Pagina 4 - Iranian APT35 Hackers Targeting Israeli Tech Experts with AI-Powered Phishing Attacks

Classificações de Malware:

- keylogger (Spyware)
- spyware (Spyware)
- ransomware (Ransomware)
- crypto (Ransomware)
- trojan (Trojan)
- trojanized (Trojan)
- virus (Virus)
- infected (Virus)
- infection (Virus)
- exploit (Exploit)
- cve (Exploit)
- dropper (Trojan)
- backdoor (Backdoor)

An Iranian state-sponsored hacking group associated with the Islamic Revolutionary Guard Corps (IRGC) has been
linked to a spear-phishing campaign targeting journalists, high-profile cyber security experts, and computer
science professors in Israel."In some of those campaigns, Israeli technology and cyber security professionals
were approached by attackers who posed as fictitious assistants to technology executives or researchers throug
h emails and WhatsApp messages," Check Pointsaidin a report published Wednesday. "The threat actors directed v
ictims who engaged with them to fake Gmail login pages or Google Meet invitations."The cybersecurity company a
ttributed the activity to a threat cluster it tracks asEducated Manticore, which overlaps with APT35 (and its
sub-clusterAPT42), CALANQUE, Charming Kitten, CharmingCypress, Cobalt Illusion, ITG18, Magic Hound, Mint Sands
torm (formerly Phosphorus), Newscaster, TA453, and Yellow Garuda.The advanced persistent threat (APT) group ha
s alonghistoryoforchestrating social engineering attacksusing elaborate lures, approaching targets on various

platforms like Facebook and LinkedIn using fictitious personas to trick victims into deploying malware on their systems.Check Point said it observed a new wave of attacks starting mid-June 2025 following theoutbreak of the Iran-Israel warthat targeted Israeli individuals using fake meeting decoys, either via emails or WhatsApp messages tailored to the targets. It's believed that the messages are crafted using artificial intelligence (AI) tools due to the structured layout and the absence of any grammatical errors.One of the WhatsApp messages flagged by the company took advantage of the current geopolitical tensions between the two countries to coax the victim into joining a meeting, claiming they needed their immediate assistance on an AI-based threat detection system to counter a surge in cyber attacks targeting Israel since June 12.The initial messages, like those observed in previous Charming Kitten campaigns, are devoid of any malicious artifacts and are primarily designed to gain the trust of their targets. Once the threat actors build rapport over the course of the conversation, the attack moves to the next phase by sharing links that direct the victims to fake landing pages capable of harvesting their Google account credentials."Before sending the phishing link, threat actors ask the victim for their email address," Check Point said. "This address is then pre-filled on the credential phishing page to increase credibility and mimic the appearance of a legitimate Google authentication flow.""The custom phishing kit [...] closely imitates familiar login pages, like those from Google, using modern web technologies such as React-based Single Page Applications (SPA) and dynamic page routing. It also uses real-time WebSocket connections to send stolen data, and the design allows it to hide its code from additional scrutiny."The fake page is part of a custom phishing kit that can not only capture their credentials, but also two-factor authentication (2FA) codes, effectively facilitating 2FA relay attacks. The kit also incorporates a passive keylogger to r ecord all keystrokes entered by the victim and exfiltrate them in the event the user abandons the process midway.Some of the social engineering efforts have also involved the use of Google Sites domains to host bogus Google Meet pages with an image that mimics the legitimate meeting page. Clicking anywhere on the image directs the victim to phishing pages that trigger the authentication process."Educated Manticore continues to pose a persistent and high-impact threat, particularly to individuals in Israel during the escalation phase of the Iran-Israel conflict," Check Point said."The group continues to operate steadily, characterized by aggressive spear-phishing, rapid setup of domains, subdomains, and infrastructure, and fast-paced takedowns when identified. This agility allows them to remain effective under heightened scrutiny."Discover real-time defense tactics to detect and block deepfakes, fake domains, and multi-channel scams before they cause damage.We'll unpack how leading teams are using AI, privacy-first design, and seamless logins to earn user trust and stay ahead in 2025. Get the latest news, expert insights, exclusive resources, and strategies from industry leaders all for free.

Link: https://thehackernews.com/2025/01/python-based-malware-powers-ransomhub.html