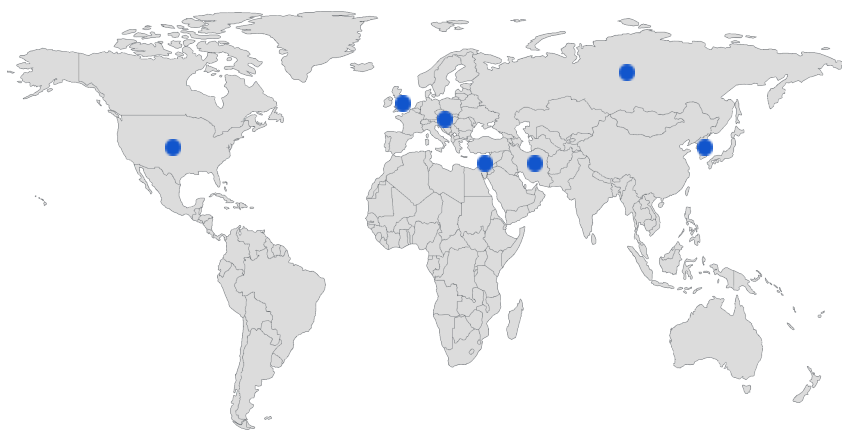


Threat Intel Report: August 5-11, 2024

Countries



Top Tags

Blank Bot

Magniber

SnakeKeylogger

Pungsan

0.0.0.0 Day

Executive Summary

Actionable Information:

- **Ransomware and Malware Proliferation:** There is a notable rise in ransomware attacks (e.g., Magniber) and sophisticated malware (e.g., BlankBot and SnakeKeylogger), particularly targeting individuals and financial services.
- **Exploitation of Software Vulnerabilities:** Critical vulnerabilities in widely-used software (e.g., Apache OFBiz) and services (e.g., Microsoft 365) are being actively exploited, emphasizing the need for timely patching and updates.
- **State-Sponsored Cyber Espionage:** State-sponsored actors, including those linked to North Korea and Iran, are leveraging sophisticated methods such as supply chain attacks and targeted phishing campaigns to infiltrate and gather intelligence.
- **Massive Data Breaches:** Large-scale data breaches, like the leak of 27 billion records of US citizens, highlight the increasing risks of identity theft and the urgent need for robust data protection mechanisms.
- **Cybersecurity in Cryptocurrency:** The exploitation of vulnerabilities in cryptocurrency platforms (e.g., Ronin Network) underscores the importance of continuous security audits and the role of white hat hackers in mitigating risks.

Outlook:

The cyber threat landscape is becoming increasingly complex and multifaceted, with a clear trend towards more sophisticated and widespread attacks. Ransomware and malware attacks are targeting a broader range of victims, including home users and financial institutions. State-sponsored cyber espionage remains a significant threat, with nation-state actors employing advanced tactics to compromise critical infrastructure and political entities. The

prevalence of software vulnerabilities being exploited for malicious purposes highlights the critical need for regular security updates and patches. Additionally, the sheer scale of recent data breaches indicates a growing risk to personal data security, necessitating stronger data protection measures. Looking forward, the collaboration between cybersecurity professionals, ethical hackers, and governmental bodies will be essential in addressing these evolving threats and protecting digital assets.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

📈 1000% [CVE-2023-34362](#)

- A SQL injection vulnerability has been found in the MOVEit Transfer web application that could allow an unauthenticated attacker to gain access to MOVEit Transfer's database.

📈 139% [CVE-2023-28770](#)

- The sensitive information exposure vulnerability in the CGI "Export_Log" and the binary "zcmd" in Zyxel DX5401-B0 firmware could allow a remote unauthenticated attacker to read the system files and to retrieve the password of the supervisor from the encrypted file.

📈 100% [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.

DDoS on Israeli Sites Grows 287%

+DDoS +Israel +Financial Services +Computing

- DDoS attacks on Israel-based websites are trending upwards over the past month. The volume of application-layer DDoS against Israeli sites has grown 287% since April, and primarily targets Financial Services and Computing sites.

Czech Site Targeted by Business Logic

+Czechia +Great Britain +Business Logic

- A Czech travel site was targeted by business logic attacks 860% above average this week. The attacks, which came primarily from Great Britain, reached over 3.5M requests.

Recent Cyber Threats

Delegated DNS Domains Vulnerable to Hijacking

+DNS Hijacking +Sitting Duck

- Researchers have identified significant security risks associated with domains using delegated name services, as these configurations can be exploited to perform cache poisoning attacks. Attackers can manipulate DNS responses to redirect users to malicious websites using a technique called [Sitting Duck](#), increasing the risk of data theft and phishing. This vulnerability impacts a wide range of internet users globally.

BlankBot Malware Targets Android Banking Apps

+BlankBot +Malware +Android +Financial Services

- The new [BlankBot](#) malware has emerged, targeting Android users' banking data by stealing credentials and bypassing two-factor authentication. This sophisticated malware hides its activities and can adapt to different

banking apps, posing a severe threat to users' financial information. The attacks have predominantly been observed in Europe.

Magniber Ransomware Surge Hits Home Users Worldwide

[+Magniber](#) [+Ransomware](#)

- There has been a significant increase in [Magniber](#) ransomware attacks, focusing primarily on home users. This ransomware exploits vulnerabilities in web browsers to deliver malicious payloads, encrypting victims' files and demanding a ransom. The widespread nature of these attacks highlights the growing risk to individual users' data security.

Critical Apache OFBiz Flaw Exposes Systems to Remote Attacks

[+CVE](#) [+OFBiz](#)

- A critical vulnerability in [Apache OFBiz](#), a popular open-source ERP system, has been discovered, allowing remote attackers to execute arbitrary code. This flaw, tracked as CVE-2024-38856, affects numerous businesses relying on OFBiz for their operations, making it crucial to apply patches immediately. Exploiting this vulnerability could lead to severe disruptions and data breaches.

SnakeKeylogger Malware Targets Windows Systems

[+SnakeKeylogger](#) [+Malware](#) [+Windows](#)

- The [SnakeKeylogger](#) malware, known for its data-stealing capabilities, is now targeting Windows systems with increased frequency. This malware captures keystrokes, screenshots, and clipboard data, posing a significant threat to personal and corporate information security. The rise in SnakeKeylogger infections calls for heightened vigilance and improved security practices.

North Korean Group Uses NPM Packages for Initial Access

[+Pungsan](#) [+North Korea](#) [+NPM](#)

- The North Korean-aligned threat actor [Pungsan](#) is leveraging NPM packages to gain initial access to target systems. By injecting malicious code into widely-used packages, they can infiltrate software development environments, posing a significant risk to businesses and developers globally. This tactic highlights the evolving strategies of state-sponsored cyber actors.

Microsoft 365 Anti-Phishing Feature Bypassed Using CSS

[+CSS Manipulation](#)

- Security researchers have found a way to bypass Microsoft 365's anti-phishing protections using [CSS manipulation](#). This technique allows attackers to deliver phishing emails that appear legitimate, increasing the risk of credential theft among Microsoft 365 users. This vulnerability emphasizes the need for ongoing vigilance and improved security measures.

Privilege Escalation Flaw in Entra ID Grants Global Admin Access

[+Privilege Escalation](#) [+Identity Management](#)

- A [privilege escalation flaw](#) in Entra ID can elevate privileged users to global admin roles, exposing systems to unauthorized access and potential abuse. This vulnerability is particularly concerning for enterprises relying on Entra ID for identity management, as it could lead to significant security breaches if exploited.

Zero-Day Flaw Puts Browsers at Risk of RCE

[+0.0.0.0 Day](#)

- A recently discovered zero-day flaw, known as [0.0.0.0 Day](#) because of the web address the vulnerability exploits, in browsers puts users at risk of remote code execution (RCE) attacks. Researchers have discovered a way to bypass browser security and interact with services running on an organization's local network from outside the network. Exploiting this vulnerability, attackers can execute arbitrary code on victims' machines, potentially leading to data theft and system compromise.

Data Breaches

Massive US Personal Data Leak on Hacking Forum

+US

- A massive leak of personal information, encompassing nearly 27 billion records of [US citizens](#), has surfaced on a hacking forum. This unprecedented breach includes sensitive data such as names, addresses, and social security numbers, posing significant identity theft and fraud risks. Authorities are investigating the source and impact of this vast data dump.

Iran-Linked Hackers Target US Political Campaign

+Iran +US +Government

- The [Trump](#) campaign has confirmed it was hacked by Iran-linked actors, after an unknown source sent several internal documents to Politico. The emails from the hacker included a research dossier the campaign had apparently done on Trump's running mate, Ohio Sen. JD Vance, among others.

White Hat Hackers Briefly Steal \$12M in Crypto Vulnerability Exploit

+Crypto

- The [Ronin Network](#) suffered a security incident when white hat hackers exploited a vulnerability in the Ronin bridge, withdrawing \$12 million in cryptocurrency. The hackers immediately informed the network about the exploit, and the bridge was paused to prevent further damage. The stolen funds, consisting of 4,000 ETH and 2 million USDC, were fully returned, and the white hats were rewarded with a \$500,000 bounty.

Russian Hackers Breach UK Government and Microsoft

+Russia +UK +Government

- [Russian hackers](#) have breached the UK Home Office and Microsoft systems, gaining access to sensitive government data. The cyber espionage campaign aims to gather intelligence and disrupt operations, highlighting ongoing geopolitical tensions. The UK government is working to assess the damage and strengthen its cybersecurity defenses.

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.