COFENSE carahsoft.

Q3 2023

Cofense

Phishing Intelligence Trends Review

Thank you for downloading this Cofense report. Carahsoft is the vendor, reseller, and OMG-Vendor for Cofense cybersecurity solutions available via NJSBA, Texas DIR, MHEC, and other contract vehicles.

To learn how to take the next step toward acquiring Cofense's solutions, please check out the following resources and information:

For additional resources:
carah.io/CofenseResources

For upcoming events:
carah.io/CofenseEvents

For additional Cofense solutions:
carah.io/CofenseSolutions

For additional cyberseurity solutions:
carah.io/Cybersecurity

To set up a meeting:
Cofense@carahsoft.com
(888)-662-2724

To purchase, check out the contract vehicles available for procurement:
carah.io/CofenseContracts

For more information, contact Carahsoft or our reseller partners:
Cofense@carahsoft.com | (888)-662-2724

Q3 2023

Cofense Phishing Intelligence Trends Review

Executive Summary

During Q3 of 2023, new and old techniques appeared, creating a high volume of campaigns that reached users in environments protected by secure email gateways (SEGs). Throughout this quarter, we saw an increase in volume for both credential phishing and malware campaigns. Cofense Intelligence also observed a resurgence in some malware families that have been less common in previous quarters, while the more notable families like QakBot and Emotet remained inactive.

The key highlights for Q3 2023 include:

- Credential phishing indicators of compromise (IOCs) increased by nearly 45% in Q3 compared to Q2 and increased 85% from Q3 2022.
- QR codes embedded in images and PDFs within phishing emails rose, likely due to the difficulty security infrastructure faces when checking links and other embedded content compared to that of raw email content.
- PDFs remain the most popular phishing email attachment for threat actors, making up nearly 50% of the malicious file extensions seen in email campaigns this quarter.
- Emotet and QakBot remained inactive throughout Q3 with QakBot staying silent since Q2 2023 and Emotet since Q1 2023. QakBot's silence is likely due to the FBI takedown and may lead to QakBots replacement by a new botnet.
- An increase in reconnaissance and utility tool malware appeared this quarter, like Browser Password Dump Utility or Email Password Dump Utility, making them the 5th most popular malware type of the quarter.

> ***Credential phishing indicators of compromise (IOCs) increased by nearly 45% in Q3 compared to Q2 and increased 85% from Q3 2022.***

Credential Phishing Activity

Credential phishing IOCs have increased across the board, with July having the highest amount for the year. However, as the quarter continued, the volume mellowed down to an average, with August and September having a similar volume to other months this year. This year, however, held an 85% higher average than the previous year. This quarter saw an approximate 45% increase in overall credential phishing emails compared to Q2 2023. This may be due to the rise in Google AMP being leveraged in phishing campaigns, as well as QR codes soaring in popularity.

> ***Credential phishing 85% higher increase than previous year, may be due to the rise of Google AMP and QR codes soaring in popularity.***

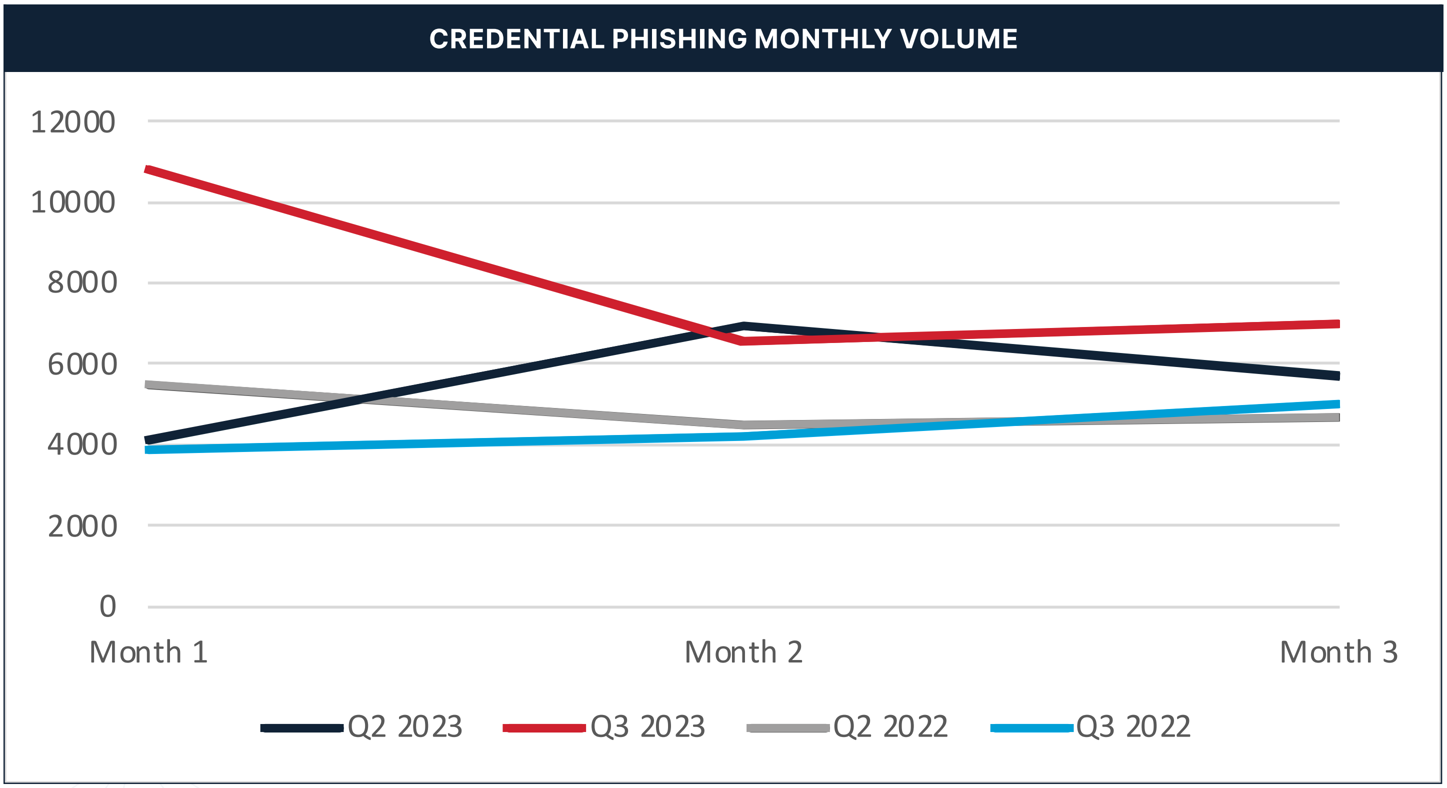

Figure 1: Comparison of monthly volume of credential phishing emails observed in Q2 and Q3 during 2022 and 2023.

Credential Phishing Activity

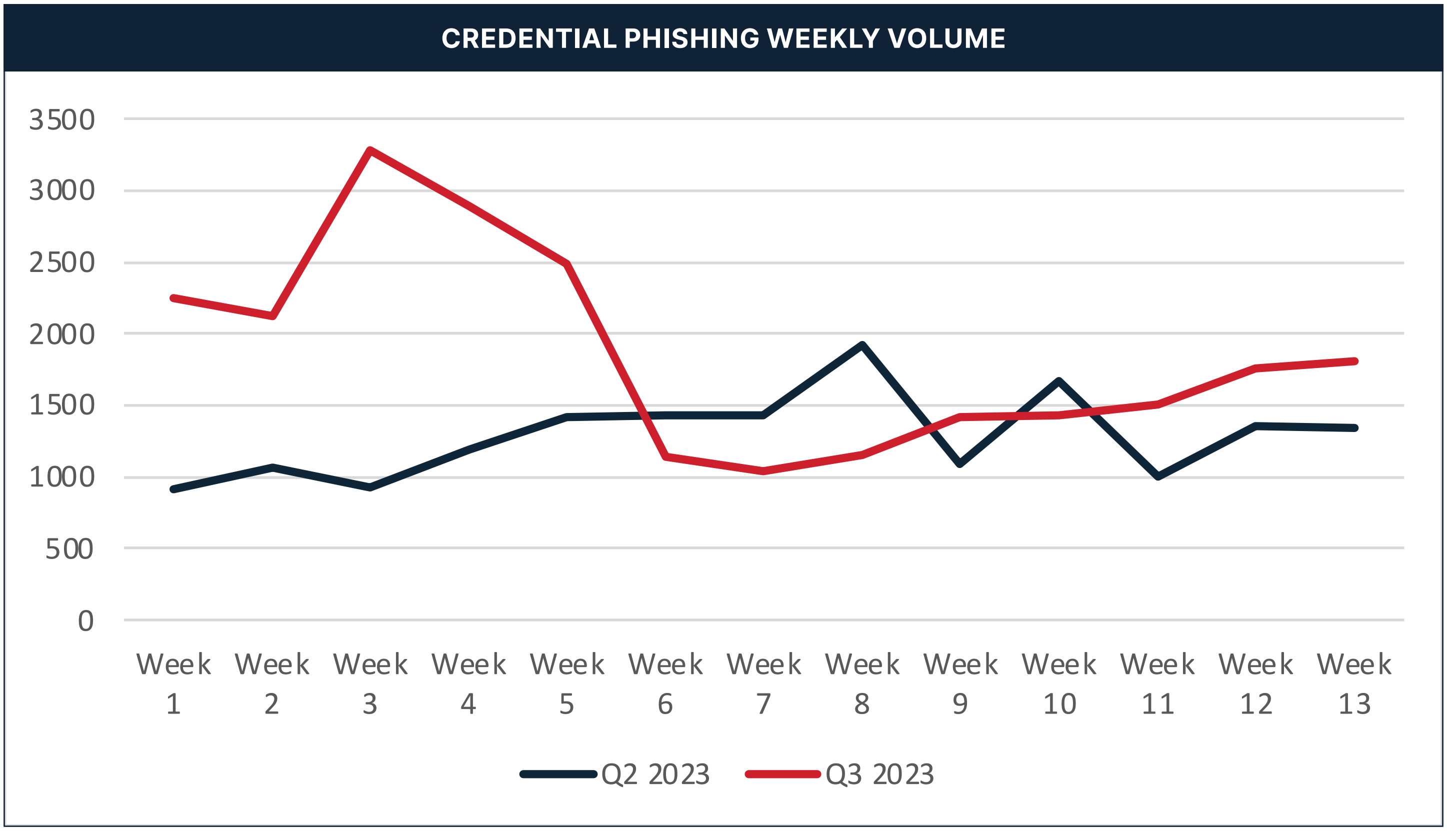

Figure 2: Comparison of weekly volume of credential phishing emails observed in Q2 and Q3 2023.

Prevalent Malware in Q3

Agent Tesla keylogger continued to reign as the most popular malware family through Q3. This, in turn, made Keylogger the top malware type of this quarter. FormBook and Loki Bot, the next most popular malware families, had a steady decrease throughout the quarter, however both were still greatly used. Remcos RAT and Vidar Stealer, on the contrary, became more popular as the quarter continued. As of the end of Q3 2023, there has been no sign of a QakBot resurgence since the law enforcement takedown in August.

A malware family that is not often seen in the top malware family list showed up this quarter: Banload, a Banker known to target Brazilian users. This malware was the most popular Banker of the quarter, due to a campaign that was occurring in August. The fifth most popular malware type for Q3 was categorized under “Other Malware,” which primarily encumbers reconnaissance and utility tools.

TOP FIVE MALWARE TYPES	TOP FAMILY IN TYPE
Information Stealer	FormBook
Keylogger	Agent Tesla
Remote Access Trojan	Remcos Remote Access Trojan
Banker	Banload
Other Malware	Email/Browser Dump Utility

Table 1: Top five malware types with the top family of each type in Q3 2023.

Despite a decrease in RAT volume, the DarkGate RAT first appeared in advanced campaigns in Q3.

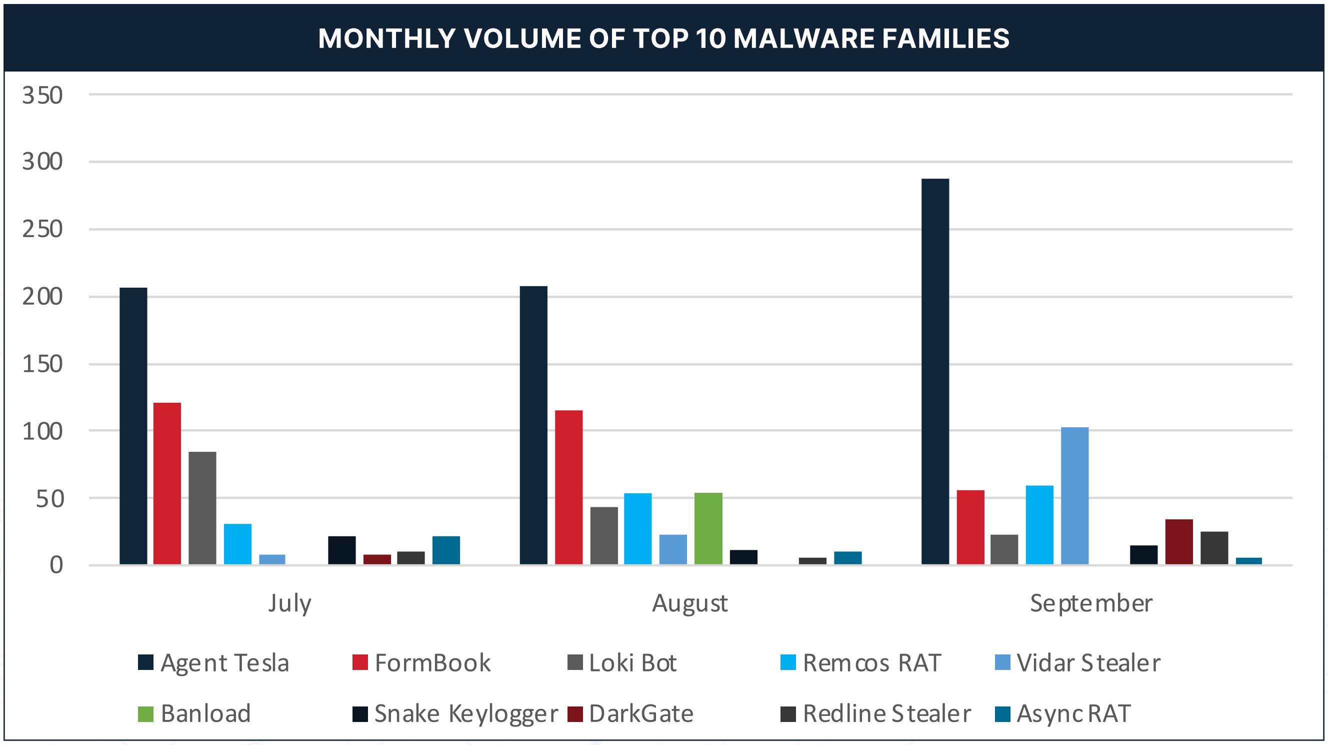

Figure 3: Monthly volume of top ten malware families in each type in Q3 2023.

Prevalent Malware in Q3

In Q3, there were more information stealers seen compared to the previous quarter, and this can be due to some information stealers rising in popularity such as Vidar Stealer, which is one of the top ten malware families seen in the quarter. Yet FormBook and Loki Bot have and continued to be the primary information stealers many threat actors use, which overlapped keyloggers. Unlike the previous quarter, keyloggers were not the most common malware type; however it was very close due to Agent Tesla, as well as some other malware such as Snake Keylogger that also contributed. RATs and bankers both saw a decrease in volume compared to Q2. The fifth malware type, "Other Malware," which consists of reconnaissance tools and browser utility dumps, was not seen throughout Q2, but did appear in Q3.

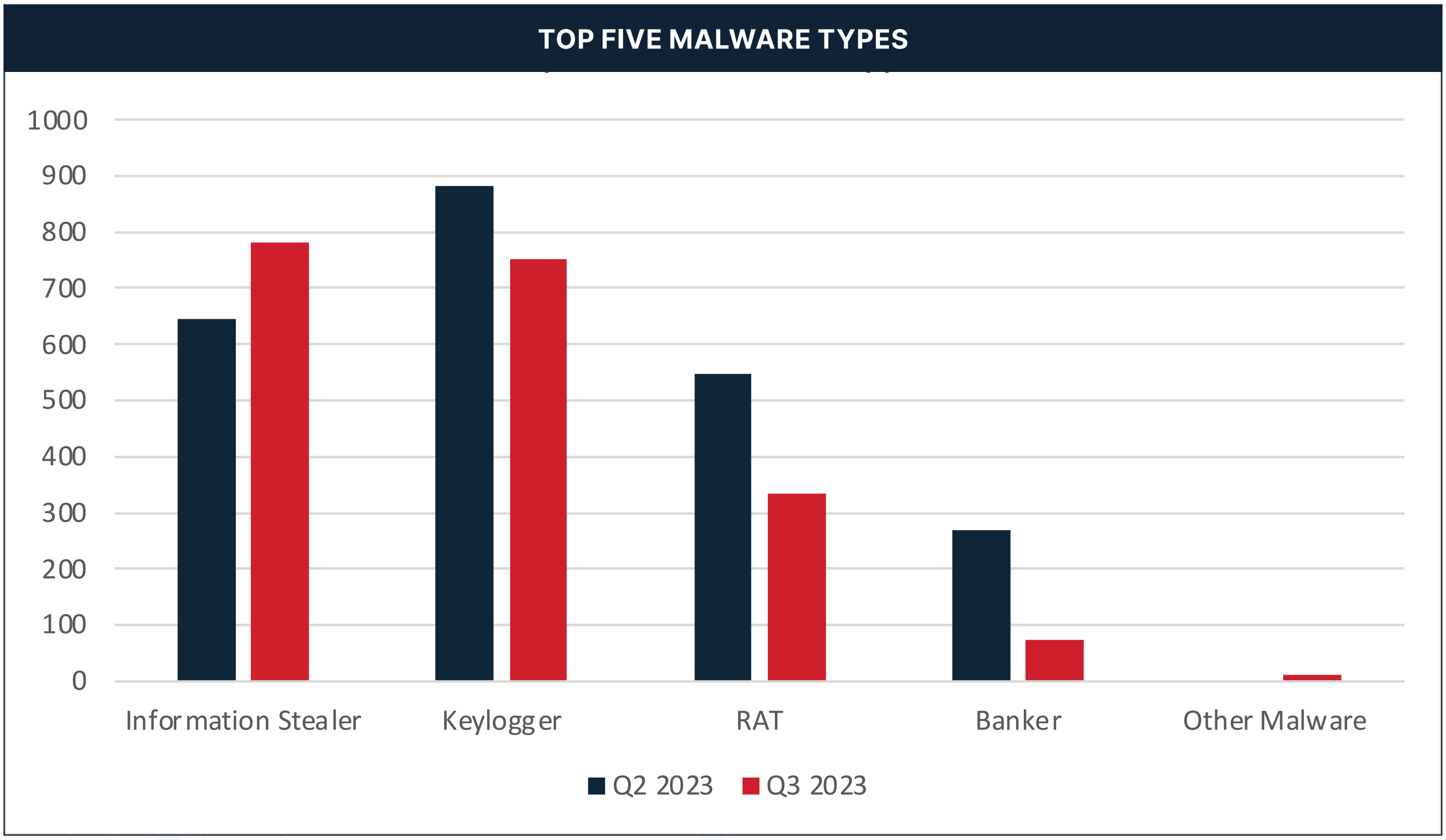
TOP FIVE MALWARE TYPES

Figure 4: Top five malware types in Q2 and Q3 2023 by volume of emails.

Delivery Mechanism Rundown

During Q3, both PDF droppers and the CVE-2017-1882 exploit remained at the same volume as Q2. The CVE-2017-0199 exploit often comes along with CVE-2017-11882, and Q3 saw an uptick of this delivery chain. The other popular delivery mechanism that appeared in Q3, which was not there during Q2, was Microsoft HTML Application. The Microsoft HTML Application could have appeared on the most common delivery mechanisms for Q3 due to the Banload campaign.

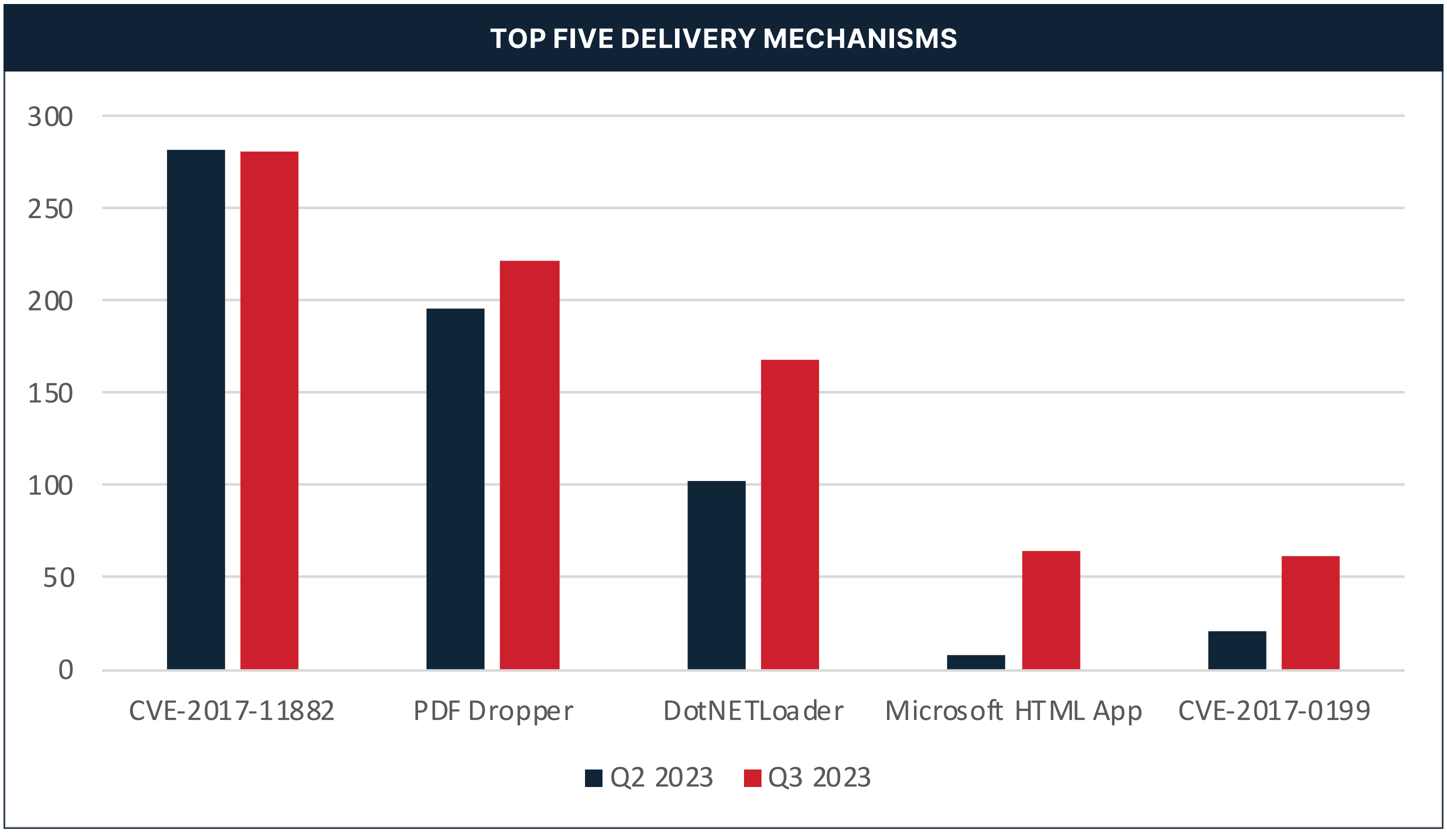

Figure 5: Top five malware delivery mechanisms by email volume in Q3 2023, with Q2 totals for comparison.

Delivery Mechanism Rundown

The CVE-2017-11882 exploit has always been a popular delivery mechanism seen by Cofense. Below is a pie chart showing the top malware families delivered via CVE-2017-11882. Agent Tesla was the most common, followed by FormBook. This was switched last quarter, with FormBook being the most common malware family delivered via CVE-2017-11882 exploit, followed by Agent Tesla. On top of this, Ave Maria was not often delivered using this exploit last quarter, however during Q3 it managed to reach the top five malware families delivered with this exploit.

TOP FIVE MALWARE CVE-2017-11882

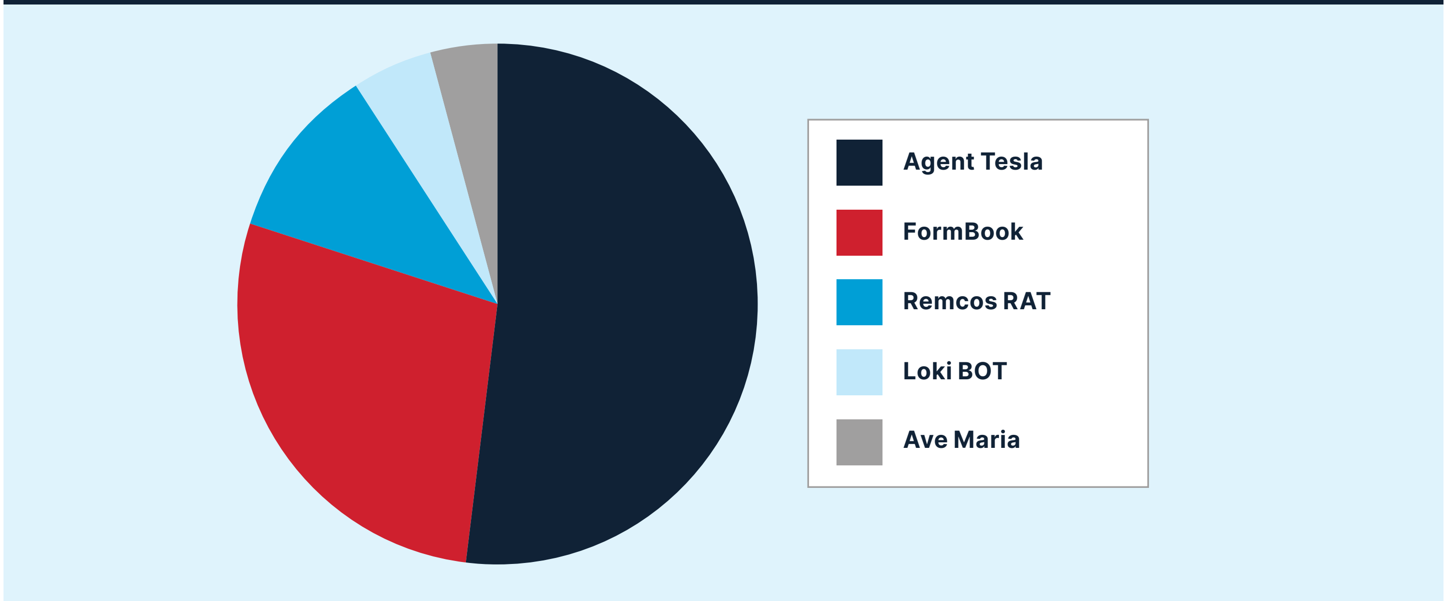

Figure 6: Top five malware families delivered by CVE-2017-11882 in Q3 2023.

Domains and TLDs Used in Credential Phishing

Each quarter, Cofense Intelligence analyzes credential phishing emails that reached users in environments protected by SEGs. We identify the individual domain names and top-level domains (TLDs) that were most prominent.

Stage 1 URLs are embedded in the phishing email itself, while Stage 2 URLs are used as redirects or embedded in credential phishing websites. The ten most common .com domains used in both stages combined are represented in Table 2. Of the domains, several trusted cloud platforms can be identified, showing continued abuse by credential phishing threat actors.

The bing.com domain increased drastically as it was used for credential phishing redirection.

RANK	Q2 2023	Q3 2023
1	myqcloud.com	bing.com
2	adobe.com	google.com
3	sharepoint.com	linkedin.com
4	bing.com	baidu.com
5	google.com	dropbox.com
6	dropbox.com	adobe.com
7	box.com	godaddy.com
8	microsoft.com	sharepoint.com
9	vk.com	microsoft.com
10	backblazeb2.com	linodeobjects.com

Table 2: Q2 and Q3 2023 ten most common .com domains used in credential phishing campaigns.

The majority of credential phishing threat actors use .com domains in their campaigns. During Q3, threat actors changed much of the order regarding the most common .com domains, most being abused .com domains. Most sites on the list during Q3 2023, including Bing, Google, Baidu, and Linodeobjects, contain an open redirect which has been heavily abused by threat actors during this quarter. LinkedIn was also abused during this quarter due to their smart links, which redirect users to a malicious link. Although these are not new tactics, the volume at which they were abused did increase this quarter.

Linkedin.com became popular as it was used in campaigns covered by our *Strategic Analysis Hundreds of Emails Re-Popularize LinkedIn Smart Links*

Domains and TLDs Used in Credential Phishing

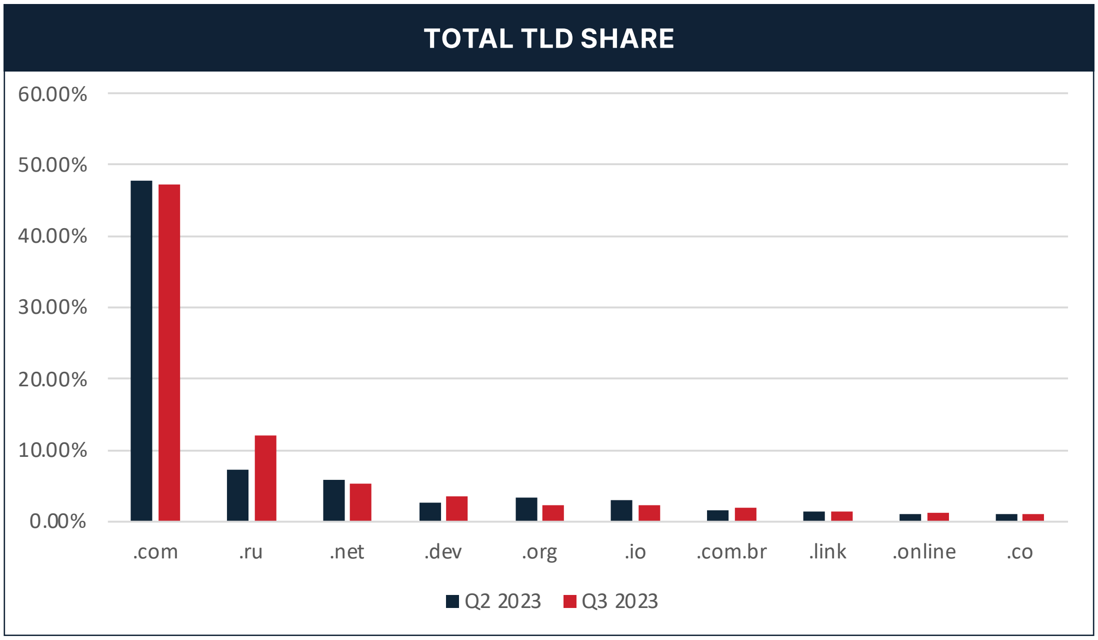

Figure 7: The top ten TLDs for both stages in Q3 2023, with Q2 totals for comparison.

Between Q2 and Q3 of 2023, the majority of TLDs remained primarily the same, despite having a higher volume of phish in Q3. The only noticeable difference between the quarters would be the increased amount of .ru TLDs being used. This could be due to the fact that Caffeine, a Phishing as a Service (PhaaS) tool, has continued to grow in popularity. Cofense wrote a Strategic Analysis earlier in 2023 regarding Caffeine titled "Caffeine Phishing Service Domains and Patterns Still Heavily Used After Store Seemingly Defunct." More can be read about this Strategic Analysis **here**.

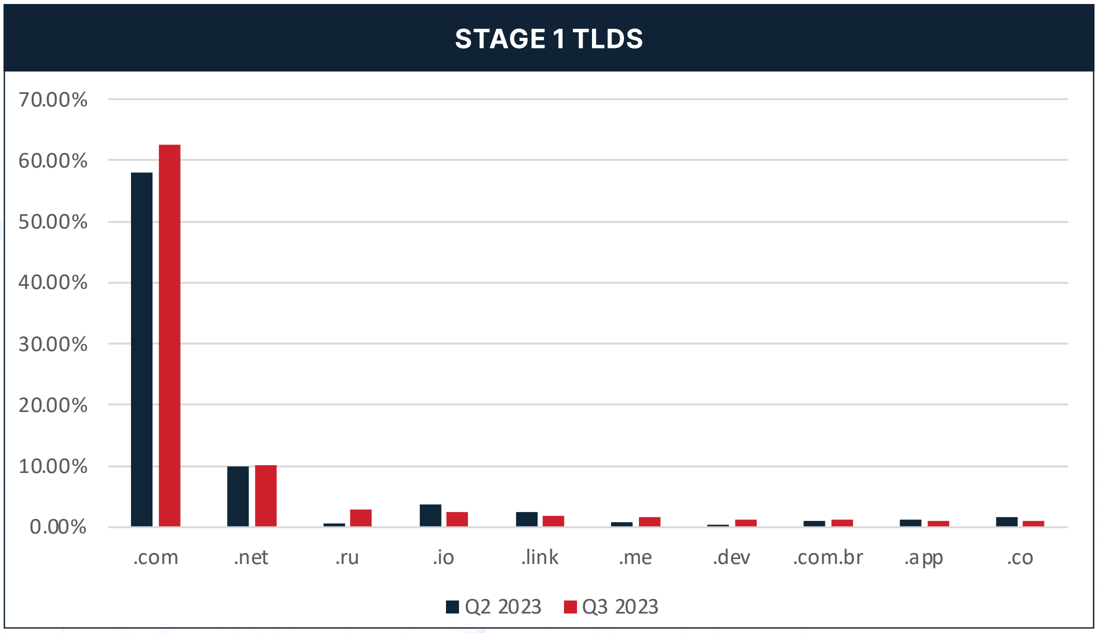

Figure 8: The top ten Stage 1 TLDs in Q3 2023, with Q2 totals for comparison.

Domains and TLDs Used in Credential Phishing

During Q3 2023, the same could be said about the Stage 1 TLDs regarding the overall TLD usage of this quarter. The .com TLD did have an increase in stage 1, which could likely be due to the increase in overall phishing volume during this quarter. The other noticeable difference is that .ru TLDs did rise a significant amount, from 0.65% in Q2 to nearly 3% in Q3. The reasoning could be due to the same regarding overall TLD share, where Caffeine has increased in popularity.

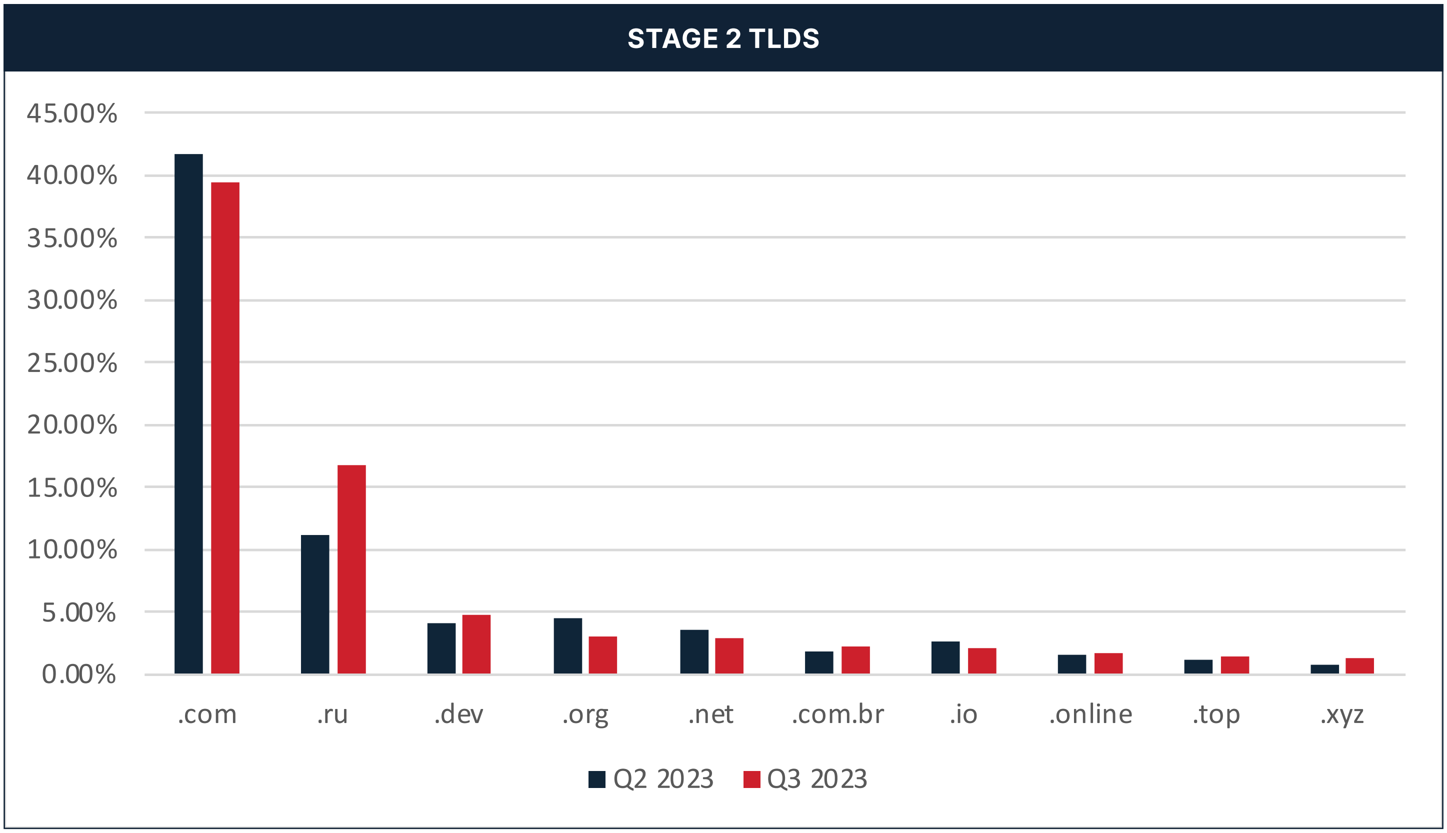

Figure 9: The top ten Stage 2 TLDs in Q3 2023, with Q2 totals for comparison.

TLDs used in Stage 2 remained mostly consistent to the last quarter, except for the .ru TLD. Although in Q2 there was still a numerous amount of .ru TLDs found in the second stage, more were found in Q3. This could be due to the same domain being used throughout a campaign. However, .com TLDs did decrease slightly for Stage 2 TLDs.

File Extensions of Attachments

PDFs were the primary file extension found in email attachments for both phishing and malware campaigns. Some may contain a clickable link towards the phishing site or could simply impersonate a reputable source and contain a password to a downloaded .zip file. This was similar to Q2, and proved Cofense's prediction that PDF attachments would continue to rise in popularity due to the complexity compared to checking raw email content.

Cofense's prediction in our Q2 2023 report that PDF attachments would continue to rise in popularity has been confirmed.

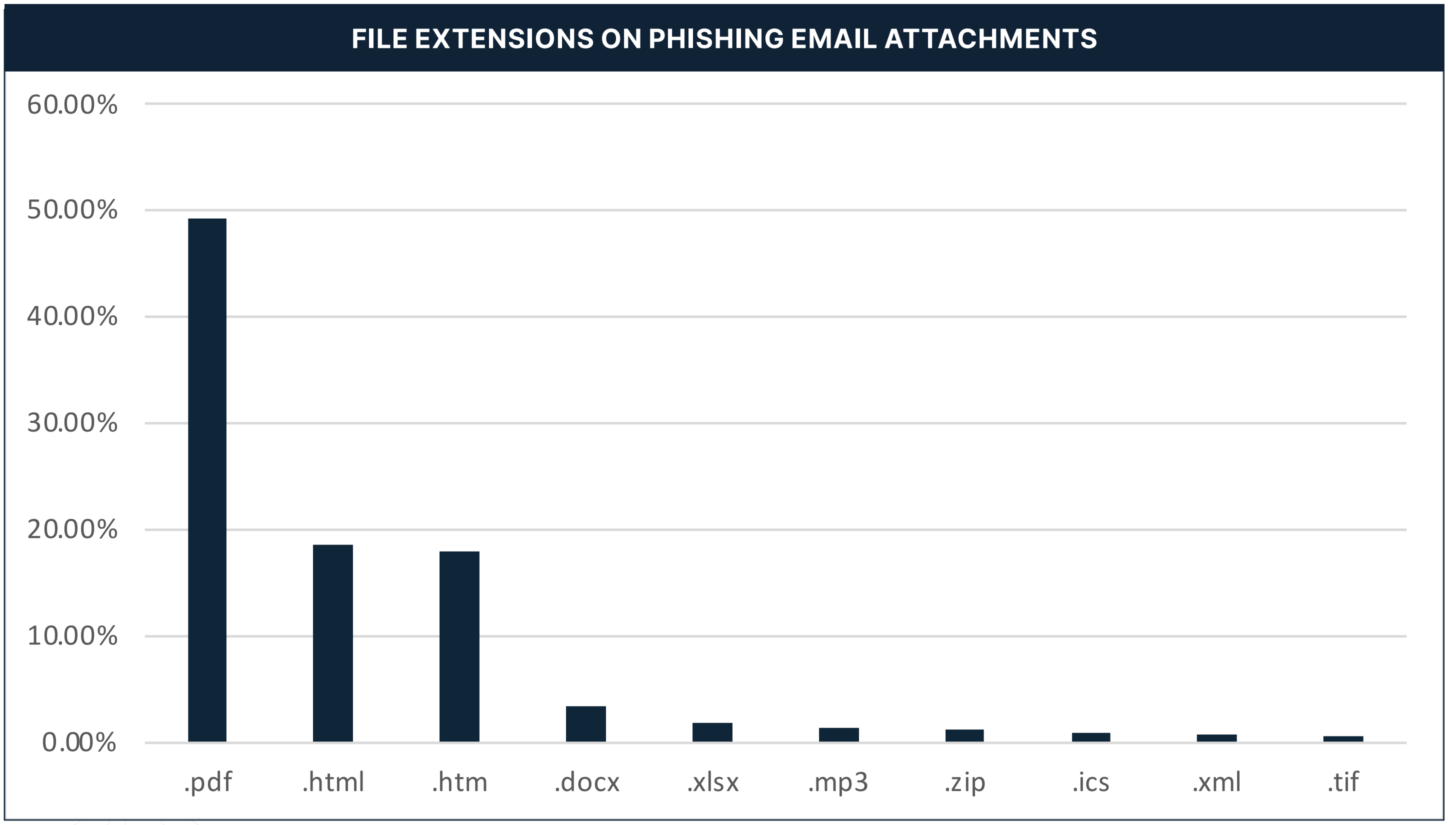

Figure 10: Top 10 most common attachment file extensions found in environments protected by SEGs in Q3 2023.

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, often receiving information and exfiltrated data from infected hosts. There were a few differences between Q2 2023 and Q3 2023. One major difference is that Canadian and Great Britain C2s greatly decreased, while other countries such as Denmark and Japan rose in popularity. However, the United States remains as the most popular C2 location.

Note: 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.

Q1 2023		Q2 2023	
Country	**Percentage**	**Country**	**Percentage**
United States	69.73%	United States	71.17%
Canada	10.79%	Canada	3.15%
Great Britain	8.13%	Great Britain	3.00%
Germany	2.11%	Denmark	2.65%
France	1.61%	Japan	2.12%

Table 3: Q2 and Q3 2023 percentages for C2 sources by IP address geolocation.

> ***The United States continues to be the top C2 source by IP address geolocation as has been the case since it was first tracked. This is likely to continue as many cloud hosting services abused by threat actors are hosted in the United States.***

Projections for Q4 2023 and Beyond

Google AMP URLs Will Continue to Rise in Popularity

At the beginning of Q3, threat actors started to use Google to their advantage to bypass SEGs. The URL will start off with google[.]com/amp/s, which is then followed by the malicious domain and path. Due to the trusting nature SEGs have with Google, this allows an unauthorized redirect to another site, which in the case of phishing, will redirect to a malicious site. Cofense has released a Strategic Analysis which goes further in depth on this topic titled "Google AMP – The Newest of Evasive Phishing Tactics." More can be read about this topic **here**.

QR Codes Will Grow in Popularity with New Techniques

QR codes have been a special interest at Cofense, due to the unexpected rise in popularity among threat actors to use QR codes. This is not a new tactic; however, with other trends such as PDFs rising in popularity, it makes sense as to why QR codes would be following. This may be due to the lack of security many SEGs have regarding scanning QR codes, especially if they are attached to other file extensions, such as PDFs, which were the most common file attachment of the quarter. QR codes have also recently been seen generated using trusted domains. A primary example of this is Google's API chart, which will generate a QR code via an embedded URL.

Spike in Banking Trojans in Q4

From what Cofense has seen in the past, Banking Trojans typically skyrocket in volume at the end of the year. Cofense does not see any reason for this to change. Cofense already saw a slight rise in use in August, where a Banker campaign was sent to customers. However, QakBot typically becomes active near the end of the year or the beginning of the year. When QakBot is active, there is a large influx of QakBot that arrives in inboxes, often making this the most popular Banking Trogan.

Law Enforcement Takedown Was Specifically Effective

The law enforcement takedown of some of QakBot's infrastructure was surprisingly effective. Despite some signs of activity, it does not appear that QakBot has made the kind of recovery that many expected. However, law enforcement was only effective on part of QakBot's infrastructure. The remaining infrastructure is still being used to deliver malware. It is likely that it will continue to be used to deliver ransomware in bulk to make up for the lost revenue due to the takedown. It is likely the next big botnet will also segregate its infrastructure now that it has been proven to be effective.

Finished Intelligence: Topics and Trends

Strategic Analysis – Google AMP – The Newest of Evasive Phishing Tactics

A new phishing tactic utilizing Google Accelerated Mobile Pages (AMP) has hit the threat landscape and proven to be very successful at reaching intended targets. Google AMP is an open-source HTML framework used to build websites that are optimized for both browser and mobile use. The websites that we observed in these campaigns are hosted on Google.com or Google.co.uk, both of which are considered trusted domains to most users. This phishing campaign not only employs Google AMP URLs to evade security, but also incorporates a multitude of other tactics, techniques, and procedures (TTPs) known to be successful at bypassing email security infrastructure.

Strategic Analysis – Major Energy Company Targeted in Large QR Code Campaign

Beginning in May 2023, Cofense has observed a large phishing campaign utilizing QR codes targeting the Microsoft credentials of users from a wide array of industries. The most notable target, a major energy company based in the US, saw about 29% of the over 1000 emails containing malicious QR codes. Other top 4 targeted industries include manufacturing, insurance, technology, and financial services seeing 15%, 9%, 7%, and 6% of the campaign traffic respectively. Most of the phishing links were comprised of Bing redirect URLs, but other notable domains include krxd[.]com (associated with the Salesforce application), and cf-ipfs[.]com (Cloudflare's Web3 services). Historically, QR codes are not a popular choice due to the limiting nature of how QR codes are interacted with. However, they have several advantages over a phishing link embedded directly in an email. QR code delivery methods have a much better chance of reaching an inbox as the phishing link is hiding inside the QR image, while the QR image is embedded inside a PNG image or PDF attachment.

Flash Alert – Government Contractor Targeted Campaign Returns

A campaign that Cofense warned about with a Flash Alert in July of 2019 and published a more in-depth Strategic Analysis of in September 2022 has returned. The campaign is sophisticated, using advanced techniques from start to finish and is currently impersonating the US Department of Agriculture.

Finished Intelligence: Topics and Trends

Strategic Analysis – The Lure of Subject Lines in Phishing Emails – How Threat Actors Utilize Dates to Trick Victims

The use of misleading dates in subject lines has long been a preferred tactic of threat actors for influencing the emotions of recipients and creating a false sense of urgency. In this report we have uncovered some interesting trends in subject lines with dates in them and targeted subsectors. We will cover the trends that Cofense Intelligence discovered during the month of July 2023.The subject lines seen were intentionally deceptive, and the dates used in the subjects covered a range from a few days before the email was sent to several days afterwards. Subject lines such as these are specially designed to create a false sense of urgency requiring the victim's immediate interaction, and not allowing them time to consider how suspicious the email is. The dates in the subjects of emails sent to 18 different subsectors were compared to the actual date the email was accessed leading to some surprising trends. The key results are divided into the ratios of subjects with dates to those without, late emails (emails with subject times before the date they were accessed), early emails (emails with subject times after the date they were accessed), and on time emails (subjects that had dates in them which matched to the date they were accessed).

Strategic Analysis – Loki Bot – Phishing Malware Baseline

Loki Bot is an information stealer with expanding capabilities depending on the threat actor. This malware family was originally written in C++ and targets Windows devices. Loki Bot was first advertised in 2015 on underground markets in Eastern Europe; however, it was not common to see it in the wild until 2018. Since then, Loki Bot has remained in the top five malware families delivered through phishing emails.

Strategic Analysis – Luxury Hotels Remain Major Target of Ongoing Social Engineering Attack

Cofense Intelligence has been tracking a well-crafted and innovative phishing campaign that targets the hospitality industry to deliver advanced information stealer malware. The campaign employs the use of reconnaissance emails and instant messages to bait hospitality email addresses into a response. Once a conversation has started, the threat actors follow up with a phishing email. This campaign uses social engineering tactics also recently seen during the MGM, Caesars and other luxury hotel resort breaches.

Overall, the campaign uses several tried-and-true methods to bypass email security infrastructure which puts targets at risk of sophisticated information stealer malware like RedLine Stealer, Vidar Stealer, Stealc, and others, most of which can deploy ransomware after successfully infecting a host.