Deepfakes, AI-Manipulated Audio, and Hijacked Social Media Surge in 2024

2024-05-14

Avast Threat Report shows nearly 90% of cyberthreats currently rely on human manipulation

TEMPE, Ariz. and PRAGUE, May 14, 2024 /PRNewswire/ -- Avast, a leader in digital security and privacy and brand of Gen™ (NASDAQ: GEN), has reported that social engineering threats – those which rely on human manipulation – account for most cyberthreats faced by individuals in 2024. According to the latest quarterly Avast Threat Report, which looks at the threat landscape from January-March 2024, scams, phishing and malvertising accounted for 90% of all threats on mobile devices and 87% of threats on desktop. Moreover, the threat research team discovered a significant spike in scams leveraging sophisticated tactics such as using deepfake technology, AI-manipulated audio synchronization, and hijacking of YouTube and other social channels to disseminate fraudulent content.

YouTube: A Potent Gateway for Criminals

While all social media is a natural breeding ground for scams, YouTube has become a significant channel for crime. According to telemetry from Avast, 4 million unique users were protected against threats on YouTube in 2023, and approximately 500,000 were protected in January-March 2024.

Automated advertising systems combined with user-generated content provides a gateway for cybercriminals to bypass conventional security measures, making YouTube a potent channel for deploying phishing and malware. Notable threats on the platform include credential stealers like Lumma and Redline, phishing and scam landing pages, and malicious software disguised as legitimate software or updates.

Scammers have also turned heavily to videos as lures. Whether from stock footage or an elaborate deepfake, scammers are using all video varieties in their threats. One of the most widespread techniques involves exploiting famous individuals and significant media events to attract large audiences. These campaigns often use deep fake videos, created by hijacking official videos from events and using AI to manipulate audio synchronization. These videos seamlessly blend altered audio with existing visuals, making it harder for the untrained eye to tell they're anything but authentic.

Additionally, YouTube serves as a conduit to Traffic Distribution Systems (TDS), directing people to malicious sites and supporting scams ranging from fake giveaways to investment schemes.

Some of the most common tactics through which YouTube is exploited for scams include:

Phishing Campaigns Targeting Creators: Attackers send personalized emails to YouTube creators proposing fraudulent collaboration opportunities. Once trust is established, they send links to malware under the guise of software needed for collaboration, often leading to cookie theft or account compromise.
Compromised Video Descriptions: Attackers upload videos with descriptions containing malicious links,

masquerading as legitimate software downloads related to gaming, productivity tools, or even antivirus programs, tricking users into downloading malware.
Channel Hijacking for Scams: By gaining control of YouTube channels through phishing or malware, attackers repurpose these channels to promote scams – such as cryptocurrency scams – often involving fake giveaways that require an initial deposit from viewers.
Exploitation of Software Brands and Legitimate-Looking Domains: Attackers create websites that mimic reputable companies that people trust and offer illegitimate downloadable software.
Social Engineering via Video Content: Attackers post tutorial videos or offers for cracked software, guiding people to download malware disguised as helpful tools. This tactic takes advantage of people seeking free access to otherwise paid services or software, leveraging YouTube's search and recommendation algorithms to target potential victims.

The Growing Business of Malware-as-a-Service (MaaS)

With scams surging, cybercriminals are capitalizing on a new business opportunity: Malware-as-a-Service (MaaS). Through this model, organized crime groups are able to recruit smaller-scale criminals who want to make quick money by distributing malware on behalf of the group. These criminals can purchase malware, subscribe to it or share profits in a commission-style partnership.

The most common malware utilized in MaaS are information stealers, which are continuing to find new distribution channels. For example, DarkGate was observed to be spread via Microsoft Teams, using phishing. Lumma Stealer, another MaaS information stealer, continues to spread via cracked software propagated on YouTube, using fake tutorials to mislead victims. This further emphasizes that such strains – and their creators – never miss an opportunity to leverage social engineering to distribute malware.

"In the first quarter of 2024, we reported the highest ever cyber risk ratio – meaning the highest probability of any individual being the target of a cyberattack," said Jakub Kroustek, Malware Research Director at Gen. "Unfortunately, humans are the weakest link in the digital safety chain, and cybercriminals know it. They pray on human emotions and the quest for knowledge to infiltrate people's lives and devices for financial gain."

For more information and to read the full Avast Q1/2024 threat report, visit https://decoded.avast.io/threatresearch/avast-q1-2024-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/deepfakes-ai-manipulated-audio-and-hijacked-social-media-surge-in-2024-302144256.html

SOURCE Gen Digital Inc.