Trust Exploited: the Rise of IT Support Impersonation and Interactive Intrusion

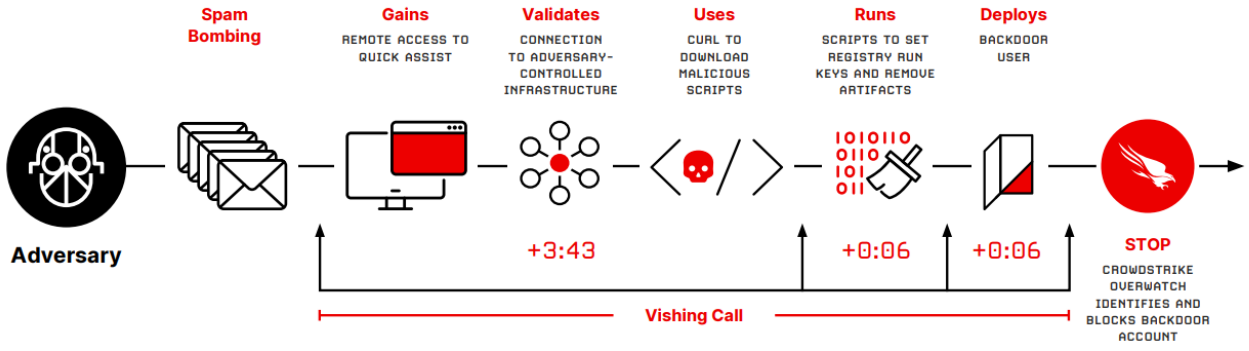
October 2025

Ilaria Sangalli, *Index Research Lead*

In today's rapidly evolving digital landscape, cybercriminals are constantly refining their tactics to exploit both human and technological vulnerabilities. Among the most concerning trends are IT support impersonation and interactive intrusions. These methods rely on familiarity, urgency, and the illusion of legitimacy.

Unlike automated attacks, interactive intrusions involve adversaries actively engaging with compromised systems, issuing commands, escalating privileges, or deploying ransomware manually. These intrusions allow attackers to tailor their actions dynamically as they learn more about the compromised environment. By imitating the actions of legitimate users or system administrators, these intrusions can seamlessly blend into normal activity, making them exceptionally difficult for traditional detection systems to identify. CrowdStrike reported a 35% increase in interactive intrusion campaigns in 2024, with the technology sector being the most targeted. Geographically, the U.S. accounted for 53% of detected cases, followed by East Asia (14%) and Europe (11%), underscoring the global nature of the threat.[1]

In 2024, CURLY SPIDER emerged as one of the fastest and most adaptive eCrime adversaries, executing high-speed, hands-on intrusions with remarkable precision. In a notable incident, the adversary completed their entire attack chain in under four minutes.[2]



Source: CrowdStrike

The attack began with a wave of spam emails impersonating charities, newsletters, or financial offers. Shortly after, the victim received a phone call from someone posing as IT support, claiming the spam was

[1] https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrikeGlobalThreatReport2025.pdf?version=0
[2] From initial user interaction and social engineering to establishing persistent access

caused by malware or outdated filters. This technique is known as vishing (voice phishing), where attackers use phone calls to trick individuals into giving up sensitive information or taking harmful actions, often by pretending to be someone trustworthy like tech support.The caller then instructed the user to join a remote session using Microsoft Quick Assist, a legitimate remote management tool. Once connected, CURLY SPIDER gained direct access to the system.[3]

Another deceptive tactic uncovered by Malwarebytes, a cybersecurity company known for its anti-malware software, involves cybercriminals leveraging malvertising[4] to trick users into calling fake tech support numbers. In this scheme, attackers purchase Google ads that appear to link to legitimate websites. When clicked, the ad redirects to a page that auto-populates the site's search bar with a fraudulent phone number. The page looks authentic, and the browser displays the real URL, making the fake number seem credible. Unsuspecting users call the number, where scammers impersonate support agents to steal personal information, financial data, or gain remote access to the victim's device.[5,6]

These developments underscore a significant shift in the tactics used by cybercriminals. As attackers become more sophisticated, organizations must respond with equal agility. Raising employee awareness, enforcing rigorous verification protocols, and investing in adaptive cybersecurity measures are no longer optional, they are essential.

As the threat landscape continues to evolve, so too must the strategies used to defend against it. Several Nasdaq-100® (NDX®) companies are at the forefront of this effort. As an example, Palo Alto Networks, CrowdStrike, Cisco, Fortinet, and Zscaler are investing heavily in advanced threat detection, zero-trust architectures, and AI-driven security platforms. These companies serve as strong examples of how continuous innovation and proactive investment can help organizations build greater cyber resilience.

[3] Within minutes, CrowdStrike OverWatch threat hunters detected the suspicious activity, alerted the customer, and neutralized the threat. CrowdStrike OverWatch (also known as Falcon Adversary OverWatch) is CrowdStrike's managed threat hunting service, designed to proactively detect and stop sophisticated cyber threats across endpoints, cloud environments, identities, and third-party data sources.
https://cs-staging-www.crowdstrike.co.uk/endpoint-security-products/falcon-overwatch-threat-hunting/
[4] A cyberattack technique where threat actors inject malicious code into online advertisements.
[5] The website itself is legitimate, and the URL in the browser looks correct. However, the scammers have manipulated the URL in a way that causes the website to display a fake phone number, one that the scammers control, instead of the company's real support number.
[6] https://www.malwarebytes.com/blog/news/2025/06/scammers-hijack-websites-of-bank-of-america-netflix-microsoft-and-more-to-insert-fake-phone-number

Disclaimer: