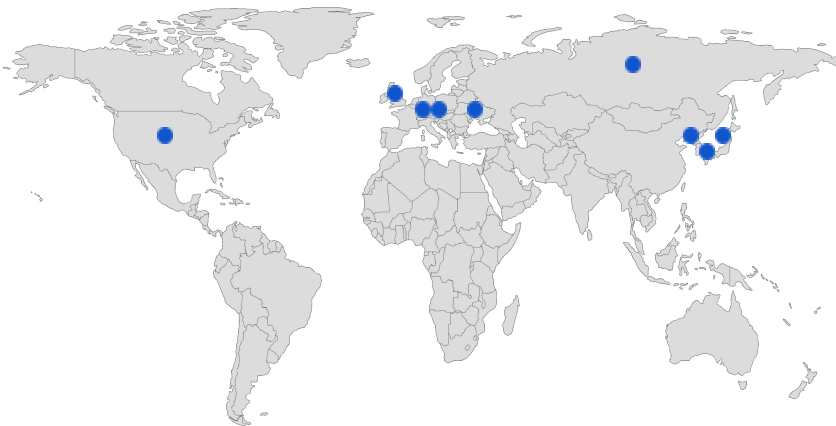


Threat Intel Report: October 7-20, 2024

Countries



Top Tags

Lazarus

APT29

Kimsuky

NoName057(16)

Kyiv's Cyber Patriots

Executive Summary

Actionable Information:

- **Increased Focus on State-Sponsored Cyber Espionage:** State-backed cyber actors continue to target sensitive industries, including government, financial services, and defense. These attackers are leveraging sophisticated malware and exploiting vulnerabilities to gain unauthorized access and exfiltrate critical data.
- **Zero-Day Exploits and Software Vulnerabilities:** The discovery of multiple zero-day vulnerabilities affecting major operating systems and widely-used applications highlights the ongoing need for proactive vulnerability management.
- **Ransomware as a Growing Threat to Essential Services:** Ransomware continues to be a significant threat, particularly for critical infrastructure such as healthcare and government services.
- **Cloud Infrastructure and Industrial Systems Under Attack:** Cloud environments and industrial control systems (ICS) are increasingly targeted by sophisticated malware and attackers exploiting specific protocol vulnerabilities.

Outlook:

The past two weeks reflect a continuation of several key trends: the persistent risk posed by state-backed cyber-espionage groups, the increasing sophistication of malware targeting both cloud infrastructure and critical industries, and a notable rise in data breaches across financial and government sectors. Looking ahead, we anticipate that cyber-espionage activities from groups like APT29 and Lazarus will continue to evolve, targeting vulnerabilities in enterprise systems and cloud platforms. Ransomware attacks, especially against healthcare and critical services, are expected to rise, necessitating stronger resilience measures. Additionally, the rapid pace of zero-day discoveries underscores the importance of proactive patch management and threat intelligence integration into security strategies.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

- ⬆ 26,118% [CVE-2024-9465](#)

 - An SQL injection vulnerability in Palo Alto Networks Expedition allows an unauthenticated attacker to reveal Expedition database contents.
- ⬆ 381% [CVE-2023-28343](#)

 - OS command injection affecting Altenergy Power Control Software.
- ⬆ 333% [CVE-2023-29298](#)

 - Adobe ColdFusion is affected by an Improper Access Control vulnerability that could result in a Security feature bypass.

Japanese Companies Hit by Three-Day Onslaught

+Japan +Telecommunications +DDoS +XSS +Automated Attack +Path Traversal +Hacktivism

- Japanese telecommunications companies were targeted by a variety of attacks this week. Over a three-day period, several Japanese companies in the industry were targeted by DDoS, automated attacks, path traversal, and cross-site scripting (XSS), related to Japanese military exercises near the coast of Russia.

Financial Sites Targeted by Backdoors

+US +Germany +Poland +Backdoor

- Several financial sites in the US, Germany, and Poland were targeted by backdoor attacks over the course of two days. Attacks came from automated tools primarily based in the US.

Recent Cyber Threats

Fake Job Applications Deliver Malware to Businesses

+Lazarus +North Korea +Business

- North Korean APT group [Lazarus](#) is using fake job applications as a vector to deliver the 'Lodeinfo' malware to organizations. The malware provides backdoor access and can exfiltrate sensitive data, primarily targeting Japanese businesses in finance and defense sectors. This campaign highlights the ongoing threat from North Korean state-backed hackers.

New macOS Safari Exploit Targets Camera, Microphone

+Mac +Safari

- A vulnerability in [macOS Safari](#) has been uncovered that allows attackers to gain unauthorized access to users' cameras, microphones, and browsing data. Attackers exploit a flaw in Safari's WebKit engine, putting millions of Apple users at risk. This vulnerability could be weaponized for surveillance or data theft.

APT29 Targets Zimbra and TeamCity Servers in Latest Campaign

+US +UK +Russia +APT29

- Recently, U.S. and U.K. cyber agencies have warned of a renewed [wave of attacks](#) led by Russian APT29 hackers. These sophisticated threat actors have been actively exploiting vulnerabilities in Zimbra Collaboration Suite and JetBrains TeamCity ([CVE-2022-27924](#) and [CVE-2023-42793](#)) to target critical systems. APT29, also known as

Cozy Bear, is exploiting vulnerabilities in these platforms to conduct espionage, likely aiming to steal sensitive information from governmental and private-sector organizations.

North Korean Hackers Deploy New Malware Against Government Agencies

+North Korea +Kimsuky +South Korea +US +Government

- North Korea's [Kimsuky](#) group has been observed using newly developed malware to target South Korean and U.S. government agencies. This malware, known for its stealthy operation, aims to exfiltrate sensitive information, including emails and classified documents. The campaign reflects ongoing cyber-espionage efforts by the North Korean government.

Perfct! Fileless Malware Infects Millions of Linux Servers

+Perfct! +Malware +Linux

- A newly discovered fileless malware, [Perfct!](#), is targeting millions of Linux servers globally, exploiting a vulnerability in the Perf performance monitoring tool. This sophisticated malware resides in memory, making it hard to detect, and allows attackers to execute arbitrary commands, steal credentials, and deploy further payloads. The attack poses a major threat to cloud infrastructure and web hosting services.

Trinity Ransomware Targets Medical Providers

+Trinity +Healthcare

- The U.S. Department of Health and Human Services has issued an alert warning healthcare providers of a growing threat from the [Trinity](#) ransomware group. This group specifically targets hospitals and other healthcare facilities, encrypting patient data and demanding ransom payments. The impact could disrupt medical services, making rapid recovery and prevention crucial.

Major Security Flaws Found in MMS Protocol

+ICS +MMS

- Multiple security vulnerabilities have been discovered in two implementations of the [Manufacturing Message Specification](#) (MMS) protocol used in industrial control systems that, if successfully exploited, could have severe impacts in industrial environments. The vulnerabilities could potentially allow remote code execution, or allow an attacker to crash an industrial device.

Popular Java Framework Vulnerable to RCE

+Java +RCE

- A critical vulnerability ([CVE-2023-25581](#)) in the Pac4j Java security framework has been identified, potentially allowing remote code execution (RCE). This flaw could enable attackers to compromise Java-based applications using the framework, posing risks for enterprises and developers relying on Pac4j for authentication and security services.

Tor Browser Users Targeted by Firefox Zero-Day

+Tor +Firefox +Zero-Day +Anonymity

- A recently patched zero-day vulnerability in Firefox is being actively exploited to target [Tor Browser](#) users. The vulnerability allows attackers to de-anonymize users, posing a significant threat to those relying on Tor for privacy and security, particularly in oppressive regimes. The exploit is likely used for surveillance or censorship.

Fake Google Meet Errors Deliver Info-Stealing Malware

+ClickFix +Google Meet +Malware

- A new ClickFix campaign is tricking users into downloading info-stealing malware by creating fake [Google Meet](#) error messages. The malware, distributed via phishing emails, is capable of stealing login credentials, browser cookies, and other sensitive information. Businesses relying on Google Meet should be vigilant about this emerging phishing campaign.

Russian DDoS Attacks on Japan Surge After Military Exercises

+NoName057(16) +Russia +Japan +DDoS

- Following recent military exercises between Japan and the U.S., Russian threat actor NoName057(16) launched a series of [DDoS](#) attacks on Japanese government and infrastructure websites. The attacks appear to be politically

motivated, disrupting services and signaling Russia's discontent with Japan's military collaboration. These attacks highlight geopolitical tensions manifesting in cyberspace.

Kyiv Hackers Launch Cyberattack on Russian State Media

+Ukraine +Russia +Kyiv's Cyber Patriots

- Ukrainian hacktivists known as [Kyiv's Cyber Patriots](#) launched a successful cyberattack on Russian state media outlet VGTRK on Putin's birthday. The attack disrupted broadcasts in retaliation for Russia's ongoing military actions. The operation marks a continued digital resistance effort in the Russia-Ukraine conflict.

Data Breaches

Transak Crypto Service Suffers Data Breach

+Crypto +Financial Services

- Crypto on-ramp service [Transak](#) disclosed a data breach affecting its user base, potentially compromising sensitive personal and financial data. The breach was allegedly caused by an employee using a work laptop for non-work purposes, and affects less than 2% of their customers. This incident underscores the growing threat to cryptocurrency platforms and their users' data security.

Internet Archive Hacked Again via Stolen Access Tokens

+GitLab +Archive

- For the second time, the [Internet Archive](#) has suffered a data breach due to stolen access tokens. The attackers gained unauthorized access to the Archive's Zendesk email support platform, potentially compromising user data. This breach comes after the Archives were warned of leaked GitLab authentication tokens.

Fidelity Investments Data Breach Affects 77,000 Customers

+Financial Services

- [Fidelity Investments](#) reported a significant data breach, impacting more than 77,000 of its customers, caused by broken access control. Attackers accessed sensitive financial information, including account details and personal identifiers, raising fears of identity theft and fraud. The breach has prompted urgent security reviews at the financial giant to prevent future incidents.

115,000 Texans' Data Exposed in State DPS Breach

+US +Government

- Over 115,000 Texans had their personal information leaked following a breach of the [Texas Department of Public Safety](#) systems. The exposed data includes driver's license numbers, addresses, and social security information. This breach adds to the growing list of state-level data compromises, sparking concerns over the security of government-managed 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.