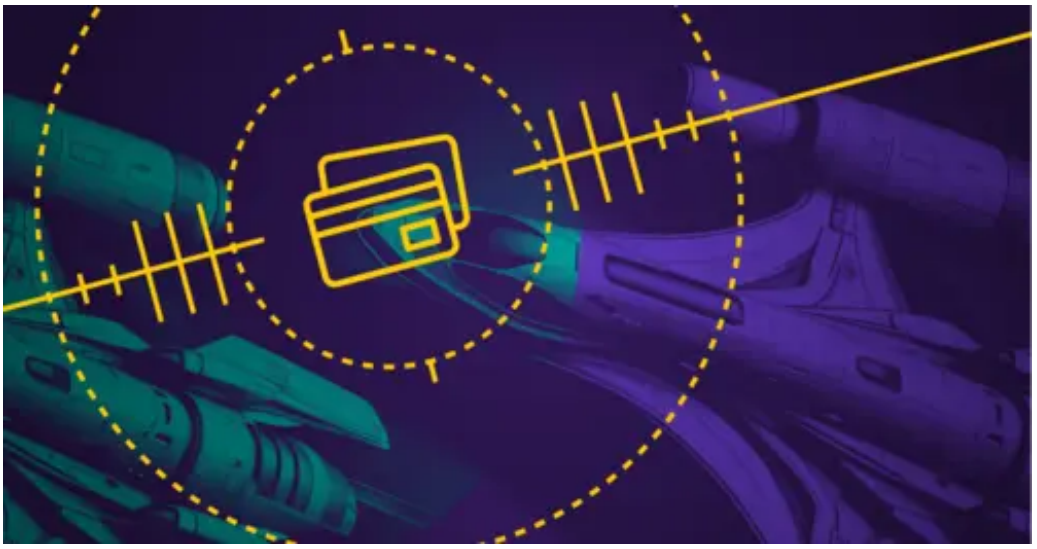
# Sansec Threat Research & News

Archived: 2026-04-05 22:49:28 UTC

Sansec specializes in digital skimming since 2015. We are often "first at the scene" to investigate high profile breaches and publish regularly about our discovery of new attack vectors.



## Mass PolyShell attack wave hits 471 stores in one hour

2026-03-30 Sansec detected 471 stores compromised in a single hour as attackers exploit the PolyShell vulnerability at scale. The attack injects obfuscated JavaScript from the freshly registered domain lanhd6549tdhse.top. New victims are still coming in every minute.

skimming magecart magento adobe-commerce +2


## Novel WebRTC skimmer bypasses security controls at $100+ billion car maker

2026-03-24 Sansec discovered a payment skimmer that uses WebRTC DataChannels to receive its payload and exfiltrate stolen data, bypassing CSP and HTTP-based security tools.

skimming magecart skimmer webrtc +2

**PolyShell: unrestricted file upload in Magento and Adobe Commerce**

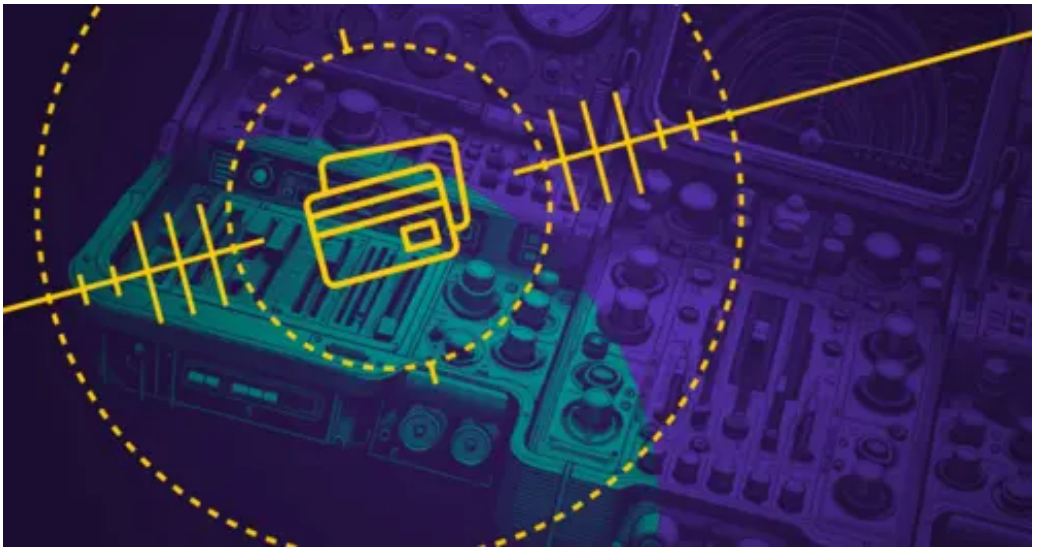
2026-03-17 PolyShell lets attackers upload executable files to any Magento or Adobe Commerce store via the REST API. Sansec has now observed attacks on 79.5% of all stores. No official patch exists for production versions. Many stores run web server configurations that enable remote code execution (RCE) or ...

skimming magento adobe-commerce rce +3

**Digital skimmer hits global supermarket chain**

2026-02-20 Sansec discovered a payment skimmer on the online store of a top-10 global supermarket chain. Despite repeated attempts to alert the company, the skimmer is still in place after 4 days.

skimming magecart skimmer prestashop



**Building a faster YARA engine in pure Go**

2026-02-18 We built a pure Go YARA engine that's 6.8x faster for text-based scanning, with no C dependencies. It now processes over 57,000 scans per day in production, and we're open-sourcing it today.

skimming ecomscan yara yargo +1


**Claude finds 353 zero-days on Packagist**

2026-01-22 We built an AI-powered security pipeline to audit popular ecommerce extensions on Packagist. The vulnerabilities we found range from password leaks to full remote code execution.

skimming magento adobe-commerce supply-chain +1

**The billion-dollar security.txt problem**

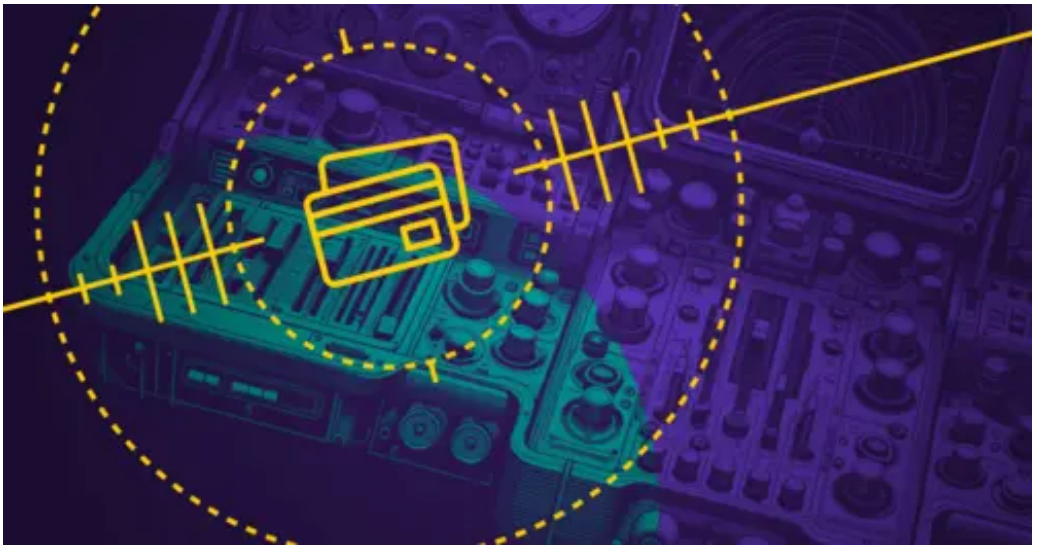
2026-01-16 When Sansec found a keylogger on a major US bank employee site, the hardest part wasn't detecting the malware. It was finding someone to tell.

skimming security-txt disclosure enterprise

**Keylogger targets 200,000+ employees at major US bank**

2026-01-15 Sansec discovered an active keylogger on the employee merchandise store of a top 3 US bank. The malware harvests all form data (including passwords and personal information) from over 200,000 potential victims.

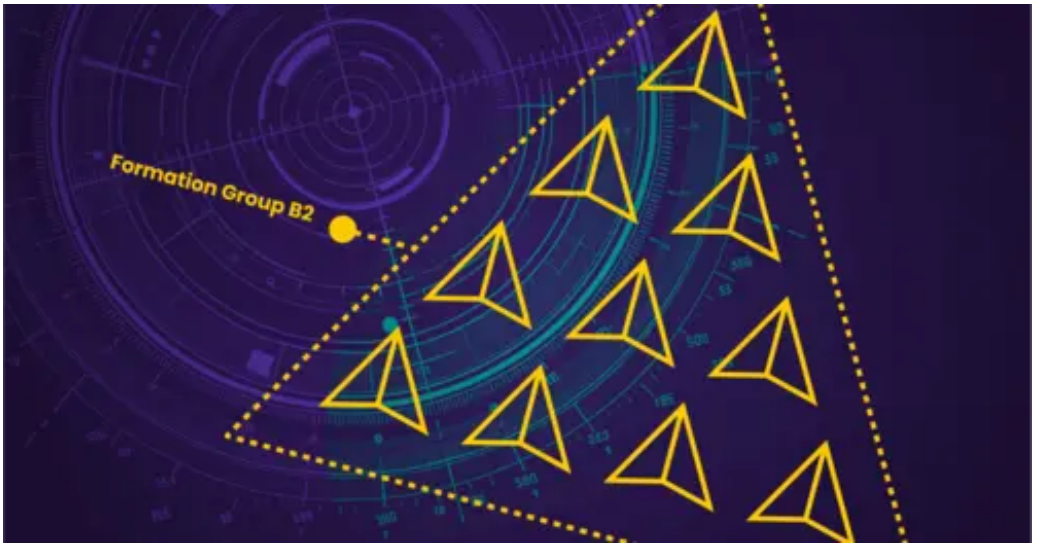
skimming magecart skimmer keylogger +1



## ConnectPOS leaked Github secrets for years

2026-01-12 Sansec discovered that ConnectPOS has been showing their Github credentials on their site for 4 years. This would enable attackers to slip malicious code into each of the thousands of ConnectPOS retail installations. Sansec recommends to verify integrity of installed code.

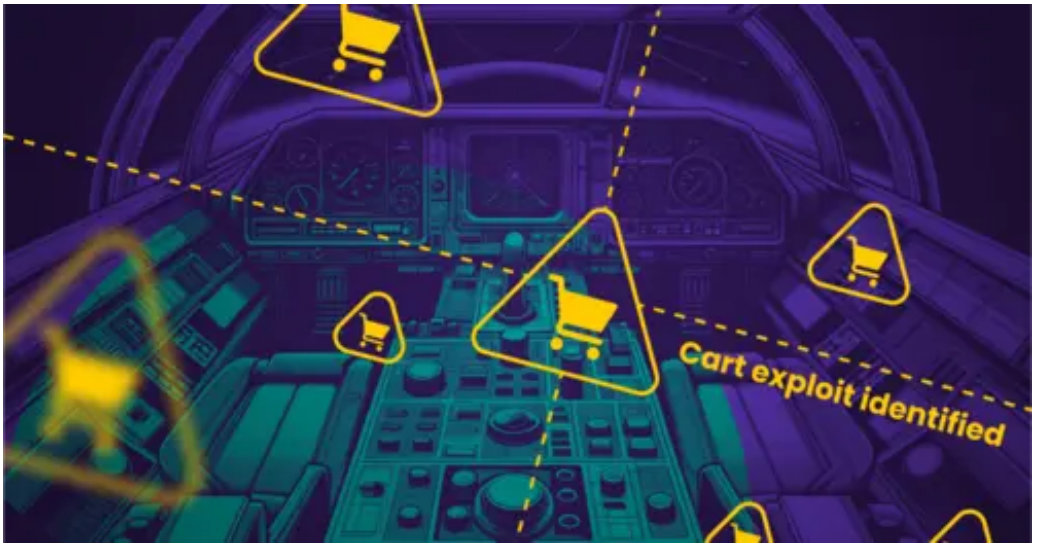
skimming supply-chain magento connectpos +2




## Critical backdoor found in MGT Varnish extension

2025-12-15 Sansec discovered an open backdoor in MGT Varnish, a popular cache manager for online stores. While the backdoor appears to be intended for remote support, it can be exploited by anyone.

skimming




**SessionReaper attacks have started, 3 in 5 stores still vulnerable**

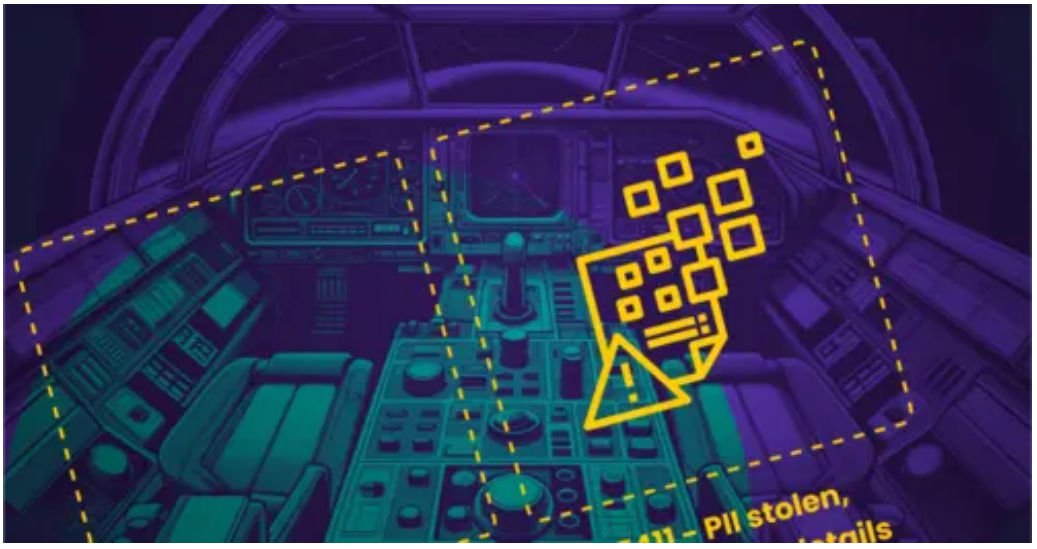
2025-10-22 Six weeks after Adobe's emergency patch, SessionReaper (CVE-2025-54236) has entered active exploitation. Sansec Shield blocked dozens of attacks today. With only 38% of stores patched and exploit details now public, mass abuse will follow in the coming hours.

skimming CVE-2025-54236 magento adobe-commerce +6

**SessionReaper, unauthenticated RCE in Magento & Adobe Commerce (CVE-2025-54236)**

2025-09-08 SessionReaper (CVE-2025-54236) is a critical bug in Magento & Adobe Commerce. The bug may hand full control of a store to unauthenticated attackers. Automated attacks have hit over 50% of all stores globally. Merchants should act immediately.

skimming CVE-2025-54236 magento adobe-commerce +5




## Adobe patches critical Magento admin takeover via menu injection

2025-06-12 A new attack on Adobe Commerce may break the menu bar for admin users. If your menu bar is missing, someone is stealing your session via CVE-2025-47110.

skimming

## Backdoor found in popular ecommerce components

2025-05-01 Multiple vendors were hacked in a coordinated supply chain attack, Sansec found 21 applications with the same backdoor. Curiously, the malware was injected 6 years ago, but came to life this week as attackers took full control of ecommerce servers. Sansec estimates that between 500 and 1000 store...

skimming


**Found defunct.dat on your site? You've got a problem.**

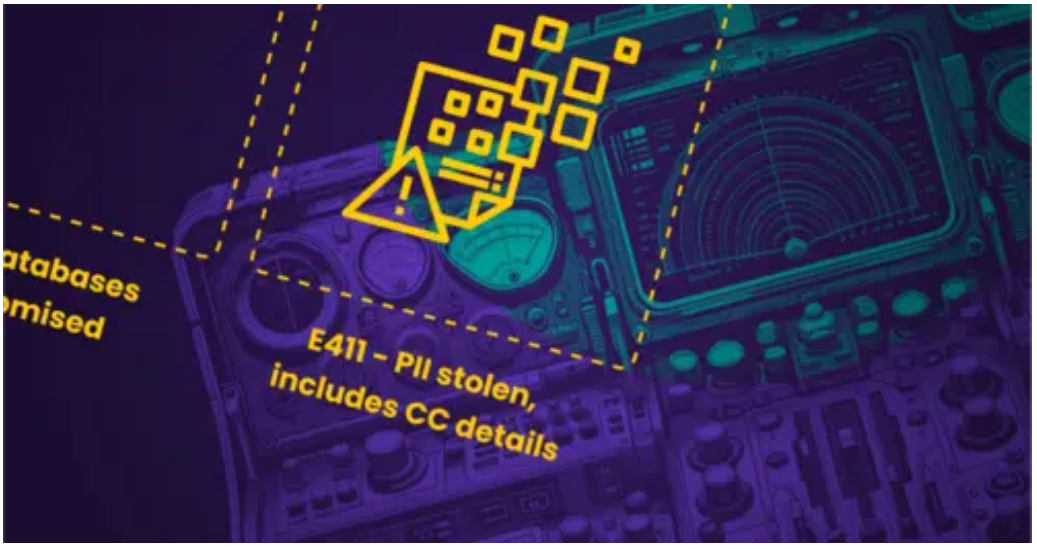
2025-04-03 Sansec found criminals mass-scanning for defunct.dat files which contain GSocket backdoor keys. A quick scan reveals dozens of infected stores.

skimming


**You have 2 weeks left to set up CSP for your store**

2025-03-17 Increasing use of Content Security Policy (CSP) as PCI-DSS 4.0 goes live on April 1st. However, our research shows that most online stores have not enabled CSP reporting - a critical requirement under the new PCI standards.

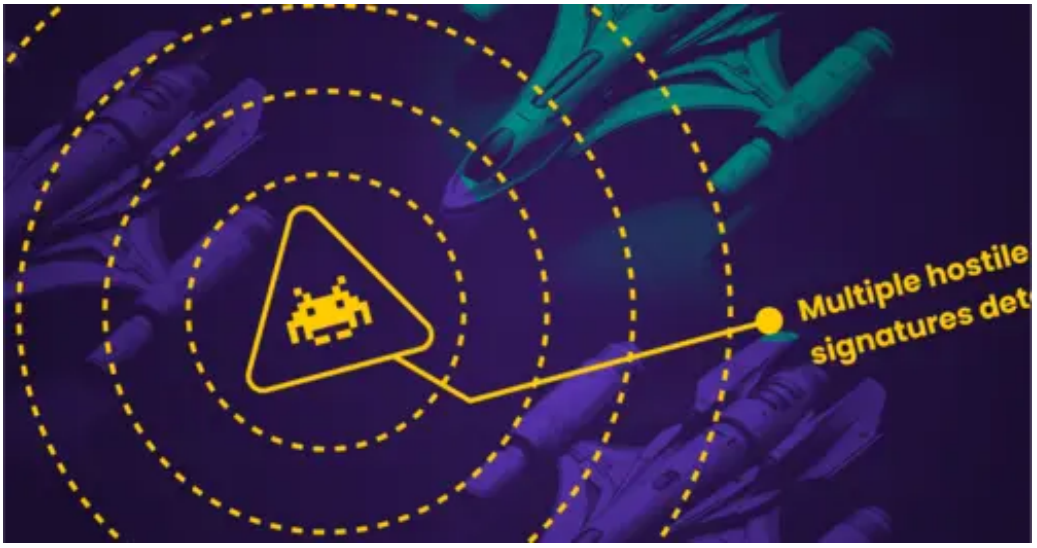
skimming




**Merchants left guessing at last-minute PCI-DSS u-turn**

2025-03-06 Merchants outraged as PCI-SSC changes compliance criteria just weeks before the new regulation comes into effect.

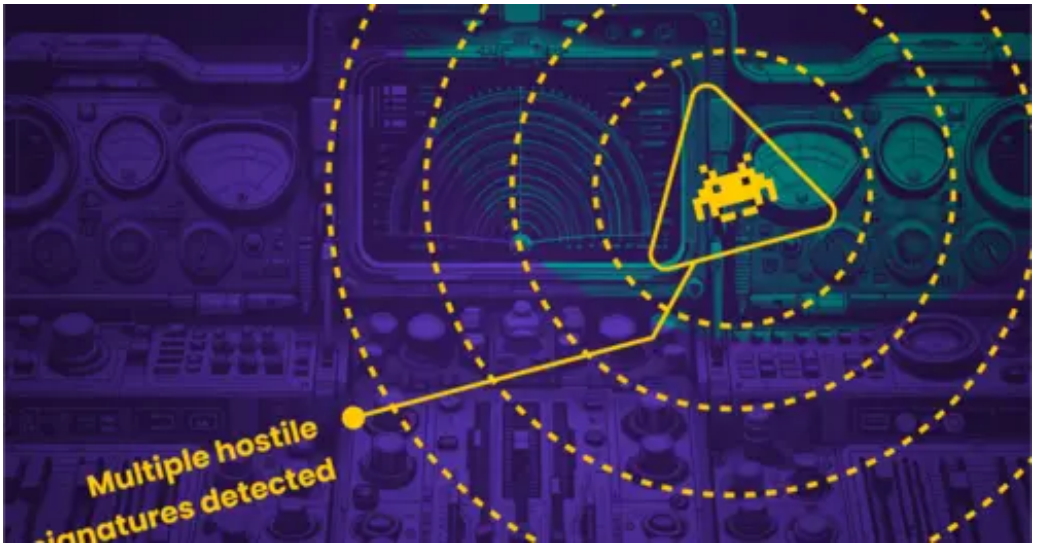
skimming




**Magento Security Release APSB25-08 [Impact Analysis]**

2025-02-12 Critical (CVSS 9.4) release enables attackers to take control of customer accounts.

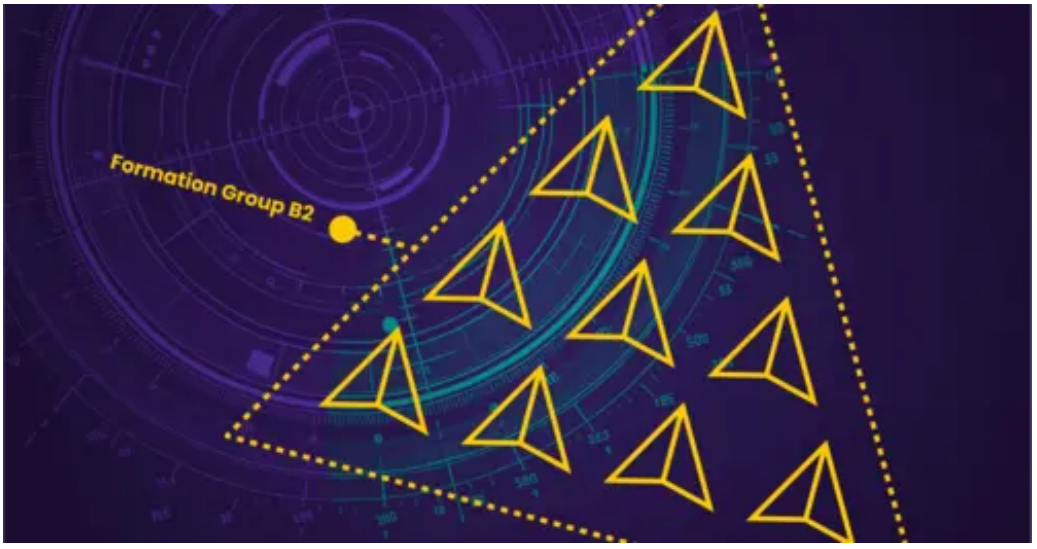
skimming




**Sorry, client-side security does not work**

2025-02-03 Browser-based protection can easily be bypassed by the majority of digital skimming attacks.

skimming




**Google services abused in skimming campaigns**

2024-12-31 Attackers are abusing Google services like Translate and YouTube to bypass security measures and execute malicious campaigns. Recent incidents and strategies employed by these threat actors are outlined below.

skimming

**Thousands of Adobe Commerce stores hacked in competing CosmicSting campaigns**

2024-10-01 Cybercriminals have hacked 5% of all Adobe Commerce and Magento stores this summer. Among the victims are large international brands. Seven distinct groups are using CosmicSting attacks to plant malicious code on victim stores.

skimming


**CosmicSting attack & defense overview**

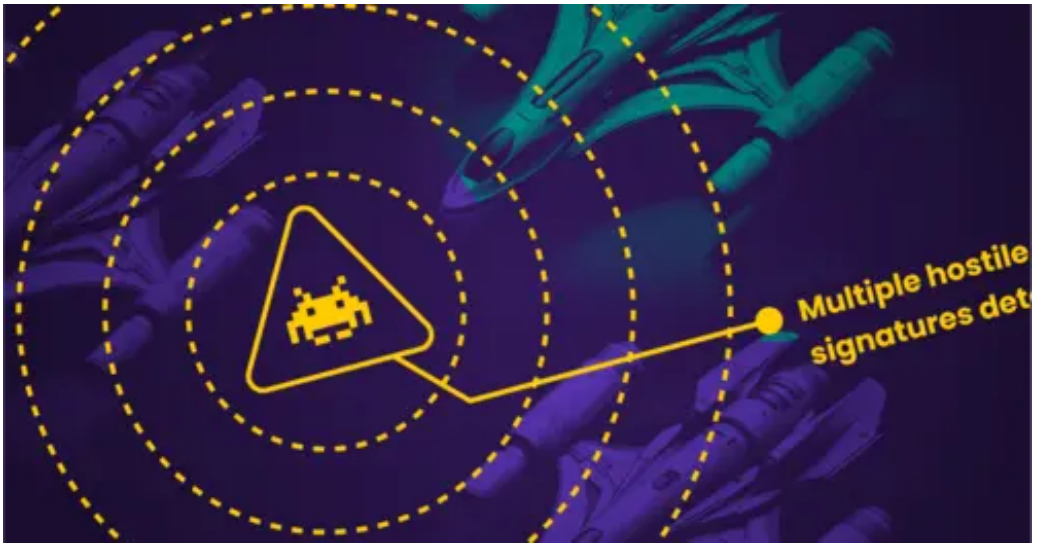
2024-09-16 CosmicSting (aka CVE-2024-34102) is the worst bug to hit Magento and Adobe Commerce stores in two years. Sansec observes that stores are getting hacked at a rate of 5 to 30 per hour. Merchants need to implement these counter measures as soon as possible.

skimming

**Persistent backdoors injected on Adobe Commerce via new CosmicSting attack**

2024-08-27 In our previous posts, we discussed how threat actors were abusing CosmicSting by injecting malicious scripts into CMS blocks. While these attacks continue, we've observed a significant escalation - attackers are now chaining CosmicSting with CNEXT to achieve remote code execution (RCE). We warne...

skimming




**CosmicSting attacks have started hitting major stores**

2024-07-12 Almost a month ago, we warned about the CosmicSting attack that threatens 75% of Adobe Commerce stores. Sansec now observes mass-abuse of this vulnerability in the wild. Stores are getting hacked at a rate of 5 to 30 per hour, our live tracking reveals. International household brands are among th...

skimming

**Polyfill supply chain attack hits 100K+ sites**

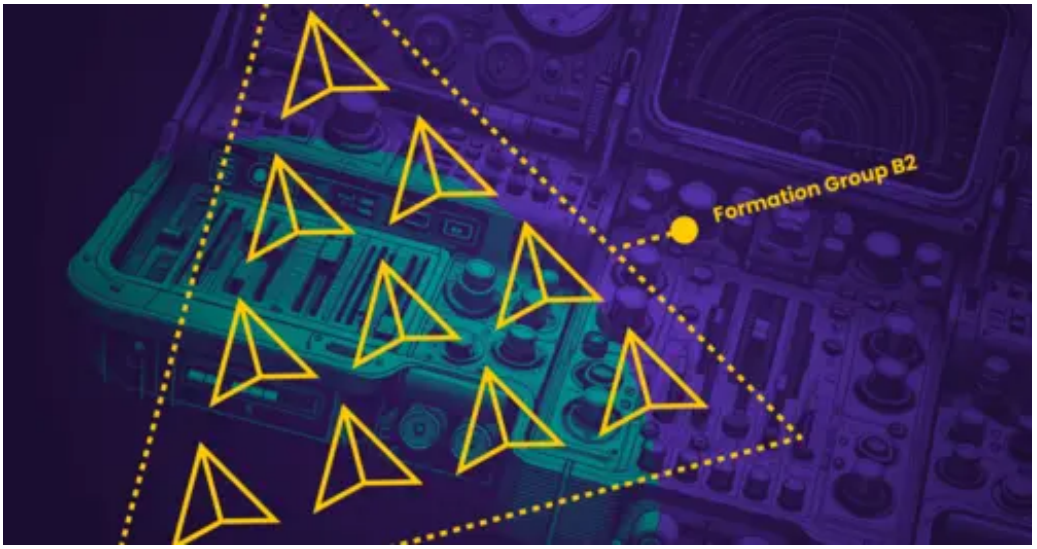
2024-06-25 The new Chinese owner of the popular Polyfill JS project injects malware into more than 100 thousand sites.

skimming

**CosmicSting attack threatens 75% of Adobe Commerce stores**

2024-06-18 One week after the release of a critical security fix, just a quarter of all Adobe Commerce and Magento stores has been patched.

skimming




**Persistent Magento backdoor hidden in XML**

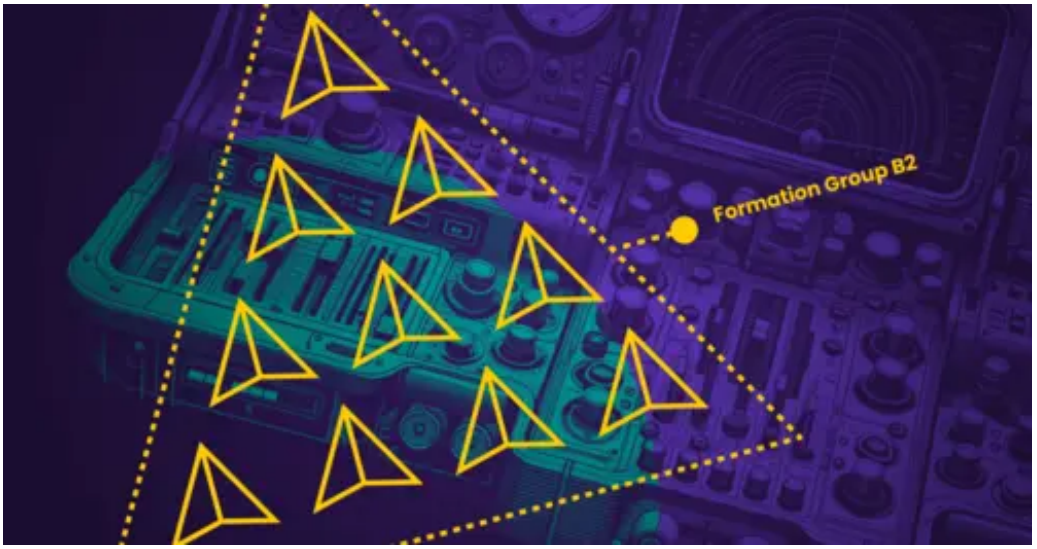
2024-04-04 Does your Interceptor.php keep getting infected? Attackers are using a new method for malware persistence on Magento servers. Sansec discovered a cleverly crafted layout template in the database, which was used to automatically inject malware.

skimming

**Sansec joins forces with Google's VirusTotal**

2024-03-08 Google, via its subsidiary VirusTotal, has selected Sansec as approved security vendor. Sansec will contribute its specialized intel on eCommerce security threats to the VirusTotal platform.

skimming




## Sansec and Europol counter online skimming

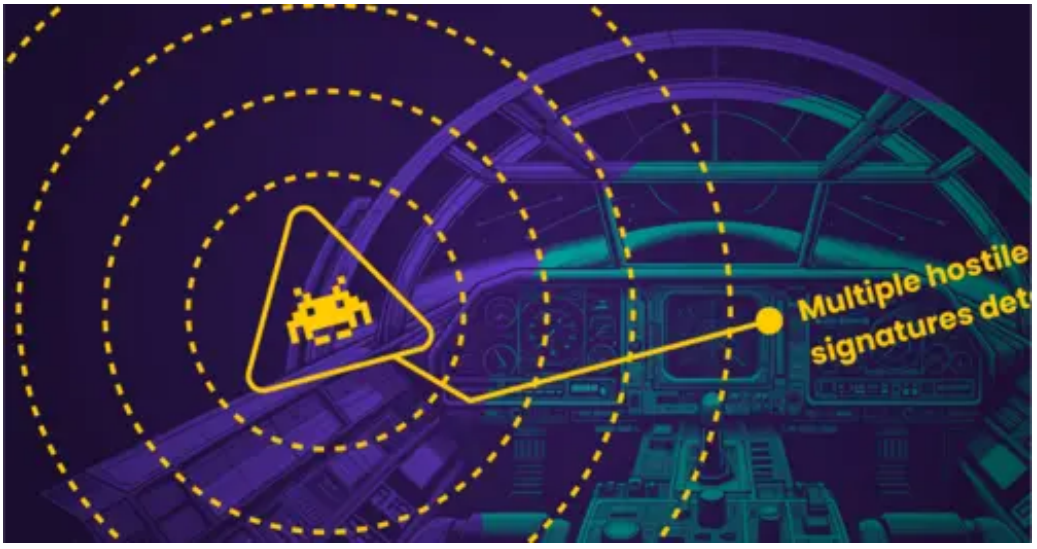
2024-01-09 Europol, law enforcement authorities from 17 countries and the European Union Agency for Cybersecurity (ENISA) have joined forces with private sector partners such as Sansec.

skimming


## Magento wish list exploit bypasses WAF protection

2023-12-18 Found your Magento 2 store hacked recently? Chances are, that attackers injected a malicious wish list. Just before Christmas? Oh the irony.

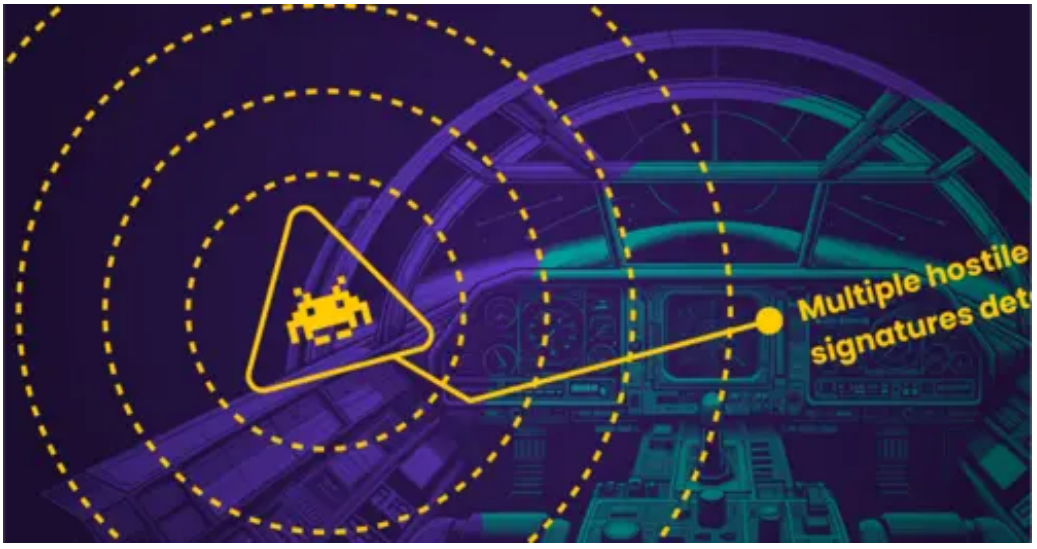
skimming trojanorder




**Is your store’s newsletter being used for phishing?**

2023-11-10 Cybercriminals in eCommerce are diversifying their targets, now aiming at entire customer databases instead of just stealing credit cards. A recent incident revealed this trend: a hacked Magento admin account was exploited to launch a phishing campaign through the platform's newsletter system, re...

skimming




**Malware Persistence via Telegram and GitHub**

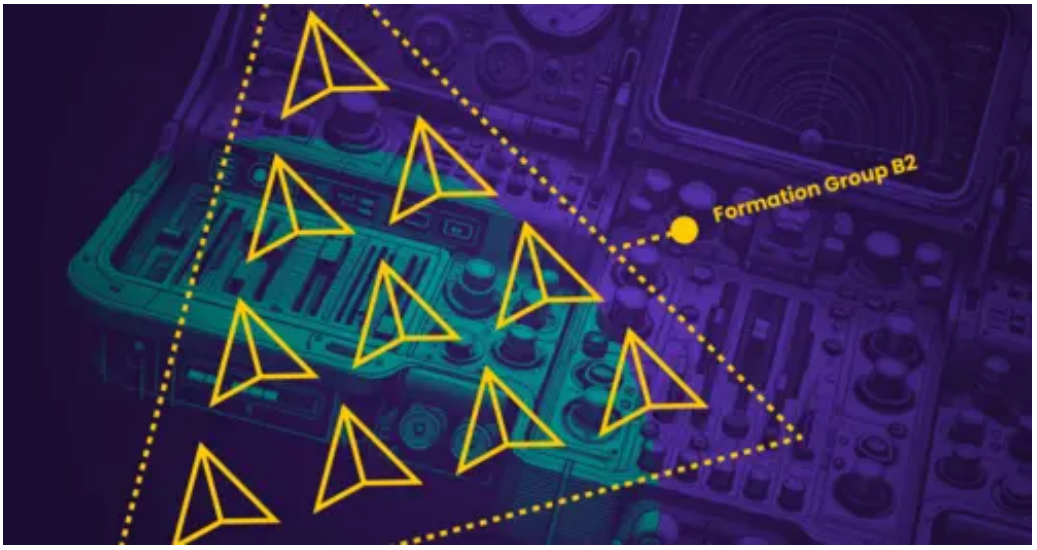
2023-08-22 Credit card thieves now use Telegram and Github to steal customer data.

skimming

**Postponed Exfiltration Evades Detection**

2023-05-09 Criminals have come up with a clever way to steal customer data only after the regular checkout flow. This stealthy attack is very hard to detect.

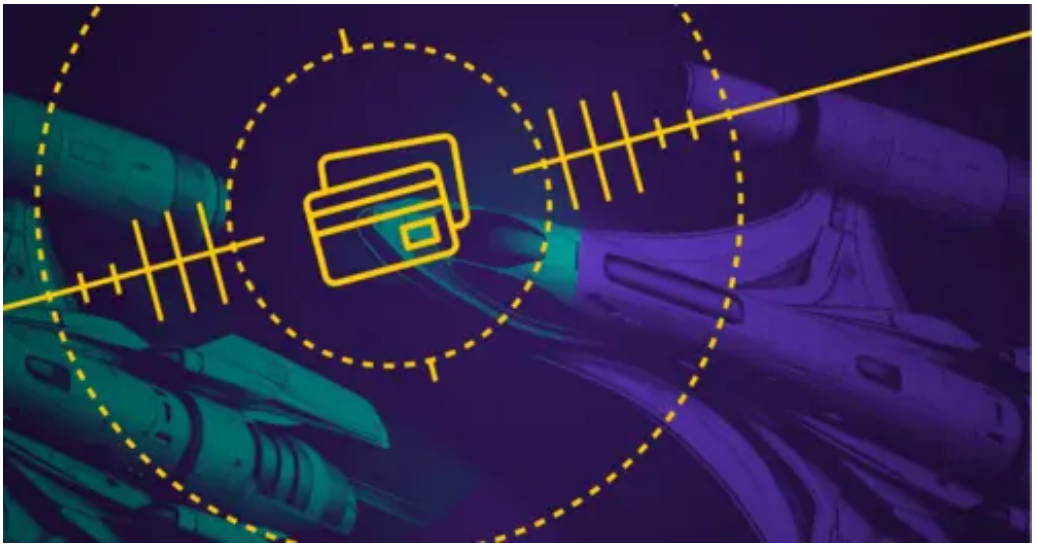
skimming




**Sansec analysis: 12% of online stores leak private backups**

2023-02-07 Sansec discovered that one in nine online stores accidentally expose private backups. This mistake could have dire consequences. Online criminals are actively scanning for these backups, as they contain passwords and other sensitive information. Exposed secrets have been used to gain control of s...

skimming



**Vendors defeat Magento security patch (+ simple check)**

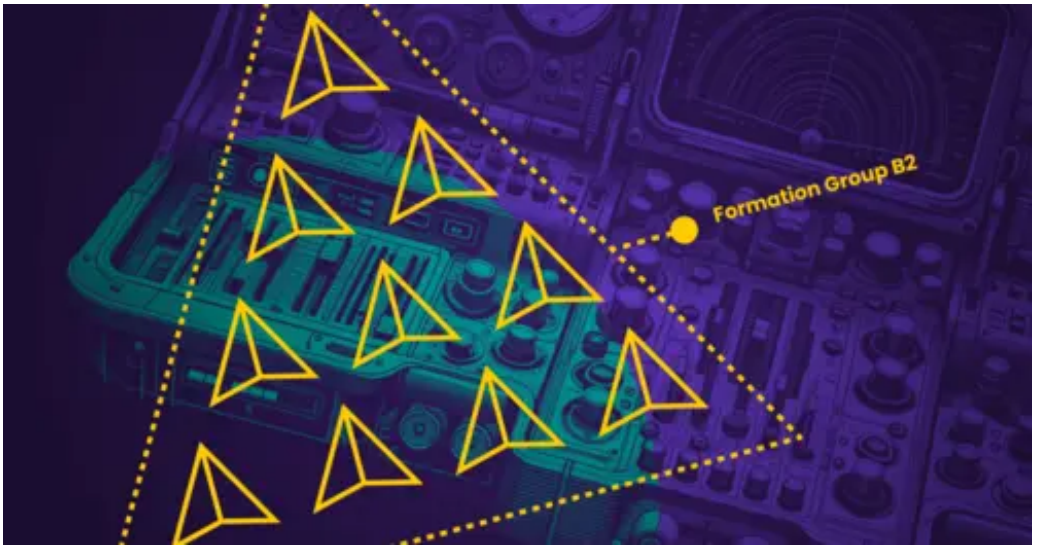
2023-01-17 Magento and Adobe Commerce stores around the world have been hammered with Trojan Order attacks this winter. And even if you have patched or installed Adobe's 2.4.4 release, you may still be vulnerable. Sansec discovered that several vendors and agencies are actively bypassing this security fix, ...

skimming trojanorder


**Fake Klaviyo accounts added to Magento**

2022-12-21 Are your Magento admin accounts legitimate? Chances are, that a klaviyo_support_XXXX account was added this week. Best to quickly remove it and read this article.

skimming




## Adobe Commerce merchants to be hit with TrojanOrders this season

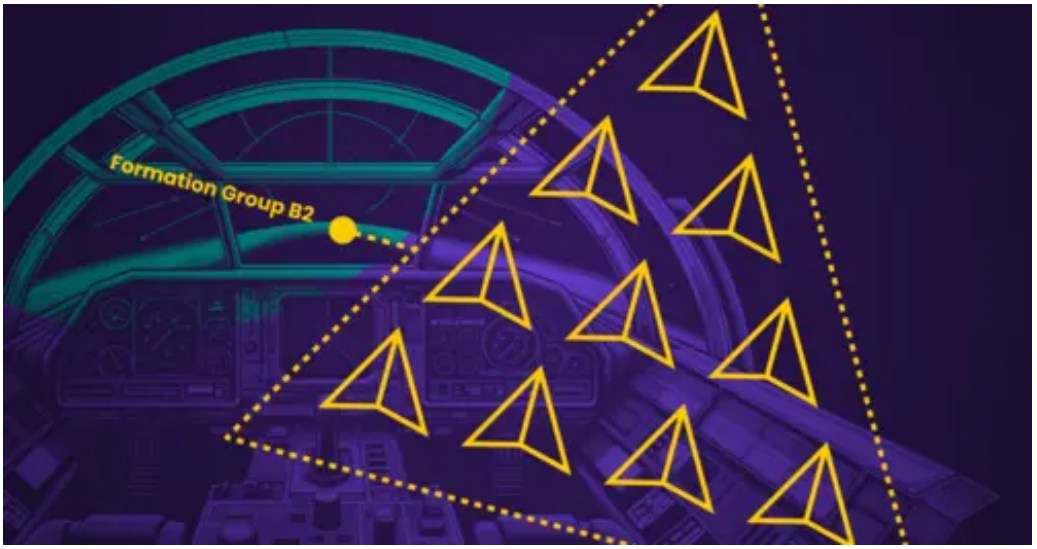
2022-11-15 At least seven Magecart groups are injecting TrojanOrders at approximately 38% of Magento and Adobe Commerce websites in November.

skimming trojanorder


## Extortion of Magento merchants

2022-11-07 Sansec has received reports of criminals trying to extort Magento merchants with the message below. As long as the sender does not produce evidence, they almost certainly did not steal your sensitive data. Ignoring them is best.

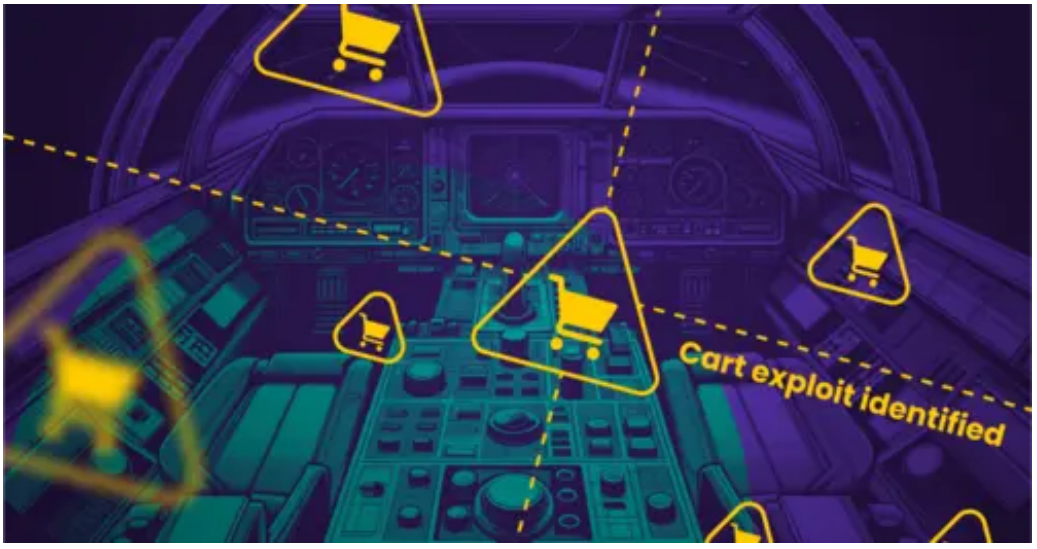
skimming




## Surge in Magento 2 template attacks

2022-09-22 The critical template vulnerability in Magento 2 (CVE-2022-24086) is gaining popularity among eCommerce cyber criminals. The majority of recent Sansec forensic cases concern this attack method. In this article we share our findings of 3 template hacks, and hope it will help you if you are confron...

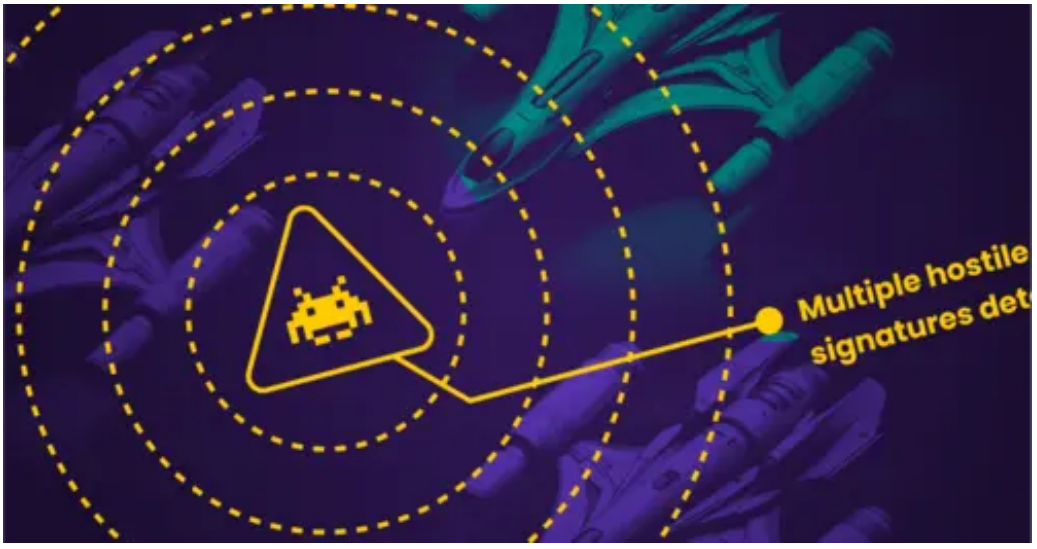
skimming trojanorder




## Magento vendor Fishpig hacked, backdoors added

2022-09-13 Fishpig, a vendor of popular Magento-Wordpress integrations, has been hacked. Sansec found that attackers have injected malware in Fishpig software and taken control of Fishpig servers. Online stores running Fishpig software may now have the "Rekoobe" malware installed on their servers,...

skimming




## Magento 2 critical vulnerability (CVE-2022-24086 & CVE-2022-24087)

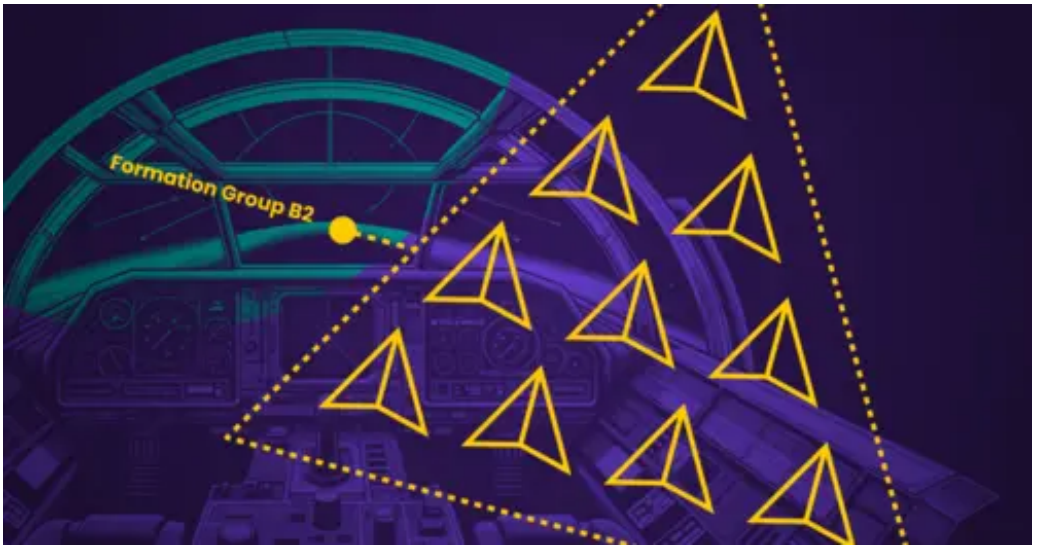
2022-02-14 Adobe has released two emergency patches for a critical vulnerability in Magento 2. You need to apply both patches, in order. The vulnerability allows unauthenticated remote code execution (RCE), which is the worst possible type. Actual abuse has already been reported. To illustrate the severity,...

skimming trojanorder

## NaturalFreshMall: a Magento Mass Hack

2022-02-08 An investigative report by Sansec researchers on how one vulnerable Magento extension leads to a mass web store attack, with Magecart attackers using naturalfreshmall.com to hide and serve malware to 500+ ecommerce websites.

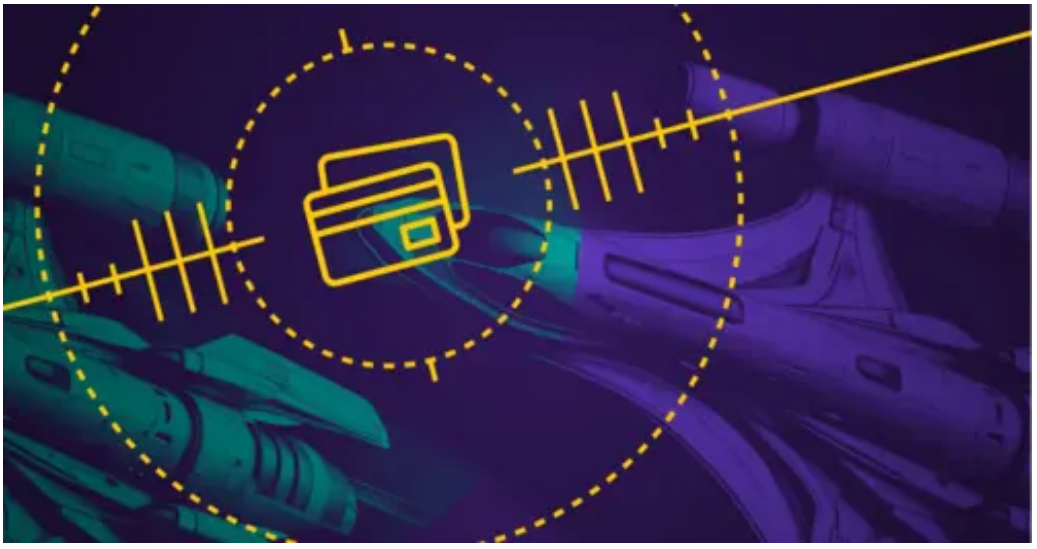
skimming




## Magento and the Log4j vulnerability

2021-12-13 Updated Dec 20th. This article describes how Magento is affected by the critical log4j vulnerability, and what you can (and should) do to prevent a hack. A critical vulnerability in the popular Log4j Java library has been massively exploited since December 1st. It exposes full control to a remote...

skimming



## NginRAT parasite targets Nginx

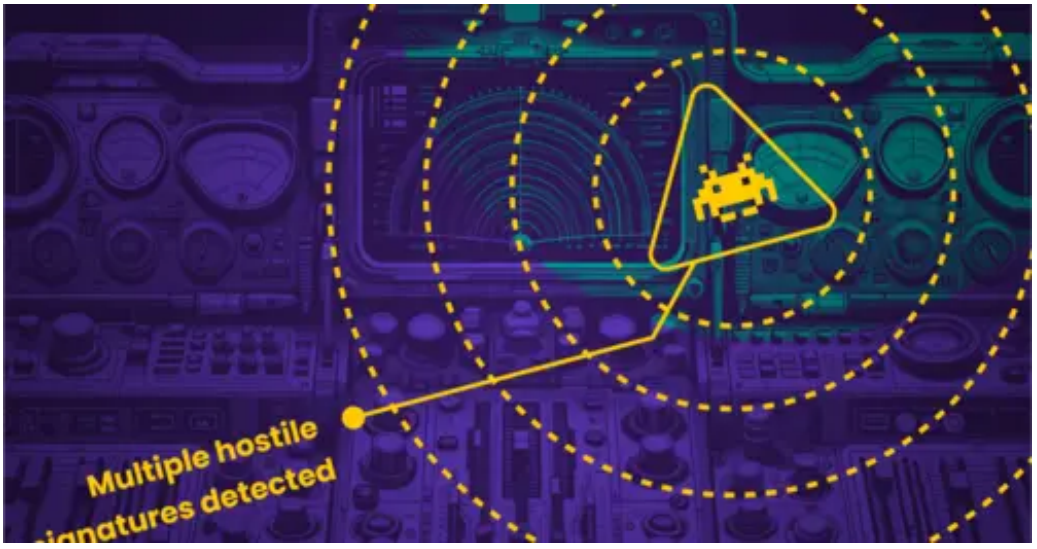
2021-12-01 A new parasitic malware targets the popular Nginx web server, Sansec discovered. This novel code injects itself into a host Nginx application and is nearly invisible. The parasite is used to steal data from eCommerce servers, also known as "server-side Magecart". The malware was found o...

skimming


## CronRAT malware hides behind February 31st

2021-11-24 In the run-up to Black Friday, Sansec discovered a sophisticated threat that is packed with never-seen stealth techniques. This malware, dubbed "CronRAT", hides in the Linux calendar system on February 31st. It is not recognized by other security vendors and is likely to stay undetected...

skimming




## New linux_avp malware hits eCommerce sites

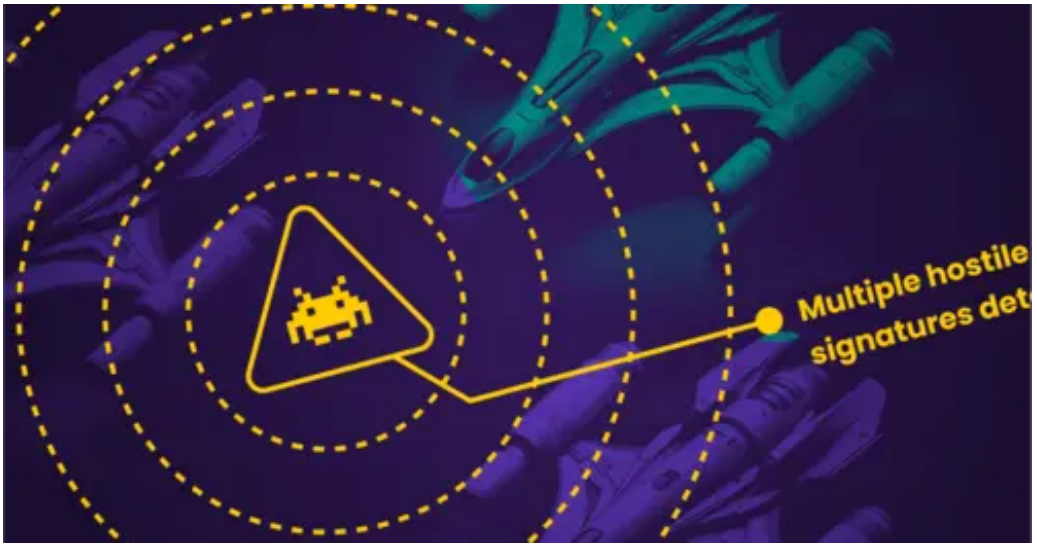
2021-11-18 Sansec discovered a new malicious agent "linux_avp" that hides as system process on eCommerce servers. It is being deployed around the world since last week and takes commands from a control server in Beijing.

skimming

## Case Study: How eCommerce Hackers Silently Steal Credit Card Data

2021-05-03 The majority of online stores have never been hacked and, as a result, take a somewhat lax approach to cybersecurity. However, no less than 20% of all online stores get hacked every year, which means it might only be a matter of time until yours becomes the next victim.

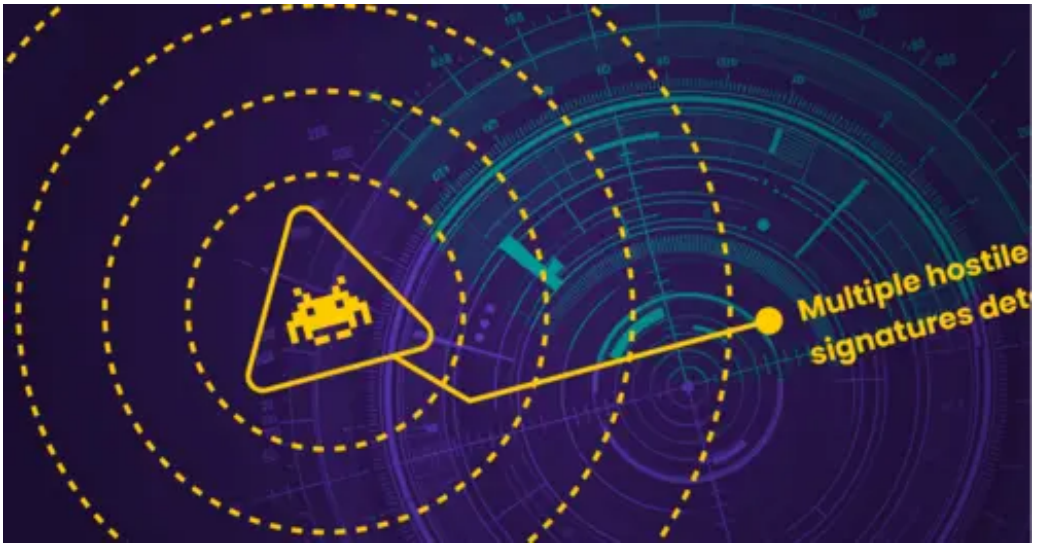
skimming




## Google Apps Script used to steal data

2021-02-18 The Google business application platform Apps Script is used to funnel stolen personal data, Sansec learned. Attackers use the reputation of the trusted Google domain script.google.com to evade malware scanners and trust controls like CSP. Thanks to some data from @sansecio, I came across another...

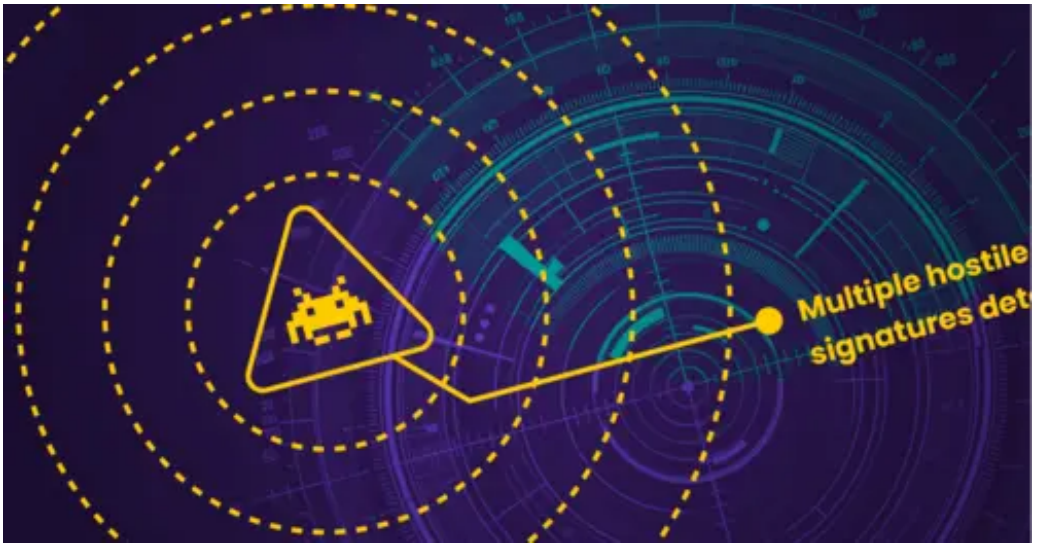
skimming




## Fake payment page before checkout on Shopify and BigCommerce

2020-12-24 A new type of web skimmer was found on a dozen stores hosted on Shopify, BigCommerce, Zen Cart and WooCommerce. Hosted (SaaS) ecommerce platforms like BigCommerce and Shopify do not allow custom JavaScript on their checkout pages. This skimmer evades that by showing a fake payment form and record...

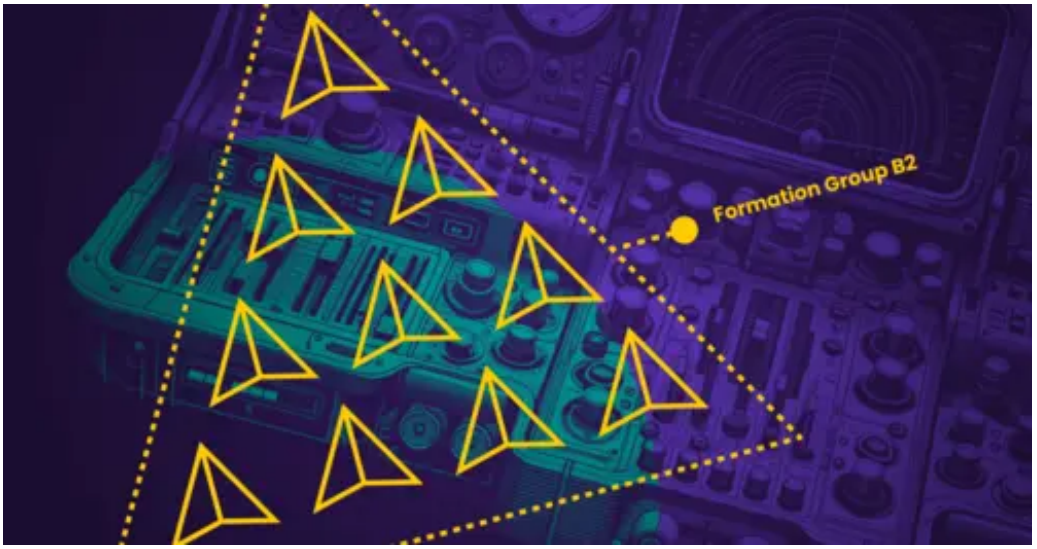
skimming




## eCommerce trojan accidentally leaks victims

2020-12-18 Sansec discovered a clever remote access trojan (RAT) that has been hiding in the alleys of hacked eCommerce servers. Despite the advanced setup, perpetrators mistakenly left a list of victim stores in a deleted file, which unveils the depth of this hacking campaign. The RAT is used to gain illic...

skimming




## Persistent parasite in EOL Magento 2

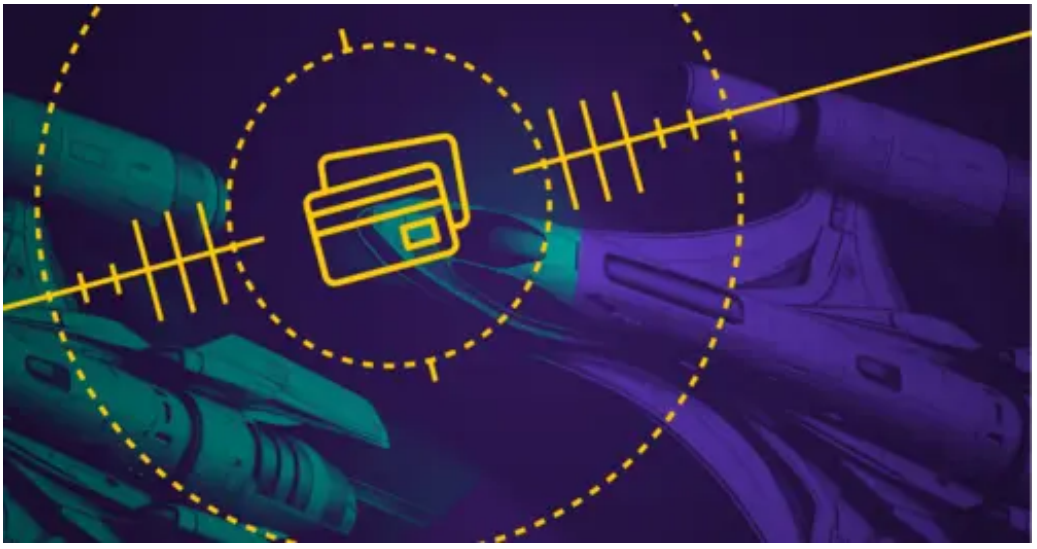
2020-12-02 Over the last months, hackers have quietly added a subtle security flaw to over 50 large online stores, only to exploit them right before Black Friday, Sansec research shows. The flaw's presence would ensure future access for the attackers, even if their primary operation was blown. Sansec has be...

skimming

## Payment skimmer hides in social media buttons

2020-11-26 Researchers at Sansec have uncovered a novel technique to inject payment skimmers onto checkout pages. This new malware has two parts: a concealed payload and a decoder, of which the latter reads the payload and executes the concealed code. While skimmers have added their malicious payload to ben...

skimming



## Cardbleed: 3% of Magento install base hacked

2020-09-14 Update Sept 18: Cardbleed has infected 2806 Magento1 stores so far (3% of total install base) Over the weekend, almost two thousand Magento 1 stores across the world have been hacked in the largest documented campaign to date. It was a typical Magecart attack: injected malicious code would inter...

skimming


## North Korean hackers are skimming US and European shoppers

2020-07-06 North Korean state sponsored hackers are implicated in the interception of online payments from American and European shoppers, Sansec research shows. Hackers associated with the APT Lazarus/HIDDEN COBRA group were found to be breaking into online stores of large US retailers and planting payment...

skimming


## Digital skimmer runs entirely on Google, defeats CSP

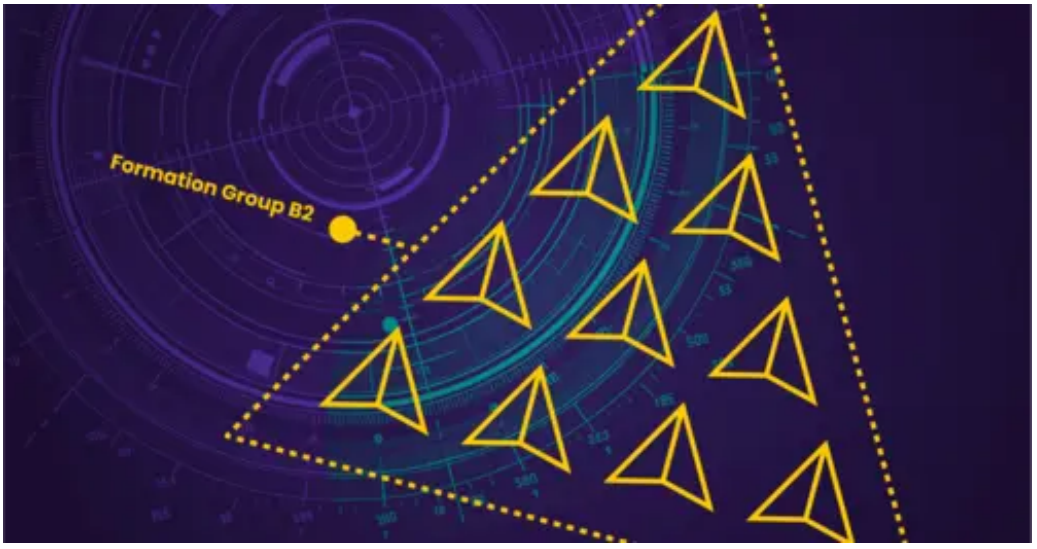
2020-06-22 A newly discovered skimming campaign runs entirely on Google servers, Sansec research shows. The novel malware sends stolen credit cards directly to Google Analytics, evading security controls like CSP. Typically, a digital skimmer (aka Magecart) runs on dodgy servers in tax havens, and its locat...

skimming

## Lockdown: Stores closed, online stores hacked

2020-06-15 A day after Claire's (fashion retailer) closed its 3,000 stores, an anonymous party registered claires-assets.com. Later, Claire's got hacked.

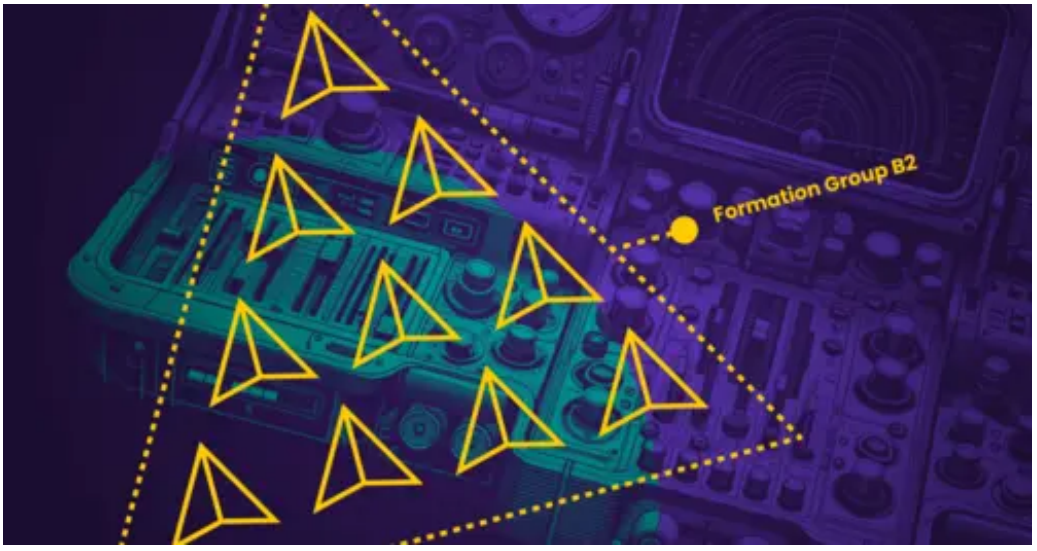
skimming




**Do these two things to keep your Magento 1 store running after June**

2020-05-28 Over a 100 thousands Magento 1 stores will be running after Adobe terminates support in June (end-of-life). Many merchants need more time to transition to Magento 2 or another platform. No need to panic, your store will not suddenly crash on July 1st. But you should make two important arrangement...

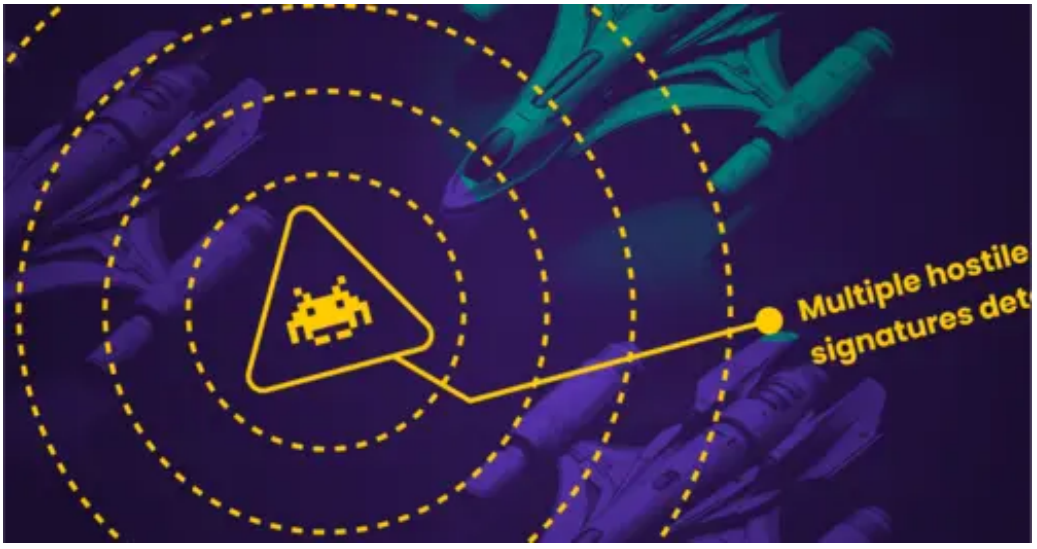
skimming magento 1 deadline




**Will Magento 1 stay PCI compliant?**

2020-05-08 Magento 1 will no longer receive official updates & security fixes per July 1st, 2020 (the end-of-life, or EOL date). Merchants are urged to upgrade to Magento 2, but for many stores this deadline is not feasible. Merchants want to know: Will my Magento 1 store still be secure after July 1st...

skimming magento 1 pci




**Sansec reveals longest Magecart skimming operation to date [Analysis]**

2020-02-25 Sansec, a global leader in eCommerce security, reveals that hackers successfully infiltrated an online printing platform for more than two and a half years. Our research shows that crooks ran keyloggers to intercept customer payment data and that multiple actors have since been fighting for contr...

skimming

**Sansec partners with Maxcluster**

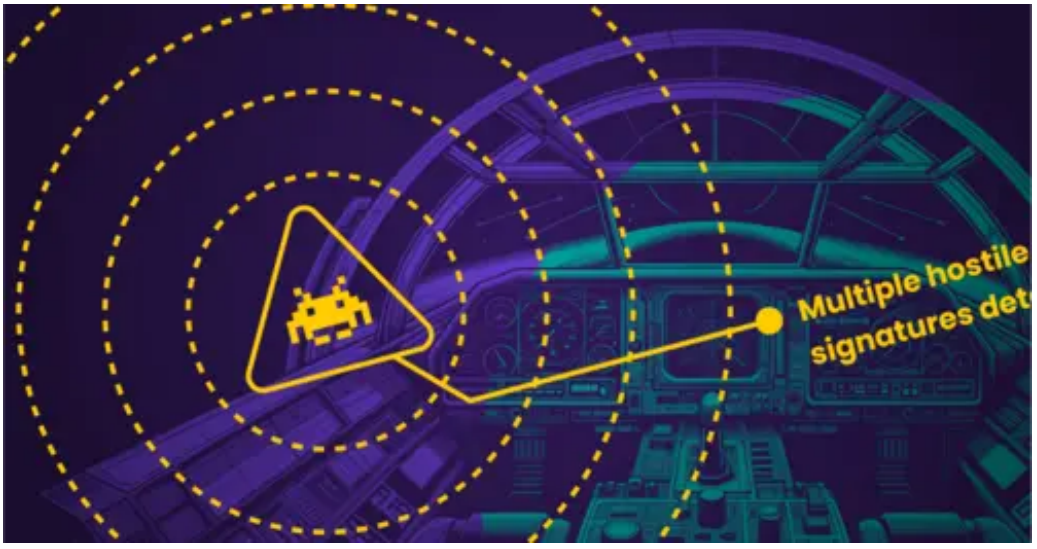
2020-02-20 Utrecht, February 20; Sansec is proud to announce that it has formed a long-term strategic partnership with maxcluster to bring its industry-leading anti-malware technology to the German e-commerce hoster. The unique alliance, which makes maxcluster the most secure e-commerce hosting platform in ...

skimming maxcluster partnership

## Indonesian Magecart hackers arrested

2020-01-25 The Indonesian police announced on Friday that they have arrested three alleged Magecart hackers on December 20th. The suspects are from Jakarta and Yogyakarta and are 23, 26 and 35 years old. After the press conference, one suspect admitted on Indonesian television that he had injected web skimm...

skimming




## Payment skimmers have impersonated Sansec

2019-12-02 Payment skimmers are hiding their malpractice by impersonating our Sansec anti-skimming service. They have registered malicious domains sansec.us and sanguinelab.net, even using a fake address in Amsterdam to make it look legitimate. Here is the fraud registration record: Domain Name: sansec.us C...

skimming


## American Cancer Society hit by payment skimmer

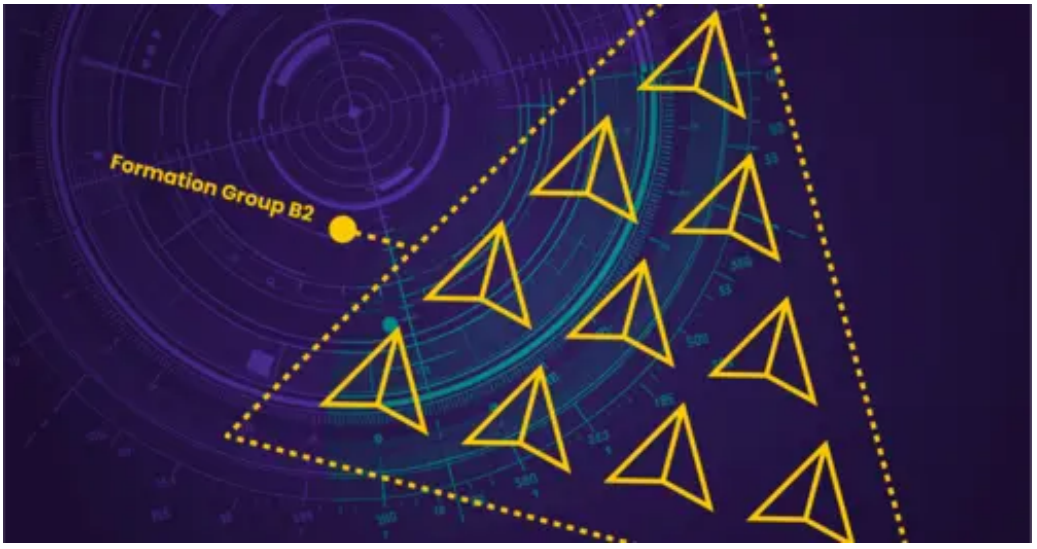
2019-10-25 Digital skimming groups (aka Magecart) hit another low, as they successfully targeted the American Cancer Society last night. Our skimmer detectors found a piece of malicious code embedded on the Cancer.org shop, which intercepts payments from unsuspecting visitors. Sansec has contacted Cancer.or...

skimming


## Magento security extentions vendor got hacked

2019-10-07 The store of a US Magento extension vendor was found compromised. Attackers had write access to the server selling extensions. We are awaiting a statement on the integrity of downloaded software. Our malware crawlers detected a compromise of Extendware, a vendor of Magento extensions such as &quo...

skimming




## FBI recommends malware scanning against skimming

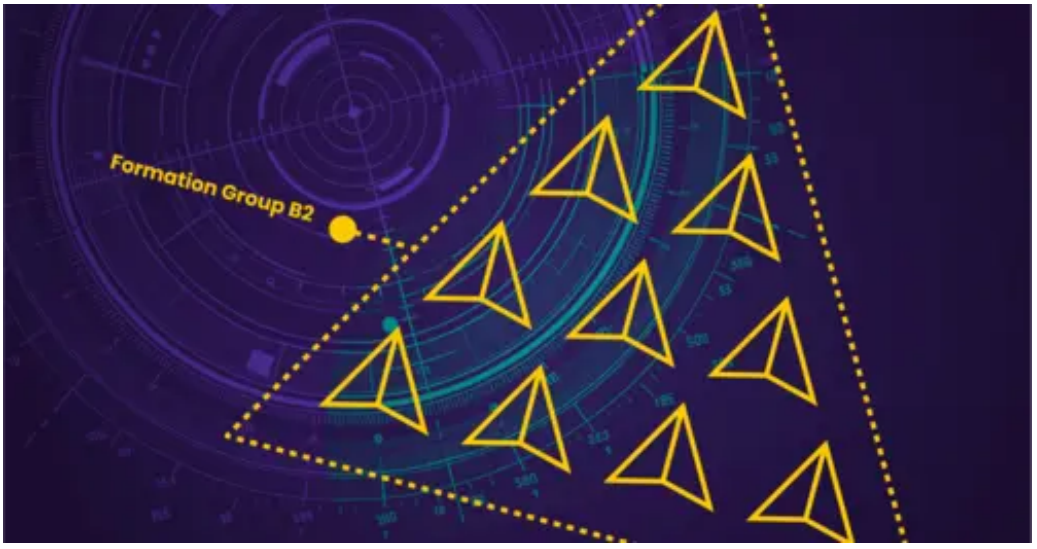
2019-08-17 The FBI warns small and medium-sized businesses and government agencies against the threat of e-skimming. E-skimming occurs when cyber criminals inject malicious code onto a website. Read the original FBI statement

skimming fbi malware

## Sansec at Europol training: 50,000+ stores hacked

2019-08-12 Cementing itself as a global force in the protection against eCommerce fraud, Sansec has been invited to speak at the fifth edition of Europol's Training Course on Payment Card Fraud Forensic Investigations in Avila, Spain. The week-long event, hosted by the Spanish National Police Academy, saw 5...

skimming sansec europol training




## PCI-SSC/RHISAC quote Sansec: 20% stores reinfected

2019-08-01 The PCI Security Standards Council and the Retail & Hospitality ISAC alert merchants to the threat of digital skimming. In its report, it quotes Sansec research, which has found that about 20% of hacked merchants eventually get re-infected. Read the full report here (PDF).

skimming


## Critical Magento 2 flaw exploited within 16 hours

2019-05-10 The number of hacked Magento 2 stores spiked in the last four weeks, after a critical security flaw was discovered in March and criminals stole admin passwords within 16 hours. Merchants are advised to implement emergency measures, even if they had already patched. Update June 12th: While there w...

skimming

## Sports brand Puma infected with advanced malware

2019-04-29 On April 25th, sports brand Puma Australia got infected with the most sophisticated payment skimmer to date.

skimming

## 57 payment gateways from Germany to Brazil targeted

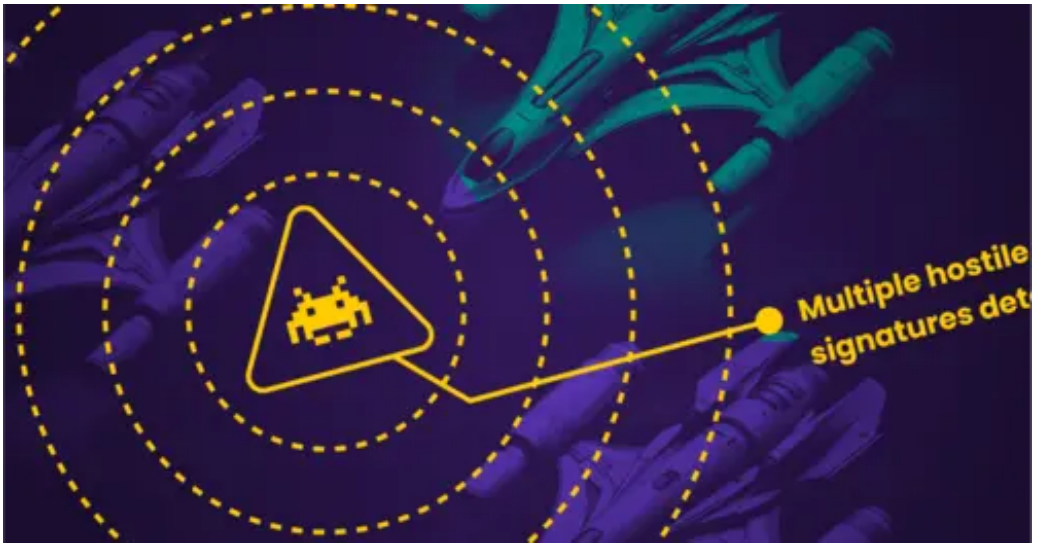
2019-04-29 Sansec discovered a polymorphic skimmer that works with 57 different payment gateways. It has global reach, affecting payment systems from Germany to Brazil. It is by far the most advanced skimmer to date. This skimmer consists of two components: a polymorphic loader, and a sophisticated exfiltra...

skimming


**Credit cards of Atlanta Hawks fans stolen**

2019-04-24 Online credit card thieves - also known as Magecart - have managed to inject a payment skimmer in the online store of the Atlanta Hawks. Fans who ordered merchandize on or after April 20th had their name, address and credit card stolen.

skimming




**Bad extensions now main source of Magento hacks: a solution!**

2019-01-29 In October last year I discovered several Magento extension 0days. As it turns out, this was only the tip of the iceberg: today, insecure 3rd party extensions are used to hack into thousands of stores. A group of Magento professionals have identified 63 vulnerable extensions, and are now releasin...

skimming

**Large sites hacked via Adminer database tool**

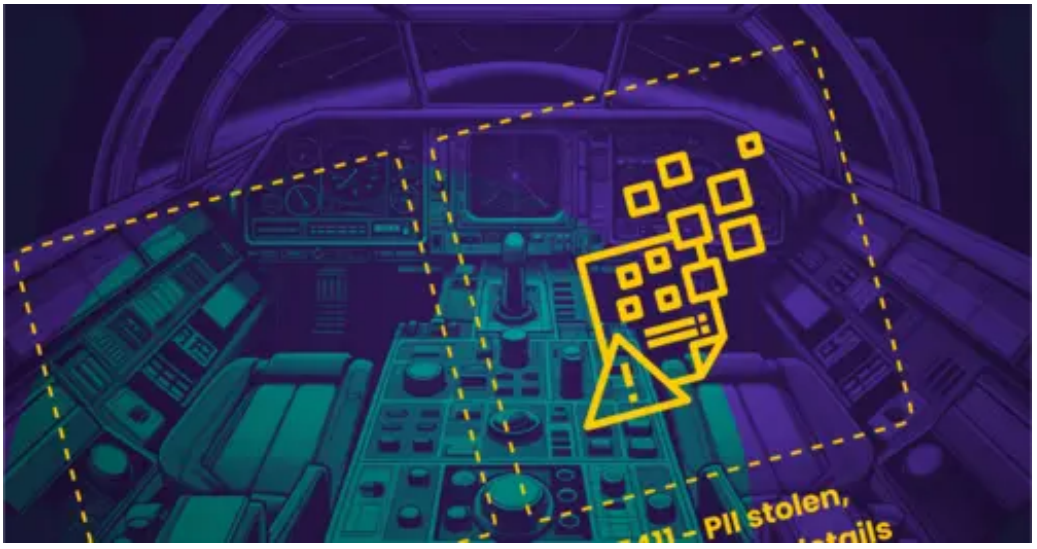
2019-01-20 This week I discovered that large ecommerce and government sites got hacked via the Adminer database tool. As it turns out, the root cause is a protocol flaw in MySQL. Curiously, it is described in the official documentation, that says: The transfer of the file from the client host to the server...

skimming

**PHP tool 'Adminer' leaks passwords**

2019-01-17 Update 2019-01-20: the root cause is a protocol flaw in MySQL. Adminer is a popular PHP tool to administer MySQL and PostgreSQL databases. However, it can be lured to disclose arbitrary files. Attackers can abuse that to fetch passwords for popular apps such as Magento and Wordpress, and gain con...

skimming




## Competing digital skimmers sabotage each other

2018-11-20 Skimmers found to subtly sabotage each others fraud operations. Competition is grim in the online skimming business (aka "MageCart"). The aggressive MagentoCore skimmer was previously observed to kick contending parasites from its victim hosts. But this week, we discovered that the bat...

skimming

## Merchants struggle with MageCart reinfections

2018-11-12 1 in 5 compromised merchants get reinfected, average skimming operation lasts 13 days MageCart, the notorious actors behind massive online card skimming, has been busy. And so have we: our crawlers are continuously tracking the raging battle between card thieves and merchants. It seems that the l...

skimming

**Backdoor found in Webgility**

2018-10-30 Update Nov 23rd: Webgility has released a patch and a public statement, urging all customers to upgrade to version 345. Update Nov 30th: Webgility has discovered another security issue and urges all customers to upgrade to version 346. The VC-funded Webgility software contains a backdoor for th...

skimming

**Unpublished security flaws (0days) massively exploited**

2018-10-23 Online credit card theft has been all over the news: criminals inject hidden card stealers on legitimate checkout pages. But how are they are able to inject anything in the first place? As it turns out, thieves are massively exploiting unpublished security flaws (aka 0days) in popular store exte...

skimming

**German political party store hacked before election**

2018-10-15 The store of German political party CSU (www.csu-shop.de) contains an identity skimmer that was planted on or before Oct 5th, right before the Bavarian election on Oct 14th. Personal identifyable information of customers gets sent to a remote server during the checkout process. Because the CSU s...

skimming

**MageCart: now with tripwire**

2018-10-04 Back in 2016, Magecart skimmers would evade detection by sleeping if any developer tools were found running. Then, their malware would 404 without correct Referer or User-Agent header. And now, Magecart sounds the alarm when it finds you snooping around, and collects a fingerprint of you on an e...

skimming

**ABS-CBN next in series of high profile breaches**

2018-09-18 While Filipinos are recovering from typhoon Mangkhut, another misfortune awaits them online. We found their broadcasting giant ABS-CBN − a $740 million conglomerate & top-500 global Internet destination − to be hacked. Criminals are running a payment skimmer on ABS-CBNs online store since at ...

skimming

**Is your Google Analytics code malicious?**

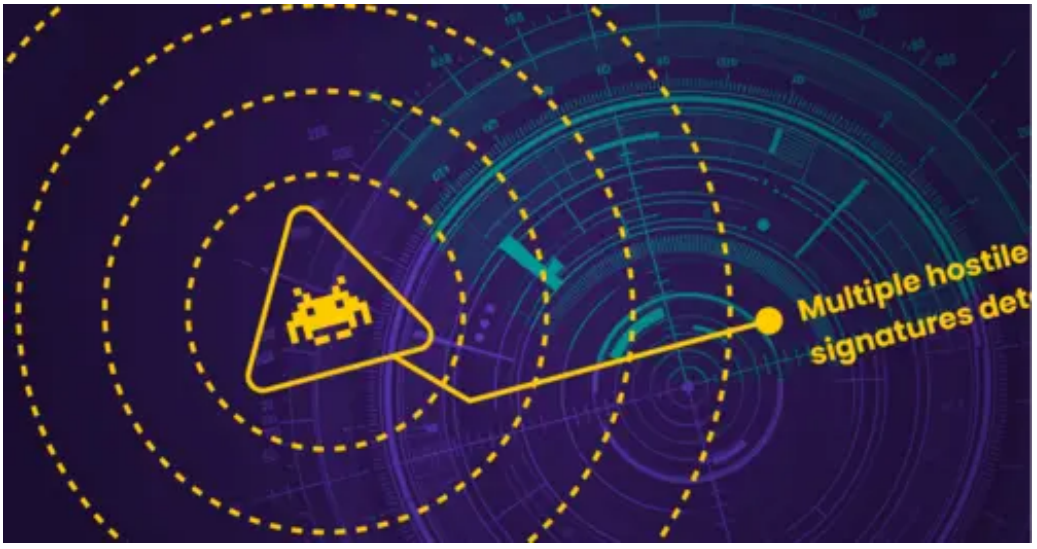
2018-09-06 Would you - a webdeveloper - get alarmed if you found the following code on your website? Probably not, as Google Analytics is embedded in pretty much every website these days: <script type="text/javascript"> (function() { var ga = document.createElement('script'); ga.ty...

skimming


## MagentoCore group hacks 7,339 stores and counting

2018-08-30 A single group is responsible for planting skimmers on 7339 individual stores in the last 6 months. The MagentoCore skimmer is now the most successful to date. Update 2018-09-07: Because Google Chrome has added the campaign to its blocklist last Saturday, the skimmers are now rapidly replacing &q...

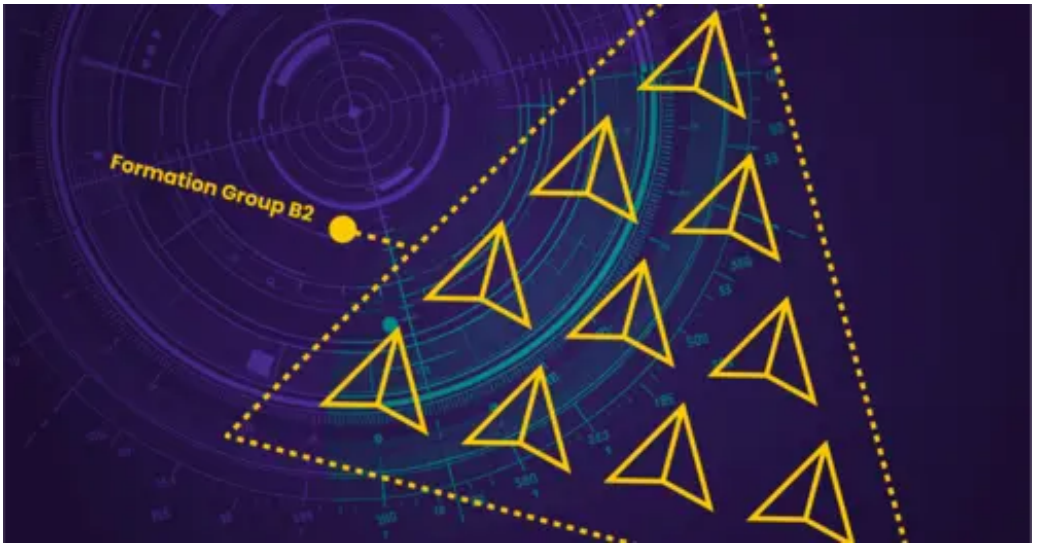
skimming MagentoCore skimmer




## Hackers breached Magento through helpdesk

2017-12-28 Magento merchants have recently received messages like this: Hey, I strongly recommend you to make a redesign! Please contact me if you need a good designer! -- knockers@yahoo.com Upon closer examination, the message contains a specially crafted sender that contains an XSS attack: an attempt to...

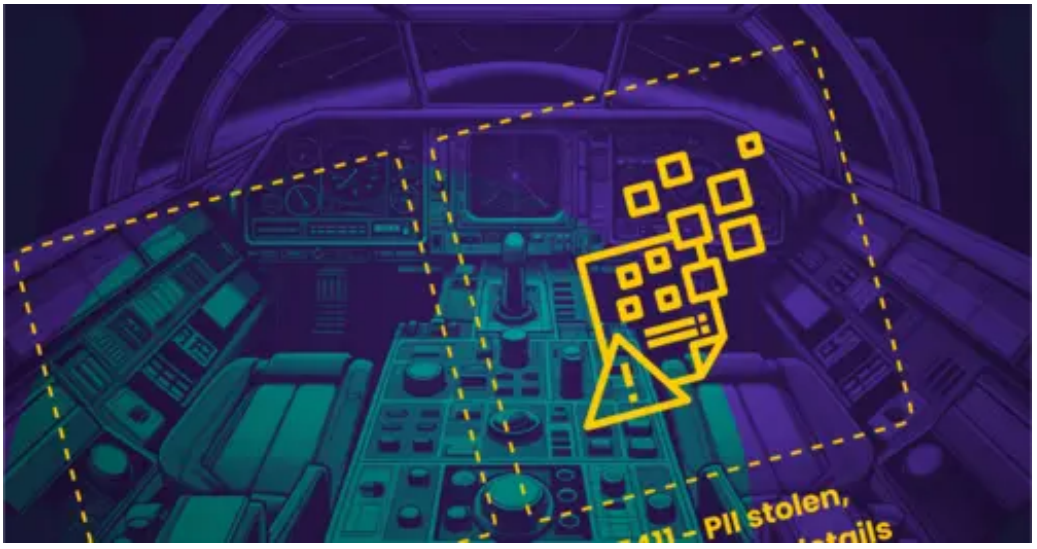
skimming




## Cryptojacking found on 2496 online stores

2017-11-07 Does your laptop get hot when visiting your favorite shop? You computer is likely mining cryptocurrencies to the benefit of a cyberthief. Cryptojacking - running crypto mining software in the browser of unsuspecting visitors - is quickly spreading around the web. And the landgrab extends to onli...

skimming




## Why ordering HTTP headers is important

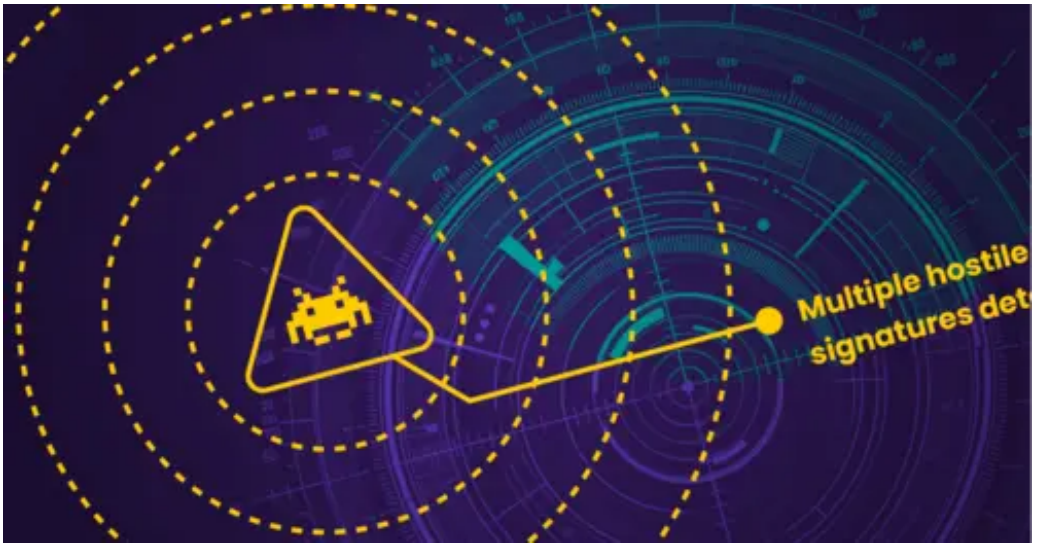
2017-05-02 If you code against Akamai hosted sites, you could be rejected because your HTTP library sends request headers in the wrong order. In fact, most libraries use undefined order, as the IETF specification says it doesn't matter. In casu: $ URL=http://www.bulgari.com $ UA="User-Agent: Mozilla/5....

skimming


## Warning: fake Magento patch 9789 contains virus

2017-04-21 Update May 21st: a similar phishing mail circulates about a fake patch SUPEE-1798. Update Apr 22nd: added reference to Neutrino Bot and POS systems This week a mail was sent out to announce the new Magento patch SUPEE-9789. It is fake and it contains malware. There is no patch 9789. The message...

skimming




## A Magento breach analysis: part 1

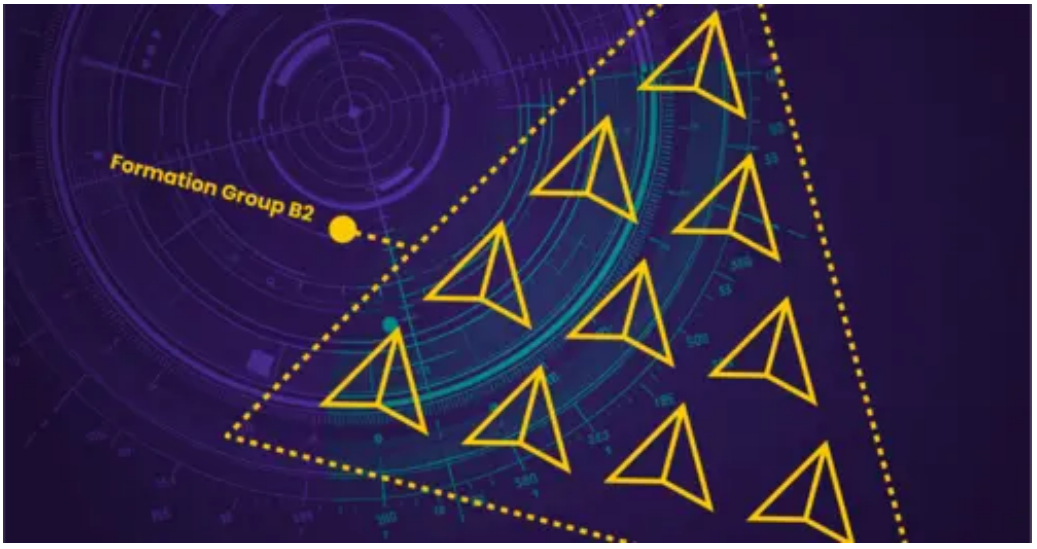
2017-04-12 Part of a series where Magento security professionals share their case notes, so that we can ultimately distill a set of best practices, tools and workflow. Part of the job of running the MageReport service is that I get to investigate tons of hacked stores. About 50-200 new stores get hacked pe...

skimming

## An OpenCart/Magento hacking dashboard

2017-04-07 This post shows how sophisticated Magento hacking operations have become nowadays. While investigating a bruteforced Magento store, we noticed that the hacker logged in using a curious referrer site: "GET /rss/catalog/notifystock/ HTTP/1.1" 200 5676 "http://194.87.232.147:777/"...

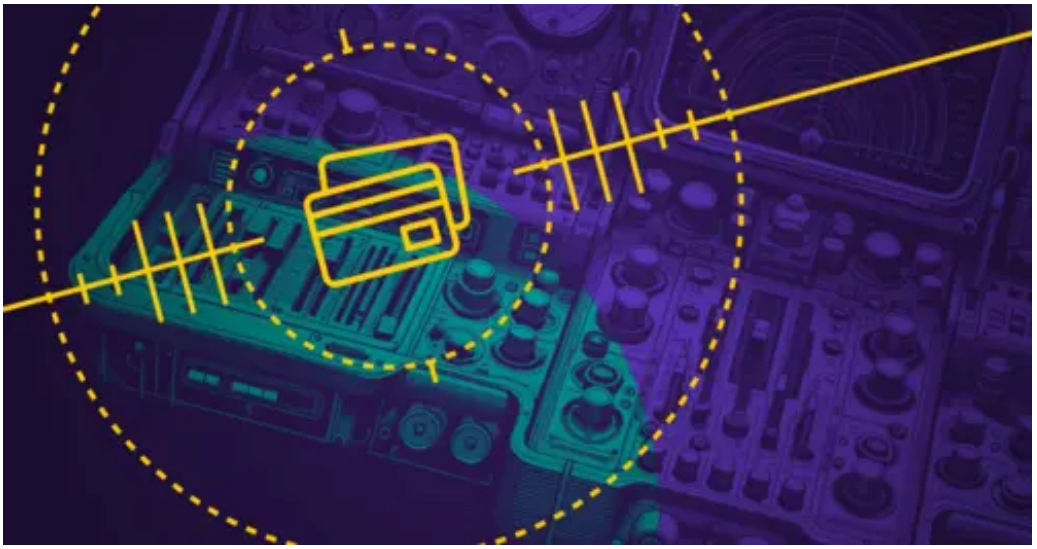
skimming




## Self-healing malware restores itself after deletion

2017-02-14 Regular Javascript-based malware is normally injected in the static header or footer HTML definitions in the database. Cleaning these records used to be sufficient to get rid of the malware. But not anymore: this week a new malware pattern surfaced. Once deleted, it uses a clever database trigge...

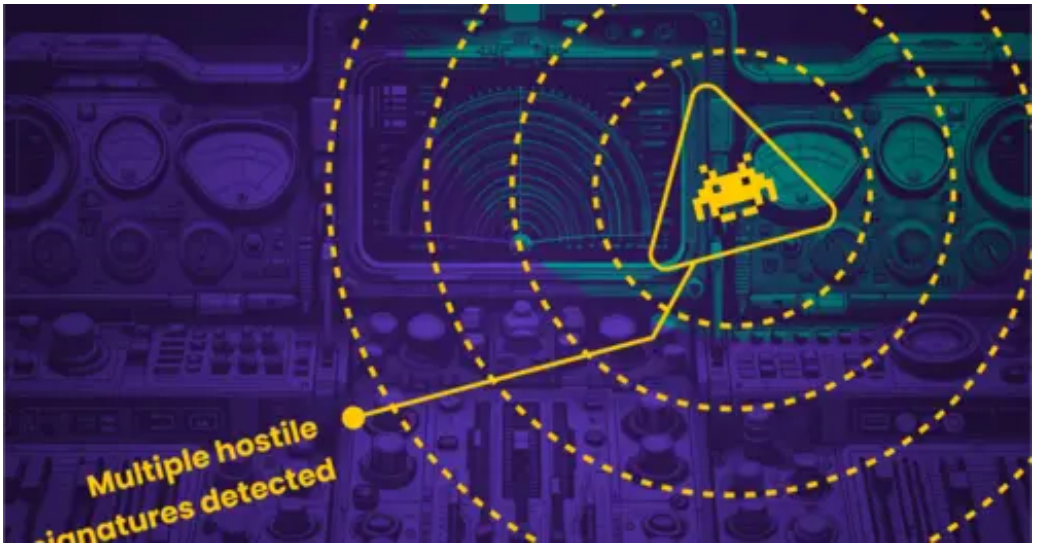
skimming



**Visbot malware found on 6691 stores [analysis]**

2016-12-01 Visbot is one of the oldest Magecart payment skimmers: it steals customer data and credit cards. The first case was documented as early as March 2015. But being publicly discussed did not stop it from spreading. We conducted a global research into 300.000 Magento stores and found active Visbot i...

skimming




**Criminals have rewired 3,500 online stores**

2015-11-17 Criminals have secretly rewired 3,500 online stores to continuously harvest credit card numbers. The fraud can be traced back as far as May 12th 2015, so if you have bought something at one of these stores in the last 6 months, your credit card is likely compromised. We received reports of suspic...

skimming

Source: https://sansec.io/labs/2020/01/25/magecart-hackers-arrested/