FLARE SYSTEMS
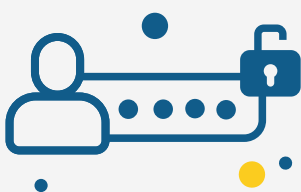
PHPMAILER ABUSE TO SEND SPAM EMAILS

Spam ranks as a high threat vector for organizations. The PHPMAILER library has been widely adopted in the criminal underground as a tool to send spam and monitor the health of spam campaigns.

Access to PHPMailer libraries is offered for sale on multiple marketplaces like Olux.io.

WHAT CAN YOU BUY ON OLUX.IO?
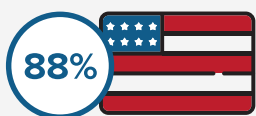
STOLEN & HACKED CREDENTIALS
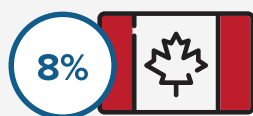
HACKED PHPMAILER INSTALLATIONS

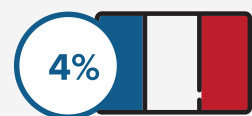**LISTS OF EMAIL ADDRESSES**

THE SIZE AND SCOPE OF THE MARKETPLACE

DISTRIBUTION OF PHPMAILER INSTALLATIONS

88% United States
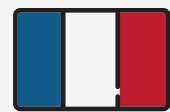
8% Canada

4% France

NUMBER OF PHPMAILERS PUT UP FOR SALE ON A DAILY BASIS:

United States
2-20

Canada
1-32
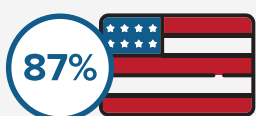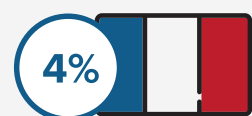
France
83-581

ORIGIN OF VISITORS TO OLUX.IO

29% Nigeria

23% Morocco

13% UK

9.9% Taiwan

REVENUE DISTRIBUTION

87% United States

9% Canada

4% France

PHPMAILER PRICING

$2
Min Price

$20
Max Price (France)

$30
Max Price (US)

$7
Avg Price

PROFILE OF HACKED PHPMAILER INSTALLATIONS

59%
Did Not Send a Test Email to Validate Uptime

7%
Run on Live Websites

30-87
Avg Days for Sale

450
Day Old Installs Questions the Operational Value

HOW SHOULD YOUR ORGANIZATION RESPOND?

1 Do not rely solely on the reputation of the SMTP server sending you emails

2 Check in with your email filtering provider to better profile suspicious senders