

Threat Intel Report: June 10-16, 2024

Countries



Top Tags

Black Basta

LockBit

ValleyRat

WarmCookie

Sleepy Pickle

Executive Summary

Actionable Information:

- *Third-Party Software Risks:* Increasingly, attackers are exploiting vulnerabilities in widely used third-party software and extensions to gain unauthorized access and steal sensitive data. This trend highlights the critical need for thorough vetting and continuous monitoring of third-party dependencies.
- *Advanced Malware and Exploit Techniques:* Sophisticated malware variants and zero-day exploits are being used more frequently to target organizations across various sectors. This trend underscores the importance of robust cybersecurity measures, including timely patching and advanced threat detection systems.
- *Emerging Threats in Artificial Intelligence:* New exploits targeting machine learning models, such as data poisoning attacks, are emerging, which can undermine the reliability and accuracy of AI systems. This emphasizes the need for securing AI pipelines and ensuring the integrity of training data.
- *Ransomware as a Persistent Threat:* Ransomware attacks continue to be a significant threat, impacting municipal systems, manufacturing, and financial sectors. The persistence of these attacks calls for comprehensive cybersecurity strategies, including robust backup solutions and incident response plans.
- *Data Breaches and Financial Impact:* High-profile data breaches involving sensitive personal and financial information are on the rise. These incidents highlight the necessity of implementing strong authentication measures, such as multi-factor authentication, and enhancing overall data protection protocols.

Outlook:

The current cyber threat landscape reveals a trend towards increasingly sophisticated attacks exploiting third-party dependencies, zero-day vulnerabilities, and machine learning models. Ransomware continues to be a significant threat,



impacting various sectors from local government to manufacturing. The importance of robust security measures, including timely patching, multi-factor authentication, and comprehensive monitoring, cannot be overstated. Organizations must prioritize these measures to mitigate the risk of data breaches and ensure the security of sensitive information against evolving threats.

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

↓ 13% [CVE-2024-27199](#)

- A path traversal vulnerability in JetBrains TeamCity

↑ 10% [CVE-2023-30185](#)

- A file upload vulnerability in some versions of CRMEB

↑ 22% [CVE-2023-35078](#)

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

Austrian Sports Site Hit By ATO Attack

+Austria +Sports +ATO

- An Austrian sports site was targeted in an account takeover attack with over 1 million attempted logins, coming from British and German-located IP addresses. The attacks were brute-force attempts, and leveraged many random username and password combinations rather than leaked credentials.

Gaming Site Attacked with Trojans

+Gaming +Trojan +Ruby +Go

- A gaming site saw many trojan attempts this week, coming exclusively from US-based IP addresses. Attackers used tools written in Ruby and Go, as well as bots, to target the site, which sells collectibles and other sought-after items.

Recent Cyber Threats

Malicious VSCode Extensions Uncovered

+Third-Party +Extensions

- Researchers have discovered several malicious [VSCode](#) extensions with over a million installs collectively. These extensions were designed to steal sensitive information, including credentials, and execute arbitrary code on developers' machines. The threat actors behind these extensions leveraged the popularity of VSCode to target a wide range of developers globally, highlighting the risks of third-party software dependencies.

New ValleyRat Variant Targets Asia

+ValleyRat +Malware

- A new variant of the [ValleyRat](#) malware has been detected, primarily targeting organizations in Asia. This latest version employs enhanced obfuscation techniques and is distributed via spear-phishing emails. Once installed, ValleyRat can steal sensitive data, conduct espionage, and maintain persistent access to compromised systems, underscoring the persistent threat of advanced persistent threats (APTs) in the region.

Chinese Biometric Access System Vulnerabilities

+China +Biometric +IoT

- Security researchers have identified 24 critical vulnerabilities in a Chinese-made [biometric access system](#) widely used in various sectors. These vulnerabilities, including hard-coded credentials and unencrypted data transmission, could allow attackers to bypass security measures and gain unauthorized access. The findings emphasize the need for stringent security assessments of IoT and biometric systems to prevent potential exploitation.

Black Basta Exploits Zero-Day in Windows

+Black Basta +Windows

- The [Black Basta](#) ransomware group has successfully exploited a zero-day vulnerability in Windows to deploy ransomware. This zero-day flaw allowed attackers to gain initial access, encrypt data, and demand ransom payments from victims. The incident highlights the critical need for organizations to implement robust patch management practices and remain vigilant against emerging threats.

WarmCookie Cyberattackers Use Backdoor for Initial Access

+WarmCookie +Backdoor

- The [WarmCookie](#) cyberattack group has been observed using a sophisticated backdoor to gain initial access to targeted systems. This backdoor, once installed, allows attackers to conduct surveillance, exfiltrate sensitive data, and deploy additional malware. The method used by WarmCookie emphasizes the importance of comprehensive monitoring and rapid response capabilities to detect and mitigate such threats.

Windows Search Abused to Redirect to Malware

+Windows +SEO

- Attackers are exploiting the [Windows Search](#) feature to redirect users to malicious websites. By spoofing search queries, they can trick users into visiting sites that download and install malware onto their systems. This method leverages the trust users place in built-in Windows functionalities, emphasizing the need for enhanced user awareness and security measures.

Veeam Recovery Orchestrator Vulnerability Exploited

+Authentication Bypass

- A critical authentication bypass vulnerability in [Veeam Recovery Orchestrator](#) has been exploited in the wild, allowing attackers to gain unauthorized access. This flaw can lead to significant data breaches and disruption of data recovery processes. Veeam has released patches, and immediate application of these updates is crucial to protect systems from potential exploits.

Sleepy Pickle Poisons Machine Learning Models

+AI +Sleepy Pickle

- The [Sleepy Pickle](#) exploit targets machine learning models by subtly poisoning their training data. This method can degrade model accuracy and reliability, leading to incorrect predictions and decisions. The attack underscores the emerging threats in AI and the importance of securing machine learning pipelines against data poisoning attacks.

Data Breaches

Uwu Lend Reimbursing Customers After Crypto Theft

+Crypto

- [Uwu Lend](#), a decentralized finance platform, is reimbursing customers after a significant crypto theft in which attackers exploited a smart contract vulnerability to steal millions in digital assets. The company is working to compensate affected users and has implemented enhanced security measures to prevent future incidents. This breach underscores the vulnerabilities in DeFi platforms and the importance of rigorous security audits.

Ransomware Hits Traverse City and Newburgh

+Government +US +Ransomware

- Traverse City, Michigan, and Newburgh, New York, have both suffered [ransomware attacks](#) that disrupted local government services, including email systems and payment processing. The attacks forced both cities to shut down certain services temporarily and initiate recovery efforts. These incidents highlight the growing threat of ransomware to municipal systems and the need for comprehensive cybersecurity strategies in public sector organizations.

Truist Bank Confirms Data Breach

+Financial +US

- [Truist Bank](#) has confirmed a data breach after sensitive customer information appeared on a hacker forum. The breach, linked to a third-party vendor, exposed personal and financial data, including Social Security numbers and account details. The bank has enhanced its security protocols and is notifying affected customers while collaborating with law enforcement and cybersecurity experts to investigate the breach.

Snowflake Clients Targeted by Ransom Demands

+Snowflake +MFA

- Hackers are demanding up to \$5 million from [Snowflake](#) clients following a data breach where attackers exploited a lack of multi-factor authentication (MFA) to gain access to sensitive data. Up to 10 clients are being threatened, leading to significant operational disruptions and financial losses. This incident highlights the critical need for [robust MFA and other security measures](#) to protect against sophisticated cyberattacks.

KeyTronic Confirms Data Breach After Ransomware Attack

+Manufacturing +LockBit

- [KeyTronic](#), an electronics manufacturing company, has confirmed a data breach after the LockBit ransomware gang leaked stolen files online. The breach, which involved unauthorized access to sensitive information, has led KeyTronic to work with cybersecurity experts to enhance its defenses and mitigate the impact. This attack underscores the ongoing threat of ransomware to the manufacturing sector and the importance of robust cybersecurity practices.

LA County Dept of Public Health Data Breach Impacts 200K

+US +Government

- The [Los Angeles County Department of Public Health](#) has reported a data breach affecting 200,000 individuals. The breach, caused by unauthorized access to a third-party vendor's systems, exposed personal and health-related information. The department is implementing additional security measures and providing support to those impacted, highlighting the need for stringent security controls in healthcare data management.

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.