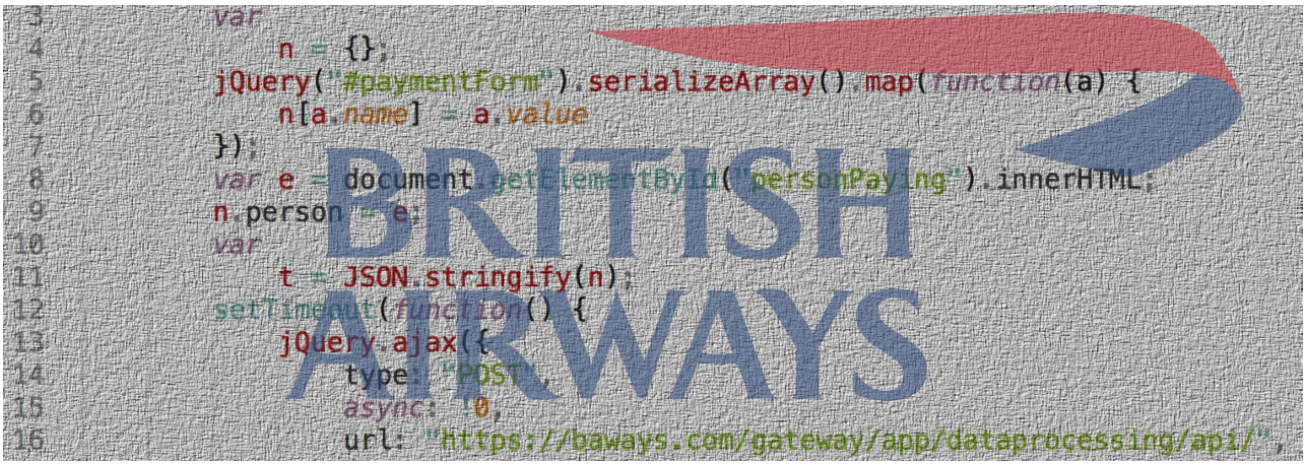
British Airways Fell Victim To Card Scraping Attack

bleepingcomputer.com/news/security/british-airways-fell-victim-to-card-scraping-attack/

Ionut Ilascu

By
Ionut Ilascu

- September 11, 2018
- 04:54 AM
- 0



The recent British Airways data breach affecting 380,000 individuals appears to be the work of a known adversary that infects websites with a script designed to collect payment card data.

The name of the group is MageCart, and the scripts it uses have the same effect as the physical card skimming devices used by cybercriiminals at ATMs. In a typical attack, the group casts a wide net by compromising commonly used third-party functionality that allows access to hundreds of websites.

British Airways was targeted

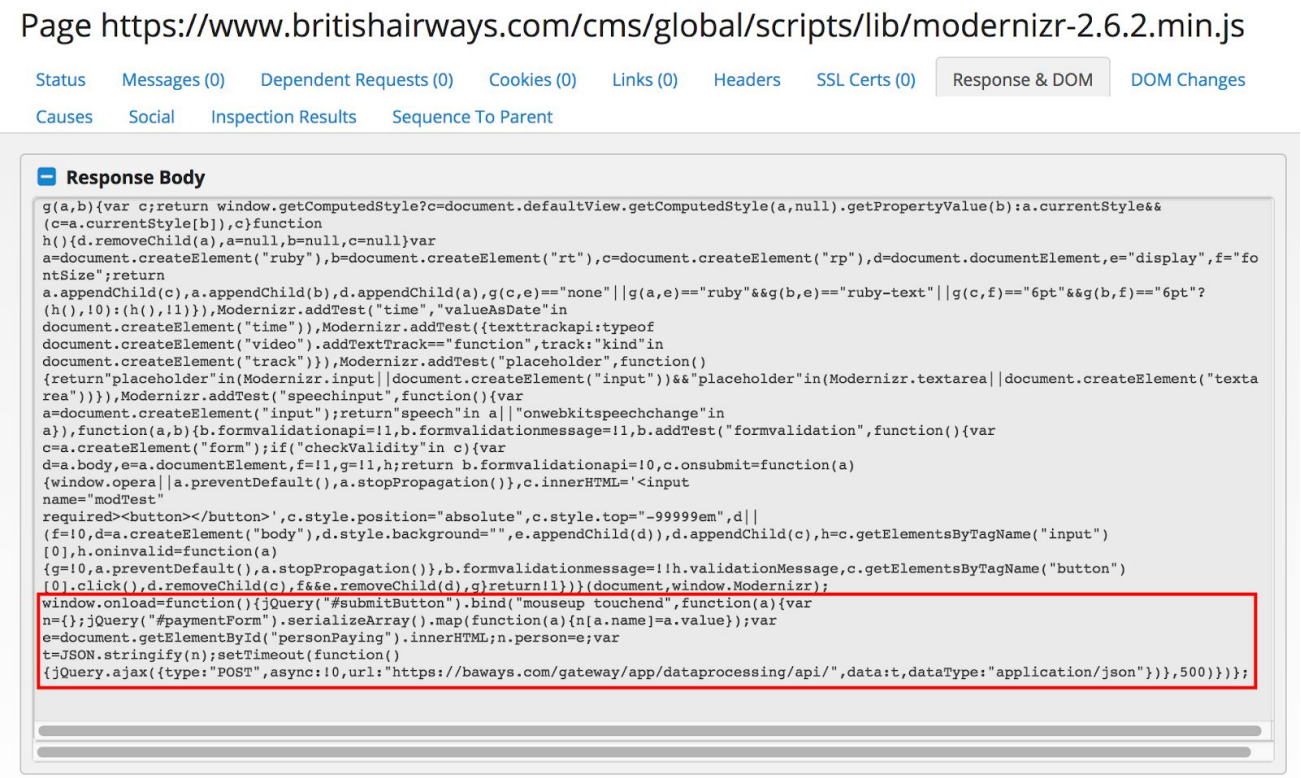
Digital threat management company RiskIQ tracks the activity of MageCart group and reported their use of web-based card skimmers since 2016. They are familiar with the threat actor and their skimmer-code and detect it almost on an hourly basis.

With British Airways, though, MageCart took a targeted approach and customized the script so that did not ring any alarm bells.

"This particular skimmer is very much attuned to how British Airway's payment page is set up, which tells us that the attackers carefully considered how to target this site instead of blindly injecting the regular
Magecart skimmer," RiskIQ says in a report shared with BleepingComputer in advance.

For this investigation, the researchers identified all the scripts loaded by the air carrier's website and searched for recent changes.

The researchers noticed that the Modernizr JavaScript library had been modified with 22 new lines of code at the bottom, a tactic often used by attackers to make sure they don't break the functionality of the script.



British Airways website loaded the library from the baggage claim information page, and the change made by MageCart threat actor allowed Modernizr to send payment information from the customer to the attacker's server.

The compromised code reacted the same whether the website launched on a computer screen or from the mobile app, since in both cases the resources for for searching, booking or managing flights were the same.

The change in the JavaScript library was confirmed by the headers sent by the British Airways server, which indicated August 21, 20:49 GMT as the time and date of the last modification in Modernizr.

In the statement on the data breach, the airline said the theft occurred between August 21, 22:58 BST, one hour after MageCart made the change in Modernizr.

Attackers use SSL certificate from Comodo

More evidence that MageCart prepared for this attack and aimed to keep it active for as long a period as possible is found in the infrastructure used for exfiltrating the payment card details.

The compromised Modernizr script delivered all the data to baways[.]com, which resembles the legitimate domain used by British Airways, and would likely not raise suspicions during a cursory look at the modified library.

RiskIQ also discovered that MageCart purchased an SSL certificate from Comodo, instead of going with the free choice from Let's Encrypt. The reason for this is that a paid certificate is less likely to attract attention.

Issued	2018-08-15
Expires	2020-08-15
Serial Number	129950451738167431558149351195969236479
SSL Version	3
Common Name	baways.com (subject) COMODO RSA Domain Validation Secure Server CA (issuer)
Alternative Names	baways.com (subject) www.baways.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)

With this attack, MageCart threat actor has stepped up the ladder and showed they are capable of refining its operations, blending in with the targeted website to maintain their presence.

It is unclear how MageCart managed to compromise the British Airways website, but RiskIQ says that being able "to modify a resource for the site tells us the access was substantial."

Update: Following BleepingComputer's report, Comodo released a statement saying that it revoked the SSL certificate issued to baways[.]com, the domain used for exfiltrating payment data.

"Comodo CA had issued the DV certificate in mid-August, 2018, after following all industry standards and Baseline Requirements from the CA/Browser Forum," reads the statement.

"While Certificate Authorities (CAs) can and must authenticate certificate requesters according to their validation level (EV, OV, or DV), they are not able to discern the intention of the certificate requester in advance of real-world use," the statement continues.

Related Articles:

Microsoft: Credit card stealers are getting much stealthier

Caramel credit card stealing service is growing in popularity

- Carding
- E-Commerce
- MageCart
- Skimmer

Ionut Ilascu

Ionut Ilascu is a technology writer with a focus on all things cybersecurity. The topics he writes about include malware, vulnerabilities, exploits and security defenses, as well as research and innovation in information security. His work has been published by Bitdefender, Netgear, The Security Ledger and Softpedia.

- Previous Article
- Next Article

You may also like: