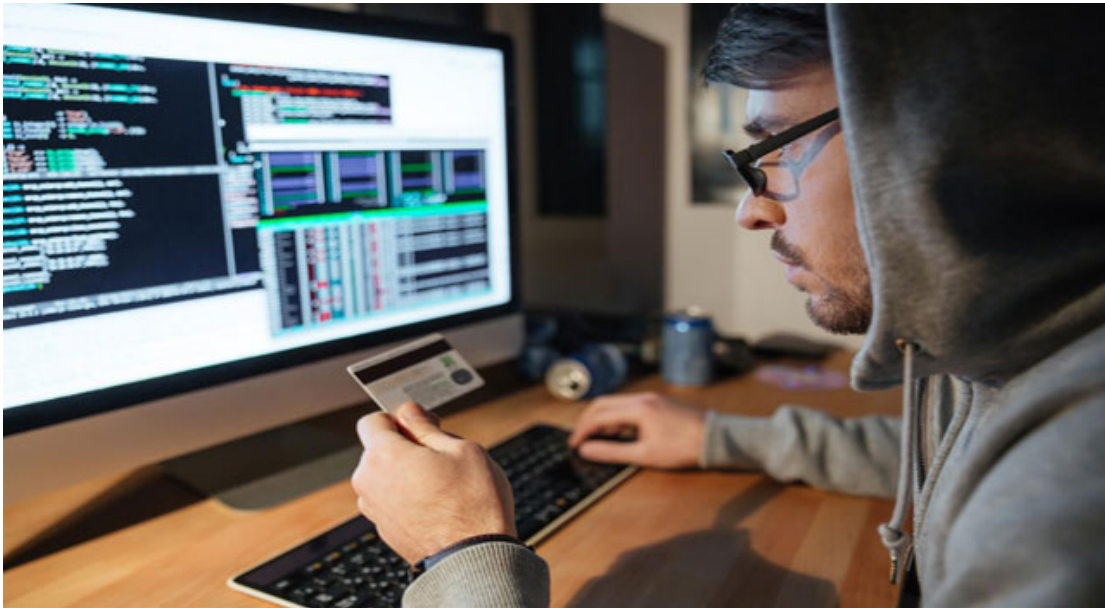


# New Magecart Attack Target US Local Government Services

blog.trendmicro.com/trendlabs-security-intelligence/us-local-government-services-targeted-by-new-magecart-credit-card-skimming-attack/

June 26, 2020



## Cyber Threats

Eight cities across three states in the United States have fallen victim to a Magecart card skimming attack. Websites were compromised to host credit card skimmers which passed on the credit card information of residents to cybercriminals.

By: Joseph C Chen June 26, 2020 Read time: ( words)

Eight cities across three states in the United States have fallen victim to a Magecart card skimming attack. In these attacks, their websites were compromised to host credit card skimmers which passed on the credit card information of residents to cybercriminals.

These sites all appear to have been built using Click2Gov, a web-based platform meant for use by local governments. It is used to provide services such as community engagement, issues reporting, and online payment for local governments. Residents can use the platform to pay for city services, such as utilities. Breaches in these sites, however, are not new: In 2018 and 2019, the websites of several towns and cities using Click2Gov were compromised.



Figure 1. Credit card skimming attack chain

Our research identified eight cities whose websites had been compromised with a JavaScript-based skimmer, as expected from a Magecart attack. The information exfiltrated included:

- Credit card information (card number, expiration date, CVV)
- Personal information (Name and contact address)

Our analysis of both the skimmer and the infrastructure used could not find any connections between this breach and the incidents in 2018 and 2019. Nevertheless, five of the eight cities were also affected in the previous breaches; we believe that these attacks started on April 10 of this year, and are still active.

### Analysis of the card skimming attack

The attack occurs when victims make an online payment on the compromised Click2Gov website. JavaScript code was injected into the payment page which loads a credit card skimmer when victims browse the payment page.


Unlike other skimmers which grab data on various types of payment forms, the skimmer used here is rather simple and only works on a Click2Gov payment form. No obfuscation or anti-debugging techniques were used. The skimmer hooks the `submit` event of the payment form; when a victim clicks the button to send the payment information, the skimmer will grab the information from the selected columns inside the payment form and immediately send the collected information to remote server via a HTTP POST request.


 Figure 2. Screenshot of credit card skimmer injected on Click2Gov payment page

Exfiltrated Data Type	Targeted Column ID	Exfiltration Request Schema
Credit card number	accountNumber	accountNumber
Credit card CVV number	cvv2	cvv
Credit card expiration year	expirationDate.year	year
Credit card expiration month	expirationDate.month	month
Credit card expiration date	expirationDate.date	date
First name of cardholder	firstName	firstName
Middle name of cardholder	middleInitial	middleInitial
Last name of cardholder	lastName	lastName
Contact address 1	contact.address1	address1
Contact address 2	contact.address2	address2
City of contact address	contact.city	city
State of contact address	contact.state	State
Zip code of contact address	contact.zip	ZipCode

Table 1. Details of exfiltrated information

We were able to identify two of the exfiltration servers used in the attack. Both hosted the actual JavaScript skimmer, as well as a .JSP file used to receive the exfiltrated data. One of the servers was used for three sites, while the other server used for the remaining five sites. The two skimmers used are identical, save for the change in the hostname of the exfiltration servers.

 Figure 3. Screenshot of the credit card skimmer script

 Figure 4. Example of exfiltration request

## Background and attribution

Click2Gov has been hit by various breaches and attacks in the past. CentralSquare Technologies, its developer, released a [2018 statement](#) concerning security issues on various locally hosted sites. Other researchers [uncovered](#) a breach of around 300,000 records from Click2Gov sites

Click2Gov at the end of that year. Another 2018 [report](#) showed a similar case where a site built using Click2Gov was targeted by an attacker to exfiltrate credit card information from its users. In 2019, another breach was discovered, where it became [apparent](#) that data from eight cities was being sold in the underground market.

It is not clear at this time if this attack which we identified is connected to the earlier breaches, since nothing about their technical details indicate a connection. The only connection is that five of the affected cities in the current incident were also affected in 2018; while two were included in the 2019 incident.

## Conclusion

Credit card skimming attacks are still a major threat to online merchants. Victims not limited to only typical e-commerce sites. During 2019, we also saw that [academic institutions](#) and [hotel chains](#) were targeted by similar attacks. This time, the attacker targeted the websites of various local governments. This shows the importance of keeping payment portals secure to protect both an organization and its customers.

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)

SHA256 Hash/URL	Type
99840885c7f248779838b08559a9f3feb16e646fad7a3d36015e4b4ca4b4173b	Credit Card Skimmer (detected as TrojanSpy.JS.MAGECART.G)
a7db455dc25d107caf8f74f7d4c492541c5d37c38bf68604a6e85b06b61af26a	Credit Card Skimmer (detected as TrojanSpy.JS.MAGECART.G)
<a href="https://cdns-static[.]com/recurring.js">https://cdns-static[.]com/recurring.js</a>	Credit Card Skimmer URL
<a href="https://renew-analytics[.]com/recurring.js">https://renew-analytics[.]com/recurring.js</a>	Credit Card Skimmer URL
<a href="https://cdns-static[.]com/validate/index.jsp">https://cdns-static[.]com/validate/index.jsp</a>	Exfiltration URL
<a href="https://renew-analytics[.]com/validate/index.jsp">https://renew-analytics[.]com/validate/index.jsp</a>	Exfiltration URL
cdns-static[.]com	Credit Card Skimmer Domain
renew-analytics[.]com	Credit Card Skimmer Domain

Content added to Folio