FOREGENIX

eCommerce Threatscape:

July 2023

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.

Increase in # of hacked sites:

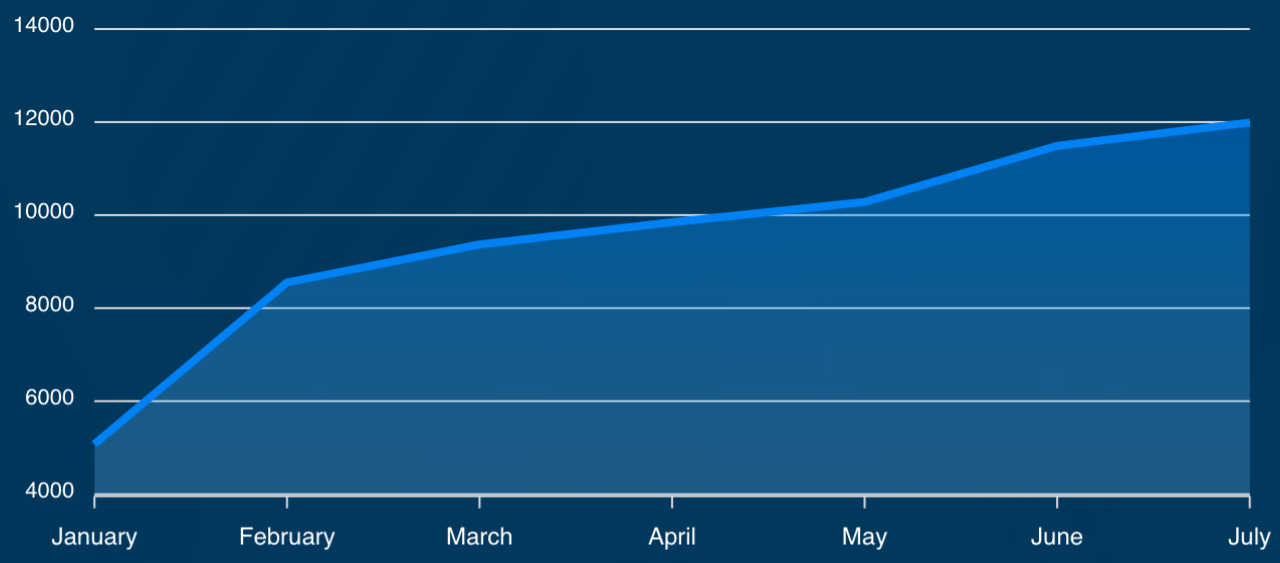
Countries with greatest proportional increase in compromised sites:

- Australia (9%)
- Germany (5%)
- Italy (5%)

The UK has a higher proportion of hacked sites relative to market share than any other country.

ALERT: MALWARE DETECTIONS

Increase in malware detected: 136% since January 2023

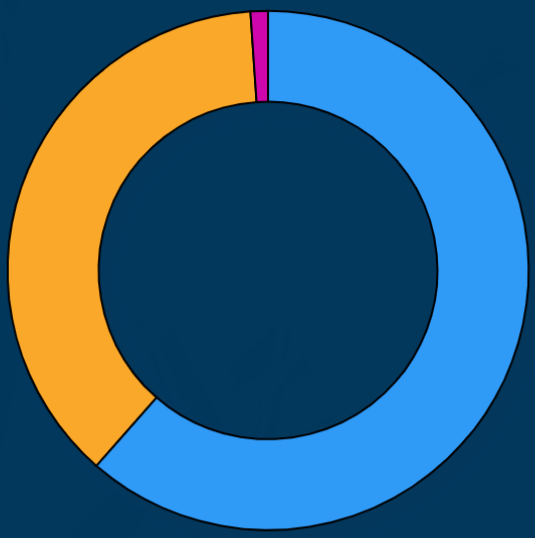


NB: Many sites are infected with multiple types of malware.

Significant increase in malware since January 2023:

- 7,874 sites compromised.
- Nearly 12,000 instances of "Loader" and "Skimmer" malware code detected worldwide.

HACKED ONLINE BUSINESSES



Malware Types

- Skimmers (61.7%)
- Loaders (37.4%)
- Heuristic (0.9%)

Hacked Sites:

7,874

High Risk Sites:

2.20%

10% decrease on last month. 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.

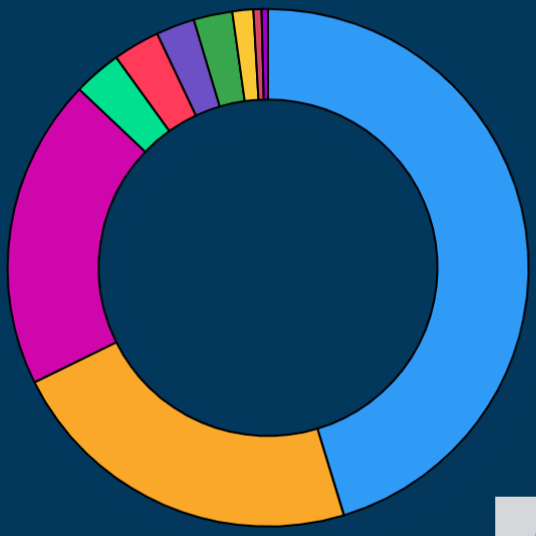
HIGH RISK WEBSITES

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.

TOP 10 TARGETED PLATFORMS



- Magento 2 (45.3%)
- Magento 1 (22.4%)
- Wordpress (19.4%)
- Custom/Unknown (3.0%)
- OpenCart (2.9%)
- TYPO3 (2.4%)
- Shopify (2.4%)
- PHP (1.3%)
- ASP (0.5%)
- BigCommerce (0.4%)

Top 6 Compromised Platforms:

1. Magento 2 (3.98%)
2. Magento 1 (3.36%)
3. Wordpress (0.19%)
4. TYPO3 (0.16%)
5. OpenCart (0.35%)
6. Shopify (0.19%)

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.

Significant increases month over month.

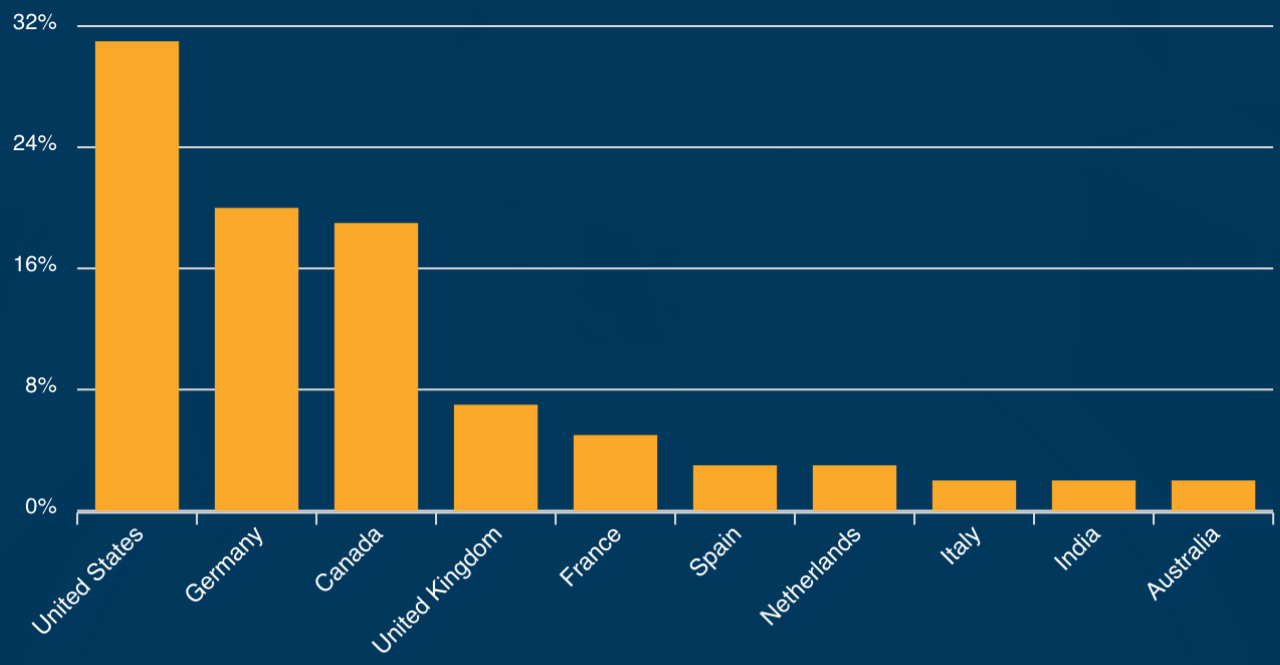
Platforms with a significant increase:

- Shopify (+12%)*
- Magento 2 (+6%)
- Wordpress (+5%)

*Hacked Shopify site growth as a percentage is quicker than all other platforms; however, in absolute numbers, Magento 2 has nearly 10x the growth in hacked sites in comparison with Shopify

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

MALICIOUS DOMAIN SOURCES



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

*Germany had a 31% increase, Netherlands had a 34% decrease in malware sources detected compared with last month.

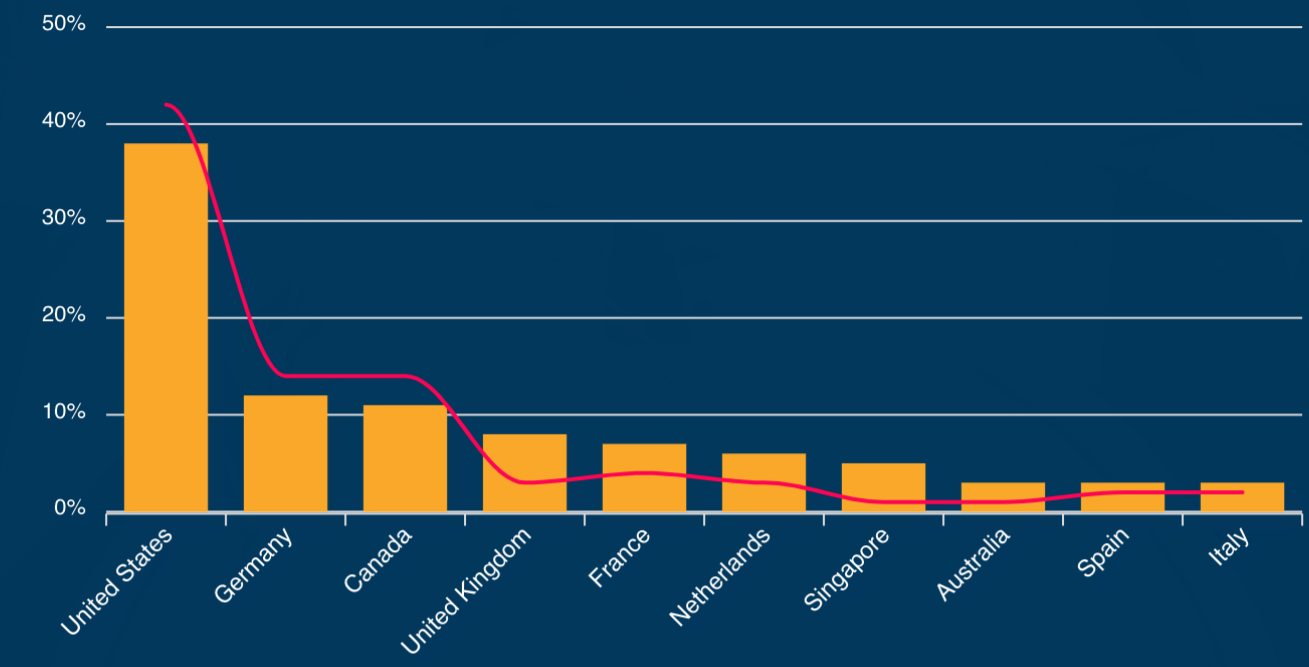
Why are these sites being hacked?

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.

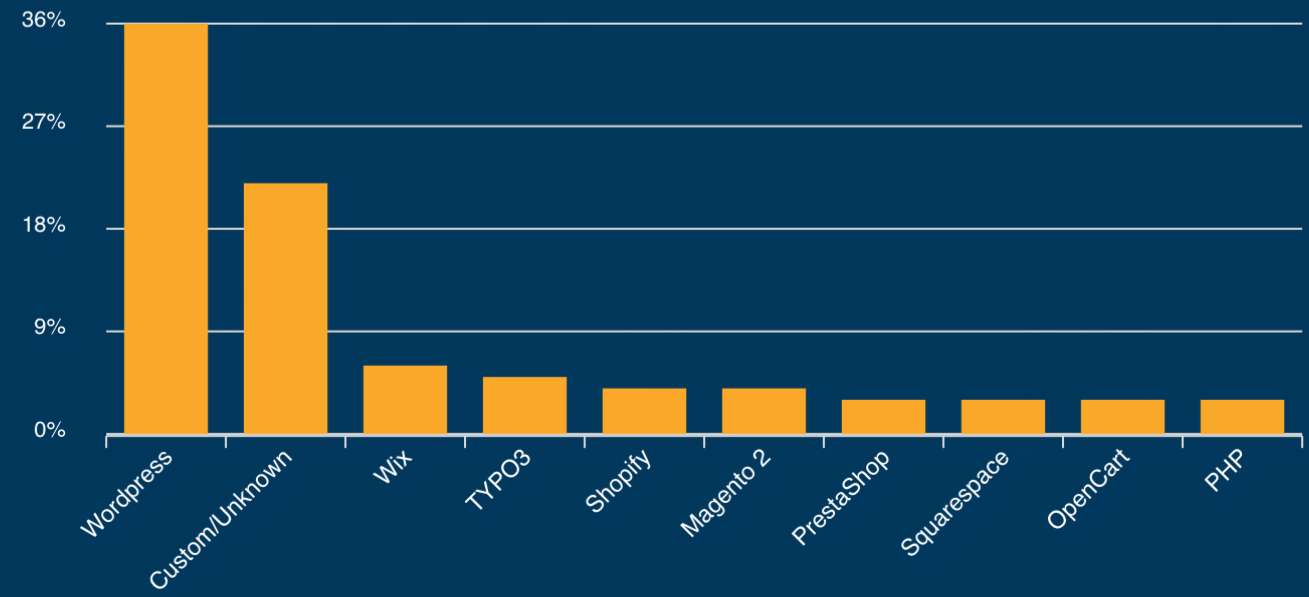
Most common denominator:
lack of security awareness/skills.

TOP 10 TARGETED COUNTRIES



NB: These websites are compromised predominantly with Payment Card Harvesting malware.

TOP 10 PLATFORM DISTRIBUTION



WHAT IS THE COST OF A BREACH?

Short answer: wide ranging & "it depends".

Depending on where you source the data, the cost of a breach can range from ~$3,000 to $500k+.

Key drivers of cost:

- Number of customer records stolen.
- Liability built up on stolen payment card data.
- GDPR/ICO penalties.
- Legal, PR etc.

You can read a blog post with our analysis on our website:
www.foregenix.com/blog/

HOW YOU CAN GET PROACTIVE:

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

GLOBAL PRESENCE

12+ Languages

1,000s of Satisfied Clients

20+ Countries

United Kingdon (HQ)

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

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.
Betzelsstraße 27, 55116
Mainz, Germany

T: +49 6131 2188747

MEA

Foregenix (Pty) Ltd.
Sec H, Big 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

T: +55 (11) 98781-4241

info@foregenix.com