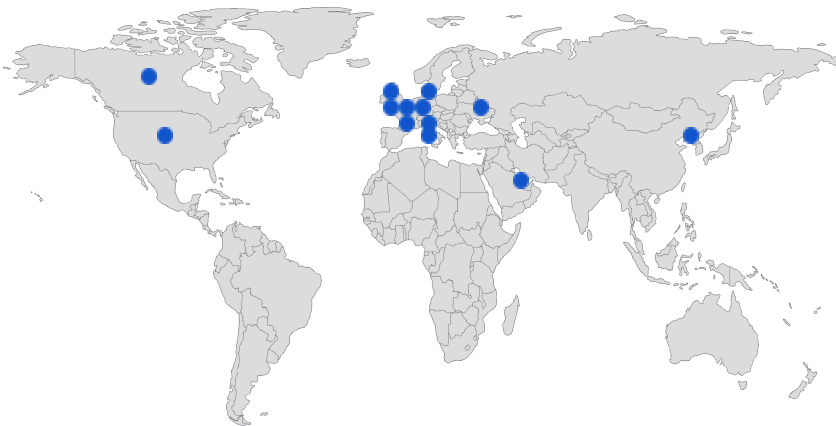


Threat Intel Report: June 3-9, 2024

Countries



Top Tags

Andariel

TellYouThePass

Fog

CobaltStrike

Sp1der

Executive Summary

Actionable Information:

- *Emerging Mobile and Communication Platform Threats:* Mobile malware and exploitation of trusted communication platforms are on the rise, necessitating stronger mobile security and user awareness.
- *Sophisticated Nation-State Espionage:* Advanced Persistent Threat (APT) groups are employing increasingly sophisticated malware for cyber espionage, targeting sensitive data across various sectors.
- *Rapid Exploitation of Critical Vulnerabilities:* The swift weaponization of newly discovered vulnerabilities highlights the critical need for timely patching and proactive cybersecurity measures.
- *Sector-Specific Ransomware Campaigns:* Targeted ransomware attacks on specific sectors, such as education and recreation, underscore their heightened vulnerability and the need for tailored security strategies.
- *Significant Data Breaches and Third-Party Risks:* Recent data breaches, often linked to third-party platforms, reveal the ongoing risks associated with external integrations and the importance of robust data protection protocols.

Outlook:

The landscape of cyber threats continues to evolve, with a noticeable trend toward exploiting trusted platforms and third-party integrations. The rapid weaponization of vulnerabilities, as seen with the PHP CVE-2024-4577, and targeted ransomware campaigns against specific sectors, such as education and recreation, indicate a shift towards more sophisticated and sector-specific attacks. Data breaches affecting major companies highlight the ongoing challenges in protecting sensitive information. Moving forward, organizations must prioritize proactive security measures, timely patching of vulnerabilities, and stringent monitoring of third-party platforms to mitigate these evolving threats.

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

▲ 14% [CVE-2024-27199](#)

- A path traversal vulnerability in JetBrains TeamCity

↓ 9% [CVE-2023-30185](#)

- A file upload vulnerability in some versions of CRMEB

↓ 6% [CVE-2023-35082](#)

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

Layer 3/4 DDoS Hits US Computing Site

+US +Computing +DDoS

- A large network-layer distributed denial of service (DDoS) attack hit a US computing company this week. The attack, reaching 186 GBPS, came from just over 1,000 IPs.

US Healthcare Company Targeted by Automated Attacks

+Automated Attack +US +Healthcare

- A US healthcare company was targeted in a large automated attack this week, reaching 9M requests. The attacks, which came entirely from the US, came from vulnerability scanning tools.

Recent Cyber Threats

Fake Bahrain Government App Used for Financial Fraud

+Bahrain +Malware

- A sophisticated fake Android app impersonating a [Bahrain](#) government service has been discovered, aimed at stealing personal data from Bahraini citizens. The stolen data is used to commit financial fraud, affecting numerous individuals and compromising sensitive information. This incident underscores the ongoing threat of mobile malware and the need for vigilant cybersecurity practices among users in the Middle East.

Andariel APT Utilizes Dorarat and Nestdoor Malware for Espionage

+North Korea +Andariel +Dorarat +Nestdoor

- The North Korean [Andariel APT](#) group has deployed Dorarat and Nestdoor malware in its latest cyber espionage campaign. These malware variants enable Andariel to infiltrate targeted systems, steal sensitive information, and disrupt operations across multiple sectors. The campaign highlights the group's evolving tactics and the persistent threat posed to global cybersecurity.

Cox Patches API Flaw Exposing Millions of Modems

+Telecommunications +API +Authentication Bypass

- [Cox Communications](#) has resolved a critical API authentication bypass vulnerability that exposed millions of modems to potential cyberattacks. The flaw allowed attackers to gain unauthorized control over modems, posing significant risks of data interception, service disruption, and privacy breaches.

Critical PHP Vulnerability CVE-2024-4577 Discovered, Spreads TellYouThePass Ransomware

+CVE +TellYouThePass +PHP

- Recently, a critical vulnerability– identified as [CVE-2024-4577](#) with an initial CVSS score of 9.8 – was discovered in PHP. This vulnerability, which allows for remote code execution due to improper input validation, poses significant

risks to web applications built with PHP. Attackers can exploit this flaw to execute arbitrary code on affected servers, potentially compromising entire systems.

- The recently identified CVE-2024-4577 vulnerability has been quickly weaponized to spread [TellYouThePass](#) ransomware. This rapid exploitation demonstrates the critical need for immediate patching and proactive security measures to protect systems from ransomware attacks. The incident underscores the evolving tactics of cybercriminals and the importance of maintaining up-to-date security protocols.

TikTok Fixes Zero-Day Vulnerability Hijacking High-Profile Accounts

+Zero-Day +Account Takeover

- [TikTok](#) has patched a zero-day vulnerability that was exploited to hijack high-profile user accounts. The vulnerability allowed attackers to gain unauthorized access and control over these accounts, posing significant risks to user privacy and security. The rapid response by TikTok highlights the importance of addressing security flaws promptly to protect users and maintain platform integrity.

Fog Ransomware Targets Education and Recreation Sectors

+Fog +Ransomware +Education +Recreation

- The [Fog](#) ransomware group has launched a new campaign targeting the education and recreation sectors. This ransomware encrypts critical data and demands a ransom for decryption, disrupting operations and causing significant financial losses. The attack underscores the vulnerability of these sectors to sophisticated cyber threats and the need for enhanced cybersecurity measures.

DarkCrystal RAT Delivered via Signal Messenger

+DarkCrystal +RAT

- A new threat has emerged with the [DarkCrystal RAT](#) being delivered through Signal Messenger. This remote access tool enables attackers to gain unauthorized access to victims' systems, exfiltrate data, and perform various malicious activities. The use of Signal Messenger as a delivery vector highlights the evolving tactics of cybercriminals in exploiting trusted communication platforms.

Critical Vulnerability in Cisco Webex Cloud Exposed

+Germany +Government +Netherlands +Italy +Austria +France +Switzerland +Ireland +Denmark

- A significant vulnerability has been identified in [Cisco Webex's](#) cloud infrastructure, potentially allowing attackers to execute arbitrary code. The bug allowed the discovery of information about past and future Webex meetings involving several German federal and state offices, as well as authorities and companies in Germany, the Netherlands, Italy, Austria, France, Switzerland, Ireland and Denmark.

CobaltStrike Used in Several Attacks

+CobaltStrike +JScripRat +Ukraine

- A coordinated cyber attack has been observed utilizing JScrip RAT and [CobaltStrike](#). These tools enable attackers to gain persistent access to compromised systems, conduct espionage, and deploy additional payloads.
- A sophisticated cyber attack involving an Excel file embedding [CobaltStrike](#) has been launched against Ukrainian entities. This method of malware deployment is part of a targeted campaign aimed at compromising systems, conducting espionage, and potentially disrupting critical infrastructure.

Security Flaws Found in WooCommerce WordPress Plugin

+WordPress +Plugin

- Multiple security vulnerabilities have been discovered in [WooCommerce](#), the popular e-commerce plugin for WordPress. These flaws could allow attackers to exploit and gain unauthorized access to sensitive customer information, posing significant risks to online retailers and their clients. Timely updates and security practices are essential to mitigate these threats.

Data Breaches

Several Companies Breached in Potential Snowflake Hacks

+Telecommunications & IT +Automotive +Sp1der

- 3TB of data allegedly stolen from [Advance Auto Parts](#), including over 380 million customer profiles, have been put up for sale by a threat actor known as Sp1der, following the company's third-party data leak in the Snowflake breaches.
- [Cylance](#) has confirmed a data breach linked to a third-party platform, compromising sensitive information. The same threat actor, Sp1d3r, has posted the data for sale, allegedly including 34 million emails, as well as personally identifiable information. Although the name of the third-party company has yet to be disclosed, the threat actor is the same.

23andMe Faces UK and Canadian Data Breach Probes

+UK +Canada +Legal

- [23andMe](#) is under investigation by UK and Canadian authorities following a significant data breach last October that exposed sensitive genetic and personal information. The breach affected a substantial number of customers, raising serious privacy concerns and prompting regulatory scrutiny. The probes aim to assess the breach's impact and ensure compliance with data protection laws, highlighting the importance of robust security measures in handling genetic data.

CoinGecko Announces Major Data Breach

+Cryptocurrency

- [CoinGecko](#) has disclosed a data breach that exposed the contact details of 1,916,596 users and led to 23,723 phishing emails being sent. The breach occurred due to unauthorized access to CoinGecko's database, compromising user privacy and security. CoinGecko is taking steps to enhance its security infrastructure and protect against future cyberattacks, underscoring the ongoing threats to cryptocurrency platforms.

Frontier Communications Suffers Data Breach

+Telecommunications

- [Frontier Communications](#) has experienced a data breach that compromised customer information, including personal and account details. The breach was caused by unauthorized access, impacting the privacy and security of numerous customers. Frontier Communications is working to address the breach, mitigate its impact, and strengthen its cybersecurity measures to prevent future incidents, highlighting the importance of robust data protection in the telecommunications 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.