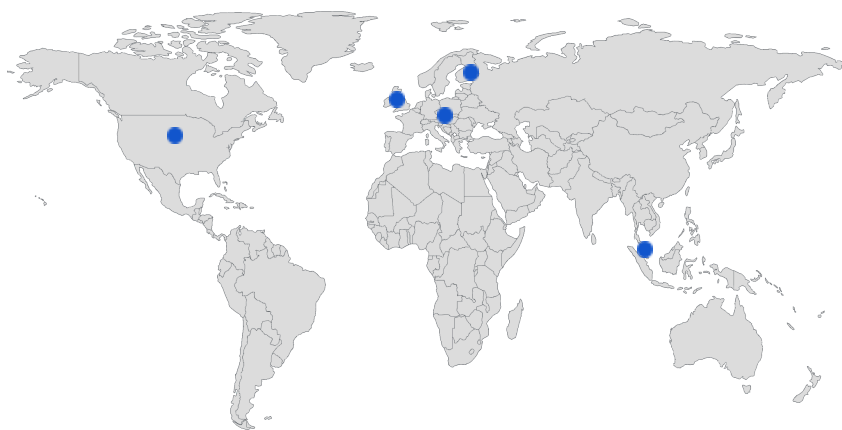


Threat Intel Report: May 6-12, 2024

Countries



Top Tags

Moobot

APT28

LockBit

Cuckoo

WordPress

Executive Summary

Actionable Information:

- *Exploitation of Established Software and Tools:* Malicious actors continue to leverage popular software and services such as VPNs, WordPress, and Microsoft Azure, utilizing existing vulnerabilities for unauthorized access and control. Monitoring and timely updates of these platforms are crucial.
- *Innovative Malware Techniques:* The rise of Android malware in Finland, Cuckoo malware on macOS, and sophisticated Remote Access Trojans indicate a trend toward more clever and targeted attacks, suggesting the need for advanced threat detection systems.
- *Persistent and Adaptive Threats:* The resilience of threats like the Moobot botnet and ongoing exploitation of older vulnerabilities such as those in D-Link devices highlight the adaptive nature of threat actors and the importance of sustained vigilance and updated defense mechanisms.
- *Cyber Espionage and Data Theft:* High-profile attacks on infrastructure such as the Baidu Apollo platform and breaches involving sensitive data from the UK military and major corporations underscore the ongoing risks of espionage and data theft.

Outlook:

The landscape of cyber threats is increasingly complex and dangerous, with adversaries not only exploiting existing technologies but also innovating to circumvent newly implemented security measures. The trend of using trusted platforms and software to deploy malware presents significant challenges, as it exploits the inherent trust users and organizations place in these systems. Furthermore, the persistence of botnets and the resurgence of older vulnerabilities indicate that threats not only evolve but also adapt to defensive measures over time. As we look to the future, it is

imperative for organizations to invest in comprehensive security solutions that include both proactive and reactive strategies. This involves enhancing real-time threat detection, improving the security of mobile and cloud platforms, and fostering a culture of security awareness across all levels of the organization. Additionally, as the intersection of technology and traditional industries becomes more pronounced, the scope of potential cyber threats broadens, necessitating a multidisciplinary approach to cybersecurity.

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

📈 29% [CVE-2024-27199](#)

- A path traversal vulnerability in JetBrains TeamCity

📈 50% [CVE-2023-30185](#)

- A file upload vulnerability in some versions of CRMEB

📈 4% [CVE-2023-35082](#)

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

Czech Electrical Site Targeted By Automated Attacks

+Czechia +Electrical +Automated Attacks +Path Traversal +US

- A Czech electrical website was targeted this week with automated attacks and path traversal. The attacks came from just over 200 US-based IPs, and primarily targeted legacy software.

Bots Attempt API Violation on Singaporean Site

+Singapore +Gambling +API Violation

- A Singaporean gambling site was targeted by API violations this week, coming from 300 Singapore-based IPs. The attack, which came primarily from bots, targeted API user portals.

Recent Cyber Threats

Persistent Threat of Moobot Botnet Remains Unchecked

+Moobot +APT28 +Russia +Botnet

- The [Moobot botnet](#), managed by Russia-linked APT28 and supported by Pawn Storm, exploits Ubiquiti EdgeRouters for a variety of malicious activities including credential harvesting, spear-phishing, and traffic proxying. The botnet has shown resilience by regenerating its command and control infrastructure even after FBI-led takedown efforts, indicating persistent cyber threat capabilities. The botnet's activities are primarily espionage and financial gain through cyber operations.

Recurrent Disruption of LockBit Ransomware Operations

+LockBit

- Global law enforcement recently seized the web operations of the [LockBit](#) ransomware group for the second time, demonstrating ongoing efforts to combat cybercrime networks. This seizure is part of a broader strategy to disrupt the infrastructure of ransomware operators who have been particularly active in targeting various industries for extortion.

Rise in Android Malware Threatening Finnish Financial Security

+Finland +Android +Malware

- Cybersecurity warnings in Finland have escalated with reports of [Android malware](#) specifically targeting bank accounts. The malware engages in unauthorized transactions and captures sensitive financial information, significantly impacting the financial security of individuals and institutions. The malware's sophisticated methods of breaching security highlight an urgent need for enhanced protective measures in mobile banking.

Critical Security Update for Citrix Networking Products

+Citrix +CVE

- [Citrix](#) has responded to a high-severity vulnerability in its NetScaler ADC and Gateway products, which are crucial for secure network traffic management. The vulnerability, if exploited, could allow unauthorized remote access, potentially leading to data breaches and significant operational disruption. The update is vital for maintaining the security integrity of networked environments.

New Cuckoo Malware Exploits macOS via Compromised Applications

+Cuckoo +Malware +macOS

- The newly identified [Cuckoo](#) malware, spreading through tampered music converter applications, targets macOS users by stealing credentials and cryptocurrency. This strategy not only highlights the ingenuity of cybercriminals in finding new infection vectors but also raises concerns over the security of commonly downloaded applications and their potential for being weaponized.

Exploit in WordPress Affects Tens of Thousands of Sites

+WordPress +CVE

- The discovery of [CVE-2024-2876](#) has led to over 90,000 WordPress websites being compromised. The exploit allows unauthorized modifications and access, posing a severe security risk to a vast number of digital content managers worldwide. This widespread vulnerability underscores the critical importance of regular security audits and updates in content management systems.

VPN Security Undermined by Innovative Cyber Attack Technique

+VPN

- A novel cyber attack has been reported that effectively neutralizes the security measures of almost all [VPN applications](#), exposing users to potential data breaches and surveillance. This attack compromises the very purpose of VPNs—ensuring secure and private online connections—highlighting a significant flaw in current VPN technologies and the necessity for advanced security protocols.

Critical Remote Code Execution Vulnerability in Tinyproxy

+RCE +Tinyproxy +CVE

- Nearly 52,000 internet-exposed Tinyproxy servers are vulnerable to a critical remote code execution (RCE) flaw, [CVE-2023-49606](#). This vulnerability, found in the proxy server software's function for removing specific HTTP headers, could lead to unauthorized code execution via a simple malformed HTTP request.

Exploitation of LiteSpeed Cache Flaw to Compromise WordPress Sites

+WordPress +CVE

- Hackers are exploiting a vulnerability in [LiteSpeed Cache](#), a popular WordPress plugin, to illicitly create admin accounts on WordPress sites. This flaw allows attackers to execute PHP code remotely, granting them administrative access and control over websites. The impact of this vulnerability is significant given the widespread use of LiteSpeed Cache among WordPress users, posing risks of data breaches and unauthorized site modifications.

Undetected Threats in F5's Central Management System

+F5 +Healthcare

- A report highlights that [F5's Central Manager](#), widely used in healthcare and other critical sectors, contains undetectable threats due to sophisticated evasion techniques. These threats can persist undetected within

networks, potentially leading to data breaches and significant disruptions in services. The findings emphasize the need for advanced detection mechanisms and heightened vigilance in network security management.

Bypassing Multi-Factor Authentication in Microsoft Azure Entra Identity Services

+MFA +Microsoft

- Researchers have demonstrated a method to bypass [multi-factor authentication](#) (MFA) in Microsoft Azure Entra's Single Sign-On (SSO) service. This vulnerability exposes users to potential unauthorized access despite using MFA, highlighting the ongoing challenges in securing authentication processes against sophisticated cyber attacks.

Vulnerability Exploitation in Ivanti Pulse Secure VPN Devices

+VPN +Ivanti

- A significant security vulnerability in [Ivanti Pulse Secure](#) VPN devices is being actively exploited, allowing unauthorized access to network resources. This exploitation is part of a broader trend of targeting VPN technologies, which are critical for secure remote access. The vulnerability underscores the necessity for timely updates and rigorous security protocols to protect network infrastructures.

Android Remote Access Trojan Targets User Credentials

+Android +RAT +Credential Harvesting

- A new [Android Remote Access Trojan](#) (RAT), equipped with sophisticated tools for credential harvesting, poses a serious threat to users. The malware can intercept and exfiltrate login details, banking information, and other sensitive data, demonstrating the increasing threat to mobile security and the need for comprehensive mobile device protection strategies.

Data Breaches

Security Breach in Baidu Apollo Autonomous Driving Platform

+Automotive

- The [Baidu Apollo](#) autonomous driving platform has been compromised through a sophisticated hack, affecting its operational security and data integrity. This breach not only highlights vulnerabilities in advanced vehicular technology but also raises concerns about the potential misuse of automotive data and the implications for user safety and privacy.

Data Breach Exposes UK Military Personnel Information

+UK +Government

- The [UK Defense Ministry](#) reported a significant data breach at a third-party payroll provider, impacting up to 272,000 military personnel and veterans. Personal and financial details were compromised, with suspicions of state-sponsored involvement. Immediate countermeasures included taking the system offline and launching an investigation to assess the extent and impact of the breach.

Innovative AI-Based Cyberattack Targets Cloud Credentials

+LLMJacking +Cloud

- A new form of cyberattack termed [LLMjacking](#) has emerged, where attackers use stolen cloud credentials to access and potentially exploit cloud-hosted AI services, incurring substantial costs. This attack demonstrates the vulnerabilities in cloud security, specifically around large language models (LLMs), and highlights the ongoing challenges in protecting cloud environments from sophisticated cyber threats.

Extensive Data Breach at JPMorgan Chase

+Financial Services

- [JPMorgan Chase](#) disclosed a data breach originating from a software flaw active since 2021, affecting 451,809 customers. Compromised data includes names, addresses, Social Security numbers, and bank details related to

retirement plans. The bank has rectified the issue and is offering credit monitoring services, although there's no evidence yet of misuse of the data.

Unpatched Flaw Leads to Data Breach in Helsinki

+Finland +Education

- A significant data breach occurred in [Helsinki's](#) education division due to an unpatched flaw in a remote access server. The breach exposed sensitive data of tens of thousands of students and staff, including personal IDs and addresses. The city is conducting an extensive investigation to determine the full scope and potential consequences of the incident.

Data Breach at Dell Technologies

+Computing

- [Dell Technologies](#) is investigating a data breach affecting a customer portal that exposed limited customer information, including names and physical addresses. The breach did not involve sensitive financial data. Dell has engaged law enforcement and forensic specialists to assess and mitigate any potential impacts of the breach.

Long-Term Impact Expected from Ascension Data Breach

+US +Healthcare

- [Ascension Healthcare System](#) is grappling with the aftermath of a cyberattack that has disrupted its electronic medical records system, affecting operations at two major hospitals in Nashville. The breach has forced the postponement of non-essential medical procedures and raised concerns about the safety of personal information in the healthcare sector.

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