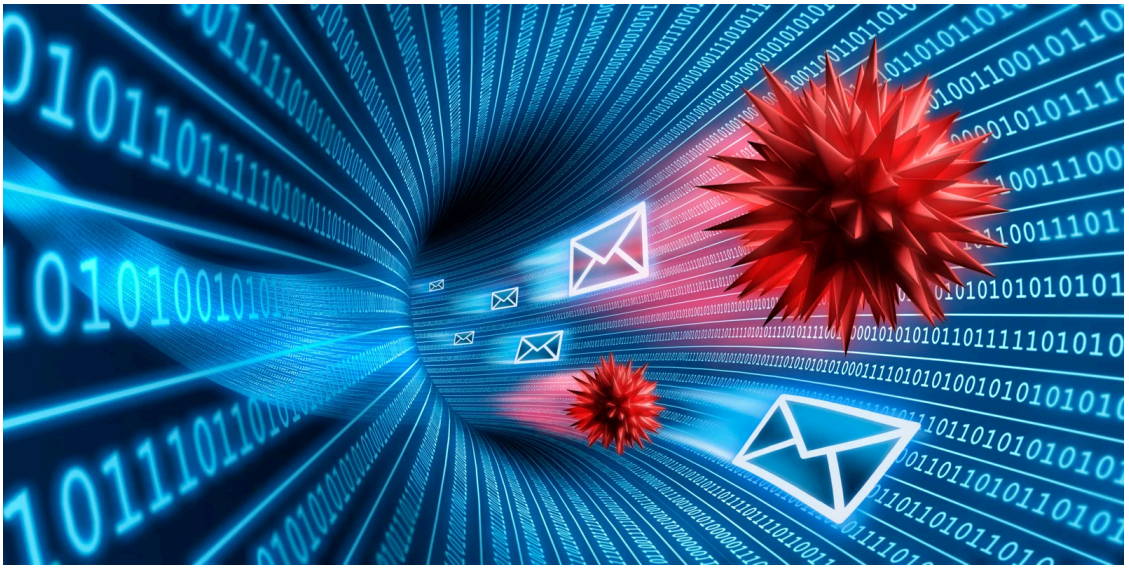
Phishing emails increasingly use SVG attachments to evade detection

By Lawrence Abrams

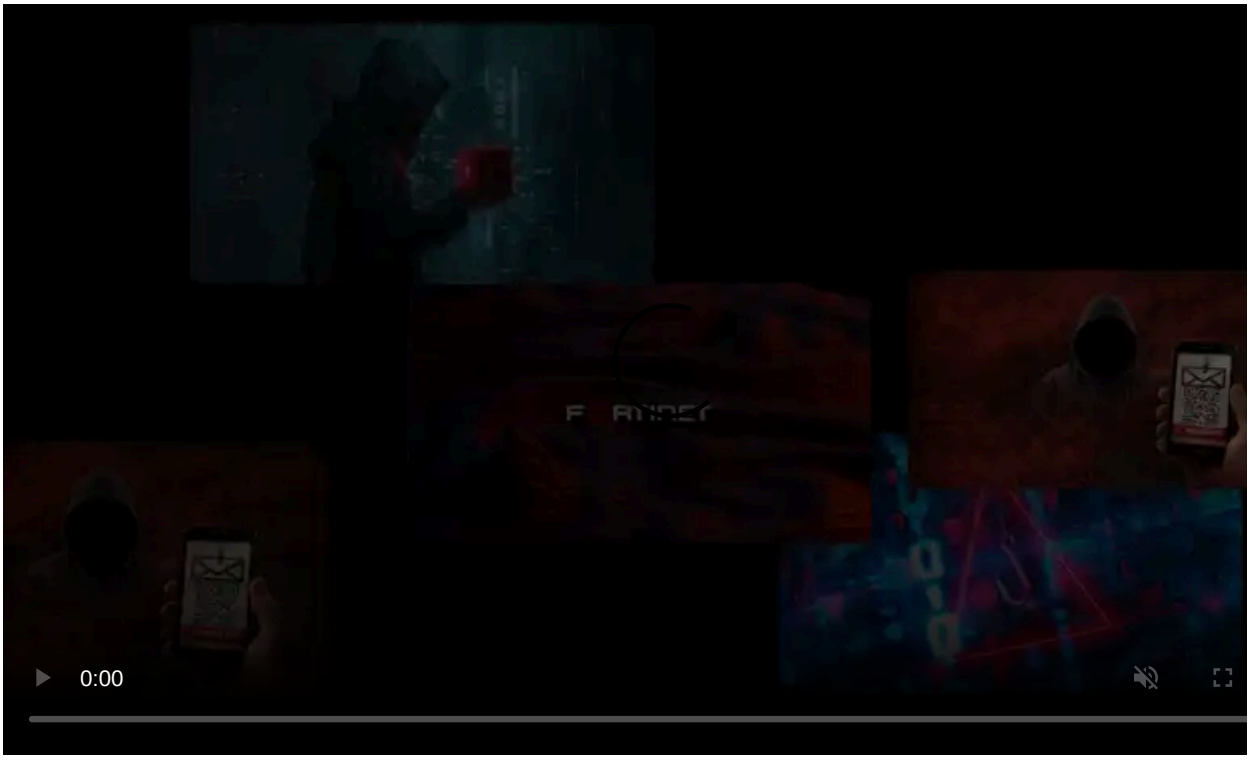
Published: 2024-11-17 · Archived: 2026-04-05 21:39:41 UTC

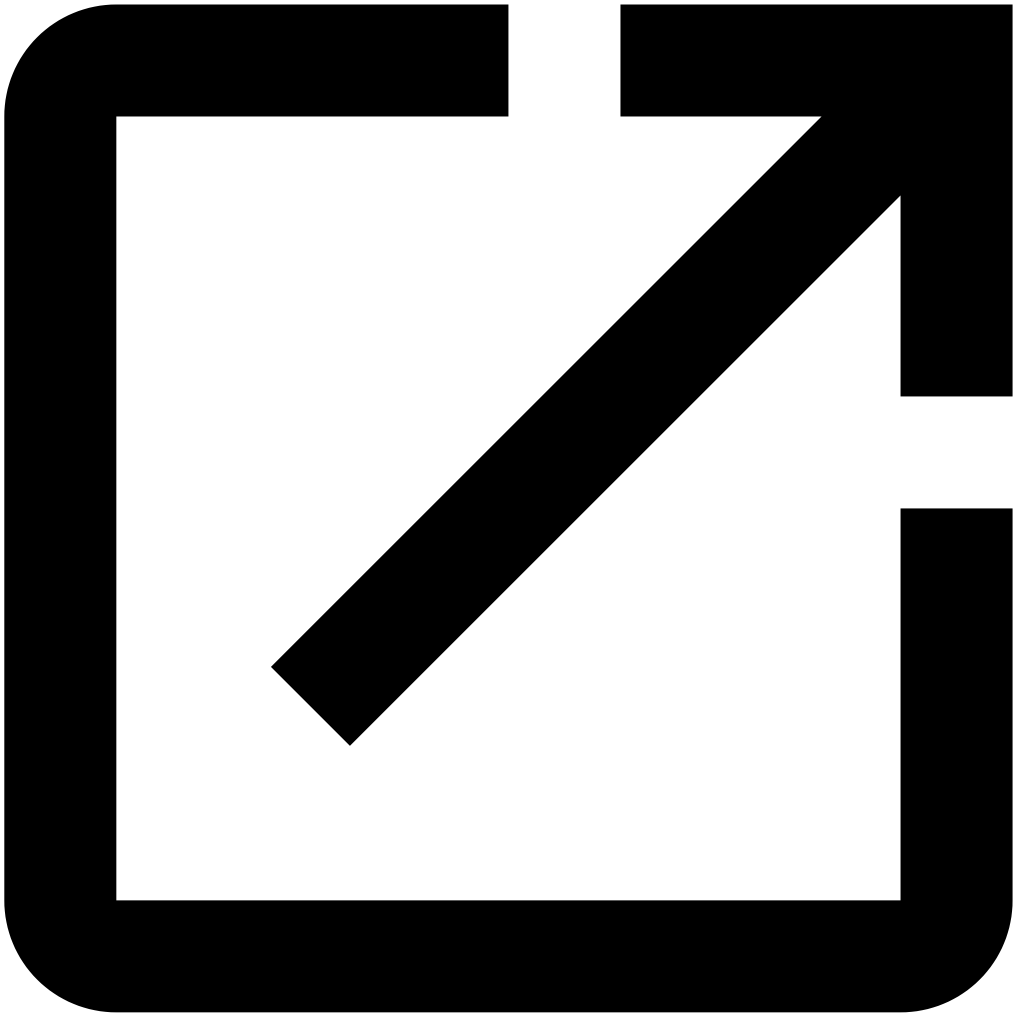


Threat actors increasingly use Scalable Vector Graphics (SVG) attachments to display phishing forms or deploy malware while evading detection.

Most images on the web are JPG or PNG files, which are made of grids of tiny squares called pixels. Each pixel has a specific color value, and together, these pixels form the entire image.

SVG, or Scalable Vector Graphics, displays images differently, as instead of using pixels, the images are created through lines, shapes, and text described in textual mathematical formulas in the code.


0:00



For example, the following text will create a rectangle, a circle, a link, and some text:

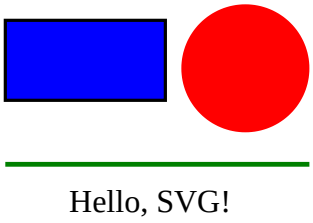
```
<svg width="200" height="200" xmlns="http://www.w3.org/2000/svg">
   <!-- A rectangle -->
   <rect x="10" y="10" width="100" height="50" fill="blue" stroke="black" stroke-width="2" />

   <!-- A circle -->
   <circle cx="160" cy="40" r="40" fill="red" />

   <!-- A line -->
   <line x1="10" y1="100" x2="200" y2="100" stroke="green" stroke-width="3" />

   <!-- A text -->
   <text x="50" y="130" font-size="20" fill="black">Hello, SVG!</text>
</svg>
```

When opened in a browser, the file will generate the graphics described by the text above.



Generated SVG image

Source: BleepingComputer

As these are vector images, they automatically resize without losing any loss to image quality or the shape, making them ideal for use in browser applications that may have different resolutions.

Using SVG attachments to evade detection

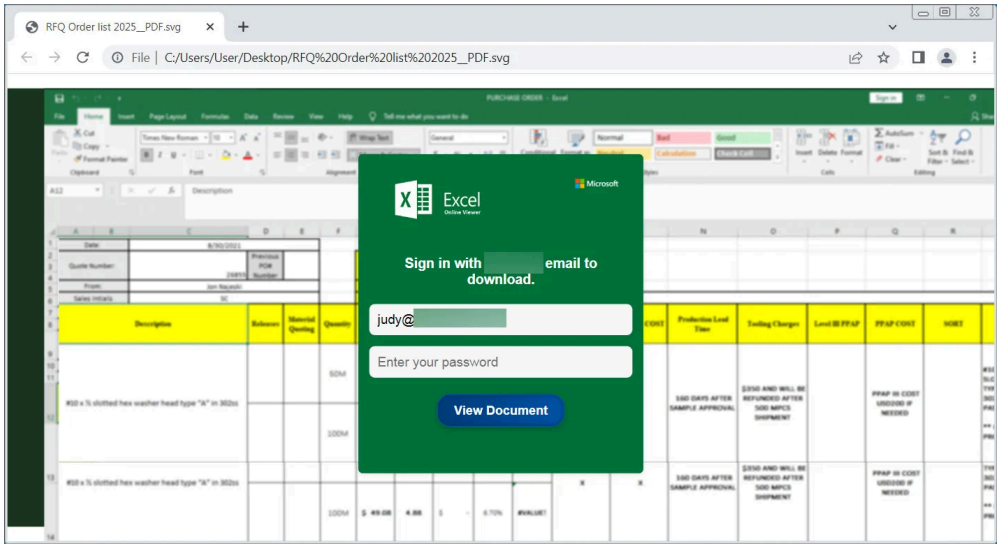
The use of SVG attachments in phishing campaigns is nothing new, with BleepingComputer reporting about their usage in previous Qbot malware campaigns and as a way to hide malicious scripts.

However, threat actors are increasingly using SVG files in their phishing campaigns according to security researcher MalwareHunterTeam, who shared recent samples [1, 2] with BleepingComputer.

These samples, and others seen by BleepingComputer, illustrate how versatile SVG attachments can be as they not only allow you to display graphics but can also be used to display HTML, using the <foreignObject> element, and execute JavaScript when the graphic is loaded.

This allows threat actors to create SVG attachments that not only display images but also create phishing forms to steal credentials.

As shown below, a recent SVG attachment [VirusTotal] displays a fake Excel spreadsheet with a built-in login form, that when submitted, sends the data to the threat actors.



SVG attachment showing a phishing form

Source: BleepingComputer

Other SVG attachments used in a recent campaign [VirusTotal] pretend to be official documents or requests for more information, prompting you to click the download button, which then downloads malware from a remote site.

SVG attachment used to distribute malware

Source: BleepingComputer

Other campaigns utilize SVG attachments and embedded JavaScript to automatically redirect browsers to sites hosting phishing forms when the image is opened.

The problem is that since these files are mostly just textual representations of images, they tend not to be detected by security software that often. From samples seen by BleepingComputer and uploaded to VirusTotal, at the most, they have one or two detections by security software.

With that said, receiving an SVG attachment is not common for legitimate emails, and should immediately be treated with suspicion.

Unless you are a developer and expect to receive these types of attachments, it is safer to delete any emails containing them.

Source: https://www.bleepingcomputer.com/news/security/phishing-emails-increasingly-use-svg-attachments-to-evade-detection/