



FOREGENIX

ECOMMERCE THREATSCAPE

MARCH 2023

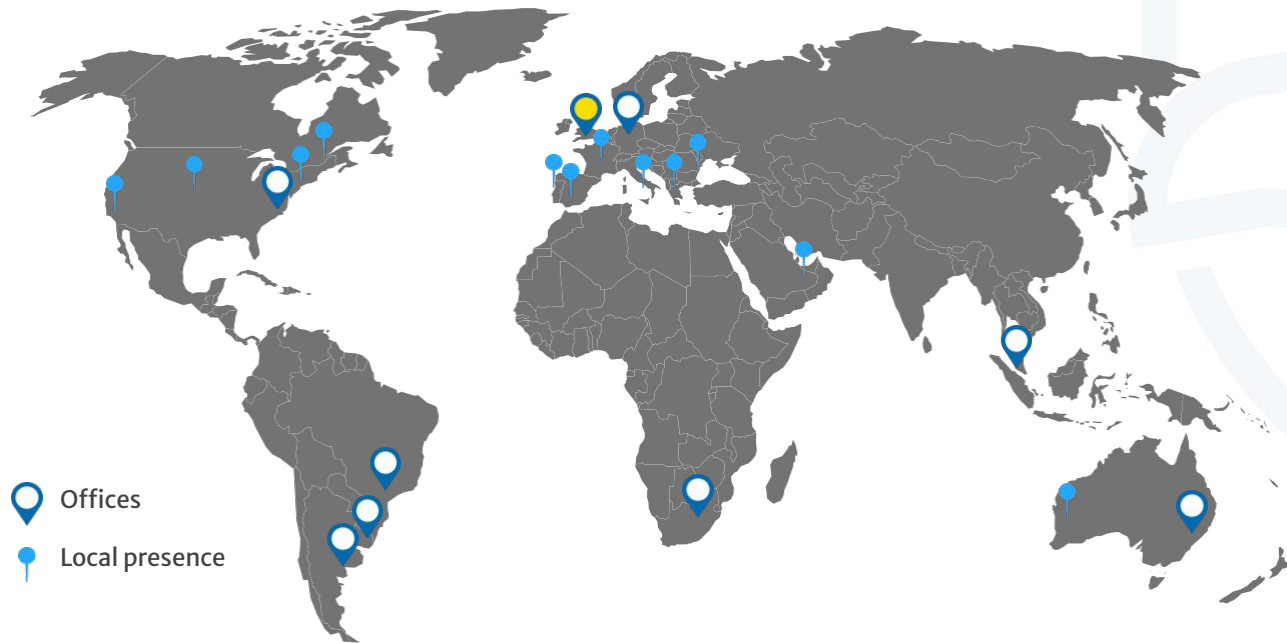
INTRODUCTION



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

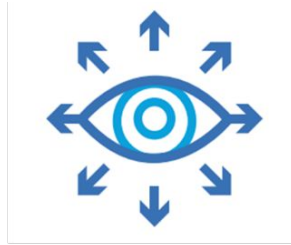
1,000s of
Satisfied Clients

EXECUTIVE SUMMARY

March 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

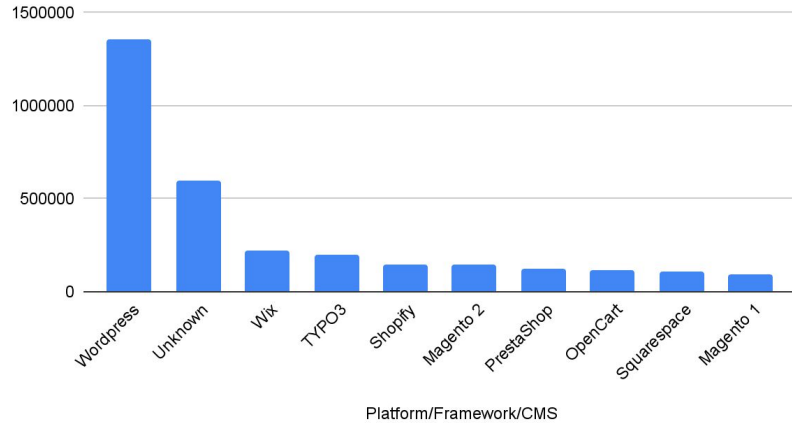


intel feeds directly into our ThreatView solution to monitor the global eCommerce Threatscape

PORTFOLIO OVERVIEW

Portfolio: 12.4m+ websites

Top 10 Platform Distribution



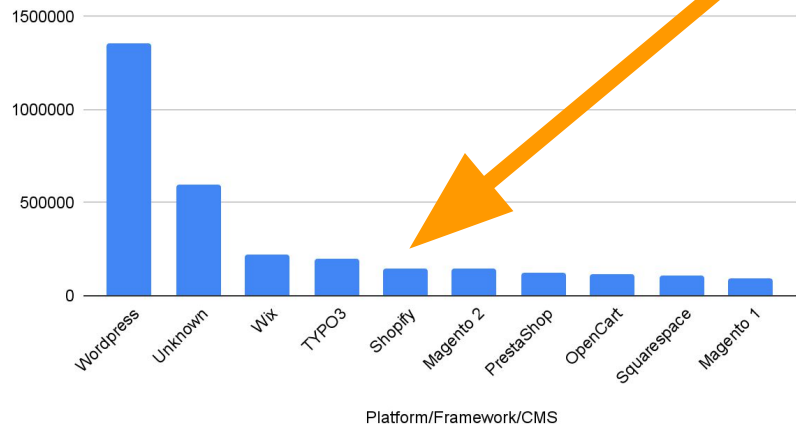
Our portfolio has built up over nearly a decade of providing free website security assessments and consists of predominantly eCommerce websites.

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: Shopify Market Growth

Top 10 Platform Distribution



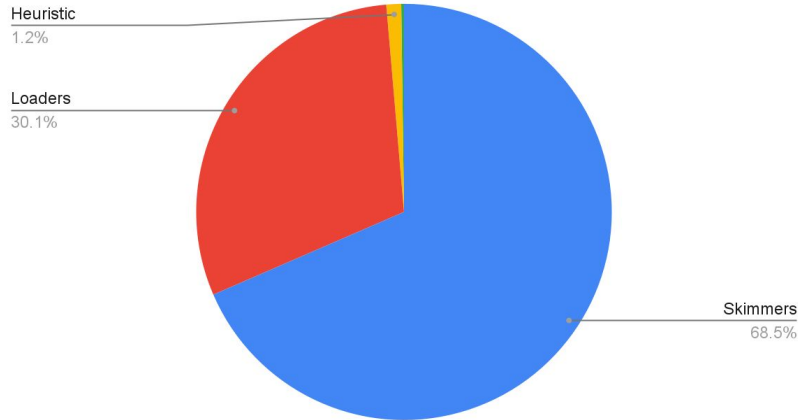
For the first time since we started monitoring eCommerce websites for threats, the number of Shopify sites has exceeded Magento 2 sites.

Shopify is also the 6th most targeted platform, which may indicate a coming of age for Shopify in the eCommerce industry.

HACKED ONLINE BUSINESSES

Hacked Sites: 8,104

Malware Types



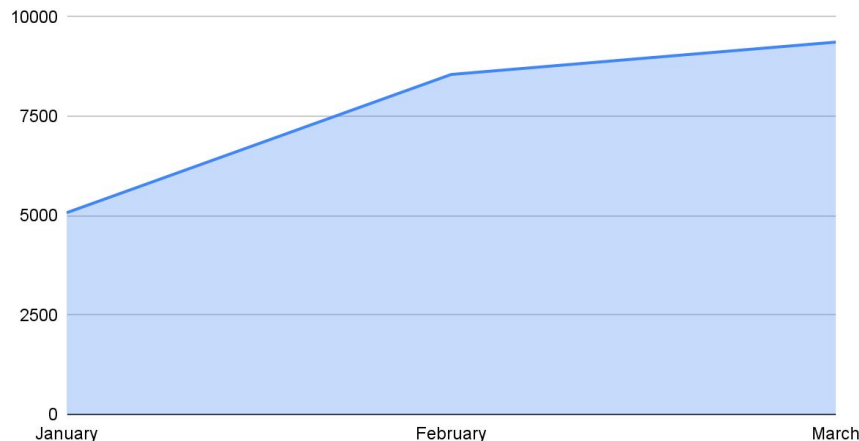
These are websites with:

- 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: GROWTH OF HACKED WEBSITES

Increase in Hacked Sites: 60% in last Quarter

Malware Detections By Month



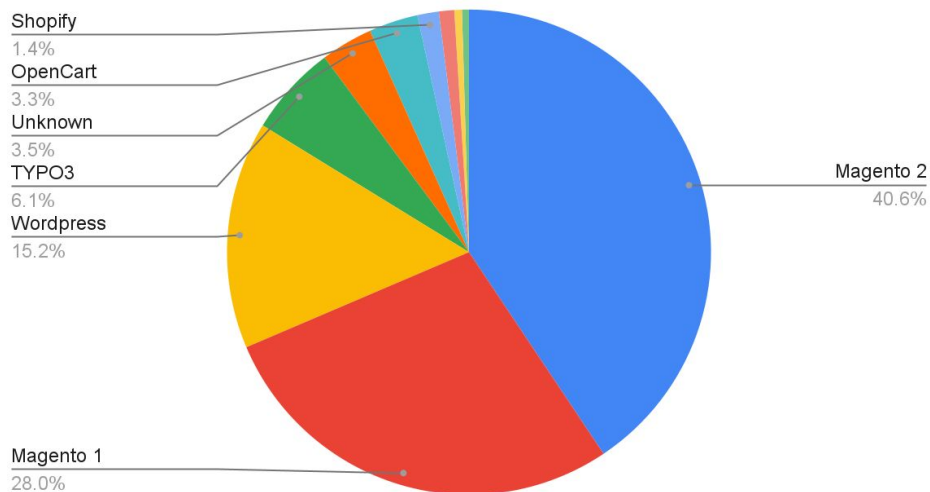
Significant increase in hacked sites in first 3 months of 2023, due to:

- Accelerated deployment of existing malware
- Wider deployment of older “Magecart variant” malware.
- 30% of increase due to 3 existing, older skimmers/malware variants.

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

TARGETED PLATFORMS

Top 10 Most Targeted Platforms



Targeted Platforms

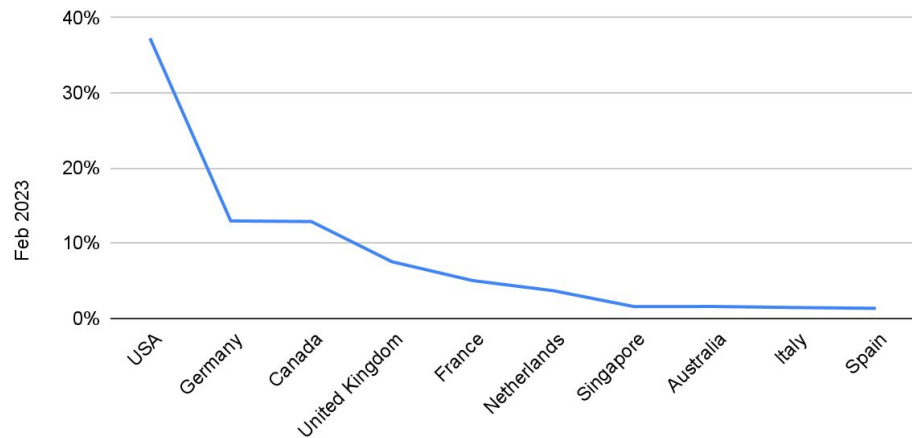
Top 5 Compromised Platforms:

1. Magento 2 (2.79%)
2. Magento 1 (3.02%)
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: 2.40%

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.

MALICIOUS DOMAINS

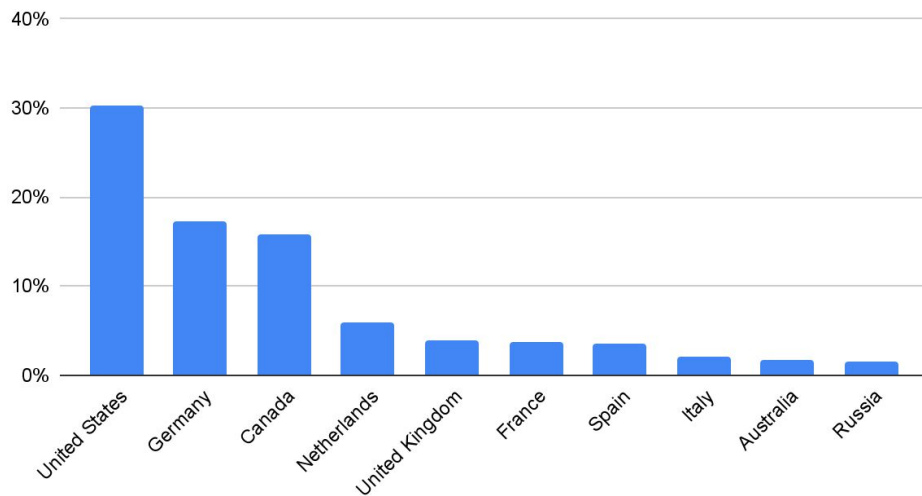
Malicious Domains serve Skimmer Malware to compromised websites infected with “Loader” malware.

Typically these are regular websites that have been compromised by criminals and are then used to serve malware to other compromised websites.

The top 5 malicious domains serve up nearly 10% of malware detected.

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. Netherlands
5. UK*

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

*new within the top 5 compared with last month. UK (marginally) exceeds France in March 2023.

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	Mar 2021	Mar 2022	Mar 2023
Magento 1	141,892	91,168	89,832
Magento 2	99,024	103,942	143,696

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 WE DEFEND THE INDUSTRY?

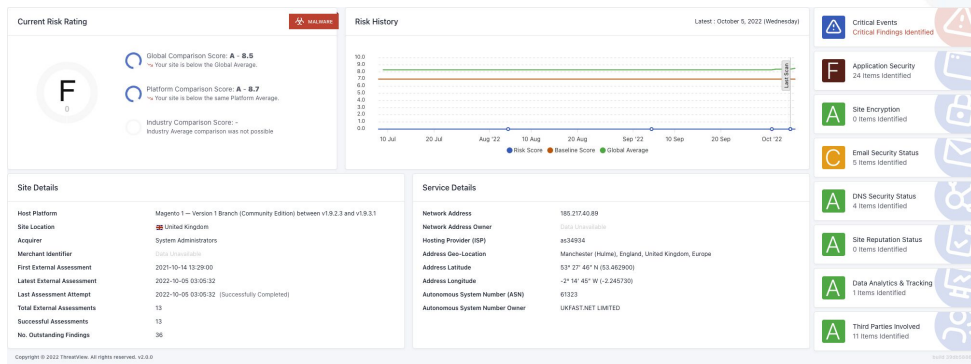
What are we doing about it?

1. Community–Use technology – [ThreatView](#) is free to use by any eCommerce business.
2. Ongoing educational outreach – social media, email, industry reports.
3. Continuing to combat cyber criminals daily with our forensic & Threat Intel teams – and our technology.

HOW CAN YOU GET PROACTIVE?

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

ThreatView – FREE Threat Detection Service





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

