THE GHOST IN YOUR DNS

UNMASKING SUBDOMAIN HIJACKING

S M Zia Ur Rashid

$whoami

- Graduate Student (TU Cyber Fellow), The University of Tulsa
- Former Information Security Specialist, Augmedix Inc.

ziaurrashid.com https://linkedin.com/in/ziaurrashid https://twitter.com/smziaurrashid

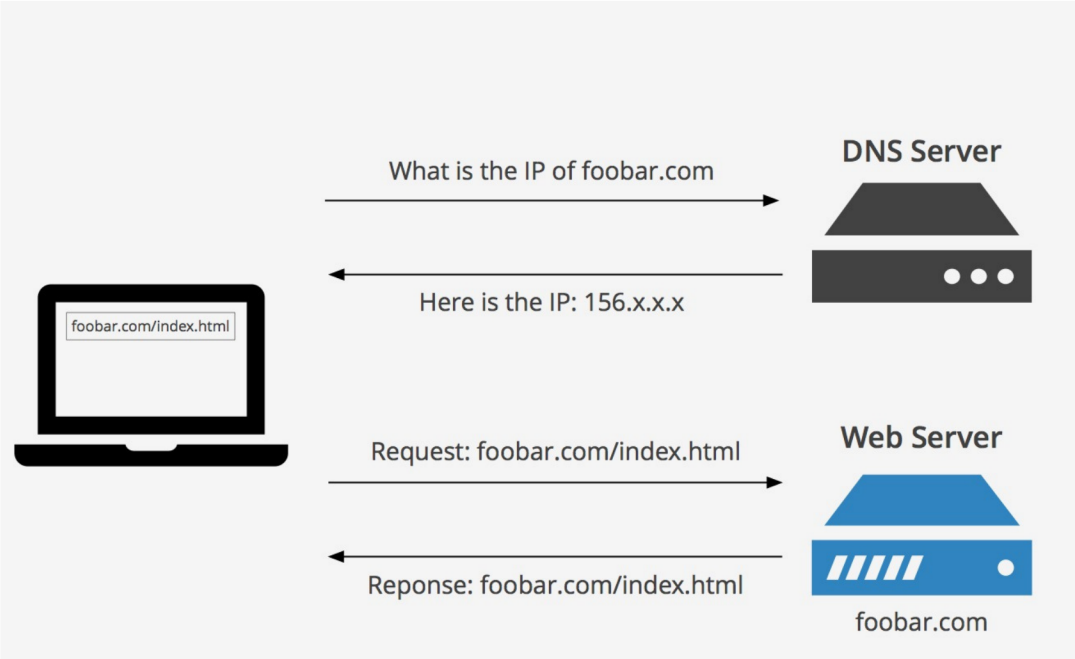
THE UNIVERSITY of TULSA

Cyber Fellows

$talkinfo

- DNS and DNS Hijacking Overview
- Subdomain Hijacking
  - CNAME Hijacking
  - NS Hijacking
  - Second Order Hijacking
  - A/AAAA Hijacking
  - MX Hijacking
- Potential Risk
- Case Study
- Tools for Pentesters
- Mitigation Strategies and Tools for Blue Team
- Q&A

What is DNS?



- DNS, or Domain Name System, is like the internet's phonebook.
- It translates human-readable domain names (like "foobar.com") into machine-readable IP addresses (like "192.0.2.1").

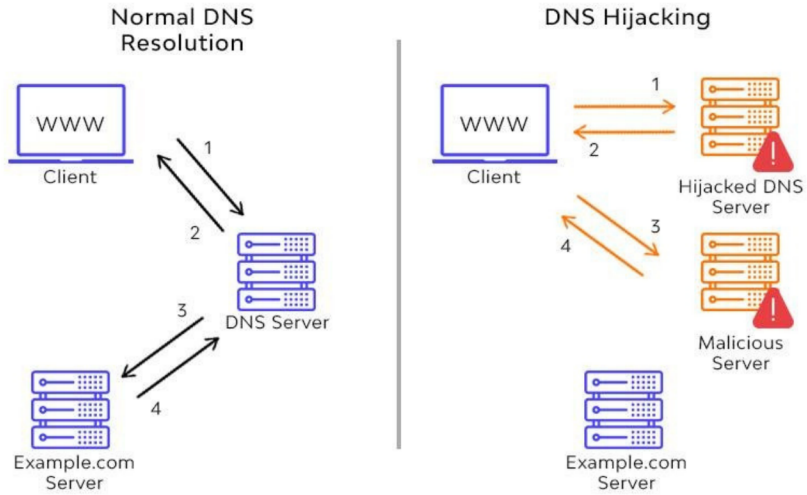
Types of DNS Record

DNS servers use DNS records to store crucial information about domains and hostnames, with one of the primary purposes being to map domain names to IP addresses.

- **Address Mapping Record (A Record)**: Holds the IP address of a domain.
- **IP Version Address Record (AAAA Record)**: Contains the IPv6 address for a domain.
- **Canonical Name Record (CNAME Record):** Aliases one domain to another without providing an IP address.
- **Name Server Record (NS Record):** Specifies the nameserver for a DNS entry.
- **Mail Exchanger Record (MX Record):** Defines an SMTP email server for the domain to route outgoing emails.
- **Other records:** Reverse Lookup Pointer Record (PTR Record), Text Record (TXT Record), Certificate Record, Service Location Record (SRV Record), Start of Authority Record (SOA Record), Certification Authority Authorization Record (CAA Record).

DNS Hijacking Overview

- An attack on the Domain Name System (DNS).
- Can render DNS unavailable or redirect users to malicious sites without their notice.



Attack Methods

- Installing malware on user computers.
- Taking over or hacking into routers.
- **Hijacking unclaimed or misconfigured DNS records.**
- Intercepting or hacking into DNS communication.

Types of DNS Hijacking

- **Local DNS Hijack:** Malware changes a computer's DNS settings or modifies the /etc/hosts file to redirect to malicious sites.
- **Router DNS Hijack:** Attackers exploit router vulnerabilities to change DNS settings, affecting all connected devices.
- **DNS Spoofing:** Attackers intercept DNS queries and provide false IP addresses, leading users to harmful sites.
- **DNS Cache Poisoning:** Inserting fake DNS entries into the DNS cache, causing users to visit spoofed sites instead of the intended destination.
- **Compromised DNS Server:** Hacking into DNS servers or admin panels to alter DNS records, redirecting traffic to attacker-controlled sites.
- **ISP Interference:** ISPs hijack DNS queries to show ads or collect data by manipulating NXDOMAIN responses.
- **Misconfigured DNS Hijack:** Exploiting DNS misconfigurations or unclaimed records to host malicious content.

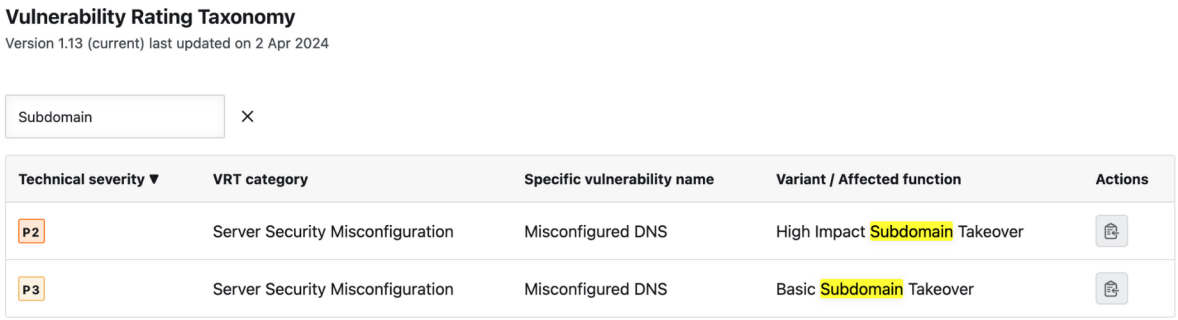
Subdomain Hijacking / Takeover

- Occurs when an attacker takes control of a subdomain due to DNS misconfigurations or oversight.
- Exploits dangling DNS records (CNAME, A/AAAA, NS, MX etc.) that point to services not currently in use or controlled by the domain owner.

- Expired Domains, Discontinued Services or De-provisioned cloud instances.

Most common DNS misconfiguration leads to:

- CNAME Record Hijacking
- A/AAAA Record Hijacking
- NS Record Hijacking
- MX Record Hijacking
- Second Order Hijacking



Vulnerability Rating Taxonomy

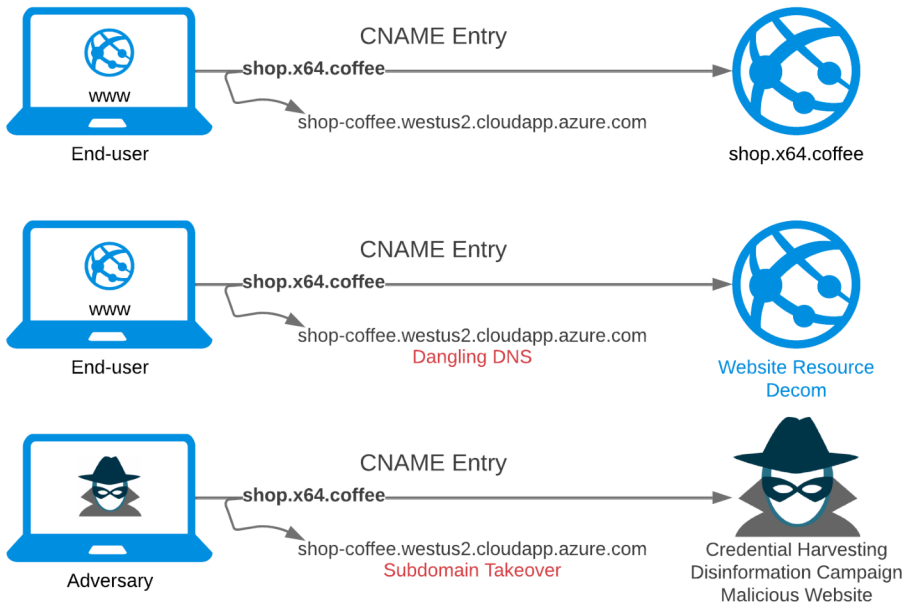
Version 1.13 (current) last updated on 2 Apr 2024

Subdomain ×

Technical severity ▼	VRT category	Specific vulnerability name	Variant / Affected function	Actions
P2	Server Security Misconfiguration	Misconfigured DNS	High Impact Subdomain Takeover	
P3	Server Security Misconfiguration	Misconfigured DNS	Basic Subdomain Takeover	

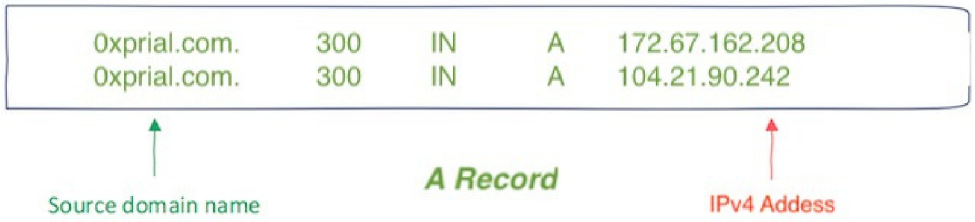
Subdomain Hijacking: CNAME

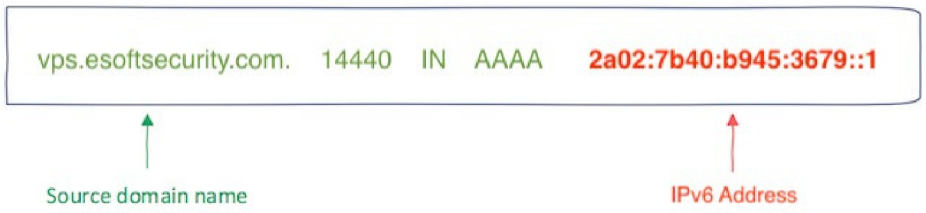
- Targets subdomains with CNAME records pointing to external services (like cloud-hosted web apps) that have been deleted or abandoned.
- Attackers register the abandoned service's domain, gaining the ability to serve content on the original subdomain.



Subdomain Hijacking: A/AAAA

- Focuses on subdomains whose A or AAAA records point to IP addresses that have been released and are available for registration.
- By acquiring the unused IP addresses, attackers can host malicious sites that appear to be legitimate subdomains



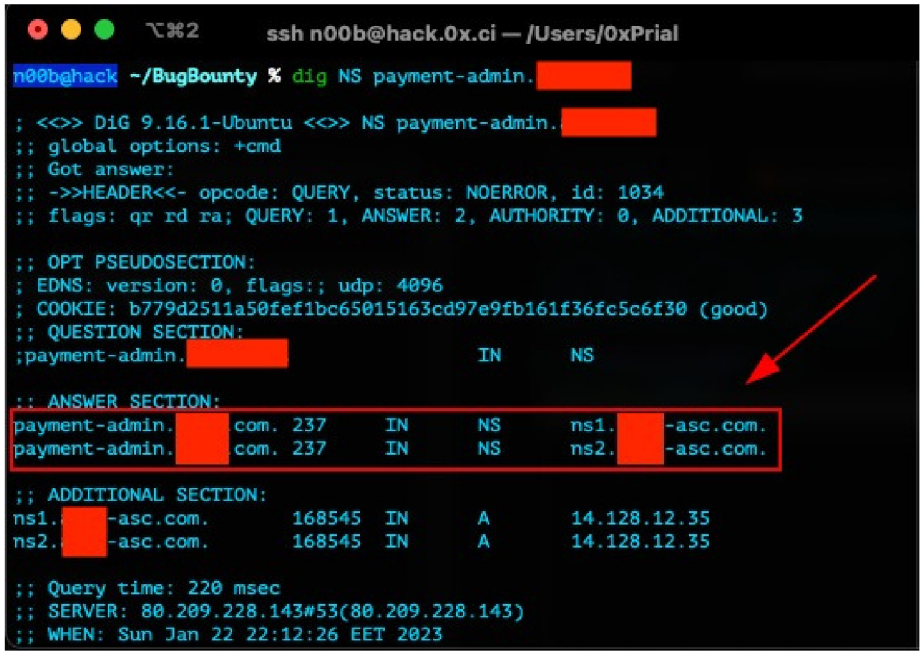


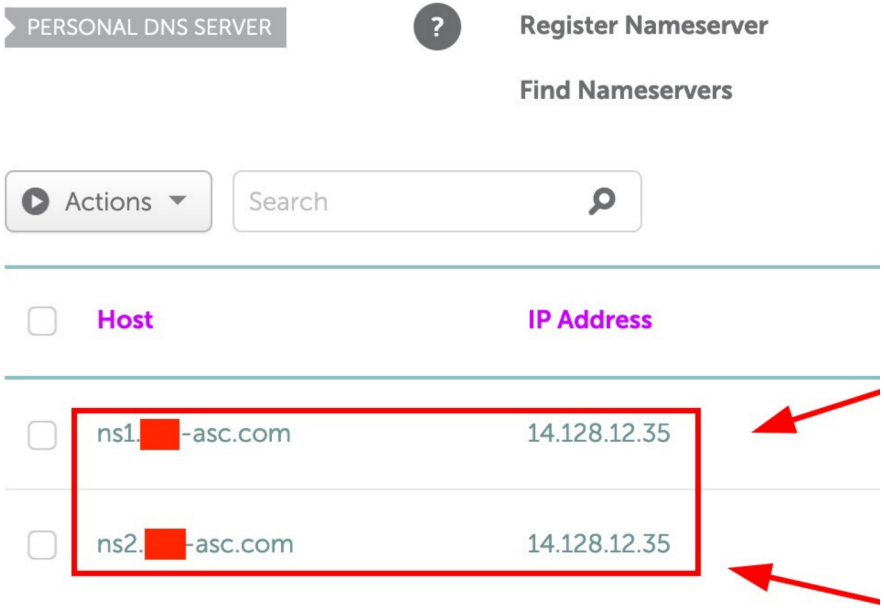

```
❯ ghostbuster scan aws --cloudflaretoken whougonnacall

Obtaining all zone names from Cloudflare.
Obtaining DNS A records for all zones from Cloudflare.
Obtained 33 DNS A records so far.
Obtaining Route53 hosted zones for AWS profile: default.
Obtaining Route53 hosted zones for AWS profile: account-five.
Obtaining Route53 hosted zones for AWS profile: account-four.
Obtaining Route53 hosted zones for AWS profile: account-four-deploy.
Obtaining Route53 hosted zones for AWS profile: account-two-deploy.
Obtaining Route53 hosted zones for AWS profile: account-one-deploy.
Obtaining Route53 hosted zones for AWS profile: account-three-deploy.
Obtaining Route53 hosted zones for AWS profile: account-six.
Obtaining Route53 hosted zones for AWS profile: account-seven.
Obtaining Route53 hosted zones for AWS profile: account-one.
Obtained 124 DNS A records so far.
Obtaining EIPs for region: us-east-1, profile: default
Obtaining IPs for network interfaces for region: us-east-1, profile:
Obtaining EIPs for region: us-east-1, profile: account-five
Obtaining IPs for network interfaces for region: us-east-1, profile:
Obtaining EIPs for region: us-east-1, profile: account-four
Obtaining IPs for network interfaces for region: us-east-1, profile:
Obtaining EIPs for region: us-east-1, profile: account-four-deploy
Obtaining IPs for network interfaces for region: us-east-1, profile:
Obtaining EIPs for region: us-east-1, profile: account-two-deploy
Obtaining IPs for network interfaces for region: us-east-1, profile:
Obtaining EIPs for region: us-east-1, profile: account-one-deploy
Obtaining IPs for network interfaces for region: us-east-1, profile:
Obtaining EIPs for region: us-east-1, profile: account-three-deploy
Obtaining IPs for network interfaces for region: us-east-1, profile:
Obtaining EIPs for region: us-east-1, profile: account-six
Obtaining IPs for network interfaces for region: us-east-1, profile:
Obtaining EIPs for region: us-east-1, profile: account-seven
Obtaining IPs for network interfaces for region: us-east-1, profile:
Obtaining EIPs for region: us-east-1, profile: account-one
Obtaining IPs for network interfaces for region: us-east-1, profile:
Obtained 415 unique elastic IPs from AWS.


Takeover possible: {'name': 'takeover.assetnotecloud.com', 'records':
```

https://www.assetnote.io/resources/research/eliminating-dangling-elastic-ip-takeovers-with-ghostbuster

Subdomain Hijacking: NS

- Involves taking control of the Name Server (NS) records of a subdomain, effectively taking over its DNS management.
- This is achieved by redirecting the NS records to attacker-controlled DNS servers, allowing full control over the subdomain's DNS entries.





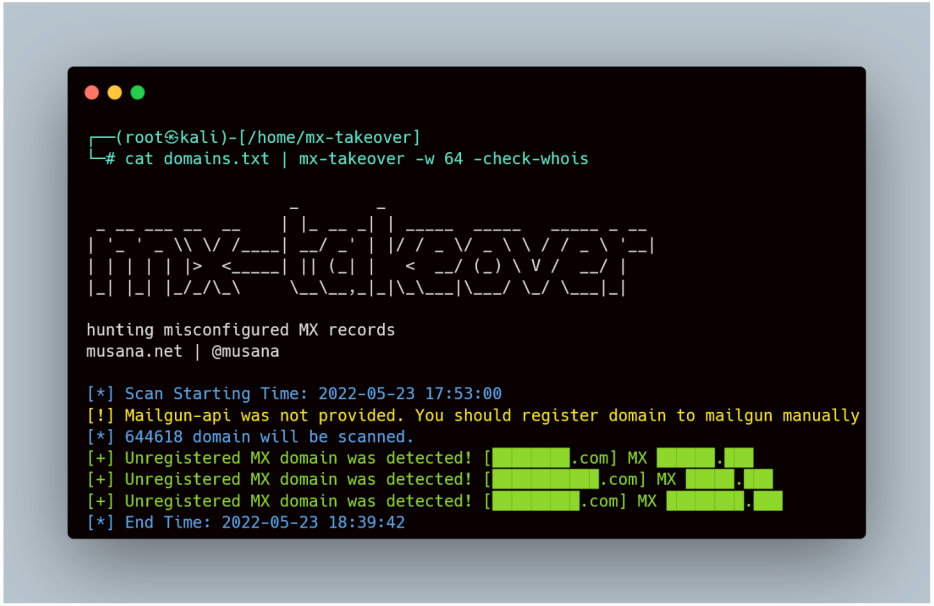
https://shivsahni2.medium.com/aws-ns-takeover-356d2a293bca

Subdomain Hijacking: MX

- Attackers change the Mail Exchange (MX) records of a subdomain to redirect incoming emails to servers they control.
- This allows them to intercept, read, and potentially alter email communications.

Mailgun Attack Scenario

- Company switches to Mailgun, pointing MX record to it (e.g., sub.domain.com MX mxa.mailgun.com).
- Company stops using Mailgun but doesn't update MX record.
- Attacker claims the domain on Mailgun with no verification, due to existing DNS setup.
- Attacker reads emails sent to the domain (e.g., <someone>@sub.domain.com).



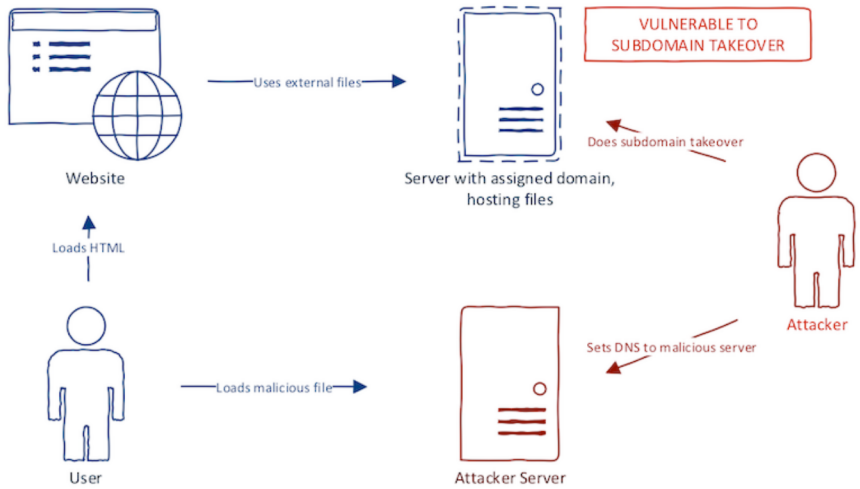
Note: Mailgun no longer vulnerable!

Subdomain Hijacking: Second Order

- This advanced technique involves hijacking a domain or subdomain that other domains or subdomains alias to via their CNAME or other DNS records.
- By taking over the target, attackers indirectly gain control over any other domain or subdomain that relies on it, leading to a widespread impact.

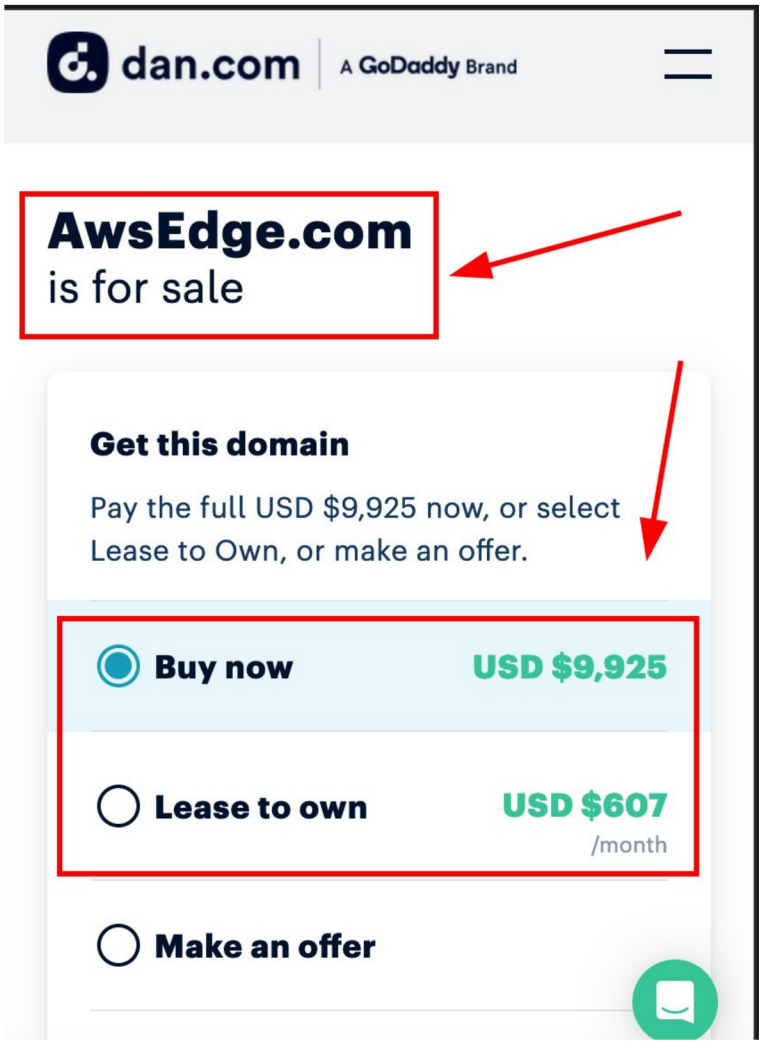
Attack Scenario

- assets.company.com is hijacked, previously hosting JavaScript files used across various company websites.
- app.company.com has a webpage that loads a JavaScript file from assets.company.com/js/app.js.
- After hijacking, the attacker replaces app.js with a malicious version.
- Visitors to app.company.com unknowingly execute the malicious JavaScript, leading to data theft or other security breaches.



Subdomain Hijacking (Example)

```
┌──(0xprial㉿trojan)-[~]
└─$ dig example.[redacted].com

; <<>> DiG 9.10.6 <<>> example.[redacted].com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 40898
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;example.[redacted].com.                IN      A

;; ANSWER SECTION:
example.[redacted].com.         3600    IN      CNAME   example.awsedge.com.

;; AUTHORITY SECTION:
awsedge.com.            600     IN      SOA     dns17.hichina.com. hostm
a.com. 2022052002 3600 1200 86400 600
```



What Can be Done?

- **Session Hijacking to Account Takeover:**
  - If cookies are set with the domain attribute set to the hijacked subdomain, attackers can hijack sessions and potentially take over accounts.
- **CORS Policy Bypass:**
  - If the Access-Control-Allow-Origin header is set to accept requests from the hijacked domain, this can bypass CORS policies, leading to data leaks.
- **OAuth Redirection for Authorization Code Theft:**
  - If the hijacked domain is whitelisted in OAuth settings, attackers can redirect OAuth responses to obtain authorization codes.
- **CSP Policy Manipulation for XSS:**
  - If a CSP (Content Security Policy) whitelists the hijacked domain, it can be exploited for cross-site scripting (XSS) attacks.
- **Clickjacking:**
  - If X-Frame-Options include the hijacked domain in its whitelist, attackers can use this for clickjacking attacks.

What Can be Done? (Cont'd)

- **Malware Distribution:**
  - The hijacked domain can serve as a platform for distributing malware.
- **JavaScript Code Execution & Stored XSS:**
  - Attackers can execute malicious JavaScript codes from the hijacked domain, enabling attacks like stored XSS.
- **Advanced Phishing & Keylogging:**
  - By serving malicious content on the hijacked domain, attackers can conduct phishing and deploy keyloggers to capture keystrokes.
- **Spoofing Emails:**
  - If an SPF (Sender Policy Framework) record includes the hijacked domain, it can be used to send spoofed emails, undermining email authenticity.

- **Email Compromise:**
  - Attackers can compose and send emails from the hijacked domain, facilitating social engineering attacks.

Scam: Mint Your Ferrari

- forms.ferrari.com takeover (AWS); NFT Scam
- Over $800 collected before domain takedown

Ferrari Subdomain Hijacked to Push Fake Ferrari NFT Collection

According to researchers, one of Ferrari's subdomains was hijacked yesterday to host a scam promoting a fake Ferrari NFT collection.

What makes the scam particularly interesting is that the carmaker had announced plans to launch NFTs in partnership with tech firm Velas earlier.

The Ethereum wallet associated with the cryptocurrency scam appears to have collected a few hundred dollars before the hacked subdomain was shut down.

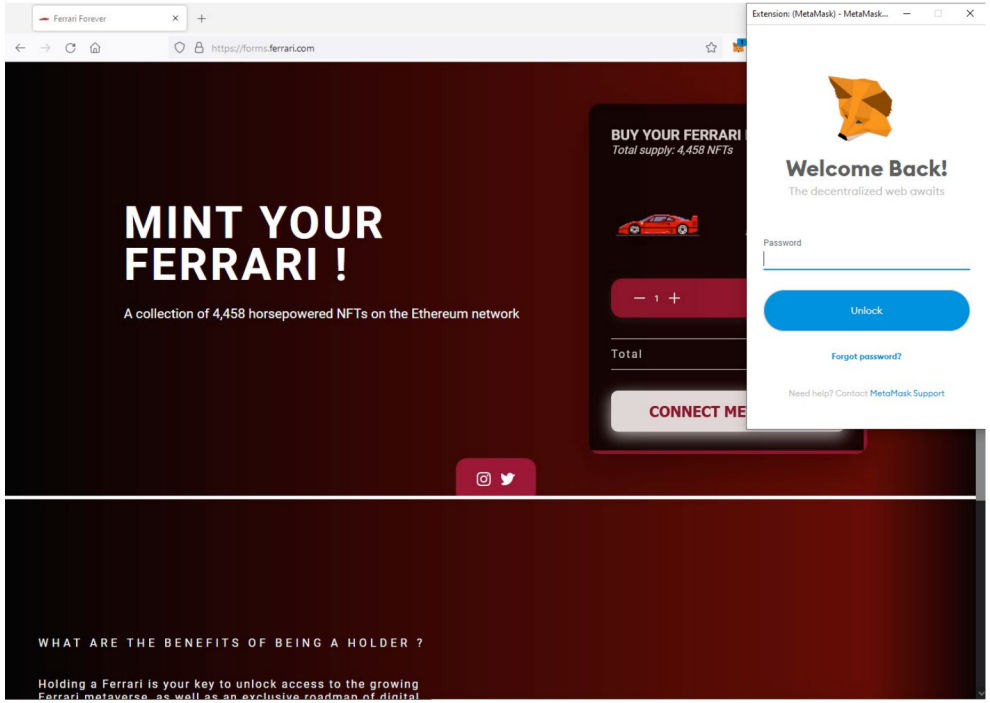
An NFT is data stored on a cryptocurrency blockchain that a digital certificate has signed to prove that it is unique and cannot be copied.

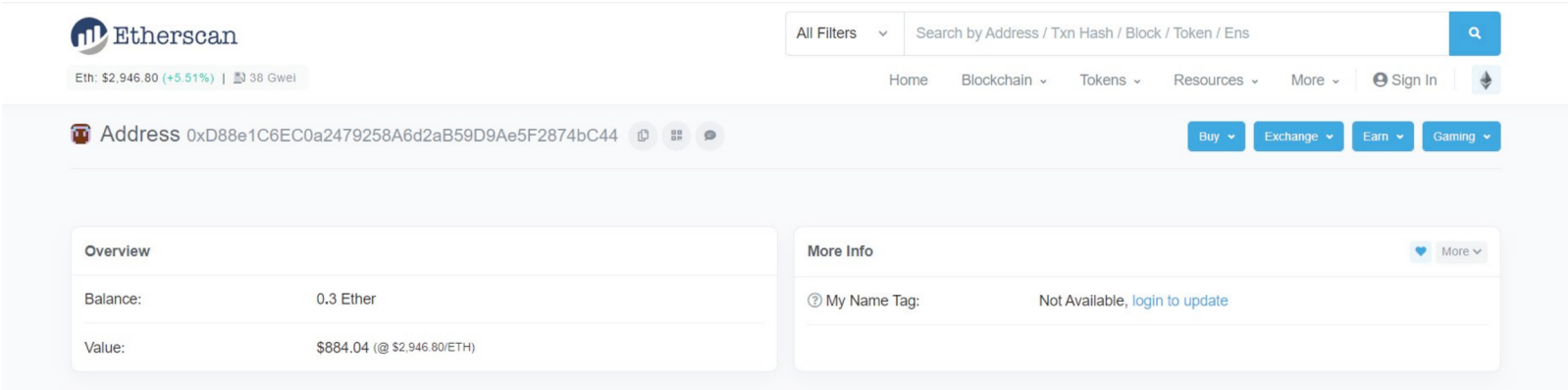
On Thursday, Sam Curry, an ethical hacker and bug bounty hunter reported seeing one of Ferrari's subdomains *forms.ferrari.com* hosting a fake NFT (Non-Fungible Token) scam.

Last year, Ferrari had announced plans to launch NFT products in partnership with Velas, making this scam all very convincing.

The crypto scam titled "Mint your Ferrari" enticed visitors to buy NFT tokens, falsely touting that Ferrari introduced "a collection of 4,458 horsepower [sic] NFTs on the Ethereum network."

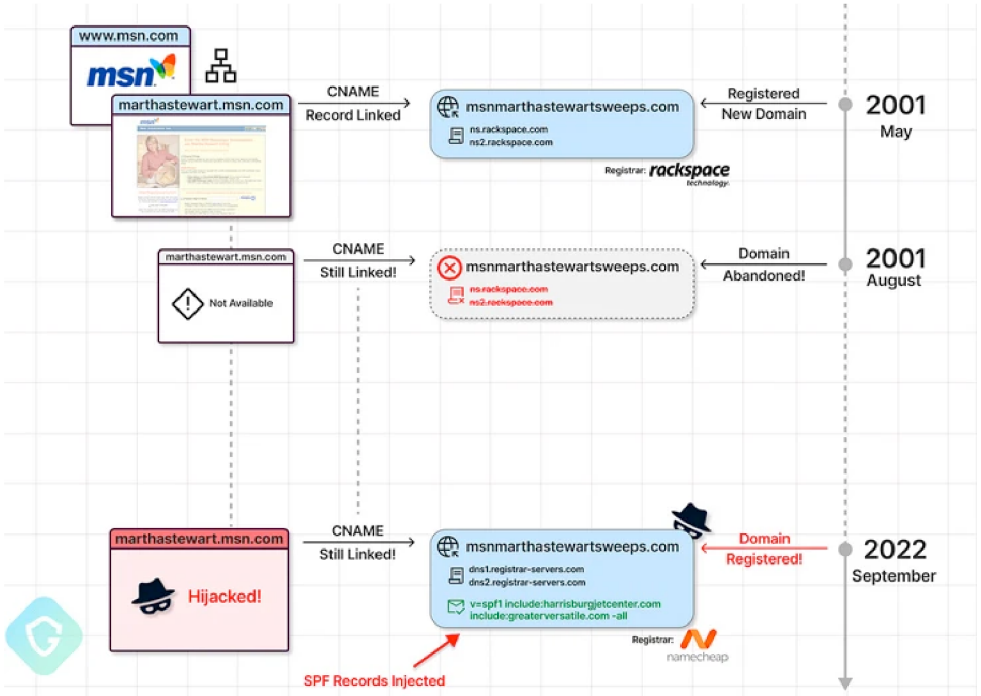
Additional investigation revealed that attackers exploited an Adobe Experience Manager flaw to hack the subdomain and host their crypto scam.

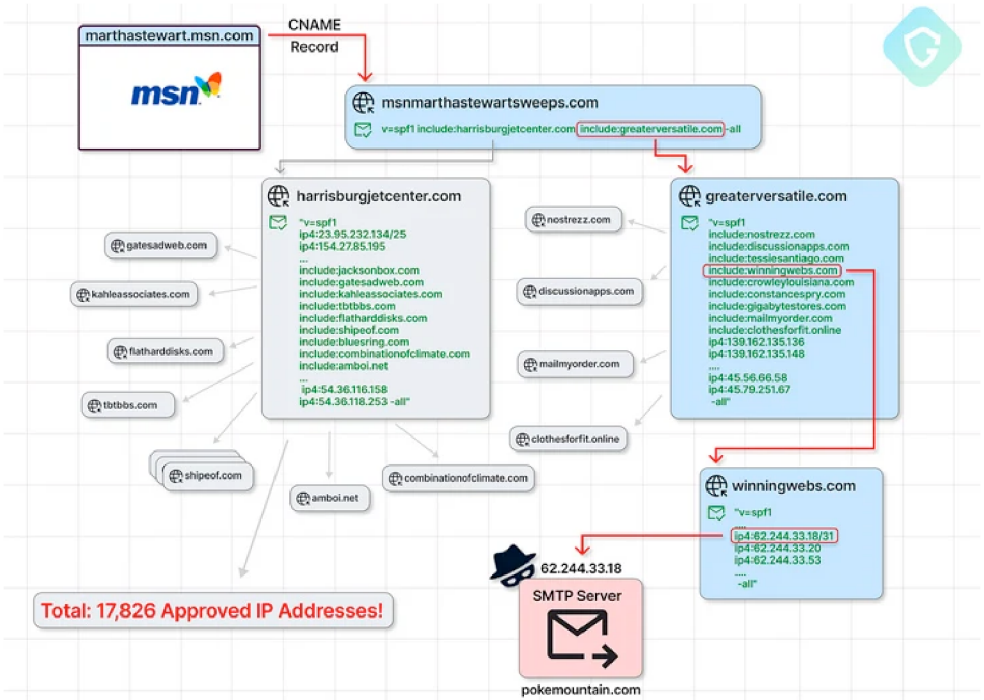




SubdoMailing Phishing Campaign

More than 8,000 domains and 13,000 subdomains associated with big brands were hijacked.

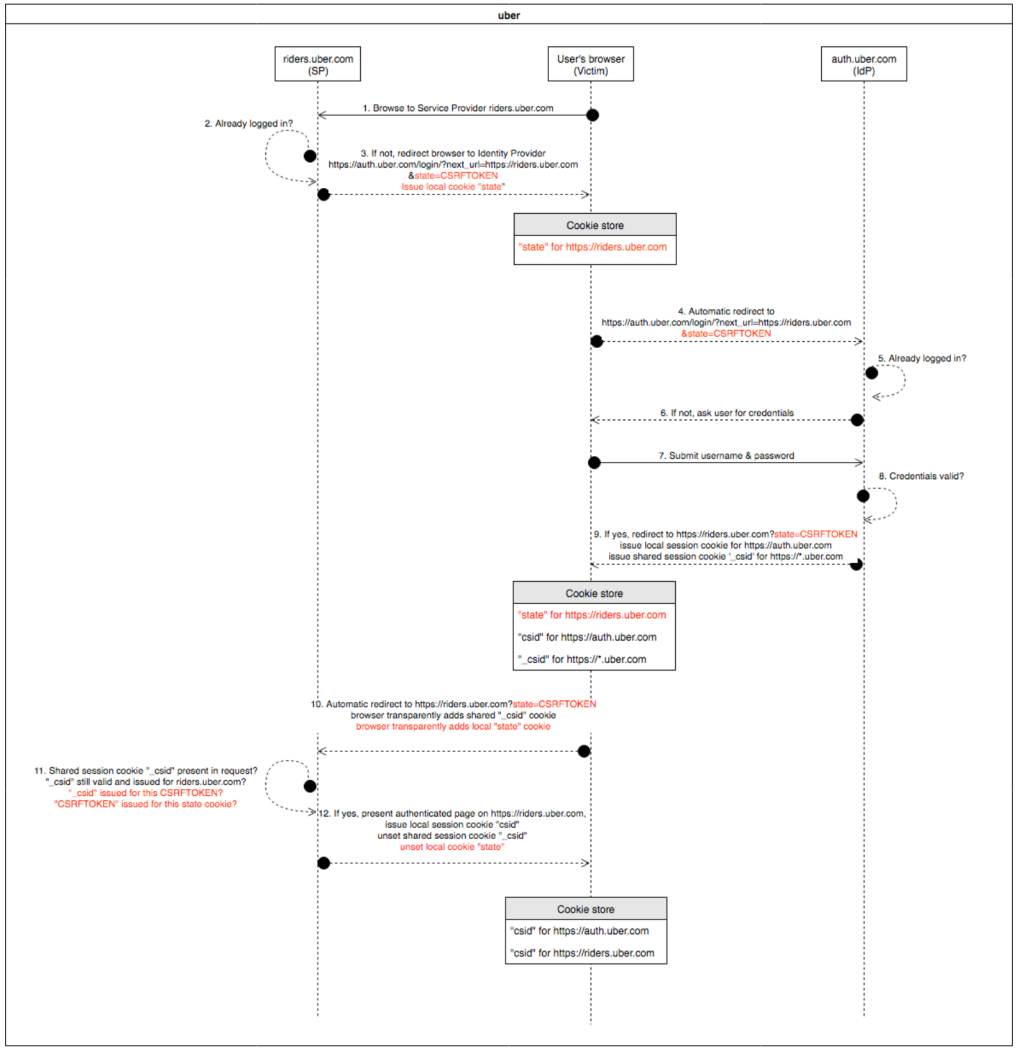




https://www.cpomagazine.com/cyber-security/massive-ad-fraud-campaign-sends-million-of-spam-emails-from-thousands-of-hijacked-reputable-domains/

Authentication Bypass (SSO): Uber & Ubiquity

- Uber's SSO allowed hijacking of session cookies from auth.uber.com
- Attack viable on any compromised *.uber.com subdomain, post-single authentication.
- saostatic.uber.com takeover (AWS Cloudfront)
- riders.uber.com generates shared session cookie "_csid" from auth.uber.com
- session cookie stolen via tricking victim to visit saostatic.uber.com



Similar Report

- Authentication bypass (SSO) on sso.ubnt.com via subdomain takeover of ping.ubnt.com

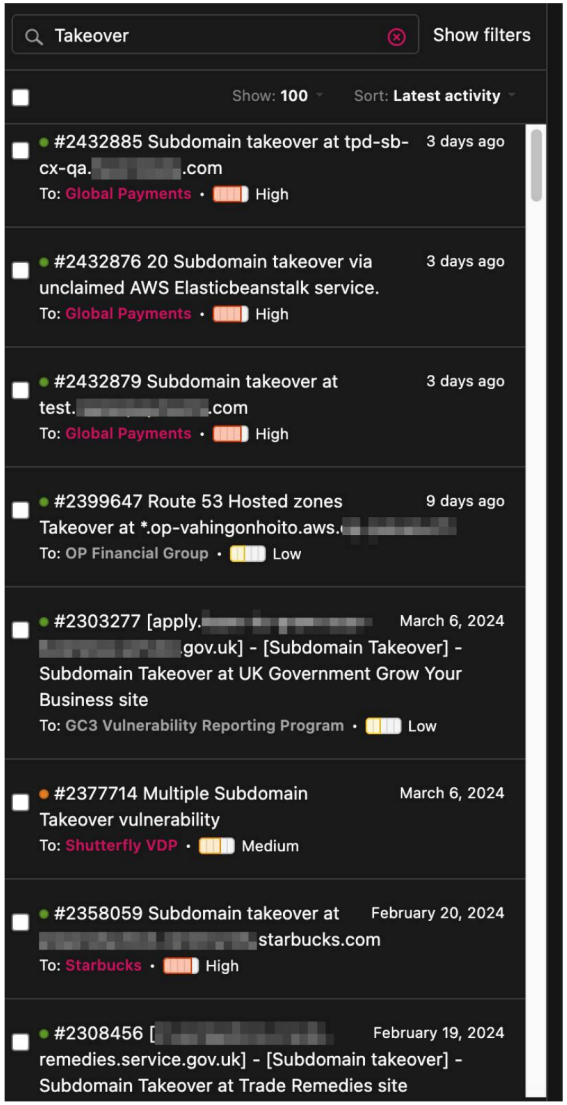
https://hackerone.com/reports/172137

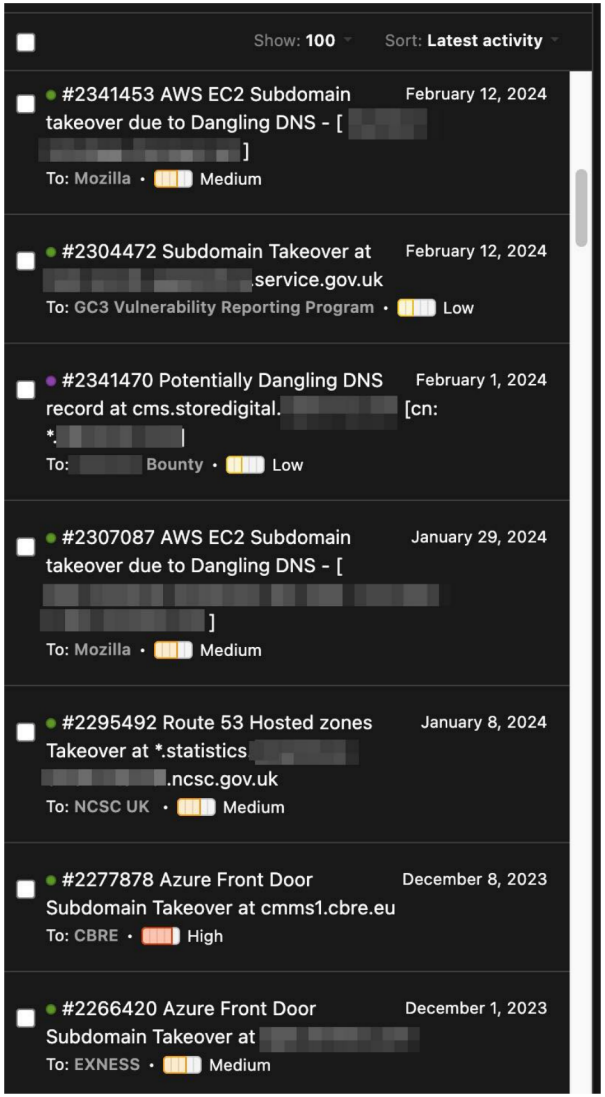
- Roblox Auth Bypass via Subdomain Takeover

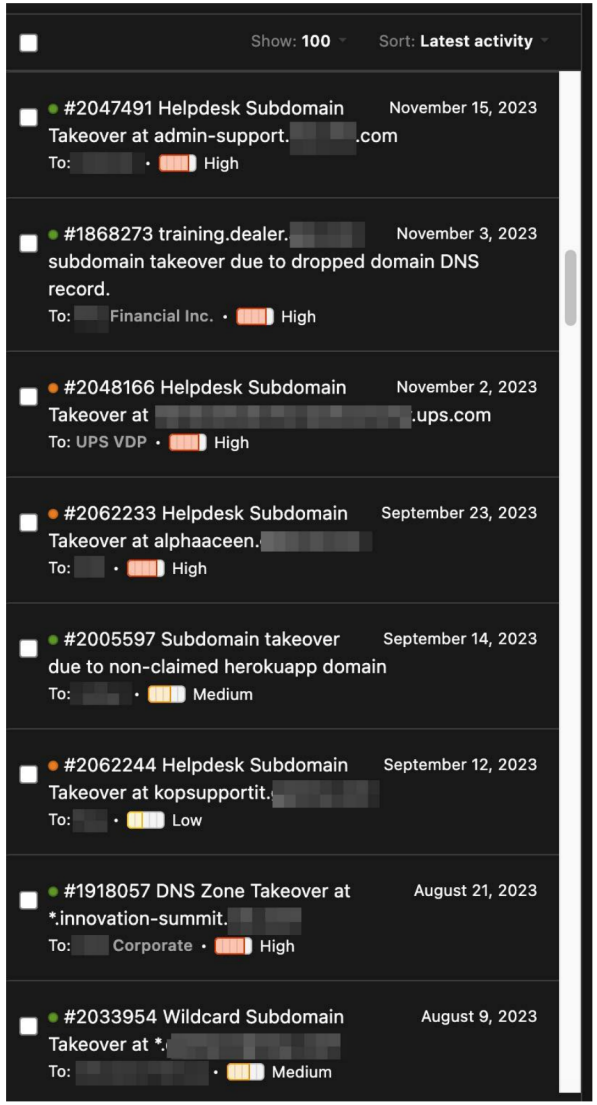
https://hackerone.com/reports/335330

https://hackerone.com/reports/219205

Subdomain Takeover: Bug Bounty







Subdomain Takeover: Bug Bounty (Cont'd)

U.S. Dept Of Defense — High — Resolved

- AWS subdomain takeover of www.[redacted]

8 — Disclosed 2 years ago by al-madjus — Improper Access Control - Generic

The AWS bucket hosted on www.[redacted] was vulnerable to a subdomain takeover, allowing an attacker to potentially steal cookies, bypass CSP and CORS policies, bypass domain whitelisting for SSRF, spy on legitimate requests sent to that domain, or use it as a phishing vector. The vulnerability was caused by a dangling DNS record pointing to an unclaimed bucket that was registered by the attacker. This summary was automatically generated.

Kubernetes — Medium — $250 — Resolved

- Subdomain Takeover Via via Dangling NS records on Amazon Route 53 http://api.e2e-kops-aws-canary.test-cncf-aws.canary.k8s.io

55 — Disclosed 3 years ago by todayisnew — Improper Authentication - Generic

HackerOne — Medium — $1,000 — Resolved

Takeover of hackerone.engineering via Github

115 — Disclosed 8 months ago by m0chan — Privilege Escalation

The hacker was able to take over the hackerone.engineering domain after a brief misconfiguration window on GitHub. They claimed the domain in their own repository while the DNS records were still pointing towards GitHub. The issue has been resolved and no malware was found on the site during the takeover. This summary was automatically generated.

Reddit — High — $5,000 — Resolved

- s3 bucket takeover presented in https://github.com/reddit/rpan-studio/blob/e1782332c75ecb2f774343258ff509788feab7ce/CI/full-build-macos.sh

81 — Disclosed 2 years ago by gaurav-bhatia — Business Logic Errors

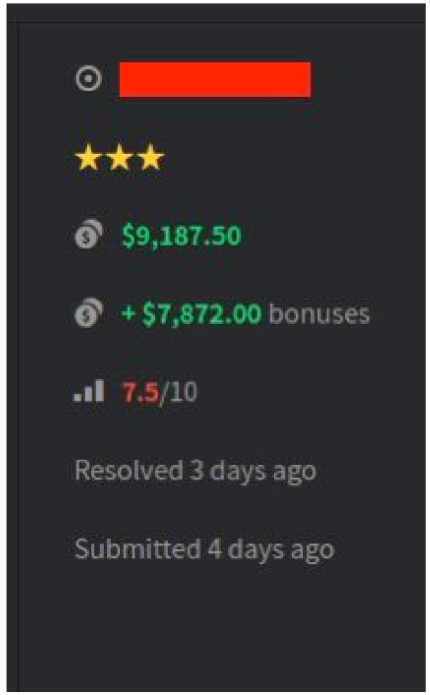
An unclaimed S3 bucket was found in the code of rpanstudio's full-build-macos.sh script on GitHub, which could be taken over by an attacker to host malicious content with the same name as the files in the code, potentially spreading ransomware and other malicious files. The vulnerability has a critical impact as the code is used by many people. This summary was automatically generated.

Uber — Subdomain takeover at signup.uber.com
By ak1t4 to Uber | Resolved | High | $3,000.00

Subdomain takeover on happymondays.starbucks.com due to non-used AWS S3 DNS record
By dpgribkov to Starbucks | Resolved | High | $2,000.00

Subdomain takeover at info.hacker.one
By ak1t4 to HackerOne | Resolved | Low | $1,000.00

Subdomain Takeover at test.shipt.com
By m7mdharoun to Shipt | Resolved | High | $750.00



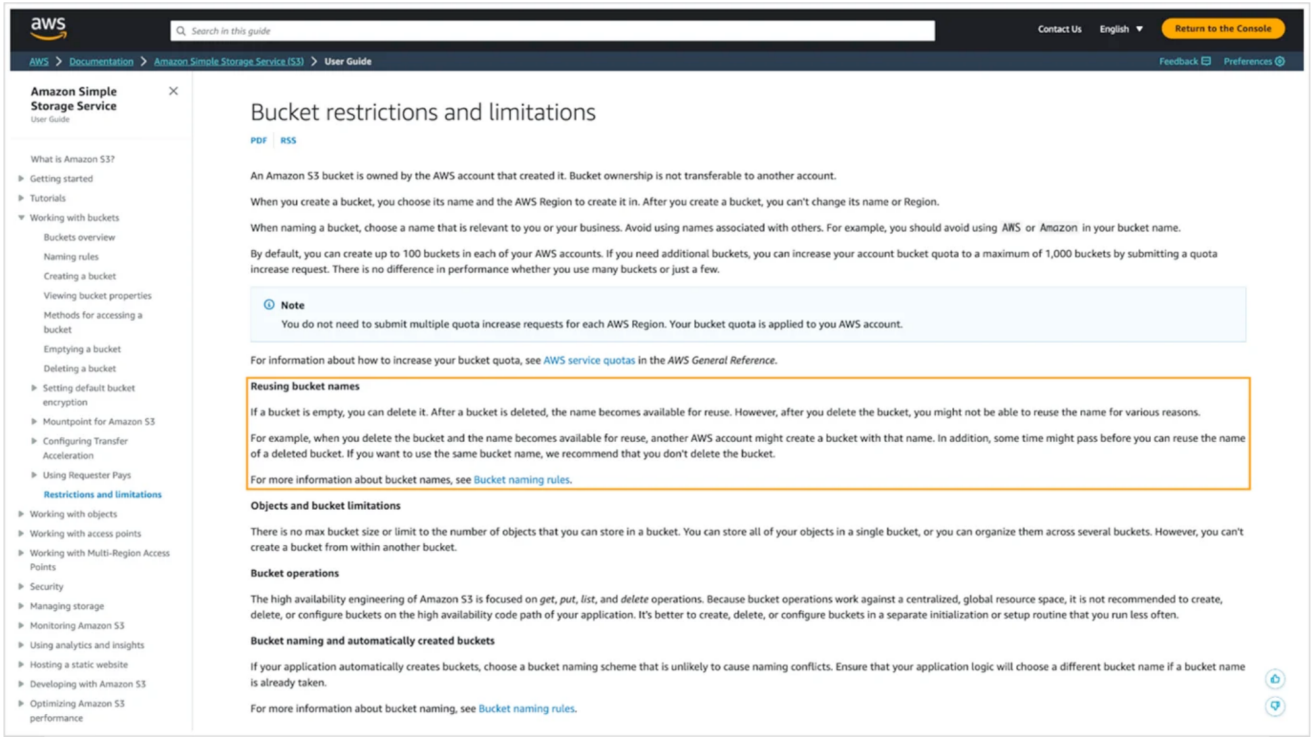
CAN I Takeover XYZ?

Edwin Foudil maintains a list of vendors susceptible to subdomain takeover in his can-i-take-over-xyz Github repository.

Engine	Status	Verified by CI/ CD	Domains	Fingerprint
AWS/Elastic Beanstalk	Vulnerable	🟩	elasticbeanstalk.com	`NXDOMAIN`
AWS/Load Balancer (ELB)	Not vulnerable	🟥	elb.amazonaws.com	`NXDOMAIN`
AWS/S3	Vulnerable	🟩	s3.amazonaws.com	`The specified bucket does not exist`
Acquia	Not vulnerable	🟥		`Web Site Not Found`
Agile CRM	Vulnerable	🟥	agilecrm.com	`Sorry, this page is no longer available.`
Airee.ru	Vulnerable	🟩	airee.ru	`Ошибка 402. Сервис Айри.рф не оплачен`
Akamai	Not vulnerable	🟥		
Anima	Vulnerable	🟩	animaapp.io	`The page you were looking for does not exist.`
Bitbucket	Vulnerable	🟩	bitbucket.io	`Repository not found`

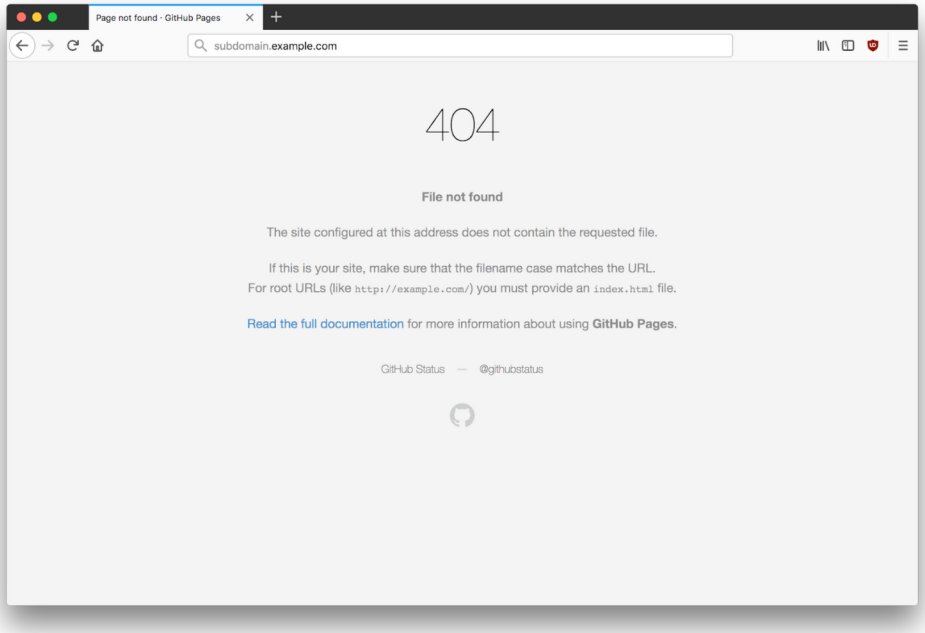
CAN I Takeover XYZ? (Fingerprint)

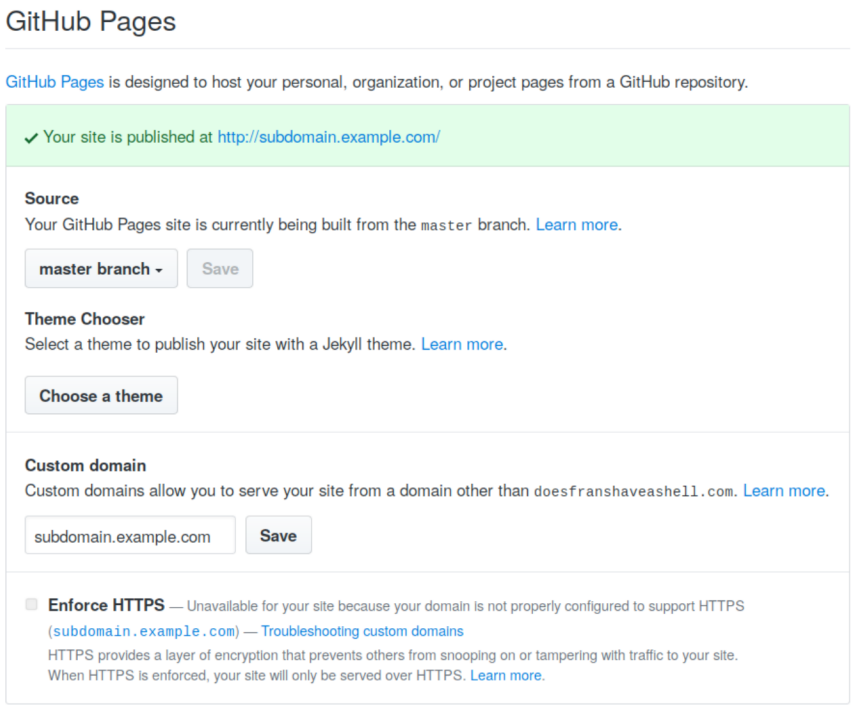
- AWS S3 Bucket Takeover



CAN I Takeover XYZ? (Fingerprint)

Github Pages





Tools for Penterster / Ethical hacker

Subdomain Enumeration

- **Amass (OWASP):** https://github.com/owasp-amass/amass
- **Sublist3r:** https://github.com/aboul3la/Sublist3r
- **Subscraper:** https://github.com/m8sec/subscraper

Use multiple tools to enumerate subdomains: Active and passive scans

Filter valid subdomains Based on DNS Records + DNS query status, and then use tools like httpx.

```
for domains in $(cat domains.txt);do dig $domains +noquestion +noauthority +noadditional +nostats | grep -wE "CNAME|A|NS";done
```

Takeover Checker

- **Nuclei:** https://github.com/projectdiscovery/nuclei
- **Nuclei Templates:** https://github.com/projectdiscovery/nuclei-templates

```
nuclei -l $1 -t $HOME/BugBounty/nuclei-templates-takeover/ -no-httpx
```

Mitigate Strategies: Blue Team

Regular Audits of DNS Records

- **Frequency:** Aim for at least quarterly audits, with increased frequency for critical or often-altered domains.
- **Scope:** Examine all DNS records, such as CNAMEs, A, TXT, and MX records.
- **Focus Areas:** Identify and remove unused records, update outdated entries, and correct records that point to unauthorized locations.

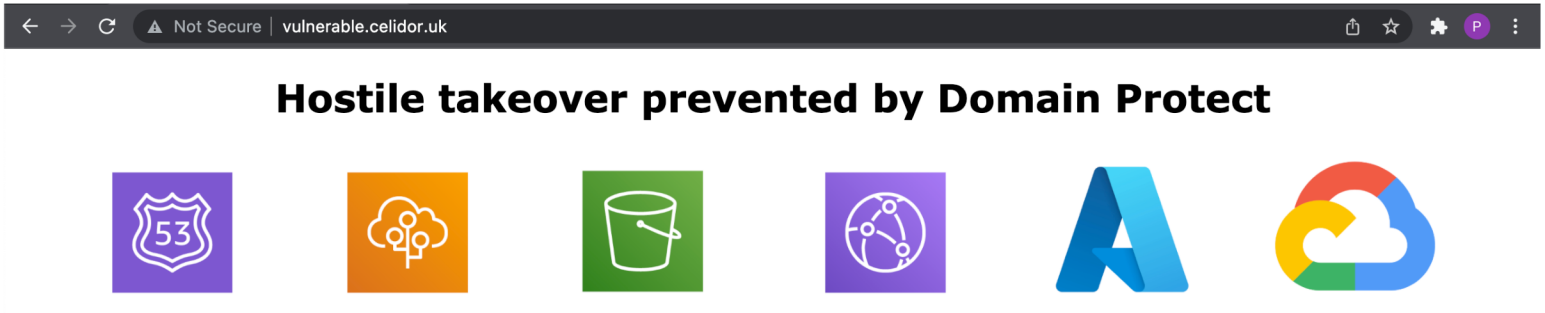
Implement Domain Monitoring Tool

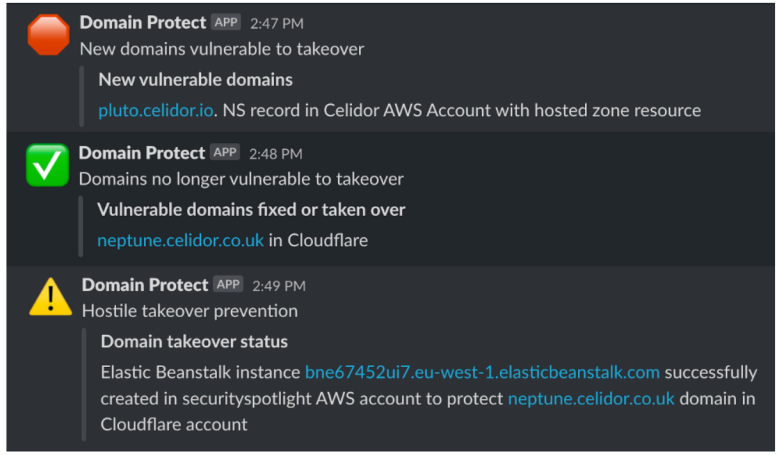
- **Tool Selection:** Opt for tools that provide ongoing monitoring, and real-time alerts for suspicious activities.
- **Monitoring Priorities:** Keep an eye on DNS record modifications, new subdomain registrations, and unauthorized access attempts.

Continuous Monitoring: Blue Team

Tool: OWASP Domain Protect

- Supports AWS, GCP, Azure, Cloudflare Integration.
- Manual scan without cloud account integration.
- Real-time notification and stats via Slack.



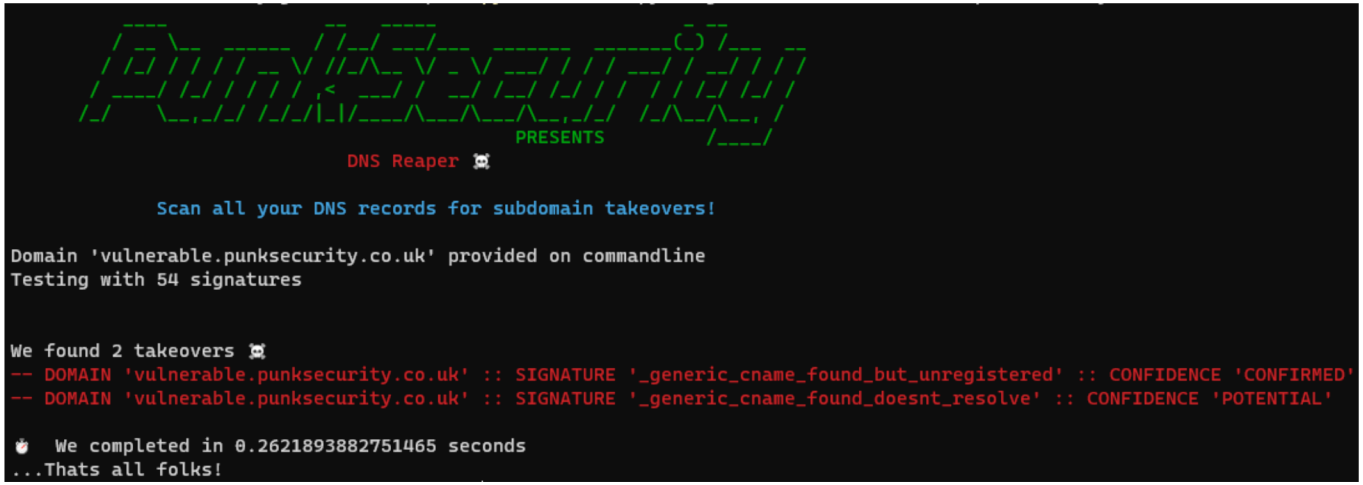


https://github.com/domain-protect/

Continuous Monitoring: Blue Team (Cont'd)

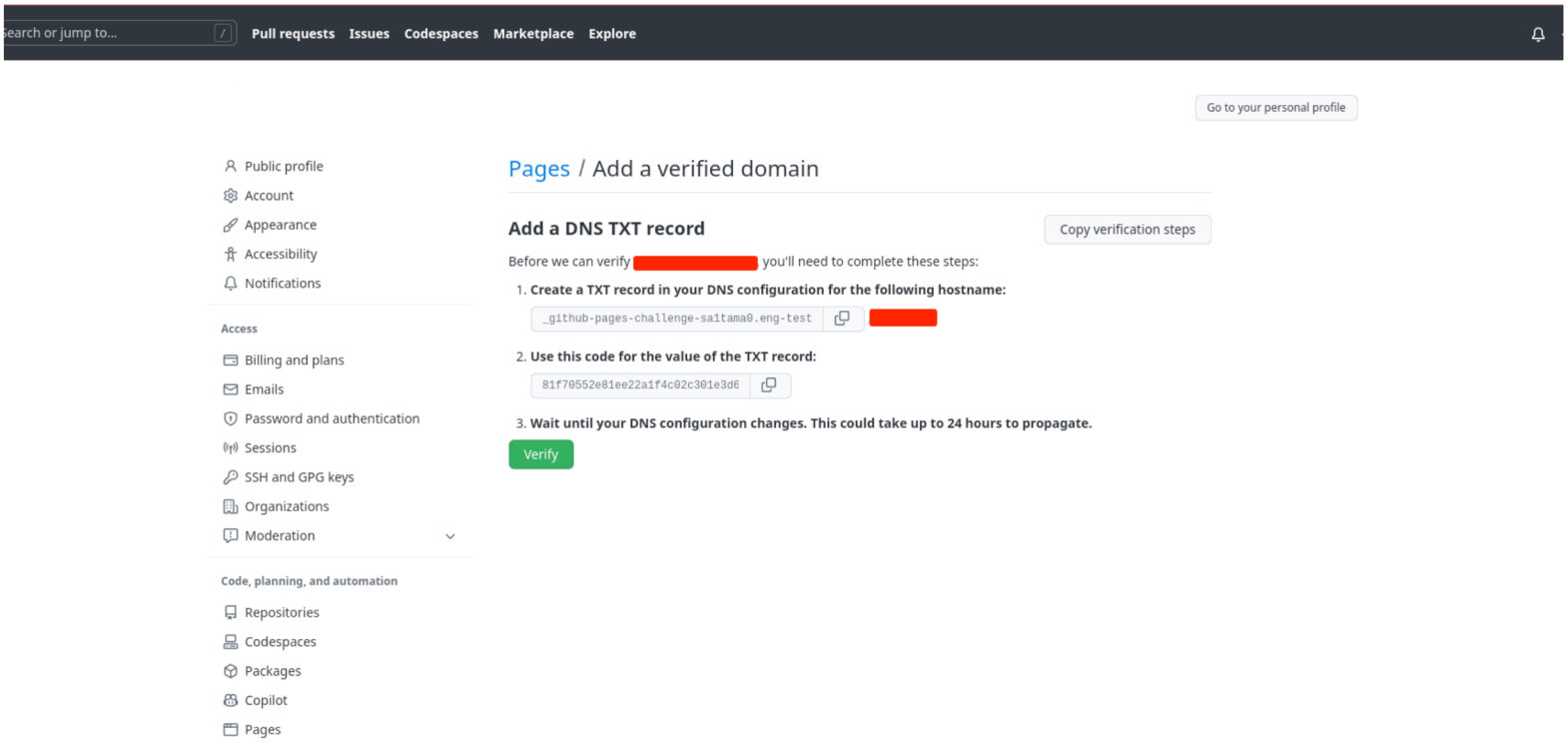
Tool: dnsReaper

- Supports AWS Route53, Cloudflare, and Azure.
- Can be integrated with ChoasDB (DNS dataset from projectdiscovery.io)



Protection from Service Provider

GitHub



https://github.com/EdOverflow/can-i-take-over-xyz/

https://github.com/indianajson/can-i-take-over-dns


QUESTION
time