Zscaler Identifies More Than 200 Malicious Apps in the Google Play Store, with Over 8 Million Installs

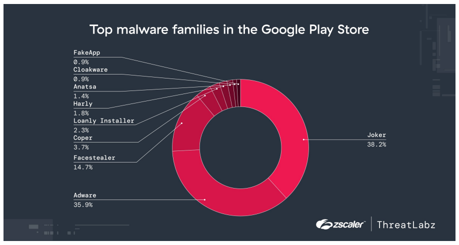
October 15, 2024

Annual ThreatLabz Report Highlights Mobile, IoT, and OT Cybersecurity Trends, Risks, and Prescriptive Zero Trust Defense Strategies

Key Findings:

- Mobile remains a top threat vector, with 111% growth in spyware and 29% growth in banking malware
- Technology, education, and manufacturing sectors continue to be most susceptible to attacks
- The United States remains the top target for IoT, OT, and mobile cybersecurity attacks

Top Malware Families in Google Play Store



Annual Zscaler ThreatLabz Report Highlights Mobile, IoT, and OT Cybersecurity Trends.

SAN JOSE, Calif., Oct. 15, 2024 (GLOBE NEWSWIRE) -- Zscaler, Inc. (NASDAQ: ZS), the leader in cloud security, today published its Zscaler ThreatLabz 2024 Mobile, IoT, and OT Threat Report, which offers an overview of the mobile and IoT/OT cyber threat landscape from June 2023 through May 2024. The findings in this report stress the urgency for organizations to reevaluate and secure mobile devices, IoT devices and OT systems. ThreatLabz identified more than 200 malicious apps in the Google Play Store, with more than 8 million collective installs, and the Zscaler cloud blocked 45% more IoT malware transactions than last year–indicative of botnets continuing to proliferate across IoT devices.

"Cybercriminals are increasingly targeting legacy exposed assets which often act as a beachhead to IoT & OT environments, resulting in data breaches and ransomware attacks," said Deepen Desai, Chief Security Officer at Zscaler. "Mobile malware and AI driven vishing attacks adds to that list making it critical for CISOs and CIOs to prioritize an AI powered zero trust solution to shut down attack vectors of all kinds safeguarding against these attacks."

Financially motivated mobile attacks remain a top threat vector
With 29% growth in banking malware attacks and a 111% rise in spyware year over year, cyberattacks have never been more profitable for threat actors, either through monetary gain via direct extortion or passthrough use of stolen personally identifiable information (PII) and user credentials that can be sold and leveraged in future attacks.

Anatsa, a known Android banking malware that uses PDF and QR code readers to distribute malware, has targeted more than 650 financial institutions, and more specifically, users in Germany, Spain, Finland, South Korea and Singapore.

Verticals most targeted by bad actors
The technology (18%), education (18%) and manufacturing (14%) sectors are the most frequent targets of mobile malware. Education in particular saw a dramatic 136% increase in blocked transactions compared to the previous year.

Additionally, for the second year in a row, manufacturing experienced the highest volume of IoT malware attacks, accounting for 36% of all IoT malware blocks observed on the Zscaler Zero Trust Exchange™ platformWhen analyzing unique devices across different verticals, this sector stands out with the highest implementation of IoT devices due to its extensive use of IoT applications, ranging from automation and process monitoring to supply chain management.

The United States remains the top target for IoT cyberattacks
With its central role in global communication and data processes, the US also stands out as the primary destination for IoT device traffic, accounting for 81% of IoT cyberattacks. The top five countries that receive the most IoT traffic are:

- United States
- Japan
- China
- Singapore
- Germany

The report also revealed that India (28%) is now the country most targeted by mobile malware. The other four are:

- United States
- Canada
- South Africa
- The Netherlands

Legacy and end-of-life operating systems leave OT systems vulnerable
Once air-gapped and isolated from the internet, OT and cyber-physical systems have rapidly become integrated into enterprise networks, enabling threats to proliferate. OT deployments can involve thousands of connected devices spread across dozens of sites, creating a substantial attack surface for external threats, such as those that exploit known zero-day vulnerabilities. Additionally, this also creates a large attack surface between

internal (east-west) OT traffic, increasing the risk of lateral movement and the potential blast radius of a successful attack.

How to secure mobile, IoT and OT

With today's hybrid-work environments, users can work from anywhere with internet access, SaaS apps and private applications, whether in the cloud or the data center. To enable secure hybrid work and provide seamless access to any application, enterprises need to retire network-centric approaches, which hamper productivity and leave them vulnerable to lateral movement. Instead, organizations must adopt a zero trust architecture that enables secure remote access from any user device to any application, from any location.

Zscaler for IoT and OT enables enterprises to reduce cyber risk while embracing IoT and OT connectivity to drive business agility and increase productivity. Powered by the Zero Trust Exchange, these capabilities protect IoT devices against compromise and prevent lateral movement with device segmentation and deception–all while allowing for remote access to OT systems without risky VPN connectivity.

The findings of the 2024 Mobile, IoT, and OT Threat Report stress the need for organizations to better secure their mobile endpoints, IoT devices, and OT systems. Download the full report here.

Research Methodology

The Zscaler ThreatLabz team analyzed a data set collected from the Zscaler Security Cloud between June 2023 and May 2024, comprising more than 20 billion threat-related mobile transactions and associated cyberthreats.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange is the world's largest in-line cloud security platform.

Media Contact:

Zscaler PR
Natalia Wodecki
press@zscaler.com

A photo accompanying this announcement is available at https://www.globenewswire.com/NewsRoom/AttachmentNg/6430484e-f976-4e51-9584-160090d397e6