Key Insights: January, 2024

Foresiet

Global Cybersecurity Trends

January 2024

A Vision Rooted in Collective Resilience

> In the face of evolving cyber threats, our commitment is not just to protect organizations but to empower the global community. This report is a testament to our proactive approach, offering insights that go beyond mere security measures. Together, let's build a resilient digital future. The Cyber Report we're providing is a valuable resource for individuals across all backgrounds, ensuring a safer digital environment for everyone.

Mohit Kohli
Founder & CEO, Foresiet

This report is the culmination of the Founder’s steadfast commitment to community welfare and education. With meticulous attention, this document aims to provide readers with crucial situational awareness concerning cyber threats impacting the global community. The underlying vision is deeply rooted in the belief that shared knowledge is pivotal for fostering collective resilience in the face of the continually evolving landscape of digital challenges. Beyond safeguarding organizational interests, these aspirations extend to fortifying the broader community against targeted cyber campaigns.

The report stands as a tangible manifestation of that commitment, seeking to quantify global risks, provide strategic insights, and cultivate a culture of cybersecurity vigilance that transcends organizational boundaries. As we navigate through this comprehensive analysis, it becomes abundantly clear that he envisions a safer digital environment, wherein individuals, businesses, and nations are equipped with the requisite tools and understanding to effectively combat cyber threats.

Foresiet

This report is intended for these roles:

- Chief Information Security Officer
- Director of Cyber Security
- Cyber Security Architect
- Cyber Security Analyst
- Cyber Security Engineer
- Cyber Security Consultant
- Cyber Security Manager
- Information Technology Security Specialist
- Information Security Manager
- Director of Information Technology

Verticals:

Accounting & Financial Services, Apparel & Fashion, Automotive, Aviation & Aerospace, Banking, Business Consulting and Services, Civic & Social Organization, Construction, Consumer Services, Defense & Space, Computer & Network Security, Delivery Services, Education, Environmental Services, Farming, Financial Services, FMCG, Furniture, Gov, Health Care, Hospitality, Human Resources Services, Industrial Engineering, Information Technology & Services, Insurance, International Trade & Development, Legal Services, Logistics & Supply Chain, Luxury Goods & Jewellery, Management Consulting, Manufacturing, Membership Organizations, Mining & Metals, Museums & Institutions, Music, Nonprofit Organization Management, Oil & Energy, Packaging & Containers, Printing, Public Policy, Publishing, Real Estate, Recreation, Research, Restaurants, Retail, Apparel & Fashion, Sports, Wholesale, Telecommunications, Transportation, Utilities, Wellness & Fitness, and Other.

Executive Summary – Cybersecurity Landscape Analysis: January 2024

The January 2024 Cybersecurity Analysis provides a comprehensive view of the evolving threat landscape. The Threat Analytics section outlines a significant global surge in breaches, with peaks and troughs indicating the necessity for adaptive security measures. Notable threat actors, such as Lockbit3 and Akira, contribute to diverse tactics ranging from ransomware to infiltration attempts.

Examining the Impact on Company Size reveals a correlation between organization size and breach occurrences. Small and mid-sized companies face heightened vulnerabilities, emphasizing the need for tailored cybersecurity strategies. Larger enterprises exhibit varying breach frequencies, potentially due to robust cybersecurity infrastructures.

The Impacted Country analysis underscores the global nature of cyber threats, with the United States being a primary target. European nations, particularly France and the United Kingdom, show significant impacts, emphasizing the need for globally informed cybersecurity strategies. The top 5 most breached countries collectively represent a substantial portion of incidents, necessitating targeted measures.

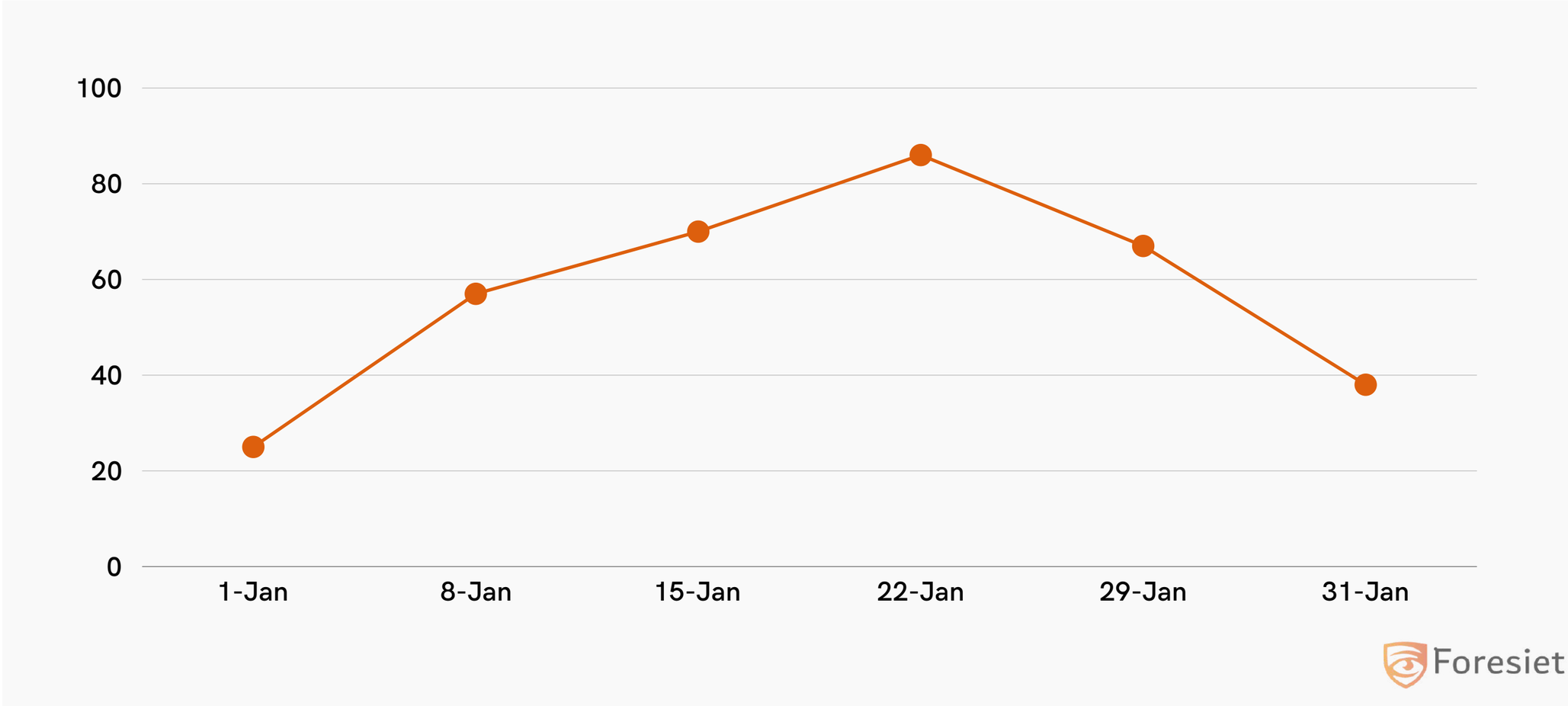
The Impact on Industry segment highlights varying degrees of cybersecurity impact across sectors. Manufacturing consistently faces challenges, while the healthcare sector and information technology & services experience notable impacts. The report emphasizes the critical importance of industry-specific cybersecurity strategies to enhance overall resilience against evolving threats.

Introduction

This report serves as a comprehensive analysis, providing essential insights into the nuances of the evolving cyber threat landscape in January 2024. By examining the trends, threat actor activities, vulnerabilities, and impacts on various sectors, it aims to equip stakeholders with crucial information necessary to bolster cybersecurity defences and adapt strategies to effectively counter the evolving threat landscape.

Threat Trend Weekly

Weekly, there were occurrences of cyber threats throughout the month of December.



In the month of January 2024, the global landscape witnessed a noteworthy escalation in cybersecurity breaches, necessitating a meticulous examination of week-to-week variations. With 197 reported breaches, January served as a baseline for subsequent evaluations. By the close of the first week, the breach count surged to 276, indicating a substantial 40.10% increase from the preceding month (December 2023).

Systematically analyzing the data reveals significant fluctuations on a week-to-week basis. The second week we experienced a decrease of 17.39%, with breaches totaling 228 incidents–a momentary respite promptly disrupted by a sharp 12.72% increase in the third week, culminating in 257 breaches. The final week saw a modest reduction to 246 breaches, reflecting a 4.28% decrease from the prior week. Of particular note is the apex of breaches occurring in the third week of January, with 257 incidents, marking a critical juncture in the monthly timeline. The percentage change from the first week to the third week reached 30.80%, emphasizing the heightened intensity of cyber threats during this period.

In the realm of global cybersecurity, these week-to-week fluctuations underscore the imperative for adaptive security strategies. As organizations navigate this dynamic landscape, a comprehensive analysis of breach trends becomes paramount, providing insights into potential vulnerabilities and guiding the implementation of proactive measures to fortify against evolving cyber threats.

Threat Trend Weekly

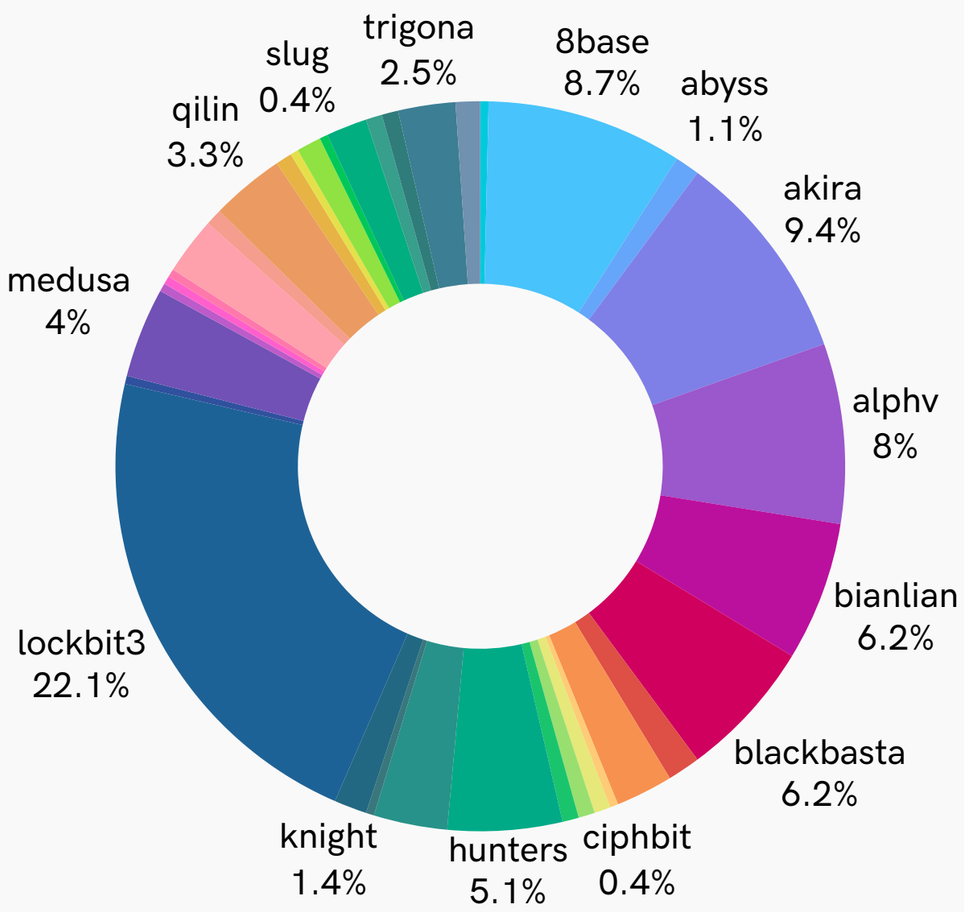
Quick Threat Analytics Reference:

- Significant threat surge on January 15, 2024, with breaches reaching 276–a 40.10% increase from December 2023.
- Notable surge in threats during the week of January 15th - 21st, 2024.
- The peak breach count on January 22nd - 28th, 2024, signifies a critical cybersecurity moment.
- Relief was observed with a decrease to 68 breaches reported on January 25, 2024. The weekly average for January stands at approximately 93 breaches.

Additional data points offer insights into fluctuations, enhancing understanding of potential vulnerabilities.

Threat Actor Groups

Popular Threat Actors



Foresiet

Threat Groups

Threat Landscape Analysis:

In January 2024, the threat landscape exhibited notable cyber activity, primarily driven by prominent threat actor groups. Lockbit3 asserted dominance, constituting a substantial percentage of the overall incidents, imposing 22.10% of the total breaches. Akira closely followed, contributing 9.42% of the breaches, indicative of its substantial presence and influence. Alphv played a notable role, representing 7.97% of the breaches, signifying substantial activity within the threat landscape. Additionally, 8base and Bianlian, each accounted for 8.70% and 6.16% of the breaches, respectively, showcasing their significance in contributing to the overall threat scenario.

Among other threat actors who have been active in the top 10, including Blackbasta, Hunters, Medusa, Incransom, and Qilin, a diverse range of cyber threats was identified. These groups, together, contributed significantly to the overall threat landscape, emphasizing the necessity for tailored cybersecurity strategies to effectively counteract specific threats and enhance organizational resilience.

Further analysis revealed fluctuations in the tactics employed by these threat actor groups, ranging from ransomware attacks to infiltration attempts. Understanding these tactics is crucial for proactive cybersecurity measures and fortifying defences against evolving threats. Additionally, ongoing monitoring and collaboration within the cybersecurity community are essential to stay ahead of emerging threat patterns. Cybersecurity strategies should adapt dynamically to the evolving threat landscape, ensuring organizations remain resilient in the face of diverse and sophisticated cyber threats.

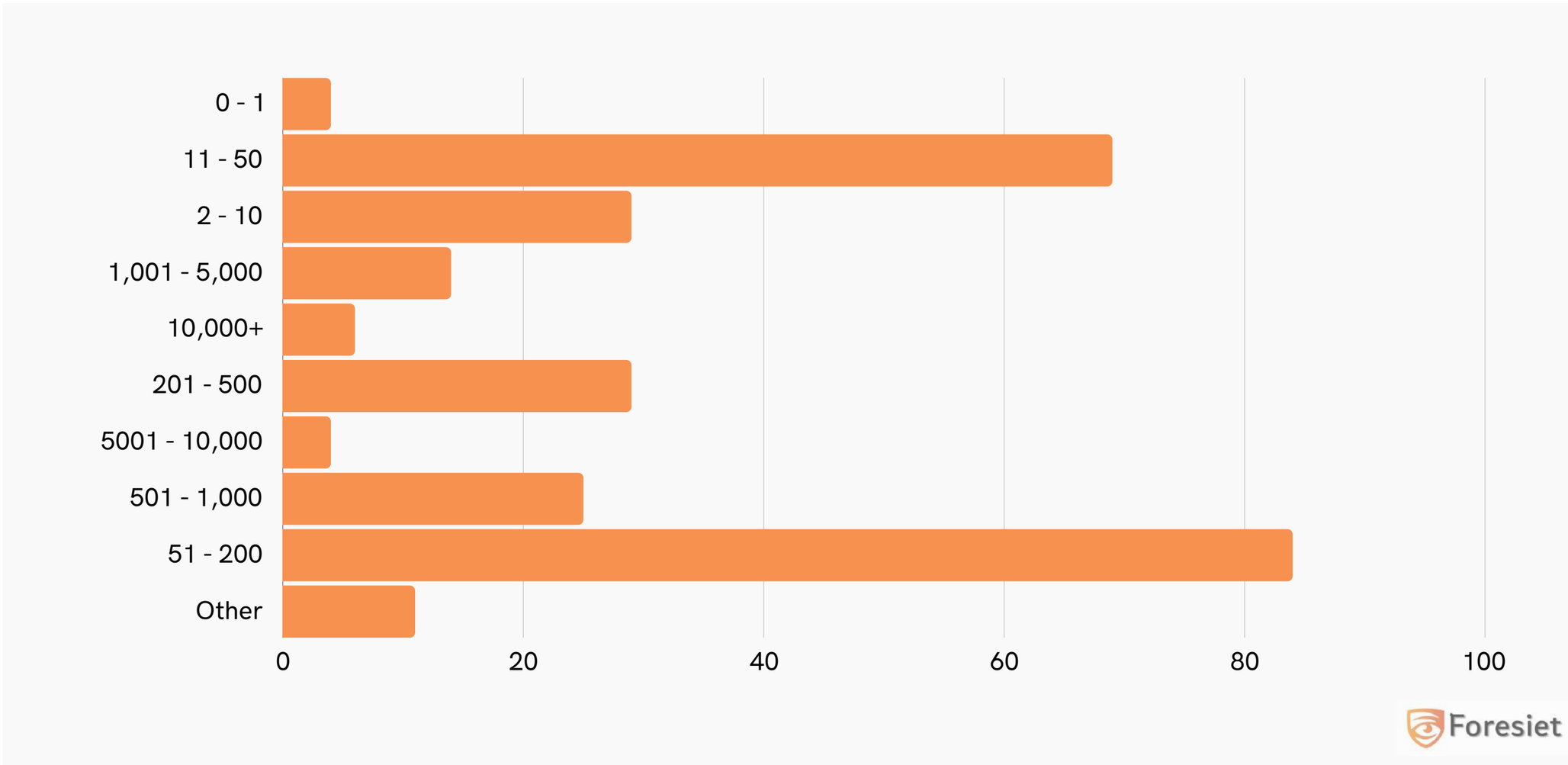
Quick Threat Analytics Reference:

- Lockbit3 emerged as the dominant threat actor, imposing a significant 22.10% of the total breaches in January 2024.
- Akira closely followed, making a substantial impact by contributing 9.42% of the breaches, while Alphv played a notable role, representing 7.97%.
- 8base and Bianlian each accounted for 8.70% and 6.16% of breaches, respectively, showcasing their significance in the threat landscape.
- Other active threat actors in the top 10, such as Blackbasta, Hunters, Medusa, Incransom, and Qilin, collectively contributed significantly to the overall threat landscape.
- The threat landscape exhibited diverse tactics, ranging from ransomware attacks to infiltration attempts, emphasizing the need for adaptive cybersecurity strategies.

Impact on Company Size

Company Employee Size

Employee size in the organization and its corresponding Threat count



Cybersecurity Incidents Overview: January 2024

In the January 2024 cybersecurity analysis, company size played a pivotal role in influencing breach occurrences. Small-sized companies, with 0-1 employees, reported 4 incidents, constituting approximately 1.45% of total breaches. This underscores potential vulnerabilities in smaller organizational structures, highlighting the need for reinforced cybersecurity measures.Mid-sized companies (11-50 employees) faced a substantial cybersecurity challenge, recording 69 incidents, representing around 25% of total breaches. This suggests an increased attractiveness as targets or specific vulnerabilities within this size range.

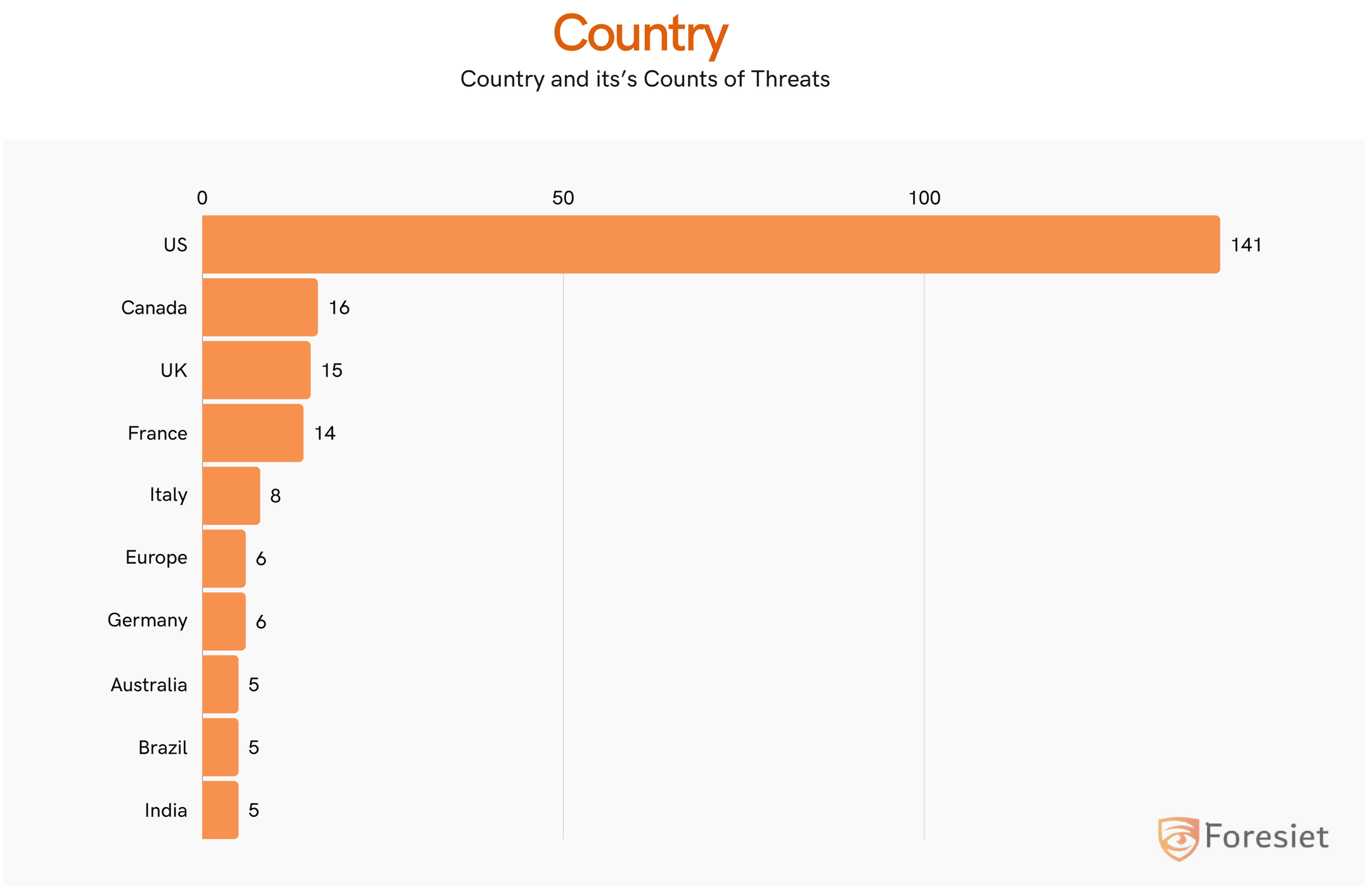
Larger enterprises exhibited varying breach frequencies. Companies with 1,001-5,000 employees reported 14 breaches, constituting approximately 5.07% of total breaches, while those with 10,000 or more employees experienced 6 breaches, making up approximately 2.17% of total breaches. This lower incidence in larger entities may be attributed to robust cybersecurity infrastructures.

This analysis underscores the need for tailored cybersecurity strategies, with small and mid-sized companies requiring heightened vigilance, while larger enterprises leverage their resources for robust defense mechanisms. Continuous monitoring and adaptive strategies remain critical in safeguarding organizations against evolving threats.

Impact on Company Size

Quick Threat Analytics Reference:

- Small companies (0-1 employees): 4 incidents, approximately 1.45% of total breaches.
- Mid-sized companies (11-50 employees): 69 incidents, around 25% of total breaches.
- Larger enterprises (1,001-5,000 employees): 14 incidents, approximately 5.07% of total breaches.
- Larger enterprises (10,000+ employees): 6 incidents, approximately 2.17% of total breaches.
- Company size influences breach occurrences; tailored cybersecurity strategies are essential.



Impacted Country

Global Breach Trends: January 2024

The analysis of cybersecurity incidents reveals a diverse impact across different countries, underscoring the global nature of cyber threats. The United States remains a primary target throughout the year, bearing the brunt of cyber threats with 141 incidents, constituting approximately 51.45% of the total breaches. Following closely, Canada experienced 16 breaches, contributing around 5.84% to the overall incidents. France, with 14 breaches, and the United Kingdom, reporting 15 incidents, represent approximately 5.11% and 5.47% of the total breaches, showcasing significant impacts in these European nations. Germany, contributing 6 breaches, constitutes approximately 2.19% of the total, while Italy, with 8 incidents, represents about 2.92%.

Other countries, such as Australia (5 breaches, approximately 1.82%), India (5 breaches, approximately 1.82%), and Brazil (5 breaches, approximately 1.82%), also experienced notable impacts, albeit to a lesser extent. The top 5 most breached countries, including the United States, Canada, France, the United Kingdom, and Italy, collectively account for a substantial portion of global cybersecurity incidents.

These varying percentages highlight the need for a globally informed cybersecurity strategy, recognizing the specific challenges and threat landscapes faced by different nations. As cyber threats continue to evolve, understanding the geographical distribution of breaches becomes imperative for implementing targeted measures to enhance the resilience of each affected country.

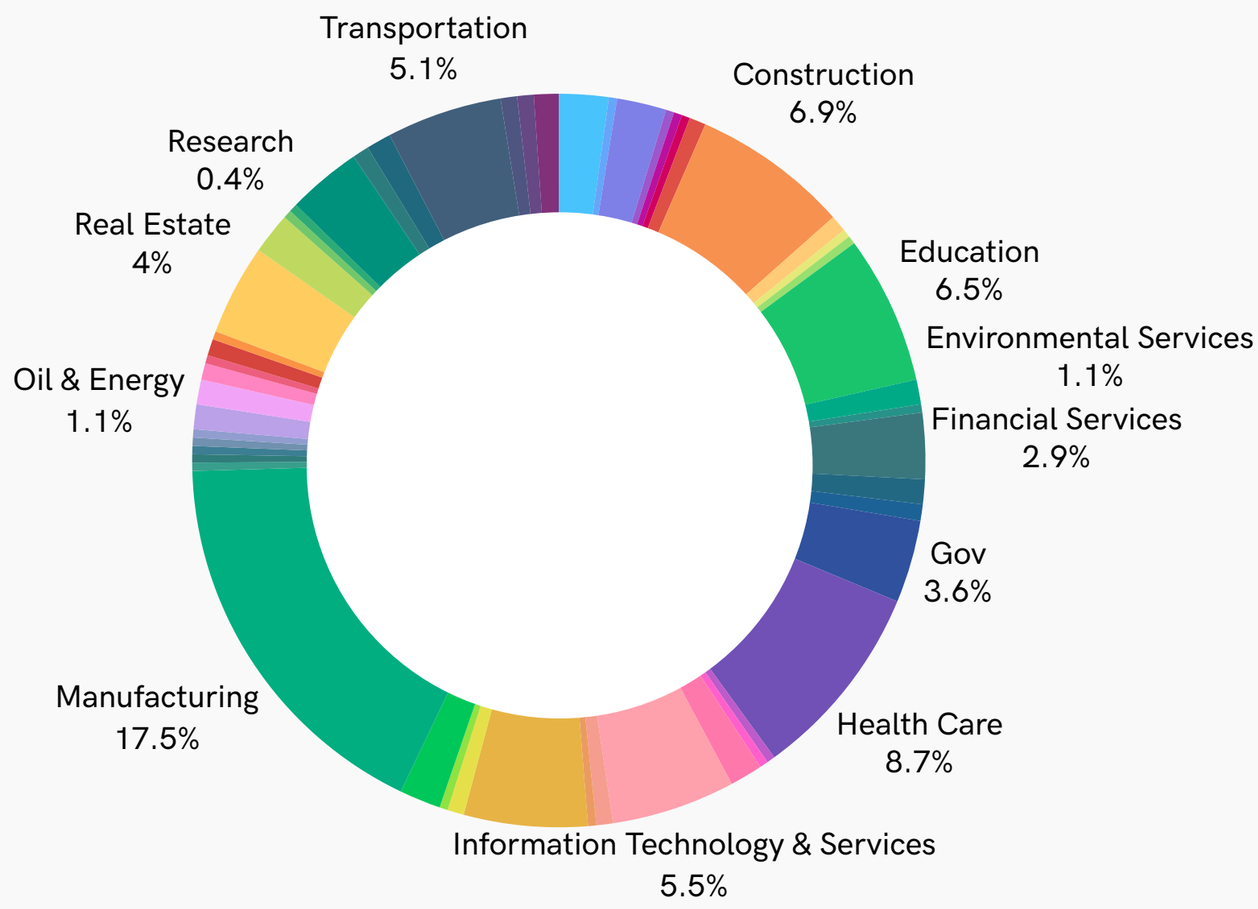
Impact on Industry

Quick Reference:

- United States Dominance: The United States stands as the primary target, accounting for over 51% of the total cybersecurity incidents.
- European Significance: France and the United Kingdom showcase significant impacts in Europe, contributing around 5.11% and 5.47% of total breaches, respectively.
- Top 5 Most Breached Countries: The top 5 most breached countries include the United States, Canada, France, the United Kingdom, and Italy, collectively representing a major share of global cybersecurity incidents.
- Continental Variances: Europe emerges as a focal point, while North America faces challenges primarily driven by the United States and Canada. Other regions, including Australia, India, and Brazil, experience notable but comparatively lesser impacts.
- Global Perspective: The United States maintains consistent prominence as a primary target, emphasizing the need for a globally informed cybersecurity strategy to address diverse challenges across nations and continents.

Top Targeted Industries

Industry & no of threats



Impact on Industry

January 2024 Industry Breach Insights:

The impact of cybersecurity incidents spans across various industries, with distinct patterns emerging from the data analysis. Notably, the manufacturing sector appears as one of the consistently affected industries, accounting for a substantial 17.39% of the total breaches. This sector's vulnerability underscores the need for heightened cybersecurity measures within manufacturing organizations to safeguard critical processes and sensitive information.

The health care industry experienced a notable impact, with 24 incidents constituting approximately 8.70% of the total breaches. This highlights the cybersecurity challenges faced by organizations in the health care sector, emphasizing the importance of securing sensitive patient data and maintaining the integrity of healthcare operations. Other industries with significant impacts include construction, representing 6.88% of total breaches, and information technology & services, contributing 5.80%. These sectors face unique cybersecurity challenges that necessitate industry-specific strategies to mitigate risks effectively.

On the contrary, certain industries, such as civic & social organization, luxury goods & jewellery, and membership organizations, experienced comparatively lower impacts, each contributing only 0.36% of the total breaches. While these industries are not immune to cybersecurity threats, the lower incident counts may indicate a need for targeted cybersecurity measures tailored to the specific challenges faced by these sectors

In conclusion, the data analysis reveals varying degrees of impact on different industries, with manufacturing consistently emerging as one of the most affected sectors over time. This underscores the critical importance of implementing robust cybersecurity strategies tailored to the specific needs and vulnerabilities of each industry to enhance overall resilience against evolving cyber threats.

Quick Reference: January 2024 Industry Breaches

- The manufacturing sector consistently faces cybersecurity challenges, contributing to 17.39% of total breaches.
- The healthcare industry experienced a significant impact, with 24 incidents accounting for approximately 8.70% of total breaches.
- Construction emerged as another industry with notable cybersecurity concerns, representing 6.88% of total breaches.
- Information Technology & Services recorded a substantial impact, contributing 5.80% to the total breaches.
- Other industries, including civic & social organizations, luxury goods & jewelry, and membership organizations, experienced comparatively lower impacts, each contributing only 0.36% of the total breaches.

Dark Web Alert: January 2024

Quick Highlight:

- Breaches Across Industries: Major corporations like Toyota Israel, Zara, and American Arms Company faced data breaches, while other entities such as upstox.com, Bitmain.com, and government portals in different countries also experienced cyber-attacks.

- Ransomware and Malware Incidents: Various ransomware attacks (LockBit, Alphv Ransomware, WereWolves, STORMOUS) targeted diverse sectors, compromising critical data and emphasizing the urgent need for stronger cybersecurity measures.

- Geopolitical Influence and Ideologically Motivated Attacks: Several incidents involved groups targeting organizations and entities supporting certain geopolitical stances, such as attacks on Israel supporters, Israeli-Gaza conflict supporters, and breaches affecting government systems and defense sectors.

- Sophisticated Cyber Weapons and Tactics: The emergence of new malware strains (Lust Stealer, CStealer), ransomware variants, and botnets (Krypton Networks, KoxyBotnet) demonstrated the continuous evolution of sophisticated cyber weapons and techniques.

- Global Reach of Threats: Cyber-attacks were not limited to specific regions; they affected nations worldwide, including Russia, UAE, Taiwan, Czech Republic, Philippines, and others, underlining the global scope and impact of cyber threats.

- Calls for Heightened Vigilance: Various groups claimed responsibility for breaches, warned of upcoming attacks, and emphasized the need for increased cybersecurity vigilance across industries, governments, and critical systems.

Incident Detail

- Nation-state attack on Microsoft: Microsoft identified a cyberattack by the Russia-linked group Nobelium, targeting their cloud-based email system.

- Data breaches: Several large-scale data breaches occurred, including a massive leak of 750 million Indians' personal data and a breach exposing the data of millions of Brazilians.

- In a groundbreaking development, a cybersecurity researcher has recently exposed a massive database comprising 26 billion leaked records, impacting potentially millions, if not billions, of individuals. This unparalleled breach has earned the title of the "mother of all breaches," setting a historic precedent in the field of cybersecurity.

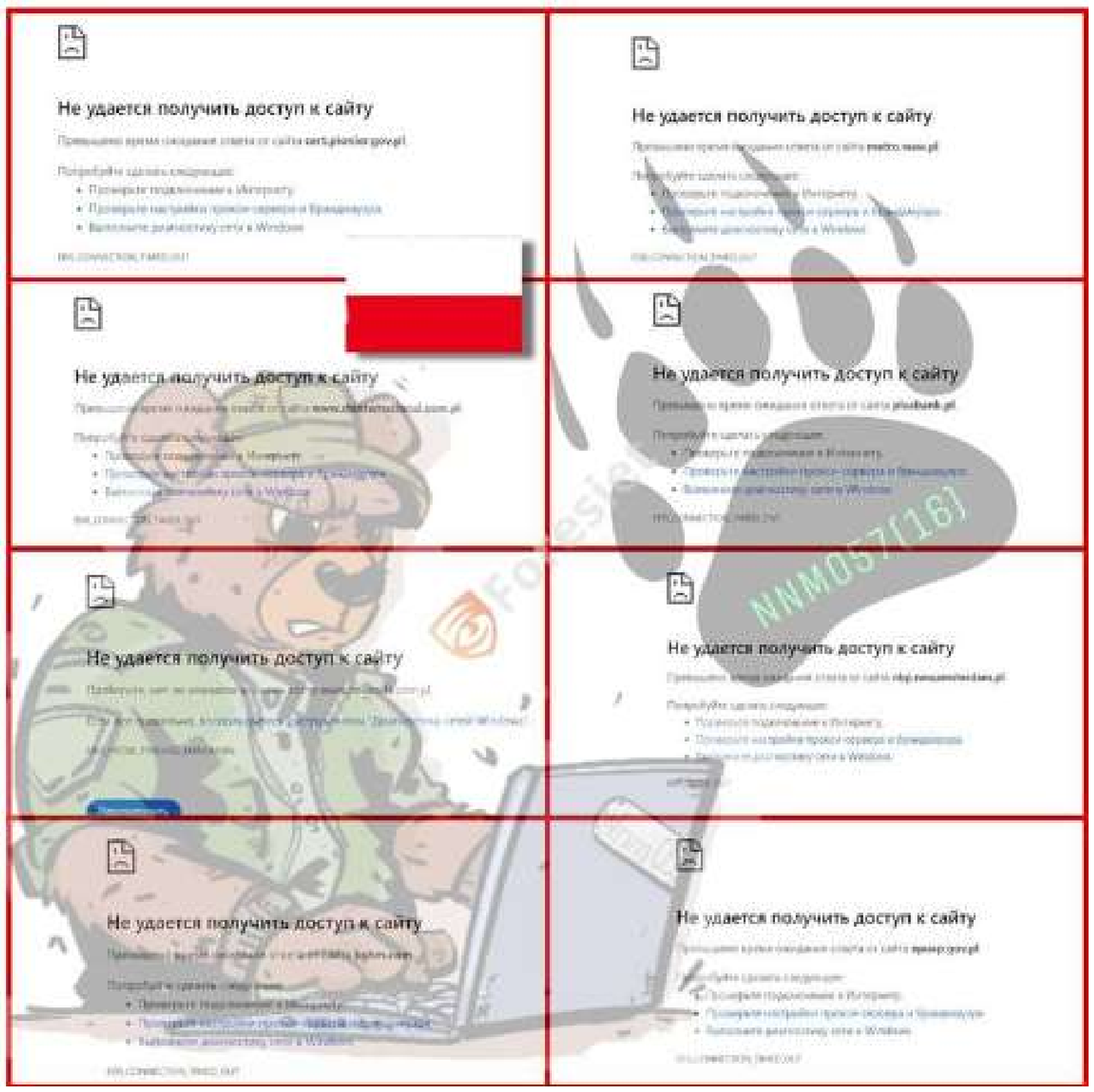
- Anonymous Sudan claims responsibility for a recent cyber-attack on the UAE, targeting 167 domains, including 120 government sites. The attacks have led to significant disruptions in various organizations, and the extent of the damage is still being assessed. Motivations behind the sustained campaign remain undisclosed.

Incident Detail

- NoName intensifies cyber-attacks on Finland, targeting key entities such as Traficom, the Cybersecurity Center, and the Finnish Railways Agency. The group's motives and specific objectives remain undisclosed as they persist in their campaign against Finnish organizations.

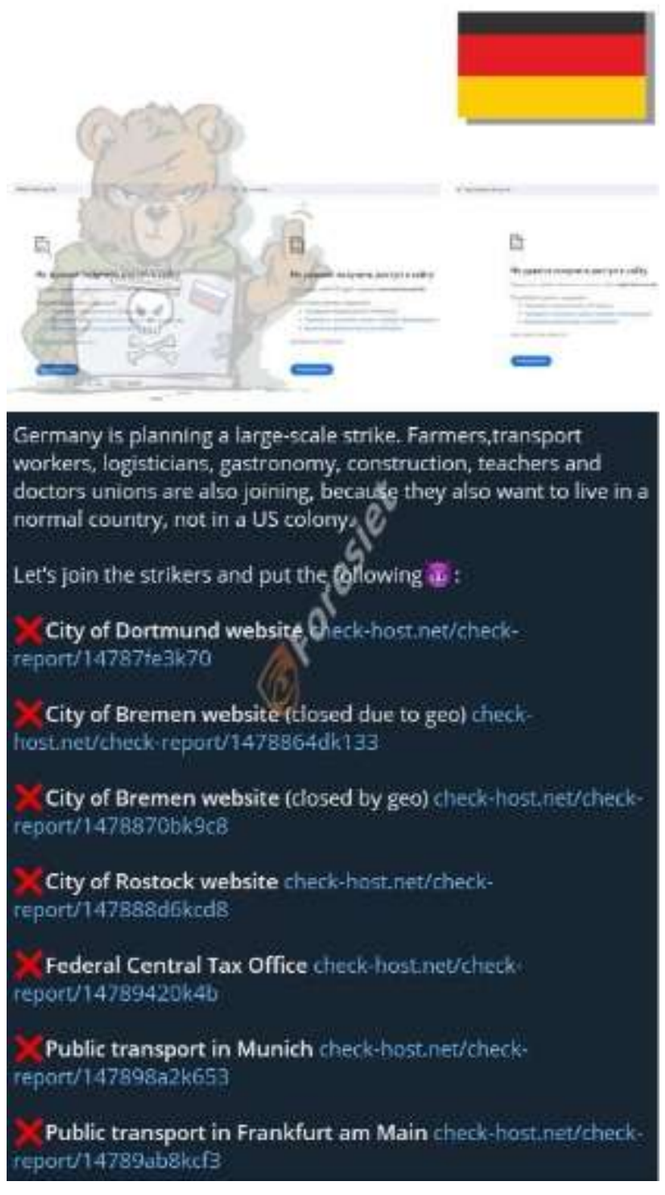
- Anonymous, led by @YourAnonTl3x, has claimed responsibility for a cyber-attack on Guatemala's presidential website, resulting in its unavailability. The impact of the attack has left the website inaccessible to users, and the motivation behind the incident remains undisclosed. [Confidential, details not to be disclosed publicly]

- Poland experiences a surge in cyber-attacks orchestrated by the NoName threat group, impacting critical sectors including railway carrier ticket purchases, energy company Polska Grupa Energetyczna SA authorization, Polish Sejm, and the Port of Gdynia.Lime, the San Francisco-based transportation company, faced a 2-hour service outage, impacting its electric scooters, bikes, and mopeds.



Incident Detail

NoName continues its cyber attacks on critical Ukrainian organizations, including Euro-Reconstruction Ltd, Accordbank, Zaporizhzhya Titanium-Magnesium Plant, State Tax Service, Central Interregional Tax Administration, Western Interregional Tax Administration, and Main Directorate of the State Tax Service in Kyiv.



NoName intensifies cyber attacks targeting multiple websites in Germany, including the City of Rostock, City of Bremen, Authorization of City of Bremen, City of Dortmund, Federal Central Tax Office, Munich Transport Company, Rhine-Main Transport Association, and Verkehrsverbund Großraum Nurnberg. These attacks pose a substantial threat to Germany's digital infrastructure, necessitating a comprehensive investigation into the motives behind targeting specific entities.

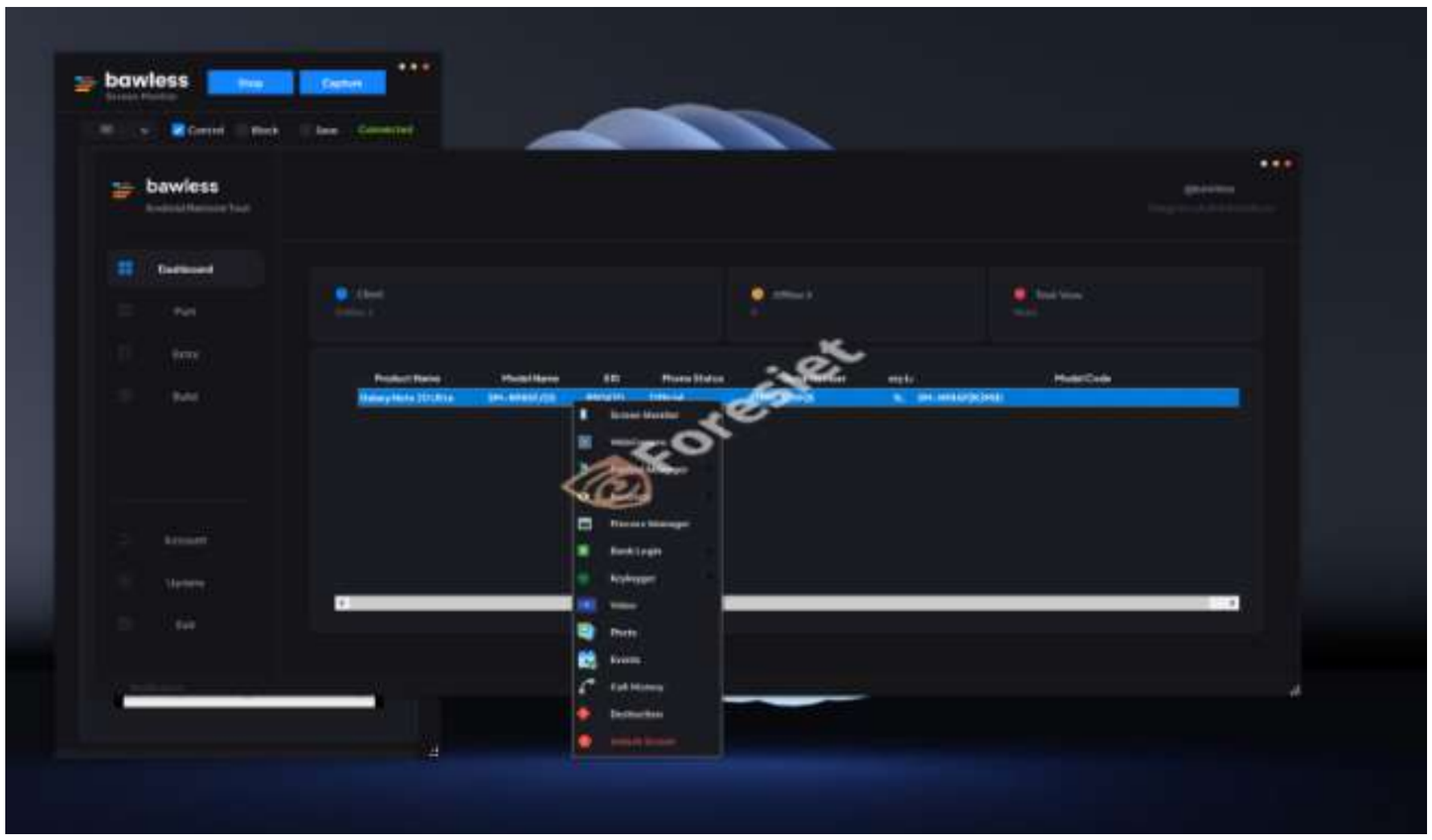
Unauthorized Admin Access Sale: A threat actor, identified as cnHunter, is reportedly selling unauthorized admin access to an undisclosed African bank. The actor claims access to 1843 customer records, including names, account numbers, phone numbers, and more. This incident raises serious concerns about the security of customer data, emphasizing the need for immediate action to mitigate potential risks and enhance overall cybersecurity measures.

Incident Detail

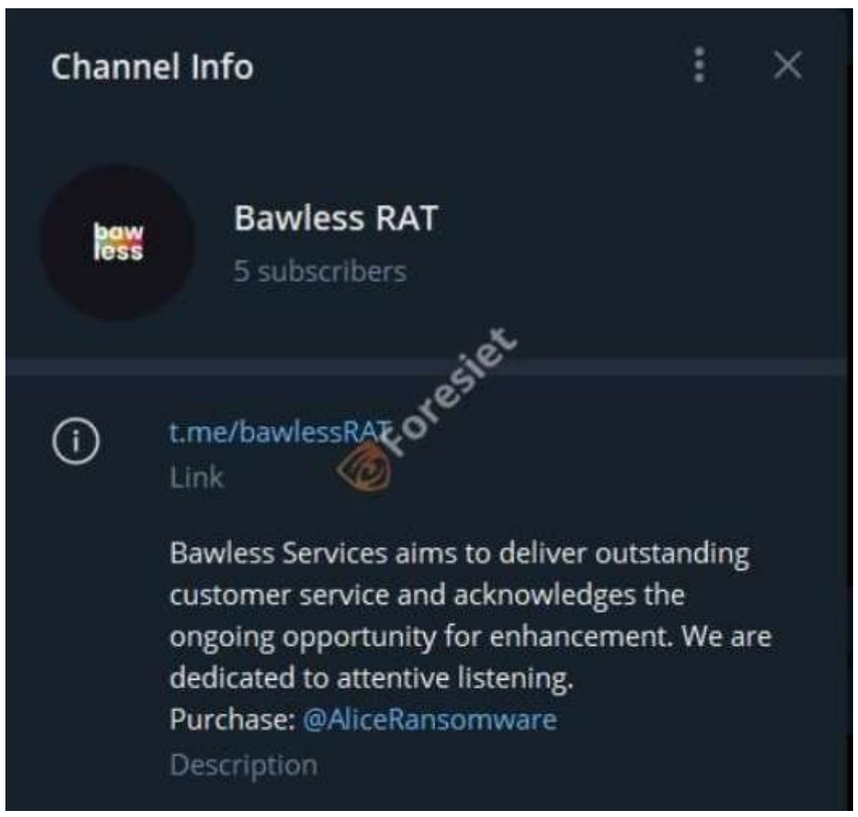
Sale of 228M Chinese Customer Records: A threat actor is advertising the sale of 228 million Chinese customer records, comprising sensitive information such as names, phone numbers, social codes, company details, industries, financial data, addresses, and cities. The sale, which includes a vast amount of personal data, poses a significant risk to individuals' privacy and highlights the ongoing challenges in safeguarding sensitive information.

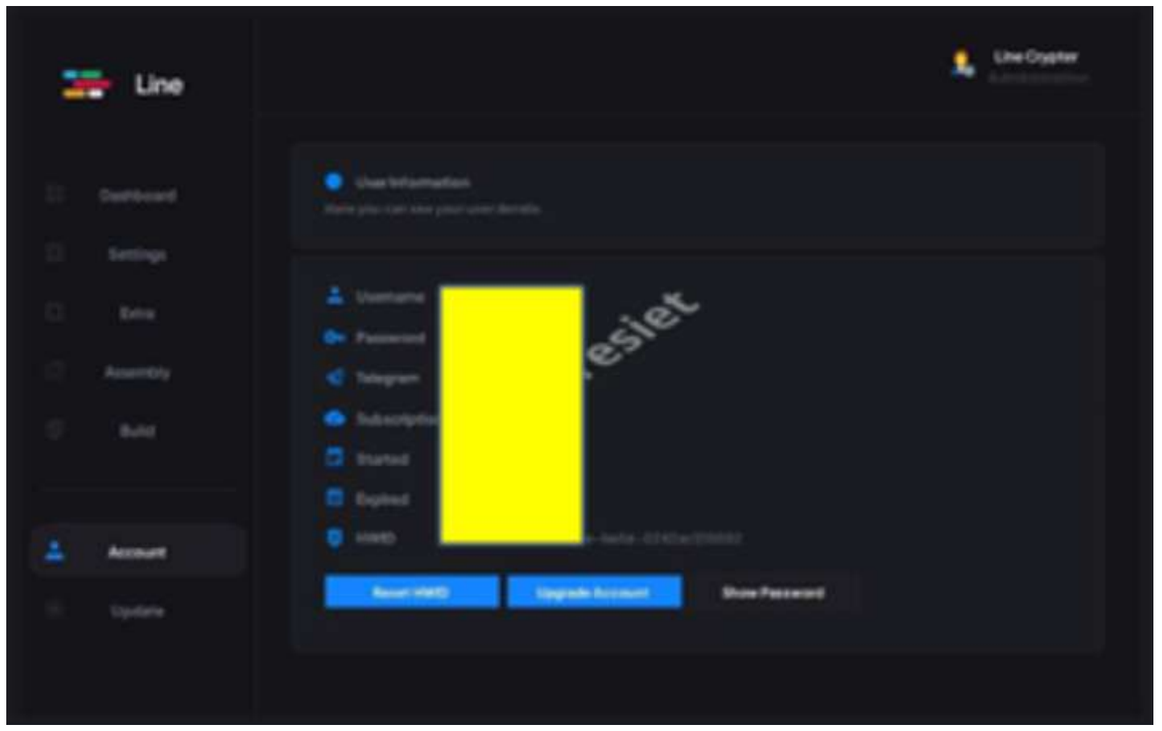
Sale of High-Quality OTPs: A threat actor is advertising the sale of high-quality One-Time Passwords (OTPs) for various countries, including Russia, Malaysia, the United States, and Indonesia. These OTPs can be utilized for applications such as KFC, Netflix, DisneyHotstar, McDonald's, Burger King, Binance, Twitter, ProtonMail, and more. The actor accepts payments in XMR (Monero), LTC (Litecoin), and BTC (Bitcoin), with prices starting from $0.5. Bulk purchases are available at discounted rates, raising concerns about potential misuse and unauthorized access.

Incident Detail



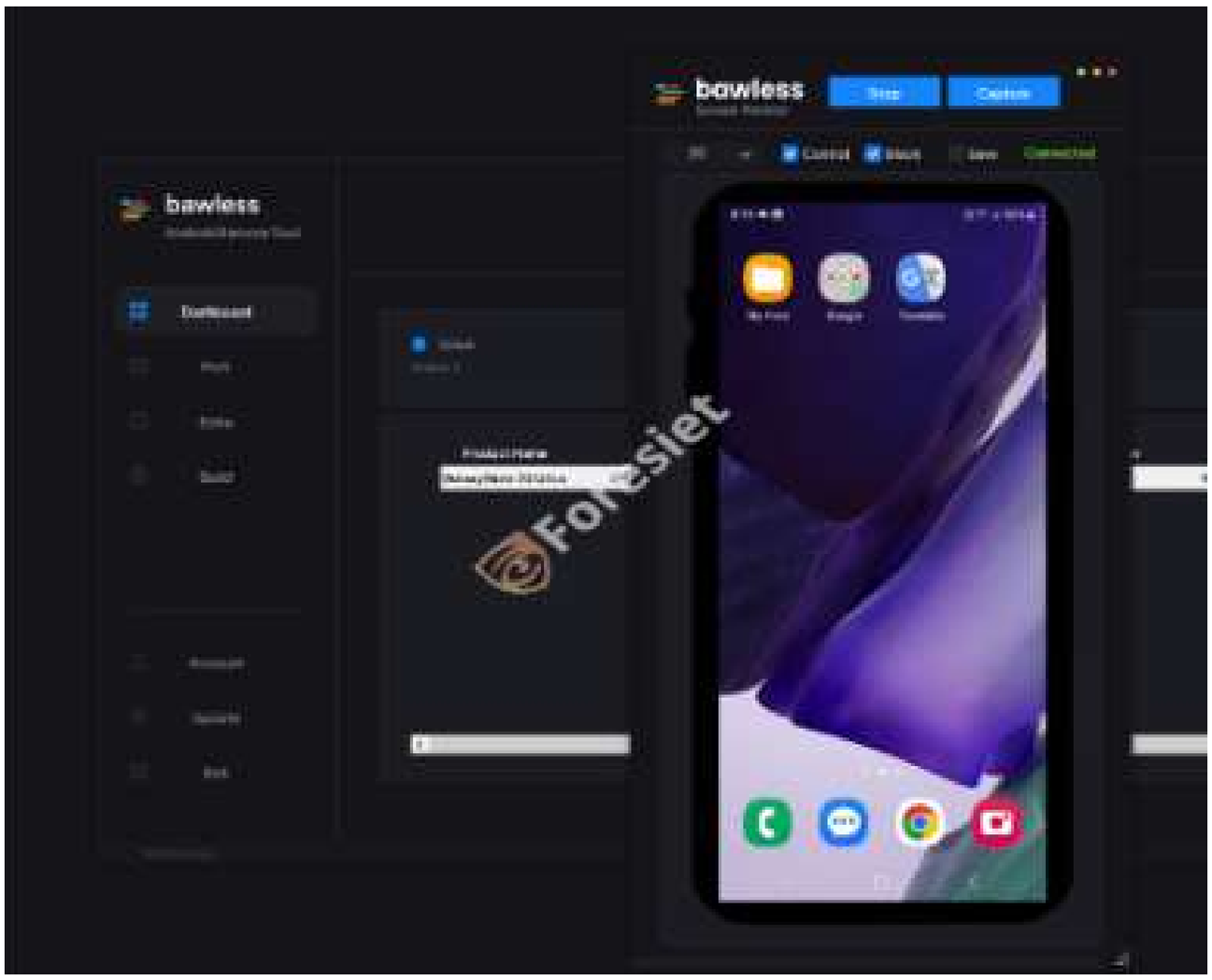
The emergence of Bawless Android RAT (Remote Access Trojan), specifically in its Version 2.2024, presents a noteworthy threat in the recent cyber landscape. This Android-targeting remote control tool boasts the ability to install directly on devices without requesting permissions, leveraging Mark of the Web (MOTW) bypass techniques. Priced at $2300, it accepts payments in popular cryptocurrencies such as BTC, ETH, LTC, and USDT, offering a full version along with the source code. Each client reportedly receives a unique stub, enhancing the longevity of payloads. The associated Telegram channels provide updates, support, and insights into the Android RAT's usage, while the GitHub repository offers further technical details. Additionally, potential connections to Luxury Crypter raise concerns, requiring further analysis. Organizations and users are advised to remain vigilant, implement updated security measures, and avoid engaging with potential threats associated with Bawless Android RAT.





Foresiet

Incident Detail



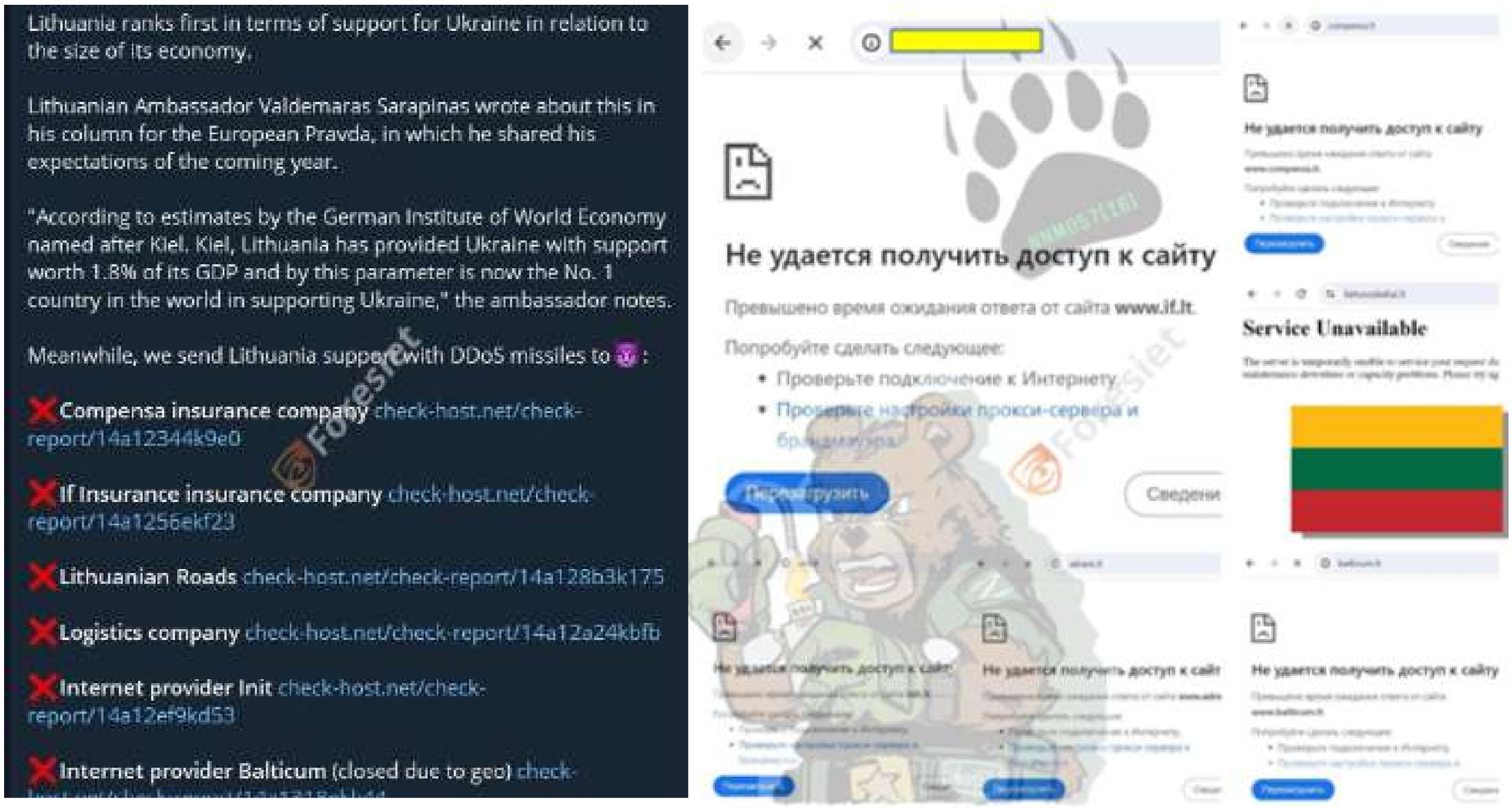
Zer0Day Lab has recently launched new cyber tools, including a CobaltStrike License for 3 users with web access priced at £500 GBP, Shellter Pro Plus v8.4 (x86 & x64) also priced at £500 GBP, and Nighthawk v2.4 Cracked available for £250 GBP. For further information or inquiries, individuals can contact the provided channel @zerosuppbot. This development raises concerns about potential misuse of these tools in cyber threats and underscores the ongoing challenges in cybersecurity.

Incident Detail

In response to Bahrain's support for the US initiative against Houthi rebels in the Yemeni conflict, the Anonymous Collective has initiated cyber attacks targeting prominent Bahraini news outlets. The affected organizations include Akhbar al-Khaleej, Al-Ayam, Gulf News Daily, and Al-Bilad. This cyber offensive is emblematic of a digital protest against Bahrain's geopolitical stance, and the situation is actively being monitored to assess its impact on the region and potential repercussions in cyberspace. The collective's actions underscore the growing intersection of cyber activities and international relations, prompting concerns about the broader implications on digital security. Key hashtags such as #Cyberattack, #Bahrain, #DDoS, #YemenConflict, #USA, #MiddleEastConflict, and #MiddleEast are emerging in discussions surrounding this incident. As the situation unfolds, there will likely be increased scrutiny on the evolving dynamics between cyber activities and geopolitical developments in the Middle East.

In a concerning development, Lithuania, recognized for its substantial support to Ukraine relative to its GDP, is now grappling with a significant cyber threat. The elusive threat group known as NoName has recently claimed responsibility for a series of Distributed Denial of Service (DDoS) attacks targeting key Lithuanian entities. The entities affected include Compensa Insurance Company, If Insurance Company, Lithuanian Roads, a logistics company, Internet Provider Init, and Internet Provider Balticum (Closed - Geo Restriction).

Incident Detail



- NoName's assertion of responsibility adds a layer of complexity to the situation, hinting at a potential motive linked to ongoing geopolitical events. As a precautionary measure, organizations in the region are being advised to fortify their cybersecurity measures to effectively counter and mitigate potential risks posed by these cyber attacks.

- The specific targets and URLs affected by the DDoS attacks include Compensa Insurance Company, If Insurance Company, Lithuanian Roads, the logistics company, Internet Provider Init, and Internet Provider Balticum (Closed - Geo Restriction). These organizations are encouraged to conduct thorough checks on their website performance and response, utilizing online monitoring tools to ensure the integrity and availability of their online platforms.

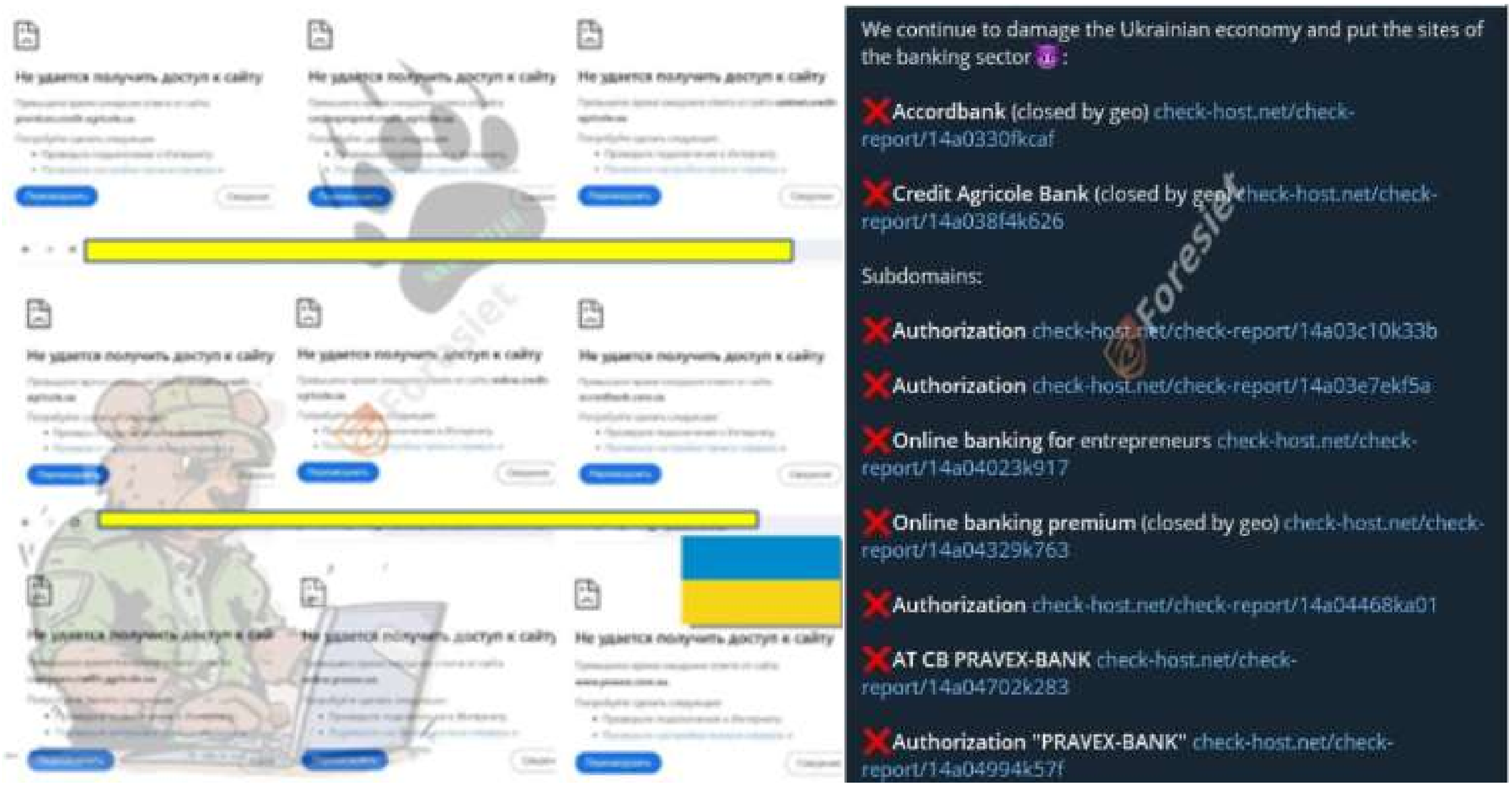
- The threat group, NoName, is identified by its utilization of DDoS attacks as its preferred method, and their acknowledgment of responsibility raises concerns about the potential geopolitical motivations behind these cyber assaults. This incident serves as a stark reminder of the susceptibility of nations to cyber threats, especially against the backdrop of evolving geopolitical dynamics.

Incident Detail

Anonymous Sudan has claimed responsibility for a significant cyber-attack on Israeli ports, targeting vital infrastructure including ISRAEL PORTS DEVELOPMENT and ASSETS COMPANY LTD and Haifa Port Company Ltd. The attack aimed at disrupting network devices, administration systems, servers, and endpoints, impacting the digital health of these crucial entities. The threat actor has also hinted at future targets, notably Israel's Credit Card Company CAL. Key hashtags circulating include #CyberAttack, #IsraelPorts, #AnonymousSudan, and #ThreatIntel, underlining the severity of the situation. Stay tuned for updates on this evolving cyber threat.

NoName has claimed responsibility for cyber-attacks on Ukrainian financial institutions, including Acordbank, Credit Agricole Bank, and Pravex Bank. The hacktivist group executed Distributed Denial of Service (DDoS) attacks, disrupting online services and posing potential operational challenges for the targeted banks. The threat actor, NoName, is known for its hacktivist engagements. Key hashtags circulating include #CyberAttack, #NoName, #Ukraine, #FinancialInstitutions, #DDoS, and #ThreatIntel, indicating the severity of the situation. Stay tuned for updates on the evolving response to these cyber threats.

Incident Detail



A significant data breach affecting Iraqi citizens has been attributed to the threat actor known as THE-HELL. The breach, reported on Monday, January 8, 2024, at 02:11 PM (UTC), exposed sensitive information, including full names, names of family members, year of birth, exact residential addresses, and various personal details. The leaked database encompasses all governorates in Iraq, raising concerns about privacy and potential identity theft. Key hashtags circulating include #DataBreach, #Iraq, #Privacy, #ThreatIntel, #IdentityTheft, and #Cybersecurity. Stay vigilant for updates on this developing incident. [Confidential, details not to be disclosed publicly]

The cybersecurity landscape faces a notable threat as the original source code for the VENOM Remote Access Trojan (RAT) has been leaked by an actor identified as empme. This significant incident, occurring on Friday, September 1, 2023, at 02:59 PM (UTC), raises concerns about potential exploitation of vulnerabilities and unauthorized activities. VENOM RAT, renowned for providing unauthorized remote access to compromised systems, now poses an increased risk as threat actors can customize and deploy their versions of the malware. Stay informed and vigilant for developments on this critical cybersecurity issue.

Incident Detail

Charles Vera, also known as "Weep," has been apprehended on charges of money laundering following an investigation by the Bergen County Prosecutor's Office and the Dumont Police Department. The arrest, which took place on June 28, 2023, at 546 Washington Avenue, Apt. 3206, Dumont, NJ, stems from Vera's alleged involvement in darknet activities, including brokering transactions on darknet marketplaces. The charges against him include second-degree financial facilitation of criminal activity (money laundering), according to N.J.S.A. 2C:21-256(1). The investigation, initiated in September 2022, revealed Vera's interactions on darknet websites specializing in the sale of stolen personal information and his association with online fraud groups. Law enforcement executed a court-authorized search warrant at Vera's residence on June 28, resulting in his arrest without incident. Charles Vera is awaiting his first appearance in the Central Judicial Processing Court in Hackensack, NJ. It is important to note that the charge against him is an accusation, and he is presumed innocent unless proven guilty beyond a reasonable doubt.

DUMONT, NJ MAN CHARGED WITH MONEY LAUNDERING

For Immediate Release:

Bergen County Prosecutor Mark Musella announced the arrest of CHARLES VERA, charge of money laundering. The arrest is the result of an investigation conducted by the Bergen County Prosecutor's Office under the direction of Chief Jason Lore and the Dumont Police Department under the direction of Chief Brian Joyce.

In September 2022, detectives from the Bergen County Prosecutor's Office Financial Crimes Unit initiated an investigation involving the movement of funds, including cryptocurrency, on various darknet websites specializing in the sale of stolen personal identifying information. CHARLES VERA was identified as a person facilitating the transfer of funds in support of darknet activities by interacting with numerous individuals from various online fraud groups and brokering transactions with darknet marketplaces for a fee. On June 28, 2023, Bergen County Prosecutor's Office and Dumont Police Department personnel executed a court authorized search warrant at CHARLES VERA's residence, where he was located and arrested without incident.

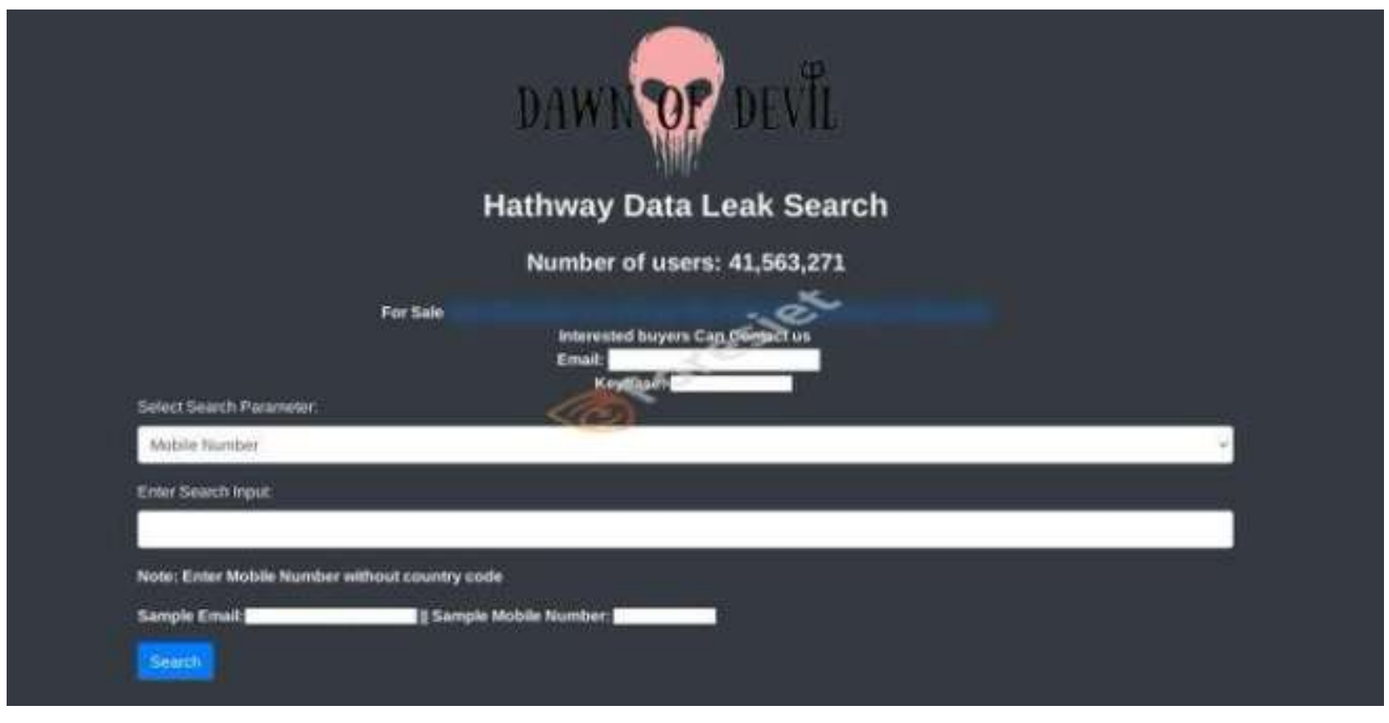
On June 28, 2023, CHARLES VERA was charged with second-degree financial facilitation of criminal activity (money laundering), N.J.S.A. 2C:21-25(b)(1). He was released on his own recognizance pending his first appearance in Central Judicial Processing Court in Hackensack, NJ.

Prosecutor Musella states that the charge is merely an accusation and that the defendant is presumed innocent unless and until proven guilty beyond a reasonable doubt. He would also like to thank the Dumont Police Department for its assistance in this investigation.

A Restoration Campaign for the Official RF Section on BreachForums, initiated by Addka72424 on November 10, 2023, seeks to rebuild the section by encouraging members to post leaks from the official list of raid forums. The objective is to restore missing threads, such as "ForeverPP Carding" and "LUPA开源社区," by verifying leaks' authenticity and contacting Addka72424 with details for consideration. Contributors are incentivized with a reward system, earning 50 to 200 credits for each topic, with the possibility of transferring to the official section and continuous support from Addka72424. The campaign, illustrated by the discovery of several threads from the list, aims to foster community collaboration and rebuild the official RF section on BreachForums.

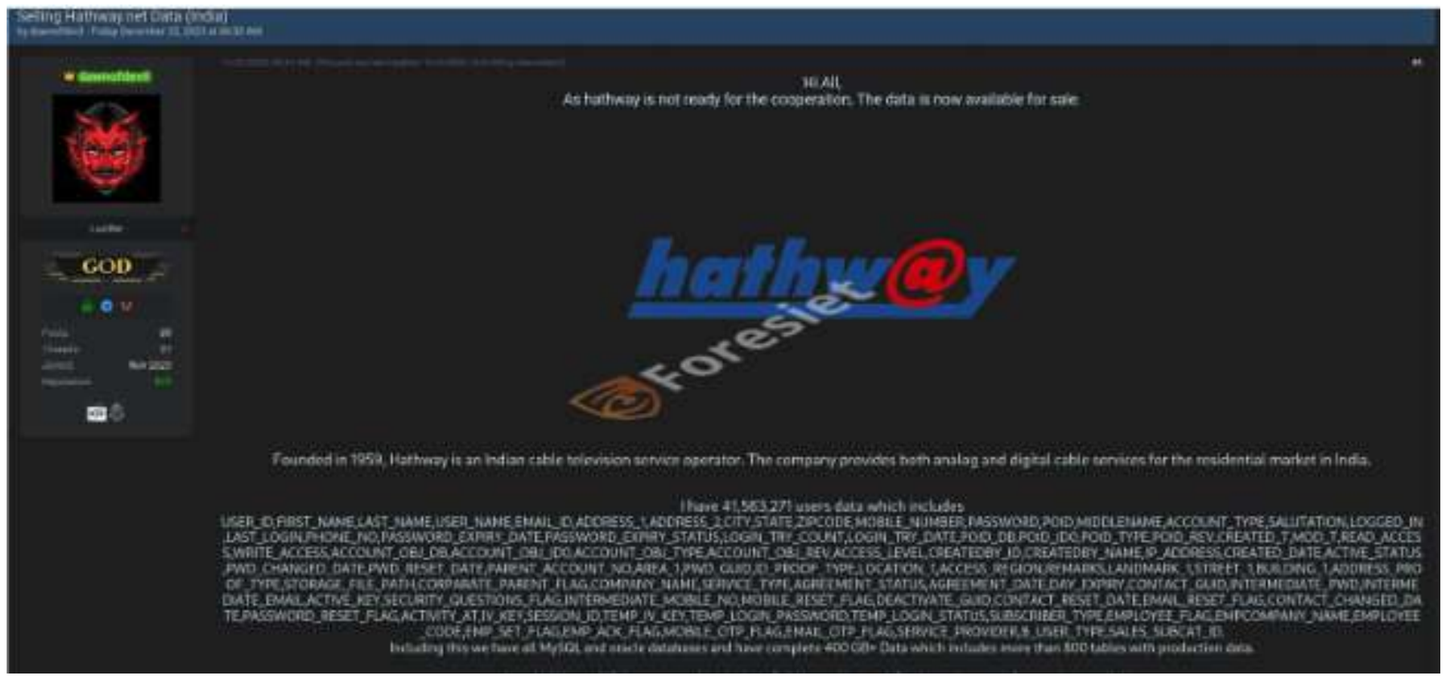
Incident Detail

Hathway, a major Indian cable TV service, faced a significant data breach in December 2023, affecting 41.5 million users. The breach, attributed to "dawnofdevil," exploited vulnerabilities in Hathway's Laravel framework. Compromised data includes sensitive user details and 4 million+ KYC documents with Aadhar and Pan card information. "Dawnofdevil" disclosed the breach on BreachForums, offering the data for $10,000 and launching a dark web portal for user account searches. Security recommendations include immediate password updates, vigilant monitoring, and enhanced data privacy practices. Users should beware of phishing attempts, update passwords, and monitor accounts for unauthorized access. Organizations are urged to conduct security audits and vulnerability assessments.



Foresiet

Incident Detail



- The threat group "NoName" launched a cyber protest targeting key transportation infrastructure in Germany, in solidarity with protesters against the German government. The focus of the attack is on disrupting services provided by major entities involved in public transportation, including National Express, Germany's bus transportation operator, and Rhine-Main Public Transportation. "NoName," known for cyber protests by government entities, aims to draw attention to the cause by disrupting normal transportation operations. [Confidential, details not to be disclosed publicly]

- The "Anonymous Collective" executed a massive cyber-attack on Legal and General, the largest insurance company in the UK, in response to perceived UK involvement in attacks on Yemen and support for Israel. The attack, employing sophisticated methods, caused significant disruption, leading to over 4 hours of downtime for the targeted websites and infrastructure, including the main, group, capital, and investment management websites. The collective's action underscores growing cyber retaliation against entities associated with geopolitical events.th geopolitical events.

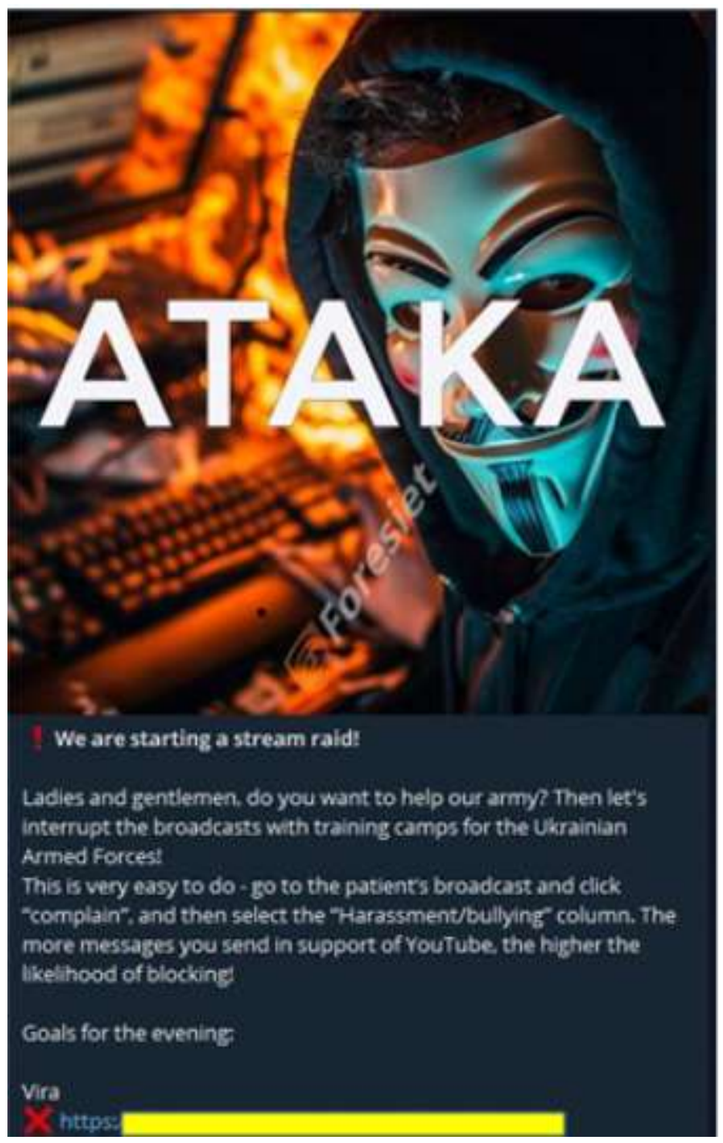
- A major data breach occurred on Trello.com, affecting 15 million accounts. The threat actor, identified as "emo," claims to be selling 15,115,516 unique lines of compromised data, including emails, usernames, full names, and additional account information. The incident highlights a significant breach of user data on the popular platform.

Incident Detail

In an ongoing cyber attack, Anonymous Sudan has targeted Bazan Group (Formerly Oil Refineries Ltd.), a major player in oil refining and petrochemicals in Israel. The attack, now lasting for over 12 hours, focuses on the digital infrastructure of Bazan Group, impacting crucial components and causing disruptions to their operations. Bazan Group, situated in Haifa Bay, Israel, holds significant economic importance as the largest oil refinery in the country. The attack's impact raises concerns about the stability of critical infrastructure and the potential economic repercussions in the region.

Incident Detail

In an ongoing stream raid, the threat group ATAKA is targeting several broadcasts, including Vira, Krayanin, Eldar from the Dnieper, Andrey Lugansky, Rural Prometheus, Edgar the Peacemaker, Shablya, and "ЗДИЧАВІЛІ В РУЛЕТЦІ." The nature and impact of the raid are not specified, but the targeted broadcasts span various content creators.



In a concerning development for the United States critical infrastructure, a threat actor has purportedly disclosed sensitive information about several major pipeline and energy companies. The leaked data encompasses company names, PGP passwords, PGP private keys, and PGP public keys, thereby posing potential security vulnerabilities for the affected entities and the wider energy sector. This breach is reported to have implications not only on the clarinet but also on the dark web, amplifying the severity of the incident. The exposure of such confidential information underscores the urgent need for heightened cybersecurity measures within the critical infrastructure domain. Authorities and affected companies are likely to intensify efforts to investigate and mitigate the repercussions of this breach. #Breach #Clearnet #DarkWeb #DarkWebInformer #Database #Leaks #Leaked #USPipeline #Pipeline

Incident Detail

A threat actor has declared a database leak from GreyHours dated January 2024, comprising usernames, encrypted passwords, password salts, full names, emails, and other information in dark web. The threat actor also claims to have shut down the GreyHours website entirely by deleting their database and all associated files. This breach emphasizes the urgency for organizations to enhance their cybersecurity defenses. Investigations are anticipated to assess the breach's scope and implement necessary containment measures.

NoName, a threat actor group in dark web, has asserted responsibility for a series of alleged cyber-attacks targeting several prominent websites in the United Kingdom. Among the affected entities are the Confederation of British Industry, Authorization of Swiftcard, Authorization UK Finance (a trade organization), MoneyHelper, Leicestershire County Council, East Cambridgeshire District Council, and Liverpool City Council. The claims made by NoName raise significant concerns about potential data breaches and service disruptions across diverse sectors. As authorities and organizations respond to these allegations, the need for robust cybersecurity measures becomes increasingly apparent to safeguard against such cyber threats.

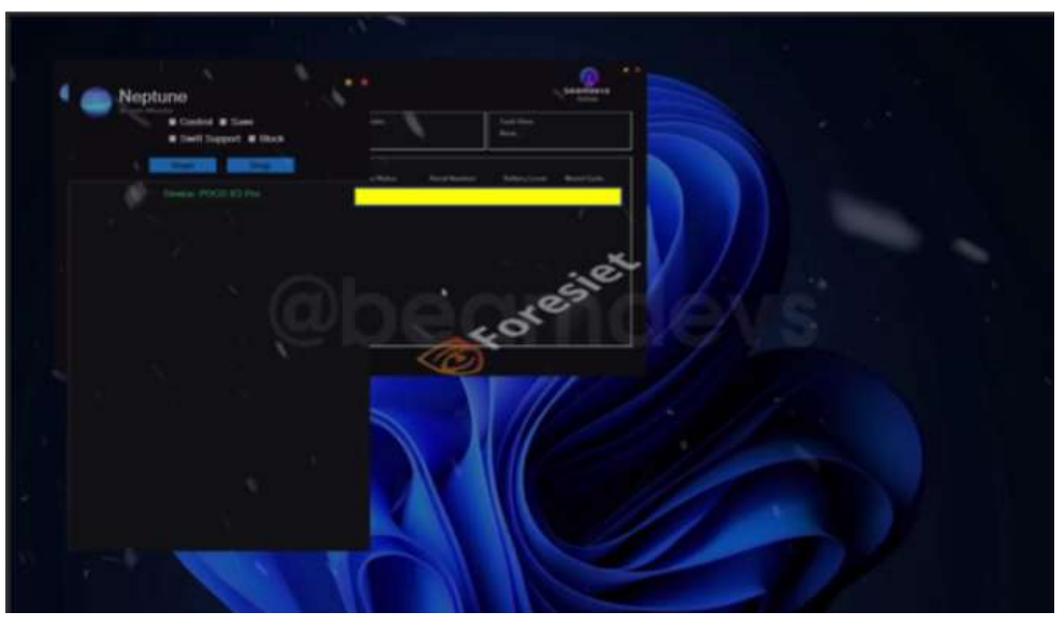
Incident Detail

Amidst the ongoing military aid from the Netherlands and Denmark to Ukraine, a threat actor group known as NoName has asserted responsibility for alleged cyber attacks on multiple entities in the Netherlands. As the first two out of 14 Leopard 2 tanks are prepared for shipment following overhaul, NoName's claims raise concerns about potential cyber disruptions targeting Dutch sites. The alleged targets include public transportation, tax administration, and information portals. Authorities are likely to investigate the veracity of these claims and take necessary measures to secure critical infrastructure and information systems.

Incident Detail

The hacking group KromSec has purportedly carried out an intrusion into a Western foundation, leaving a message on the homepage while asserting that no damage was inflicted on the database and system. The message conveys the group's opposition to what it perceives as a system marked by corruption, discrimination, oppression, cruelty, and crime. Archived links indicate the claimed hack on the Help4Children homepage and blog, both defaced with messages attributed to KromSec. Authorities are likely to investigate the incident to verify the breach's authenticity and assess potential implications.

In a significant data breach, a threat group named "Anonymous Central," collaborating with "RHA R," claims to have acquired the personal information of all FBI agents across the United States. The leaked document, purportedly spanning over 700 pages, includes sensitive details such as phone numbers, email addresses, job titles, and the first and last names of the agents. The breach has been publicized through various channels, including Telegram groups such as "Red Hackers Alliance Adapter" and "ANONM0S_RU." This incident poses serious security concerns and underscores the persistent challenges faced by law enforcement agencies in safeguarding sensitive information. Authorities are expected to investigate the breach and take appropriate measures to mitigate its impact.

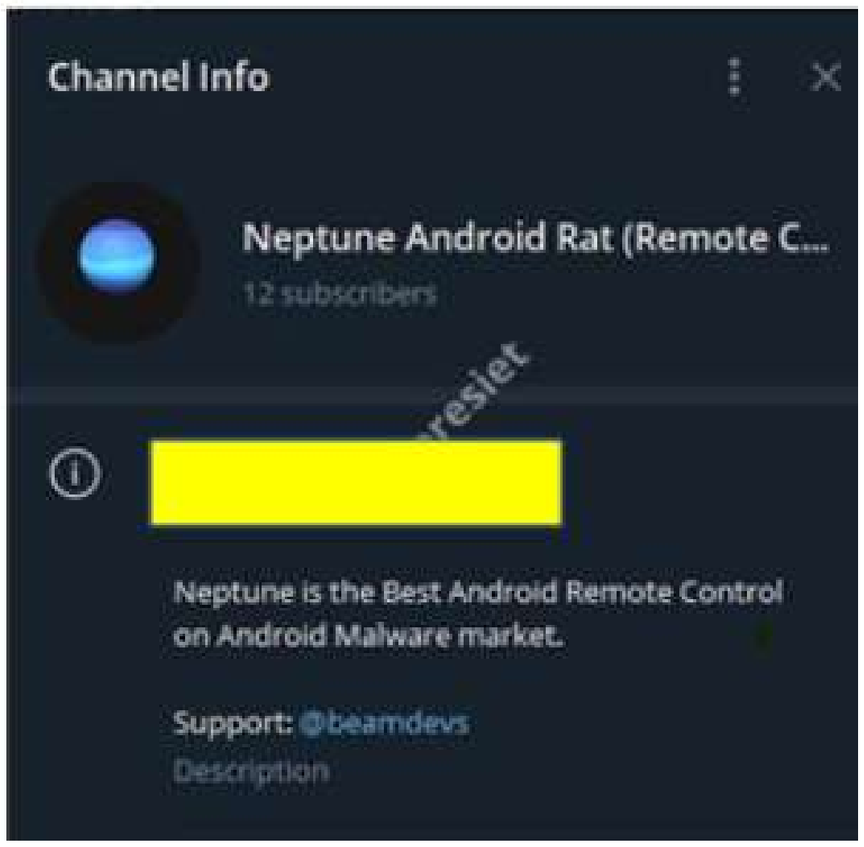


Incident Detail

- A reported data leak has been brought to light from the dark web that compromised a database containing information from 1 million users of a China virtual currency exchange. The leaked data includes details such as names, mobile phone operators, transaction amounts, registered accounts, website code verification, and the website platform. This incident raises concerns about the security of user information within the virtual currency exchange sector, emphasizing the need for robust cybersecurity measures to safeguard sensitive data. Authorities and relevant stakeholders are likely to investigate the breach and take necessary actions to address potential risks associated with the leaked information.

- A new WhatsApp scam has surfaced, with users receiving APK files from unknown numbers. These files, falsely linked to the inauguration of the Ram Mandir, pose a potential threat to device security, with the risk of hacks or financial loss. Users are advised to refrain from installing any APK files received from unfamiliar or suspicious sources, stay vigilant for potential scams on messaging platforms, and contribute to spreading awareness to ensure online safety for all.

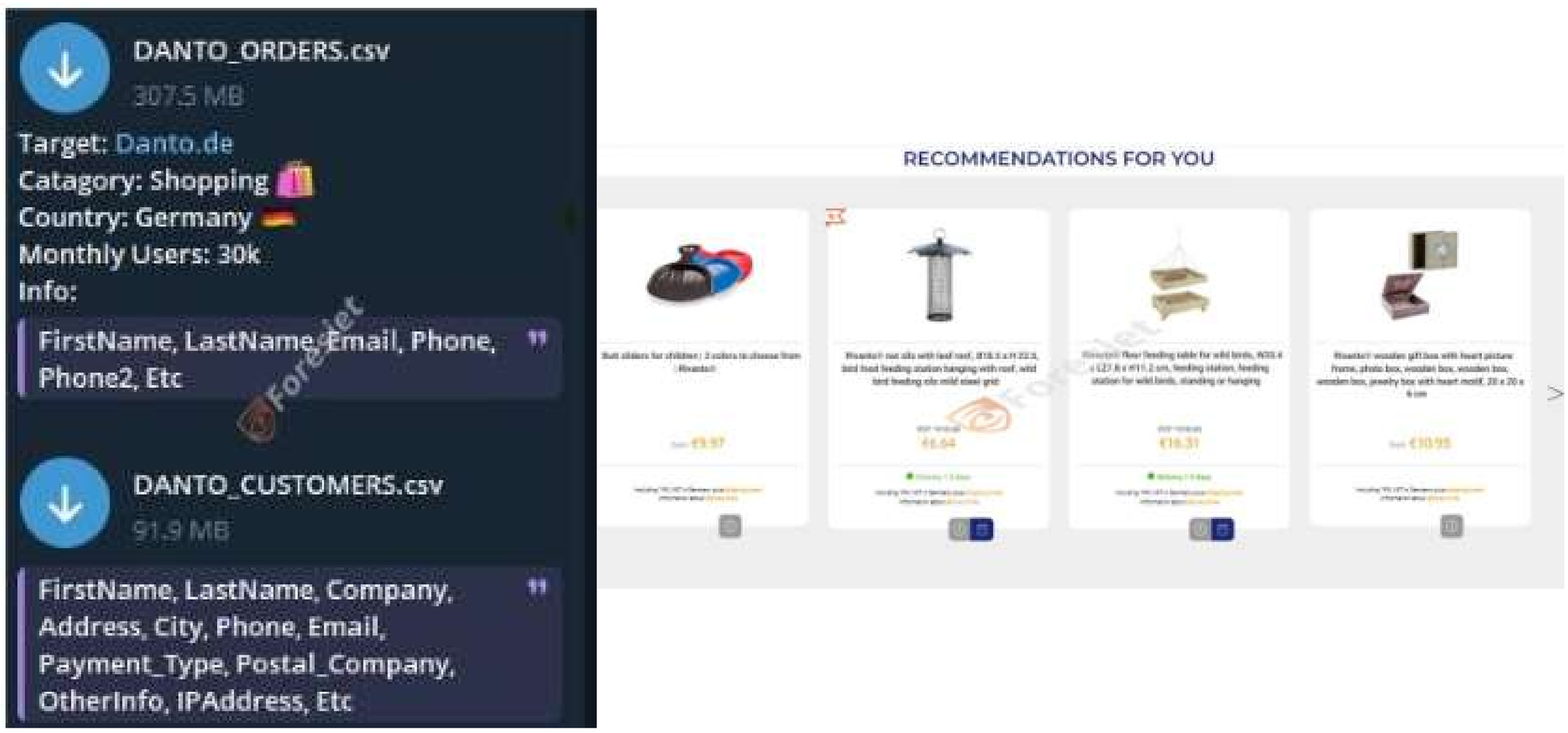
- The Neptune Android Remote Control is a sophisticated threat, boasting a range of invasive features that compromise user privacy and device security. From file and application management to location tracking, call monitoring, SMS manipulation, and more, this tool poses a serious risk for unauthorized access and data theft. Users are urged to exercise caution, refrain from downloading applications from untrusted sources, and prioritize robust security practices to mitigate potential risks associated with this advanced Android Remote Control tool.



Incident Detail

- Incident Report: Romanian internet sites have encountered disruptions following a visit from NoName057(16). Notable entities affected include the Romanian government, the website of the President of Romania, the Ministry of Foreign Affairs (MID), dedicated telecommunications services, and the Ministry of Labor and Social Solidarity. The disruption is purportedly a response to statements made by Romanian Foreign Minister Luminica Odobescu regarding Russia and Ukraine. This incident underscores the potential for cyber actions in response to geopolitical developments, emphasizing the need for robust cybersecurity measures. Authorities are likely to investigate the source and impact of the disruptions on these critical online platforms. [Confidential, details not to be disclosed publicly]

- Data Leak Alert: Danto.de, a Germany-based shopping website, has reported a breach affecting approximately 30,000 monthly users. The exposed information comprises user details, including first and last names, emails, and phone numbers, alongside additional information such as secondary phone numbers. Company-related data, including company names, addresses, and payment details, is also part of the leaked information. The breach extends to include IP addresses and other relevant details. This incident underscores the importance of heightened cybersecurity measures for online platforms to protect user information. Users are advised to monitor their accounts for any suspicious activity and consider changing passwords where necessary.



Incident Detail

- The Bahrain Airport website has reportedly faced disruption as it was taken offline by the threat group known as anonymousArabia. The group claims this action is a response to Bahrain's alleged support for the Israeli government and collaboration with the US-UK coalition in military operations in Yemen. anonymousArabia has declared its intention to persist in targeting key infrastructures in Bahrain until the government ceases its support for Israel and military actions in Yemen. The affected website, Bahrain Airport, is being monitored through the Uptrends platform. This disruption is indicative of a protest against the perceived actions of the Bahraini government, reflecting ongoing geopolitical tensions in the region. [Confidential, details not to be disclosed publicly]

- In a significant cybersecurity development, the threat group CyberDragon has claimed to successfully breached the servers of the European Parliament, asserting access to data on numerous employees even if the site is taken down. As part of their campaign, the group has publicized the contact details of an employee in the Directorate General for Safety and Security of the European Parliament. CyberDragon issued a warning to European Parliament staff, urging them to prevent the publication of personal data by disrupting document flows related to projects perceived as anti-Russian or supportive of separatist forces. The threat group hints at possessing a comprehensive document package, suggesting that the disclosure of personal data is just the initial phase of cooperation against the Russian Federation. This situation underscores the escalating tensions and geopolitical cyber activities between threat actors and European institutions.

Foresiet

Incident Detail

- Several Romanian internet sites have reportedly fallen victim to a cyber attack, claimed by a threat actor known as "noname," who declares a strategic defeat. The targeted sites include the Romanian Chamber of Deputies, MIA of Romania, the website of the Minister of Labor and Social Justice (Lia Olguta Vasilescu), Henri Coanda International Airport in Bucharest, Bucharest Metro, and the Ministry of Development, Public Works, and Administration of Romania. Noname suggests that Romanian authorities should prioritize their own security over Ukraine's. While the motive and extent of the cyber attack remain undisclosed, the incident highlights the challenges faced by government entities in safeguarding their digital infrastructure. [Confidential, details not to be disclosed publicly]

- The cyber army, NoName05716, has released an updated manifesto, extending an invitation to individuals who align with its values to join their cause. The group underscores its commitment to causing harm to Russia's adversaries, asserting a growing membership. The manifesto, available at https://telegra.ph/Manifest-NoName05716-01-22, outlines the group's mission. Interested individuals are encouraged to follow the group on their Russian version channel @noname05716, their DDoS project channel @fiTz615tQ6BhZWFi, and their reserve channel @noname05716_reserve. Operating under the identity "no name," the threat group has been actively advocating for Russian interests on the information front.

- A significant data leak has exposed information related to the Israeli surveillance system provided by IntuView. Specializing in artificial intelligence, IntuView offers services such as document exploitation, social media monitoring, new media monitoring, legal support, and name analysis. The system is reportedly utilized by the defense sector in the Palestinian sector and is associated with Mer Group, featuring an advisory board that includes former heads of Mossad and the CIA. The leaked information raises concerns about mass-scale analysis and monitoring of personal data, communications, and activities, potentially infringing on privacy and freedom of expression. The threat group behind the leak is identified as PRANA NETWORK.

Incident Detail

In a collaborative effort with the @lol_security team, the Egypt national airline company has been taken offline by the Anonymous Collective. The group cites dissatisfaction with the Egyptian government's refusal to permit humanitarian aid into Gaza as the motive behind the action. Anonymous Collective claims to have been monitoring the government's actions and presents this cyber attack as a warning, urging a reconsideration of policies related to humanitarian aid. This incident highlights the use of cyber actions as a form of protest against perceived political shortcomings. #AnonymousCollective #CyberAttack #HumanitarianAid #EgyptAirline [Confidential, details not to be disclosed publicly]

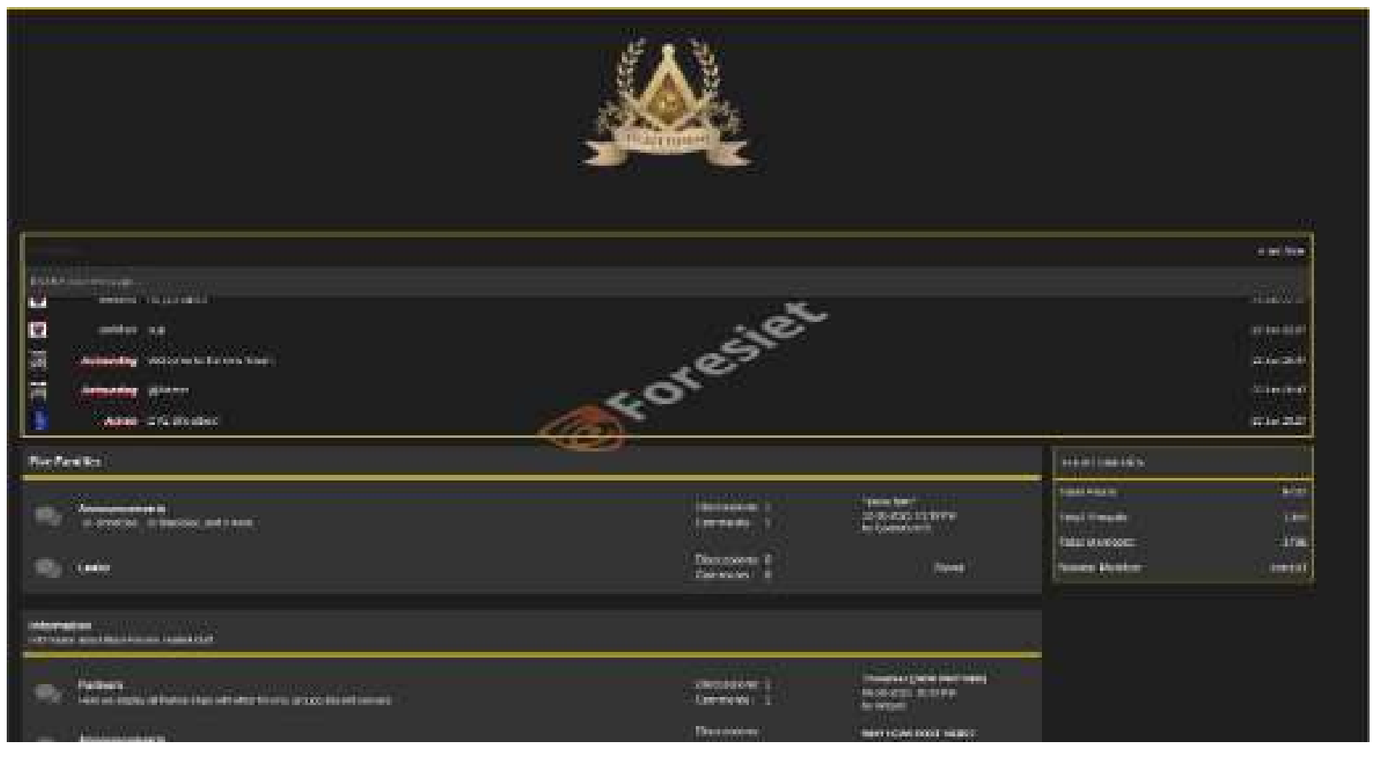
The hacker group LulzSecBlackhat has asserted responsibility for a database leak containing information from the largest hotels in Israel. The attack, labeled as "Leaked," specifically targets Israel. The data, presented in CSV format, encompasses fields such as ID, Category, Company Name, Email, Address, City, State, Zipcode, Phone Number, Fax Number, SIC Code, SIC Description, and Web Address. The disclosure was made on January 23, 2024, underscoring potential risks to the affected hotels and emphasizing the ongoing challenges in securing sensitive information online. Authorities and affected entities are likely to investigate the breach and take necessary measures to address the aftermath.

Incident Detail

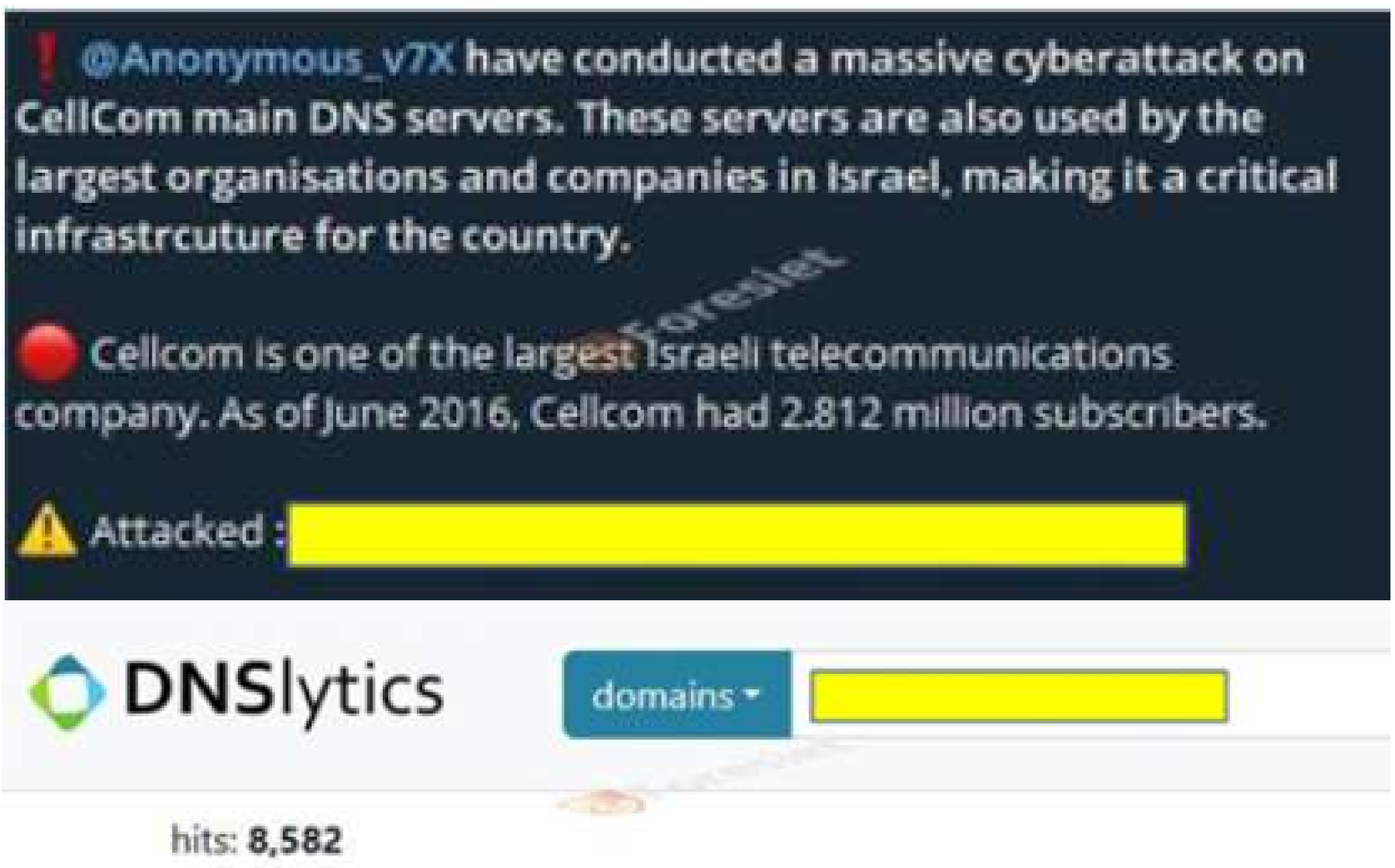
A new forum named "SecretForums Propaganda" is on the verge of launching, orchestrated by the threat actor @astounding. This forum is poised to replace blackforums, and @astounding is currently seeking theme suggestions for the impending platform. The actor assures users that data security will be maintained at the level of blackforums, with planned security patches. Upon the forum's official announcement, the channel will be transitioned to a new owner, marking a complete rebranding effort. Notably, access to the new forum will be exclusively through Tor, adding an extra layer of anonymity. This development underscores the evolving nature of illicit online forums and the persistent challenges in monitoring and addressing emerging cyber threats.

A new online forum, "SecretForums," has been launched, serving as the successor to the underground forum Blackforums. While the site is still under development, users are encouraged to report any bugs. Currently, access is limited to Tor, with clearnet access expected to be added in the near future. The forum will soon transition to a new owner, introduced by Astounding, the former admin of Blackforums. This development underscores the adaptability of illicit online forums and ongoing challenges in monitoring and addressing emerging cyber threats.

Incident Detail

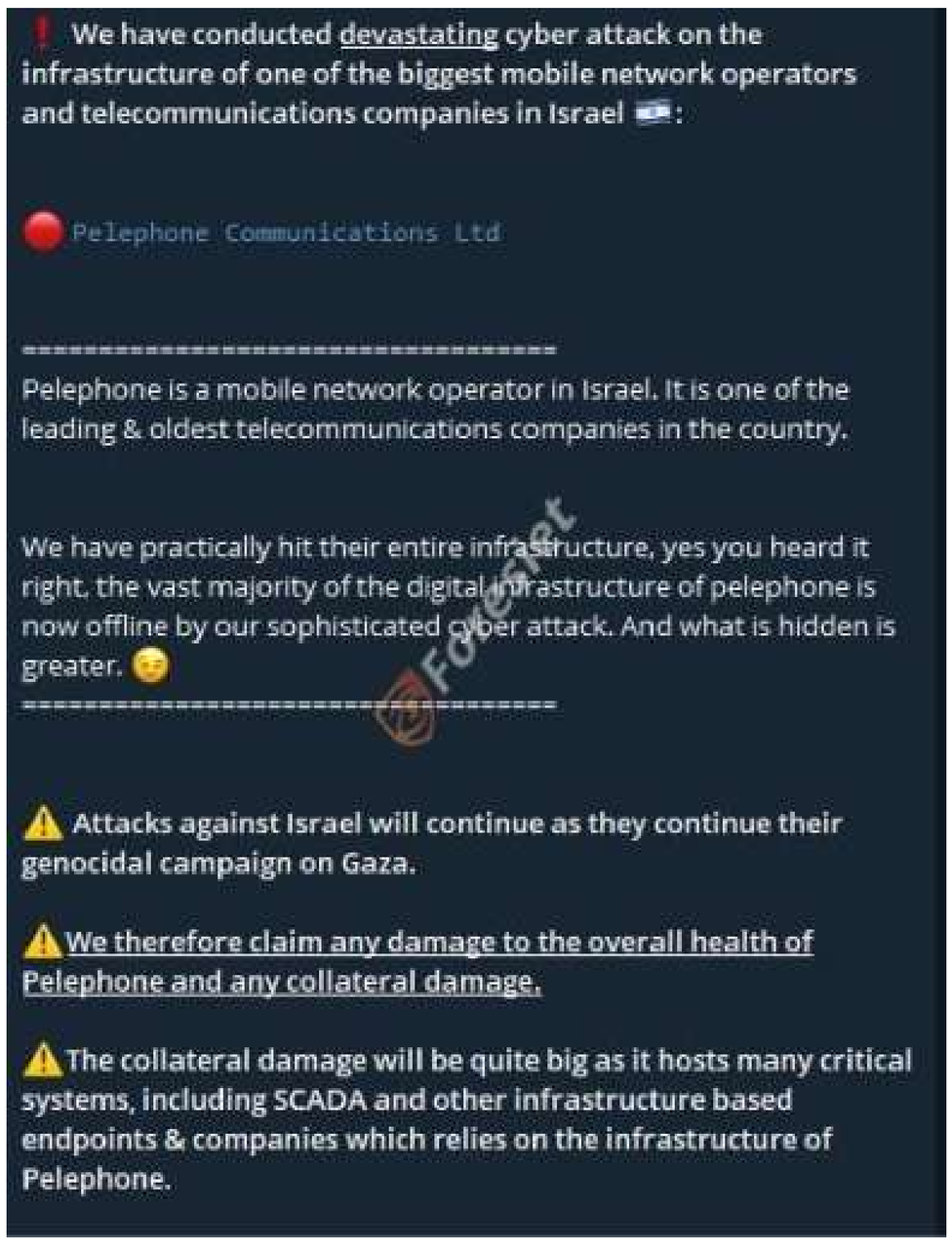


The group @Anonymous_v7X has claimed responsibility for a significant cyberattack on CellCom's main DNS servers. These servers play a critical role in the country's infrastructure, serving as the backbone for major organizations and companies in Israel. CellCom, being one of the largest telecommunications companies in the country with millions of subscribers, underscores the potential impact of the attack. The targeted DNS servers include [dns.netvision.net.il] and [nypop.netvision.net.il]. This incident raises concerns about the security of vital telecommunications infrastructure and the potential disruptions faced by both private and public entities. Authorities are likely to investigate the attack and take measures to restore services and prevent future incidents.



Incident Detail

The group #AnonymousSudan has asserted responsibility for a severe cyberattack on the infrastructure of Pelephone Communications Ltd, one of Israel's major mobile network operators and telecommunications companies. The attack reportedly inflicted substantial damage on the vast majority of Pelephone's digital infrastructure. #AnonymousSudan declares its intention to persist with these attacks as long as they perceive Israel to be conducting a genocidal campaign on Gaza. The group takes responsibility for any damage caused to Pelephone's overall health, emphasizing potential collateral damage due to the hosting of critical systems, including SCADA and other infrastructure-based endpoints and companies. This incident underscores the intersection of cyber threats with geopolitical tensions and raises concerns about the potential impact on essential services. Authorities are likely to investigate the attack and implement measures to restore services and enhance cybersecurity.



In a groundbreaking development, a cybersecurity researcher has recently exposed a massive database comprising 26 billion leaked records, impacting potentially millions, if not billions, of individuals. This unparalleled breach has earned the title of the "mother of all breaches," setting a historic precedent in the field of cybersecurity.

Vulnerability and Attack Surface Management

Vulnerability and Attack Surface Management

- In January 2024: we identified 2895 vulnerabilities, with 280 classified as critical vulnerabilities. Among these critical vulnerabilities, 90 currently have publicly available exploits. It's worth noting that all 350 exploits out of 2895 vulnerabilities carry an EPSS score ranging from 0.04% to 10.26%, indicating a High Level of Potential Exploitation.

- Foresiet research team has identified exploits available for Opportunistic Threat actors found in the Dark web, to target easy attacks. Listing a few: CVE-2024-23652, CVE-2023-49617, CVE-2024-23622, CVE-2024-23621, CVE-2024-23619, CVE-2024-23616, CVE-2024-23615, CVE-2024-23614, CVE-2024-23613, CVE-2023-52221, CVE-2024-0643, CVE-2023-52225, CVE-2023-52218, CVE-2023-51438, CVE-2023-7221, CVE-2023-7220, CVE-2023-7028, CVE-2023-48419, CVE-2023-48418, etc.,

- A critical vulnerability (CVE-2024-0204) in GoAnywhere can enable unauthenticated attackers' administrative access to the MFT service; exploitation of a similar vulnerability (CVE-2023-0669) enabled ransomware attacks on approximately 130 high-profile enterprises in early 2023.

- Google Chrome Update Addresses Actively Exploited Zero-Day CVE-2024-0519 and Two Vulnerabilities

- Apple Addresses CVE-2024-23222 Vulnerability on Its iPhones, Macs, and Apple TVs

CVE Monthly Prominent Vulnerability Disclosures

#	Vulnerability	Affected Vendor/ Product	Vulnerability Type/ Component	Zero Day
1	CVE-2023-22527 Risk Score: 99	Atlassian Confluence Data Center and Server versions 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x, and 8.5.0-8.5.3	A template injection vulnerability on older versions of Confluence Data Center and Server allows an unauthenticated attacker to achieve RCE on an affected instance. Customers using an affected version must take immediate action.	Yes
2	CVE-2024-23897 Risk Score: 99	Jenkins 2.441 and earlier, LTS 2.426.2 and earlier	Jenkins 2.441 and earlier, and LTS 2.426.2 and earlier, does not disable a feature of its CLI command parser that replaces an “@” character followed by a file path in an argument with the file's contents, allowing unauthenticated attackers to read arbitrary files on the Jenkins controller file system.	Yes
3	CVE-2024-0204 Risk Score: 99	Fortra's GoAnywhere MFT prior to 7.4.1	Authentication bypass in Fortra's GoAnywhere MFT prior to 7.4.1 allows an unauthorized user to create an admin user via the administration portal	Yes
4	CVE-2024-21887 Risk Score: 99	Ivanti Connect Secure, Ivanti Policy Secure	A command injection vulnerability in web components of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows an authenticated administrator to send specially crafted requests and execute arbitrary commands on the appliance. Chained with exploitation of CVE-2023-46805 to enable unauthenticated RCE.	Yes
5	CVE-2023-49954 Risk Score: 99	Citrix NetScaler ADC and NetScaler Gateway: 14.1-12.35, 13.1-51.15, 13.0-92.21; Specific NetScaler ADC configurations: 13.1-37.176, 12.1-55.302, and 12.1-55.302	Improper restriction of operations within the bounds of a memory buffer in NetScaler ADC and NetScaler Gateway allows unauthenticated denial-of-service.	Yes
6	CVE-2023-50164 Risk Score: 99	Apache Struts 2	Improper control of the generation of code (“Code Injection”) in NetScaler ADC and NetScaler Gateway allows an attacker with access to NSIP, CLIP, or SNIP with management interface to perform authenticated (low-privileged) remote code execution on Management Interface.	Yes
7	CVE-2024-23222 Risk Score: 99	Apple iOS 16.7.5, iPadOS 16.7.5, macOS Monterey 12.7.3, and tvOS 17.3	A type of confusion issue was addressed with improved checks. Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been exploited. This issue is fixed in tvOS 17.3, iOS 17.3, and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, Safari 17.3, macOS Ventura 13.6.4, and macOS Monterey 12.7.3.	Yes
8	CVE-2024-0519 Risk Score: 99	Google Chrome prior to 120.0.6099.224	Out-of-bounds memory access in V8 in Google Chrome prior to 120.0.6099.224 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High.)	Yes
9	CVE-2023-21674 Risk Score: 79	Microsoft Windows 10, 11, Server	Windows Advanced Local Procedure Call (ALPC) elevation-of-privilege vulnerability	No
10	CVE-2023-5356 Risk Score: 79	GitLab CE/EE all versions from 8.13 before 16.5.6, versions from 16.6 before 16.6.4, versions from 16.7 before 16.7.2	Incorrect authorization checks in GitLab CE/EE from all versions starting from 8.13 before 16.5.6, all versions starting from 16.6 before 16.6.4, all versions starting from 16.7 before 16.7.2, allows a user to abuse slack/mattermost integrations to execute slash commands as another user.	No
11	CVE-2024-21591 Risk Score: 79	Junos OS, various versions	An out-of-bounds write vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to cause a denial-of-service (DoS), or remote code execution (RCE) and obtain root privileges on the device. This issue is caused by the use of an insecure function allowing an attacker to overwrite arbitrary memory.	No
12	CVE-2022-1609 Risk Score: 79	Weblizar School Management Pro Edition for WordPress, various versions	The School Management WordPress plugin before 9.9.7 contains an obfuscated backdoor injected in its license-checking code that registers a REST API handler, allowing an unauthenticated attacker to execute arbitrary PHP code on the site.	No

*Source: Recorded Future

CVE Monthly Prominent Vulnerability Disclosures

#	Vulnerability	Affected Vendor/ Product	Vulnerability Type/ Component	Zero Day
13	CVE-2024-20656 Risk Score: 79	Microsoft Visual Studio, various versions	Visual Studio elevation-of-privilege vulnerability.	No
14	CVE-2023-40547 Risk Score: 79	Red Hat Enterprise Linux and Red Hat Shim, various versions	A remote code execution vulnerability was found in Shim. The Shim boot support trusts attacker-controlled values when parsing an HTTP response. This flaw allows an attacker to craft a specific malicious HTTP request, leading to a completely controlled out-of-bounds write primitive and complete system compromise.	No
15	CVE-2023-50643 Risk Score: 79	Evernote 10.68.2 for macOS	An issue in Evernote for MacOS v.10.68.2 allows a remote attacker to execute arbitrary code via the RunAsNode and enableNodeCliInspectArguments components	No
16	CVE-2024-20253 Risk Score: 79	Cisco Adaptive Security Appliance (ASA) Software, Cisco Packaged Contact Center Enterprise, Cisco Unified Communications Manager, Cisco Unity Connection Software, Cisco Virtualized Voice Browser	A vulnerability in Cisco Unified Communications and Contact Center Solutions allows an unauthenticated remote attacker to execute arbitrary code on affected devices. The issue stems from improper processing of user-provided data, allowing the attacker to send a crafted message to a listening port. Successful exploitation could lead to arbitrary command execution with web services user privileges, enabling potential root access on the affected device.	No
17	CVE-2024-20272 Risk Score: 79	Cisco Unity Connection Software	A vulnerability in Cisco Unity Connection allows an unauthenticated remote attacker to upload arbitrary files and execute commands on the underlying operating system. This results from a lack of authentication in a specific API, enabling the attacker to store and execute malicious files with elevated privileges.	No
18	CVE-2023-6000 Risk Score: 79	Sygnoos Popup Builder for WordPress	The Popup Builder WordPress plugin before 4.2.3 does not prevent simple visitors from updating existing popups and injecting raw JavaScript in them, which could lead to Stored XSS attacks	No
19	CVE-2024-0200 Risk Score: 79	GitHub Enterprise Server	GitHub Enterprise Server had a security flaw (reflection injection) allowing remote code execution. Exploitable by an actor with an organization owner role, it affected versions before 3.12 and was fixed in versions 3.8.13, 3.9.8, 3.10.5, and 3.11.3, reported through GitHub Bug Bounty.	No
20	CVE-2024-0517 Risk Score: 79	Google Chrome prior to 120.0.6099.224	Out-of-bounds write in V8 in Google Chrome prior to 120.0.6099.224 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High.)	No
21	CVE-2024-20674 Risk Score: 78	Microsoft Windows 10, 11, Server	Windows Kerberos Security Feature Bypass Vulnerability	No
22	CVE-2023-41474 Risk Score: 77	Ivanti Avalanche 6.3.4.153 Premise Edition	Directory Traversal vulnerability in Ivanti Avalanche 6.3.4.153 allows a remote authenticated attacker to obtain sensitive information via the javax.faces.resource component.	No
23	CVE-2023-6875 Risk Score: 76	WPExperts Post SMTP for WordPress, various versions	The WordPress plugin "POST SMTP Mailer" (versions up to 2.8.7) has a vulnerability on the connect-app REST endpoint, allowing unauthorized access and data modification due to a type juggling issue. This enables unauthenticated attackers to reset the API key, view logs, and potentially take over the site, including accessing password reset emails.	No
24	CVE-2023-39336 Risk Score: 75	Ivanti Endpoint Manager 2016, 2017, 2018, 2019, 2020, 2021, 2022	An unspecified SQL Injection vulnerability in Ivanti Endpoint Manager released prior to 2022 SU 5 allows an attacker with access to the internal network to execute arbitrary SQL queries and retrieve output without the need for authentication. Under specific circumstances, this may also lead to RCE on the core server	No

*Source: Recorded Future

CVE Monthly Prominent Vulnerability Disclosures

#	Vulnerability	Affected Vendor/ Product	Vulnerability Type/ Component	Zero Day
25	CVE-2023-50919 Risk Score: 75	GL.iNET GL-A1300 Firmware	An issue was discovered on GL.iNet devices before version 4.5.0. There is an NGINX authentication bypass via Lua string pattern matching. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7.	No
26	CVE-2024-23898 Risk Score: 75	Jenkins 2.441 and earlier, LTS 2.426.2 and earlier	Jenkins 2.217 through 2.441 (both inclusive), and LTS 2.222.1 through 2.426.2 (both inclusive), do not perform origin validation of requests made through the CLI WebSocket endpoint, resulting in a cross-site WebSocket hijacking (CSWSH) vulnerability, allowing attackers to execute CLI commands on the Jenkins controller.	No
27	CVE-2024-0402 Risk Score: 75	GitLab Community Edition, Enterprise Edition	An issue has been discovered in GitLab CE/EE affecting all versions from 16.0 prior to 16.6.6, 16.7 prior to 16.7.4, and 16.8 prior to 16.8.1, which allows an authenticated user to write files to arbitrary locations on the GitLab server while creating a workspace.	No

Recommended Actions

- Enhanced Cybersecurity Measures: Urgent reinforcement of cybersecurity protocols, including regular updates, patches, and securing critical systems against known vulnerabilities.

- Heightened Vigilance: Continuous monitoring of networks and systems, particularly in critical sectors like government, defense, healthcare, and finance.

- Employee Awareness Training: Educate employees on cybersecurity best practices, including password hygiene, phishing awareness, and device security.

- Incident Response Planning: Develop robust incident response plans to minimize damage in case of a cyber attack or breach.

- Dark Web Monitoring: Continuous monitoring of Dark Web channels for potential data leaks, threats, or indications of upcoming attacks.

This threat intelligence report highlights the critical need for proactive measures to defend against a diverse range of cyber threats emanating from various threat actors, emphasizing the importance of cybersecurity preparedness and resilience across industries and government sectors.

Please note that the information provided is based on available data and intelligence reports. For comprehensive threat intelligence & mitigation strategies please reach out to Foresiet Threat Intelligence team.

Foresiet Integrated Digital Risk Protection (IDRP)

(One-Click Plug and Play IDRP Solution)

Digital Risk Protection

Real-time digital risk monitoring to secure operations from unseen threats.

Brand Protection

Powerful surveillance to deter intellectual property theft and protect brand integrity.

Attack Surface Management

Comprehensive attack surface management to reduce exposure and seal off vulnerabilities.

Threat Intelligence

Advanced threat analytics to gain unparalleled foresight and outsmart potential cyber attacks.

Compliance & Third-party Assessment

Thorough assessments to ensure impeccable standards within the organization and across the entire vendor network.

Anti-Phishing Shield

Proactive phishing defense system to ward off deceptive threats and keep communications and data secure.

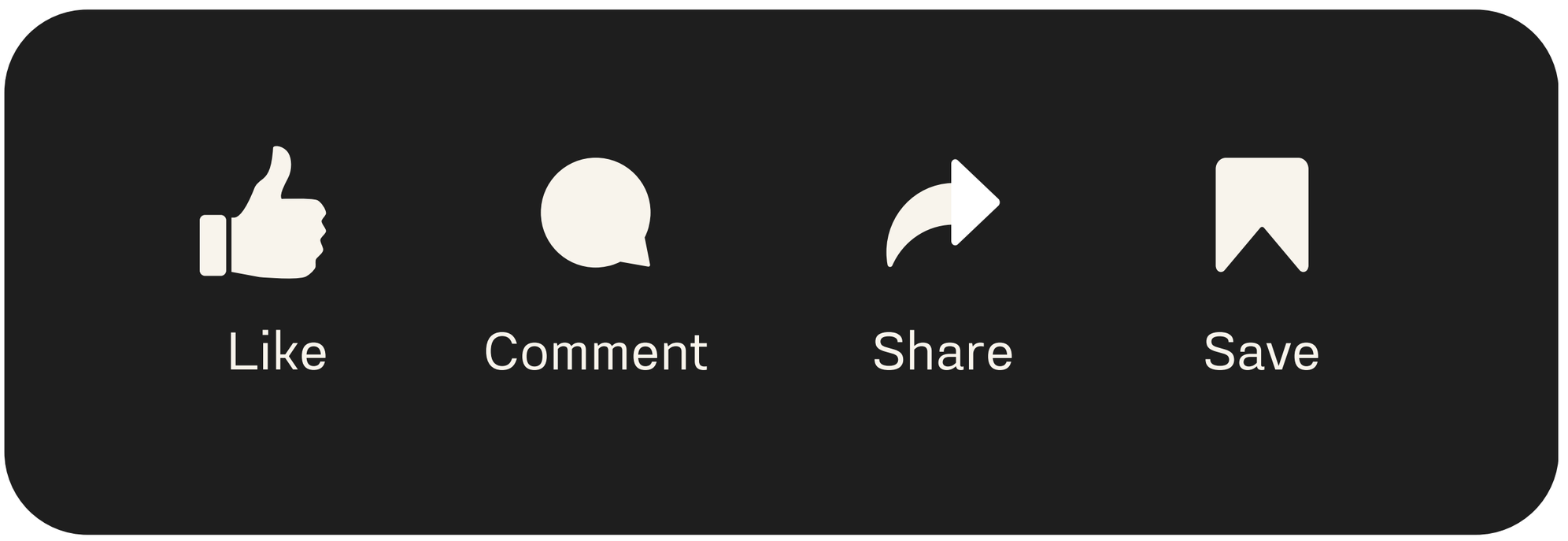
Foresiet's Integrated Digital Risk Protection (IDRP) solution is your one-stop shop for cyber defense. It scans the deep and dark web for threats to your brand, identifies vulnerabilities in your IT infrastructure, and assesses the cybersecurity posture of your vendors. Plus, it shields your employees from phishing attacks and protects your online reputation from impersonation and counterfeiting. In short, Foresiet IDRP gives you 360-degree visibility and protection against today's most sophisticated cyber threats.

Contact us: +91 8169451052 | info@foresiet.com

Foresiet

Is this post useful to you?

Feel free to like, share, and save if you find this post useful!



Contact us: +91 8169451052 | info@foresiet.com