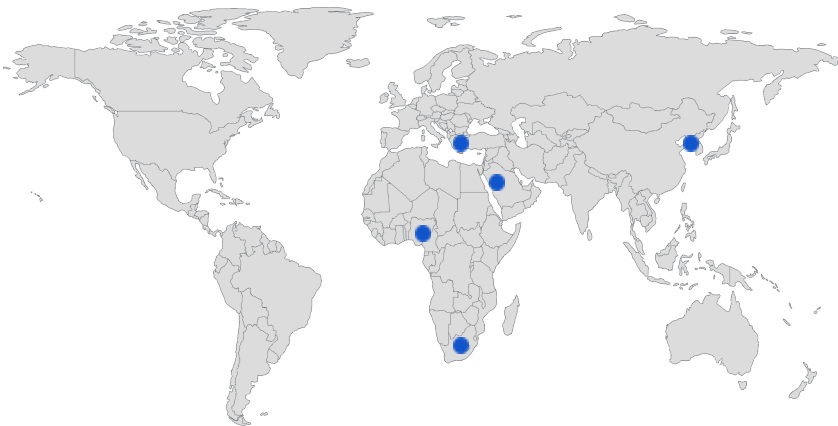


Threat Intel Report: July 15-21, 2024

Countries



Top Tags

CrowdStrike

VoidBanshee

Adload

AWS

Cisco

Executive Summary

Actionable Information:

- **Software Update Risks:** The incident with CrowdStrike's Falcon Sensor highlights the risks associated with deploying security updates. Organizations should implement comprehensive testing and contingency plans to mitigate potential disruptions caused by software updates.
- **Advanced Social Engineering:** The discovery of the ClickFix tactic underlines the growing sophistication of social engineering attacks. It is crucial to enhance user training and awareness programs to combat these deceptive techniques effectively.
- **Exploitation of Vulnerabilities:** The ongoing exploitation of critical vulnerabilities, such as those in Internet Explorer and Cisco SSM On-Prem, indicates a persistent threat. Prompt patch management and the use of modern, secure software versions are essential to reduce exposure.
- **Supply Chain Security:** The use of fake AWS packages to distribute C2 malware within JPEGs underscores the importance of supply chain security. Organizations need to rigorously verify software sources and implement robust security controls to protect against such threats.
- **Targeted Attacks on High-Value Sectors:** The attacks on WazirX and the Greek Land Registry demonstrate an increased focus on high-value targets like financial institutions and government agencies. Enhanced security measures and threat detection capabilities are necessary to protect these critical sectors.

Outlook:

The cyber threat landscape is evolving with a marked increase in the sophistication and variety of attacks. The reliance on outdated software and inadequate security practices continues to be exploited by threat actors. Organizations must

adopt a proactive approach to cybersecurity, emphasizing thorough testing of updates, rigorous user training against social engineering, and stringent supply chain security measures. As high-value targets such as financial institutions and government databases remain prime focuses for attackers, there is a pressing need for enhanced security frameworks and rapid vulnerability management. Moving forward, the emphasis should be on fostering a culture of strong cybersecurity practices and continuous improvement to mitigate these evolving threats effectively.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

⬆ 560280% [CVE-2024-4879](#)

- An input validation vulnerability in ServiceNow

⬆ 633% [CVE-2023-0669](#)

- A command injection vulnerability in GoAnywhere MFT

⬆ 80% [CVE-2023-20198](#)

- An unprotected alternate channel vulnerability in Cisco IOS XE

Record-Breaking African DDoS Attack Targets Nigeria

+Nigeria +Travel +DDoS

- A Nigerian travel site experienced a 4.3M requests per second (RPS) DDoS attack this week, in a record-breaking attack that stands as the largest we've seen this year– not just for Nigeria, but also for Africa as a whole. This attack, which lasted just 10 minutes, came from under 100 IPs.

South African Mining Company Targeted by Business Logic

+South Africa +Mining +BLA

- A South African mining company was targeted this week by business logic attacks in a three-day onslaught. The attacks came from several different countries, including the US, Vietnam, Kazakhstan, and Singapore, and leveraged the WebKit browser to conduct the attack.

Recent Cyber Threats

Falcon Sensor Update Causes Global Microsoft User Outages

+CrowdStrike +Supply Chain

- A recent update to the Falcon Sensor product by [CrowdStrike](#) led to widespread outages for Microsoft users worldwide. The update, intended to enhance security features, inadvertently caused system crashes and connectivity issues globally.

ClickFix: New Social Engineering Tactic for Malware Deployment

+ClickFix +Social Engineering

- Researchers have uncovered a social engineering tactic named [ClickFix](#), which involves deceiving users into clicking malicious links under the guise of solving a problem. This technique is being used to deploy various forms of malware, exploiting user trust and increasing infection rates.

Void Banshee Using Internet Explorer Bug

+CVE +VoidBanshee

- A critical vulnerability (CVE-2024-38112) in Internet Explorer has been discovered to be exploited by APT group [Void Banshee](#). This flaw is being used to infect victim machines with the Atlantida info-stealer.

Fake AWS Packages Hide C2 Malware in JPEGs

[+AWS](#) [+C2 Malware](#)

- Researchers have identified [fake AWS packages](#) that conceal command-and-control (C2) malware within JPEG files. These packages are distributed via compromised software repositories, highlighting the need for stringent supply chain security measures.

Cisco SSM On-Prem Bug Allows Password Changes

[+Cisco](#) [+CVE](#)

- A vulnerability in [Cisco's](#) SSM On-Prem software has been found, enabling attackers to change any user's password without authorization. This flaw could lead to unauthorized access and control over affected systems. Cisco has released updates to address the issue.

macOS Can Be Compromised by Sneaky Adload Variant

[+Adload](#) [+Malware](#)

- A new variant of the [Adload](#) malware that targets macOS systems has been reported. This variant bypasses traditional security mechanisms, installs adware, and compromises user privacy. Mac users are advised to enhance their security settings and remain vigilant.

SAP AI Core Vulnerability Could Expose Customer Data

[+AI](#)

- A vulnerability in [SAP's](#) AI Core has been discovered, potentially exposing customer data to unauthorized access. The flaw could allow attackers to exploit the system and access sensitive information. SAP has issued patches and is urging customers to update their systems immediately.

Data Breaches

WazirX Targeted by North Korean Attackers

[+India](#) [+North Korea](#) [+Crypto](#)

- [WazirX](#), an Indian crypto exchange, lost virtual assets valued at over \$230 million after a cyber attack that has since been linked to North Korea. The attack, which targeted a multi-signature wallet, exploited a discrepancy between one of the signatory's interfaces and the actual transaction data.

Greek Land Registry Hit by Massive Cyberattack Wave

[+Greece](#) [+Government](#)

- [Greece's](#) land registry agency has suffered a breach amid a wave of 400 cyberattacks. The attacks, believed to be orchestrated by unknown threat actors, stole 1.2GB of government data. Authorities are investigating the incidents and working to strengthen defenses.

Fractal ID Data Breach Linked to 2022 Password Reuse Hack

[+Crypto](#) [+Technology](#)

- A data breach at [Fractal ID](#) has been traced back to a 2022 hack involving an employee who reused passwords across platforms. The breach exposed sensitive customer information for over 6,000 users, highlighting the risks of poor password hygiene. Fractal ID is taking steps to enhance security measures and prevent future incidents.

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.