COFENSE™

Q3 2019

MALWARE TRENDS

Strategic Analysis provided by Cofense Intelligence | COFENSE.COM

Q3 2019 Malware Trends

Executive Summary

Throughout the summer, malware seen in the phishing landscape has demonstrated a shift from predominantly information stealers (such as Loki Bot) to keyloggers (namely Agent Tesla). Overall, threat actors were relatively quiet in Q3 2019. The most significant player on the block—Emotet—resurfaced towards the end of the quarter and wasted no time in compromising email chains or tricking users with convincing templates. Additionally, threat actors continued to capitalize on CVE-2017-11882 to deliver malware, with malicious Microsoft Office macros and Windows Script Component (WSC) downloaders rounding off the trending delivery mechanisms. The United States found a sizeable portion of Command and Control (C2) servers hosted within its borders, with Russia, Germany, Netherlands, and Great Britain trailing behind.

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

Phenotype Overview

While new variants of malware surface daily, the key participants remain somewhat consistent. Q3 saw no major break from this trend. In Q2 2019, information-stealing malware maintained its lead in propagation, outpacing the "competition" as it did in Q1. Agent Tesla, a keylogger for sale on underground forums, leaped ahead in Q3 to overtake the other phenotypes. This surge is likely due to the ease of use that Agent Tesla provides through a consumer web interface, coupled with support from the authors on the messaging app Discord. Furthermore, phishing-delivered Ransomware-as-a-Service (RaaS) has greatly decreased, as these ransomware families have largely discontinued while more targeted ransomware campaigns have spiked. The most prevalent RaaS suite, GandCrab, was taken offline by its creators, significantly lowering the amount of malicious spam emails that contain ransomware attachments. Sodinokibi, a ransomware that shows possible codebase overlap with GandCrab, has seen a very low rate of dissemination. Similarly, the lull of Emotet demonstrated a drop in widespread ransomware. In turn, threat actors have taken to more targeted ransomware attacks, opting to keep a lower profile with a higher return ratio by aiming at high availability systems such as those found in healthcare, transportation and local government services.

Cofense Intelligence tracks a broad set of malware families, which presents a large data set. In the chart below, our top malware phenotype hits primarily consist of (in order of magnitude from left to right):

- Keylogger – Agent Tesla, HawkEye, FormGrabber
- Stealer – Loki Bot, AZORult, Pony
- RAT – NanoCore, Remcos
- Other – Credential Phishing with Malware
- Loader – Shortcut (.LNK) Files, Batch Scripting

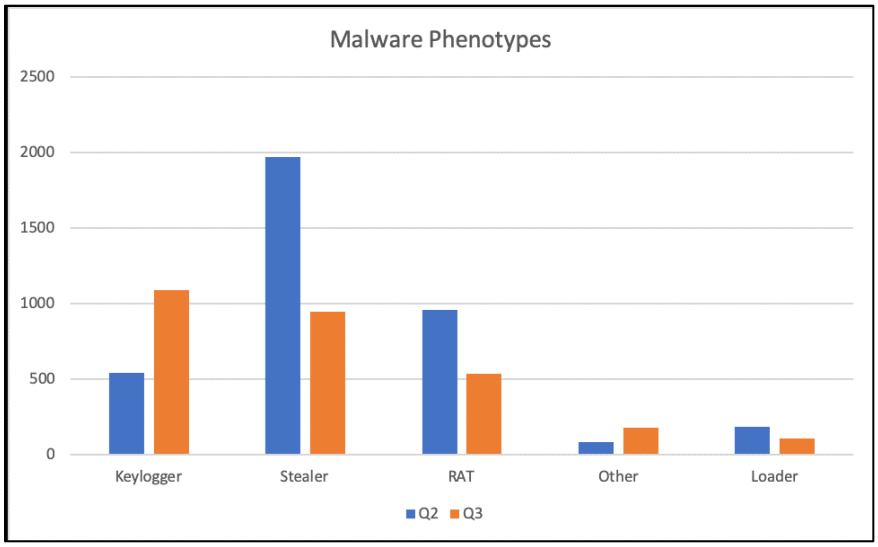

Figure 1: Q3 phenotype trends compared with Q2 2019

Note that these are malware families delivered via phishing emails, and often seen as a 'stage two' download from the top delivery mechanisms outlined below. For credential phishing, these statistics only focus on emails that contain malicious attachments; the amount of "non-malware" credential phishing is far higher.

Delivery Mechanism Rundown

Throughout Q2 and Q3, there was little change to the significant delivery mechanisms used for malware propagation. The top 3 ‘stage one’ delivery methods exhibited in phishing are CVE-2017-11882, Office macros, and Windows Script Component (WSC) downloaders.

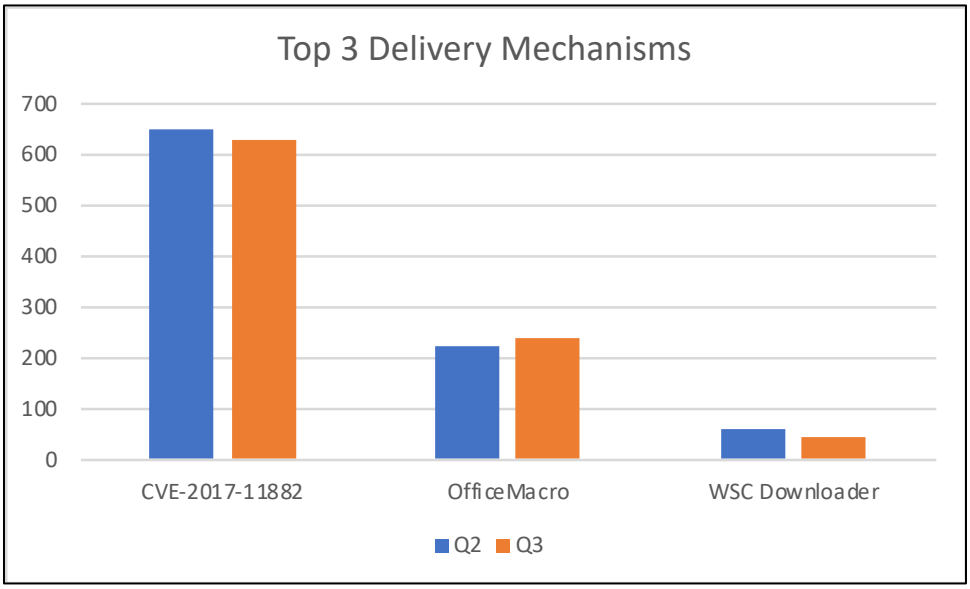

Figure 2: Top 3 delivery mechanisms observed in phishing

The consistent use of the same top 3 delivery mechanisms across Q2 and Q3 is indicative of the relatively steady state maintained during the absence of Emotet and is likely to become more volatile as the holidays approach. As far as methods go, CVE-2017-11882 (the abused-although-patched Equation Editor vulnerability) remains a prolific technique for threat actors to spread malware through phishing. The vulnerability is exploited using Microsoft Office attachments, which can range from Excel spreadsheets to Word documents to Rich Text Format (RTF) files. When a victim accesses a rigged document, the exploit triggers on the machine, generally downloading a ‘stage two’ malware.

Your business runs on email.
Unfortunately, **so does his.**

WE CAN HELP

COFENSE

UNITING HUMANITY
AGAINST PHISHING

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 and often receive information from infected hosts. The United States dramatically outweighs the rest of the world. Russia accounts for a sizeable portion of the nodes, while Germany, Netherlands, and Great Britain trail behind. 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) originating from one of these nations.

Country	Percentage	Country	Percentage
Q3 2019		Q2 2019	
United States	35.84%	United States	36.35%
Russia	10.15%	Germany	5.53%
Germany	6.57%	Russia	5.30%
Netherlands	4.52%	Netherlands	3.75%
Great Britain	3.44%	Great Britain	3.58%

Figure 3: Q3 and Q2 percentages for C2 sources by IP geolocation

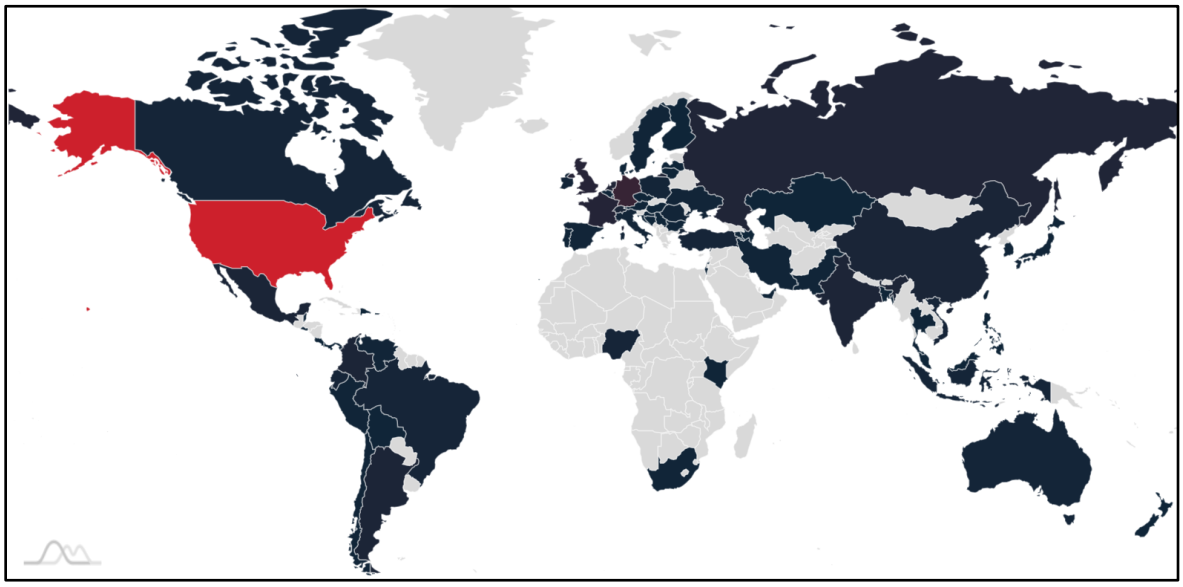

Figure 4: C2 sources global heatmap.

Emotet's Impact on the Phishing Landscape

A once-predominant force in the phishing realm, Emotet (also known as Geodo) went quiet for most of 2019. Q2 2019 saw a vacuum that was never fully occupied by any competing malware families. When the botnet increased activity in mid-September, the end of Q3 saw an immediate ramp-up in malware activity. Not one to miss out on an opportunity, Emotet quickly took advantage of trends such as Edward Snowden's book and the tax season in Australia, adding the themes to its ever-growing repertoire. In the case of the tax season in Australia, Emotet has recently begun spoofing the Australian Taxation Office to deliver phishing emails with malicious attachments to email accounts with the .au top-level domain (shown in Figure 5).

Cofense Intelligence asses that Emotet will further ramp up the volume and sophistication—or at least the frequency of impersonation—of its campaigns leading up to the holidays, but will likely go inactive during the actual holidays. In particular, as previously noted by Cofense, the threat actors seem to take leave on Russian Orthodox Christmas before resuming normal operations sometime afterward. Cofense Intelligence expects Q4 to see the full effect of Emotet.

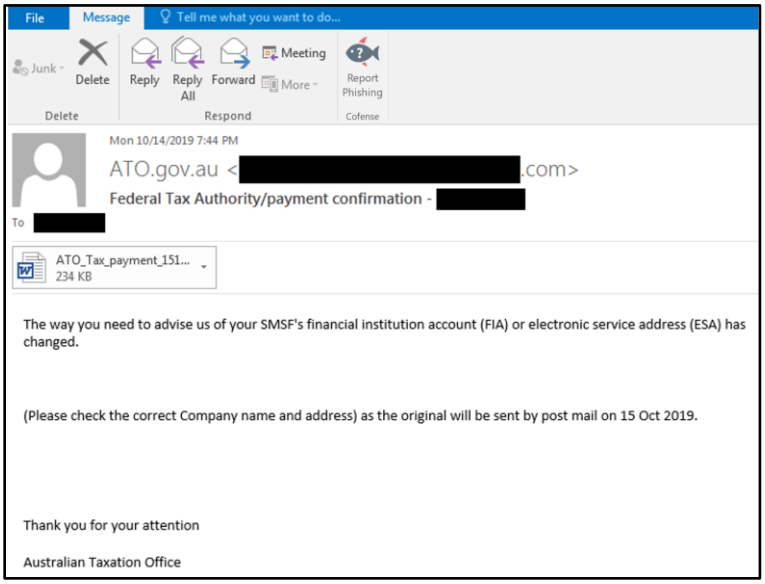

Figure 5: Emotet phishing email sample targeting Australians through ATO impersonation.

HTML Attachments Popularity Heightens

Attackers often include HTML files in phishing emails as a way to circumvent gateway protections. Some organizations do not block HTML attachments automatically, making the rather inconspicuous webpage file a perfect vessel for credential phishing "pages" or as the first stage in a chain of attack. When serving as a credential phishing page, HTML files can exfiltrate entered credentials without having to visit a web site, which serves to avoid some software. When acting as a downloader, opening the HTML page causes it to refresh (much like a normal redirect page would) and automatically proceed to download another file or request that the victim follow another link to acquire the file.

By using these methods, threat actors can avoid some of the pitfalls associated with hosting multiple external resources in addition to circumventing some protections. As such, the amount of HTML attachments in phishing emails have risen in Q3, which Cofense Intelligence expects to continue increasing in Q4.

Forecast for the Fourth Quarter

Cofense Intelligence expects to see an uptick in malware activity—largely driven by the resurgence of Emotet—up until the holiday lull. Threat actors will continue to abuse legitimate business operational software (like Microsoft Office products) while also taking advantage of unpatched and legacy operating systems. However, to ensure their success in phishing campaigns, threat actors will almost certainly progress their Tactics, Techniques, and Procedures (TTPs). New phishing templates, malware variants, and delivery mechanisms will find their way to organizations and individuals. As threat actor TTPs continue to evolve, innovation for security solutions will need to grow in the same way.