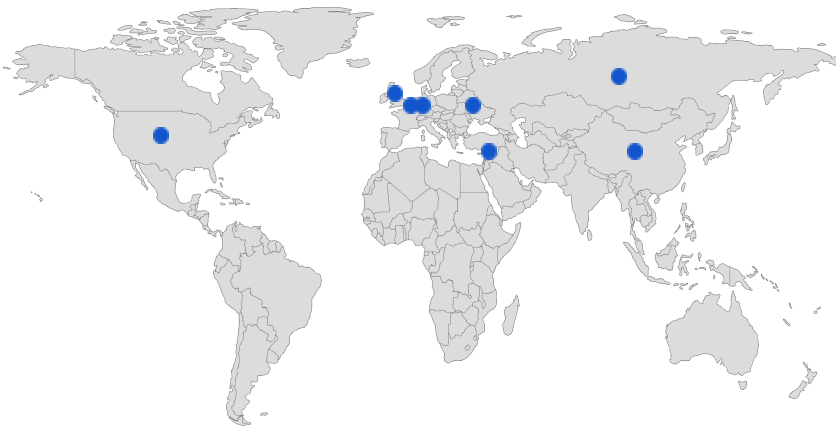


Threat Intel Report: March 25-31, 2024

Countries



Top Tags

TheMoon

ShadowRay

APT29

Sointsepek

Sandworm

Executive Summary

Actionable Information:

- *Supply Chain Vulnerabilities:* Organizations should scrutinize their supply chains for potential vulnerabilities, especially in software dependencies, and adopt a multi-layered security approach to mitigate risks.
- *AI and Zero-Day Exploits:* The rise in AI-facilitated scams and zero-day exploits calls for continuous monitoring and updating of security systems, alongside regular security audits to identify and patch vulnerabilities promptly.
- *Nation-State Cyber Espionage:* The involvement of state-sponsored actors in cyberattacks against political parties and critical infrastructure necessitates enhanced collaboration between governments and the private sector to share intelligence and bolster defenses.
- *Ransomware Resilience:* Municipalities and organizations must prioritize the development of robust incident response plans and backup strategies to ensure business continuity in the face of ransomware attacks.

Outlook:

The current trajectory of cyber threats indicates an increasingly sophisticated and diverse threat landscape, with cybercriminals and nation-state actors leveraging advanced techniques to exploit vulnerabilities across a wide range of targets. The strategic targeting of political entities, critical infrastructure, and the financial sector suggests that cybersecurity is not merely a technical challenge but a critical component of national and economic security. As such, the outlook for the near future underscores the imperative for organizations and governments to invest in comprehensive cybersecurity strategies, encompassing threat intelligence, robust defense mechanisms, and international cooperation to mitigate the evolving threats. The role of AI and machine learning in both facilitating and defending against cyberattacks



is expected to grow, highlighting the need for ethical considerations and regulatory frameworks to govern the use of these technologies in cybersecurity.

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

↓ 8% [CVE-2023-30185](#)

- A file upload vulnerability in some versions of CRMEB

↑ 4% [CVE-2024-27199](#)

- A path traversal vulnerability in JetBrains TeamCity

↑ 394% [CVE-2023-20887](#)

- A command injection vulnerability in VMWare Aria Operations for Networks

Israeli Financial Sites Targeted by DDoS

+Israel +Financial Services +DDoS

- Several Israeli financial services companies were targeted this week in distributed denial of service (DDoS) attacks, each reaching over 1M requests per second (RPS). Israeli companies are frequently targeted by hackers and other attackers, and these sites are frequently victims of attempted DDoS.

Belgian Computing Site Attacked by Bots

+Belgium +Computing & IT +Financial Services +Bots

- A Belgian computing site was targeted in automated attacks this week. This site offers computing solutions for financial institutions, so attackers are most likely looking to gather sensitive financial data.

Recent Cyber Threats

Sophisticated Supply Chain Attack Utilizes Fake Python Infrastructure

+Supply Chain +Python

- A sophisticated attack on the [software supply chain](#) affected over 170,000 users, including the Top.gg GitHub organization and individual developers. Attackers employed stolen browser cookies for account takeovers, contributed malicious code, and created a fake Python package repository to distribute malware. The attack harvested sensitive data like passwords and credentials from victims' systems, demonstrating a complex multi-vector approach to exploit the software supply chain vulnerabilities.

Stealth Industrial Espionage via NuGet Package

+Backdoor +China +ICS

- Researchers have uncovered a .NET package, [SqzrFramework480](#), potentially used for industrial espionage, linked to a Chinese manufacturer. The package, which has been downloaded 3,000 times, contains functionality that could capture screenshots and exfiltrate data, raising suspicions of its use as a backdoor for cyber espionage. This discovery highlights the ongoing cyber threats to industrial systems and the sophisticated methods employed by attackers to infiltrate and spy on industrial software systems.

Truck-to-Truck Worm Threatens US Transportation Infrastructure

+US +Transportation

- Researchers have identified vulnerabilities in [Electronic Logging Devices](#) (ELDs) used in US commercial trucks, potentially affecting over 14 million vehicles. Demonstrating through a proof-of-concept worm, they showed how these devices could be exploited to spread malware between trucks, manipulate data, and take control of the vehicles. This research underscores the urgent need for improved security measures in the transportation sector to protect against such vulnerabilities.

Exploiting ChatGPT for Persistent Access and Data Exfiltration

+AI +XSS

- Security researchers have demonstrated how attackers could exploit vulnerabilities in [ChatGPT](#), including Cross-Site Scripting (XSS), to gain persistent access to user data and manipulate application behavior. By exploiting these vulnerabilities, attackers could exfiltrate sensitive information, including JWT access tokens, and manipulate ChatGPT's responses for malicious purposes. This analysis highlights the potential post-exploitation risks associated with integrating AI into daily routines and the importance of securing such technologies.

TheMoon Malware Campaign Targets ASUS Routers

+TheMoon +Malware +IoT +Faceless

- A new variant of [TheMoon](#) malware has been observed infecting thousands of outdated ASUS routers and IoT devices across 88 countries, linking to the "Faceless" proxy service used by cybercriminals to anonymize their activities. In less than 72 hours, 6,000 ASUS routers were compromised, leveraging known vulnerabilities or weak credentials. This campaign underscores the critical importance of maintaining updated and secure devices to protect against such widespread malware infections.

AI Tools Amplify Tax Season Scams

+AI +Financial Services

- Cybercriminals are increasingly using [AI tools](#), including deepfake technology and AI-generated robocalls with regionally appropriate accents, to deceive victims. Despite a high level of confidence among Americans in identifying fake content, 29% admit they wouldn't recognize fraudulent AI-generated content. This study emphasizes the importance of vigilance during tax season, especially in recognizing phishing emails and safeguarding personal information.

Surge in Enterprise Zero-Day Exploits

+Zero-day +Enterprise

- Researchers report a [56% increase](#) in zero-day vulnerabilities exploited in 2023, with a significant 64% rise in attacks targeting enterprise-specific technology. The shift towards exploiting enterprise software and appliances, including security software, highlights a growing trend in cybercriminal activity focusing on high-value targets. The report underscores the challenges enterprise vendors face in responding to sophisticated attacks and the importance of robust security measures to protect against these threats.

ShadowRay Campaign Exploits Unpatched Ray Framework Flaw

+ShadowRay +Cryptocurrency

- The [ShadowRay](#) campaign targets an unpatched vulnerability in the Ray framework, affecting thousands of companies across various sectors. Attackers hijack computing resources for cryptocurrency mining and leak sensitive data, including AI models and cloud environment access tokens. Despite dispute over the vulnerability's classification, the lack of authentication in Ray deployments has led to widespread exploitation.

Cisco Alerts on Password Spraying Attacks Against Secure Firewall Devices

+Password Spraying

- Cisco warns of [password spraying attacks](#) targeting Remote Access VPN services on Cisco Secure Firewall devices, as well as third-party VPN concentrators. These brute force attacks aim to compromise accounts by using common passwords across multiple usernames, potentially leading to denial of service conditions. Cisco's recommendations for defense include enabling logging, securing default VPN profiles, and using certificate-based authentication for enhanced security against these attacks.

Data Breaches

Russian Hackers Target German Political Parties with WineLoader Malware

+APT29 +Russia +Germany +Government

- APT29, a Russian espionage group, has shifted its focus to [German political parties](#), deploying WineLoader malware through phishing campaigns. This marks a significant change in their operations, previously centered on diplomatic entities. The malware allows remote access to compromised devices, indicating a strategic move to influence or monitor political processes in Germany.

Ukrainian ISPs Disrupted by Sandworm-Linked Group

+Ukraine +Russia +ISP +Solntsepek +Sandworm

- [Four Ukrainian ISPs](#) were attacked, likely by Russian state-backed hackers linked to the GRU's Sandworm operation. A group known as Solntsepek claimed responsibility, impacting services and potentially accessing sensitive client data. This continues a pattern of cyber aggression towards Ukrainian infrastructure amidst ongoing geopolitical tensions.

Communications Workers Union in the UK Faces Cyberattack

+UK +Union +Telecommunications

- The [Communications Workers Union](#), representing tech and telecoms workers in the UK, is addressing a cyberattack initially mistaken for an IT outage. The extent of the attack is under investigation, with potential implications for member data security. This incident underscores the vulnerability of even non-commercial organizations to cyber threats.

Ransomware Attacks Disrupt Municipal Services in Texas and Georgia

+US +Ransomware +Government

- Municipalities in [Texas and Georgia](#), including Gilmer County and Tarrant County, have experienced service disruptions due to ransomware attacks. These incidents highlight the ongoing challenge of securing local government networks against cybercriminals, with essential services like 911 remaining operational despite the attacks.

Prisma Finance Falls Victim to Crypto Theft Amidst Confusing Hacker Motives

+Crypto +Financial Services

- [Prisma Finance](#), a DeFi platform, and Munchables, a blockchain game, were compromised, with millions in cryptocurrency stolen. The incidents featured unusual twists, including a hacker claiming to be a "white hat" and offering to return stolen funds. These events cap a strange week in the crypto world, underscoring the complex landscape of digital asset security.

Imperva Protection

Imperva provides comprehensive digital security solutions, including protection against threats to web applications and APIs— including security vulnerabilities, fraud, and bad bots, data security solutions, and security against disruptive network- and application-level DDoS attacks.



By Phone:
650-345-9000

By mail:

Imperva Headquarters
One Curiosity Way, Suite
203 San Mateo, CA 94403