Warning: This is the most evil lecture of them all
~this week in security~

a cybersecurity newsletter by @zackwhittaker

volume 4, issue 41

View this email in your browser

~ ~
Core member of ransomware gang identified

Ransomware groups extort billions but almost never get caught. In a rare success German police were able to identify a member of one of the most notorious hacker gangs.

Von Kai Biermann

28. Oktober 2021, 13:55 Uhr / ZEIT ONLINE
A Rare Win in the Cat-and-Mouse Game of Ransomware

A team of private security sleuths, in their first public detailing of their efforts, discuss how they used cybercriminals’ mistakes to quietly help victims recover their data.

Fuel storage tanks connected to the Colonial Pipeline system in Baltimore. Colonial paid nearly $5 million to hackers to recover its stolen data. Samuel Corum/Bloomberg

By Nicole Perlroth

Oct. 24, 2021
How are network intrusion attacks orchestrated over the Internet?
How are network intrusion attacks orchestrated over the Internet?

Europol detains suspects behind LockerGoga, MegaCortex, and Dharma ransomware attacks

- Twelve members of a ransomware group were detained this week in Ukraine and Switzerland, Europol said.
- Suspects are believed to have orchestrated the ransomware attack that crippled aluminum provider Norsk Hydro in 2019.
- The group was linked to 1,800 ransomware attacks across 71 countries.

NRA responds to reports of Grief ransomware attack

The gun rights organization would not confirm or deny whether they had been hit with a ransomware attack.
U.S. federal investigators today raided the Florida offices of PAX Technology, a Chinese provider of point-of-sale devices used by millions of businesses and retailers globally. KrebsOnSecurity has learned the raid is tied to reports that PAX's systems may have been involved in cyberattacks on U.S. and E.U. organizations.

Several days ago, KrebsOnSecurity heard from a trusted source that the FBI began investigating PAX after a major U.S. payment processor started asking questions about unusual network packets originating from the company's payment terminals.

According to that source, the payment processor found that the PAX terminals were being used both as a malware "dropper" — a repository for malicious files — and as "command-and-control" locations for staging attacks and collecting information.
How are botnets and other distributed network attacks configured from a systems perspective?
In latest DMCA review, US Copyright Office eases rules on computer security research, right to repair

Game console fixes are limited – and there's no allowance for exploit tools

Among the changes is the removal of a passage that made the exemption for computer security research contingent upon "not violating any applicable law."

Security company Rapid7, among others, lobbied to have this passage purged because it created ambiguity for researchers [PDF]. The firm argued that security researchers, faced with looking into devices that might have hardware, mobile, and cloud components, each with its own end-user license agreement and jurisdiction, couldn't be sure which laws might apply.

"An increasing portion of contemporary computer security research involves collaboration among researchers across international borders," said John
Where do we draw the line on whitehat vs blackhat security research?

In latest DMCA review, US Copyright Office eases rules on computer security research, right to repair

Game console fixes are limited – and there's no allowance for exploit tools

Thomas Claburn in San Francisco
Fri 29 Oct 2021 // 00:07 UTC

Among the changes is the removal of a passage that made the exemption for computer security research contingent upon "not violating any applicable law."

Security company Rapid7, among others, lobbied to have this passage purged because it created ambiguity for researchers [PDF]. The firm argued that security researchers, faced with looking into devices that might have hardware, mobile, and cloud components, each with its own end-user license agreement and jurisdiction, couldn't be sure which laws might apply.

"An increasing portion of contemporary computer security research involves collaboration among researchers across international borders," said John"
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

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 cryptlockers. 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

Layer 4 Handshake: find all TCP responsive hosts

Client

ZMap

SYN

SYN/ACK

RST

Server

Port 80

HTTP
Most commonly used* TCP Internet scanning methodology

Layer 4 Handshake: find all TCP responsive hosts

Layer 7 Handshake: find what service is running on the host

**Client**

- ZMap
- HTTP
- ZGrab

**Server**

Port 80

- SYN
- SYN/ACK
- RST

```
HTTP/1.1 301 Moved Permanently
Vary: Accept-Encoding
Content-Type: text/html
Content-Length: 167
```

“HTTP GET/”

“Service Banner”
Layer 4 Internet scanning (continued)
Finding services using Internet scanning

IPv4: connect to all $\sim2^{32}$ IP addresses on a subset of “interesting” ports and protocols
(e.g., HTTP/80, TLS/443, TELNET/23)

- $\sim1$ 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!
"Internet search engines" exist to help map and track all services on the Internet.

Companies operating Internet search engines scan the Internet for you.
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)
  - Industrial control system/ IoT deployment
  - Censorship
  - 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)
  - Industrial control system/ IoT deployment
  - Censorship
  - 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) provides 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 research.esrg.stanford.edu
  - (2) host a webpage that explains the nature
  - (3) provides an email address that can be c

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 could DarkSide infiltrate colonial pipeline?
How could 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
- 268,399 Ajarn accounts
- 15,003,961 Epik accounts
- 20,154,583 IndiaMART accounts
- 878,209 Imavex accounts
How could 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 could 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

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 beings encrypting ~100GB of their files
Aftermath of Colonial Pipeline Hack

- Colonial Pipeline shuts down the pipeline to stop lateral movement/the spread of ransomware
- FBI, CISA, DoE, DoH 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 and the spread of ransomware
- FBI, CISA, DoE, DoH 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

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
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
Covid: The Rise of Remote Work

In Q1 2021, Nuspire (a cybersecurity firm) witnessed a 1,916% increase in attacks against Fortinet’s SSL-VPN (CVE-2018-13379) and a 1,527% increase in Pulse Connect Secure VPN (CVE-2019-11510) when analyzing 90 billion traffic logs.

How should one protect an Internet service from Internet Scans?
Defenses against Internet Scanning

- Don’t expose unnecessary services to the public internet
- Constantly upgrade (CVEs get patched all the time)
Defenses against Internet Scanning

- Don’t expose unnecessary services to the public internet
- Constantly upgrade (CVEs get patched all the time)

Not “good-practice” defenses (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
How to detect unassigned port usage

How to detect port 80 is actually hosting SSH?
How to detect unassigned port usage

How to detect port 80 is actually hosting SSH?

Use LZR (a system for identifying unexpected Internet services)

- sends specially crafted network packets to fingerprint the running service
- can detect up to 18 unique popular protocols (HTTP, SSH, TLS, etc) with 1 packet
How to detect unassigned port usage

How to detect port 80 is actually hosting SSH?

Use LZR (a system for identifying unexpected Internet services)

- sends specially crafted network packets to fingerprint the running service
- can detect up to 18 unique popular protocols (HTTP, SSH, TLS, etc) with 1 packet

How to detect that an IoT manufacturer configured a group of devices to use port 12345 to host Telnet?
How to detect unassigned port usage

How to detect port 80 is actually hosting SSH?

Use LZR (a system for identifying unexpected Internet services)

- sends specially crafted network packets to fingerprint the running service
- can detect up to 18 unique popular protocols (HTTP, SSH, TLS, etc) with 1 packet

How to detect that an IoT manufacturer configured a group of devices to use port 12345 to host Telnet?

Use GPS (a system for discovering IPv4 services across all ports)

- Using a small “seed scan”, detects patterns of port usage (by computing massive conditional probabilities) for groups of devices
How to detect unassigned port usage

- How to detect an individual operator decision to assign a single service to a random port?
  - Passive data source
  - Brute force scanning
  - ??
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
The BrightSide of DarkSide

About charity.

As we said in the first press release - we are targeting only large profitable corporations. We think it's fair that some of the money they've paid will go to charity. No matter how bad you think our work is, we are pleased to know that we helped change someone's life. Today we sended the first donations:
- children.org - helping poor children to get education.
  Donation amount: $10,000.
- thewaterproject.org - helping Africans with access to drinking water.
  Donation amount: $10,000.
Let's make this world a better place :)
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

**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.
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)
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 push back from Government. Sometimes, even encouragement

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/](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
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.
Peer2Peer Botnet Anatomy

How P2P botnets are often incorrectly represented
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 “malicious” peers into the network
  - Introduce by advertise the peer as a new “infected” peer
  - “malicious” : peers with the intention of taking down the botnet
- Have the peers provide workers with peer IP addresses that only belong to “malicious” peers
- “Malicious” peers/workers will soon become a majority of the network
- at some point, use “malicious” 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 Man-in-the-middle and spoofing attacks!
Bulletproof Hosting
Bulletproof Hosting

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

- Maxided uses 395 unique upstream ASes
- $3.3M revenue
### Configure Intel Xeon E5650, Saudi Arabia

**Easily add hardware & software upgrades to server**

<table>
<thead>
<tr>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Location:</strong> Saudi Arabia</td>
</tr>
<tr>
<td><strong>Data center:</strong></td>
</tr>
<tr>
<td><strong>Speed Test Files:</strong> Private Network - more freedom of content and speech</td>
</tr>
<tr>
<td><strong>Delivery time:</strong> Unix/Linux-based OS – 24 hours, Windows-based OS – 48 hours</td>
</tr>
<tr>
<td><strong>Allowed:</strong> adult, erotic, movies, doorways, dating, vpn, blogs</td>
</tr>
<tr>
<td><strong>Allowed:</strong> Xrumer, Zennoposter and etc. Use without proxy</td>
</tr>
<tr>
<td><strong>Not Allowed:</strong> CP, Zoo, anti-government sites</td>
</tr>
</tbody>
</table>

---

**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)

**Customer B:** xrumer ...

**Provider:** What were you running?

**Customer B:** xrumer ...

**Provider:** OK. Proceed.

**Provider:** Reinstall OS please. I had C&C and XOR DDoS on it. Possibly causing complaints.

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

---

**Customer B:** Server is down!

**Provider:** It was suspended due to abuse complaints

**Customer B:** You were informed of what it is used for! Shouldn’t have suspended!

**Provider:** Pay “abuse fee” and server will be re-enabled

**Customer B:** how much?

**Provider:** $300

**Provider:** ... Invoice sent ...

**Customer B:** That’s a steep price!

---

**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).
“Neutral Hosting”
What terms of services/acceptable use policies should benign hosting providers have?

Specifically prohibit harassing or abusive content, including racially or ethnically offensive content

- e.g., OVH, Digital Ocean

Disavow sites that incite violence, but do not extend to hate speech or misinformation

- e.g., GoDaddy, Amazon, Unified Layer, WordPress, Fastly

Content-neutral: “cannot remove material from the Internet that is hosted by others”

- e.g., Cloudflare
What terms of services/ acceptable use policies should benign hosting providers have?

Specifically prohibit harassing or abusive content, including racially or ethnically offensive content

- e.g., OVH, Digital Ocean

Disavow sites that incite violence, but do not extend to hate speech or misinformation

- e.g., GoDaddy, Amazon, Unified Layer, WordPress, Fastly

Content-neutral: “cannot remove material from the Internet that is hosted by others”

- e.g., Cloudflare
Misinformation

- extreme bias
  - (breitbart.com)
- peddle conspiracy theories or bigoted pro-paganda
  - (infowars.com, barenakedislam.com)
- promote junk science
  - (naturalnews.com).
Misinformation has real-world consequences and costs lives

For example, study shows that believing misinformation is correlated with resisting vaccines

Which of the following vaccine beliefs that routinely circulate on social media are true?

- COVID-19 vaccines will alter people’s DNA;
- COVID-19 vaccines contain microchips that could track people;
- COVID-19 vaccines contain the lung tissue of aborted fetuses;
- And COVID-19 vaccines can cause infertility, making it more difficult to get pregnant.
Misinformation websites often migrate to Cloudflare to seek protection from vigilante DDoS attacks

<table>
<thead>
<tr>
<th>Cloudflare Sites</th>
<th>Attack</th>
<th>Cloudflare Migration</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Date</td>
<td>Post-Attack</td>
</tr>
<tr>
<td>barenakedislam.com</td>
<td>2/4/15</td>
<td>8/31/17</td>
</tr>
<tr>
<td>drudgereport.com</td>
<td>12/30/16</td>
<td>1/4/17</td>
</tr>
<tr>
<td>frontpagemag.com</td>
<td>3/23/15</td>
<td>3/24/15</td>
</tr>
<tr>
<td>godlikeproductions.com</td>
<td>4/13/16</td>
<td>8/9/17</td>
</tr>
<tr>
<td>naturalnews.com</td>
<td>8/8/17</td>
<td>8/8/17</td>
</tr>
<tr>
<td>off-guardian.org</td>
<td>9/26/19</td>
<td>5/6/19</td>
</tr>
<tr>
<td>returnofkings.com</td>
<td>9/2/15</td>
<td>10/23/14</td>
</tr>
<tr>
<td>russia-insider.com</td>
<td>4/11/18</td>
<td>4/13/18</td>
</tr>
<tr>
<td>thegatewaypundit.com</td>
<td>4/15/18</td>
<td>6/12/15</td>
</tr>
<tr>
<td>weaselzippers.us</td>
<td>1/5/15</td>
<td>1/1/14</td>
</tr>
<tr>
<td>infostormer.com</td>
<td>12/7/19</td>
<td>8/15/17</td>
</tr>
</tbody>
</table>

Table 5: DDoS Attacks Against Cloudflare Misinformation Sites—Misinformation sites with known DDoS attack history and when they were first observed using Cloudflare hosting in our dataset.

- Misinformation websites are 1.7x more likely to be hosted on Cloudflare compared to a mainstream site (due to free DDoS protections)
A handful of advertisers disproportionately support misinformation

<table>
<thead>
<tr>
<th>Ad Provider</th>
<th>Misinformation with Ads</th>
<th>Mainstream with Ads</th>
<th>Effect Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>RevContent</td>
<td>22.8%</td>
<td>0.2%</td>
<td>0.91</td>
</tr>
<tr>
<td>DoubleClick</td>
<td>34.4%</td>
<td>14.1%</td>
<td>0.48</td>
</tr>
<tr>
<td>Outbrain</td>
<td>8.0%</td>
<td>1.5%</td>
<td>0.32</td>
</tr>
<tr>
<td>AppNexus</td>
<td>2.2%</td>
<td>0.0%</td>
<td>0.39</td>
</tr>
<tr>
<td>Google Syndication</td>
<td>14.5%</td>
<td>6.1%</td>
<td>0.28</td>
</tr>
</tbody>
</table>

- A mis-information website is 114x more likely to use RevContent than a mainstream website.
What terms of services/ acceptable use policies should benign hosting providers have?

Do misinformation and DoS attacks have similar consequences? Should they be treated the same?
Donation/Payment Processing

- 9.8% of misinformation sites rely on PayPal (93% of which use it to solicit donations) compared to 0.01% of mainstream websites
- PayPal blocks sites that host hateful and non-inclusive content
- Return of Kings (men’s rights) and Daily Stormer

“We are not allowed to use any form of advertisement. We cannot use PayPal. We cannot even use credit card processors. We had a P.O. box, and even that was shut down. The only way we can receive money is through crypto currency” [16].

“The first factor for this hiatus is that site revenues are too low. We’ve been banned from Paypal and countless ad partners, which forced me to lay off the site editor last year and also lower payments to regular contributors. This started a negative spiral of declining content quality, site traffic, and revenues. Even the beloved comments section, which many see as the highlight of ROK, was badly hit when Disqus banned us. Currently, ROK receives half the traffic of its peak and less than one-fifth of the income” [54].
The End.

So, how do you all feel about the world now?