FOREGENIX

eCommerce Threatscape:

1st Quarter 2024

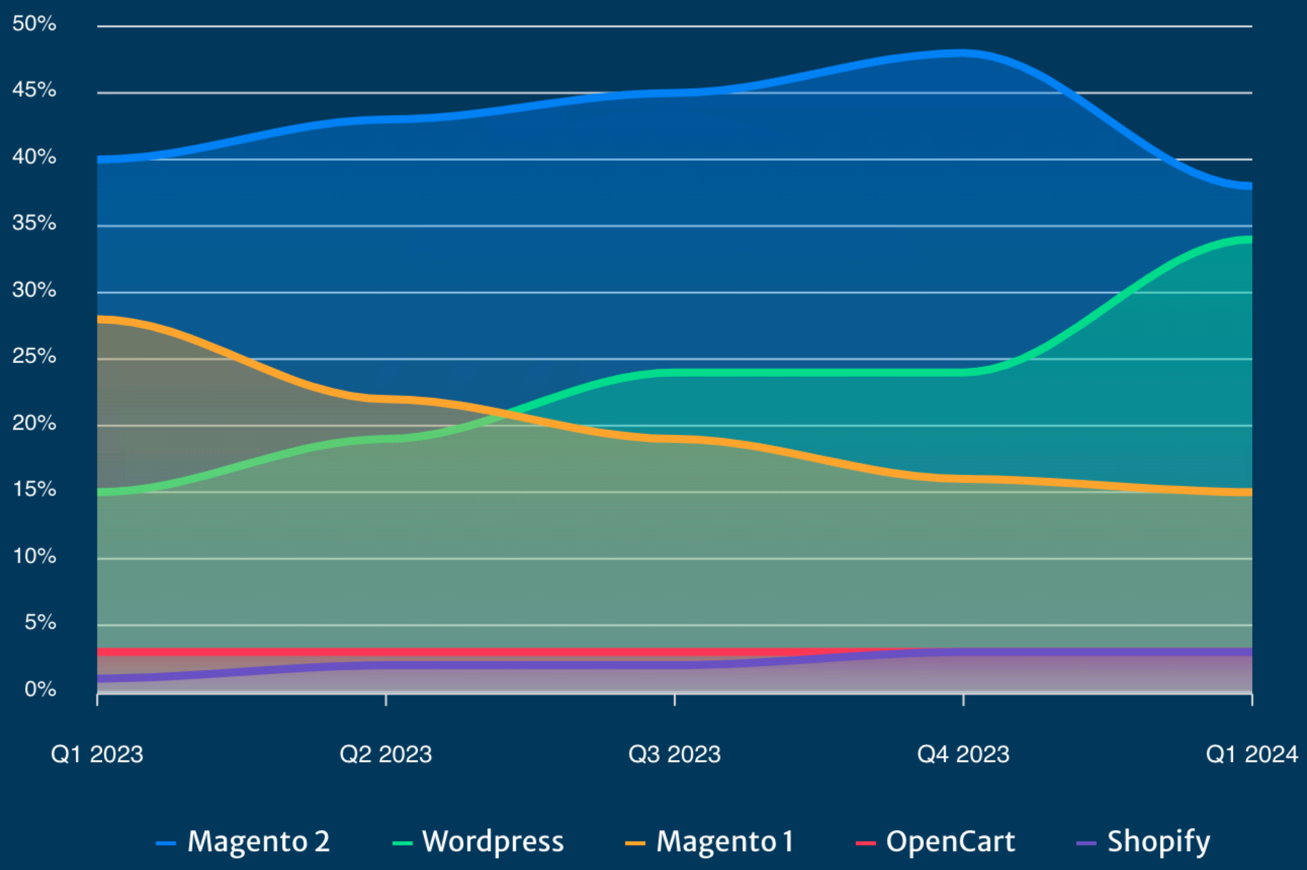
PORTFOLIO OVERVIEW

Portfolio: 14.5m+ 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 15 years of eCommerce forensic investigations.

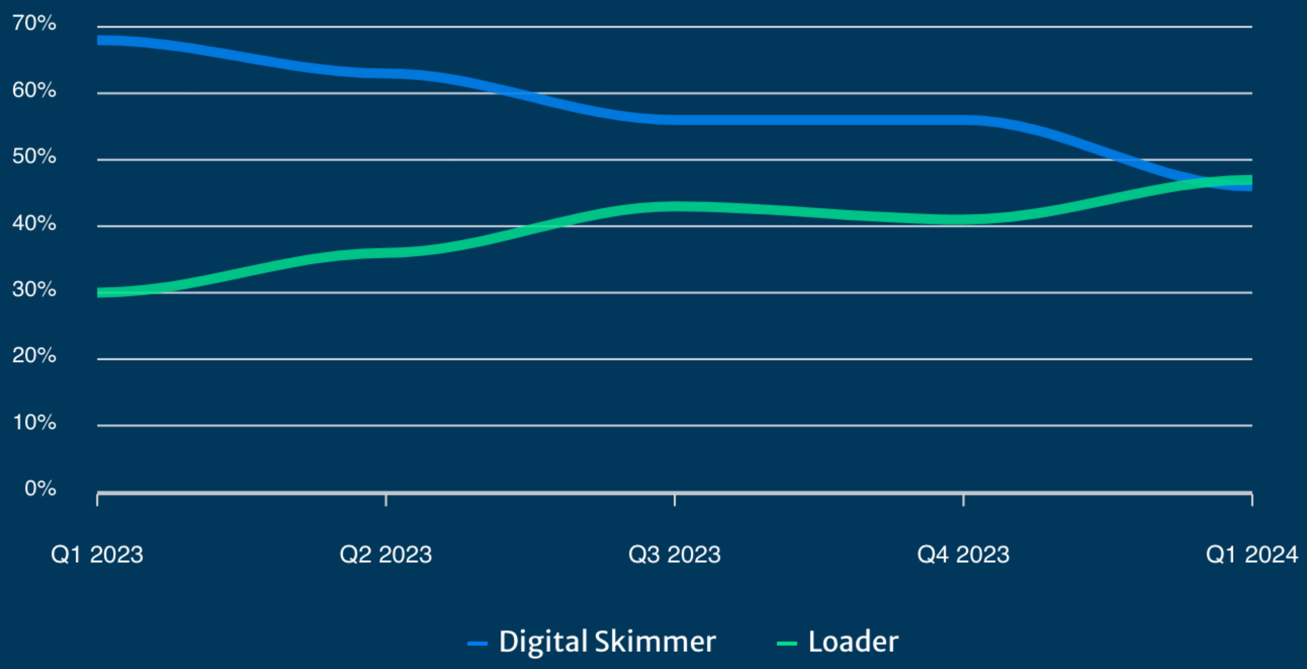
TOP 5 TARGETED PLATFORMS



Targeted platforms

- These Top 5 eCommerce platforms account for **92%** of the malware detected this quarter.

DIGITAL SKIMMERS & LOADERS



March Hacked Sites:

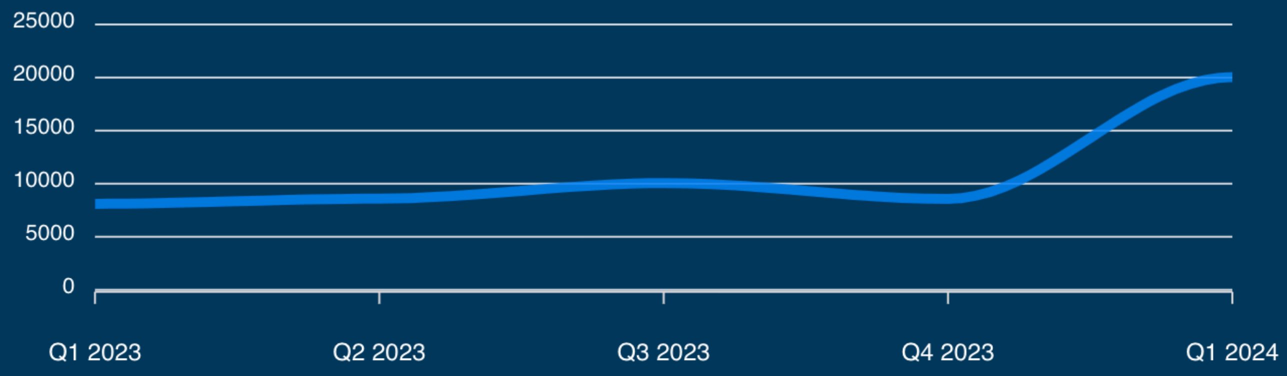
20,044

Notable observations:

- Loader malware on victim websites is now more prevalent than skimmers.
- Digital skimmers are still part of the attack chain, but being used *WITH* loaders and more complex attacks.

MALWARE ANALYSIS

Hacked eCommerce sites



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

Significant growth in hacked sites:

- Portfolio growth.
- Adapting threatscape making it challenging to detect criminals.

Top 5 loaders & skimmers and the platforms being targeted

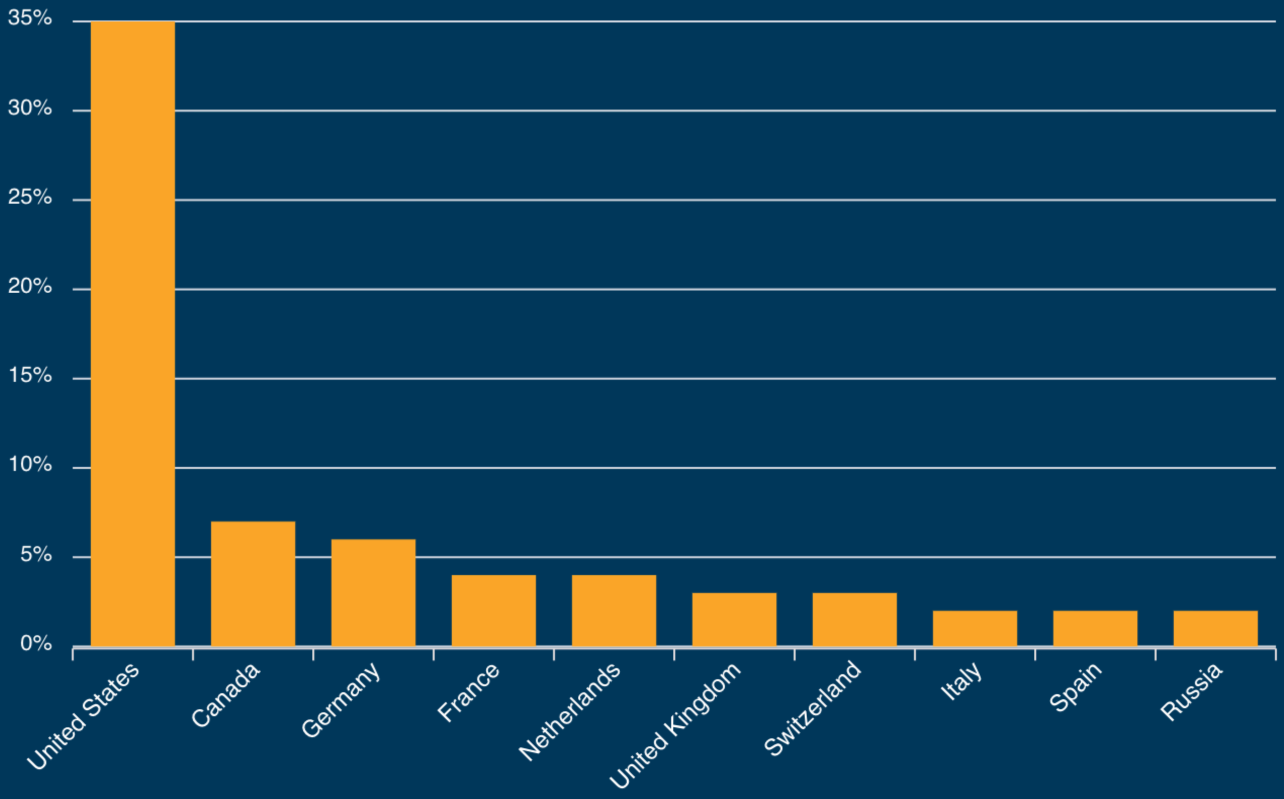
Malware rule (loaders)	Affected platforms
JS_loader_parrot	Wordpress, Joomla, Drupal, Magento 1, Magento 2, OpenCart
JS_loader_firstkiss	Magento 2, BigCommerce, Magento 1
JS_loader_injector_google_ads	Wordpress, Magento 2, OpenCart, Magento 1, Joomla
JS_loader_cloudsonicwave	Wordpress, PHP
JS_loader_kritec	Magento 2, Wordpress, Prestashop, OpenCart, Magento 1, OpenMage

Top 5 account for 70% of all loaders detected.

Malware rule (skimmers)	Affected platforms
JS_skimmer_z3r0day	Magento 1, Magento 2, Wordpress, Squarespace
JS_Skimmer_Gclon	Magento 1, Magento 2
JS_skimmer_united81	Magento 1, Magento 2, Wordpress, Drupal
JS_skimmer_dedwards_packed	Wordpress, OpenCart, Magento 1, Magento 2, Joomla
JS_skimmer_google_ads	Wordpress, OpenCart, Magento 1, Magento 2

MALICIOUS DOMAIN SOURCES

Top 10 countries serving up malware



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

Why are these sites being hacked?

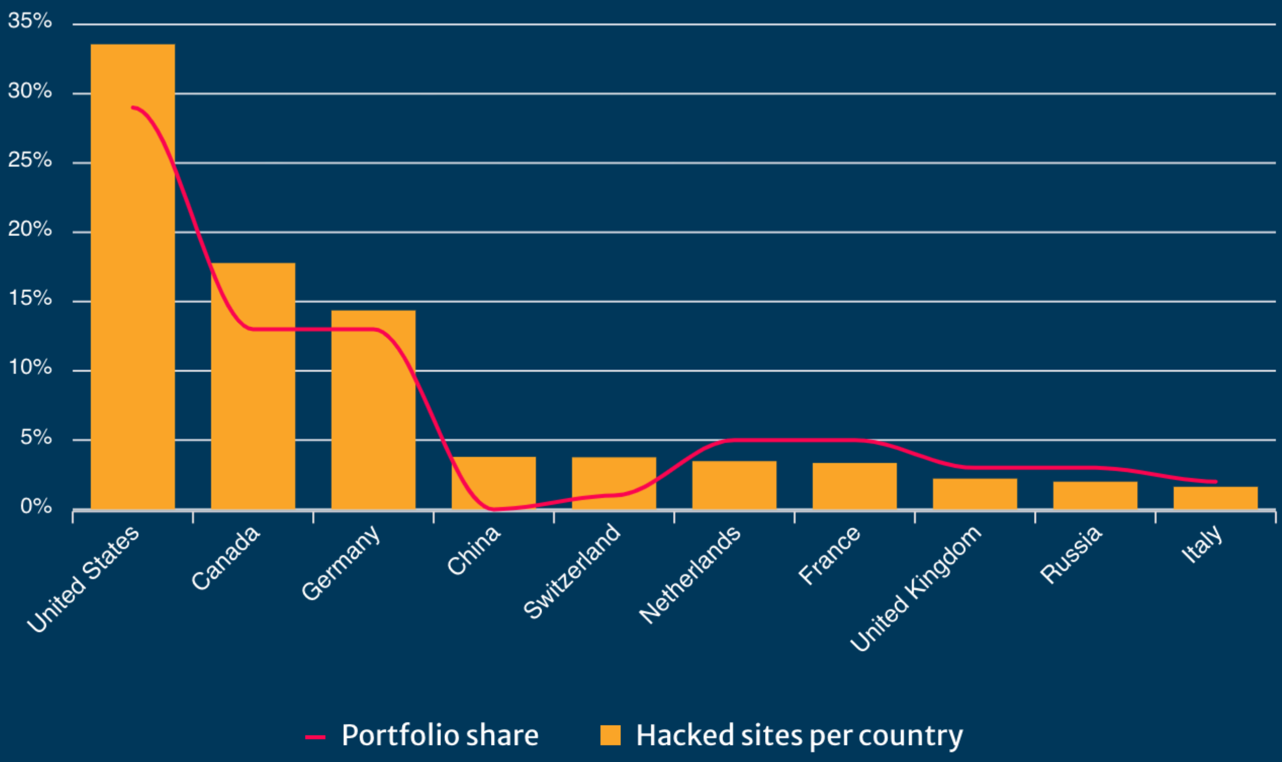
Criminals target the websites easiest to hack. The vast majority of hacked sites share the same characteristics:

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

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

TOP 10 TARGETED COUNTRIES

Hacked sites vs portfolio share by country



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 CAN YOU 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.

You can easily check if your business is one of the many hacked sites detected. You will need to create a free account then run a scan using the latest Threat IOCs.

It takes 2 minutes and is completely free – no credit card required.

www.foregenix.com/threatview

GLOBAL PRESENCE

Office
Local presence

12+ Languages

1,000s of Satisfied Clients

20+ Countries

United Kingdom (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

FOREGENIX