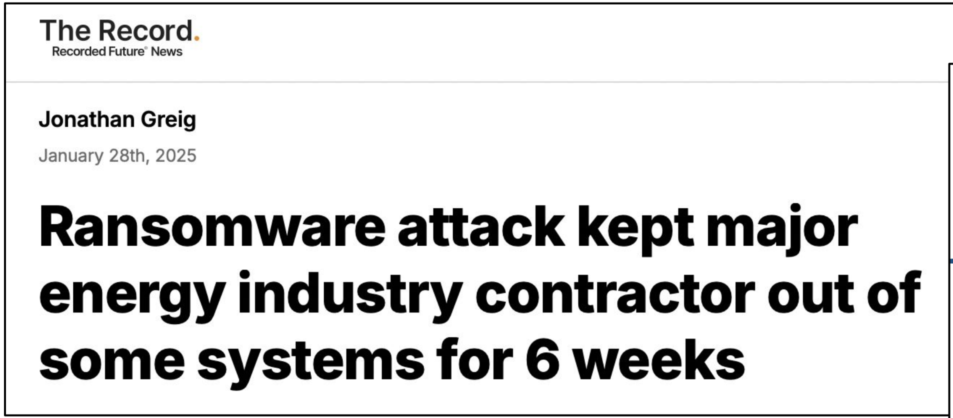
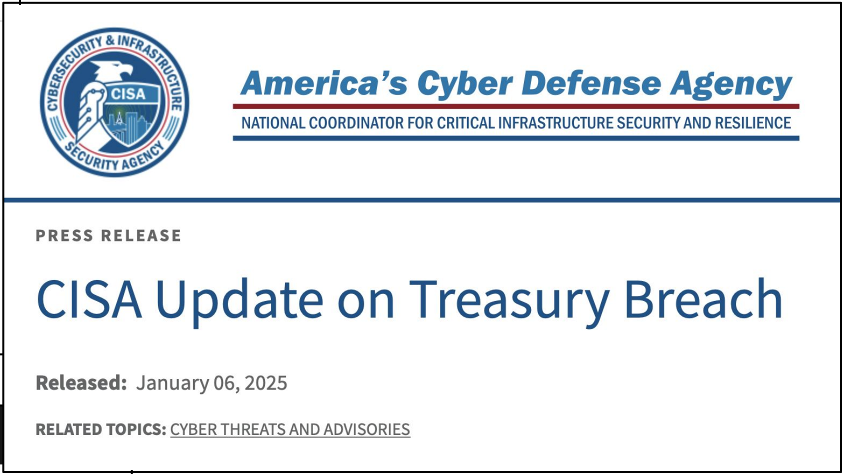
How do these attacks happen over the Internet?



The Record.
Recorded Future® News

Jonathan Greig
January 28th, 2025

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



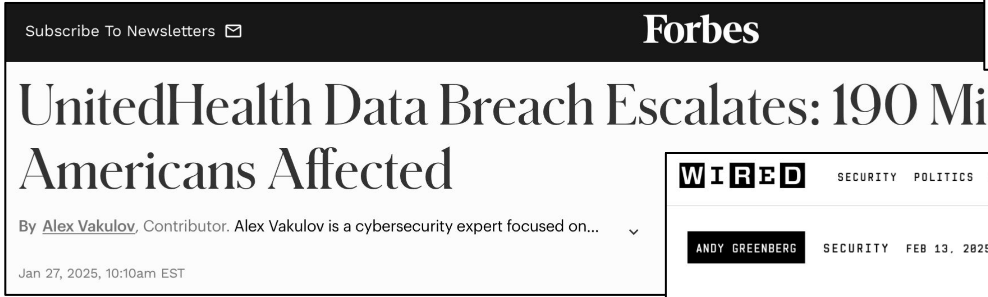
America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

PRESS RELEASE

CISA Update on Treasury Breach

Released: January 06, 2025

RELATED TOPICS: CYBER THREATS AND ADVISORIES

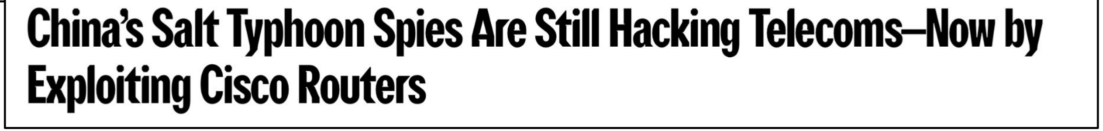


Subscribe To Newsletters ✉ Forbes

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

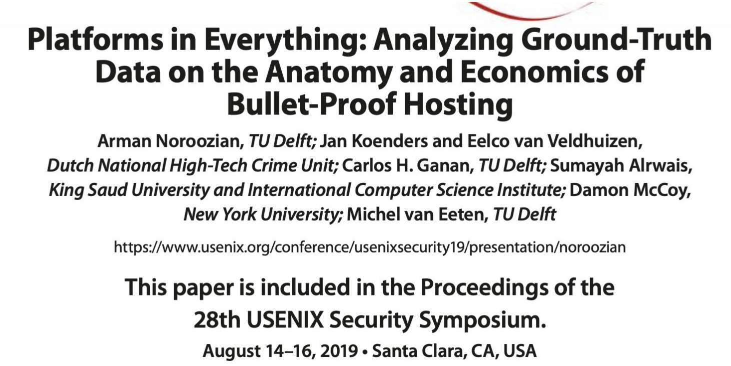
Real world consequences

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

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

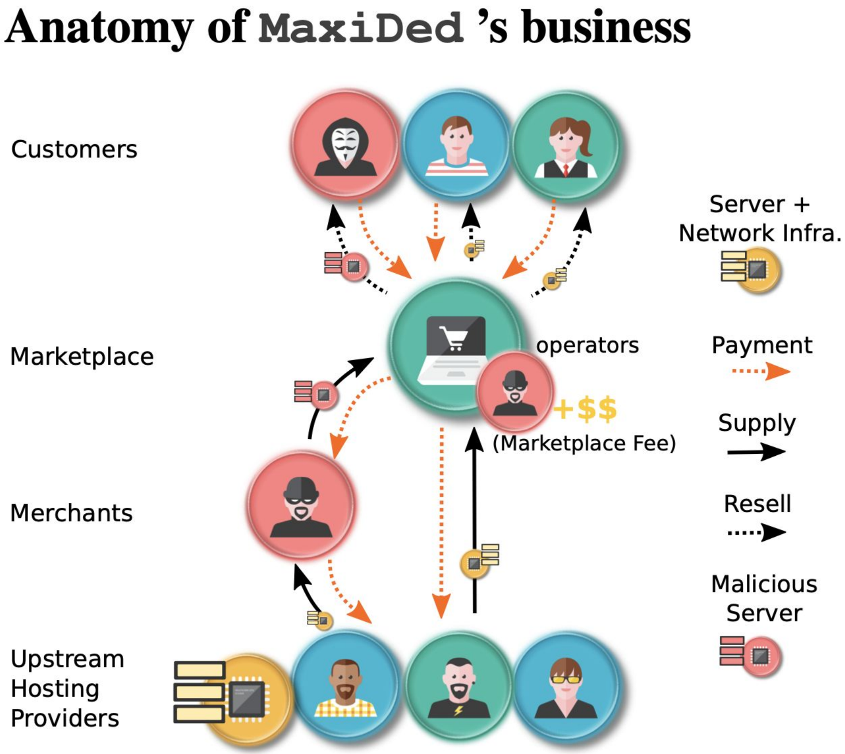
Bullet-Proof Hosting

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

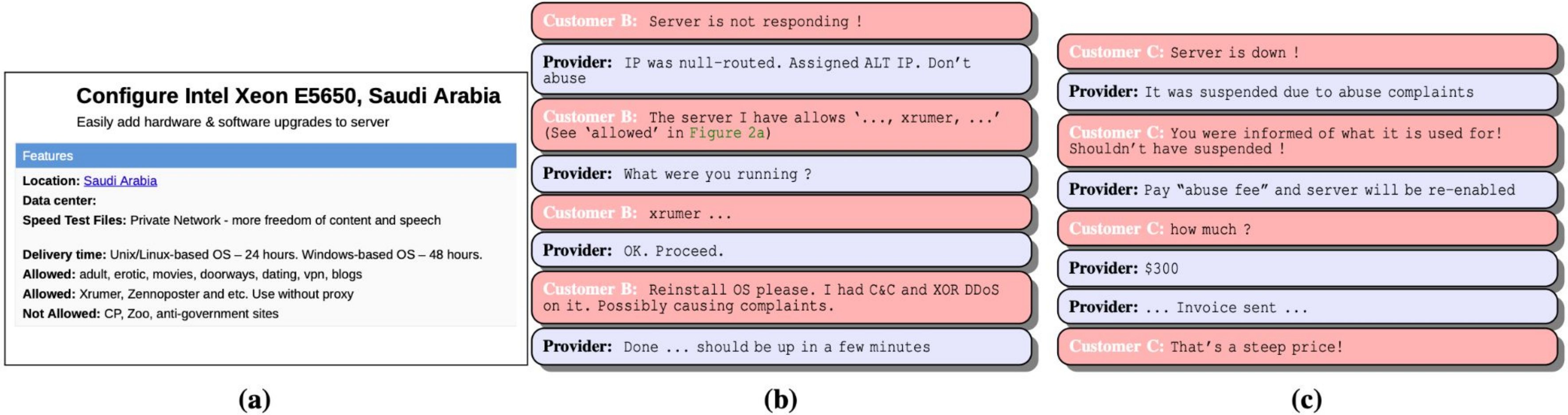
(+) Malicious traffic mixed with benign traffic -> hard to block

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

MaxiDed bulletproof hosting



- 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 ...

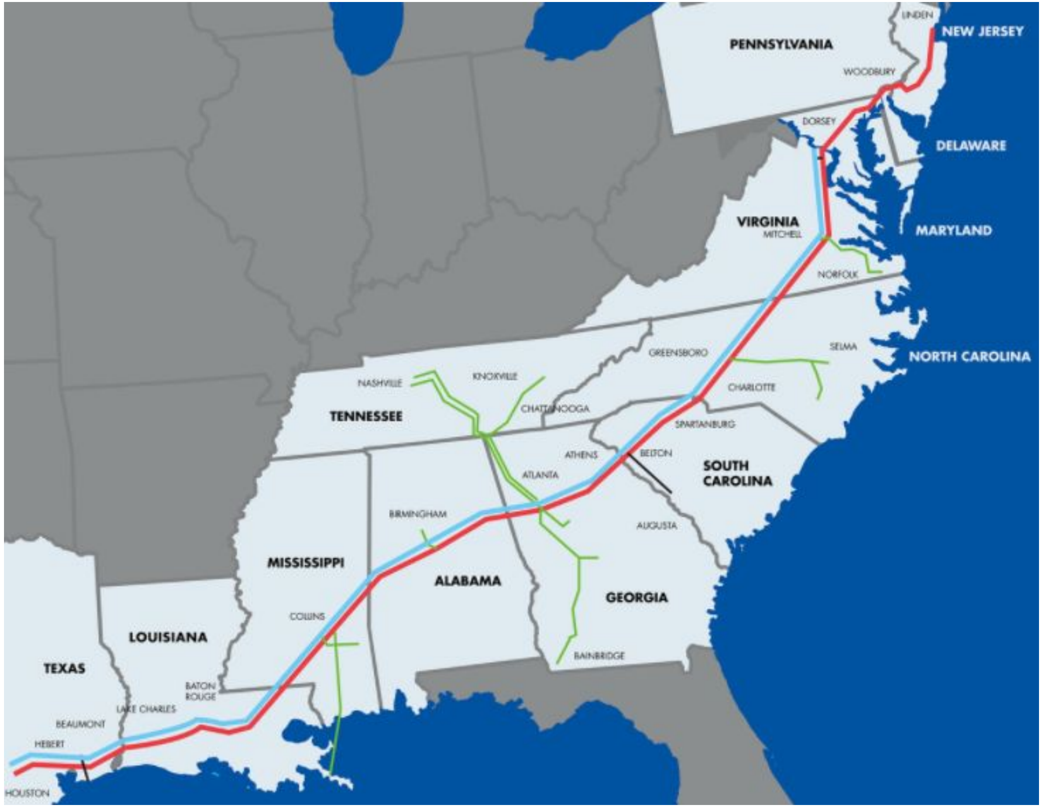
Customer C: That's a steep price!

(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).

How are network intrusion attacks orchestrated on the Internet?

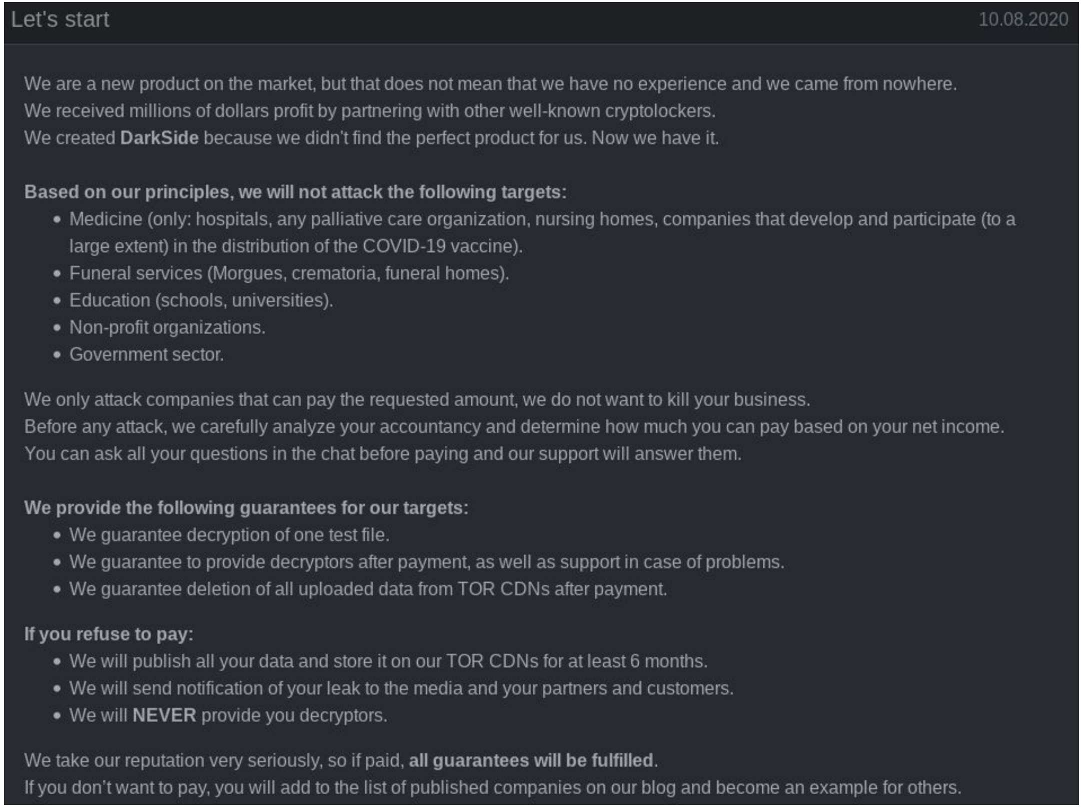
Colonial Pipeline ransomware attack - May 2021



- 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.

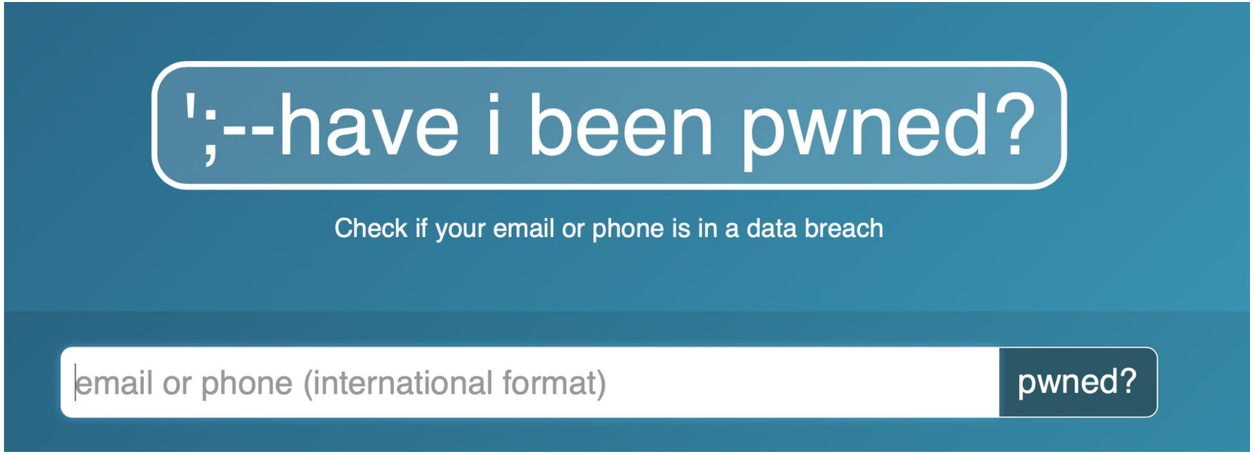
We take our reputation very seriously, so if paid, **all guarantees will be fulfilled**.
If you don’t want to pay, you will add to the list of published companies on our blog and become an example for others.

How did DarkSide infiltrate Colonial Pipeline?

How did DarkSide infiltrate Colonial Pipeline?

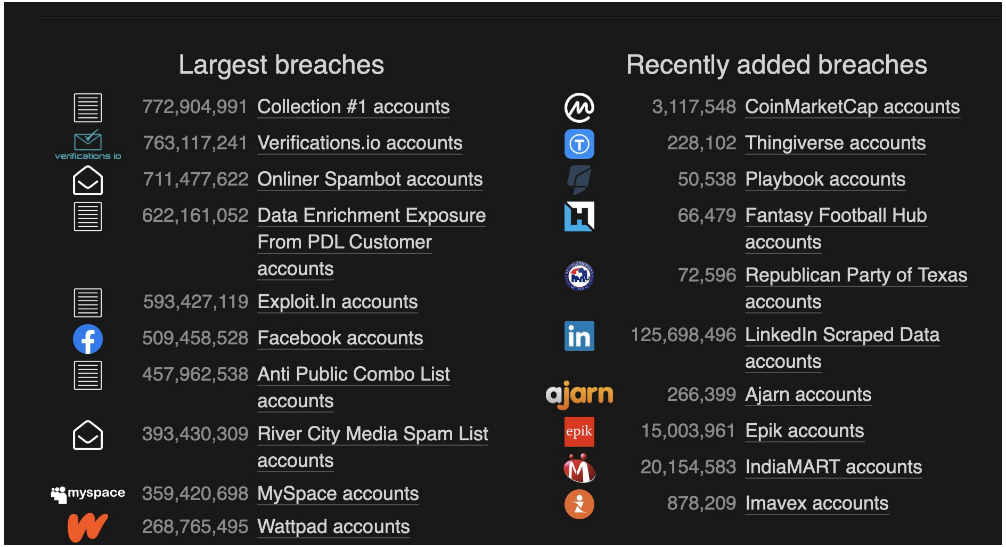
- “RockYou2021” password leak (~8.2 billion credentials) on the dark web
    - Contained an outdated, but still used, credential to a Colonial Pipeline Virtual Private Network (VPN)
        - Businesses typically use a VPN **to give remote employees access to internal applications and data**, or to create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



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.

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

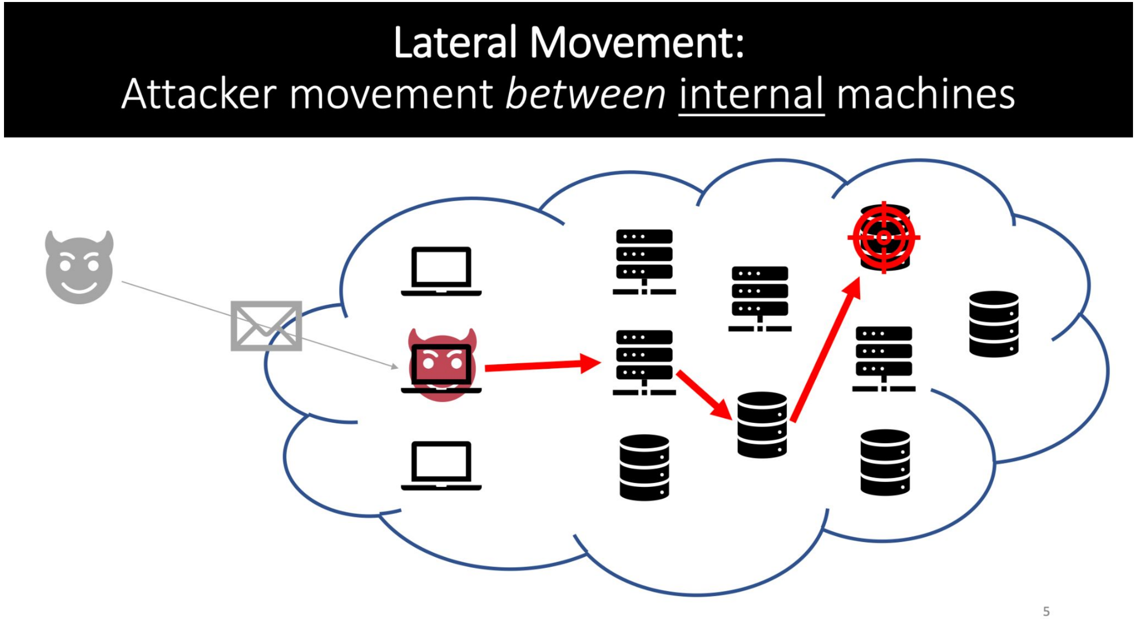
Lateral Movement

(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

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

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

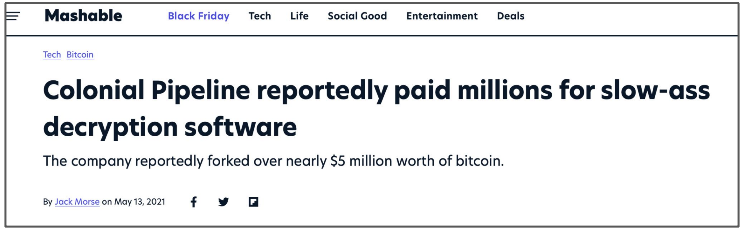
DarkSide succeeds in lateral movement...and begins encrypting ~100GB of their files

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



Tech Bitcoin

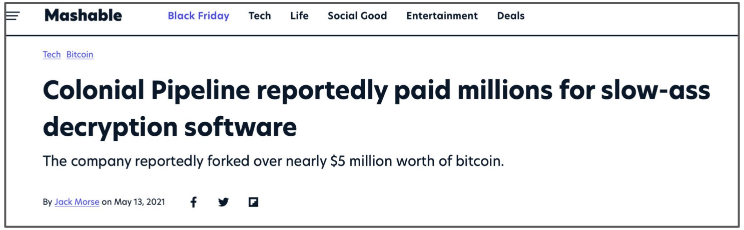
Colonial Pipeline reportedly paid millions for slow-ass decryption software

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

By Jack Morse on May 13, 2021

Aftermath of Colonial Pipeline Hack

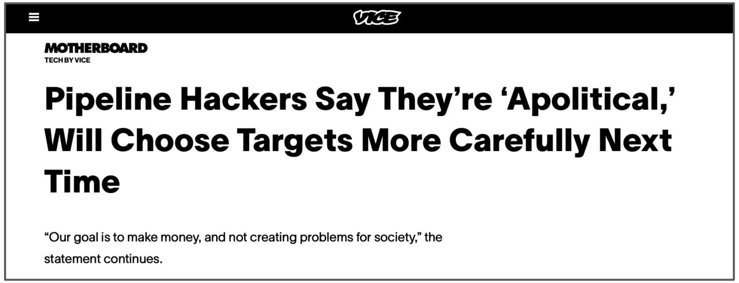
- Colonial Pipeline shuts down to stop lateral movement / ransomware spread
- FBI, CISA, DoE, DHS all notified
- Colonial Pipeline pays ransom
    - It is illegal for companies to pay ransom to terrorist organizations, but it is not illegal (only “advised against”) to pay ransoms in general
- Colonial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



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

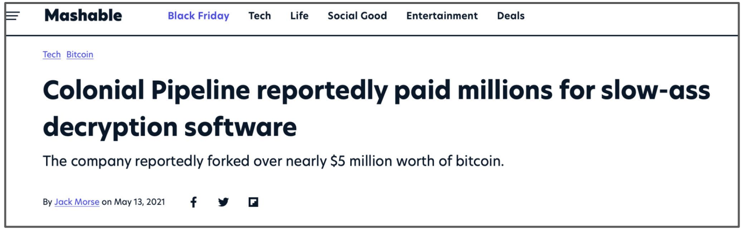


Pipeline Hackers Say They’re ‘Apolitical,’ Will Choose Targets More Carefully Next Time

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

Aftermath of Colonial Pipeline Hack

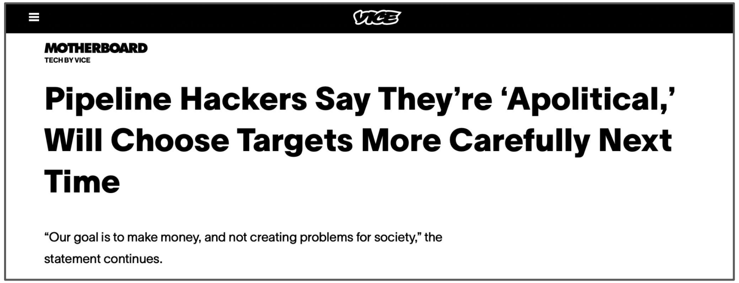
- Colonial Pipeline shuts down to stop lateral movement / ransomware spread
- FBI, CISA, DoE, DHS all notified
- Colonial Pipeline pays ransom
  - It is illegal for companies to pay ransom to terrorist organizations, but it is not illegal (only “advised against”) to pay ransoms in general
- Colonial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



Colonial Pipeline reportedly paid millions for slow-ass decryption software

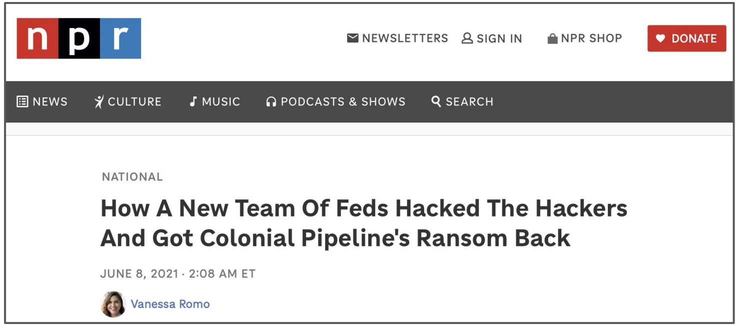
The company reportedly forked over nearly $5 million worth of bitcoin.

By Jack Morse on May 13, 2021



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.



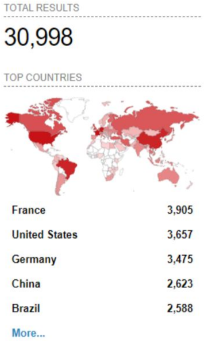
How A New Team Of Feds Hacked The Hackers And Got Colonial Pipeline's Ransom Back

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



TOTAL RESULTS

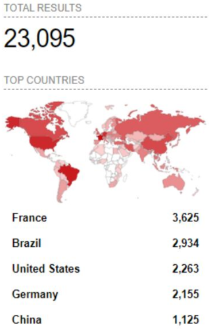
30,998

TOP COUNTRIES

France	3,905
United States	3,657
Germany	3,475
China	2,623
Brazil	2,588

More...

VMware ESXi 6.7.0



TOTAL RESULTS

23,095

TOP COUNTRIES

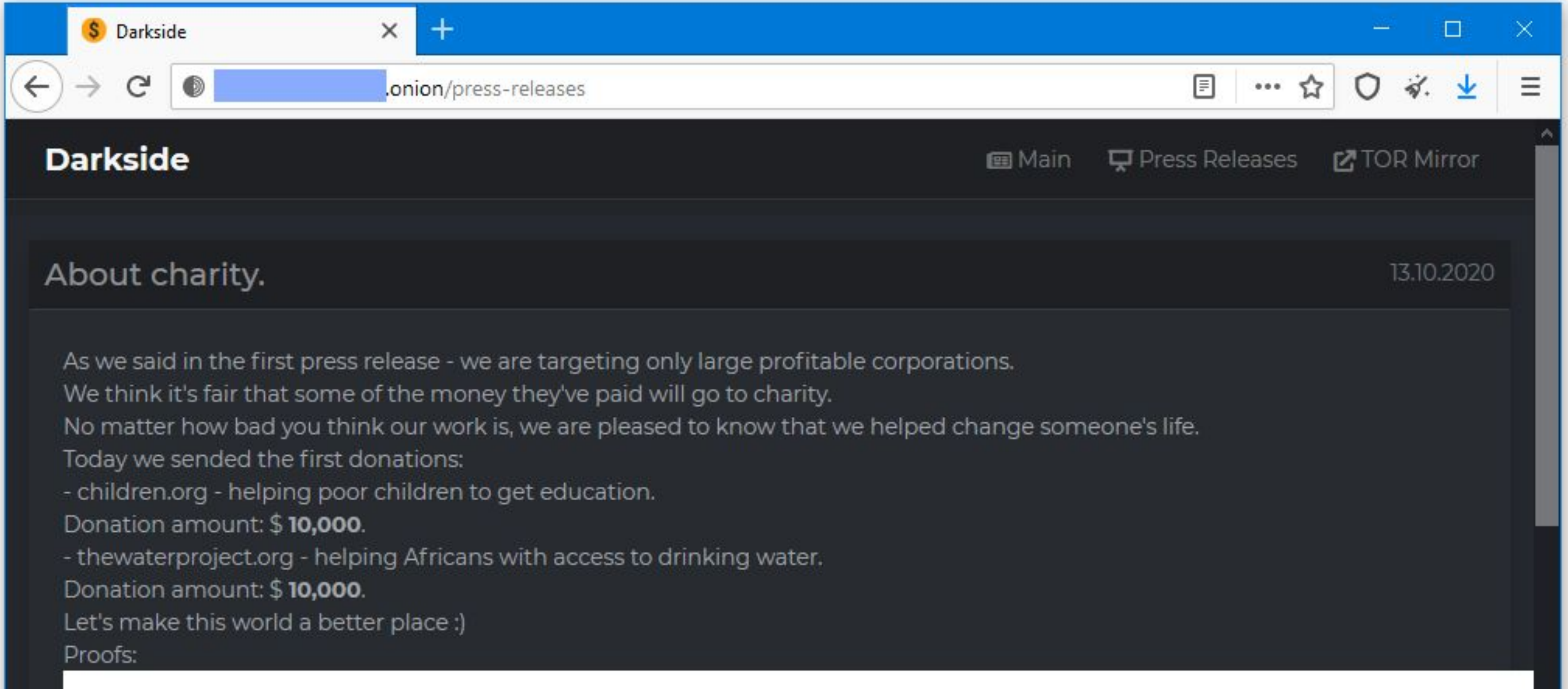
France	3,625
Brazil	2,934
United States	2,263
Germany	2,155
China	1,125

VMware ESXi 6.5.0

May 2021 (Shodan)

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

The BrightSide of DarkSide



About charity.

13.10.2020

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 :)
Proofs:

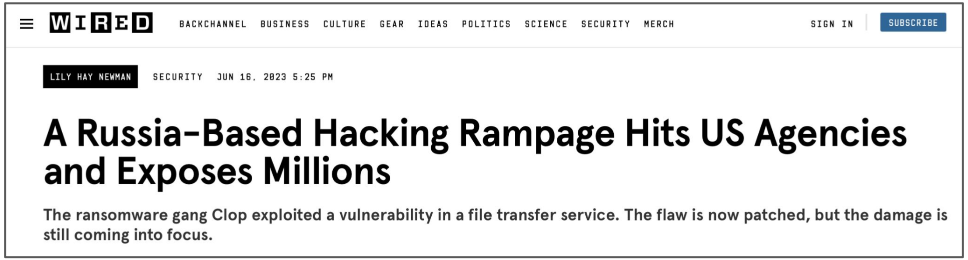
An increasingly common variation: software supply chain attacks

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

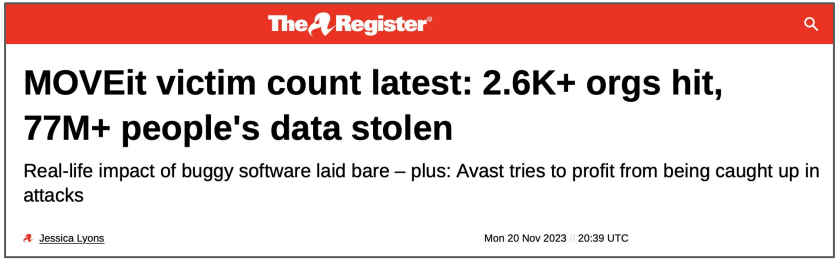
- Zero-day SQL injection vulnerability in MOVEit file transfer software
  - New CVE, old OWASP vulnerability class
- Cl0p ransomware gang seem to have developed attack for ~2 years before mass-exploiting organizations using MOVEit
- Hundreds of organizations affected, including British Airways, the BBC,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



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

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

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



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

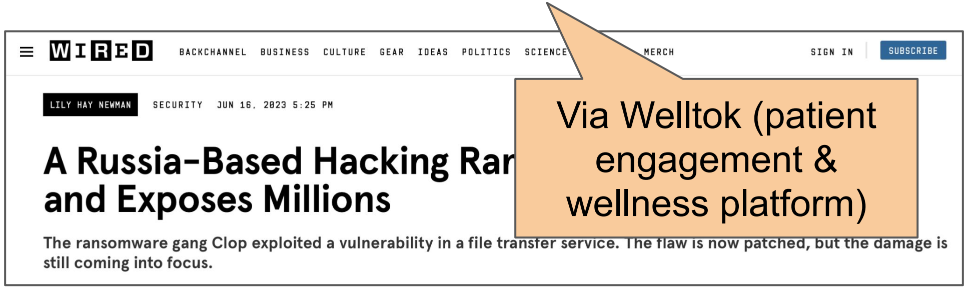
MOVEit ransomware attacks - 2023

- Zero-day SQL injection vulnerability in MOVEit file transfer software
  - Ne erability class
- Cl0p ra eem to have developed atta fore mass-e ions 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)

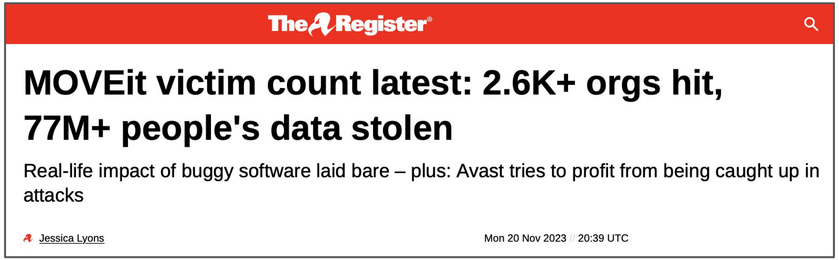
Via Welltok (patient engagement & wellness platform)


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 Ran and Exposes Millions

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



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

Easier said than done!

- 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)

Defenses against Internet Scanning

Easier said than done!

- 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)

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

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