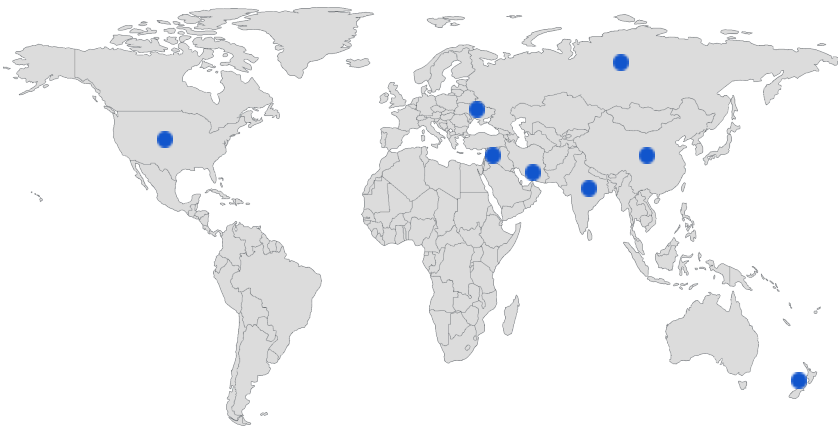


Threat Intel Report: March 18-24, 2024

Countries



Top Tags

AcidRain

PhantomBlue

Sysrv

SmokeLoader

Handala Hack

Executive Summary

Actionable Information:

- *Enhance Detection and Response:* Organizations must improve their ability to detect and respond to sophisticated phishing campaigns, such as Operation PhantomBlu, which bypass traditional security measures.
- *Secure Configuration and Patch Management:* The widespread Firebase misconfiguration and the discovery of the Loop DoS vulnerability underscore the necessity for robust configuration management and timely application of security patches.
- *Awareness and Training:* Increasing awareness about the potential for acoustic side-channel attacks and the importance of securing personal devices against malware campaigns targeting platforms like Android.
- *Sector-Specific Security Measures:* Financial institutions, hospitality services, and critical infrastructure entities must adopt sector-specific security measures to defend against targeted attacks, such as those by SmokeLoader malware and Iranian hackers.

Outlook:

The current trend of cyber threats indicates a continued focus on exploiting vulnerabilities in both technology and human behavior. The diversity of attack vectors, from acoustic side-channel attacks to sophisticated phishing and malware campaigns, suggests that attackers are constantly innovating to find new ways to breach security measures. The emergence of unpatchable vulnerabilities and the exploitation of misconfigurations highlight the ongoing challenge of securing complex systems against determined adversaries. Looking ahead, it is crucial for organizations to adopt a multi-layered security strategy that includes advanced detection capabilities, regular security training for employees, and a proactive approach to vulnerability management and patching. Additionally, collaboration between industries and

sharing of threat intelligence will be key to staying ahead of emerging cyber threats. As geopolitical tensions continue to influence cyber operations, organizations must also be prepared for the possibility of state-sponsored attacks targeting critical infrastructure and key industries.

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

📈 821% [CVE-2024-27199](#)

- A path traversal vulnerability in JetBrains TeamCity

📈 68% [CVE-2023-30185](#)

- A file upload vulnerability in some versions of CRMEB

📈 3% [CVE-2023-35078](#)

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

Frequently Targeted Israeli Site Sees 3.5M RPS Attack

+Israel +Financial Services +DDoS

- A frequently targeted Israeli financial services site experienced its largest application-layer DDoS attack yet this week, with an hour-long attack reaching 3.5M requests per second (RPS). The attack came from over 13,000 unique IP addresses, meaning the attacker had access to a large botnet. This site has been attacked over 15 times since the beginning of the year with large DDoS attacks, probably coming from financial or politically-motivated attackers.

ATO Attack on US Car Rental Company

+Automotive +US +ATO

- A US car rental company saw an account takeover (ATO) attack this week that came almost entirely from compromised credentials. There are no known data breaches involving this company, so it's likely the attacker acquired the credentials from third-party breaches or credential stuffing.

Recent Cyber Threats

Keystroke Prediction Through Acoustic Analysis

+Side-Channel Attack

- Researchers have developed an [acoustic side-channel attack](#) capable of deducing keystrokes from typing patterns, achieving a 43% success rate even in noisy environments. This method does not require controlled conditions or specific typing platforms, making it a viable threat in real-world scenarios. The attack leverages the distinct sound emissions of keystrokes, captured via specialized software, to predict user input.

Operation PhantomBlu Deploys NetSupport RAT

+PhantomBlue +Phishing

- Operation [PhantomBlu](#) has been identified as a sophisticated campaign delivering the NetSupport RAT through evasive methods. The attackers utilize crafted phishing emails to trick victims into executing malicious payloads,

effectively bypassing traditional security measures. This campaign targets various sectors, highlighting the need for heightened awareness and defense strategies against such evasive threats.

AcidPour Malware Variant Spotted

+AcidRain +AcidPour +Russia

- A new variant of the AcidRain malware that targeted ViaSat modems in 2022 has been seen in the wild, dubbed [AcidPour](#). The malware may be part of a larger Russian disruption, demonstrating the evolving landscape of cyber warfare and posing a severe impact on national security and civilian infrastructure.

Sysrv Botnet Variant Exploits Google Subdomains

+Sysrv +XMRig +Cryptominer

- A new variant of the [Sysrv](#) botnet has been discovered making use of Google subdomains to spread the XMRig miner, targeting vulnerable Windows and Linux servers. This strategy enhances the botnet's ability to evade detection and underscores the importance of robust cybersecurity measures to protect against such sophisticated threats.

SmokeLoader Malware Targets Financial Institutions

+SmokeLoader +Financial Services +Ukraine +Russia

- [SmokeLoader](#) malware has been actively targeting financial institutions in Ukraine, attributed to Russian cybercriminals. This campaign not only disrupts financial operations but also poses significant risks to the confidentiality and integrity of sensitive financial data, highlighting the ongoing cyber threats in the context of geopolitical tensions.

Loop DoS Attack Uncovered

+DoS +Loop +UDP

- Researchers have identified a new denial-of-service attack, named [Loop DoS](#), affecting up to 300,000 systems globally. The attack exploits a vulnerability in the UDP protocol, allowing attackers to create a self-perpetuating traffic loop, potentially leading to service instability or network outages. Vendors like Broadcom, Cisco, Honeywell, Microsoft, and MikroTik are affected.

Malware Campaign Targets Android Users in India

+MaaS +India +Android

- A malware-as-a-service (MaaS) campaign is actively targeting [Android users in India](#), distributing malicious APKs to steal banking information and SMS messages. The campaign disguises itself under useful applications, posing a significant threat to personal data security.

Unpatchable Vulnerability in Apple M-Series Chips

+Apple

- An unpatchable vulnerability in [Apple's M-series chips](#) could expose secret encryption keys, posing a significant security risk. The flaw, inherent in the chip's architecture, allows attackers to extract sensitive data during cryptographic operations, affecting Mac devices globally.

Unsaflok Flaw in Hotel Door Locks

+Travel +Unsaflok

- Over 3 million Saflok electronic RFID locks in hotels worldwide are vulnerable to the [Unsaflok](#) flaw, discovered by researchers. This series of vulnerabilities allows attackers to unlock any door within a hotel, posing a significant security risk to the hospitality industry.

Apex Legends Tournament Hacked

+Gaming +RCE

- The North American finals of the [Apex Legends Global Series](#) were postponed after players were compromised mid-match by hackers exploiting a potential remote code execution flaw. The incident, which affected players' game clients with unauthorized cheat tools, marks an unprecedented security breach in the tournament's history.

Data Breaches

Hackers Claim Massive Data Breach at Viber

+Handala Hack +Hacktivism

- https://www.hackread.com/hackers-claim-740gb-of-data-viber-messaging-app/?web_view=true
- Pro-Palestinian group [Handala Hack](#) claims to have accessed 740GB of data from Viber, including its source code, demanding a ransom of 8 Bitcoin. Viber denies the breach but is investigating the claim. The data allegedly includes user information, sparking concerns over privacy and security.

AT&T Denies Data Leak Claims

+Telecommunications

- [AT&T](#) refutes claims that data affecting 71 million individuals originated from their systems, despite a hacker's assertion of a 2021 breach. The leaked data includes sensitive personal information, but its source remains unconfirmed, raising questions about data security and privacy.

MediaWorks NZ Faces Data Breach Extortion

+New Zealand +Entertainment

- [MediaWorks](#) in New Zealand investigates a hacker's claim of stealing data on 2.4 million individuals, now facing extortion. The breach involves competition entry data, including personal information but not financial details. The incident underscores the growing threat of cyber extortion.

Massive Firebase Misconfiguration Exposes Data

+Database Misconfiguration

- A study reveals a widespread [Firebase](#) misconfiguration, leading to the exposure of approximately 125 million user records across 900 sites. The exposed data includes plaintext passwords and sensitive billing information, highlighting the risks of cloud storage misconfigurations.

Iranian Hackers Allegedly Target Israeli Nuclear Facility

+Israel +Iran +Critical Infrastructure

- An Iran-linked hacking group claims to have breached the [Shimon Peres Negev Nuclear Research Center](#) in Israel, releasing documents as a protest against the war in Gaza. While there's no evidence of operational technology compromise, the incident raises concerns about cybersecurity in critical infrastructure.

SCAA Cyberattack Compromises Member Data

+China

- The [South China Athletic Association](#) (SCAA) reports a cyberattack affecting its servers, potentially compromising the personal data of 70,000 members. The breach prompts an investigation and recommendations for members to secure their personal information, highlighting the importance of cybersecurity in protecting sensitive data.

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