Botnets & Worms

ECE 239AS

Liz Izhikevich

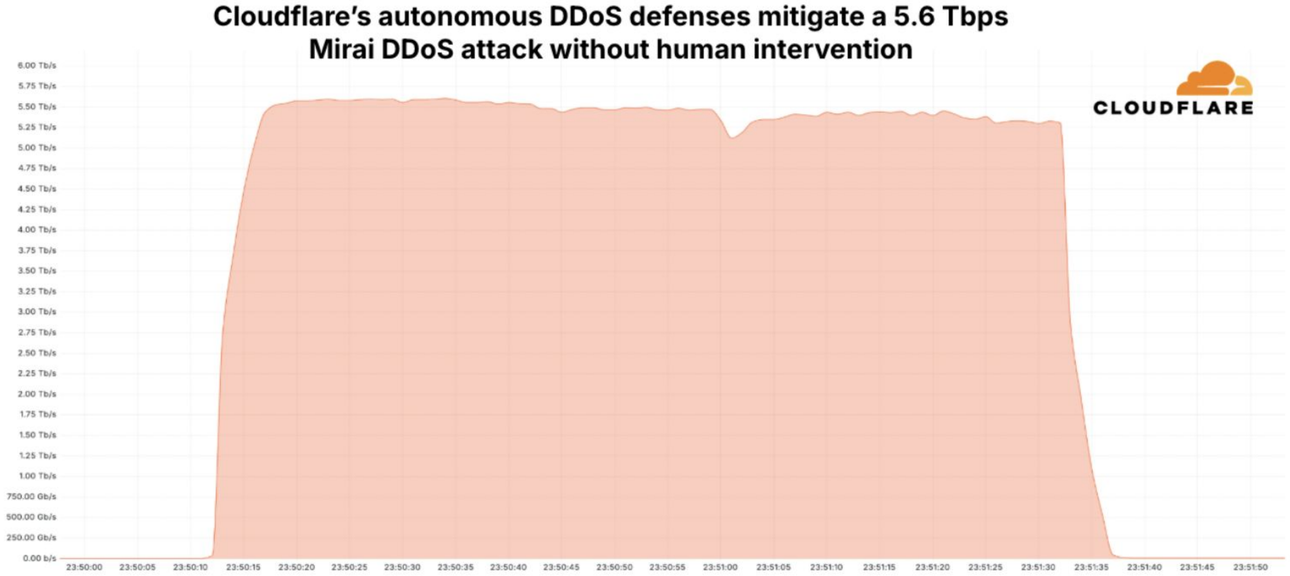
Botnets (Mirai)

Mirai Botnet

- Command and Control botnet
- At its peak, infected over 600K IoT devices (routers, cameras, printers, etc)
- In 2016, orchestrated one of the largest DDoS attacks at 623 Gbps on https://krebsonsecurity.com/ and against DYN (DNS provider) that GitHub, HBO, Twitter, Reddit, PayPal, Netflix, and Airbnb all rely on
- Code leaked online -> TONS of new variants

Mirai is still active

October 2024: Largest DDoS attack on record caused by Mirai variant



Cloudflare's autonomous DDoS defenses mitigate a 5.6 Tbps Mirai DDoS attack without human intervention

https://blog.cloudflare.com/ddos-threat-report-for-2024-q4/#the-largest-ddos-attack-on-record

Understanding the Mirai Botnet

Manos Antonakakis[◇] Tim April[‡] Michael Bailey[†] Matthew Bernhard[◁] Elie Bursztein[○]
Jaime Cochran[▷] Zakir Durumeric[◁] J. Alex Halderman[◁] Luca Invernizzi[○]
Michalis Kallitsis[§] Deepak Kumar[†] Chaz Lever[◇] Zane Ma[†*] Joshua Mason[†]
Damian Menscher[○] Chad Seaman[‡] Nick Sullivan[▷] Kurt Thomas[○] Yi Zhou[†]

[‡]*Akamai Technologies* [▷]*Cloudflare* [◇]*Georgia Institute of Technology* [○]*Google*
[§]*Merit Network* [†]*University of Illinois Urbana-Champaign* [◁]*University of Michigan*

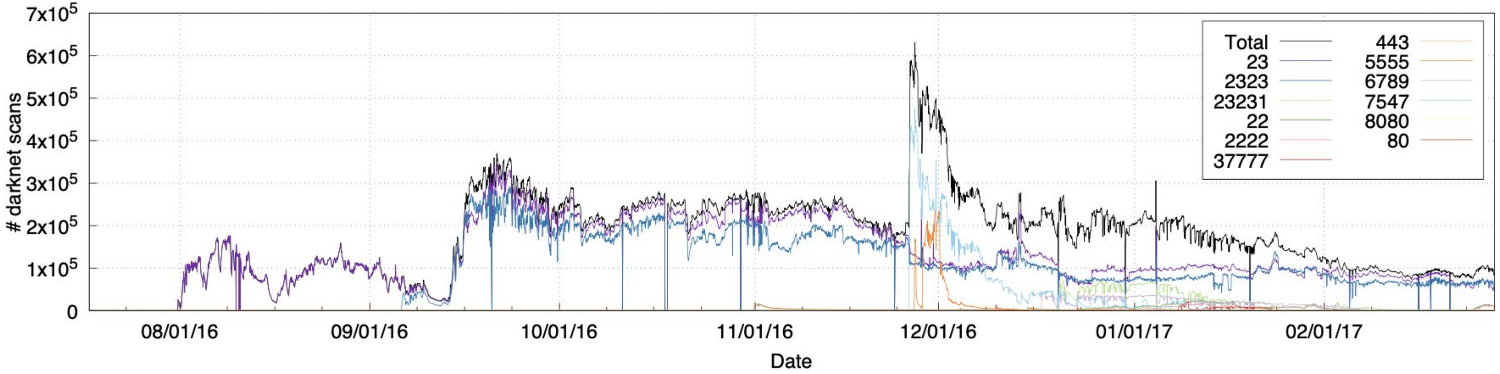
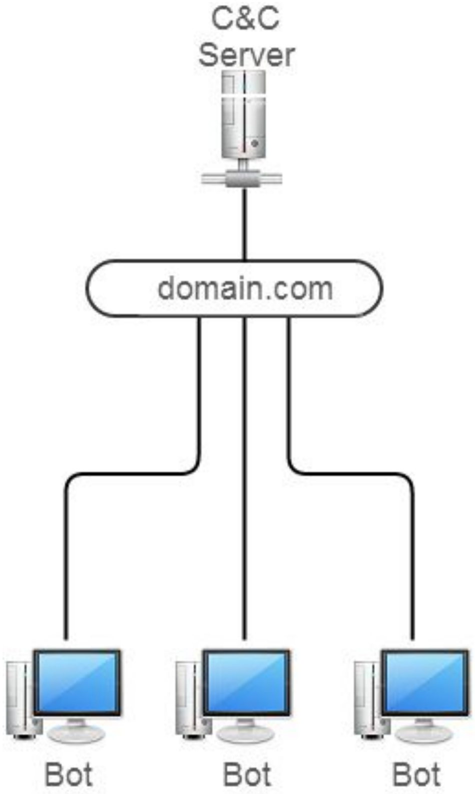


Figure 3: **Temporal Mirai Infections** — We estimate of the number of Mirai-infected devices over time by tracking the number of hosts actively scanning with Mirai fingerprint at the start of every hour. Mirai started by scanning Telnet, and variants evolved to target 11 additional protocols. The total population initially fluctuated between 200,000–300,000 devices before receding to 100,000 devices, with a brief peak of 600,000 devices.

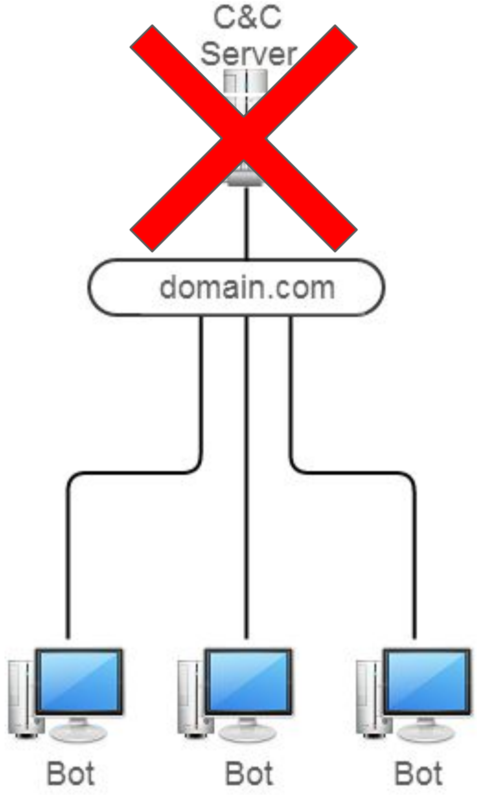
C&C Botnet Anatomy



- Centralized “command and control” (C&C) server that instructs the bots what to do
- C&C server will likely have multiple domains that the bots can reach it over
    - Complicates the process of shutting down botnet: need to take down all domains, can’t just take down the actual server
- C&C server will likely be hosted on a “bulletproof” server

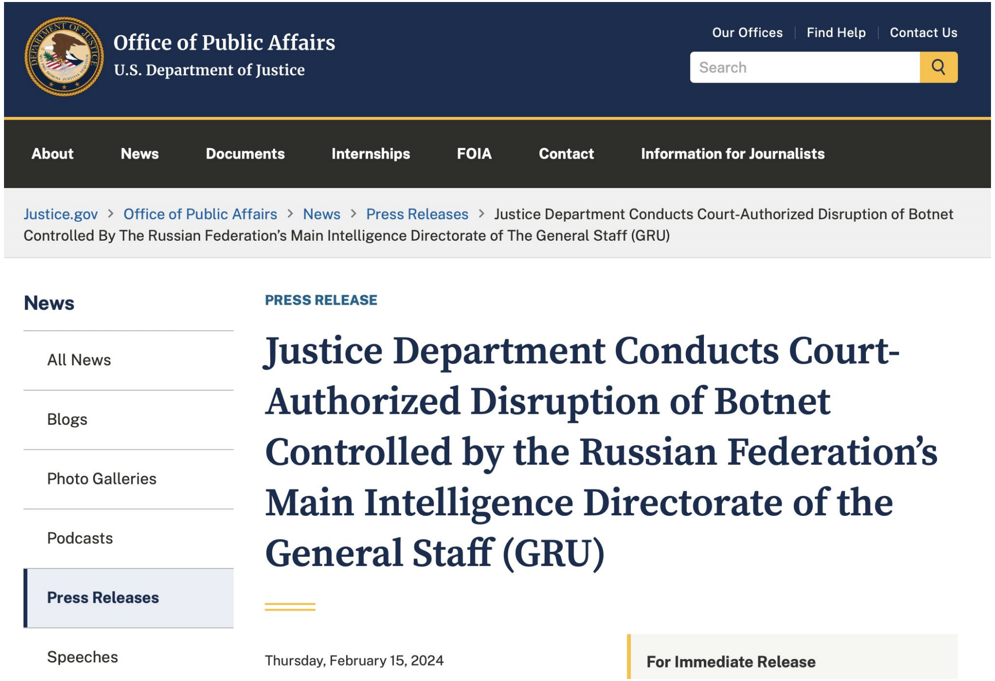
Taking down C&C botnets

- Take control of C&C server
- Issue remediation commands to compromised devices as if C&C had issued them
- Bots think they're taking orders from C&C and clear out the malware



Taking down C&C botnets

- Botnet run by Russian military hacking group Fancy Bear
- Commodity malware “Moobot” repurposed to log in to routers with default admin passwords
  - Moobot is a Mirai variant… it haunts us still
- February 2024: FBI takedown



Justice.gov > Office of Public Affairs > News > Press Releases > Justice Department Conducts Court-Authorized Disruption of Botnet Controlled By The Russian Federation’s Main Intelligence Directorate of The General Staff (GRU)

PRESS RELEASE

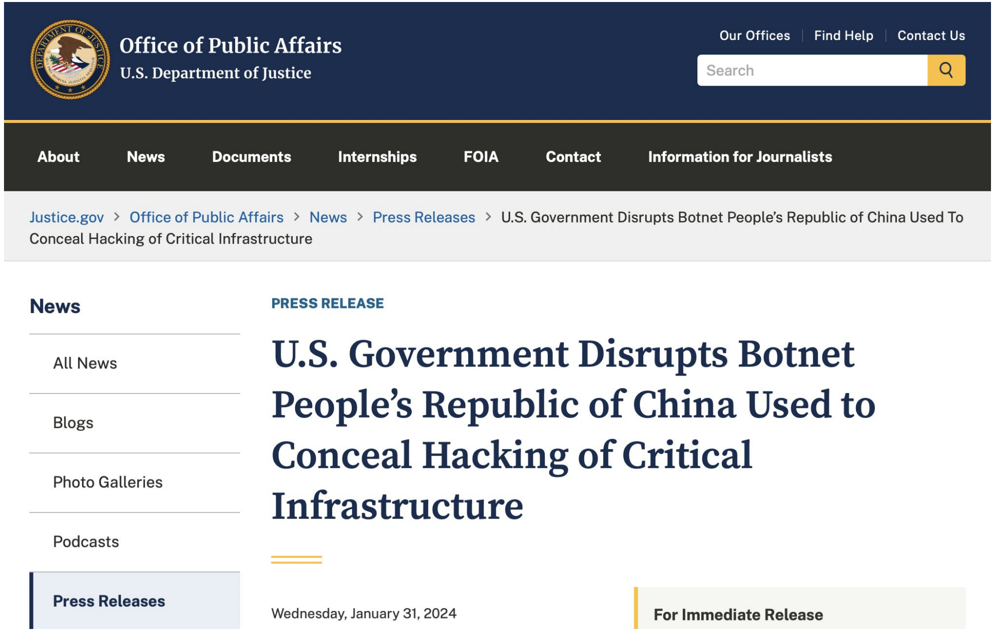
Justice Department Conducts Court-Authorized Disruption of Botnet Controlled by the Russian Federation’s Main Intelligence Directorate of the General Staff (GRU)

Thursday, February 15, 2024

For Immediate Release

Taking down C&C botnets

- “KV Botnet” run by Chinese state-sponsored hacking group Volt Typhoon
- Provided cover for group working to infiltrate US critical infrastructure
- Botnet targeted vulnerable end-of-life routers
- January 2024: FBI takedown



Office of Public Affairs
U.S. Department of Justice
Our Offices
Find Help
Contact Us
Search
About
News
Documents
Internships
FOIA
Contact
Information for Journalists
Justice.gov > Office of Public Affairs > News > Press Releases > U.S. Government Disrupts Botnet People’s Republic of China Used To Conceal Hacking of Critical Infrastructure
News
All News
Blogs
Photo Galleries
Podcasts
Press Releases

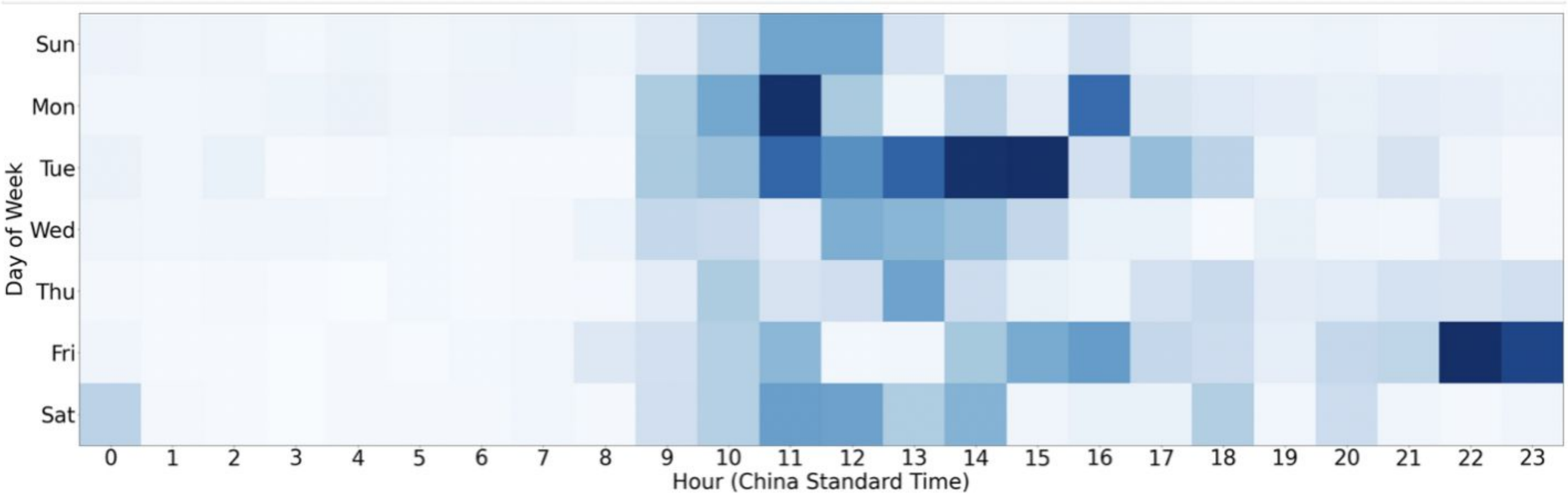
PRESS RELEASE

U.S. Government Disrupts Botnet People’s Republic of China Used to Conceal Hacking of Critical Infrastructure

Wednesday, January 31, 2024

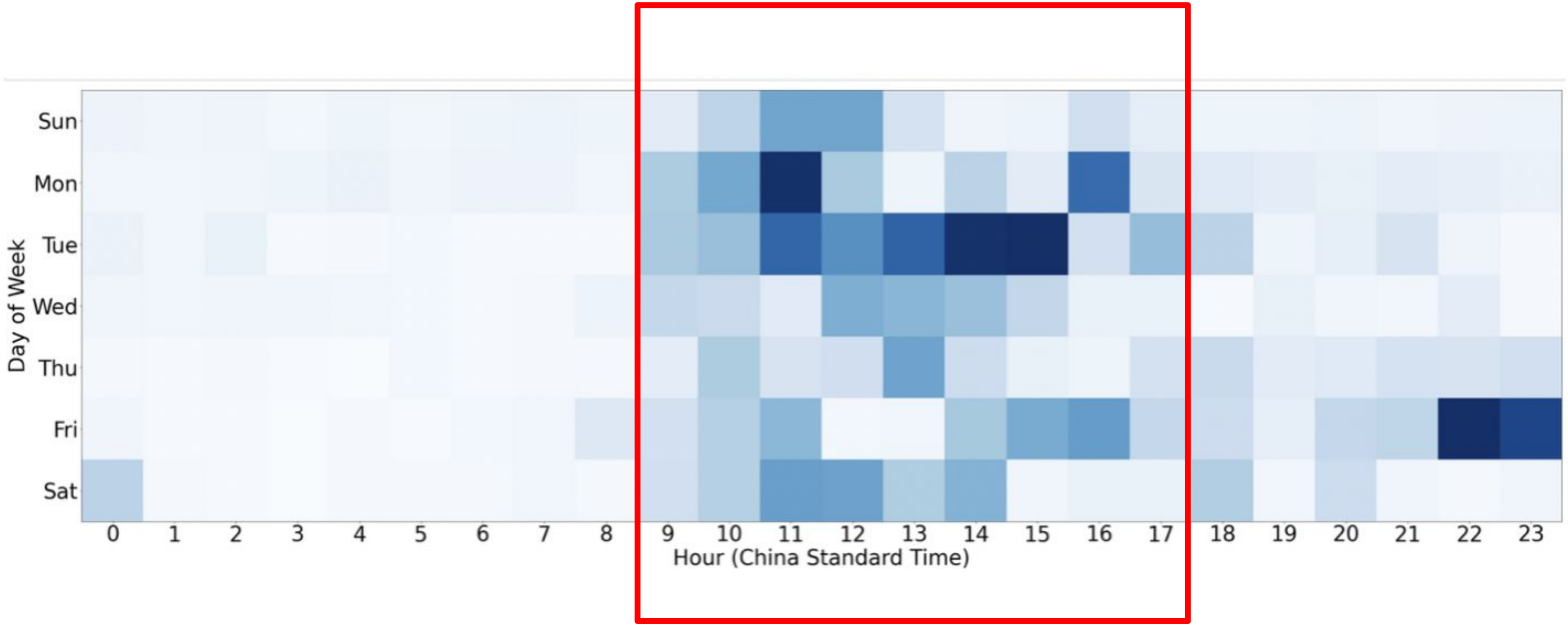
For Immediate Release

Sidenote: State-sponsored hacker working hours



Source:
https://blog.lumen.com/routers-roasting-on-an-open-firewall-the-kv-botnet-investigation/

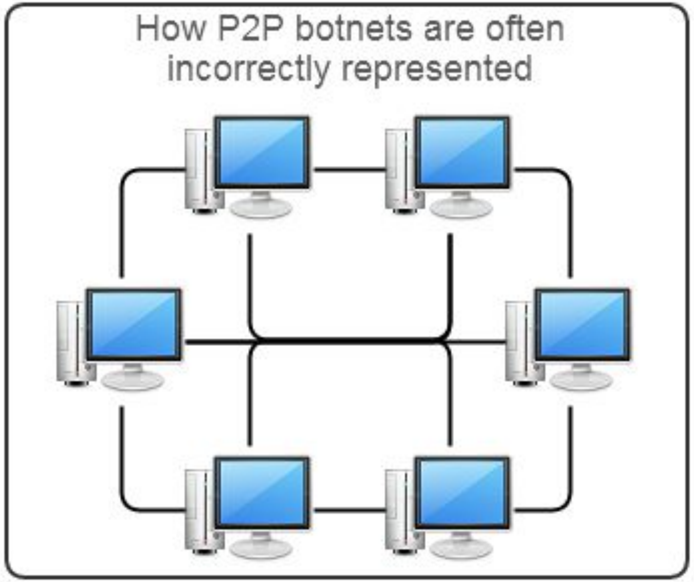
Sidenote: State-sponsored hacker working hours



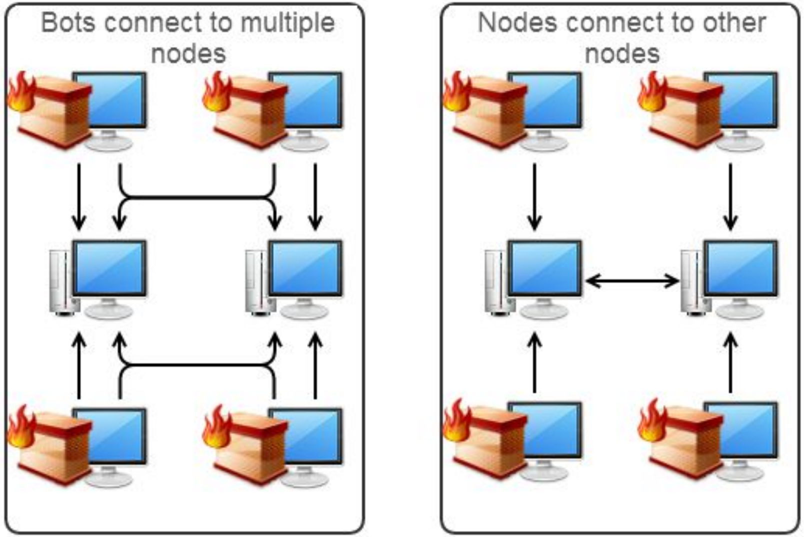
They’re working a 9-5 job!

Source: https://blog.lumen.com/routers-roasting-on-an-open-firewall-the-kv-botnet-investigation/

Peer2Peer Botnet Anatomy



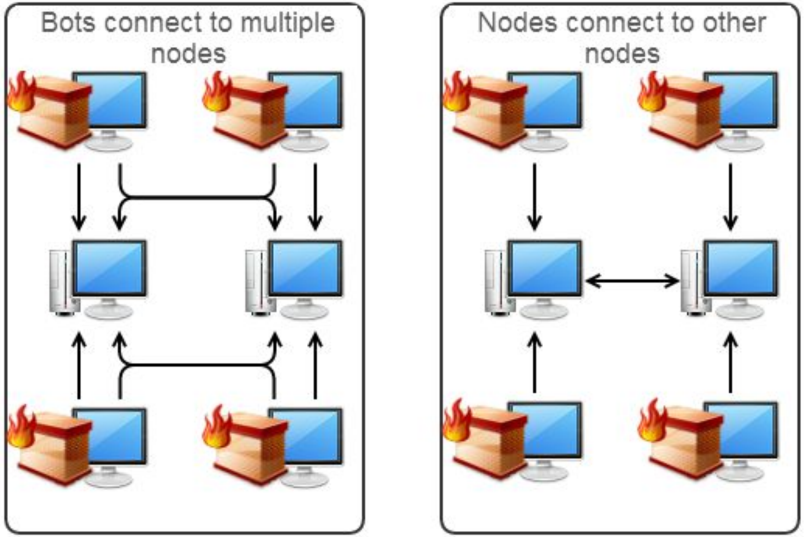
Peer2Peer Botnet Anatomy



- “**Nodes/Peers**”: Servers that are able to receive incoming connections (i.e., not behind a NAT/Firewall)
- “**Workers**”: Servers that cannot receive incoming connections

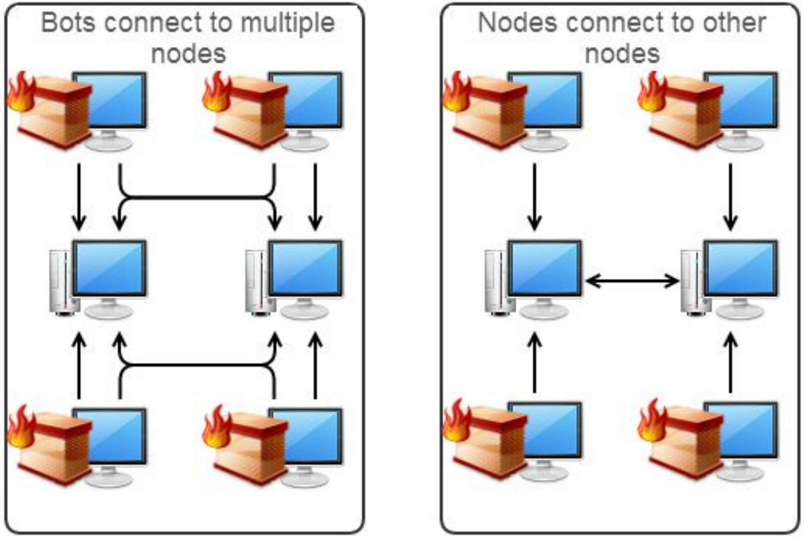
- Commands circulate the P2P network by passing commands between peers
    - Commands get passed to a worker once it reaches out

Peer2Peer Botnet Anatomy



- When a worker joins the botnet it is given a list of IP addresses (peers) to connect to.
  - Long list of candidates ensures that all peers need to be taken down for new bots to join
- If all peers get taken down...existing bots may continue to carry out existing attack

Dismantling P2P Botnets



- Need to introduce many "deceptive" peers into the network
  - Introduce by advertise the peer as a new "infected" peer
  - "deceptive" : peers with the intention of taking down the botnet)
- Have the peers provide workers with peer IP addresses that only belong to "deceptive" peers
- "Deceptive" peers/workers will soon become a majority of the network
- At some point, use "deceptive" network to tell workers to stop

Mozi Botnet

- Peer-to-Peer botnet
- Discovered in 2019 and supposedly has > 1.5 million peers (majority in China)
- Uses the Distributed Hash Table (DHT) protocol (i.e., Bittorrent protocol)
- Mostly infects Netgear, D-Link and Huawei routers -> Microsoft shared that botnet can perform MitM and spoofing attacks
- July 2021: Mozi botnet authors arrested by Chinese law enforcement
- August-September 2023: Sudden drop in botnet activity and activation of botnet “kill switch”
- Nobody claimed credit for takedown

Worms (WannaCry)

Bureau 121

- A group within the North Korean General Bureau of Reconnaissance that is in charge of cyber warfare
- UN 2019 reported that North Korea raised > $2 billion from hacking (and spends the $ on nuclear missile development)
- North Korea generally denies involvement
- Affiliated with Lazarus group (also from North Korea)
- U.S Justice Department indicted 3 men from this group for:
  - 2014 hack of Sony Pictures
  - the global “WannaCry ransomware contagion” of 2017
  - the theft of roughly $200 million and attempted theft of more than $1.2 billion from banks and other victims worldwide.

WannaCry / WannaCrypt Attack

- The NSA developed an exploit (“EternalBlue”) and a backdoor tool (“DoublePulsar”) that both target Microsoft SMB (port 445)
  - SMB “Server Message Block” protocol allows users to access files on remote servers
  - Exploit/backdoor sends specially crafted packets using SMB to allow for remote code execution on server

WannaCry / WannaCrypt Attack

- The NSA developed an exploit (“EternalBlue”) and a backdoor tool (“DoublePulsar”) that both target Microsoft SMB (port 445)
    - SMB “Server Message Block” protocol allows users to access files on remote servers
    - Exploit/backdoor sends specially crafted packets using SMB to allow for remote code execution on server

- Exploit/Backdoor leaked by “The Shadow Brokers” hacker group
    - Microsoft releases patches (Microsoft was unaware that vulnerabilities had even existed before..)...but not all organizations update in time

WannaCry / WannaCrypt Attack

- The NSA developed an exploit ("EternalBlue") and a backdoor tool ("DoublePulsar") that both target Microsoft SMB (port 445)
    - SMB "Server Message Block" protocol allows users to access files on remote servers
    - Exploit/backdoor sends specially crafted packets using SMB to allow for remote code execution on server

- Exploit/Backdoor leaked by "The Shadow Brokers" hacker group
    - Microsoft releases patches (Microsoft was unaware that vulnerabilities had even existed before..)...but not all organizations update in time

- Bureau 121 uses EternalBlue and DoublePulsar to build a ransomware attack (WannaCry)

WannaCry / WannaCrypt Attack

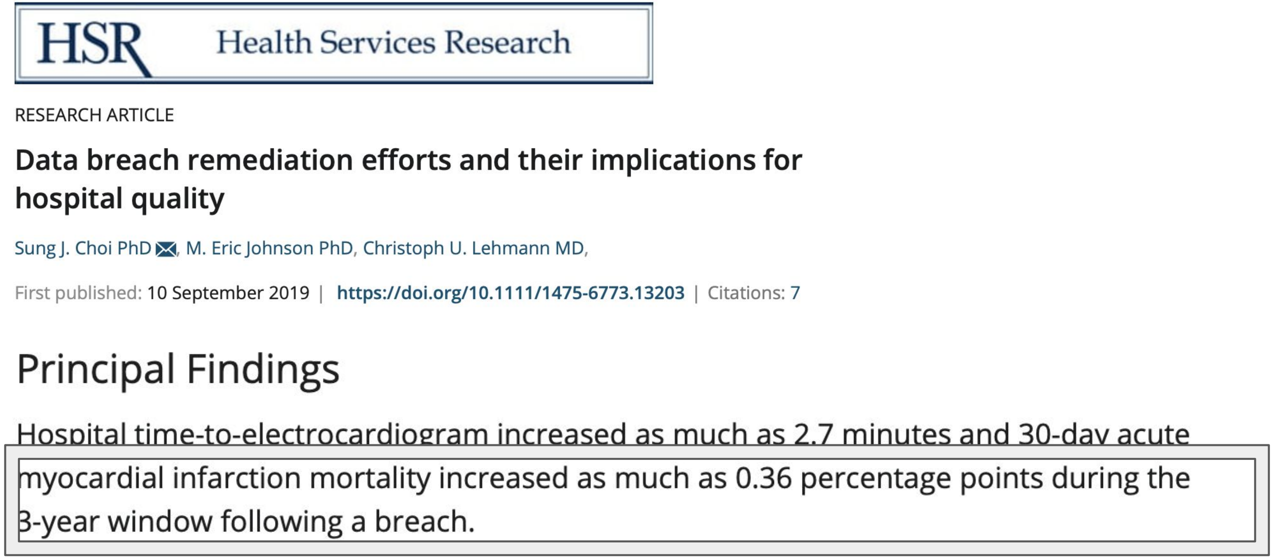
- Upon Infection, WannaCry will:
    - (1) Encrypt all the content + demands a ransom
    - (2) Scan for other vulnerable targets (within internal network and external network) to replicate infection

WannaCry / WannaCrypt Attack

- Upon Infection, WannaCry will:
  - (1) Encrypt all the content + demands a ransom
  - (2) Scan for other vulnerable targets (within internal network and external network) to replicate infection
    - If target already has DoublePulsar (creates a back door and allows for root execution of code):
      - Infect machine with WannaCry.
    - If target is vulnerable to EternalBlue:
      - use EternalBlue to deliver DoublePulsar
      - Use DoublePulsar to infects the machine with WannaCry

WannaCry / WannaCrypt Attack

- Within a day the code was reported to have infected more than 230,000 computers in over 150 countries
- ~70K devices (computers, MRI scanners, blood-storage refrigerators) in England's National Health Service were estimated to be affected and some non-critical emergencies and ambulances were diverted



HSR Health Services Research

RESEARCH ARTICLE

Data breach remediation efforts and their implications for hospital quality

Sung J. Choi PhD, M. Eric Johnson PhD, Christoph U. Lehmann MD,

First published: 10 September 2019 | https://doi.org/10.1111/1475-6773.13203 | Citations: 7

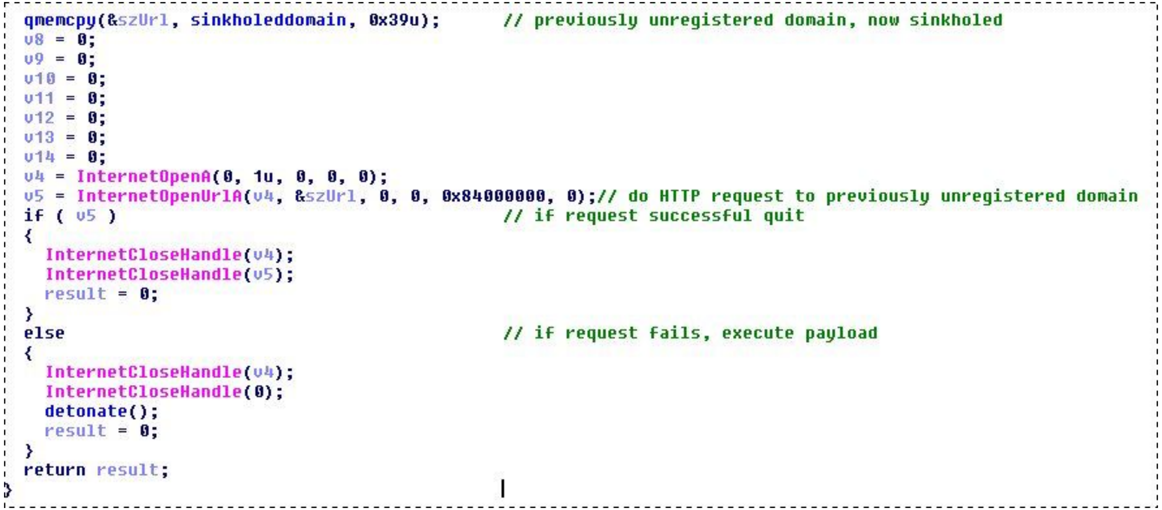
Principal Findings

Hospital time-to-electrocardiogram increased as much as 2.7 minutes and 30-day acute myocardial infarction mortality increased as much as 0.36 percentage points during the 3-year window following a breach.

How to Accidentally Stop a Global Cyber Attacks

By : MalwareTech May 13, 2017 Category : Personal Stories Tags: ms17-010, ransowmare, stories, WannaCry

- WannaCry gets “accidentally” stopped because Marcus Hutchins---a free-lance(ish) security geek---began reverse-engineering the code and noticed a domain
- Domain was unregistered and it turned out to be a baked in “kill-switch” with the following logic
    - If: domain is unregistered, continue with infection
    - Else: stop the encryption/infection
- Marcus quickly registered the domain name and the infection stopped (and for the most part doesn’t reach the US)

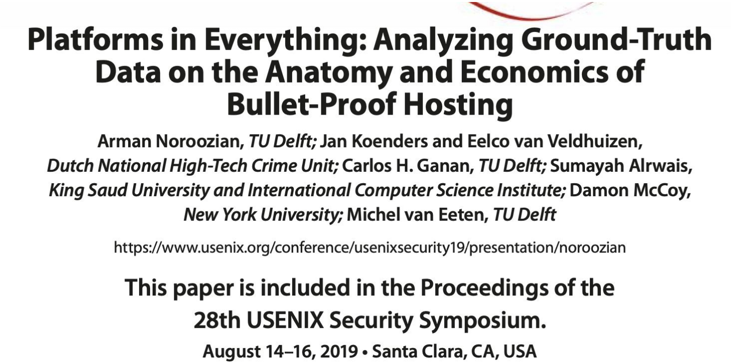


```
qmemcpy(&szUrl, sinkholeddomain, 0x39u);      // previously unregistered domain, now sinkholed
v8 = 0;
v9 = 0;
v10 = 0;
v11 = 0;
v12 = 0;
v13 = 0;
v14 = 0;
v4 = InternetOpenA(0, 1u, 0, 0, 0);
v5 = InternetOpenUrlA(v4, &szUrl, 0, 0, 0x84000000, 0);// do HTTP request to previously unregistered domain
if ( v5 )                                     // if request successful quit
{
  InternetCloseHandle(v4);
  InternetCloseHandle(v5);
  result = 0;
}
else                                          // if request fails, execute payload
{
  InternetCloseHandle(v4);
  InternetCloseHandle(0);
  detonate();
  result = 0;
}
return result;
}
```

Bulletproof Hosting

Bulletproof Hosting

- Operators allow/assist in hosting abusive content
- “Basic building block” of malicious activity (proxy, command & control)



Platforms in Everything: Analyzing Ground-Truth Data on the Anatomy and Economics of Bullet-Proof Hosting

Arman Noroozian, *TU Delft;* Jan Koenders and Eelco van Veldhuizen, *Dutch National High-Tech Crime Unit;* Carlos H. Ganan, *TU Delft;* Sumayah Alrwais, *King Saud University and International Computer Science Institute;* Damon McCoy, *New York University;* Michel van Eeten, *TU Delft*

https://www.usenix.org/conference/usenixsecurity19/presentation/noroozian

This paper is included in the Proceedings of the 28th USENIX Security Symposium.

August 14–16, 2019 • Santa Clara, CA, USA

Bulletproof Hosting

“Static” hosting: organization owns and operates infrastructure/networks/ASes

(+) Independent, “stable”

Bulletproof Hosting

“Static” hosting: organization owns and operates infrastructure/networks/ASes

(+) Independent, “stable”

(-) Easily blocked at the AS-level (other ASes would de-peer with them)

(-) Servers at risk of getting seized

Bullet-Proof Hosting

“Agile” hosting: rent/resell infrastructure from legitimate (cheap, often under-invest in security) ISPs

(+) Malicious traffic mixed with benign traffic -> hard to block

Bullet-Proof Hosting

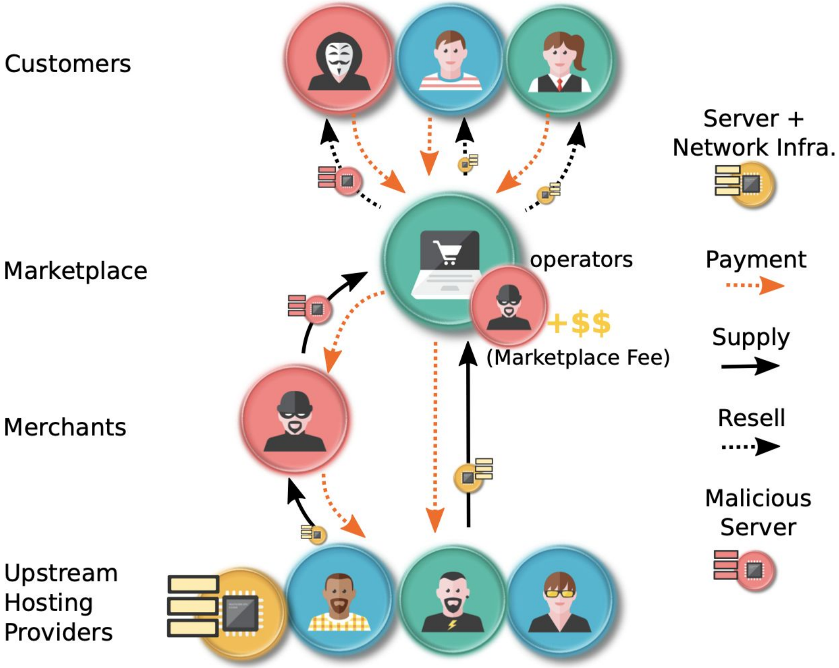
“Agile” hosting: rent/resell infrastructure from legitimate (cheap, often under-invest in security) ISPs

(+) Malicious traffic mixed with benign traffic -> hard to block

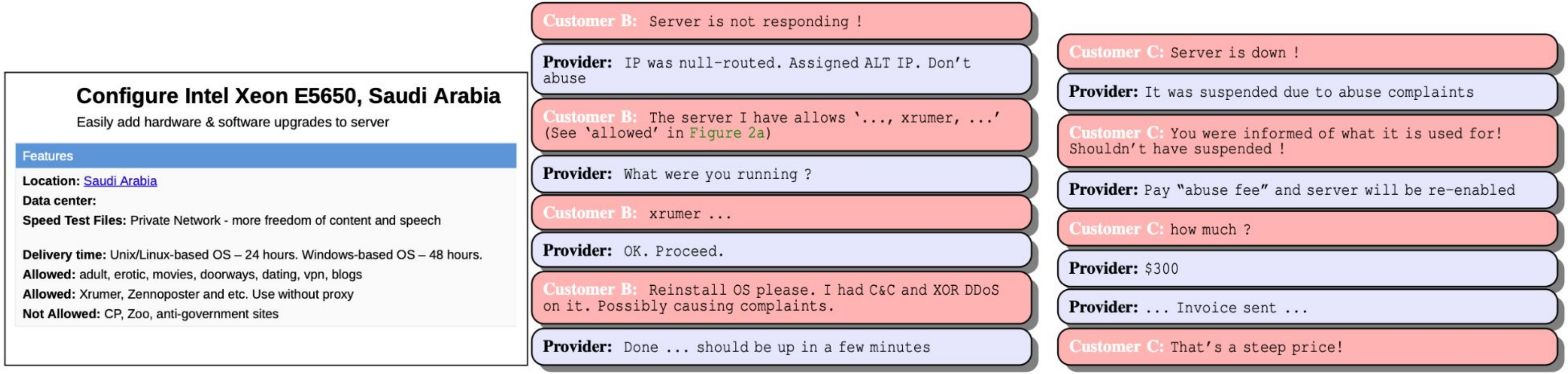
(-) Upstream providers can get angry, infrastructure can get shut-down

MaxiDed bulletproof hosting

Anatomy of MaxiDed 's business



- Maxided uses 395 unique upstream ASes
- $ 3.3M revenue



Configure Intel Xeon E5650, Saudi Arabia

Easily add hardware & software upgrades to server

Features

Location: Saudi Arabia

Data center:

Speed Test Files: Private Network - more freedom of content and speech

Delivery time: Unix/Linux-based OS – 24 hours. Windows-based OS – 48 hours.

Allowed: adult, erotic, movies, doorways, dating, vpn, blogs

Allowed: Xrumer, Zennoposter and etc. Use without proxy

Not Allowed: CP, Zoo, anti-government sites

(a)

Customer B: `Server is not responding !`

Provider: `IP was null-routed. Assigned ALT IP. Don't abuse`

Customer B: `The server I have allows '..., xrumer, ...' (See 'allowed' in Figure 2a)`

Provider: `What were you running ?`

Customer B: `xrumer ...`

Provider: `OK. Proceed.`

Customer B: `Reinstall OS please. I had C&C and XOR DDoS on it. Possibly causing complaints.`

Provider: `Done ... should be up in a few minutes`

(b)

Customer C: `Server is down !`

Provider: `It was suspended due to abuse complaints`

Customer C: `You were informed of what it is used for! Shouldn't have suspended !`

Provider: `Pay "abuse fee" and server will be re-enabled`

Customer C: `how much ?`

Provider: `$300`

Provider: `... Invoice sent ...`

Customer C: `That's a steep price!`

(c)

Figure 2: Examples of `MaxiDed`'s bullet-proof behavior. (a) screenshot of server publicly advertised to customers. (b) and (c) are excerpts of a conversation between customer and administrator (edited for readability).