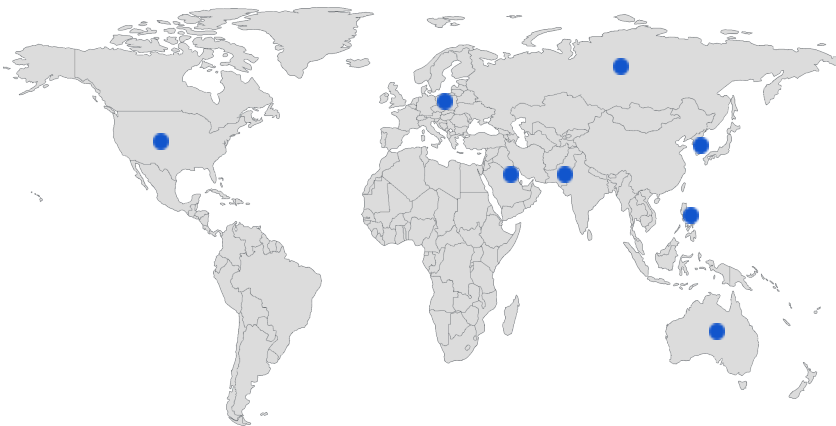


Threat Intel Report: June 17-23, 2024

Countries



Top Tags

NiceRat

Oyster

PHANTOM#SPIKE

Snowflake

Powershell

Executive Summary

Actionable Information:

- **Increasing Sophistication of Exploits and Malware Campaigns:** Cyber threats are becoming more advanced, with attackers leveraging zero-day vulnerabilities and sophisticated malware to infiltrate systems. Organizations must prioritize timely patching and employ advanced threat detection systems to counter these evolving threats.
- **Data Security and Breaches:** There is a rising trend in data breaches across various sectors, from retail and automotive to education and food services. Implementing robust data protection protocols and immediate response strategies is crucial to mitigate the impact of these breaches.
- **Social Engineering and Deceptive Tactics:** The effectiveness of social engineering techniques, such as fake error messages and malvertising, continues to grow. Enhancing user awareness and education is essential to prevent falling victim to these tactics.
- **Cyber Warfare and Politically Motivated Attacks:** Politically motivated cyber attacks, such as DDoS attacks on critical infrastructure and events, are increasing. Enhanced cybersecurity measures and international cooperation are necessary to protect against these threats.

Outlook:

The cyber threat landscape is increasingly characterized by sophisticated exploits, targeted malware campaigns, and significant data breaches. The persistence of politically motivated attacks and advanced social engineering techniques highlights the need for comprehensive cybersecurity strategies. Organizations must adopt proactive measures, prioritize timely updates, and enhance user education to protect against these evolving threats. Continuous monitoring and improvement of security practices are essential to safeguard sensitive information and maintain resilience against cyber attacks.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 1146% [CVE-2024-2879](#)

- A SQL injection vulnerability in the LayerSlider plugin for WordPress

↑ 434% [CVE-2023-49070](#)

- A pre-authenticated RCE vulnerability in Apache Ofbiz

↑ 255% [CVE-2024-20767](#)

- An improper access control vulnerability in Adobe ColdFusion

US Computing Site Targeted in 2.6M RPS DDoS Attack

+US +Computing +DDoS

- A US computing company was targeted this week in a 2.6M RPS DDoS attack, coming from almost 11,000 IPs. The attacks, mainly coming from US and Great Britain-based IPs, came from bots and Chrome.

Kuwaiti Travel Site Attacked with SQLi and RCE

+Kuwait +Travel

- A Kuwaiti travel site was targeted by SQL injection (SQLi) and remote code execution (RCE) attacks this week, coming from US-based IPs. The attacks were conducted by malicious bots, and probably aimed to access personal information about users.

Recent Cyber Threats

ARM TikTag Attack Targets Google Chrome and Linux Systems

+Chrome +Linux +TikTag

- A newly discovered [TikTag](#) attack impacts Google Chrome and Linux systems by exploiting vulnerabilities in ARM processors. This attack allows threat actors to bypass Chrome's security features and gain control over Linux systems by manipulating pointer authentication codes. The attack highlights significant weaknesses in the implementation of ARM's security features, necessitating urgent updates and patches to mitigate potential risks.

NiceRat Malware Targets South Korean Organizations

+NiceRat +South Korea +Malware

- The [NiceRat](#) malware has been detected targeting South Korean organizations through sophisticated phishing campaigns. This malware, distributed via malicious email attachments, grants attackers remote access to infected systems, enabling them to steal sensitive data and conduct espionage. The NiceRat campaign underscores the persistent threat of malware in the region and the critical need for heightened email security and user awareness training.

SolarWinds Serv-U Vulnerability Exploited

+CVE +SolarWinds

- A critical vulnerability in SolarWinds Serv-U, identified as [CVE-2024-28995](#), has been actively exploited by cybercriminals to gain unauthorized access and execute arbitrary code on affected systems. This vulnerability, which affects the Serv-U Managed File Transfer and Serv-U Secure FTP products, poses severe security risks by

potentially allowing attackers to breach network defenses and access sensitive data. Organizations using these products are urged to apply patches immediately to mitigate potential threats.

Critical Flaws in VMware vCenter Discovered

+VMWare +CVE

- Security researchers have identified multiple critical vulnerabilities in [VMware](#) vCenter, including issues that allow for remote code execution and privilege escalation. These vulnerabilities, if exploited, can enable attackers to take full control of virtualized environments, disrupt services, and access sensitive information. VMware has released patches and updates to address these flaws, urging administrators to implement them promptly to secure their systems.

Fake Google Chrome Errors Deploy Malicious PowerShell Scripts

+Chrome +PowerShell

- Cybercriminals are deploying fake [Google Chrome](#) error messages to deceive users into executing malicious PowerShell scripts. These scripts facilitate the download and execution of additional malware, allowing attackers to gain control of the infected systems, exfiltrate data, and perform further malicious activities. This attack vector highlights the effectiveness of social engineering techniques and the importance of user education to recognize and avoid such threats.

Mailcow Mail Server Flaws Expose Sensitive Data

+CVE

- Several critical vulnerabilities have been identified in the [Mailcow](#) mail server software, exposing sensitive data to potential attackers. These flaws include issues with input validation and authentication, which could allow unauthorized access to email accounts and data leaks. Administrators are urged to apply patches and implement additional security measures to protect their mail servers from exploitation.

Malvertising Campaign Leads to Oyster Backdoor Execution

+Oyster

- A recent malvertising campaign has been uncovered, leading to the execution of the [Oyster](#) backdoor. This sophisticated attack uses malicious ads to deliver malware that grants attackers remote access to infected systems, enabling data theft and espionage. The campaign highlights the ongoing threat of malvertising and the need for robust ad-blocking and security measures.

Military-Themed Emails Used to Spread Malware

+PHANTOM#SPIKE +Pakistan

- Attackers are using military-themed phishing emails to spread malware, targeting defense and government sectors in Pakistan in a new campaign known as [PHANTOM#SPIKE](#). These emails contain malicious attachments that, when opened, install malware on the victim's system, enabling data theft and espionage. This tactic highlights the importance of user education and robust email security measures to defend against targeted phishing attacks.

Data Breaches

Poland Blames Russia for Euro 2024 DDoS Attack

+Poland +Russia +DDoS +Sports

- Poland has accused Russian hackers of launching a DDoS attack on the online broadcast of the [Euro 2024](#) football tournament. The attack disrupted streaming services, affecting viewers across Poland and highlighting the ongoing cyber conflict between Russia and European nations. This incident underscores the need for enhanced cybersecurity measures to protect against politically motivated attacks.

Levi's Data Breach Exposes Data of 72,000 Customers

+Retail

- A data breach at [Levi's](#) has exposed the personal information of 72,000 customers. The compromised data includes names, addresses, and contact information, potentially putting affected individuals at risk of identity theft and phishing attacks. Levi's is investigating the breach and has implemented additional security measures to prevent future incidents.

CDK Global Suffers Data Breach During Recovery Efforts

+Automotive

- [CDK Global](#) experienced a data breach while attempting to recover from a previous security incident. The breach resulted in the exposure of sensitive customer data, including financial information, affecting numerous clients in the automotive industry. This highlights the risks associated with recovery processes and the need for stringent security protocols during such operations.

Snowflake Data Breach Hits Los Angeles School Board

+US +Education +Snowflake

- A data breach involving Snowflake has compromised the [Los Angeles School Board](#), resulting in the theft of data on thousands of students. The stolen information includes personal and academic records, raising concerns about student privacy and data protection. The incident emphasizes the importance of robust security measures in educational institutions.

Jollibee Investigates Alleged Data Breach Affecting Millions

+Food & Beverage +Philippines

- [Jollibee](#), a popular Filipino fast-food chain, is investigating an alleged data breach that may have exposed the personal information of millions of customers. The breach reportedly involves sensitive data, including payment information, which could lead to significant financial and reputational damage. The company is working with cybersecurity experts to determine the breach's scope and mitigate its impact.

TEG Ticket Sales Data Breach Potentially Hits Millions

+Australia +Ticketing

- A data breach at [TEG](#), a major Australian ticket sales platform, has potentially exposed the personal information of millions of users. The breach includes customer names, contact details, and payment information, putting affected individuals at risk of fraud and identity theft. TEG is investigating the incident and implementing additional security measures to protect user 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.