Malware Review

Q2 2016

PHISHME

www.phishme.com

Executive Summary

During the second quarter of 2016, PhishMe Intelligence generated 559 Active Threat Reports detailing new delivery of malware via phishing email, including the indicators of compromise and the tactics and techniques utilized by threat actors.
Three major trends stand out.

Encryption ransomware is now a primary business model.
Ransomware is no longer merely a clever means for reaping a quick, meager profit. Given the tenacity and frequency of ransomware phishing attacks, they are likely a permanent fixture on the threat landscape.

More phishing attacks are designed to outsmart protection solutions.
PhishMe Intelligence encountered an increase in the number and volume of malware deployments that incorporate simple anti-analysis techniques designed to circumvent the protection provided by security solutions and the efforts of security researchers.

Less sophisticated attacks still pack a punch.
While a great deal of attention is directed toward the most advanced and sophisticated crimeware varieties, PhishMe Intelligence still records numerous deployments of malware utilities associated with less sophisticated actors who still wield robust feature sets.

In Brief

Between April 1 and July 1, 2016 PhishMe Intelligence conducted 559 malware analyses, showing a slight decrease from the 612 analyses conducted in the first quarter of 2016. The decrease is due to the three-week absence of the Locky encryption ransomware in June attributed to an unexplained disruption in delivery infrastructure. However, despite this brief absence more *unique* Locky deployments were identified during the second quarter than during the first quarter of 2016.

In total, 125 unique sets of phishing emails were used to deliver Locky during Q2 while only 103 were identified during Q1.

As the frequency analysis in Figure 1 demonstrates, the most-common malicious file type identified during the second quarter was the myriad JavaScript downloader applications, identified in PhishMe's reporting as JSDropper. This file type leaped to the forefront of malware trends through its use in delivering the Locky encryption ransomware. The ubiquity and simplicity of this utility as a malware delivery tool has also led to its use in the delivery of other malware types, including the Dridex botnet malware as well numerous ransomware and botnet utilities.

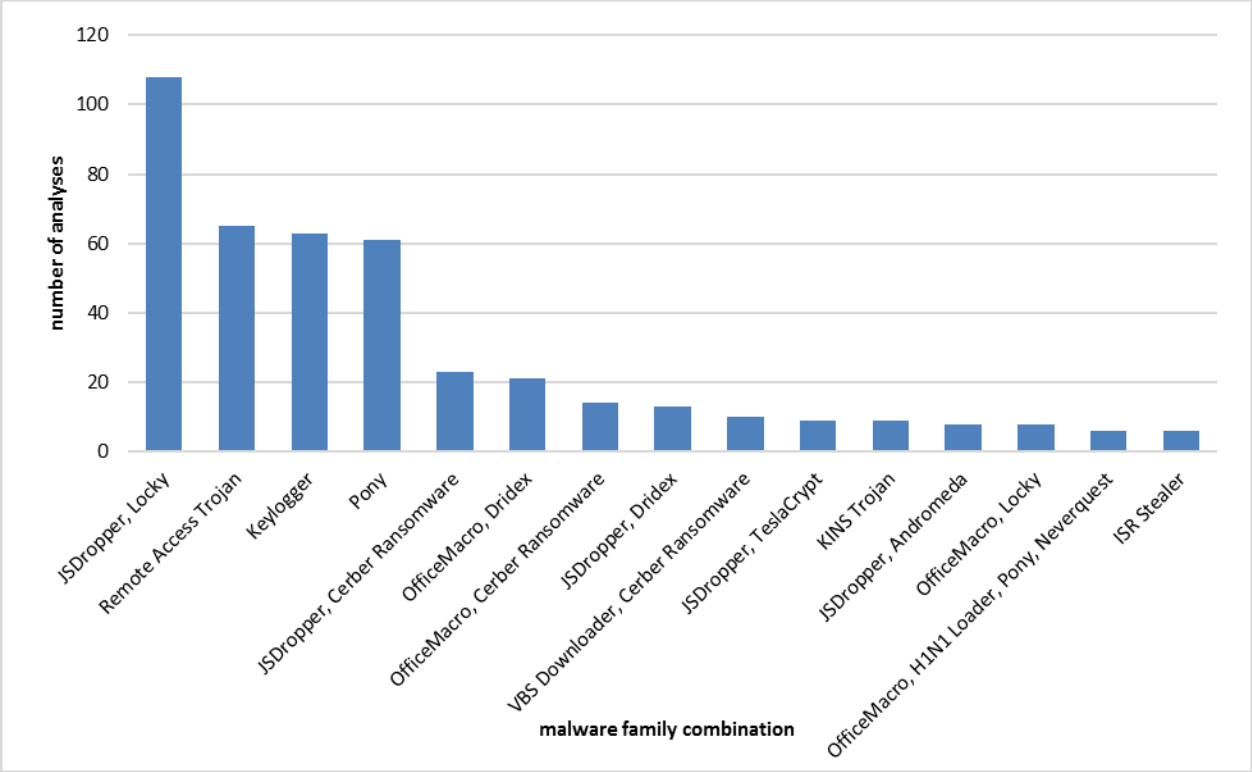


Figure 1 – frequency of malware deliveries during Q2 2016

The most notable change in malware delivery during the second quarter was the drop in usage of OfficeMacro documents.

PhishMe Intelligence recorded a 51 percent decrease as more threat actors adopted lightweight script applications using JavaScript or Visual Basic. While 2015 could easily be dubbed "the year of the macro," during the first half of 2016 Office documents with macro scripting lost their grip on the #1 spot. However, these documents still represent the second-most-popular delivery technique.

The Cerber Encryption ransomware surged in popularity. Cerber was not even among the top twenty most commonly analyzed malware varieties during the first quarter. During the second quarter, it rose to the position of seventh-most-common *malware* variety and the second-most-common *ransomware* variety. Furthermore, it was the third-most-common payload malware overall, following Locky and the Pony information stealer.

The Pony malware remains a dark horse. It was the third-most-commonly analyzed malware variety, favored by threat actors for its reliability and simplicity in collecting stored login credentials and other private information from victims' computers.

Ransomware Settles in for the Long Haul

Barely a year ago, ransomware was a frightening trend. Now it's come into its own as a fully established business model and reliable profit engine. Halfway through 2016, the encryption ransomware threat is causing many sleepless nights.

Figure 2 shows that encryption ransomware (the five red bars) accounts for half of the ten most common malware delivery configurations.

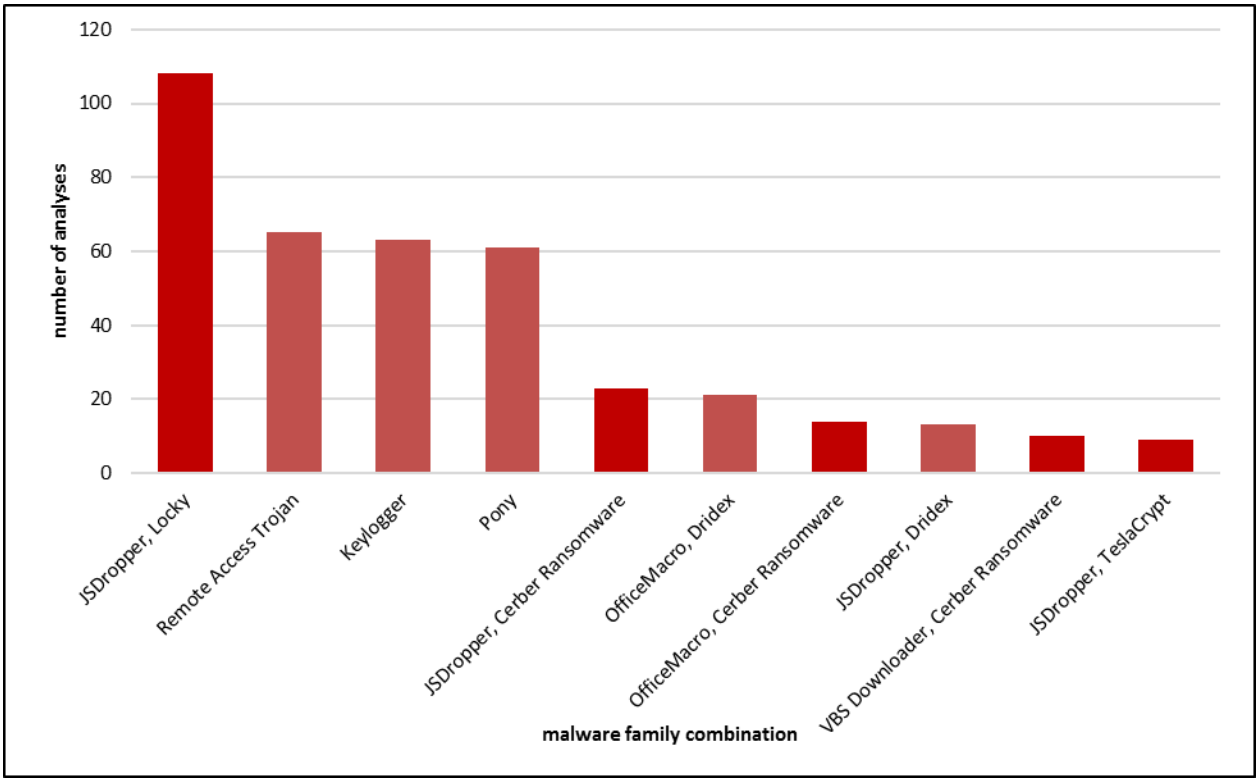


Figure 2 – top malware delivery combinations highlighting ransomware usage

Figure 2 shows the most prolific encryption ransomware varieties. Locky was both the most commonly observed malware variety and most commonly analyzed encryption ransomware.

Cerber encryption ransomware has gained a surprising amount of market share during the past three months.

This is reinforced in Figure 3, which shows a peak in ransomware diversification in March 2016 and later consolidation in May and June, with Cerber and Locky dominating the ransomware scene.

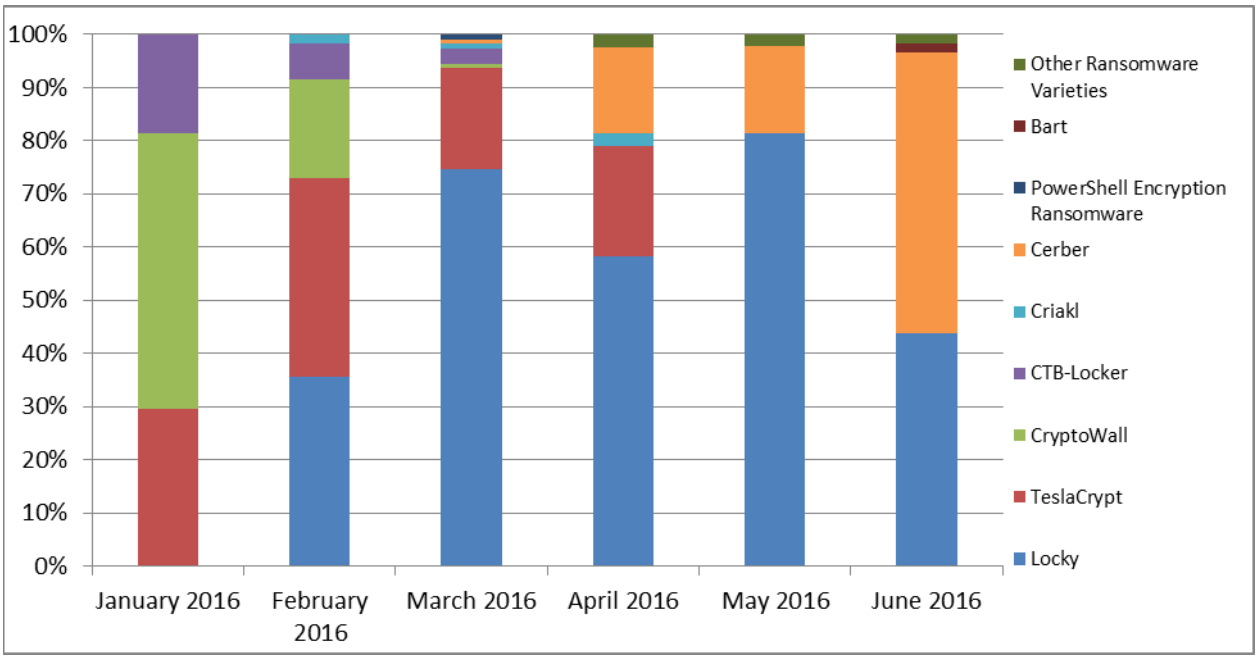


Figure 3 – Proportions of ransomware samples analyzed Q1 and Q2 2016

An important trend is Cerber's overtake of Locky in June as the most frequently observed ransomware variety. This is due in large part to a three-week absence of the Locky encryption ransomware while its delivery infrastructure suffered from a lengthy outage. Other notable changes from the first quarter are the abandonment of TeslaCrypt by its threat actors and the absence of new CTB-Locker distributions via phishing email.

The Business of Ransomware

With ransomware growing so rapidly, it is worth evaluating as a business model. The threat actors leveraging ransomware tools, like the users of many other malware utilities, are ultimately businesspeople. They seek the most advantageous and cost-efficient means for collecting a profit. However, the business of ransomware and the ecosystem that makes it profitable are distinctive among online criminal tools.

Ransomware, by necessity, requires the threat actor to interact with the victim. Rather than relying on silent monitoring and collection of information from victims, ransomware notoriously informs them they have lost access to files on their computer. The ransom note itself requires both power and finesse. It must be strong enough to compel payment and yet not over-reach. Otherwise, the threat actor makes no profit off the malware deployment and will, by business principle, pursue other avenues.

Figure 4 – compelling ransom notes are crucial to threat actor success

While the ransom notes above convey unmistakable threats, an almost equally important aspect is setting a price the victim will pay. Generally, ransomware demands are between the Bitcoin equivalent of 200 and 500 USD and often include an added threat that the required amount will double. As seen in Figures 5 and 6, both Locky and Cerber demand payments in this range. Note that Cerber includes the threat of increasing the ransom amount if a certain amount of time should pass, but Locky does not.

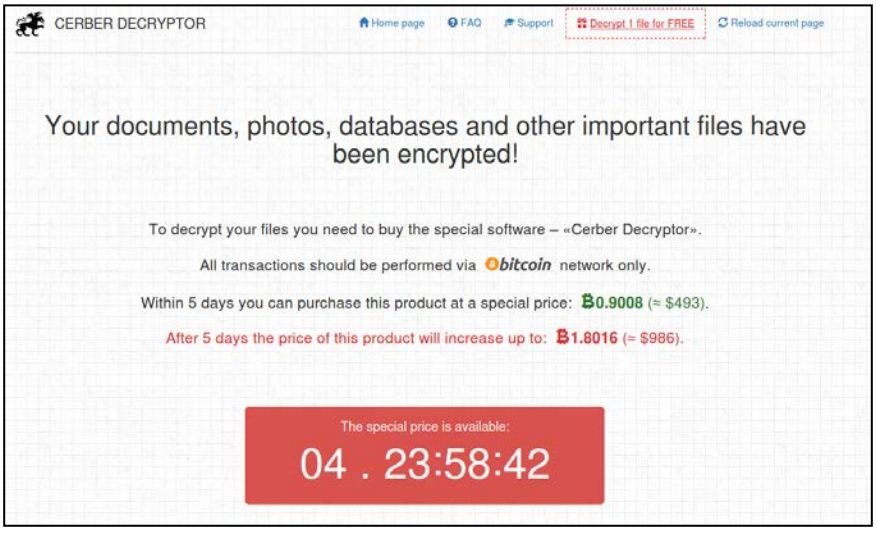


Figure 5 – Cerber ransom demand with countdown timer for doubled ransom

Figure 6 – Locky ransom demand

While 500 USD may seem like a steep price for an individual to pay for access to his or her computer's content, that same price point is very low for most companies—even small- and medium-sized businesses—when those organizations' ability to do business is at stake. For many organizations, the prospect of paying a few hundred dollars in ransom is more palatable than losing access to months or years of work and information. For some, paying the ransom may even seem more appealing than engaging in a wipe-and-restore operation.

Ransomware threat actors rely on this cost-benefit analysis. By convincing victims that it is more expedient to pay the ransom than to attempt to restore files or lose the encrypted content, threat actors get their way. They even offer to be "helpful." The note in Figure 6 states that purchasing Bitcoin is "getting simpler every day," with the "Locky Decryptor™ described as an easy-to-purchase software product.

Again, if the victim doesn't pay, the criminal gains no profit. Therein lies the best way to combat the threat actor.

By ensuring that an organization has sufficient backup and segmentation processes in place, along with established response processes to prevent data loss, the risks associated with encryption ransomware are diminished.

Steganography and Ciphers in Malware Delivery

To ensure the delivery of malware tools, threat actors carefully craft messages that are both appealing to victims and capable of evading email filters. Therefore, many organizations layer security solutions to cover the gaps left by email and sandbox protections. In order to circumvent such added protection, threat actors turn to other interesting techniques designed to hide the existence of malware content as it's delivered.

An increasingly popular and long-lived technique is hiding malware content in other benign content.

One method, widespread through the second quarter to facilitate the delivery of the Cerber encryption ransomware, uses a classic steganographic technique—hiding the executable content of a malware payload within an apparently harmless image file. Once downloaded, this image file can then be manipulated by a script application to create a functional malware executable. This technique's reliable reuse in delivering the Cerber encryption ransomware (along with an earlier Dridex sample) serves as a warning: sophisticated steganography in the wrong hands is proliferating.

On April 28, 2016, a Microsoft Word document analyzed for PhishMe Threat ID 5943 was shown to leverage a macro script to download a seemingly-harmless JPEG image shown here in Figure 7. The Visual Basic scripting featured the capability to extract a blob of data from the foot of this JPEG image's binary content and perform a number of transforms to create a Windows executable.

Figure 7 – screenshot of image containing Cerber executable

This obfuscated executable corresponded to that of another file written to disk as an intermediary step in the deobfuscation process. Figure 8 illustrates the start of this data and a potential pair of characters that might serve as a marker for the beginning of the obfuscated executable content.

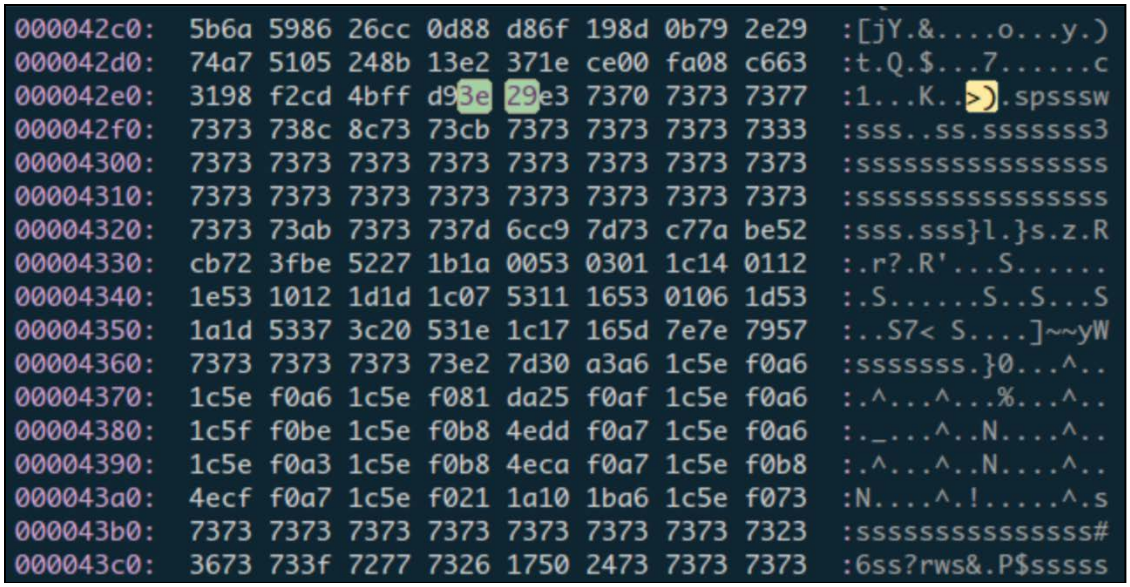


Figure 8 – start of data later transformed into a malware application

The steganographic embedding of an executable in an image file serves to decrease the likelihood that the malware will be detected as it is downloaded and used during the infection process. However, it does not serve to stymie researchers in the same manner that other methods might.

Following a three-week absence during June, the Locky encryption ransomware returned with the addition of some simple enhancements designed to make the malware more difficult to analyze. None of these enhancements were particularly sophisticated, but were clearly designed to make it more difficult for both security solutions and individual researchers to identify the crucial infrastructure elements required by the malware for successful infections. Two primary techniques were introduced. First, the payloads stored on compromised hosts were obfuscated using a simple XOR operation along with file-content-reversal. Secondly, once deobfuscated, the executable application will immediately crash if not run with a certain value passed as a command line argument. An XOR cipher relies on the bitwise exclusive disjunction operation to transform the plaintext executable content of a payload binary into unrecognizable data without the hallmarks of any Windows application, much less one designed to encrypt users' important documents and files. This cipher also has the advantage of being simple to implement and alter.

Enhancements such as these are meant to frustrate the efforts of researchers who obtain Locky samples without having access to the original email by which the JavaScript application facilitated the payload delivery.

The addition of an XOR and reversal cipher means that researchers privy to the most up-to-date lists of Locky payload locations cannot easily download and run the executables. Furthermore, the addition of a set of command-line arguments for each Locky application delivered by a JavaScript application means that shared samples or samples obtained from infected endpoints cannot be run again without knowledge of those arguments.

Figure 9 demonstrates an example of a file available to the JavaScript applications on the left while the deobfuscated and runnable Locky executable is shown on the right. This highlights the difference between the file to which the anti-analysis technique has been added and the payload that is created by the JavaScript application as it transforms the obfuscated blob into a functional application.

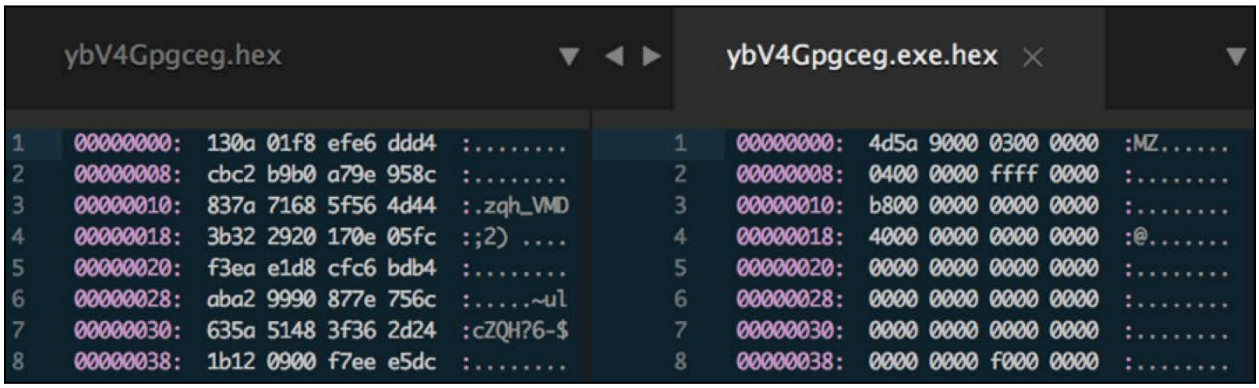


Figure 9 – comparison of obfuscated and deobfuscated Locky binaries

As Figure 10 shows, this obfuscation technique is also coupled with the requirement of a simple command line argument for the malware to successfully execute. This serves to prevent the execution of Locky samples in a sandbox environment without the initial delivery of a JavaScript downloader application.

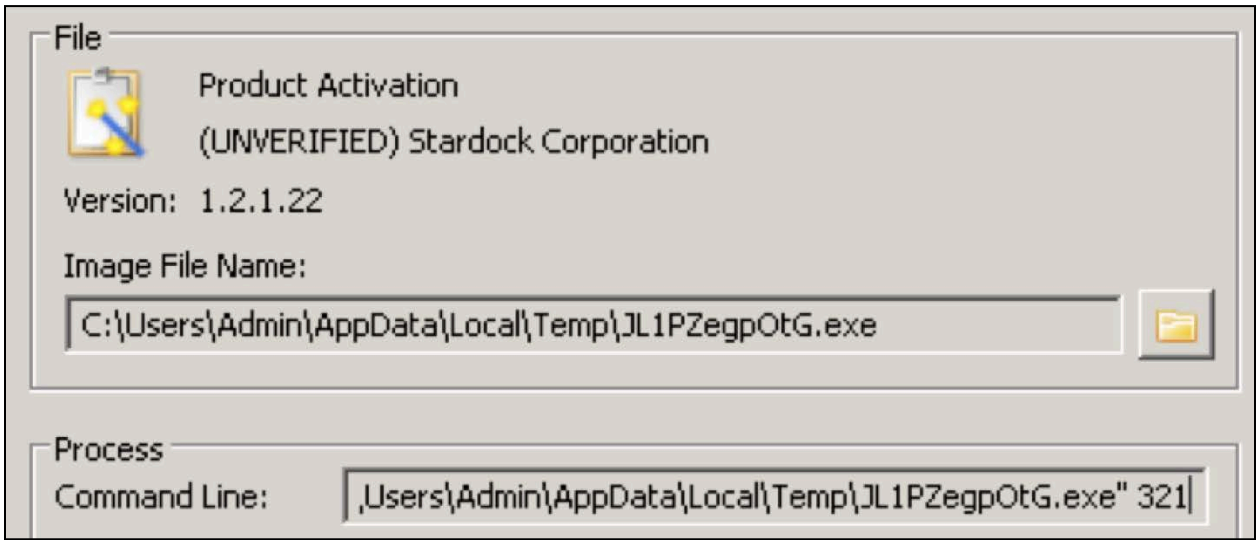


Figure 10 – simple console argument following Locky executable invocation

These extremely simple anti-analysis methods are meant to ensure that the malware will work only in those environments the threat actor desires.

This serves to underscore the hazards of relying entirely on sandbox, network, and endpoint detection and mitigation utilities for securing an organization against malware threats, as these techniques are meant to foil many standard analysis processes.

Instead, addressing threats like this requires educating end users to identify phishing threats and applying threat intelligence to empower information security professionals.

However, the Locky encryption ransomware is not the only malware for which the simple obfuscation of payload binaries serves as an integral part of the delivery process. The Bart encryption ransomware was also delivered as enciphered payloads by the RockLoader malware downloader on Friday, June 24, 2016. Figure 11 showcases an example of the XOR-ciphered content delivered as a Bart ransomware payload.

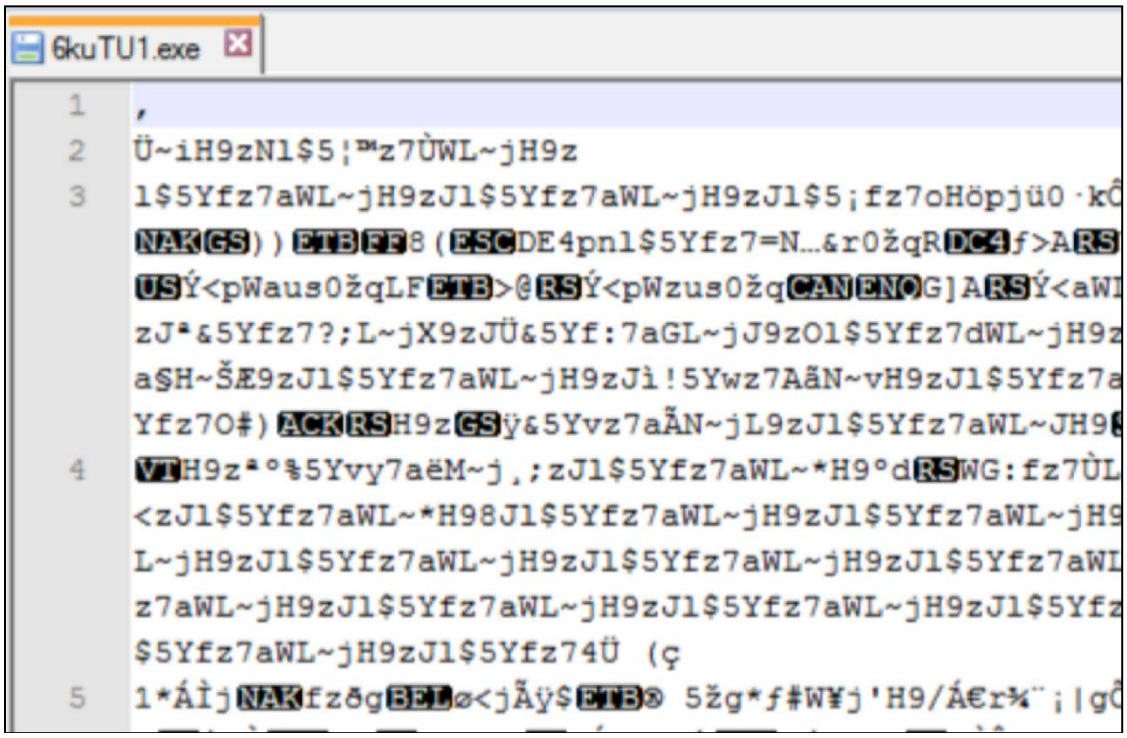


Figure 11 – mismatch of file header bytes where "MZ" has been replaced

Since multiple unique Bart payloads were being distributed by RockLoader contemporaneously, PhishMe researchers attacked this XOR-based obfuscation method to create a way to reliably deobfuscate each file, like the one shown in Figure 11, into a working executable. The approach taken began with a known-plaintext attack based on characteristic byte sequences that are frequently found in Windows executables. The selected known-plaintext and characteristic byte sequence present in most Windows executables was the binary "NOP" or "no-operation" instruction represented in hexadecimal as "90." These were identified through the isolation of a set of repeating values--16-byte value "aWL~jH9zJl$5Yfz7" as shown in Figure 12. (Note that the file header "MZ" was not selected as a known-plaintext due to its short length.)

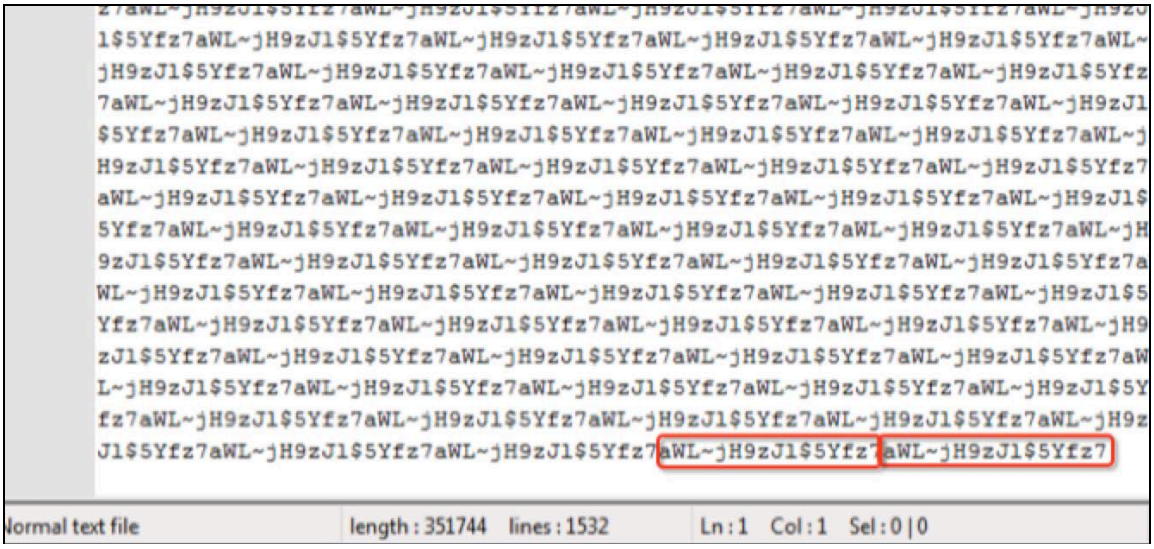


Figure 12 – repeating binary values indicating a known-plaintext

In order to render these values into the desired NOP's, it is necessary to XOR each value with itself. Since the value repeats every 16 bytes, there is some surety that this will be the XOR key. However, this technique can be derailed when file size throws off the position used for iterative decoding. In order to avoid this, it is necessary to read the bytes backwards (or swap them), do the same to the key, and decode the data with the inverse of the XOR key. Doing so created an output that looks much more like a Windows executable. As a result of this work, PhishMe researchers were able to create a Python script tool that can be reliably used to decode these executables. A copy of the tool utilized during this analysis is available for download here.

What's Old is New Again… And Again
jRAT: A Remote Access Trojan with Growing Popularity

Remote access trojan utilities have garnered recent attention due to their purported use in the high-profile intrusion and apparent theft of data from the Democratic National Committee. While details regarding that attack are still private, deployment of remote access trojans via phishing email is a frequent occurrence. Some of the most notable examples from the second quarter were deliveries of a remote access trojan known as jRAT. This remote access utility is a mature and well-supported tool self-identified in its configuration documents as a project of *jrat.io*. Analysis shows this remote access trojan is very similar to the JSocket remote access trojan that was popular during the last months of 2015 and beginning of 2016. The product and service provided by jrat.io and their associated Twitter and GitHub accounts are meant to attract a broad base of users. This, coupled with the support operations and simplicity of this remote access malware, makes it a logical choice for less-sophisticated and script kiddie actors, as well as more advanced actors seeking a multipurpose malware utility.

The modular nature of tools such as jRAT allows threat actors to make the malware do what they want, expanding on and extending the capabilities of relatively simple tools. Once threat actors land a multipurpose utility such as jRAT within a targeted environment, these extended

capabilities afford the threat actors the ability to perform reconnaissance, expand their reach, and customize a set of tools used in the intrusion to accomplish a specific set of goals.

PhishMe analyzed 46 jRAT campaigns during the second quarter. On average, these sets of phishing emails used to deliver jRAT samples consisted of only two sample messages. Compare this to the 176 campaigns delivering encryption ransomware during the second quarter; the average set contained over 34 thousand messages and, as a median, 92 messages were identified per campaign. When juxtaposed with the volume of ransomware campaigns analyzed during the same period, these email sets seem insignificant.

While it is easy to disregard these low-volume phishing email sets and focus on large-volume deployments, the risks associated with less-sophisticated, yet feature-packed malware utilities have been underscored time again through their use by advanced actors. While jRAT and other more basic utilities might be associated with less sophisticated actors, their use by advanced actors is still significant.

One notable attribute of these small jRAT distribution campaigns is their use of phishing narratives meant to appeal to industrial organizations. The content of these narratives varies somewhat from the subtle or vague content shown in Figure 13 to the clear, soft-targeting content seen in Figure 14, the latter designed to appeal to industrial or import/export firms.

Figure 13 – vague spam sample delivering jRAT


Dear sir,

We are pleased to invite you to quote for subject enquiry - attached herewith list of items.

Kindly go through the details and quote us your best price CIF USA, mention the earliest delivery and send us the specification/catalogue.

Your offer complete offer should reach us on or before 10/06/2016.

Awaiting your earliest attention.

Best Regards,

Mrs Shannon Belly

General Manager

The Greenville Trading & Exports Co. LLC
1492 ct hw 17,hendricks, MN 56136
PHONE NUMBER : +1 (507) 5317-1526
USA.

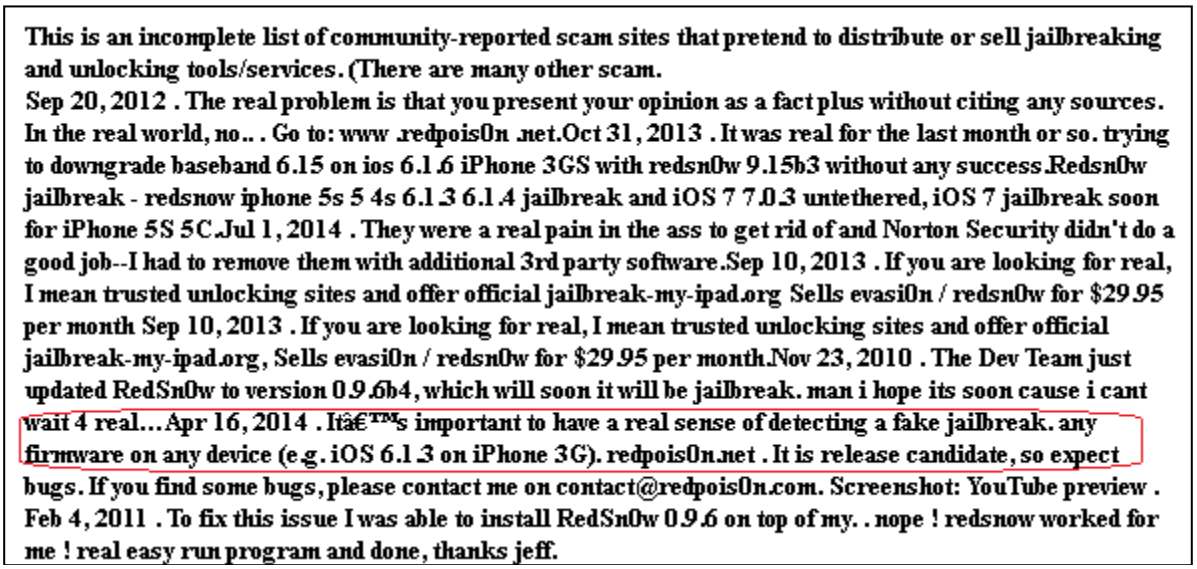
Figure 14 – email using an industrial or import/export soft-targeting narrative

The jRAT remote access trojan is believed to represent the latest iteration and branding of an older and much longer-lived codebase that has been the origin of a number of remote access trojans including Frutas, UNRECOM, AlienSpy, (most notably) Adwind, and (most recently) JSocket. The relationship of jRAT to this codebase is most evident in its configuration document's similarity to the JSocket configuration methodology.

The domain from which threat actors can obtain jRAT is revealed in its configuration file as *jrat.io*; it was registered by “Anders Johansson” of “JSOFT, Storgatan 5, Karlskoga, Vastergotland, SE” on 2014-11-24. The registrant changed on 2014-12-19 to “Gabriel Lundgren” at “Alsteravagen 60, Borensberg, Ostergotland, SE”. “Gabriel Lundgren” is the name of the person who also registered *jrat.me* on 2014-02-17 and *redpois0n.com* on 2010-08-19. This name corresponds to a widely known alternative to the GreenPois0n iOS jailbreak software known as RedPois0n. Despite its creators’ claims, RedPois0n was widely thought to be a rip-off. Lundgren maintains a profile on Keybase as “redpois0n” and links to his GitHub account where the individual’s name is listed as “Oskar Persson” and the email address as red@cmail[.]nu.

The domain *redpois0n.com* is registered to redpois0n@countermail[.]com, which was also used for *jrat.me*. So, how to draw a further connection between the *jrat.io* and the *jrat.me* and *redpois0n.com* domains, registered using the same name but different email addresses? First, look at the hosting resources utilized: less than two months apart, the domains *jrat.io* and *jrat.me* both resolved to 46.227.69.153, and within the same time frame, *redpois0n.com* resolved to a nearby address in the same net block 46.227.64.0/21, belonging to Obenetwork—Sweden. Further, the jRAT Twitter account @java_rat mentions the domain *jrat.se*, which was also hosted on that IP address in the same time frame (early 2015).

A Google-cached blog post from 2012 helps to further tie *redpois0n.com* to *redpois0n.net* which at that point offered a jailbreak tool. From the Google cache[1] of hxxp://fifta35.imahillbilly.com/P3Is-Redpois0N-Real2.html which now hosts a fake tech support scam page, we see the following discussion preserved, where the builder of the product offered on redpois0n.**net** suggests contacting him at contact@redpois0n.**com** with bug reports.



This is an incomplete list of community-reported scam sites that pretend to distribute or sell jailbreaking and unlocking tools/services. (There are many other scam.
Sep 20, 2012 . The real problem is that you present your opinion as a fact plus without citing any sources. In the real world, no.. . Go to: www .redpois0n .net.Oct 31, 2013 . It was real for the last month or so. trying to downgrade baseband 6.15 on ios 6.1.6 iPhone 3GS with redsn0w 9.15b3 without any success.Redsn0w jailbreak - redsnow iphone 5s 5 4s 6.1.3 6.1.4 jailbreak and iOS 7 7.0.3 untethered, iOS 7 jailbreak soon for iPhone 5S 5C.Jul 1, 2014 . They were a real pain in the ass to get rid of and Norton Security didn't do a good job--I had to remove them with additional 3rd party software.Sep 10, 2013 . If you are looking for real, I mean trusted unlocking sites and offer official jailbreak-my-ipad.org Sells evasi0n / redsn0w for $29.95 per month Sep 10, 2013 . If you are looking for real, I mean trusted unlocking sites and offer official jailbreak-my-ipad.org, Sells evasi0n / redsn0w for $29.95 per month.Nov 23, 2010 . The Dev Team just updated RedSn0w to version 0.9.6b4, which will soon it will be jailbreak. man i hope its soon cause i cant wait 4 real...Apr 16, 2014 . Itâ€™s important to have a real sense of detecting a fake jailbreak. any firmware on any device (e.g. iOS 6.1.3 on iPhone 3G). redpois0n.net . It is release candidate, so expect bugs. If you find some bugs, please contact me on contact@redpois0n.com. Screenshot: YouTube preview . Feb 4, 2011 . To fix this issue I was able to install RedSn0w 0.9.6 on top of my. . nope ! redsnow worked for me ! real easy run program and done, thanks jeff.

Figure 15 – screenshot of redpois0n discussion with added emphasis in red

The domain *redpois0n.net* was first registered in 2012 using the email address bmwdriver@windowslive[.]com, an address that is directly tied to the Facebook profile for "Arkadiusz Nawojski." The email address was also used to register the names *crysta1.com* and *cyberelevat0r.net*, both of which profess to offer phone jailbreaking tools. Further investigation reveals additional associations to a host of related jailbreak tools, including rubyra1n, limesn0w, blackra1n, and purplera1n.

The name jRAT was in 2013 known to be provided by "redpois0n" as seen in a Swedish discussion forum thread where the developer offers to answer questions about the tool,[2] and others suggest it has disappeared due to strong suspicions regarding its true intended use. One post there points out the article on HelpNetSecurity[3] "Multi-platform Java RAT targeting government agencies."
When one visits the current *jrat.io* site, the GitHub page is linked to: *https://github.com/java-rat/jrat-web*, where the most current updates were posted by "redpois0n."

In these ways, the operator of the domains is known. Furthermore, it is also clear that this individual knows that the jRAT tool is being used for nefarious purposes. Yet this individual and other associates have continued to distribute the tool with impunity.

[1] http://webcache.googleusercontent.com/search?q=cache:Fo62PRorJtQJ:fifta35.imahillbilly.com/P3Is-Redpois0N-Real2.html
[2] https://www.flashback.org/t2176557
[3] https://www.helpnetsecurity.com/2013/07/08/multi-platform-java-rat-targeting-government-agencies/

An overview of the infrastructure used by the samples analyzed by PhishMe is seen in **Appendix A**. Each set of emails is represented by a small yellow caution symbol and the host name or IP address that was hardcoded into the jRAT is shown with a server or IP address icon. The country of the owner (autonomous system) is shown as a flag. Most of the jRAT infrastructure is hosted in Russia, but the U.S., where most computing infrastructure is found, is not far behind.
Another item that stands out is the use of dynamic DNS hosts. There is no whois data available for the few interesting domain names—such as jrocketmassive[dot]cf, oscanprohd[dot]cf, and perawindi[dot]cf. These infrastructure details, such as the prevalence of the use of dynamic DNS hosts and the resolution to IP addresses within the 185.17.1[.]0/24 net block, are characteristics shared with other remote access Trojans encountered by PhishMe. For instance, the Russian net block includes IP addresses associated with exfiltration of data enabled by the Adwind, JSocket, and NetWire remote access Trojans since December.
PhishMe also examined jRAT configuration documents for interesting correlations among the "NICKNAME," where one of the entries is a "NICKNAME" for the jRAT. Below are a few examples of these names, case-sensitive.

16th-JUN-AU-FARM
admin
ALFREDO
BJ
bless me God
BLESSED_LOGs
Chi m
Dub
emma
EngineBoy
HOME-02-06-16
jun9
kings
KPAJIE
me
MONDAY
MONDAY-FILE
NEWEXCH
payment
pc03
PERACHI-29TH-JUNE
second

SERVER-MONDAY
SHINIKOO
Sunny1
TUESDAY-FILE-28TH-JUN
User
User19
vin 06062016
WIZZY
YES

These “NICKNAME” values fall into three rough categories. First, numerous values refer or correspond to the date of deployment for the jRAT sample—some even specify the day of the week. Examples such as *TUESDAY-FILE-28TH-JUN* or *Monday* show the threat actor customizing the deployment of his or her remote access trojan for a particular day. Second, some “NICKNAME” values refer to plausible usernames or phrases known to be associated with categories of less sophisticated actors. Entries such as *WIZZY* or *SHINIKOO* are plausible usernames while *bless me God* and *BLESSED_LOGs* are phrases often related to threat actors from Nigeria or other Sub-Saharan states. Third, some values represent the threat actor’s desire to generalize the “NICKNAME” field as much as possible by including nondescript terms like *User*, *pc03*, or *admin*. These threat actors are providing far less information in the “NICKNAME” field, likely as a means to deferring any likelihood of being identified.

Conclusion

The second quarter of 2016 saw ransomware settling in as a mature business model—no one should expect it to diminish anytime soon. There was also an escalation in anti-analysis techniques designed to work around security solutions and researchers. Furthermore, the increased deployment of simple remote access malware tools remind us that all intrusion attempts have potentially significant impact.

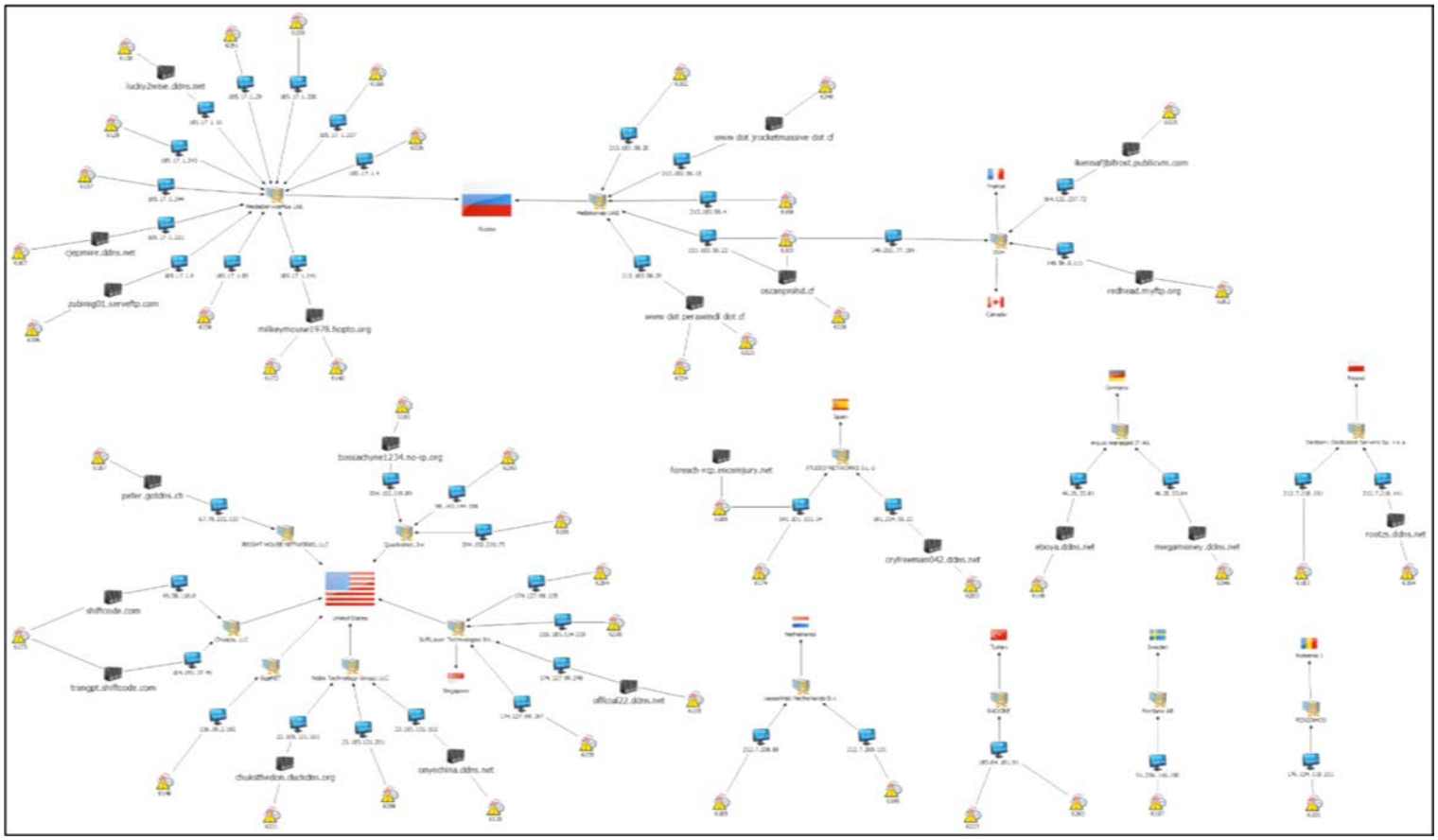
PhishMe Intelligence provides reporting that its customers can use to effectively prepare and respond to phishing threats and attempts to deploy sophisticated and simple intrusion utilities. PhishMe Intelligence provides essential insight into threat actors’ phishing activities by profiling both emerging and established techniques and tools. This reporting is provided in multiple formats designed to help organizations best protect themselves.

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 sales@phishme.com if you have any questions about this report or threat intelligence services.

Appendix A

jRAT support, command and control infrastructure



ABOUT PHISHME, INC.

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