FLARE SYSTEMS

The Spam Email Business: A Comparison between Canada, USA, and France

May 2021

Authors

David Hétu, PhD, Chief Research Officer
Luana Pascu, Cybersecurity Researcher

Executive Summary

Despite the numerous sophisticated attack methods, spam still ranks as a high threat vector for organizations. According to the latest numbers, as many as 95% of attacks targeting enterprise networks are generated by successful spear-phishing. Some 30% of phishing emails are opened by users, with 12% of these targeted users clicking on the malicious link or attachment. The statistics claim 1 in every 8 employees shares information on a phishing site, with a single spear-phishing attack resulting in an average loss of $1.6 million.

Many spammers lack the time, expertise, and resources to acquire an infrastructure that can pump out large amounts of spam. Instead, they rent out infrastructures that have been hacked by others and use them to send spam for as long as they can.

This research report offers a glimpse into the reasons why detecting and blocking inbound spam in your corporate network may be a challenge. Malicious actors often rent out servers with a good reputation to appear legitimate. As a result, the email coming from these servers might not be detected by company networks as infected with malware or with links to phishing sites.
Flare Systems researchers investigated how easily accessible PHPMailers are on Olux.io and how they can be abused to send out spam campaigns. Based on an analysis of Canada, U.S., and France, the team also looked into the size and scope of the Olux.io marketplace, and vendor and hosting service profiles, as well as the profile of hacked PHPMailer installations.

At the time of writing, our team has found that malicious actors can easily rent PHPMailers from Olux.io because there are thousands available for rent at a low cost. In case of malfunction, they can easily be replaced for cheap. This leads us to believe that there could be no benefit in purchasing a PHPMailer located in a specific country. As far as Olux.io traffic sources are concerned, our data reveal Nigeria, Morocco and the UK are the top sources driving traffic to this website.

Moving forward, organizations can protect themselves by looking into the methods deployed by their email filtering providers and keep in mind that geolocation analysis for spam might not protect them from incoming spam.

Table of Contents

1 | PHPMailer Library Abuse

PHPMailer is perhaps the oldest, and most popular, PHP library to send emails. Anyone can download it from Github and install it in a matter of minutes. Known for its reliability and efficiency, the library provides additional features such as the ability to send HTML and non-HTML emails, as well as extensive error messages to report on its activities. It was first created in 2001 by a Brent R. Matzelle and was used in 2009 by over 9 million individuals. It is still run by volunteers and available in 47 languages.

It is not surprising that this script has been extensively adopted in the criminal underground. Many posts in underground forums talk favorably about the library. See the example below:

> *Using a SMTP mailer (like phpmailer for example) is a much better and easier option, as it gives you much more options out of the box.*

Malicious actors can install the script on a hacked web server. The server's resources and reputation are then abused to **send out spam that appears to be coming from a legitimate source.**

News report of a vulnerability in PHPMailer

Another option is to exploit a vulnerability in an installed version of PHPMailer to make it send spam. PHPMailer is regularly updated to fix security flaws, but it is not always timely updated on web servers. This opens an important window of attack that can be abused by malicious actors.

2 | PHPMailers for Rent on Olux.io

Olux.io is a popular clearnet marketplace that facilitates the sale of numerous illicit goods and services, including:

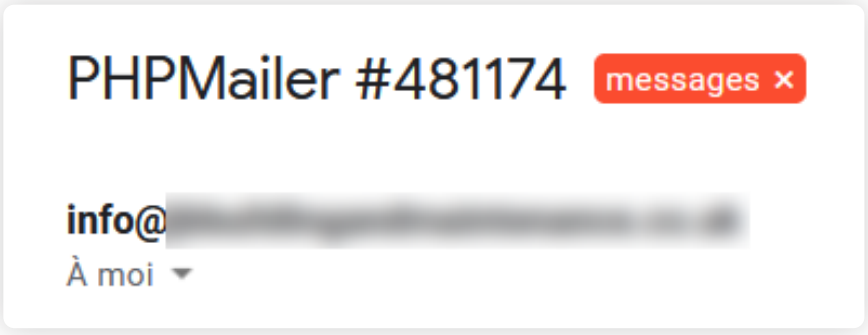
- Stolen and hacked credentials for remote desktop protocol sessions, SSH connections, and shells
- Hacked PHPMailer installations
- List of email addresses

All the products for sale on Olux.io are conveniently organized by country and type. In the screenshot below, you can see the **information available when purchasing a hacked PHPMailer.** The buyer knows the seller's ID, how long the PHPMailer has been up for sale, on what server it is hosted, as well as the country where the server is hosted.

ID	Country	Detected Hosting	Seller	Send Test to	Price	Added on	Buy
451031	Brazil	AWS EC2 (sa-east-1)	seller74	Send	6	01/26/2021 01:06:29 am	Buy
467819	United States	Cloudflare, Inc.	seller165	Send	7	03/01/2021 06:07:46 am	Buy
484438	France	OVH SAS	seller127	Send	5	04/05/2021 10:54:14 pm	Buy
390476	United States	Incapsula Inc	seller26	Send	7	10/18/2020 06:01:17 pm	Buy
478103	France	OVH	seller74	Send	10	03/22/2021 02:40:34 pm	Buy
484317	Germany	Hetzner	seller26	Send	7	04/05/2021 08:39:38 pm	Buy

PHPMailers for sale on Olux.io

Customers are allowed to test a hacked PHPMailer installation before the purchase. When they do, they receive an email that contains the ID of the PHPMailer for sale, as well as the domain name of the hacked server that is hosting the PHPMailer's installation.



Spam test email received from Olux.io

3 | Methodology

For 10 days in April 2021, our research team scraped the PHPMailers for rent from Canada, the United States, and France on Olux.io on a daily basis. This enabled us to determine which PHPMailers were put up for sale on any given day, and which disappeared (sold) on those same days. The data is usually collected and available in our Firework tool. **These countries were chosen for the following reasons:**

Based in Canada, our mission is to provide an empirical analysis of the often overlooked Canadian criminal underground.

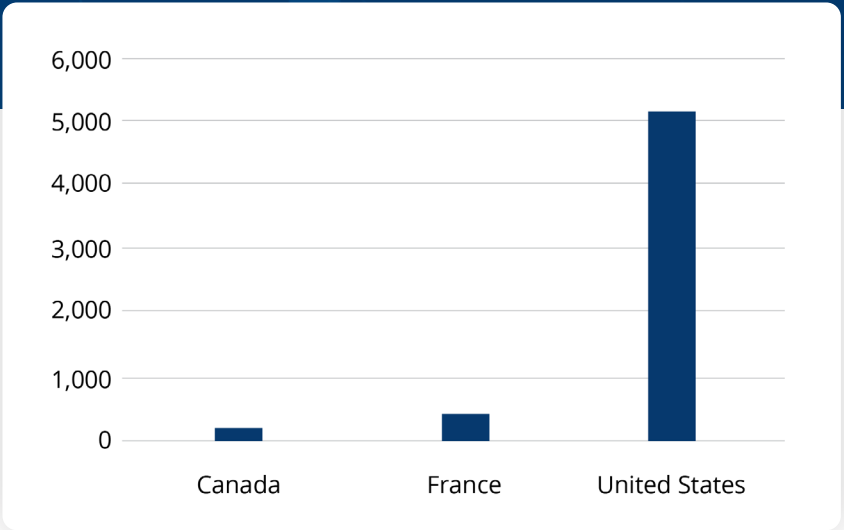
The United States is the biggest source of PHPMailers.

France is the closest country to Canada, in terms of population and GDP per capita. The comparison is not perfect, as France does have a larger population.

Moving forward, in our analysis, we take a closer look at the size and scope of the Olux.io marketplace, and vendor and hosting service profiles, as well as the profile of hacked PHPMailer installations.

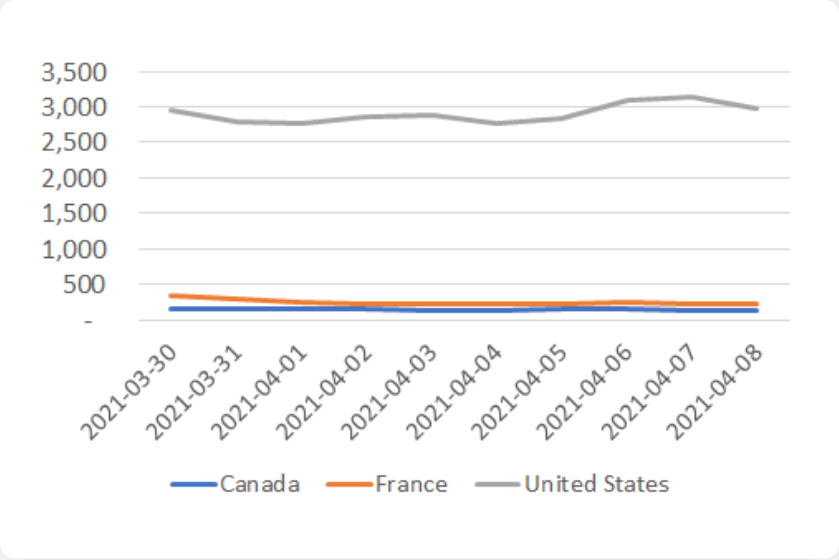
4 | The Size and Scope of Olux.io

For 10 days, we identified a total of 5,773 PHPMailer installations for rent on Olux.io. Most are represented by the United States (N = 5,103), while Canada comes in third with 234 PHPMailers. France, our reference country, has almost twice as many PHPMailers (N = 436) as Canada.



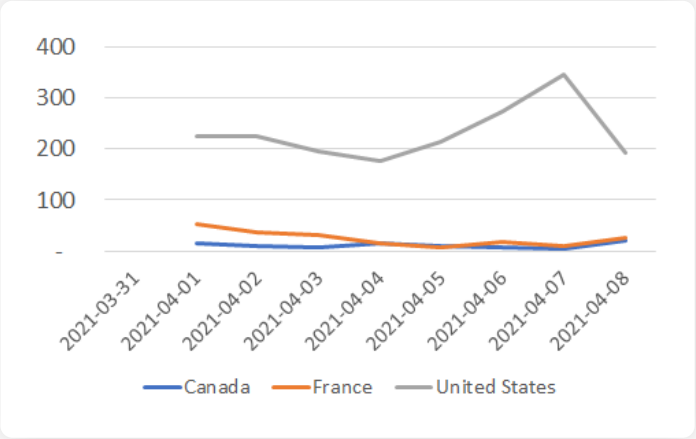
Distribution of PHPMailers in Canada, France and the United States

The number of PHPMailers offered on any given day on Olux.io remains relatively stable for each country. The United States varies in absolute numbers more than the other two countries combined, but this is to be expected since it owns the majority of PHPMailers for rent. For Canada, the number varies between 129 and 159 in the given timeframe.



Evolution of the distribution of PHPMailers across 3 countries

If the number of PHPMailers remains stable over time, it is likely due to the balance between the new PHPMailers being put up for sale, and those being sold. In the figure below, we show the daily number of PHPMailers sold on Olux.io. A PHPMailer is considered sold if it is seen on the website during the data collection period but disappears before the end of the period. There are between 5 and 20 PHPMailers hosted in Canada sold on any given day, about a third of the sales for France, and a few percent of those made in the United States.



Distribution of new PHPMailers for sale in Canada, France and the United States

In Canada, the number of PHPMailers put up for sale on a daily basis varies between 2 and 20. As far as France is concerned, this number ranges from 1 and 32, and for the United States between 83 and 581. In all cases, the flow (difference between new PHPMailers and those sold), remains under 100 per day.

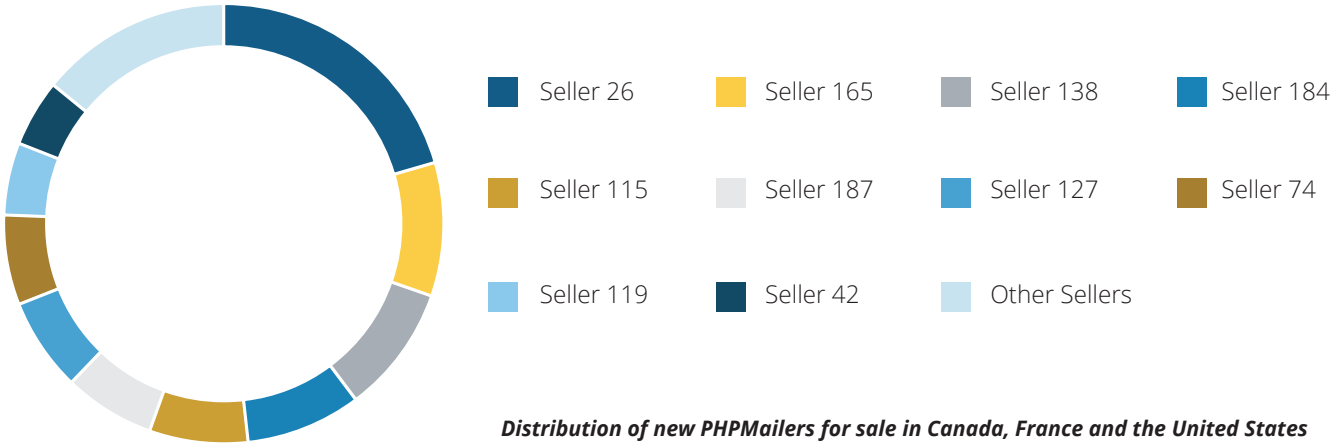
We used the marketing service SEMRush service to identify the source of traffic going to Olux.io. The figure below suggests that Nigeria, a country well-known for its spamming and Nigerian scams, is the biggest driver of traffic with 29% of visitors. Another African country, Morocco, comes in second. The UK ranks third. Canada was driving most of the traffic to the website until April 2020. Since then, for unknown reasons, the number of visitors went down significantly.

Countries	Traffic Share
Worldwide	100%
NG	29%
MA	23%
UK	13%
TN	9.9%
Other	25%

Origin of web traffic to Olux.io

5 | Vendor Profile

While some are more active than others, there is little known about the vendors beyond their ID on Olux.io. The main seller, seller26, posted about 20% of all PHPMailer installations for rent. Seller165 and seller138 come in with 10% of all PHPMailers each. As a result, there is a distinct group of about 10 sellers able to post more PHPMailers.



Distribution of new PHPMailers for sale in Canada, France and the United States

To calculate their revenue, we added up the price of PHPMailers sold by each seller. This provided us with a nine-day estimate per seller, which we can use to extrapolate revenue for a year if scaled linearly.

	9-DAY REVENUE (USD)	ESTIMATE FOR A YEAR (USD)
seller26	**$3,992**	$161,898
seller115	**$1,859**	$75,393
seller138	**$1,715**	$69,553
seller165	**$1,316**	$53,371
seller74	**$1,092**	$44,287
seller187	**$1,005**	$40,758
seller184	**$945**	$38,325
seller127	**$660**	$26,767
seller195	**$513**	$20,805
seller119	**$445**	$18,047
All other sellers	**$2,112**	$85,653

Revenues of vendors

Our estimates suggest that, on average, sellers only make a few hundred dollars per year selling PHPMailers on Olux.io. Of course, they can probably count on multiple revenue streams so this figure does not represent the entirety of their income. The top earner, seller26, has likely earned over $165,000 through Olux.io. Only 8 other sellers probably broke through the $20,000 barrier.

While there appears to be a correlation between the number of PHPMailers for sale and revenue, the link is not perfect given that seller115, for example, is the second top earner, but comes in fifth when the number of PHPMailers for sale is counted. This suggests that both metrics must be calculated to identify the key players on Olux.io.

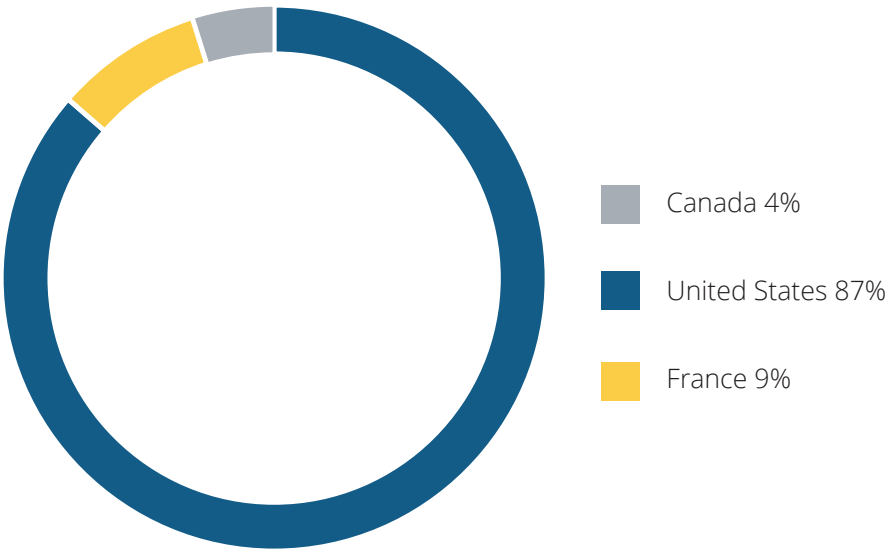
Revenue distribution across countries almost perfectly matches PHPMailer distribution. Canada has 4% of all PHPMailers and represents 4% of all sales. This can be explained by PHPMailer pricing:

THE MINIMUM PRICE FOR A PHPMAILER IS $2 IN ALL THREE COUNTRIES.

THE MAXIMUM PRICE IS $20 FOR CANADA & FRANCE, $30 FOR THE UNITED STATES.

THE AVERAGE PRICE OF A PHPMAILER VARIES BETWEEN $6.90 IN CANADA, & $7.50 IN FRANCE.

This finding suggests that malicious actors do not put a premium to rent out a PHPMailer in one country or another. Therefore, there could be no benefit in purchasing a PHPMailer located in a specific country.

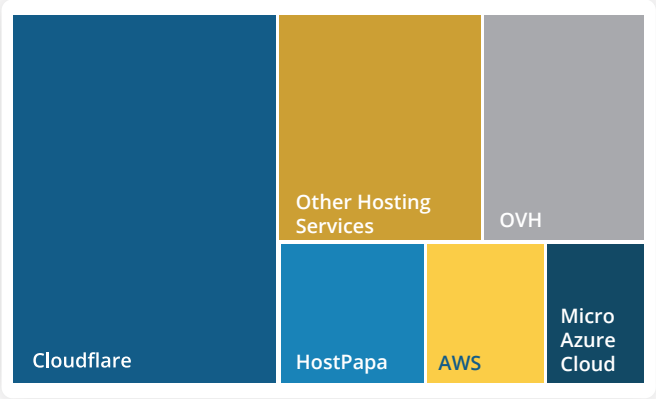


Distribution of revenues from the sale of PHPMailers in Canada, France and the United States

6 | Hosting Service Profile

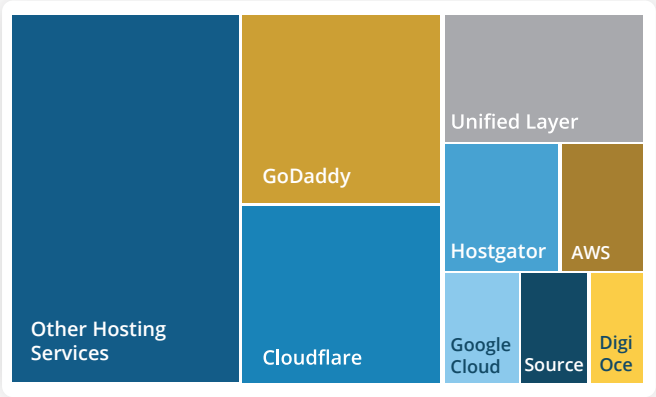
Web hosting services are not responsible when one of their thousands of users is hacked. However, they have a role in identifying potential compromise.

It is difficult to profile web hosting services through public scanning. Servers can be behind load balancers, anti-DDoS services which obfuscate the true hosting service. This appears to be the case with Canadian PHPMailers who are disclosed as hosted by CloudFlare, a popular anti-DDoS service. OVH is the most common web hosting service in Canada, followed by HostPapa, a Canadian web hosting service.



OVH is a popular hosting service in France. The vast majority of PHPMailers for rent are hosted on OVH. To a lesser extent, we also see that some AWS and Microsoft Azure Cloud servers are abused.

The picture in the United States is complex, with a lot more players being attacked. Besides Cloudflare, we see that GoDaddy and Unified Layer appear to be major sources of PHPMailers for rent.



These results suggest that some web hosting services are more targeted than others. Our dataset does not indicate why. Malicious actors may either be targeting larger web hosting services to hide among the mass of customers or targeting services less prone to search for hacking evidence in their customers' infrastructure.

This is not necessarily a bad thing for web service providers. Many have the policy to let their users operate on their own, without any checks and control of what is happening on their servers. This freedom however comes at the cost of more spam being sent out.

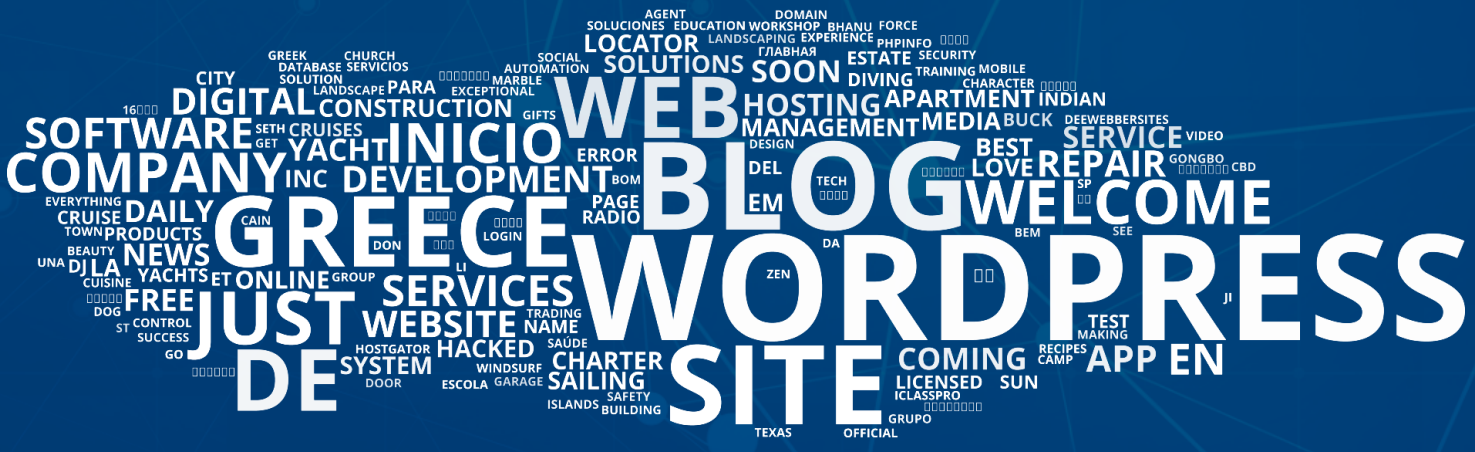
7 | Profile of Hacked PHPMailer Installations

When we tested the 5,773 PHPMailers, we only received 2,395 test emails. This suggests a 41% success rate.

This does not mean that 59% of PHPMailers for sale are fraudulent, meaning that they could not be used to send out spam if rented. There are many reasons why emails do not get to their destination, and unfortunately, we could not test each PHPMailer more than once for technical reasons. Still, it is something to consider when evaluating the service of Olux.io.

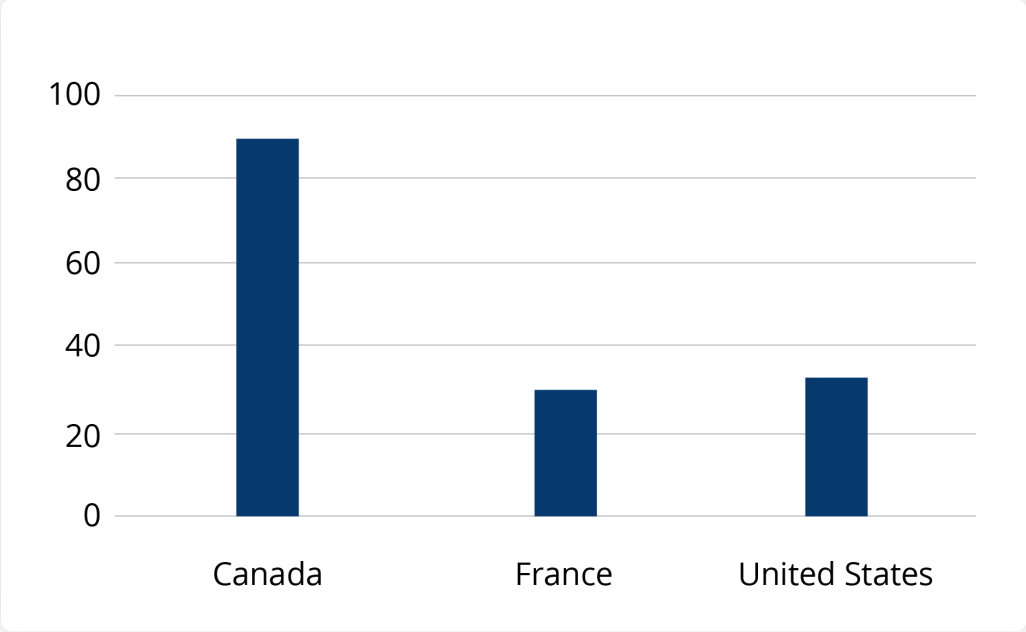
For each PHPMailer, we obtained the domain name of the server it was hosted on. We tried to download the home page of each domain, pinging either the domain name itself or prepending www to it if nothing was returned on the first try. In this analysis, we found that only 394 websites were up and running. This suggests that only 7% of PHPMailers are being run on servers hosting a website, most of them being run from web servers that appear to not be in use currently to host a website.

For each, we extracted the content of the title tag of the page. The word cloud below presents the main words found in the titles. We notice that WordPress and blog are the two most common words found, perhaps pointing to these as targets of malicious actors. The word Greece appears to be predominant, but that is mainly due to a single web page about Greek yachts and sailing that has the word repeated over and over again in the title. Another interesting finding is the word company which suggests that many hosting services appear to be related to companies rather than individuals.



Word cloud of the titles of hacked websites hosting PHPMailers

Finally, we calculated the average age of PHPMailers, respectively how long they had been for sale on Olux.io. Our data suggest that, on average, PHPMailers are for sale between 30 days (France, Canada) and 87 days (United States). The higher number for the United States can be explained by the higher level of competition among sellers, and the increased supply of PHPMailers. The maximum age of PHPMailers is around 450 days, meaning that unsold PHPMailers remain available on the website even when they are probably not operational anymore, or have not been maintained for quite some time.



Length of time for sale of PHPMailers in Canada, France and the United States

8 | Conclusion

Based on our analysis, malicious actors do not require much effort to rent out PHPMailers for spam campaigns. On any given day, there are thousands of PHPMailers available for rent for just a few dollars. Even when mailers do not perform adequately, they can be quickly replaced for cheap.

Our findings highlight the challenge of detecting and blocking inbound spam in your corporate network. Malicious actors rent out virtual private servers that should have a somewhat high reputation. They are, or were at some point, used to host blogs and corporate websites, and therefore appear legitimate. Emails coming from these servers are likely to be seen as innocuous even though they could be spreading malware or links to phishing sites.

While easily accessible, the PHPMailers we profiled may not be of equal quality. Indeed, many of them never managed to send us a confirmation email, raising doubt about whether they are still online or not. Moreover, there are quite a few PHPMailers that have been for sale for weeks, if not months on Olux.io. This artificially increases the number of available PHPMailers on the website and makes it look as though the marketplace is more active than it is. In reality, much of the new daily supply is offset by the sales, and the number of mailers for sale, therefore, remains relatively stable.

Our analysis raises once again concerns regarding the role web hosting services play in spam prevention. Some web hosting companies actively monitor what their customers do with their servers, and their internet connection. There is a debate to be had about the freedom to operate with no surveillance from large companies and the freedom that the internet was supposed to afford to its users. Still, given the significant impact that spam has on companies large and small, the question remains whether web hosting services should be good citizens and detect as often as possible these hacked PHPMailers. The limited number of web hosting services also helps us understand how small changes in just a few providers could go a long way to fight against spam.

9 What Should Your Company Do?

This report suggests that the spam you receive daily could be coming from virtual private servers with a high reputation. Your company should inquire with your email filtering providers how such emails are treated, and if they receive extra inspection given the suspicious nature of their sender.

You should also know that spam can and will be coming from all countries in the world and that Canadian servers are not immune from sending out spam. Despite common belief that spam originates from Russia and China, that facilitated by Olux.io is likely coming from the United States. This reminds us that any geolocation analysis for spam will likely not protect us much from incoming spam.

You could also incorporate the data stream for the hosting service provider into your spam filtering systems to look more closely at emails coming from hosting services that appear to be victimized by hacked PHPMailers. We identified the biggest players in this ecosystem, and it may be reasonable to give a second look at emails that are coming from these companies' web servers.

About Flare Systems

Since 2017, Flare Systems has been developing AI-driven technologies that automate fraud detection and prevention. Firework offers an easy-to-use platform that gets you the right information before risks become unmanageable. Reduce digital risk and fraud with Firework, the digital risk protection (DRP) platform that automates your dark, deep and clear web monitoring to deliver real-time actionable intelligence.

Book a Demo

www.flare.systems
hello@flare.systems

1751 Rue Richardson, Unit 3.107
Montreal, Quebec, H3K 1G6