



Q1 2016 Malware Review

EXECUTIVE SUMMARY

During the first quarter of 2016, PhishMe Intelligence generated 612 Active Threat Reports detailing waves of phishing emails that delivered malware to victims around the world each day. These reports are the product of detailed analysis to isolate both the indicators of compromise for the malware delivered as well as the tactics and techniques used by threat actors to deliver that malware.

The goal of such reporting is to empower PhishMe's clients by delivering high quality, actionable intelligence regarding the most current phishing campaigns. This intelligence is available in machine-readable formats, analyst reports, and an investigation app. PhishMe publishes intelligence via API, email, and web interfaces throughout each day as new threats are confirmed by our analyst team. Access to the Intelligence API allows for the automated consumption of data that is enriched with context for use in a wide variety of security solutions. PhishMe Intelligence professionals also produce weekly Strategic Analysis documents addressing the threat landscape as a whole and investigating the nature of threat actor activity from a more holistic perspective.

As this report details, the first three months of 2016 brought three key trends recorded throughout 2015 to full fruition.

Encryption Ransomware:

Most notable is the proliferation of encryption ransomware.

Targets: Individuals, small- and medium-sized businesses, hospitals, and global enterprises are all faced with the reality that encryption ransomware is now one of the most favored online criminal enterprises. The current trend for this category of malware can be traced back to 2013 with the successful CryptoLocker malware used to further monetize machines added to the GameOver Zeus botnet.

Successes: The success of this malware triggered a cascade of imitations and further development of ransomware tools.

Status: Encryption ransomware has become a fixture of the phishing threat landscape and will continue to loom large as long as it proves a viable means for generating revenue for online criminals.

Soft Targeting by Functional Area:

Another 2015 trend that emerged into fuller fruition during the first quarter of 2016 is threat actors' use of soft targeting in phishing.

Targets: In contrast to both broad distribution and the careful targeting of spear phishing emails, soft targeting focuses on a category of individuals based on their role within any organization anywhere in the world.

Successes: Examples of soft targeting have demonstrated threat actors' interest in impacting disproportionately-sensitive elements within companies of all sizes. Encryption ransomware distributors have targeted human resources and hiring managers. Remote access trojan operators have targeted sales representatives at industrial firms.

Status: By the end of the quarter, using some of the most elaborate content, Nymaim botnet operators were observed targeting financial controllers at a variety of organizations, using publicly available details.

[In first quarter 2016, PhishMe intelligence conducted 612 malware analyses compared to 662 such analyses in fourth quarter 2015; however, the raw number of phishing email messages collected and analyzed was far greater in 2016. The number of unique email samples analyzed by PhishMe Intelligence, obtained through global collection points, can be used to extrapolate the relative size of the global count of phishing emails. This extrapolation compares the top one hundred largest phishing email sets from the first three months of 2016 to those of fourth quarter 2015, qualitatively clustered by content and malware payload. Disturbingly, this shows a real-number increase in global phishing email of 6.3 million and a percentage increase of 789%.]

Downloader/Ransomware: the one-two combination:

Targets: The source of this increase is the introduction of the Locky encryption ransomware and its distribution using massive numbers of JavaScript downloader applications.

Successes: Table 2 lists the ten largest collections of hostile emails and demonstrates the indisputable dominance of the JavaScript/Locky delivery combination.

Table 1 – largest sets of phishing emails Q1 2016

Threat ID	Malware Combination
5692	JSDropper, Locky
5667	JSDropper, Locky
5712	JSDropper, Locky
5560	JSDropper, Locky
5714	JSDropper, Locky
5545	JSDropper, Locky
5691	JSDropper, Locky
5530	OfficeMacro, JSDropper, Locky
5518	JSDropper, Locky
5592	JSDropper, Locky

PhishMe customers have access to the full threat detail by clicking on the Threat ID.

Status: Data hinted toward the growing prevalence of JavaScript downloader applications as a malware delivery option near the end of 2015 and over the first three months of 2016—most notably through its prolific use by the distributors of Locky—it became the favored malware delivery mechanism. During the first quarter, JavaScript applications (called JSDropper in Figure 1) even surpassed Office documents with macro scripts to become the most common malicious file type analyzed with JSDropper applications present in nearly one third of all analyses.

A Growing Concern:

While the Locky encryption ransomware represents the most commonly-analyzed malware variety from the first quarter, other mainstays were also strongly represented. Notable among these mainstays were the ever-popular Pony information stealer and malware downloader, the Dridex banking and general-purpose crimeware, as well as the Neverquest trojan, keyloggers, and the Andromeda botnet malware.

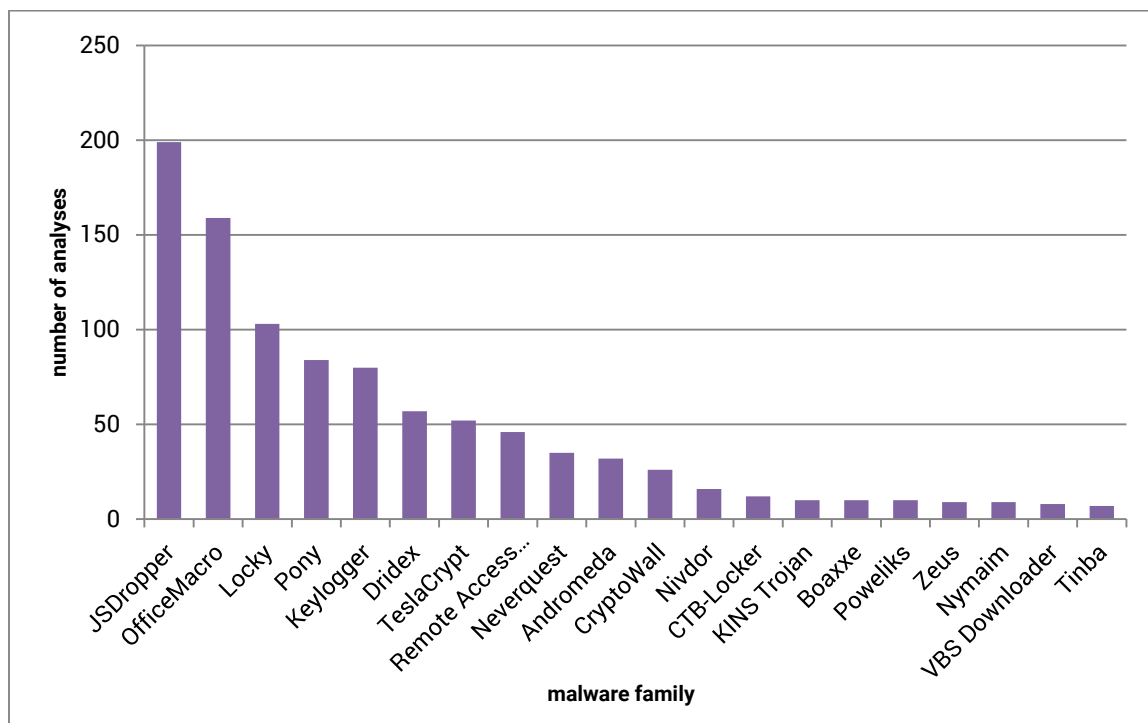


Figure 1 – malware analyses by family Q1 2016

USE OF MALWARE BY FAMILY

Many of the malware varieties identified during the first quarter are mainstays used by a variety of threat actors of varying sophistication levels. Many of the keyloggers analyzed are commonly associated with script kiddie actors as were many of the Pony malware samples. However, some examples of Pony deployments served as part of the distribution of a more sophisticated malware payload. Most notably, Pony was used as an intermediary tool through which the Neverquest financial crimes trojan was delivered to infected endpoints.

JavaScript applications used to download malware

In the fourth quarter of 2015, Visual Basic macro scripts included in Microsoft Office documents were the most popular means of delivering malware. However, as the year ended, JavaScript applications began to be used with greater frequency. Script applications written in JavaScript and Visual Basic are a logical choice for many threat actors due to the relative simplicity and ubiquity of these scripting languages. Furthermore, due to the presence of both the cscript.exe and wscript.exe applications, the small script applications used by threat actors are effectively executable programs within the Windows environment. This affords threat actors the ability to write and deploy a large number of hard-to-detect script applications to a widespread field of potential victims, with minimal investment in both knowledge and resources.

Monetizing infected endpoints: Growth in use of JavaScript as a malware delivery mechanism is closely tied to the growth in threat actors' encryption ransomware usage.

As Figure 1 shows, Locky - analyzed over one hundred times between February 16 and the end of the first quarter - secured the third position among all malware types. Locky holds the first position among "payload" malware varieties—those malware varieties delivered as the end-goal

for a threat actor. The prevalence of Locky, encryption ransomware as a whole - and to a lesser degree - the popularity of JavaScript downloaders both fit into a trend in which threat actors tend toward this easy means for monetizing infected endpoints.

Figure 2 shows that the overwhelming proportion of Locky and TeslaCrypt deliveries during the first quarter used JavaScript applications as a malware downloader. Of the nearly 200 uses of JSDropper applications during the first quarter, over half were used as the means for delivering either of these two encryption ransomware varieties.

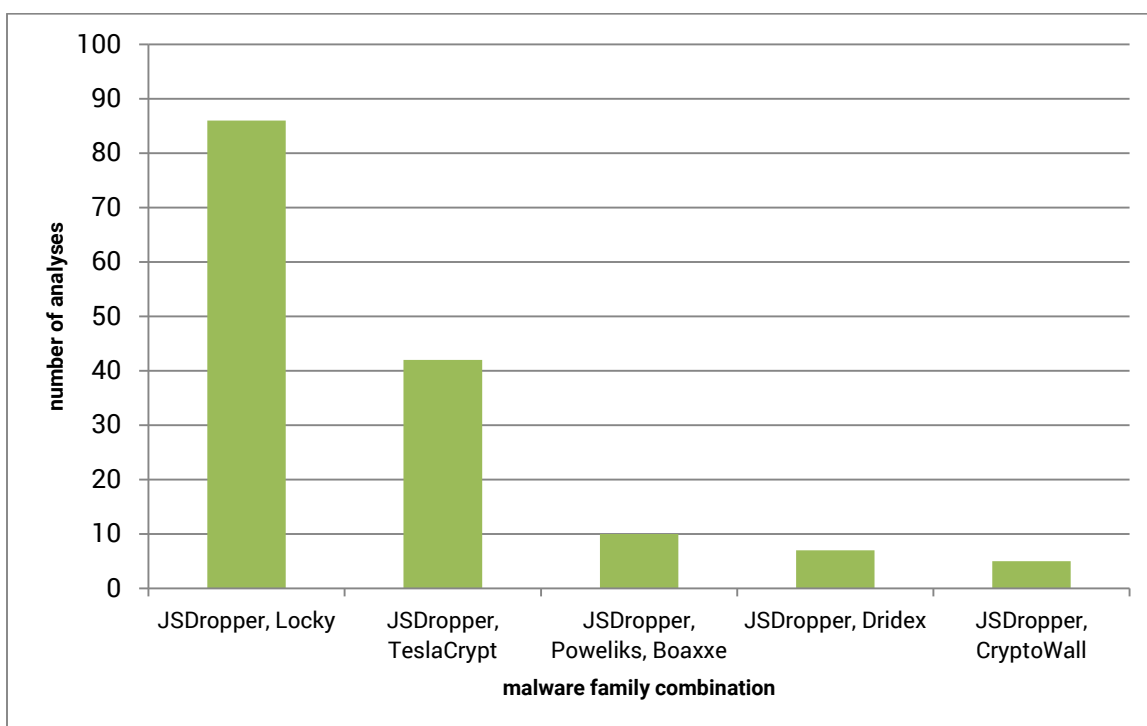


Figure 2 – top five malware varieties delivered using JSDropper applications

USE OF MICROSOFT OFFICE DOCUMENTS AS TOOLS STAYS STRONG

While overtaken by JavaScript applications during the first quarter of 2016, Microsoft Office documents containing malware delivery scripting continue to serve threat actors as a reliable tool. Much of this continued use was in conjunction with well-established tools such as Dridex, Neverquest, and CryptoWall as can be seen in Figure 3. However, the relative newcomer Locky was also delivered using this technique in a number of cases evidencing diversification in this malware’s distribution.

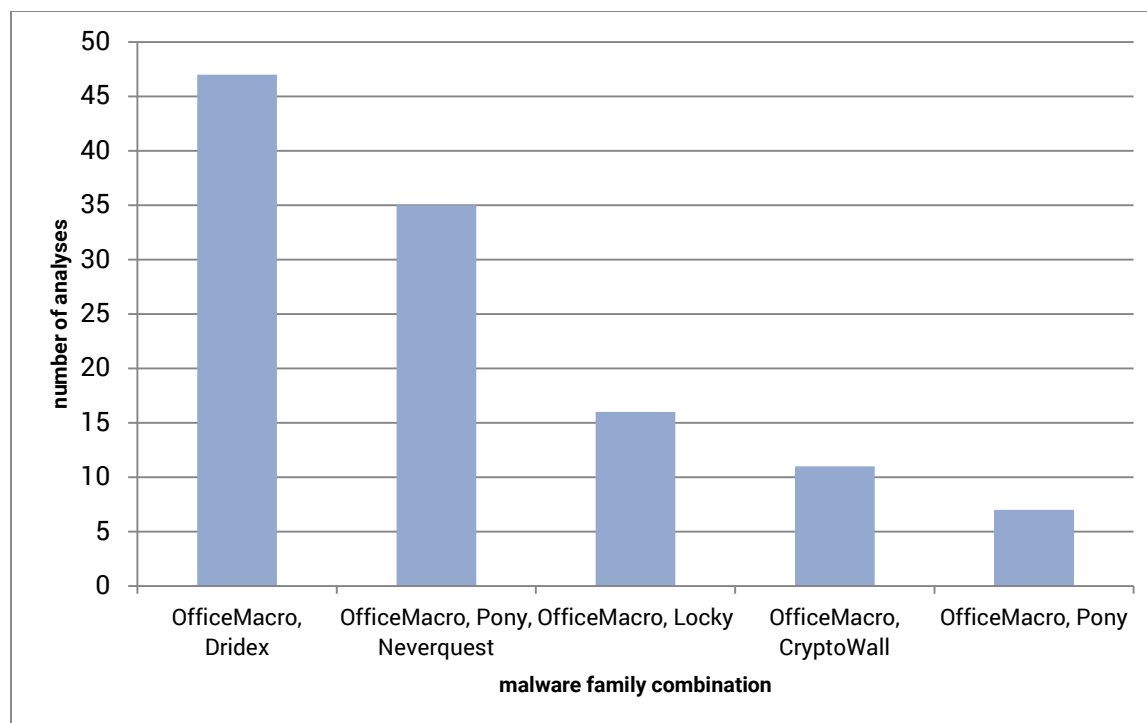


Figure 3 – top five malware varieties delivered using OfficeMacro documents

While JavaScript applications became a preferred utility for malware delivery during the first quarter of 2016, the reliability and utility of OfficeMacro documents has not diminished. The popularity gained by this malware delivery mechanism will likely continue to persist alongside JavaScript applications.

ENCRYPTION RANSOMWARE USAGE CLIMBS DRAMATICALLY

Among the top five malware combinations delivered by JSDropper applications, three are encryption ransomware. Among this top five, TeslaCrypt and CryptoWall accompany Locky to account for over a fifth of all malware analyses performed during the first quarter. This excludes deliveries of these ransomware varieties through other means but includes the explosive activity of the Locky encryption ransomware during February and March.

A closer look at time and tactics:

Over the past six months an increasing number of malware analyses involve encryption ransomware as shown in Figure 4. This trend began during the fourth quarter of 2015 but made the largest gains over the first quarter until approximately half of all malware analyses performed in March 2016 involved some variety of encryption ransomware. This marks a significant increase in the use of potentially destructive malware and threat actors' reliance on ransomware as a means for monetizing infections.

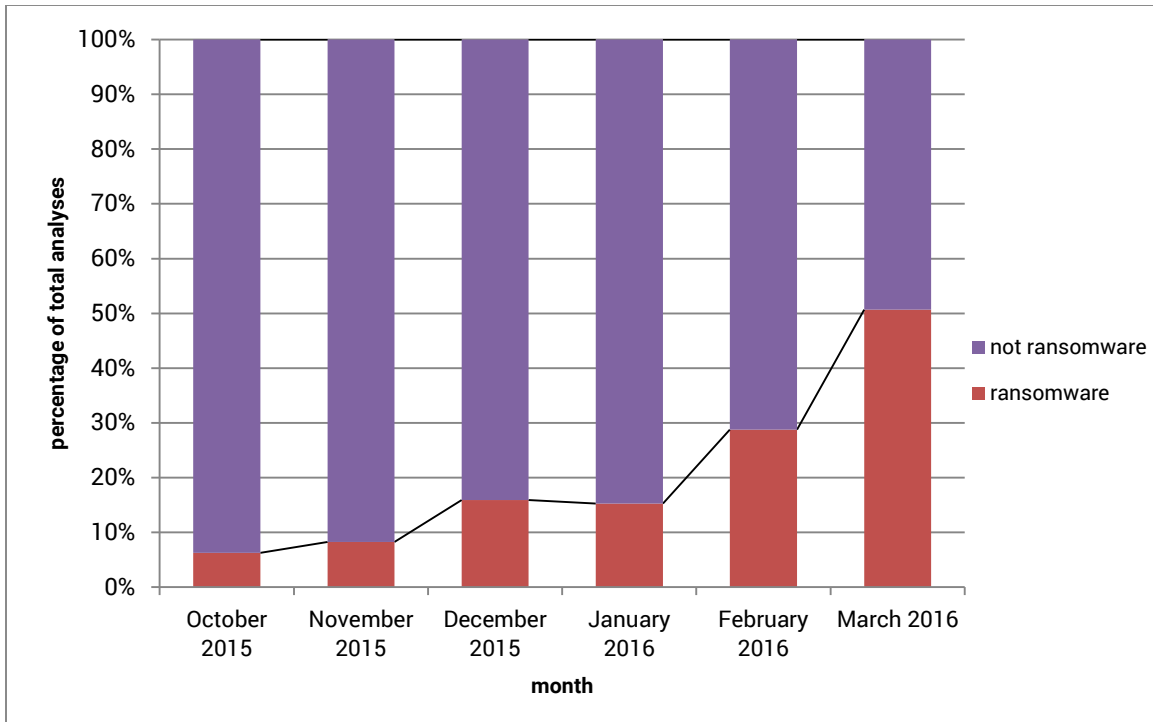


Figure 4 – growth of encryption ransomware against all other malware Q1 2016

Even more concerning is the proportion of phishing emails delivering encryption ransomware. While one of every two malware analyses focused on an encryption ransomware sample during March, 93% of all phishing email collected was intended to infect victims with ransomware. Reinforcing the data shown in Figure 1 that depicts how the ten largest sets of phishing emails delivered Locky, Figure 5 shows that by the end of the first quarter, only 7% of phishing messages by volume were delivering other malware tools.

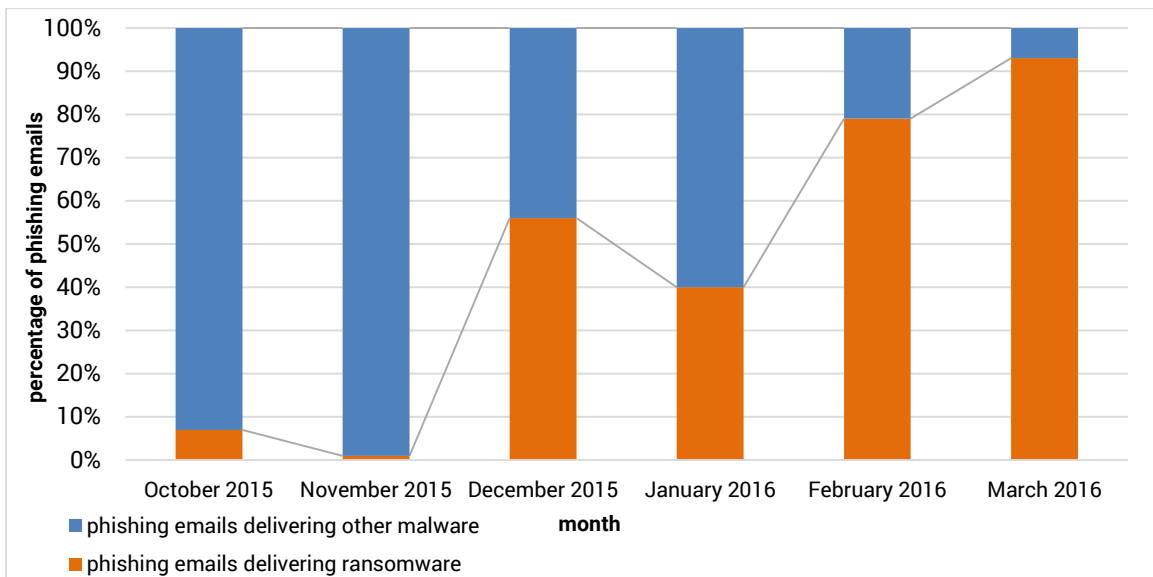


Figure 5 – percentage of phishing emails delivering ransomware

RUMBLE IN THE RANSOMWARE JUNGLE

However, not all encryption ransomware varieties have seen a proportional increase in usage by threat actors. Instead, varieties like Locky and TeslaCrypt show significant recent successes while CryptoWall seems to have fallen out of favor.

TeslaCrypt and Locky on the rise: Empirical data represented in Figure 6 shows that while CryptoWall samples represented over ninety percent of encryption ransomware analyzed during October and November 2015, deployment of new CryptoWall samples has shrunk to a minimal amount while TeslaCrypt and Locky usage has flourished.

Notable diversification: Another interesting fact illustrated in Figure 6 is the growth in variety of encryption ransomware during the first quarter. By the end of March 2016, eight distinct encryption ransomware varieties were analyzed as the payloads for phishing emails. These eight ranged in popularity from the aforementioned most popular Locky and TeslaCrypt to the less-common outliers Criakl and Troldesh. An honorable mention among the outliers is the use of PowerShell scripting to create a malicious application capable of acting as a ransomware.

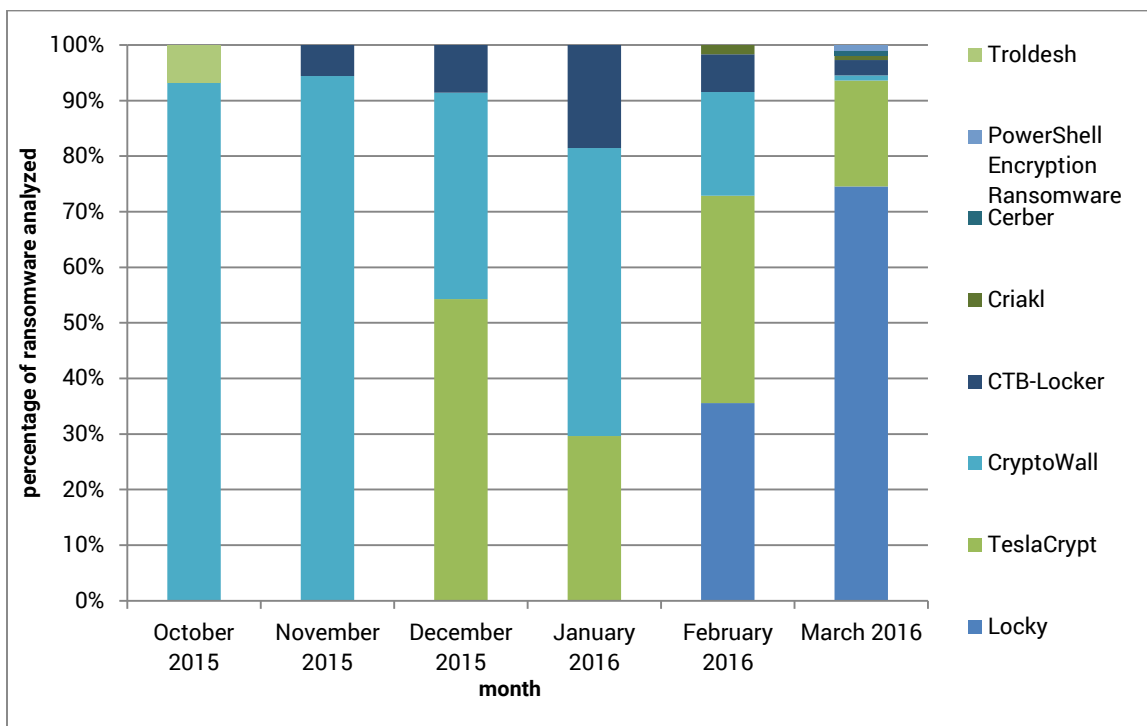


Figure 6 – proportions of ransomware samples analyzed Q4 2015 and Q1 2016

Nearly seventy-five percent of the ransomware samples analyzed in March 2016 and over one eighth of all malware samples during the first quarter of 2016 were Locky encryption ransomware binaries. The dramatic entry of this malware onto the threat landscape is a testament to the capabilities of threat actors associated with the use of Dridex, one of the most prominent banking and botnet trojans in both 2015 and early 2016.

Locky and Dridex similarities imply collaboration:

On February 16, 2016, PhishMe Intelligence identified several large sets of emails delivering Word documents containing macro scripts used to download the Locky encryption ransomware. The similarity of the messages and the OfficeMacro documents used to deliver this encryption ransomware to those used to deliver Dridex was striking. Even the payload URLs were constructed to resemble the naming convention used to deliver Dridex. Since these early days of Locky deployment, these similarities have been proven to be an indication of a significant degree of collaboration between some subset of the Dridex threat actors or the organization as a whole.

Historical precedent: Furthermore, this was not the first time that users of a premier financial crimes and espionage toolkit branched out into the ransomware market. This was precisely the move made by the GameOver Zeus botnet operators when that once-dominant botnet malware began deploying the CryptoLocker ransomware—a malware often credited for inspiring the myriad encryption ransomware varieties currently present on the threat landscape.

PASSIVE INCOME: THE SLEEPER

While Dridex has provided threat actors with deep levels of access to infected machines since 2014, Locky represents a much more passive means of monetizing infections. Whereas the Dridex crimekit allows for threat actors to collect login credentials, delve into the everyday activities of victims, and even take full remote control of infected machines, Locky—as Figure 7 shows—prompts victims to take action by rendering payment to the threat actors. The encryption ransomware provides a much easier means of generating income for the threat actor, eliminating the need to seek out, collect, process, and monetize stolen information.

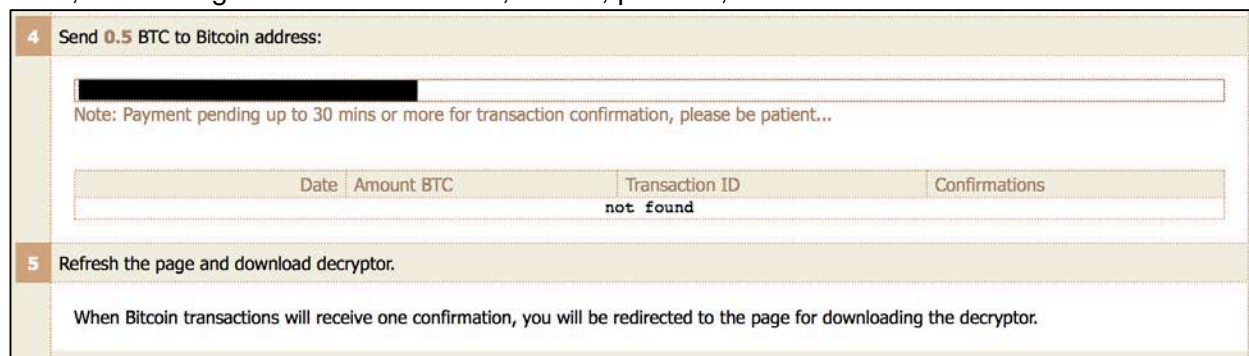


Figure 7 – demand for a half-Bitcoin ransom by Locky threat actors

Soft targeting increases effectiveness of phishing emails

Soft targeting is a technique for malware delivery that saw increases in both frequency and sophistication during the first quarter of 2016. The term soft targeting refers to the design of email messages meant to appeal to a certain category of individual or people in a specific role. These messages often include a particular job title or leverage a narrative most relevant to a small number of individuals within an organization.

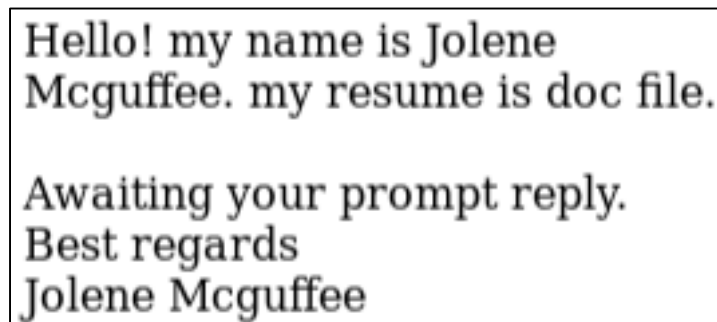
A CONTINUUM OF VICTIMS AND PRECISION MESSAGING

Rather than describing the targeting of phishing emails using the polar distinctions of *targeted* or *not targeted*, the ways that threat actors attempt to reach their targets are better viewed as a continuum. Instead of selecting just a few individuals or the public at large, threat actors may also attempt to reach subsets of victims, with the size of each subset logically determined by the specificity of the phishing emails. Furthermore, increasing the degree of specificity generally also involves increasing the amount of research necessary to successfully deliver a phishing email.

Functional relevance: the surprise left hook

An example of a soft targeting narrative observed over the past year is the prolific “resume” or “job application” phishing narrative used to deliver the CryptoWall encryption ransomware. Should critical human resources documents be impacted by this destructive ransomware, the victims may be more likely to capitulate to the ransom demands.

Human Resources: Figure 8 shows an example of this role-based targeting. The message is designed to appeal to human resources personnel or managers making hiring decisions and indicates that the sender’s “resume” can be found attached to the email.

The image shows a screenshot of a phishing email body. The text is as follows:

Hello! my name is Jolene
Mcguffee. my resume is doc file.

Awaiting your prompt reply.
Best regards
Jolene Mcguffee

Figure 8 – purported delivery of a resume in soft targeting phishing email

Resume or job applicant emails such as this require little research into or foreknowledge of the identity of the recipients. Instead, the threat actor is first relying on the broad distribution of these emails to ensure they reach the proper parties. The universal appeal of a potential job application or resume resonates with individuals in human resources or hiring positions.

Billing, Shipping or Sales: A perpetually-relevant example of soft-targeting can be found in the large number of small-volume phishing campaigns claiming to deliver documentation of an industrial quote or invoice. Messages like these claim to deliver paperwork for a large order of industrial goods similar to the one featured in Figure 9. These emails represent the largest avenue for delivering off-the-shelf remote access trojans and keylogger malware and are meant to appeal to anyone in a billing, shipping, or sales position within an industrial organization.

Dear Sir/Ma,

You are hereby invited to submit your quotation for the above Request for Quotation (RFQ) package (enclosed) as per instructions specified within.

Full details of the Materials required are provided in the attached RFQ package.

REPLY DATE: 29-DECEMBER-2016

Regards,

Jip Noushad Moosa
Sr. Sales Engineer

Figure 9 – soft targeting message intended to appeal to industrial organizations

A common purpose for each of these soft targeting phishing messages is to place a malware tool within a victim environment that disproportionately affects a specific category of individual. The delivery of remote access and keylogger tools using industrial soft targeting provides threat actors with a very flexible set of utilities for exfiltration of a wide variety of data including account information and intellectual property—both of which are meant to maximize the monetization of infected endpoints within industrial organizations.

Finance and the personal touch: Similarly, soft targeting messages delivering the Nymaim malware have used lures intended for individuals handling financial information. While historically noted for delivering ransomware tools, this botnet malware is closely tied to the deployment of tools facilitating various financial crimes. Figure 11 depicts a sample of a recent phishing email template used to deliver the Nymaim malware with this particular message reaching the inbox of PhishMe Vice President of Finance Sam Hahn. Being savvy and empowered in the detection and reporting of phishing emails, Sam Hahn quickly used PhishMe Reporter to pass along this message to Triage analysts for processing. This message was carefully crafted to address its recipient in several very personal ways. In the first line, the message provides a disclaimer of the message including the title and organization with which the recipient is affiliated. The email then greets the recipient with the most personal touch—the inclusion of the recipient's first and last name in the salutation.

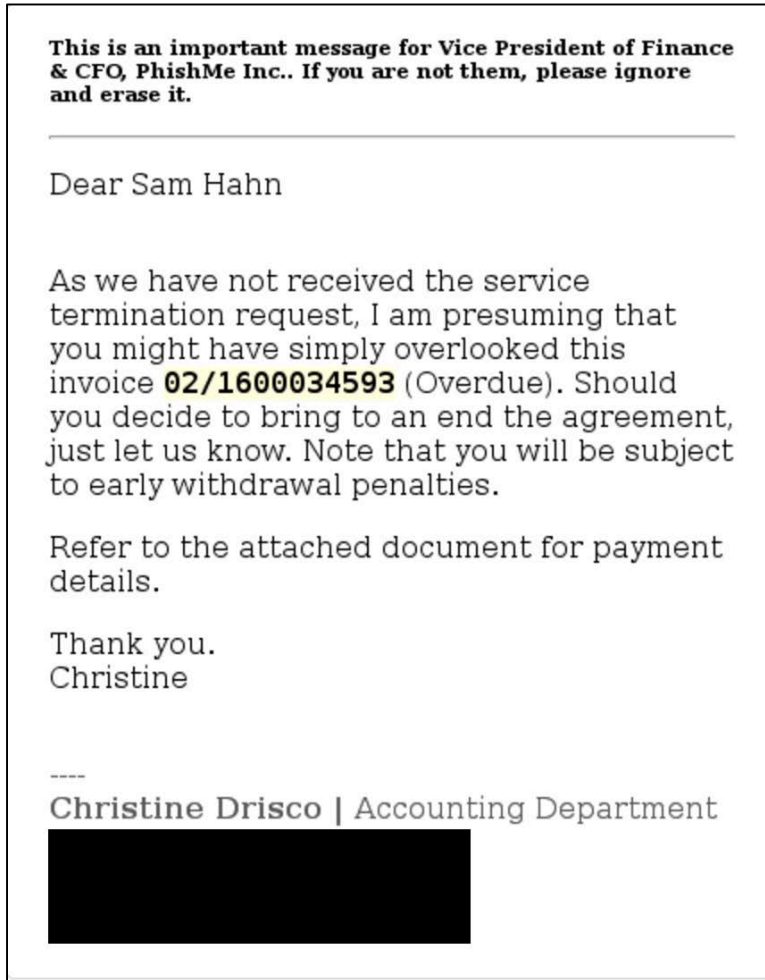


Figure 11 – A more thoroughly-researched but still broadly-distributed phishing message

This level of specificity creates the impression that only one copy of this message was delivered. However, PhishMe’s global phishing email collection proved otherwise. In fact, dozens of similar emails were harvested from various collection points with similar references to individuals whose job titles include the word “finance” and whose contact information and company affiliation were somehow publicly available. Figure 11 provides two additional examples of these messages, collected from other sources and demonstrating the ability of the threat actor to broadly deliver emails to a class of individual in many organizations.

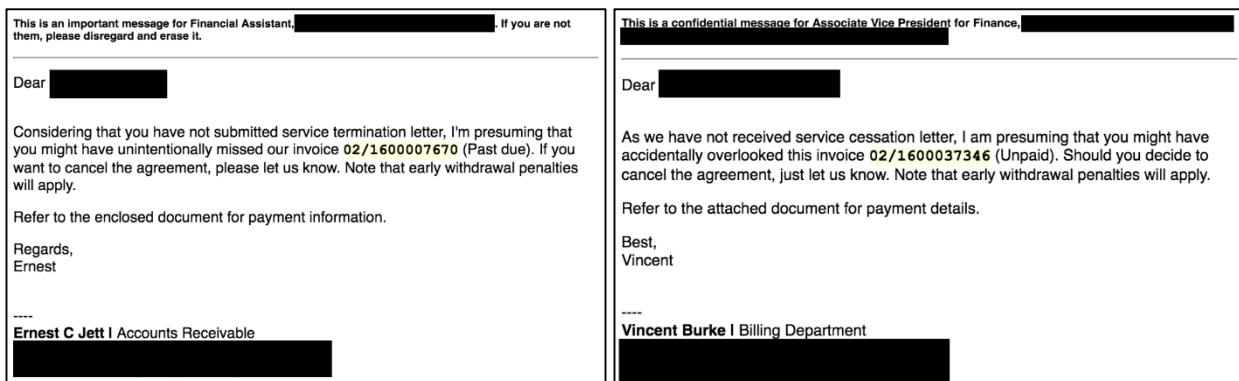


Figure 11 – additional examples of soft targeting emails delivered to employees in finance departments

These examples are part of an underlying trend of soft targeting in bulk where the threat actor is able to derive enough information from available online sources to generate large quantities of phishing emails for a specific class of individual. The emails produced as a result combine both the advantage of being broadly distributed as well as tailored enough to be far more convincing than many other phishing emails.

KEY TAKEAWAYS:

- During the month of March 2016, 93% of all global phishing attacks detected using PhishMe Intelligence contained ransomware, with only 7% containing malware.
- Disturbingly, a real-number increase in global phishing email of 6.3 million and a percentage increase of 789% is observed from fourth quarter 2015 to first quarter 2016
- Encryption malware is proliferating – almost half of malware analyses in March 2016 involved encryption malware
- Locky holds the first position among “payload” malware varieties followed by TeslaCrypt; both have overtaken CryptoWall which led in the fourth quarter of 2015
- Over half of JS Dropper applications were used to deliver Locky or TeslaCrypt
- Microsoft Office documents containing malware delivery scripting are key infiltration tools
- Soft targeting with relevant content is an increasingly effective phishing tactic. When combined with Microsoft Office documents a malware delivery method, the impact intensifies
- History can repeat itself – Locky and Dridex similarities imply collaboration between subsets of threat actors
- Insight is the best offense – detection, reporting and investigation are the triple threat to subvert damage

THE MISSION

While threat actors introduced several novel tools and techniques during the first quarter of 2016, PhishMe Intelligence was able to help organizations effectively prepare and respond to each improvement in criminal utility. PhishMe Intelligence provides essential insight into threat actors' phishing activities by profiling every step of their attack process. Daily analysis follows threat actors' every move from the delivery of the message through the completion of a malware infection trajectory. The data collected during this process is enriched and turned into actionable intelligence complete with full context to support network defense and incident response. Furthermore, PhishMe's analysts also provide strategic analysis that carefully considers and expands upon the daily observations made regarding active threats. With this intelligence, organizations can become more agile, adept, and astute at detecting and mitigating phishing threats.

For more information, contact PhishMe at sales@phishme.com if you have any questions about this report or threat intelligence services.



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