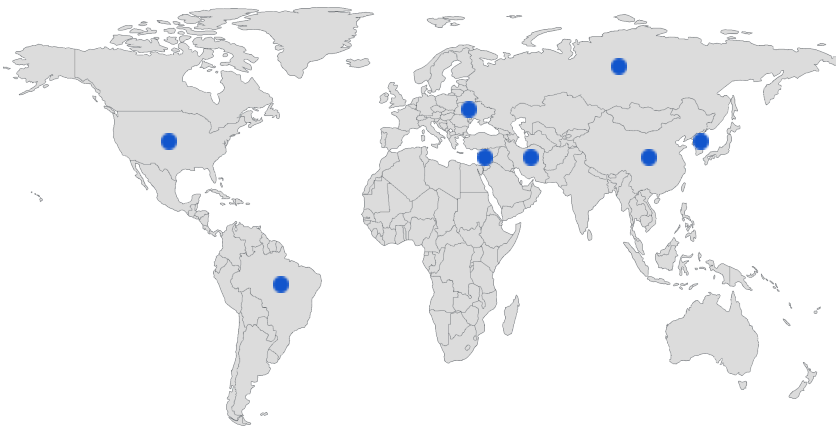


Threat Intel Report: July 22-28, 2024

Countries



Top Tags

Handala

EvilVideo

Daggerfly

Zeus

LockBit

Executive Summary

Actionable Information:

- **Phishing and Impersonation Attacks:** There is a notable increase in sophisticated phishing campaigns impersonating trusted entities to deliver malware, posing significant risks to businesses and individuals.
- **Persistent Threats in E-commerce:** Cybercriminals are targeting e-commerce platforms with advanced techniques like swap file exploitation to steal sensitive financial information, highlighting the need for enhanced security measures.
- **Mobile and Cloud Vulnerabilities:** The discovery of critical vulnerabilities in mobile applications and cloud services underscores the urgent need for regular updates and robust security protocols.
- **State-Sponsored Cyber Espionage:** There is a continued rise in state-sponsored cyber espionage activities, with attackers targeting multiple operating systems and critical infrastructures.
- **Escalating Cyber Conflicts:** Cyber warfare between nations is intensifying, as evidenced by recent DDoS attacks and data breaches, emphasizing the importance of geopolitical cybersecurity strategies.

Outlook:

The recent surge in cyber threats highlights several alarming trends: the increasing sophistication of phishing attacks impersonating trusted entities, the exploitation of vulnerabilities across a wide range of platforms and services, and the persistent risks posed by state-sponsored cyber espionage. The expanding attack surface, from cloud infrastructures to mobile applications, requires robust and continuous security measures. Organizations must prioritize immediate patching of known vulnerabilities, enhance phishing detection capabilities, and bolster security protocols to safeguard sensitive

data. The ongoing geopolitical cyber conflicts further underscore the need for vigilant cyber defense strategies to mitigate nation-state threats and protect critical infrastructure.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

⬆ 422% [CVE-2024-20767](#)

- An improper access control vulnerability in Adobe ColdFusion

⬆ 350% [CVE-2023-29357](#)

- An elevation of privilege vulnerability in Microsoft SharePoint Server

⬆ 200% [CVE-2023-3460](#)

- A vulnerability in in the Ultimate Member WordPress plugin that allows attackers to create administrator accounts

Israeli Telecommunications Site Hit By Two DDoS Attacks

+Israel +Telecommunications +DDoS

- An Israeli telecommunications site was targeted twice this week in application-layer DDoS attacks totaling almost 2M requests per second (RPS) over two days, and coming from over 7,000 IP addresses.

Attackers Target Brazilian Insurance Site in GraphQL Attacks

+Brazil +Financial Services +GraphQL

- A Brazilian insurance site experienced a variety of attack attempts, including path traversal, remote code execution, data leakage, and cross-site scripting this week in attacks coming from exclusively US-based IP addresses and primarily targeting GraphQL resources.

Recent Cyber Threats

Fake CrowdStrike Updates Deliver Malware and Data Wipers

+Crowdstrike +Malware +Israel +Iran +Handala

- Cybercriminals are exploiting recent issues with [CrowdStrike](#) updates to distribute fake fixes that install malware, including data wipers and the Remcos remote access tool. These attacks, targeting companies globally, involve phishing emails impersonating CrowdStrike support. The malware disguised as updates causes significant disruption by overwriting files and compromising systems, with one campaign by pro-Iranian hacktivist group Handala specifically targeting Israeli companies.

Attackers Exploit Swap Files to Steal Credit Card Information

+Magento +E-commerce +Skimmer

- Cybercriminals are using swap files on compromised [Magento](#) e-commerce sites to persistently install credit card skimmers. This technique allows the malware to survive multiple cleanup attempts by security teams. By capturing and exfiltrating payment data through hidden scripts, attackers can steal sensitive customer information, including credit card details, posing a significant threat to online merchants and consumers.

EvilVideo Exploit Targets Telegram for Android

+EvilVideo +Telegram

- Researchers have uncovered that the [EvilVideo](#) vulnerability in Telegram for Android is being exploited to execute arbitrary code on victims' devices. This exploitation could lead to unauthorized access and control over users' data, making it a critical security concern for Telegram users worldwide.

Chinese Malware Group Upgrades Toolkit to Target Multiple OS

+China +Daggerfly

- The Chinese espionage group [Daggerfly](#) has updated its malware arsenal to target Windows, Linux, macOS, and Android operating systems. These enhanced capabilities reflect the group's intent to infiltrate a wide range of systems, posing significant risks to various industries. This development underscores the ongoing sophistication and adaptability of Chinese cyber espionage efforts.

Privilege Escalation Vulnerability in GCP Cloud Functions

+ConfusedFunction +Cloud

- Researchers have identified a privilege escalation vulnerability named [ConfusedFunction](#) in Google Cloud Platform (GCP) Cloud Functions. This flaw allows attackers to exploit the Cloud Build service account, gaining unauthorized access to other GCP services. While Google has partially mitigated the issue for new deployments, existing instances remain vulnerable, highlighting ongoing risks in cloud infrastructure security.

ServiceNow RCE Vulnerabilities Exploited for Credential Theft

+ServiceNow +Financial Services

- Critical remote code execution (RCE) vulnerabilities in [ServiceNow](#) have been exploited to steal user credentials from thousands of sites, especially financial services. Despite ServiceNow releasing patches on July 10, many systems remain unpatched and vulnerable. Attackers leverage these flaws to execute arbitrary code and access sensitive data, including hashed and plaintext credentials, posing significant risks to affected organizations.

Ukrainian Cyberattack Disrupts Major Russian Banks

+Ukraine +Russia +DDoS

- Ukrainian military intelligence (HUR) has claimed responsibility for [DDoS attacks](#) on major Russian banks, including VTB, Russian Agricultural Bank, and Gazprombank. These attacks temporarily disrupted online services and payment systems, highlighting ongoing cyber conflicts between Ukraine and Russia. Despite quick remediation by the banks, the incident underscores vulnerabilities within Russia's financial sector.

Data Breaches

HealthEquity Data Breach Affects 4.3 Million Individuals

+US +Healthcare

- [HealthEquity](#) reported a data breach affecting 4.3 million people, compromising names, addresses, phone numbers, and payment data. The breach was discovered in June, though unauthorized access began in March via a compromised vendor account. The company has taken steps to secure affected accounts and is offering credit monitoring and identity theft services to those impacted.

Massive Bank Breach Exposes Millions of Customers' Data

+Financial Services +US +LockBit

- A major data breach at [Evolve Bank & Trust](#) has exposed the personal information of 7.6 million customers, including names, Social Security numbers, addresses, and bank account details. The attack, executed by the Russian-linked LockBit group, also affected multiple financial firms associated with the bank. Evolve Bank has advised customers to monitor their accounts and is offering two years of credit and identity monitoring services.

Casper Network Halts Operations After Security Breach

+Crypto

- [Casper Network](#) has halted its operations following a security breach that threatened its blockchain integrity. The breach has raised serious concerns about the network's security protocols and the potential loss of trust among its users and investors.

South Korean HUMINT Agency Investigates Major Data Breach

+South Korea +Government

- South Korea's [Defense Intelligence Command](#) (KDIC) is probing a severe data breach that may have compromised the identities of undercover operatives. The leak, potentially originating from a hacked personal laptop of a KDIC employee, led to the recall of several agents. This incident underscores significant vulnerabilities within the agency and could have far-reaching implications for its intelligence operations.

Zeus Hacker Group Leaks Israeli Olympic Athletes' Data

+Zeus +Israel +Olympics

- The [Zeus](#) hacker group has leaked sensitive data of Israeli Olympic athletes, including medical records and login credentials. This breach occurred just before the 2024 Paris Olympics, aiming to disrupt the athletes' preparations and privacy. The leaked information could pose significant risks to the athletes' safety and personal security.

Russian Hackers Compromise Ukrainian Telegram Channels

+Russia +Ukraine +FleepBot

- Russian hackers exploited the FleepBot service to hijack several popular Ukrainian news channels on [Telegram](#), spreading propaganda messages to millions of subscribers. The breach allowed the attackers to post content on behalf of channel owners, disrupting the flow of accurate information. Ukrainian cyber officials have warned against using software from Russia and advised Telegram channel owners to revoke FleepBot access to prevent further incidents.

Spytech's Operations and Data Exposed in Major Breach

+Spyware

- [Spytech](#), a provider of multi-platform spyware, has suffered a significant data breach revealing the global scale of its operations and exposing vast amounts of unencrypted victim data. The breach compromised device activity logs from over 10,000 devices worldwide, including PCs, Macs, Chromebooks, and Android devices. This incident highlights serious privacy concerns and potential violations of data breach notification laws, as Spytech has yet to notify affected individuals or authorities.

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.