ECOMMERCE SECURITY

A YEAR IN REVIEW 2024

ABOUT TURACO LABS

We are an independent cybersecurity specialist technology focused on keeping eCommerce websites secure.

Our team has nearly two decades of forensic investigation expertise and experience in assisting hacked eCommerce websites, which has formed the basis of our solution, ThreatView.

ThreatView is the world's most comprehensive eCommerce security solution, keeping online businesses safe while enabling them to remain PCI DSS Compliant.

WHAT IS THREATVIEW?

ThreatView is an advanced cybersecurity solution designed to detect, monitor, and respond to eCommerce threats in real-time.

ThreatView is our comprehensive eCommerce Threat Defence Technology, providing real-time threat detection and protection to websites worldwide. ThreatView Advanced takes care of a few of the more challenging PCI DSS requirements, simplifying the challenge of maintaining PCI DSS compliance for businesses. In addition, ThreatView Advanced comes with an industry-first $10,000 Breach Protection Warranty.

Our Mission

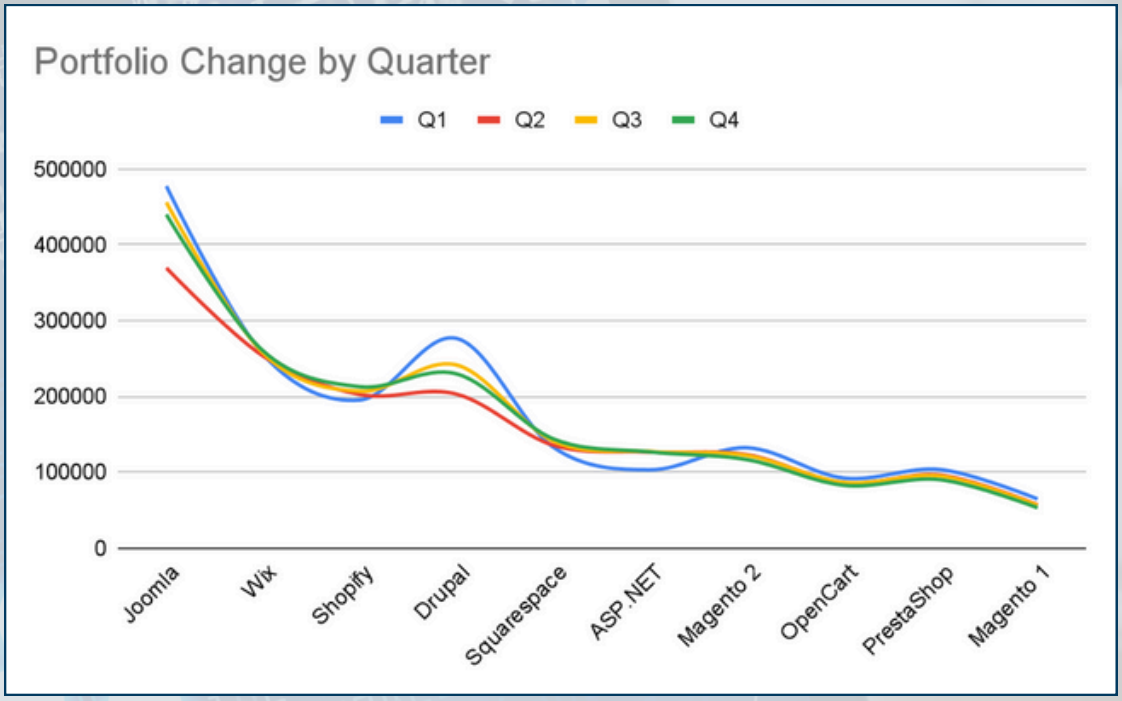
Our mission is to protect online businesses from cyber criminals.

2024 PORTFOLIO MONITORING SUMMARY

1. Fortnightly security assessment across over 16m websites.
2. **WordPress** remains the most prevalent platform.
3. **WordPress, Magento 2 (Adobe Commerce) and Magento 1** remain the most targeted platforms for PII and Payment Data theft.
4. Surprise inclusion within top 5 targeted platform: Shopify.

TOP 10 PLATFORMS

Our dataset: Over 16m websites globally. WordPress makes up a significant proportion of the market (over 50%), therefore we have excluded it from this chart to make the data easier to read - and we've included Magento 1 due to its significance further down the report:

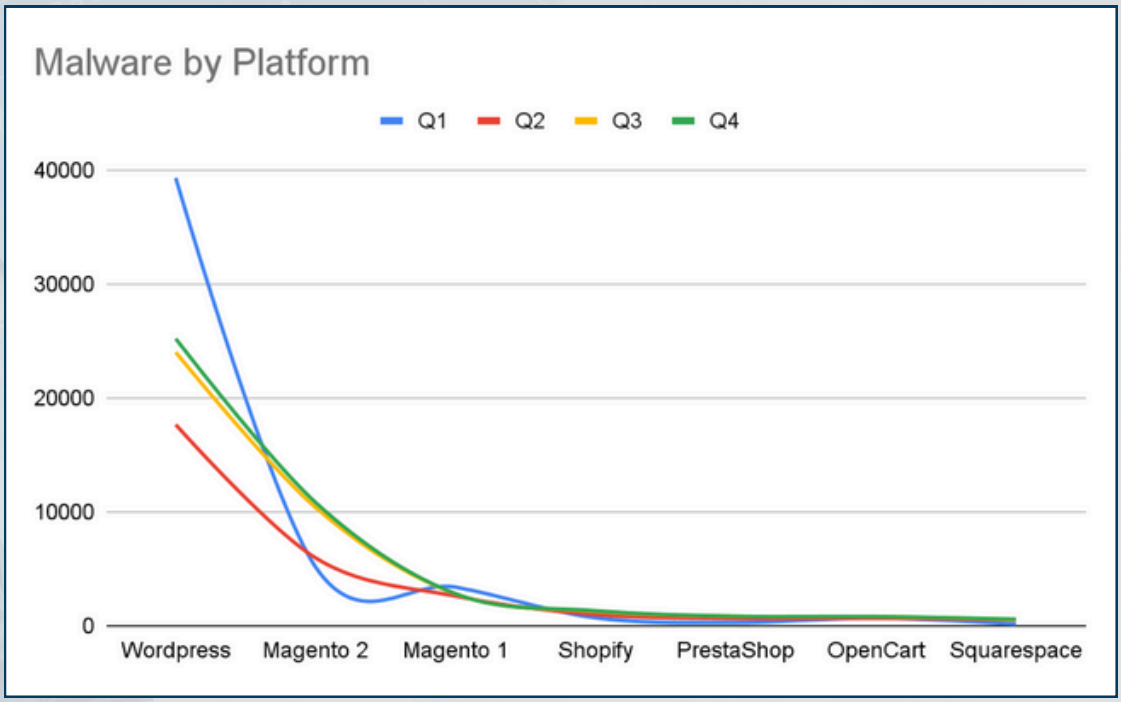


Interestingly we've seen a slight decrease in Q1 2025 for a couple of the platforms. Of particular interest the is number of Magento 1 sites that still exist - a technology that was "End of Lifed" years ago. When correlated with our threat stats, Magento 1 features highly as one of the most targeted platforms in the eCommerce sector. Perhaps due to this long tail of websites still operating on the obsolete and relatively insecure platform.

TOP 7 PLATFORMS BY COMPROMISED SITE COUNT

WordPress remains the most compromised platform in our portfolio, which is unsurprising given that well over 50% of our portfolio is made up of WordPress sites. Of interest are the Magento 1 and Magento 2 / Adobe Commerce findings - Adobe Commerce / Magento 2 has seen a steady increase in data compromises through the year, while Magento 1 seems to present consistent results in the 2,500-3,400 range throughout the year.

Shopify is attracting more criminal attention and is now a consistent contender in the top 5 most targeted platforms.



MALWARE PREVALENCE

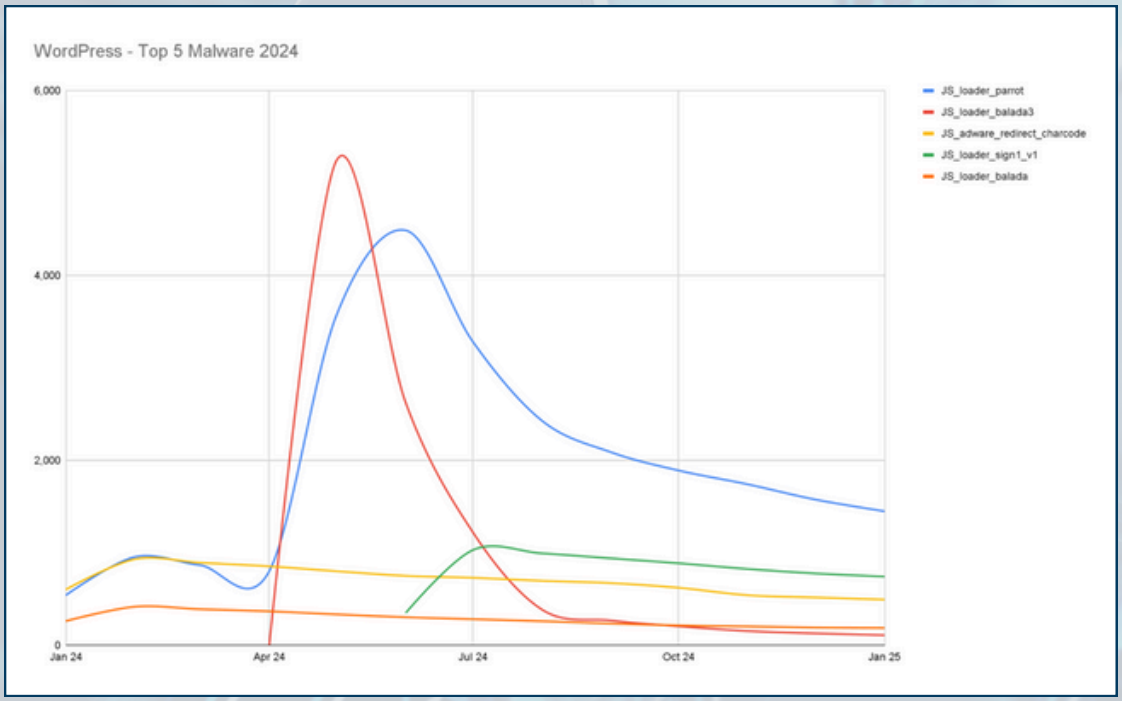
We've seen an exceptional year in the growth of malware targeting the Top 7 platforms. To distill the data further, we are going to focus on card harvesting malware targeting the Top 3 most targeted platforms: WordPress, Magento 2 and Magento 1.

WORDPRESS

We detected a couple of significant surges in WordPress sites infections through the year, with the following malware being the most prevalent:

- JS_loader_parrot with nearly 4,500 hacked sites detected in June 2024 (~1,500 currently still compromised with this malware).
- JS_loader_balada with nearly 5,250 hacked sites detected in May 2024.This infection has decreased down to just over 100 sites now.
- JS_loader_sign1_v1 infected over 1,000 sites in July 2024.
- JS_loader_socgholish appears to be on the rise, emerging in August 2024 and currently with nearly 700 sites infected.

Here's a graphical representation of the Top 5 by sheer volume of detections aggregated through the year:



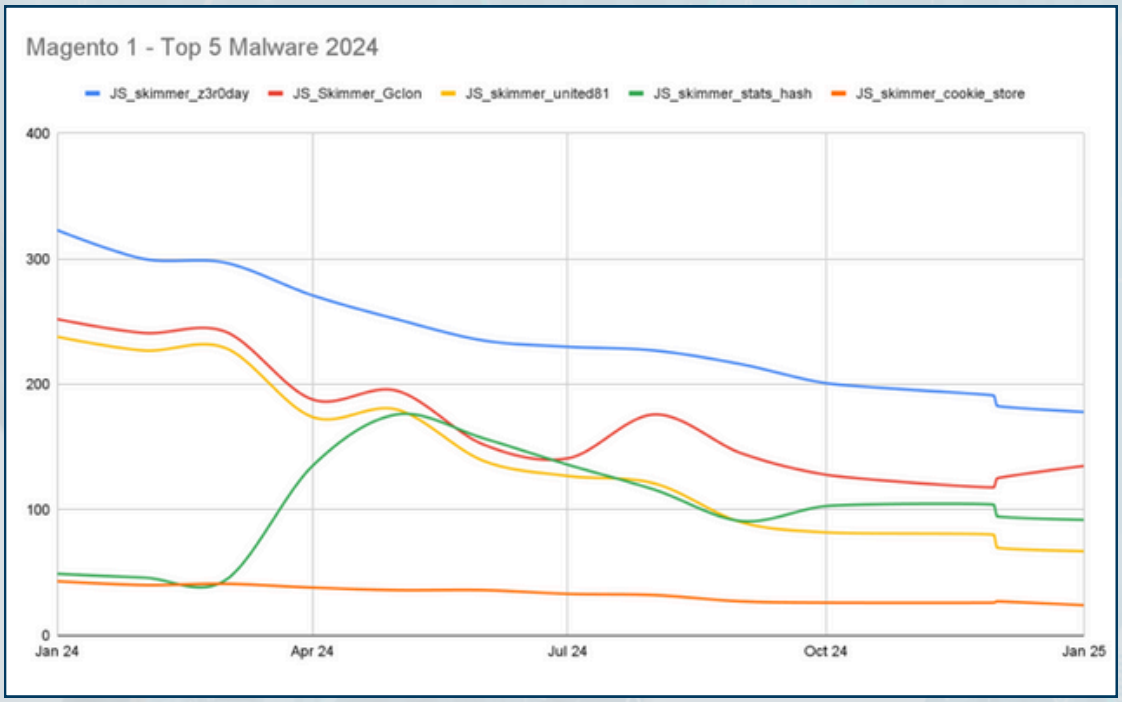
The numbers of Magento 1 sites appear to have stabilised at around 52,000 worldwide.In terms of our portfolio, Magento 1 sites no longer feature in our Top 10 by count; however, it consistently features in the Top 3 most targeted platforms and has done so for the last couple of years. Put simply, criminals are targeting this platform.

Having said that, 2024 has seen a slow and gradual decline in infected Magento 1 sites.

The top 3 malware targeting Magento 1 sites through the year are:

- JS_skimmer_z3r0day peaked at 323 infected sites in January 2024 (178 at present).
- JS_Skimmer_Gclon peaked at 252 infected sites in January 2024 (135 at present).
- JS_skimmer_united81peaked in May with 176 sites infected (92 at resent).

Here's a graphical representation:



ADOBE COMMERCE / MAGENTO 2

There are around 115,000 Adobe Commerce / Magento 2 sites in our portfolio, which just gets it into our top 10 platforms within our portfolio.However, the number of infected Magento 2 / Adobe Commerce sites puts it second behind WordPress sites.

Criminals are actively targeting this platform - our opinion is that this is happening because the size and type of business using this platform tend to be larger, growing quickly and requiring more capability from their eCommerce platform. But, with the added power and options, comes a larger attack surface and a requirement to run the eCommerce operation securely. Security should be an important part of day-to-day business in these organisations as they present a lucrative target for criminals.

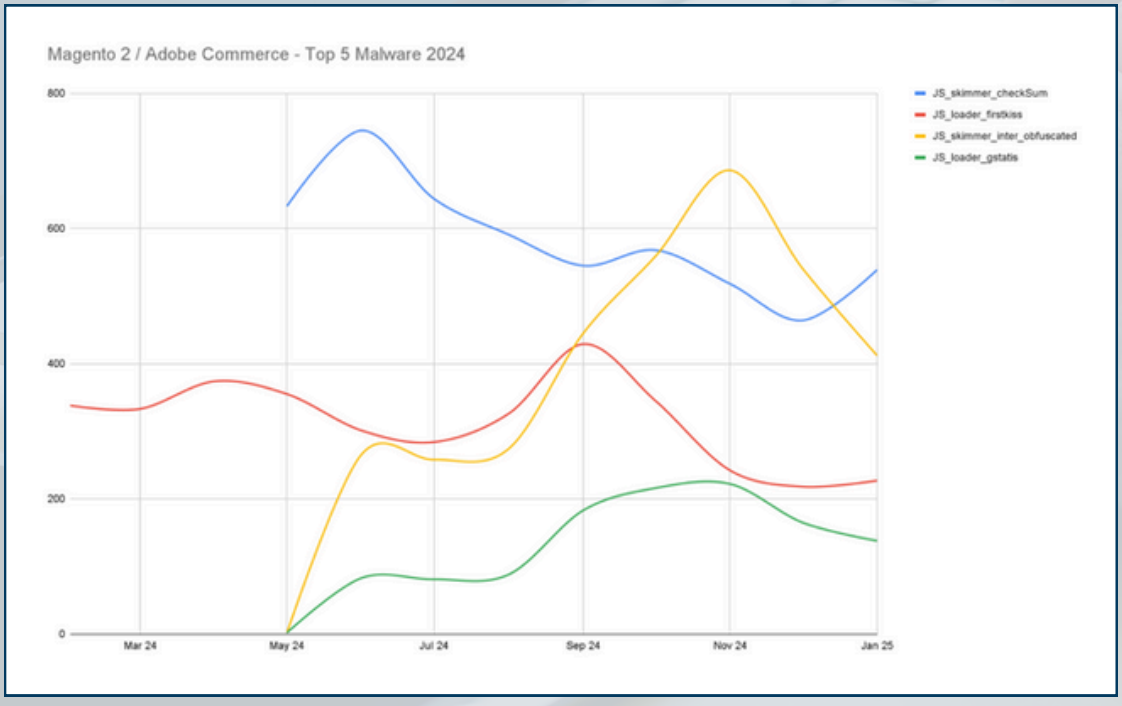
The 2024 story for Magento 2 / Adobe Commerce sites is one of increasing threat and infection.

The top 3 malware infecting this platform through 2024 were:

- JS_skimmer_checkSum first detected in April 2024, peaked in May with 745 sites infected (674 infected at present).
- JS_loader_firstkiss peaked in August 2024 with 429 sites infected (178 currently infected).
- JS_skimmer_inter_obfuscated first detected in April 2024, peaked in October 2024 with 686 sites infected (437 currently infected).

Of interest is JS_loader_statnestt, which was first detected inAugust 2024 with 431 sites infected, zero detected in September-November and the 437 infected sites in December 2024.

Here's a graphical representation:

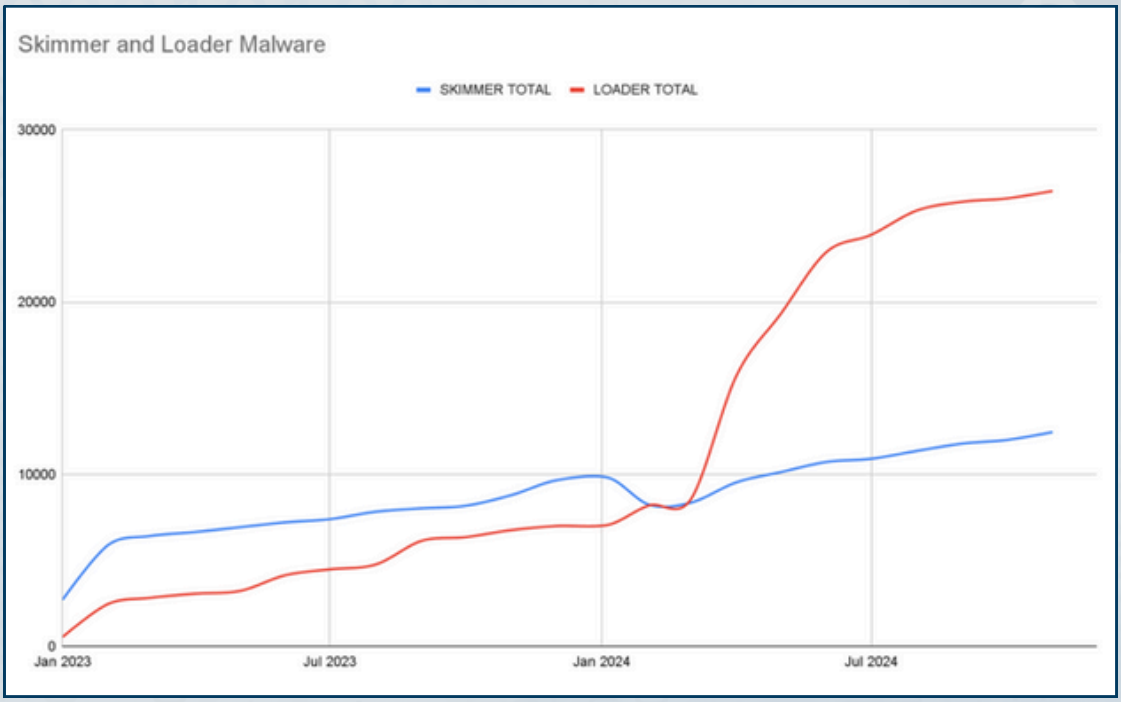


The most notable change in the types of malware over the last 12 months has been the emergence of a more stealthy approach to stealing payment data from eCommerce sites.

Going back through the last 8 years, we saw the emergence of Digital Skimmers (anyone remember the British Airways breach in 2018?). Over the last 8 years the industry has (broadly speaking) become quite good at detecting Digital Skimmers, pressuring criminals to change their tactic in order to profit off vulnerable sites.

What we saw was the evolution of Loader Malware, essentially the first stage of a two stage attack on vulnerable eCommerce websites. The Loader Malware instructs a website visitor's browser to load code from elsewhere - which is, in fact, usually a Digital Skimmer.A neat and simple adjustment to their tactics which evades detection by most security solutions.

Here's a graphical perspective showing the moment that Digital Loaders became more prevalent than Digital Skimmers in 2024:



OUR INSIGHTS

The eCommerce ThreatScape is constantly evolving and the criminals are adapting to our capability to defend eCommerce sites. The change in types of malware being detected (Loaders vs Skimmers) clearly highlights how the criminals are adapting their attack to steal data.

We've seen a record number of hacked sites in the last 12 months, a strong indicator that the eCommerce sector is easily the most targeted within the payment card industry.

The good news is that with a few key steps/controls, the risk of cybercrime on an eCommerce website can be dramatically reduced.

These are the top 3 steps an eCommerce site can take to significantly reduce risk:

1. Implement 2FA for ALL Admin accounts using Google Authenticator or similar.
2. Patch your software, quickly.
3. Monitor your site for threats.

We cannot help you with 2FA or Patching, but we can help you with Monitoring for Threats.
We provide one of the industry's best threat detection solutions - ThreatView - which can also take care of some of the more onerous PCI DSS requirements too.

GET FREE ACCESS TO THREATVIEW HERE

CONTACT US

We hope you have found the report useful. Now it's your turn to take action.

Go and get a ThreatView Community account and monitor your website for **free** on:
www.turacolabs.com/scan

If you have questions, queries or feedback please get in touch.

We'd love to hear from you.
Call us or send us an email at hello@turacolabs.com

CHECK YOUR SITE NOW

Over 16 million sites analysed each month for the latest cyber threats targeting eCommerce sites.

HOW CAN YOU GET PROACTIVE?

STEP 1: Understand your website's current risk status.
STEP 2: Take action to mitigate the risks (see our blog for simple steps to secure your online business).
STEP 3: Monitor for threats. Keep secure while the threatscape evolves.

You can easily check if your business is one of the many hacked sites detected. You will need to create a FREE account with ThreatView, then run a scan using latest Threat IOCs.

It takes 2 minutes and is completely free - no credit card required.

www.turacolabs.com/scan

SIMPLIFYING ECOMMERCE SECURITY

16+MILLION SITES MONITORED

ECOMMERCE CYBER SECURITY SPECIALISTS

THREAT INTEL FOR THE INDUSTRY

Turaco Labs Ltd
31a Charnham Street, Hungerford
Berkshire, RG17 0EJ, United Kingdom

hello@turacolabs.com