



Email Threat Trends Report: 2024: Q2

**An Expert Look at
Email-Based Threats**

Content

Introduction	03	Feature: BEC and GenAI: A Dangerous Duo	13
Detection Stats: What We Caught in Our Net this Quarter	04	Phishing: Catch Anything New?	15
Feature: Finding the Invisible Threat	04	What's Worse than Spam? Malspam	17
YoY Trends	05	Feature: Malspam Caught in the Wild	19
Feature: New Threats, New Rules	07	Conclusion	20

Introduction

VIPRE's Email Threat Trend Report is published quarterly. That's how fast today's attackers are changing their tactics, and as industry leaders in advanced email security solutions, we feel it is our responsibility to not only keep up, but to lead the charge.

Q2 2024 sees more and more exploits that are evading traditional email security scans and requiring the advanced capabilities of AI-driven solutions to catch. Fortunately, we have those and have been putting them to good use, because this quarter we caught 74% more non-signature-based threats and double the number of evasive malicious email attachments as we did one year ago. Business Email Compromise (BEC) emails accounted for half of an already staggering spam count, and AI-generated scams are making up high percentages of the emails we found.

And those are just a few of our Q2 findings!

Overall, our intent is not to alarm, but to inform. When global organizations understand the flavor of evolving email threats, they can evolve their security solutions to keep pace. Every quarter of every year, we make it our mission to analyze these trends, inform the industry, and present our bespoke solutions to help companies like yours stay abreast of the changes and stay ahead of the emerging threat landscape.



Detection Stats: What We Caught in Our Net this Quarter

Let's start off with the basics. In Q2, we:



Processed
1.8 billion
emails globally



Of those **226.45 million**
were spam emails
(or about 13%)



And **16.91 million** malicious
URLs were caught by our
proprietary Link Isolation tool

Feature: Finding the Invisible Threat

VIPRE Link Isolation is a sandboxing solution that tests potentially dangerous links in a safe environment prior to you opening them.

Rather than you finding out the hard way if a URL will ultimately try to infect your device with malware, our tool will leverage heuristics and machine learning to scan the site against malicious website lists and AV engines, and – even better – will sniff out polymorphic and zero-day threats that traditional scanning alone can not catch.

From over 225 million spam emails detected, we discovered:

- **51% Content** | 115 million were detected due to their content.
- **48% Links** | 110 million were detected due to embedded links.
- **1% Attachments** | Just over 2 million were red-flagged for their malicious email attachments.

And nearly 200,000 were detected by our behavioral analysis tools. These were malicious email attachments never seen before which were caught by VIPRE ThreatAnalyzer, our behavioral machine learning analysis solution, and Deeplink, an option that allows for in-depth, cloud-based scanning and previews of potentially malicious URLs.

YoY Trends

Spam Sample Size Increased by 74% in 3 Months

A remarkable finding was that our total sample size increased from approximately 20,000 spam emails to no less than 35,000 in the span of a single quarter – a neck-breaking increase of 74%.

- **Q1 sample size: 20,374**
- **Q2 sample size: 35,396**

The majority of the increase is attributable to commercial spam emails, specifically aggressive marketing, which we'll cover in more detail later.

Malicious Links Threats Increase by 74%

For starters, the number of malicious URLs trapped in our Link Isolation net increased by 74% year-over-year.

In Q2 of 2023, Link Isolation detected 9.7 million treacherous sites; this past quarter, it detected no less than 16.91 million. While this could indicate that our solutions are getting sharper quarter by quarter, it but it could also signal that there are many more email exploits today that utilize non-signature-based methods. Organizations without a way to catch this type of foul play are exposed to nearly three-quarters more danger than they were twelve months ago.

Non-Signature-Based Attacks

Traditional email security solutions are programmed to detect the signatures of known malware. When a piece of malware is caught, the vendor or security researcher that caught it assigns it a signature based on its unique code.

It is then saved in a database, either a public one or one owned by the vendor. These signatures are used to power some security solutions, but the solutions that rely solely on signatures are at a disadvantage; as cybercriminals get craftier, they develop malware that can hide or change its code, thereby avoiding detection. They can also spin up new malware attacks every time so that there is no signature on record to catch.

However, despite how undetectable the code might be, malware always shows its colors eventually by deviating from what a healthy program or application would do. For this reason, tools have evolved that look for signs of malicious behavior - not signatures alone - in order to catch the next generation of exploits.

More Links, Less Content

Additionally, this time last year 58% of spam emails were caught due to their content and around 42% due to links.

It is interesting to note that within twelve months we're seeing a roughly 50/50 split, indicating that more spam emails are leaning towards malicious links as a weapon of choice.

Attachment Sandboxing Detected Twice as Many Emails

Also worth noting is that twice as many malicious emails were discovered due to VIPRE's attachment sandboxing, compared with Q2 2023. Before you open that PDF, VIPRE lets you check out the attachment in a secure environment.

Last year, our solution detected 90,000 malicious email attachments before VIPRE clients could click on, open, or download them. This year, that same attachment sandboxing feature prevented 186,000 malicious email attachments from compromising our customers, an increase of over 100%.

Interestingly, overall malicious attachment figures were slashed by half, however. In Q2 of 2023, 5.36 million spam emails could be attributed to it; in Q2 of 2024, only 2.31 million. This could indicate that while easy-to-catch malicious email attachments are slowing down, attachments with not-so-easy-to-catch exploits (I.e., the ones that only attachment sandboxing can detect) are on the rise. Behavioral-driven email solutions are truly of their era, and are becoming more and more necessary as cybercriminals get better at evading traditional tactics.

Additionally, trickier techniques call for a more educated employee base. [Security Awareness Training \(SAT\)](#) is needed to raise the level of awareness among employees and help them play a stronger defensive game against subtle, non-signature-based ploys like BEC attacks and links hidden in attachments.



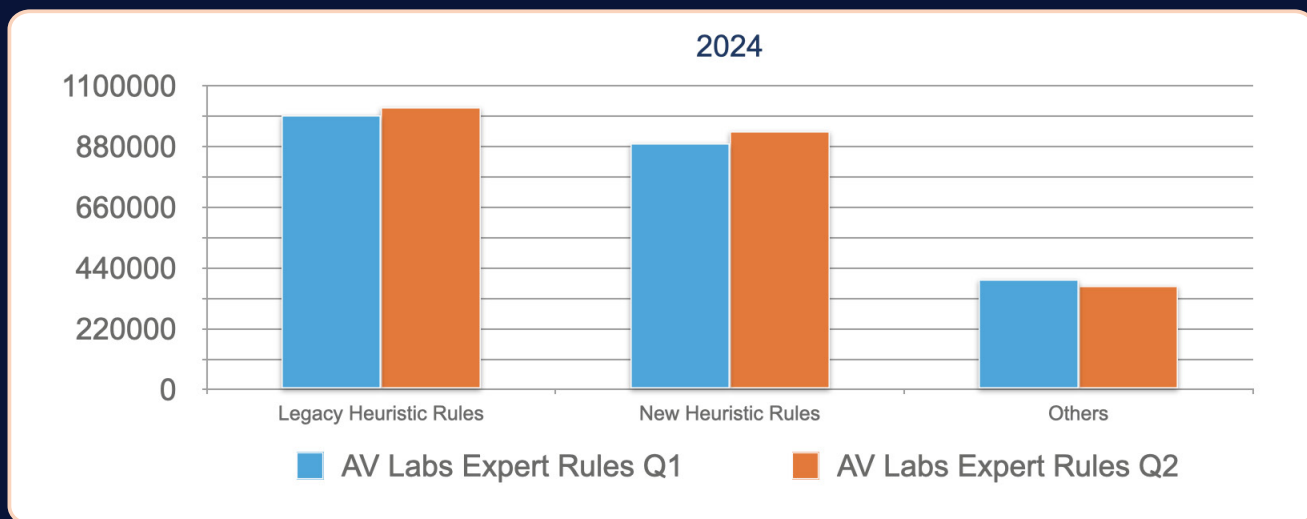
“This year, that same attachment sandboxing feature prevented 186,000 malicious email attachments from compromising our customers, an increase of over 100%.”

Feature: New Threats, New Rules

Being ahead of the curve is what helps us protect our customers and that's why VIPRE's AV Labs constantly creates new rules based on the new threats that come across our desk every single day. **And guess what? They're working.**

These rules are curated and maintained by AV labs to enhance detection and keep up with the latest email threats. Even compared to last quarter, we've increased the number of spam emails detected in both the Legacy Heuristic Rules and Generic Heuristic Rules categories.

Heuristics are shortcuts, or generalized rules that can spot not only known malware, but anything that looks like it. They widen the scope of the search, and therefore catch more in their nets. All in all, our AV Labs Expert Rules detected a total of more than 2.3 million spam emails in Q2 using these methods.



The Slow Upward Creep of Spam Emails

In Q2 of last year, spam emails accounted for 92% of our total quarterly catch. Last quarter, they were up to 95%. This quarter, they're charting at 96%.

It doesn't take a statistician to predict where they'll be a few quarters from now – and if there's any way attackers could push that number above 100%, we know they'd do it.

The second-most popular category (by a wide mile) is Marketing, though Marketing emails have consistently dwindled: from 5% in Q2 2023, to 3% in Q1 2024, to 1% this quarter.

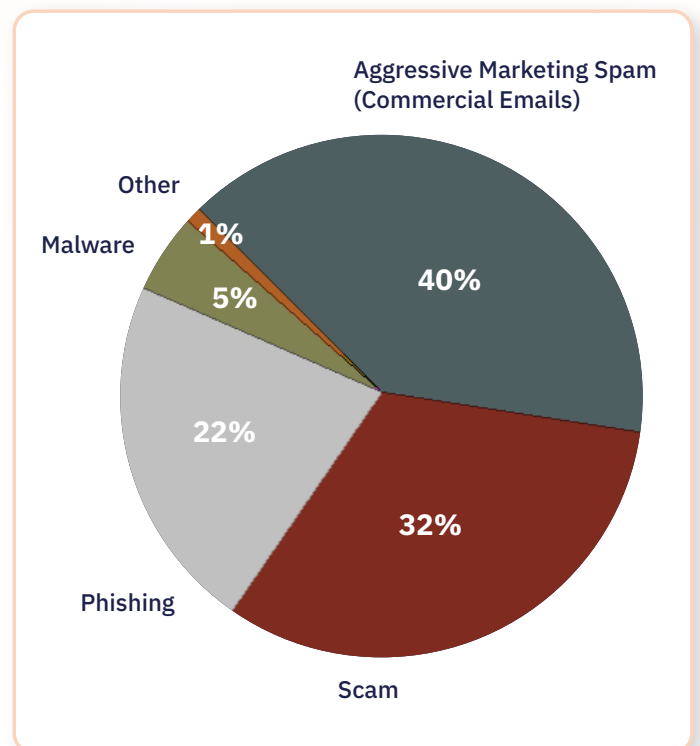
Pick a Spam, Any Spam

Our spam varieties and their rankings have stayed fairly constant from the last quarter to this one.

Classified by their behavior and purpose, here's how they stacked up:

- **40% Aggressive Marketing Spam (Commercial Emails)**
- **32% Scam**
- **22% Phishing**
- **5% Malware**
- **1% Others: This includes financial, health, adult, and job-related spam**

While the percentages varied slightly in Q1, the hierarchy did not. Aggressive Marketing Emails still accounted for the majority, Scam and Phishing were next in line, and Malware and Others were responsible for the least. At least we know email hackers aren't being obvious. And it is precisely because so many malicious links, attachments, and snippets of content are hidden in colorful marketing messages, friendly "change your password reminders", and other non-obvious forms that they are so pernicious.



USA: Still #1 in Spam Emails

This quarter 66% of all spam originated from the United States, the same as last quarter and a percentage point down from Q2 2023.

Because 33% of the world’s data centers are [located in the US](#), it stands to reason that a disproportionate number of spam emails bear a US thumbprint. Threat actors from around the world leverage US data centers, and so the number not only represents US citizen attackers, but those from the global community as well. Germany recently overtook Great Britain as the country with the second-highest number of data centers, leaving Great Britain to come in third, followed by China, Canada, France, and Australia.

The data center pecking order is vaguely reflected in the spam sources below - with the notable exception of Germany. Here are the top five offenders in Q2, along with comparisons.

Q2 2024	Last quarter (Q1 2024)	Last quarter (Q2 2023)
United States - 66%	United States - 66%	United States - 67%
Great Britain - 13%	Great Britain - 9%	Denmark - 10%
Canada - 8%	Ireland and Japan - 3%	Ireland - 8%
Sweden - 4%	France - 2%	China - 7%
Iceland - 3%	Other - 17%	Other - 16%

Manufacturing Still the Prime Target – But Not by Much

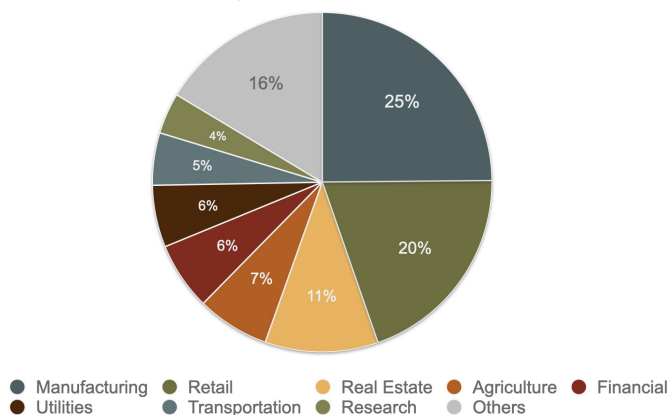
In Q1 of this year, we saw an interesting jump; the sector targeted most by email attackers in 2023 was Finance (25%), but when the data was gathered at the end of March, it was Manufacturing by a landslide.

During Q1, Manufacturing took 43% of the hits when it came to sector-targeted inbox attacks, and now in Q2, it's still holding on to its lead at 25%.

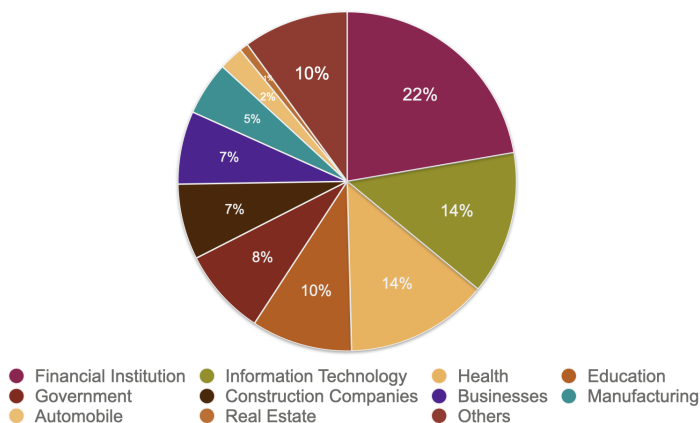
Next in the lineup are Retail (20%), which didn't even make the yearly list last year, Real Estate (11%) - which only represented 1% of the 2023 totals – and Agriculture (7%), which again, was nowhere near a targeted sector last year.

It appears that attackers are targeting industries traditionally perceived as lacking advanced technological capabilities or extensive cybersecurity education. After being the popular targets for so long, threat actors might assume that Finance and IT (two of last year's quarterly toppers) would by now be well-versed and well-prepared in spotting signs of fraud, and therefore, harder to dupe.

Sectors Targeted by BEC, Phishing, and MalSpam Emails for Q2 of 2024



Organizations Targeted by Phishing and MalSpam Email in 2023



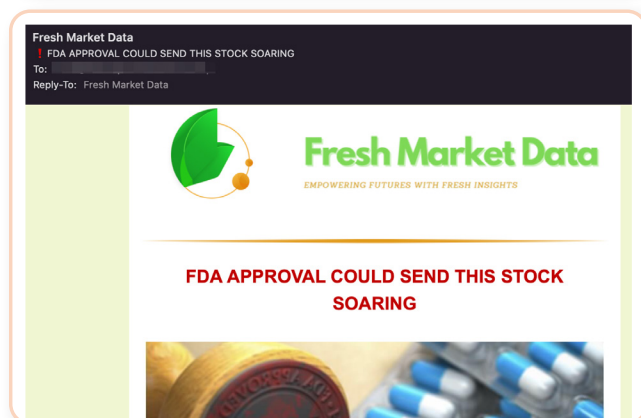
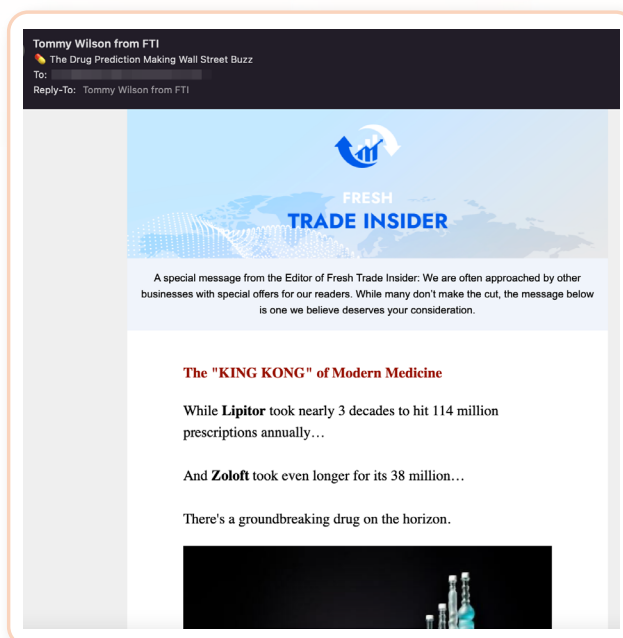
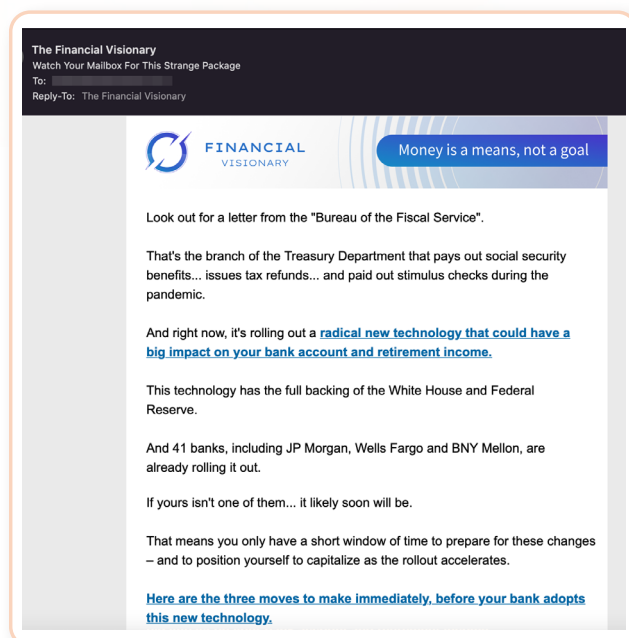
Love to Hate: Aggressive Marketing Spam

We promised we'd get back to it. We noted earlier that of the 74% increase in spam emails during Q2, the majority belonged to commercial spam emails, specifically aggressive marketing.

Aggressive marketing spam emails are those that persistently promote products or services in a manner that can be intrusive and overwhelming to recipients. These emails often utilize high-pressure tactics to drive immediate action, such as making a purchase or subscribing to a service. The content of these emails typically includes bold claims, urgent language, and frequent call-to-action buttons to capture the recipient's attention and compel them to respond.

One example of these aggressive marketing spam emails is a campaign that led to a spike in spam samples in April 2024. This campaign exploited the xt.local mailing list to send out a large volume of marketing emails. By utilizing the xt.local domain to send marketing messages that appeared legitimate, it was able to bypass many traditional spam filters. These emails often included enticing offers and promotions designed to capture the recipients' attention and prompt them to engage with the content.

Some examples of aggressive marketing emails that leveraged an xt.local mailing list include:



Note how this last one transcends technical cleverness and isn't afraid to manipulate people's emotions with speculation, "exclusive" information, and the unspoken promise of an increased income stream during an uncertain US market. Also, note the use of sensationalism and overtly "salesy" tactics in all three. Tip: If it sounds like the heading of a tabloid ad, it likely isn't legitimate.

BEC Rears Its Ugly Head

Business Email Compromise (BEC) is a beast, not least because it was 48 times more costly than Ransomware last year.

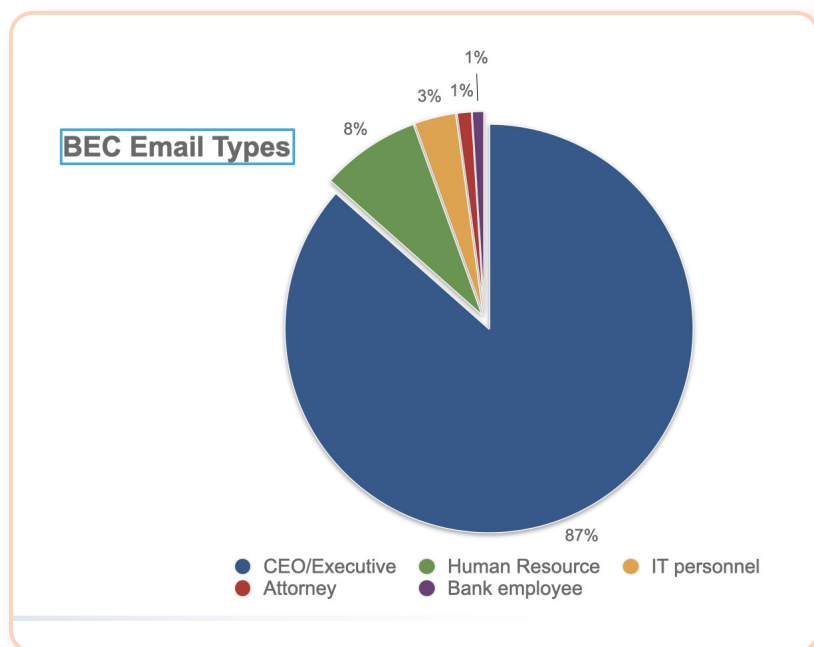
According to the FBI's Internet Crime Report, BEC fraud was responsible for \$2.9 billion in adjusted losses in 2023, whereas ransomware only accounted for a (comparably paltry) \$59.6 million.

For reasons financial and other, BEC emails are one of the most prominent threats to organizations. These emails are meticulously crafted to appear as legitimate communications from high-ranking individuals or known persons within the organization. In a BEC attack, an attacker falsifies an email message to trick the victim into performing an action, most often transferring money to an account or location controlled by the attacker.

In our Q2 research, we found that nearly half (49%) of all detected spam emails were attributed to BEC scams. This represents a 20% growth in the total number of BEC emails we received in Q1 and Q2 compared to last year.

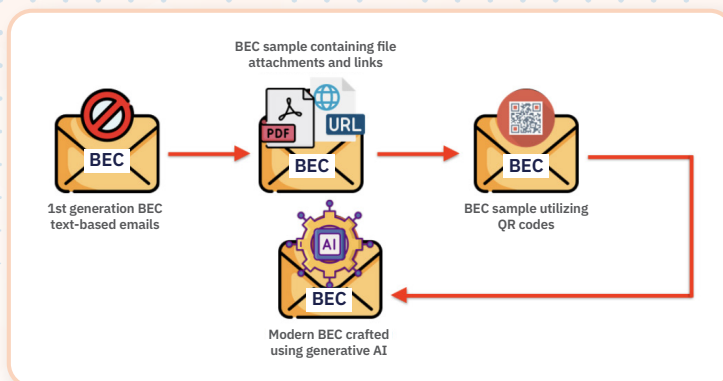
BEC Email Recipients: Are You on the List?

Who might be the most likely one at your office to have received a well-crafted BEC email this past quarter?
Our research suggests your CEO would be top of the list, followed by HR and IT.



The Evolution of BEC Scams

Over the years, we have observed the evolution of BEC samples, transitioning from simple text-based emails to those with attachments and links, then to BEC emails utilizing QR codes, and most recently to BEC emails created using generative AI.



Feature: BEC and GenAI: A Dangerous Duo

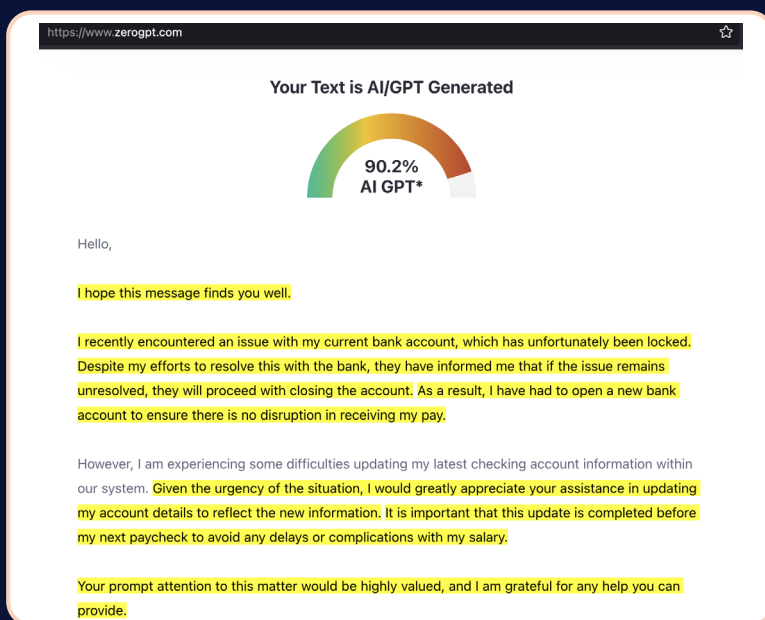
You may not be surprised to know that a full 40% of the BEC emails we uncovered in Q2 were AI-generated. We weren't!

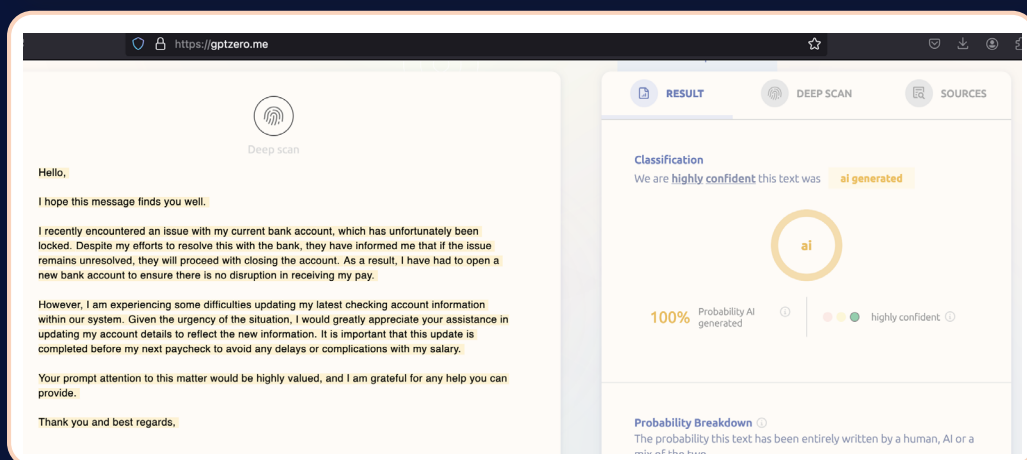
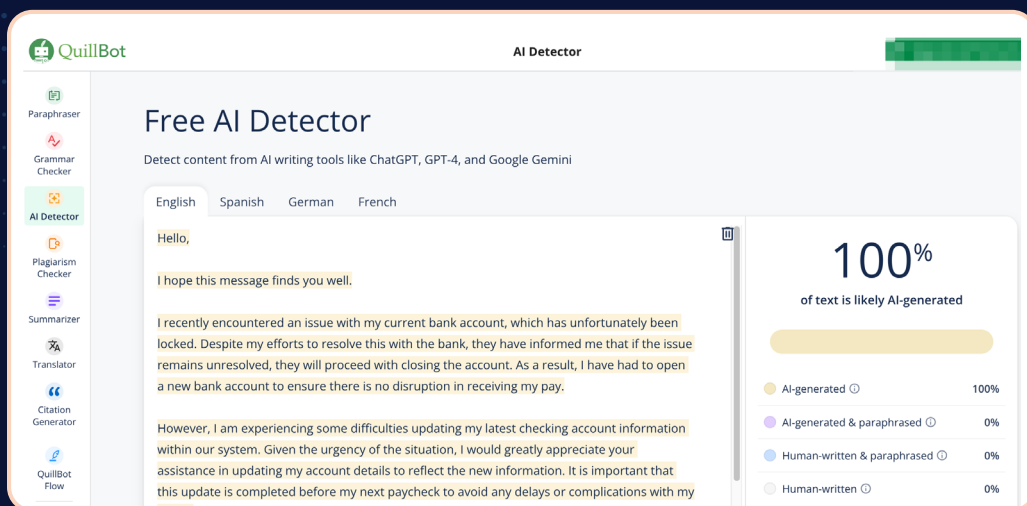
These past few months we noticed an increasing trend of AI-generated business email compromise (BEC) emails in our clients' email inboxes. To understand their nature, we tested some of these emails using multiple AI text detection tools like GPTZero, ZeroGPT, and Quillbot to identify AI-generated content.

In several instances, these tools revealed that nearly the entire BEC message was likely created by AI. With AI-generated text, phishing emails are becoming more convincing by eliminating the language and grammatical mistakes that were common in traditional phishing attempts.

However, Security Awareness Training (SAT) can help educate users so that even the sneakiest attempts have a higher likelihood of getting caught. With SAT, employees will be taught the red flags of phishing and BEC emails beyond just looking for grammatical and spelling errors. They will be taught to detect things like pilfered logos, a sense of urgency, "too good to be true" schemes, and other subtle traits.

In addition to user education, the right solutions can also make a huge difference when it comes to spotting AI fakes. Here are some AI-generated BEC samples tested on multiple AI detection tools.





And in case you were curious, here's how those detection tools fared:

AI Detector Tool	Verdict
GPTZero	100% Probability AI generated
Quillbot	100% Probability AI generated
ZeroGPT	90.2% Probability AI generated
Sapling	74.3% Probability AI generated
Scribbr	100% Probability AI generated

Phishing: Catch Anything New?

It's no secret that phishing is one of the primary – if not prime – suspect when it comes to business email compromise (BEC). It always has been, and it likely always will be.

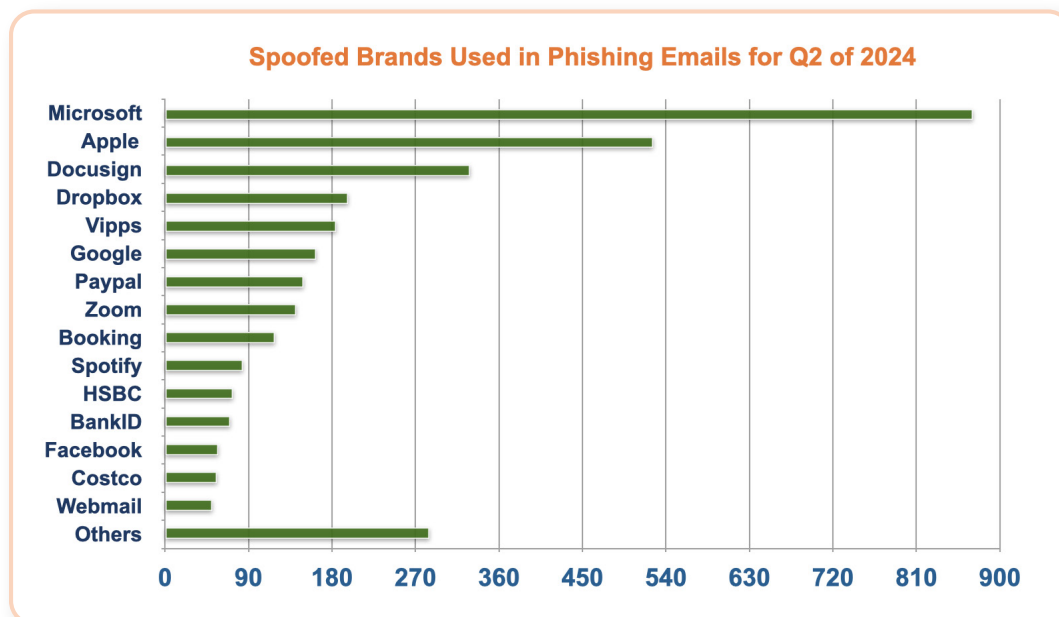
Attacker's Favorites: Brands, Tactics, and More

Brand of Choice: Microsoft

This first fact should come as no surprise, especially to anyone who's been keeping up with any of our previous reports (or the news), but Microsoft is again the most spoofed company of the quarter, accounting for nearly 900 caught cases over three months.

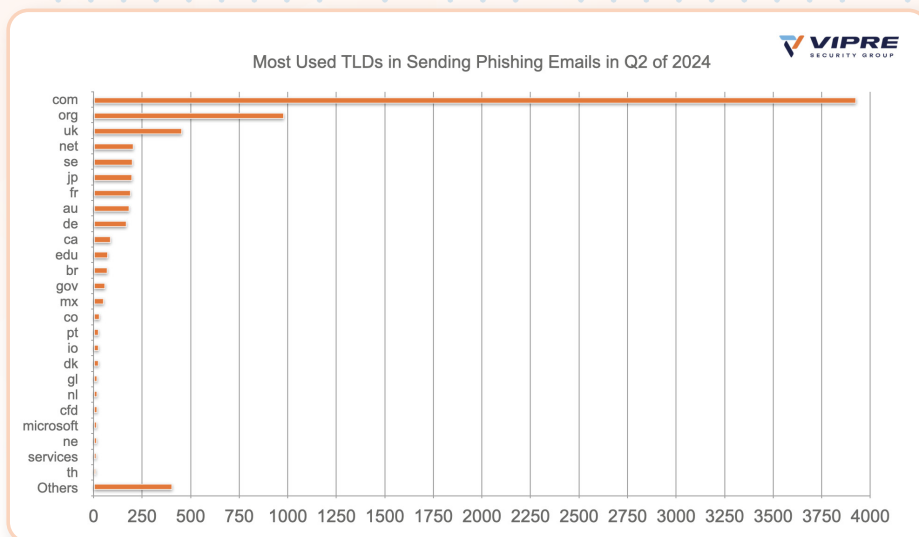
Microsoft also took the top spot last quarter (730 cases) and in Q2 of last year (380 cases), although the number of incidents has been steadily and sharply on the rise. Second was Apple – the same as Q2 2023 – by a little over half, rising from a little under half twelve months ago. And third was DocuSign, completing the exact same “Top 3 Lineup” as last year.

One distinct trend we did notice was more financial organizations on the list, such as Vipps, PayPal, HSBC, and BankID.



Top TLD: .com

And while we're on the topic of "most," the most commonly used Top Level Domain (TLD) by attackers is still ".com," coming in at nearly 4,000 incidents. Next are ".org" and ".uk"; identical to last quarter. A year back the top three TLDs ranked ".com," ".es," and ".edu."



Favorite Country to Target: United States

Just like the United States was the "top offender" in sending out malicious email spam, it is also the Network Vulnerability Scanner & Monitoring Service | Alert Logic number one geography to receive it. The US again topped the list of most targeted countries when it comes to phishing emails, receiving nearly half of all sent out in Q2.

The most targeted countries this quarter were as follows:

1. **United States – 46%**
2. **Great Britain – 16%**
3. **Sweden – 13%**
4. **Canada – 10%**
5. **Iceland – 7%**
6. **Denmark – 4%**
7. **Ireland – 3%**

Favorite Strategy? URL Redirection

Not all phishing links are created equal, and threat actors know that. Judging by how heavily Q2's email attackers leaned into certain types of phishing URLs, we can only assume they are finding more success with some as compared to others – and we had better take note of which ones.

This quarter, the most popular strategies employed in phishing links were:

- **URL Redirection – 48%** | When a domain's visitors are redirected to another site – the phishing site. Last year, this only accounted for 39%, while in the last quarter it was up to 64%.
- **File-Hosting Service – 26%** | Cloud-storage services like Box or Drive are prime targets because it is impossible for traditional email solutions to scan what's in there. That's why Link Isolation is key. This tactic is gaining steam; last quarter it was at 6%, and a year ago it didn't make the list.
- **Compromised Websites – 16%** | Manipulated code makes these seemingly legitimate sites serve malicious third parties. This trend is on the decline; last quarter it was the second-most favored (22%) and this time last year it was first with a whopping 45%.
- **Newly Created Domain – 9%** | Traditional email solutions can't catch something without it having been caught before and assigned a signature, so nascent (malicious) sites have a distinct advantage. In consequence, newly created domains took 10% a year ago and 15% last quarter.
- **XSS Vulnerability Link – 1%** | This basic web vulnerability ploy is new on the recent horizon, not showing up in last year's analysis and pulling in about 4% in Q1.

What's Worse than Spam?

Malspam

Make Up Your Mind: Links vs. Attachments

We noted a massive change in tactics between last quarter and this in the malspam department. Malspam is defined as an email carrying a malicious payload, such as malware in a link or attachment.

The figures were nearly the opposite of each other; In Q1, the majority of malspam emails (78%) employed malicious email attachments while the minority (22%) used malicious links. Our Q2 figures indicate a tectonic shift, with the vast majority (86%) now employing malicious links, and the minority (14%) leaning on attachments.

One theory is that everyone in the industry read our Q1 report and went out and made some changes. While we would always love to hope, a more probable definition could be that links are getting trickier and trickier to hide, leading as they can to “safe” and legitimate websites that will pass a scan but are infested with infected links once you get inside.

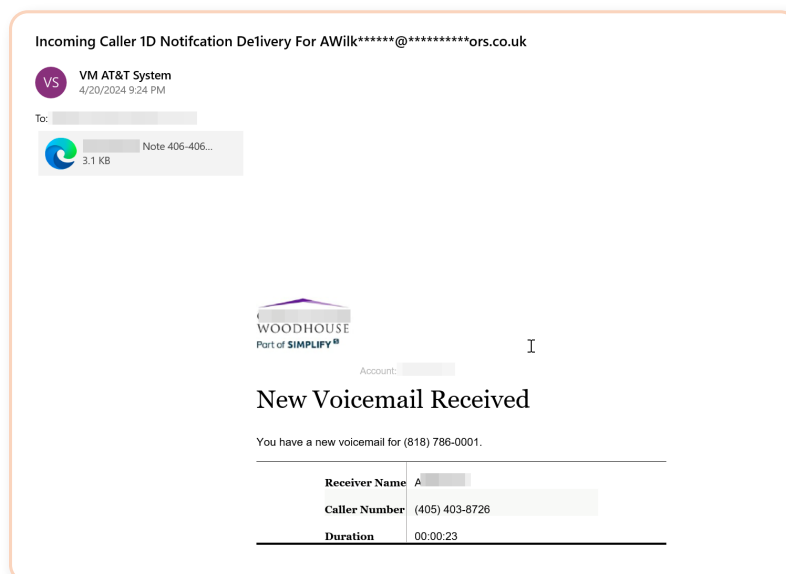
Trickier link tactics are one of the primary reasons VIPRE Link Isolation was engineered, as it gives you the chance to safely view sites in action before you click on any links. Concerned the pendulum might swing back toward attachments? We always are, too. That's why VIPRE Attachment Sandboxing is something every SOC should have in its back pocket.

What Kind of Attachments?

Speaking of malicious email attachments, the most common forms this quarter were:

- ZIP (62%), which mostly contain malicious .EXE or .DLL files.
- DOCM/DOCX (16%)
- HTML (12%)
- XLSX (10%)

Here is an example of a phishing email using a malicious attachment as bait:

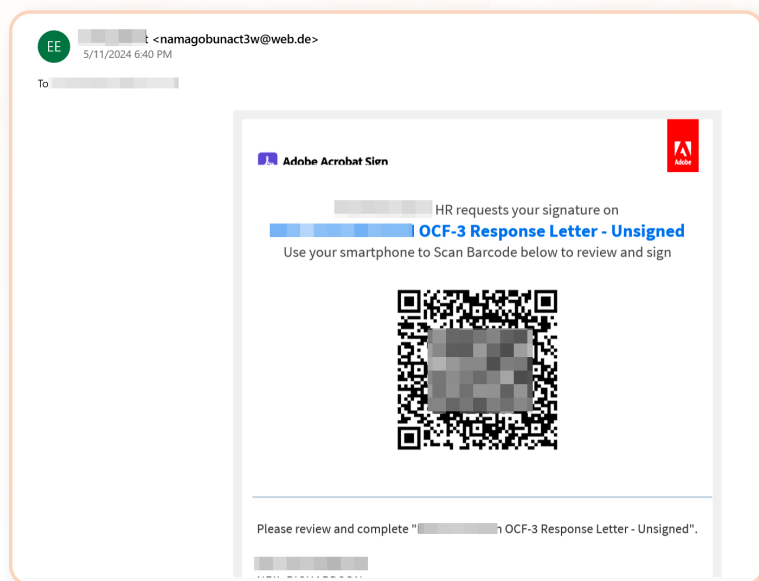


What About Quishing (QR Code Phishing)?

This quarter, all of the PDF attachments we received contained Quishing (QR phishing) attempts.

The use of PDF files by threat actors for phishing and malware delivery has surged since Microsoft began blocking macros by default in Office files like Word and Excel. Due to their complex structure, PDF files enable threat actors to embed malicious URLs, scripts, or concealed content, allowing them to evade traditional security measures.

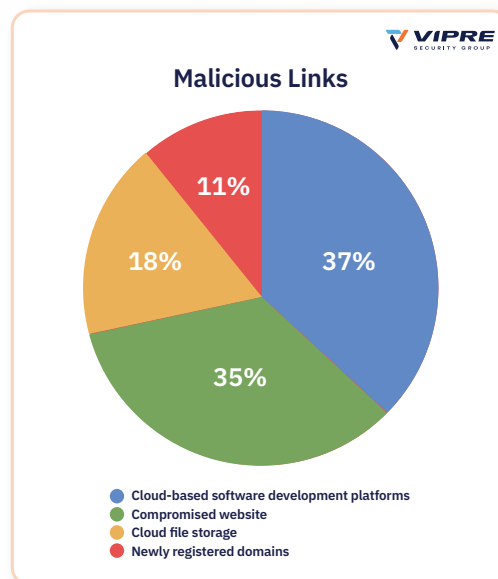
Here's an example of one we caught:



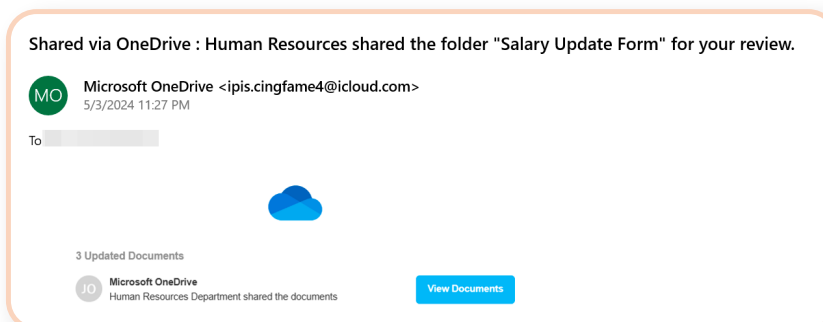
And Where Can We Find Those Links?

In Q2, we discovered the four primary methods that attackers are using to deliver malware through links in malicious spam samples.

The most common method involves using cloud-based software development platforms like GitHub to host the malware. Other methods include utilizing compromised websites, cloud storage platforms like Google Drive, and newly registered domains.



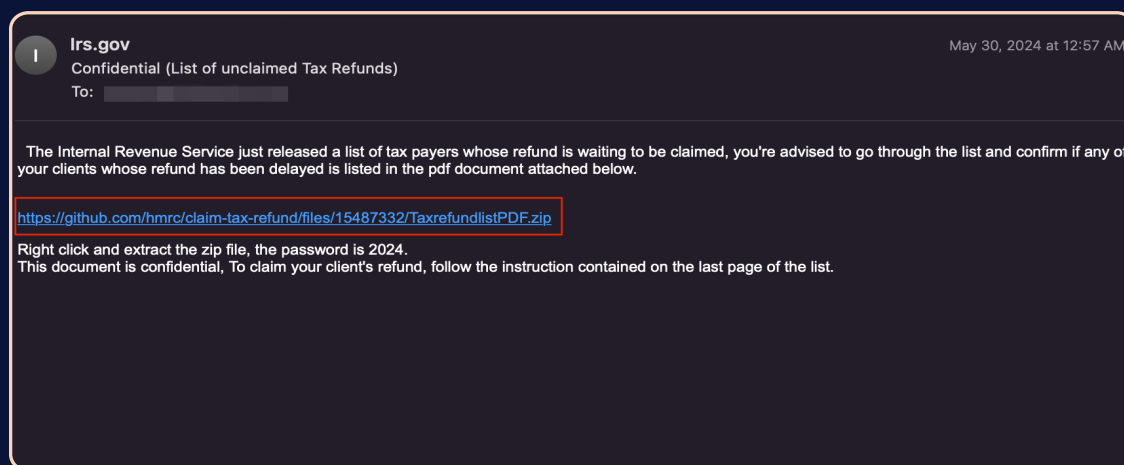
Check out this example of a link-using phishing email caught in the wild:



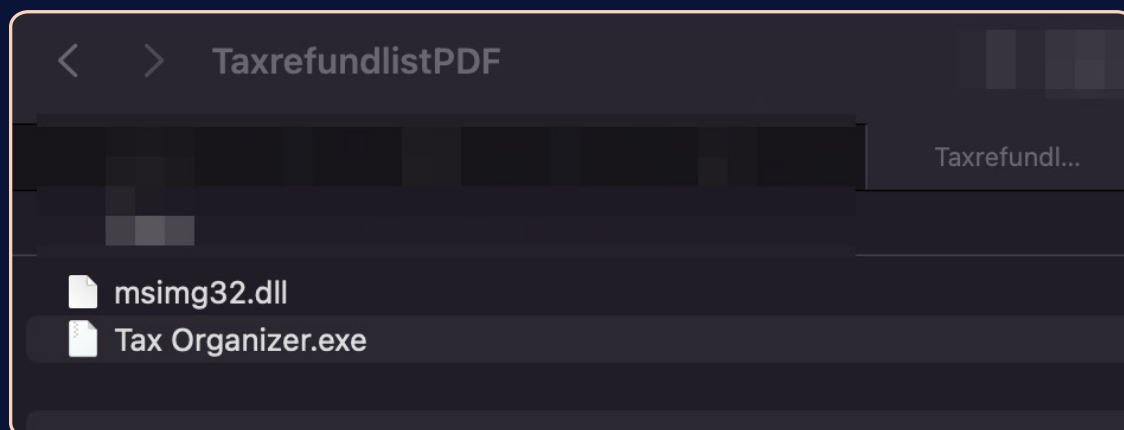
Feature: Malspam Caught in the Wild

Here's an example of malspam email we found in Q2 utilizing cloud-based software development platforms.

- The malicious email is disguised as a tax-related communication appearing to be from IRS.gov, claiming there is a refund waiting to be claimed.
- Threat actors used a legitimate GitHub repository to host a malicious file found inside a password-protected zip file. The password for the zip file was included in the email content, likely to evade detection during download.



- Upon downloading and extracting the zip file, it was found to contain two files: a .dll and a .exe file. The .dll file serves as a component of the .exe file, and the .dll file is associated with the malicious Remote Access Trojan (RAT) known as Agent Tesla.
- Agent Tesla malware is recognized as a .NET information stealer with capabilities to extract sensitive information from the infected machine, assume control over it, and download additional malware.



Conclusion



VIPRE Email Security has been a leading force in email protection for over 25 years, dedicated to providing top-notch defense solutions.

Our tireless research ensures we stay ahead of the latest email threats, and we're eager to share our findings with you each and every quarter. Join the 50,000 global customers who rely on our threat intelligence to see what email attackers are up to, spot their developing trends, predict what they are going to do next and more importantly get your organization protected.

For more information about VIPRE email security, our Security Awareness Training courses and our endpoint technology, [schedule a demo](#) today.

Stay up to date and look out for the next installment of the **VIPRE Email Threat Trends Report**.



**Email Threat
Trends of 2024**

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