FOREGENIX

ECOMMERCE THREATSCAPE

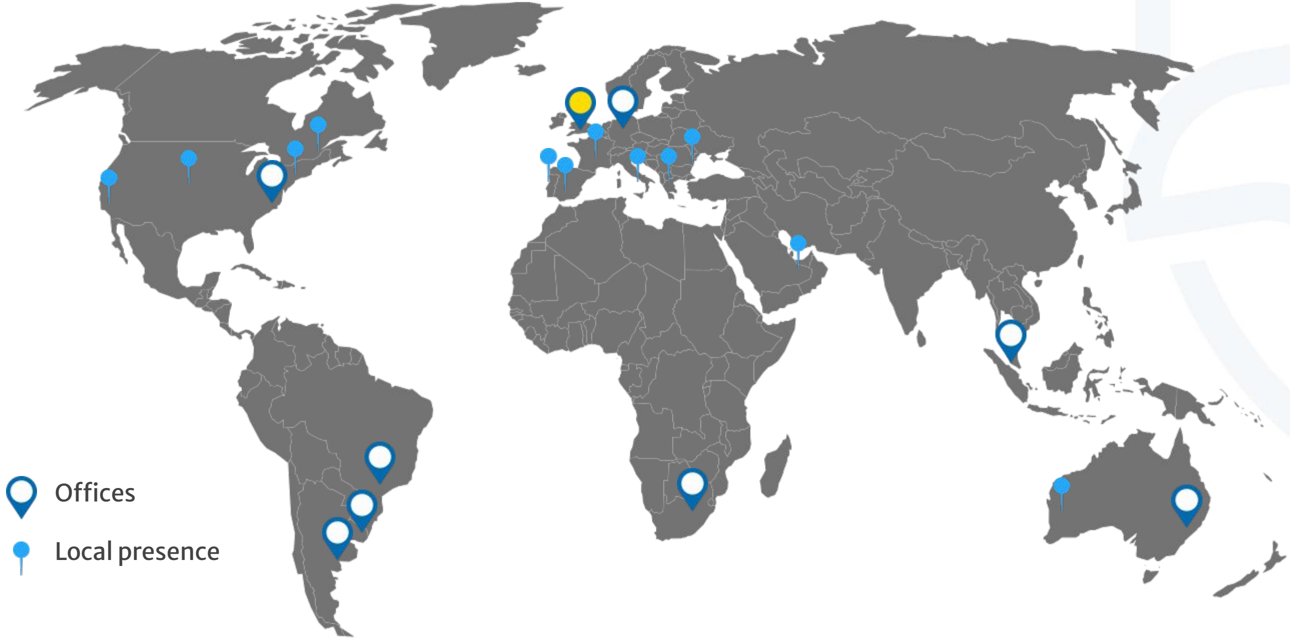
FEBRUARY 2023

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

FOREGENIX

EXECUTIVE SUMMARY

February 2023 eCommerce Threatscape

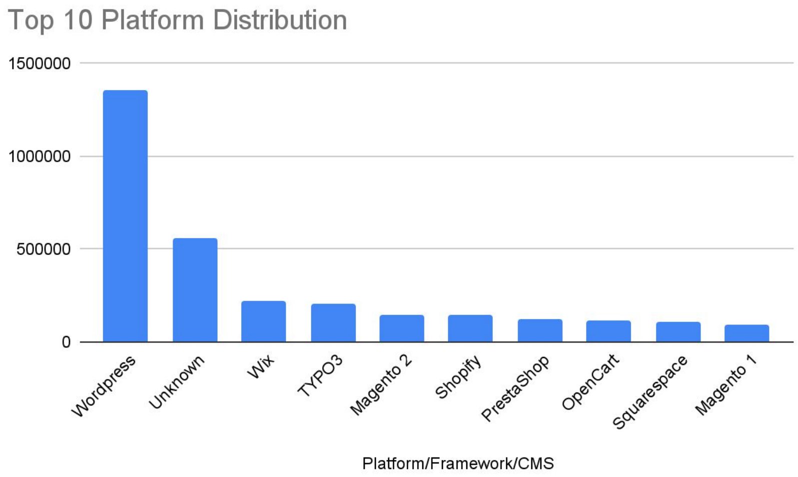
Digital Forensic and Incident Response team works with large numbers of hacked eCommerce sites globally

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



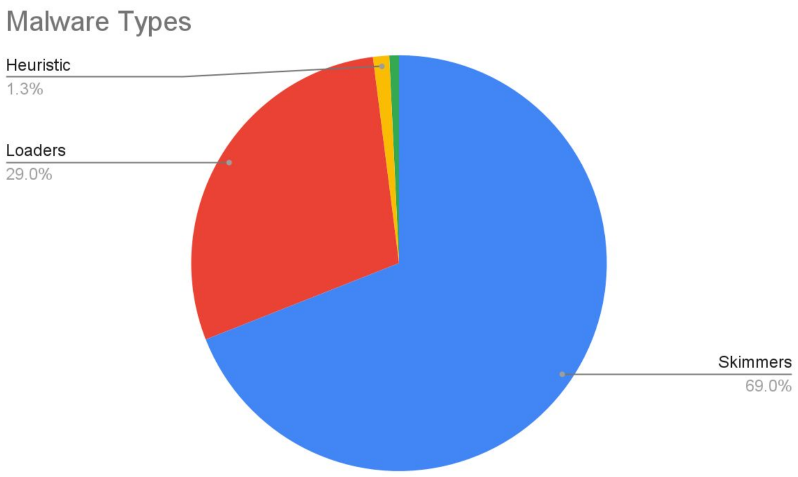
Portfolio: 12.4m+ websites

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



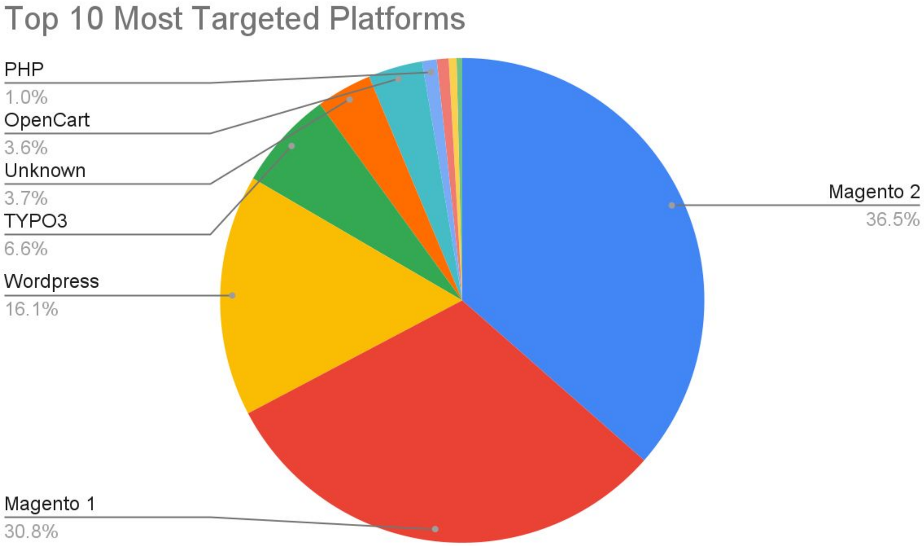
Hacked Sites: 7,110

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

TARGETED PLATFORMS



Targeted Platforms

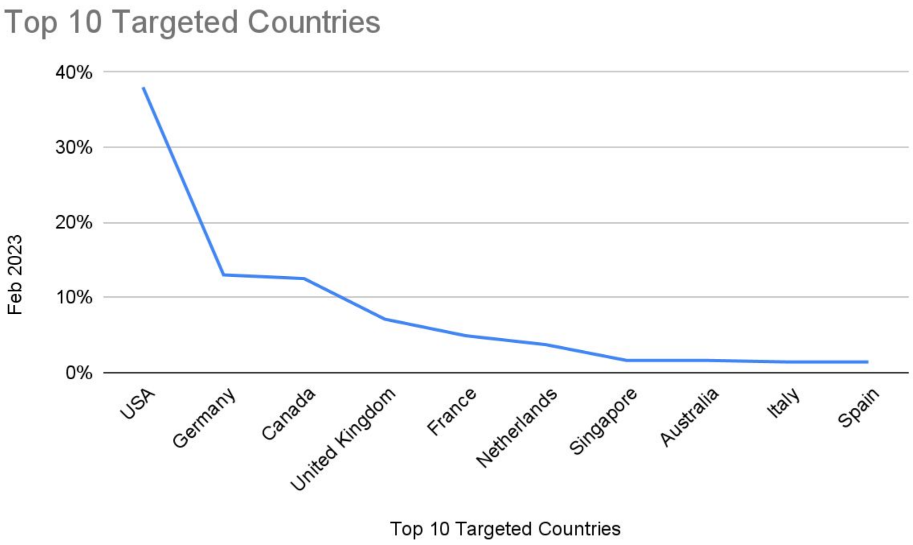
Top 5 Compromised Platforms:

1. Magento 2 (2.28%)
2. Magento 1 (3.03%)
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.

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

HIGH RISK WEBSITES

High Risk Sites: 2.47%

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.

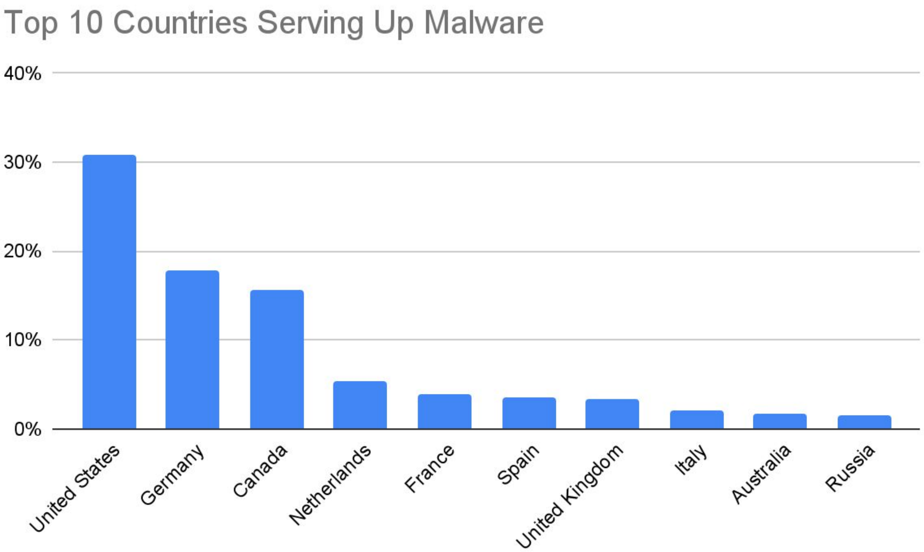
MALICIOUS DOMAINS

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



Serving up Malware

Top 5 Countries serving up Card Harvesting Malware:

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

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.

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:

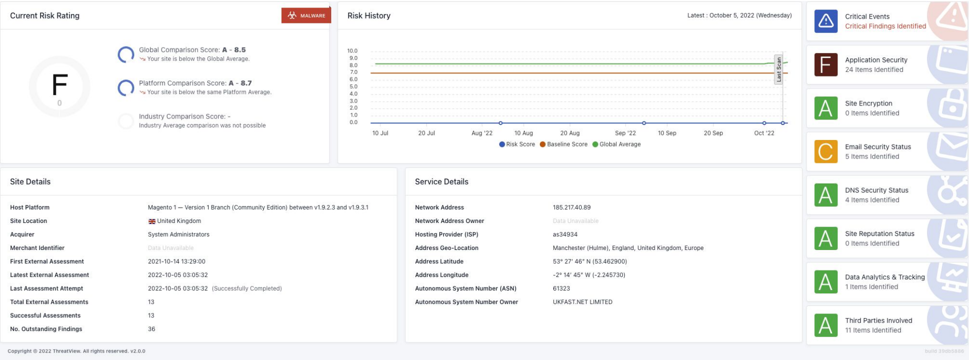
Platform	Feb 2021	Feb 2022	Feb 2023
Magento 1	152,946	99,044	91,521
Magento 2	100,500	103874	144,478

COMMUNITY DEFENCE

Our ThreatView Community solution is available for FREE for any eCommerce website to use, providing them with:

- A monthly website assessment
- The latest Threat Detection capability

Access ThreatView here.



Current Risk Rating

MALWARE

F
0

Global Comparison Score: **A - 8.5**
↘ Your site is below the Global Average.

Platform Comparison Score: **A - 8.7**
↘ Your site is below the same Platform Average.

Industry Comparison Score: -
Industry Average comparison was not possible

Risk History

Latest : October 5, 2022 (Wednesday)

A	Critical Events Critical Findings Identified
F	Application Security 24 Items Identified
A	Site Encryption 0 Items Identified
C	Email Security Status 5 Items Identified
A	DNS Security Status 4 Items Identified
A	Site Reputation Status 0 Items Identified
A	Data Analytics & Tracking 1 Items Identified
A	Third Parties Involved 11 Items Identified

Site Details

Host Platform	Magento 1 — Version 1 Branch (Community Edition) between v1.9.2.3 and v1.9.3.1
Site Location	United Kingdom
Acquirer	System Administrators
Merchant Identifier	Data Unavailable
First External Assessment	2021-10-14 13:29:00
Latest External Assessment	2022-10-05 03:05:32
Last Assessment Attempt	2022-10-05 03:05:32 (Successfully Completed)
Total External Assessments	13
Successful Assessments	13
No. Outstanding Findings	36

Service Details

Network Address	185.217.40.89
Network Address Owner	Data Unavailable
Hosting Provider (ISP)	as34934
Address Geo-Location	Manchester (Hulme), England, United Kingdom, Europe
Address Latitude	53° 27′ 46″ N (53.462900)
Address Longitude	-2° 14′ 45″ W (-2.245730)
Autonomous System Number (ASN)	61323
Autonomous System Number Owner	UKFAST.NET LIMITED

Copyright © 2022 ThreatView. All rights reserved. v2.0.0

build 39db5886

FOREGENIX

PROTECTING THE INDUSTRY

How do we protect the industry from criminals?

The vast majority of hacked sites share the same characteristics:

- Out of date software
- Basic security errors
- Limited/no proactive security measures

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

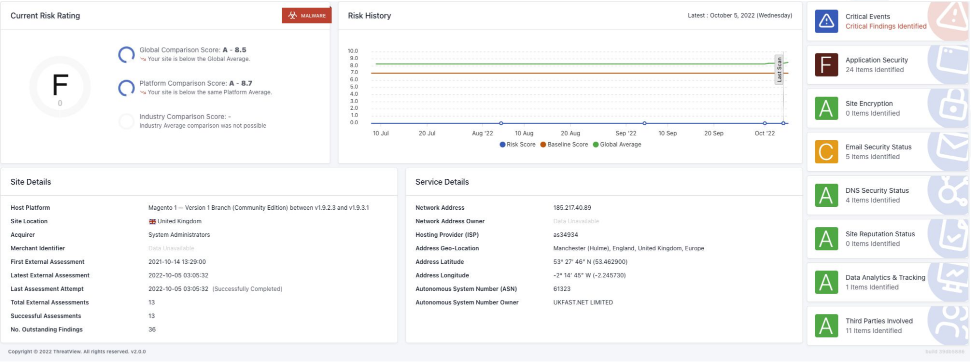
PROTECTING THE INDUSTRY

What are we doing about it?

1. Community use technology – **ThreatView – FREE to any merchant/bank.**
2. Ongoing outreach – social media, email, industry reports.
3. Continuing to combat cyber criminals daily with our forensic & Threat Intel teams – and our technology.

GET PROACTIVE – FOR FREE

[ThreatView – Sign up here]



Current Risk Rating

MALWARE

F
0

Global Comparison Score: **A - 8.5**
Your site is below the Global Average.

Platform Comparison Score: **A - 8.7**
Your site is below the same Platform Average.

Industry Comparison Score: -
Industry Average comparison was not possible

Risk History

Latest : October 5, 2022 (Wednesday)

Critical Events
Critical Findings Identified

F Application Security
24 Items Identified

A Site Encryption
0 Items Identified

C Email Security Status
5 Items Identified

A DNS Security Status
4 Items Identified

A Site Reputation Status
0 Items Identified

A Data Analytics & Tracking
1 Items Identified

A Third Parties Involved
11 Items Identified

Site Details

Host Platform	Magento 1 — Version 1 Branch (Community Edition) between v1.9.2.3 and v1.9.3.1
Site Location	United Kingdom
Acquirer	System Administrators
Merchant Identifier	Data Unavailable
First External Assessment	2021-10-14 13:29:00
Latest External Assessment	2022-10-05 03:05:32
Last Assessment Attempt	2022-10-05 03:05:32 (Successfully Completed)
Total External Assessments	13
Successful Assessments	13
No. Outstanding Findings	36

Service Details

Network Address	185.217.40.89
Network Address Owner	Data Unavailable
Hosting Provider (ISP)	as34934
Address Geo-Location	Manchester (Hulme), England, United Kingdom, Europe
Address Latitude	53° 27' 46" N (53.462900)
Address Longitude	-2° 14' 45" W (-2.245730)
Autonomous System Number (ASN)	61323
Autonomous System Number Owner	UKFAST.NET LIMITED

build 39db5886

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

2019