Kroll | A Division of DUFF & PHELPS

The MONITOR

VOLUME 2

Understanding and Fighting Against Banking Trojans

The Monitor, Issue 4

Kroll has seen a rise in banking trojan incidents over the last few months, with a growing number in April 2019, including cases that involved Emotet, Trickbot and Qakbot. Much of the insight and guidance in this month's newsletter comes from a recent article on banking trojans by Managing Director Devon Ackerman. Banking trojans primarily aim to steal the banking credentials of an organization or individual, usually moving silently in the background leveraging several propagation methods, waiting until victims go to access their personal or corporate financial accounts. At that point, credentials are captured through a variety of means and ultimately funds are drained, paychecks are diverted, fraudulent transactions occur, etc.

According to Devon, banking trojans are most commonly introduced into networks by users at all levels of the organization. Many of the strategies used by fraudsters are not new and include:

- Social engineering attacks, including phishing (email), vishing (voicemail) and smishing (mobile messaging), where victims most often click on infected links
- Email attachments that contain macro viruses (i.e., maldocs)
- Compromised internet ad campaigns
- "Drive-by" attacks: users visit a website infected by malware that in turn infects users' computers
- Visiting contractors or clients with infected laptops

Devon says that two characteristics make banking trojans like Emotet particularly insidious. First, they are polymorphic in nature, such that actors can rotate code and signatures virtually every day, enabling them to evade standard antivirus detection. Second, beyond aiming to capture banking credentials, this malware is able to scrape or steal the contents of locally stored emails on infected endpoints. "Imagine how much more believable a new phishing campaign is when an attacker has a technically valid email and an entire conversation thread to build on," explains Devon. "Messages that leverage conversation threads from spoofed senders not only have an easier time getting through email filters, they are typically recent enough that recipients will likely have lowered their "mental" defenses from annual cyber awareness training. The 'clickability' of these well-disguised emails jumps astronomically, and so the attacker gains a continuous stream of new victims."

Statistically, Kroll usually sees less than a 24-hour turnaround between fraudulent domain registrations for spoofing campaigns and actors leveraging those domains for email fraud.

Additionally, Devon warns that in recent months, the newest strains of banking trojans don't stop at bank-related fraud. "Some join with other malware as secondary and tertiary payload drops into infected networks, which aim to saturate victims with unauthorized remote access looking for additional information to steal. Some infected victims become part of a larger botnet. Kroll has also observed actor groups moving to deploy ransomware post network saturation as a means to cover their tracks and to further monetize their intrusion through ransomware payments," says Devon.

Emotet banking on Eternal Blue

Emotet is known for its ability to maintain persistence and spread across networks thanks to its use of the now infamous Eternal Blue exploit. Eternal Blue is an exploit that capitalizes on a vulnerability within the SMB (Server Message Block) protocol. If Emotet finds an unpatched instance of this vulnerability, it can enable the installation of malware without human interaction. Microsoft issued an emergency patch for the Eternal Blue vulnerability in March 2018, but many systems cannot or do not install updates. Consequently, threat actors have continued to capitalize on SMB vulnerabilities for ransomware and trojan attacks.

Technically Speaking

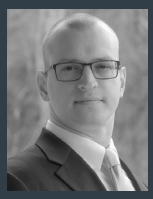
While each banking trojan is unique in the mechanisms it employs to inflict harm and further spread malware, the following is a simplified overview of the way Kroll typically handles common banking trojans such as Emotet or Trickbot and provides a glimpse into the steps of an effective response:

- Deploy Kroll's endpoint detection and response ("EDR") solution to combine forensic and incident response tools, threat intelligence feeds, human analysts and client feedback about their own networks to identify and ban identified malware hashes (i.e., unique fingerprints of malicious processes or binaries). This allows for containment and banning of running processes and prevents subsequent execution. When deployed at an enterprise level, this gives us the ability to block the execution of malware network-wide, sometimes within minutes of sensor deployment and initial data analysis
- When necessary, Kroll is able to isolate infected systems to prevent data acquisition or exfiltration from client networks due to unauthorized access and network intrusions.
- Identify and block actor command and control ("C2") IPs at the network perimeter.
- Pull selected events to generate a timeline of infections and determine user accounts being utilized by malware for installation and/or spreading.
- Reset domain and local user account credentials for all accounts known to have been used by the malware to spread (or at the appropriate time, perform an enterprise-wide password reset); also ensure all local administrator user account passwords are unique.
- Ultimately, create and deploy a custom remediation script to purge remaining malware artifacts.

Case Study

Kroll recently worked an investigation where a comptroller for a large engineering firm received an email request from a known, legitimate business associate. Despite recognizing that the request was somewhat out of character, the comptroller—who routinely works with financial information and invoice for payment—opened the attachment expecting an invoice. The document was in fact a maliciously crafted document disguised as an older legitimate invoice, which triggered a chain of events on the endpoint that were invisible to the user. The user, upon interview, stated that they discounted the invoice as having been sent in error since it was dated months earlier and was known to have been paid.

The employee's manager soon received a call from one of the company's major clients saying they had received a strange email from this employee and it could be malicious. Upon being engaged by the client's counsel, a Kroll forensics specialist immediately began analyzing the supervisor's email account remotely. Kroll confirmed the account had suffered unauthorized access but with no signs of the password to the account having been brute forced. Kroll then worked backwards and identified the suspicious email and malicious document and turned their investigation to the user's computer.



Devon Ackerman
Managing Director

Kroll Experts Corner:
Mitigating Banking Trojan Risks

Following are insights on how to better defend against banking trojan malware.

Managing Director Devon Ackerman says because of the persistent, polymorphic nature of banking trojans, organizations should be prepared with a diversified defense that blends "back to the basics" security with advanced threat monitoring and response capabilities.

Employee education and awareness still key for defense. Devon recommends conducting more frequent training with staff at all levels, including executive leadership and boards of directors.

- Issuing regular bulletins that share examples of deceptive emails can prove enlightening to employees.
- To gauge the effectiveness of their training programs, many enterprises are proactively making social engineering exercises part of their technical penetration testing programs.
- Annual training should be conducted along with tabletop exercises that involve IT security teams, corporate staff, internal and external legal counsel and a third-party incident response firm like Kroll.

Be prepared with threat intelligence, endpoint monitoring and expert response. Traditional anti-virus solutions have historically proved ineffective against polymorphic, bit-shifting and process-hollowing techniques characteristic of today's banking trojans.

- A sophisticated endpoint detection and response solution will continuously search for known bad and unusual behaviors and alert the organization to potential intrusions.
- Kroll's CyberDetectER® Endpoint leverages multiple threat intelligence sources and IOCs, including Kroll's learnings from real-world intrusions.

Get the Latest Trends and Insights from Kroll In Your Inbox

Sign up for *The Monitor* newsletter and every month you'll gain access to exclusive cyber threat trends derived from Kroll's global case intake, along with tailored recommendations and examples from our threat intelligence experts.

→ Free subscription at kroll.com/themonitor

Point-of-Sale (POS) Compromise and MID Refund Frauds

The Monitor, Issue 5

Kroll has identified a growing number of point-of-sale (POS) compromise incidents over the last few months, most commonly affecting the retail and service sectors. Cases included POS Shell and POSlurp malware variants as well as fraudulent Merchant Identification Number (MID) refund incidents.

According to Managing Director J. Andrew Valentine, many POS incidents today can be traced to networks being compromised by phishing emails. “About eight to 10 years ago, retail-focused cybercriminals saw the success other threat groups were having with social engineering tactics as an entry vector. They started to move from primarily technical attacks to phishing employees such as store managers and customer care personnel to gain access to networks,” explains Andy.

Andrew notes a recent case that underscores how cybercriminals have gotten very deliberate in their decision-making: “In this situation, a store manager received an email for an extremely lucrative catering order with details in an attachment. The Word document contained remote access malware that was designed to allow unauthorized access and facilitated the threat actor moving laterally to all the stores in the restauranteur’s environment. The attackers then deployed RAM scrapers set to deploy on Fridays when system memory was loaded with a full week’s worth of transactional data ripe for a maximum return of payment account numbers.”

MID refund fraud making a comeback

Kroll has also been seeing a resurgence of MID refund fraud, which Andrew says was prevalent about two years ago before a substantial drop-off in activity. In many of these cases, cybercriminals take advantage of virtual terminals offered by financial institution – either merchant acquirer or processor. Merchants are offered this option typically for instances where they don’t have physical access to customer cards, or physical payment terminals are down. (e.g., mail or telephone orders). These solutions allow merchants to accept credit card payments using their internet-connected computers. The trouble is that retailers often don’t know this resource is available. Attackers obtain merchant credentials (usernames and passwords) in any number of ways, including but not limited to social engineering, looking for credentials not erased from POS devices resold online or through auctions, or even from merchant information printed on receipts. With access to these merchant acquirer or processor virtual terminals, attackers can then force high-dollar refunds to be loaded onto gift cards or compromised credit cards without a corresponding initial transaction.

"Unfortunately, many acquirers have no technology to validate that refunds are legitimate," says Andrew, "and until very recently there were no requirements to match refunds to corresponding sales." Andrew also points out that people who are assigned to validate refunds might not recognize high-dollar refunds as a red flag if these are common for the industry or business.

Beyond POS attacks, retailers are experiencing more ransomware as cybercriminals across industry sectors seek to optimize ways to monetize network access. Andrew says, "As we described in a previous newsletter, criminals have been following up banking trojan infections with ransomware after draining or diverting funds. We also recently had a case where attackers infected a system with cryptomining malware, but then launched ransomware when the return wasn't sufficient. The moral of the story is that companies have to be as strategic in their defense as cybercriminals are in their attacks." *(See this issue's **Experts Corner** for Andrew's best practices for preventing and mitigating POS compromises.)*

Technically Speaking – POS Malware Attack

POS malware attack generally follows a five-step strategy:

1. **Infection:** Malware is introduced onto the targeted system or network, often via email compromise or after exploring vulnerable / unpatched systems.
2. **Execution:** Malware then scans and monitors processes to find data, creates or modifies registry entries to maintain persistence, and may even introduce additional elements such as keyloggers or bot functionality.
3. **Collection:** Using RAM "scrapers", it evaluates the clear-text RAM data to differentiate between encrypted payment data versus other types of data.
4. **Extraction:** Payment card data is extracted and transmitted back to the criminals via a command and control (C2) server.
5. **Profit:** Attackers use the information to create fraudulent cards for physical use at retail stores and automated teller machines (ATMs), to make online purchases, or to sell for profit on black market websites or forums.

** Source: New Jersey Cybersecurity and Communications Integration Cell (NJCCIC)*

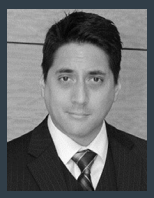
Technically Speaking – MID Refund Fraud

How and why recent MID refund frauds work:

1. **Intelligence Gathering:** Criminals obtain a merchant's credentials (e.g., username, password, merchant ID number) through social engineering, email-based attacks, purchase of used POS devices where credentials have not been erased, etc.
2. **Compromise:** Attackers program purchased POS devices with the merchant's credentials or gain access to a merchant's virtual terminal with credentials obtained during intelligence-gathering.
3. **Attack:** Refunds are forced through the payment system without a corresponding sales transaction, and the funds are loaded on a gift card.
4. **Evade Detection:** Refund requests are rarely validated against real transaction IDs; monitoring is human-based and often not vigilant; attackers can mask fraudulent requests with legitimate batches so detection becomes even harder.
5. **Loss Recognition:** Businesses recognize an imbalance in their financial reporting after extensive losses.

Case Studies

- Threat actors posed as disgruntled customers and sent a strident complaint to a company's online customer care center. As a follow-up to the company's initial response, the fraudsters submitted a Word document that they claimed provided full details of their complaint. Upon opening the attachment, the customer care representative unwittingly unleashed malware that allowed unauthorized access to the merchant's systems environment. This was followed shortly thereafter by a significant POS attack.
- In one MID case that Kroll examined, a threat actor was using the credentials associated with a small enterprise's payment terminal to issue fraudulent refunds of up to $1.3 million. Many of these refunds happened in the off-hours when no one was on the premises, which was indicative of a remote intrusion. An additional red flag was the fact that this client routinely processed only low-dollar transactions. Kroll determined the threat actors likely compromised a virtual terminal that was provided to the client by their payment processor and used this terminal to issue the fraudulent refunds.



Andrew Valentine
Managing Director

Kroll Experts Corner:
Top Five Best Practices for Mitigating POS Compromises

Based on their fieldwork investigating numerous POS compromise cases, Managing Director Andrew Valentine and Director Brandon Nesbit recommend these top five best practices for avoiding or mitigating POS fraud:

Segregate payment and corporate networks.
This separation will help keep intruders from moving between these systems. On a related note, ensure systems in the cardholder data environment cannot communicate directly to the internet nor to other systems with that capability.

Restrict outbound activity from the card processing environment.
Restrict this activity to only specific destinations required for transaction processing. Consider going further by including a whitelist of only trusted programs, websites, IP addresses and associated ports and protocols.

Implement end-to-end encryption (E2EE) on payment devices.
E2EE effectively prevents RAM-scraping malware from carving cardholder data out of memory.

Conduct regular employee training and security awareness.
Pay particular attention to social engineering schemes and help employees learn how to spot phishing emails and other attempts to manipulate them into providing access.

Implement multi-factor authentication for all privileged accounts and remote access.
Merchants should work to implement a multi-factor authentication schema for all remote access into both corporate and PCI environments.

Web Application Compromise and E-commerce Exploits

The Monitor, Issue 6

Kroll identified a growing number of web compromise incidents over the last few months, including cases that involved code injection techniques and sniffers. Web compromises most commonly affected the e-commerce platforms in the retail sector.

Web application compromises involve a variety of exploits directed at web applications (e.g., content management systems) and e-commerce platforms, such as the popular e-commerce platform Magento. Actors use techniques such as structured query language (SQL) injection, cross-site scripting (XSS) and account takeover (ATO) attacks to gain access to payment data and other personal information submitted on payment sites.

The National Vulnerability Database (NVD) posted an alert in April 2019 specifically on an SQL injection vulnerability in Magento which could allow an unauthenticated user to execute arbitrary code and gain access to payment information.

According to Kroll Managing Director J. Andrew Valentine, bad actors are primarily focusing their web compromise attacks on vulnerabilities in three areas: (1) the Magento platform itself, (2) third-party plug-ins and (3) misconfigured Amazon S3 buckets.

“Users can address the S3 bucket issue by simply configuring their AWS accounts with the proper access controls,” says Andrew. “However, dealing with the Magento and third-party plug-in issues is a more difficult proposition and requires both proactive and ongoing mitigation efforts. For example, a Magento idiosyncrasy requires users to patch sequentially. In other words, if a user applies the patch for the Magento issue noted in the April 2019 NVD alert but hasn’t applied earlier patches in sequential order, that vulnerability will remain unpatched until all previous patches have been applied first.”

Andrew also notes that many exploits used against the Magento platform and third-party plug-ins can be difficult to spot: “We find alterations in nondescript areas of websites, e.g., headers and footers, which can help them evade detection, or in PHP functions or third-party plug-ins, like customer support chat capabilities. Sometimes, attackers will strategically alter scripts in multiple areas of an e-commerce platform; in many of these cases, website owners may see one exploit, but not the others.”

From a proactive standpoint, Andrew says Magento users might want to consider running the Magento Security Scan Tool on their sites to help monitor and detect potential issues. The growing risk landscape may also warrant upgrading to a higher, more robust version of the Magento platform or exploring the PCI Security Standards Council list of Validated Payment Applications for potential alternatives.

See more of Andrew’s recommendations in the Experts Corner of this newsletter.

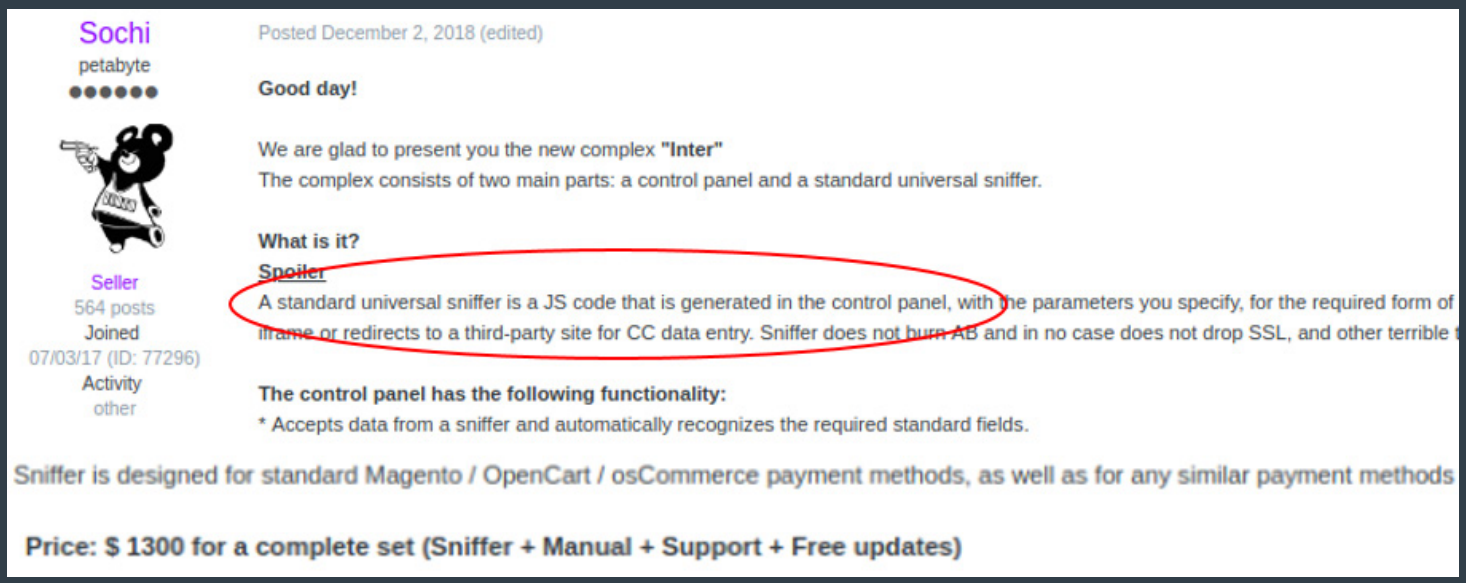
Magecart Compromises

Many exploits leveraged against e-commerce systems are often labeled or attributed to "Magecart." According to Kroll consultant and dark web specialist Samuel Colaizzi, "Magecart is a generic term that is used by the cyber security industry to classify JavaScript inject attacks that sniff and scrape payment card data from e-commerce platforms, such as Magento. There is no specific code that would define an attack as being Magecart; rather, any JavaScript inject that sniffs and scrapes payment card data as well as other personally identifying information (PII) from payment sites would be classified as Magecart.

Technically Speaking:
Sniffer E-commerce Exploits on the Dark Web

A packet analyzer, aka "sniffer," is not an inherently malicious program; system administrators commonly use it to monitor network traffic. Bad actors, however, use sniffers to intercept data that they can monetize directly or through its sale, such as unencrypted passwords, usernames, account numbers, etc.

Below are screen captures of activity on the dark web where someone was selling a sniffer exploit (screenshot 1 below) and a credit card aggregation/dump (screenshot 2) that could have been obtained via this type of sniffer.



Sochi
petabyte

Seller
564 posts
Joined
07/03/17 (ID: 77296)
Activity
other

Posted December 2, 2018 (edited)

Good day!

We are glad to present you the new complex **"Inter"**
The complex consists of two main parts: a control panel and a standard universal sniffer.

What is it?
Spoiler
A standard universal sniffer is a JS code that is generated in the control panel, with the parameters you specify, for the required form of
iframe or redirects to a third-party site for CC data entry. Sniffer does not burn AB and in no case does not drop SSL, and other terrible t

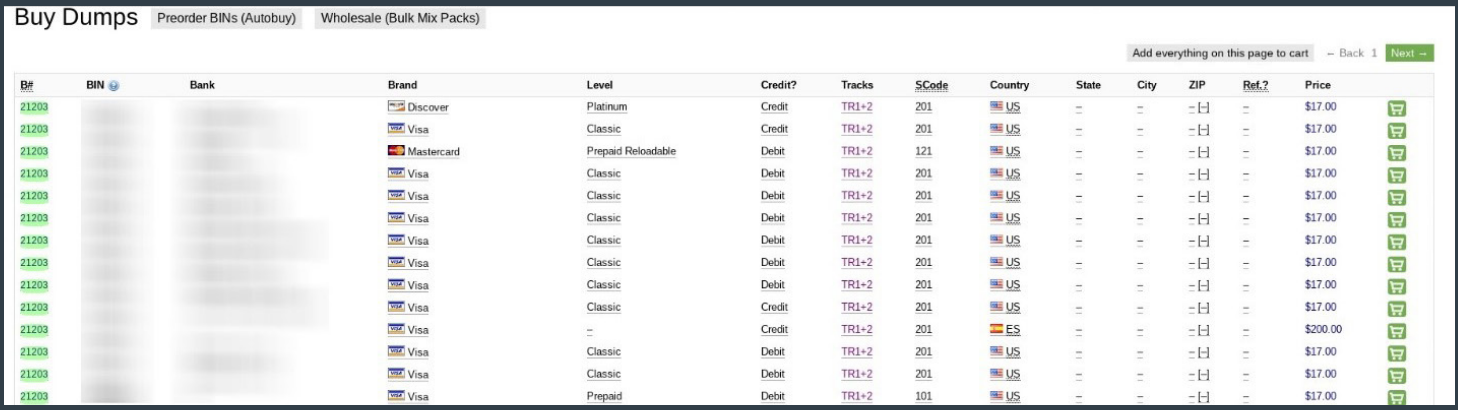
The control panel has the following functionality:
* Accepts data from a sniffer and automatically recognizes the required standard fields.

Sniffer is designed for standard Magento / OpenCart / osCommerce payment methods, as well as for any similar payment methods

Price: $ 1300 for a complete set (Sniffer + Manual + Support + Free updates)

What is happening in the screenshot above:

- E-commerce exploit called "Inter" for sale on the dark web
- Seller "Sochi" posted advertisement on exploits forum on December 2, 2018
- According to open sources, this exploit continues to be sold by criminal actors.



Buy Dumps Preorder BINs (Autobuy) Wholesale (Bulk Mix Packs)

Add everything on this page to cart ← Back 1 Next →

B#	BIN	Bank	Brand	Level	Credit?	Tracks	SCode	Country	State	City	ZIP	Ref.?	Price
21203			Discover	Platinum	Credit	TR1+2	201	US	–	–	– [–]	–	$17.00
21203			Visa	Classic	Credit	TR1+2	201	US	–	–	– [–]	–	$17.00
21203			Mastercard	Prepaid Reloadable	Debit	TR1+2	121	US	–	–	– [–]	–	$17.00
21203			Visa	Classic	Debit	TR1+2	201	US	–	–	– [–]	–	$17.00
21203			Visa	Classic	Debit	TR1+2	201	US	–	–	– [–]	–	$17.00
21203			Visa	Classic	Debit	TR1+2	201	US	–	–	– [–]	–	$17.00
21203			Visa	Classic	Debit	TR1+2	201	US	–	–	– [–]	–	$17.00
21203			Visa	Classic	Debit	TR1+2	201	US	–	–	– [–]	–	$17.00
21203			Visa	Classic	Debit	TR1+2	201	US	–	–	– [–]	–	$17.00
21203			Visa	Classic	Credit	TR1+2	201	US	–	–	– [–]	–	$17.00
21203			Visa	–	Credit	TR1+2	201	ES	–	–	– [–]	–	$200.00
21203			Visa	Classic	Debit	TR1+2	201	US	–	–	– [–]	–	$17.00
21203			Visa	Classic	Debit	TR1+2	201	US	–	–	– [–]	–	$17.00
21203			Visa	Prepaid	Debit	TR1+2	101	US	–	–	– [–]	–	$17.00

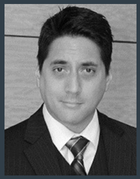
What is happening in the screenshot above:

- On July 9, 2019, JokerStash forum published an aggregated list of credit cards, which could have been obtained via a sniffer like the one that was being offered in screenshot 1.
- The JokerStash credit card dump provided credit card details, including track 1 and track 2 data for major U.S. credit cards.
- Card identifiers included bank and BIN number. (Kroll's CyberDetectER® BINWatch can monitor for this activity, enabling clients to take quick action on these cards to preempt fraud.)

Case Studies

- Kroll reviewed one web compromise incident in which a software-as-a-service (SaaS) company discovered the website it used for transactions was injected with malicious code. When analysts reverse-engineered the code, we discovered it was scraping sensitive data, temporarily storing it and then sending the data outbound. The malicious code impacted the victim's cloud storage platform and affected the client-side browser.

- Another web compromise incident affected the payment system of a food service retailer. The retailer's web developer conducted a security scan and found a JavaScript code exploit in the content management system (CMS) block. According to the web developer, the exploit was announced in March 2019 and identified as PRODSECBUG-2198 (an exploit against Magento).



Andrew Valentine
Managing Director

Kroll Experts Corner:
Best Practices for Mitigating Web Compromise

Managing Director Andrew Valentine recommends the following strategies for mitigating web compromises, particularly those affecting e-commerce sites.

- Understand and precisely follow the patching regimen for your e-commerce platform. In the case of Magento, remember that you must patch sequentially in order for patches to fully execute.
- Regularly review and properly configure access controls on Amazon S3 buckets.
- Implement a file integrity monitoring (FIM) solution, create hash sets for payment pages and monitor the findings every day for any alterations to payment functions.
- Similarly, consider employing an endpoint threat monitoring solution such as Kroll's CyberDetectER® Endpoint Powered by Red Canary to provide early visibility to potential attack vectors enterprise-wide.
- Update to the latest version of your website's content management system (CMS).
- Monitor the NIST National Vulnerability Database for new vulnerabilities related to the type of e-commerce platform your organization utilizes.
- Encourage the use of secure coding practices to prevent SQL injection and XSS.

Contact Us

Keith Wojcieszek
Associate Managing Director, Cyber Risk
keith.wojcieszek@kroll.com | +1 443 295 5082

Based in Washington, D.C., Keith joined Kroll from the United States Secret Service, where he served with distinction for 15 years. Most recently, Keith led the USSS Cyber Intelligence Section, Criminal Investigation Division, where he managed the agency's national response to cyber investigative initiatives focused on protecting the financial infrastructure of the United States. In this role, Keith also coordinated complex international investigations that targeted transnational organized crime networks with an emphasis on cyber and information security.

Nicole Sette
Director, Cyber Risk
nicole.sette@kroll.com | +1 609 514 8225

Based in the Secaucus office. Nicole is a highly accomplished security professional, who brings unique insight to the multiple dimensions inherent in client challenges from her years of federal law enforcement and military experience. Nicole served as a Cyber Intelligence Analyst with the Federal Bureau of Investigation for nearly 10 years, and was an Intelligence Specialist with the U.S. Army Communications-Electronics Command for four years.

Kroll | A Division of DUFF & PHELPS

Browse the latest editions of *The Monitor* and subscribe free at kroll.com/themonitor

About Kroll

Kroll is the leading global provider of risk solutions. For more than 45 years, Kroll has helped clients make confident risk management decisions about people, assets, operations and security through a wide range of investigations, cyber security, due diligence and compliance, physical and operational security and data and information management services. For more information, visit www.kroll.com.

About Duff & Phelps

Kroll is a division of Duff & Phelps, a global advisor with nearly 3,500 professionals in 28 countries around the world. Our clients include publicly traded and privately held companies, law firms, government entities and investment organizations such as private equity firms and hedge funds. We also advise the world's leading standard-setting bodies on valuation and governance best practices.

For more information, visit www.duffandphelps.com.