ECOMMERCE THREATSCAPE:

OCTOBER 2024

ThreatView
BY TURACO LABS

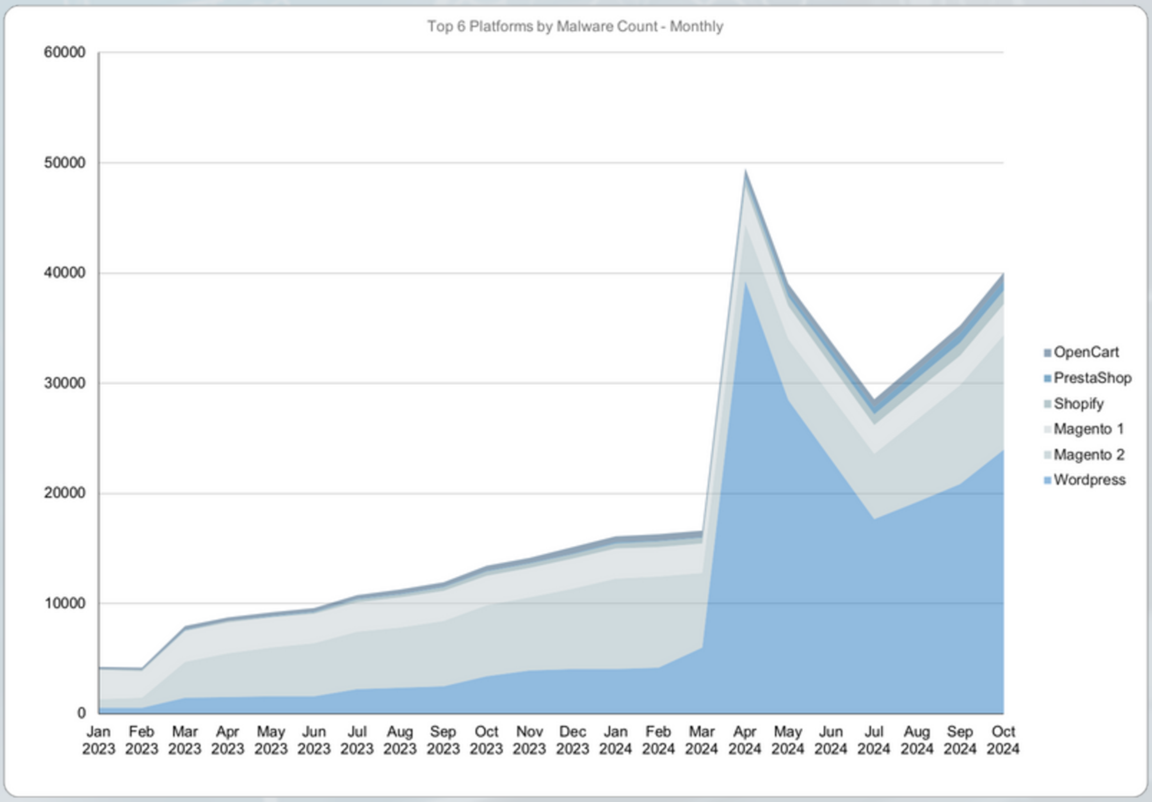
PORTFOLIO OVERVIEW

Portfolio: 16m+ websites

Our portfolio has built up over nearly a decade of providing free website security assessments and consists of predominantly eCommerce websites.

The portfolio is assessed every fortnight using the latest threat intel, combined with a threat database from nearly 15 years of eCommerce forensic investigations.

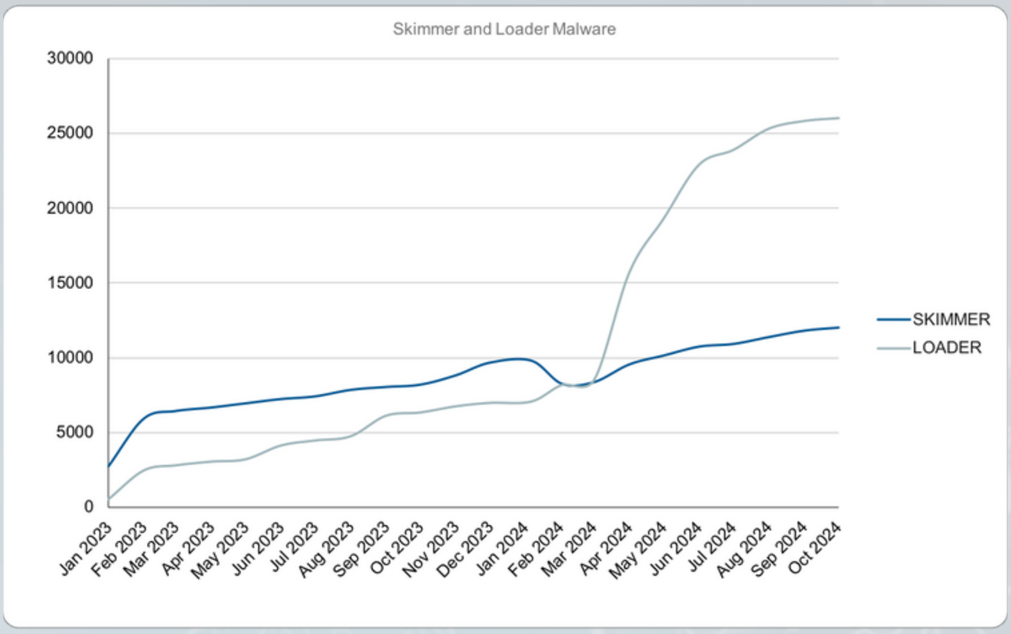
TOP 6 TARGETED PLATFORMS



Targeted Platforms

These Top 6 eCommerce platforms account for **89.9%** of the malware detected this quarter.

DIGITAL SKIMMERS & LOADERS

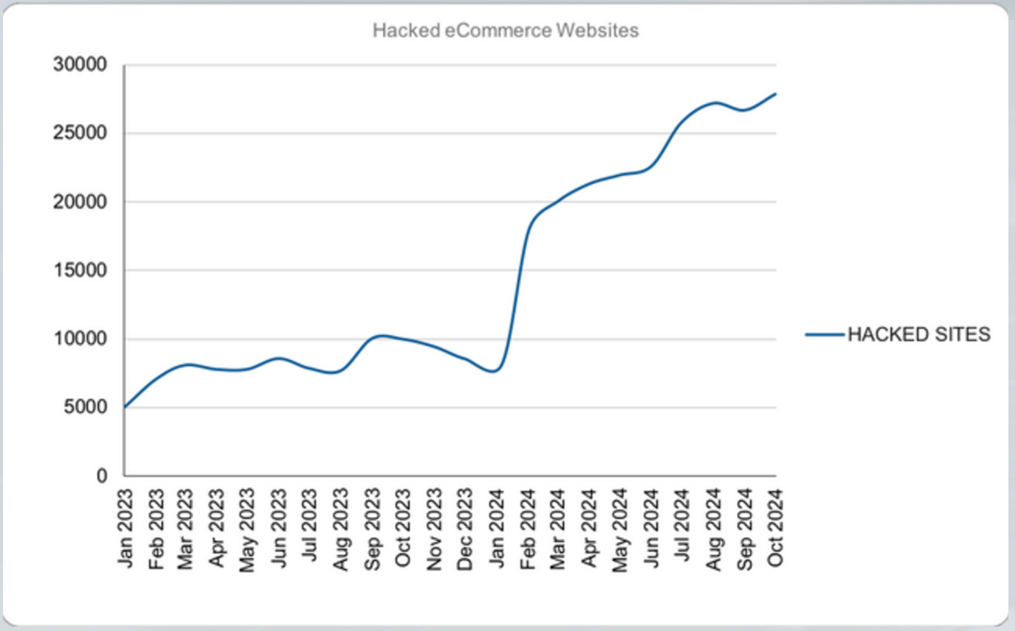


OCTOBER HACKED SITES

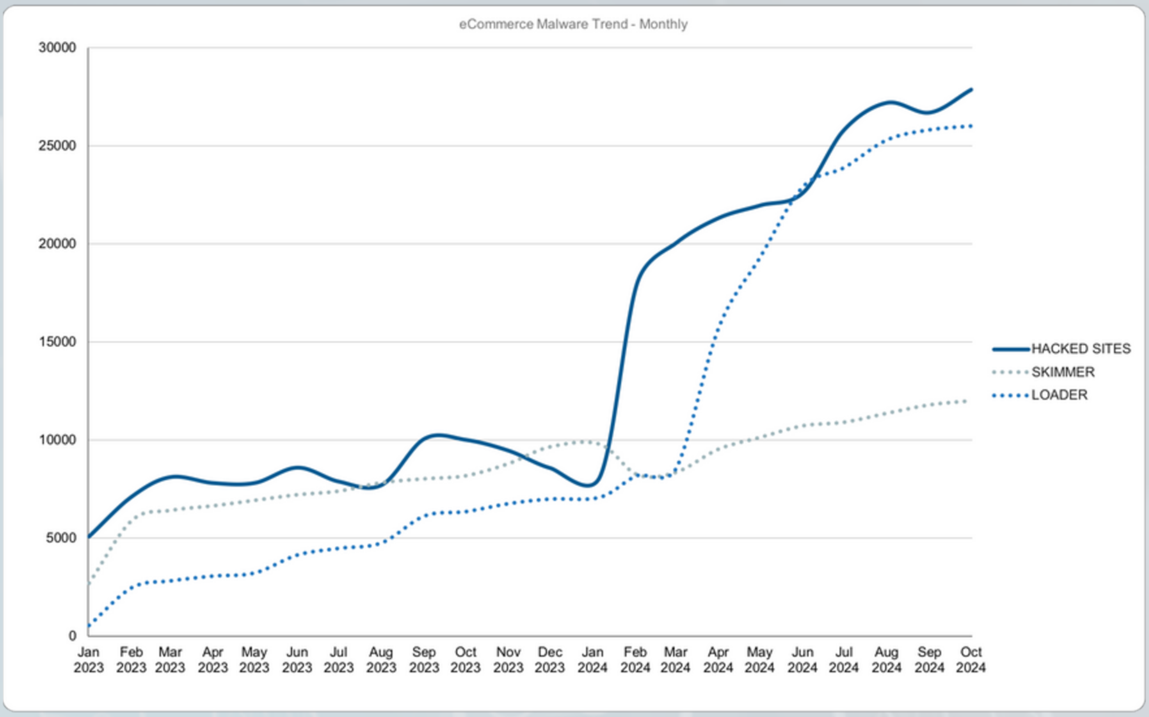
27,884

Notable Observations

- Loader malware on victim websites is now much more prevalent than skimmers.
- Digital skimmers are still part of the attack chain, but being used WITH loaders in more complex multi-stage attacks.



MALWARE ANALYSIS



Significant growth in hacked sites:

- Portfolio growth.
- Adapting threatscape making it challenging to detect criminals.

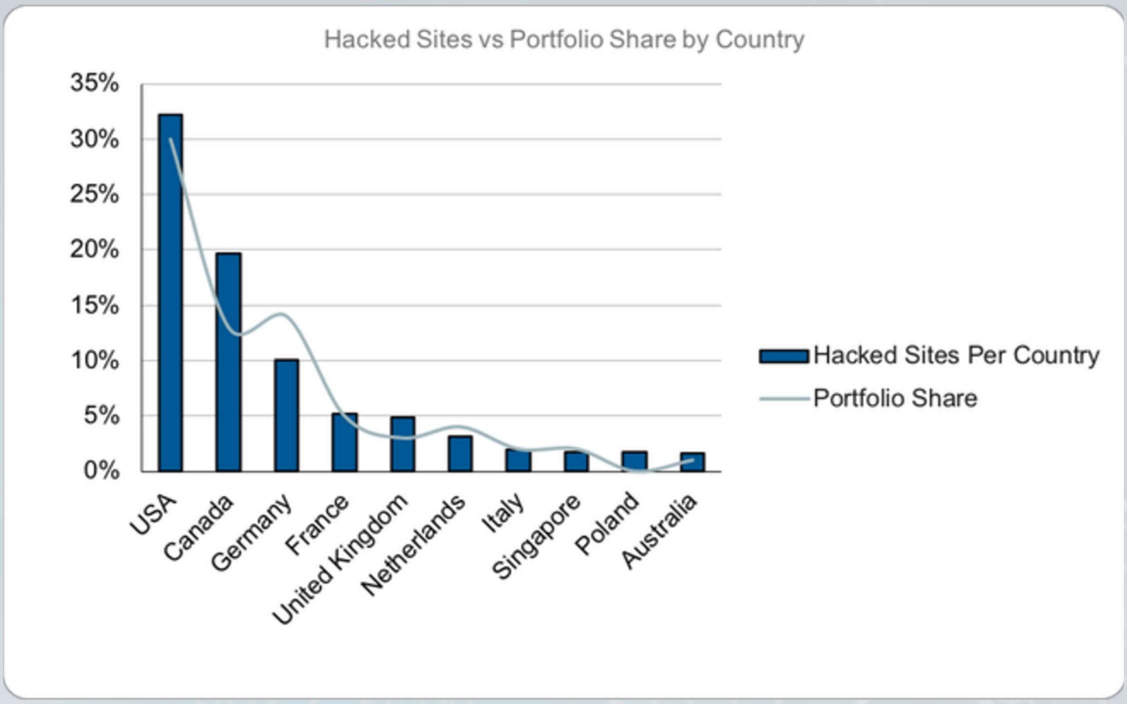
*NB. Many sites are infected with multiple types of malware.

TOP 5 ACCOUNT FOR 70% OF ALL LOADERS DETECTED

MALWARE RULE (LOADERS)	AFFECTED PLATFORMS
JS_loader_parrot	Wordpress, Joomla, Drupal, Magento 1, Magento 2, OpenCart
JS_loader_firstkiss	Magento 2, BigCommerce, Magento 1
JS_loader_injector_google_ads	Wordpress, Magento 2, OpenCart, Magento 1,Joomla.
JS_loader_cloudsonicwave	Wordpress, PHP.
JS_loader_kritec	Magento 2, Wordpress, Prestashop, OpenCart, Magento 1, OpenMage.

MALWARE RULE SKIMMERS)	AFFECTED PLATFORMS
JS_skimmer_z3r0day	Magento 1, Magento 2, Wordpress, Squarespace
JS_Skimmer_Gclon	Magento 1, Magento 2
JS_skimmer_united81	Magento 1, Magento 2, Wordpress, Drupal
JS_skimmer_dedwards_packed	Wordpress, OpenCart, Magento 1, Magento 2, Joomla
JS_skimmer_google_ads	Wordpress, OpenCart, Magento 1, Magento 2

TOP 10 TARGETED COUNTRIES



Top 5 Countries with most breached websites:

US, Canada, Germany, France, United Kingdom.

Why are these sites being hacked?

Criminals target the websites easiest to hack. The vast majority of hacked sites share the same characteristics:

- Out of date software
- Basic security errors (exposed Admin login)
- Limited/no proactive security measures

Most common denominator:
lack of cybersecurity awareness/skills.

Check your eCommerce site now.

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 the latest Threat IOCs.

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

www.turacolabs.com/scan

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