

Threat Intel Report: August 12-18, 2024

Countries



Top Tags

DotNet

Dark Skippy

Banshee

DeathGrip

Black Basta

Executive Summary

Actionable Information:

- **Rise in Malware and Ransomware Attacks:** The emergence of new malware like Banshee targeting macOS, and DotNet malware hijacking websites for cryptomining, alongside the introduction of DeathGrip Ransomware-as-a-Service, indicates an increasing diversity in attack methods. This suggests a growing threat landscape where both sophisticated and low-skill attackers can launch impactful campaigns.
- **Vulnerabilities in Critical Infrastructure:** Security flaws have been discovered in vital sectors, including a breach in solar power systems and vulnerabilities in Azure AI Health Bot used in healthcare. These incidents highlight the urgent need for stronger security measures in critical infrastructure and healthcare systems, where the impact of a breach can be severe.
- **IoT and Smart Devices at Risk:** Recent findings of vulnerabilities in Sonos smart speakers and Google Pixel devices shipping with pre-installed malware underline the escalating risks in IoT and consumer electronics. As these devices become more integrated into daily life, the potential for widespread disruption and data theft increases.
- **Data Breaches Continue to Surge:** Significant breaches, such as those affecting National Public Data, the Central Bank of Iran, and Toyota, expose the persistent risk to personal and financial information. These breaches reveal weaknesses in both public and private sectors, stressing the need for enhanced data protection and incident response strategies.

Outlook:

The cybersecurity landscape is growing more complex, with threats emerging across multiple fronts, from sophisticated malware and ransomware services to vulnerabilities in critical infrastructure and IoT devices. As attackers diversify their

methods and targets, organizations across all sectors must prioritize robust cybersecurity measures, continuous monitoring, and timely updates to mitigate risks. The trend toward more frequent and severe data breaches, coupled with the rise in accessible tools for launching attacks, suggests that the threat environment will continue to intensify. Looking ahead, collaboration between industry, government, and cybersecurity experts will be essential in defending against these evolving threats.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

📈 2750% [CVE-2023-3460](#)

- The Ultimate Member WordPress plugin before 2.6.7 does not prevent visitors from creating user accounts with arbitrary capabilities, effectively allowing attackers to create administrator accounts at will.

📈 313% [CVE-2024-2879](#)

- The LayerSlider plugin for WordPress is vulnerable to SQL Injection due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query.

📈 301% [CVE-2024-23897](#)

- Jenkins does 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.

Malaysian Financial Site Targeted By Network and Application DDoS

+Malaysia +Financial Services +DDoS

- This week, a large network-layer DDoS attack on a Malaysian financial services site reached 7.2 GBPS. The site was also targeted before and during the network-layer attack with application-layer DDoS. This coordinated attack strategy indicates a level of sophistication, as the attackers sought to disrupt the site's operations on multiple fronts simultaneously.

Bad Bots Target US Financial Company

+US +Financial Services +Automated Attack

- A US financial services company was targeted by automated attacks this week. The attacks, which came entirely from US-based IPs, targeted several sites owned by the company.

Recent Cyber Threats

Widespread Trojan Malware Targets Browser Extensions

+Trojan

- A new [Trojan](#) malware campaign is spreading rapidly by targeting popular browser extensions. This malicious software can hijack users' browsers, steal credentials, and manipulate web traffic, posing a significant threat to online security. The campaign is highly sophisticated, with the ability to evade detection by traditional antivirus programs, making it a widespread concern globally.

Solar Power Harvesting Attack Exposes Critical Infrastructure

+Energy +US

- Researchers have uncovered a security flaw that allowed them to gain unauthorized access to [solar power systems](#) capable of generating enough energy to power the entire United States. By exploiting this vulnerability, attackers could potentially disrupt or control large-scale energy production, highlighting significant security risks within critical infrastructure sectors.

Sonos Smart Speakers Vulnerable to Remote Attacks

+IoT +CVE

- Security flaws in [Sonos](#) smart speakers have been discovered, allowing attackers to execute remote code and take control of the devices. These vulnerabilities could enable eavesdropping, network infiltration, and other malicious activities, raising concerns about the security of IoT devices in consumers' homes. Users are advised to update their devices immediately to mitigate these risks.

Cyberattack Hits Central Bank of Iran

+Iran +Financial Services

- The [Central Bank of Iran](#) has been targeted in a significant cyberattack, disrupting its online services and access to financial data. The attack, carried out by unidentified hackers, temporarily took down the bank's website, though the extent of the breach and potential data compromise remain unclear. This incident highlights the ongoing vulnerability of critical financial infrastructure in the face of increasingly sophisticated cyber threats, particularly in geopolitically sensitive regions like Iran.

DotNet Malware Hijacks Websites for Cryptomining

+DotNet +Malware +Cryptomining

- A new variant of [DotNet](#) malware has been identified, targeting websites to hijack their resources for cryptomining. This malware silently installs itself on compromised sites, using server resources to mine cryptocurrency without the owners' knowledge. The attack has been observed across multiple platforms, significantly impacting website performance and potentially leading to financial losses for affected businesses.

Dark Skippy Attack Targets Linux and IoT Devices

+Dark Skippy +Linux +IoT +Malware

- The [Dark Skippy](#) attack is a new cyber threat targeting Linux-based systems and IoT devices. This attack utilizes a combination of techniques, including brute-force attacks and vulnerability exploitation, to gain control of devices. Once compromised, the malware can be used for various malicious activities, such as launching DDoS attacks or stealing sensitive data, posing a significant threat to both individual users and enterprises.

Banshee macOS Stealer Malware Emerges

+Banshee +Malware +MacOS

- The [Banshee](#) malware, a new macOS-specific data stealer, has been detected in the wild. This malicious software is designed to exfiltrate sensitive information from infected systems, including passwords, cookies, and financial data. The emergence of Banshee highlights the growing focus of cybercriminals on macOS platforms, traditionally considered more secure than their Windows counterparts.

DeathGrip Ransomware-as-a-Service Emerges

+DeathGrip +RaaS +Ransomware

- A new Ransomware-as-a-Service (RaaS) platform named [DeathGrip](#) has surfaced, offering cybercriminals an easy-to-use tool for launching ransomware attacks. This service lowers the barrier for entry, enabling even less technically skilled attackers to deploy sophisticated ransomware campaigns. The rise of DeathGrip is concerning as it increases the potential for widespread and devastating ransomware incidents across various industries.

Azure AI Health Bot Compromised by Critical Vulnerabilities

+AI +Healthcare

- Security researchers have uncovered critical vulnerabilities in Microsoft's Azure [AI Health Bot](#), which is widely used in the healthcare industry. These flaws could allow attackers to gain unauthorized access to patient data, manipulate bot responses, or disrupt healthcare services. The discovery underscores the importance of securing AI-driven applications, particularly those handling sensitive health information.

Black Basta Ransomware Leveraging SystemBC in New Campaign

+BlackBasta +Ransomware

- The [Black Basta](#) ransomware group has launched a new campaign, utilizing the SystemBC proxy tool to enhance their attacks. This campaign is characterized by its ability to obfuscate malicious traffic, making it harder for defenders to detect and mitigate the ransomware. The combination of Black Basta's ransomware with SystemBC's capabilities poses a heightened risk to organizations globally.

Google Pixel Devices Shipped with Pre-Installed Malware

+Android +Malware

- Several [Google Pixel](#) devices have been found to ship with pre-installed malware, exposing users to security risks right out of the box. The malware is capable of collecting sensitive data, tracking user activity, and potentially allowing remote control of the device. This incident raises concerns about the security of supply chains and the need for rigorous testing before devices reach consumers.

Data Breaches

National Public Data Confirms Massive Data Breach

+US +Government

- [National Public Data](#) has officially confirmed a data breach that exposed the personal information of millions of users. The breach, which had been rumored for weeks, compromised sensitive data including names, addresses, and financial details. The company is now facing scrutiny for its delayed response and potential impact on affected users, highlighting the growing risks of large-scale data breaches in the public sector.

Columbus Cyberattack Exposes Private Citizen Data

+US +Government

- A cybersecurity expert revealed that a recent cyberattack on [Columbus, Ohio](#), has led to the theft of private citizen data. The breach affected municipal systems and compromised sensitive personal information, leaving many residents at risk of identity theft. The attack underscores the vulnerabilities in local government cybersecurity and the potential consequences for the privacy of citizens.

Toyota Data Breach Affects Thousands of Customers

+Automotive +Japan

- [Toyota](#) has disclosed a data breach that exposed the personal information of thousands of its customers. The breach, which impacted users of Toyota's connected services, included details such as vehicle identification numbers and location data. This incident raises concerns about the security of automotive technology and the potential risks for consumers as cars become increasingly connected.

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.