



Q2 2023

Cofense Phishing Intelligence Trends Review



Executive Summary

Each quarter, Cofense Intelligence has analyzed malware and credential phishing emails that reached users in environments protected by SEGs. This quarter we saw increases in credential phishing, SuperMailer campaigns, NetSupport Manager RAT campaigns, and compromised domains to deliver malware via embedded URLs. In Q2 2023, Cofense Intelligence saw a slowdown in malicious email activity as prominent malware operators reduced or paused their campaigns. Despite the overall lower volume during this quarter, significant new phishing threats emerged.

The key highlights for Q2 2023 include:

- Credential phishing indicators of compromise increased 10% in Q2 and increased 85% from the same quarter last year.
- A massive credential phishing campaign abusing the legitimate mailing software, SuperMailer rose an impressive 87% in Q2.
- The use of compromised domains to deliver malware via embedded URLs increased by 25% in Q2.
- NetSupport Manager RAT re-appeared and increased by 82% in Q2.
- Malware delivery mechanism, JSDropper impressively rose 240%.
- PDF documents represented the most common malicious choice for threat actors representing 42.4% of all total malicious file attachments.
- More than half (51%) of malware-delivery URLs embedded in malicious emails abused compromised legitimate domains.

Malware delivery mechanism, JSDropper impressively rose 240%.

Overall credential phishing indicators of compromise increased 10% from Q1 to Q2 and increased 85% from the same quarter last year.

Credential Phishing Activity

Overall credential phishing indicators of compromise increased 10% from Q1 to Q2 and increased 85% from the same quarter last year. The enormous surge in volume in late March had cooled down by the time Q2 started, and volume was much steadier throughout the rest of the quarter. Threat actors did send more emails on average during the month of May, as seen in Figure 1, attributable at least in part to high-volume campaigns sent using SuperMailer. A massive credential phishing campaign abusing the legitimate mailing software, SuperMailer rose an impressive 87% in Q2.

A massive credential phishing campaign abusing the legitimate mailing software, SuperMailer rose an impressive 87% in Q2.

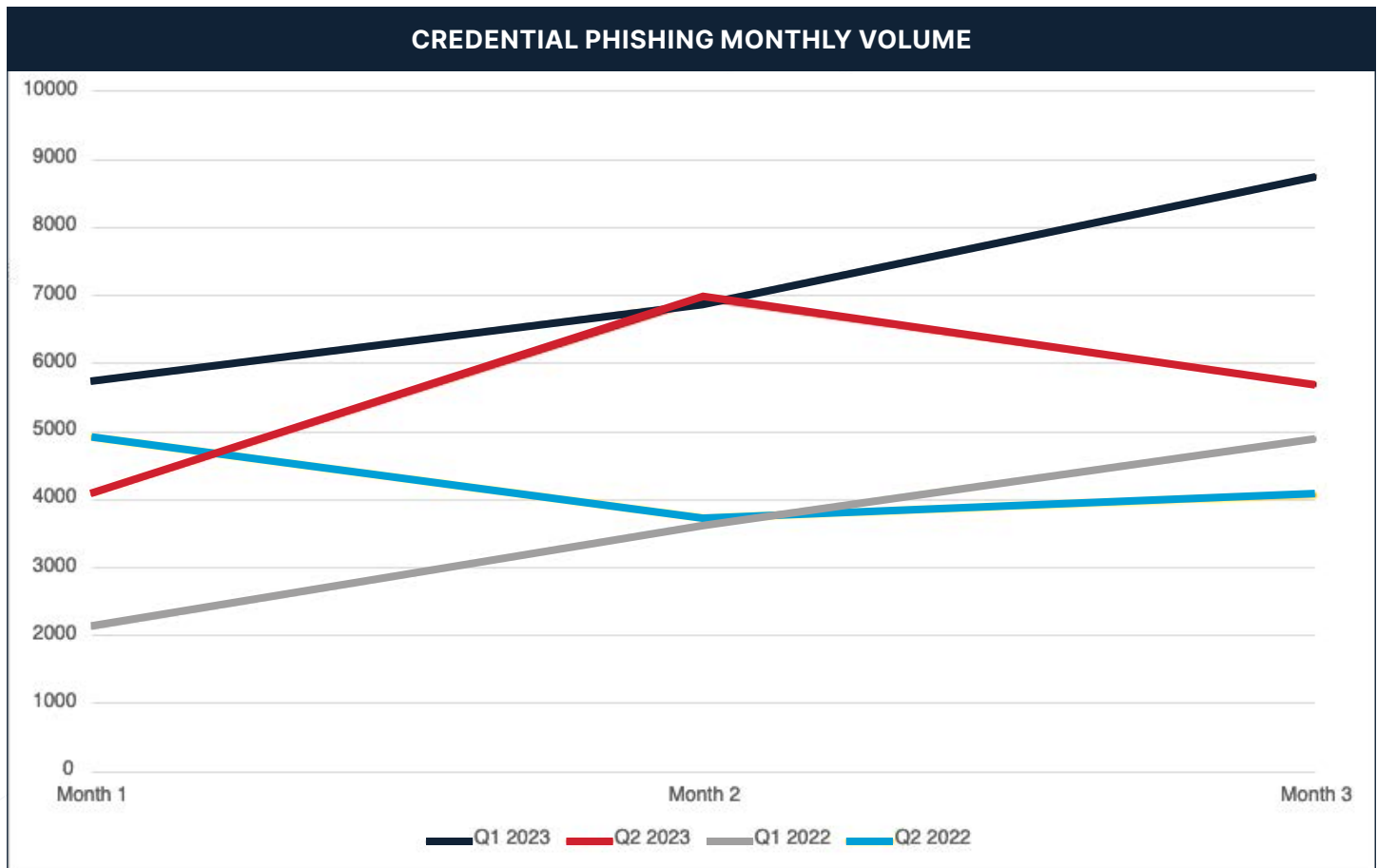


Figure 1: Comparison of monthly volume of credential phishing emails observed in Q1 and Q2 2023.

Credential Phishing Activity

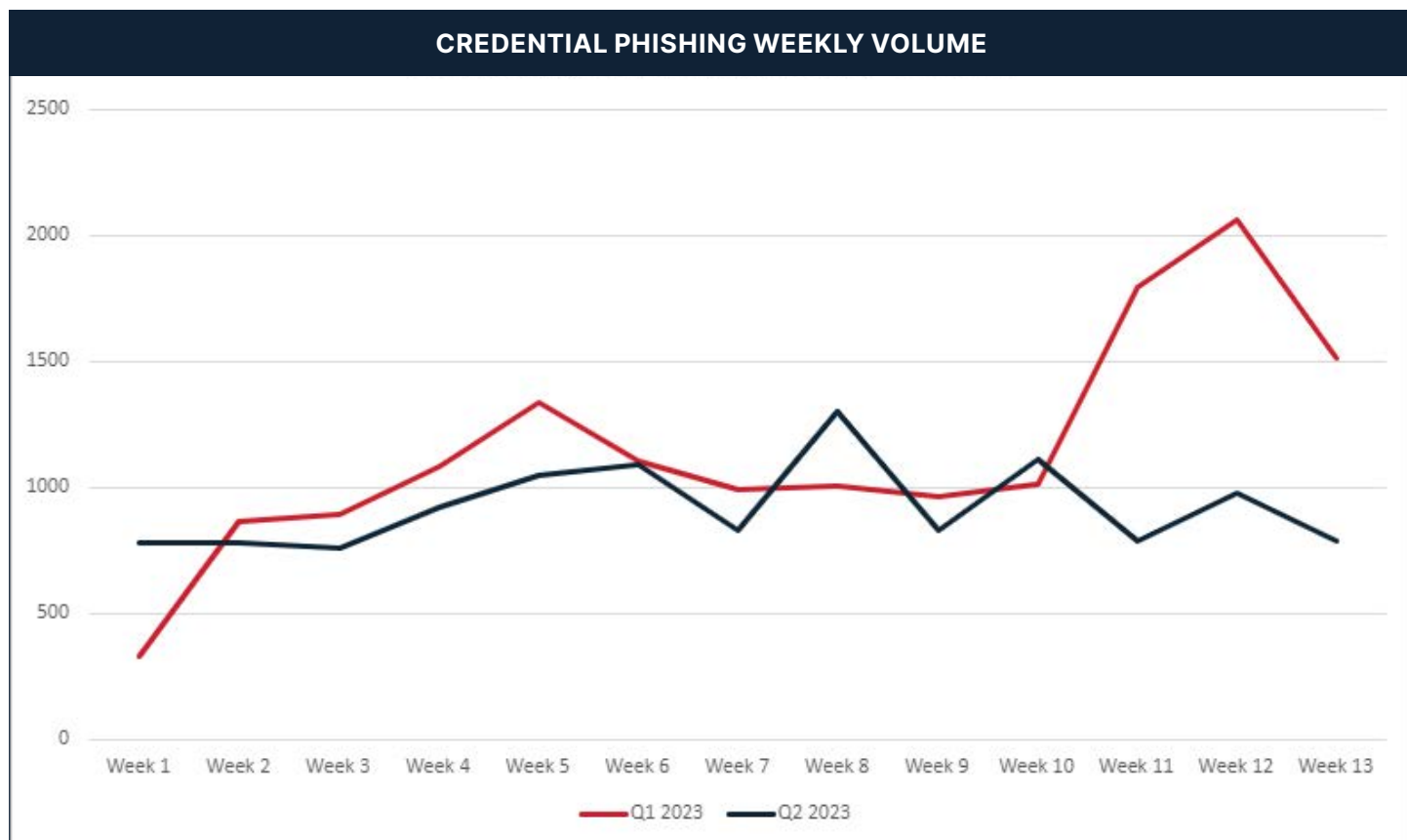


Figure 2: Comparison of weekly volume of credential phishing emails observed in Q1 and Q2 2023.



Prevalent Malware in Q2

Agent Tesla has long been a fixture in the phishing threat landscape and maintained consistent high volume throughout Q2. Other malware families like FormBook and Remcos RAT fluctuated from month to month, as seen in Figure 3. May was a breakout month for several families: QakBot, NetSupport Manager RAT, Snake, and Loki Bot all posted considerably higher volume in May than in April or June.

Emotet botnet did not send any emails during Q2, dropping the Loader malware type from the top to just the fifth most common. In Emotet's absence, Amadey represented most of the loaders sent in Q2. The NetSupport Manager Remote Access Trojan increased in volume enough to edge out Remcos as the most common RAT. Keyloggers and Information Stealers remained consistent with Q1 2023.

TOP FIVE MALWARE TYPES	TOP FAMILY IN TYPE
Keylogger	Agent Tesla
Information Stealer	FormBook
Remote Access Trojan	NetSupport Manager RAT
Banker	QakBot
Loader	Amadey

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

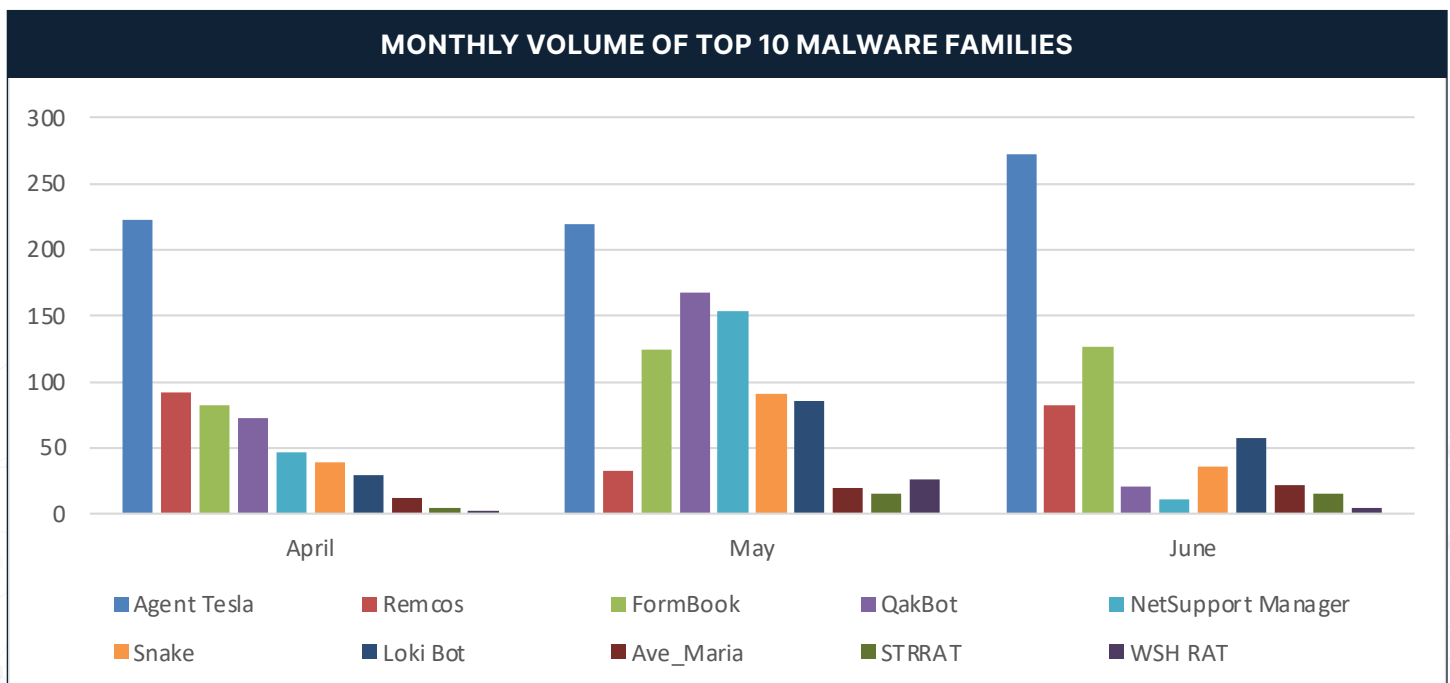


Figure 3: Monthly volume of top ten malware families in each type.

Prevalent Malware in Q2

Agent Tesla constituted most of the keylogger volume, with a minor contribution by Snake. Similarly, FormBook accounted for most of the information stealer volume with Loki Bot playing a minor role. QakBot was by far the most common banking trojan, and Amadey virtually the only loader. RATs were the only malware type with much diversity, with NetSupport Manager, Remcos, STR RAT, and WSH RAT all crowding the field.

RATs increased by 82% from Q1 to Q2; bankers also increased slightly at 9%.

Cofense Intelligence saw a slowdown in malicious email activity as prominent malware operators reduced or paused their campaigns. A significant drop in Loader was due to Emotet absence. Keylogger volume diminished considerably: for example, the number of emails delivering Agent Tesla dropped by almost half. FormBook and other information stealers dropped as well. RATs increased by 82% from Q1 to Q2; bankers also increased slightly at 9%, as seen in Figure 4.

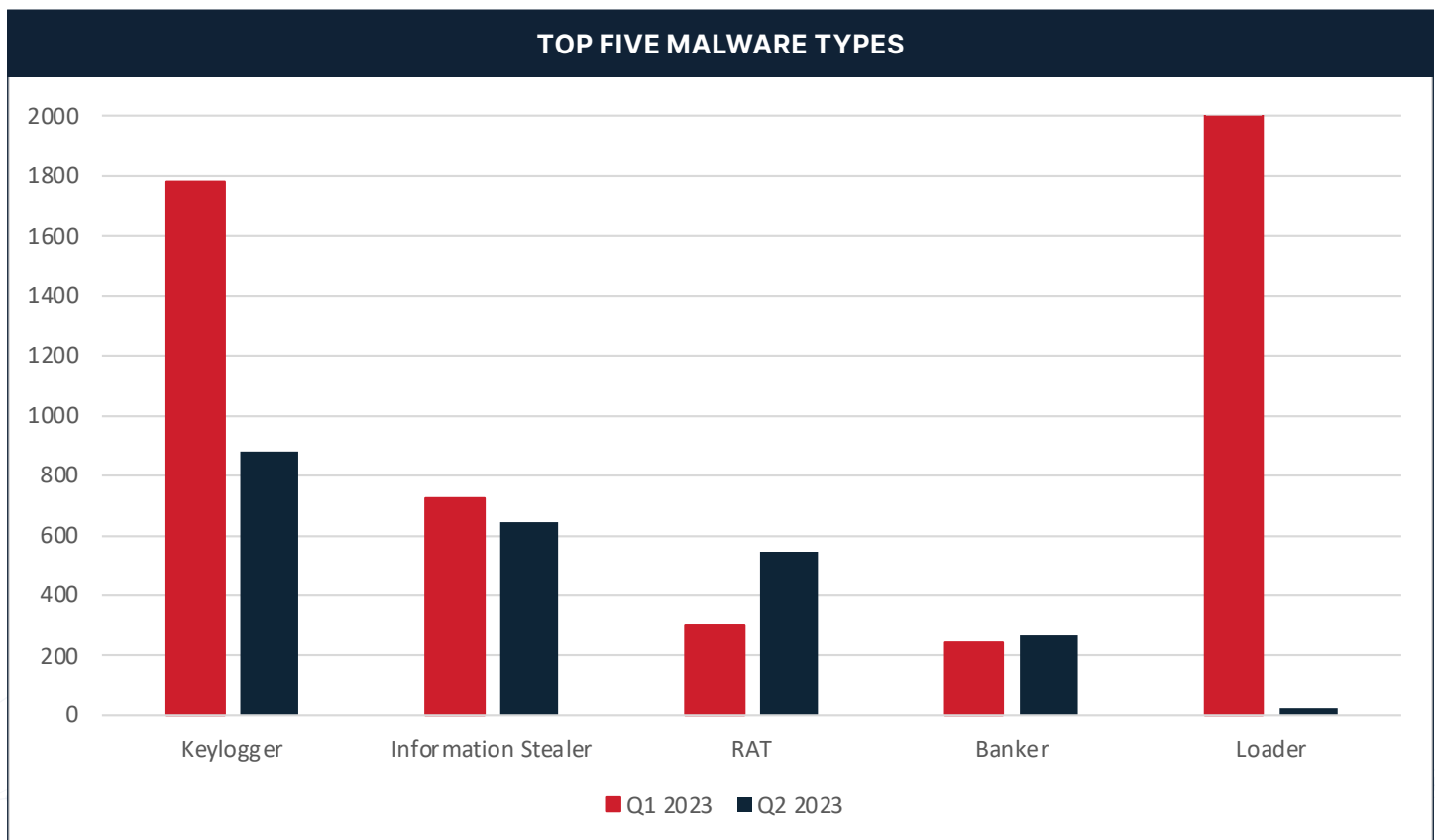


Figure 4: Top five malware types in Q1 and Q2 2023, by volume of emails. The maximum value for this chart has been capped and does not show the full proportion of the Loader malware type from Q1.

Delivery Mechanism Rundown

Two malware families served as trendsetters in delivery mechanism usage in Q2, JSDropper and PowerShell. JSDropper rose significantly by 240% in Q2. The threat actors behind QakBot followed a behavioral pattern from previous quarters, regularly cycling through different delivery mechanisms. In April they favored PDF attachments leading to WSF files, but in May they switched to JSDropper attachments. The other malware family was NetSupport Manager RAT, which was delivered using a chain of JSDroppers to PowerShell scripts. Together the two families made JSDroppers the most common delivery mechanism of the quarter, with malicious PowerShell scripts and PDF droppers in the top five as well.

JSDropper rose significantly by 240% in Q2.

Cofense Intelligence saw many exploits of CVE-2017-11882 in Q1 but then dropped in Q2. Agent Tesla represents much of the difference, as it had used CVE-2017-11882 heavily in Q1. Note, the overall volume of Agent Tesla emails decreased 47% in Q2, bringing CVE-2017-11882 usage down with it.

In Q1, Emotet put malicious OLE Package files and WSF Downloaders at the top of the list, but since the botnet was silent during Q2, those two delivery mechanisms saw relatively little use, as seen in Figure 5.

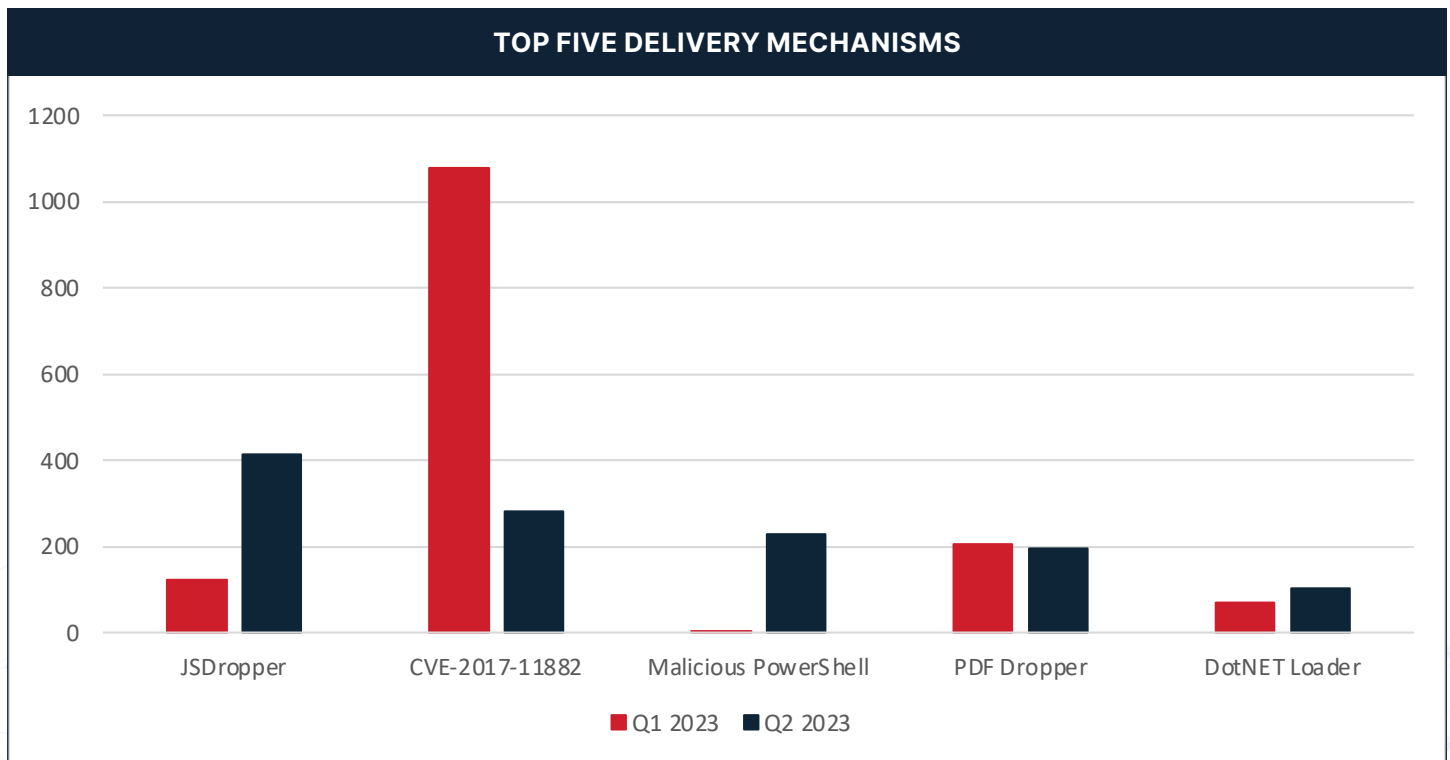


Figure 5: Top five malware delivery mechanisms by email volume in Q2 2023, with Q1 totals for comparison.

Delivery Mechanism Rundown

Cofense Intelligence saw many exploits of CVE-2017-11882 the 1st half of this year. This over a decade old Microsoft (OLE) vulnerability used to deliver these top malware families, FormBook came in #1 at 33% and Agent Tesla a quick second place, as seen in Figure 6.

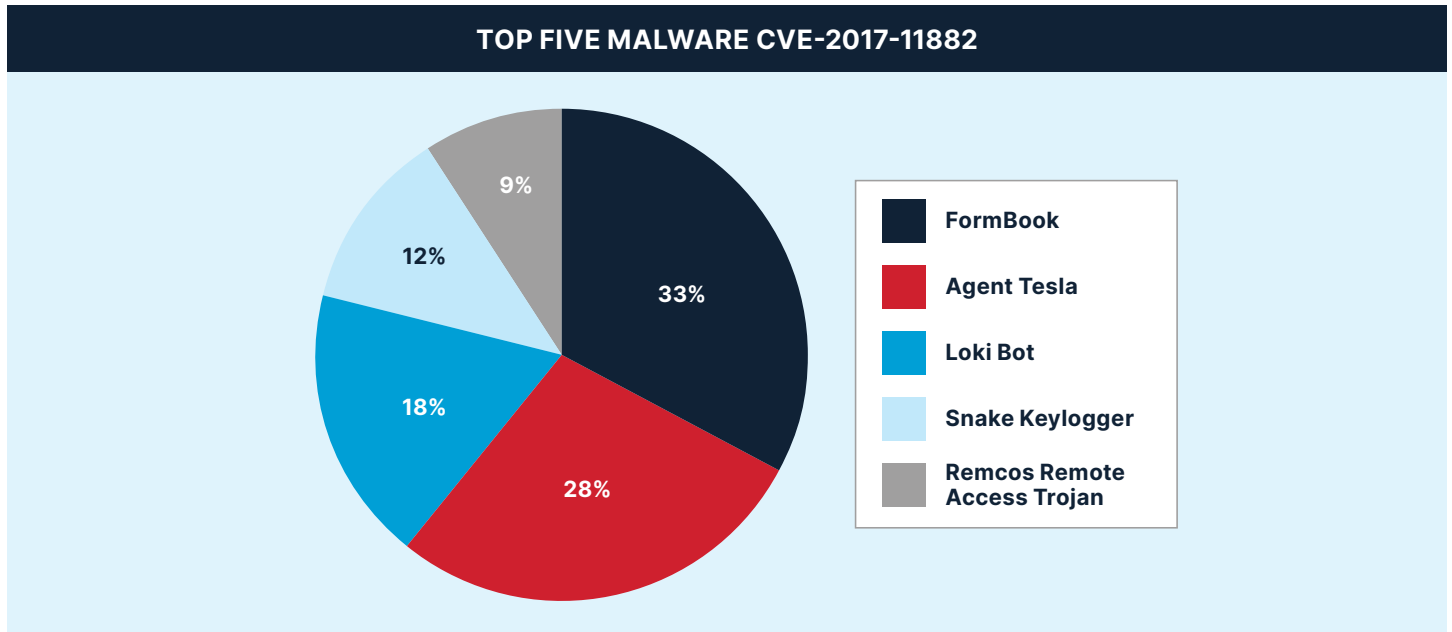


Figure 6: Top five malware families delivered by CVE-2017-11882.

The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) names CVE-2017-11882 as one of the top vulnerability's and most frequently used by state-sponsored cyber actors from China, Iran, North Korea, and Russia.



Domains and TLDs Used in Credential Phishing

Each quarter, Cofense Intelligence has analyzed 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. The use of compromised domains to deliver malware via embedded URLs increased by 25% in Q2.

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 use of compromised domains to deliver malware via embedded URLs increased by 25% in Q2.

RANK	Q1 2023	Q2 2023
1	amazonaws.com	myqcloud.com
2	sharepoint.com	adobe.com
3	google.com	sharepoint.com
4	backblazeb2.com	bing.com
5	microsoft.com	google.com
6	dropbox.com	dropbox.com
7	adobe.com	box.com
8	youtube.com	microsoft.com
9	box.com	vk.com
10	myportfolio.com	backblazeb2.com

Table 2: Q1 and Q2 2023 ten most common .com domains used in credential phishing campaigns.

Several of the top domains are almost always near the top, as they represent trusted services like Adobe, Microsoft, and Google, which are unlikely to be blocked by SEGs. Two new top domains made the top 10 list in Q2, myqcloud.com, a new cloud network platform and vk.com, a Russian social network. A less-common domain, myqcloud.com, made a sudden appearance in the top spot, accounting for 3.43% of .com URLs. The domain represents Tencent's content delivery network, and demonstrates how threat actors can make heavy use of even a relatively new trusted platform. Another new one made the list, Russian social network vk.com, as it was often used as a redirector in the high-volume SuperMailer campaigns in Q2.

Two new top domains made the top 10 list in Q2, myqcloud.com, a new cloud network platform and vk.com, a Russian social network.

Most of the TLDs used in credential phishing campaigns stayed at consistent volume from Q1 to Q2, as seen in Figure 7. TLD most used was .com at 48.1% of the total. URLs in the .ru TLD declined slightly after a sharp jump in Q1. The .me and .co TLDs appeared in the top ten for Q1 but were supplanted in Q2 by .dev and .site.

Domains and TLDs Used in Credential Phishing

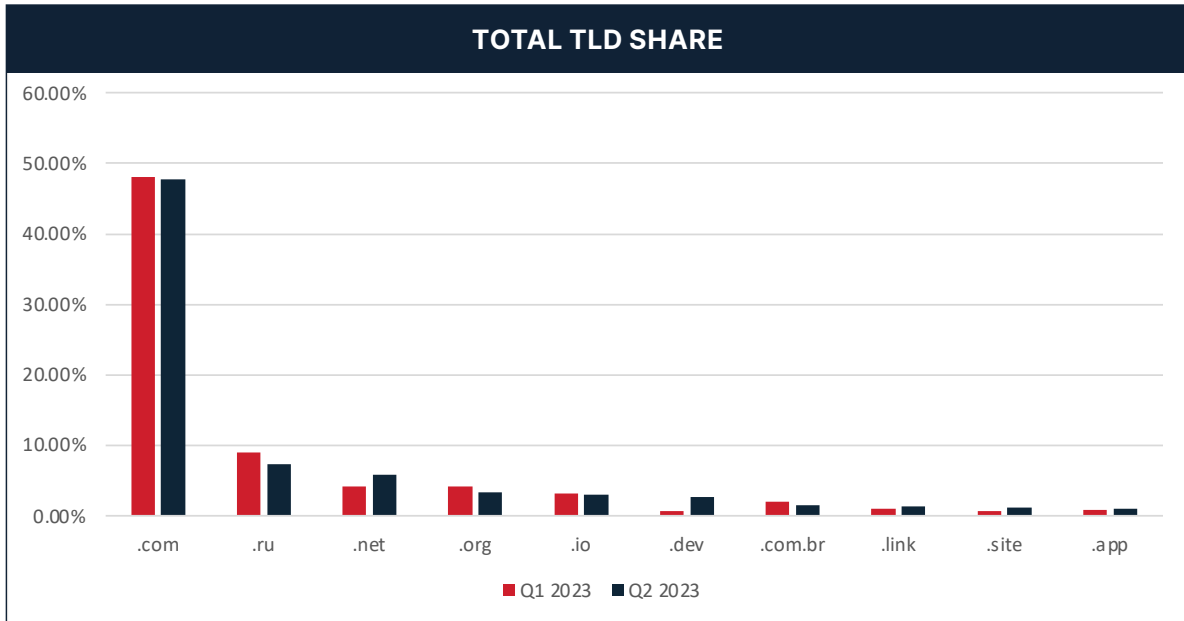


Figure 7: The top ten TLDs for both stages in Q2 2023, with Q1 totals for comparison.

TLDs used in Stage 1 were also fairly consistent with Q1 totals, as seen in Figure 8. Since Stage 1 URLs are included in phishing emails, threat actors tend to use domains that belong to trusted services, or otherwise appear legitimate when examined by SEGs or users. As such, despite a nearly 5% drop from Q1, .com domains still dominated in Q2 at just over 58% of the total. The .net domains climbed by almost 5%.

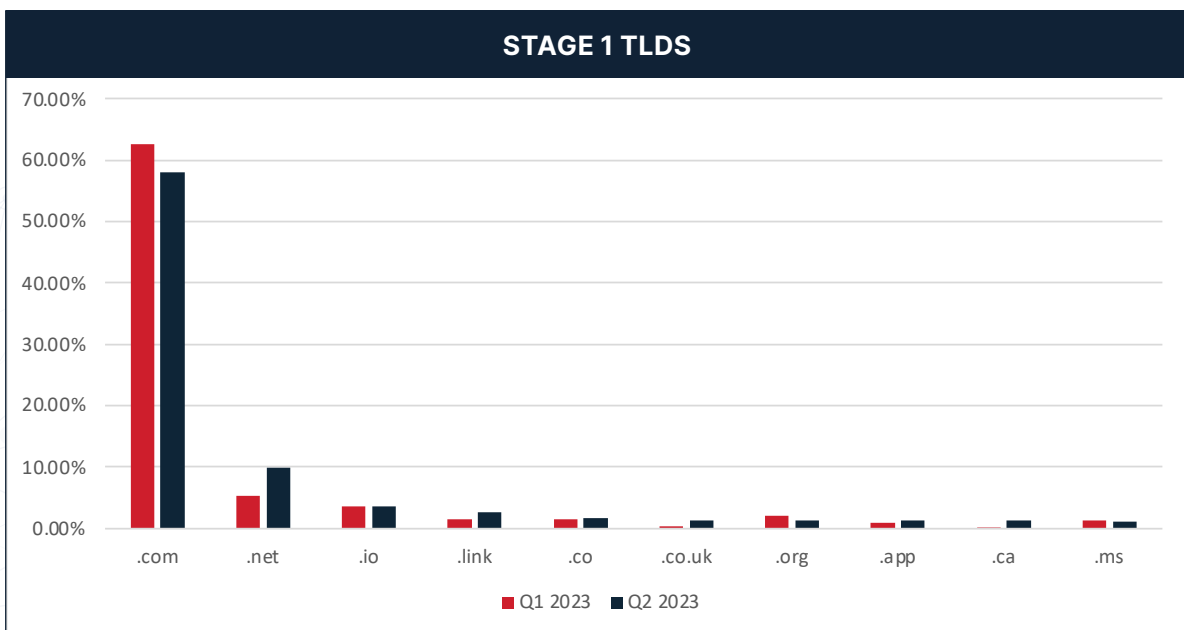


Figure 8: The top ten Stage 1 TLDs in Q2 2023, with Q1 totals for comparison.

Domains and TLDs Used in Credential Phishing

URLs in Stage 2 tend to be more diverse, since they are generally subject to less examination by SEGs or other security measures. The .com TLD is still on top at 41.7%, while .ru is still the second most common TLD, used in over 11% of Stage 2 URLs, as seen in Figure 9. Newcomers to the top 10 include .dev, .site, and .top, replacing .tk, .me, and .info.

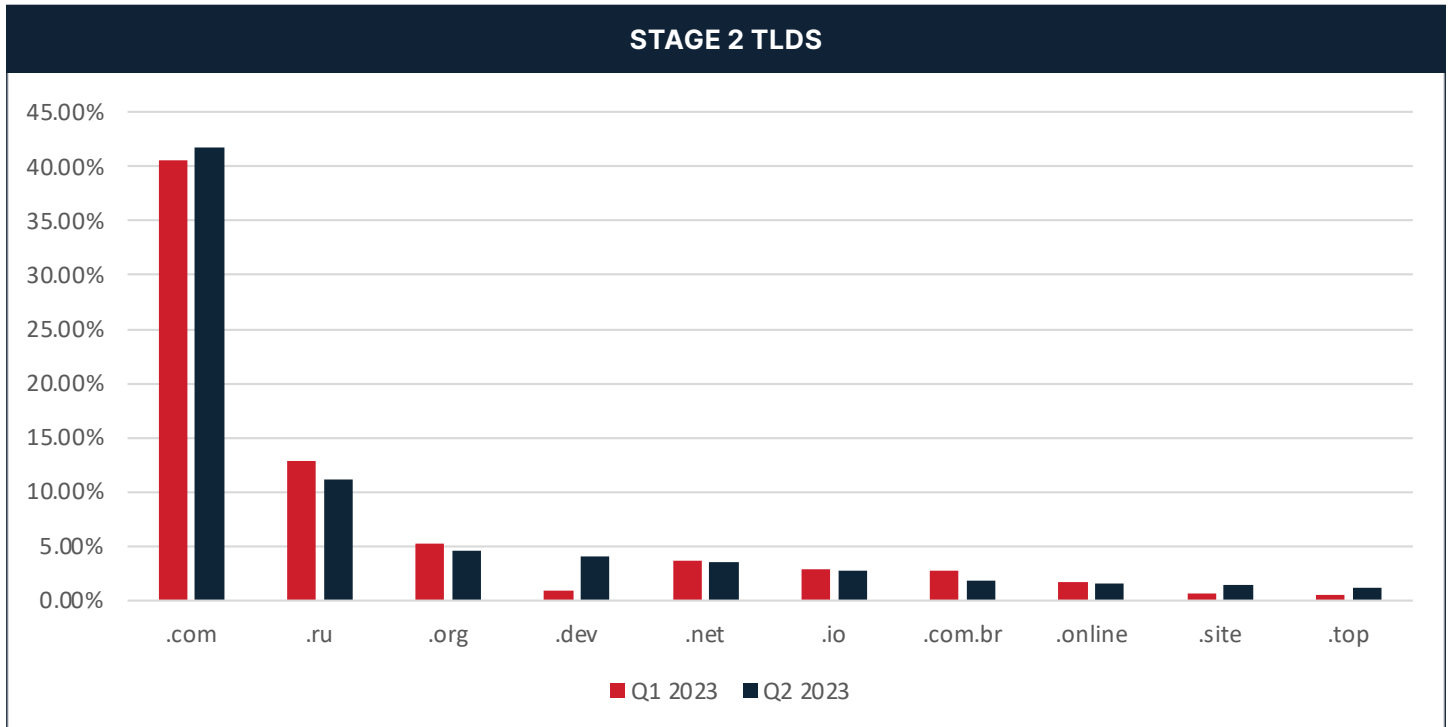


Figure 9: The top ten Stage 2 TLDs in Q2 2023, with Q1 totals for comparison.

URLs in Stage 2 tend to be more diverse, since they are generally subject to less examination by SEGs or other security measures.

File Extensions of Attachments

PDF documents represented the most common malicious attachment file extension abused 42.4% of all phishing attachments. Threat actors use PDFs with embedded links to a variety of malicious destinations or payloads, including credential phishing, QakBot, and NetSupport Manager RAT. The HTM and HTML file extensions together were second to PDFs, totaling 29.7%. Like PDFs, HTM(L) documents can be used to direct users to credential phishing pages or malware installers. They are also commonly used as self-contained phishing pages. Zip file usage increased slightly, as it delivered a variety of malware, usually with password protection. Malicious calendar invitations in the form of .ics files were not in the top file extensions in Q1, but the usage jumped to 3% in Q2, as seen in Figure 10. Malicious Office documents round out the list for Q2, with CVE-2017-11882 still regularly used as a delivery mechanism.

PDF documents represented the most common malicious attachment file extension abused 42.4% of all phishing attachments.

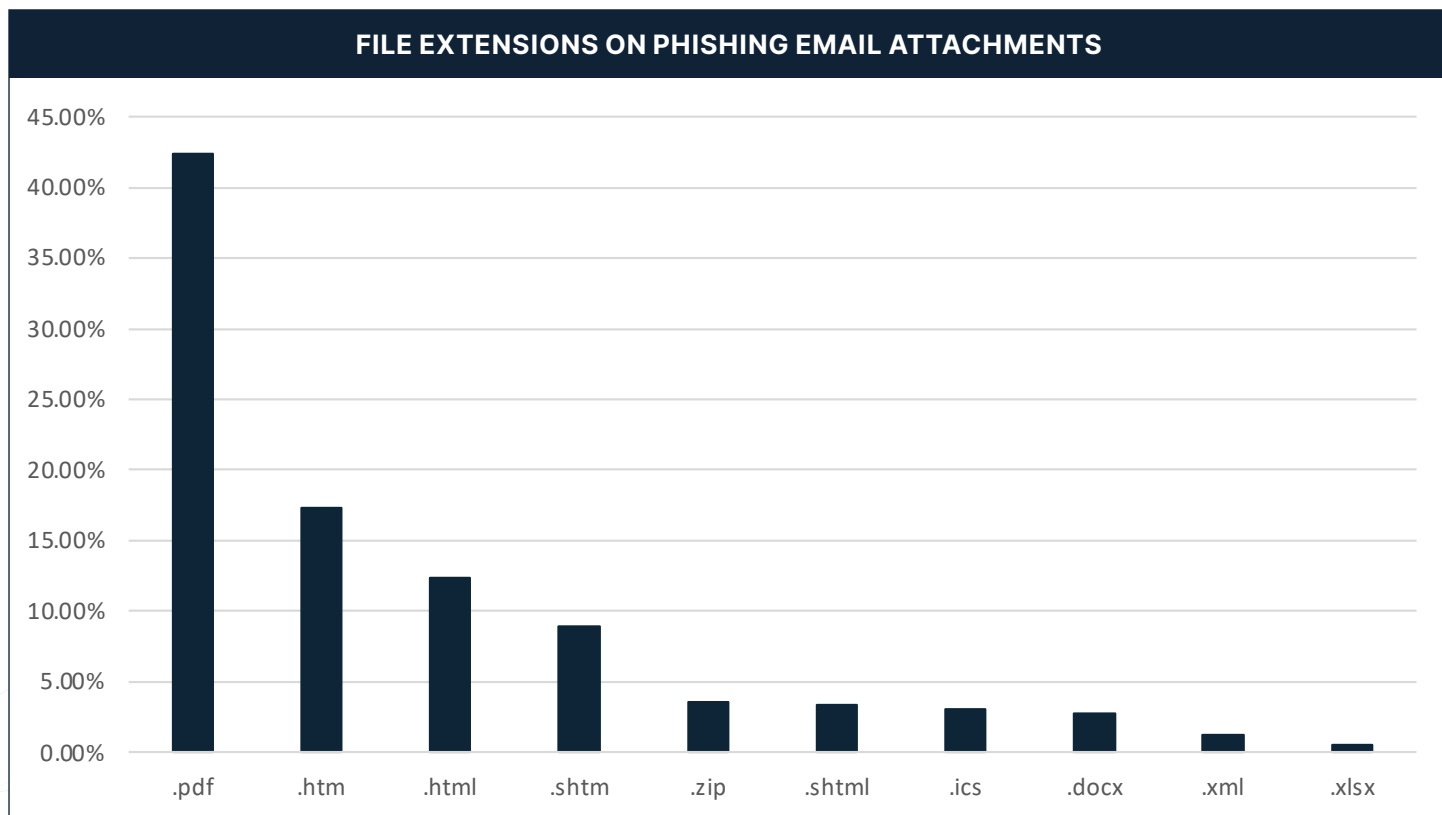


Figure 10: Top 10 most common attachment file extensions found in environments protected by SEGs.


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, often receiving information and exfiltrated data from infected hosts. The only significant changes between Q1 and Q2 were that C2 nodes increased slightly in Canada and decreased slightly in Great Britain.

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	68.60%	United States	69.73%
Great Britain	10.30%	Canada	10.79%
Canada	6.97%	Great Britain	8.13%
Germany	2.95%	Germany	2.11%
France	1.60%	France	1.61%

Table 3: Q1 and Q2 2023 percentages for C2 sources by IP address geolocation.



Tracking Command and Control (C2) servers provides insight into a range of malicious cyber activities across the globe.

Projections for Q3 2023 and Beyond

Tailored Content Makes Phishing Emails More Effective At Scale

In Q2 2023, we saw remarkable developments in phishing emails tailored specifically for targeted users or organizations. The operators responsible for the prolific SuperMailer-generated credential phishing campaigns used the software's template features to automatically craft emails featuring users' email addresses and organization names. Other threat actors generated unique images in each email, with similar user details rendered within the image. As threat actors hone their techniques, expect a greater level of detail in tailored phishing emails, even in high-volume campaigns.

Phishing Services Struggle to Maintain Momentum Under LE Pressure, Some Succeed

Individuals or small-scale operations dealing in credential phishing may be under increasing pressure from law enforcement and market forces. Authorities dismantled several notable threat actor marketplaces recently, including the Genesis Market in April and Breach Forums in late March. Without them, small operations will have a harder time connecting with customers. At the same time, certain prominent credential phishing services remain operational. Our recent Strategic Analysis highlighted the **Caffeine** service still running, although they no longer maintain a public website. Another service we've investigated, **BulletProftLink**, continues to run openly, apparently unconcerned with potential exposure to authorities.

Smaller operators may also have trouble matching the features offered by established credential phishing services, including tailored email content, bulletproof hosting, multi-factor authentication capture, and easy-to-use management of campaigns. In the long term, the legal risks and barriers to entry could drive credential phishing operators into more centralized, organized teams akin to the Conti ransomware organization.

MOVEit Vulnerabilities

The MOVEit vulnerabilities seen in Q3 were disastrous vulnerabilities that led to compromise in a number of systems and data theft for a number of organizations. Given the value of the systems compromised and the data stolen it is certain that threat actors will continue to attempt to exploit similar vulnerabilities in the future. They will likely continue to target processes that are considered to be vital to business operations so that compromise to those systems will be difficult to detect and harder to prevent. These attacks demonstrate the need for up-to-date actionable intelligence that reports even when legitimate processes are compromised.

Projections for Q3 2023 and Beyond

Use of Malicious PDF Attachments to Continue Growth

The past two years have seen growth in the number of PDF files among malicious file attachments, from 15% in Q2 2021 to over 40% every quarter since Q2 2022, as seen in Figure 11. PDF documents have several features that make them attractive as a delivery mechanism for malware or malicious links:

- PDFs can include images and formatting to make them appear more legitimate, which can be difficult to accomplish with content embedded directly in emails.
- Automated analysis of PDF files is more complicated than analysis of raw email content. Obfuscation, password protection, and other measures can further thwart defenses.
- In a business setting, legitimate PDF attachments are common, making malicious ones more likely to avoid detection.

The operators of QakBot have been quick to experiment with and adopt different delivery mechanisms in the past several months. Their use of PDFs in Q2 2023 signals that PDFs are effective as a delivery mechanism. Going forward, look for other threat actors to follow their lead.

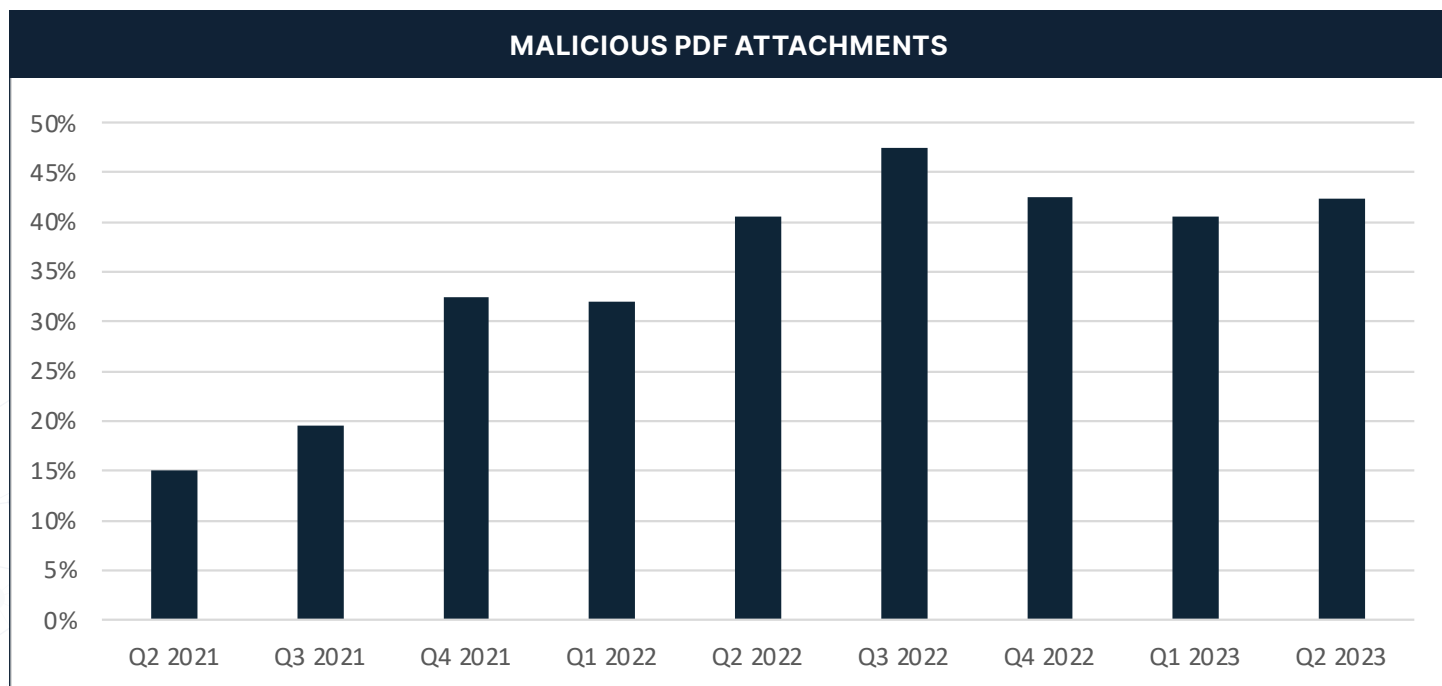


Figure 11: Share of ".pdf" among malicious attachment filename extensions over the last two years.

Finished Intelligence: Topics and Trends

Throughout Q2 2023, Cofense Intelligence performed in-depth analyses on various threats to provide readers with a strategic understanding of the phishing threat landscape and notify readers of sudden or upcoming developments. Below, we summarize finished intelligence reports that Cofense Intelligence produced on notable topics and trends identified during this period.

Strategic Analysis – Straight from the Source: Domain Spoofing vs Compromised Accounts Used in Evasive Phish

Threat actors try their best to make phishing emails look authentic. Simply spoofing a trusted sender email domain can get them part of the way there, but this tactic can also be simple to detect. So, what is a more convincing way for a threat actor to get an email through a Secure Email Gateway (SEG) and into the user's inbox? Actually, sending an authentic email from a compromised account at that trusted domain. A trusted domain is any domain name that is recognized and trusted by the recipient. It is not just the sender's address domain that is used to add to the believability and verifiability, but also legitimate domains within URLs used to distribute phishing content. Combined, these elements create legitimate-looking and trusted email, which allows the emails to reach inboxes, bypasses SEGs, builds trust with the user, and increases the chance of a successful attack.

Strategic Analysis – MitM Phishing Grows, Using Real Login Process to Steal Credentials

A man-in-the-middle (MitM) attack is an adversary's attempt to steal information by inserting himself between victims and their legitimate, expected destination. Threat actors combining credential phishing with MitM attacks have been another evolution in the threat landscape. In this context, rather than setting up one fake login page, the attacker lures victims to his web server, which will broker the entire authentication process between the user and the actual destination. If successful, threat actors can use the harvested usernames, passwords, and session cookies to gain access to a victim's account and even bypass multi-factor authentication.

While MitM credential phishing campaign volume was significantly above average from September 2022 to March 2023, leading to the publishing of this report, the volume declined sharply across Q2 2023, with 54% fewer campaigns in total, as seen in Figure 12 on the next page.

Finished Intelligence: Topics and Trends

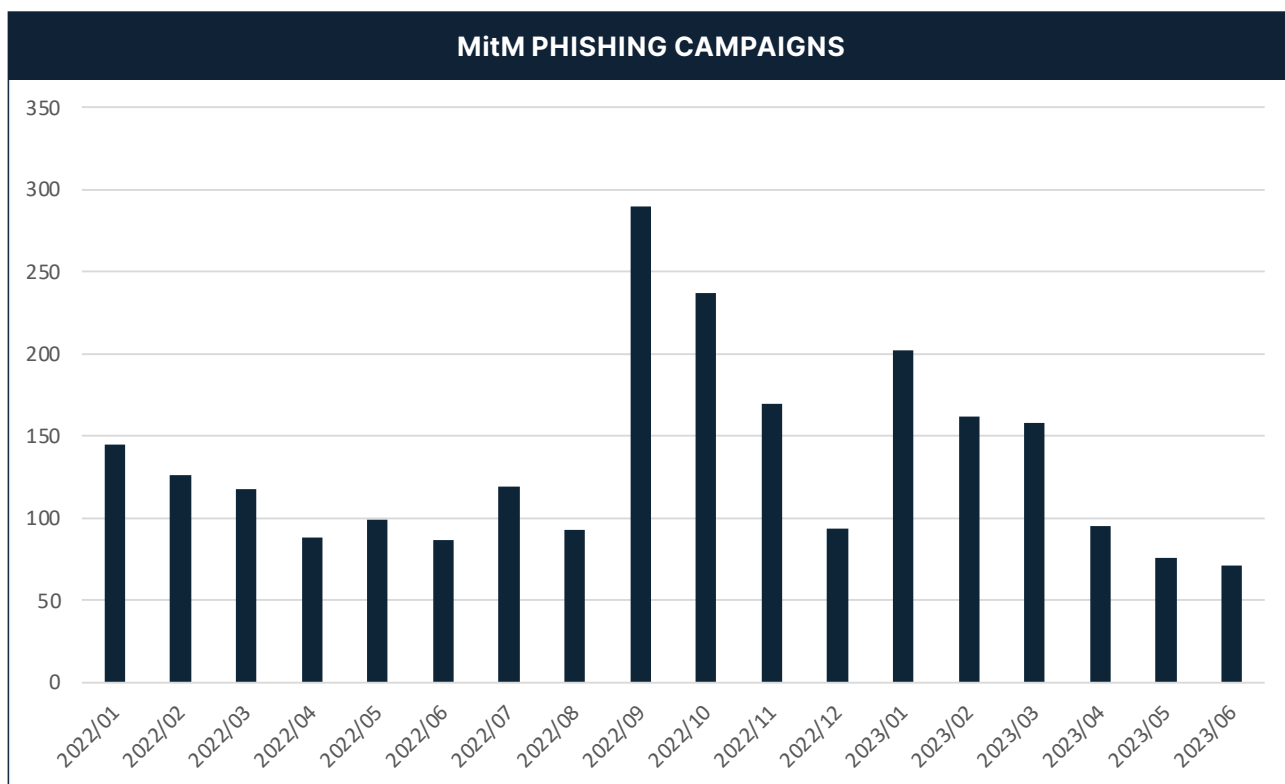


Figure 12: Updated monthly totals of MitM phishing campaigns since 2022.

Strategic Analysis – Threat Actor Mistake Reveals Extensive Phishing Campaign Abusing SuperMailer

In early 2023, an increasing number of credential phishing URLs in emails reported to the Cofense Phishing Defense Center (PDC) included a unique string, `sf_rand_string_lowercase`. The inclusion of the string is a mistake threat actors made when crafting credential phishing emails using a legitimate email newsletter program named SuperMailer. The error occurred in a small subset of what has turned into a high-volume credential phishing campaign. By combining SuperMailer's customization features and sending capabilities with SEG evasion tactics, the threat actors behind the campaign have delivered tailored, legitimate-looking emails to inboxes spanning every industry.

In our [Q1 Phishing Intelligence Trends Review](#), one of our projections for Q2 was that open redirects would spread further across credential phishing campaigns. The SuperMailer-based campaigns did exactly that, relying heavily on a wide variety of websites with open redirects as a way to make their Stage 1 URLs pass inspection. The volume of emails abusing SuperMailer stayed high through the end of May, peaking at 14% of total reported credential phishing volume, but started to taper off in June. Despite the decline, it still accounted for an impressive 6.2% of credential phishing emails reported to the Cofense Phishing Defense Center during the final month of the quarter. Note: Following the release of this Strategic Analysis report, we were able to identify previously unrecognized activity from March and April. This showed that the campaign was responsible for 9% and 10% of credential phishing activity in those months, respectively (compared to approximately 4% each in our original findings). Figure 13 on the next page is updated with the latest data.

Finished Intelligence: Topics and Trends

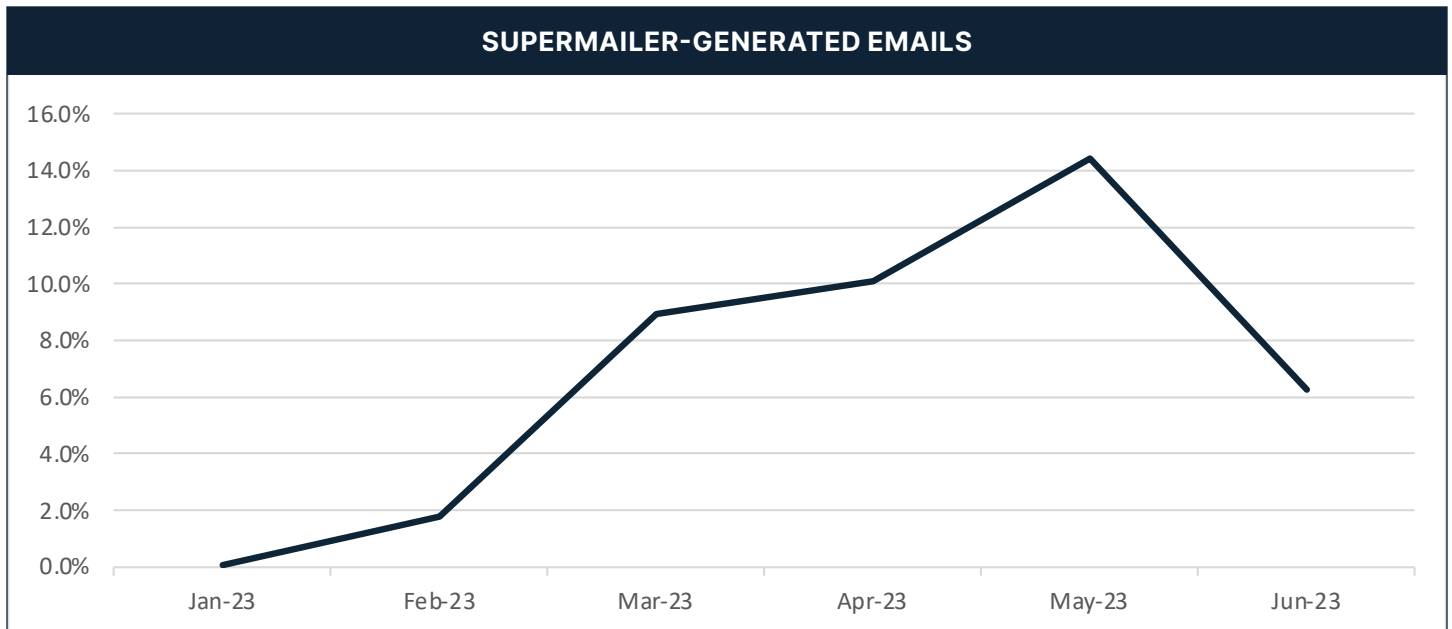


Figure 13: Emails from the SuperMailer-generated campaigns as a share of all credential phishing emails reported to the Cofense PDC.

Flash Alert – PikaBot Malware Now Reaching Enterprise Email Inboxes

A phishing campaign delivering a relatively new malware family called PikaBot was observed by Cofense Intelligence and the Cofense Phishing Defense Center in inboxes that are protected by secure email gateways. The PikaBot family was first identified publicly in February 2023, and started to proliferate via email in May 2023.

Strategic Analysis – Caffeine Phishing Service Domains, Patterns Still Heavily Used After Store Seemingly Defunct

An evolving set of credential phishing activity targeting Microsoft Office 365 credentials has been observed reaching enterprise email inboxes. This activity is categorized by several key components that make it stand out, including the use of "bulletproof" registrar R01-RU and the use of domains and patterns associated with the seemingly defunct "Caffeine" phishing service run by phishing kit maker MRxCODER.

Emails matching the indicators identified in our analysis peaked in March 2023, as seen in Figure 14 on the next page. Volume tapered off afterward, likely signaling that the service's operators changed tactics to use less detectable URLs, or that email security gateways began to identify and block associated emails.

The volume of emails abusing SuperMailer stayed high through the end of May, peaking at 14% of total reported credential phishing volume, but started to taper off in June. Despite the decline, it still accounted for an impressive 6.2% of credential phishing emails reported to the Cofense Phishing Defense Center during the final month of the quarter.

Finished Intelligence: Topics and Trends

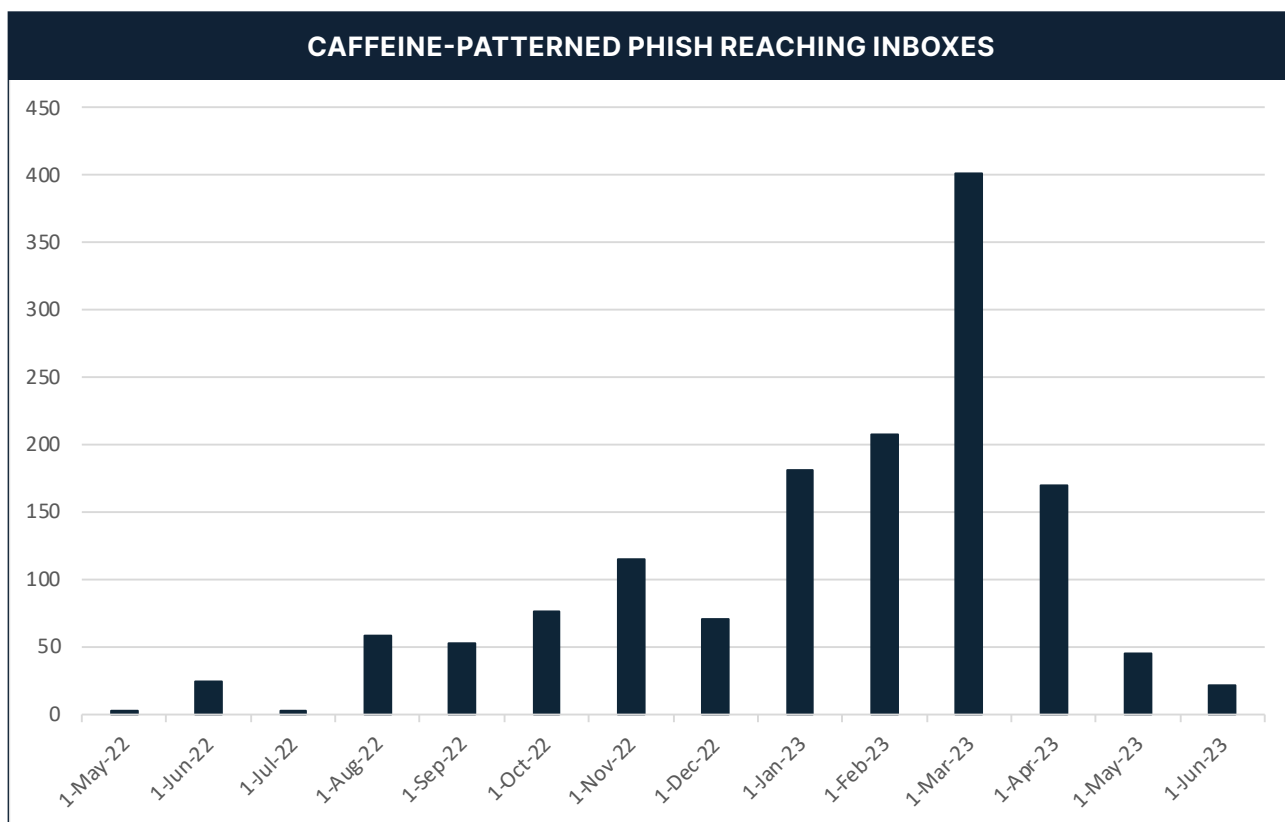


Figure 14: Unique URLs matching the “Caffeine” phishing service’s domains, reported by enterprise users.

Strategic Analysis – Compromised Domains Dominate Among Embedded URLs in Malware Phish

Domains hosting malware fall into roughly three categories: threat actor created, compromised, and abused. Threat actor created domains are domains created by a threat actor before a phishing campaign and are used in that campaign to deliver malware. Compromised domains are domains that have had some portion of their resources compromised and used to host malware. Abused domains are legitimate services, such as Google Docs, which are being abused to deliver malware. It is important for both network defenders and everyday users to understand the differences, how often each is seen, and to know what to look out for. Although the categories are consistent with those seen in credential phishing, the ratios and the makeup of the domains are different. Compromised domains are the most common for use in malware delivery at 51%, followed by abused domains at 39%. Intentionally created malicious domains accounted for the other 10%.

Compromised domains are the most common for use in malware delivery at 51%

Strategic Analysis – Remcos RAT – Phishing Malware Baseline

Remcos (an acronym for “Remote Control and Surveillance”), is a RAT which provides an attacker the ability to remotely manage an infected system. Remcos allows threat actors to run keyloggers, take screenshots, exfiltrate files, dump credentials, upload other malware, and more. It was first advertised in hacking forums in July of 2016. Since then, more functionality has been added over the years to provide stable access to remote systems.