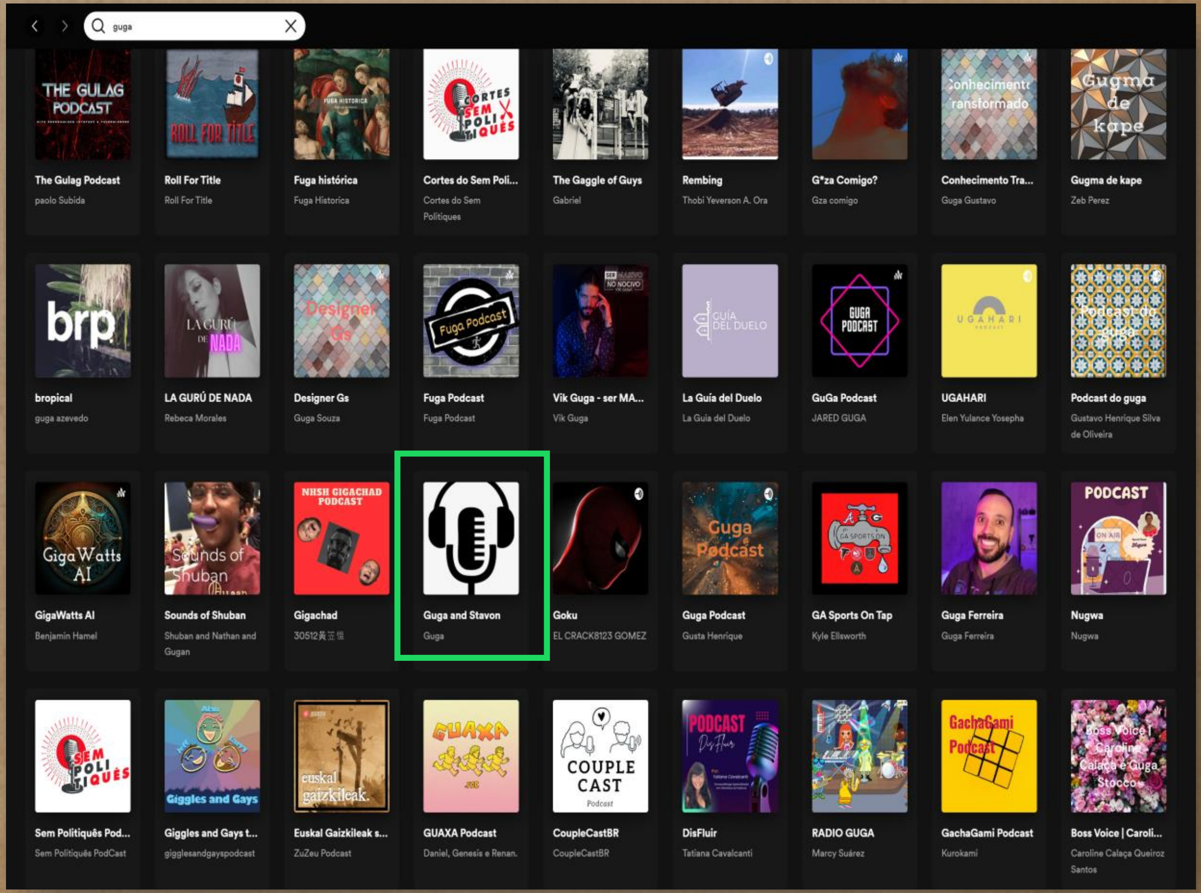
Jun 2022 · 33 sec

Episode Description

The first episode recorded in English, We are going to show a magic trick that always works. It is the peak of our demo, #ec*eccalc.exe, #ne0jud9pWI80eK4zMopVUy0q, Your computer is mine!signature6IPjBsBHL9M8a+5ToIYiWYdQCWyGaAPMPA8a2mrlXH5XDVT7ZV2IQuhTYV+S8bdU

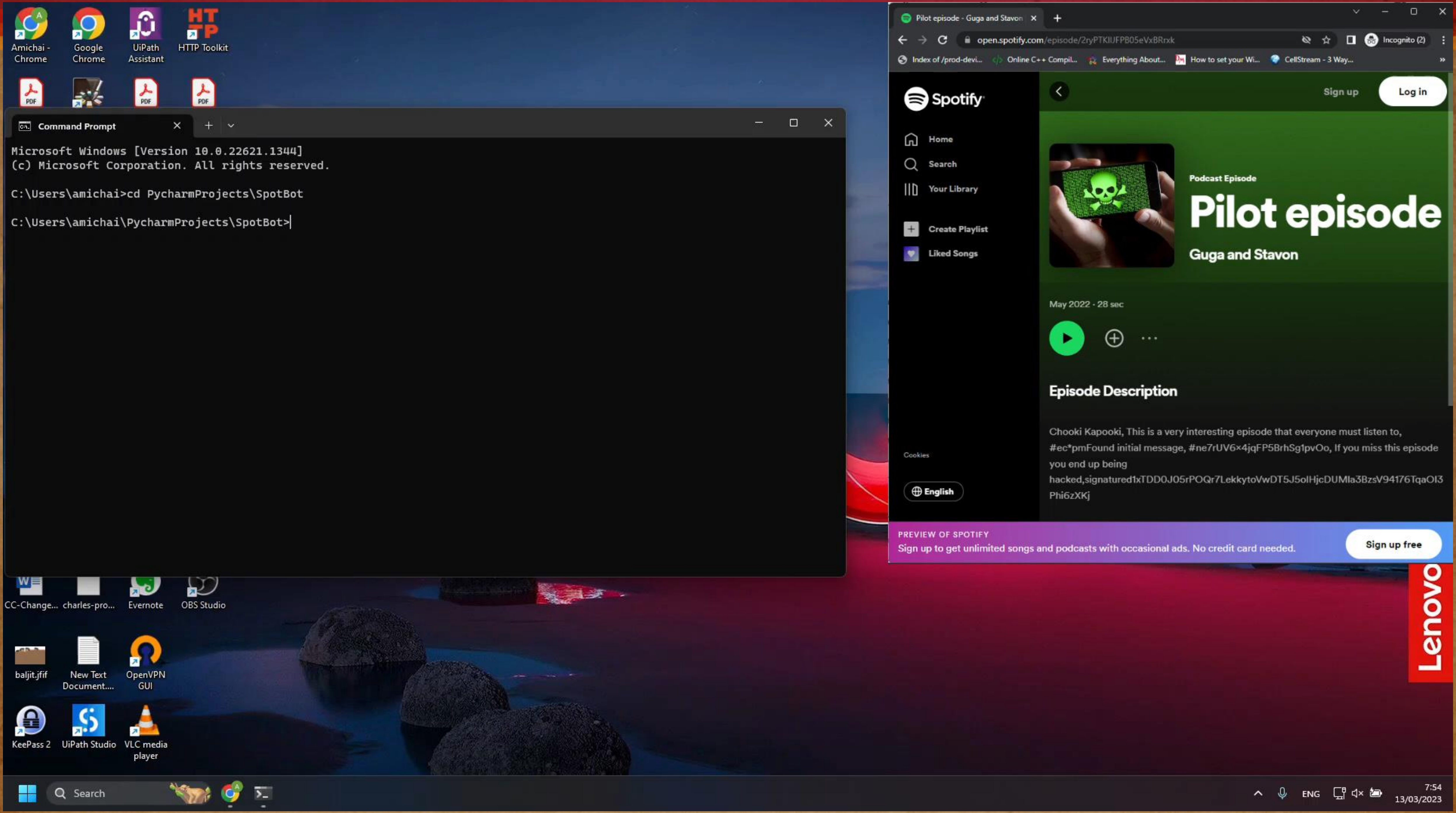
Keep the Show Running

- Assuming ALL episode links are being blocked OR even removed from Spotify
- Search Spotify again
  - o https://open.spotify.com/search/guga/podcasts
  - o Key words are changed from time to time through botnet commands



guga

The Gulag Podcast paolo Subida	Roll For Title Roll For Title	Fuga histórica Fuga Historica	Cortes do Sem Poli... Cortes do Sem Politiques	The Gaggle of Guys Gabriel	Rembing Thobi Yeverson A. Ora	G*za Comigo? Gza comigo	Conhecimento Tra... Guga Gustavo	Gugma de kape Zeb Perez
bropical guga azevedo	LA GURÚ DE NADA Rebeca Morales	Designer Gs Guga Souza	Fuga Podcast Fuga Podcast	Vik Guga - ser MA... Vik Guga	La Guía del Duelo La Guia del Duelo	GuGa Podcast JARED GUGA	UGAHARI Elen Yulance Yosepha	Podcast do guga Gustavo Henrique Silva de Oliveira
GigaWatts AI Benjamin Hamel	Sounds of Shuban Shuban and Nathan and Gugan	Gigachad 30512黄立恒	Guga and Stavon Guga	Goku EL CRACK8123 GOMEZ	Guga Podcast Gusta Henrique	GA Sports On Tap Kyle Ellsworth	Guga Ferreira Guga Ferreira	Nugwa Nugwa
Sem Politiquês Pod... Sem Politiquês PodCast	Giggles and Gays t... gigglesandgayspodcast	Euskal Gaizkileak s... ZuZeu Podcast	GUAXA Podcast Daniel, Genesis e Renan.	CoupleCastBR CoupleCastBR	DisFluir Tatiana Cavalcanti	RADIO GUGA Marcy Suárez	GachaGami Podcast Kurokami	Boss Voice | Caroli... Caroline Calaça Queiroz Santos



```
Microsoft Windows [Version 10.0.22621.1344]
(c) Microsoft Corporation. All rights reserved.

C:\Users\amichai>cd PycharmProjects\SpotBot

C:\Users\amichai\PycharmProjects\SpotBot>
```

open.spotify.com/episode/2ryPTKIUFPB05eVxBRxk

Podcast Episode

Pilot episode

Guga and Stavon

May 2022 · 28 sec

Episode Description

Chooki Kapooki, This is a very interesting episode that everyone must listen to, #ec*pmFound initial message, #ne7rUV6×4jqFP5BrhSg1pvOo, If you miss this episode you end up being hacked,signatured1xTDD0J05rPOQr7LekkytoVwDT5J5oIHjcDUMla3BzsV94176TqaOI3Phi6zXKj

PREVIEW OF SPOTIFY

Sign up to get unlimited songs and podcasts with occasional ads. No credit card needed.

Further Research

- Bidirectional communication
  - Analytics based approach failed so far
- Ads based botnets
  - Let the botnet find you!
- Instrumenting existing accounts

Summary

- Multiple public platforms provide opportunity for resilient botnet infrastructure
- All these platforms can be easily put to work using simple APIs
- Cost of creating and maintaining such robust infrastructure is dropping sharply

Conclusions

- Defender toolbox must change
- Generic defenses based on request IOCs fail to provide any protection
- Cheap and simple construction vs. expensive and complex dismantling
- New breed of tools
  - Content (response) based
  - Platform agnostic

Thank You!