An SVG file disguised as a PDF led victims to a fake login

Data: 2025-09-27 10:58:35

Autor: Inteligência Against Invaders

Redazione RHC**:27 September 2025 11:15**

Microsoft Threat Intelligence specialists have identified an attack in which attackers *used artificial intelligence for the first time to disguise phishing code.* The goal was to steal credentials from companies in the United States.

The **malicious SVG** file hid its true functionality behind a layer of *pseudo-corporate terminology and a simulated analytics dashboard* , allowing it to **bypass simple checks.** Analysis revealed that *the code's structure was uncharacteristic of handwriting and was likely generated by a generative model.*

The emails came from **a hacked corporate account** , with the sender's address matching the recipient's, and the actual addresses BCCed. The attachment **mimicked a PDF document, but was actually an SVG file with embedded JavaScript** . When opened, the file redirected the victim to a CAPTCHA page, which, according to Microsoft, then opened a fake login form to collect passwords.

The main feature of the attack was its unusual obfuscation.

Elements with names like *"Business Performance Dashboard"* were hidden within the SVG code, *remaining invisible due to the complete lack of transparency.* Furthermore, the malicious functionality was disguised using a series of business terms *("revenue," "operations," "dashboard," "KPI," etc.), converted into symbols and commands using a multi-step algorithm.* The script redirected the browser to a malicious resource, initiated environmental fingerprinting, and monitored sessions.

Microsoft's analysis system concluded that **the code was most likely generated by artificial intelligence.** Among the warning signs were *overly descriptive function names with hexadecimal suffixes, excessive modularity and repetitive logic blocks, cumbersome comments in the style of corporate documentation, and the formal use of XML constructs typical of generative models.*

Despite the complexity of the disguise, **the campaign was blocked by Microsoft Defender cloud protection.** Heuristics based on several indicators were activated: *suspicious use of BCC, automated emails, an SVG attachment disguised as a PDF,* a redirect to the previously detected kmnl[.]cpfcenters[.]de phishing domain, the presence of hidden logic, and session tracking detection.

Microsoft emphasized that the use of AI doesn't eliminate the ability to detect attacks. On the contrary, synthetic code often leaves behind additional artifacts that can be used for analysis. The company recommends that administrators *enable on-click safe link checking, activate Zero-Hour Auto Purge to isolate messages that have already been delivered, use browsers with SmartScreen support, and implement phishing-resistant multi-factor authentication via Microsoft Sign In.*

Redazione
The editorial team of Red Hot Cyber consists of a group of individuals and anonymous sources who actively collaborate to provide early information and news on cybersecurity and computing in general.

Lista degli articoli