PHISHING THREAT & MALWARE REVIEW

2019

COFENSE.COM

TABLE OF CONTENTS

EXECUTIVE SUMMARY

You've got mail. Look out. This report is about evolution, how phishing emails and malware are in a state of constant flux. But one thing hasn't changed: phishing is still the #1 cyber-attack vector. The vast majority of breaches begin with malicious emails or other social engineering[1] and most malware is delivered by email.[2]

The following pages cover threats that made it through the email gateway, rapid changes in Emotet (aka Geodo), the dominance of credential phishing in a world of email scams, and a great deal more, all viewed through dual lenses: threats we know to have reached enterprise users' inboxes and threats in the wild over the past 12 months.

KEY INSIGHTS

Threat Actors Are Innovating Relentlessly. They are constantly refining their tactics, techniques, and procedures (TTPs) as they develop new delivery mechanisms, phishing techniques, and ways to get around network defense technologies. This is precisely why so many phishing emails are reaching the inbox.

Example: Over the last 12 months, attackers' use of shortened URL services, especially Bitly, has surged. Shortened URLs are difficult to inspect, both with technology and by users themselves. It becomes difficult to determine the final destination of any link.

Technologies Like Email Gateways Can't Keep Pace. In many cases, the speed of threat actors' "product development" keeps network defense technologies a step or two behind. In particular, tactics that make automated detection more difficult have increased in popularity. Secure email gateways (SEGs) play a key role in phishing defense, but they are not infallible. Every day, Cofense™ finds examples of threats that get through.

Example: From October 2018 to March 2019, the Cofense Phishing Defense Center™ verified over 31K malicious emails. Further analysis revealed that 90% of them were found in environments using secure email gateways.

Human Intelligence Is Vital to Phishing Defense. When phishing emails containing malware or a social engineering scam land in users' inboxes, the human factor becomes decisive. It's imperative to educate users through a phishing awareness program, focusing on threats that utilize the latest TTPs. It's also smart to empower your security operations center with the purpose-built systems and human expertise to combat phishing quickly and effectively. Both user education and incident response thrive when fed by threat intelligence on emerging TTPs.

Example: A major healthcare company stopped a phishing attack in just 19 minutes when users reported suspicious emails so the SOC could take quick action. A global financial company did the same thing, using human intelligence to stop an attack in only 10 minutes.

A UNIQUE VIEW OF PHISHING AND MALWARE THREATS

Like the threats it describes, this year's report has evolved. In years past, the Cofense Intelligence™ team looked almost exclusively at malware trends. The 2019 edition retains a strong malware focus, but other Cofense teams, Cofense Research™ and the Cofense Phishing Defense Center, have joined in to share insights on Emotet, credential phishing, and a range of other topics, reflecting our broader mission of stopping phishing threats in their tracks.

Together, our teams offer a unique view of phishing and malware threats. Cofense Intelligence processes and analyzes millions of emails and malware samples each day, providing a macro view of threats in the wild. The Cofense Phishing Defense Center provides a more focused view: the volume, type, and nature of phishing threats that real enterprises (our customers) are facing. This team identifies the attacks and associated TTPs enabling threat actors to evade perimeter controls. Cofense Research is responsible for intelligence-driven research and development. In March 2019, for example, the team was the first to report on significant changes in the Emotet botnet and malware.

For best practices to protect against phishing and malware threats, see a list of proven tips on page 31.

EMAIL GATEWAY MISSES

The secure email gateway (SEG) is an important layer of phishing defense. But it's not a silver bullet. SEGs simply can't keep pace with rapid changes in the phishing landscape. No technical control is 100% effective. The reasons are many and varied, but tend to fall into one of these broad categories:

1. Configuration errors
2. Balancing protection and productivity
3. Previously unknown or unconsidered threat types
4. Unpatched known vulnerabilities or opportunities for feature abuse

In the context of phishing threats, categories 2 and 3 present the greatest risk to controls such as SEGs. Phishing threat actors go to great lengths to understand common business processes and communication habits, then exploit them through novel tactics and techniques.

Cofense enjoys a unique perspective on the actual performance of market-leading SEGs. Every email reported by customers of the Cofense Phishing Defense Center has typically passed through multiple layers of perimeter controls—and still reached the inbox of the targeted recipient.

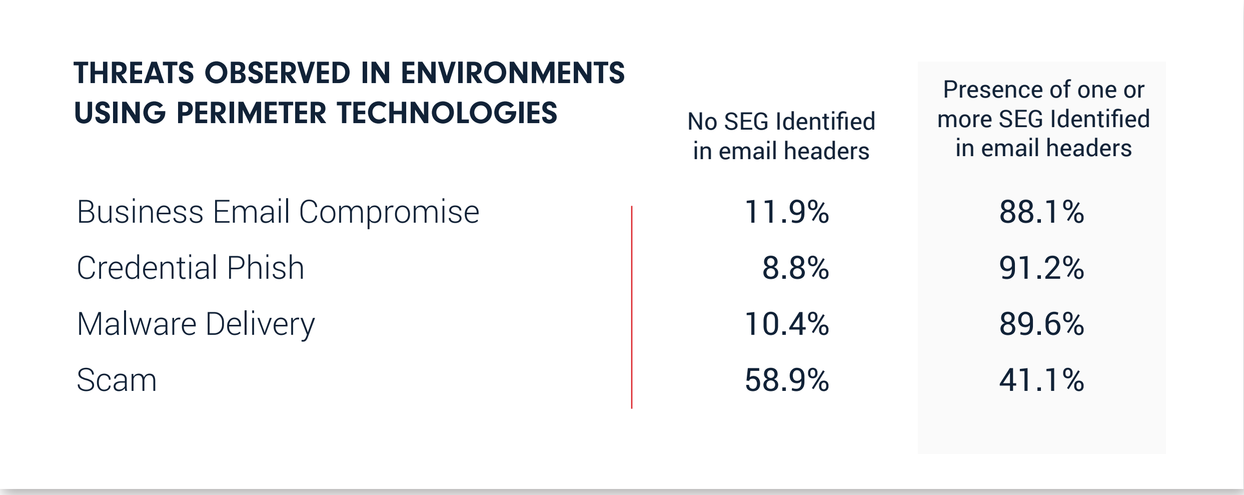
Our team identified the following volume of threats across the most common threat types, as seen in Figure 1.

PHISHING THREATS BY TYPE
October 2018 - March 2019

Business Email Compromise	2,681
Credential Phish	23,195
Malware Delivery	4,835
Scams	718
TOTAL	**31,429**

Figure 1: As identified by the Cofense Phishing Defense Center.

Of these, where the scanning by a SEG or other email protection mechanism could be reliably identified through the presence of X-Headers, Figure 2 shows the percentage of threats which were observed in environments using one or more SEG solutions.



THREATS OBSERVED IN ENVIRONMENTS USING PERIMETER TECHNOLOGIES	No SEG Identified in email headers	Presence of one or more SEG Identified in email headers
Business Email Compromise	11.9%	88.1%
Credential Phish	8.8%	91.2%
Malware Delivery	10.4%	89.6%
Scam	58.9%	41.1%

Figure 2: Threats seen in environments using secure emails gateways[3].

Using the totals in Figure 1, showing 31,429 verified malicious emails, we discovered:

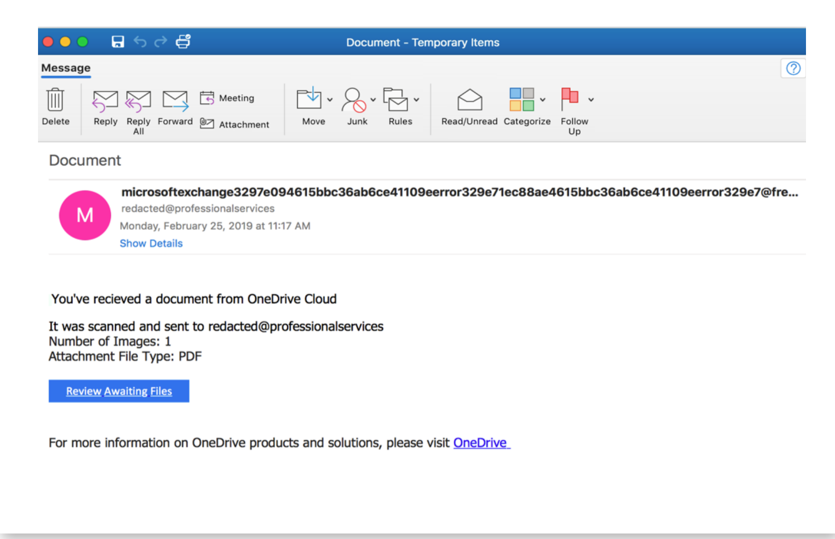
90% OF THE PHISHING EMAILS COFENSE VERIFIED WERE FOUND IN ENVIRONMENTS THAT USE SECURE EMAIL GATEWAYS (SEG).

What the numbers confirm is that all nets have holes—and that end users empowered to spot and report suspicious emails are a critical layer of defense in depth. According to Gartner, 2019 SEG spending is forecast to be $1,785M[4]. Despite significant investments in technology, large volumes of phishing threats are still reaching the inbox.

WHAT THREATS ARE GETTING THROUGH MOST FREQUENTLY

CREDENTIAL PHISH

Credential phish can be difficult to stop at the gateway. Often, the associated infrastructure contains no obvious malicious content. To further mask their intent, these campaigns sometimes send emails from genuine Office365 tenants, using previously compromised credentials or legitimate accounts. When the fake login page is also hosted on Microsoft infrastructure, for example a windows.net, it becomes nearly impossible to tell the bad from the good.



Document

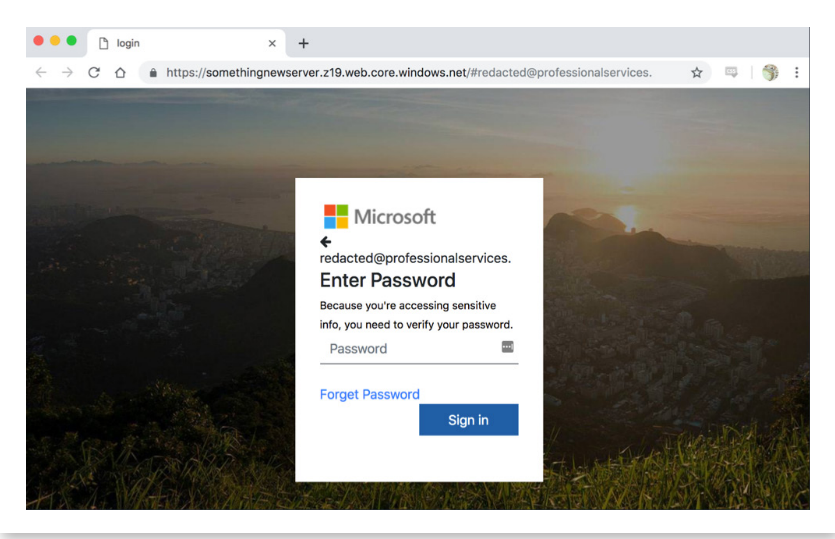
microsoftexchange3297e094615bbc36ab6ce41109eerror329e71ec88ae4615bbc36ab6ce41109eerror329e7@fre...
redacted@professionalservices
Monday, February 25, 2019 at 11:17 AM

You've recieved a document from OneDrive Cloud

It was scanned and sent to redacted@professionalservices
Number of Images: 1
Attachment File Type: PDF

For more information on OneDrive products and solutions, please visit OneDrive

Figure 3: Credential phish attempting to abuse a file-sharing service.



https://somethingnewserver.z19.web.core.windows.net/#redacted@professionalservices.

redacted@professionalservices.
Enter Password
Because you're accessing sensitive info, you need to verify your password.

Figure 4: Fake login page designed to harvest credentials.

Moreover, many gateways don't actually scan every inbound URL. Instead, they limit their scope by only scanning a sampling of URLs that users actually click on. As more phishing campaigns leverage single-use URLs, the risk to enterprises grows. Usernames and passwords are the keys to the enterprise kingdom, explaining why credential phishing is such a thriving business.

As companies move their infrastructure and applications to the cloud, they also move login pages and thus access to network credentials. When an attacker compromises a single user's account, success! Other accounts that share the same password are instantly vulnerable. And if the accounts belong to users in HR or finance, for instance, they become high-value targets giving attackers greater freedom to roam about the network unseen.

An example of the risk: seconds after pulling off a credential phishing attack, one threat actor logged into the host payroll application to change direct deposit information. In an attack on a different company, another attacker lurked in an IT support mailbox, sending "legitimate" emails to employees. This attacker went unnoticed for two entire weeks, until an employee became suspicious of certain requests in an email and alerted the security team.

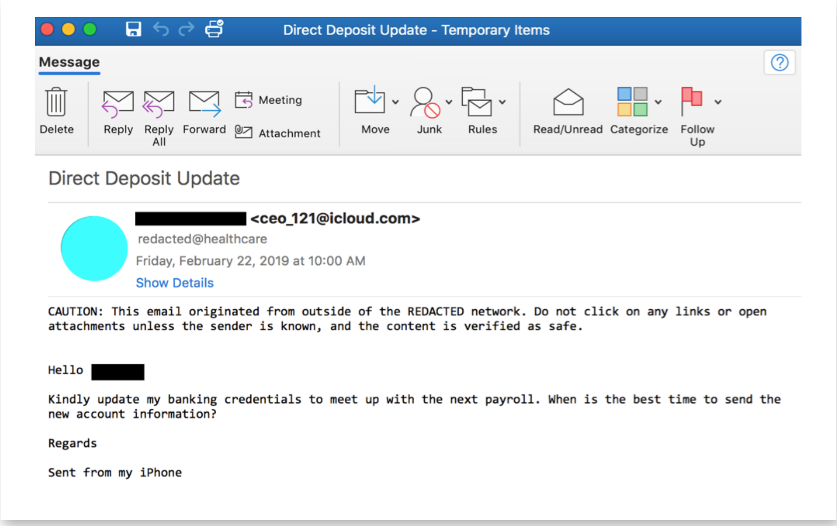
DISTINCT CREDENTIAL PHISHING URLS IDENTIFIED BY COFENSE IN THE WILD

Q1 2018	73,846
Q2 2018	59,016
Q3 2018	49,902
Q4 2018	53,211
TOTAL 2018	**235,975**
Q1 2019	63,575

Figure 5: Cofense has identified nearly 300K distinct phishing URLs since Q1 2018.

BUSINESS EMAIL COMPROMISE

Traditional Business Email Compromise scams typically target accounts payable teams and spoof senior company execs. With many of these scams proving hugely successful, organizations worked hard to raise awareness and technology vendors introduced new defensive capabilities. As a result, towards the end of 2018 the Cofense Phishing Defense Center observed a shift in tactics. Threat actors posed as ordinary employees to target payroll administrators with a simple request: change payroll bank details, so attackers could help themselves to payroll deposits.



Direct Deposit Update

[redacted] <ceo_121@icloud.com>
redacted@healthcare
Friday, February 22, 2019 at 10:00 AM
Show Details

```
CAUTION: This email originated from outside of the REDACTED network. Do not click on any links or open
attachments unless the sender is known, and the content is verified as safe.


Hello [redacted]

Kindly update my banking credentials to meet up with the next payroll. When is the best time to send the
new account information?

Regards

Sent from my iPhone
```

Figure 6: BEC targeting a payroll administrator.

SEXTORTION

Sextortion pushes two buttons, fear and urgency, that cause people to act before they think. And who can blame them? Sextortion emails often include user names, passwords, and other personal information scooped up on legitimate sites or the dark web to make the emails look credible.

The basic narrative: "Your device has been compromised with malware. We've stolen passwords or other personal data. We've been watching you and have webcam footage from visits to dubious sites. Pay up in Bitcoin or another cryptocurrency and your secret is safe." None of which is usually true, despite what a guilty conscience might think.

Though filtering catches sextortion emails, many still get through. No longer just sending text-based emails, sextortionists are switching up tactics. One campaign included:

- Base64 encoded HTML message content
- Body text as embedded images, rather than plain text, to minimize risk of content scanning
- Largely unique, but incorrectly formatted URLs per email, likely to confuse scanning tools
- Unique bitcoin address per email, split into multiple parts in the HTML code (similar to the base href split technique described on page 21), again to minimize risks of pattern matching
- Use of embedded QR code image for the bitcoin address

These elements appeared consistently in a large number of emails, suggesting automation was used to prepare and deliver the campaign. It also shows how easy it is to monetize breached data. Upon reviewing the Bitcoin wallet associated with a recent sextortion scam, the Cofense Research team found the value was roughly $26K. According to Bitcoin Who's Who, as of January 22, 2019 the top 50 reported bitcoin wallets associated with sextortion scams had received nearly 93 bitcoin—as of this writing, just over $481K[5].

BOMB THREATS

Of course, not all extortion campaigns are adult-themed. Bomb-threat emails made headlines in December 2018, when a massive campaign forced evacuations and tied up emergency response and law enforcement for days. Fortunately, they were empty threats. But with subjects like “Better listen to me” and “keep calm,” the emails commanded attention. Cofense obtained and examined a number of these emails. We found they differed in key details to make them harder to detect and originated from junk email accounts at domains that were likely compromised.

EVOLVING THREAT ACTOR TACTICS

Each year our Intelligence team identifies new or resurging TTPs and the Cofense Phishing Defense Center analyzes millions of customer-reported emails. Between March 2018 and March 2019, 1 in 7 reported emails reported to the PDC were confirmed as malicious. Every one of them bypassed technical controls. Some of the tactics and techniques used to deliver malware and evade defense technology detection were simple, adding a creative touch to a sound grasp of technology. Others pitted tech against tech, obscuring malicious intent from mostly automated analysis.

MALWARE DELIVERY MECHANISMS

Of all malware delivered via malicious attachments, Cofense observed a strong preference for the exploitation of CVE-2017-11882 over the last 12 months. While malicious macros were the dominant delivery mechanism during previous years, 45% of all malicious attachments analyzed by Cofense Intelligence over the past year exploited this CVE to deliver malware. During this period, malicious macros accounted for 22% of malware delivery techniques.

We assess this as another example of vulnerabilities ebbing and flowing. Attackers have exploited this CVE in volume. As more defenders patch it and move on from legacy versions of Microsoft Office, expect this tactic’s popularity to fade.

CVE-2017-11882 allows a threat actor to take advantage of a flaw in Microsoft Equation Editor, enabling arbitrary code execution. Microsoft Equation Editor is an older application without many of the restrictions and protections seen in most recent Microsoft programs. Threat actors can chain together multiple OLE objects to create a buffer overflow. This buffer overflow can then be used to execute arbitrary commands, most often involving the download and execution of a malicious executable. This vulnerability can be exploited in almost any version of Microsoft Office currently used by enterprises and is not limited to RTF documents. However, it is most frequently seen being used in RTF documents, because the file format allows automatic OLE Object updates when the file is opened, letting the threat actor launch the attack without requiring the victim to do anything but click.

Threadkit is an RTF file created by a builder which bears the same name. Documents are weaponized to exploit three different CVE's, including CVE-2017-11882. Threadkit will rotate through the exploits until one can be successfully leveraged against Microsoft Office. The other CVE's it exploits by default are CVE-2017-8570 and CVE-2018-0802.

TRICKY EXTENSIONS

Although regular documents were the most common attachment included in phishing campaigns, archive files made up almost 25% of malicious attachments. A breakdown of those commonly used archive types is shown at right and provides insight on what should be blocked at the email gateway in any network environment. Some of these archive types likely have no real use for normal business operations. Businesses may reduce risk by blocking those that serve no legitimate purpose.

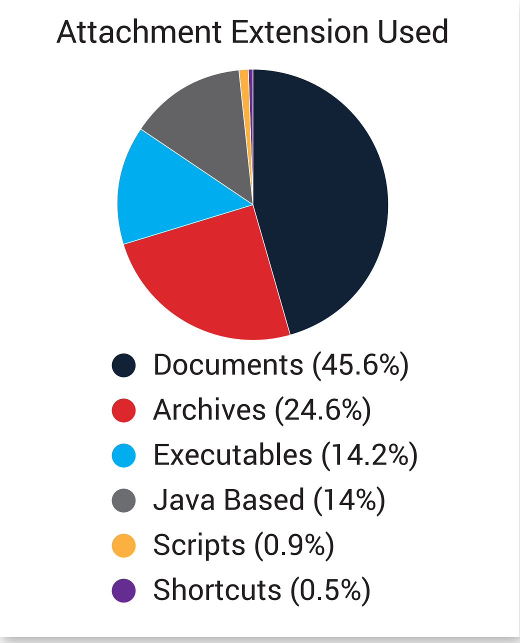


Figure 7: Extension of attached file used to deliver malware April 2018-March 2019.

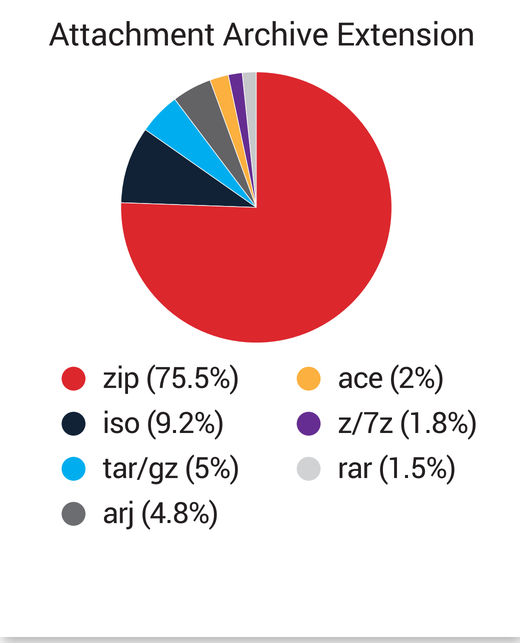
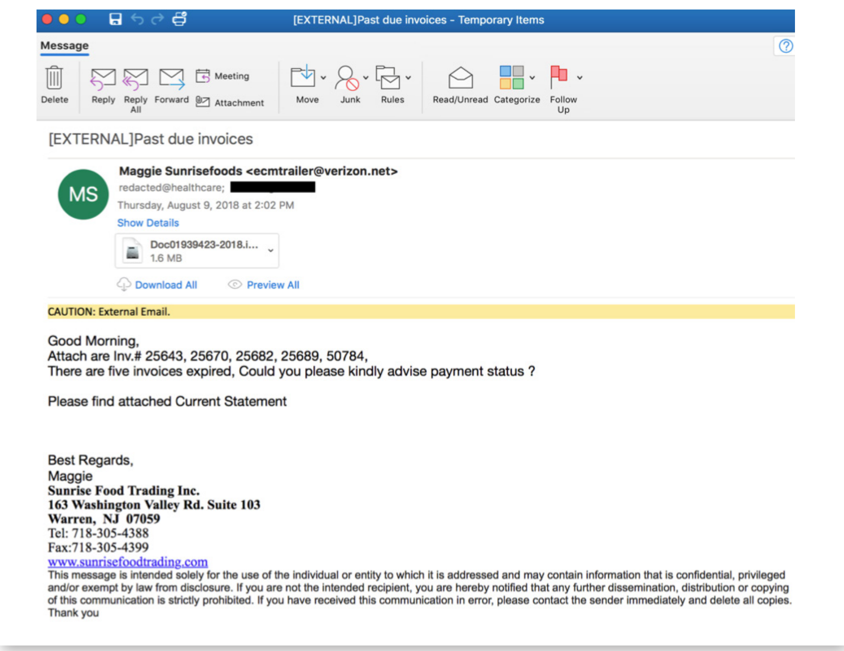


Figure 8: Extension of attached archives delivered via phishing April 2018-March 2019.

UNUSUAL ATTACHMENT TYPES

To bypass the attachment-type controls of secure email gateways, threat actors often use novel file types to distribute payloads. When Windows 10 changed file handling for .ISO files, it presented an opportunity for threat actors to shift away from .ZIP or .RAR files, which are routinely inspected by gateway solutions. Between August 2018 and February 2019, Cofense observed malicious .ISO files bypassing gateways, including Proofpoint—some 3 years after the .ISO file handling changed. In April of 2019, Cofense observed attackers renaming .ISO files to .IMG, which successfully transmitted malware through a Proofpoint gateway.



[EXTERNAL]Past due invoices

Maggie Sunrisefoods <ecmtrailer@verizon.net>
redacted@healthcare; [redacted]
Thursday, August 9, 2018 at 2:02 PM

Doc01939423-2018.i...
1.6 MB

CAUTION: External Email.

Good Morning,
Attach are Inv.# 25643, 25670, 25682, 25689, 50784,
There are five invoices expired, Could you please kindly advise payment status ?

Please find attached Current Statement

Best Regards,
Maggie
Sunrise Food Trading Inc.
163 Washington Valley Rd. Suite 103
Warren, NJ 07059
Tel: 718-305-4388
Fax:718-305-4399
www.sunrisefoodtrading.com
This message is intended solely for the use of the individual or entity to which it is addressed and may contain information that is confidential, privileged and/or exempt by law from disclosure. If you are not the intended recipient, you are hereby notified that any further dissemination, distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please contact the sender immediately and delete all copies.
Thank you

Figure 9: .ISO attachment meant to bypass security controls.

INSTALLATION-AS-A-SERVICE

Why go through the hassle of setting up a spam campaign or compromising websites with exploit kits? Now you can simply pay to have your malware installed on a machine, or series of machines, anywhere in the world. No one has embraced the Installation-as-a-Service (IaaS) business model more than Emotet in 2018. Despite its heredity as a modular banker, Emotet seldom saw action as such. Rather, it became more popular as an intermediary loader for other malware. The last year saw not only a surge in volume of Emotet campaigns but also in those resulting in the installation of dedicated bankers, such as TrickBot, IcedID, and QakBot.

This type of infrastructure offers attackers many advantages, including:

- A laser-focus on a single area of expertise, allowing attackers to refine their craft without spreading themselves thin
- Targeted installations
- Guaranteed delivery for the buyer
- Guaranteed revenue for the seller

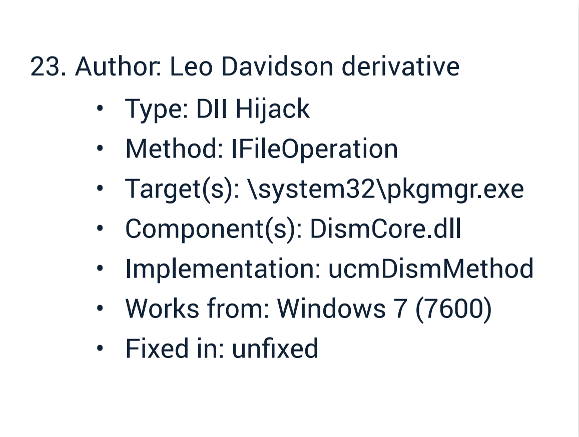
The Emotet gang seems to prefer acting as an intermediary, or loader, rather than a banker. Emotet's evolution over the last 12 months is described at length within the "Evolution of Major Malware Types" section of this report.

BRUTE-FORCING

This novel attack vector gained popularity during late 2018 and into 2019. Brute-forcing involves persistent attacks on Remote Desktop Protocol (RDP) services exposed to the internet. The idea is to guess, over and over, the username and password of an RDP service, until the scripts run out of guesses, the host blocks their connection attempts, or login is successful. Brute-force attacks have delivered a mix of malware types, but ransomware has been the overwhelming favorite, including SamSam, GlobeImposter, GandCrab, and CrySiS.

DETECTION EVASION TECHNIQUES

Every year sees a flood of new toys for the criminally inclined: free tutorials, malware builders, and malware delivery kits, many taking advantage of old flaws and vulnerabilities. The sheer volume of these can overwhelm new patches and fixes. Over the last year, Cofense Intelligence saw the resurgence of older malware that used freely available, well-documented techniques and tools to evade detection and disguise their activities. Also common were changes in C2, customized and limited-use URLs, and the use of ever-popular heavily obfuscated macros.



23. Author: Leo Davidson derivative

- Type: Dll Hijack
- Method: IFileOperation
- Target(s): \system32\pkgmgr.exe
- Component(s): DismCore.dll
- Implementation: ucmDismMethod
- Works from: Windows 7 (7600)
- Fixed in: unfixed

Figure 10: Description on GitHub of the vulnerability abused by the new Ave_Maria malware.

The use of open source tools and information is reflected in the heavy reliance on PowerShell scripts, which have numerous obfuscation tutorials and script generators. Previously, phishing campaigns utilizing PowerShell scripts used minimal obfuscation as part of high-volume campaigns to download malware such as Ammyy Admin, Banload, Client Maximus, Ursnif, or URLZone. Attackers have recently used PowerShell in a large variety of low-volume campaigns. This variety is no surprise to see—publicly available tools and tactics are often used in low-volume campaigns as they are so easily acquired and disseminated. By downloading a PowerShell script with an obfuscated embedded file, attackers are able to avoid network defenses which would detect normal executables.

Executables that make use of the .NET framework have also become more common. They too can make automated detection more difficult. These executables often serve as intermediary loaders, capable of containing or downloading multiple other malware binaries. In the last year, in over 70% of the cases when .NET executables downloaded a binary, the downloaded binary was an image containing an embedded executable. Because the file is a legitimate image, most anti-virus (AV) systems will examine the file different and the download will successfully bypass the AV. This allows the .NET executable to extract the embedded malware, load it into memory, and run it without the AV system noticing.

Cofense has also observed increased manipulation of files to hide their contents in PowerShell scripts with embedded executables and in the image files downloaded by .NET executables. Some threat actors have taken advantage of a different form of file manipulation by crafting files that appear to be broken, allowing them to bypass some defenses. This manipulation is used to avoid detection when files are downloaded, opened, and even sent as attachments.

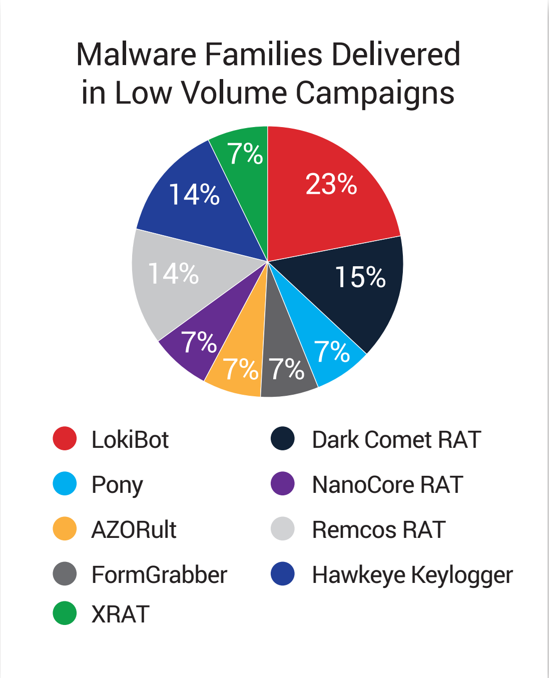


Figure 11: Percentage of malware families delivered via PowerShell in unique low volume campaigns.

One more example of innovation: Cofense Intelligence has observed an increase in phishing campaigns in which malicious payload locations were obfuscated with link shorteners such as Bitly. The campaigns commonly utilize a Microsoft Word document that exploits CVE-2017-11882 to download a payload from a site obfuscated and directed to via a shortened URL. Threat actors leverage the fact that link shorteners are rarely blocked and that they obfuscate the true location of a malicious payload. This allows the true location to bypass URL content filtering as well as other security measures. Bitly itself is not inherently malicious and is used to host links for many legitimate websites, making it all the more attractive for threat actors to abuse.

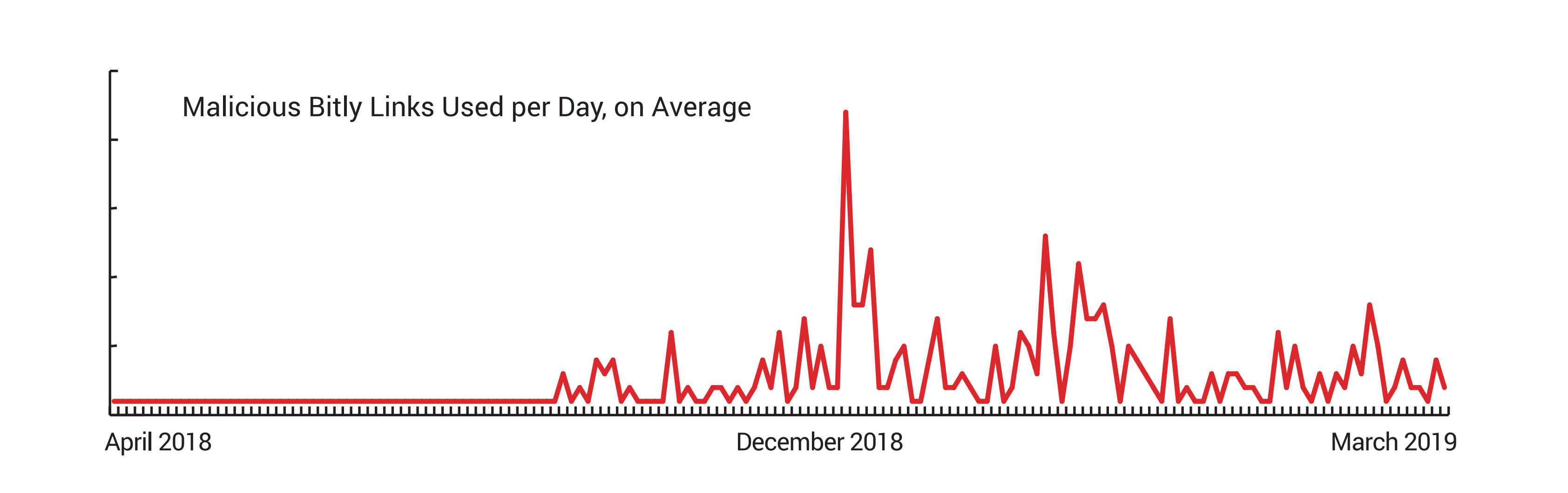
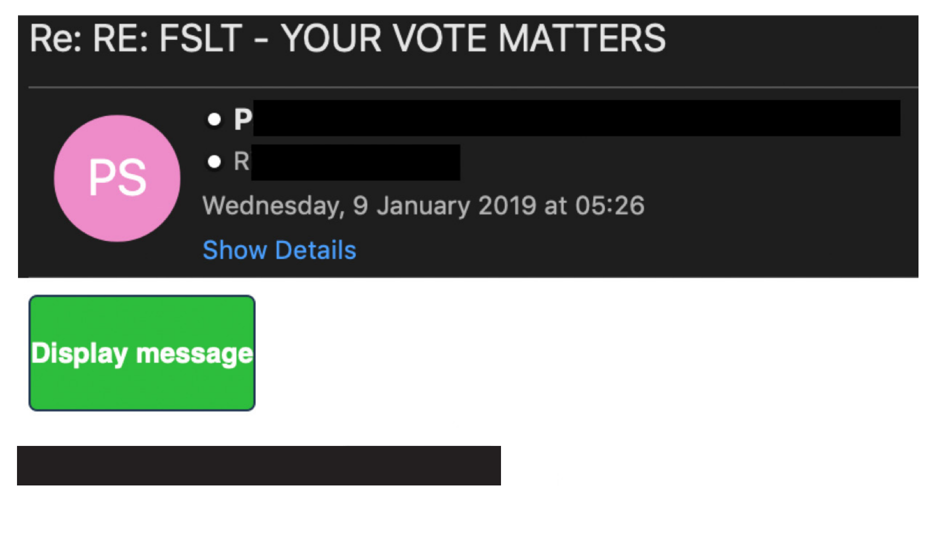


Figure 12: Malicious Bitly links spiked in December 2018 and have continued to be popular since.

REAL PHISH THAT GOT THROUGH

This year, the TrickBot and Emotet botnets became more sophisticated and dangerous. Cofense has seen several Emotet campaigns reach users' inboxes. By moving from simple text block email lures to well-crafted impersonations, often scraping real emails from compromised users and generating templates based on legitimate emails, they have become much more effective. Recently, TrickBot used social engineering to trick victims into downloading malware masquerading as a "plugin" required to view a web-hosted document.

If we had to name a winner for craftiest detection-evasion technique, it would be the Zombie Phish. Cofense saw this well-known technique put to new use: a Zombie Phish campaign in which fraudsters hijacked compromised email accounts and, using those accounts' inboxes, replied to long-dead conversations with a phishing link. Because the subject of the email is relevant to the victim, he or she is likely to click. And who would ever think that a legitimate email chain among people who know each other would become a medium for malware delivery?



Re: RE: FSLT - YOUR VOTE MATTERS

- P [redacted]
- R [redacted]

Wednesday, 9 January 2019 at 05:26

[redacted]

Figure 13: Zombie Phish reviving a dormant email thread.

When combined with other techniques—for example, malicious content hosted in cloud-sharing services like Dropbox, OneDrive, or Sharepoint.com—the zombie phish can neutralize inline tech controls.

ABUSE OF CLOUD FILESHARING SERVICES

Here again the cloud becomes an attack vector. Threat actors know that organizations are investing in technical controls to identify, analyze, and remove malware attached to emails. They also know that companies rely on file-sharing platforms such as Dropbox and Google, which are not routinely blocked by many enterprises. Users are often comfortable with downloading content from these "trusted" locations. For example, many of us rely on Office365 for our daily business operations. It should be no surprise that it's now one of the most abused cloud services.

As a result, the Cofense Phishing Defense Center and Cofense Intelligence teams often see the abuse of these filesharing platforms to host and spread malicious content, including "legitimate" links to the content embedded in the phishing email. This makes it difficult for automated URL analysis tools to determine whether the link is malicious, particularly if users are required to enter credentials. As adoption of Dropbox, OneDrive, or SharePoint grows for benign business purposes, technologies find it more difficult to separate good from bad. Automated controls commonly don't flag these services as malicious. Worse still, the filesharing platforms appear unable, or unwilling, to resolve the problem.

Among other reasons for their growth, cloud filesharing and its abuse are often free and automatable, requiring no technical skill. Just sign up for an account—or upload a PDF containing a phishing link. For those with enough technical knowledge, many of these services offer API's to help automate the share and uploading of files. Once an attacker has his pipeline in place, he can create and send phishing emails en masse. When the security team spots the attack, it's no big deal for the attacker to create another account, tweak a few parameters, and get back in the game.

Between March 2018 and March 2019, the Cofense Phishing Defense Center analyzed 9,445 phishing emails that utilized cloud filesharing services to deliver a malicious payload. Sharepoint.com holds the top spot among the badly abused, closely followed by OneDrive.

PHISHING EMAILS UTILIZING CLOUD FILESHARING SERVICES

	Count	% of Cloud Service Phish (9,445)
Sharepoint	5,211	55%
OneDrive	1,965	21%
Sharefile	912	10%
WeTransfer	514	5%
DropBox	408	4%
Egnyte	238	3%
Google Docs	197	2%

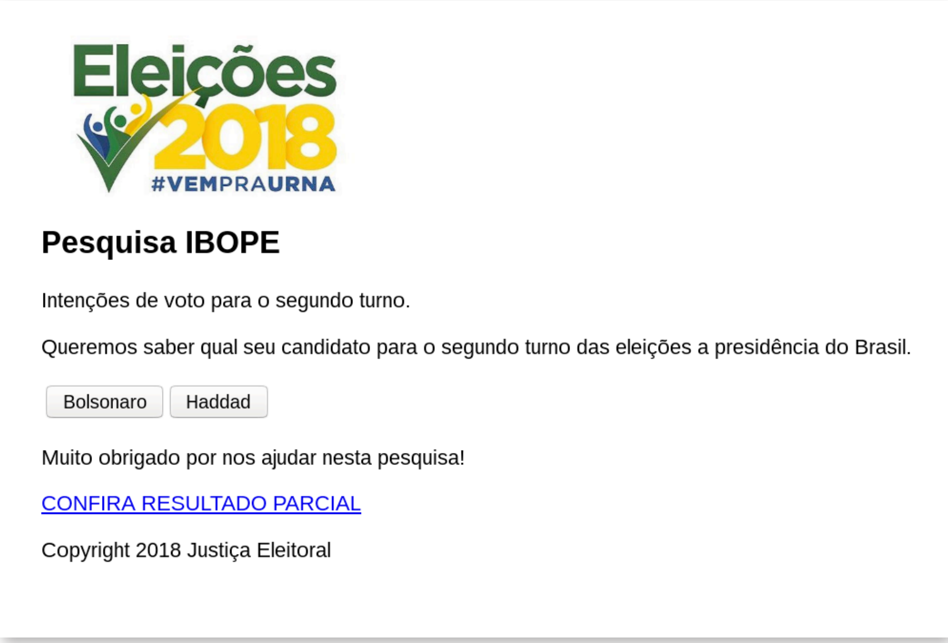
Figure 14: Sharepoint was the most-abused cloud filesharing service observed by Cofense.

GEOLOCATION-AWARE PAYLOADS

It's now common for threat actors to deliver phishing emails whose payloads behave differently depending where the recipient is. For example, a user in one country could be served benign content, while a user in a different country could be served something malicious. Or, different malware is retrieved and delivered depending on the target's location. We're talking about the use of IP/geolocation.

This tactic also helps prevent analysis by security tools or human researchers. For example, if a threat actor knows or suspects that specific cloud-based security tools might be in use, benign content is served to the known security vendor's IP addresses—or more broadly to certain cloud-hosting providers' IP ranges. Once deemed to be safe, the email sails away and the malicious payload is delivered.

Example: Brazilian Targets. Joining the US elections as a phishing target, the 2018 Brazilian elections inspired emails impersonating the IBOPE (Brazilian Institute of Public Opinion and Statistics). This campaign leveraged multiple election-themed phishing narratives and geolocation techniques to target Brazilian users. Once the user downloaded a malicious archive file via the embedded link or attachment, the remote hosts that delivered files for further infection would only deliver to users confirmed to be in Brazil. Other users were redirected to Google.com. By narrowly targeting only intended victims, the campaign made it harder for international researchers to identify and defend against it.



Pesquisa IBOPE

Intenções de voto para o segundo turno.

Queremos saber qual seu candidato para o segundo turno das eleições a presidência do Brasil.

Muito obrigado por nos ajudar nesta pesquisa!

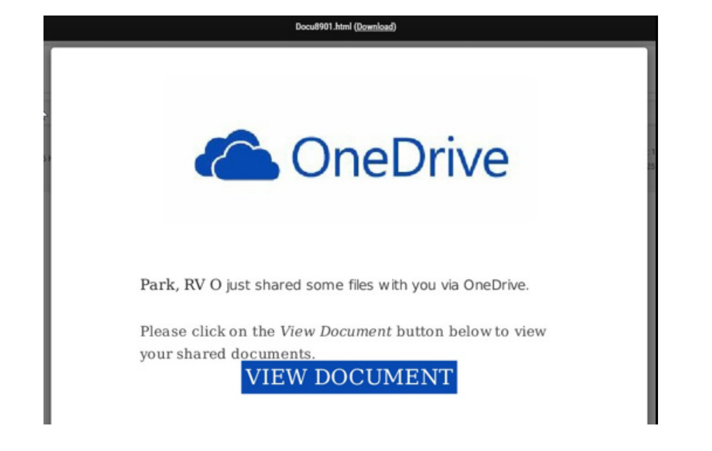
CONFIRA RESULTADO PARCIAL

Copyright 2018 Justiça Eleitoral

Figure 15: Image of the email content spoofing IBOPE targeting Brazilian users.

In a different campaign—this time a credential phish—a Cofense customer in Brazil received email attachments that seemed benign, but smelled a little phishy. Deeper (human) analysis revealed why. When an analyst gave his workstation a Brazilian IP address, the attachment behaved differently, connecting to payload infrastructure and downloading a malicious script. Though the script didn't execute, further analysis showed more "location validation" checks. After a bit more digging, we captured the indicators of compromise.

Attackers don't just apply this technique to malware delivery. The use of traffic misdirection, IP range filters, and geolocation validation have all been observed in credential phishing. In the following example, Cofense analyzed an email with an HTML attachment.



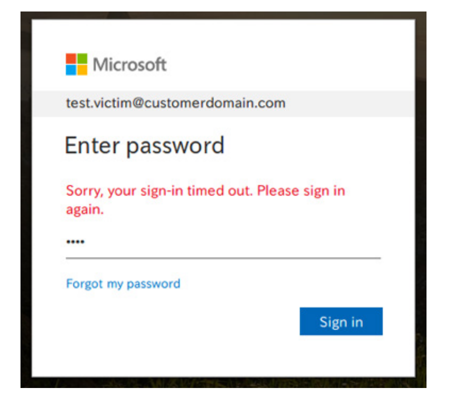
Docu8901.html (Download)

Park, RV O just shared some files with you via OneDrive.

Please click on the *View Document* button below to view your shared documents.

Figure 16: Credential phishing email linking to geolocation aware fake login page.

Upon clicking the 'View Document' link, the recipient is directed to a fake Microsoft login page, with the victim's username automatically embedded (in this case, test.victim@customerdomain.com). Despite having all the hallmarks of a simple credential harvesting phish, this email displays unusual behavior when characters are entered into the password field and submitted.



test.victim@customerdomain.com

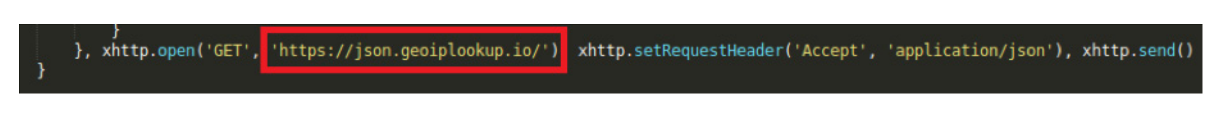
Enter password

Sorry, your sign-in timed out. Please sign in again.

••••

Figure 17: Error message displayed if not submitted from target geolocation.

Upon closer inspection of the source code, the analyst was able to determine that the phish would be submitted only if the user tried to access the document from a specified location, in this case Mexico. This was accomplished with a geolocation lookup:



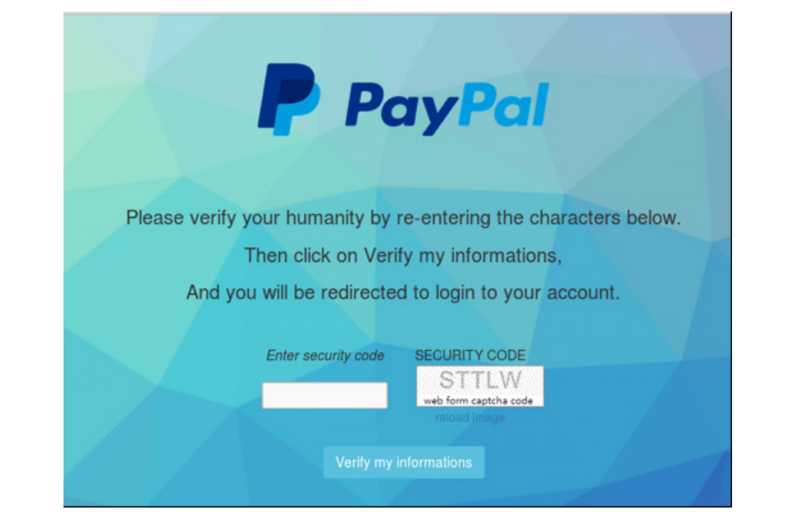
```
        }
    }, xhttp.open('GET', 'https://json.geoiplookup.io/')  xhttp.setRequestHeader('Accept', 'application/json'), xhttp.send()
}
```

Figure 18: Use of geolocation lookup in login page code.

THE CAPTCHA PHISH

Phishing emails have started to utilize CAPTCHA technology, which ironically is designed to block bots. In this example, the simple CAPTCHA mechanism is turned against machines performing legitimate content analysis. It's another way to circumvent technical controls.

Poor grammar notwithstanding, this phish requires the user to enter and submit the CAPTCHA phrase. Users are then directed to the credential phishing site.

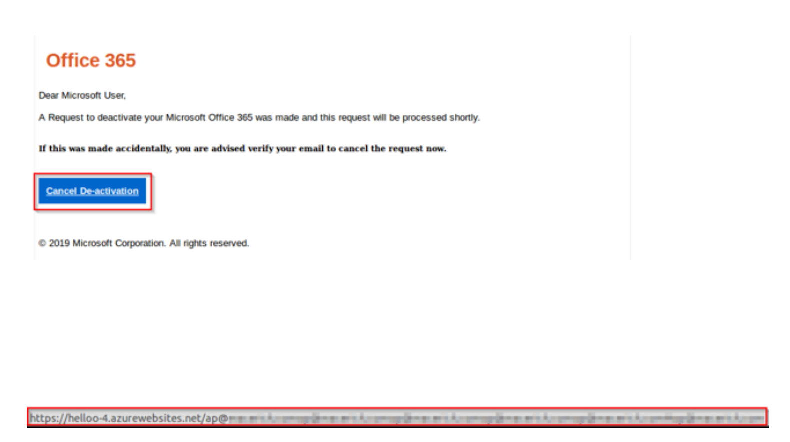


Please verify your humanity by re-entering the characters below.
Then click on Verify my informations,
And you will be redirected to login to your account.

Figure 19: Use of CAPTCHA to verify human interaction.

EXPLOITING HTML STRUCTURE

Threat actors have long exploited their knowledge of HTML to deceive email defenses. Techniques such as zerofont and Unicode bi-directional have been around for some time and threat actors continue to innovate. In an emerging detection evasion tactic, actors are using base href splitting to confuse content scanning engines. Here's a sample that appears to be a straightforward credential phish.



Dear Microsoft User,

A Request to deactivate your Microsoft Office 365 was made and this request will be processed shortly.

If this was made accidentally, you are advised verify your email to cancel the request now.

© 2019 Microsoft Corporation. All rights reserved.

https://helloo-4.azurewebsites.net/ap@[redacted]

Figure 20: Email using various techniques including text padding and base href split method – content is displayed appropriately within the client.

Further analysis revealed a number of techniques to ensure delivery of malicious content. Among them:

- Heavily padding HTML with hidden garbage text “wd6w3df1w2wfv” between each letter to break keyword detection
- Using the “base href” split method to separate the URL parameters (ap@victim.com) from the base domain (helloo-4.azurewebsites.net) to further confuse standard defenses. Email scanners often only parse the base href domain, which is the trusted Microsoft hosting site “azurewebsites.net”.
- One other sneaky trick is the reversal of the second slash in the standard hTTPs://, using instead “hTTPs:/\”. This may cause an email scanner to ignore the link, but modern browsers are able to detect and automatically fix the “typo.”

EVOLUTION OF MAJOR MALWARE TYPES

EMOTET IS DOMINANT

The Emotet trojan first appeared as a piece of banking malware in 2014, but has since evolved into a complex botnet that carries out multiple functions. Today, it looms as one of the biggest threats in the malware landscape. The threat actors behind it work deliberately to expand and monetize their operation. Over the last year, Cofense observed notable changes to the Emotet malware and its botnet.

Typical Compromise Timeline

The predominant delivery mechanisms for Emotet is an email bearing an office document with macros, a message body containing a link, or a PDF with a link. For the messages that contain a link in the body or attachment, the URL typically leads to the download of a macro-enabled document. The final Emotet binary is retrieved via the macros in the document.

Emotet then installs itself on the machine, using a unique name generated from an embedded wordlist based on attributes of the infected computer. Then, it gathers data from the host such as email credentials, email contact lists, and email signature blocks. In the latter half of 2018, Emotet also began to exfiltrate and scrape emails to use as templates in future campaigns. As this data is handed off, the actors use the account of a compromised user to send malicious emails to that user’s contact list.

Emotet is modular and will pull down additional utilities as needed. It has been known to brute-force credentials of computers within the same network and spread laterally. This further complicates efforts to remove the infection once a single person within an organization is hit. Beyond Emotet's ability to compromise hosts, the actors behind it appear to sell off many high-value infections to other groups. In the past year, we've seen Emotet act as a loader for TrickBot, QakBot, and BokBot, among others. Often, those secondary infections drop ransomware to generate extra revenue.

Emotet Infrastructure

The Emotet botnet is comprised of two distinct groups. These have come to be known as Epoch 1 and Epoch 2. While the underlying malware is identical, each epoch utilizes a distinct RSA key as well as C2 infrastructure. When reviewing the C2 interactions of two clients on each epoch, it becomes very evident that there are unique groups within the botnet.

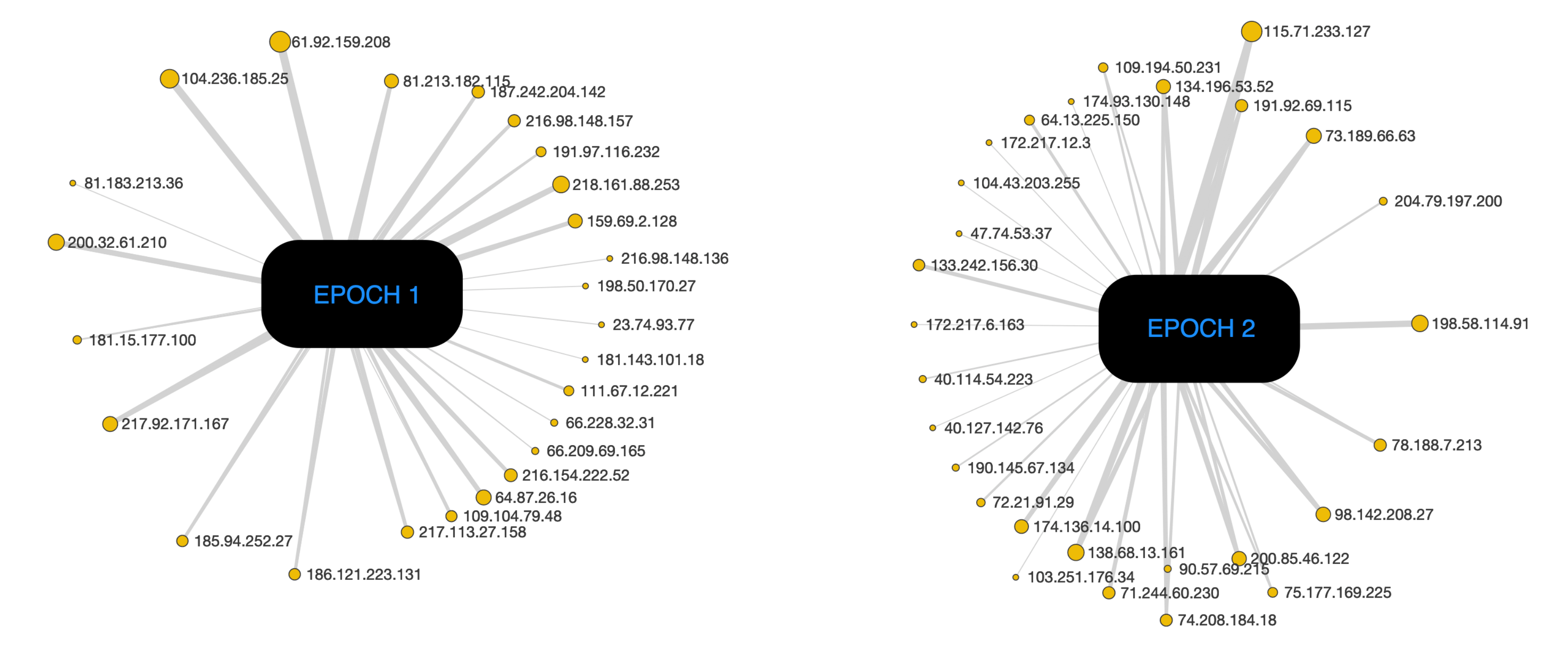


Figure 21: Emotet's botnet infrastructure comprised of two distinct "epochs."

Past versions of the botnet would communicate with their C2 via a GET request with an encoded cookie value to an IP with no path. This recently changed to a POST with form data and includes anywhere from 1 to 4 variable words in a path. The apparent reason for this change is to impair detection and the efforts of researchers emulating the botnet code.

Tier 1 C2's for the botnet can change daily, typically totaling about 60. This distributed and ever-evolving architecture makes takedowns difficult to coordinate. There are a vast number of tier 1 hosts, with many more layers beyond, which makes tracking much harder. The number of C2's utilized daily has grown in the past year, likely due to the rapid expansion of the botnet itself. While it isn't possible to give an exact number of active bots, Cofense can definitively state that we've seen at least 678,000 unique infections since early 2018.

Emotet relies on compromised sites to deliver its payloads. Some host the malicious document that is downloaded from clicking links or embedded macros. Others host the actual Emotet binary. There have been days when over 500 unique domains were recorded in use at once, which indicates that the actors have the time or money to keep up this compromise rate for new hosts, with many added every day.

Email Evolution

For the greater part of 2018, the email templates delivering Emotet remained fairly generic and always delivered the final payload via one of the standard methods outlined above. The last six months have seen rapid change, possibly a response to the growing army of security vendors defending against Emotet. Some of the most recent changes include:

- **Removal of message-id field auto-generated within the template code.** Defenders used the message-id field as an easy way to filter out Emotet messages. Removing this generated field causes the relay to add another one, making it impossible for defense technologies to detect that a message is tied to an Emotet campaign.
- **Weaponized JS attachments.** This is non-standard for Emotet and appears to be a deliverability test.
- **Zip attachments.** Zipping up the attachments may allow for the payloads to bypass some gateways.
- **Password protected zip archives.** The use of AES encryption is novel, since standard Windows libraries cannot decompress it. This means, however, that it likely bypasses most gateway technologies as well, requiring the end user to use a program such as 7zip to open the attachment.

The actors behind the Emotet botnet are skilled and extremely businesslike. They favor slow, measured changes to their production environment, plus continued testing of gateway bypass techniques. Emotet is a serious threat to any organization. Credential theft is bad enough, but it's nothing compared to compromised machines being sold to the highest bidder.

While Emotet was dominant in the threat landscape, other malware families were also quite active. The following comparisons do not include Emotet—because it has been so highly active in the past few months, we are still calculating its size and impact. Suffice it to say its dissemination and propagation are massive.

Top Malware Families Delivered via Malicious Attachments Outside of Emotet

2018-2019	
LokiBot	35%
Other	33%
Pony	13%
Hawkeye Keylogger	6.5%
NanoCore	6.5%
jRAT	6%

Figure 22: Outside of Emotet, LokiBot was the top malware family delivered via malicious attachment over the past 12 months.

2017-2018	
Other	50%
Generic Remote Access Trojan	16%
Pony	15%
LokiBot	11%
Generic Keylogger	4%
Locky Ransomware	4%

Figure 23: In 2017-2018, no single malware family dominated the landscape in delivery via malicious attachments.

TRICKBOT: A ONE-STOP SHOP

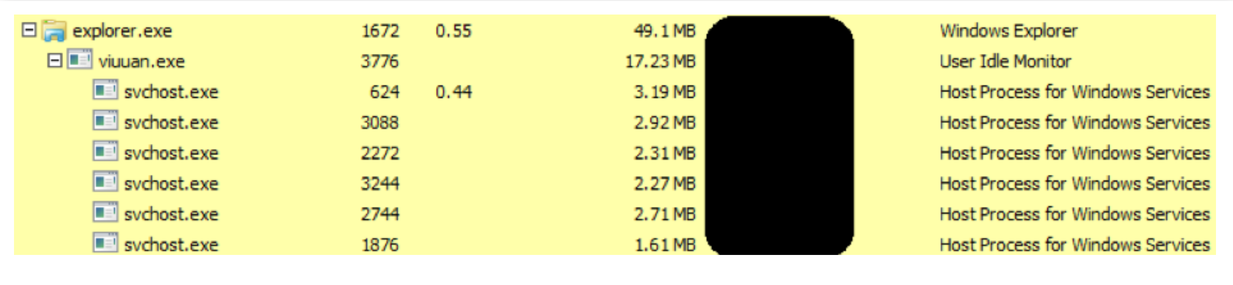
TrickBot is a modular banking trojan, an ancestor of Dyer, and maybe the most potent banker threatening the world today. With modules available to drive lateral movement, back-connections, and data-theft, TrickBot stands alone as a one-stop shop for criminal activity. TrickBot has two primary methods to infiltrate victim computers: phishing and Installation-as-a-Service.

TrickBot, and previously Dyre, have been linked to distribution by several botnets, among them Cutwail, Trik/Phorpiex and Necurs, used to distribute phishing messages to specific countries or regions and to abuse legitimate, hacked email accounts. The campaigns have a very distinct pair of features:

- They use incredibly well-crafted spoofs of major financial companies or online services
- They use spoofed (or cybersquatting) domains to add legitimacy

In examples analyzed by Cofense, the URLs included in the phishing message were often legitimate, leading to the webpages of whatever brand was spoofed. Only the document was weaponized. As a modular trojan, Trickbot has a discrete module for most any kind of nefarious activity. The modules are stored in a hardcoded folder within the victims %appdata% directory.

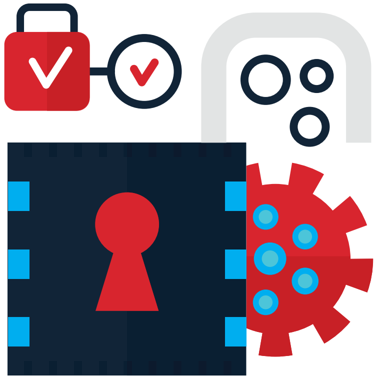
Each module is an encrypted executable that is decrypted and subsequently injected into its own svchost.exe process.



⊟ explorer.exe	1672	0.55	49.1 MB	[redacted]	Windows Explorer
⊟ viuuan.exe	3776		17.23 MB	[redacted]	User Idle Monitor
svchost.exe	624	0.44	3.19 MB	[redacted]	Host Process for Windows Services
svchost.exe	3088		2.92 MB	[redacted]	Host Process for Windows Services
svchost.exe	2272		2.31 MB	[redacted]	Host Process for Windows Services
svchost.exe	3244		2.27 MB	[redacted]	Host Process for Windows Services
svchost.exe	2744		2.71 MB	[redacted]	Host Process for Windows Services
svchost.exe	1876		1.61 MB	[redacted]	Host Process for Windows Services

Figure 24: A typical process tree for a TrickBot infection.

Modules



Rather than hardcoding functionality into a binary, TrickBot uses modules—essentially standalone executables that are injected into legitimate Windows processes—to perform its lucrative activity. Most modules come with a separate configuration file stored in %installdir%\data\<modulename>_configs\ and usually any or all of: dpost, dinj, and sinj.

- **InjectDll32.** This is the banking module, responsible for injecting DLLs into Chrome, Firefox, and other supported browsers to facilitate financial theft (i.e. banking).
- **networkDll32.** Responsible for retrieving information about the local network topology. It does so by executing native commands such as ipconfig and net.
- **psfin32.** Attempts to identify if any PoS (Point of Sale) computers exist on the local domain.
- **pwgrab32.** The major data-theft engine. This module steals information such as logins, history, and cookies from browsers. In early 2019 this module received an update which included the theft of remote application credentials like Putty and RDP.
- **shareDll32.** Attempts to propagate TrickBot by logging into discovered remote machines' admin$ share and dropping a freshly downloaded copy of itself to the root of %systemdrive% (usually C:).
- **systeminfo32.** Recovers basic information about the machine, such as operating system version and bitness, accounts, and GUIDs.
- **tabDll32.** Uses leaked NSA exploits in an attempt to spread. Additionally, uses a screen locker component to disable Windows security features and facilitate the use of Mimikatz.
- **wormDll32.** Attempts to spread itself via SMB.

CHANITOR: DITCHING ZEUS PANDA FOR URSNIF

Chanitor, otherwise known as Hancitor, is a downloader spread via phishing campaigns. Uniquely, the malware is typically macro-based. Rather than having an Office macro download and execute an intermediary payload, the actors behind Chanitor use the macro to inject code directly into a hollowed process. This type of fileless infection makes Chanitor more difficult to detect.

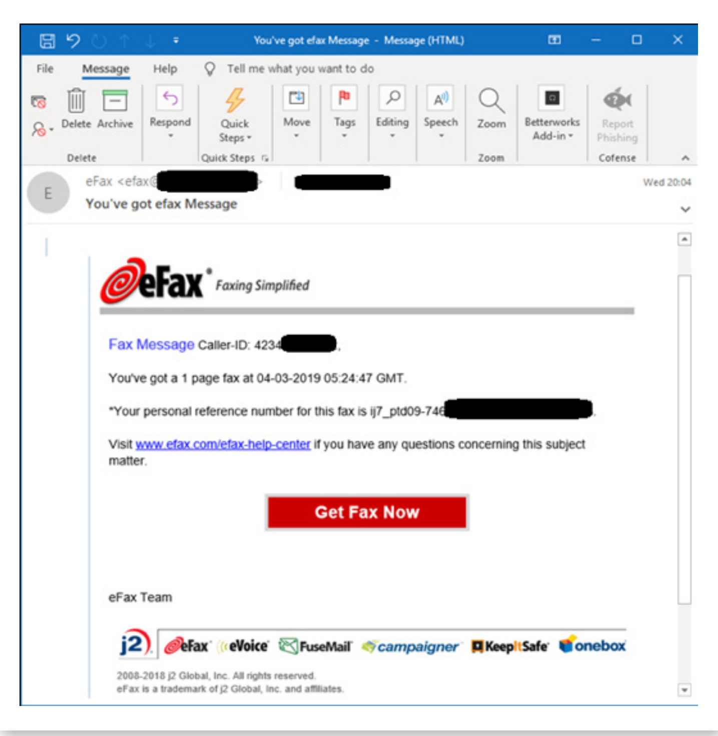
Propagation

Chanitor arrives on a target machine through well-crafted phishing emails containing URLs which point to weaponized Office documents. Chanitor spoofs a wide array of entities and verticals.

The retrieved Office documents contain hostile macros, which will either decode and inject a sample of Chanitor directly into a legitimate Windows process or download and execute a sample from a remote host. The former is significantly more common.

Activity

Chanitor is a downloader—not unique in type or objective, but the way it works merits discussion. Its modus operandi is to download two instances of Pony, together with at least one additional payload, usually a banker. Originally favouring Zeus Panda, Chanitor has recently developed a fondness for Ursnif and has been serving it exclusively throughout 2019.



eFax <efax@[redacted]> [redacted] Wed 20:04

You've got efax Message

eFax Faxing Simplified

Fax Message Caller-ID: 4234[redacted].

You've got a 1 page fax at 04-03-2019 05:24:47 GMT.

*Your personal reference number for this fax is ij7_ptd09-746[redacted].

Visit www.efax.com/efax-help-center if you have any questions concerning this subject matter.

Get Fax Now

eFax Team

j2 eFax eVoice FuseMail campaigner KeepItSafe onebox

2008-2018 j2 Global, Inc. All rights reserved.
eFax is a trademark of j2 Global, Inc. and affiliates.

Figure 25: An example, eFax-spoofing email delivering Chanitor.

‘SUP WITH RANSOMWARE?

Ransomware has steadily declined since its 2017 heyday. That year, Cofense Intelligence identified over 15 unique ransomware families delivered in high-volume, widespread phishing campaigns, versus fewer than 10 in 2018 and 2019 to date.

RANSOMWARE FAMILIES, 2018-2019

GANDCRAB	64%
SIGMA	16%
CRIAKL	7%
HERMES	3%
TROLDESH	3%
GLOBEIMPOSTER	1%
JSDROPPER-PHP	1%
Other	5%

Figure 26: GandCrab was the dominant broadly disseminated ransomware during this 12-month period.

RANSOMWARE FAMILIES, 2017-2018

LOCKY	40%
CERBER	19%
GLOBEIMPOSTER	11%
JAFF	7%
JSDROPPER-PHP	4%
GANDCRAB	3%
SAGE	2%
BTCWARE ALETA	2%
BTCWARE GRYPHON	1%
MOLE	1%
SIGMA	1%
Other	9%

Figure 27: Locky was more prevalent in 2017-2018, within a much more crowded ransomware marketplace.

The total number of ransomware attacks has also dropped substantially. Today, threat actors use ransomware against select targets more likely to pay big bucks. Recent victims include local governments, hospitals, and transportation providers—high-profile organizations that can't afford to be offline.

Why is ransomware flagging? It simply isn't as profitable as in days gone by, especially ransomware-as-a-service operations. Our assessment:

- Technology is doing a better job in preventing ransomware infections
- Law enforcement has improved its ability to track cryptocurrency transactions and disrupt the infrastructure used by ransomware operators
- News has spread that ransom payments often do not result in full decryption

Operators of GandCrab, today's most prominent commoditized ransomware, have learned how costly broadly targeted ransomware operations can be. They must constantly update the malware and its infrastructure to overcome take-downs and disruptions.

And besides, there's an easier way to make money: cryptomining. In greater numbers, threat actors are illicitly placing cryptomining software on unwitting users' computers and mining their processing power for financial gain. If it doesn't hog the processing power, it's hard to identify—a quieter, drama-free way to plunder the unsuspecting.

TIPS TO PROTECT AGAINST PHISHING AND MALWARE

EDUCATE USERS

Train and condition users to spot phishing emails. Faster incident response begins with better human intelligence.

FOCUS EDUCATION ON NEW TTPs

Make sure to educate your SOC team and end users on emerging threats and phishing tactics. Threat actor TTPs are constantly evolving. Complacency can breed painful consequences.

TRAIN USERS TO SPOT CREDENTIAL PHISHING

Pay special attention to phishing scenarios where users are asked to login and supply credentials.

ENABLE MUTLIFACTOR AUTHENTICATION

It's especially urgent if you have single sign-on.

AIM FOR INCIDENT RESPONSE TIMES OF 1 HOUR OR LESS

When users report suspicious emails, the SOC should respond in minutes, not hours or days. Delayed response is a potential bottom-line risk.

EMPOWER YOUR SOC

Equip your SOC to separate email noise from genuine threats, combining automated systems with human expertise.

USE PHISHING-SPECIFIC THREAT INTELLIGENCE

Make sure you ingest threat intelligence specific to phishing threats, and demand timely, high-fidelity reporting

COFENSE CAN HELP

Cofense™, formerly PhishMe®, is the leading provider of human-driven phishing defense solutions world-wide. Cofense delivers a collaborative approach to cybersecurity by enabling organization-wide engagement to active email threats. Our collective defense suite combines timely attack intelligence sourced from employees with best-in-class incident response technologies to stop attacks faster and stay ahead of breaches. Cofense customers include Global 1000 organizations in defense, energy, financial services, healthcare and manufacturing sectors that understand how changing user behavior will improve security, aid incident response and reduce the risk of compromise. To learn more, visit https://cofense.com/

SOURCES

1. Verizon, "Data Breach Investigations Report," 2018.
2. Ibid.
3. Identified SEG providers included Barracuda, BitDefender, Cisco Ironport, CloudMark, Cyren, Fortinet, Kaspersky, Microsoft Exchange Online Protection, Microsoft Advanced Threat Protection, Mimecast, Proofpoint, Symantec Email Security, and Trend Micro.
4. Gartner, "Forecast: Information Security and Risk Management, Worldwide, 2017-2023, 1Q19 Update," 2018.
5. Bitcoin, "Who's Who," 2019.

FURTHER READING

MALWARE DELIVERY TTPS

hTTPs://cofense.com/closer-look-qakbot-malware-dangerous/
hTTPs://cofense.com/unsubscribe-emails-subscribe-loda-rat/
hTTPs://cofense.com/sharing-isnt-caring-phishing-attacks-abusing-file-sharing-sites/
hTTPs://cofense.com/upgrades-delivery-support-infrastructure-revenge-rat-malware-bigger-threat/
hTTPs://cofense.com/emo-qak-geodo-emotet-botnet-delivers-qakbot-malware-first-stage-payload/
hTTPs://cofense.com/phishing-campaigns-manipulating-windows-control-panel-extension-deliver-banking-trojans/
hTTPs://cofense.com/exploiting-unpatched-vulnerability-ave_maria-malware-not-full-grace/
hTTPs://cofense.com/domain-fronting-phishing-attacks-cisos-need-know/
hTTPs://cofense.com/phishing-emails-com-extensions-hitting-finance-departments/
hTTPs://cofense.com/potential-misuse-legitimate-websites-avoid-malware-detection/
hTTPs://cofense.com/microsoft-office-macros-still-leader-malware-delivery/
hTTPs://cofense.com/update-necurs-botnet-banks-second-bite-apple-new-malware-delivery-method/
hTTPs://cofense.com/abusing-microsoft-windows-utilities-deliver-malware-fun-profit/
hTTPs://cofense.com/turning-blind-eye-end-users-nlp-ai-tricked-clever-phishing-techniques-like-zerofont/
hTTPs://cofense.com/azorult-malware-finds-new-ride-recent-stealer-phishing-campaign/
hTTPs://cofense.com/windows-software-abuse-microsoft-excel-query-files-used-deliver-malware/
hTTPs://cofense.com/cofense-covered-office-attachment-attacks-grow/

TRENDS IN OBFUSCATION AND DETECTION EVASION TECHNIQUES

hTTPs://cofense.com/broken-file-hides-malware-designed-break-targets/
hTTPs://cofense.com/emotet-update-new-c2-communication-followed-new-infection-chain/
hTTPs://cofense.com/read-manual-bot-gives-phishing-campaign-promising-future/
hTTPs://cofense.com/closer-look-qakbot-malware-dangerous/
hTTPs://cofense.com/kutaki-malware-bypasses-gateways-steal-users-credentials/
hTTPs://cofense.com/exploiting-unpatched-vulnerability-ave_maria-malware-not-full-grace/
hTTPs://cofense.com/threat-actors-customize-urls-avoid-detection/
hTTPs://cofense.com/recent-geodo-malware-campaigns-feature-heavily-obfuscated-macros/

RECENT TOP MALWARE FAMILIES

EMOTET

hTTPs://cofense.com/flash-update-emotet-gang-distributes-first-japanese-campaign/
hTTPs://cofense.com/emotet-gang-switches-highly-customized-templates-utilizing-stolen-email-content-victims/
hTTPs://cofense.com/emotet-update-new-c2-communication-followed-new-infection-chain/
hTTPs://cofense.com/flash-bulletin-emotet-epoch-1-changes-c2-communication/
hTTPs://cofense.com/closer-look-qakbot-malware-dangerous/
hTTPs://cofense.com/emo-qak-geodo-emotet-botnet-delivers-qakbot-malware-first-stage-payload/
hTTPs://cofense.com/major-us-financial-institutions-imitated-advanced-geodo-emotet-phishing-lures-appear-authentic-containing-proofpoint-url-wrapped-links/
hTTPs://cofense.com/recent-geodo-malware-campaigns-feature-heavily-obfuscated-macros/
hTTPs://cofense.com/twin-trouble-geodo-malware-url-based-campaigns-use-two-url-classes/
hTTPs://cofense.com/dark-realm-shifting-ways-geodo-malware/
hTTPs://cofense.com/geodo-malware-targets-patriots-phishing-attack-eve-american-independence-day-holiday/

CHANITOR

hTTPs://cofense.com/malware-holiday-ends-welcome-back-geodo-chanitor/

RANSOMWARE

hTTPs://cofense.com/phishing-campaign-spoofed-cdc-warning-deliver-latest-gandcrab-ransomware/
hTTPs://cofense.com/2018-reverse-course-ransomware/
hTTPs://cofense.com/staying-king-krab-gandcrab-malware-keeps-step-ahead-network-defenses/

TRICKBOT AND OTHER BANKING TROJANS

hTTPs://cofense.com/beware-payroll-themed-phishing-heres-one-example/
hTTPs://cofense.com/read-manual-bot-gives-phishing-campaign-promising-future/
hTTPs://cofense.com/geodo-trickbot-malware-morph-bigger-threats/
hTTPs://cofense.com/zeus-panda-advanced-banking-trojan-gets-creative-scam-affluent-victims-italy/
hTTPs://cofense.com/trickbot-operators-rapidly-adopt-plug-delivery-possibly-following-dreambots-lead/

CRAFTY PHISHING TECHNIQUES

hTTPs://cofense.com/read-manual-bot-gives-phishing-campaign-promising-future/
hTTPs://cofense.com/tv-license-phishing-scam-tricks-uk-users-giving-personal-information/
hTTPs://cofense.com/major-us-financial-institutions-imitated-advanced-geodo-emotet-phishing-lures-appear-authentic-containing-proofpoint-url-wrapped-links/
hTTPs://cofense.com/re-zombie-phish/
hTTPs://cofense.com/potential-misuse-legitimate-websites-avoid-malware-detection/
hTTPs://cofense.com/man-inbox-phishing-attack-highlights-concerning-gap-perimeter-technology-defenses/

CREDENTIAL PHISHING

hTTPs://cofense.com/company-turned-phishing-attack-teachable-moment/
hTTPs://cofense.com/expect-credential-phishing-continue-surging-2019/
hTTPs://cofense.com/kutaki-malware-bypasses-gateways-steal-users-credentials/
hTTPs://cofense.com/threat-actors-seek-credentials-even-reach-url/
hTTPs://cofense.com/cofense-report-reveals-10-percent-user-reported-emails-across-key-industries-malicious-half-tied-credential-phishing/
hTTPs://cofense.com/customer-satisfaction-survey-leads-credential-phishing/

EXTORTION CAMPAIGNS AND BUSINESS EMAIL COMPROMISE (BEC)

hTTPs://cofense.com/hey-know-ive-never-talked-can-send-money-quick/
hTTPs://cofense.com/jigsaw-ransomware-returns-extortion-scam-ploys/
hTTPs://cofense.com/threats-of-terror-pervade-recent-extortion-phishing-campaigns/
hTTPs://cofense.com/fbis-global-business-email-compromise-bec-wire-wire-bust-personal-perspective/