SECURITY INSIGHTS:

Understanding SVG Smuggling

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

A new and one of the latest tricks used by cybercriminals is called **SVG smuggling**. SVG stands for **Scalable Vector Graphics**, which are image files used for icons, logos, and illustrations on websites. Unlike regular image files, SVGs are built using XML, a type of code that can include scripts (small programs). This makes SVGs very flexible and useful, but it also opens the door for cybercriminals to hide malicious code inside them.

Imagine receiving an email with an innocent-looking image file attached. When you open it, hidden code inside the SVG file runs quietly in your browser, redirecting you to a fake website that looks like a real login page. If you enter your username and password, the attackers will be able to steal your credentials.

WHAT MAKES SVG SMUGGLING SO DANGEROUS?

- **Hard to Detect:** SVG files are often treated as harmless images by email filters and security software, making it easier for them to slip through unnoticed.
- **No Installation Needed:** Unlike traditional malware, SVG smuggling doesn't require you to download or install anything. Just opening the file is enough to trigger the malicious code.
- **Widespread Use:** SVGs are used everywhere on the web, from icons to illustrations, making them a common and trusted file type.

TAKEAWAYS

Here are a few simple steps you can take to stay safe from SVG smuggling:

- **Be Cautious with Email Attachments:** Avoid opening image files from unknown or unexpected sources. If you receive an email with an attachment that looks suspicious, delete it or contact the sender to verify its authenticity.
- **Nothing Actionable:** While SVG files have some extended capabilities, they are still image files. If opening it initiates any action (e.g., opening a website and prompting to log in), steer clear.