



**FOREGENIX**

**ECOMMERCE THREATSCAPE**

**APRIL 2023**

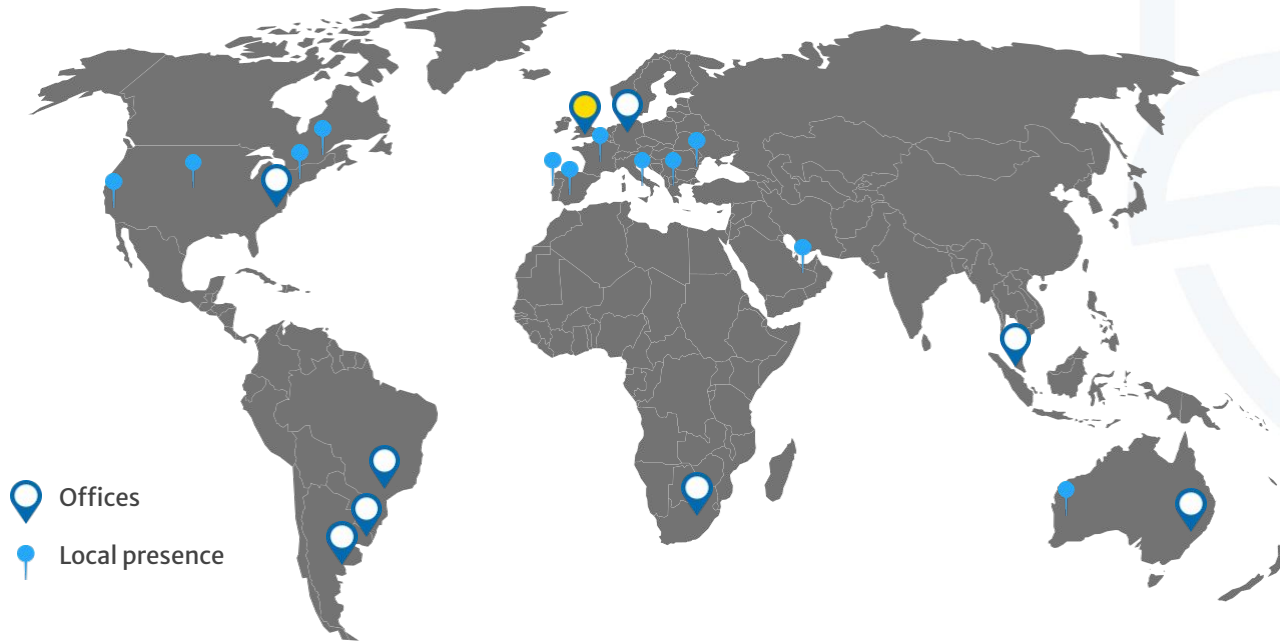
# INTRODUCTION



THE QUEEN'S AWARDS  
FOR ENTERPRISE:  
INTERNATIONAL TRADE  
2019

- Cyber security business, strong focus within “payments”
- Specialist, global business / ~95 Global Employees
- Queen’s Award for Enterprise 2019
- Privately held, profitable & self-funded
- Founded in 2009

# GLOBAL PRESENCE



## Offices

- Australia
- Brazil
- Germany
- Singapore
- South Africa
- United Kingdom (HQ)
- Uruguay
- USA

**12+**  
**Languages**

**20+**  
**Countries**

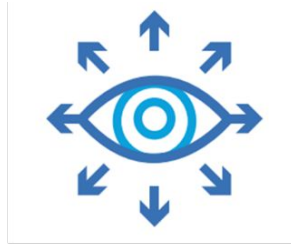
**1,000s of**  
**Satisfied Clients**

# EXECUTIVE SUMMARY

## April 2023 eCommerce Threatscape



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

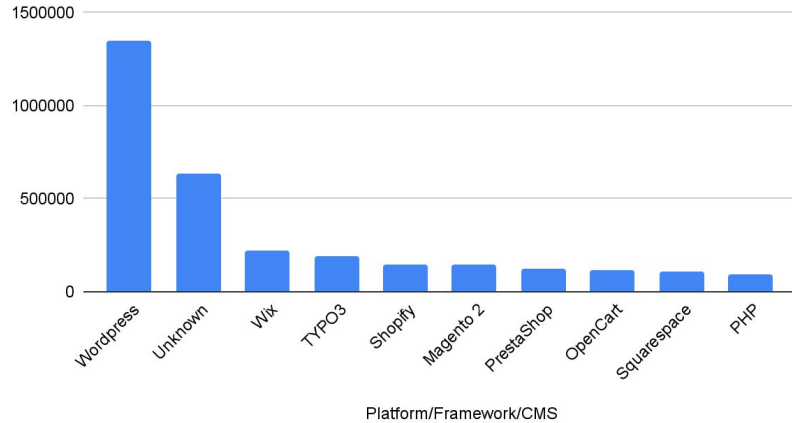


intel feeds directly into our ThreatView solution to monitor the global eCommerce Threatscape

# PORTFOLIO OVERVIEW

**Portfolio: 12.4m+ websites**

Top 10 Platform Distribution



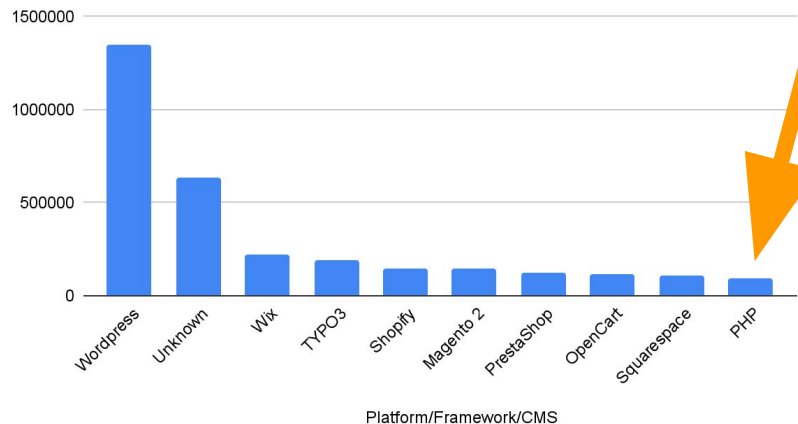
Our portfolio has built up over nearly a decade of providing free website security assessments and consists of predominantly eCommerce websites.

The portfolio is assessed every fortnight using the latest threat intel, combined with a threat database from nearly 14 years of eCommerce forensic investigations.

# PORTFOLIO OVERVIEW

## Notable Notes: Magento 1 drops off Top 10

Top 10 Platform Distribution



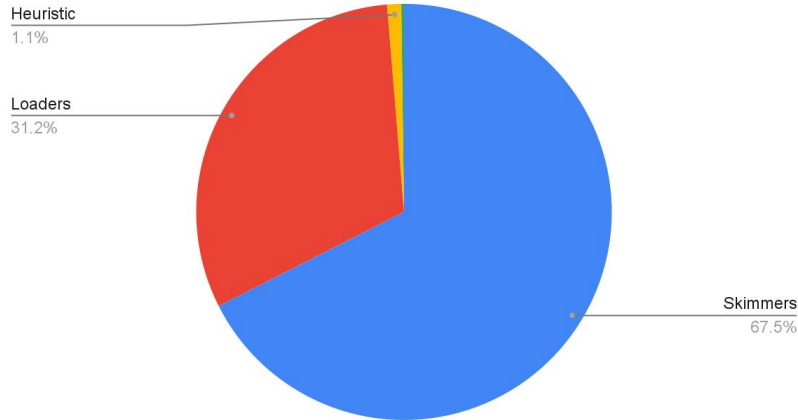
For the first time since we started monitoring eCommerce websites for threats, Magento 1 has dropped out of the Top 10 Platforms.

It does however, retain it's position as the most targeted-by-criminals and compromised eCommerce platform. No surprises there, since it was officially "End of life'd" in June 2020.

# HACKED ONLINE BUSINESSES

Hacked Sites: 7,801

Malware Types



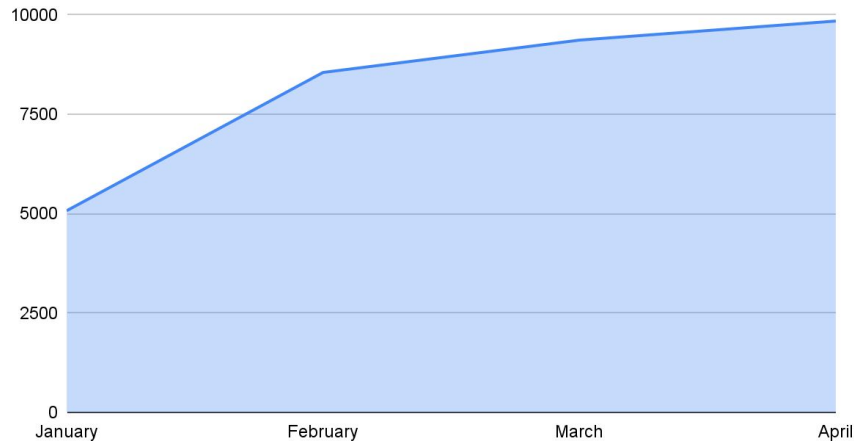
These are websites with:

- Card skimmers stealing payment data
- “Loaders” that load malware from malicious domains to skim/steal payment data
- Heavily obfuscated files that trigger heuristic detection rules for card harvesting malware.

# ALERT: MALWARE DETECTIONS GROWTH

Increase in Malware detected: 94% since Jan 2023

Malware Detections By Month



Significant increase in Malware since Jan 2023:

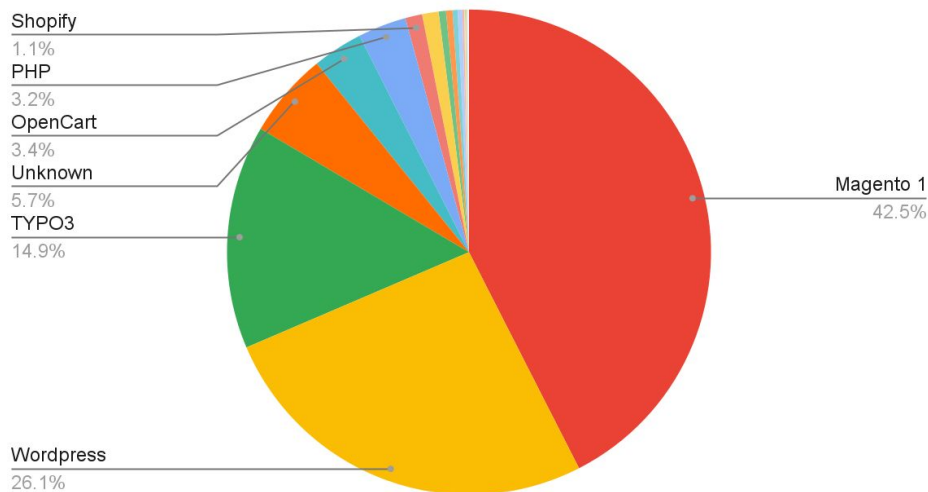
- 7,801 sites compromised (down from 8,104 last month)
- Wider deployment of older “Magecart variant” malware.
- Increase mainly due to 3 existing, older skimmers/malware variants.

NB: Many sites have infections with multiple types of malware. “Riddled” with malware.



# TARGETED PLATFORMS

Top 10 Most Targeted Platforms



## Targeted Platforms

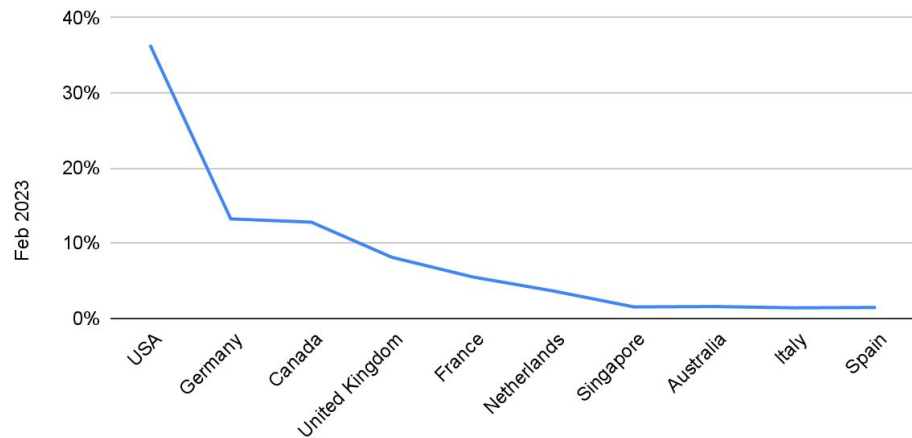
Top 5 Compromised Platforms:

1. Magento 2 (2.79%)
2. Magento 1 (3.32%)
3. Wordpress (0.11%)
4. TYPO3 (0.3%)
5. OpenCart (0.28%)

The figure in brackets is the percentage of the merchants using that platform that are compromised. This adds further context to the risk associated with each platform.

# TOP 10 TARGETED COUNTRIES

Top 10 Targeted Countries



Top 10 Targeted Countries

## Targeted Countries

Top 5 Countries with most breached websites:

1. US
2. Germany
3. Canada
4. United Kingdom
5. France

**NB: These websites are compromised predominantly with Payment Card Harvesting Malware**

# HIGH RISK WEBSITES

**High Risk Sites: 2.35%**

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.

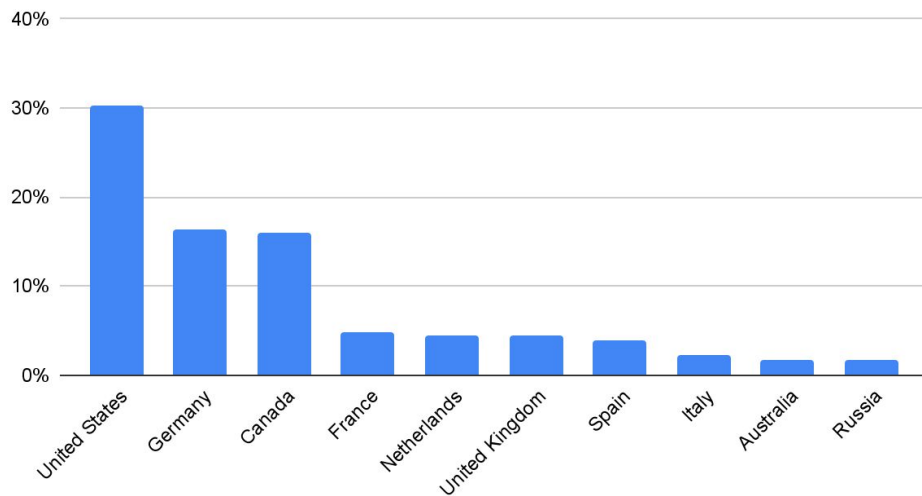
# MALWARE: LOADERS/SKIMMERS

## Additional Info:

- Nearly 8,000 instances of “Loader” and “Skimmer” malware code detected worldwide.
- Over 90% of the detections were targeting the Magento 1 and Magento 2 platforms.
- 12,832 heuristic detections (looks, smells and feels like malware, but cannot determine further without deep manual analysis).
- Most heuristic detections on Wordpress platform (nearly  $\frac{1}{3}$ ).

# MALICIOUS DOMAIN SOURCES

Top 10 Countries Serving Up Malware



## Serving up Malware

### Top 5 Countries serving up Card Harvesting Malware:

1. US
2. Germany
3. Canada
4. France\*
5. Netherlands

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

**\*France** regains 4th position, UK pushed into 6th.

# FOREGENIX MAGENTO UPDATE

## Magento (Adobe Commerce).

Magento 1 was “end of lifed” in June 2020. As the most targeted platform by criminals over the last 4-5 years, we keep a close watch on the Magento Threatscape. Here are the migration stats:

Platform	April 2021	April 2022	April 2023
Magento 1	137,521	94,739	87,799
Magento 2	102,009	104,110	142,616

# WHY ARE THESE SITES BEING HACKED?

**Criminals target the websites easiest to hack.**

The vast majority of hacked sites share the same characteristics:

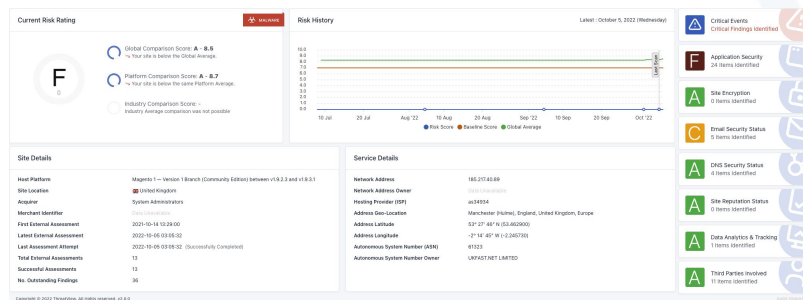
- Out of date software
- Basic security errors (exposed Admin login)
- Limited/no proactive security measures

**Most common denominator: lack of cyber security awareness/skills.**

# HOW CAN YOU GET PROACTIVE?

Step 1: Understand your website's CURRENT risk status:

## ThreatView – FREE Threat Detection Service



**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.





# FOREGENIX

## THANK YOU

(Any feedback on content would be gratefully received so that we can improve the information provided)



# FOREGENIX

## United Kingdom (HQ)

Foregenix Ltd.  
1 Watts Barn, Badbury  
Swindon, UK, SN4 0EU

T: +44 845 309 6232

## MEA

Foregenix (Pty) Ltd.  
Sec H, Blg E, Coachman's Crossing  
Office Park 4  
Brian Street, Lyme Park,  
Sandton, South Africa

T: +27 860 44 4461

## North America

Foregenix Inc  
75 State Street, 1st Floor  
Boston, MA, 02109, USA

T: +1 877 418 4774

## APAC

Foregenix (Pty) Ltd.  
1 Market Street, Sydney  
NSW 2000  
Australia

T: +61 420 904 914

## Europe

Foregenix Germany GmbH.  
Betzelsstrabe 27, 55116  
Mainz, Germany

T: +49 6131 2188747

## LATAM

Foregenix do Brasil  
São Paulo, Brazil

Foregenix Argentina  
Santa Fe, Argentina

+55 (11) 98781-4241

[sales@foregenix.com](mailto:sales@foregenix.com)

