Avast Blocks Record Breaking 10 Billion Attacks in 2023, Nearly a 50% Increase from Previous Year

2024-02-07

Malicious push notifications, PDF deception, cookie exploiting information stealers and more in Q4 2023

TEMPE, Ariz. and PRAGUE, Feb. 7, 2024 /PRNewswire/ -- Avast, a leader in digital security and privacy and brand of Gen™ (NASDAQ: GEN), blocked an unprecedented 10 billion attacks in 2023 for a remarkable 49% increase year-over-year. According to the latest quarterly Avast Threat Report, which looks at the threat landscape from October-December 2023, scams, phishing and malvertising continue to account for more than 75% of all cyber threats. These threats often leverage malicious push notifications and new AI methods such as deepfakes to lure victims into sophisticated financial fraud. The past quarter was also marked by a surge in malware attacks utilizing PDF files and new techniques of exploiting Google to steal information.

"In the past three months, we have seen cybercriminals move from relying only on social engineering to further exploiting trusted digital mediums, be it highly believable deepfake video scams or threats spreading through PDF files," explains Jakub Křoustek, Malware Research Director for Avast. "This trend not only reflects the ever-changing methods of cybercriminals but also highlights the vulnerabilities inherent in our everyday digital life. Now more than ever, people need to verify what they encounter online and utilize tools to help stay safe."

Careful What You Open: PDF File Deception

In the last quarter of 2023, Avast blocked more than 10 million PDF-based attacks, protecting more than 4 million users worldwide. Threat actors turned their attention to PDF files in the final months of the year, weaving a complex web of attacks. Avast researchers observed a spectrum of PDF-related threats and scams, ranging from simple lottery and dating scams, to documents containing deceptive information such as phishing links directing people to pages mimicking well-known brands like Netflix or Amazon. Researchers also saw an uptick in complex campaigns delivering more sophisticated threats like password stealers such as AgentTesla.

The proliferation of PDF-based cyber threats underscores a significant shift in the tactics of cybercriminals. PDF files are popular due to their platform-agnostic nature, which allows them to be seamlessly opened from any device, making them the ultimate delivery payload. Furthermore, PDF attachments are often allowed by default by spam gateways, adding another layer of vulnerability.

Scams Get More Aggressive, From Push Notifications to Deepfakes

Web threats continued to dominate, with scams, phishing, and malvertising ranking as the top threat types overall. The use of malicious browser push notifications escalated, becoming a preferred tool for scammers across various domains, from adult content sites to technical support scams.

Beyond the methods of delivery for scams, AI continues to help criminals create more believable scams. Deepfake videos, especially those endorsing investment scams, displayed a heightened level of sophistication in the final quarter of the year, challenging the ability to distinguish between real and fabricated content.

Information Stealers Exploit Cookies

The final quarter of 2023 also brought a new and interesting stealing capability which was rapidly adapted by information stealers: abusing the Google OAuth endpoint, which is used for synchronizing accounts across Google services, for recovering authentication cookies. This type of cookie can store a unique identifier that verifies a user's identity and permissions when accessing websites. With authentication cookies, threat actors are able to gain access to login information and other sensitive data. One of the first info-stealers to adapt this technique was Lumma, a rapidly rising malware-as-a-service stealer, with others quickly following.

For more information and to read the full Avast Q4/2023 threat report, visit https://decoded.avast.io/threatresearch/**avast-q4-2023-threat-report**

About Avast

Avast is a leader in digital security and privacy, and part of Gen™ (NASDAQ: GEN), a global company dedicated to powering Digital Freedom with a family of trusted consumer brands. Avast protects hundreds of millions of users from online threats, for Mobile, PC or Mac are top-ranked and certified by VB100, AV-Comparatives, AV-Test, SE Labs and others. Avast is a member of the Coalition Against Stalkerware, No More Ransom and Internet Watch Foundation. Learn more at Avast.com. Visit: www.avast.com.

Brittany Posey-Thomas
Gen
Press@GenDigital.com

Courtney Rowles
Edelman for Gen
Courtney.Rowles@edelman.com

View original content to download multimedia:https://www.prnewswire.com/news-releases/avast-blocks-record-breaking-10-billion-attacks-in-2023-nearly-a-50-increase-from-previous-year-302056082.html

SOURCE Gen Digital Inc.