Latest Avast Threat Report Discovers Cybercriminals Using Common Applications from Microsoft and Adobe to Lure Victims

2023-05-04

Report shows two out of three cyber threats now leverage social engineering, driving phishing and scam attacks

TEMPE, Ariz. & PRAGUE, May 4, 2023 – In the first quarter of 2023 there was a significant increase in cyberattacks exploiting trust in established tech brands Microsoft and Adobe, according to Avast, a leader in digital security and privacy, and a brand of Gen™ (NASDAQ: GEN). The Avast Q1 2023 Threat Report, released today, also found a 40 percent rise in the share of phishing and smishing attacks over the previous year. Overall, two out of three threats people encounter online today use social engineering techniques, taking advantage of human weaknesses.

Malware, scams, and phishing attacks attempt to steal consumers' sensitive data, like passwords, Social Security numbers, and other personal identifiable information. When this data gets into the wrong hands, cybercriminals have the arsenal to easily steal someone's identity. Identity theft can lead to a nightmare of events, from scammers ruining people's credit score, to selling their information on the dark web, and even impersonating people to pass background checks.

"If you think your data has no value then why would scammers spend so much time trying to steal your data if it's worthless? The truth is that *anyone* can be affected and it is important to stay vigilant and use proper protection," said Jakub Kroustek, Avast Malware Research Director. "Unfortunately, scammers have made it nearly impossible to take any message as face value – all communications, whether seemingly from a friend, boss, or household brand, have potential to be fraudulent."

New Malware Distribution Tactics Abusing Microsoft OneNote & Adobe Acrobat Sign

Cybercriminals know they can lure victims by using the names and likeness of well-known brands that consumers already trust. Avast has observed this trend among two popular applications commonly used for work: Microsoft OneNote and Adobe Acrobat Sign.

Scammers are sending out Microsoft OneNote files as email attachments to victims. When someone opens the attachment, it triggers the download of malware onto a device. Avast has spotted malware such as Qbot and Raccoon using this distribution technique to steal information, and has also observed IcedID, a banking Trojan, using OneNote attachments to steal money. During Q1 of 2023, Avast protected more than 47,000 global customers> and more than 18,000 U.S. customers from these types of attacks.

In some cases, Avast researchers also observed cybercriminals exploit Adobe Acrobat Sign by adding malicious links into documents that are sent from legitimate Adobe email addresses. These links prompt victims to download .ZIP files, which contain a variant of the Redline Trojan that can steal passwords, crypto

wallets, and more.

“My advice is to take extra caution with any email asking you to download files or click on a link, even those that appear to be from reputable brands,” advises Jakub Kroustek. “Cyber Safety software can act as a safety net for providing an extra layer of security to these types of savvy attacks that are increasingly targeting people.”

Avast’s Web Shield technology, part of all Avast Antivirus versions, is capable of scanning and unpacking OneNote files to detect malware. The threat research team has also developed specific heuristics and Yara rules to keep people safe from these threats.

Scammers are Casting More Lures as the Share of Phishing Attacks Increases 40% YoY

Phishing continues to be another way scammers take advantage of trust, posing a significant and rising threat to consumers. The Avast team found that the share of global phishing attempts among all threats blocked in Q1 was up 40% compared to the same quarter in 2022.

One type of phishing scam on the rise is refund and invoice scams, which happen when fraudsters send false bills or invoices for goods or services that were never ordered or received. Scammers often use household names with recognizable branding and logos to make these scams appear legitimate. Invoice scams had a sharp uptick in Q1 2023, rising 19% in the U.S. compared to Q4 2022.

The pervasiveness of attacks via mobile text messages, called smishing attacks, has also contributed to the rising rate of phishing incidents. The issue has become so severe that in March of this year, the U.S. Federal Communications Commission (FCC) announced its first rules targeting smishing by requiring that mobile service providers block certain robotext messages that are likely to be illegal. Common smishing attack themes include financial alerts, package delivery notifications, tax alerts, charity scams and lottery scams.

“Scammers often play off victims’ emotions by creating a sense of urgency in their messages. If you receive an email or text out of the blue with an urgent request, or a message that seems too good to be true, take a few extra moments to verify it before acting,” says Jakub Kroustek. “Always take a close look to confirm that an email or text is coming from a trusted sender, and if you have any doubt, go directly to the source, whether that be a person you know or a company’s help portal.”

Avast Free Antivirus, all Avast’s premium versions, and Avast Secure Browser provide top protection against phishing attacks, which is verified in quarterly tests by independent testing organization AV-Comparatives.

The Avast Q1 2023 Threat Report can be found here: https://decoded.avast.io/threatresearch/avast-q1-2023-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 including Norton, Avast, LifeLock, Avira, AVG, ReputationDefender and CCleaner. With hundreds of million users online, Avast protects hundreds of millions of users from online threats, for Mobile, PC or Mac that 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. Visit: www.avast.com.