Q3 2022

Cofense Phishing Intelligence Trends Review

Executive Summary

The phishing threat landscape never stops transforming itself, and Q3 2022 has been another illustration of this. Emotet, despite changing tactics back to using macro laden Office documents for its delivery mechanism, drastically decreased in volume and then ceased activity in early Q3. However, because of the change in tactics by Emotet (even for a short period), macro laden Office documents became the top delivery mechanism for this quarter. All the top malware families from last quarter have found a place among the top families this quarter, although there was an overall increase in volume for Keyloggers and Remote Access Trojans. QakBot is the top malware family reaching enterprise users, which has led to a spike in volume for the banker malware type starting in late Q3.

In our strategic analyses during Q3, Cofense investigated both new and long-standing phishing trends. We delineated threat actors' abuse of legitimate services such as Dropbox, DocuSign, and other legitimate and trusted domain names in order to ensure that malicious emails would reach inboxes. We investigated a long-standing activity set, which we first reported in 2019, outlining its evolution over time as it targeted government contractors. We also sought to provide readers with a broad, introductory understanding of malware types in the phishing threat landscape, as well as baseline reports on specific malware families, such as Snake Keylogger. In addition to providing these baseline reports, Cofense also gave readers an insight into the continuation of the improving services through the Intelligence product update report.

In our Q2 Trends Review, Cofense Intelligence identified QakBot as the malware family to watch during Q3, and QakBot has not disappointed. Despite not showing high on the charts in terms of overall volume across the quarter, a few significant developments and new, successful TTPs have given QakBot the limelight again at the tail end of Q3. QakBot is still our Malware Family to Watch for the foreseeable future, and each of our projections for Q4 touch on QakBot developments to some extent.

Overall Activity

Once again, the overall observed malware-delivery activity decreased significantly over the course of the quarter, largely due to Emotet volume dropping off completely in mid-July. The volume for Q3 remained steady after July's drop.

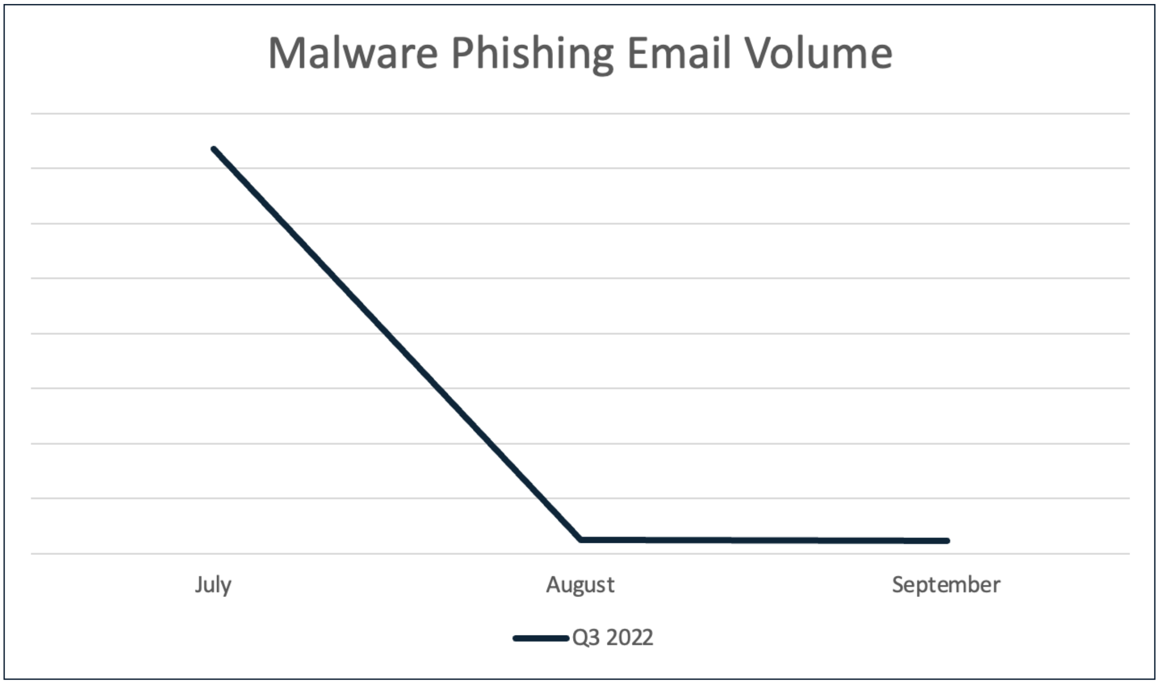

Figure 1: Volume of phishing emails delivering malware in Q3 2022.

Prevalent Malware in Q3

Each of the five most common malware types and the top families for each type from Q2 found a place on the charts in Q3, although the order of the malware types differed slightly due to changes in volume. Notably, there was an increase in position for Keyloggers and Remote Access Trojans.

TOP FIVE MALWARE TYPES	TOP FAMILY IN TYPE
Loader	Emotet/Geodo
Keylogger	Agent Tesla
Information Stealer	FormBook
Remote Access Trojan	Remcos RAT
Banker	QakBot

Table 1: Top five malware types with the top family of each type.

The continued position of Emotet (and consequently Loaders) at the top of the list is a testament to its extreme outscaling of all other malware-delivery campaigns, even as it decreased in July. The chart in Figure 2 has been capped to show distinguishable volumes of other phishing activity.

Keyloggers saw the largest increase in volume between Q2 and Q3, with malware families like Agent Tesla and Snake Keylogger both being popular in the phishing threat landscape. The Remote Access Trojans (RATs) malware type passed Banker types due to a lower volume of QakBot phishing emails during a large portion of the quarter. However, the Banker malware type threatens to increase significantly and overtake other malware types, with the return of QakBot in late Q3. Remcos RAT continues to be the top RAT, followed by NanoCore RAT.

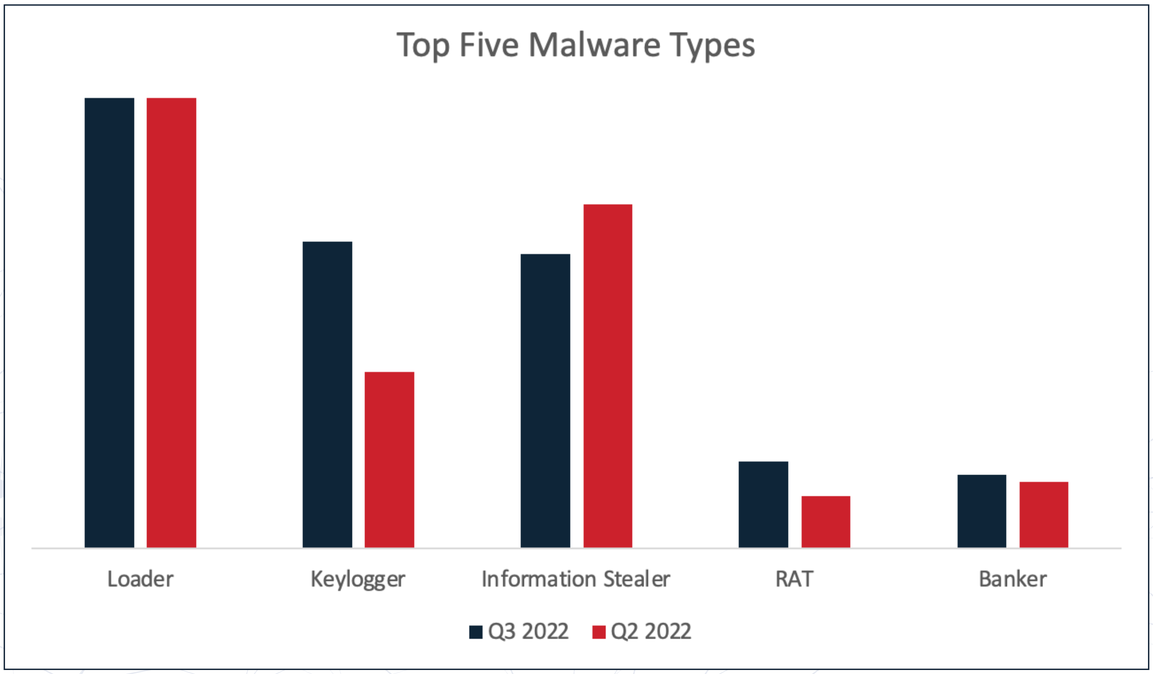

Figure 2: Top five malware types in Q3 2022 and Q2 2022, by volume of emails.

Delivery Mechanism Rundown

OfficeMacros have become the top delivery mechanism, overtaking LNK Downloaders as malware families like Emotet dropped the delivery type. However, the volume for Office macros has not been consistent across the quarter, as it decreased significantly with the cessation of Emotet activity. With the removal of LNK downloaders from the Top Malware Delivery Mechanisms chart, malicious HTML files increased significantly in volume, overtaking both DotNETLoader and the CVE-2017-11882 vulnerability. This is due to QakBot returning in late Q3, utilizing malicious HTML attachments to deliver the malicious payload. The volumes for the DotNETLoader and CVE-2017-11882 delivery mechanisms appear minute when compared to that of Emotet delivery using OfficeMacro, or even QakBot via malicious HTML, but still pose a credible threat. Other noteworthy delivery mechanisms seen delivering malware in Q3 are DBatLoader, and PDF droppers.

The top delivery mechanism for this quarter is once again heavily influenced by Emotet volume (despite its short period of operation), and the chart shown in Figure 3 has accordingly been capped, to make other mechanisms perceptible.

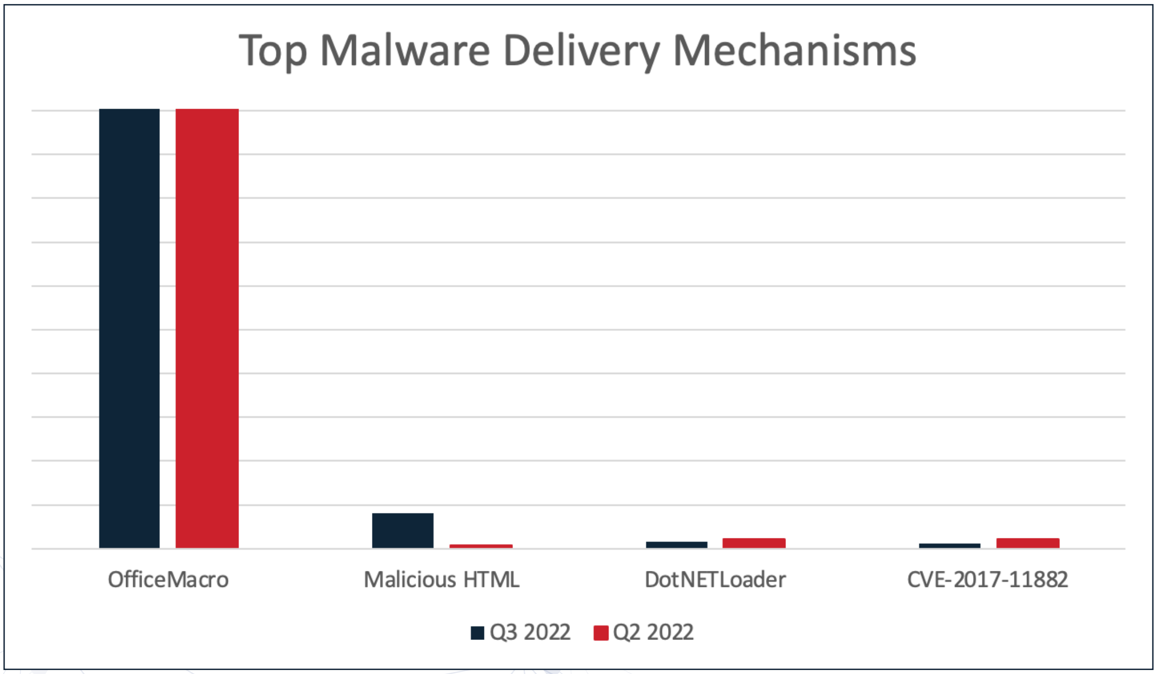

Figure 3: Top Malware Delivery Mechanisms by Email Volume in Q3 2022 and Q2 2022.

TLDs and Domains Used in Credential Phishing

For Q3 2022, Cofense Intelligence analyzed URLs used in credential phishing emails that reached users in environments protected by SEGs, to identify the top-level domains (TLDs) and domains that were most prominent. The URLs analyzed are split into two categories: Stage 1 and Stage 2. Stage 1 URLs are embedded in the phishing emails and are the first step in the infection chain, whereas Stage 2 URLs can only be reached if the user acts with the embedded URL.

When both stages are combined, the volumes associated with most TLDs are largely comparable between Q2 and Q3, although some changed significantly, and a new TLD joined the list. Domains using the .com TLD accounted for approximately 53% of the total, a slight decrease from Q2. The .net TLD increased once again, now amounting to 9.60% of the total. Other notable TLDs that were also top 10 for Q3 are .com.br, .org, .io, .co, .page, .xyz. .in, and .me. The only new addition for this quarter was the. page TLD.

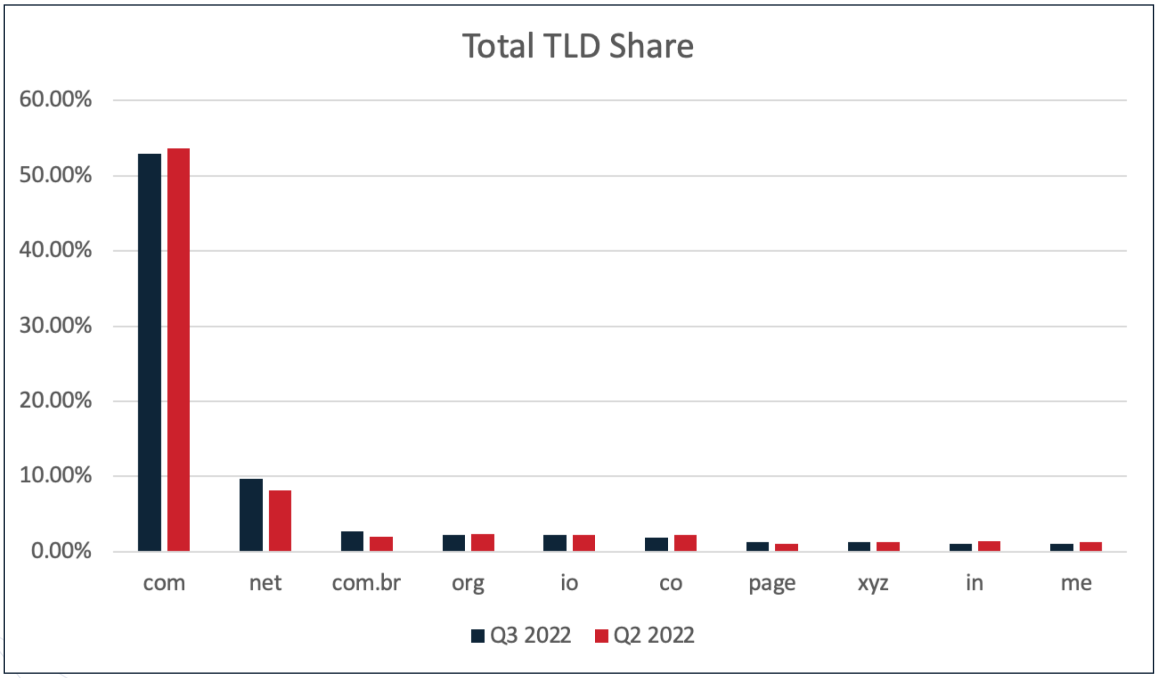

Figure 4: Top 10 TLDs in Q3 2022 compared with Q2 2022.

TLDs and Domains Used in Credential Phishing

The majority of top 10 TLDs for Stage 1 URLs remained consistent with those of Q2, although two of the top 10 were eclipsed. The TLDs .site, and .ly are now top 10 Stage 1 TLDs, replacing .ms, and .app from Q2. The differences among all Q3 TLDs are negligible, ranging from a fraction of a percent to near 2% positive and negative delta.

COM	Q3 2022
net	54.85%
io	10.96%
com.br	2.65%
co	2.49%
org	1.81%
in	1.76%
me	1.19%
site	1.08%
ly	0.95%
me	0.92%

Table 2: Stage 1 TLDs in credential phishing during Q3 2022

The top 10 Stage 2 TLDs for this quarter saw multiple changes outside of the top three. The top three Stage 2 TLDs remain mostly consistent with the largest change being the volume of .me domains decreasing dropping off the list and .org taking its place. The number of URLs with the .co.uk, .online, and .live TLDs increased this quarter, replacing .app, .io, and .ru for this chart.

STAGE 2 TLD	Q3 2022
com	45.60%
net	4.70%
org	4.04%
xyz	3.87%
com.br	3.53%
page	3.01%
online	2.95%
co	2.35%
live	1.29%
co.uk	1.26%

Table 3: Stage 2 TLDs in credential phishing during Q3 2022.

TLDs and Domains Used in Credential Phishing

The 10 most common .com domains used in both stages combined are represented below. Of the domains, several trusted cloud platforms can be identified, showing a continued use for credential phishing threat actors.

- Adobe
- Google
- Sharepoint
- Evernote
- Amazonaws
- Myportfolio
- Canva
- Petanitest
- Axshare
- clickfunnels

Compared to the previous quarter, the top 10 most common .com domains had multiple changes. Adobe.com remains the top spot for this quarter, while the Sharepoint, Evernote, and Canva .com domains increased in volume. The Amazonaws, Petanitest, Axshare, and Clickfunnels .com domains replaced Backblazeb2, Weebly, Live, and Digitaloceanspaces .com domains. Myportfolio.com remained on the list, although it has decreased in volume.

File Extensions of Attachments

The chart below represents the distribution of filename extensions on email attachments that reached users in SEG-protected environments in Q3. PDF attachments remained the top extension analyzed, and saw another large increase compared to the previous quarter, growing by approximately 7% and now making up over 48%. This continues to be more than the combined percentage of the next two extensions, .html and .htm, which together make up 36%. These file extensions are more commonly associated with credential phishing attacks, and delivery of QakBot in late Q3.

Office files like .docx, .xlsx, and .doc continue to be top 10 file extensions on phishing email attachments. These files are used for a variety of purposes such as delivering credential phishing, malicious Office macros, and exploit vulnerabilities. Notably, the .xls and .lz extensions disappeared from the Top 10, being replaced by .shtml and .rpmsg, while several other extensions switched positions due to changes in volume.

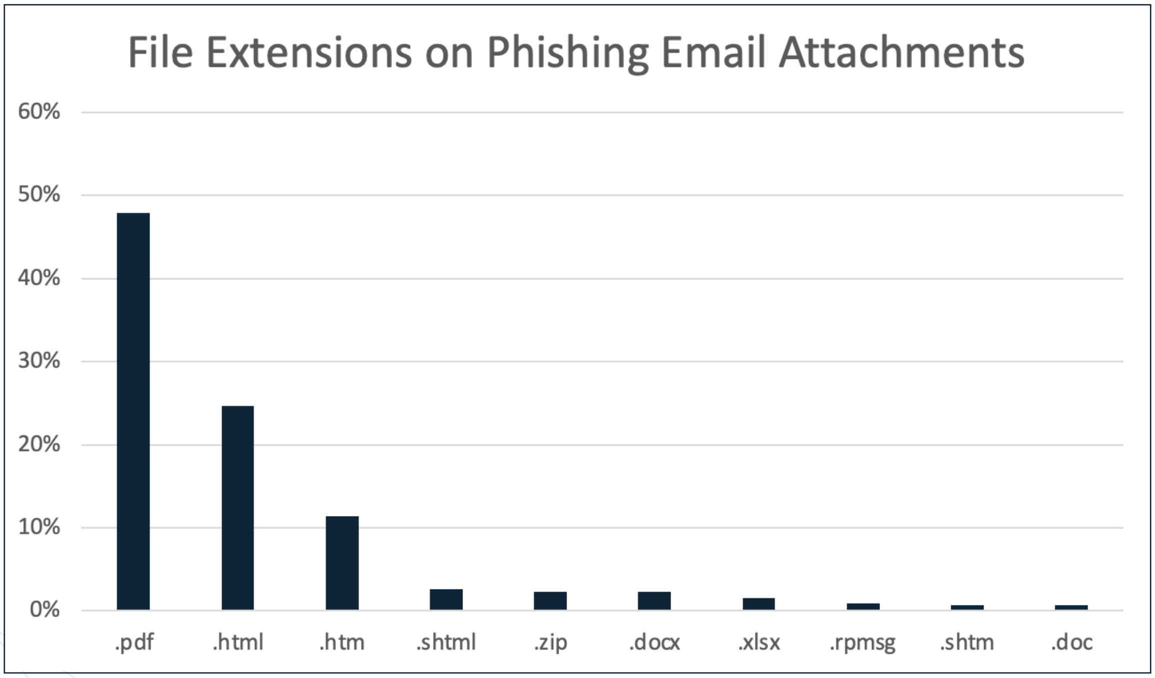

Figure 5: Top 10 most common attachment file extensions found in environments protected by SEGs.

Command and Control Server Locations

Tracking Command and Control (C2) servers provides insight into a range of malicious cyber activities across the globe. These C2 nodes can deliver phishing campaigns or command malware, and often receive information and exfiltrated data from infected hosts. The top five locations for this quarter were very similar to that of Q2, except that servers in Great Britain increased in usage to replace the usage of servers in the Netherlands. The other four countries remained the same and even held similar percentages with a slight increase in usage. These statistics do not directly correlate with the full range of infrastructure threat actors use, and they should only be interpreted as C2 locations, rather than where operations originate.

Q2 2022		Q3 2022	
Country	**Percentage**	**Country**	**Percentage**
United States	59.76%	United States	60.78%
Germany	4.61%	Germany	4.91%
Canada	2.60%	Canada	2.62%
Hong Kong	2.31%	Hong Kong	2.60%
Netherlands	2.08%	Great Britain	2.12%

Table 4: Q2 2022 and Q3 2022 percentages for C2 sources by IP address geolocation.

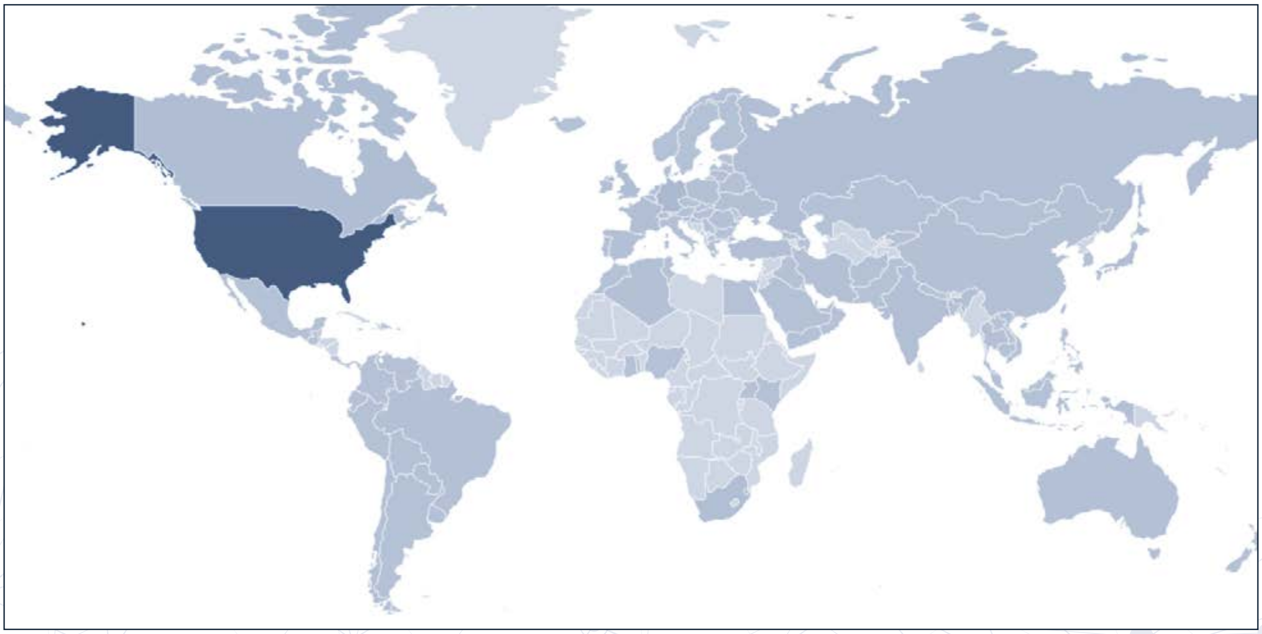

Figure 6: Global heatmap of C2 sources. Darker shades reflect more IP addresses.

Finished Intelligence: Topics and Trends

Throughout Q3 2022, Cofense Intelligence performed in-depth analysis on various threats to provide you with a strategic understanding of the phishing threat landscape and notify you of sudden or upcoming developments. Below, we summarize finished intelligence reports and flash alerts that Cofense Intelligence produced on notable topics and trends identified during this period. Along with these, Cofense Intelligence customers will also find a brief overview of the highlights among Cofense Intelligence **product updates for the first half of 2022!**

The Tactics of a Prolific Phishing Campaign Abusing Dropbox

During August and September of 2022, Cofense has observed an effective credential phishing campaign abusing Dropbox and reaching end users across many industries. The threat actor(s) behind the campaign have put in a considerable amount of effort to increase the chances of successfully stealing the email login credentials of enterprise users. By utilizing various tactics, techniques, and procedures (TTPs), the phishing emails have been very successful at reaching inboxes. These phishing emails reached inboxes in August at a volume far outscaling any other campaign that Cofense has seen effectively abuse Dropbox this year. However, monthly volume from this phishing campaign has been inconsistent, dropping drastically from August to September.

Credential Phishing Targeting Government Contractors Evolves Over Time

Threat actors are running a series of campaigns spoofing several departments of the United States government. The emails claim to request bids for government projects but lead victims to credential phishing pages instead. These campaigns have been ongoing since at least mid-2019 and were first covered in our Flash Alert in July 2019. These advanced campaigns are well crafted, have been seen in environments protected by secure email gateways (SEGs), are very convincing, and appear to be targeted. They have evolved over time by improving the email contents, the PDF contents, and the appearance and behavior of the credential phishing pages.

Snake Keylogger - Phishing Malware Baseline

Snake Keylogger, a staple in the phishing threat landscape throughout 2021 and 2022, is a keylogger written in .NET. It can monitor a user's keystrokes, scan applications to steal saved credentials, and exfiltrate this data through a variety of protocols. Although it is not as popular as other malware families such as FormBook or Agent Tesla, it does maintain a significant presence, and its usage is increasing. In this report, we take an in-depth look at Snake Keylogger, including background information, Snake Keylogger's capabilities, its behavior observed in the wild, and some characteristics that can help with mitigation.

Finished Intelligence: Topics and Trends

Top Domain Names in Evasive Credential Phishing Attacks

A domain name is an essential part of a malicious URL used in a credential phishing attack. Following on our research into the most-used top-level domains (TLDs) in credential phishing threats, we analyzed recent data to look for trends in full domain names. We found that no single domain name appeared in more than a relative handful of campaigns. The only domain names that are both consistently reused by threat actors and consistently reach inboxes are those that belong to legitimate, implicitly trusted services.

DocuSign-Spoofing Campaign Heavily Targets Executives

Cofense Intelligence has identified an ongoing credential phishing campaign that spoofs DocuSign and has bypassed secure email gateways. Through initial collaboration with Cofense Intelligence customers and subsequently with the Cofense Phishing Defense Center (PDC), we determined that the campaign was almost exclusively targeting executive-level employees, primarily CFOs.

An Introduction to Phishing Malware Types

This Cofense Intelligence report is part of a small group of reports that are intended to provide introductory understanding of the phishing threat landscape. With very few exceptions, the malware that Cofense Intelligence finds being delivered through phishing campaigns generally falls into one of the following malware types: Banker, Information Stealer, Keylogger, Loader, Ransomware, and Remote Access Trojan (RAT). These malware types are important to track because they can provide valuable insight into the landscape. For example, Information Stealers becoming more common than Keyloggers in 2021 could provide some indication of a shift in focus on the part of the threat actors. In this report, we explain each of the types, some of the challenges they present, how they apply, and why using them is valuable.

Projections for Q4 2022 and Beyond

Qakbot Still the Malware Family to Watch, with Version 5 and New Tricks.

Qakbot continues to be the top malware family seen in phishing emails reported to the Cofense Phishing Defense Center from users in environments protected by SEGs. The success rate of the phishing emails reaching enterprise inboxes can be attributed to the use of hijacked email threads and embedded URLs, among other TTPs that are known to aid in bypassing security. In late Q3, threat actors using the new version 5 of QakBot have been seen making several changes to their phishing tactics. The most notable new tactic employs attached malicious HTML files to deliver the payload. This new tactic does not utilize an embedded payload or redirect URL, as typical of most malicious emails delivering via HTML file attachments. Instead, the malicious payload is hardcoded into the HTML file, dropping when the HTML is executed inside the browser. This makes the delivery mechanism versatile (since every browser can read and execute HTML files) and stealthy (since the HTML file drops the payload locally without having to reach out to an external resource). QakBot continues to evolve defensive mechanisms against malware analysis, and phishing emails delivering QakBot continue to successfully reach inboxes. This makes QakBot the malware family to continue to watch as we enter Q4 2022, especially since a successful QakBot infection can lead to more costly threats like ransomware.

Other Malware Delivery Campaigns Copycatting Successful Tactics of QakBot.

Threat actors are known for collaborating, sharing, or even just taking successful ideas from others in their practice. One way this is apparent is that successful TTPs used in phishing campaigns entering the wild tend to emerge in other campaigns later on. During Q2 and continued into Q3, phishing campaigns delivering QakBot started using malicious HTML attachments as the first step of the infection chain in their highly successful and prolific phishing emails. Since this tactic emerged at such a large scale and had success reaching end users, other malware campaigns have been seen utilizing this tactic. Campaigns using malicious HTML files to download archives have emerged, delivering a variety of information stealers and RATs, most notably including a large NetSupport Manager RAT campaign. We anticipate this type of TTP to continue to be adopted by other malware delivery campaigns due to its versatility, stealth, and success in reaching inboxes protected by SEGs.

Emotet is Missing, What's Next?

In the beginning of Q3, we continued to see large volumes of Emotet emails, until about mid-July when Emotet phishing activity ceased. Following a **spike in Emotet C2 traffic observed by Cofense** on Oct. 10, 2022, it is plausible that Emotet itself will recommence sending malicious emails at some point in the coming quarter. However, for as long as this lull lasts, other malware families have an opportunity to step in and fill the void. With the high-volume return of QakBot in late Q3, along with its continual evolution of analysis evasion and TTPs, we may see a significant increase in QakBot volumes across Q4 to make up for the current lack of Emotet distribution.