Mirrorthief Hits Campus Online Stores Using Magecart

blog.trendmicro.com/trendlabs-security-intelligence/mirrorthief-group-uses-magecart-skimming-attack-to-hit-hundreds-of-campus-online-stores-in-us-and-canada/

May 3, 2019

We uncovered a recent activity involving the notorious online credit card skimming attack known as Magecart. The attack, facilitated by a new cybercrime group, impacted 201 online campus stores in the United States and Canada.

We started detecting the attacks against multiple campus store websites on April 14, during which the sites were injected with a malicious skimming script (detected by Trend Micro as Trojan.JS.MIRRORTHEIF.AA) at their payment checkout pages. The skimming script can scrape credit card information, as well as personal details entered on the payment page. The stolen information is consequently sent to a remote server. After looking into this attack, we learned that the attackers compromised PrismWeb, which is an e-commerce platform designed for college stores by company PrismRBS, a subsidiary of Nebraska Book Company.

The attacker injected their skimming script into the shared JavaScript libraries used by online stores on the PrismWeb platform. We confirmed that their scripts were loaded by 201 campus book and merchandise online stores, which serves 176 colleges and universities in the U.S. and 21 in Canada. The amount of payment information that was stolen is still unknown.

We disclosed our findings to PrismRBS. The company has since released an official statement regarding the skimming attack: "On April 26, 2019, PrismRBS became aware that an unauthorized third-party obtained access to some of our customers' e-commerce websites that PrismRBS hosts. Upon learning of this incident, we immediately took action to halt the current attack, initiated an investigation, engaged an external IT forensic firm to assist in our review, notified law enforcement and payment card companies. Our investigation is ongoing to determine the scope of the issue, including who and what information may have been impacted. Based on our review to date, we have determined that an unauthorized party was able to install malicious software designed to capture payment card information on some of our customers' e-commerce websites.

We are proactively notifying potentially impacted customers to let them know about the incident, the steps we are taking to address the situation, and steps they can take to protect their end users. We deeply regret any concern or frustration this incident may cause. Protecting the security and privacy of information remains a top priority. We are taking steps to further strengthen the security of our systems, including enhanced client-side and back-end monitoring tools and a comprehensive end-to-end audit of our systems. Once our investigation concludes, we will be providing our customers with additional information and guidance."

Since we can’t connect the said attack to any previous Magecart groups — even if the attack shared some similar characteristics with a few of them — we labeled this new group “Mirrorthief”.

Figure 1. Mirrorthief attack chain

Figure 1. Mirrorthief attack chain

Figure 2. Payment page of PrismWeb online store loads Mirrorthief’s skimming script

Figure 3. Mirrorthief injection on PrismWeb checkout payment’s library

How Mirrorthief performs their skimming activities

On April 14, the attackers injected a script to the payment checkout libraries used by the PrismWeb platform. The location of injected payment checkout libraries on affected online stores were:

- hxxps://[online store domain]/innerweb/v4.0/include/js/checkout_payment[.]js
- hxxps://[online store domain]/innerweb/v3.1/include/js/checkout_payment[.]js

The injected script forged the Google Analytics script format, but loaded a different script from the attackers’ server. The loaded script is the main script that steals the payment information. Unlike many web skimmers, which are designed to collect information from many kinds of e-commerce payment pages in general, the skimmer that the Mirrorthief group used was designed specifically for PrismWeb’s payment page. The skimmer collects data only from HTML elements with the specific IDs on PrismWeb’s payment form. The stolen credit card information includes card number, expiry date, card type, card verification number (CVN), and the cardholder’s name. The skimmer also steals personal information like addresses and phone numbers for billing.

Once the user has finished filling in the payment form and clicked on the payment review, the skimmer copies the targeted information into JavaScript Object Notation (JSON) format data and encrypts it with AES encryption and Base64 encoding. Next, the skimmer will send it to a remote server by creating an HTML image element, which connects to their URL appended with the encrypted payment information as a query string. The server then receives the skimmed data from the URL’s query string and returns a 1 pixel PNG picture.

HTML Element ID	Mirrorthief JSON Data Schema	Information
_cc_number	aa	Credit card number
_cc_expmonth	bb	Credit card expiration month
_cc_expyear	cc	Credit card expiration year
cc_type	dd	Credit card type

_cc_cvn	ee	Credit card CVN number
cc_first_name	ff	First name of cardholder
cc_last_name	gg	Last name of cardholder
bill_to_phone	hh	Phone number for billing
bill_to_country	ii	Billing address (country)
bill_to_state	jj	Billing address (state)
bill_to_street1	kk	Billing address (street)
bill_to_street2	ll	Billing address (street)
bill_to_city	mm	Billing address (city)
bill_to_zip	nn	Billing address (zip code)

Table 1. Sensitive data targeted by Mirrorthief's skimmer

Figure 4. Mirrorthief skimming script copies payment information and encrypts it with AES encryption (deobfuscated)

Figure 4. Mirrorthief skimming script copies payment information and encrypts it with AES encryption (deobfuscated)

Comparing Magecart-wielding groups

The Mirrorthief group made the injected script on the compromised libraries similar to legitimate Google Analytics script and registered their malicious domain (which also appears similar to the original Google Analytics domain) to disguise their activity. Impersonating the Google Analytics service is a known tactic also used by Magecart Group 11, the group behind the Vision Direct breach. Another group called ReactGet, which infected many e-commerce websites around the world, was also recently seen adopting a similar impersonation tactic.

When we checked Mirrorthief's network infrastructure, we found that it did not have any overlap with any known cybercrime groups. In addition, the skimmer Mirrorthief used in the attack is very different from the others since it's specially designed to skim PrismWeb's payment form. It sends the skimmed data through a unique JSON schema, which may hint that they use a unique backend data receiver instead of popular skimming kits. Moreover, the three groups encrypted the skimmed data before the transfer, but used different JavaScript libraries. Below is a table for comparison.

Group	Encryption Algorithm	JavaScript Library
Magecart Group 11	AES	Gibberish-AES
ReactGet	RSA	JSEncrypt
Mirrorthief	AES	Crypto-JS

Table 2. Comparison of encryption algorithms used by the different groups

Figure 5. Magecart Group 11 injection pattern

Figure 5. Magecart Group 11 injection pattern

Figure 6. ReactGet Group injection pattern

Figure 6. ReactGet Group injection pattern

Figure 7. Mirrorthief Group injection pattern

Figure 7. Mirrorthief Group injection pattern

Magecart has evolved its tactics and exposed many sites to skimming attacks over the years. Groups that employ this digital attack have been known to come up with new ways to stay undetected on the sites they compromise. 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

Indicators of Compromise (IoCs)

Indicator	Attribution
30c8be0d9deb59d98f7e047579763559f2c2dd9a7b4477636afcbebaaebc7dc5	Mirrorthief skimming script hash (detected as Trojan.JS.MIRRORTHEIF.AA)
cloudmetric-analytics[.]com	Mirrorthief malicious domain
hxxps://cloudmetric-analytics[.]com/ga[.]js	Mirrorthief malicious URL
hxxps://cloudmetric-analytics[.]com/analytics[.]js	Mirrorthief malicious URL
hxxps://cloudmetric-analytics[.]com/analytic[.]php?ccm_post=	Mirrorthief malicious URL
hxxps://g-analytics[.]com/libs/analytics[.]js	Magecart Group 11 malicious URL
hxxps://ebitbr[.]com/api[.]js	ReactGet Group malicious URL

With special thanks to our colleagues at abuse.ch and The Shadowserver Foundation for helping with the sinkholing of Mirrothief's malicious domain and remediation reporting

Malware

We uncovered a recent activity involving the notorious online credit card skimming attack known as Magecart. The attack, facilitated by a new cybercrime group, impacted 201 online campus stores in the United States and Canada.

By: Joseph C Chen May 03, 2019 Read time: (words)

Content added to Folio