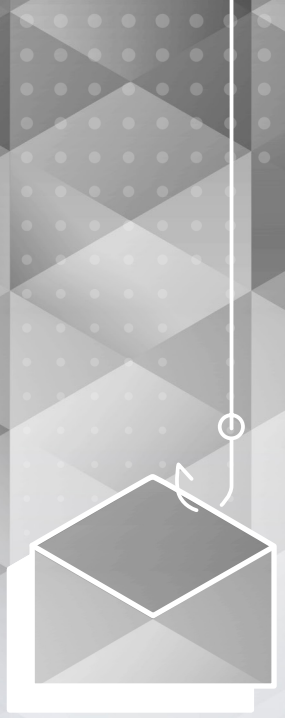
VIPRE SECURITY GROUP



Email Threat Trends Report: 2023: Q3

PDF Popularity, Callback Phishing and Redline Malware.

Content

Introduction

Overall, it's no surprise that threat actors are getting consistently, if not moderately, better at launching email-based attacks that steal our data.

VIPRE's AV Labs keeps a finger on the pulse of the email security industry, and we are proud to put out our third consecutive Email Threat Trends Report this year. After ingesting a billion emails, and then some, we feel it our responsibility to share what we've noticed about the trends specific to this attack vector and how you can stay safe.

Knowledge is power, and knowing what dangers lie on the horizon makes all the difference when it comes to securing your organization's email landscape in Q4 and beyond.

Key Trends

When dissecting our Q3 data, there were a couple of key trends that stood out.

Threat actors are increasingly hiding malicious links in Google Drive and other cloud storage spaces, and QR codes are continuing to pick up steam as attackers leverage our willingness to click into the unknown. PDFs have grown in popularity as a malspam delivery tool, and cybercriminals are leaning into low-tech options like Callback phishing and user-friendly Redline malware.

ChatGPT continues to improve phishers' abilities to dupe us, and LinkedIn Slink has proven an unforeseen malicious workaround. And of course, billions of dollars in and BEC shows no signs of stopping now.

From a defender's perspective, some links don't prove malicious until sandboxed and investigated further, and VIPRE AV Labs tools detected ten percent more nuanced threats with Link Isolation than the quarter before.

Additionally, heuristics is doing some heavy lifting when it comes to catching spam emails en masse. Combined heuristics approaches (Yara Rules) detected roughly ten times more instances of spam than did a comparable signature-based detection approach that used strings or phrases of known spam emails.

Ultimately, we circle back to the trend of doing more with less. It would seem attackers are shooting low when it comes to technical sophistication - not high - and the Q3 figures would indicate that it's working. Clever Callback phishing and BEC schemes don't need to fool advanced cybersecurity tooling, after all - they just need to fool you. And as the Verizon Data Breach Investigations Report reminds us every year, upwards of 74% human error rates indicate that we are still incredibly fallible.

Cloud Storage **QR Code**

Attack Trend

Phishers increased use of
ChatGPT and AI

74%
HUMAN ERROR RATES
indicate that we are still incredibly fallible

What kind of emails are being sent?

Overall, we processed between 1.6 and 1.8 billion emails this past quarter, giving us a fair sample size to draw from. Of those nearly 2 billion emails, over 200 million (233.9 million to be exact) were malicious.

One in every ten emails we scanned were bad, and that's just in the past few months. Thankfully, over 11 million of those were protected by VIPRE's Link Isolation, a tool that checks the origin of an email-embedded URL before routing you there - every single time. That's over one million more malicious emails detected that way than in either Q2 or Q1, despite the fact that the total number of malicious emails remained basically the same; just a little over 200 million each time. This data supports the claim that cybercriminals are trending towards foul links that require ever more investigation to uncover, possibly because current signature-based investigation tools are now so effective (and ubiquitous) that threat actors are forced to either contrive a way around them or get caught.

Digging into those nefarious 233.9 million emails, 110 million were detected due to content and 118 million were detected due to links; a pretty even split. After that came attachments at 5.44 million and never-before-seen behaviors at roughly 150,000. While this number looks comparatively low, it is not insignificant. Without attachment sandboxing, these 150,000 emails would have released previously unseen exploits on organizations that would have had no context with which to fight them. Barring the entry gate – email – is often a faster, easier, and more cost-efficient solution than opening Pandora's attachments.

Without attachment sandboxing, 150,000 emails would have released previously unseen exploits on organizations that would have had no context with which to fight them.

Feature: Attachment Sandboxing

Basic email protection solutions alone would have let 150,000 malicious attacks go undiscovered and free to cripple companies.

Attackers are spinning up new exploits everyday, and some of them are bound to hit your inbox. When they fall outside the range of known-bad, organizations are left without defense. In an effort to evade savvy cybersecurity tools, attackers use these never-before-seen behaviors to slip through scans and arrive without red flags. Users protected by these basic email protection tools alone will never know the difference, and that could have been the case 150,000 times over this past quarter if it wasn't for VIPRE's Attachment Sandboxing.

With attachment sandboxing, users are able to send all attachments to a safe place for vetting before risking exposure to whatever might be inside. VIPRE Attachment Sandboxing tracks system data like network activity, changed files, and registry keys in order to provide a multi-vector assessment of whether the unidentified attachment ranks as No Risk Found, Suspect, or Malicious.

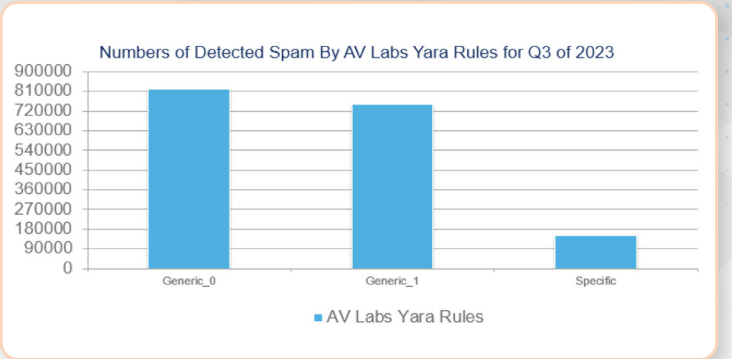
Now let's look at those 11.2 million clicks protected by Link Isolation. Of those, nearly 70,000 were detected at click time, meaning that these malicious links managed to evade all other detections and were only detected by sandboxing the link once it was clicked. Without Link Isolation, how many of these would have simply led unwitting users to a seemingly benign web page, only to dupe them in the process?

Diving deeper, 89% were detected due to content – bad links and attachments discovered upon arrival – and 11% were only discovered due to DeepLink, another VIPRE technology that analyzes webpage behavior before giving the okay. DeepLink enhances LinkIsolation, allowing it to perform deep, cloud-based scanning to analyze URLs further, even providing screenshots and previews of malicious URLs.

As attackers are getting better at hiding phishing links, further investigative technology is needed to root them out. These particular solutions proved critical this past quarter at finding seemingly innocent links that routed users to pages with suspicious behavior, flagging them and providing a sanitized version instead.

Spam highlights

Using heuristics, AV Labs Yara Rules were able to identify over one million spam incidents between two different subsets. Legacy heuristic rules caught 810,000 and new heuristic rules pulled in an additional 72,000 plus. By comparison, traditional signature-based approaches just caught a little over 150,000. With rampant phishing-as-a-service and new malware models being spun up in record numbers, signature-based detection tools are falling behind and solutions are needed that can make an educated guess. As the numbers show, it pays off.



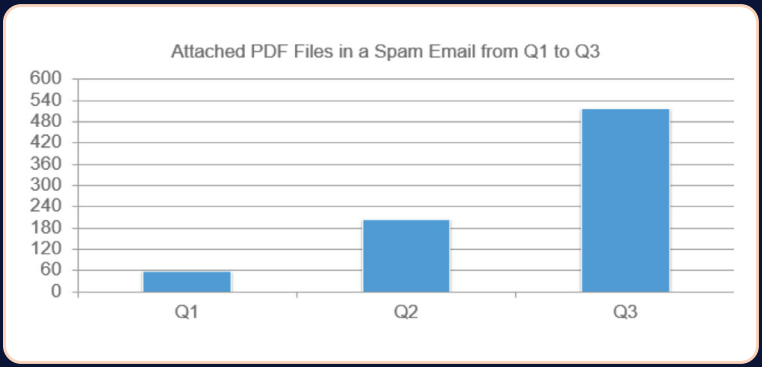
Speaking of analyzing behaviors, another interesting attack trend was that there were less attack emails this quarter than the two quarters before. Are email security tools just doing their job? Sure. But cybercriminals are doing theirs, too, and we can anticipate that a quiet Q3 lull means heavy holiday spam traffic in the quarter to come. Expect the usual onslaught of holiday spam, package delivery scams, and maybe even AI-spawned phishing emails from your favorite online retailers. That being said, this quarter still saw 93% of all emails ingested by VIPRE AV Labs turn up as malicious. Not bad for the slow season.

In terms of content, the spam emails this quarter were primarily made up of scams, half of which were classified as Business Email Compromise (BEC). According to the FBI's 2022 Internet Crime Report (IC3), BEC total adjusted losses ($2.7 billion) outweighed those of ransomware ($34.3 million) by a factor of 78 times. It's no wonder threat actors continue to pour resources into it, and the specifically crafted phishing emails that serve as bait are only more crafty with AI. Following scams, commercial emails and phishing proper took second and third spots, respectively.

Feature: PDFs as an Attack Vector

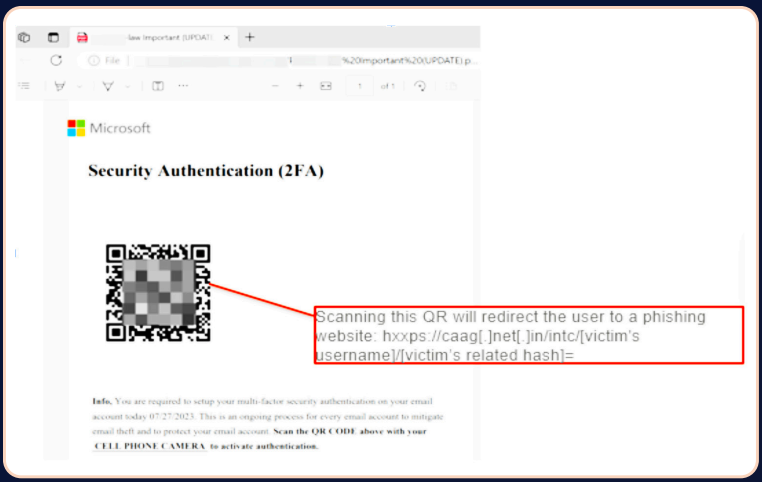
We've all attached PDFs to emails, and we've all received them that way, too. And cybercriminals count on it.

That's why this popular file sending method is being co-opted as one of the upward trending email attack vectors this quarter. The numbers of attached PDF files in a spam email have more than quintupled since Q1 of this year, and the pattern is unmistakable. One of the reasons PDFs prove a popular method of attack is because malicious hackers can make us think there's payment-related information inside. And there is, just not in the way we'd think. Once opened, the PDF could contain a link to a malicious page or release malware all its own.

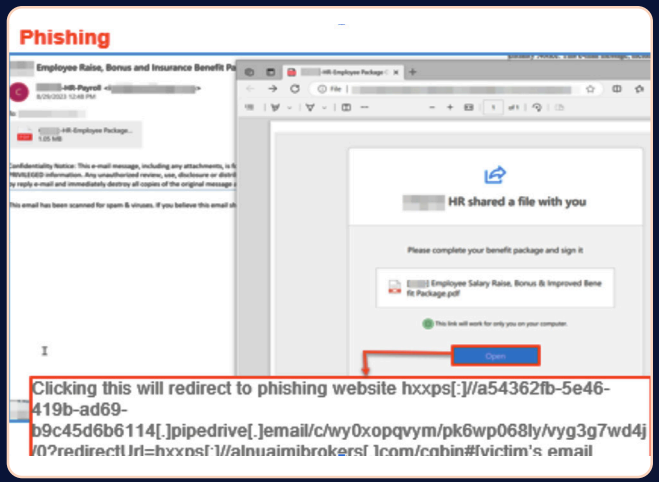


On the technical side, a majority of devices and operating systems have an integrated PDF reader. This universal compatibility across all platforms makes it an ideal weapon of choice for attackers looking to cast a wide net. We discovered malicious PDFs are typically used in one of three ways:

1: A vehicle for QR codes



2: A way to deliver malicious links (largely) undetected

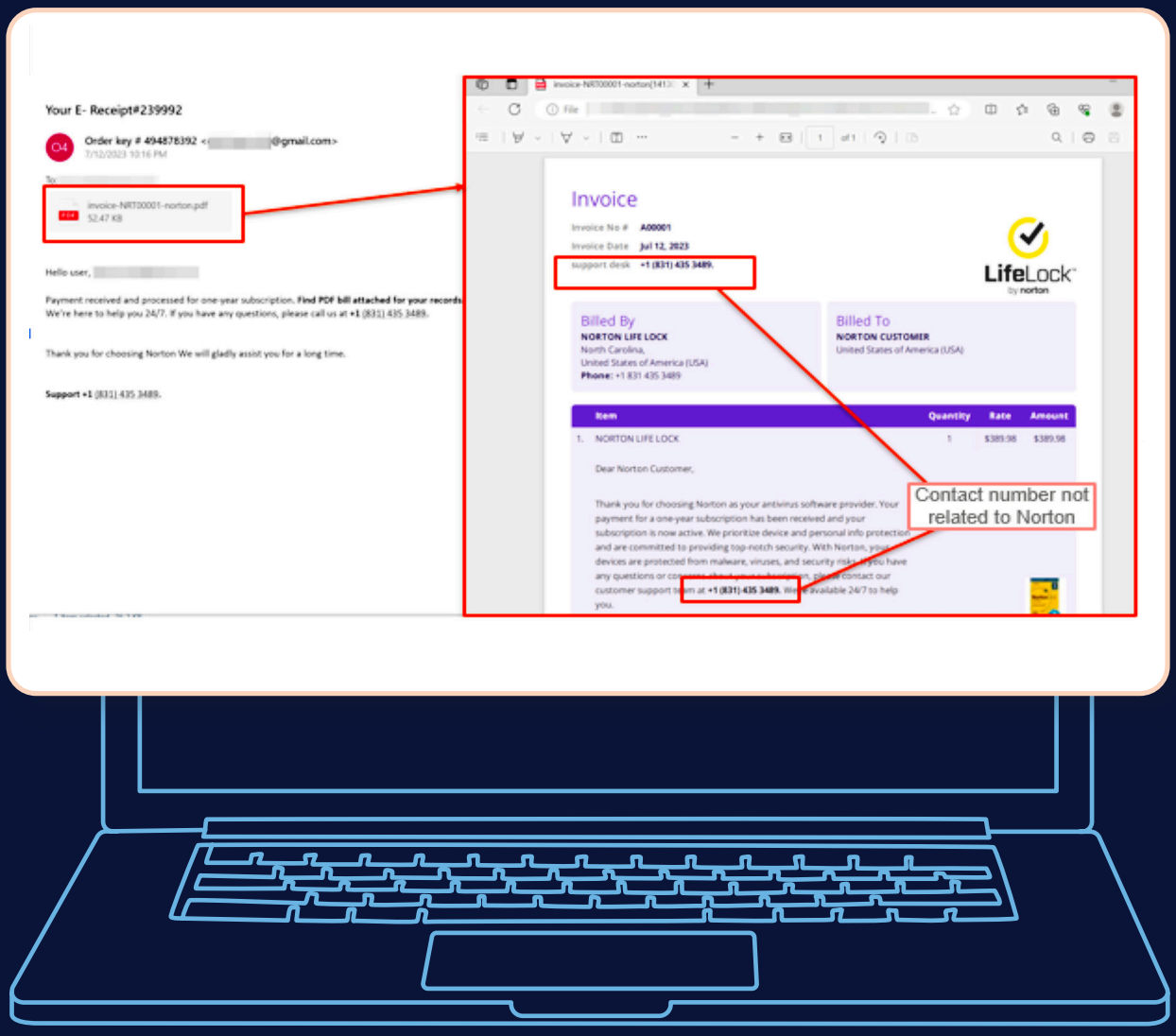


3: As attachments in Call Back phishing attempts...

Feature: Callback Phishing

This type of phishing scheme has a surprisingly low-tech bar to entry. Sometimes, no malicious links are even involved until the person engages.

Callback phishing is when cybercriminals send an email to an unwitting employee, posing as a service or product provider. Instilling urgency, it will prompt the customer to "call back", leaving a phone number to do so. Once the user calls in, they are duped out of their information over the phone, or they are given "sign in" links to verify information and end up losing sensitive data in the process. The absence of malicious files within the content of either the email or attachments makes it easier to slip past the radar and evade detection.



Business Email Compromise (BEC)

Have you ever read this in an email?

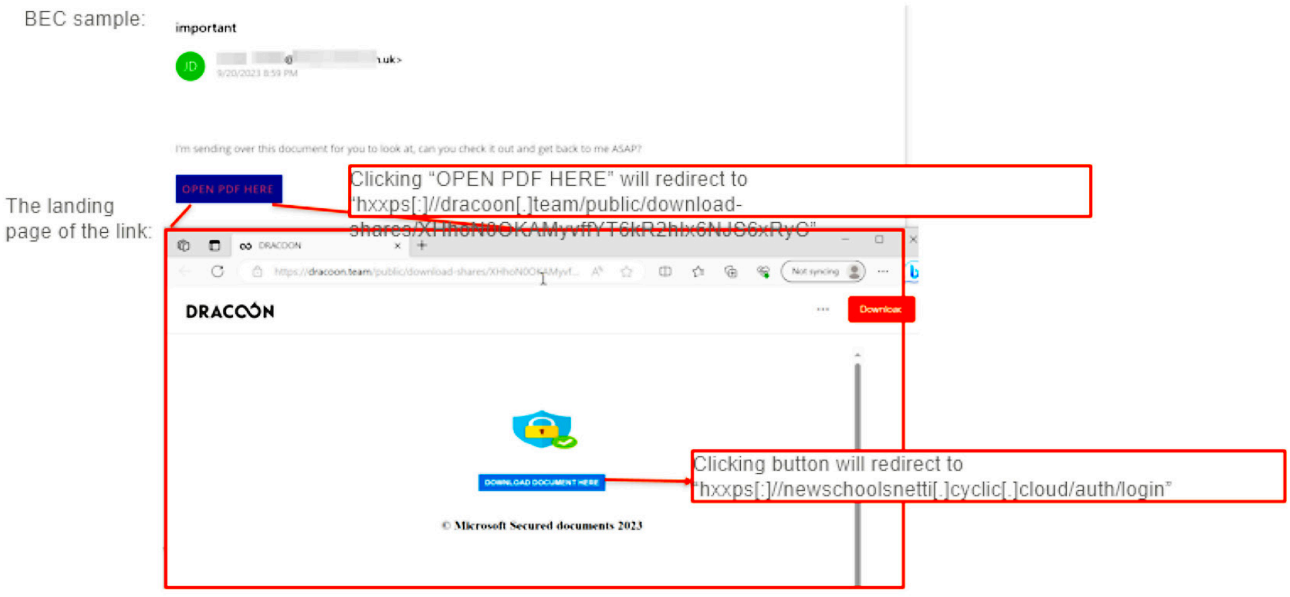
- Did you get my previous email?
- Drop me your phone number...
- I need you to take care of something for me.

From someone like a:

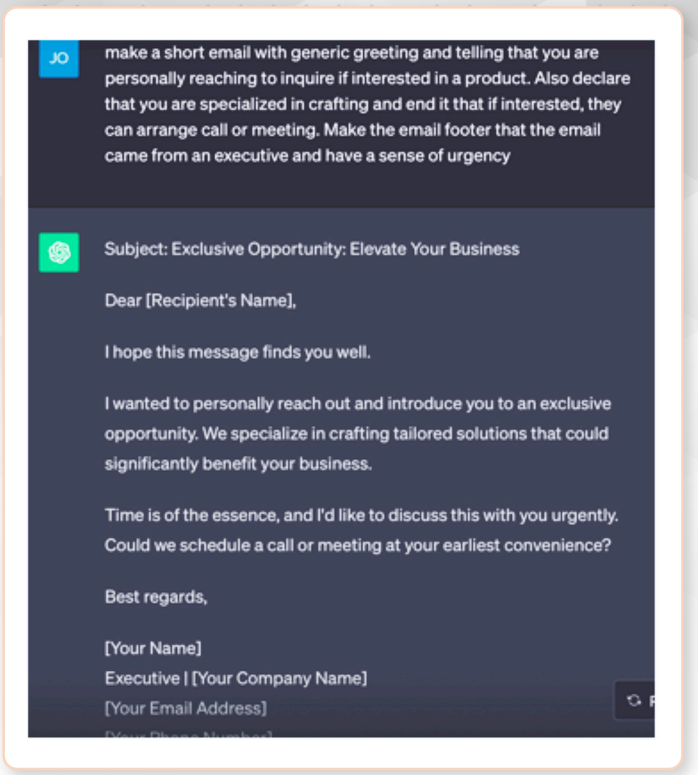
While it may have been legitimate, phrases and senders like these make up the profile of a typical BEC scam. As noted in the FBI's 2022 IC3 report, there were a staggering 21,832 complaints last year about BEC alone, and this method continues to be a favorite.

Tides are shifting, however. Now, BEC emails are including malicious links in the text, and AI has made it easier than ever for more customized, convincing BEC phishing emails to be sent out by increasingly amateur threat actors. This democratization of such an intense form of cybercrime has served to skyrocket the numbers even further, sending damages into the billions.

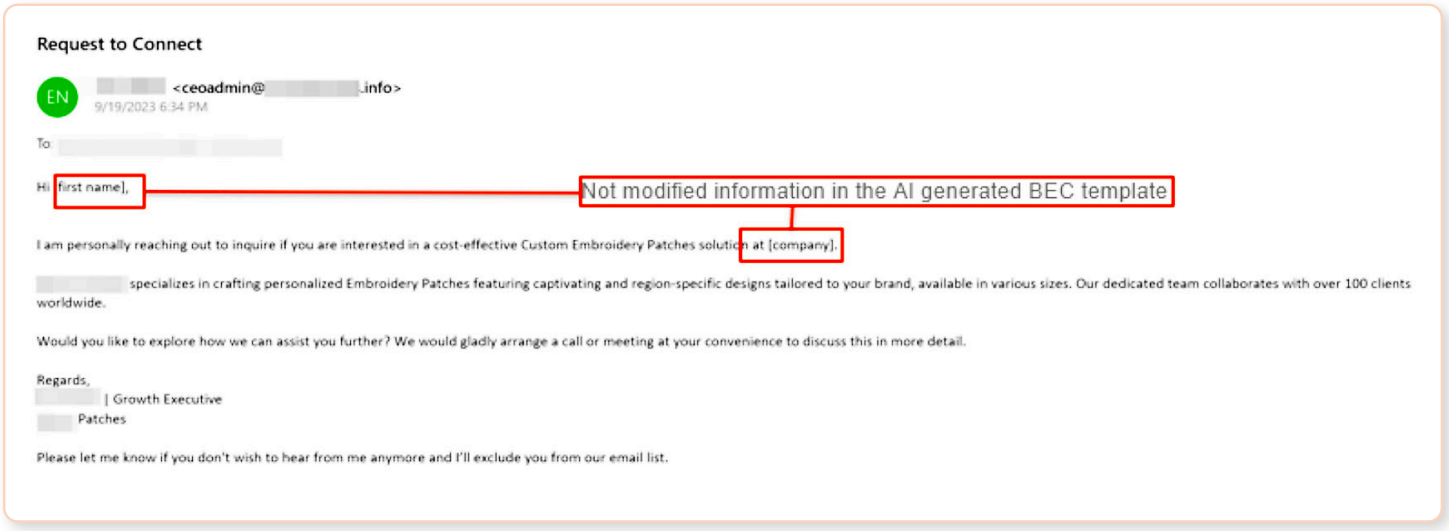
Business Email Compromise (BEC) emails that include links in their content:



Here is an example of a ChatGPT-generated email that could be used for BEC purposes. While generated ethically by VIPRE AV Labs, these are the kinds of emails a user might very well see:



As are these; AI created templates that leave in critical tell-tale markers like “name of target victim”.



While some are crafty and others are humorous, the fact remains that BEC persists as a viable cybercriminal email ploy that is only expanding its reach through new technology.

Phishing

What's important to note in this quarter's phishing trends is that QR codes are taking a more prominent role in this type of social engineering, and that passwords still reign supreme.

The end-goal of most phishing attempts is still to steal your password, typically through requests for changes or updates.

This is evidenced by the prevalence of these common phishing phrases found in Q3:

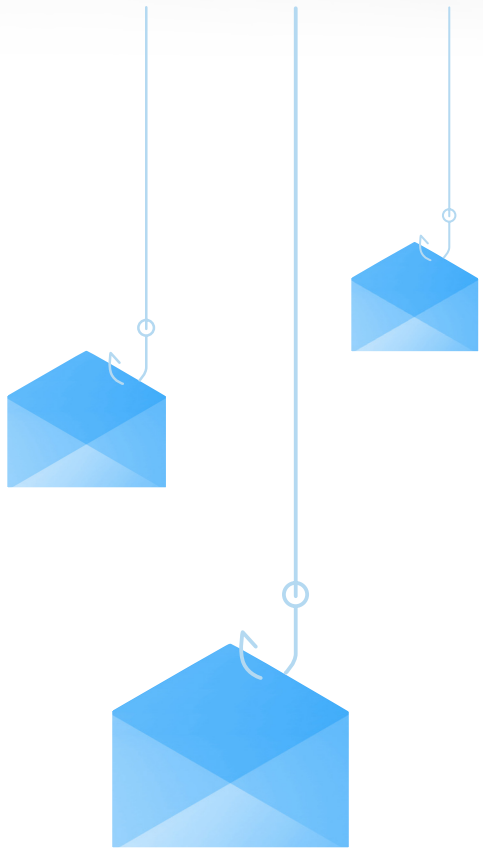
- **2FA Review Update**
- **Click below to change password**
- **Your password is set to expire**
- **Keep current credentials**
- **Update your email account**

And countless permutations of the above.

QR codes are notably on the rise, as well, making the list for the first time in our Q3 report. Out of the gates, QR code-based phishing emails accounted for a full ten percent of the total phishing emails we received this quarter. It's clear that as technology is changing, threat actors are eager to exploit its potential for creative and nefarious purposes. But beyond that, as we become desensitized to requests for online interaction, routine asks for password updates, QR code scans, and other forms of digital engagement become dangers too familiar to see.

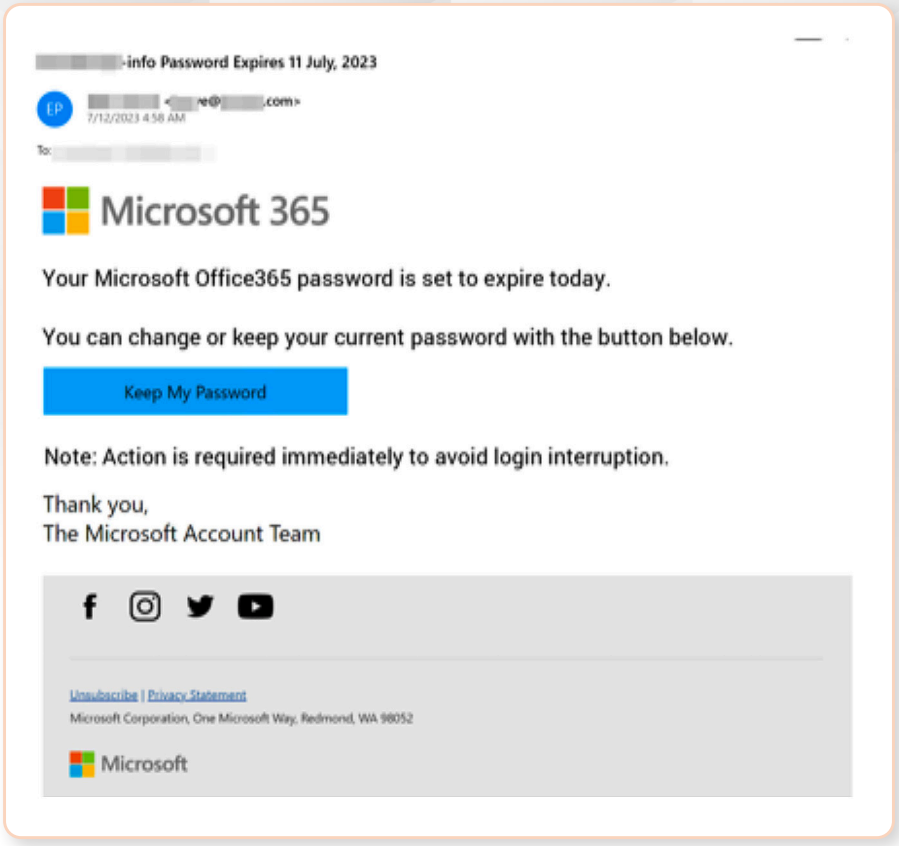
Threat actors are counting on this, and their tactics reflect it.

That familiarity plays off popular brands as well, and Microsoft remains the most spoofed name in Q3. Following are Google and Dropbox, a slight departure from Q2's Apple and DocuSign.



Even knowing all the facts, it's easy to be duped. Phishing emails are convincing because of their innocuous nature.

Take this password update request from "Microsoft", for example:



And as always, be wary of these most common Top-Level Domains (TLD) used by phishers to blend in with the digital crowd and not arouse suspicion in your inbox:

- **.com**
- **.org**
- **.uk**
- **.edu**

What matters more than the TLD is the nature of the link itself. Phishing links this quarter fall into four categories.

Most used:

1. **URL redirection** or the practice of sending a user to a malicious web page
2. **Compromised websites** or legitimate websites that have been riddled with bad links and malware
3. **File storage** URLs (like Dropbox and Drive)
4. **Newly created domains** – or ones too fresh to have established a rap sheet

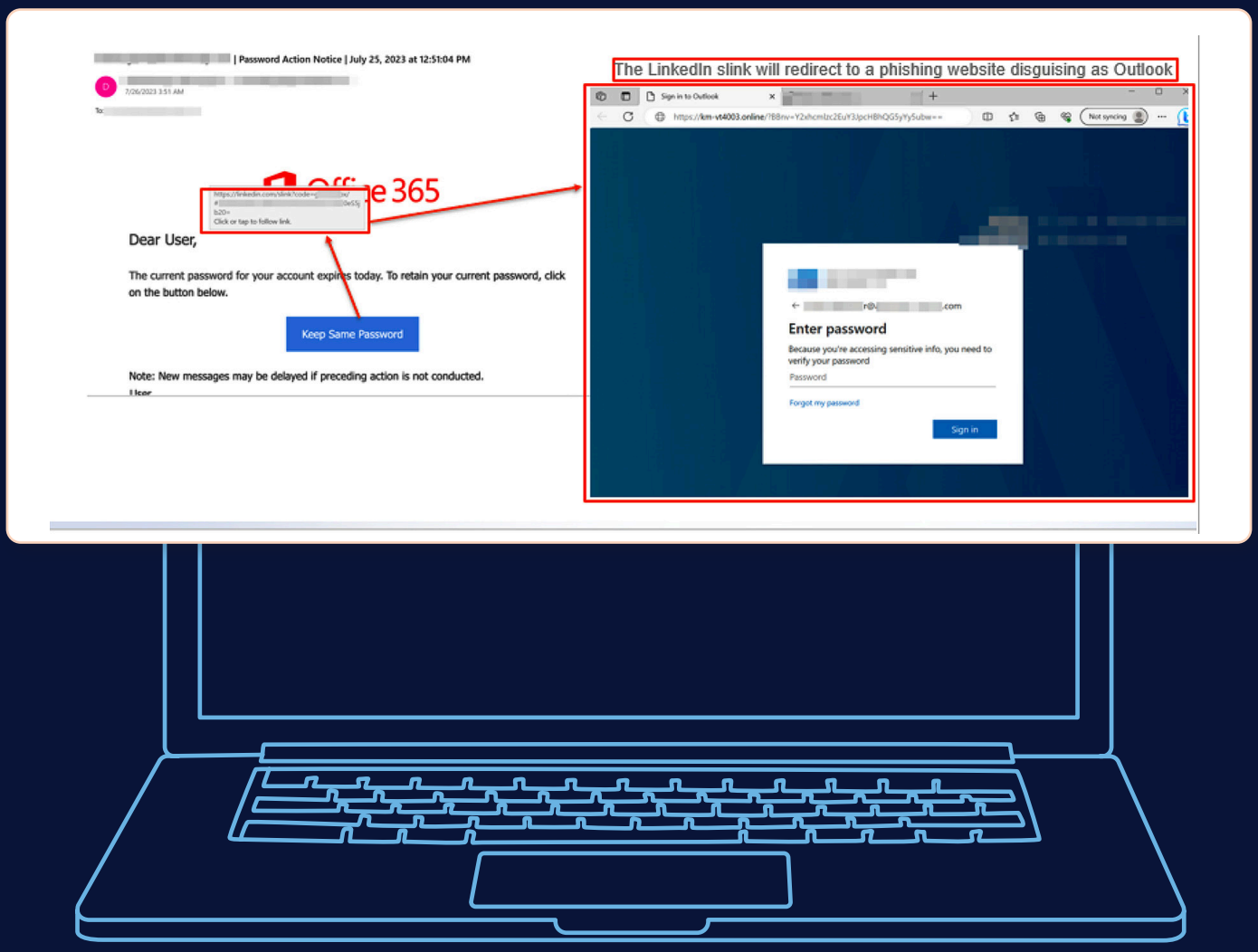
While much of this can be expected, two new trends we noticed in Q3 were the utilization of LinkedIn Slink for URL redirection and the incorporation of file storage links like the InterPlanetary File System (IPFS). We'll investigate those in further depth.

Feature: LinkedIn Slink for URL Redirection

To allow its platform users to better promote their own ads or websites, LinkedIn introduced LinkedIn Slink ("smart link").

This "clean" LinkedIn URL (formatted "https://www.linkedin.com/slink?code=" plus an alphanumeric string) enables users to redirect traffic directly to external websites while more easily tracking their ad campaigns. While useful, these types of links slip through the net of many security protocols and have thus become a favorite of social engineers.

Here's an example of a LinkedIn Slink exploit caught in the wild:

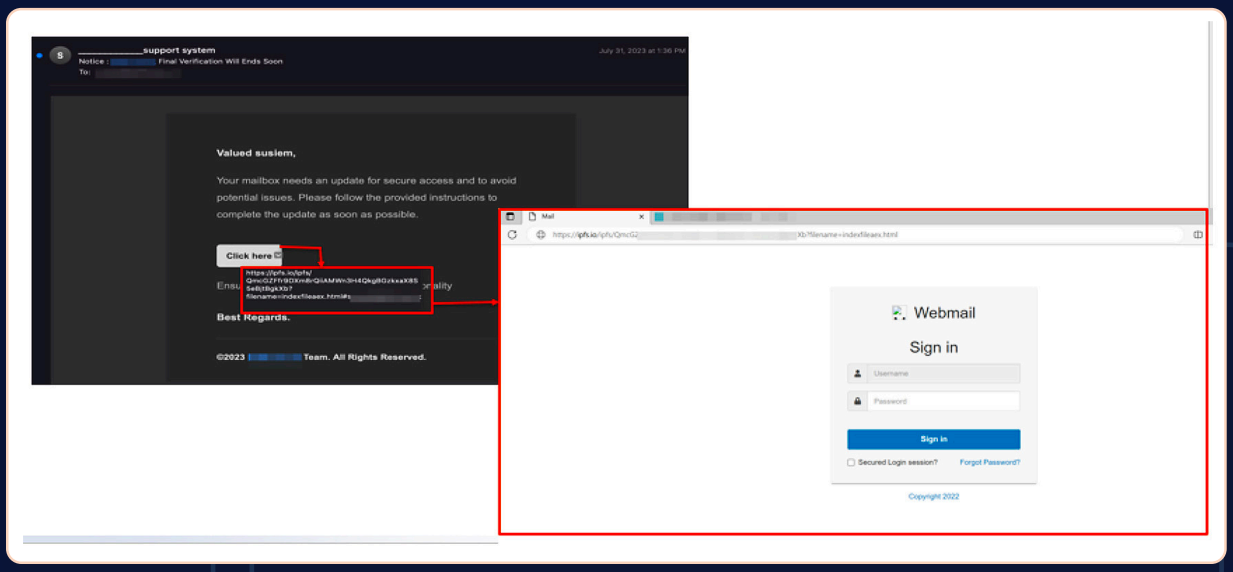


Feature: Vehicle for Malware

Exploiting the InterPlanetary File System (IPFS) is nothing new for scammers, but it is nonetheless widespread and worth noting.

A decentralized, peer-to-peer file sharing system, the IPFS is the perfect place for storing malicious HTML files with phishing forms embedded inside. The best part is that gateways can be employed as proxies so even users without an IPFS client can still be redirected there via links in everyday phishing emails. Remember – don't click the links. Or, have a URL sandbox if you do. You never know what's on the other side.

Here's one example of what an IPFS phishing scheme can look like:



And another, even trickier one:

Malspam

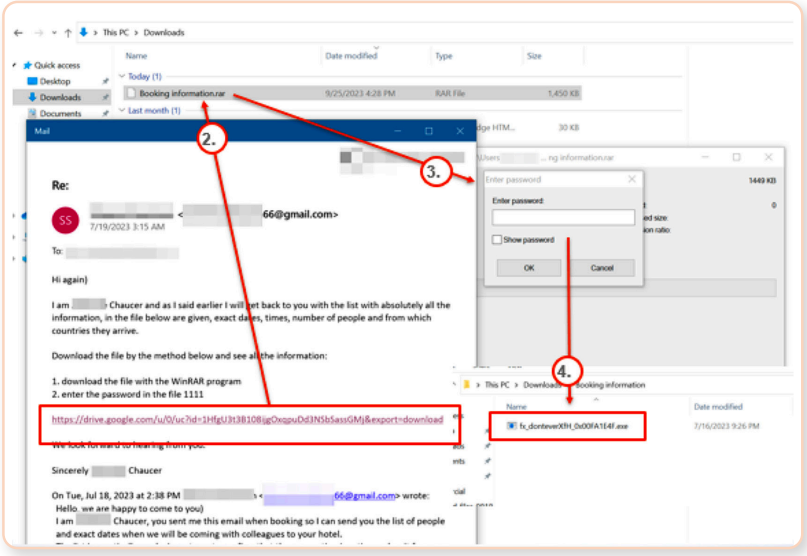
When it comes to malspam, the majority of threat actors still favor link-based delivery (58%) over attachments (42%). Beyond that, there are two primary methods of choice.

One is directing users to cloud storage platforms like Google Drive, and that accounts for two-thirds (67%) of malspam delivery. The other third (33%) uses legitimate websites – ones that won't trip a detection sensor - and compromises them, making them hosts and distributors of malware.

Malware delivered via Google Drive

Google Drive is a convenient, centralized location for hiding malware and a great watering hole for unsuspecting users. Cybercriminals can stuff docs full of malicious links and click to download malware that otherwise wouldn't make it through traditional email protection solutions. That's why finding an email security platform that can isolate, quarantine, and investigate links before you visit the site is key to getting around some of the smarter phishing hacks in use in Q3.

Here is just one example of a malspam email we found in Q3 utilizing Google drive to deliver malware:



- **A malspam email instructs the victim to download a file from a provided link.**
- **The provided link directs the recipient to a Google Drive location where a WinRAR file is stored.**
- **The downloaded file, "Booking information.rar," is protected with a password. The password necessary to access the contents of the archive can be found within the email's content.**
- **The archive file contains a .exe file and the exe file is related to "StealC" malware.**

Popular Malspam Attachments

Like in Q2, PDFs accounted for the lion's share of malspam attachments. Unlike Q2 however, in Q3 they accounted for a full 87% overall - up significantly from last quarter's 55%. Also of note is what comes next. In Q2 it was DOC (33%) and ISO (5%) files. This quarter PDFs were followed distantly by HTML files (7%), an indication of HTML smuggling.

Top Malware Family for Q3

Last report it was Qakbot, also known as Qbot. This report it's Redline that takes the top spot for Malware Family of the Quarter, and here's why.

Redline came about during the height of the pandemic and gained traction because of its user-friendly control panel and extensive functionalities. It has been posing a severe threat to Windows systems ever since.

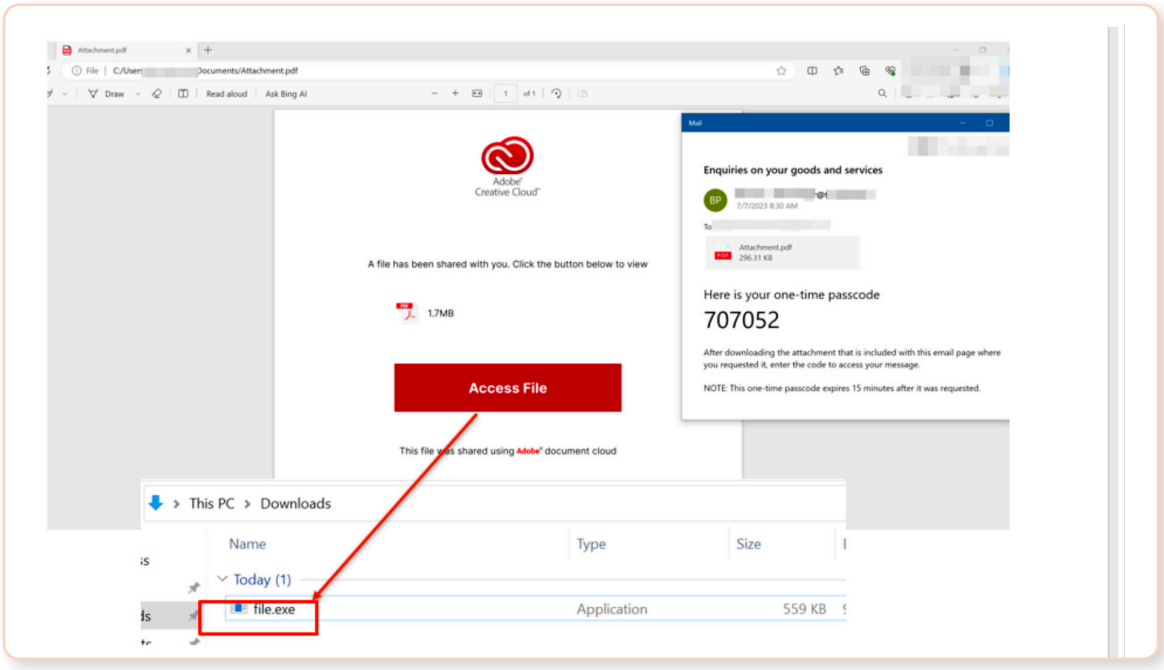
Why so dangerous? Redline has the ability to exercise complete control over a compromised machine. It can exfiltrate sensitive data like banking credentials, passwords, and even cryptocurrency-related information. It can be spread via innocuous phishing emails and can appear in various formats such as PDFs, executable files, and Office Suite documents, to name three.

Once a device has been infected, Redline can:

- **Steal user data like login credentials.**
- **Target specific user files within the PC's Desktop and Documents directories.**
- **Steal information out of cryptocurrency wallets.**
- **Take screenshots of sensitive information.**
- **Execute commands and introduce additional payloads on already compromised systems.**

And so much more. In this Redline instance, found by VIPRE AV Labs in Q3, the attack started with a PDF-bearing spam email. Simple enough. However, when you open the PDF file, you'll see a button that redirects you to a malicious website where Redline malware (formatted as file.exe) will be downloaded.

It looks like this:



Q3 Conclusions

Email is your first line of defense against many of today's threats, and sometimes your last. Staying ahead of this quarter's email security threats is vital to business continuity in the months ahead and security in the immediate future. VIPRE's Q3 2023 Email Threat Trends Report offers insights into the email security landscape only found with boots-on-the-ground experience and an in-depth knowledge of the trenches.

We see these exploits every day. We sift through hundreds of thousands of them, and millions - even billions - of emails. Informed with this to-the-minute threat knowledge, we put everything we have into our email security solution and offer it, and this report, to you as a way to stay safe, stay informed, and stay ready for whatever challenges your inbox next.

Stay up to date and look out for the next installment of the Q4 VIPRE Email Threat Bulletin

An Expert Look at Email-Based Threats 2023

BEC is on the Rise 2023

PDF Popularity, Callback Phishing and Redline Malware.

Sign up today for your FREE 30 day VIPRE Email Security Trial.

North America
sales@vipre.com
+1 855 885 5566

UK and other regions
uksales@vipre.com
+44 (0)800 093 2580

DACH Sales
dach.sales@vipre.com
+49 30 2295 7786

Nordics Sales
nordic.sales@vipre.com
+45 7025 2223