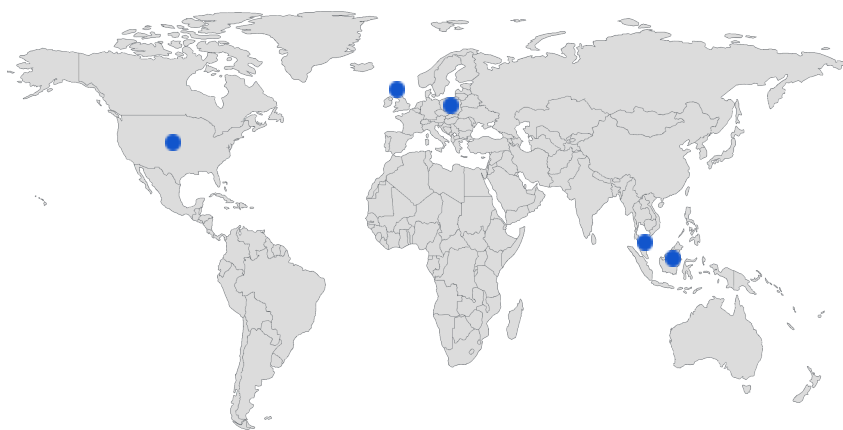


Threat Intel Report: July 29-August 4, 2024

Countries



Top Tags

PyPI

Mirai

Mandrake

ModiLoader

DarkAngels

Executive Summary

Actionable Information:

- **Rising DDoS Threats:** The Azure outage caused by a massive DDoS attack highlights the increasing threat of large-scale DDoS assaults on cloud infrastructure. Similar threats are anticipated around high-profile events like the Olympics.
- **Supply Chain Vulnerabilities:** Malicious PyPI packages targeting macOS developers and the WhatsApp vulnerability underline the persistent risks in software development and messaging platforms.
- **Phishing Campaigns:** Multiple phishing attacks, including those targeting W-2 form searchers in the US and Polish SMBs via ModiLoader, indicate a growing trend in targeted phishing schemes aimed at financial and business sectors.
- **Malware and Botnets:** The Mirai botnet's focus on Apache OFBiz servers and the widespread infection of Android devices by Mandrake spyware demonstrate the evolving nature of malware and botnet threats.
- **Data Breaches:** Significant data breaches affecting Health Savings Accounts, voter data, and the pharmaceutical sector emphasize the need for enhanced data protection measures across various industries.
- **Educational Sector Attacks:** Security breaches in educational apps and special education data in Northern Ireland highlight vulnerabilities in the education sector, necessitating stringent security protocols.

Outlook:

The current landscape of cyber threats reveals a trend towards more sophisticated and large-scale attacks, targeting critical infrastructure, personal data, and high-profile events. The rise in DDoS attacks, as seen with Azure and potential Olympic threats, combined with persistent vulnerabilities in software supply chains, suggests an urgent need for enhanced security measures. Phishing and malware attacks continue to evolve, exploiting new vectors and affecting

diverse sectors such as finance, healthcare, and education. Moving forward, organizations must prioritize robust cybersecurity defenses, timely updates, and comprehensive monitoring to mitigate these escalating threats.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

📈 313% [CVE-2024-25600](#)

- Improper Control of Generation of Code ('Code Injection') vulnerability in Codeer Limited Bricks Builder allows Code Injection.

📈 169% [CVE-2023-34960](#)

- A command injection vulnerability in the wsConvertPpt component of Chamilo v1.11.* up to v1.11.18 allows attackers to execute arbitrary commands via a SOAP API call with a crafted PowerPoint name.

📈 150% [CVE-2024-20767](#)

- ColdFusion versions 2023.6, 2021.12 and earlier are affected by an Improper Access Control vulnerability that could lead to arbitrary file system read.

Indonesian Government Site Faces 4.7M RPS Layer 7 DDoS Attack

+Indonesia +Government +DDoS

- This week, an Indonesian government website was hit by a significant Layer 7 DDoS attack, peaking at 4.7 million requests per second (RPS). The attack originated from 11,700 unique IP addresses, showcasing the increasing sophistication and scale of modern cyber threats targeting governmental digital infrastructure.

US Business Site Hit by XSS Attacks on Media URLs

+US +Business +XSS

- This week, a US business site was targeted by XSS attacks originating from masking proxies, specifically focusing on URLs ending in /media. These attacks aim to exploit vulnerabilities in media endpoints to inject malicious scripts, leveraging the high traffic and interaction in these content-rich areas.

Recent Cyber Threats

Massive DDoS Attack Causes Azure Outage

+Cloud Computing +DDoS

- [Microsoft](#) disclosed that a massive DDoS attack caused a significant outage on its Azure platform, impacting numerous services and customers globally. The disruption lasted several hours, affecting critical applications and operations for businesses relying on Azure. This incident underscores the growing threat of large-scale DDoS attacks on cloud infrastructure.

Potential Cyber Threats to the Olympics Highlighted

+Sports +Cyber Threats +France

- As the [Olympics](#) occur, cybersecurity experts warn of potential threats that could disrupt the event. These threats range from DDoS attacks and ransomware to targeted phishing campaigns and data breaches. The high-profile nature of the Olympics makes it a lucrative target for cybercriminals, emphasizing the need for comprehensive security measures to protect the games.

Targeted PyPI Package Steals Google Cloud Credentials

+Software Development +Credential Theft +PyPI

- A malicious [PyPI](#) package has been found targeting macOS developers, specifically designed to steal Google Cloud credentials. The package, discovered by security researchers, masquerades as a legitimate library but exfiltrates sensitive information to external servers. This attack highlights the risks of supply chain attacks in software development.

WhatsApp for Windows Vulnerability Executes Python, PHP Scripts

+Messaging +Vulnerability

- A newly discovered vulnerability in [WhatsApp](#) for Windows allows Python and PHP scripts to execute without user warnings, posing significant security risks. This flaw can be exploited to run malicious code on affected systems, potentially leading to data breaches and unauthorized access. Users are advised to update their software promptly to mitigate this risk.

Hackers Target W-2 Form Searchers in New Phishing Scheme

+US +Financial Services +Phishing

- Cybercriminals are targeting individuals searching for [W-2 forms](#) through a sophisticated phishing campaign. The attackers use fraudulent websites to harvest personal and financial information, posing a threat to the privacy and security of taxpayers. This attack is a reminder of the importance of vigilance during tax season.

Mirai Botnet Targets Apache OFBiz Servers

+Mirai +Business Software +Botnet

- The [Mirai](#) botnet has been observed targeting Apache OFBiz servers in a new wave of attacks. By exploiting known vulnerabilities, the botnet attempts to compromise these servers to expand its network of infected devices. This campaign highlights the continuous evolution of the Mirai botnet and the need for timely patching of software vulnerabilities.

Mandrake Spyware Infects 32,000 Android Devices

+Mandrake +Android +Mobile +Spyware

- The [Mandrake](#) spyware has infected over 32,000 Android devices globally, according to recent reports. This sophisticated malware has been active since 2016, capable of stealing sensitive data, tracking user activity, and taking control of infected devices. The long-term operation and the high number of infections highlight the persistent threat posed by advanced mobile spyware.

ModiLoader Phishing Campaign Targets Polish SMBs

+ModiLoader +Poland +Business +Phishing

- A new phishing campaign using [ModiLoader](#) is targeting small and medium-sized businesses (SMBs) in Poland. The attackers aim to distribute malware by sending fraudulent emails that appear to come from trusted sources. This ongoing threat underscores the importance of robust email security measures for SMBs to protect against phishing attacks.

Vulnerabilities Found in Multiple SMTP Servers

+Email Servers +Vulnerability

- Several [SMTP](#) servers have been found vulnerable to exploitation, putting numerous email systems at risk. These vulnerabilities could allow attackers to intercept, modify, or delete emails, potentially leading to significant data breaches. Organizations are urged to apply security patches and updates to mitigate these risks.

SMS Stealer Targets Multiple Countries with Deceptive Apps

+Mobile +SMS Stealer

- A new [SMS stealer](#) malware has been detected targeting users across several countries through deceptive mobile apps. These apps disguise themselves as legitimate software but covertly steal SMS messages, compromising user privacy and security. This incident highlights the ongoing threat of mobile malware and the need for vigilance when downloading apps.

Bytecode Interpreters Attacked to Conceal Malicious Activity

+Software +Malware Injection

- Researchers have uncovered new attacks on [bytecode interpreters](#) used to hide malicious injection activities. These attacks exploit vulnerabilities in the interpreters to inject and execute malicious code, making detection and remediation more challenging. This technique demonstrates the evolving sophistication of cyber threats targeting software infrastructure.

Data Breaches

Massive Health Savings Account Data Breach Exposes 4.3M Americans

+US +Healthcare

- A massive data breach has exposed the personal information of 4.3 million Americans with [Health Savings Accounts](#). The breach involved sensitive data, including names, Social Security numbers, and account details, highlighting significant vulnerabilities in healthcare data security. This incident underscores the critical need for enhanced protective measures in the healthcare sector.

Tech Contractor Exposes Data of 4.6M US Voters

+US +Government

- A tech contractor inadvertently exposed the personal data of 4.6 million [US voters](#) due to a misconfigured database. The exposed information included voter registration details and personal identifiers, raising concerns about election security and data privacy. This breach highlights the importance of stringent data protection protocols in handling voter information.

Dark Angels Ransomware Group Reaps Record Ransoms

+Dark Angels +Ransomware

- The [Dark Angels](#) ransomware group has been linked to record-breaking ransom payments, successfully extorting millions from various victims. The group employs sophisticated tactics to infiltrate networks and encrypt critical data, demanding substantial ransoms for decryption. This surge in activity underscores the growing threat of ransomware and the need for robust cybersecurity defenses.

Schools Remove App from Students' Devices Following Security Breach

+Singapore +Education

- Following a significant security breach on 13,000 [Singaporean](#) students, schools are removing a compromised app from students' Chromebooks and iPads. The breach potentially exposed sensitive student information, prompting swift action to mitigate risks. This incident highlights the need for rigorous security measures in educational technology.

Pharma Giant Cencora Alerts Millions About Data Breach

+US +Pharmaceutical

- [Cencora](#), a major pharmaceutical company, is notifying millions of individuals about a recent data breach that exposed sensitive information. The breach affected both customers and employees, compromising personal and financial data. This incident emphasizes the vulnerabilities in the pharmaceutical industry and the importance of robust data protection measures.

Minister Apologizes for Northern Ireland Special Education Needs Data Breach

+Northern Ireland +Education

- A data breach in [Northern Ireland's](#) special education needs department has exposed sensitive information of students. The breach, which involved personal and educational details, prompted an official apology from the Minister. This incident highlights the critical need for stringent data protection in educational institutions.
-



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.