



# **Threat Intelligence Report**

**TEAM 4  
CYBLACK  
INTERNSHIP  
29TH JANUARY, 2025**

## Table of Contents

Executive Summary.....	4
Company Profile.....	6
Threat Profile.....	8
<b>2.1 Cybersecurity Threats .....</b>	<b>8</b>
<b>2.2 Insider Threats .....</b>	<b>9</b>
<b>2.3 Physical Security Threats.....</b>	<b>9</b>
<b>2.4 Reputational Threats .....</b>	<b>9</b>
Threat Intelligence .....	11
<b>3.1 Threat intelligence tools for information gathering.....</b>	<b>13</b>
<b>3.2 Professional Organisations/Advisory Groups .....</b>	<b>16</b>
Information Gathering.....	19
<b>4.1 Cyberbulwark 2021 Breach.....</b>	<b>19</b>
Risk Assessment Exercise for Cyberbulwark.....	21
<b>5.2 Approach .....</b>	<b>25</b>
Vulnerability Research.....	37
<b>6.1 Current Relevant Vulnerabilities .....</b>	<b>37</b>
<b>6.2 Latest Zero-Day Vulnerabilities .....</b>	<b>38</b>
<b>6.3 Threat Actors Exploiting Vulnerabilities.....</b>	<b>38</b>
<b>6.4 Top Five Threat Actors Against CyberBulwark.....</b>	<b>39</b>
<b>6.5 Recent Incidents and Relevance to CyberBulwark .....</b>	<b>44</b>
Overview of Number 1 Threat Actor .....	46
<b>7.1 Relevant Companies Impacted by Lazarus Group .....</b>	<b>49</b>
<b>7.3 Tactics, Techniques, and Procedures (TTPs).....</b>	<b>50</b>
<b>7.4 Mitigating Lazarus group's Attacks .....</b>	<b>53</b>
Conclusion .....	55
References .....	56

Glossary of Terms.....	58
APPENDICES.....	61
Appendix A: Members contribution to the exercise .....	61
Appendix B: Attendance.....	62

CyberBulwark

## **Executive Summary**

This Cyber Threat Intelligence (CTI) report provides a comprehensive analysis of the evolving threat landscape impacting CyberBulwark, a global leader in consulting and technology services. Given CyberBulwark's extensive role in managing sensitive client data across various industries, it has become a prime target for cybercriminals. The report highlights critical threats, including ransomware attacks, phishing campaigns, and targeted data breaches. Threat actors are increasingly leveraging advanced social engineering techniques and exploiting vulnerabilities in cloud infrastructure, remote access tools, and supply chains to infiltrate systems and compromise security.

A thorough risk assessment conducted in this report underscores several key vulnerabilities in CyberBulwark's cybersecurity posture. Publicly available employee and project data present significant risks, as cybercriminals can exploit this information for phishing and social engineering attacks. Additionally, vulnerabilities within CyberBulwark's digital infrastructure could be exploited for unauthorized access, putting both internal and client-facing systems at risk. Past security incidents, such as the 2021 LockBit ransomware attack, demonstrate the urgency of implementing stronger security measures to prevent future breaches.

The report also examines the Lazarus Group, a state-sponsored cybercriminal organization identified as the most significant threat to CyberBulwark. Lazarus Group is notorious for cyber espionage, financial theft, and disruptive attacks targeting large corporations and government entities. The analysis includes key Indicators of Compromise (IoCs) observed within CyberBulwark's threat environment and evaluates recent vulnerabilities that could further expose the company to cyber threats.

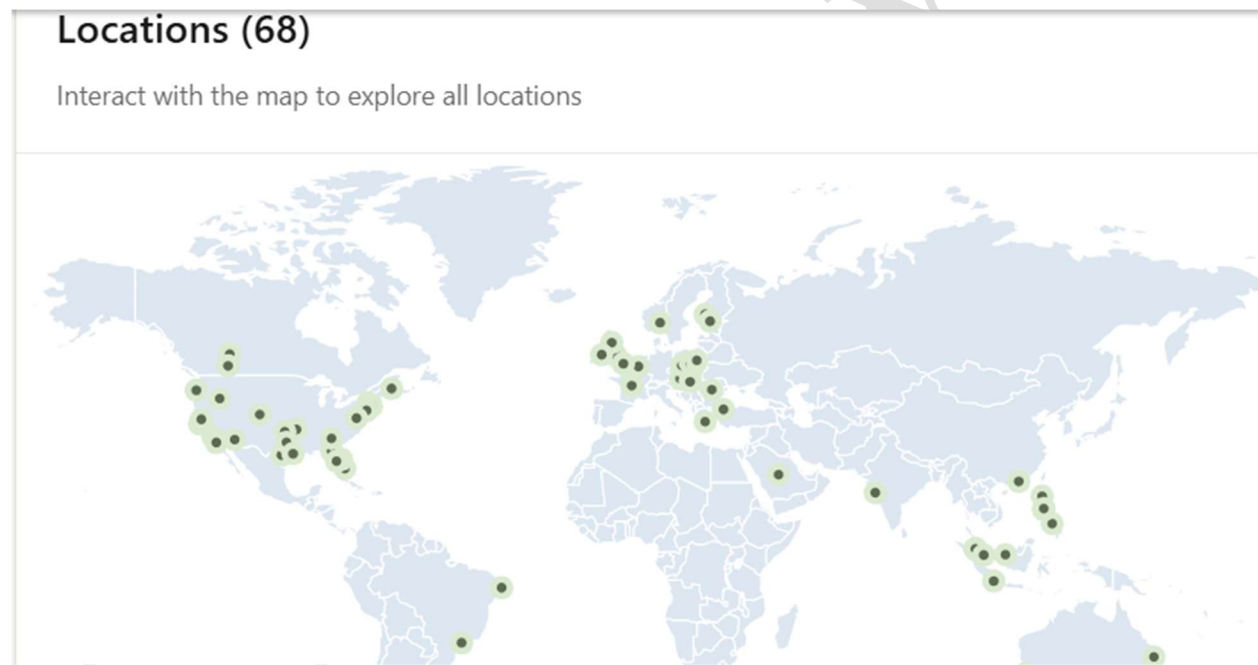
To mitigate these risks, the report recommends several critical security enhancements. Strengthening phishing awareness training and conducting regular cybersecurity education for employees will help prevent social engineering attacks. Additionally, implementing multi-factor authentication (MFA) and robust access control policies can significantly reduce the risk of unauthorized access. The adoption of a Zero Trust security model will limit lateral movement within the network, making it harder for attackers to gain persistent access. Furthermore, proactive threat intelligence and dark web monitoring will enable early detection of potential cyber threats. Regular patch management and vulnerability assessments are also essential to addressing security gaps before they can be exploited by malicious actors.

By adopting these measures, CyberBulwark can strengthen its cybersecurity defenses, safeguard client data, and maintain operational resilience in the face of emerging cyber threats.

## Company Profile

Cyberbulwark is a leading global professional services company that helps the world's leading businesses, governments and other organizations build their digital core, optimize their operations, accelerate revenue growth and enhance citizen services creating tangible value at speed and scale.

Cyberbulwark is a talent and innovation-led company serving clients in more than 120 countries. It combines strength in technology and leadership in cloud, data and AI with unmatched industry experience, functional expertise and global delivery capability.



*Figure 1.0: Geographic map showing locations of Cyberbulwark offices globally*

**Website address:** <http://www.Cyberbulwark.com>

**Employees:** Over 774,000

**Social media handles:**

LinkedIn: <https://www.linkedin.com/company/Cyberbulwark/about/>

X: [https://x.com/Cyberbulwark\\_US](https://x.com/Cyberbulwark_US)

CyberBulwark

## **Threat Profile**

CyberBulwark, a global consulting and technology services leader, faces an evolving and complex threat landscape. As a high-profile firm managing sensitive client data, proprietary business intelligence, and critical IT infrastructures across multiple industries, CyberBulwark is an attractive target for cybercriminals, nation-state actors, and insider threats. This report identifies key risks that could impact CyberBulwark's operations, security, and reputation.

### **2.1 Cybersecurity Threats**

CyberBulwark's vast digital footprint makes it a high-value target for cyberattacks. The company has previously been targeted by ransomware groups, most notably the LockBit attack in 2021, where attackers claimed to have exfiltrated over 6 terabytes of data and demanded a \$50 million ransom. Such incidents highlight the ongoing risk posed by ransomware, phishing campaigns, and data breaches.

Threat actors, including Advanced Persistent Threats (APTs) such as Lazarus Group, pose a significant risk to CyberBulwark. These groups employ sophisticated techniques to conduct long-term espionage, financial theft, and sabotage. Their attacks often exploit zero-day vulnerabilities and weaknesses in cloud infrastructure and remote access tools. Additionally, the company must remain vigilant against supply chain attacks, where cybercriminals infiltrate third-party vendors to gain access to CyberBulwark's systems and client networks.

Another major concern is social engineering and credential theft. Publicly available employee information, including names, roles, and contact details, increases the risk of spear-phishing attacks aimed at stealing login credentials or deploying malware. The presence of



CyberBulwark employee data on platforms such as "Have I Been Pwned" further exposes the company to account compromise risks.

## **2.2 Insider Threats**

With over 774,000 employees worldwide, CyberBulwark faces the risk of insider threats, including disgruntled employees who might steal sensitive data, sabotage internal systems, or leak proprietary information. Additionally, industrial espionage is a concern, as competitors or nation-state actors may attempt to recruit insiders to gain unauthorized access to confidential client data, intellectual property, or strategic initiatives.

## **2.3 Physical Security Threats**

Corporate espionage remains a threat, with attackers attempting to gain unauthorized physical access to CyberBulwark's offices, data centers, or partner facilities to plant malware, conduct surveillance, or steal assets. The company's vast infrastructure also makes it vulnerable to hardware-based attacks, where compromised devices are introduced into its network.

## **2.4 Reputational Threats**

A major data breach could have severe financial and reputational consequences for CyberBulwark, leading to client distrust, regulatory fines, and operational disruptions. Failure to comply with global cybersecurity regulations such as ISO 27001, GDPR, and NIST standards could result in legal action and significant financial penalties. Additionally, CyberBulwark's role

in high-profile IT projects means that service disruptions caused by cyber incidents could erode customer confidence and damage its standing as a trusted consulting partner.

CyberBulwark operates in a rapidly evolving threat landscape, facing challenges from sophisticated cyber threats, insider risks, supply chain vulnerabilities, and reputational risks. To strengthen its security posture, CyberBulwark must prioritize: enhanced phishing awareness training and continuous employee cybersecurity education. Strengthening multi-factor authentication (MFA) and implementing zero-trust security models will help limit lateral movement within networks. Proactive threat intelligence and dark web monitoring are essential for early threat detection, while regular patch management and vulnerability assessments will help mitigate security gaps. Furthermore, stronger supply chain security measures will reduce third-party risks.

## Threat Intelligence

Cyber threat intelligence is a critical component in defending against modern cyber threats, providing organizations with the necessary information to identify, analyze, and mitigate potential risks. The six major sources of cyber threat intelligence are;

Six major sources of cyber threat intelligence include:

- 1. Open source intelligence (OSINT):** Open-source threat intelligence platforms leverage threat intelligence data gathered from publicly available open sources. Because no single team can keep up with the steady influx of data surrounding modern cyber dangers, security forums and dedicated national and international security lists allow professionals and volunteers to pool their knowledge. Open-source threat feeds are automatically updated with new information. Businesses can stay informed about new cybersecurity developments by subscribing to reliable feeds.
- 2. Dark web monitoring:** Finding and tracking information about your company on the dark web is known as "dark web monitoring." Tools for monitoring the dark web are comparable to those for monitoring the main search engines. They draw in raw intelligence in real time and search the dark web continuously. Sites are monitored for specific information, such as business email addresses, or general information, such as the firm name and industry, rather than trying to investigate every bit of material on the dark web.
- 3. Vulnerability data:** Vulnerability data refers to information about security weaknesses or flaws in software, hardware, or network systems that attackers can exploit. This data is a critical component of cyber threat intelligence, helping organizations proactively identify and address potential risks before they are exploited by threat actors. Information about vulnerabilities help organizations prioritize patch management.

- 4. Forensically acquired data:** Forensically acquired data refers to digital evidence gathered from compromised systems, networks, or devices during cyber incident investigations. This data includes malware samples, system logs, memory dumps, and file artifacts. It serves as a crucial cyber threat intelligence source, enabling analysts to identify attack vectors, understand adversary tactics, and attribute incidents to specific threat actors. By studying this data, organizations can enhance defenses, develop countermeasures, and prevent future attacks.
- 5. Internet traffic data:** Internet traffic data provides valuable insights into cyberthreat activities by analyzing patterns, anomalies, and communication flows across networks. It helps detect malicious behavior, such as Command-and-Control (C2) traffic, Distributed Denial-of-Service (DDoS) attacks, and phishing campaigns. By monitoring and analyzing traffic metadata, threat actors' techniques, tactics, and procedures (TTPs) can be identified, aiding in threat detection and prevention. Tools like packet analyzers (e.g., Wireshark) and network monitoring systems are commonly used for this purpose.
- 6. Vendor and Security Research Reports:** Vendor and security research reports are key sources of cyber threat intelligence, providing insights into emerging threats, vulnerabilities, and attacker tactics. Published by cybersecurity firms and researchers, these reports compile data from real-world incidents, honeypots, and threat analysis. They often include Indicators of Compromise (IoCs), mitigation strategies, and threat actor profiles. Such reports help organizations stay informed about the latest attack trends and improve defenses. Examples include reports from companies like Kaspersky, FireEye, and CrowdStrike, as well as open-source publications like Verizon's Data Breach Investigations Report (DBIR).

### 3.1 Threat intelligence tools for information gathering

Threat intelligence tools are vital for collecting, analyzing, and sharing data about potential threats and vulnerabilities. Threat intelligence and threat modeling tools have become increasingly important in recent years as the cybersecurity landscape has become more complex and sophisticated. There are several types of threat modeling tools available, each with its unique features and benefits. Here are some commonly used tools for information gathering:

#### 1. Open-Source Intelligence (OSINT) Tools

- **Maltego:** For mapping relationships between people, companies, domains, and other entities.
- **Shodan:** To gather information about internet-connected devices, including exposed services and vulnerabilities.
- **SpiderFoot:** An automation tool that collects OSINT data from over 100 sources.
- **theHarvester:** A tool for email, domain, and subdomain enumeration from public sources.
- **Recon-ng:** A reconnaissance framework with various modules for OSINT data collection.
- **Google Alerts:** Monitors the web for specific keywords and sends alerts when new content is found.

#### 2. Threat Intelligence Platforms (TIPs)

- **Recorded Future:** Provides real-time threat intelligence and risk analysis.
- **Anomali ThreatStream:** Aggregates threat data from multiple sources and correlates it with internal threat data.

- **MISP (Malware Information Sharing Platform):** An open-source tool for sharing, storing, and correlating indicators of compromise (IoCs).
- **AlienVault Open Threat Exchange (OTX):** A collaborative platform for sharing and accessing threat intelligence data.
- **Cisco Talos Intelligence:** Provides detailed threat analysis and intelligence feeds.

### **3. Network Analysis and Monitoring Tools**

- **Wireshark:** A packet analyzer for inspecting network traffic in detail.
- **Zeek (formerly Bro):** A network monitoring tool that provides detailed logs of network activity.

### **4. Vulnerability Scanning and Enumeration Tools**

- **Nessus:** For vulnerability assessment and compliance checks.
- **OpenVAS:** An open-source vulnerability scanning and management tool.
- **Qualys:** A cloud-based vulnerability management platform.

### **5. Dark Web Monitoring Tools**

- **IntSights:** For gathering intelligence from dark web forums, marketplaces, and other hidden sources.
- **DarkOwl:** Provides dark web intelligence and monitoring solutions.

### **6. Domain and Email Intelligence**

- **DNSDumpster:** For domain information and mapping DNS servers.
- **MXToolBox:** For analyzing email headers, DNS records, and blacklists.

- **FOCA:** A metadata analysis tool that extracts data from publicly available documents.
- **The Spamhaus Project:** Provides DNS-based blacklists (DNSBLs) for email and domain protection, focusing on identifying spam sources.

## **7. Social Media Intelligence (SOCMINT) Tools**

- **Social-Searcher:** For monitoring mentions and posts across social media.
- **Twint:** A Twitter intelligence tool for gathering public data without API access.

## **8. Threat Feed Aggregators**

- **AlienVault OTX (Open Threat Exchange):** A platform to share and access threat indicators.
- **CIRCL Passive DNS:** For historical DNS lookup data.
- **Department of Homeland Security (DHS), CISA Automated Indicator Sharing (AIS):** Shares cyber threat indicators across organizations to facilitate collaboration.
- **FBI: InfraGard:** A partnership for sharing threat intelligence between the FBI and private sectors.
- **SANS: Internet Storm Center:** Provides real-time threat feeds and analysis to help identify global internet threats.

## **9. Custom Scripts and APIs**

- Use Python or tools like **BeautifulSoup** and **Selenium** for web scraping.
- APIs like VirusTotal or Hybrid Analysis for file and URL analysis.

## 3.2 Professional Organisations/Advisory Groups

Cybersecurity advisory groups are collections of experts in cybersecurity who come together to provide guidance, analysis, and recommendations on cybersecurity risks and best practices to organizations, often including government agencies, businesses, and critical infrastructure providers. These groups help multiple entities improve their security postures and mitigate potential threats by sharing insights and strategies for managing evolving cyber risks. Some of them are;

### 1. Cyber Threat Alliance (CTA)

- **Purpose:** A collaborative platform for cybersecurity vendors and organizations to share and improve threat intelligence.
- **Why it's relevant for Cyberbulwark:** As a leading global cybersecurity service provider, Cyberbulwark can contribute to and benefit from actionable intelligence shared by major industry players.
- **Benefits:**
  - Access to detailed threat intelligence reports.
  - Collaboration with other global cybersecurity leaders.
  - Improved client services through shared insights.

### 2. Information Sharing and Analysis Centers (ISACs)

- **Purpose:** Sector-specific threat intelligence sharing networks.
- **Why it's relevant for Cyberbulwark:** Cyberbulwark works across industries like finance, healthcare, and energy, making ISACs a critical resource.



- **Relevant ISACs for Cyberbulwark:**
  - **FS-ISAC** (Financial Services).
  - **H-ISAC** (Healthcare).
  - **IT-ISAC** (Information Technology).
- **Benefits:**
  - Industry-specific threat intelligence.
  - Access to incident response best practices and collaboration forums.

### **3. Forum of Incident Response and Security Teams (FIRST)**

- **Purpose:** A global organization promoting cooperation and collaboration between incident response teams.
- **Why it's relevant for Cyberbulwark:** FIRST's global reach aligns with Cyberbulwark's multinational operations, providing insights into emerging threats across regions.
- **Benefits:**
  - Access to training and technical knowledge.
  - Early threat detection through global collaboration.
  - Improved incident response capabilities.

### **4. MITRE Engenuity Center for Threat-Informed Defense**

- **Purpose:** Collaborative R&D for advancing the art and science of cyber defense.
- **Why it's relevant for Cyberbulwark:** Cyberbulwark's focus on innovation and technology makes MITRE an ideal partner to align with its cyber threat intelligence efforts.
- **Benefits:**
  - Access to frameworks like ATT&CK.

- Participation in cutting-edge R&D projects.
- Development of advanced threat-informed defense strategies.

## **5. Global Forum on Cyber Expertise (GFCE)**

- **Purpose:** An international platform for collaboration on cybersecurity capacity building.
- **Why it's relevant for Cyberbulwark:** Cyberbulwark's global presence and leadership in cybersecurity position it as both a contributor and beneficiary of GFCE initiatives.
- **Benefits:**
  - Opportunities to collaborate with governments and private sector leaders.
  - Insights into global cybersecurity trends and policies.
  - Contribution to capacity-building initiatives worldwide.

## **Information Gathering**

Cyberbulwark has an active presence across several social media platforms, including Instagram, LinkedIn, Twitter and Facebook. On LinkedIn, they share their professional updates, primarily company news, and recruitment opportunities. They regularly share company milestones, cybersecurity enlightenments and technological evolution. On Twitter, Cyberbulwark segregated their accounts by region where they mainly discuss technological advancements, benefits of purchasing their company stock, sharing news and client success stories. On Facebook, Cyberbulwark spotlights their staff where they speak about technological innovations as well, they also highlight the company culture and history.

All of this information can;

1. Provide attackers with details about Cyberbulwark's operations, focus areas and projects.
2. Employee posts particularly on LinkedIn might disclose sensitive information about internal tools used for ongoing projects.
3. The profiles of the employees can be targeted for phishing and spear-phishing attempts. The public disposal of the tools used to carry out specific projects can be leveraged on by attackers to further create believable phishing attempts.
4. Employers or Stakeholders might /can share sensitive information such as photos, ID's or documents which can be exploited.

### **4.1 Cyberbulwark 2021 Breach**

On Aug 11, 2021, Cyberbulwark became the latest victim of LockBit 2.0 Ransomware. The attackers claimed to have accessed a significant amount of data and demanded a ransom, which Cyberbulwark did not pay. The attackers then published some files allegedly taken during the incident. Cyberbulwark confirmed that some information was compromised but did not specify the details. The breach impacted data related to approximately 33,000 individuals.

The data exposed in the breach included proprietary information, as well as emails, names, and broadcast dates of current and former employees. The LockBit ransomware operators breached Cyberbulwark's systems, stealing over 6 terabytes of data and demanding a \$50 million ransom. Cyberbulwark quickly contained the incident, restoring affected systems from backups. The specific methods used by the hackers and the exact nature of the stolen data remain unclear.

## Risk Assessment Exercise for Cyberbulwark

This risk assessment exercise helped identify, analyze, and mitigate potential risks to Cyberbulwark's operations, assets, and reputation.

The scope of this vulnerability assessment related to the state of the Cyberbulwark website. The assessment covered a period of 24 hours, with NIST SP 800-30 Rev. 1 used to guide the risk analysis of the information system.

The Cyberbulwark website was used for a variety of purposes, including: communicating with employees, providing consulting services, sharing information about the company, promoting environmental, social, and governance goals, and sharing information about emerging technologies. Securing the website was critical due to its regular use for marketing operations and other activities.

**Table 1: Cyberbulwark Artifacts**

Artifacts	Vulnerabilities	Threats	Risk
<b>Email</b>	Staff use a firstname.lastname naming convention for their emails	Attackers can use this pattern to craft phishing emails targeting employees.	High
<b>Projects</b>	Public posts about partnerships and client engagements.	Social engineering attacks leveraging publicly available project details.	High

<b>Photos and Videos</b>	Sensitive information such as employee IDs visible in media	Hackers can exploit this to create fake IDs, impersonate employees, or conduct targeted attacks	Medium
<b>Key Personnel</b>	Public profiles and posts about senior executives.	Attackers can conduct spear-phishing, impersonation attacks, or create fake accounts to target employees or stakeholders.	High
<b>Publicly Accessible Documents</b>	PDF files available online after Google dorking (e.g., reports, surveys).	Documents contain metadata or strategic information that attackers can exploit to plan attacks or create convincing phishing campaigns.	Medium
<b>Employee Records</b>	Employee records are accessible through tools like RocketReach.	Attackers can extract employee contact information to conduct phishing campaigns or gather intelligence for social engineering.	High
<b>SSL Certificate</b>	Certificate provided by DigiCert	The information of the SSL certificate provider online, the third party supply chain may be attacked.	

<b>Transfer Protocol</b>	The website redirects traffic to an HTTPS/SSL version by default		
<b>Web Info</b>	Using Builtwith web analyzer, we observed that the C-suites executives' information is online.	This can create avenue for phishing campaigns	

### Controls

1. Creation of a Social Media policy for staff and assess the risk of oversharing.
2. Audit and Limit Company Data exposure
3. Conduct phishing simulations and regular security awareness training.
4. Implement the use of email masks.

**Table 2: Comprehensive List of Threats, Risks, Vulnerabilities, Risk Ownership, and Timeline for Remediation**

Artifacts	Sources	Threats	Vulnerabilities	Recommended Controls	Risk Owner	Risk Level	Timeline
Email	Rocketreacher.co	Phishing, Email harvesting for spam	High exposure of valid email addresses enables targeted attacks	Implement email filtering systems. Enhanced phishing training	IT Security Team	High	3 months
Digital Certificates	Shodan, DNS checker	SSL misconfiguration exploitation. Man-in-the-middle attacks	Exposed certificate information reveals infrastructure details	Regular certificate audit. Remove unnecessary subdomains.	Infrastructure Team	Medium	2 months
Client Information	Client Case studies	Supply chain attacks. Competitive intelligence gathering	Client relationship details enable	NDAs enforcement. Client information	Legal & Marketing Teams	High	2 months



			targeted attacks	in disclosure policy.			
DNS Records	Nslookup	Spoofing.Do main hijacking.	Unsecured or misconfigured DNS records.	Spoofing of corporate domains for phishing or email impersonation.	IT Security Team	High	2 months

## 5.2 Approach

As a global leader in consulting, technology, and outsourcing services, Cyberbulwark handles a vast amount of sensitive data for clients across industries such as finance, healthcare, and technology. As a result, it is essential to identify, analyze, and address cybersecurity vulnerabilities in order to protect the company's operations, assets, and reputation. A thorough vulnerability assessment of Cyberbulwark's systems highlights a number of critical risks that could undermine its security posture.

For instance, persistent firewall vulnerabilities, similar to those reported by Chinese hackers exploiting weaknesses in firewall devices over a five-year period, pose significant risks. This type of vulnerability could allow unauthorized access to sensitive systems, jeopardizing

Cyberbulwark’s intellectual property and client data. As part of its ongoing security efforts, Cyberbulwark must continue strengthening firewall protocols, implement continuous monitoring, and conduct regular penetration tests to ensure robust protection against such threats.

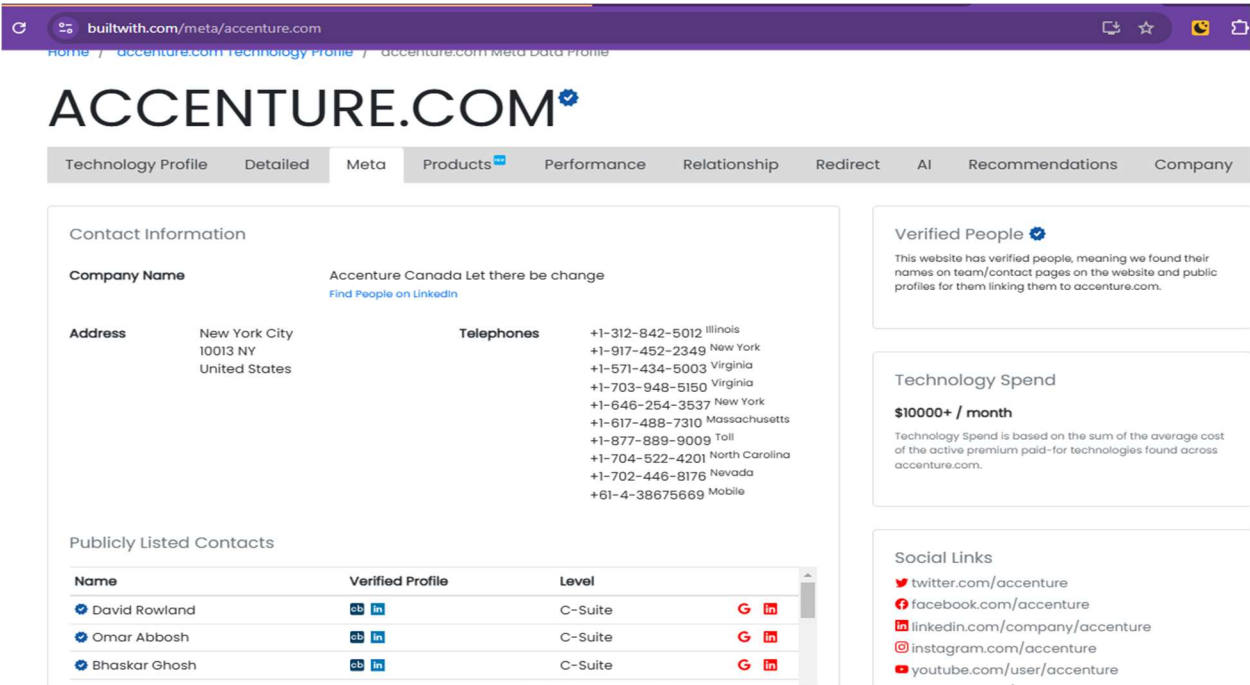


Figure 3.0: Information of Cyberbulwark on Builtwith

Mobile application threats are also relevant, as demonstrated by recent malware attacks targeting Australian banking apps. Given Cyberbulwark’s involvement in developing and managing applications for its clients, these threats could potentially compromise the company’s own mobile applications. To mitigate this, Cyberbulwark’s cybersecurity team must prioritize mobile app security by conducting thorough security audits, identifying vulnerabilities, and adopting advanced security solutions to protect against malicious attacks.

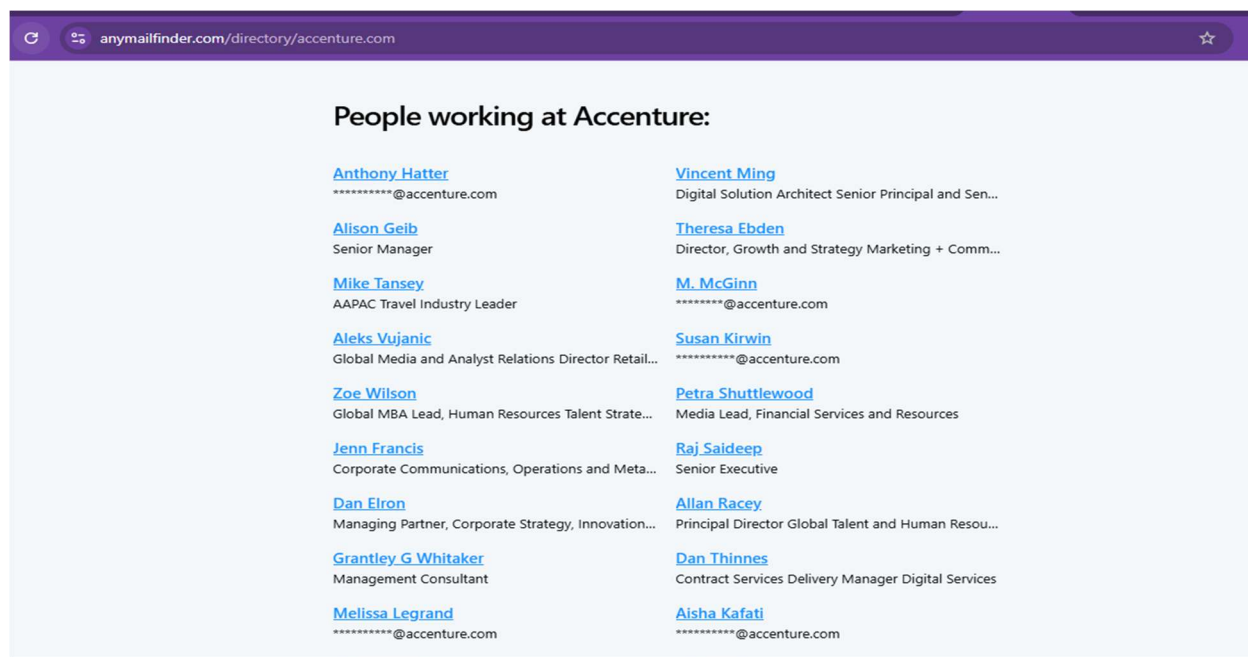


Figure 4.0: Cyberbulwark staffs details on *anymailfinder*

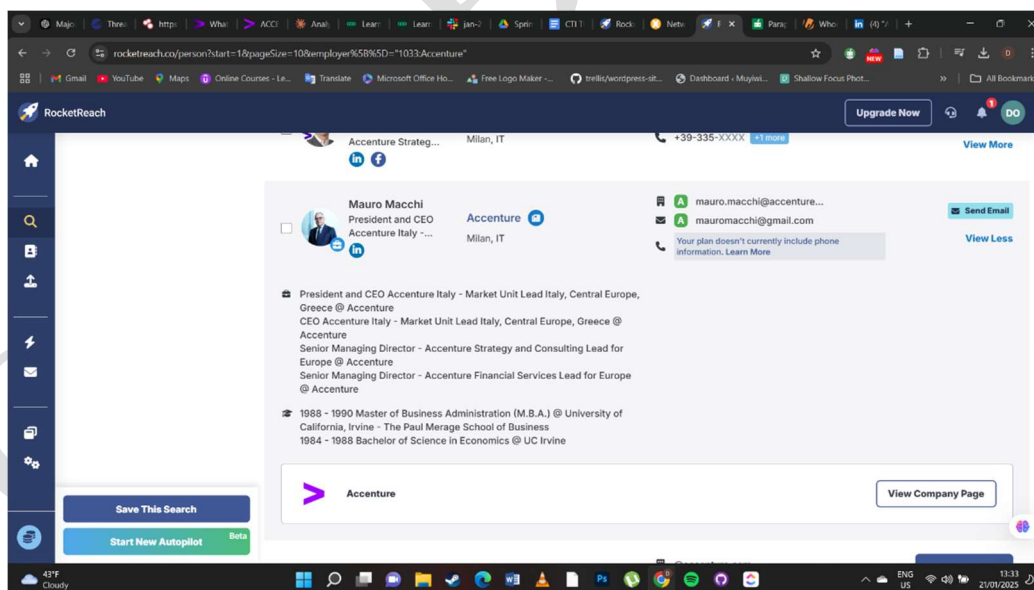
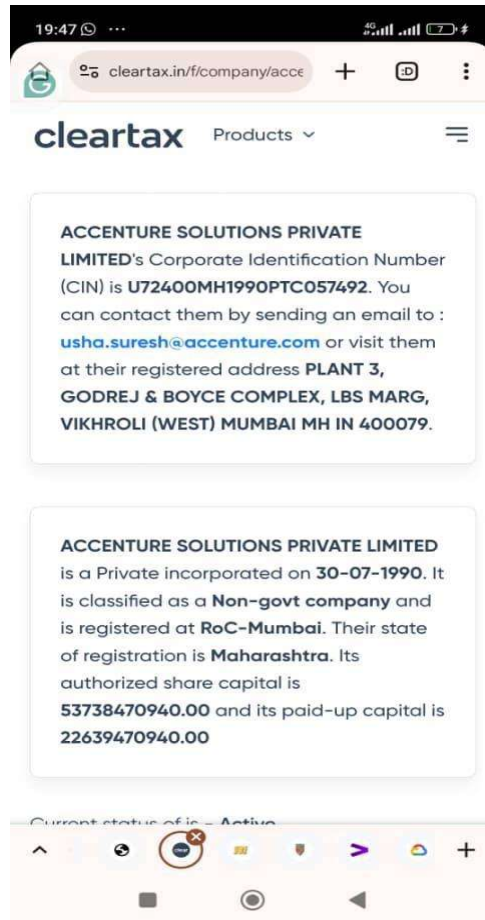


Figure 5.0 Employee email addresses exposed publicly



*Figure 6.0: Cyberbulwark staff information on Cleartax.in platform*

Zero-day vulnerabilities are a pressing concern as well. Platforms like the Zero Day Initiative actively monitor emerging zero-day vulnerabilities. By staying updated on these vulnerabilities, Cyberbulwark can proactively identify potential risks, quickly apply necessary patches, and develop tailored strategies to mitigate these newly discovered threats. This allows the company to stay ahead of adversaries and prevent attacks that take advantage of these previously unknown weaknesses.

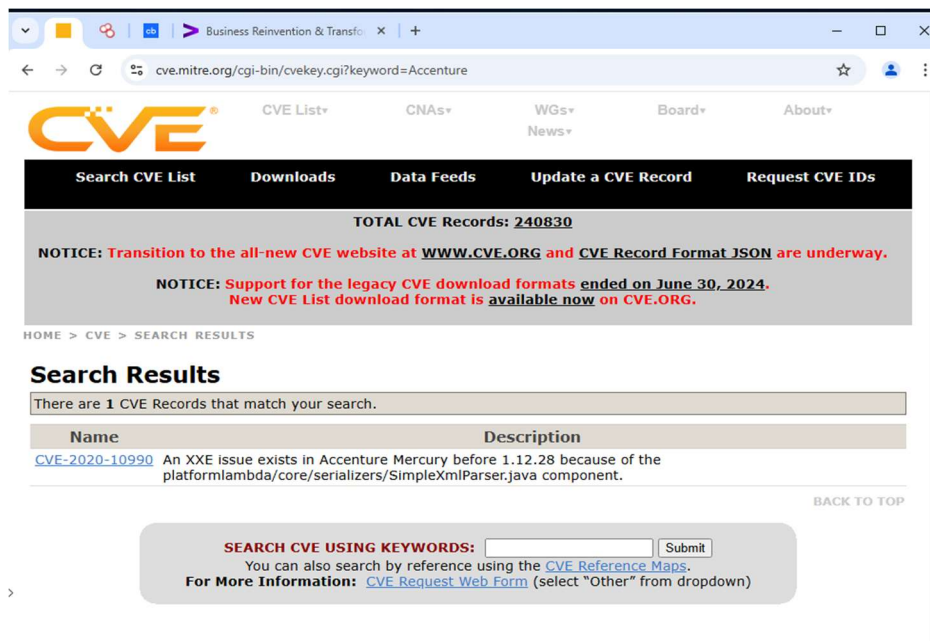


Figure 9.0: Cyberbulwark Vulnerability Search on “CVE”

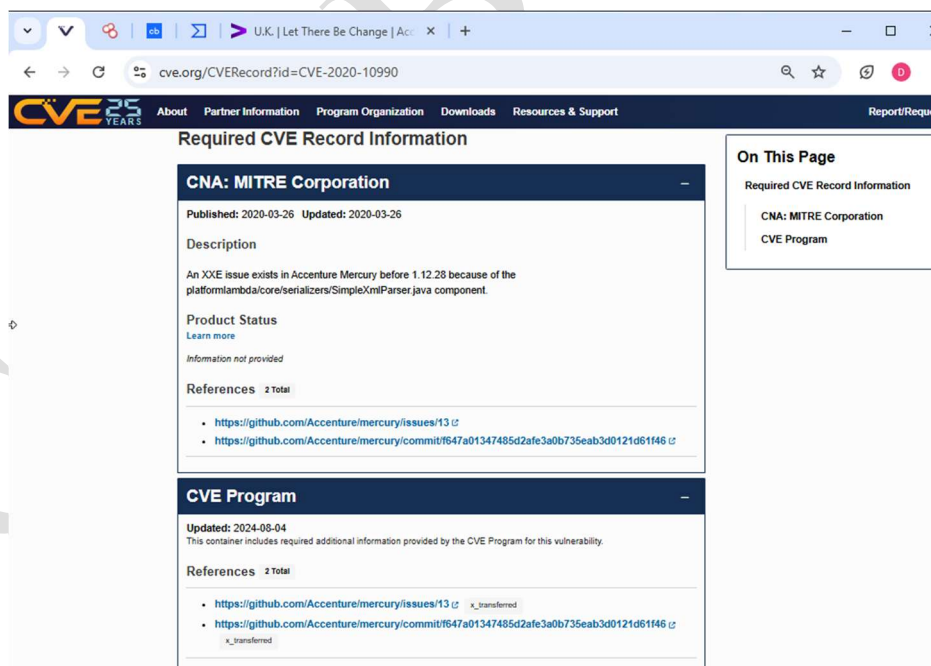


Figure 10.0: Cyberbulwark Vulnerability on “CVE” Result


## Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-611	Improper Restriction of XML External Entity Reference	 NIST

## Known Affected Software

### Configurations [Switch to CPE 2.2](#)

#### Configuration 1 ([hide](#))

 <code>cpe:2.3:a:accenture:mercury:*:*:*:*:* Up to</code>	(excluding)
<a href="#">Show Matching CPE(s)</a>	1.12.28

 Denotes Vulnerable Software

[Are we missing a CPE here? Please let us know.](#)

## Change History

3 change records found [show changes](#)

**NIST** NATIONAL INSTITUTE OF  
STANDARDS AND TECHNOLOGY  
U.S. DEPARTMENT OF COMMERCE



Figure 11.0: Cyberbulwark Vulnerability on “CVE” Result

Cyberbulwark also faces risks through tools such as theHarvester and MXToolbox, which are used to analyze its email servers, subdomains, and DNS configurations. theHarvester helps identify exposed email addresses and subdomains, providing attackers with potential entry points.



```

kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
└─$ theHarvester -d accenture.com -l 1000 -b bing

*****
*                                     *
* [THE HARVESTER]                   *
*                                     *
* theHarvester 4.0.3                 *
* Coded by Christian Martorella      *
* Edge-Security Research             *
* cmartorella@edge-security.com      *
*                                     *
*****

[*] Target: accenture.com

    Searching 0 results.
[*] Searching Bing.

[*] No IPs found.

[*] Emails found: 3
alexander.aizenberg@accenture.com
jens.derksen@accenture.com
recruiting.ch@accenture.com

[*] Hosts found: 33
acpindia-mobile.accenture.com:3.162.20.96, 3.162.20.101, 3.162.20.109, 3.162.20.84
atci.techexpressway.accenture.com:144.36.140.180
atci.techleap.accenture.com:144.36.140.235

```

Figure 12.0: Using theHarvester to identify email address and subdomains associated with Cyberbulwark

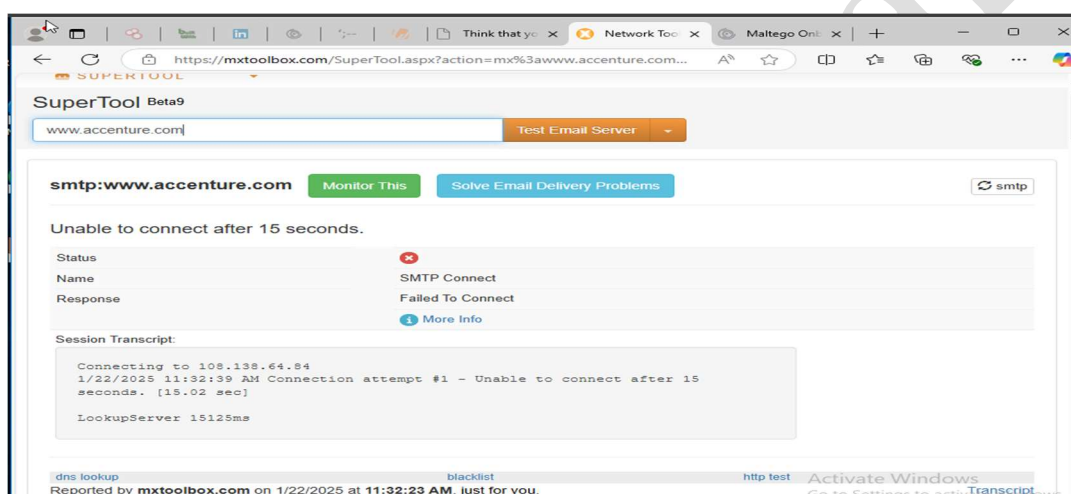
```

kali@kali: ~
File Actions Edit View Help
dynamicmedia.accenture.com:95.101.63.56, 95.101.63.232
iaspire-learning.ciostage.accenture.com:13.235.35.223, 13.126.120.91
in.accenture.com:172.64.152.227, 104.18.35.29
indiacampus.accenture.com:52.77.52.153
infolaboral.accenture.com:54.230.10.47, 54.230.10.96, 54.230.10.127, 54.230.10.43
interviewscheduling.accenture.com:34.231.149.227
investor.accenture.com:104.18.10.9, 104.18.11.9
jobsgateway.accenture.com:54.230.10.78, 54.230.10.122, 54.230.10.84, 54.230.10.29
lifesciences.accenture.com:18.208.125.13, 3.215.172.219, 52.54.96.194, 34.237.219.119, 3.92.120.28
myappid.accenture.com:20.26.31.224
mycompetency.accenture.com:18.165.160.34, 18.165.160.110, 18.165.160.91, 18.165.160.43
myemail.accenture.com:52.96.71.143, 52.96.214.67, 52.96.47.34, 52.96.61.15, 52.96.214.99, 52.96.217.201, 52.96.218.201, 52.96.221.231
myholdings.accenture.com:18.165.160.108, 18.165.160.93, 18.165.160.59, 18.165.160.99
myid.accenture.com:13.224.81.106, 13.224.81.16, 13.224.81.18, 13.224.81.57
mylearning.accenture.com:172.64.144.47, 104.18.43.209
myoffice.accenture.com:13.107.137.10, 13.107.139.10
myte.accenture.com:104.18.33.137, 172.64.154.119
negocios.acceservices.accenture.com:45.60.153.35
newsroom.accenture.com:54.230.10.23, 54.230.10.126, 54.230.10.63, 54.230.10.31
portal.accenture.com:104.18.41.157, 172.64.146.99
realms.accenture.com:144.36.138.57
rewards.accenture.com:18.172.89.39, 18.172.89.83, 18.172.89.75, 18.172.89.30
support.accenture.com:149.96.29.117
techselfsupport.accenture.com:144.36.140.158
touchpoint.accenture.com:34.231.149.227
workforce.accenture.com:104.18.35.232, 172.64.152.24
www.accenture.com:54.230.10.96, 54.230.10.16, 54.230.10.35, 54.230.10.69
www.investor.accenture.com:104.18.10.9, 104.18.11.9

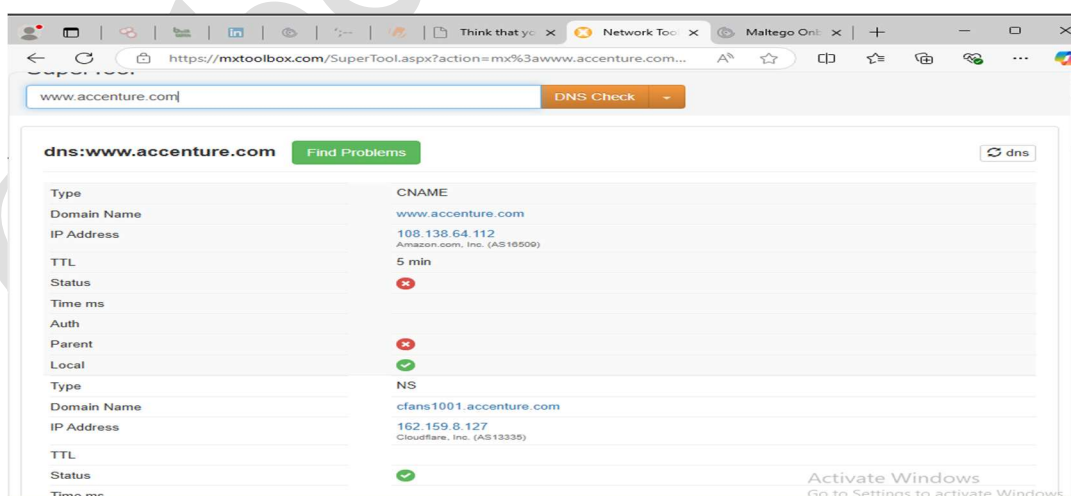
```

*Figure 12.1: Using theHarvester to identify email address and subdomains associated with Cyberbulwark*

Additionally, MXToolbox tests the security features of Cyberbulwark’s email servers, specifically assessing the effectiveness of SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting, and Conformance) records—critical protocols for preventing email spoofing and phishing attempts.

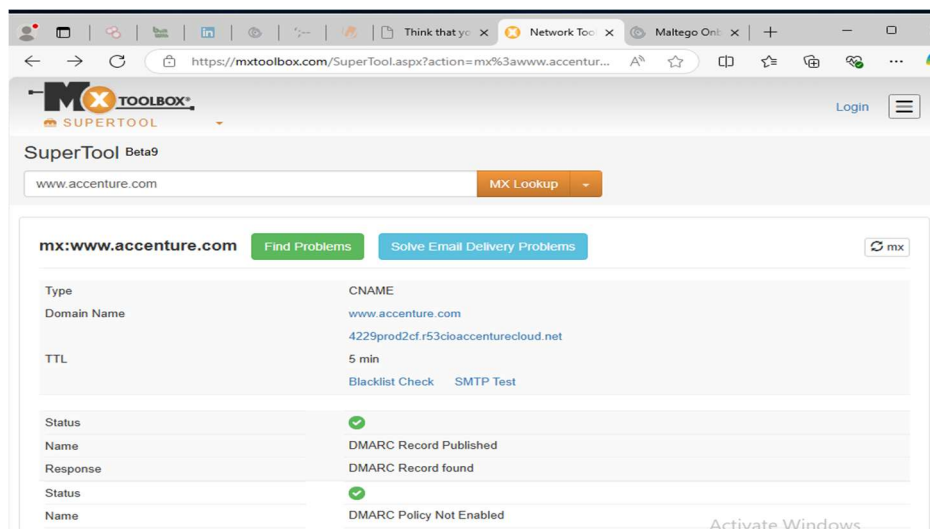


*Figure 13.0: MXToolbox used for testing email server security*



*Figure 13.1 MXToolbox used for testing email server security*





*Figure 13.2: MXToolbox used for testing email server security*

The discovery of employee email addresses on the “Have I Been Pwned” platform underscores the importance of Cyberbulwark implementing strong password management practices and multi-factor authentication (MFA). This exposure highlights the vulnerability of user credentials and the need to reinforce security policies to prevent unauthorized access to sensitive accounts and systems

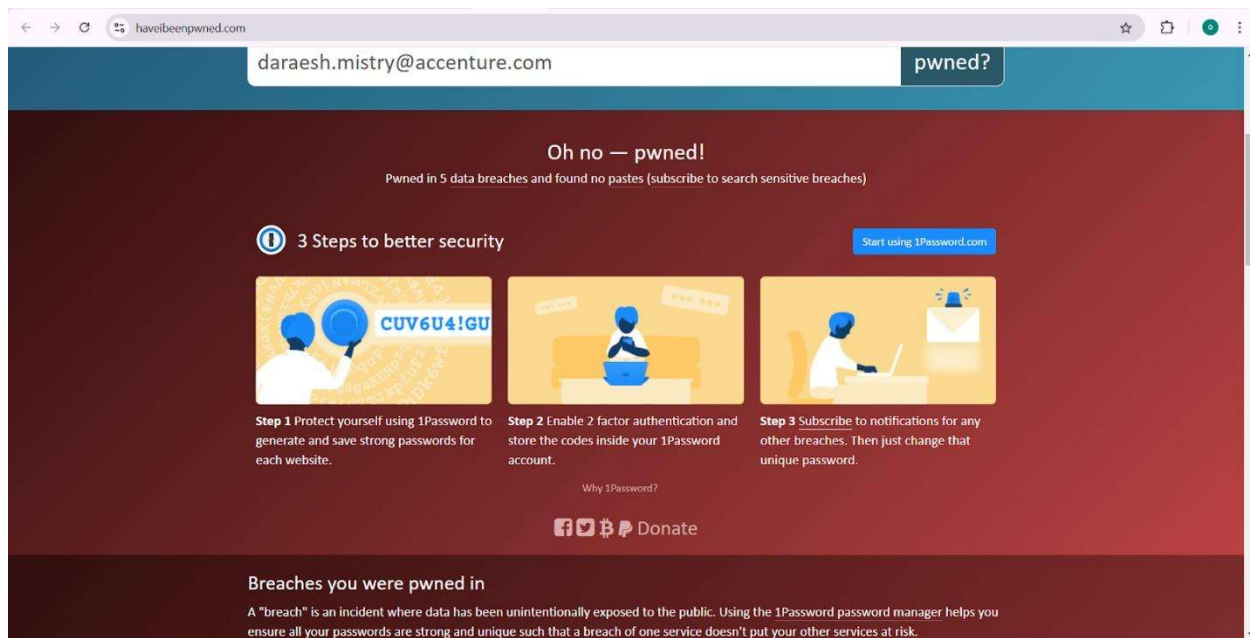


Figure 8.0: Employee email found on “Have I been pwned” -A

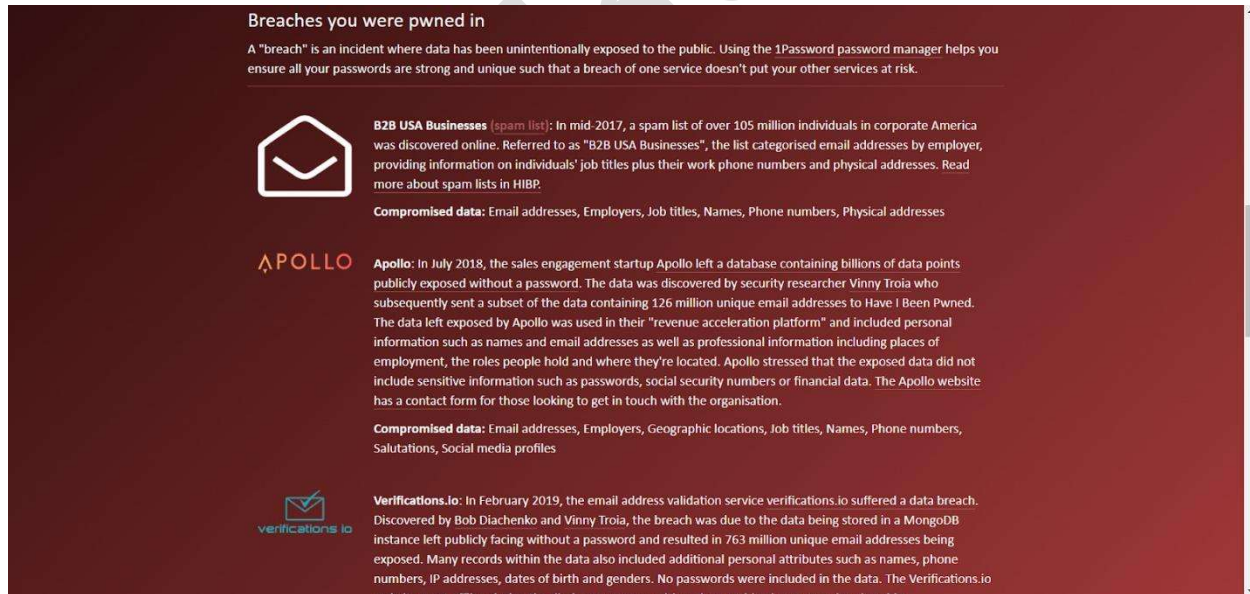


Figure 8.1: Employee email found on “Have I been pwned” -B

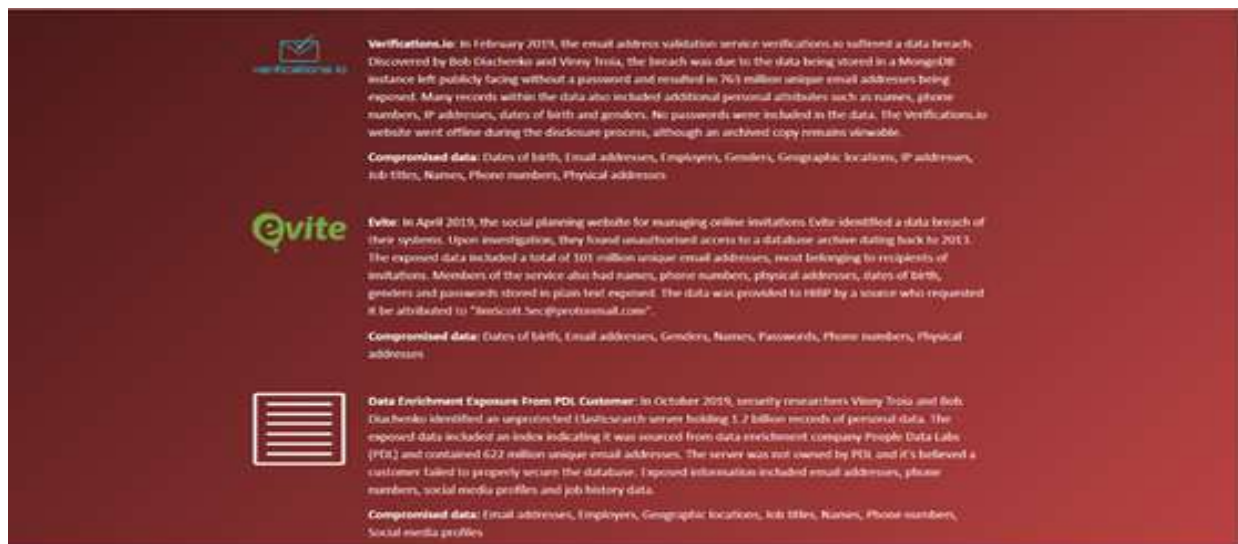


Figure 8.2: Employee email found on “Have I been pwned”- C

Furthermore, Cyberbulwark's email servers' DNS information, which reveals reliance on Amazon AWS for hosting, shows that while the company is using cloud services for hosting web services, it must continue to monitor and secure cloud infrastructure. Regular configuration audits and alignment with best practices are necessary to safeguard against potential threats to cloud-based services.

Lastly, the analysis of DNS and email security configurations suggests gaps in Cyberbulwark's DMARC, SPF, and DKIM implementations. To mitigate the risk of phishing attacks and email spoofing, Cyberbulwark should prioritize the strengthening of these email security measures. A fully enforced DMARC policy and strict email validation protocols will significantly enhance the company's defenses against malicious email activity.

In summary, Cyberbulwark must take decisive action to address the vulnerabilities identified in this assessment. By leveraging advanced cybersecurity tools, adopting proactive risk management strategies, and ensuring continuous monitoring of its systems, Cyberbulwark can safeguard its operations and provide secure services to clients. Ensuring that the company remains

resilient against evolving cyber threats is vital for maintaining its reputation as a global leader in consulting and technology services.

CyberBulwark

## Vulnerability Research

The Common Vulnerabilities and Exposures (CVE) database is a comprehensive list of publicly disclosed cybersecurity vulnerabilities. Each CVE entry contains an identification number, a description, and at least one public reference.

The Common Vulnerability Scoring System (CVSS) is used to assess the severity of security vulnerabilities. The CVSS score ranges from 0 to 10, with higher scores indicating more severe vulnerabilities. The score is calculated based on several metrics, including exploitability, impact, and the complexity of the attack.

### 6.1 Current Relevant Vulnerabilities

1. **CVE-2024-50603:** Aviatrix Controllers OS Command Injection Vulnerability
  - **Description:** This vulnerability allows an unauthenticated attacker to execute arbitrary code by sending shell metacharacters to specific API endpoints.
  - **Impact:** Could lead to unauthorized access and control over the affected systems.
  - **Exploited in the Wild:** Yes.
2. **CVE-2024-55591:** Fortinet FortiOS and FortiProxy Authentication Bypass Vulnerability
  - **Description:** This vulnerability may allow an unauthenticated, remote attacker to gain super-admin privileges via crafted requests to the Node.js websocket module.
  - **Impact:** Could result in complete control over the affected systems.
  - **Exploited in the Wild:** Yes.
3. **CVE-2025-21333:** Microsoft Windows Hyper-V NT Kernel Integration VSP Heap-based Buffer Overflow Vulnerability

- **Description:** This vulnerability allows a local attacker to gain SYSTEM privileges through a heap-based buffer overflow.
- **Impact:** Could lead to privilege escalation and full system compromise.
- **Exploited in the Wild:** Yes.

## 6.2 Latest Zero-Day Vulnerabilities

### 1. Fortinet FortiManager CVE-2024-47575

- **Description:** A critical zero-day vulnerability affecting FortiManager network management solution.
- **Impact:** Allows attackers to exploit the vulnerability before a patch is available.
- **Exploited in the Wild:** Yes.

### 2. MOVEit Transfer CVE-2023-34362

- **Description:** A critical vulnerability in Progress Software's MOVEit Transfer solution.
- **Impact:** Allows attackers to exploit the vulnerability across multiple customer environments.
- **Exploited in the Wild:** Yes.

## 6.3 Threat Actors Exploiting Vulnerabilities

- **Lazarus Group:** Known for exploiting various vulnerabilities to target organizations across different sectors, including energy and government agencies.
- **APT Groups:** Multiple nation-state advanced persistent threat (APT) actors have been observed exploiting vulnerabilities like CVE-2022-47966 and CVE-2022-42475.

## Advisory for CyberBulwark

Based on the research, here is a brief advisory for CyberBulwark:

1. **Patch Management:** Ensure timely application of patches for all systems, especially for known exploited vulnerabilities (KEVs). Implement a centralized patch management system to streamline this process.
2. **Endpoint Detection and Response (EDR):** Deploy EDR solutions to monitor and detect unauthorized activities on endpoints. This will help in identifying and mitigating potential threats in real-time.
3. **Network Security:** Use web application firewalls and network protocol analyzers to protect against exploitation of vulnerabilities in public-facing applications.
4. **User Awareness:** Conduct regular cybersecurity training for employees to recognize and avoid phishing attempts and other social engineering attacks.
5. **Vulnerability Assessment:** Regularly perform vulnerability assessments and penetration testing to identify and remediate security weaknesses in the network.

## 6.4 Top Five Threat Actors Against CyberBulwark

### 1. Lazarus Group

- a. **Profile:** The Lazarus Group is a highly sophisticated cybercrime organization believed to be linked to the North Korean government. Active since at least 2007, the group specializes in cyber espionage, financial theft, and disruptive attacks. It operates under various aliases, including APT38, Hidden Cobra, and Guardians of Peace. Lazarus is motivated by both financial gain and political objectives.

- b. Targeted Industry:** The group targets a broad range of industries, including **finance, cryptocurrency, defense, energy, media, healthcare, and government.** Notably, they have attacked financial institutions worldwide to fund North Korea's regime and have been involved in high-profile incidents like the Sony Pictures hack and the WannaCry ransomware outbreak.
- c. Methods Used:** Lazarus employs a variety of advanced techniques, including Phishing attacks, Malware, Supply Chain Attacks, Exploiting vulnerabilities, & Cryptocurrency Theft.
- d. Source:** Kaspersky, Symantec, and FireEye.

## 2. Ransom Hub

- a. Profile:** RansomHub is a ransomware gang or platform that operates as a Ransomware-as-a-Service (RaaS) network, allowing affiliates to deploy ransomware attacks in exchange for a share of the profits. The group emerged in recent years and is known for its aggressive tactics, including double extortion schemes where victims' data is encrypted and threatened to be leaked publicly unless a ransom is paid.
- b. Targeted Industry:** RansomHub targets a wide array of industries, focusing on organizations with sensitive or valuable data, such as **healthcare, financial services, education, technology, manufacturing, and government agencies.** The group often focuses on entities with inadequate cybersecurity measures or high stakes, making them more likely to pay ransoms.



- c. Methods Used:** Phishing Attacks, Exploitation of vulnerabilities, Network Infiltration, Data encryption, Data theft and Double extortion.
- d. Source:** Palo Alto Networks and Crowdstrike

### 3. Akira

- a. Profile:** Akira is a ransomware group that emerged in 2023 and gained attention for its focus on targeted ransomware attacks. The group is named after its proprietary ransomware strain, "Akira," which encrypts files and appends the .akira extension. Akira has been associated with double extortion tactics, demanding payment for both data decryption and preventing the release of stolen information.
- b. Targeted Industry:** Akira primarily targets medium to large enterprises across various industries, including **healthcare, finance, education, technology, manufacturing, and professional services.**
- c. Methods Used:** Phishing Attacks, Exploitation of vulnerabilities, Credential Theft, Data encryption, and Double extortion.
- d. Source:** Sophos, Palo Alto Networks, and Malwarebytes

### 4. Blackcat / ALPHV

- a. Profile:** BlackCat, also known as ALPHV, is a sophisticated ransomware group that emerged in late 2021. It is notable for its advanced ransomware written in the Rust programming language, making it highly efficient and adaptable across different operating systems. BlackCat operates as a Ransomware-as-a-Service (RaaS), recruiting affiliates to deploy attacks in exchange for a share of the profits.

The group is also recognized for its innovation, such as providing a customizable ransom portal for victims.

- b. Targeted Industry:** BlackCat targets a wide range of industries with valuable data and deep pockets such as **healthcare, finance, technology, manufacturing, education, critical national infrastructure (CNI), and retail.**
- c. Methods Used:** Phishing Attacks, Exploitation of vulnerabilities, Credential Theft, Data Encryption, Data theft, Double extortion and Highly customizable Malware.
- d. Source:** Kaspersky, Sophos, Palo Alto Networks

## 5. LockBit

- a. Profile:** LockBit is a Ransomware-as-a-Service (RaaS) operation that has been active since 2019 and has been ranked as the most prolific and destructive group. LockBit was the most deployed ransomware variant across the world from 2022-2023. Since January 2020, affiliates using LockBit have attacked organizations of varying sizes across an array of critical infrastructure sectors, including financial services, food and agriculture, education, energy, government and emergency services, healthcare, manufacturing, and transportation. The group uses advanced double-extortion tactics: encrypting victims' files while threatening to release sensitive data if the ransom is not paid.
- b. Targeted industry:** LockBit targets various sectors, including **healthcare, financial institutions, IT services, and government entities.**
- c. Methods Used:** Phishing campaigns, exploitation of software vulnerabilities.

d. Source: CISA Flashpoint

Pie Chart of Threat Actors

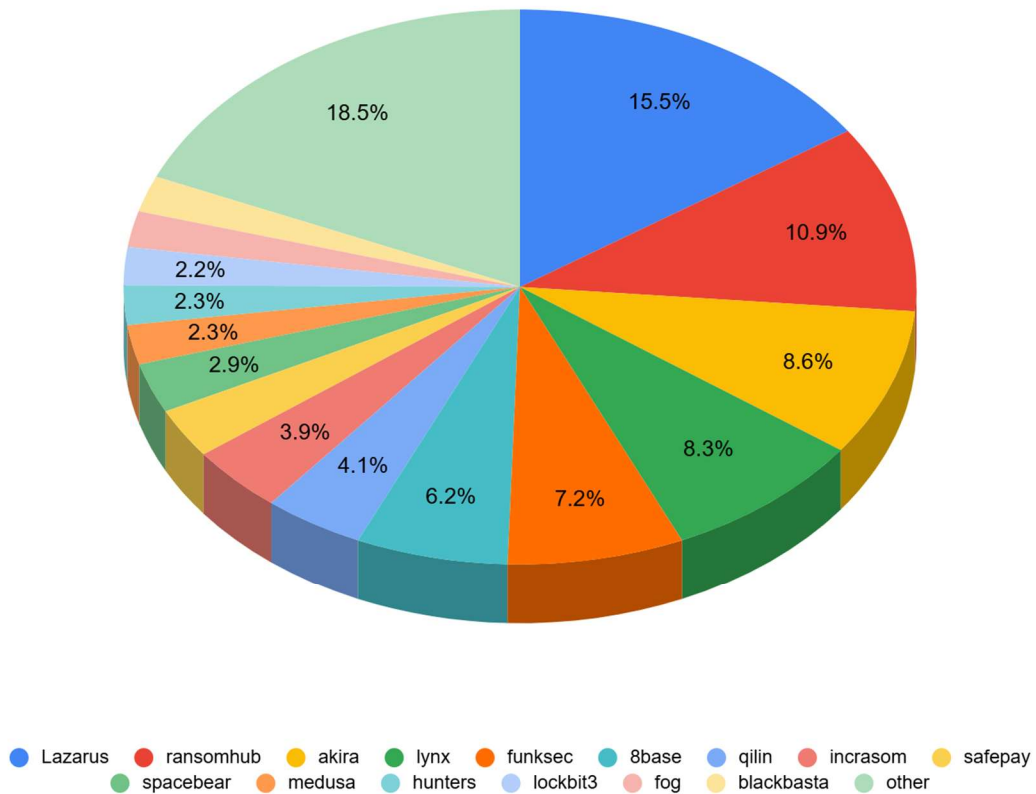


Figure 9.0: Pie chart of threat actors

Source: Ransomware.live - Statistics

## 6.5 Recent Incidents and Relevance to CyberBulwark

### a. Royal Mail (2023)

According to [BBC](#), Lockbit hit the royal mail in 2023, disrupting its international deliveries, this attack highlighted the vulnerabilities in operational and public service sectors. CyberBulwark works with clients in logistics, transportation, and public services, where business continuity is very important. A ransomware attack like the one on Royal Mail could lead to significant reputational damage and client dissatisfaction if their digital transformation projects are impacted.

### b. Reddit (2023)

Ransomware gang ALPHV, most commonly known as BlackCat, was allegedly responsible for the theft of 80GB of data from their social media site [Cybersecurity Hub](#). The spear-phishing emails sent employees to a bogus website that looked like the company's intranet gateway. The landing page was designed to trick people into giving their credentials and second-factor tokens. With a workforce of over 700,000 employees, CyberBulwark faces risks of insider threats and spear-phishing campaigns. A Reddit-style attack could compromise sensitive internal data, client information, or intellectual property.

### c. AT&T (2024)

AT&T said in April 2024 that almost all of the data of its cell customers had been stolen. Records of most of AT&T's customers' call and text conversations were stolen during the cyberattack, which happened between April 14 and April 25,

2024. The information that was stolen is from May 1, 2022, to October 31, 2022, with a few records from January 2, 2023. As a technology consultant, CyberBulwark often interacts with client systems vulnerable to phishing. The AT&T incident highlights the risks of social engineering and credential theft, which could compromise client networks and data if mishandled.

## Overview of Number 1 Threat Actor

**Group Name:** Lazarus Group

**Origin/Affiliations:** North Korea

**Motive:** State sponsored/ Nation-State

### Sample Indicator of Compromise

#### IP Addresses:

- Specific IP addresses linked to Lazarus Group activities have been identified in various investigations. [AlienVault](#)

#### Malware and Tools:

- Mimikatz: A tool used for credential extraction from Windows systems.
- WannaCry: Ransomware that encrypts data and demands payment for decryption.
- Hermes: Ransomware used in various attacks attributed to the group.
- Electricfish: A tunneling tool used to exfiltrate data.
- AppleJeus: Malware targeting cryptocurrency exchanges.
- TraderTraitor: Malware used in phishing campaigns targeting cryptocurrency users.

#### Domains and URLs:

- The group has been known to use compromised or malicious domains to host command and control servers, phishing pages, or malware distribution sites.

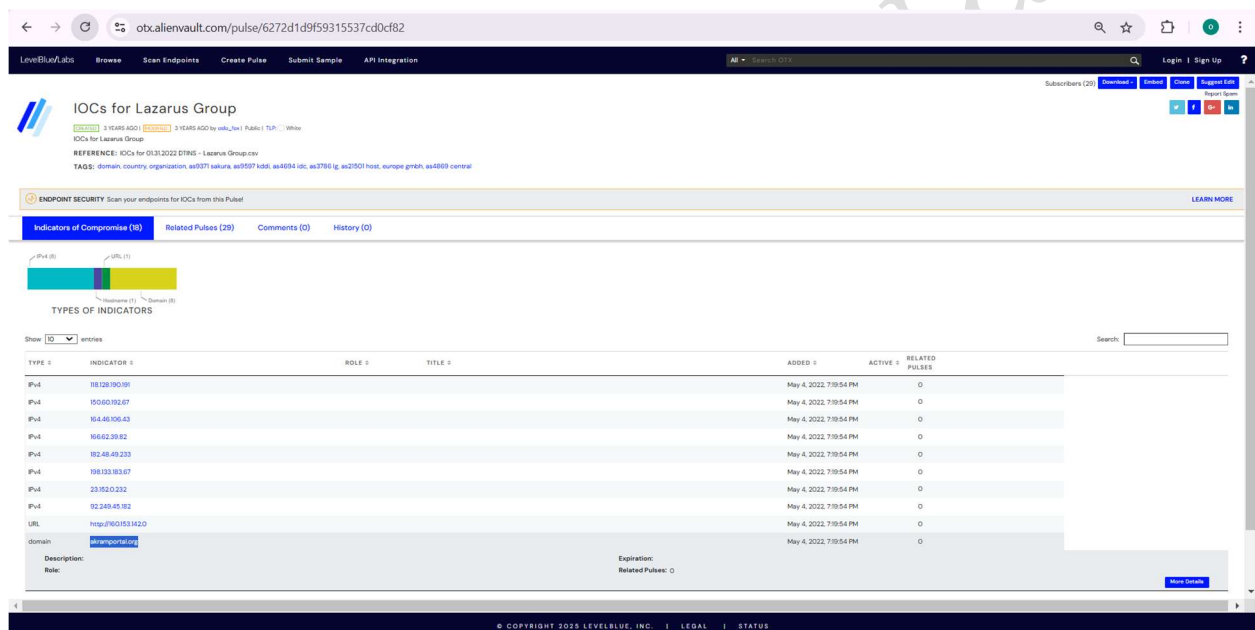
#### File Hashes:

- Specific file hashes corresponding to Lazarus Group malware have been documented in threat intelligence reports.

## **Email Addresses and Phishing Artifacts:**

- The group often employs spear-phishing emails with malicious attachments or links, sometimes impersonating trusted entities to lure victims.

## **Sample Testing**



*Figure 10.0: IoCs for Lazarus group*

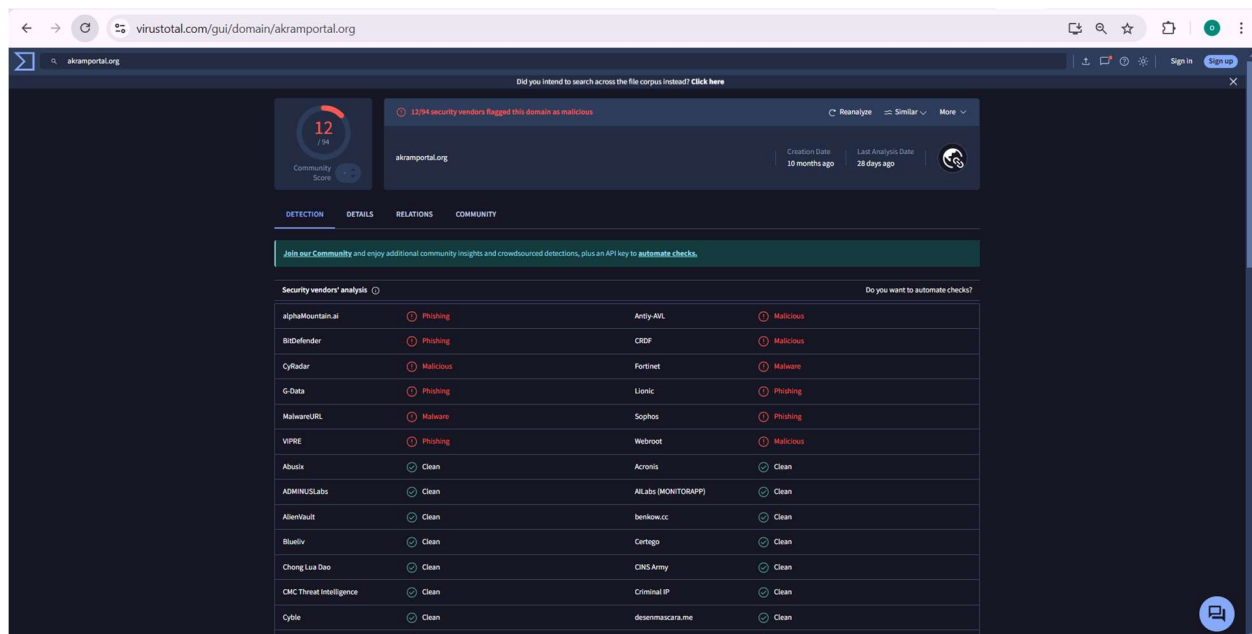


Figure 11.0: Malware analysis on VirusTotal 1

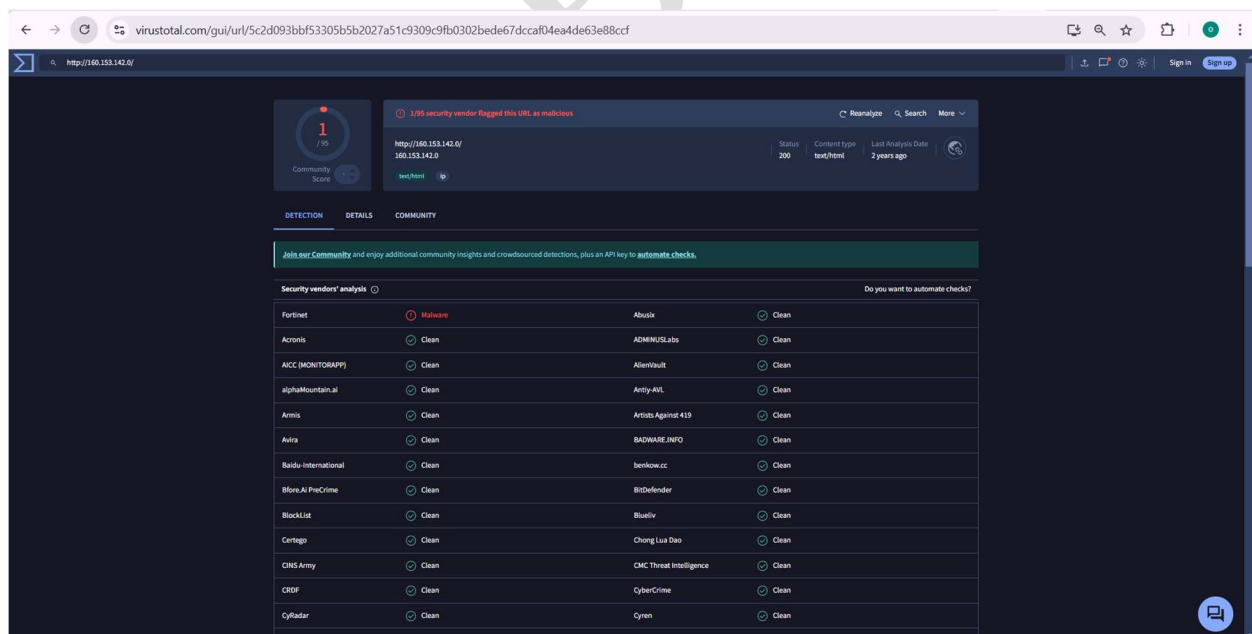


Figure 12.0: Malware analysis on VirusTotal 2



## 7.1 Relevant Companies Impacted by Lazarus Group

### 1. EDF Energy (2024)

- **Industry:** Energy
- **Revenue:** €69 billion (2022)
- **Number of Employees:** 165,000
- **Brief Description of the Attack:** The Lazarus Group targeted EDF Energy as part of a broader campaign against energy providers worldwide. The campaign involved exploiting vulnerabilities in VMware Horizon to gain initial access and deploying malware like VSingle, YamaBot, and MagicRAT. The attackers aimed to establish long-term access and exfiltrate data of interest to North Korea.
- **Impact in Terms of Revenue, Operations, etc.:** Potential operational disruption and financial impact.
- **Source:** [InfoSec](#)

### 2. Siemens Energy (2023)

- **Industry:** Energy
- **Revenue:** €28.8 billion (2022)
- **Number of Employees:** 91,000
- **Brief Description of the Attack:** The Lazarus Group targeted Siemens Energy in their attacks on the energy sector. The campaign involved the use of sophisticated malware and exploitation of vulnerabilities to gain access to the company's systems. The attackers aimed to gather intelligence and potentially disrupt operations.

- **Impact in Terms of Revenue, Operations, etc.:** Potential operational disruption and financial impact.
- **Source:** [AttackIQ](#)

### 3. Nuclear Regulatory Commission (NRC) (2024)

- **Industry:** Government Agency
- **Revenue:** Not publicly disclosed
- **Number of Employees:** 3,000
- **Brief Description of the Attack:** The Lazarus Group targeted employees of nuclear-related organizations, including those associated with the NRC, using sophisticated malware like CookiePlus. The attack involved sending malicious documents and remote access tools to lure victims into downloading and running malware on their systems.
- **Impact in Terms of Revenue, Operations, etc.:** Potential operational disruption and security concerns.
- **Source:** [Rhyno](#)

### 7.3 Tactics, Techniques, and Procedures (TTPs)

In this research, we have conducted a detailed analysis of the tactics, techniques, and procedures (TTPs) used by the Lazarus Group, a top threat actor. The analysis is based on the MITRE ATT&CK Framework, which provides a comprehensive knowledge base of adversary tactics and techniques based on real-world observations. The table below lists all the techniques, including their unique MITRE IDs, used by the Lazarus Group at each stage of their attack lifecycle, adopting the 14 MITRE Tactics.

**Table 4: Tactics Techniques and Procedures**

MITRE Tactic	Technique ID	Technique Description
Initial Access	T1078	Valid Accounts: Adversaries may steal or forge credentials to gain access to systems.
	T1190	Exploit Public-Facing Application: Adversaries may exploit vulnerabilities in internet-facing systems to gain access.
Execution	T1059	Command and Scripting Interpreter: Adversaries may use command-line interfaces to execute malicious code.
	T1203	Exploitation for Client Execution: Adversaries may exploit vulnerabilities in client applications to execute code.
Persistence	T1078	Valid Accounts: Adversaries may maintain access by using stolen or forged credentials.
	T1547	Boot or Logon Autostart Execution: Adversaries may configure systems to execute malicious code at startup.
Privilege Escalation	T1068	Exploitation for Privilege Escalation: Adversaries may exploit vulnerabilities to gain higher-level permissions.
	T1078	Valid Accounts: Adversaries may use stolen credentials to gain elevated privileges.
Defense Evasion	T1070	Indicator Removal on Host: Adversaries may delete or alter logs to avoid detection.
	T1562	Impair Defenses: Adversaries may disable security tools to avoid detection.
Credential Access	T1003	OS Credential Dumping: Adversaries may extract credentials from operating systems.
	T1056	Input Capture: Adversaries may capture user input to steal credentials.

Discovery	T1083	File and Directory Discovery: Adversaries may search for files and directories to gather information.
	T1018	Remote System Discovery: Adversaries may identify remote systems to facilitate lateral movement.
Lateral Movement	T1021	Remote Services: Adversaries may use remote services to move laterally within a network.
	T1075	Pass the Hash: Adversaries may use hashed credentials to authenticate to systems.
Collection	T1113	Screen Capture: Adversaries may capture screenshots to gather information.
	T1056	Input Capture: Adversaries may capture user input to gather information.
Command and Control	T1071	Application Layer Protocol: Adversaries may use application layer protocols to communicate with compromised systems.
	T1090	Proxy: Adversaries may use proxies to obscure the origin of their communications.
Exfiltration	T1041	Exfiltration Over C2 Channel: Adversaries may exfiltrate data over their command and control channel.
	T1020	Automated Exfiltration: Adversaries may use automated methods to exfiltrate data.
Impact	T1485	Data Destruction: Adversaries may destroy data to disrupt operations.
	T1490	Inhibit System Recovery: Adversaries may inhibit system recovery to make it difficult to restore systems.
Resource Development	T1583	Acquire Infrastructure: Adversaries may acquire infrastructure to support their operations.

	T1584	Compromise Infrastructure: Adversaries may compromise existing infrastructure to support their operations.
Reconnaissance	T1592	Gather Victim Host Information: Adversaries may gather information about victim hosts to plan future operations.
	T1595	Active Scanning: Adversaries may use active scanning to gather information about target systems.

## 7.4 Mitigating Lazarus group's Attacks

For our company to strengthen its security posture and protect against disruptive attacks from threat actors like Lazarus Group, we need a comprehensive defense strategy that encompasses multiple layers of protection. This strategy should include:

1. **Proactive Threat Detection and Monitoring:** Continuous surveillance of network traffic and system activity to identify suspicious behavior early. Leveraging advanced threat intelligence tools can help us detect anomalies indicative of malicious activity before they escalate.
2. **Robust Network Defense:** Ensuring our network infrastructure is fortified with firewalls, intrusion detection/prevention systems (IDS/IPS), and rate-limiting mechanisms to mitigate potential attack vectors. Regular security audits and vulnerability assessments can help uncover and address weaknesses in our network.
3. **Access Control and Authentication:** Implementing stringent access control measures such as multi-factor authentication (MFA), role-based access control (RBAC), and the

principle of least privilege to limit unauthorized access to critical systems. This will help prevent attackers from exploiting stolen credentials.

4. **Incident Response and Recovery Planning:** Establishing an incident response team (IRT) that can quickly identify, contain, and mitigate attacks when they occur. Having a well-documented recovery plan ensures that we can restore operations swiftly after an attack, minimizing downtime and data loss.
5. **Employee Training and Awareness:** Conducting regular cybersecurity training and awareness programs to educate employees on identifying phishing attempts, social engineering tactics, and safe handling of sensitive information. A well-informed workforce is a crucial line of defense against initial access threats.
6. **Collaboration with External Threat Intelligence Providers:** Engaging with third-party threat intelligence sources can provide real-time information about emerging threats and tactics used by threat actors like Lazarus Group. This helps us stay ahead of potential attacks and adopt the latest security practices.
7. **Continuous Patching and Vulnerability Management:** Regularly updating and patching all software, systems, and applications to close any security gaps that could be exploited by adversaries. Automation tools can be leveraged to ensure that critical updates are deployed in a timely manner across the organization.

By implementing these multi-layered strategies, we can significantly reduce the risk of attacks from advanced persistent threat groups like Lazarus Group, safeguarding our company's data, systems, and reputation.

## **Conclusion**

This Cyber Threat Intelligence (CTI) report underscores the critical need for CyberBulwark to enhance its cybersecurity defenses in the face of an evolving threat landscape. The company's prominent role in managing sensitive client data makes it a prime target for cybercriminals, with threats such as ransomware, phishing, and data breaches posing significant risks. Key vulnerabilities, including publicly available employee data and weaknesses in digital infrastructure, exacerbate these threats.

The identification of the Lazarus Group as a key threat actor highlights the sophistication of potential attacks, while past incidents, such as the 2021 LockBit ransomware attack, serve as stark reminders of the importance of strengthening security measures. The recommended actions, including strengthening employee training, implementing multi-factor authentication, adopting a Zero Trust model, and enhancing threat intelligence capabilities, are crucial steps toward mitigating risks and safeguarding the organization's assets.

By prioritizing these measures, CyberBulwark can improve its cybersecurity posture, reduce exposure to cyber threats, and ensure the continued protection of client data, ultimately enhancing its operational resilience in an increasingly complex digital environment.

## References

"APT32," MITRE ATT&CK, 2024. [Online]. Available: <https://attack.mitre.org/groups/G0032/>.

[Accessed: Jan. 24, 2025].

**BuiltWith**, "Cyberbulwark.com technology profile." [Online]. Available: <https://builtwith.com/meta/Cyberbulwark.com>. [Accessed: Jan. 21, 2025].

**crocodyli**, *Threat Actors TTPs*. GitHub Repository. [Online]. Available: <https://github.com/crocodyli/ThreatActors-TTPs>. [Accessed: Jan. 21, 2025].

**Cybersecurity and Infrastructure Security Agency (CISA)** "*Ransomware Advisory AA24-242A*," 2024. [Online]. Available: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a>. [Accessed: Jan. 24, 2025].

**Cyberbulwark**, "Commit f647a01347485d2afe3a0b735eab3d0121d61f46 - Mercury," GitHub, Jan. 2024. [Online]. Available: <https://github.com/Cyberbulwark/mercury/commit/f647a01347485d2afe3a0b735eab3d0121d61f46>. [Accessed: 29-Jan-2025].

**Cyberbulwark**, "Issue #13 - Mercury," *GitHub*, Nov. 2023. [Online]. Available: <https://github.com/Cyberbulwark/mercury/issues/13>. [Accessed: Jan. 29, 2025].



**InfoSec Institute**, "Information Gathering in Penetration Testing," InfoSec Resources. [Online]. Available: <https://www.infosecinstitute.com/resources/penetration-testing/information-gathering/>. [Accessed: Jan. 21, 2025].

**National Institute of Standards and Technology (NIST)**, "CVE-2020-10990 Detail," *National Vulnerability Database (NVD)*, May 2020. [Online]. Available: <https://nvd.nist.gov/vuln/detail/CVE-2020-10990>. [Accessed: 29-Jan-2025].

**Ransomhub Ransomware: Darktrace's Investigation of the Newest Tool in ShadowSyndicate's Arsenal,** Darktrace, 2024. [Online]. Available: <https://darktrace.com/blog/ransomhub-ransomware-darktraces-investigation-of-the-newest-tool-in-shadowsyndicates-arsenal>. [Accessed: Jan. 24, 2025].

**"Ransomware Statistics,"** *Ransomware Live*, 2025. [Online]. Available: <https://www.ransomware.live/stats>. [Accessed: Jan. 21, 2025].

## Glossary of Terms

**Advanced Persistent Threat (APT):** A stealthy cyberattack conducted by organized and skilled groups, often for espionage or sabotage, targeting specific entities over a prolonged period.

**Botnet:** A network of compromised devices controlled by a threat actor to perform malicious tasks, such as launching DDoS attacks.

**Command-and-Control (C2):** A server or infrastructure used by threat actors to communicate with compromised devices within a network.

**CVE (Common Vulnerabilities and Exposures):** A unique identifier for publicly known security vulnerabilities, managed by MITRE to standardize naming and sharing of vulnerability information.

**CVSS (Common Vulnerability Scoring System):** A framework for scoring the severity of vulnerabilities (0-10) based on exploitability, impact, and environment.

**Cyber Kill Chain:** A framework describing the stages of a cyberattack, from initial reconnaissance to data exfiltration or system compromise.

**Data Exfiltration:** The unauthorized transfer of data from a system or network to an external location.

**Double Extortion:** A ransomware tactic where attackers encrypt data and threaten to release sensitive information publicly if the ransom is not paid.

**Exploit:** A method or code used by attackers to take advantage of a vulnerability in software or systems.

**Indicators of Compromise (IoCs):** Observable artifacts or data (e.g., IP addresses, hashes, domain names) that signal a potential security breach.

**Malware:** Malicious software designed to infiltrate, damage, or disrupt systems, including viruses, ransomware, and spyware.

**MITRE ATT&CK:** (Adversarial Tactics, Techniques and Common Knowledge) is a framework, set of data matrices, and assessment tool developed by MITRE Corporation to help organizations understand their security readiness and uncover vulnerabilities in their defenses.

**Phishing:** A social engineering attack where victims are tricked into providing sensitive information through fraudulent emails or websites.

**Ransomware:** A type of malware that encrypts a victim's data and demands a ransom payment for its release.

**Reconnaissance:** The phase of an attack where threat actors gather information about a target to identify vulnerabilities and plan their attack strategy.

**Threat Actor:** An individual, group, or organization conducting malicious activities in cyberspace, such as hackers, hacktivists, or state-sponsored groups.

**Tactics, Techniques, and Procedures (TTPs):** The specific methods and behaviors used by threat actors to achieve their objectives during an attack.

**Vulnerability:**

A flaw in software, hardware, or systems that attackers can exploit to gain access, disrupt operations, or steal data

**Zero-Day Vulnerability:** A software vulnerability that is unknown to the vendor and exploited by attackers before a patch is available.

CyberBulwark

## APPENDICES

### *Appendix A: Members contribution to the exercise*

S/N	NAME	CONTRIBUTION
1	Ololade Elizabeth Adesagba	Information Gathering, Analysis and Editorial
2	Oluwaseyi Adebayo	Information Gathering, Threat Landscape and Threat Profile
3	Muizz Babatunde Majeed	Sprint Leader 1, Reporting.
4	Dike promise Chimamanda	Information Gathering
5	Shado Peculiar Unini	Information Gathering, Threat Landscape, Risk Assessment
6	Etinosa Imafidon	Vulnerability Research
7	Daniel Owoeye-wise	Sprint Leader 2, Threat Landscape and Threat Profile
8	Alli-Balogun, Luqman Damilare	Analysis, Reporting and Editorial
9	Motunrayo Sanusi	Threat Landscape, Presentation

## Appendix B: Attendance

S/N	NAME	1/19	1/20	1/21	1/22	1/23	1/24	1/25	1/26	1/27	1/28	1/29	1/30	1/31
		Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri
1	Ololade Elizabeth Adesagba	P	P	P		P	P		P			P	P	P
2	Oluwaseyi Adebayo	P	P	E		E	P		P			P	P	P
3	Muizz Babatunde Majeed	P	P	E		P	P		P			P	P	P
4	Dike Promise Chimamanda	P	P	E		E	E		E			P	P	P
5	Shado Peculiar Unini	P	P	P		P	P		P			P	P	P
6	Etinosa Imafidon	P	P	P		P	P		P			P	P	P
7	Daniel Owwoeye-Wise	P	P	P		P	P		P			P	P	P
8	Alli-Balogun, Luqman Damilare	P	P	P		P	P		P			P	P	P
9	Motunrayo Sanusi	P	P	P		P	P		E			P	P	P

### **Codes:**

P- Present

E- Excused Absence

**NB:** On the blank days, we had no meetings scheduled.