COFENSE™

Q4 2019

MALWARE TRENDS

Strategic Analysis provided by Cofense Intelligence | COFENSE.COM

Q4 2019 Malware Trends

Executive Summary

The fourth quarter of 2019 finds a strong start with a rather dull finish, maintaining the aphorism that "even criminals take a holiday." Q4 2019 demonstrated an overall decrease in malware volume, as Emotet (also known as Geodo) overtook the limelight and threat actors spooled down for the holidays. Kicking off October, the major botnet and banking trojan picked up even more steam in delivering malicious emails. Email reply chain compromises, macro-laden malicious documents, and convincing phishing templates made their way into user inboxes from the infected machines, which closely reflects its historical pattern. Displaying similar techniques from previous campaigns, Emotet sent finance invoices, invited recipients to a Christmas party, and spread TrickBot through its carefully crafted emails. Although limited in distribution, the operators reintroduced link-based templates that direct users to download malicious files.

Other malware families found less footing in proliferation. The information stealer Loki Bot edged out once-abundant Agent Tesla keylogger from its top spot as the most prevalent non-Emotet malware, demonstrating perpetual lead changes between the two. Less-experienced threat actors have likely favored Loki Bot over its competition thanks to easy deployment and low maintenance, enabling more distribution with less effort.

Using macro-enabled documents for malware delivery accounted for a sizeable portion of malware phishing emails, predominantly as part of Emotet campaigns. Unlike Q3 2019, threat actors diminished the use of CVE-2017-11882 to enable further payloads, which typically involves a malicious Rich Text Format (RTF) or Excel Spreadsheet file that downloads or executes another malware such as Loki Bot or HawkEye Keylogger. This decline, to some extent, is a possible result of system upgrades due to Windows 7’s End of Life, better patching awareness, and more preemptive security focus. Globally, Command and Control (C2) servers for malware related to phishing campaigns stood fast, as the United States continued to account for a sizable portion at over 40%. The U.S. grew by 6% while Russia fell by 4% in total C2 distribution. Germany, France, and Great Britain trailed behind in malware delivery or command.

For Q1 2020 and beyond, Cofense Intelligence anticipates several trends in the phishing threat landscape. At the start of the year, Windows 7’s End of Life is likely to spawn new malware variants as organizations struggle with upgrades. Targeted ransomware will probably continue to see an increase, while widespread campaigns remain on a downward trend. Geopolitical events in the physical world may result in more impact within the cyber realm, such as a virtual retaliation for a kinetic strike. Cofense also expects the 2020 U.S. election season to bring forth more phishing directed at candidates, critical systems, and citizens. And finally, Emotet will likely continue to deliver malicious emails and compromise users while steadily evolving.

Cofense Intelligence continually provides phishing campaign updates throughout the year, which include the Flash Alert, Strategic Analysis (a comprehensive threat report), and Executive Phishing Summary (a bi-weekly trend synopsis) communiqués.

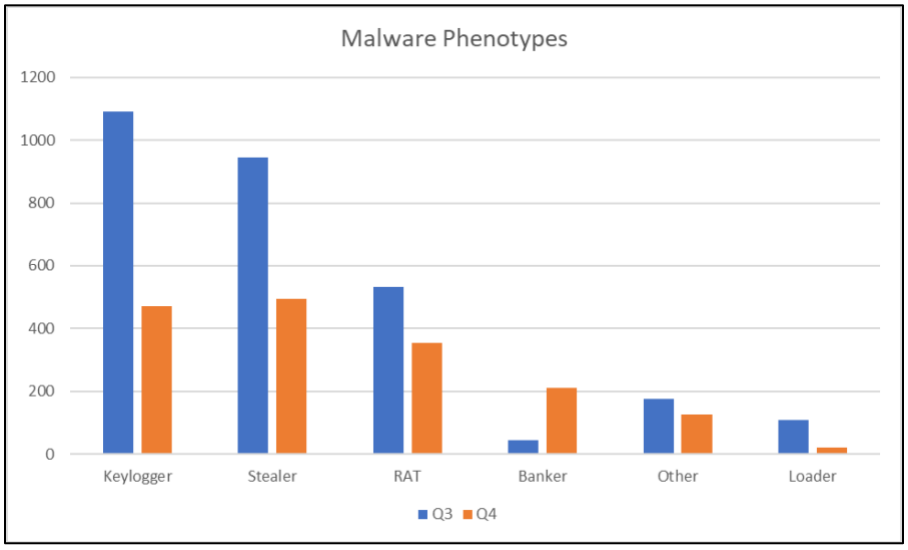
Phenotype Overview

Phenotypes are distinguished by the observable characteristic that consists of the malware's primary function. For example, malware that mainly performs keystroke capturing is labeled as a keylogger. Cofense Intelligence tracks a broad set of malware families, which produces a large data set. Each set is seen in phishing-borne vectors, such as an email attachment or a download via URL enclosed in the email body.

A holistic decrease in the malware volumes of Q4 2019 led to yet another consistent group of participants san one significant player. On the flip side, the behemoth malware and botnet Emotet took over the landscape up until roughly December 20th, when a holiday recess ensued. At the tip of the previous quarter, we reported on the resurgence of phishing kingpin Emotet as it spun up and carried out attacks. Throughout Q4, the botnet continued to spam users with compromised reply-chain emails, malicious attachments, and download links to malware. Ranging in sophistication and theme, Emotet employed various templates to lure users into infecting their machines. It also accounted for a majority of the banker phenotype growth. Other malware phenotypes saw a holistic down trot in their activity.

The decline of widespread ransomware sustained, as actors take up targeted attacks for more sizeable payouts. Cofense Intelligence released an article looking over ransomware headlines and 2020 predictions, which speaks to this trend. Threat actors are likely reducing the spread surface of an attack and making it more specific to the target, which helps circumvent heightened security measures, while potentially seeking out organizations that may have cyber insurance to ensure a paid ransom. Healthcare (a crucial vertical that requires a high degree of information availability) suffers the most from these targeted ransomware attacks, prompting more facilities to pay out the ransom in hopes of returning systems to operational capacity.

The chart below identifies our top 6 malware phenotypes which primarily consist of (but not limited to):



Keylogger: Agent Tesla, FormGrabber, HawkEye, '404 Keylogger'

Stealer: Loki Bot, AZORult, Pony

RAT: NanoCore, Remcos, jRAT, NetWire

Banker: Emotet, TrickBot, Ursnif

Other: Credential Phishing from Attachment

Loader: Shortcut (.LNK) Files, Batch

Figure 1: Q4 (orange) phenotype trends compared with Q3 (blue) 2019

Note: These malware families are either directly delivered via unique phishing campaigns or as a secondary download. The delivery mechanisms noted below are responsible for some of these distributions. For credential phishing, these statistics only focus on emails that contain attachments; the amount of link-based credential phishing emails is far higher.

Delivery Mechanism Rundown

Reflecting on the resurgence of Emotet, Q4 2019 witnessed a shift in delivery mechanisms used to propagate malware in phishing. Macro-enabled documents (labeled OfficeMacro in the chart below) sharply rose, mainly due to Emotet's use of them. On the other hand, the previous heavy lifter CVE-2017-11882 faced a decline, possibly as a result of system upgrades due to Window 7's End of Life in combination with patching awareness campaigns and improvements in preemptive security measures. CVE-2017-11882 sharply increased in early- to mid-2019, quickly overtaking all other delivery mechanisms in popularity. Windows Script Component (WSC) maintained its relatively low profile to round off the top 3 delivery mechanisms seen by Cofense Intelligence in malware-bearing phishing emails.

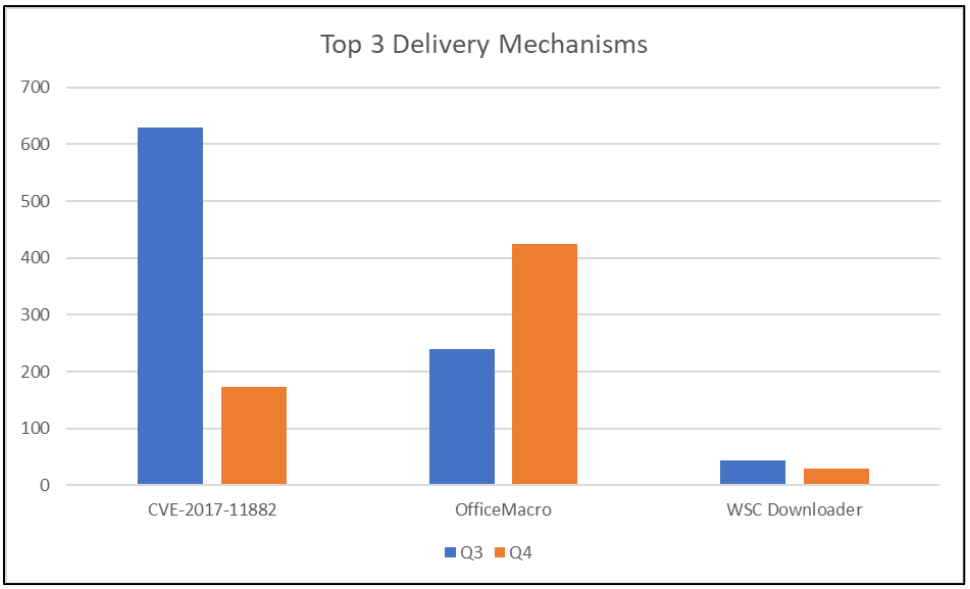


Figure 2: Q4 (orange) delivery mechanisms compared with Q3 (blue) 2019

Organizations continue to struggle against the malevolent use of "trusted" sources and software. Despite awareness and security efforts, macro-enabled documents continue to find their way into users' inboxes. These documents are an initial intrusion vector for several malware families, such as the Emotet trojan itself. Few companies can outright disable macros, as they provide a valuable function in many environments. The Microsoft Office suite offers a warning for each macro-enabled document opened and requires a user to enable content before a macro can come to action. As such, repetitiveness may be met with complacency, resulting in a ritual of merely pressing the "enable content" button without much scrutiny. Training employees to examine the origin of each email and thoroughly inspect a document before acting on the warning banner helps reduce the risk posed by malicious macro-enabled documents.

Command and Control Servers Geolocations

Tracking Command and Control (C2) servers demonstrates a full range of activity across the globe. These nodes can deliver or command malware related to phishing campaigns and often receive information from infected hosts. As with the rest of 2019, the United States accounts for the majority of C2 locations worldwide. In Q4, the U.S. grew by 6% while Russia fell by 4%. The growth of C2 nodes in the United States may be loosely attributed to the resurgence of Emotet, as a sizeable portion of the infrastructure is based in the nation. The Netherlands fell to the sixth spot, dropping off of the top 5 chart shown below, while France rose above Great Britain. Germany maintained its relative profile of 6.33%. Some nations on the African continent have seen a minor escalation of C2 count in malware phishing campaigns, highlighting new regions on the map. Although these statistics do not directly correlate with the infrastructure threat actors use, security teams may see a C2 server (likely as part of a server-hosting farm like AWS or Azure) originating from one of these top nations.

Country	Percentage	Country	Percentage
Q3 2019		Q4 2019	
United States	35.84%	United States	41.77%
Russia	10.15%	Germany	6.33%
Germany	6.57%	Russia	3.10%
Netherlands	4.52%	France	2.99%
Great Britain	3.44%	Great Britain	2.82%

Figure 3: Q3 and Q4 percentages for C2 sources by IP address geolocation.

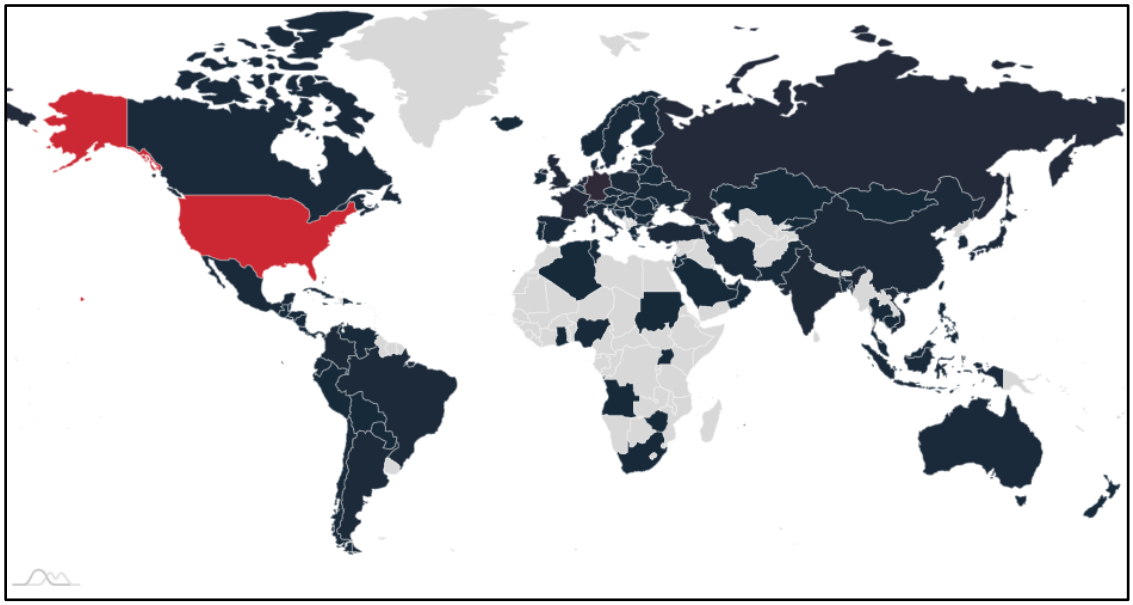


Figure 4: Global heatmap of C2 sources. Darker shades result in more IP addresses, with red being the highest.

REGISTER NOW

SUBMERGE 2020

COFENSE USER CONFERENCE | LONDON | ORLANDO

DIVE INTO THE DETAILS

COFENSE™

Emotet Roundabout

Emotet continues to be front and center in malspam botnets, as demonstrated throughout this review. 2019 saw several changes to their operations, from small changes in the check-in URI structure used to maintain their botnet, to the implementation of the reply-chain tactic. During Q4, Cofense saw the operators utilize a few new custom-created templates. Examples include a Halloween Party, Christmas Party, and even some related to Greta Thunberg. A particularly noteworthy instance during the last week of activity occurred, as we noted an increase in the targeting of U.S. government and military email addresses.

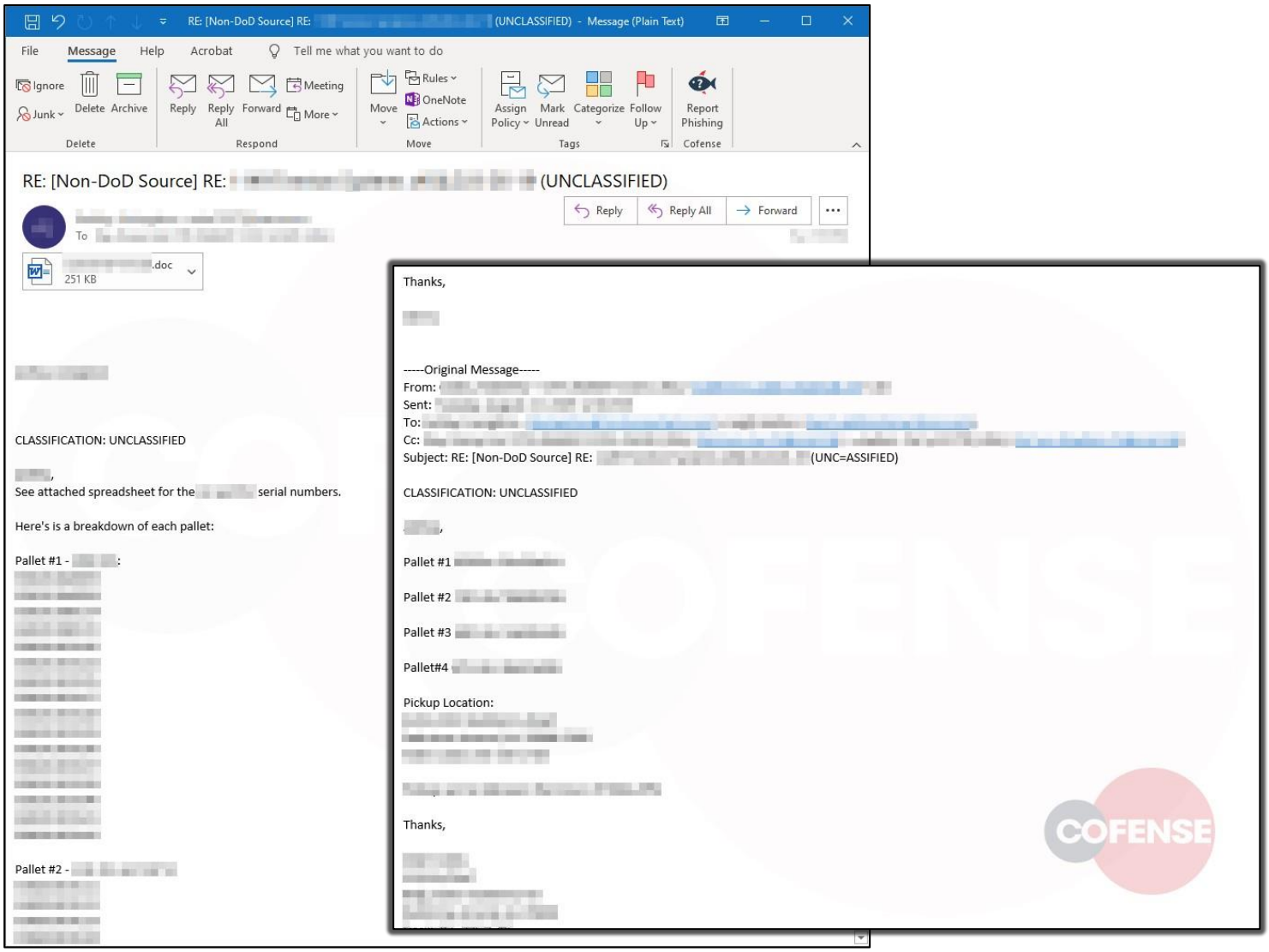


Figure 5: Emotet "trusted" email reply chain compromise in official DoD correspondence.

The threat actors behind Emotet put a lot of time and effort for course corrections to maintain effectiveness, which is reflected by the data points listed below. However, the botnet operators also continue their personal lives, as Emotet took a winter vacation at the end of 2019 on December 20th and returned on January 13th, 2020.

During Q4 2019 alone, Cofense observed the following trends for Emotet:

- The use of over 290,000 unique compromised email addresses to send Emotet malspam.
    - Out of these, 140,000+ unique and new email accounts compromised.
- More than 33,000 unique attachment hashes recorded.
- Over 5,800 unique payload URLs were spotted.
- Emotet delivered malicious emails to approximately 16 million users worldwide.
- Japanese users and companies found the sharpest spike in targeting and compromise, in conjunction with a generalized increase in the targeting of Asian and Middle Eastern countries.

Dutch to Darkness: A Varenyky Story

A highly volatile spambot trojan known as Varenyky—named after a delicious Ukrainian pastry—was reported on by Cofense Intelligence in Q4. Varenyky carried out malicious activity throughout mid- to late-2019, setting off as a French-targeting campaign with a focus on sextortion. While initially limited to France, we noted a shift in December towards Dutch-speaking users that bypassed a FireEye Secure Email Gateway (SEG). This campaign used a financial theme that imitated the Dutch Tax Authority to lure recipients into opening an HTML attachment. Once a recipient of the spambot's email navigates to a link enclosed in the attachment, downloads the archive bearing malicious JavaScript, and opens the file, a sample of Varenyky is dropped onto the machine. Varenyky attempts to record specific activity on the device through keyword searches. A particular set of keyword looks for mentions of explicit content to capture a user navigating adult sites. In turn, this is used for a follow-up sextortion campaign after the C2 server receives this recording. The malware was spotted using freeware tools to exfiltrate credentials as well.

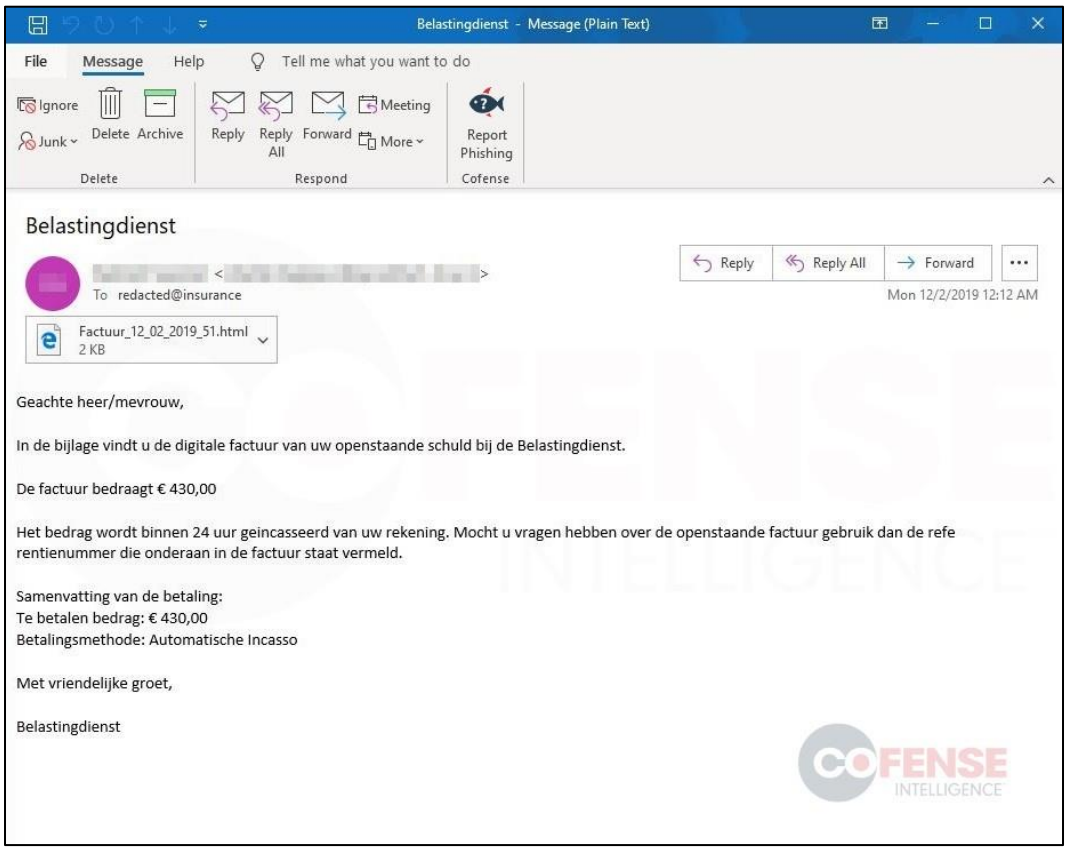


Figure 6: Varenyky spambot impersonating the Dutch Tax Authority in a nefarious email.

404 Keylogger Finds A Foothold

Towards the end of Q3 2019, Phoenix and Alpha Keylogger became progressively popular. These two keyloggers were practically indistinguishable from each other, overlapping in their offerings and features. Midway through the fourth quarter, 404 Keylogger gained even more traction amongst threat actors. The 404 Keylogger suite provided many of the same services and functions as both Phoenix and Alpha Keylogger, as well as some of the capabilities of the prolific Agent Tesla keylogger. Specifically, 404 Keylogger was able to use similar evasion mechanisms as Agent Tesla, perform some basic anti-analysis techniques, and check the geolocation of the infected computer. Later versions of 404 Keylogger became almost homogenous with Agent Tesla before data exfiltration takes place, but it did introduce the ability to exfiltrate logs via Pastebin. Although both keyloggers are nearly undifferentiated before and after system logs are sent, a brief window of time during the log exfiltration process reveals a set of strings unique to 404 Keylogger.

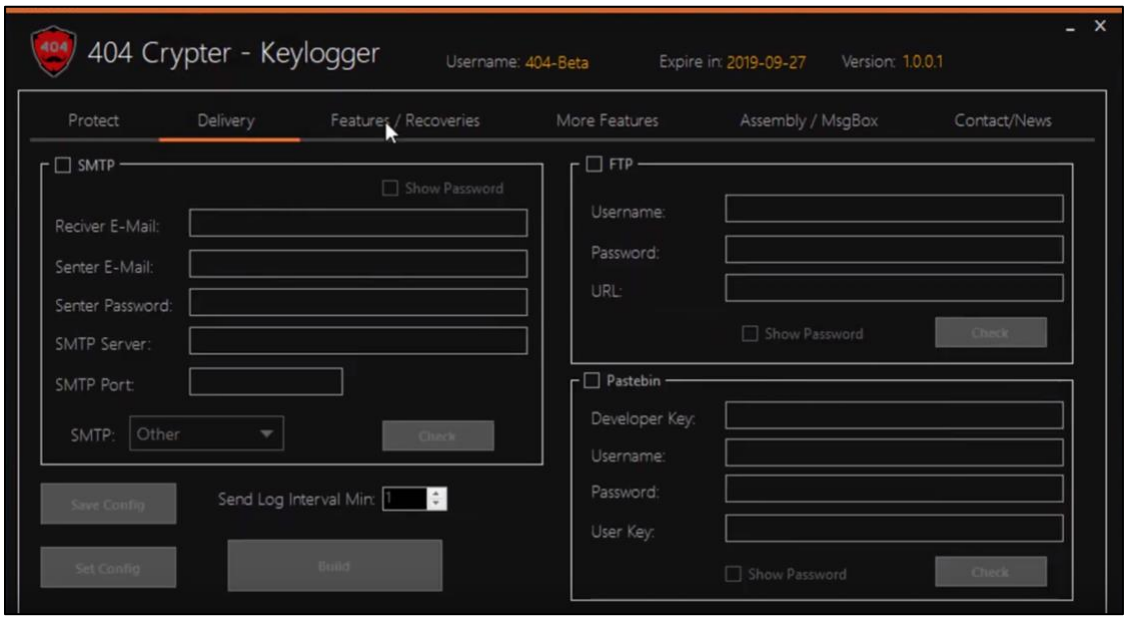


Figure 7: A screenshot of 404 Crypter, the interface used to deploy 404 Keylogger.

Given that 404 Keylogger has several advantages over Agent Tesla—such as having an active development by a dedicated, individual team—it is likely that the most significant factor sustaining Agent Tesla's popularity is its long-term name recognition and underground fame. Agent Tesla remained the keylogger of choice for Q4, as it did in Q3, but not without an overall decrease in the number of unique campaigns. If this downward trend continues, different competing keyloggers may overtake Agent Tesla in terms of frequent deployment. Cofense Intelligence anticipates the likes of 404 Keylogger, HawkEye Reborn, FormGrabber, and other keyloggers to increase in their use throughout 2020.

Italian Language Campaign Uses FTCode Ransomware and Jasper Loader

In early Q4 2019, an Italian language campaign targeted Italian insurance and legal companies via phishing that bypassed FireEye Secure Email Gateways (SEGs). Primarily claiming to be secure correspondence, or "Posta Elettronica Certificata," the emails were delivered with embedded links that lure users into downloading malicious files. When opened, these links obtained .zip archives that contained .vbs scripts. The scripts retrieved and displayed distracting images to the user, such as a map of the toll roads in Italy. Afterward, the .vbs script downloaded several PowerShell files that contain Jasper Loader, which then retrieves FTCode Ransomware.

FTCode Ransomware gathers basic information about infected systems, exfiltrates it to a Command and Control server, generates a unique encryption key, and then encrypts certain file types based on the extension. These included finance-related files (.ibank and .tax), office documents, and certificate files (.crt and .der). FTCode Ransomware itself is not notably more effective than other ransomware. However, its relatively small profile and minimal complexity harken back to older PowerShell ransomware variants and stand out amongst the current executable-focused ransomware market. Conversely, the initial scripts and Jasper Loader are both obfuscated and advanced. In some cases, it has even downloaded and played music to distract users from identifying the threat. This pattern of behavior indicates a higher skill level on the part of the threat actor as well as an awareness of the intended target.

All your files was encrypted!

Yes, You can Decrypt Files Encrypted!!!

Your personal ID: **redacted**

1. Download Tor browser - https://www.torproject.org/download/

2. Install Tor browser

3. Open Tor Browser

4. Open link in TOR browser: **http://qvo5sd7p5yazwbrgioky7rdu4vslxrcaeruhjr7ztn3t2pihp56ewlqd.onion/?guid=redacted**

5. Follow the instructions on this page

***** Warning*****

Do not rename files

Do not try to back your data using third-party software, it may cause permanent data loss(If you do not believe us, and still try to - make copies of all files so that we can help you if third-party s oftware harms them)

As evidence, we can for free back one file

Decoders of other users is not suitable to back your files - encryption key is created on your computer when the program is launched - it is unique.

Figure 8: FTCode Ransomware message displayed after a successful infection.

Forecast for Q1 2020 and Beyond

The year of 2020 may bring about a new vision for threat actors. As network defenders adapt to longstanding tactics, upgrade older systems, and reinforce email security, cybercriminals will need to seek out new ways to infiltrate an organization. Yet, certain patterns are likely to continue and expand. Windows 7's End of Life will likely bring about more exploits, and targeted ransomware increases. While widespread ransomware declines, cyber activity may reflect geopolitical events, the 2020 U.S. elections will probably lead to more phishing, and Emotet is expected to keep progressing.

Windows 7 End of Life Can Signify Creation of New Malware

Coming to an end is the enterprise-favorite Windows 7. Judging by how long it took (and still is taking) some organizations to transition from Windows XP, this operating system may linger well after its End of Life. Despite a free upgrade to Windows 10 in stock at the time of this writing, users and administrators are finding it difficult to break away from Windows 7. Cybercriminals can capitalize on the lack of patching to develop exploits, leading to intrusions in networks with deficient safeguards. The phishing threat landscape will likely reflect this effort as threat actors use the tried-and-true method of engineered emails to propagate malware.

Targeted Ransomware Continues to Increase

Cofense Intelligence reported on the impact of ransomware throughout 2019 and predictions going forth for 2020. We found that ransomware has taken up global headlines, painting a picture that the average reader may attribute to growth in widespread infections. From a broad phishing perspective, ransomware has lessened in general proliferation. Targeted ransomware is on the up-and-up, as profitability from these attacks rises and actors find success in their efforts. Organizations impacted by or at a high risk of ransomware are likely to opt for cyber insurance, as are proactive companies that want to lessen the burden of paying a ransom out of pocket. More cybersecurity firms may act as a third-party negotiator for these payments, and likewise, businesses will probably increase their budget to obtain premium packages.

Geopolitical Events Potentially Result in Cyber Threats

In several cases, events in the real world reflected in the cyber realm. Whether it is a physical attack followed by a virtual response or a spammer capitalizing on a protest to lure unsuspecting users into downloading malware, geopolitics play a role in technology. In mid-2019, the United States reportedly carried out a targeted cyber-attack that disrupted intelligence operations and weapon systems in response to Iranian forces downing a surveillance drone and earlier action on oil tankers. This alleged virtual response to a kinetic action indicated that cyberwarfare is rapidly escalating. Cybercriminals and scammers also use real-life events in their day-to-day; Cofense Intelligence previously reported on the use of weaponized archive file attachments in Brazilian elections lure emails. In 2020, we anticipate further use of geopolitical events to fuel phishing and targeted cyber-attacks. Nations are likely to continue moving away from expanding physical resources into virtual conflicts.

Election Season May Bring About More Phishing

2020 in the United States brings forth a new election cycle. Presidential campaigns are at the highest risk for interference by foreign powers, as reportedly seen in the 2016 elections. The upcoming election cycle is likely to be no different, as cybercriminals and state-sponsored threat actors seek to gain entry into voting systems, email services, and social media accounts. Phishing is a capable vector of intrusion into critical systems and servers, enabling attackers to reach sensitive data or essential functions for nefarious purposes. It can also be used to

sway the opinions of voters, create disinformation, and disrupt county systems to prevent voting entirely. Cofense Intelligence expects to see campaigns that target elections or use it thematically to spread malware.

Emotet Keeps Growing

Cofense Intelligence notes that the holiday lull of Emotet—effective from approximately December 20th to January 13th—will lead to little immediate change in the malware or botnet itself. However, their TTPs are likely to shift, demonstrating different templates, additional "second stage" payloads dropping after initial infection, and possibly new delivery mechanisms. The operators will continue to proliferate Emotet, spreading it to as many machines as possible while harvesting emails and compromising reply chains. Cofense tracks the activity of Emotet vigorously, reporting on and helping defend against it.

ABOUT COFENSE

Cofense is uniting humanity against phishing. Every day phishing attacks evade perimeter defenses, including secure email gateways, to reach employee inboxes. Cofense gives incident responders the tools they need to analyze, identify, and stop attacks in minutes, while conditioning employees to recognize and report phishing threats, thereby turning soft targets into active human sensors. By combining human intelligence and advanced technology, our solutions enable organizations to prevent breaches, loss of funds, data theft, and reputational damage. No one delivers a more complete, end-to-end phishing defense. Cofense has thousands of enterprise customers worldwide, spanning every major vertical including defense, energy, financial services, healthcare, retail, and manufacturing. Learn more at https://cofense.com