



Email Security in 2024

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

Content

Introduction	03	Feature: The Rise of the EML File Attachment	09
Overview: What We Caught in Our Net	04	Malspam	10
Phishing	06	Feature: Top Malware Families by Quarter	10
Feature: Google Group Fake Order Scam	07	Conclusions	11
Feature: It's a Jolly Holiday for Spammers	08	VIPRE Email Threat Predictions for 2024	12

Introduction

Email Security in 2024: What to Expect from the Evolving Email Threat Landscape.

With more than 20 years of email security experience, we at VIPRE Security Group know one thing – this year is different.

This difference should come as no surprise, given the fact that rapid AI advancements have changed everything for everyone, but it still needs to be accounted for and prepared against. Attackers have revolutionized the way they phish, and security experts need to revolutionize the way we defend.

The inbox is often the first thing employees see in the morning and the last before they wrap up at night. Whoever controls it controls the high ground. As attackers are getting stealthier, more creative, and more powerful in their schemes, it becomes vital to make data-driven decisions when planning a successful counter-strategy.

In our annual Email Security Trends Report, we offer an analysis of nearly 1 billion (953.39 million) malicious emails gathered by our worldwide VIPRE network over the past twelve months. From deepfake-riddled phishing to new file extensions, quishing, emerging mobile threats, and more, we present our proprietary findings for the benefit of the security community at large and hope this report shines some light on the advanced methods needed to secure the corporate email landscape in 2024.



Overview: What We Caught in Our Net

VIPRE Overall Detection

This year, VIPRE processed 7.2 billion emails worldwide.

Of those, 950.39 million malicious emails were detected (roughly 13 percent). The good news? VIPRE Email Security Link Isolation, one of our features that works very much like URL sandboxing for your email, detected and protected over 41.9 million links clicked by users. We're pretty proud of that.

Now, let's look into the roughly 950 million malicious emails that were found. There was roughly a 50/50 split between those caught due to content (52%) and those caught due to links (48%). Twenty million were flagged for their malicious attachments and the remaining 500,000 or so were only detected due to VIPRE technology that could spot nefarious behavior. These were never-before-seen threats that would have passed undetected by other signature-based email security solutions, but they did not pass by ours.

Let's drill down deeper and analyze those 42 million links protected by Link Isolation. Of those, 89% were flagged due to content, and 11% were detected by DeepLink, our webpage behavior analysis tool. Over 300,000 total were detected at click time, evidencing zero-lag coverage.

Lastly, our YARA rules accounted for additional millions caught in malicious attempts. YARA rules look for statistical patterns and indicators that follow particular malware families and serve to catch malicious exploits that might otherwise fall through the cracks. Last year, our YARA rules caught between one and two million generic malware instances each quarter, with a nearly 20% jump in Q4. The numbers were significantly less for specific instances, ranging from 70,000 – 400,000, but the Q4 jump exceeded 200%.



The good news?

VIPRE Email Security Link Isolation, one of our features, detected and protected over 41.9 million links clicked by users.

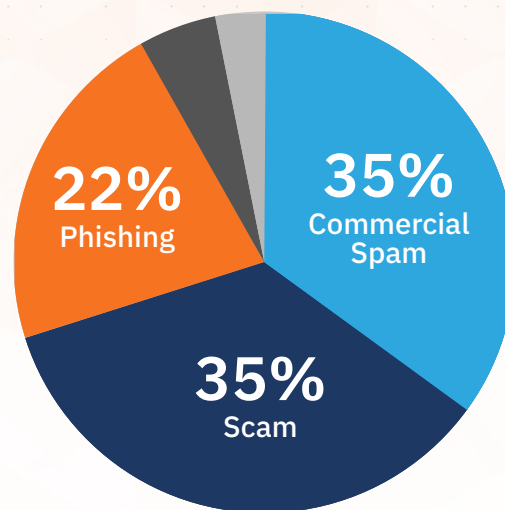
We're pretty proud of that.

Email Security Report Breakdown

For the purpose of this report, VIPRE labs pulled from a sample size of 44,913 emails, 41,716 (95%) of which were classified as spam (which includes phishing, malware, scam, adult, job, health, financial, and commercial categories).

The various spam types broke down accordingly:

- 35% Commercial Spam (14,738)
- 35% Scam (14,658)
- 22% Phishing (9,182)
- 5% Malware (1,967)
- Less than 3% Adult, Job, Health, Financial



Spam Trends by Quarter

It was interesting to note a rise and fall in favored spam types each quarter and across the span of the year. In 2023, we noticed:

- A 276% increase in malware between Q1 and Q4
- A 23% rise in scam emails between Q1 and Q4, with a 179% spike in Q2
- A 6.4% decrease in phishing emails between Q1 and Q4, with a resolving dip between Q2 and Q3

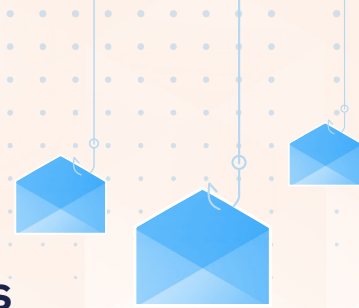
Regardless of the slight percentage decrease, phishing emails continue to tie with scam emails in volume, making them a perennial favorite of hackers and a constant threat to inboxes.

Targeted Sectors by Quarter

In 2023, Financial Services (22%) was the sector most targeted by phishing and malspam emails, followed by Information Technology (14%), Healthcare (14%), Education (10%), and Government (8%).

Quarterly stats revealed that while Financial Services, Healthcare, and Education ranked high in numbers, the overall frequency of attacks diminished between the first and fourth quarters. However, IT experienced a 59% increase within the same timeframe, and attacks on Government inboxes went up by a staggering 16,000%.

Phishing



Links, Attachments, and QR Codes

When it comes to phishing, the vast majority (71%) of emails are still using links as their primary bait. Attachments show up in 22% of cases, and the remaining 7% is attributed to embedded QR codes, or quishing.

Interestingly, between Q1 and Q4 of 2022, attachment-based phishing increased slightly (4%), link-based phishing decreased sharply (43%), and quishing went from zero instances to 417, a recorded jump of over 41,000%.

Who Was Spoofed?

Just like last year, our research (and [others](#)) revealed Microsoft as the top-spoofed URL by a landslide, garnering 2,400 spoofs to second-place Apple's roughly 350.

Dissimilar to last year, the ensuing list looks as follows:

1. Microsoft
2. Apple
3. DHL
4. Google
5. DocuSign
6. Amazon
7. Dropbox

Previous years' data showed Spotify and Zoom coming in high on the list; this year they were nowhere to be seen. Possible reasons include the rush-to-remote effect we were still feeling strongly in 2022, whereas an August 2023 [ResumeBuilder](#) survey revealed that 90% plan on having their employees return to the office by this year.

Phishing Links by Type

In 2023, malicious links were comprised mainly of compromised websites (45%), down slightly from last year, followed by URL redirection (34%), which wasn't even a category in 2022.

Next comes newly created domains (13%), down significantly from last year's 39%, and file storage/cloud sharing (8%), which also didn't make 2022's list.

The main differences? URL redirection and file storage/cloud sharing were new this year, while one of last year's categories (subdomain cybersquatting) did not appear in 2023.

When viewing the quarterly trends, we notice a decline in all categories (compromised websites plummeting by 80%) except for URL redirection, which experienced a 463% uptick.

Phishing Attachments

HTML attachments accounted for over half (52%) of all malicious attachments.

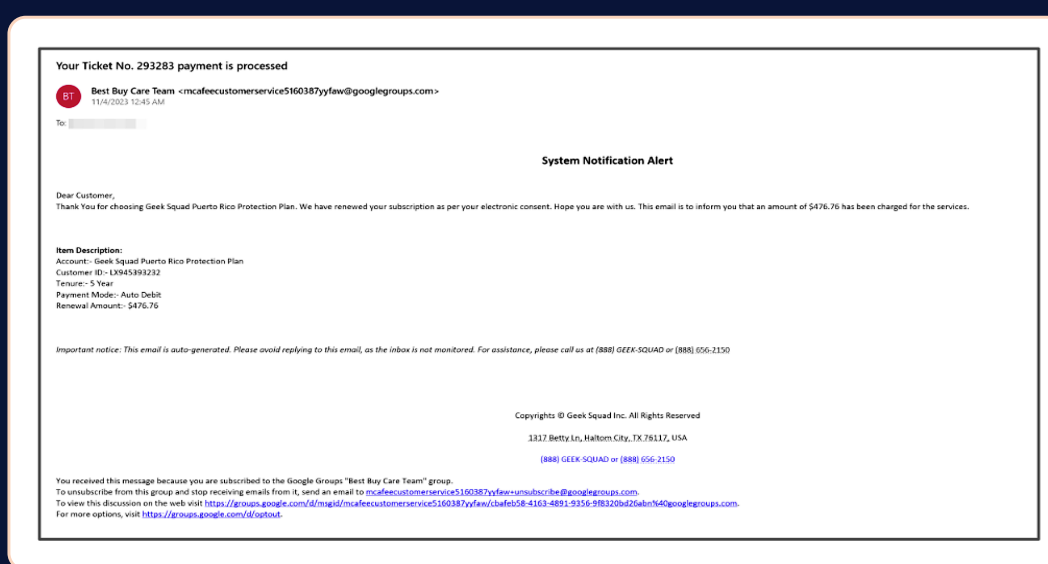
- HTML (52%)
- PDF (26%)
- EML (20%)
- ZIP (2%)

This is the first year .eml attachments have made the list in any significant way. Companies would be wise to spot the trend and prepare their users now. Last year, we flagged a growing uptick in HTML usage, and this year it was our primary contender. Significantly, HTML attachments declined by 27% by year's end, but PDFs rose by over 100% and EMLs by a drastic 4600%.

Feature: Google Group Fake Order Scam

What's so harmless about a purchase confirmation? If the ruse was to get you to buy something (and therefore enter your credentials), it would seem that the danger has passed.

However, cybercriminals have been leaning into fake order scams, especially through Google Groups, for the payout they can get when you call in to “cancel.” They leverage Google Groups because it allows them to customize the header, “Best Buy Care Team” in this case, while hoping you don’t think too much about what’s after the “@” symbol.



While the above email may appear harmless, the danger comes when you realize you never bought XYZ product, and you click the link or call in to cancel the order. After all, an unknown purchase may be a sign that you’ve been scammed. When you call in, helpful “Customer Service” agents are ready and waiting to take your personal information (email address, phone number, possible card number that could have been used) in order to “remediate” the issue.

Want to stay on the lookout? Here are the tell-tale signs, which you can cross-reference in the real-world example above.

- Lookalike email confirmation templates are mass-distributed to all members of a Google Group. If you don’t want to be added to a Google Group without your permission, you can follow [these instructions](#) to turn the feature off.
- Fake specifics like invoice number, warranty expiration date, transaction data, order number, and customer ID will be added in for authenticity.
- Watch out for “Dear Customer.” If it was a legitimate receipt, it would include the customer’s name, instead.
- The call-to-action comes in the form of anything you can call or click. Do not call the telephone number provided or click the “Customer Service” link. If you have any doubts, Google the actual phone number or support site and see if they match up.

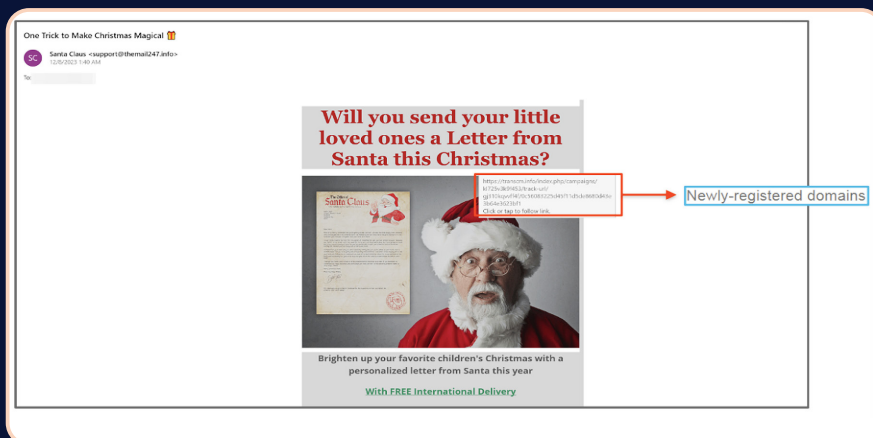
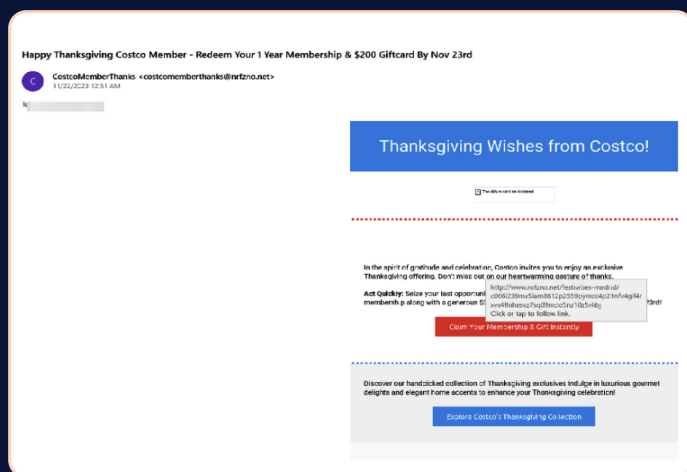
Feature: It's a Jolly Holiday for Spammers

In the hustle and bustle of year-end madness, it's easy to go on “autopilot,” especially when doing the mundane things like making sure packages arrived on time.

As Fredrik Heiding, PhD and Research Fellow at Harvard University, noted, “Phishing attacks work because they hijack shortcuts in your brain. But if you pause and reflect on the contents of an email, your rationale brain will take over.”

In Q4 of 2023, we noticed festive scam emails for Halloween, Thanksgiving, and Christmas. Overwhelmingly, links embedded in these kinds of emails may lead to phishing and scam attempts. These links often leverage newly registered domains to successfully bypass web filters. Again, if ever in doubt, look up the actual website of the company “sending” you the email and see if that sale, deal, or order really exists.

Can you spot where your brain might be looking for the shortcut in these holiday hacks we found in the wild?

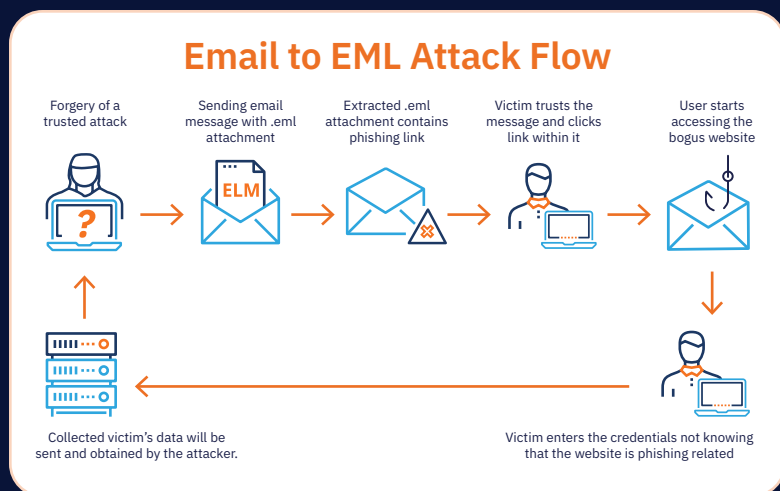


Feature: The Rise of the EML File Attachment

We noticed a marked growth in the number of malicious .eml file attachments in Q4 of last year.

This is the format an email takes when you send or save it in a plain text version, like when you want to forward a batch of old emails to a new address.

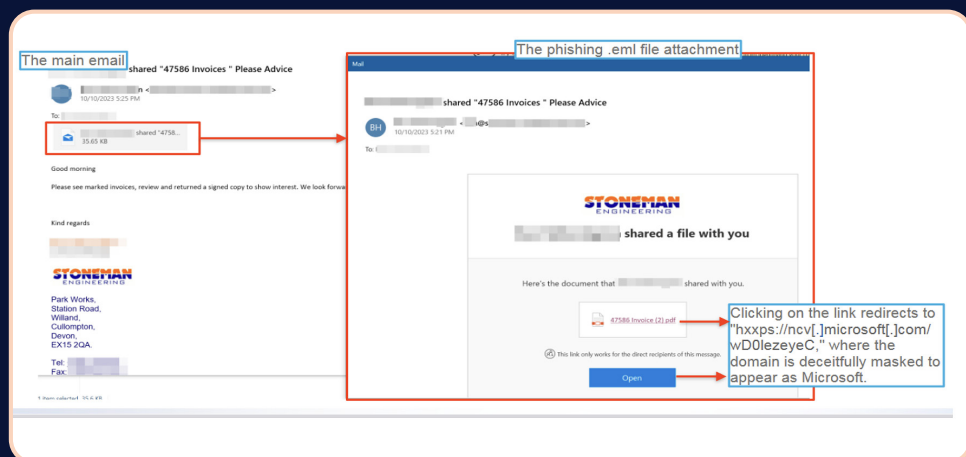
Cybercriminals will place the malicious content inside the .eml file, which gets attached to the actual phishing email and subsequently overlooked by many email security solutions. The fact that this type of file extension is seen so rarely in the business world (but does still happen) increases user curiosity and therefore, chances of opening the .eml file and following its direction, whether it be clicking on a link, opening a web page, or providing credentials.



Here are several signs of an .eml file attack:

- The .eml file can contain plain ASCII text for the header and body, along with hyperlinks and attachments.
- The phrase “shared a file” will commonly appear in the subject line.
- These scams like to incorporate a corporate email footer, complete with company logo and the name of a legitimate company employee.

When you see them in your inbox, they look (and break down) like this:



While .eml scams were popping up all year long, Q4 2023 saw them increase by a factor of ten. It is safe to assume the trend will continue into 2024, as no hacker wants to stop a good thing.

Malspam

Malspam is a spam email that delivers a malicious payload.

In our 2023 findings, there was an even divide between malspam emails with malicious attachments and those leveraging links. This divide is interesting, as last year's figures showed malspam attachments favored 22% more.

The split between quarters is worth noting as well; in Q1, there were 38 times more malspam attachments than links. By the end of the year, malspam links won out nearly two to one. Of those malicious links, 57% belonged to compromised websites while 43% were attributed to cloud storage. Of the attachments, 35% were PDFs, 20% were [ONEs](#), 16% were some form of DOC file, and 13% or less each belonged to XLSX, HTML, ISO, and others.

Feature: Top Malware Families by Quarter

This year, several malware families traded off for “top spot” each quarter.

In Q1, AsyncRAT took the lead in malicious attacks. Known for its ability to remotely monitor and control an infected system, it was introduced on GitHub as a legitimate tool for administrative use but was quickly co-opted for its powerful capabilities. Its most recent versions can evade detection by signature-based antivirus tools.

In Q2, Qbot, also known as Qakbot, left its mark on every single malware link we discovered that quarter. Qbot is delivered via compromised email threads, and the link is most commonly a compromised website or a newly created domain. Created to steal banking information, it also maintains the ability to evade detection, configure persistence, and escalate privileges.

In Q3, RedLine led the pack in malware attacks. This malware family can take full control of a victim's computer, exfiltrate sensitive information (banking credentials and Bitcoin), and is sent via the most innocuous of means, namely Office docs, PDFs, and executables.

In Q4, AgentTesla accounted for the lion's share of malware attacks, followed (distantly) by Redline, Remcos, and NjRAT. This quarter, it seemed all the malware we encountered was designed to target Windows systems, and most are related to Remote Access Trojans (RATs).

AgentTesla, known as a .NET information stealer, scans a victim's machine to see if it hosts one of the browsers on its kill list. If they do, it infiltrates and harvests the victim's sensitive data, sending information like the machine's username, computer name, operating system, CPU name, RAM, and IP address to the attacker's malicious server. It can also take screenshots, kill processes, and collect keystrokes on the infected machine. Targeted browsers include: [Opera](#), [Yandex](#), [Iridium](#), [Chromium](#), [7Star](#), [Torch](#), [Cool Novo](#), [Kometa](#), [Amigo](#), [Brave](#), [Cent](#), [Chedot](#), [Orbitum](#), [Sputnik](#), [Comodo Dragon](#), [Vivaldi](#), [Citrio](#), [360](#), [Uran](#), [Liebao](#), [Elements](#), [Epic Privacy](#), [Coccoc](#), [Sleipnir 6](#), [QIP Surf](#), [Coowon](#), [Tencent QQ](#), [falkon](#), [UC](#), [SeaMonkey](#), [WaterFox](#), [Apple Safari](#), [PaleMoon](#), [IceCat](#), [K-Meleon](#), [Cyberfox](#), [Firefox](#), [BlackHawk](#).

Conclusions



As attackers turn an eye toward the future, security experts must look one step ahead.

Email attack methods are diversifying, and current email security solutions continue to fall further behind. QR code hacks are intensifying, AI is continuing to revolutionize attacks, and more and more malware is being spun up that evades traditional defenses.

VIPRE's Email Security solutions offer layers of protection in the cloud, on-premises, and wherever your workforce does business. Get the benefit of link isolation, attachment sandboxing, link click analysis, threat exploration, and more when you trust VIPRE for your email security and future-proof your defenses.

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.](#)

VIPRE Email Threat Predictions for 2024

Our research over the past year has led to the following predictions for the email threat landscape in 2024:

01

Quishing | We anticipate that attackers will continue to leverage QR codes, or quishing, in their attacks this year.

02

Artificial Intelligence | Cybercriminals will continue to get creative in their nefarious use of AI, using its highly attuned processes to increase the efficiency, reach, and impact of attacks. Scenarios include the regular and continued use of AI to create content for spam emails via deepfakes, AI-generated email content, highly personalized social media mining, and more.

03

Identity Theft | Black Hats will break into inboxes and use AI/ML to learn the victim's communication style when sending emails, then leverage that knowledge for data exfiltration.

04

Cyber Warfare | There will be an uptick in state-sponsored attacks with a particular emphasis on undermining critical infrastructure via phishing, malicious attachments, and other email-based threats.

05

File Types | A wider array of file types will be used to propagate phishing and malware attacks. File formats may include .eml, .pdf, and .ppt, among others.

06

Mobile Threats | Mobile malware is on the rise, as the average user is not highly security educated and more gullible to common attack methods. Mobile users should also be on the lookout for banking trojans and mobile-targeted phishing attacks.



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