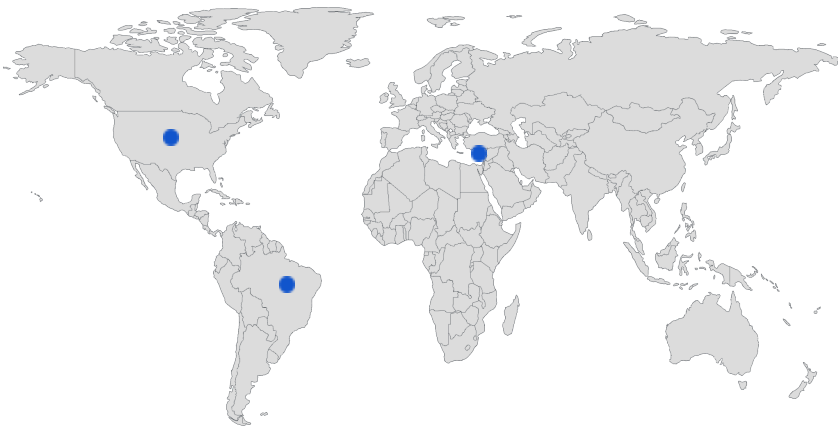


Threat Intel Report: July 1-7, 2024

Countries



Top Tags

regresshion

CapraRAT

Grasshopper

Mekotio

RockYou2024

Executive Summary

Actionable Information:

- **Increasing Sophistication of Social Engineering:** There is a notable rise in cybercriminals using sophisticated social engineering tactics, such as fake IT support websites and phishing campaigns, to distribute malicious payloads and gain unauthorized access to sensitive data.
- **Exploitation of Critical Vulnerabilities:** Several high-impact vulnerabilities have been identified across widely-used software and platforms, including OpenSSH, CocoaPods, and Ghostscript. These vulnerabilities allow attackers to execute arbitrary code and inject malicious code, posing significant security risks.
- **Growing Threats to Mobile Security:** The emergence of advanced spyware like CapraRAT targeting Android devices highlights the persistent and evolving threats to mobile security, emphasizing the need for robust mobile defense mechanisms.
- **Increasing Use of Open-Source Malware:** Advanced Persistent Threat (APT) groups, such as Grasshopper, are leveraging open-source malware and impersonating trusted entities to conduct cyberespionage, complicating detection and attribution efforts.
- **Escalating DDoS Attacks:** The occurrence of record-breaking DDoS attacks, such as the 3.3 Tbps attack utilizing MikroTik routers, underscores the escalating scale and impact of DDoS threats, necessitating enhanced DDoS mitigation strategies.
- **Widespread Data Breaches:** The week has seen several significant data breaches, including the largest password leak in history and breaches affecting major organizations, highlighting the critical need for advanced data protection measures and secure API implementations.

Outlook:

The cybersecurity landscape this week underscores the escalating sophistication and variety of threats targeting different platforms and services. The notable trends include an increase in targeted attacks through phishing campaigns and exploitation of critical vulnerabilities in widely used software. The emergence of powerful botnets and advanced spyware indicates a heightened risk for both individual users and organizations. Vigilance in patch management, robust security protocols, and continuous monitoring are crucial to mitigate these evolving threats. The significant data breaches highlight the importance of advanced security measures and employee training to protect sensitive information and prevent unauthorized access. Organizations must stay proactive in their cybersecurity strategies to navigate the complex threat environment effectively.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

⬆ 4,400% [CVE-2023-29357](#)

- An elevation of privilege vulnerability in Microsoft SharePoint.

⬆ 3,089% [CVE-2023-34960](#)

- A command injection vulnerability in the wsConvertPpt component of Chamilo.

⬆ 233% [CVE-2023-3460](#)

- The Ultimate Member WordPress plugin allows attackers to create administrator accounts at will.

2.3M RPS DDoS Attack Targets Automotive Site

+Automotive +DDoS

- An automotive sales site experienced a 2.3M requests per second (RPS) application-layer DDoS attack this week, coming from 58,000 distinct IPs.

Brazilian Travel Site Targeted by Massive Business Logic Attack

+Brazil +Travel +Business Logic

- A Brazilian travel site was targeted by massive business logic attacks this week, reaching over 85M requests in three days. Attacks came from within Brazil, and leveraged browsers like Chrome and Edge.

Recent Cyber Threats

Malicious PowerShell Scripts Disguised as Windows Fixes

+PowerShell

- Cybercriminals have created [fake IT support websites](#) that offer supposed Windows fixes but actually distribute malicious PowerShell scripts. These websites are designed to resemble legitimate technical support pages, deceiving users into downloading the harmful scripts. Once executed, the scripts allow attackers to run arbitrary commands on the victim's system, potentially leading to severe consequences such as data breaches, unauthorized access, and further malware installations. This tactic highlights the importance of verifying the authenticity of support sites and being cautious with unsolicited technical assistance.

Critical OpenSSH Vulnerability Discovered

+regression +OpenSSH

- A new vulnerability in OpenSSH server, named [regressshion](#), has been identified by security researchers. This critical flaw allows unauthenticated remote attackers to execute arbitrary code on affected systems without needing valid credentials. The vulnerability is present in the OpenSSH server's default configuration, making numerous systems potentially susceptible to exploitation. Successful exploitation could grant attackers full control over the compromised systems, leading to data theft, system manipulation, and broader network compromises. System administrators are urged to apply patches and updates immediately to mitigate the risk.

CocoaPods Bugs Pose Code Injection Risks

+CocoaPods +Injection

- Security experts have found two critical vulnerabilities in [CocoaPods](#), a widely used dependency manager for Swift and Objective-C Cocoa projects. These flaws, identified in the dependency resolution process, enable attackers to inject malicious code into applications that use CocoaPods. Such code injection could compromise the integrity of affected applications, leading to unauthorized access, data leakage, and potential execution of harmful payloads. Given the extensive use of CocoaPods in app development, developers are strongly advised to update to the latest version to safeguard their applications from these threats.

CapraRAT Spyware Targets Android Devices

+CapraRAT +Android

- Researchers have uncovered a new strain of spyware named [CapraRAT](#), which targets Android users. This sophisticated spyware can infiltrate devices to steal sensitive information such as call logs, SMS messages, and GPS location data. Additionally, it has capabilities to record audio and video, providing attackers with comprehensive surveillance tools. CapraRAT is distributed through deceptive means, often masquerading as legitimate applications to gain installation on target devices. This discovery underscores the persistent threats to mobile security and the need for robust anti-malware defenses.

Grasshopper Operators Impersonate Israeli Entities

+Grasshopper +Israel

- Threat actors associated with the [Grasshopper](#) Advanced Persistent Threat (APT) group have been found impersonating Israeli government agencies and private companies to spread open-source malware. This campaign aims to conduct cyberespionage by tricking targets into executing the malware, thereby enabling the attackers to gather intelligence and sensitive information. The impersonation of trusted entities increases the likelihood of successful infections, posing significant risks to targeted organizations. The use of open-source malware tools also makes attribution and detection more challenging, highlighting the sophisticated tactics employed by Grasshopper operators.

Record-Breaking DDoS Attack Attributed to MikroTik Botnet

+DDoS +MikroTik

- A record-breaking Distributed Denial-of-Service (DDoS) attack has been reported, attributed to a botnet exploiting [MikroTik](#) routers. The attack reached a staggering 3.3 Tbps, making it one of the largest DDoS attacks ever recorded. The botnet leveraged vulnerable MikroTik devices to generate massive traffic volumes, overwhelming infrastructure and causing service disruptions. This incident underscores the importance of securing IoT devices and implementing robust DDoS protection measures.

Mekotio Banking Trojan Targets Latin American Users

+Mekotio +Financial Services +Trojan

- Researchers have detailed the activities of the [Mekotio](#) banking trojan, which primarily targets users in Latin America. Mekotio is distributed through phishing emails and uses various techniques to evade detection, including obfuscation and modular components. Once installed, the trojan steals banking credentials and other sensitive information, enabling attackers to conduct fraudulent transactions.

Hackers Exploit HFS Servers to Deploy Malware and Cryptominers

+HFS +Malware +Cryptocurrency

- Cybercriminals are exploiting vulnerabilities in [HTTP File Server](#) (HFS) to drop malware and Monero cryptocurrency miners onto compromised systems. Attackers scan for vulnerable HFS instances, then use known exploits to gain

access and deploy their malicious payloads. This campaign has led to numerous infections, with affected systems being used to mine Monero, consuming significant resources and potentially leading to broader system compromises.

Severe Ghostscript Vulnerability Discovered

+GhostScript

- A newly discovered vulnerability in [Ghostscript](#), an interpreter for PostScript and PDF files, has been rated as highly severe. This flaw allows attackers to execute arbitrary code by exploiting the Ghostscript interpreter when processing malicious files. The vulnerability affects multiple applications that rely on Ghostscript for rendering documents, posing a widespread risk. Users and administrators are urged to apply available patches immediately to prevent exploitation and potential system compromises.

Data Breaches

Largest Password Leak in History: 10 Billion Exposed in RockYou2024

+RockYou2024

- A massive data leak, dubbed [RockYou2024](#), has exposed 10 billion passwords, making it the largest password breach ever recorded. The leaked data includes passwords from previous breaches compiled into a single, easily accessible file. This unprecedented leak increases the risk of account takeovers and underscores the need for robust password security measures, such as using unique passwords for different accounts and enabling multi-factor authentication.

OpenAI Hack Compromises Sensitive Data

+AI

- [OpenAI](#) suffered a significant security breach that exposed sensitive user data in 2023. The attackers gained unauthorized access through a sophisticated phishing campaign targeting employees. The compromised data includes user email addresses, API keys, and internal documents. This incident highlights the vulnerabilities even in advanced tech companies and the critical need for enhanced security protocols and employee training to prevent such breaches.

Data Breach Exposes Personal Information of Roblox Creators

+Gaming

- A recent data breach at [Roblox](#) has exposed the personal information of its creators. The compromised data includes names, addresses, email addresses, and other sensitive details of those who create and publish content on the platform. This breach puts affected individuals at risk of identity theft and targeted attacks, emphasizing the importance of robust data protection measures within the gaming industry.

Twilio Data Breach Exposes 33 Million Authy Phone Numbers

+MFA +API Security

- A data breach at [Twilio](#) has exposed the phone numbers of 33 million users of its Authy two-factor authentication service. The breach was caused by an unsecured API endpoint, which attackers exploited to gain access to sensitive information. This exposure poses significant risks to users' security and privacy, stressing the need for secure API implementations and vigilant monitoring of access points.

Geisinger and Nuance Communications Suffer Data Breach

+Healthcare +US

- [Geisinger Health and Nuance Communications](#) have been affected by a data breach that exposed sensitive patient information. The compromised data includes medical records, personal identification details, and billing information. The breach came from a former employee, impacting thousands of patients. This incident underscores the critical need for stringent security measures in healthcare data management to protect patient privacy.



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.