Multi-million-dollar Deepfake Campaigns Blocked by Gen

2024-09-04

Gen Quarterly Threat Report shows AI-fueled scams, digital identity attacks and ransomware dominating consumer cybersecurity landscape

TEMPE, Ariz. and PRAGUE, Sept. 4, 2024 /PRNewswire/ -- Gen™ (NASDAQ: GEN), a global leader in consumer Cyber Safety with a family of brands, Norton, Avast, LifeLock, Avira, AVG, ReputationDefender and CCleaner, today released the Q2/2024 Gen Threat Report. The report spotlights the most notable cyberattacks targeting consumers from April to June 2024. Gen experts warn that it is more important than ever to stay vigilant as cybercriminals increasingly use generative AI to create sophisticated scams using voices, images and videos to make their schemes more convincing. Attackers are using celebrities, global events, and brands as shiny lures. And as more people find themselves navigating economic hardships, the promise of easy money through phony investments, cryptocurrency giveaways and part-time job offers has also become a timely hook for scammers preying upon unsuspecting victims seeking financial security.

"We continue to see cybercriminals expand their toolkits with even more uses of AI to strengthen their attacks," said Siggi Stefnisson, Chief Technology Officer at Gen. "Scammers are cunning and adept at exploiting what is most likely to be on consumers' minds – whether it has to do with elections, love or financial security. Now with AI and other new tech, their schemes are more sophisticated and convincing than ever before. We urge consumers to stay informed and alert. We will continue to keep a watchful eye on the latest threats and provide the latest knowledge and tools needed to be safer despite the evolving threat landscape."

Gen has one of the world's largest consumer Cyber Safety networks protecting people around the globe against advanced online threats. Throughout Q2, Gen Cyber Safety brands blocked over one billion unique attacks each month, up 46% compared to last year. Interestingly, a staggering 95% of attacks happen while people use their browser and surf the web. In addition to blocking threats directly as part of our customers' products and services, Gen researchers discovered and reported security vulnerabilities so that they could be patched by other companies, helping protect people from further attacks.

Gen experts shared some of the most prevalent threats to watch for based on this quarter's findings:

Scammers' Playbook: New and Revamped Tactics
The accessibility and rise of AI allow cybercriminals to add a modern twist to their old tricks to lure more victims. We have seen bad actors using deepfakes of celebrities to promote fake cryptocurrency investment schemes, and now, scammers are targeting widely publicized events that will be broadcast live to draw a large audience. For example, recently, scam group CryptoCore lured victims with highly convincing deepfakes of official events disseminated on compromised YouTube accounts and used QR codes to direct victims to fake crypto giveaway campaigns, stealing $5 million. During the SpaceX Starship integrated flight test (IFT-4) in June, nearly 50 YouTube accounts were hijacked, and the campaign resulted in 500 transactions amounting to a total value of $1.4 million. Gen products helped protect thousands of people from this threat in Q2, with the largest amounts in the US, UK, Brazil and Germany.

Amid challenging economic conditions, scammers are capitalizing on consumers' needs with part-time job scams that promise quick money by completing simple tasks, like promoting goods on social media. Once trust is established, the scammers convince their victim to send them money so they can steal it. These scams have now evolved from text-based interactions on Telegram to more sophisticated AI-generated voice communications, adding a whole new layer of deception and realism.

This quarter saw the revival of the classic antivirus scam that was first popular in the late 2000s, when cybercriminals were making millions of dollars by selling fake antivirus products. Nowadays, cybercriminals deploy aggressive pop-up alerts that mimic real antivirus programs, often claiming the computer is infected to urge immediate action. These fake alerts abuse the Windows notification system to appear as credible system messages to scare the person into purchasing antivirus software so the scammers can earn commissions through third-party referral programs.

Digital Identity Theft: The New Gold Rush
As large-scale company breaches seemingly become the norm in 2024, cybercriminals turn an eye toward stealing digital identities. Attackers are using direct methods such as Information Stealers (InfoStealers) and Mobile Bankers, going beyond buying data on the Dark Web to snap up consumers' valuable personal information.

InfoStealers breach devices to steal login details, session cookies, passwords and financial information. While InfoStealers saw a slight decline in Q2/2024, notable malware families continue to grow, with the most dominant AgentTesla increasing its market share by 11 %.

Mobile bankers, on the other hand, specifically target mobile devices to steal banking details, cryptocurrency wallets, and instant payments credentials. In Q2/2024, Bankers such as TeaBot, disguised as a PDF reader, targeted Revolut customers. Meanwhile, spyware threats such as XploitSpy and AridSpy are sneaking onto the PlayStore, stealing files and monitoring users through their cameras and microphones.

LifeLock provides a 12-step guide to help people if they believe their identity may have been compromised.

On the Rise: Consumer Ransomware
Consumers remain an attractive target for ransomware as they often have less protection in place than large companies. According to Gen telemetry, there was a 24% rise quarter over quarter in consumer ransomware attacks in Q2/2024. India saw a staggering 379% increase, followed by notable spikes in the United States, Canada and the United Kingdom. A popular delivery technique is to hide ransomware payload in pirated content. Even though some operators of major ransomware gangs like LockBit have been brought to justice in the last quarter, Gen urges consumers to take precautions to keep their data safe, such as doing regular back-ups.

Gen researchers collaborate with governments across the globe to combat ransomware by providing free decryption tools for victims, and most recently released the Avast DoNex Ransomware Decryptor.

To read the full Q2/2024 Gen Threat Report, visit: https://www.gendigital.com/blog/news/innovation/q2-2024-threat-report.

This marks the inaugural Gen Threat Report. Previously, Gen brands separately reported quarterly threat news with the Norton Pulse Report and Avast Quarterly Threat Report. The Gen Threat Report now offers a comprehensive look at the rising threats we monitor and protect our customers from each day and trends we see across the threat landscape.

About Gen

Gen™ (NASDAQ: GEN) is a global company dedicated to powering Digital Freedom through its trusted Cyber Safety brands, Norton, Avast, LifeLock, Avira, AVG, ReputationDefender and CCleaner. The Gen family of consumer brands is rooted in providing safety for the first digital generations. Now, Gen empowers people to live their digital lives safely, privately, and confidently today and for generations to come. Gen brings award-winning products and services in cybersecurity, online privacy and identity protection to nearly 500 million users in more than 150 countries. Learn more at GenDigital.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/multi-million-dollar-deepfake-campaigns-blocked-by-gen-302237761.html

SOURCE Gen Digital Inc.