Gone Phishing: 2015 Global Malware Round Up Report

WWW.PHISHME.COM
Executive Summary

In 2015, the information security community witnessed a series of the most devastating cyber-attacks and costly data breaches—from Primera and Anthem, to OPM and the Ukraine power plants—all of which had a consistent trend in common: the inevitable failure of both the perimeter and weakened layers of automated security technology. Next-generation firewalls, machine-generated intelligence feeds, anti-virus and secure email gateways could not defend networks against the harsh proliferation of data resulting from carefully planned spear phishing attacks that ultimately impacted the world’s biggest brands and government organizations at the core; trampling bottom lines, forcing resignations for C-level executives and shutting down business operations affecting hundreds and thousands of people worldwide.

We continued to observe that legacy perimeter defenses have consistently failed to identify and stop every phishing attack targeting your employees’ email inboxes. Sooner or later, a phishing email will slip past security technology layers, land in the inbox of employees that haven’t been conditioned to identify and report suspicious communications, and then trick them into participating in a malicious activity, such as a fraudulent wire transfer, giving up information that exposes networks or downloading malware.

This white paper provides information security professionals, technology leaders, incident response teams and threat intelligence analysts with insights into the most effective phishing attacks in use today and the malware payloads they deliver. The report helps readers understand why standard perimeter defenses and machine-based intelligence are simply not enough to thwart phishing attacks. In the report, we provide a number of actionable insights designed to add immediate value to your security programs:

- Dyre malware ceased operations in 2015, leading our threat researchers to conclude that an entirely new strain, yet to be identified by machine technologies, may be in use and on the rise.
- Attackers frequently used Microsoft Office Documents attached to phishing emails to slip malware such as Dridex, Pony and Dyre past technology layers and into corporate networks.
- Spam filters and other automated engines are no match for attackers’ ability to adapt and customize phishing email elements such as subject lines, making it easier and easier for criminals to get in.
- A combination of human-vetted intelligence, analysis, response and conditioning is the only defense against phishing attacks that make their way past perimeter defenses, and what made identification of the above threats possible.
- How some of the largest organizations in the world, including 45 of the Fortune 100, are using PhishMe to build an effective phishing defense strategy that leverages conditioning, phishing analysis and deep malware intelligence to transform humans into the strongest links in the security chain.
Introduction

Incident Response (IR) teams are forever fighting an uphill battle as attack vectors continually evolve to spoil the latest and greatest security defenses. As information security professionals manage to quarantine and eliminate one type of malware, more dangerous malware alternatives are being bred for use in their stead, forcing organizations to remain alert and on their toes for the next attack.

The challenge in cyber-security is simple; it's a numbers game. The more security teams and comprehensive programs your organization has in place, the better chances you have to prevent attacks and mitigate risk. However, hiring experienced security experts and investing in enterprise security technology can be daunting for many organizations. Experts who can effectively protect your network are expensive and there's a shortage because their skillset is incredibly in demand. Malicious actors know this, and use it to their advantage when planning attacks. Some security software vendors try to sell a generalized vision of prevention that offsets the shortage of human resources. Sadly, these visions are rarely realized, as it takes both qualified humans and strong toolsets to effectively combat attacks and reduce risk.

If you look at any notable breach report in the last five years, there are three consistent themes:

• Breaches continue to occur in record numbers.
• Identification takes place well after the damage has occurred.
• The most consistently preferred attack target is an organization's human assets.

As security budgets skyrocket and businesses scramble to determine the best products and services to fit their programs, one major solution is often overlooked: transforming human assets that were once risk factors into a powerful engine of sensors that feed vetted intelligence into your incident response teams in real time. Every organization has these human sensors, often only viewed as potential areas of risk. These groups can add tremendous value to defensive strategies, as there's already a natural desire in place for these employees to help.
2015 – Major Moments in Malware

We’ve taken a look at the major events that have shaped phishing and the malware that has been delivered throughout 2015. There are several interesting trends that we’ve observed.

- Major phishing infrastructure was taken offline last year
- Continued use of weaponized Office Documents
- Testing of new delivery methods exploits
- Mass customization of senders and subjects to bypass controls

The Death of Dyre

One of the biggest events of last year was the demise of Dyre. PhishMe first identified Dyre in June 2014, and this trojan quickly evolved from a straightforward remote access trojan to a full-fledged financial crime and espionage toolkit backed by a robust botnet infrastructure. However, after November 19, 2015 this powerful malware disappeared from the threat landscape.

It is not clear what led to Dyre’s disappearance but as the chart below shows, the number of unique samples collected by PhishMe Intelligence were identified as delivering the Dyre malware. Starting about halfway through 2015, the raw numbers of Dyre emails began to decline, with a 94% drop in number of emails collected from April 2015 through October 2015, indicating that the threat actors were drawing back their distribution. As the final date of Dyre distribution neared, the number of emails delivering the malware continued to trend downward. The decline continued until the middle of November after which no further emails were identified.

As is frequently the case, whenever a prominent malware disappears from the threat landscape a handful of other malware varieties often emerge. Sometimes these new varieties constitute full-fledged replacements for a major malware in the way that Dyre was a logical successor of the GameOver Zeus botnet. In other cases, these represent experimentation by threat actors with more obscure or less popular malware varieties.
The Rise (and Fall) of Nymaim and TeslaCrypt

In November when the number of new Dyre samples was on the decline, a handful of malware varieties that did not previously have a strong foothold in the phishing landscape began immediately popping up in Dyre’s wake. Two of the most notable were the older Nymaim botnet malware and the innovative TeslaCrypt encryption ransomware. As the chart below shows, threat actors made new inroads on the phishing market using these malware varieties in late November.

Figure 1: Entrance of Nymaim and TeslaCrypt onto threat landscape as Dyre recedes

However, as can be seen above, the rise of these new introductions to the threat landscape were short lived as they subsided before the end of the year. It is notable that as of the end of 2015, no clear successor to the Dyre trojan had emerged. What has become obvious is that attackers are continuing to adapt their attacks to find new ways to beat technologies.

Dridex: Continued Rise to Malware Fame in 2015

One of the most popular attack evolutions is the frequent weaponization of the full spectrum of Microsoft Office documents using hostile macro scripts. These OfficeMacro documents persist as one of the most popular techniques used by attackers to gain a foothold in enterprises. The reason is simple—Office documents are mission critical to organizations of all sizes. Therefore, blocking these types of threats is virtually untenable.

Additionally, a wide variety of malware payloads are being delivered via this medium. This serves as a testament to the adaptability and ease of use provided to threat actors by this malware delivery technique. At the top of the list of malware payloads delivered by OfficeMacro documents is Dridex, followed by Pony and Dyre.
Looking at the usage of Office documents over the year, it’s very clear that threat actors have been experimenting with this type of payload to determine if it would be successful. Threat actors using Dridex have been leveraging this mechanism all year, dramatically accelerating in October of 2015. Dyre, on the other hand, began using this more frequently in April.

Finally, threat actors delivering Pony were first observed in March, and really began to expand their usage throughout the year as a medium for delivery. An honorable mention is the delivery of the Neverquest financial crimes trojan, often seen in conjunction with the Pony information stealer and downloader. Delivery of this financial crimes trojan surged over the last half of the year with OfficeMacro documents providing a reliable means for securing infections.

JavaScript: Malware’s Latest Partner in Crime

Another payload delivery method that had a noticeable uptick in 2015 was the use of obfuscated JavaScript applications tasked with downloading malware payloads. Use of these JSDropper applications was observed with some initial testing in Q1 and Q2 of 2015, but we observed a rapid growth in Q4.

There were a number of payload malware families that were distributed using JSDropper throughout the year. The heaviest users were Cryptowall, TeslaCrypt, FakeAV and Poweliks.
What's extremely interesting is that three of those malware families showed absolutely no activity using this delivery method until Q4 of 2015. As discussed in our Q4 report, these families made a resurgence after the Dyre botnet stopped, and they have remained very active in the time since.

The Decline of Unique Subject Lines in SPAM Emails

One trend that remained consistent over the past year was the continued use of unique subject lines and senders. In an analysis of 218 distinct spam campaigns being used to deliver Dyre, we observed more than 30,000 unique subject lines. Only a single subject-line was used more than a dozen times. The spam campaigns used three types of mass-customization to customize email subjects using templates that allowed keyword substitution from a list of potential values.

The subject of the email messages in these cases involves combining a word from each of three variables:

\[ S1 = \text{[Negotiated|Oustanding|Potential|Prepared|Suggested]} \]

\[ S2 = \text{[income tax|levy|tax]} \]

\[ S3 = \text{[advice|memo|note|plan|report|statement]} \]

The combinations yield ninety possible subject lines, ranging from “Negotiated income tax advice” to “Suggested tax statement”.

Here's an example of another template, just showing the variations where the first term was ACH:

<table>
<thead>
<tr>
<th>ACH failed due to system failure</th>
<th>ACH failed due to technical error</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACH payment failure notice</td>
<td>ACH transaction failure report</td>
</tr>
<tr>
<td>ACH payment failure report</td>
<td>ACH transaction technical failure</td>
</tr>
<tr>
<td>ACH payment technical error</td>
<td>ACH transfer error</td>
</tr>
<tr>
<td>ACH system failure</td>
<td>ACH transfer failure notice</td>
</tr>
<tr>
<td>ACH transaction error</td>
<td>ACH payment error notification</td>
</tr>
<tr>
<td>ACH transaction error report</td>
<td>ACH Payment Notification</td>
</tr>
<tr>
<td>ACH transaction failed</td>
<td>ACH transfer failure</td>
</tr>
<tr>
<td>ACH transaction failure notice</td>
<td>ACH transfer failure notification</td>
</tr>
</tbody>
</table>

Or another, warning of additional fees for delaying the filing and submission of tax information:

<table>
<thead>
<tr>
<th>Additional penalty amounts for failure to file</th>
<th>Extra fine amounts for failure to fill up</th>
</tr>
</thead>
<tbody>
<tr>
<td>Additional penalty amounts for failure to fill up</td>
<td>Extra fine amounts for failure to provide</td>
</tr>
<tr>
<td>Additional penalty amounts for failure to send</td>
<td>Extra fine amounts for failure to send</td>
</tr>
<tr>
<td>Additonal amounts for failure to file</td>
<td>Fine amounts for failure to file</td>
</tr>
<tr>
<td>Additonal amounts for failure to fill up</td>
<td>Fine amounts for failure to fill up</td>
</tr>
<tr>
<td>Additonal amounts for failure to send</td>
<td>Fine amounts for failure to provide</td>
</tr>
<tr>
<td>Extra fine amounts for failure to file</td>
<td>Fine amounts for failure to send</td>
</tr>
</tbody>
</table>

Although a human reader would quickly see that all of these subjects seem to be closely related, many spam filters are still based on exact matching of forbidden subject lines. With mass customization, this problem gets worse, where random numbers can be used to provide infinite subject line possibilities.
The use of Randomization grew more complete as the year went on, with many campaigns using [Random First Name] [Random Last Name] as part of the subject, as seen in the following two sample sets:

Tammie Stevenson shared MonthlyStatement_AUG15.pdf“ with you”
Tammy Lawson shared MonthlyStatement_AUG15.pdf“ with you”
Tammy Mclaughlin shared UPDATE_VACATIONS_SCHEDULE_09_2015.pdf“ with you”
Tammy Solomon shared MonthlyStatement_AUG15.pdf“ with you”
Tamra Hyde shared MonthlyStatement_AUG15.pdf“ with you”
Tanisha Barrera shared MonthlyStatement_AUG15.pdf“ with you”
Tanisha Levine shared MonthlyStatement_AUG15.pdf“ with you”

The Bank INTERAC to Adam Pettit was accepted.
The Bank INTERAC to Adam Rattray was accepted.
The Bank INTERAC to Adam Riverman was accepted.
The Bank INTERAC to Alex Faed was accepted.
The Bank INTERAC to Alexis Savage was accepted.
The Bank INTERAC to Alexis Slocomb was accepted.
The Bank INTERAC to Anthony Pombert was accepted.
The Bank INTERAC to Anthony Szusa was accepted.
The Bank INTERAC to Antoine Stone was accepted.
The Bank INTERAC to Arnaud Peters was accepted.
The Bank INTERAC to Arnaud Shipley was accepted.
The Bank INTERAC to Arthur Shea was accepted.

Names were combined with templates to create extraordinary levels of customization such as the fax message subject lines seen below:

fax (Adell Oberbrunner forward research executive)
fax (Adrain Prohaska forward data manager)
fax (Adrianna Bartoletti direct mobility facilitator)
fax (Aileen Powlowski district applications administrator)
fax (Al Wuckert central interactions assistant)
fax (Aleen Bruen regional response manager)
In that campaign, 21 “org chart positions” (such as [central|chief|corporate|customer|direct|...]) were combined with 37 “department names” ([accountability|accounts|applications|assurance|brand|...]) and 25 “employee roles” ([administrator|agent|analyst|architect|...]) to create 19,425 possible subject bases, which then were each assigned a randomly selected First Name and Last Name. It is quite possible that millions of recipients each received a message with a globally-unique subject line.

Company names were also abused in this way, both in the form of real company names and realistic company names. A few thousand names were used in an Invoice INV-[random#] from [random company] [random#] campaign featuring real companies that ranged from AMERCO to Whirlpool Corporation.

**Authentically Fake Company Names Increase SPAM Open Rates**

In another campaign, at least thousands of imaginary law firms were created for a campaign featuring subject lines including realistic firm names, such as Hintz, Altenwerth and McCullough or Hickel, Decow and Breitenberg. In some cases, the credibility was further spoofed by appending a fake domain name to the subject, such as Invoice Block-Tillman—Mitchell.com or Invoice Bogan and Sons—buckridgereynolds.info.

As mentioned previously, this mass randomization has proven quite successful to bypass controls put in place to block on specific subjects and senders. While technology alone struggles to catch up to these attack evolutions, PhishMe customers continually prove that the conditioning and empowering of human sensors is a viable and strong defense in detecting and reporting these types of attacks.

**Phishing Simulation Trends – The 1st Line of Defense**

In 2015 we observed a 221% increase in the number of phishing simulation messages that we sent to our customers. Looking back at the last three years, we’ve observed a pattern shift in the types of scenarios that our customers have run. Between 2014 and 2015, the use of data entry scenarios has remained the same. Click-only scenarios remain our most popular among customers, but, for the first time, we’ve noticed a decline in the number of click only scenarios as customers have increased their attachment scenarios.

This transition is not unexpected and is fully supported by PhishMe. For years, users have been conditioned to believe that their organizations have a tremendous number of protections in place, so when an email attachment is received in their inbox, it’s safe to interact with. Sadly, that’s not the case, and we’ve been encouraging organizations to continue to condition their employees to report any and all suspicious activities that they observed in their inbox.
The conditioning of our users is proving to be effective. Between 2014 and 2015, we’ve observed a noticeable increase in the number of simulations where we observed more user reports than responses. There has been a 7% increase of reporting for attachments and click only scenarios.

This number has grown for two key reasons. First, user conditioning is proving effective, and second, we’ve seen an extremely large adoption of the PhishMe Reporter solution. Additionally, this continues to reap benefits for our customers’ incident response teams, as those empowered human sensors are also funneling them quality intelligence.

### Conclusion: Transforming Risk into Serious Security Defenses

It’s abundantly clear that the best way to defend against the evolving malware landscape is to fortify the attack targets, transforming once at-risk groups of employees and end-users into incident response professionals. As noted above, our research proves that when humans are properly conditioned and empowered, there’s a direct correlation in the spike of real-time attack alerts producing data and trends that are not just valuable, but completely indispensable for combatting attacks.

Through simulation and awareness, new forms of malware can be discovered quicker, reducing the window of opportunity for damage and immediately reducing risk.

Today, millions of end-users are being transformed into security defense powerhouses through the use of PhishMe technology. Now, security operations centers (SOCs) have a new partner in detecting and preventing malicious email attacks, effectively turning a major risk group into a strong, fortified defense.
About PhishMe
PhishMe® is the leading provider of human-focused phishing defense solutions for organizations concerned about their susceptibility to today’s top attack vector—spear phishing. PhishMe’s intelligence-driven platform turns employees into an active line of defense by enabling them to identify, report, and mitigate spear phishing, malware, and drive-by threats. Our open approach ensures that PhishMe integrates easily into the security technology stack, demonstrating measurable results to help inform an organization’s security decision making process. PhishMe’s customers include the defense industrial base, energy, financial services, healthcare, and manufacturing industries, as well as other Global 1000 entities that understand changing user security behavior will improve security, aid incident response, and reduce the risk of compromise.

Headquarters
PhishMe, Inc.
1608 Village Market Blvd.
Suite #200
Leesburg, VA 20175

New York Office
PhishMe, Inc.
817 Broadway, 4th floor
New York, NY 10003

San Francisco Office
PhishMe, Inc.
One Embarcadero Center
Suite # 510
San Francisco, CA 94111

London Office
PhishMe, Inc.
c/o Regus
London – Covent Garden
90 Long Acre
London, WC2E 9RZ

Dubai Office
PhishMe, Inc. (DMCC Branch)
Unit No: 30-01-449
Jewellery & Gemplex 3
Plot No: DMCC-PH2-J&GplexS
Jewellery & Gemplex
Dubai
United Arab Emirates

Singapore Office
PhishMe, Inc. (Singapore Branch)
c/o Regus
1 Raffle Place
Level 24 Tower 1
Singapore, 048616. Singapore