

Internet Security

CS 249i

How do these attacks happen over the Internet?

The Record.
Recorded Future News

Jonathan Greig

January 28th, 2025

Ransomware attack kept major energy industry contractor out of some systems for 6 weeks



America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

PRESS RELEASE

CISA Update on Treasury Breach

Released: January 06, 2025

RELATED TOPICS: [CYBER THREATS AND ADVISORIES](#)

Subscribe To Newsletters

Forbes

UnitedHealth Data Breach Escalates: 190 Million Americans Affected

By [Alex Vakulov](#), Contributor. Alex Vakulov is a cybersecurity expert focused on...

Jan 27, 2025, 10:10am EST

WIRED

SECURITY POLITICS GEAR THE BIG STORY BUSINESS SCIENCE CULTURE IDEAS MERCH

SIGN IN

ANDY GREENBERG

SECURITY FEB 13, 2025 12:00 AM

China's Salt Typhoon Spies Are Still Hacking Telecoms—Now by Exploiting Cisco Routers

What Internet security problems plague us *today*?

- (1) Vulnerable/Exposed Services on the Internet
 - (a) Sensitive data leakage
 - (b) Ransomware
 - (c) Botnets → Distributed Denial of Service

- (2) “Bulletproof”/ “Neutral” Hosting
 - (a) Network attacks
 - (b) Misinformation

Real world consequences

(attacks on natural resources, hospitals, information sources, vaccination rates)

How are network intrusion attacks orchestrated on the Internet?

Colonial Pipeline ransomware attack - May 2021



- May 7: Attackers penetrate, encrypt, and hold internal systems for ransom
- May 7 -- May 12: colonial pipeline operations are shut down
- Fuel shortages across the entire east coast (affected drivers, airlines, etc)

DarkSide (“Ransomware-as-a-Service”)

- Responsible for Colonial Pipeline Hack
- Operates from Russia

Let's start

10.08.2020

We are a new product on the market, but that does not mean that we have no experience and we came from nowhere. We received millions of dollars profit by partnering with other well-known cryptolockers. We created **DarkSide** because we didn't find the perfect product for us. Now we have it.

Based on our principles, we will not attack the following targets:

- Medicine (only: hospitals, any palliative care organization, nursing homes, companies that develop and participate (to a large extent) in the distribution of the COVID-19 vaccine).
- Funeral services (Morgues, crematoria, funeral homes).
- Education (schools, universities).
- Non-profit organizations.
- Government sector.

We only attack companies that can pay the requested amount, we do not want to kill your business. Before any attack, we carefully analyze your accountancy and determine how much you can pay based on your net income. You can ask all your questions in the chat before paying and our support will answer them.

We provide the following guarantees for our targets:

- We guarantee decryption of one test file.
- We guarantee to provide decryptors after payment, as well as support in case of problems.
- We guarantee deletion of all uploaded data from TOR CDNs after payment.

If you refuse to pay:

- We will publish all your data and store it on our TOR CDNs for at least 6 months.
- We will send notification of your leak to the media and your partners and customers.
- We will **NEVER** provide you decryptors.

We take our reputation very seriously, so if paid, **all guarantees will be fulfilled.**

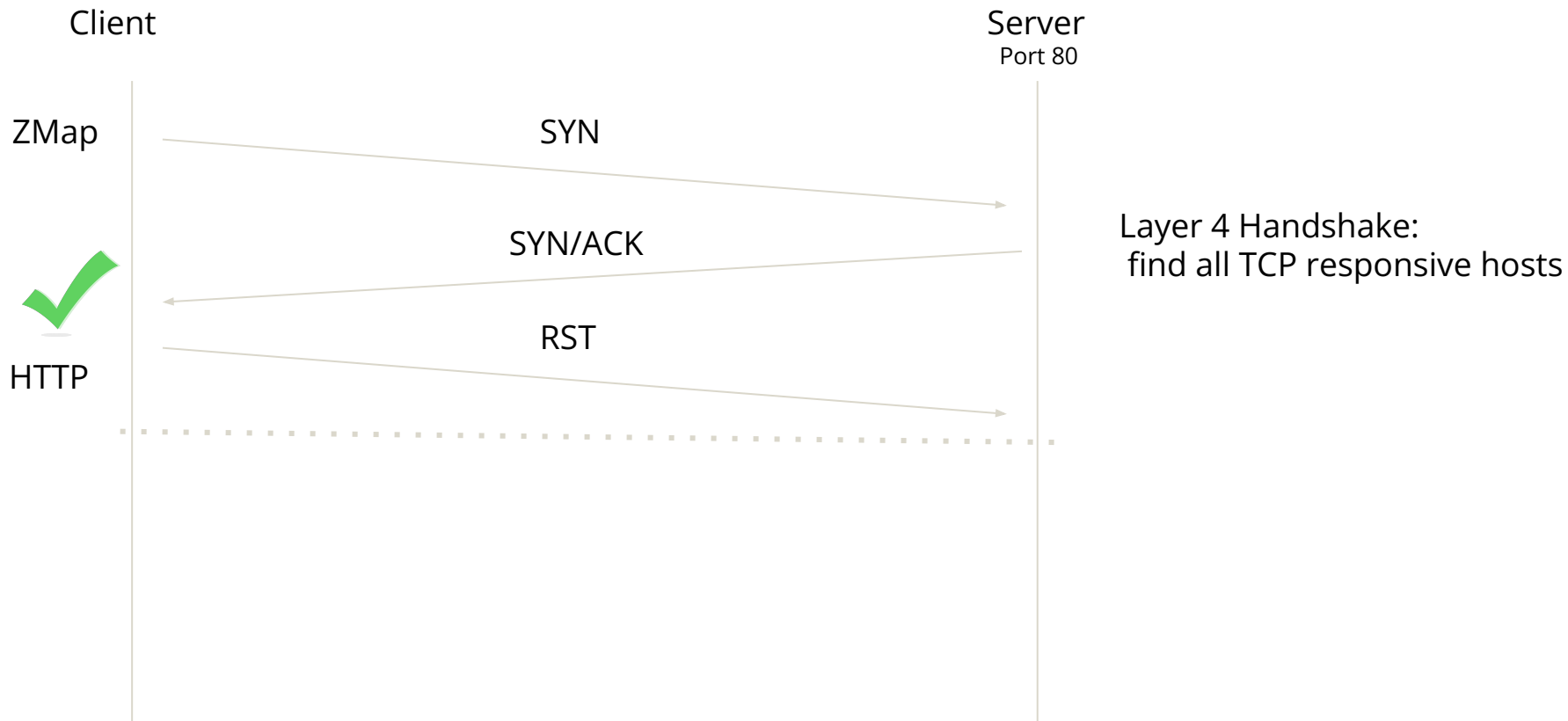
If you don't want to pay, you will add to the list of published companies on our blog and become an example for others.

How do attackers (and researchers) find Internet services to gain control of (study) ?

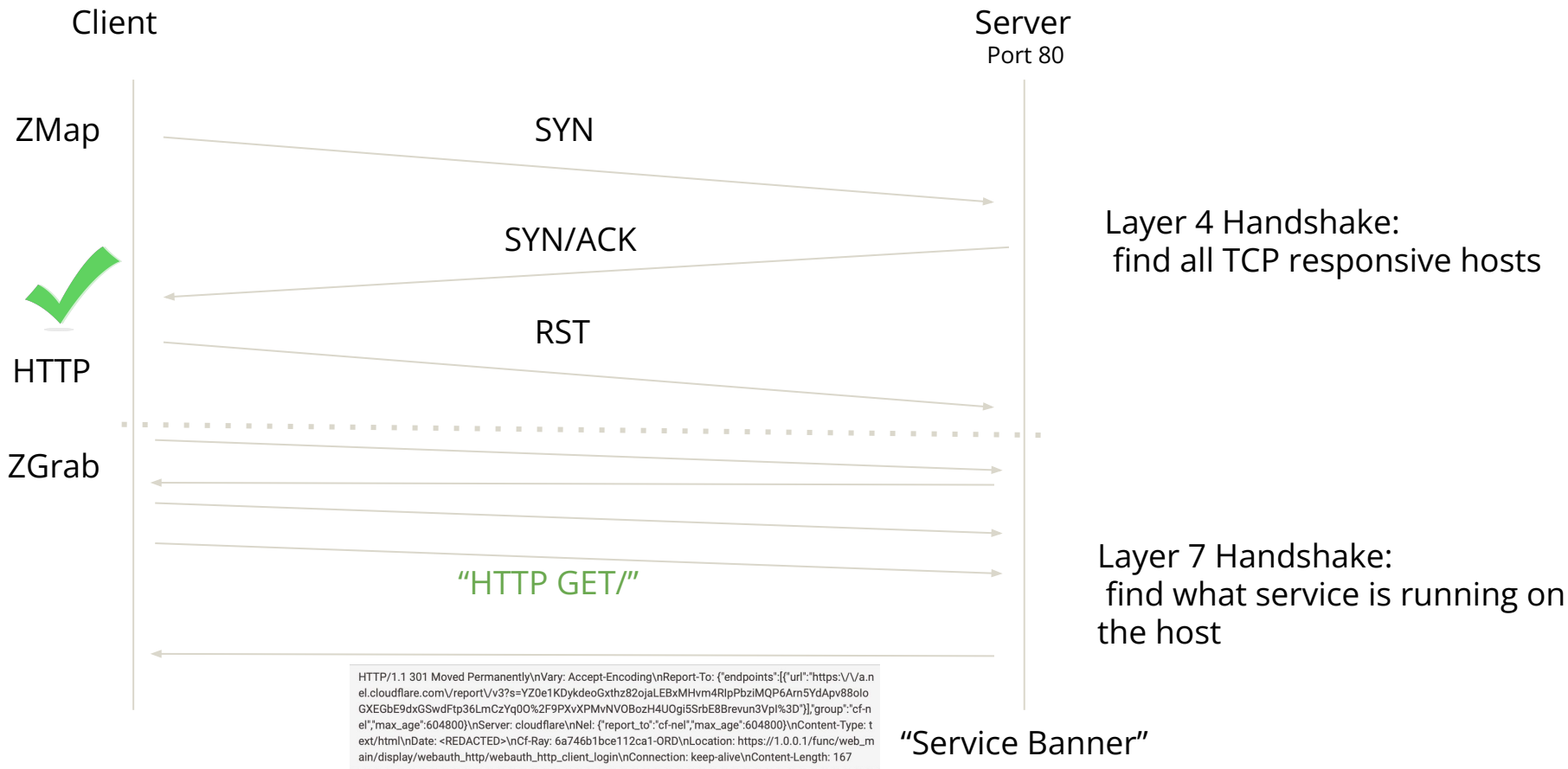
Finding services using Internet scanning

- Internet Scanning: The process of connecting to IP addresses on chosen ports in order to detect active services

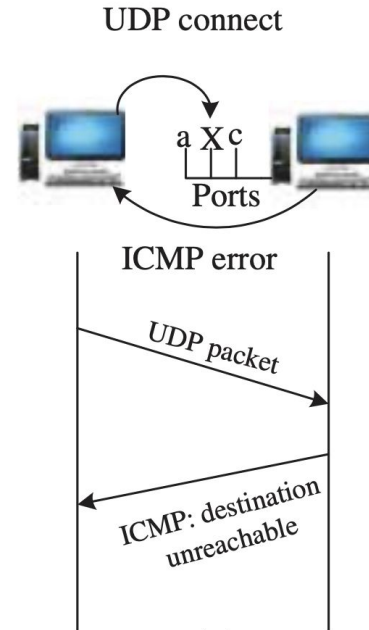
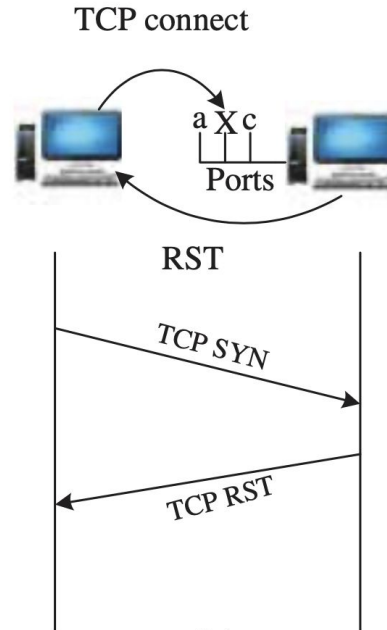
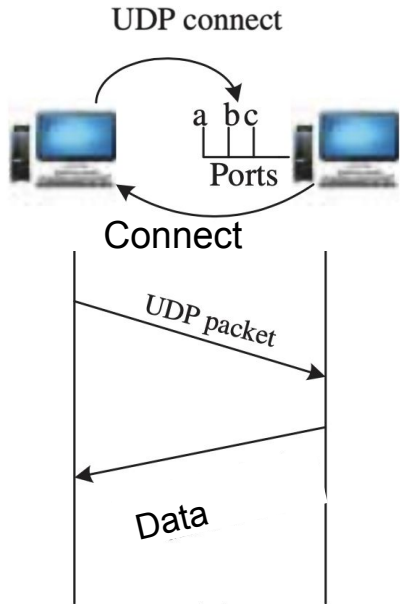
Most commonly used* TCP Internet scanning methodology



Most commonly used* TCP Internet scanning methodology



Layer 4 Internet scanning (continued)



Finding services using Internet scanning

IPv4: connect to all $\sim 2^{32}$ IP addresses on a subset of “interesting” ports and protocols

(e.g., HTTP/80, TLS/443, TELNET/23)

- ~ 1 hour to scan 100% of IPv4 on 1 port at 1Gb/s bandwidth

Finding services using Internet scanning

IPv4: connect to all $\sim 2^{32}$ IP addresses on a subset of “interesting” ports and protocols

(e.g., HTTP/80, TLS/443, TELNET/23)

- ~ 1 hour to scan 100% of IPv4 on 1 port at 1Gb/s bandwidth

IPv6: not possible to connect to all $\sim 2^{128}$ IP addresses...need a smart way of predicting which IP addresses will most likely respond

- IPv6 scanning is an open research problem!

Results

Report Docs

Host Filters

Autonomous System:

9.84M AMAZON-02
7.24M AKAMAI-AS
6.57M BT-UK-AS BTnet
UK Regional
network
6.01M ASN-IBSNAZ
5.56M DTAG Internet
service provider
operations

More

Location:

53.58M United States
18.12M United Kingdom
16.80M Germany
14.96M China
11.22M South Korea

More

Service Filters

Service Names:

860.36M HTTP
56.88M UNKNOWN
26.84M SSH
15.96M SMTP
10.18M FTP

More

Ports:

57.61M 80
45.55M 443
24.28M 7547
20.82M 22
12.26M 30005

More

Software Vendor:

30.86M nginx
25.84M Apache
21.61M Microsoft
21.21M OpenBSD
18.82M Squid Cache

More

Software Product:

54.71M linux
30.86M nginx
24.37M HTTPD
21.75M linux

Hosts

Results: 223,457,367 Time: 0.00s

1.0.0.0

CLOUDFLARENET (13335) Australia
80/HTTP 443/HTTP

1.0.0.1 (one.one.one.one)

CLOUDFLARENET (13335) Australia
53/DNS 80/HTTP 443/HTTP

1.0.0.2

CLOUDFLARENET (13335) Australia
53/DNS 80/HTTP 443/HTTP

1.0.0.3

CLOUDFLARENET (13335) Australia
53/DNS 80/HTTP 443/HTTP

1.0.0.4

CLOUDFLARENET (13335) Australia
80/HTTP 443/HTTP

1.0.0.5

CLOUDFLARENET (13335) Australia
80/HTTP 443/HTTP

1.0.0.6

CLOUDFLARENET (13335) Australia
80/HTTP 443/HTTP

1.0.0.7

CLOUDFLARENET (13335) Australia
80/HTTP 443/HTTP

1.0.0.8

CLOUDFLARENET (13335) Australia
80/HTTP 443/HTTP

1.0.0.9

CLOUDFLARENET (13335) Australia
80/HTTP 443/HTTP

1.0.0.10

CLOUDFLARENET (13335) Australia
80/HTTP 443/HTTP

1.0.0.11

- “Internet search engines” exist to help map and track all services on the Internet
- Companies operating Internet search engines scan the Internet for you

TOTAL RESULTS

5,886,146

TOP COUNTRIES



United States	987,894
Viet Nam	373,306
United Kingdom	294,580
Germany	268,283
China	235,469
More...	

TOP PORTS

80	1,949,772
81	414,584
443	242,032
8080	160,375
82	148,393
More...	

TOP ORGANIZATIONS

Amazon Technologies Inc.	279,565
Viettel Group	164,143
Amazon.com, Inc.	158,481
Vietnam Posts and Telecommunications Group	140,441
Korea Telecom	104,785
More...	

TOP PRODUCTS

Hikvision IP Camera	3,351,931
Apache httpd	80,231
Apache Advanced Extranet Server httpd	76,057
nginx	68,431
TruVision NVR/DVR/IP Camera	29,147

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

Security check

104.16.51.111
Cloudflare, Inc.
United States, San Francisco

cdn

SSL Certificate

Issued By:
Common Name:
Cloudflare Inc ECC CA-3

Organization:
Cloudflare, Inc.

Issued To:
Common Name:
endgameinc.zendesk.com

Organization:
Cloudflare, Inc.

Supported SSL Versions:
TLSv1.2

HTTP/1.1 403 Forbidden

Date: Fri, 29 Oct 2021 17:38:19 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: close
CF-Chl-Bypass: 1
Permissions-Policy: accelerometer=(),autoplay=(),camera=(),clipboard-read=(),clipboard-write=(),fullscreen=(),geolocation=(),gyrosc...

2021-10-

301 Moved Permanently

141.90.14.228
finanzamt-marburg-biedenkopf.hessen.de
Wiesbaden
Germany, Wiesbaden

SSL Certificate

Issued By:
Common Name:
SwissSign Server Gold CA 2014 - GZ2

Organization:
SwissSign AG

Issued To:
Common Name:
p2.hessen.de

Organization:
Land Hessen

Supported SSL Versions:
TLSv1.2, TLSv1.3

HTTP/1.1 301 Moved Permanently

Strict-Transport-Security: max-age=15768000
Date: Fri, 29 Oct 2021 17:36:14 GMT
Server: Apache
Referrer-Policy: no-referrer-when-downgrade
X-Xss-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src https; data: 'unsafe-in...

2021-10-

52.55.45.182

ec2-52-55-45-182.compute-1.amazonaws.com
Amazon Technologies Inc.
United States, Ashburn

cloud

SSL Certificate

Issued By:
Common Name:
Amazon

Organization:
Amazon

Issued To:
Common Name:
pursultdealerstore.com

HTTP/1.1 302 302

Date: Fri, 29 Oct 2021 17:34:53 GMT
Content-Length: 0
Connection: keep-alive
Set-Cookie: JSESSIONID=BCE4BF7379EEB7DA72D4E5181548140E; Path=/; secure; HttpOnly; SameSite=None; Secure; HttpOnly
Set-Cookie: navigation-20201211483--14379359801635528893733; Path=/./; secure; Http...

2021-10-

Internet Scanning

- Researchers use Internet scanning to:
 - Uncover new attacks (e.g., DDoS amplification techniques, email delivery security)
 - Understand botnets (Mirai)
 - Find cryptographic weaknesses (TLS, SSH, Web PKI)
 - Examine industrial control system/ IoT deployment
 - Study censorship
 - Measure operator behavior

Internet Scanning

- Researchers use Internet scanning to:
 - Uncover new attacks (e.g., DDoS amplification techniques, email delivery security)
 - Understand botnets (Mirai)
 - Find cryptographic weaknesses (TLS, SSH, Web PKI)
 - Examine industrial control system/ IoT deployment
 - Study censorship
 - Measure operator behavior

- Attackers use Internet scanning to:
 - Find and exploit services

Common practices for good Internet scanning citizenship

- Slow down scanning speeds to not overwhelm end networks (major bottleneck in Internet scanning)
 - You might have a 40Gb/s link--but you should not be scanning at 40Gb/s, or you might denial of service a small end-network

Common practices for good Internet scanning citizenship

- Slow down scanning speeds to not overwhelm end networks (major bottleneck in Internet scanning)
 - You might have a 40Gb/s link--but you should not be scanning at 40Gb/s, or you might denial of service a small end-network
- Configure source scanning address to
 - (1) point to a DNS record that indicates the scanning is a part of a research study (e.g., research.esrg.stanford.edu)
 - (2) host a webpage that explains the nature of scans
 - (3) provide an email address that can be contacted to request exclusion from future scans

Common practices for good Internet scanning citizenship

- Slow down scanning speeds to not overwhelm end networks (major bottleneck in Internet scanning)
 - You might have a 40Gb/s link--but you should not be scanning at 40Gb/s, or you might denial of service a small end-network
- Configure source scanning address to
 - (1) point to a DNS record that indicates the scanning is a part of a research study (e.g., research.esrg.stanford.edu)
 - (2) host a webpage that explains the nature of scans
 - (3) provide an email address that can be contacted to request exclusion from future scans



Stanford University

Why am I receiving connection attempts from this host?

These connections are part of a long-term computer science research project at Stanford University. This research involves making a small number of harmless connection attempts to every publicly accessible computer worldwide each day. This allows scientists to measure the global Internet and analyze trends in technology deployment and security.

As part of this research, every public IP address receives a handful of packets on common ports. These consist of standard connection attempts followed by RFC-compliant protocol handshakes with responsive hosts. We never attempt to exploit security problems, guess passwords, or change device configurations. We only receive data that is publicly visible to anyone who connects to a particular address and port.

Why are you collecting this data?

How did DarkSide infiltrate Colonial Pipeline?

How did DarkSide infiltrate Colonial Pipeline?

- “RockYou2021” password leak (~8.2 billion credentials) on the dark web
 - Contained an outdated, but still used, credential to a Colonial Pipeline Virtual Private Network (VPN)
 - Businesses typically use a VPN **to give remote employees access to internal applications and data**, or to create a single shared network between multiple office locations.

"It was a complicated password, I want to be clear on that. It was not a Colonial123-type password." - Colonial Pipeline CEO in Senate Hearing











!;--have i been pwned?

Check if your email or phone is in a data breach











email or phone (international format)

pwned?

Largest breaches

	772,904,991 Collection #1 accounts
	763,117,241 Verifications.io accounts
	711,477,622 Onliner Spambot accounts
	622,161,052 Data Enrichment Exposure From PDL Customer accounts
	593,427,119 Exploit.In accounts
	509,458,528 Facebook accounts
	457,962,538 Anti Public Combo List accounts
	393,430,309 River City Media Spam List accounts
	359,420,698 MySpace accounts
	268,765,495 Wattpad accounts

Recently added breaches

	3,117,548 CoinMarketCap accounts
	228,102 Thingiverse accounts
	50,538 Playbook accounts
	66,479 Fantasy Football Hub accounts
	72,596 Republican Party of Texas accounts
	125,698,496 LinkedIn Scraped Data accounts
	266,399 Ajarn accounts
	15,003,961 Epik accounts
	20,154,583 IndiaMART accounts
	878,209 Imavex accounts

How did DarkSide infiltrate Colonial Pipeline?

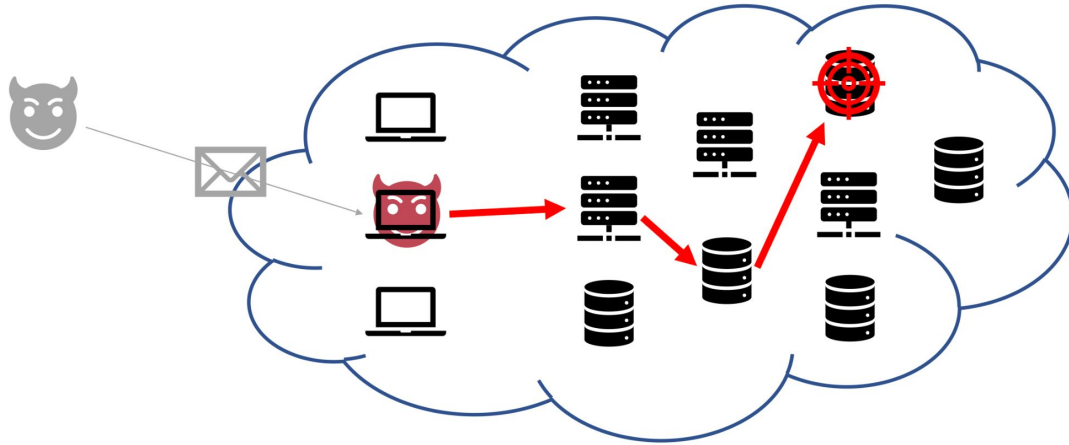
- “RockYou2021” password leak (~8.2 billion credentials) on the dark web
 - Contained an outdated, but still used, credential to a Colonial Pipeline VPN
 - Businesses typically use a VPN **to give remote employees access to internal applications and data**, or to create a single shared network between multiple office locations.
- Scanned to find all VPNs (e.g., port 427 if using VMware ESXi, port 3389 if searching for applications that use the Remote Desk Protocol)

How did DarkSide infiltrate Colonial Pipeline?

- “RockYou2021” password leak (~8.2 billion credentials) on the dark web
 - Contained an outdated, but still used, credential to a Colonial Pipeline VPN
 - Businesses typically use a VPN **to give remote employees access to internal applications and data**, or to create a single shared network between multiple office locations.
- Scanned to find all VPNs (e.g., port 427 if using VMware ESXi, port 3389 if searching for applications that use the Remote Desk Protocol)
- Try the Colonial Pipeline/leaked credentials
- Attempted the credential---no two-factor authentication (legacy VPN)---so it just worked!
- Direct access to internal network/systems/files.

Once inside a network, attackers “laterally move”

Lateral Movement:
Attacker movement *between* internal machines



5

Hopper: Modeling and Detecting Lateral Movement

Grant Ho, *UC San Diego, UC Berkeley, and Dropbox*; Mayank Dhiman, *Dropbox*;
Devdatta Akhawe, *Figma, Inc.*; Vern Paxson, *UC Berkeley and International
Computer Science Institute*; Stefan Savage and Geoffrey M. Voelker,
UC San Diego; David Wagner, *UC Berkeley*

<https://www.usenix.org/conference/usenixsecurity21/presentation/ho>

Lateral Movement

- (1) Reconnaissance: explore and map the network (e.g., netstat, ifconfig, arp cache, ip tables...)
- (2) Privilege Escalation: gain access to the credentials needed to log into the next server (e.g., social engineering, exploit)
- (3) Movement

DarkSide succeeds in lateral movement...and
begins encrypting ~100GB of their files

Aftermath of Colonial Pipeline Hack

- Colonial Pipeline shuts down to stop lateral movement / ransomware spread
- FBI, CISA, DoE, DHS all notified
- Colonial Pipeline pays ransom
 - It is illegal for companies to pay ransom to terrorist organizations, but it is not illegal (only “advised against”) to pay ransoms in general

Aftermath of Colonial Pipeline Hack

- Colonial Pipeline shuts down to stop lateral movement / ransomware spread
- FBI, CISA, DoE, DHS all notified
- Colonial Pipeline pays ransom
 - It is illegal for companies to pay ransom to terrorist organizations, but it is not illegal (only “advised against”) to pay ransoms in general
- Colonial ends up using its own back-ups to restore data



Aftermath of Colonial Pipeline Hack

- Colonial Pipeline shuts down to stop lateral movement / ransomware spread
- FBI, CISA, DoE, DHS all notified
- Colonial Pipeline pays ransom
 - It is illegal for companies to pay ransom to terrorist organizations, but it is not illegal (only “advised against”) to pay ransoms in general
- Colonial ends up using its own back-ups to restore data
- DarkSide regrets going high-profile



Aftermath of Colonial Pipeline Hack

- Colonial Pipeline shuts down to stop lateral movement / ransomware spread
- FBI, CISA, DoE, DHS all notified
- Colonial Pipeline pays ransom
 - It is illegal for companies to pay ransom to terrorist organizations, but it is not illegal (only “advised against”) to pay ransoms in general
- Colonial ends up using its own back-ups to restore data
- DarkSide regrets going high-profile
- FBI recovers some of the ransom money (blockchain analysis + secrets)



Mashable Black Friday Tech Life Social Good Entertainment Deals

Tech Bitcoin

Colonial Pipeline reportedly paid millions for slow-ass decryption software

The company reportedly forked over nearly \$5 million worth of bitcoin.

By Jack Morse on May 13, 2021 f t q



MOTHERBOARD
TECH BY VICE

Pipeline Hackers Say They're 'Apolitical,' Will Choose Targets More Carefully Next Time

"Our goal is to make money, and not creating problems for society," the statement continues.



npr NEWSLETTERS SIGN IN NPR SHOP DONATE

NEWS CULTURE MUSIC PODCASTS & SHOWS SEARCH

NATIONAL

How A New Team Of Feds Hacked The Hackers And Got Colonial Pipeline's Ransom Back

JUNE 8, 2021 · 2:08 AM ET

 Vanessa Romo

DarkSide has used more sophisticated ways to gain access to networks...

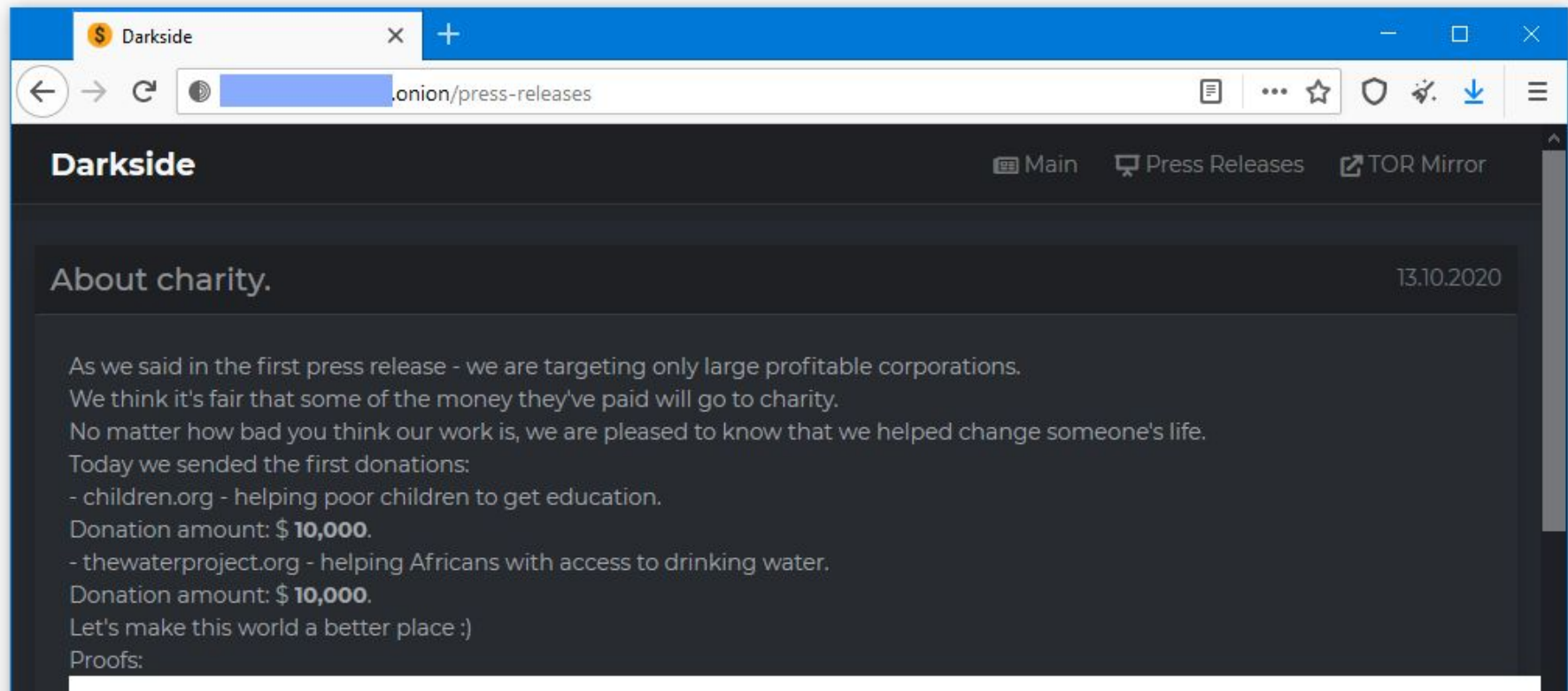
- Critical VPN/ Remote Access tools CVEs (Common Vulnerabilities and Exposures)
 - [CVE-2021-20016](#) : “A SQL-Injection vulnerability in the SonicWall SSLVPN SMA100 product allows a remote unauthenticated attacker to perform SQL query to achieve remote control execution”
 - [CVE-2019-554/ CVE-2020-3992](#): Targets a use-after-free bug in VMware ESXi that allows an attacker to achieve remote control execution



May 2021 (Shodan)

<https://cybersecurityworks.com/blog/ransomware/darkside-the-ransomware-that-brought-a-us-pipeline-to-a-halt.html>

The BrightSide of DarkSide



An increasingly common variation: software
supply chain attacks

MOVEit ransomware attacks - 2023

- Zero-day SQL injection vulnerability in MOVEit file transfer software
 - New CVE, old OWASP vulnerability class
- Cl0p ransomware gang seem to have developed attack for ~2 years before mass-exploiting organizations using MOVEit

MOVEit ransomware attacks - 2023

- Zero-day SQL injection vulnerability in MOVEit file transfer software
 - New CVE, old OWASP vulnerability class
- Cl0p ransomware gang seem to have developed attack for ~2 years before mass-exploiting organizations using MOVEit
- Hundreds of organizations affected, including British Airways, the BBC, Shell, Ernst & Young, US Medicare/Medicaid Services, US Department of Energy... and Stanford Healthcare and LPCH

WIRED BACKCHANNEL BUSINESS CULTURE GEAR IDEAS POLITICS SCIENCE SECURITY MERCH SIGN IN SUBSCRIBE

LILY HAY NEWMAN SECURITY JUN 16, 2023 5:25 PM

A Russia-Based Hacking Rampage Hits US Agencies and Exposes Millions

The ransomware gang Cl0p exploited a vulnerability in a file transfer service. The flaw is now patched, but the damage is still coming into focus.

The Register

MOVEit victim count latest: 2.6K+ orgs hit, 77M+ people's data stolen

Real-life impact of buggy software laid bare – plus: Avast tries to profit from being caught up in attacks

Jessica Lyons

Mon 20 Nov 2023 20:39 UTC

MOVEit ransomware attacks - 2023

- Zero-day SQL injection vulnerability in MOVEit file transfer software
 - New MOVEit vulnerability class
- Cl0p ransomware group seem to have developed attack vectors for mass-email phishing campaigns using MOVEit
- Hundreds of organizations affected, including British Airways, the BBC, Shell, Ernst & Young, US Medicare/Medicaid Services, US Department of Energy... and Stanford Healthcare and LPCH

Via Maximus (govt health tech services contractor)

Via Zellis (payroll services provider)

Via Welltok (patient engagement & wellness platform)

WIRED BACKCHANNEL BUSINESS CULTURE GEAR IDEAS POLITICS SCIENCE MERCH SIGN IN SUBSCRIBE

LILY HAY NEWMAN SECURITY JUN 16, 2023 5:25 PM

A Russia-Based Hacking Ransomware Gang and Exposes Millions

The ransomware gang Cl0p exploited a vulnerability in a file transfer service. The flaw is now patched, but the damage is still coming into focus.

The Register

MOVEit victim count latest: 2.6K+ orgs hit, 77M+ people's data stolen

Real-life impact of buggy software laid bare – plus: Avast tries to profit from being caught up in attacks

Jessica Lyons

Mon 20 Nov 2023 20:39 UTC

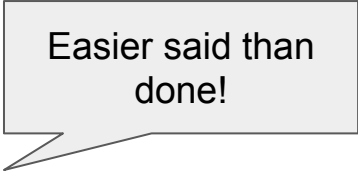
MOVEit ransomware attacks - 2023

- MOVEit issued a patch quickly and organizations scrambled to apply it, but attackers were faster
- Cl0p has demanded money from organizations in exchange for not leaking all their data
- Many leaks subsequently happened

How should one protect an Internet service
from Internet Scans?

Defenses against Internet Scanning

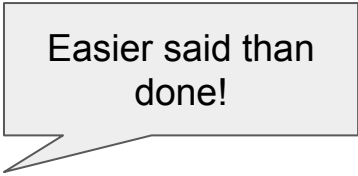
- Don't expose unnecessary services to the public internet
- Use 2FA to minimize impact of a compromised credential
- Constantly upgrade (CVEs get patched all the time)



Easier said than
done!

Defenses against Internet Scanning

- Don't expose unnecessary services to the public internet
- Use 2FA to minimize impact of a compromised credential
- Constantly upgrade (CVEs get patched all the time)

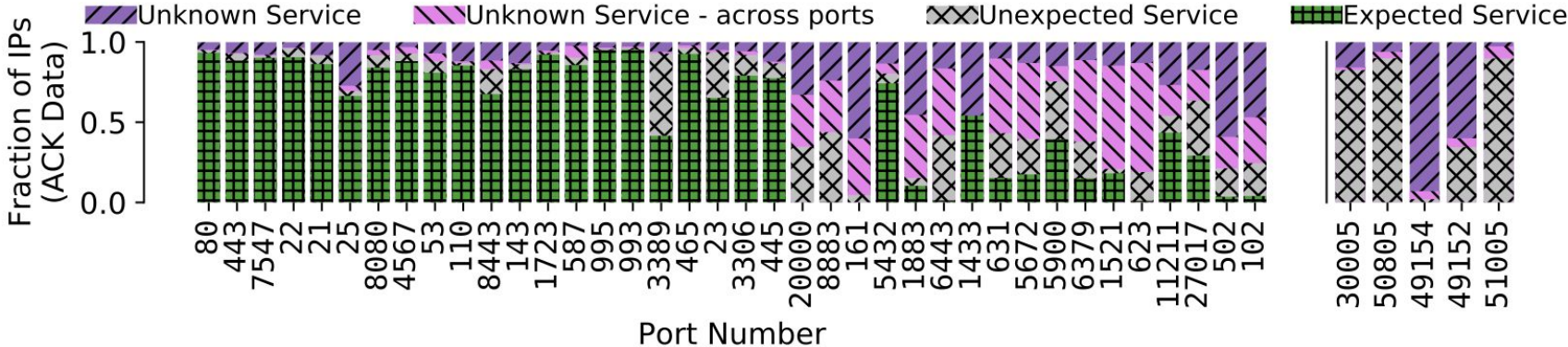


Easier said than
done!

Not a sufficient substitute (i.e., obscuring a service):

- Use IPv6 address
 - May show up in passive data sources (e.g., DNS, network taps)
- Use an unassigned/unexpected port
 - New scanners/techniques have been developed to find such hosts

People try security by obscurity, but are still findable



LZR: Identifying Unexpected Internet Services

Liz Izhikevich
Stanford University

Renata Teixeira
Inria, Paris*

Zakir Durumeric
Stanford University

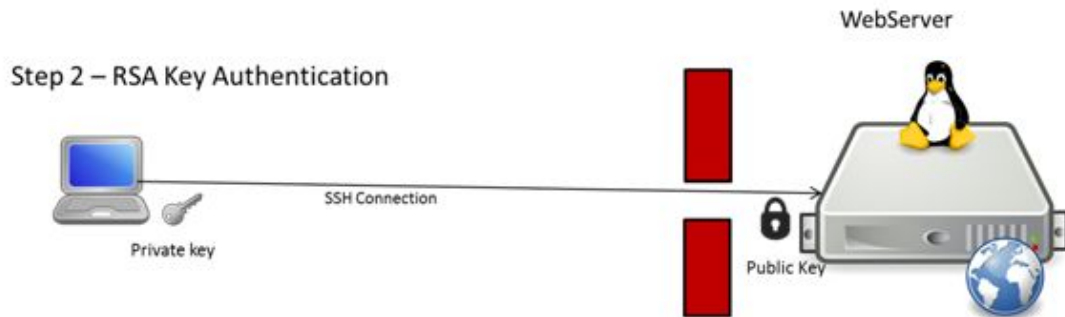
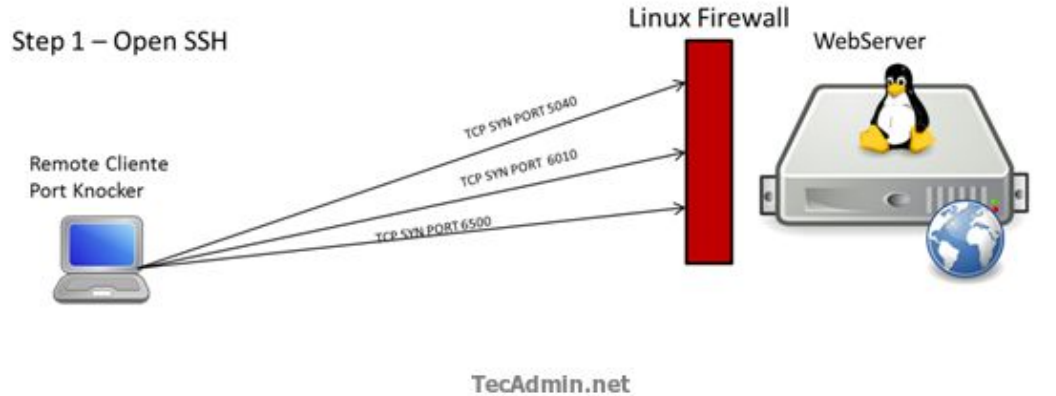
Predicting IPv4 Services Across All Ports

Liz Izhikevich
Stanford University

Renata Teixeira
Inria, Paris

Zakir Durumeric
Stanford University

Security Through Obscurity: Port Knocking



“Knock” on a sequence of ports before being allowed into the port that is hosting the service

- Unsolved: how to detect and bypass port knocking

Where do other attackers originate?
What do they target?

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



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, 0x04000000, 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;
}
```

Why do hacker groups generally operate out of Russia, North Korea, China?

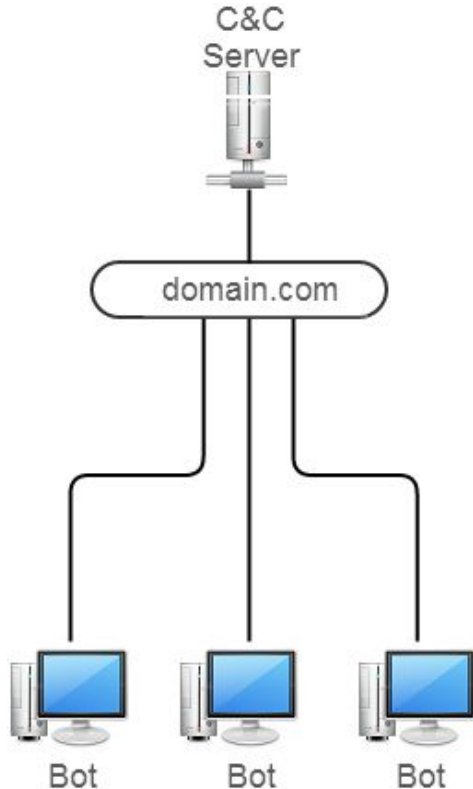
- “Anti-western” philosophies
- Good STEM education
- Russia in particular: Russian law only applies to crime against Russia
 - No pushback from government; sometimes, even encouragement
- North Korea in particular: Goal is to fund nuclear weapons program despite international sanctions



Installing a Russian keyboard deters Russian attackers from compromising the device

How are botnets/“contagions” designed from a systems perspective?

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

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

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

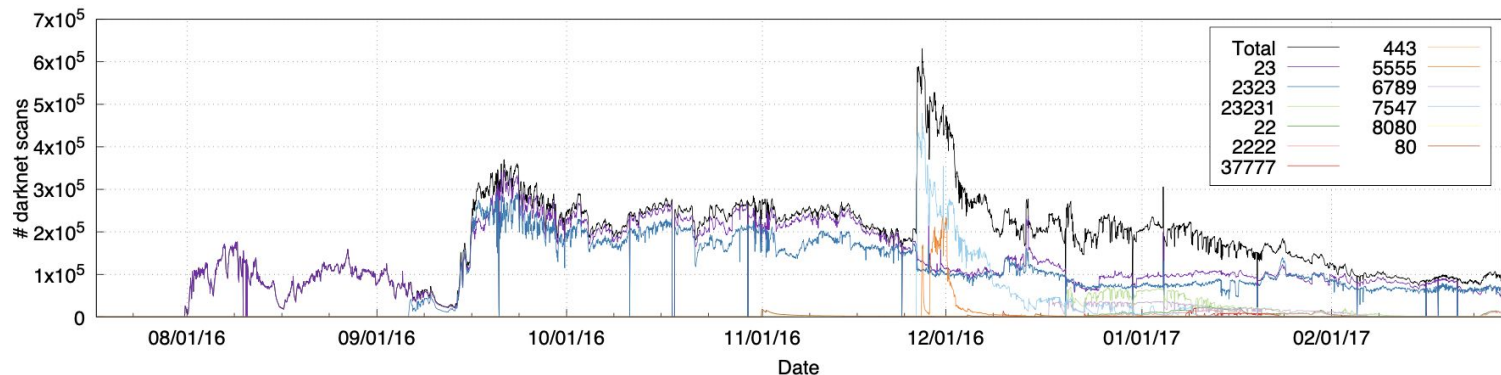
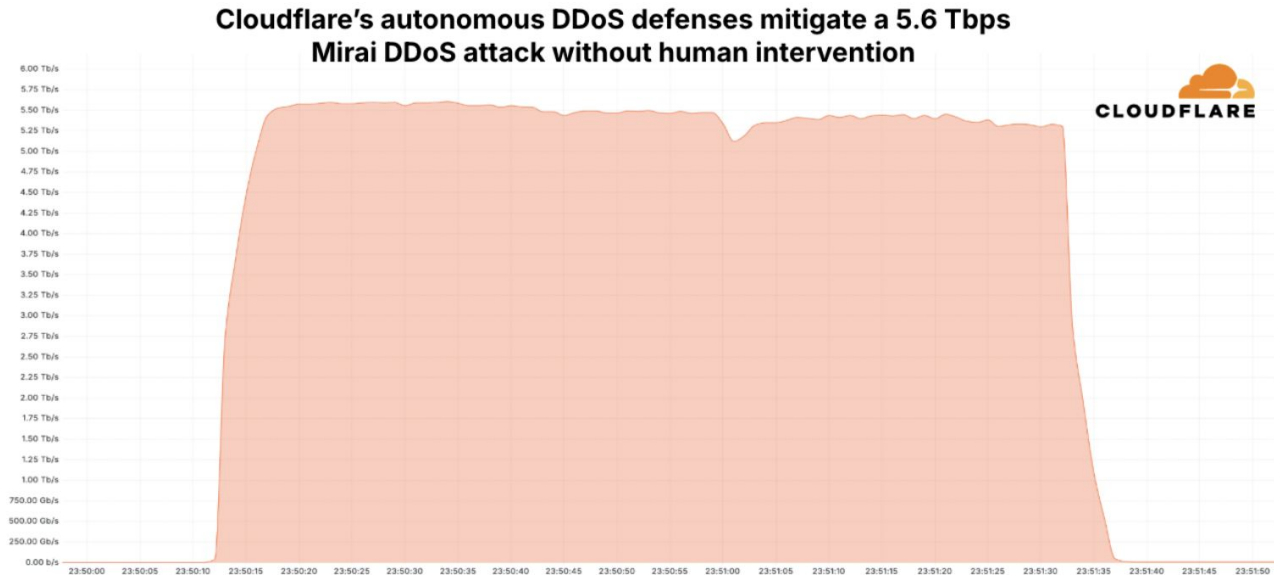


Figure 3: **Temporal Mirai Infections**—We estimate of the number of Mirai-infected devices over time by tracking the number of hosts actively scanning with Mirai fingerprint at the start of every hour. Mirai started by scanning Telnet, and variants evolved to target 11 additional protocols. The total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

Mirai is still active

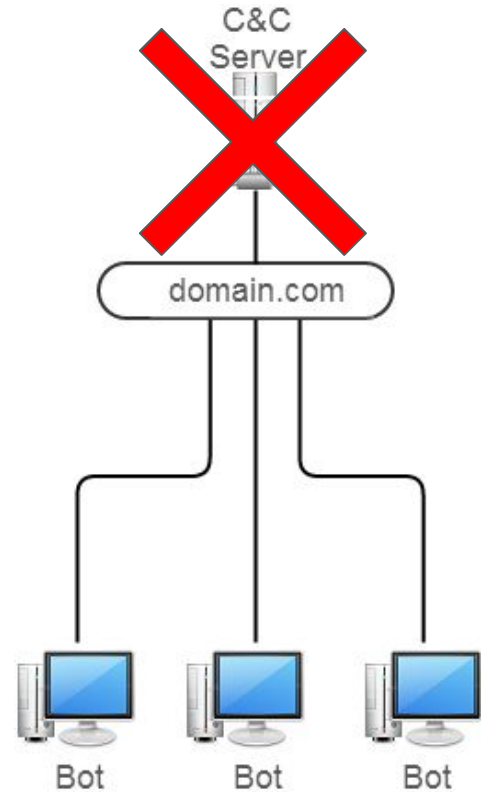
October 2024: Largest DDoS attack on record caused by Mirai variant



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

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



The screenshot shows the official website of the U.S. Department of Justice, Office of Public Affairs. The header includes the department's logo, name, and navigation links for 'Our Offices', 'Find Help', and 'Contact Us'. A search bar is also present. Below the header is a dark navigation bar with links for 'About', 'News', 'Documents', 'Internships', 'FOIA', 'Contact', and 'Information for Journalists'. The main content area features a breadcrumb trail: '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)'. On the left, a 'News' sidebar lists categories: 'All News', 'Blogs', 'Photo Galleries', 'Podcasts', 'Press Releases' (highlighted), and 'Speeches'. The main article is titled 'Justice Department Conducts Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate of the General Staff (GRU)' and is dated 'Thursday, February 15, 2024'. A 'For Immediate Release' badge is visible in the bottom right corner.

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 > Justice Department Conducts Court-Authorized Disruption of Botnet Controlled By The Russian Federation's Main Intelligence Directorate of The General Staff (GRU)

News

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



The screenshot shows the official website of the U.S. Department of Justice, Office of Public Affairs. The header includes the department's seal, the text "Office of Public Affairs U.S. Department of Justice", and navigation links for "Our Offices", "Find Help", and "Contact Us". A search bar is located on the right. Below the header is a dark navigation bar with links for "About", "News", "Documents", "Internships", "FOIA", "Contact", and "Information for Journalists". A breadcrumb trail reads: "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**

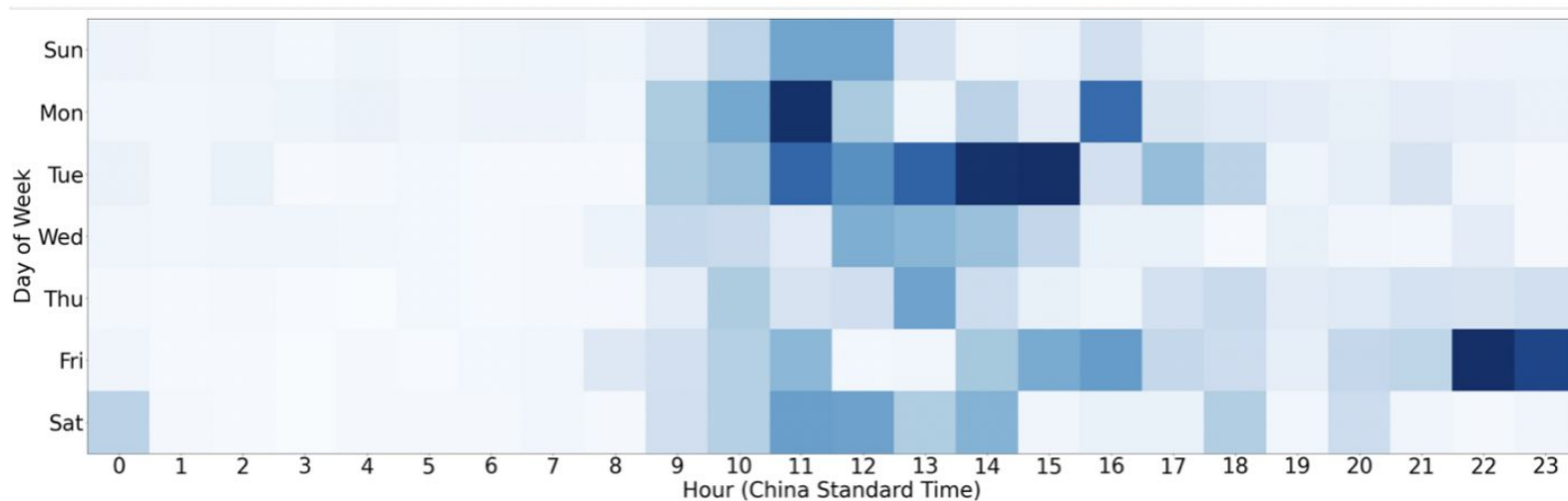
PRESS RELEASE

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

Wednesday, January 31, 2024

For Immediate Release

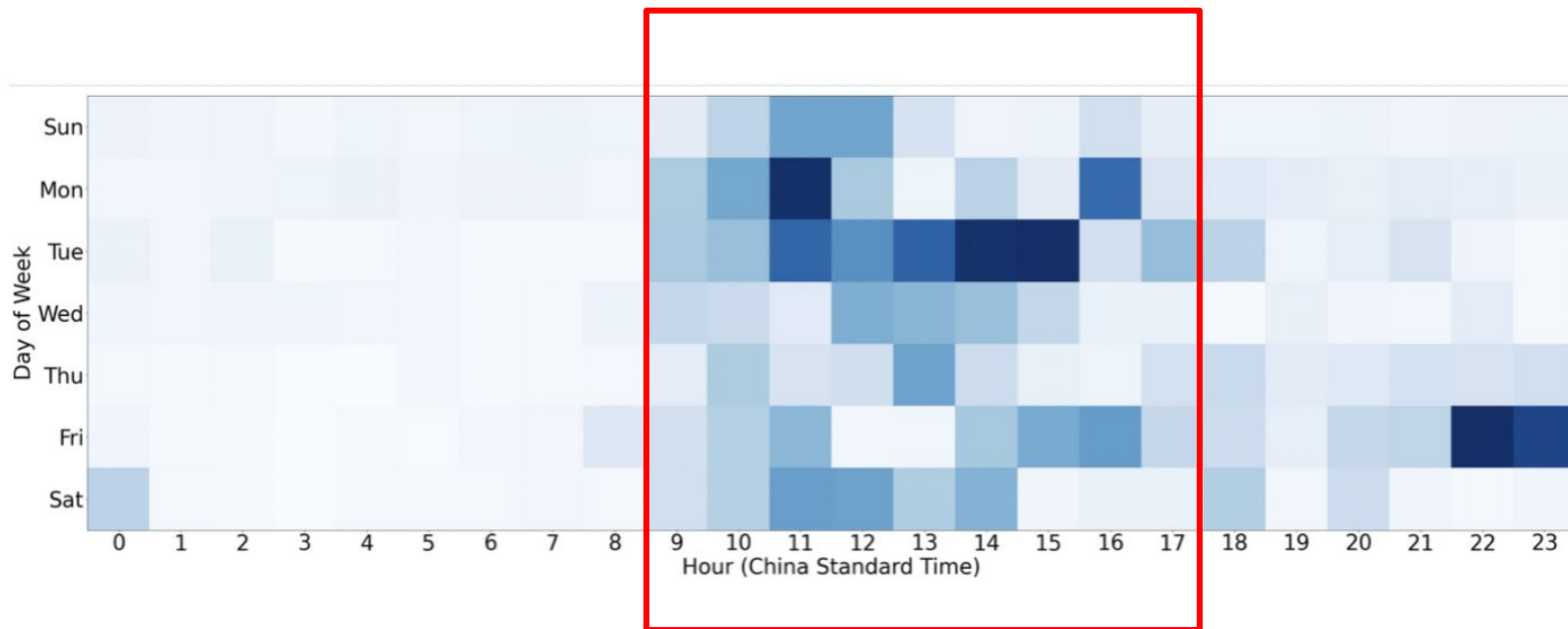
Sidenote: State-sponsored hacker working hours



Source:

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

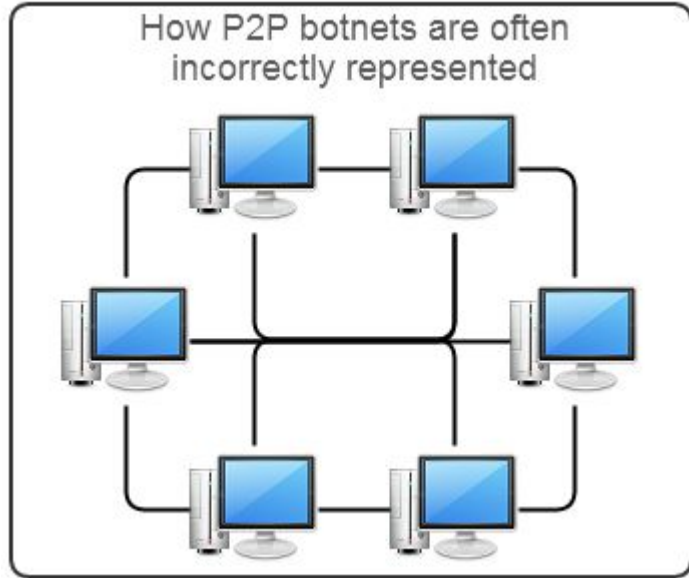
Sidenote: State-sponsored hacker working hours



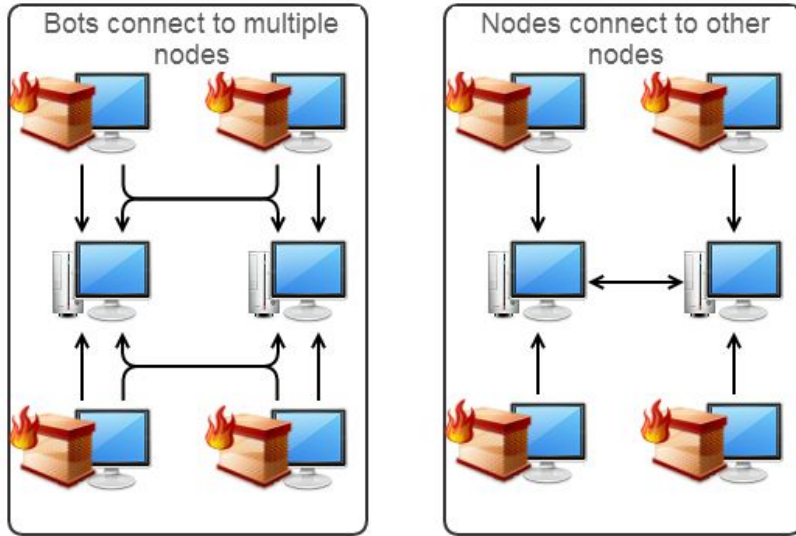
Source:
<https://blog.lumen.com/routers-roasting-on-an-open-firewall-the-kv-botnet-investigation/>

They're working a 9-5 job!

Peer2Peer Botnet Anatomy

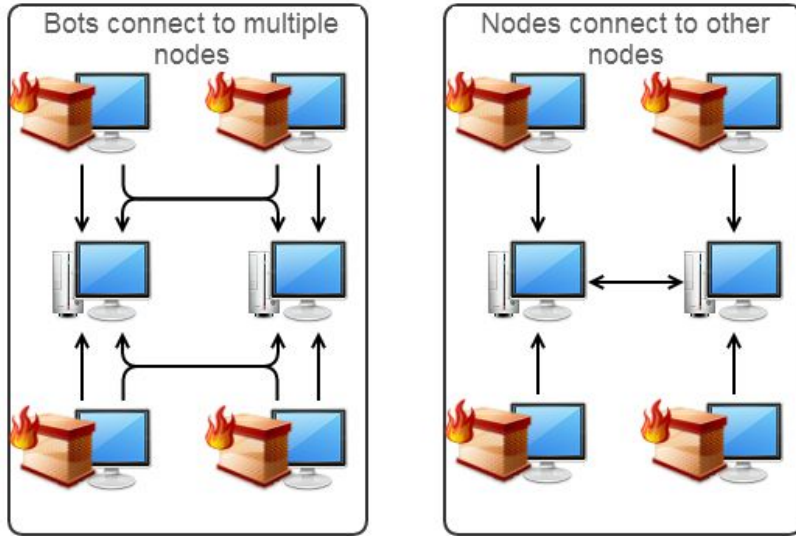


Peer2Peer Botnet Anatomy



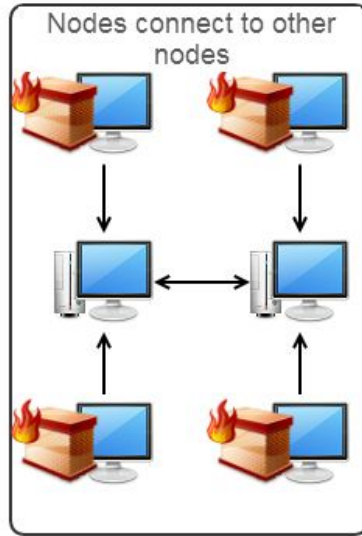
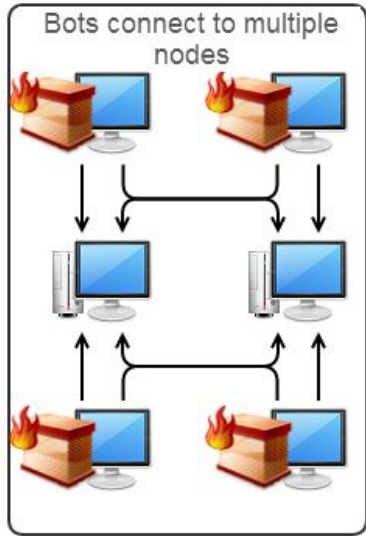
- **“Nodes/Peers”**: Servers that are able to receive incoming connections (i.e., not behind a NAT/Firewall)
- **“Workers”**: Servers that cannot receive incoming connections
- Commands circulate the P2P network by passing commands between peers
 - Commands get passed to a worker once it reaches out

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

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

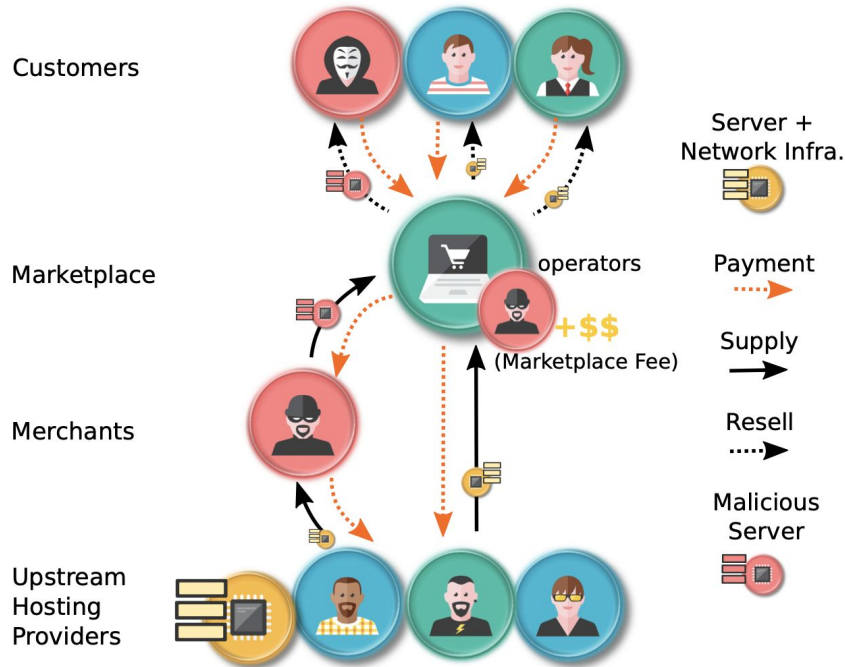
“Agile” hosting: rent/resell infrastructure from legitimate (cheap, often under-invest in security) ISPs

(+) 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

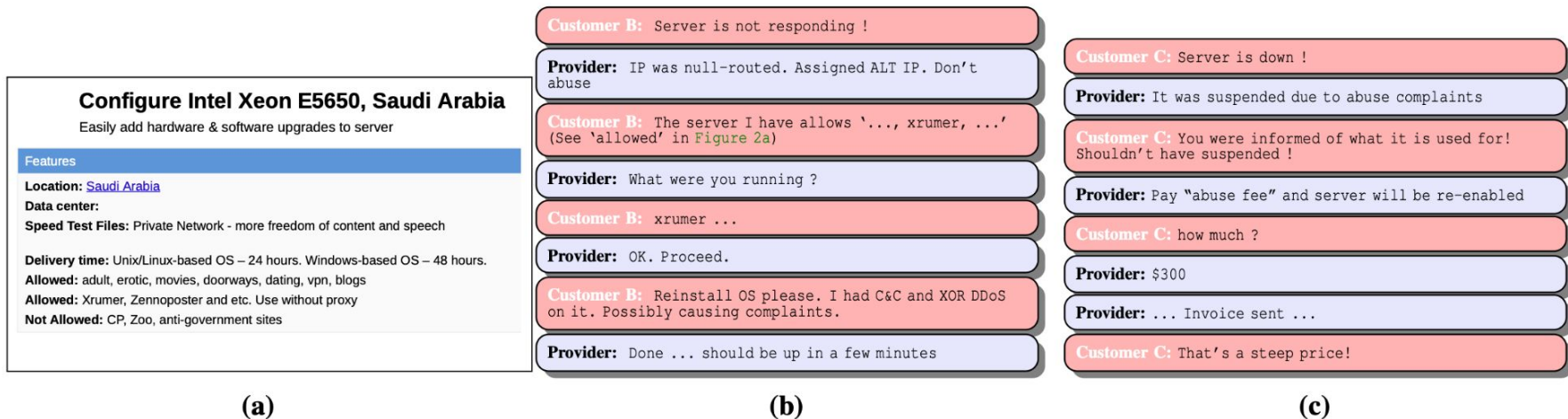


Figure 2: Examples of MaxiDed's bullet-proof behavior. (a) screenshot of server publicly advertised to customers. (b) and (c) are excerpts of a conversation between customer and administrator (edited for readability).

The End.

But take CS 155 and CS 356 if you want more!