FOREGENIX

ECOMMERCE THREATSCAPE

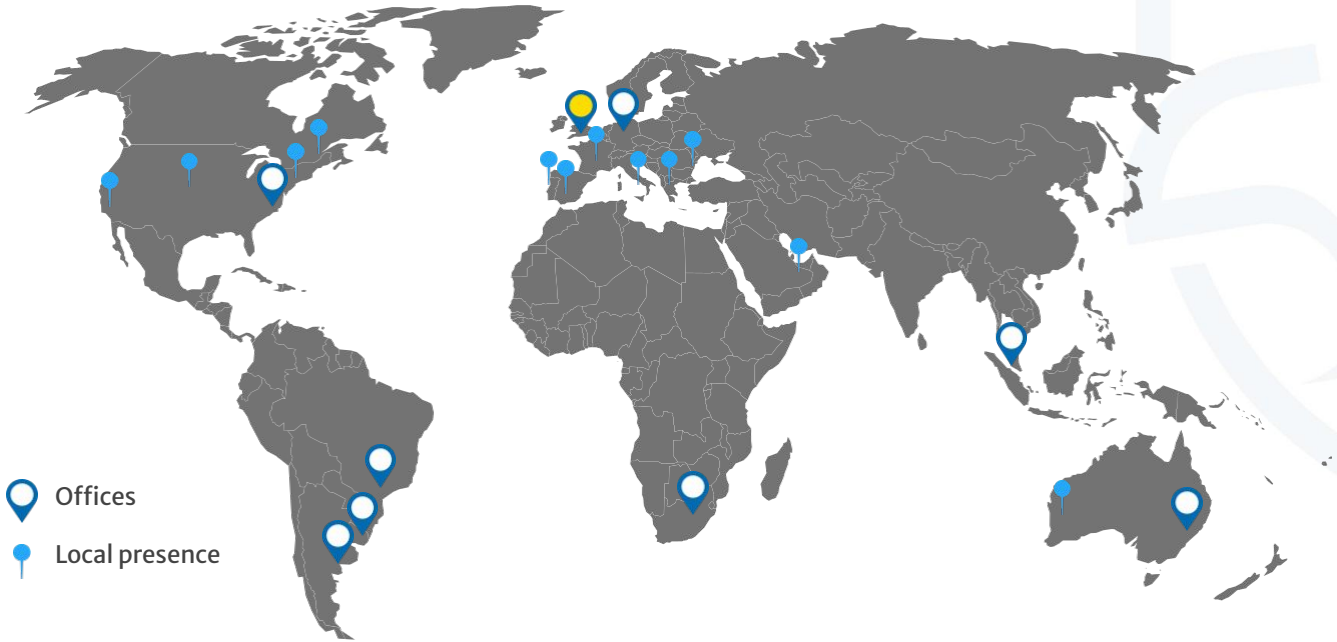
MAY 2023

INTRODUCTION

- 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

FOREGENIX

GLOBAL PRESENCE



Offices

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

12+
Languages

20+
Countries

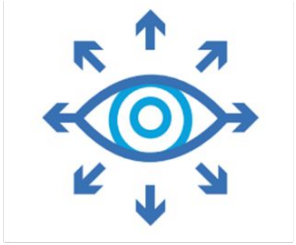
1,000s of
Satisfied Clients

FOREGENIX

EXECUTIVE SUMMARY

Foregenix eCommerce Threatscape

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



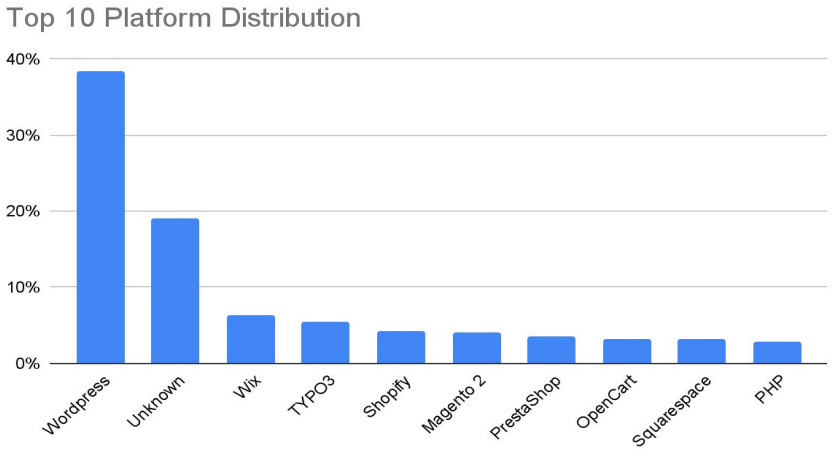
provides us with **vital intelligence** on:

- 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**

FOREGENIX

PORTFOLIO OVERVIEW



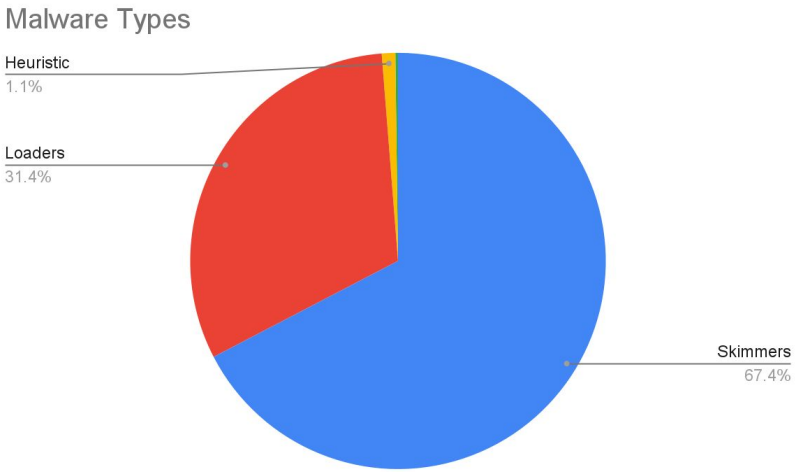
Portfolio: 12.4m+ websites

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 14 years of eCommerce forensic investigations.

FOREGENIX

HACKED ONLINE BUSINESSES



Hacked Sites: 7,805

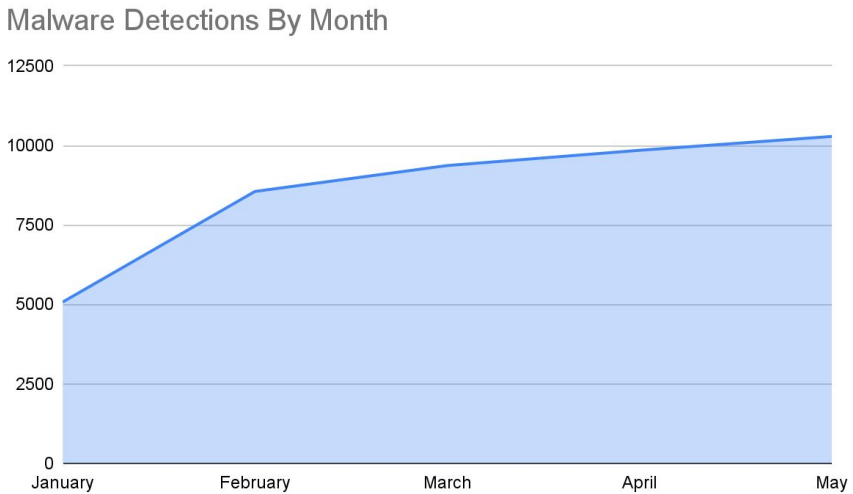
These are websites with:

- 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.

FOREGENIX

ALERT: MALWARE DETECTIONS GROWTH

Increase in Malware detected: 102% since Jan 2023



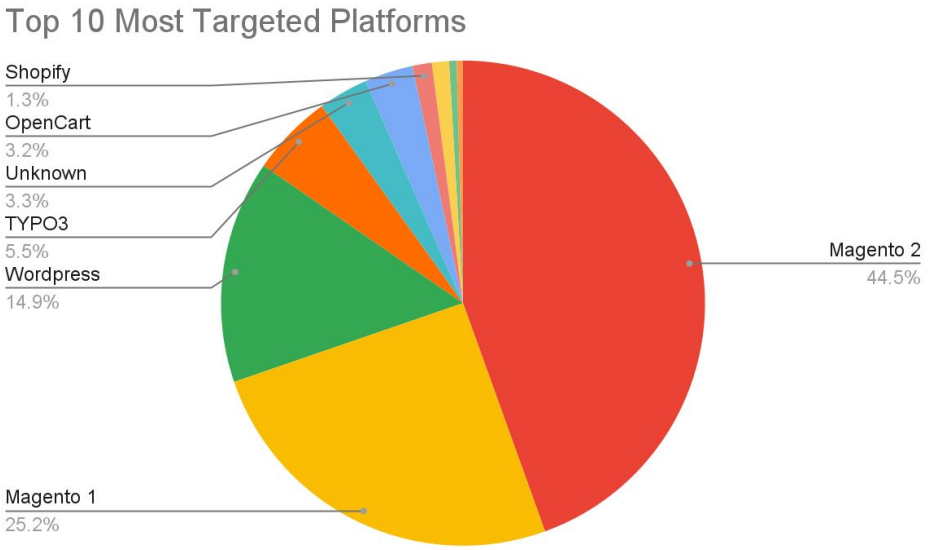
Significant increase in Malware since Jan 2023:

- 7,805 sites compromised (up from 7,801 last month)
- Over 10,000 instances of “Loader” and “Skimmer” malware code detected worldwide.

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

FOREGENIX

TARGETED PLATFORMS



Targeted Platforms

Top 5 Compromised Platforms:

1. Magento 2 (3.37%)
2. Magento 1 (3.14%)
3. Wordpress (0.12%)
4. TYPO3 (0.31%)
5. OpenCart (0.31%)

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.

FOREGENIX

TARGETED PLATFORMS

Significant Increases month over month:

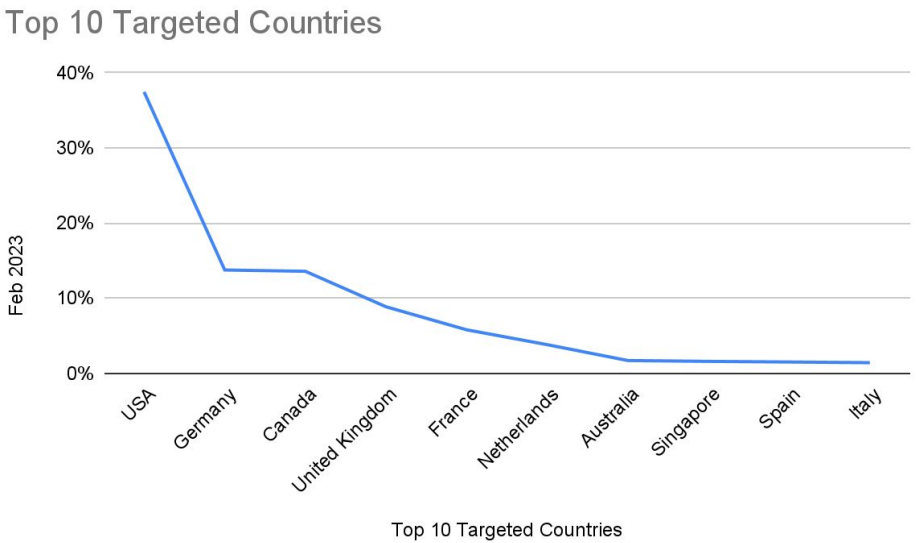
Platforms with significant increase in hacked sites month over month:

1. Magento 2 (+345)
2. Wordpress (+39)
3. Shopify (+24)

The figure in brackets is the number of additional sites compromised compared with previous month.

FOREGENIX

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

FOREGENIX

TOP 10 TARGETED COUNTRIES

Increases in # of hacked sites

Countries with greatest proportional increase in compromised sites:

1. United Kingdom (9.14%)
2. Australia (8.44%)
3. Canada (6.11%)

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

FOREGENIX

HIGH RISK WEBSITES

High Risk Sites: 2.33%

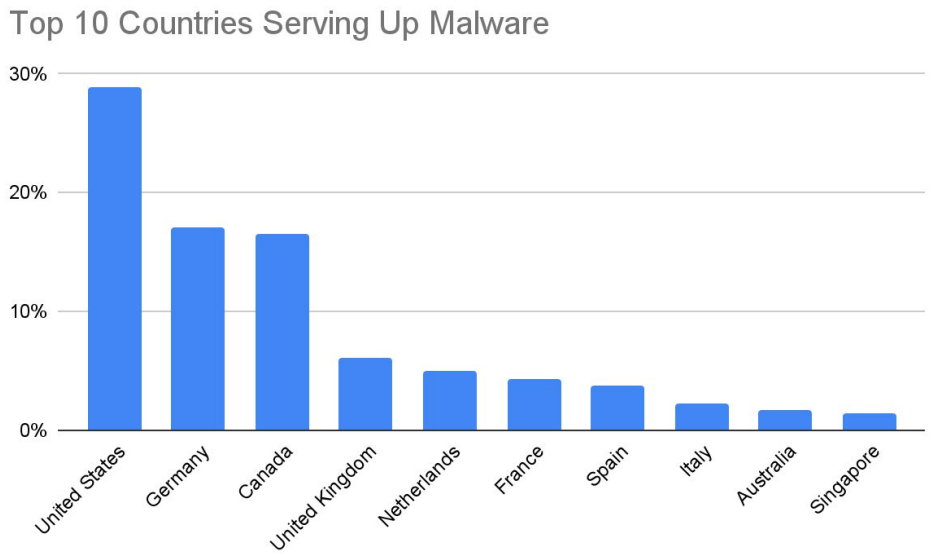
These are sites that are likely to be targeted by criminals.

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.

FOREGENIX

MALICIOUS DOMAIN SOURCES



Serving up Malware

Top 5 Countries serving up Card Harvesting Malware:

1. US
2. Germany
3. Canada
4. United Kingdom*
5. Netherlands

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

***UK had a 42% increase in malware sources detected compared with last month.**

FOREGENIX

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	May 2021	May 2022	May 2023
Magento 1	134,924	91,817	86,411
Magento 2	101,795	103,781	141,746

WHY ARE THESE SITES BEING HACKED?

Criminals target the websites easiest to hack.

The vast majority of hacked sites share the same characteristics:

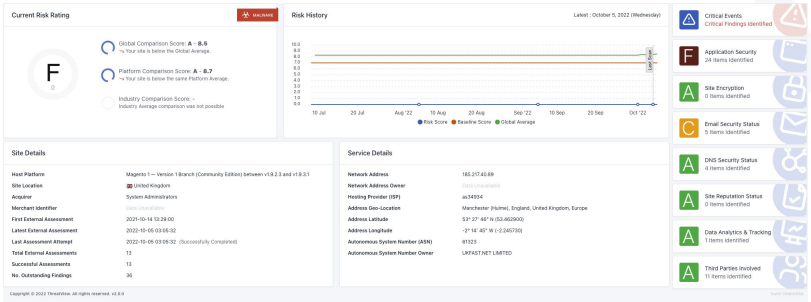
- Out of date software
- Basic security errors (exposed Admin login)
- Limited/no proactive security measures

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

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

North America

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

T: +1 877 418 4774

Europe

Foregenix Germany GMbH.
Betzelsstrabe 27, 55116
Mainz, Germany

T: +49 6131 2188747

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

APAC

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

T: +61 420 904 914

LATAM

Foregenix do Brasil
São Paulo, Brazil

Foregenix Argentina
Santa Fe, Argentina

+55 (11) 98781-4241

sales@foregenix.com