SECURITY INSIGHTS:

There is a tool kit for everything

Genady Vishnevetsky, Chief Info Security Officer, Stewart Title Guaranty Company

Today, there is a tool available for almost anything, including malicious activities carried out by hackers and cybercriminals. The era of manually crafted emails and poor language is over. Currently, many practical tools used by attackers are bundled into what is known as Phishing-as-a-Service. These kits automate the phishing process, removing the complexities and making it more accessible.

For example, a toolkit can effortlessly insert victims' email addresses into a phishing URL, making it appear more legitimate. This tactic can easily convince victims that they are accessing a trusted service or that they have visited it before. Site scrapers enable attackers to duplicate login pages for virtually any service in a matter of minutes. Once the hacker selects a location to host the fake page—whether on a compromised site or a hacker's own server—the toolkit can generate random URLs for every campaign. This approach significantly reduces the likelihood of detection by email security technologies and minimizes the chance of blacklisting. Most of these URLs are used only once or a few times.

Additionally, these toolkits can implement legitimate or fake CAPTCHA page redirects for extra or superficial security. Code obfuscation techniques are employed to evade impersonation checks by legitimate entities such as Microsoft or Google during Attacker-in-the-Middle attacks.

Just as any legitimate business watches for competitors, cybercriminals monitor for rivals encroaching on their turf. Traffic filtering is used to identify specific locations, bots, proxies, and VPNs commonly associated with abuse. And yes, this can all be done with just a few clicks.

We are witnessing the rise of Advessary-in-the-Middle phishing kits distributed through a Phishing-as-a-Service model. These kits primarily aim to harvest Microsoft 365 or Gmail session cookies to bypass the Multi-Factor Authentication (MFA) process during subsequent logins. Despite our investments in security technologies, you, as the user, remain the last line of defense.

TAKEAWAYS:

- **Don't log in from a link:** If you landed on a page from the link and it's asking you to enter credentials, close it and log in directly from the authentic website
- **Check the URL:** Always hover over the link to examine the URL. The longer the URL, the riskier it is
- **Sailing should be smooth:** Log in with 2FA, which is a multi-step process. Watch for any odd page flashes, page redirects, or page mismatches throughout the process. The entire login should be seamless and uninterrupted
- Educate yourself about the latest threats