FUTURE SHOCK: “The Future of Fraud…today”

TECHNOLOGY FIRST®

Bryan K. Fite [bfite@getsecure.com]

Taste of IT Conference – November 8th, 2023

My journey

From the guy that said NO… to the person that **facilitates YES**

Hacker & Entrepreneur

Researcher

Field Engineer & Cyber Instructor

Consultant

Architect, Policy Scribe & Risk Manager

Security & Compliance Director

Product Manager

Cyber-Physical Specialist

CTO/CSO/CISO

Innovator, “Herder of Cats” & Trusted Advisor

Original Premise– “2006”

Based on my technical paper - Corporate Identity Fraud: Life-Cycle Management of Corporate Identity Assets

Corporate Identity Fraud

It can be defined as the abuse of traditional and nontraditional identity assets with the intent to divert, deceive or defraud consumers.

Trademarks and Brands

These are traditional corporate identity assets. Trademark enforcement and brand protection programs are governed by legal precedence and legacy business procedures.

The Litmus Test

Asking yourself, “Is it actionable?” These mature practices are based on very narrow criteria.

Corporate Identity Fraud II: 15 years later

Purpose:

To **assess** how the practice or corporate identity asset protection has **matured** and if organizations are prepared for the world of software defined everything nation state threat actors and coexisting with the **Internet of dangerous things**.

SANS Link - https://www.sans.org/white-papers/corporate-identity-fraud-ii-future-fraud-today/

Digital (Identity) Assets

Corporate Identity Assets (2006)

- Trademarks/Service Marks/Logos
- Domain Names & Email addresses
- SSL Certificates
- Cryptographic Keys/Digital Signatures
- IP Address Space
- Vanity Phone Numbers
- Online Forum Identities
- Personal Identities of Key Human Associates

Organizational Digital Asset (2021)

- Social Media Accounts (professional & personal)
- Usernames & Passwords
- Cloud Conferencing Platforms
- Blockchains, Crypto wallets and Smart Contracts
- Personally Identifiable Information
- GitHub/Software Repositories
- ASN’s, BGP Peering Tables, and Routing Paths
- Abandoned or Doxed Artifacts

What are they? What are they worth? Who could be harmed? Who is responsible?

Digital Identity Fraud (DIF)

The **abuse** of digital identity assets executed via one or more electro magnetic **communication medium** with the intent to **divert, deceive, or defraud** identity stakeholders

Transformational Trends

Something wicked this way comes

Chaos breeds opportunity: Marketing, security, and operations can join forces to "turn the tables" on their adversaries by becoming hard targets

Wicked Problems:

- Growing number of unmanaged digital assets
- Hidden dependencies
- Asymmetric nature of "cyber"
- Colliding domains

- **Unique Opportunities:**

- Adopt a holistic lifecycle management of digital assets
- Leverage latent capabilities
- Protect what matters the most

Transformational trends in mobility, compute, and social media conspire to make organizations more vulnerable

What’s in your threat catalogue?

- Threat catalogs are basically a list of “bad things” that have or could happen to an organization
- Organizations should use threat catalogues in their risk assessment and treatment practices
- Some Threat catalogue items to consider:
  - ➢ Extortion
    - ➢ Multi-Domain DDoS, Ransomware, Sabotage/Quality Control (poisoning)
  - ➢ IP Theft & Data Loss
    - ➢ Nationalization of Assets
  - ➢ Market, Consumer & Voter Manipulation

The Curious Case of Mr. Pink

Threat Assessment and Response

Cyber Extortion Observations

Then:

- SPAM
- Basic Tactics
- Easily spotted indicators of BS
- “Perfect crimes”

Now:

- Targeted
- Sophisticated, automated, and outsources (aka G-commerce)
- Evolving, morphing, and increasing
- Demands exceeding $1 million
- No gas for you & “where’s the beef?”

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

“Paying ransom will not ensure your data is decrypted or that your systems or data will no longer be compromised. CISA, MS-ISAC, and federal law enforcement do not recommend paying ransom.”

Pharming, Phishing, Smishing, and Whaling… oh my

CEO Fraud
(aka business email compromise 2018)

“This type of cyberattack –targeted at companies’ employees – has been increasing steadily during the last year. The ‘CEO fraud’ can affect any type of company, from small family businesses to large multinationals and it is essential to understand how it works in order protect companies from it”
– Ana Gómez Blanco

Phase 1

Picking the victim--Recon

Phase 2

Manipulating the employee- social engineering- employee/customer/mark

Phase 3

Employee reaction– do something.. Now!

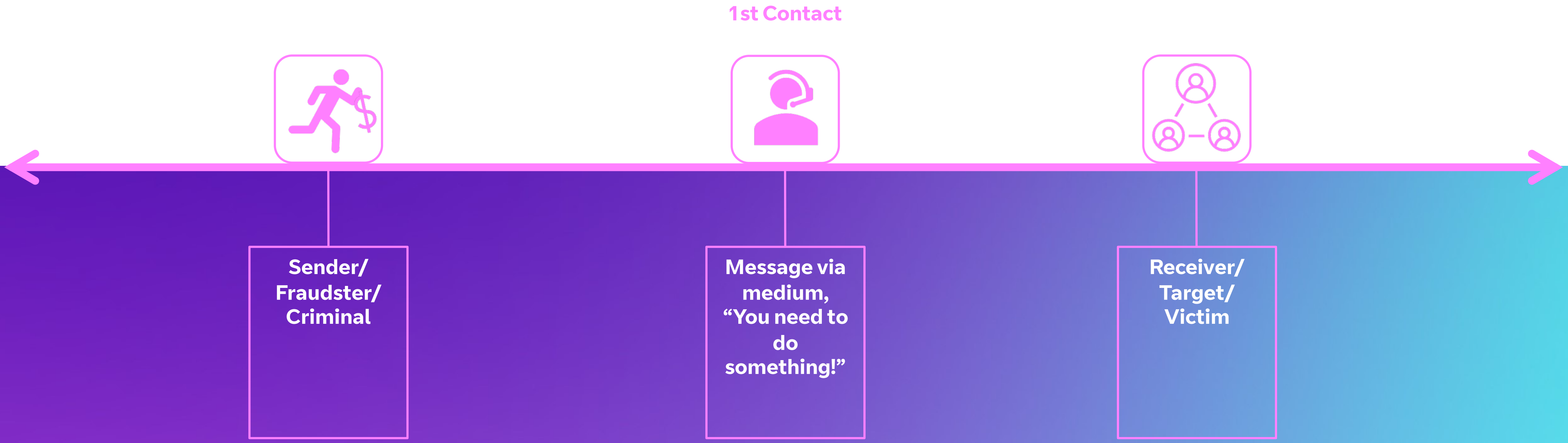
Phase 4

The impact– Catch me if you can

“Serious adversaries innovate then others imitate and industries automate.”

€1.1 billion

Anatomy of Fraud



1st Contact

Sender/
Fraudster/
Criminal

Message via
medium,
“You need to
do
something!”

Receiver/
Target/
Victim

2020: BEC scams ($1.8 billion in losses), romance scams ($600 million in losses), and investment fraud ($336 million)

2022: Investment fraud (~$3.3 billion in losses), BEC scams (~$2.7 billion in losses), and tech support (~$807 million)

Go to https://Ic3.gov to learn more!

Deep Fakes & Anti-Social Behavior

A threat to humanity?

"What are the roles of Morals, Ethics and Regulations in regards to the Safety, Security and Privacy of the intended human beneficiaries?"

Spoofing then:

- Email
- Caller ID
- Web pages

Deep fake:

- Real and fabricated "leaked" artifacts
- Voice
- Video (the final frontier)
- Anti-social media, algorithms, and AI's (we will make good pets)

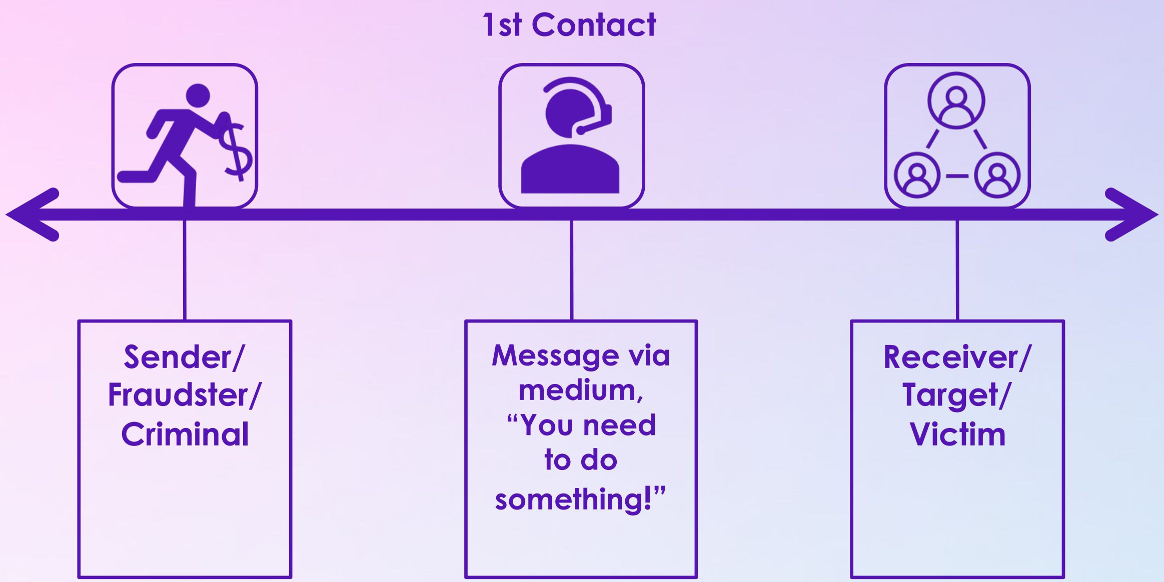
Trending:

- High-profile Twitter hacks
- Hacking humans/social engineering (confirmation bias, cognitive dissonance, loss aversion)
- Insurance, unemployment, and IRS fraud on the rise
- AI's playing the stock market
- Swatting and flash mobs (aka human botnets)

Poisoned Pipelines, Organized Retail Crime, AI Enhanced Deception Services [WORMGPT]

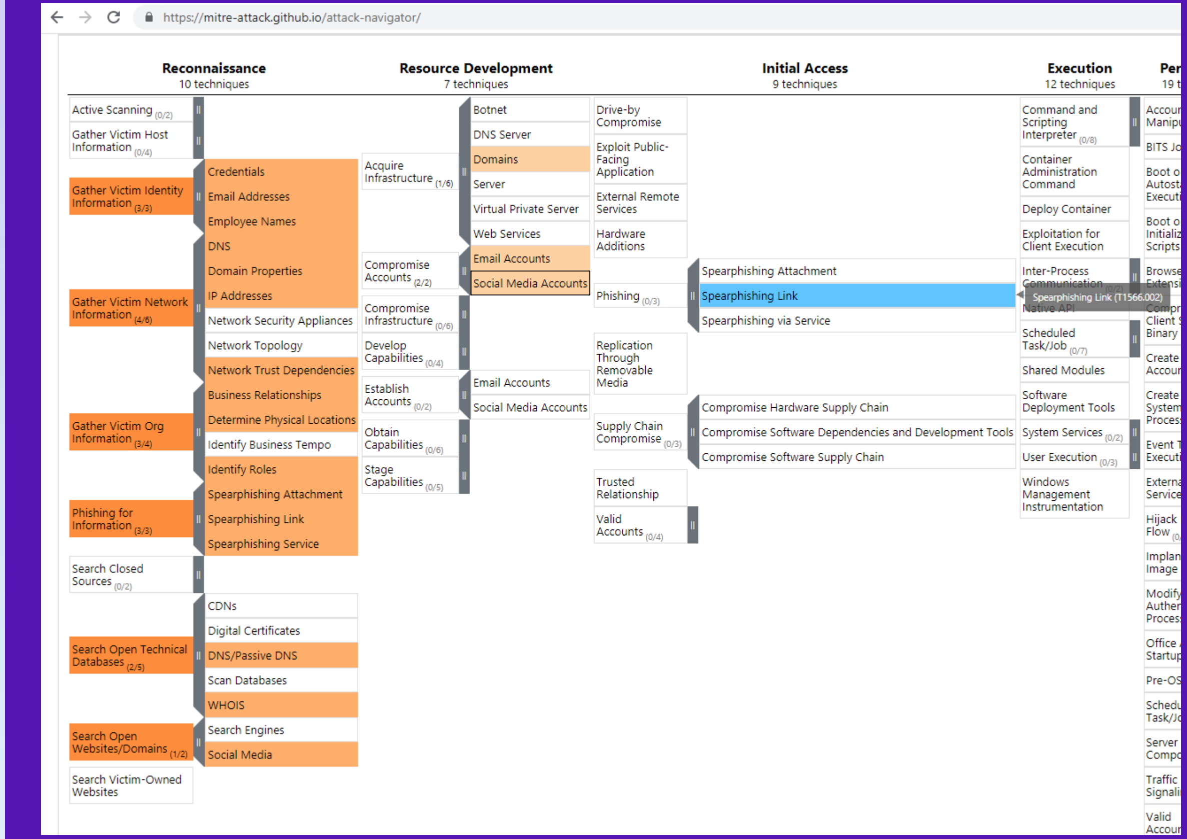
Takedown as Entertainment? YouTube @ScammerPayback

Modelling Digital Identity Fraud & Testing Controls


1st Contact
Sender/ Fraudster/ Criminal
Message via medium, “You need to do something!”
Receiver/ Target/ Victim

Persona’s (Actors w/Context)

Threat Catalogue


https://mitre-attack.github.io/attack-navigator/

Reconnaissance
10 techniques

- Active Scanning (0/2)
- Gather Victim Host Information (0/4)
- Gather Victim Identity Information (3/3)
  - Credentials
  - Email Addresses
  - Employee Names
- Gather Victim Network Information (4/6)
  - DNS
  - Domain Properties
  - IP Addresses
  - Network Security Appliances
  - Network Topology
  - Network Trust Dependencies
- Gather Victim Org Information (3/4)
  - Business Relationships
  - Determine Physical Locations
  - Identify Business Tempo
  - Identify Roles
- Phishing for Information (3/3)
  - Spearphishing Attachment
  - Spearphishing Link
  - Spearphishing Service
- Search Closed Sources (0/2)
- Search Open Technical Databases (2/5)
  - CDNs
  - Digital Certificates
  - DNS/Passive DNS
  - Scan Databases
  - WHOIS
- Search Open Websites/Domains (1/2)
  - Search Engines
  - Social Media
- Search Victim-Owned Websites

Resource Development
7 techniques

- Acquire Infrastructure (1/6)
  - Botnet
  - DNS Server
  - Domains
  - Server
  - Virtual Private Server
  - Web Services
- Compromise Accounts (2/2)
  - Email Accounts
  - Social Media Accounts
- Compromise Infrastructure (0/6)
- Develop Capabilities (0/4)
- Establish Accounts (0/2)
  - Email Accounts
  - Social Media Accounts
- Obtain Capabilities (0/6)
- Stage Capabilities (0/5)

Initial Access
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (0/3)
  - Spearphishing Attachment
  - Spearphishing Link
  - Spearphishing via Service
- Replication Through Removable Media
- Supply Chain Compromise (0/3)
  - Compromise Hardware Supply Chain
  - Compromise Software Dependencies and Development Tools
  - Compromise Software Supply Chain
- Trusted Relationship
- Valid Accounts (0/4)

Spearphishing Link (T1566.002)

Execution
12 techniques

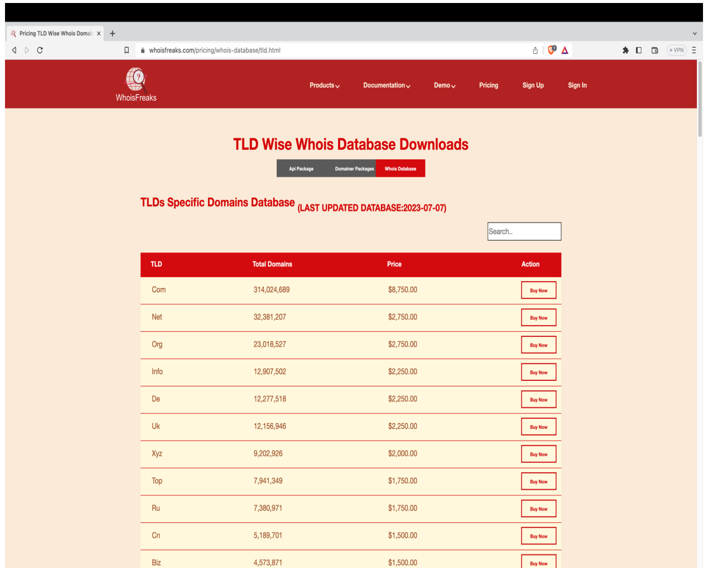
- Command and Scripting Interpreter (0/8)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (0/2)
- Native API
- Scheduled Task/Job (0/7)
- Shared Modules
- Software Deployment Tools
- System Services (0/2)
- User Execution (0/3)
- Windows Management Instrumentation

Per
19 t

- Accour Manipu
- BITS Jo
- Boot o Autost Executi
- Boot o Initializ Scripts
- Browse Extensi
- Compr Client Binary
- Create Accour
- Create System Proces
- Event T Executi
- Externa Service
- Hijack Flow (0
- Implan Image
- Modify Authen Proces
- Office Startup
- Pre-OS
- Schedu Task/Jo
- Server Compo
- Traffic Signali
- Valid Accour

Evolution of TLDs & gTLDs (aka expanding attack surface)

- How many specific domains are there?
- **~500 million**
- How many specific dot COM domains are there?
- **~300 million**



Pricing TLD Wise Whois Domai
whoisfreaks.com/pricing/whois-database/tld.html
VPN
WhoisFreaks
Products
Documentation
Demo
Pricing
Sign Up
Sign In

TLD Wise Whois Database Downloads

TLDs Specific Domains Database (LAST UPDATED DATABASE:2023-07-07)

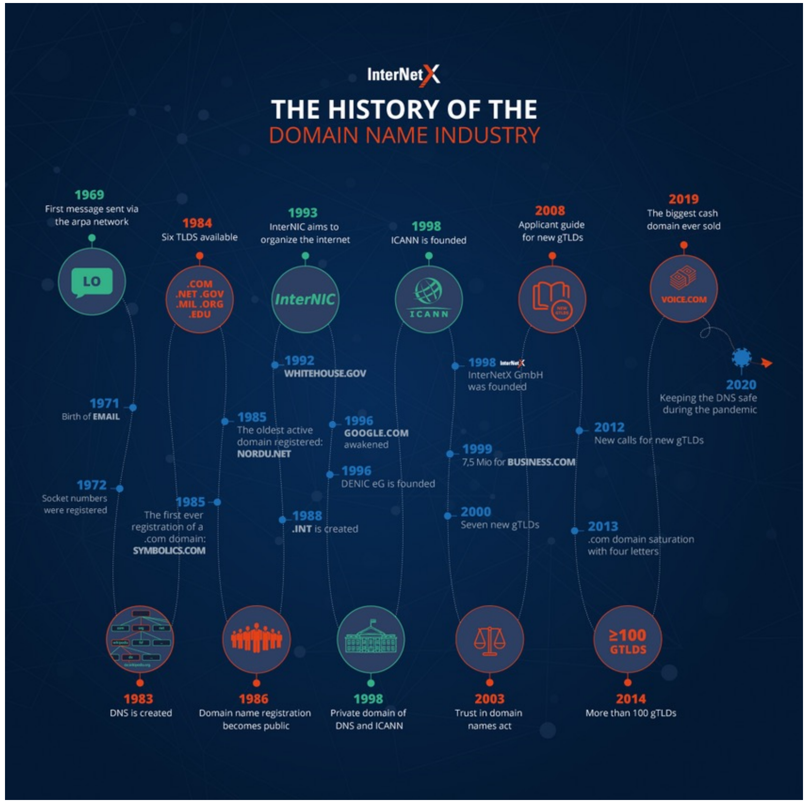
TLD	Total Domains	Price	Action
Com	314,024,689	$8,750.00	Buy Now
Net	32,381,207	$2,750.00	Buy Now
Org	23,018,527	$2,750.00	Buy Now
Info	12,907,502	$2,250.00	Buy Now
De	12,277,518	$2,250.00	Buy Now
Uk	12,156,946	$2,250.00	Buy Now
Xyz	9,202,926	$2,000.00	Buy Now
Top	7,941,349	$1,750.00	Buy Now
Ru	7,380,971	$1,750.00	Buy Now
Cn	5,189,701	$1,500.00	Buy Now
Biz	4,573,871	$1,500.00	Buy Now

https://whoisfreaks.com/pricing/whois-database/tld.html ($4K to $9K since Dec for dot com)

"Even beyond the financial toll the gTLD program will exact on millions of U.S. businesses, the Association believes that ICANN's program will confuse consumers by spreading Internet searches across hundreds or even thousands of new top-level domains."

In a statement to the US Congress on December 9, 2011, National Restaurant Association vice president Scott DeFife stated

https://en.wikipedia.org/wiki/Generic_top-level_domain



InterNetX
THE HISTORY OF THE
DOMAIN NAME INDUSTRY
1969
First message sent via the arpa network
LO
1984
Six TLDS available
.COM .NET .GOV .MIL .ORG .EDU
1993
InterNIC aims to organize the internet
InterNIC
1998
ICANN is founded
ICANN
2008
Applicant guide for new gTLDs
NEW GTLDS
2019
The biggest cash domain ever sold
VOICE.COM
1992
WHITEHOUSE.GOV
1998
InterNetX
InterNetX GmbH was founded
2020
Keeping the DNS safe during the pandemic
1971
Birth of EMAIL
1985
The oldest active domain registered: NORDU.NET
1996
GOOGLE.COM awakened
2012
New calls for new gTLDs
1999
7,5 Mio for BUSINESS.COM
1972
Socket numbers were registered
1996
DENIC eG is founded
1985
The first ever registration of a .com domain: SYMBOLICS.COM
1988
.INT is created
2000
Seven new gTLDs
2013
.com domain saturation with four letters
≥100 GTLDS
1983
DNS is created
1986
Domain name registration becomes public
1998
Private domain of DNS and ICANN
2003
Trust in domain names act
2014
More than 100 gTLDs

https://www.internetx.com/en/news-detailview/the-history-of-the-domain-name-industry/

But wait, there's more…

- Google Announces 8 New Top Level Domains Including One For Lawyers

The eight new gTLDs are:

.dad

.phd

.prof

.esq

.foo

.zip

.mov

.nexus

You Get This >

https://financialstatement.zip/

Riddle me this…

- How many gTLDs/TLDs are there? **A Sh*T TON**
- How many subdomains named “status” exist across all gTLDs/TLDs? **< “A Sh*T TON”**
- Pick 1 (example: **HACME.COM**)
- Are there any interesting observations or shared attributes across the dataset?
- Can these observations be used to identify (hidden) dependencies that can be exploited?

Sneak Peek - Future Shock: Supply Chain Smoking

Mohammed “Mo” Kharij

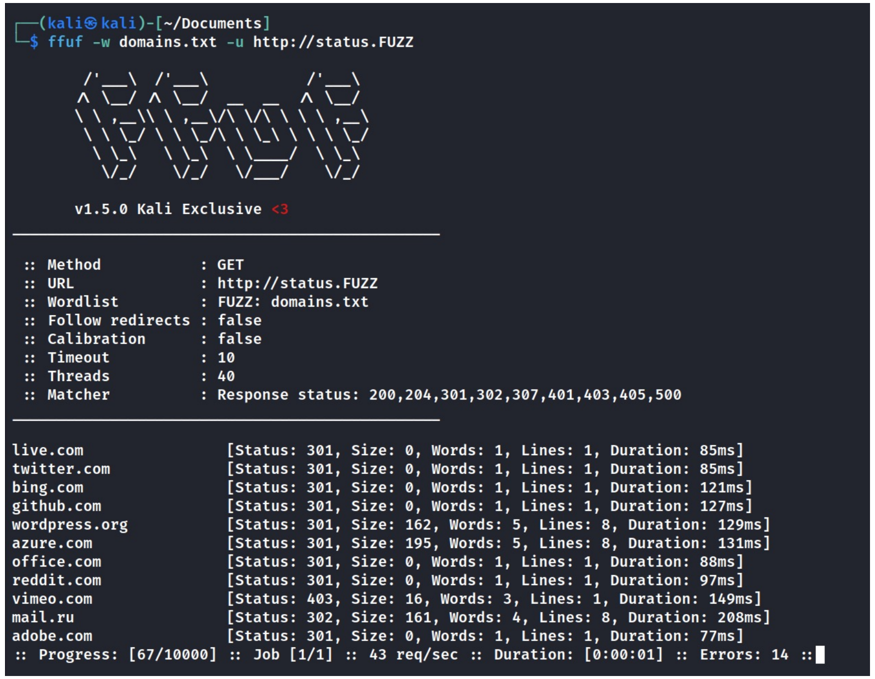
Don’t Pay to Play

The heroes of the day at Tranco:

- Victor Le Pochat, Tom Van Goethem, Samaneh Tajalizadehkhoob, Maciej Korczyński and Wouter Joosen
- https://tranco-list.eu/

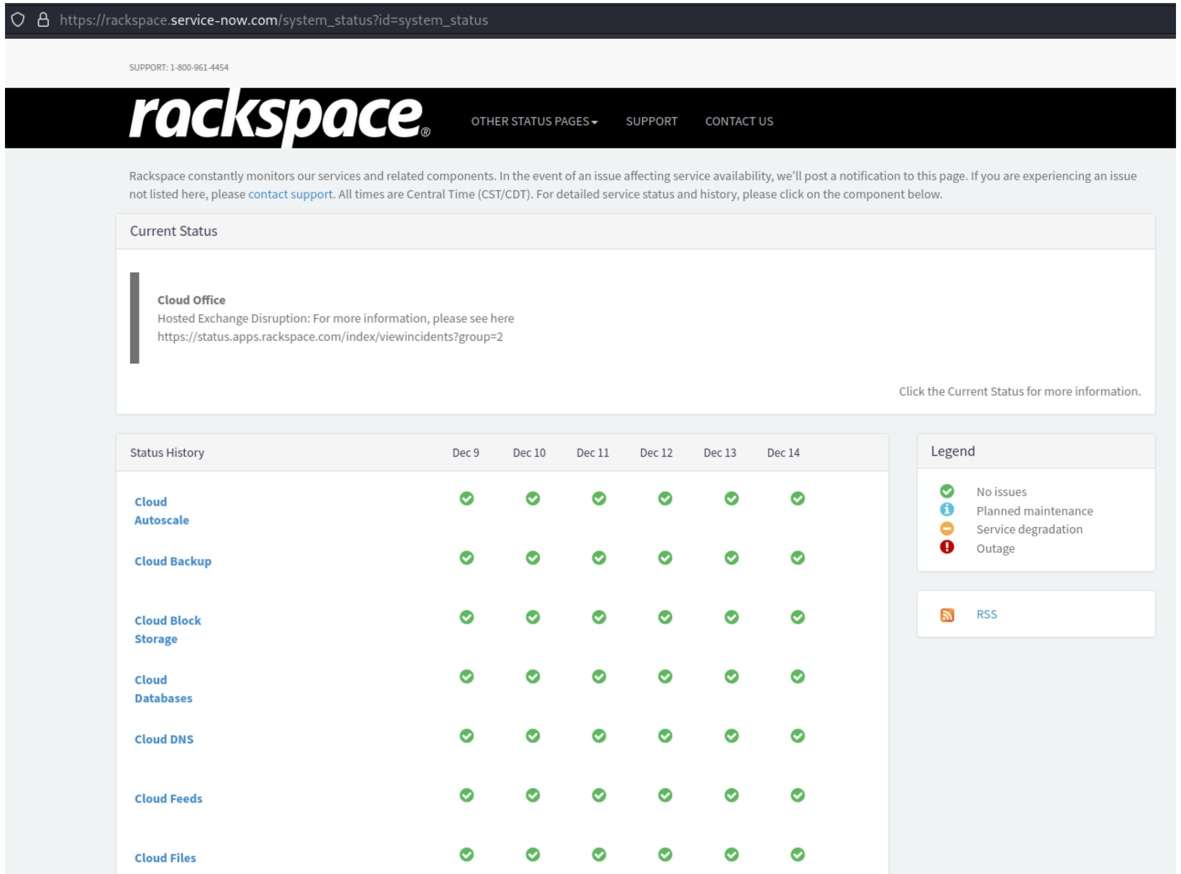
Tools (1821 / 20000)

- Use bash and cURL?
- Use bash and host?
- Use Ffuf, don’t reinvent the wheel



```
┌──(kali㉿kali)-[~/Documents]
└─$ ffuf -w domains.txt -u http://status.FUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.5.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://status.FUZZ
 :: Wordlist         : FUZZ: domains.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

live.com                [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 85ms]
twitter.com             [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 85ms]
bing.com                [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 121ms]
github.com              [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 127ms]
wordpress.org           [Status: 301, Size: 162, Words: 5, Lines: 8, Duration: 129ms]
azure.com               [Status: 301, Size: 195, Words: 5, Lines: 8, Duration: 131ms]
office.com              [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 88ms]
reddit.com              [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 97ms]
vimeo.com               [Status: 403, Size: 16, Words: 3, Lines: 1, Duration: 149ms]
mail.ru                 [Status: 302, Size: 161, Words: 4, Lines: 8, Duration: 208ms]
adobe.com               [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 77ms]
:: Progress: [67/10000] :: Job [1/1] :: 43 req/sec :: Duration: [0:00:01] :: Errors: 14 ::
```

The Success Stories



https://rackspace.service-now.com/system_status?id=system_status

SUPPORT: 1-800-961-4454

Rackspace constantly monitors our services and related components. In the event of an issue affecting service availability, we'll post a notification to this page. If you are experiencing an issue not listed here, please contact support. All times are Central Time (CST/CDT). For detailed service status and history, please click on the component below.

Current Status

Cloud Office
Hosted Exchange Disruption: For more information, please see here
https://status.apps.rackspace.com/index/viewincidents?group=2

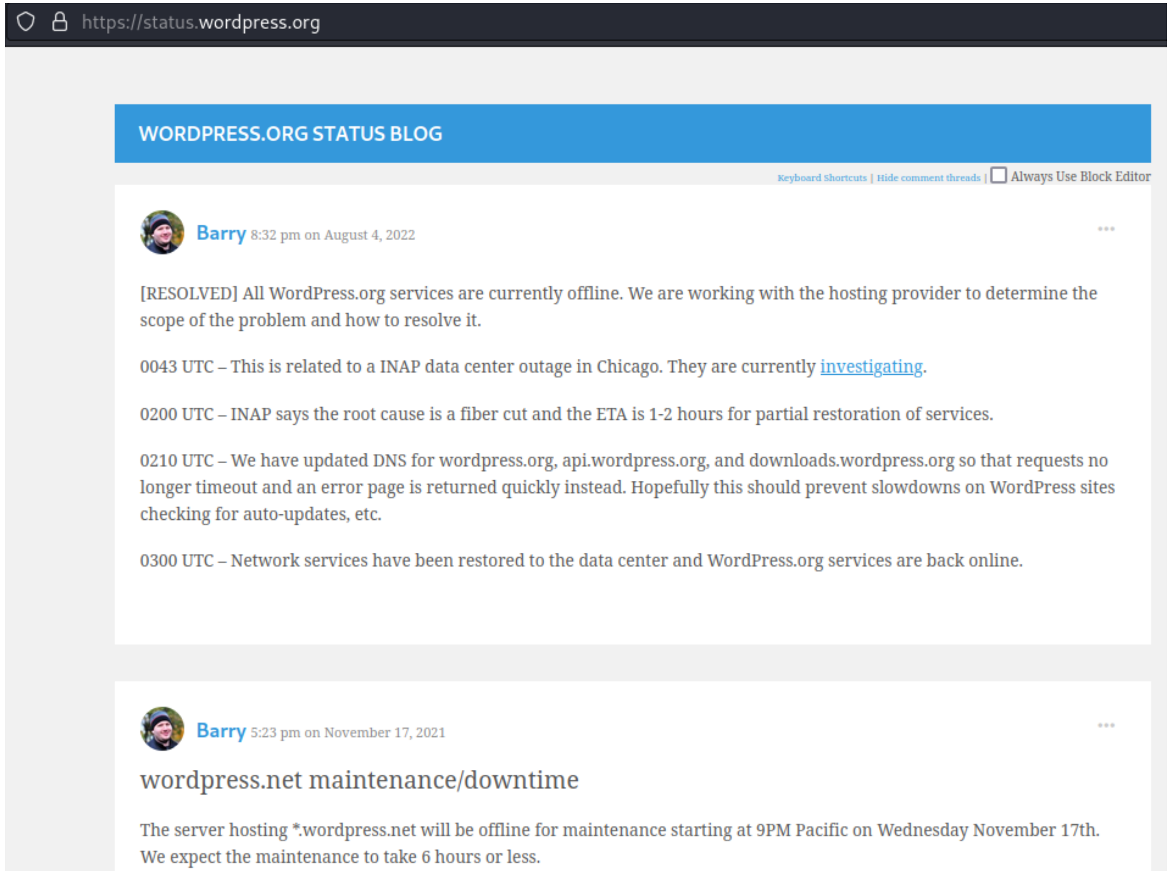
Click the Current Status for more information.

Status History	Dec 9	Dec 10	Dec 11	Dec 12	Dec 13	Dec 14
Cloud Autoscale	✓	✓	✓	✓	✓	✓
Cloud Backup	✓	✓	✓	✓	✓	✓
Cloud Block Storage	✓	✓	✓	✓	✓	✓
Cloud Databases	✓	✓	✓	✓	✓	✓
Cloud DNS	✓	✓	✓	✓	✓	✓
Cloud Feeds	✓	✓	✓	✓	✓	✓
Cloud Files	✓	✓	✓	✓	✓	✓

Legend

- ✓ No issues
- ℹ Planned maintenance
- ⊖ Service degradation
- ❗ Outage

RSS



https://status.wordpress.org

WORDPRESS.ORG STATUS BLOG

Keyboard Shortcuts | Hide comment threads | □ Always Use Block Editor

Barry 8:32 pm on August 4, 2022

[RESOLVED] All WordPress.org services are currently offline. We are working with the hosting provider to determine the scope of the problem and how to resolve it.

0043 UTC – This is related to a INAP data center outage in Chicago. They are currently investigating.

0200 UTC – INAP says the root cause is a fiber cut and the ETA is 1-2 hours for partial restoration of services.

0210 UTC – We have updated DNS for wordpress.org, api.wordpress.org, and downloads.wordpress.org so that requests no longer timeout and an error page is returned quickly instead. Hopefully this should prevent slowdowns on WordPress sites checking for auto-updates, etc.

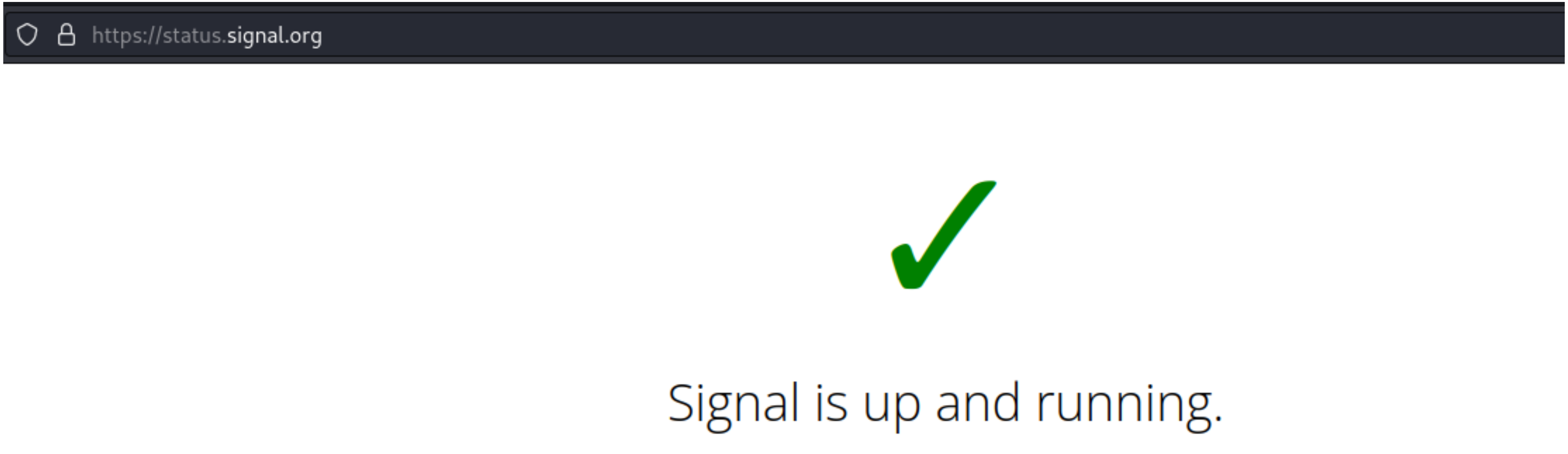
0300 UTC – Network services have been restored to the data center and WordPress.org services are back online.

Barry 5:23 pm on November 17, 2021

wordpress.net maintenance/downtime

The server hosting *.wordpress.net will be offline for maintenance starting at 9PM Pacific on Wednesday November 17th. We expect the maintenance to take 6 hours or less.

The informative…

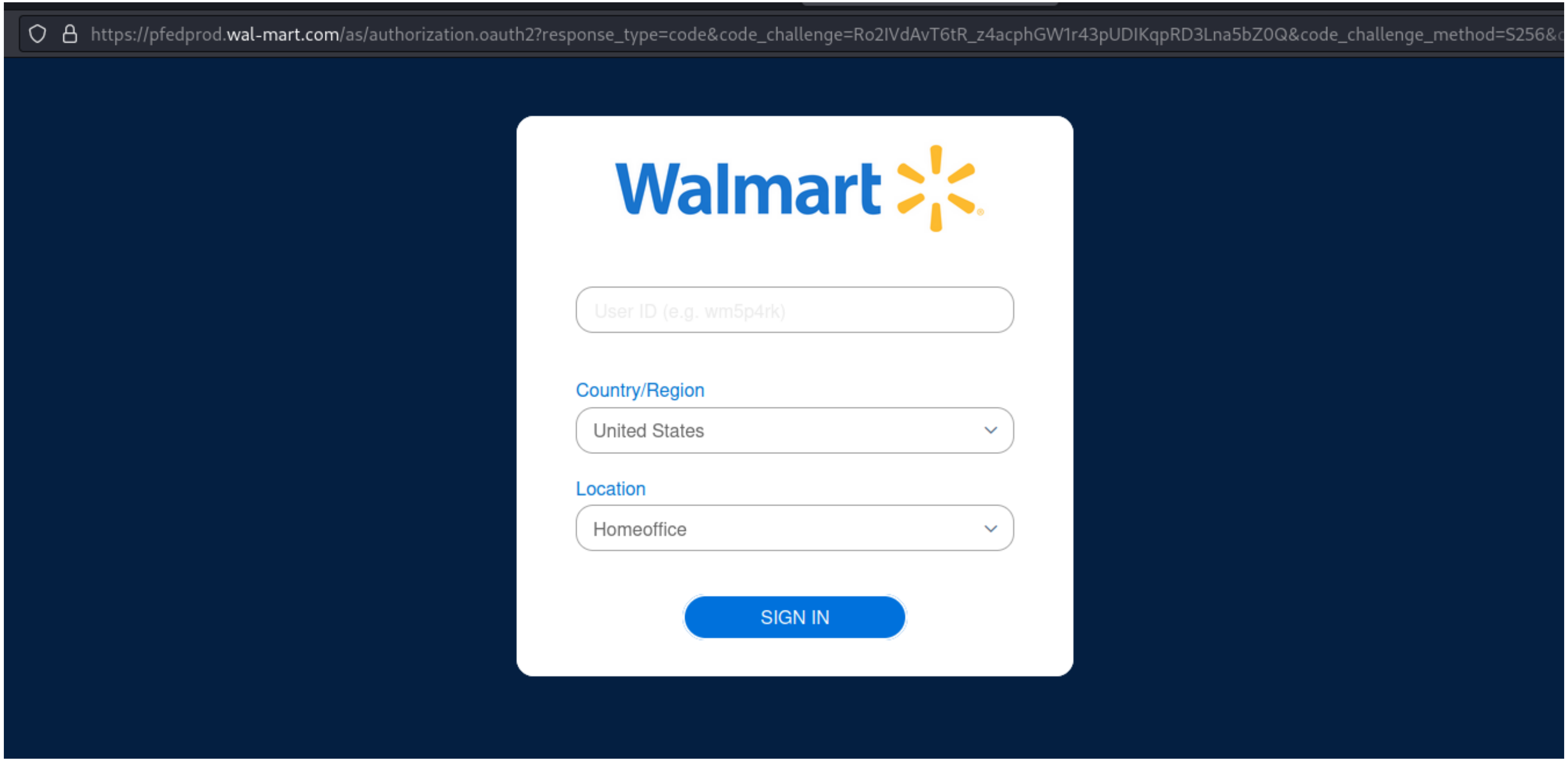


https://status.signal.org

✓

Signal is up and running.

The Strange



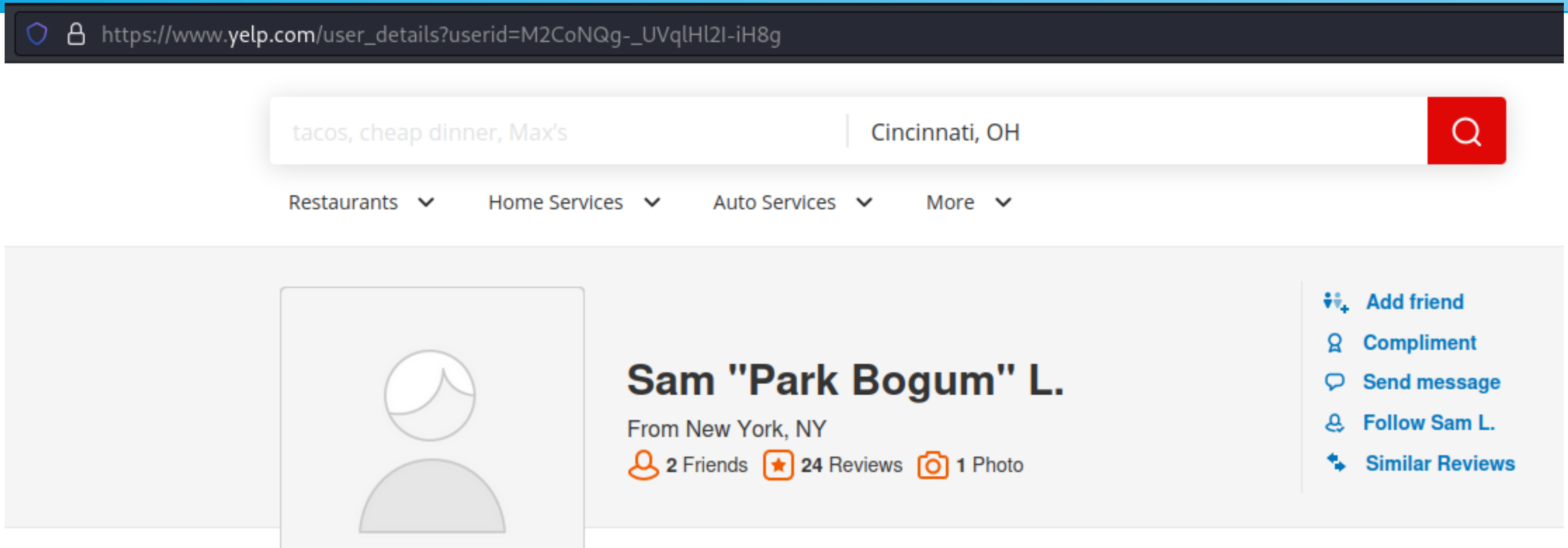
https://pfedprod.wal-mart.com/as/authorization.oauth2?response_type=code&code_challenge=Ro2IVdAvT6tR_z4acphGW1r43pUDIKqpRD3Lna5bZ0Q&code_challenge_method=S256&c

Walmart

User ID (e.g. wm5p4rk)

Country/Region: United States

Location: Homeoffice

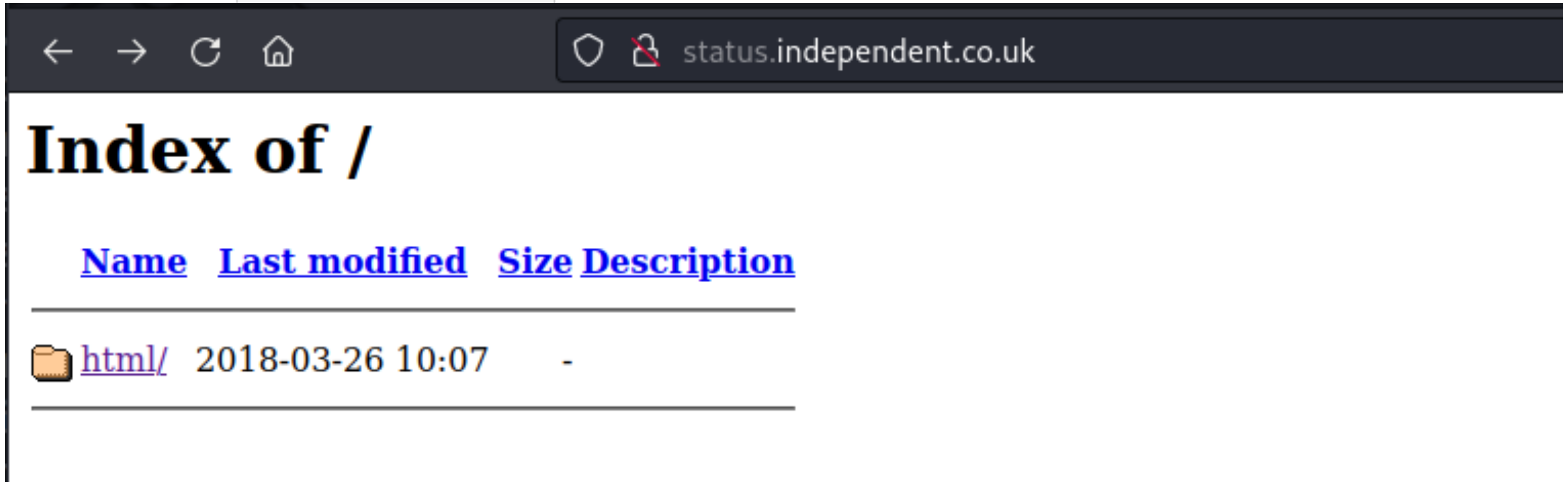


https://www.yelp.com/user_details?userid=M2CoNQg-_UVqlHl2I-iH8g

Sam "Park Bogum" L.

From New York, NY

2 Friends 24 Reviews 1 Photo



status.independent.co.uk

Index of /

```
Name  Last modified     Size Description
html/ 2018-03-26 10:07    -
```

Reasonable Response

- Global Asset Registry
- Holistic Risk Register & Governance
- Operationalize to Protect, Detect, Respond & Learn

"Remove discretion, make it easy to do the right thing and hard to do the wrong thing!"

Don’t panic!

It’s inevitable, so plan accordingly.