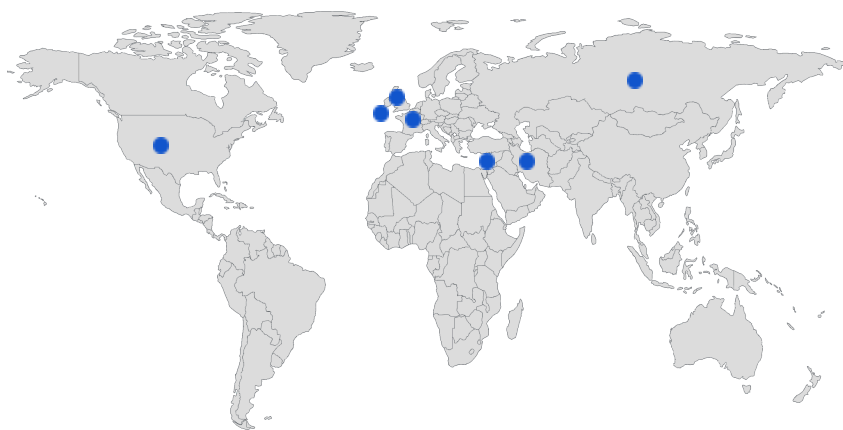


Threat Intel Report: March 11-17, 2024

Countries



Top Tags

DarkGate

Lord Nemesis

Anonymous Sudan

Muddled Libra

BlackByte

Executive Summary

Actionable Information:

- *Ransomware Evolution:* The emergence of new ransomware like DoNex, employing double-extortion tactics, indicates a need for robust backup and encryption strategies to protect sensitive data.
- *AI and Software Vulnerabilities:* Attacks exploiting vulnerabilities in AI models and software products (e.g., Ivanti) call for continuous monitoring and updating of all systems to patch known vulnerabilities promptly.
- *Supply Chain and Pentesting Tools Misuse:* The utilization of pentesting tools by groups like Muddled Libra for malicious purposes highlights the importance of securing the supply chain and vetting third-party tools and services.
- *Government and Critical Infrastructure Attacks:* The targeting of government entities and critical infrastructure by DDoS attacks and ransomware campaigns necessitates a collaborative approach to cybersecurity, involving both public and private sectors.
- *Data Breaches:* Incidents like the KidsEmpire database exposure and the massive breach at France Travail demonstrate the ongoing risk of data breaches, emphasizing the need for stringent data protection measures and quick response mechanisms.

Outlook:

The landscape of cyber threats is evolving rapidly, with attackers continuously refining their tactics and targeting a broader array of victims. The recent incidents reveal a clear trend towards more sophisticated and targeted attacks, leveraging vulnerabilities in both new and established technologies. As ransomware groups become more audacious in their demands and methods, and as the exploitation of AI and software vulnerabilities becomes more common, the

importance of proactive cybersecurity measures has never been more critical. Organizations must prioritize the security of their digital assets and personal data to mitigate the risk of significant operational and reputational damage. Looking ahead, the focus should be on enhancing resilience through advanced threat detection, comprehensive incident response planning, and fostering a culture of cybersecurity awareness across all levels of an organization. The collaborative effort between governments, private sector entities, and individuals will be pivotal in countering the sophisticated cyber threats of tomorrow.

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

⬆ 44% [CVE-2023-30185](#)

- A file upload vulnerability in some versions of CRMEB

⬇ 1% [CVE-2023-35078](#)

- A remote unauthenticated API access vulnerability in Ivanti Endpoint Manager Mobile

⬆ 3% [CVE-2023-35082](#)

- A remote unauthenticated API access vulnerability in Ivanti Endpoint Manager Mobile

Romanian Retail Site Hit in Second-Largest DDoS Attack of the Year

+Romania +Retail +DDoS +China

- The second largest application-layer DDoS attack so far this year occurred this week, targeting a Romanian retail site with just over 4M requests per second (RPS). The attack came from 2,000 IPs, primarily based in Romania and China.

US Financial Site Targeted by ATO

+ATO +US +Financial Services

- A US-based financial site was hit by account takeover (ATO) this week, totaling almost 1M malicious logins. Coming from 58,000 IPs, 14% of the logins used in this attack were previously compromised.

Recent Cyber Threats

New DoNex Ransomware Targets Enterprises

+DoNex +Ransomware

- The newly identified [DoNex](#) ransomware has been targeting enterprises in Europe and the US, employing a double-extortion tactic. This involves encrypting files and exfiltrating sensitive data, putting additional pressure on victims to pay the ransom. The use of Tox Messenger for communication underscores the attackers' preference for secure, anonymous channels.

Closed AI Models Vulnerable to Information Extraction

+AI

- Researchers have demonstrated a method to extract sensitive information from [closed AI models](#) operated by OpenAI and Google. This attack reveals the embedding projection layer of transformer models, potentially allowing for the replication of proprietary models. The findings have prompted both companies to implement defenses against such attacks.

DarkGate Operators Exploit Microsoft Windows SmartScreen Bypass

+DarkGate

- [DarkGate](#) operators exploited CVE-2024-21412, a zero-day vulnerability, to bypass Microsoft Windows SmartScreen, distributing malware through fake software installers. The campaign employed open redirect URLs from Google Ad technologies to distribute fake Microsoft software installers posing as legitimate software, including Apple iTunes, Notion, NVIDIA, and others.

Malware Hidden in SVG Files

+SVG

- Hackers are embedding malware within [SVG](#) (Scalable Vector Graphics) files to deliver ransomware and banking Trojans, bypassing security measures. This technique, observed in a campaign delivering Agent Tesla Keylogger and XWorm RAT, exploits the SVG file format's ability to describe images using mathematical equations, allowing for scalability without quality loss. The campaign leverages AutoSmuggle, an open-source tool, to embed malicious content within SVG or HTML files, evading email gateways and enhancing malware delivery success.

Iran-Linked Hacktivists Target Israeli Organizations

+Iran +Israel +Lord Nemesis +Hacktivism

- The Iranian state-backed hacking group, [Lord Nemesis](#), infiltrated Rashim Software, an academic administration software maker, to intimidate Israeli organizations. The attack, aimed at hacktivism rather than financial gain, used credentials from Rashim Software to access its clients, including academic institutes. This activity aligns with Iran's support for Hamas and represents a continuation of cyber threats from Iranian state-backed hackers against Israeli targets.

GhostRace Attack Exposes CPU Vulnerabilities

+GhostRace +CPU

- Researchers have disclosed a new attack type, [GhostRace](#), affecting major CPU manufacturers by exploiting Speculative Race Conditions (SRCs). This vulnerability could allow attackers to access sensitive information like passwords and encryption keys. The attack requires either physical access to the device or privileged access, making it a challenging but potent threat to system security.

French Government Faces Intense Cyberattacks

+France +DDoS +Government

- [French government agencies](#) experienced intense cyberattacks, described as DDoS (Distributed Denial of Service) incidents, of unprecedented intensity. The attacks, which began on a Sunday night, did not compromise networks or system data but disrupted access to several ministerial services. A crisis cell was activated to deploy countermeasures, reducing the impact and restoring access to state websites.

Meduza Under Cyberattack Ahead of Russian Presidential Election

+Russia +News +Hacktivism

- [Meduza](#), a Russian independent media outlet, reported facing an unprecedented cyber campaign ahead of the presidential election. The attacks, more intense than any previously experienced by Meduza, aim to disrupt or block the organization's internet presence. The campaign began around the time of Russian opposition leader Alexey Navalny's death, with attackers attempting to block Meduza's servers and disable its main website through DDoS attacks.

Alabama Targeted by Russian-Backed DDoS Attack

+US +DDoS +Government +Anonymous Sudan +Hacktivism

- [Alabama's](#) state and city governments were disrupted by cyberattacks, with the state grappling with network disruptions days after the incidents. The attacks, confirmed by Governor Kay Ivey, did not compromise networks or data. Anonymous Sudan, a Russian-backed hacktivist group, claimed responsibility for the DDoS attack on the state government, highlighting the ongoing threat of cyberattacks supported by state-sponsored groups.

Muddled Libra Hackers Utilize Pentesting Tools

+Muddled Libra +Supply Chain

- The [Muddled Libra](#) hacking group is using pentesting tools to gain admin access to target systems. Emerging in late 2022 with the Oktapus phishing kit, Muddled Libra has been linked to complex supply chain attacks targeting the cryptocurrency sector. The group's tactics include using lookalike domains for smishing attacks and leveraging legitimate tools for data and credential theft, demonstrating a sophisticated understanding of their targets and a broadening scope of operations.

Data Breaches

CISA Systems Offline After Ivanti Compromise

+US +CISA +Government

- [CISA](#) took two systems offline following a breach via Ivanti product vulnerabilities. The affected systems, speculated to be the Infrastructure Protection Gateway and the Chemical Security Assessment Tool, contained sensitive U.S. infrastructure and chemical security data. Despite the breach, CISA reported no operational impact and emphasized the importance of incident response plans for resilience.

Leicester City Council Cyberattack

+UK +Government

- [Leicester City Council's](#) IT systems and phone lines have been down since a cyberattack on March 7, with recovery expected to start midweek. The nature of the attack remains undisclosed, but it's part of a trend affecting local authorities. Emergency lines have been set up, and the council is prioritizing critical services during the outage.

KidsEmpire Data Breach Exposes Millions of Records

+Entertainment

- Over 2.3 million records from [Kids Empire](#), a family entertainment business, were exposed due to an unsecured database. The breach included sensitive customer information, such as partial credit card numbers and personal details. The database was secured three weeks after discovery, with no evidence of data misuse reported.

Encina Wastewater Authority Targeted by BlackByte Ransomware

+Utilities +US +BlackByte

- The [Encina Wastewater Authority](#) in Carlsbad, California, was allegedly attacked by the BlackByte ransomware group. While the organization's website remained operational, the claim raises concerns about potential access to sensitive company documents. The extent of the breach and the data's security status remain unconfirmed.

Irish Government Website Exposed COVID-19 Vaccination Records

+Ireland +Government +Healthcare

- A vulnerability in the [Irish Health Service](#) Executive's COVID-19 vaccination portal exposed around a million residents' vaccination records. Discovered in December 2021, the flaw allowed unauthorized access to health information. The issue was fixed, but details were only disclosed two years later, highlighting challenges in coordinating public disclosure.

French Unemployment Agency Data Breach Affects 43 Million

+France +Government

- [France Travail](#), formerly Pôle Emploi, reported a cyberattack that exposed the personal details of 43 million people. The breach, occurring between February 6 and March 5, included sensitive information like social security numbers and contact details. This incident marks a significant data breach in France, surpassing previous records.
-



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