

[REDACTED]

## Domain Analysis for [REDACTED]

### Whois:

uncovered detailed information about the domain [REDACTED]. Registered with [REDACTED] the domain was created on September 15, 1995, and last updated on September 15, 2020. It is scheduled to expire on September 14, 2030. The registrar's contact details, including [REDACTED] are provided for addressing any abuse or inaccuracy concerns. The domain's status is "clientTransferProhibited," indicating restrictions on domain transfers. Two name servers, [REDACTED] and [REDACTED] are listed. However, it's noteworthy that the domain does not have DNSSEC enabled. This comprehensive analysis provides insights into the domain's longevity, registration details, and infrastructure, facilitating a deeper understanding of its online presence and potential security implications.

```
Domain Name: [REDACTED]
Registry Domain ID: [REDACTED]
Registrar WHOIS Server: [REDACTED]
Registrar URL: [REDACTED]
Updated Date: 2020-09-15T02:21:11Z
Creation Date: 1995-09-15T04:00:00Z
Registry Expiry Date: 2030-09-14T04:00:00Z
Registrar: [REDACTED]
Registrar [REDACTED]
Registrar Abuse Contact Email: [REDACTED]
Registrar Abuse Contact Phone: [REDACTED]
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: [REDACTED]
Name Server: [REDACTED]
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-04-29T21:51:24Z <<<
```

Figure 1: whois data

### MXToolbox:

#### 1. Hostname and IP Address Analysis:

- The hostname "us-smtp-inbound-1.mimecast.com" and "us-smtp-inbound-2.mimecast.com" both resolve to the same IP address, [REDACTED]
- This IP address belongs to the AS30031 network, and it is associated with the email service provider "Mimecast."

## 2. DNS and DMARC Analysis:

- A DNS lookup performed on [REDACTED] on April 29, 2024, at 4:54:50 PM (UTC -5) indicates that the DMARC record is not published.
- The DMARC policy is not enabled, as indicated by the warning status.

## 3. Supertool Functionality:

- The Supertool provides integrated MX record, DNS, blacklist, and SMTP diagnostics.
- Users can input domain names, IP addresses, or host names to conduct various tests and lookups.
- Specific commands, such as "blacklist," "smtp," "mx," "spf," and "txt," can be used to force tests or lookups.

[REDACTED]

Find Problems

Solve Email Delivery Problems

mx

Pref	Hostname	IP Address	TTL	
500	us-smtp-inbound-1.mimecast.com	[REDACTED]	5 sec	Blacklist Check SMTP Test
505	us-smtp-inbound-2.mimecast.com	[REDACTED]	5 sec	Blacklist Check SMTP Test

Test	Result	
✖ DMARC Record Published	No DMARC Record found	More Info
⚠ DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled	More Info
✔ DNS Record Published	DNS Record found	

Your email service provider is "Mimecast" [Need Bulk Email Provider Data?](#)

Figure 2: MXToolbox data

In the world of online security, not having a DMARC record for [REDACTED] leaves it wide open to sneaky email threats. Imagine if someone could easily pretend to be from [REDACTED] and send emails asking for sensitive info or try to trick people into doing something risky. That's the risk of phishing and spoofing attacks without DMARC. It's like leaving the front door wide open for hackers to stroll in and wreak havoc.

And it's not just about keeping the bad guys out. Without DMARC, [REDACTED] can't even see if someone's trying to break in. You know, like not having security cameras to see who's knocking at your door. So, it's tough for them to spot those sneaky email impostors or even know if their emails are getting flagged as spam. Plus, it could hurt their reputation – nobody wants to be known as the domain that's always getting impersonated. So, getting DMARC set up and running smoothly is like putting up sturdy locks and installing security cameras to keep [REDACTED] safe from online intruders.

## Network Analysis:

### Nessus:



Figure 3: Nessus tool


After scanning the website in Nessus tool we delve into the SYN "Half-open" port scanner plugin, to assess the security of network ports on target systems. Unlike full connection scans, which can

be intrusive, this plugin employs SYN scanning techniques, offering a less disruptive approach to evaluating port status. It provides valuable insights into potential vulnerabilities while minimizing the risk of service disruption, making it a preferred choice for assessing network security.

**Understanding the Risks and Recommendations:** While SYN scans offer advantages such as reduced intrusion, they are not without their challenges. Less robust firewalls may struggle to handle SYN packet traffic, potentially allowing scans to bypass security measures. Additionally, there's a risk of leaving unclosed connections on target systems, particularly under heavy network loads. To mitigate these risks, it's crucial to fine-tune firewall configurations and implement measures to limit network overload. By monitoring for unusual network activity and promptly addressing unclosed connections, organizations can enhance their network security posture and minimize the impact of SYN scanning activities.

## **Website Infrastructure and Security:**

██████████ Drupal 9 CMS for its website, leveraging its robust features and functionality to enhance user experience and content management. However, it's important to acknowledge that like any software platform, Drupal 9 is not immune to vulnerabilities. Being an open-source content management system, Drupal is susceptible to potential security risks, including vulnerabilities in core code, plugins, or third-party integrations. These vulnerabilities can range from SQL injection and cross-site scripting to authentication bypass and remote code execution. It's imperative for ██████████ to remain vigilant in applying security patches and updates promptly to mitigate the risk of exploitation. Additionally, implementing best practices in web security, such as regular security audits, user access controls, and network monitoring, can further fortify the website against potential threats. By staying proactive and informed about Drupal's security landscape, ██████████ can maintain the integrity and security of its online presence effectively.



<a href="#">CVE-2020-13671</a>	Drupal core does not properly sanitize certain filenames on uploaded files, which can lead to files being interpreted as the incorrect extension and served as the wrong MIME type or executed as PHP for certain hosting configurations. This issue affects: Drupal Core 9.0 versions prior to 9.0.8, 8.9 versions prior to 8.9.9, 8.8 versions prior to 8.8.11, and 7 versions prior to 7.74.
<a href="#">CVE-2020-13670</a>	Information Disclosure vulnerability in file module of Drupal Core allows an attacker to gain access to the file metadata of a permanent private file that they do not have access to by guessing the ID of the file. This issue affects: Drupal Core 8.8.x versions prior to 8.8.10; 8.9.x versions prior to 8.9.6; 9.0.x versions prior to 9.0.6.
<a href="#">CVE-2020-13669</a>	Cross-site Scripting (XSS) vulnerability in ckeditor of Drupal Core allows attacker to inject XSS. This issue affects: Drupal Core 8.8.x versions prior to 8.8.10; 8.9.x versions prior to 8.9.6; 9.0.x versions prior to 9.0.6.
<a href="#">CVE-2020-13668</a>	Access Bypass vulnerability in Drupal Core allows for an attacker to leverage the way that HTML is rendered for affected forms in order to exploit the vulnerability. This issue affects: Drupal Core 8.8.x versions prior to 8.8.10; 8.9.x versions prior to 8.9.6; 9.0.x versions prior to 9.0.6.
<a href="#">CVE-2020-13667</a>	Access bypass vulnerability in of Drupal Core Workspaces allows an attacker to access data without correct permissions. The Workspaces module doesn't sufficiently check access permissions when switching workspaces, leading to an access bypass vulnerability. An attacker might be able to see content before the site owner intends people to see the content. This vulnerability is mitigated by the fact that sites are only vulnerable if they have installed the experimental Workspaces module. This issue affects Drupal Core 8.8.x versions prior to 8.8.10; 8.9.x versions prior to 8.9.6; 9.0.x versions prior to 9.0.6.

*Figure 5: Vulnerabilities for Drupal 9*

From Figure 2, we observe the vulnerability that can be used against Drupal 9.

1. **Information Disclosure Vulnerability in File Module:** This vulnerability in the file module of Drupal Core enables attackers to access metadata of permanent private files by guessing the file ID. Unauthorized access to sensitive file metadata poses a risk of data exposure.
2. **Access Bypass Vulnerability in Workspaces Module:** The Workspaces module in Drupal Core is susceptible to an access bypass vulnerability, allowing attackers to access data without proper permissions. This vulnerability arises from insufficient access permission checks when switching workspaces, potentially granting unauthorized access to content before it's intended to be made public.

Given that the organization utilizes Drupal 9 CMS for its website, it is advisable to construct the website using PHP 7.4. This alignment ensures compatibility and optimization, enhancing the website's performance and security. By employing PHP 7.4 alongside Drupal 9, we can effectively address vulnerabilities inherent to both platforms, mitigating the risk of potential security breaches and safeguarding the integrity of the website against malicious attacks.



2010-03-25	📄	✓	SiteX CMS 0.7.4 Beta - 'photo.php' SQL Injection	WebApps	PHP	So0rpi0n
2008-09-12	📄	✓	WebPortal CMS 0.7.4 - 'download.php' SQL Injection	WebApps	PHP	StAkeR
2006-03-30	📄	✓	Claroline 1.7.4 - 'scormExport.inc.php' Remote Code Execution	WebApps	PHP	rgod
2005-02-09	📄	✓	PHP-Nuke 7.4 - Admin	WebApps	PHP	Silentium
2004-09-08	📄	✓	PHP-Nuke 7.4 - Privilege Escalation	WebApps	PHP	mantra

Figure 6: code to exploit php 7.4 from Exploit-db

<a href="#">CVE-2023-46726</a>	GLPI is a free asset and IT management software package. Starting in version 10.0.0 and prior to version 10.0.11, on PHP 7.4 only, the LDAP server configuration form can be used to execute arbitrary code previously uploaded as a GLPI document. Version 10.0.11 contains a patch for the issue.
<a href="#">CVE-2020-6144</a>	A remote code execution vulnerability exists in the install functionality of OS4Ed openSIS 7.4. The username variable which is set at line 121 in install/Step5.php allows for injection of PHP code into the Data.php file that it writes. An attacker can send an HTTP request to trigger this vulnerability.
<a href="#">CVE-2020-6143</a>	A remote code execution vulnerability exists in the install functionality of OS4Ed openSIS 7.4. The password variable which is set at line 122 in install/Step5.php allows for injection of PHP code into the Data.php file that it writes. An attacker can send an HTTP request to trigger this vulnerability.
<a href="#">CVE-2019-16124</a>	In YouPHPTube 7.4, the file install/checkConfiguration.php has no access control, which leads to everyone being able to edit the configuration file, and insert malicious PHP code.

Figure 7: Vulnerabilities from CVE for php 7.4

From Figure 3, PHP-Nuke 7.4 Admin, this vulnerability in PHP allows an attacker to exploit a web portal by creating a new administrative account with a password specified through parameters in the exploit. Upon successful exploitation, the attacker gains full administrative control over the web portal. This unauthorized administrative access poses a significant security risk, potentially leading to data breaches, unauthorized modifications to website content, and other malicious activities. It underscores the importance of implementing robust security measures, such as regularly updating PHP versions, applying security patches promptly, and implementing strong access controls, to mitigate the risk of such exploits and protect web portals from unauthorized access and manipulation.

## Whatweb:

```
(kali@kali)-[~]
$ whatweb -a 3 [redacted]
http://[redacted] [301 Moved Permanently] Country[RESERVED][22], HTTPServer[Pantheon], IP[redacted], RedirectLocation[https://[redacted]], UncommonHeaders[retry-after,x-pantheon-redirect,x-served-by,x-cache-hits,x-timer], Via-Proxy[1.1 varnish]
https://[redacted] [200 OK] Content-Language[en], Country[RESERVED][22], Drupal, Frame, HTML5, HTTPServer[nginx], IP[redacted], MetaGenerator[Drupal 9 (https://www.drupal.org)], Open-Graph-Protocol, Script[application/json], Strict-Transport-Security[max-age=300], Title[redacted], UncommonHeaders[x-content-type-options,x-drupal-cache,x-drupal-dynamic-cache,x-generator,x-pantheon-styx-hostname,x-styx-req-id,x-served-by,x-cache-hits,x-timer], Via-Proxy[1.1 varnish, 1.1 varnish], X-Frame-Options[SAMEORIGIN], X-UA-Compatible[IE=edge], nginx
```

Figure 8: Analysis of the [redacted] through whatweb tool

1. Website Fingerprinting: WhatWeb employs advanced techniques to analyze the structure and components of a website, effectively creating a unique fingerprint that can be used for identification.

2. **Technology Identification:** By analyzing various aspects of a website's infrastructure, such as server headers, HTML code, and response patterns, WhatWeb can accurately determine the technologies and software used in its development.
3. **Comprehensive Analysis:** WhatWeb provides a comprehensive analysis of a website's technology stack, including details about the server software (e.g., Apache, Nginx), CMS platforms (e.g., WordPress, Joomla), programming languages (e.g., PHP, Python), and frameworks (e.g., Laravel, Ruby on Rails) employed.

2014-06-10	📄	✓	WordPress Plugin JW Player for Flash & HTML5 Video - Cross-Site Request Forgery	WebApps	PHP	Tom Adams
2015-06-12	📄	✓	WordPress Plugin SE HTML5 Album Audio Player 1.1.0 - Directory Traversal	WebApps	PHP	Larry W. Cashdollar
2012-06-05	📄	✓	WordPress Plugin HTML5 AV Manager 0.2.7 - Arbitrary File Upload	WebApps	PHP	Sammy FORGIT

*Figure 9: exploits for HTML5 from exploithub*

2013-11-19	📄	✓	Nginx 1.1.17 - URI Processing SecURity Bypass	Remote	Multiple	Ivan Fratric
2010-01-11	📄	✓	Nginx 0.7.64 - Terminal Escape Sequence in Logs Command Injection	Remote	Multiple	evilaliv3

*Figure 10: exploits for nginx from exploithub*

## Web Application Firewalls (WAFs):



*Figure 11: Analysis of the web application to check for the firewall vulnerability*

A Web Application Firewall (WAF) serves as a critical component of modern cybersecurity infrastructure, designed to protect web applications from a variety of cyber threats. However, reliance solely on a WAF, particularly with default configurations, may present significant security risks for organizations.

**Red Flag:** Relying solely on a WAF as the primary defense mechanism against cyber threats can be considered a red flag in cybersecurity practices. While WAFs are effective tools for filtering and blocking incoming web traffic, they should not be viewed as a comprehensive solution to all security challenges. Depending solely on a WAF may create a false sense of security, leaving critical vulnerabilities unaddressed.

Unauthorized disclosure of sensitive data, privileges or other information.  
[CVE-2023-45132](#) NAXSI is an open-source maintenance web application firewall (WAF) for NGINX. An issue present starting in version 1.3 and prior to version 1.6 allows someone to bypass the WAF when a malicious 'X-Forwarded-For' IP matches 'IgnoreIP' 'IgnoreCIDR' rules. This old code was arranged to allow older NGINX versions to also support 'IgnoreIP' 'IgnoreCIDR' when multiple reverse proxies were present. The issue is patched in version 1.6. As a workaround, do not set any 'IgnoreIP' 'IgnoreCIDR' for older versions.

*Figure 12: Exploits for firewall vulnerability from exploitdb*

## OSINT of Employees:

### 1. [REDACTED]

[REDACTED] we've uncovered a nuanced profile enriched with diverse interests and potential affiliations. [REDACTED] educational background includes studies at [REDACTED], indicating a commitment to academic pursuits. Her online presence reveals a multifaceted individual with a keen interest in fashion, as evidenced by her engagement with Fashion Week content on Twitter. Additionally, her passion for boxing and admiration for Cole Sprouse further diversified her interests. Notably, her VSCO account suggests close friendships, possibly including a romantic relationship.

However, it's essential to note [REDACTED] affiliation with Satanism on Facebook, which may indicate alternative spiritual beliefs or a statement of individuality. Furthermore, additional information about [REDACTED] potential residence is the address located at [REDACTED]  
[REDACTED]



2. [REDACTED]

I've meticulously pieced together a detailed profile of [REDACTED], also known as [REDACTED]. Initially, the search began with limited information, primarily sourced from his LinkedIn profile. However, a breakthrough came when employing Yandex image search using [REDACTED] LinkedIn profile picture, leading to the identification of his wife, [REDACTED]. Their recent marriage in February 2024 was evident from their shared Facebook profile picture. Furthermore, it was noted that [REDACTED] prefers using his middle name on Facebook, possibly indicative of a desire for privacy or professional identity. His educational background includes graduation from a military school, specifically from [REDACTED] and he boasts a distinguished career as a veteran of the United States Marine Corps (USMC), complemented by various security certifications. Notably, [REDACTED] demonstrates entrepreneurial acumen by overseeing [REDACTED], headquartered in Albany. Additionally, exhaustive details regarding the circumstances of his and his wife's meeting were uncovered, providing valuable insights into his personal life and relationships.

3. [REDACTED]

[REDACTED], we've pieced together a detailed profile unveiling both his professional expertise and personal life. Initially identified on LinkedIn as a graduate of [REDACTED] with a bachelor's degree in electrical engineering, [REDACTED] professional prowess is evident. Further insights into his personal life emerged as we discovered he is married to [REDACTED] and they have a daughter, residing at [REDACTED]. Our search on Facebook yielded a profile picture featuring [REDACTED] with his wife and daughter, although [REDACTED] was untagged. Utilizing Yandex image search to gather more information about his wife proved fruitless. However, employing a people finder service provided crucial details, revealing his wife's full name as [REDACTED] and indicating they are a long-time couple who tied the knot in 2019. His interests were tagged on Facebook supporting for the New York Yankees, reflecting his passion for sports, and an affinity for boats, suggesting recreational pursuits.

This amalgamation of professional expertise, familial ties, and recreational interests presents a nuanced understanding of [REDACTED], encapsulating both his professional prowess and personal inclinations.

#### 4. [REDACTED]

Joining the company in 2017, the individual exhibits a limited presence on mainstream social media platforms, with no active Instagram or Facebook accounts. However, their email address has been implicated in multiple breaches, according to the "haveibeenpwned" website, exposing sensitive information such as credit card details and residence address. Further investigation reveals additional personal information, including the individual's wife's name and email address, obtained through people finder services. Moreover, it was discovered that the individual's spouse is an investor in Scoutandcellar wine, a Texas-based wine company, hinting at their personal interests and financial engagements beyond their professional role. This comprehensive analysis underscores the importance of implementing robust cybersecurity measures to mitigate the risks posed by data breaches and safeguard personal privacy in both professional and personal domains.

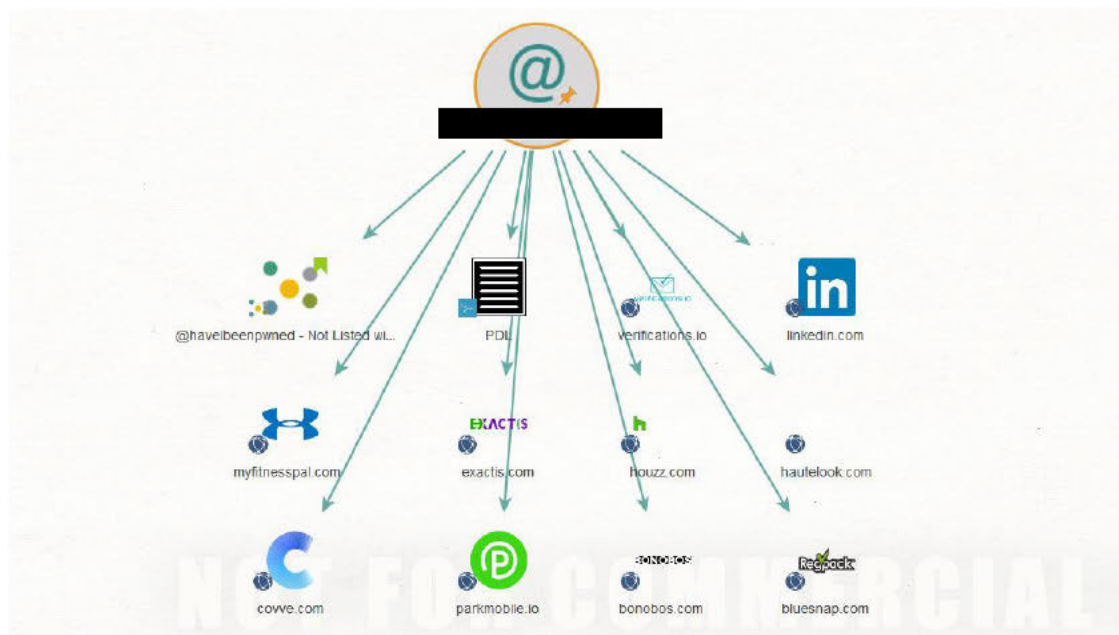


Figure 13: email breach shown from Maltego

## Conclusion:

In wrapping up, our deep dive into ██████████ has given us a rich tapestry of insights. We've explored its storied past, its diverse portfolio, and the intricate web of its online presence. Over the years, ██████████ not only shaped transportation and infrastructure but has also become a vital part of communities nationwide. Yet, as we've uncovered, there are vulnerabilities lurking in its digital footprint.

Beyond the corporate facade, our investigations into key employees have revealed real people with real lives, interests, and connections. From ██████████ eclectic tastes to ██████████ entrepreneurial spirit, and ██████████ blend of family and sports passions, each individual brings a unique story to the table. But with this personal insight comes the reminder of the importance of safeguarding their privacy and security.

As we chart the course ahead, it's clear that ██████████ must navigate the digital realm with caution. By shoring up its online defenses, leveraging advanced tools, and fostering a culture of cybersecurity awareness, ██████████ can not only protect its digital assets but also honor the trust of its employees and clients. In the ever-evolving landscape of cyber threats, staying one step ahead is not just a necessity but a responsibility—one that ██████████ is well-equipped to embrace.

## References:

- <https://www.linkedin.com>
- <https://www.instagram.com>
- <https://www.facebook.com>
- <https://www.twitter.com>
- <https://www.peoplefinders.com>
- <https://www.rocketreach.com>
- 

## Tools:

- Exploitdb
- MXToolbox

- **Maltego**
- **Whatweb**
- **Wafoof**
- **Haveibeenpawnd**
- **Yandex**
- **Nessus**
- **whois**