

Threat Intel Report: August 28- September 4, 2023

Countries



Top Tags

QakBot

ALPHV

LockBit

Earth Estries

Akira

Executive Summary

Cyber Threats: Over the past week, multiple cyber threats have surfaced, showing a diversified attack landscape. Notable incidents include a cross-site scripting attack on a US financial site, an application layer DDoS on a Kenyan computing site, and a malware attack targeting Rust developers on the Crates.io platform. Additionally, various software and platforms, including Microsoft Azure, Skype, and Cisco VPNs, have had vulnerabilities discovered. Criminal and state-sponsored groups, such as Anonymous Sudan, Muddled Libra, Akira, GREF, and Kimsuky, have been active, emphasizing the need for organizations to stay vigilant and update their defense mechanisms according to the latest TTP.

Data Breaches: A series of significant data breaches has affected various sectors and regions. High-profile incidents include Callaway golf company's exposure of 1.1 million customers' data, LogicMonitor's security lapse due to default passwords, and SourceGraph's access token leak. Several governmental entities have also been affected, from Georgia county's ransomware ordeal to Japan's cybersecurity agency enduring a 9-month breach, possibly by Chinese military hackers. A major oversight was witnessed by the National Safety Council, leaving over 10K members' data exposed for more than 5 months.

Actionable Information: Organizations are advised to regularly update and patch systems, especially those using vulnerable software. Employee awareness training, especially concerning social engineering campaigns, is imperative. Special attention should be given to securing and monitoring VPNs, as they remain a hot target for unauthorized access, and verifying systems' availability. Emphasis on changing weak or default passwords and ensuring authentication and data access controls can prevent many breach incidents. Given the landscape, organizations must also monitor for signs of intrusion continuously and implement multi-factor authentication where possible.

Outlook: With state-sponsored and criminal groups continuously evolving their tactics, proactive cyber defense strategies and international collaboration are paramount in thwarting these threats.

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

⬆ 20% [CVE-2023-21371](#)

- a remote directory traversal vulnerability in Oracle WebLogic Server

⬆ 12% [CVE-2022-22965](#)

- a RCE vulnerability in Spring programs ("Spring4Shell")

⬇ 25% [CVE-2023-30185](#)

- A file upload vulnerability in some CRMEB versions

US financial site attacked by XSS

+Financial Services +US +XSS

- A US-based accounting company was targeted in a cross-site scripting attack (XSS) on August 28. The attacks mostly used the Go HTTP library, and came from 17K IPs.

Kenyan computing site targeted by DDoS weeks after Anonymous Sudan attack

+Kenya +Computing & IT +DDoS

- A Kenyan computing site was targeted by application layer DDoS on September 1, reaching 1.9M requests per second (RPS). This site was previously attacked by Anonymous Sudan in mid August, but the group did not claim this attack.

Recent Cyber Threats

Social engineering campaign targets Okta users

+Social Engineering +Muddled Libra

- [Okta](#) issued a warning about an ongoing social engineering campaign targeting its users. Although the threat actor behind the attacks is unknown, the TTPs overlap with Muddled Libra.

Microsoft Azure vulnerability could redirect users to malicious sites

+URL Takeover

- A URL takeover vulnerability in Microsoft Azure's [authentication](#) mechanism was discovered, potentially allowing attackers to redirect users to malicious sites. Microsoft has been alerted to the issue, and users are advised to be cautious of unexpected redirects.

Malware targeting Rust developers discovered

+Rust +Malware

- Evidence of a malware attack targeting Rust developers was discovered on the [Crates.io](#) platform. The malicious code was embedded in certain packages, and although the exact details are unknown, attackers were probably attempting to steal sensitive files.

Skype vulnerability allows attackers to steal IP addresses

+Skype

- A vulnerability in the [Skype](#) mobile app allows attackers to obtain users' IP addresses. The flaw only requires the victim to open a malicious message, and has not yet been addressed by Microsoft.

FBI dismantles Qakbot infrastructure

+Qakbot +US +Malware

- The FBI successfully dismantled the infrastructure behind the [Qakbot](#) malware, freeing thousands of infected devices. The operation seized over \$8 million in cryptocurrency, and no arrests have been announced yet.

MMRat malware targets Southeast Asian financial sector

+MMRat +Malware +Financial Services +Southeast Asia

- A new Android malware named [MMRAT](#) is actively targeting banking users in Southeast Asia. The malware steals banking credentials and can bypass two-factor authentication mechanisms.

Akira hacking campaign targets Cisco VPNs

+Akira +Brute Force

- A hacking campaign by the [Akira](#) ransomware group is actively brute-forcing Cisco VPNs to gain unauthorized access to networks. Organizations using Cisco VPNs are advised to strengthen their security measures and monitor for suspicious activities.

BadBazaar hacking campaign targets Android users via trojanized apps

+BadBazaar +GREF

- The [BadBazaar](#) espionage tool is targeting Android users, stealing sensitive information from infected devices. The tool is believed to be part of a larger cyber-espionage campaign from the Chinese hacking group GREF using trojanized apps.

Hacking campaign exploits Barracuda zero-day

+US +Government

- Email servers, including those of the US government, were compromised in attacks exploiting a zero-day vulnerability in [Barracuda](#) Email Security Gateway products. The attackers have been exploiting this bug for at least seven months, along with previously unseen malware.

Trojan targets South Korean journalists

+SuperBear +Kimsuky +South Korean +News

- A new trojan named [SuperBear](#) has emerged, targeting various South Korean journalists with sophisticated attack techniques. The trojan is capable of evading detection, and is suspected to be related to North Korean group Kimsuky.

POC developed for Chrome extension password grabbing

+POC +Password Theft

- [Researchers](#) have demonstrated a proof-of-concept Chrome extension that can extract plaintext passwords from a website's source code. Many high-traffic websites, including Gmail and Facebook, either store passwords in plaintext within the HTML DOM or are vulnerable to DOM API access, which could allow up to 17K existing Chrome extensions to potentially extract this information.

Data Breaches

Callaway golf company data breach exposes over 1M customers information

+Retail

- Golf equipment manufacturer [Callaway](#) suffered a data breach that exposed the personal information of approximately 1.1 million customers. The breach was attributed to unauthorized access to their systems, and the company is currently investigating the incident.

LogicMonitor customers hacked due to default passwords

+Computing & IT

- [LogicMonitor](#), a cloud-based IT infrastructure monitoring platform, faced a security incident as hackers exploited default passwords. The company did not require users to change the default “Welcome@” password, and several customers have been affected.

SourceGraph hacked in access token leak

+Computing & IT

- [Sourcegraph](#), a code search tool, disclosed a data breach after an access token leak. The company identified and rectified the issue, ensuring that no customer code or data was affected.

Georgia county targeted in ALPHV ransomware attack

+ALPHV +Government +US

- [Forsyth County](#) in Georgia was hit by a ransomware attack, with the AlphV hacking group claiming responsibility. The county's IT systems were affected, and the group demanded a ransom for data decryption.

Earth Estries hacking group targets government and IT organizations in several countries

+Earth Estries +FamousSparrow +Government +Computing & IT

- The [Earth Estries](#) hacking group has been actively targeting government and IT organizations. Their tactics, techniques, and procedures (TTPs) suggest a sophisticated and coordinated approach to cyber espionage, and have some overlap with the FamousSparrow attack group.

US non-profit exposes 10K members' information

+US +Non-Profit

- The [National Safety Council](#) recently exposed over 10K members' data, including employees of several high-profile organizations, including NASA, Tesla, DOJ, and Verizon. The company left their web directories containing this information exposed for over 5 months.

Montreal energy provider hacked by LockBit

+Energy +Canada +LockBit

- Montreal electricity provider [Commission des services electriques de Montréal](#) became a victim of the LockBit ransomware attack. The company allegedly refused to pay the ransom, and its IT systems are back online.

Japanese cybersecurity agency discovers 9-month breach

+Japan +Government +China

- Japan's [cybersecurity agency](#) faced a breach, with the attacker living on the system for over 9 months. The attacker has not been revealed, but reports suggest Chinese military hackers.

German federal financial agency offline since Friday in long DDoS attack

+Germany +Government +Financial Services

- The German Federal Financial Supervisory Authority ([BaFin](#)) recently announced that it has been the victim of an ongoing DDoS attack since Friday. The exact perpetrators behind the DDoS attack remain unidentified, but there is speculation that pro-Russian hacktivists might be responsible due to Germany's support for Ukraine.

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.



By Phone:
650-345-9000



By Fax:
888-611-7282

By mail:

Imperva Headquarters
One Curiosity Way, Suite
203 San Mateo, CA 94403