Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **HT-W01**

Botnets Don't Die: Resurrecting the Dead to Feed on the Living

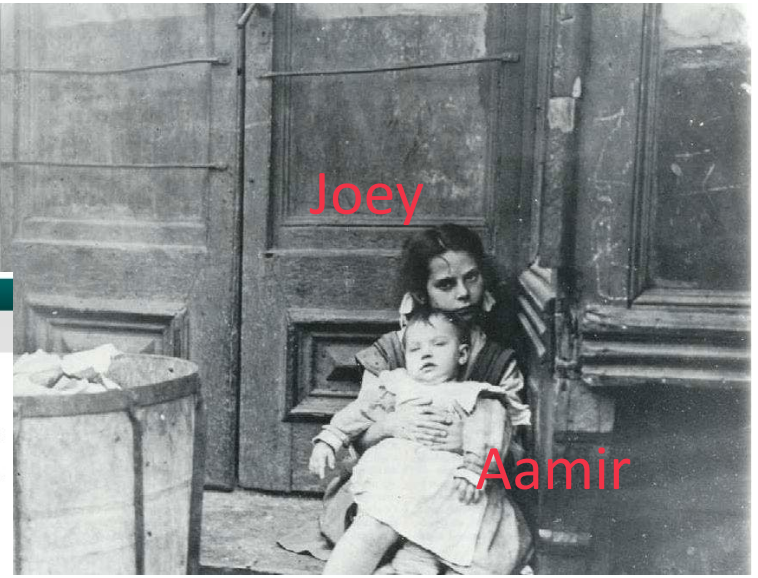
Joseph Muniz

Director of Business Development
Security Solutions - Microsoft
@SecureBlogger

Aamir Lakhani

Senior Principal of Zero Dark Research
FortiGuard Labs – Fortinet
@aamirlakhani

Long time friends



RSAConference2022

Act 1: BotNet Foundational Concepts

RSAConference2022

….but first a quick Botnet demo

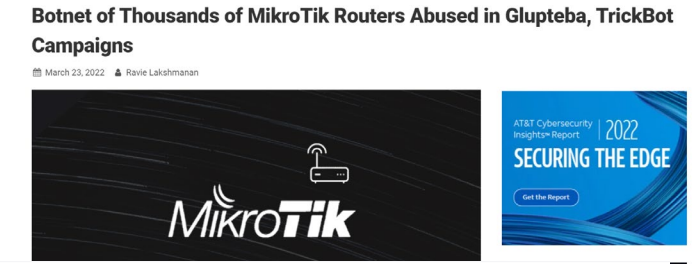
Bot Backend Demo

Why Not Hijacking Modern BotNets?

- Technology has **improved** but same concepts
- Ex: Russia war used **weaponized** botnets

- **Key characteristics of new botnets**
  - Uses 3rd party authentication
  - Much better encryption
  - Harder to track
  - You need BotNet protocol to connect

Key Point: Harder to take over, so older is a better target!!!



Old BotNet Examples

- EarthLink Spammer: 2000 – Phishing attack sent 1.25 Million emails from legitimate websites. Attacker was sued for 25m by earthlink. First large botnet attack
- Storm: 2007 – Network grew to 1millon+ devices. First peer-to-peer botnets
- Neverquest – Targeted users of more than 100 banks leverging the Neutrino exploit kit
- Mirai: 2018 – DDoS attack took out the USA east coast internet capabilities hitting insecure IoT devices

Good People Try To Help

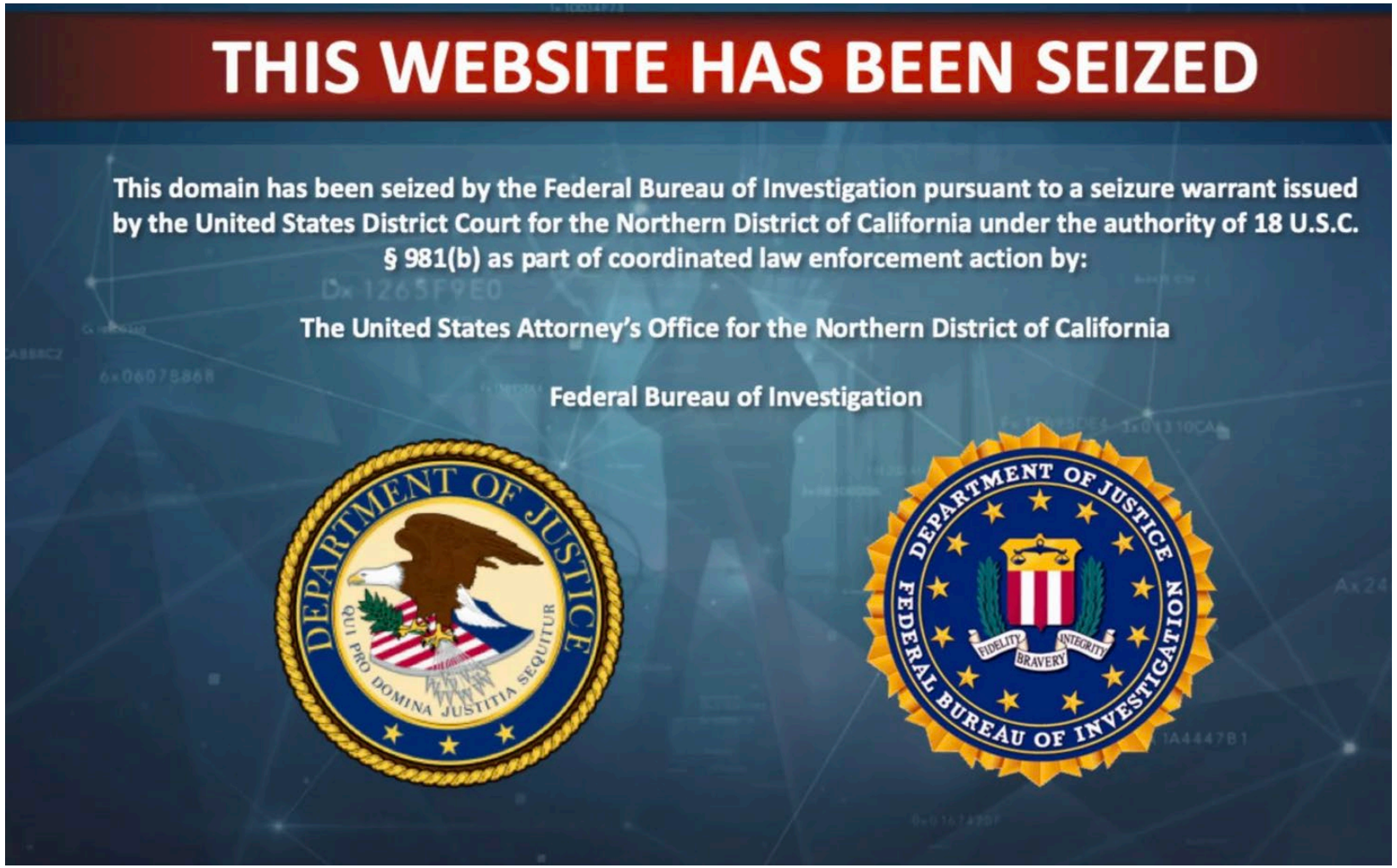
- **Buy / Take over** attacker servers to identify victims
- Identify **communication** from infected systems

Good People will Contact Victim if

- Victim is a customer to the vendor
- Contact seems possible
- No concerns of privacy by identifying the victim
- Or don't contact but note the possible victim

Often Doesn't Happen!

Post Takedown – Governments Take Over



Let’s Call This the “Goldilocks Zone!” for our Research

RSAConference2022

Act 2: ….
Turning into a bot

Host Systems Post BotNet Infection

- Botnet services and features are ”**post exploitation**” aka a separate **Attack** before becoming a bot
- **Plug-ins features** include RATs, keyloggers, webcam captures, password dumps, file exfiltration services, uploads, etc.
- Accomplished thru helper applications, DLLs, Registry Keys
- **Helper applications** are run under the botnet process, migrated to other processes, and in some cases uses privilege escalation.

BotNet Pre and Post Behavior

Common Attacks

- Phishing sends to exploit kit
- Common vulnerability exploitation
- Password compromise

Standard exploitation can lead to BotNet infection

Post Exploitation

- Wrapped with more than Bot aka chain exploitation
- Wipers triggered when Botnet needed
- Ransomware or other Malware
- Spreading focus to grow botnet

Specific BotNet Leave Behinds

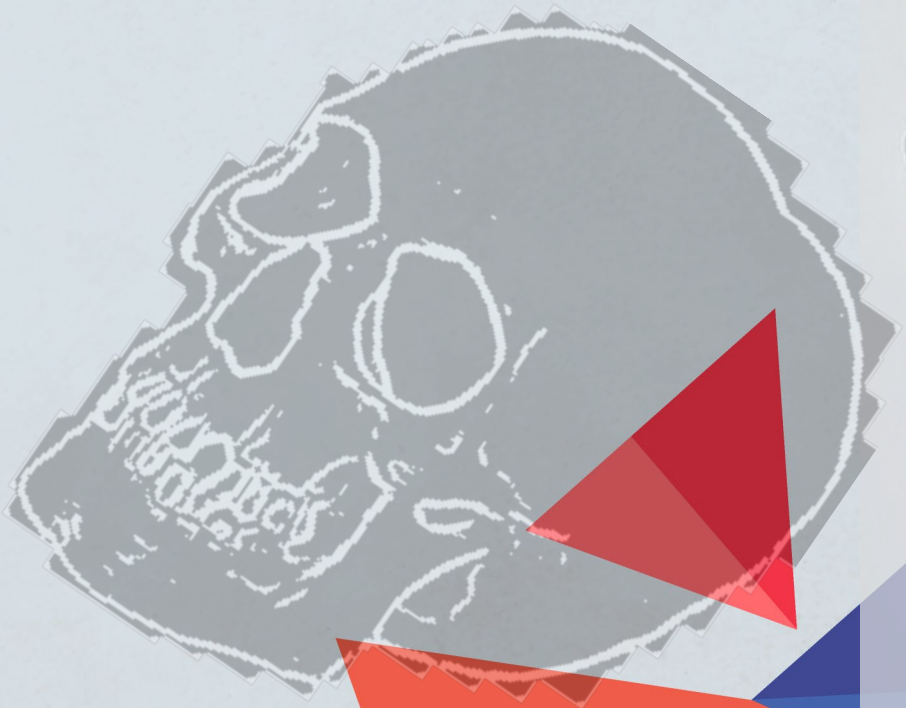
- Command and Control remote shell software
- **Modified** routing tables
- Infected **registry**
- **Bootup** modification
- Execution path **hijacked**
- AutoStart setting modified
- New **windows services** such as allowing greater access than system administrators

Botnet Incident Response Timeline from investigated attack Part 1

- Initial Access and Exploitation (Phishing Email attachment)
- UserPrpfileSvcEop.exe downloaded from GitHub (Escalate Privileges)
- Create additional accounts (Persistence)
- RDP to internal systems (Move Laterally)
- Process Explorer (Internal Recon)
- Process Hacker (Establish foothold)

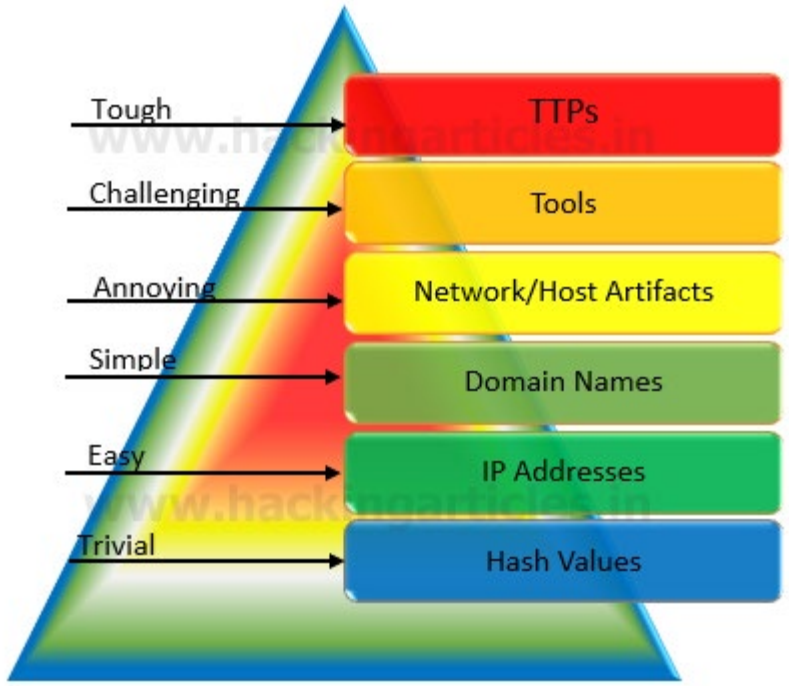
RSAConference2022

Act 3: Trying to find old Botnets – Steps we tried



Threat Hunting 101

- Proactive or Reactive
- **Proactive needs a hypothesis which continues to change**



A Deep Drive on Proactive Threat Hunting - Hacking Articles - https://www.hackingarticles.in/a-deep-drive-on-proactive-threat-hunting/

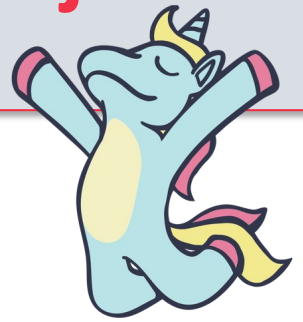
Threat Hunting Botnets

- Examining major Botnets from **2001 – 2009**
  - **Theory:** Botnets have unused domains easier to obtain
- **Problem 1:** Most major Botnets from this time didn't use direct C&C
  - Most were written for **DDoS attacks** and spread thru worms
- **Problem 2:** Major Botnets had their static domains taken or seized
  - Gov agencies or private security firms were using them

Threat Hunting Botnets

- **Problem 3:** Botnets with DDNS traffic are hard to predict on the cycle the botnet was active on.
  - DDNS domain names are predicable, but the order and time the botnets connected are not always predicable.
- **Problem 4:** Botnet traffic is being monitored and reported on.

Scope adjustment: Well known older BotNets off the table



New Focus for Research

From what was **learned**, we had to **adjust** the focus

- Target unpopular botnets
  - *Popular ones are taken over or unusable due to defender responses*
- Validate they have connected to C&C
- Successfully obtain the domain(s)

- **We have our domains … cool ….what's next**?

RSAConference2022



Act 4: Our Hypothesis – Necromancer?

Can we hijack already hijacked systems?

Botnet Resurrection Workflow

Step 1

Research old botnets (unpopular ones). **Buy** associated domains

Step 2

Create listener and wait for communication from compromised systems. Results = **list of infected systems**

Step 3

Attack user **(from list)** to gain system access. Locate and obtain botnet to reverse engineer

OR use research about botnet

OR obtain botnet from disclosed information about the botnet

Step 4

Reverse engineer botnet binary to identify communication protocol

Step 5

With protocol identified, **connect** to any future systems that communicate with domain and use as part of new BotNet

Upgrade authentication, encryption, etc. to protect your new victims

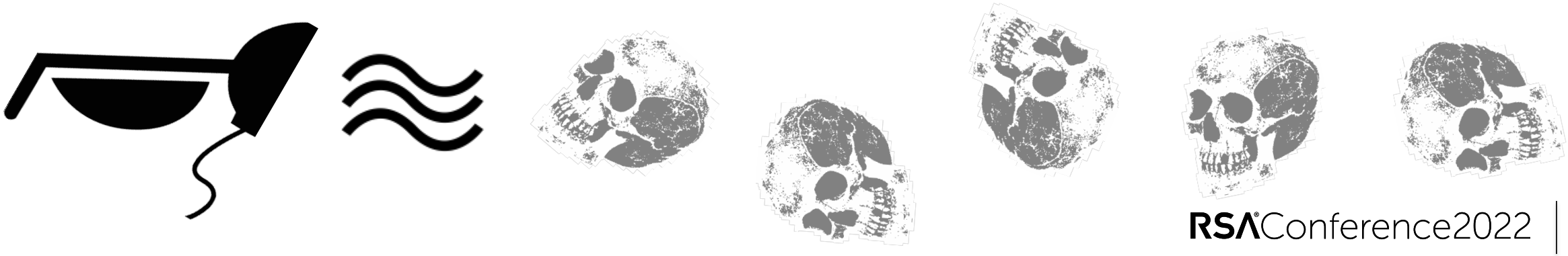
RSAConference2022

Act 5: How we did it

Let's get back to our story

- We now have **domains** we purchased. What's next?
  - Do we have any traffic going to these domains.
  - Easy enough, get a cloud VPS and point the DNS to the IP address
  - Run packet captures.

- Okay looks like we have **incoming traffic** on ports. Can we do anything with this????



PCAP Files

Protocol	Length	Info
TCP	62	1040 → 5678 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
TCP	62	[TCP Out-Of-Order] [TCP Port numbers reused] 1040 → 5678 [SYN] Seq=0 Win=64240 Len=0 MSS=14…
TCP	62	5678 → 1040 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM=1
TCP	60	1040 → 5678 [ACK] Seq=1 Ack=1 Win=64240 Len=0
TCP	60	[TCP Dup ACK 4#1] 1040 → 5678 [ACK] Seq=1 Ack=1 Win=64240 Len=0
TCP	61	1040 → 5678 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=7
TCP	61	[TCP Retransmission] 1040 → 5678 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=7
TCP	60	5678 → 1040 [ACK] Seq=1 Ack=8 Win=65535 Len=0
TCP	174	1040 → 5678 [PSH, ACK] Seq=8 Ack=1 Win=64240 Len=120
TCP	174	[TCP Retransmission] 1040 → 5678 [PSH, ACK] Seq=8 Ack=1 Win=64240 Len=120
TCP	61	5678 → 1040 [PSH, ACK] Seq=1 Ack=128 Win=65535 Len=7
TCP	2967	5678 → 1040 [ACK] Seq=8 Ack=128 Win=65535 Len=2913
TCP	60	1040 → 5678 [ACK] Seq=128 Ack=1468 Win=64240 Len=0
TCP	60	[TCP Dup ACK 13#1] 1040 → 5678 [ACK] Seq=128 Ack=1468 Win=64240 Len=0
TCP		
TCP	60	[TCP Dup ACK 81#1] 1040 → 5678 [ACK] Seq=128 Ack=48796 Win=64240 Len=0
TCP	60	1040 → 5678 [ACK] Seq=128 Ack=50256 Win=64240 Len=0
TCP	60	[TCP Dup ACK 83#1] 1040 → 5678 [ACK] Seq=128 Ack=50256 Win=64240 Len=0
TCP	60	1040 → 5678 [ACK] Seq=128 Ack=53176 Win=64240 Len=0
TCP	60	[TCP Dup ACK 85#1] 1040 → 5678 [ACK] Seq=128 Ack=53176 Win=64240 Len=0
TCP	60	1040 → 5678 [ACK] Seq=128 Ack=54636 Win=62780 Len=0
TCP	60	[TCP Dup ACK 87#1] 1040 → 5678 [ACK] Seq=128 Ack=54636 Win=62780 Len=0
TCP	60	[TCP Window Update] 1040 → 5678 [ACK] Seq=128 Ack=54636 Win=64240 Len=0
TCP	60	[TCP Dup ACK 87#2] 1040 → 5678 [ACK] Seq=128 Ack=54636 Win=64240 Len=0

PCAP Artifacts

- Odd destination ports
- Source port does not increase
- Duplicate and reused ACK

Netcat Listener

- A simple Netcat listener test showed incoming connections
- Data and connections on ports were not useable
- Data was not readable and looked like garbage
- Data was most likely encrypted or using something other than clear text (this is to be expected).

Results 1

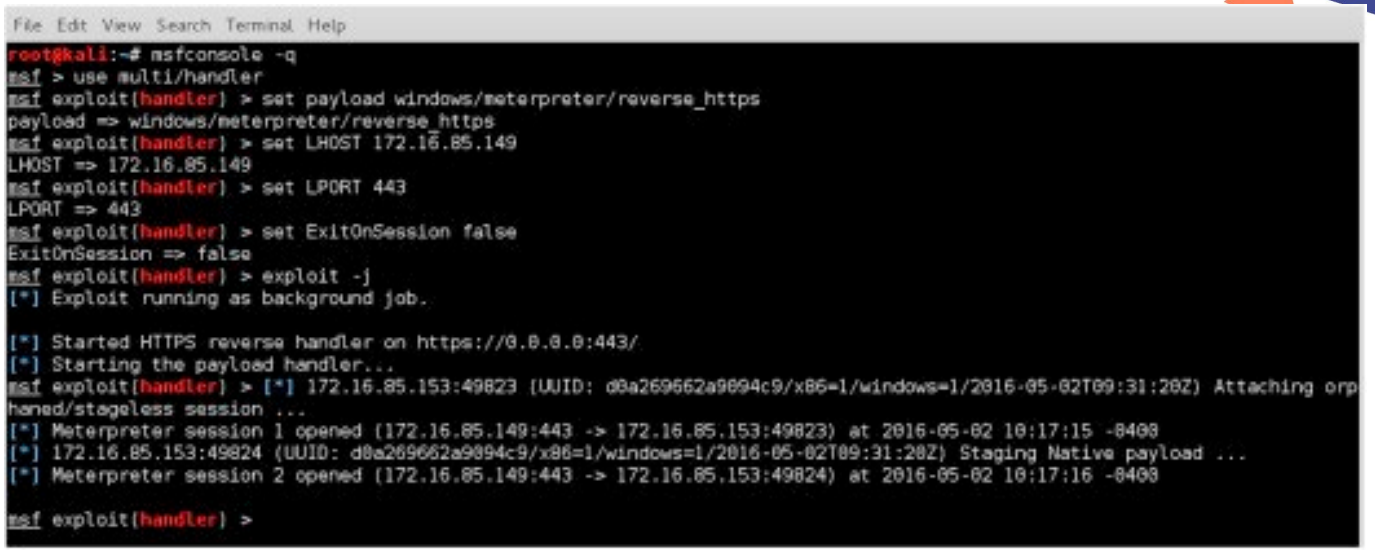
- We observed quickly data is **encoded** and not readable.
- Examining the binary **encryption** being used, we probably don't have time to break it.
- However, it tells us that these **Bots** are still active – at least the client portion.
- We want to take over a bot – **what is the next step**?

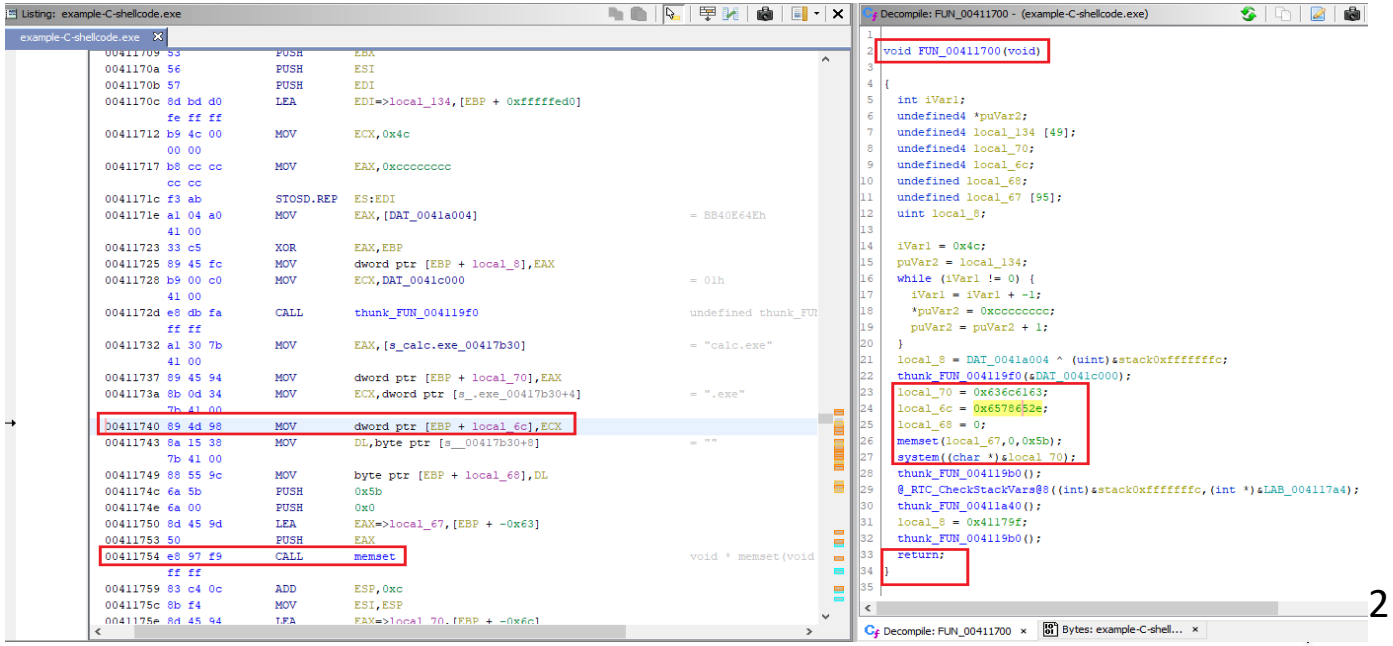
Try 2 - Cheating

- Finding **binaries** with known analysis of botnet C&C authentication
- **Registering** the domains
- Writing our own C&C server…. or better … try using a Metasploit Listener
- Seeing reverse connections

Discussing a reverse shell example

- **Setting reverse-shell listener worked**
- **Why?**
- **We didn't have full access to the Botnet but did have partial access.**
- **We used Bot binaries in our analysis that had the features we are looking for…let's discuss this example**





Screenshots are examples of function not from live test systems

The Results

- Wait did we succeed? Did we just have an old dead Botnet connect to our new command and control

What we achieved and could not achieve

Living on the (Botnet) Edge

- Basic access to infected endpoints
- Access to C&C domains
- In some cases, remote shell access to systems
- Ability to install additional software on endpoints.

- Full control of Botnet features
- Full Control of Botnet software and features
- Control or access to Botnet developers or learning their identities.

RSAConference2022

Remediation Recommendations

Fixing the "Impacted" is on YOU

- It is very unlikely infected system owners will be notified of a Botnet Controller **takedown**
- You must perform forensics and build a defense in depth strategy to identify potential **BotNet hijacking** or other threats
- Systems may not show activity for years before being **resurrected!**

RSAConference2022

Wrap Up

Take aways ….

- There are many very large BotNet takedowns that have thousands to millions of endpoints **still compromised**.
- With the right focus, you can identify ronin BotNet artifacts and **piggyback** off another attacker's breach.
- You should **assume compromise** when building a defense in depth strategy
- This problem is not going away on its own. It requires **YOU to take action!**

RSAConference2022

Thank you

RSAConference2022

Thank you

RSAConference2022

Thank you

RSAConference2022

Thank you

RSAConference2022

Thank you

RSAConference2022

Thank you

RSAConference2022

Thank you

RSAConference2022

Thank you

RSAConference2022

Thank you

RSAConference2022

Thank you

RSAConference2022

Thank you

RSAConference2022

Thank you