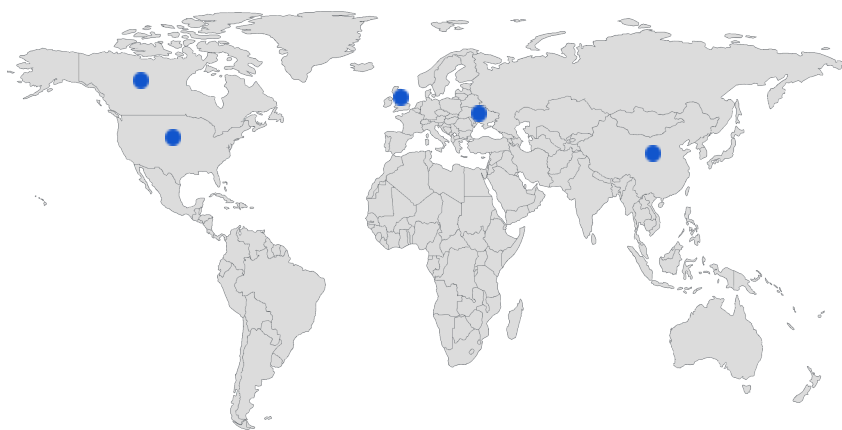


Threat Intel Report: August 19-25, 2024

Countries



Top Tags

UNC4536

Velvet Ant

Cthulhu Stealer

nGate

MOVEit

Executive Summary

Actionable Information:

- **Increased Targeting of Critical Infrastructure and Financial Services:** Multiple incidents this week, including attacks on the Florida Department of Health, Patelco Credit Union, and Monobank, highlight an ongoing trend of cybercriminals focusing on critical infrastructure and financial services. These sectors remain prime targets due to the sensitive nature of the data they handle and their critical role in national security and economic stability.
- **Rising Threats from State-Sponsored Actors and APTs:** The discovery of China's Velvet Ant APT exploiting zero-day vulnerabilities in Cisco switches underscores the increasing sophistication of state-sponsored attacks, particularly against telecommunications infrastructure. These threats often go undetected for extended periods, allowing attackers to cause significant damage.
- **Ongoing Exploitation of Known Vulnerabilities:** The new Log4j campaign and the active exploitation of the LiteSpeed Cache plugin in WordPress sites reveal that many organizations are still failing to patch widely known vulnerabilities. This negligence leaves them vulnerable to opportunistic attacks that could have been easily prevented.
- **Emergence of Novel Malware and Exploits:** The appearance of the Cthulhu Stealer malware targeting macOS users and nGate malware hijacking NFC traffic on Android devices shows that cybercriminals are diversifying their tactics. These sophisticated attacks exploit lesser-protected systems, highlighting the need for continuous adaptation of security strategies.
- **Security Weaknesses in Cloud-Based and Mobile Platforms:** The Unicorn hack via GSuite and privilege escalation vulnerabilities in Azure Kubernetes Service demonstrate the growing risks associated with cloud-based services. As businesses increasingly rely on cloud infrastructure, attackers are exploiting these platforms to gain unauthorized access to sensitive data.

Outlook:

The cybersecurity landscape continues to evolve rapidly, with both state-sponsored actors and cybercriminals leveraging increasingly sophisticated tactics to exploit vulnerabilities across various industries. The consistent targeting of critical infrastructure, financial services, and cloud-based platforms suggests that these sectors will remain under significant threat. Organizations must prioritize timely patching, robust incident response strategies, and continuous monitoring to defend against these evolving threats. As new vulnerabilities and malware emerge, proactive defense measures and cross-industry collaboration will be essential to mitigate risks and protect sensitive data from being compromised.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

📈 340% [CVE-2024-23897](#)

- Some versions of Jenkins do not disable a feature of its CLI command parser that replaces an '@' character followed by a file path in an argument with the file's contents, allowing unauthenticated attackers to read arbitrary files on the Jenkins controller file system.

📈 242% [CVE-2023-40044](#)

- In WS_FTP Server versions prior to 8.7.4 and 8.8.2, a pre-authenticated attacker could leverage a .NET deserialization vulnerability in the Ad Hoc Transfer module to execute remote commands on the underlying WS_FTP Server operating system.

📈 94% [CVE-2023-49070](#)

- Pre-auth RCE in Apache Ofbiz due to XML-RPC no longer maintained but still present.

US Travel Site Targeted by Business Logic

+US +Travel +Business Logic

- A US travel site recently experienced a two-day business logic attack, which was executed using automated tools. These attacks exploited vulnerabilities in the site's processes, aiming to disrupt operations and potentially harvest sensitive data. The malicious traffic originated from US-based IP addresses, suggesting a compromised network within the country.

US Education Site Experiences Short but Intense DDoS Attack

+US +Education +DDoS

- A US-based education site was hit by an application-layer DDoS attack this week, with traffic peaking at 1.3 million requests per second (RPS). Despite the high volume of malicious requests, the attack lasted only 7 minutes, demonstrating the attackers' ability to inflict significant disruption in a short time frame.

Recent Cyber Threats

Security Flaws Expose UK Political Campaigns

+UK +Government +Election Security

- Critical security flaws have been discovered in the websites of several [UK political campaigns](#), making them vulnerable to cyberattacks. These vulnerabilities could allow attackers to manipulate campaign content, steal sensitive data, or disrupt campaign activities. The exposure of these flaws raises concerns about the integrity of political processes in the lead-up to national elections.

Monobank Targeted by DDoS Amid Ukraine Donations Surge

+Ukraine +Financial Services +Hacktivism +DDoS

- Ukraine's [Monobank](#) suffered a significant DDoS attack this week, coinciding with a surge in donations to support the country's defense efforts. The attack aimed to disrupt the bank's online services, potentially hindering financial support for Ukraine during a critical time. This incident highlights the ongoing cyber threats faced by Ukrainian institutions amid the ongoing conflict.

Oracle NetSuite Exposes Customer Data on E-Commerce Sites

+eCommerce +CVE

- Security researchers have identified vulnerabilities in [Oracle NetSuite's](#) e-commerce platforms that expose customer data, including payment information. These flaws could be exploited by cybercriminals to steal sensitive customer details, leading to potential financial fraud and reputational damage for businesses using the platform. Companies are urged to apply security patches immediately to mitigate the risk.

Microsoft macOS Apps Vulnerable to Malicious Library Injection

+macOS +Library Injection

- Multiple [Microsoft applications](#) on macOS have been found vulnerable to malicious library injection attacks, which could allow attackers to execute arbitrary code on affected systems. These vulnerabilities pose a significant risk to remote workers relying on Microsoft apps, emphasizing the need for prompt updates to prevent exploitation.

Cybercriminals Disguise Malware as Popular Software

+UNC4536 +FakeBat +Malware

- Threat group UNC4536 is conducting malvertising campaigns distributing a loader called [FakeBat](#), passing the malware off as legitimate software. The infection utilizes a trojanized MSIX installer, which executes a PowerShell script to download a secondary payload. Attack chains propagating the loader malware make use of drive-by download techniques to push users searching for popular software toward bogus lookalike sites that host booby-trapped MSI installers.

Privilege Escalation Discovered in Azure Kubernetes Service

+Privilege Escalation +Azure

- A serious privilege escalation vulnerability has been identified in [Azure Kubernetes Service](#) (AKS), potentially allowing attackers to gain unauthorized access to cloud resources. This flaw could be exploited to compromise entire cloud environments, posing significant risks to organizations relying on AKS for their cloud infrastructure. Microsoft has issued patches, and users are urged to apply them without delay.

China's Velvet Ant APT Exploits Zero-Day in Cisco Switches

+Velvet Ant +China +Telecommunications

- The China-based [Velvet Ant](#) APT group has been found exploiting a zero-day vulnerability in Cisco switches, allowing them to gain unauthorized access to telecom infrastructure. This sophisticated attack leverages previously unknown flaws in the switches, enabling the attackers to intercept and manipulate network traffic. The discovery raises concerns about the security of critical network infrastructure globally, particularly in sectors relying heavily on Cisco equipment.

Zero-Click Vulnerability in Microsoft Outlook Revealed

+CVE

- A severe zero-click vulnerability in [Microsoft Outlook](#), identified as CVE-2024-38021, has been disclosed. This flaw allows attackers to compromise Outlook accounts without user interaction, posing a significant risk to individuals and organizations. The vulnerability underscores the importance of keeping software updated and highlights the evolving nature of threats targeting widely-used communication tools.

LiteSpeed Cache Plugin Exploited in Over 30,000 Attacks

+WordPress

- The [LiteSpeed Cache](#) plugin, popular among WordPress users, has become the target of active exploitation, with over 30,000 attacks blocked in just 24 hours. The vulnerability, tracked as CVE-2024-28000, allows attackers to execute arbitrary commands, potentially leading to website defacement or data theft. Site administrators are urged to update the plugin immediately to prevent further exploitation.

Shanghai Fudan RFID Cards Found with Backdoor

+Manufacturing +China +Government

- RFID cards manufactured by [Shanghai Fudan Microelectronics](#) have been discovered to contain a backdoor, potentially allowing unauthorized access to secure facilities. The backdoor was uncovered in the cryptographic mechanism of the cards, which are widely used in government and corporate settings. This revelation has sparked concerns over the security of RFID-based access systems and the potential for espionage.

New Log4j Campaign Exploits Unpatched Systems

+Log4j

- A new opportunistic campaign exploiting the infamous [Log4j](#) vulnerability has been detected, targeting unpatched systems across various industries. Despite the vulnerability being widely publicized since late 2021, attackers are still finding success due to incomplete patching and awareness gaps. This ongoing exploitation highlights the need for continuous vigilance and thorough patch management in organizations.

Cthulhu Stealer Malware Targets macOS Users

+Cthulhu Stealer +macOS +Malware

- The newly identified [Cthulhu Stealer](#) malware is targeting macOS users, designed to exfiltrate sensitive information such as credentials and financial data. This malware operates stealthily, avoiding detection by traditional antivirus software, and poses a significant threat to macOS users, particularly those who are less aware of security practices. The rise of Cthulhu Stealer emphasizes the increasing focus of cybercriminals on macOS platforms.

nGate Android Malware Hijacks NFC Traffic to Steal Funds

+nGate +Android +Malware

- The [nGate](#) malware, a new Android threat, has been discovered hijacking NFC traffic to steal funds from contactless payment systems. By intercepting and relaying NFC transactions, the malware allows attackers to siphon off money from victims' accounts undetected. This sophisticated attack method highlights the evolving risks associated with mobile payments and the need for enhanced security in mobile financial apps.

Data Breaches

Unicoin Cryptocurrency Company Hacked via GSuite

+Financial Services +Crypto

- The [Unicoin](#) cryptocurrency company recently fell victim to a security breach that compromised its GSuite accounts. Hackers exploited weaknesses in the email and collaboration platform to access sensitive company data, raising concerns about the security of cloud-based tools in the rapidly growing cryptocurrency sector. This breach underscores the importance of robust security measures for companies operating in digital finance.

Florida Department of Health Discloses Data Breach

+US +Healthcare +Government

- The [Florida Department of Health](#) has reported a significant data breach affecting an undisclosed number of individuals. The breach involved unauthorized access to the department's systems, potentially compromising sensitive health and personal information. This incident highlights the ongoing vulnerabilities in public health systems and the critical need for enhanced cybersecurity measures to protect patient data.

Park 'N Fly Breach Exposes Personal Data of 1M Canadians

+Financial Services +Canada

- [Park 'N Fly](#), a popular airport parking service, has disclosed a data breach that exposed the personal information of 1 million Canadian customers. The compromised data includes names, addresses, and payment details, posing significant risks of identity theft and fraud. The breach has sparked concerns over the security practices of service providers handling large volumes of customer data.

Patelco Credit Union Notifies 726,000 Customers of Ransomware Breach

+US +Financial Services +Ransomware

- [Patelco Credit Union](#) has informed 726,000 customers of a ransomware attack that led to a data breach. The attackers encrypted sensitive data and demanded a ransom for its release, potentially exposing personal and financial information of the credit union's members. This incident underscores the growing threat of ransomware in the financial sector and the need for comprehensive data protection strategies.

Credit Union Reveals Delayed Notification of MOVEit Data Breach

+US +Financial Services +MOVEit

- A US-based credit union has issued a belated notification regarding a data breach linked to the [MOVEit](#) file transfer software vulnerability. The breach, which occurred months earlier, compromised sensitive customer data but was only recently disclosed, raising concerns about the timeliness and transparency of breach notifications in the financial services industry.

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.