Malware Review

Q3 2016

PHISHME

www.phishme.com

Executive Summary

In the third quarter of 2016, PhishMe generated **689 Active Threat Reports**, recording and delivering intelligence on malware delivered by phishing email. These reports document the IOCs (Indicators of Compromise), tactics, and techniques that serve as the hallmarks of these attacks. Two defining trends were identified for the third quarter:

TREND 1: Locky continues to dominate

Encryption ransomware flourished in 2016, finding a disproportionate market share and attracting a great deal of attention from journalists, analysts, and information security strategists. Remaining at the forefront since February is the Locky encryption ransomware. While numerous encryption ransomware varieties have been identified, analyzed, and disappeared throughout this year, the developers of Locky have evidenced creativity, agility, and adaptability in their deployment of repeated improvements to frustrate the efforts of analysts and researchers as well as the security professionals tasked with protecting their organization from ransomware attacks.

Locky has introduced a number of techniques to resist detection during the infection process and to reduce the ability for researchers to gain insight into the malware's operations. The pace with which these innovations have been introduced to samples distributed to potential victims has set this encryption ransomware apart from many of its challengers.

TREND 2: Quiet malware continues to steal data in the shadow of ransomware

While ransomware has received a great deal of focus over the past year, threat actors have not forgotten about the reach and flexibility offered by remote access trojans (RATs) and other malware utilities that allow threat actors not just the ability to explore one affected endpoint, but to perform extended network reconnaissance and data exfiltration. Examples such as jRAT, a derivative of the long-lived AdWind remote access trojan, have been deployed prolifically by threat actors due to their ease of use, flexibility, and multiplatform access.

During the third quarter, PhishMe identified an increase in the deployment of remote access trojan malware like jRAT. This evidences an interest in a different business model than that maintained by the users of encryption ransomware varieties like Locky. Rather than looking for the fastest way to gain revenue through paid ransoms, these threat actors intend to remain within their victims' networks for extended periods of time.

Significant Q3 findings include:

- The yearly proportion of phishing emails analyzed that delivered some form of ransomware had grown to 97.25%, leaving only 2.75% of phishing emails to deliver all other forms of malware utilities.
- Locky distribution dwarfs most malware from 2016.
- More *unique* samples delivered by and analyzed from non-ransomware malware.
- Non-ransomware attacks can be harder to detect due to the smaller number of emails sent and the higher entropy in malware samples delivered.

Malware in Q3

Between July 1, 2016 and October 1, 2016, PhishMe Intelligence conducted 689 malware analyses, showing a significant increase over the 559 analyses conducted during the second quarter of 2016. This increase is due in large part to the growth in use and consistent deployment of the Locky encryption as well as a spike in remote access trojan usage.

The frequency analysis in **Figure 1** shows that Locky executables were the most commonly-identified file type during the third quarter with various malware distribution techniques also featuring top ten malware file classifications. Other key malware varieties in play during this period include the ever-popular Pony information stealer and various remote access trojan utilities.

The Pony malware, despite its age and simplicity, still maintains a nontrivial position among the malware tools used by threat actors of varying sophistication levels. Valued for its utility as both an information stealer and downloader, threat actors rely on Pony to steal credentials and data stored on victims' computers as well as to facilitate the delivery of much more full-featured malware utilities ranging from keylogger malware to financial crimes and botnet trojans like Neverquest, also known as Vawtrak.

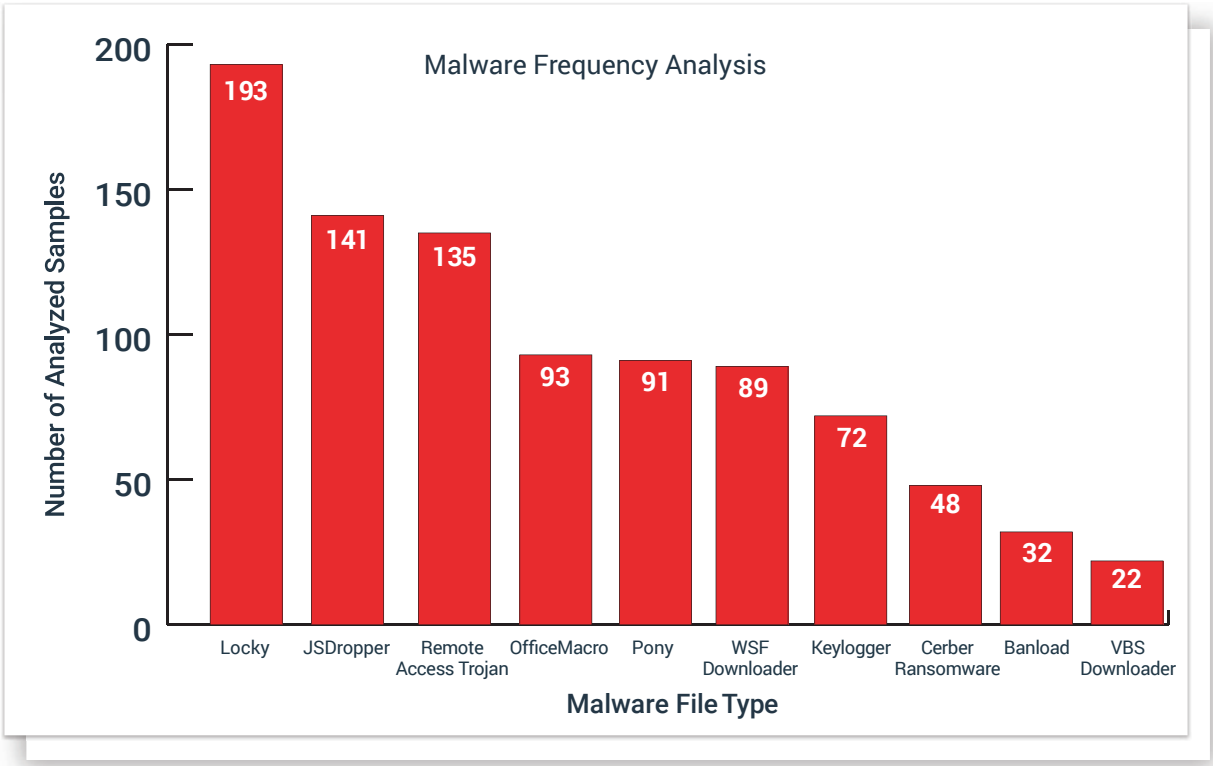

Figure 1: Frequency of malware file types analyzed during Q3 2016

The delivery mechanisms preferenced by threat actors during the third quarter of 2016 have tended toward a more uniform distribution of JavaScript applications, Windows Script File (WSF) downloaders, and OfficeMacro documents. This is a change from the first half of the year during which script applications written in JavaScript, Visual Basic, or combinations superseded OfficeMacro documents as the preferred method for malware delivery. Another example of malware delivery utility with growing deployments is the Microsoft HTML Application—a file format that is natively executable in Windows and represents a different way to package script content designed to download and run malware applications.

As **Figure 2** shows, these delivery techniques have all seen a good deal of mileage in delivering the Locky encryption ransomware but have also been seen as delivery mechanisms in attacks by other enterprising threat actors. It also demonstrates how the less-well-known WSF application has become the most-common mechanism for delivering the Locky encryption ransomware.

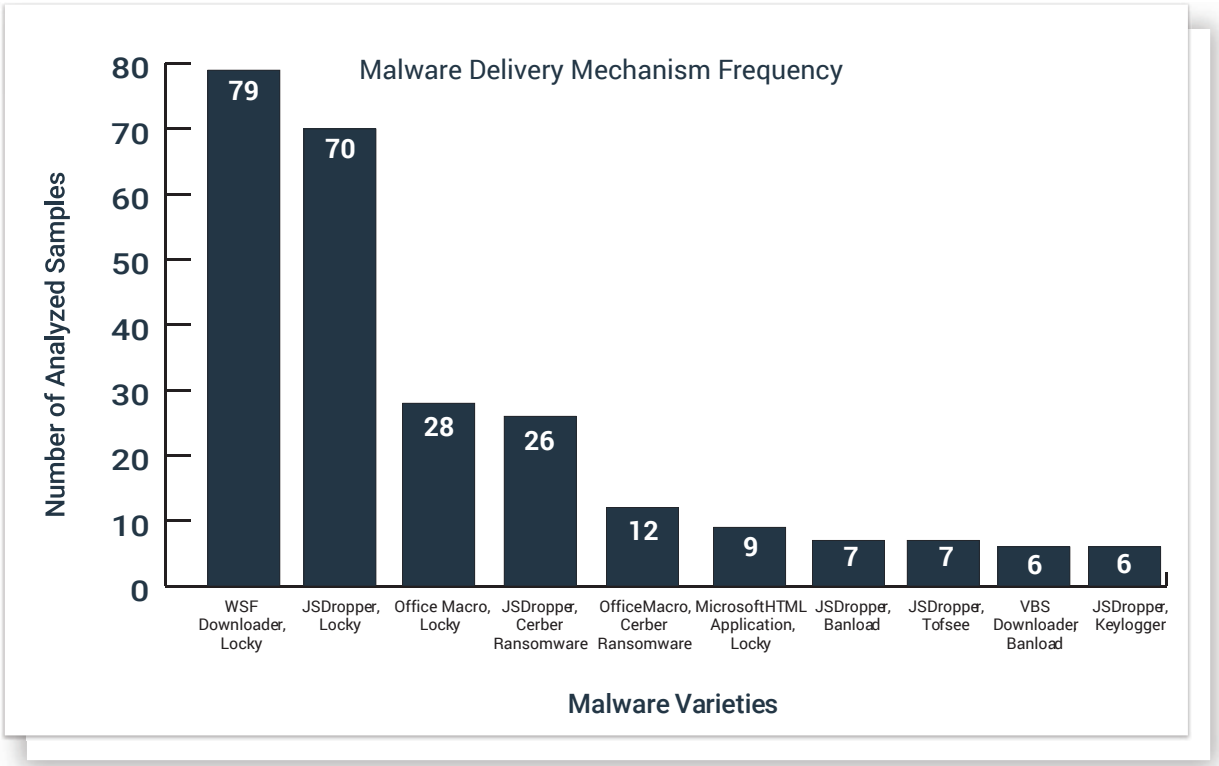

Figure 2: Frequency of top ten malware varieties and their delivery mechanisms Q3 2016

The other notable malware varieties exhibited in **Figure 2** include the Cerber encryption ransomware, which has made its mark as a very successful ransomware-as-a-service platform for criminals, and Banload, a financial crimes and information stealer malware leveraged extensively in targeting residents of Brazil.

Locky remains dominant as ransomware continues to steal headlines

It cannot be disputed that the top information security story of 2016 will be the impact of encryption ransomware on individuals and companies of all sizes. By the end of the third quarter, the yearly proportion of phishing emails **analyzed** that delivered some form of ransomware had grown to 97.25% percent leaving only 2.75% percent of phishing emails to deliver all other forms of malware utilities. This incredible proportion was driven by the exceptionally large campaigns used to deliver ransomware utilities. These exceptionally large campaigns underscore an important part of the ransomware business model that relies on maximization of infected endpoints for the most financial gain. This, combined with the fact that ransomware is rarely stealthy but instead also relies on victims knowing they are infected so they can begin the ransom payment process, helps to explain the overwhelming volume of phishing email delivering ransomware this year. This can be contrasted with the malware utilities being delivered by the much smaller proportion. These other utilities represent malware types that require and thrive upon stealth for their success in stealing sensitive information from their victims over extended periods of time.

At the forefront of this explosive ransomware trend is the Locky encryption ransomware. This malware will be remembered alongside 2013's CryptoLocker as a top-tier ransomware tool that fundamentally altered the way information security professionals view the threat landscape. For much of 2016, two or more distinct sets of phishing emails could be observed delivering this prolific malware. On many days, PhishMe's analysts identified up to five distinct sets of Locky phishing emails, making it the most commonly-delivered malware so far in 2016.

97.25

Percentage of phishing emails delivering ransomware

By the end of September 2016, PhishMe Intelligence had produced 438 reports focused on the behavior, tactics, and indicators of compromise related to the Locky encryption ransomware. Almost half of those analyses were performed during the third quarter alone with 193 distinct analyses taking place between July 1 and October 1. This is part of a continued trend of increasing activity from this prolific and successful ransomware variety.

Not only does Locky distribution dwarf most malware from 2016, but it also towers over other ransomware varieties. As **Figure 3** shows, the next-largest set of ransomware distributions during July, August, and September delivered the Cerber encryption ransomware—a ransomware-as-a-service platform that has made a significant impact during 2016.

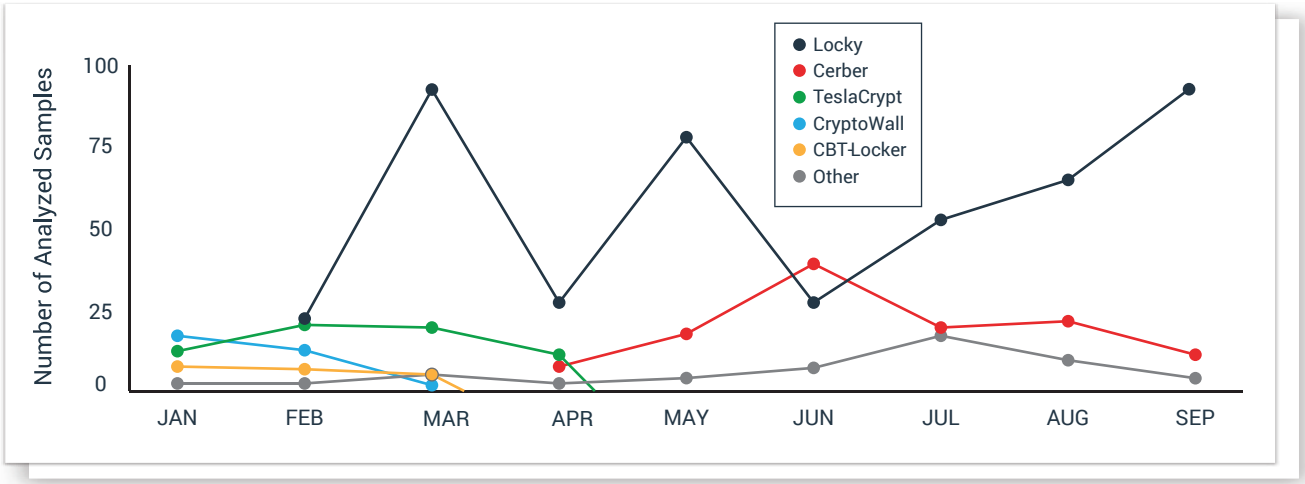

Figure 3: Relative proportions of ransomware varieties analyzed in 2016

Figure 3 also shows that while researchers are reporting more and more new ransomware varieties across the threat landscape, the most successful ransomware varieties take the lion's share of the market. In fact, in the "other" ransomware category includes only slightly more than one percent of the analyzed ransomware samples from the September 2016. Another way of looking at this trend is to consider the quarter-over-quarter growth in Locky distribution. As **Figure 4** demonstrates, the quarter-over-quarter number of analyses has been on a steady increase since the malware's introduction during the first quarter of 2016 as this malware has enjoyed increased success.

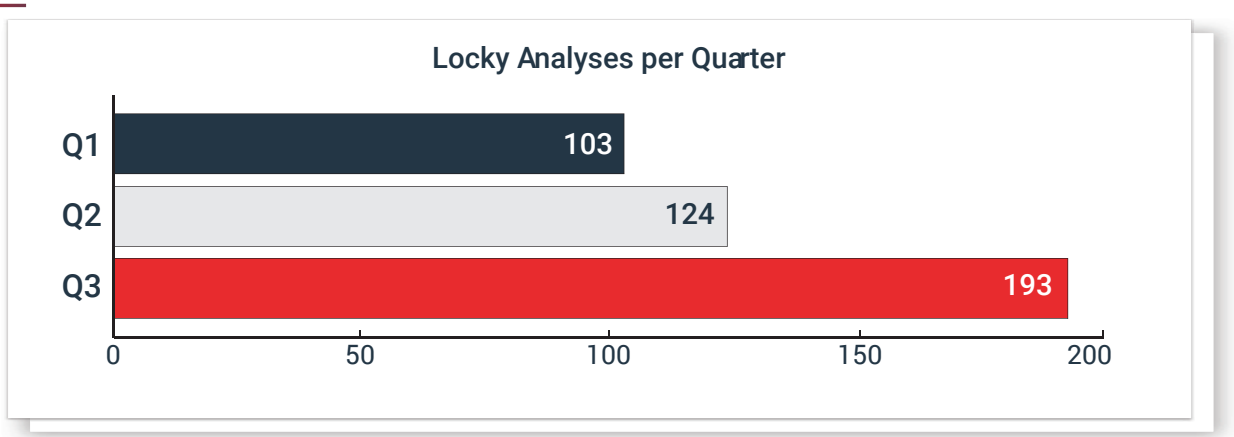

Figure 4: Number of Locky analyses performed in each quarter of 2016

With this steady increase in use also comes more awareness and more concerted efforts to prevent this ransomware from being delivered to victims. To counter this, the Locky developers and distributors have added a number of interesting features and iterated on their evasion techniques throughout the year.

Figure 5 presents a timeline of Locky distribution frequency along with the most notable developments and additions to the malware's behavior and techniques. Two interesting facts presented by this timeline are the myriad methods used to deliver the Locky encryption ransomware and the correlation of new development to decreases in deployment.

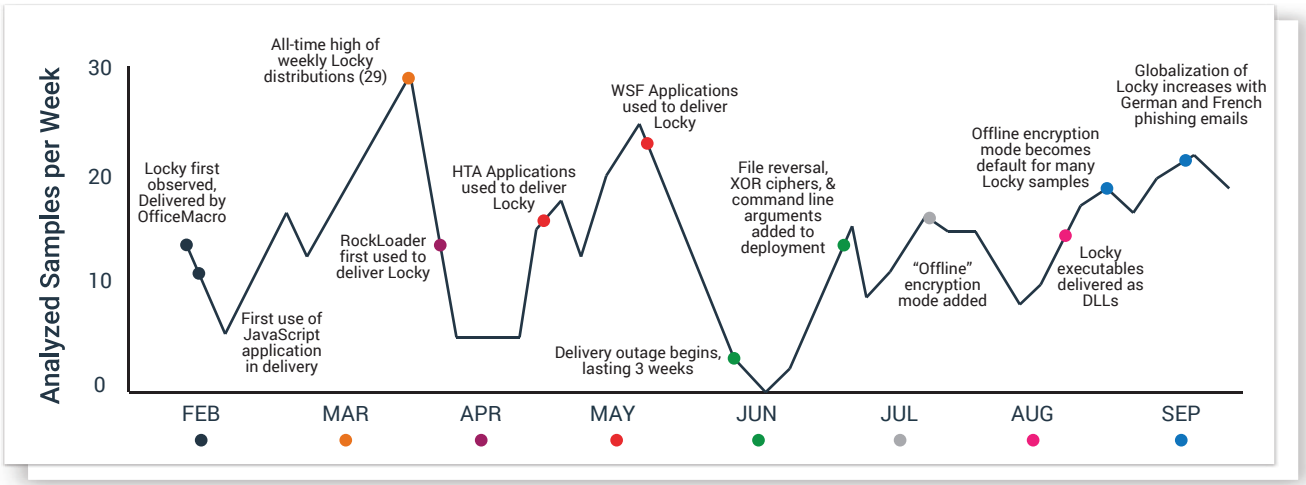

Figure 5: Timeline of Locky distribution volume and innovations

Within the first months of Locky's deployment during the first and second quarters of 2016, this ransomware was delivered using script applications, native Windows HTML applications, and by the RockLoader malware downloader. These were all departures from the original OfficeMacro documents used to deliver Locky on its first day of deployment. Once these different utilities were all in use, the threat actors then began to focus on improving less-visible portions of the delivery process. This included the introduction of file reversal, XOR-ciphered payloads, and command line arguments as well as the move to DLL files as the chosen executable format for the Locky ransomware. Each one of these developments served to defy the expectations set by earlier Locky deliveries and to frustrate the efforts of researchers and security professionals seeking to protect against this malware. Beyond the substance of these changes, the timing was also worth noting. Many of these improvements emerged immediately following downturns or outages in Locky distribution. This indicates that the threat actors are capable of retooling and returning with expanded feature sets when their infrastructure and resources are diminished or unavailable.

Malware in the shadows still stealing data

While the biggest story of 2016 will be ransomware's rise to prominence, it is important to note that other forms of malicious software delivered via phishing email continue to infect victims around the world. Locky, Cerber, and other successful ransomware varieties are key to a criminal business model that relies on the rapid collection of ransom payments and have supported very large criminal ventures. However, many threat actors are still able to successfully leverage other types of malware utilities with great success.

The success of ransomware has provided an exciting and profitable avenue for online crime, but the same avenues for compromise using remote access trojans, keyloggers, and botnet malware still represent a significant hazard in 2016. Malware in this category relies on a very different business model than ransomware. Where ransomware relies on the victim discovering the infection and understanding the degree of damage that has been inflicted, these other malware varieties are designed to avoid detection while maintaining a presence within the affected organization for extended periods of time.

Despite the attention garnered by encryption ransomware in 2016 and the massive volume of phishing emails used to deliver ransomware samples, a significant proportion of unique malware binaries were not ransomware. In fact, almost two-thirds of unique analyses performed during the third quarter featured non-ransomware malware. This interesting inversion shows that while only 2.75% of phishing emails delivered not-ransomware malware, the diversity of unique malware samples delivered by these emails far exceeded that of the more numerous ransomware delivery campaigns.

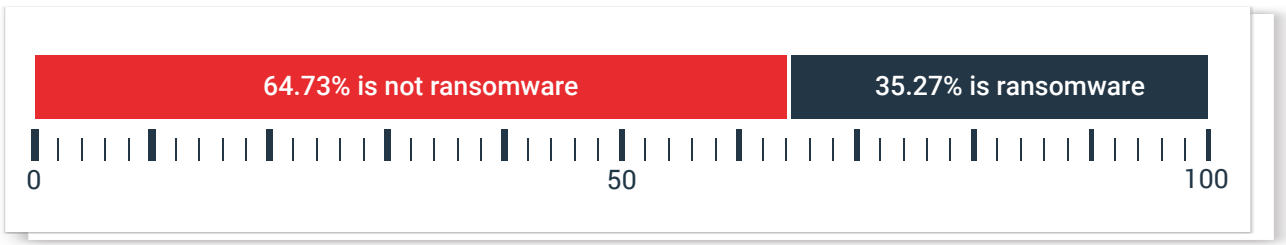

Figure 6: – Percentage of malware samples representing some form of ransomware

This is relevant because it means that these attacks, due to an interesting twist on economies of scale, can be harder to detect due to the smaller number of emails sent and the higher entropy in malware samples delivered. Coupled with the fact that these malware varieties, unlike ransomware, are generally designed to avoid detection, this malware stands to not only reach and take hold within an organization, but also exist for extended periods of time. This gives threat actors the ability to perform reconnaissance, identify the information or systems that are most valuable for their purposes, and conduct extended operations to exfiltrate sensitive information.

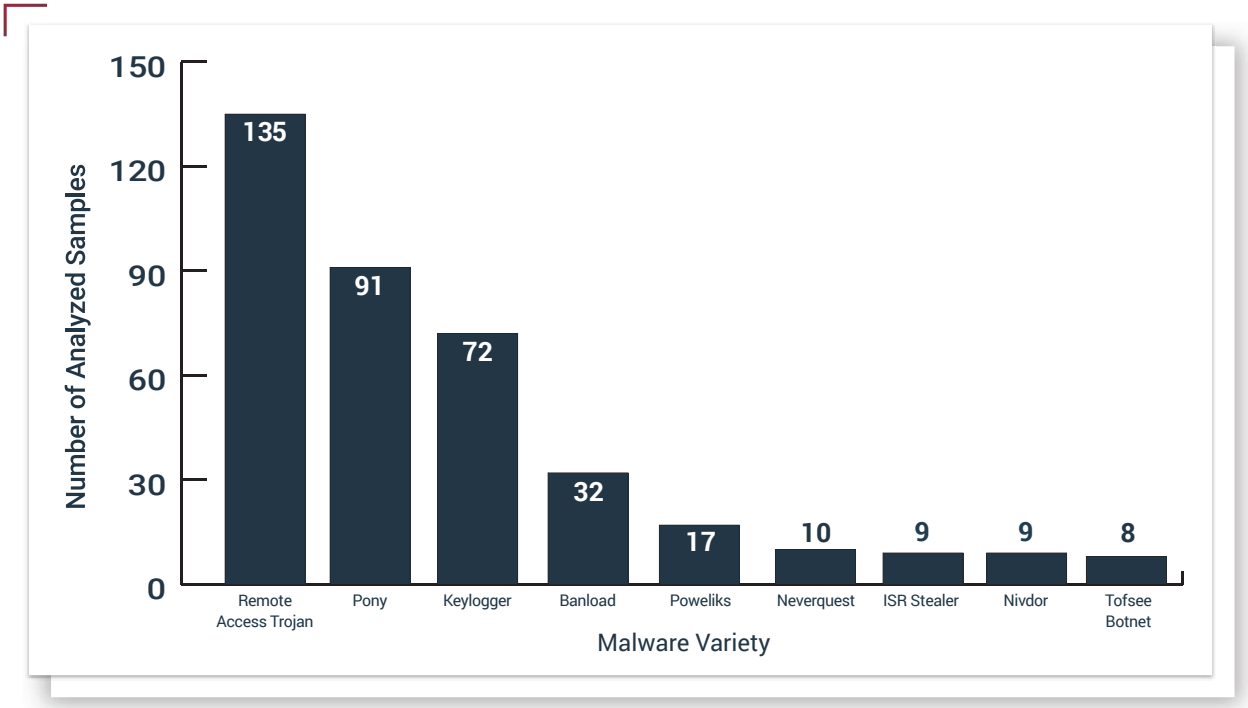

Figure 7: Most-commonly-analyzed non-ransomware

Figure 7 details the most commonly-utilized non-ransomware malware from the third quarter of 2016. Ranging from the ever-present and ever-growing collection of off-the-shelf remote access trojan malware to the feature-rich financial crimes trojans like Neverquest, these criminal tools all rely on stealth and secrecy to allow threat actors to monetize infections and achieve their goals. This is, of course, the primary purpose of these tools and has been the primary malware threat for many years.

During the third quarter, one the most popular off-the-shelf remote access utilities was the jRAT fork of the Java remote access trojan family that includes JSocket, Alienspy, and Adwind. This prolific and multi-platform trojan represents one of the most-commonly deployed malware varieties during the third quarter and the majority of remote access trojans. In addition to the adaptable jRAT, the Pony information stealer and downloader malware has remained remarkably active despite its age and simplicity. This malware was implicated in nearly a hundred phishing campaigns during the month of July, August, and September 2016 as a standalone tool for harvesting login credentials and private data as well as an intermediate tool used to facilitate the download and execution of other malware utilities. Furthermore, the Pony malware is currently undergoing a renaissance wherein it is being modified to be deployed as a plugin for other malware varieties and to serve as a more feature-rich standalone utility.

While off-the-shelf remote access trojans continue to feature large on the threat landscape, off-the-shelf keylogger malware also remains a significant threat as well. Following just behind Pony as frequently-deployed malware used in the third quarter is a large number of off-the-shelf keyloggers like Hawkeye, LuminosityLink, and iSpy. These are all utilities that give threat actors sufficient insight not just into the things a victim types, but also the applications and websites the victim frequents.

In all, the continued deployment of these utilities proves that the business model they serve is still profitable and successful for threat actors despite the recent prevalence of ransomware. While ransomware garners a great deal of attention both as part of its criminal business model and as a trending topic among information security professionals, it is still important to note that a greater variety of unique non-ransomware malware samples are still being deployed to quietly infiltrate organizations and exfiltrate sensitive information.

Conclusion

The evolution of the phishing threat landscape in 2016 has brought about the ascendancy of ransomware with Locky at its forefront. However, there is no indication that the non-ransomware malware threats that have been relevant for so many years prior have seen any significant decrease in popularity among threat actors. Furthermore, the rapid pace with which awareness of the ransomware threat has spread and the attention it has received has forced the threat actors using these tools to pivot and iterate their tactics frequently. However, the continued tenacity of these threat actors shows that awareness is not enough. Without a holistic phishing defense strategy, organizations are still susceptible to not just the voluminous phishing emails used to deliver ransomware, but also the smaller and less-visible sets of emails delivering the same malware that threat actors have used for many years.

The third quarter of 2016, like the rest of this year, has shown how the two business models associated with ransomware and non-ransomware malware are continuing to support successful criminal ventures using phishing email as the primary means of gaining the infections required for that success. By preparing users for these attacks, it is possible to empower them to act as both human sensors for detecting these attacks and as partners in preventing threat actors from succeeding. By reporting emails to security professionals, users then help organizations collect intelligence about the attacks impacting them in real time. When these reports are coupled with and contextualized by external intelligence from highly-vetted and enriched sources, organizations stand the best chance to overcome these threats.

Phishing Threats and PhishMe Intelligence

On a daily basis, PhishMe provides phishing threat intelligence reporting used by customers to effectively prepare and respond to phishing threats and attempts to deploy sophisticated and simple intrusion utilities. PhishMe's research teams collect and analyze phishing emails from around the world to provide essential insight into threat actors' phishing activities by profiling both emerging and established techniques and tools.

These reports are produced to empower PhishMe's customers through the delivery of high-fidelity, actionable threat intelligence that can be used to mitigate the newest phishing campaigns. Each Intelligence report is available in multiple machine-readable formats, as a human-readable analyst's report, and through the ThreatHQ investigation app. PhishMe publishes new intelligence via API, email, and web interfaces following the analysis of each new phishing attack. 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.

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