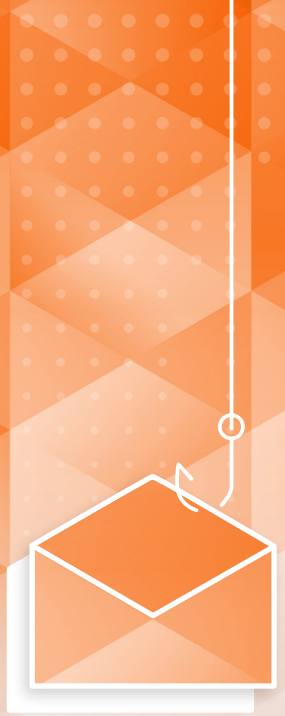
VIPRE SECURITY GROUP



Email Threat Trends Report: 2023: Q1

An Expert Look at Email-Based Threats

Content

Introduction

Hundreds of thousands of emails don't lie. In fact, they tell a story. Here at VIPRE, our mission is to find that story and articulate it to you.

VIPRE is an award-winning global cybersecurity, privacy and data protection organization that's been securing client data for over a quarter of a century. With over four thousand active channel partners, we've been able to protect over 20 million endpoints from malicious attacks. Email threats are out there, and we make it our business to know the tactics, statistics, and attack trends so we can be the best at what we do. While we could withhold this proprietary information, **we've decided that what helps one, helps all. In that spirit, we offer the findings of over 1.8 billion emails (processed between January and March 2023) to the greater security community at large.**

We hope you find our discoveries enlightening. Learning from them will help you prepare against email-based attacks lurking on the threat horizon.

Email Threat Trends of 2023

In Q1 of 2023, VIPRE analyzed nearly 2 billion emails worldwide and 228,000 malicious samples were identified. Of those, 222,000 were classified as spam, with 137,000 attributable to content and 85,000 due to links. An additional 5,000 or so were the result of malicious attachments.

2 billion emails worldwide

228,000 malicious samples

137,000 attributable to content

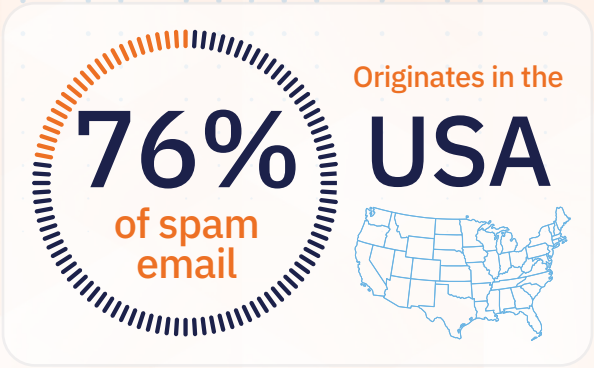
5,000 or so were the result of malicious attachments.

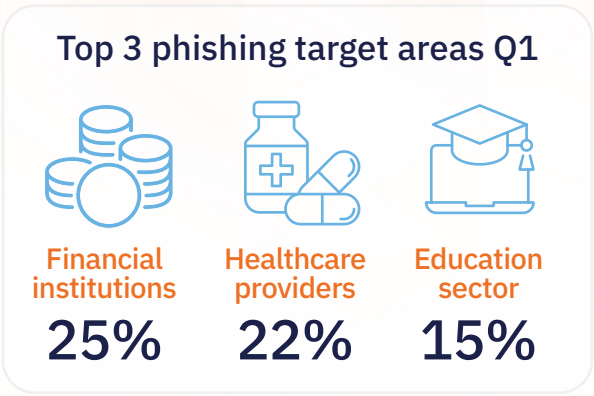
222,000 classified as spam

85,000 due to links

February saw a dramatic increase in malicious email activity, while January and March experienced similar patterns. Contributing to the second month-spike was the activity of Microsoft OneNote malware and various types of phishing campaigns, which will each be reviewed in greater depth further down in this bulletin.

Most of the spam emails were commercial in nature, which differed from last year's report in which scam emails account for most of the list. Second to commercial emails were phishing emails (which can often come across as the same thing). Malware-related emails were the fourth most common form of inbox spam in Q1, influenced also by the aforementioned Microsoft OneNote campaign.





Coming in at number one for the **top country of origin for spam emails was the United States (76%),** for the second year in a row. Three years ago, Russia took the lead, but North America has since commanded the unfortunate top spot. This year, Germany (11%) and Turkey (7%) were the runners-up by a very long shot.

Where phishing is concerned, the United States also claimed a commanding share of malicious IPs, followed by a collective 6% contribution from countries Russia, China, Japan, Canada, Ireland, Singapore, Italy and others. Keep in mind that most data centers are housed in North America, so even if the origin country of the actual exploit was different, US-based servers would skew the figures. However, without the actual country of origin being known, it remains unclear by just how much.

Not surprisingly, for the new attacks **financial institutions received the most heat from phishing and malspam emails** (25%), followed by healthcare (22%) and education (15%). Towards the bottom of the list are construction (7%) and automotive (5%) companies.

Interestingly, phishing and malspam emails also seemed to center around certain geographies; **Europe in particular.** While several European countries were the targets of particularly high attack rates, **the UK saw the majority of them.** One possible explanation for high numbers across the pond was the precipitating climate leading up to the coronation of King Charles III and all the media wave-riding that goes along with it.

The last few years were still inundated with pandemic and post-pandemic-related threats, seeing more campaigns targeting things such as work-from-home job searches. The data from this past quarter would suggest that consumers – and their attackers – are moving beyond Covid-19 and on to the struggles of a striving consumer economy; commercial spam emails topped the list, while health-related ones fell at the bottom (with over 80% fewer targeted campaigns).

Feature: Gone Phishing with Combining Grapheme Joiner (CGJ)

Back in February, we started to notice a pattern of phishing campaigns that utilized CGJ Unicode characters. For example, "CD 8F" (a CGJ hexadecimal character) was found hiding between typical phishing keywords such as "expires", "today", and interestingly, "phishing".

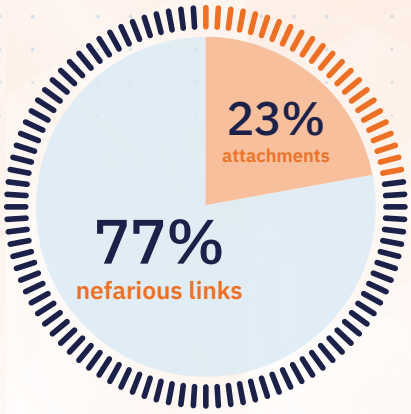
Since many viewer applications don't display this Unicode character, hackers would pepper it in to avoid getting flagged by dictionary-type phishing filters.

The use of CGJ in phishing is a new phenomenon. Here is an example of what a phishing email with CGJ Unicode characters looks like using hex viewer:

Deep Dive: Phishing

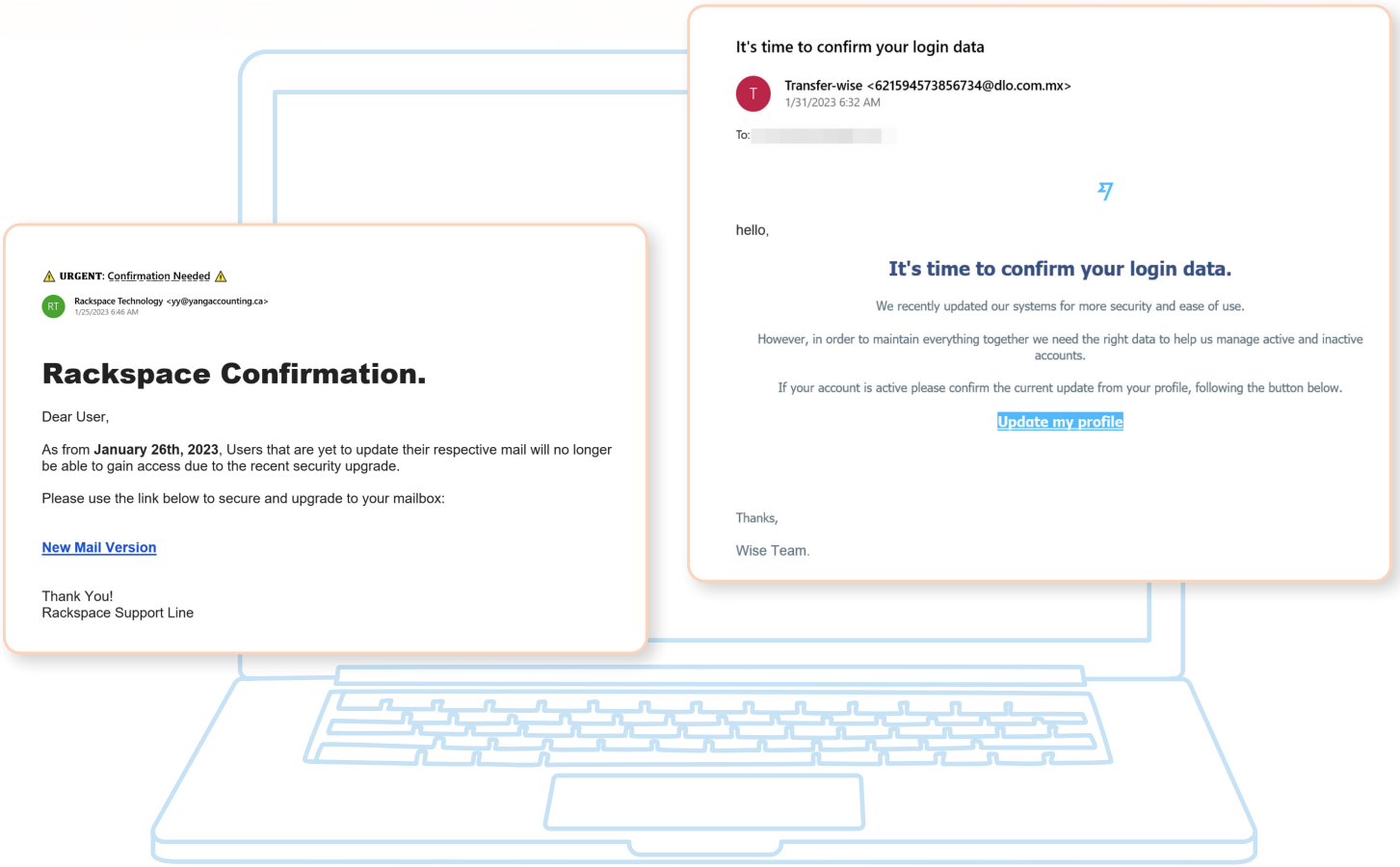
Over one in every four (28%) spam emails we tracked belonged to a phishing campaign.

Of those, 77% utilized nefarious links and 23% leveraged attachments. This shows a 26% increase in the use of malicious links over the email threat landscape last year.

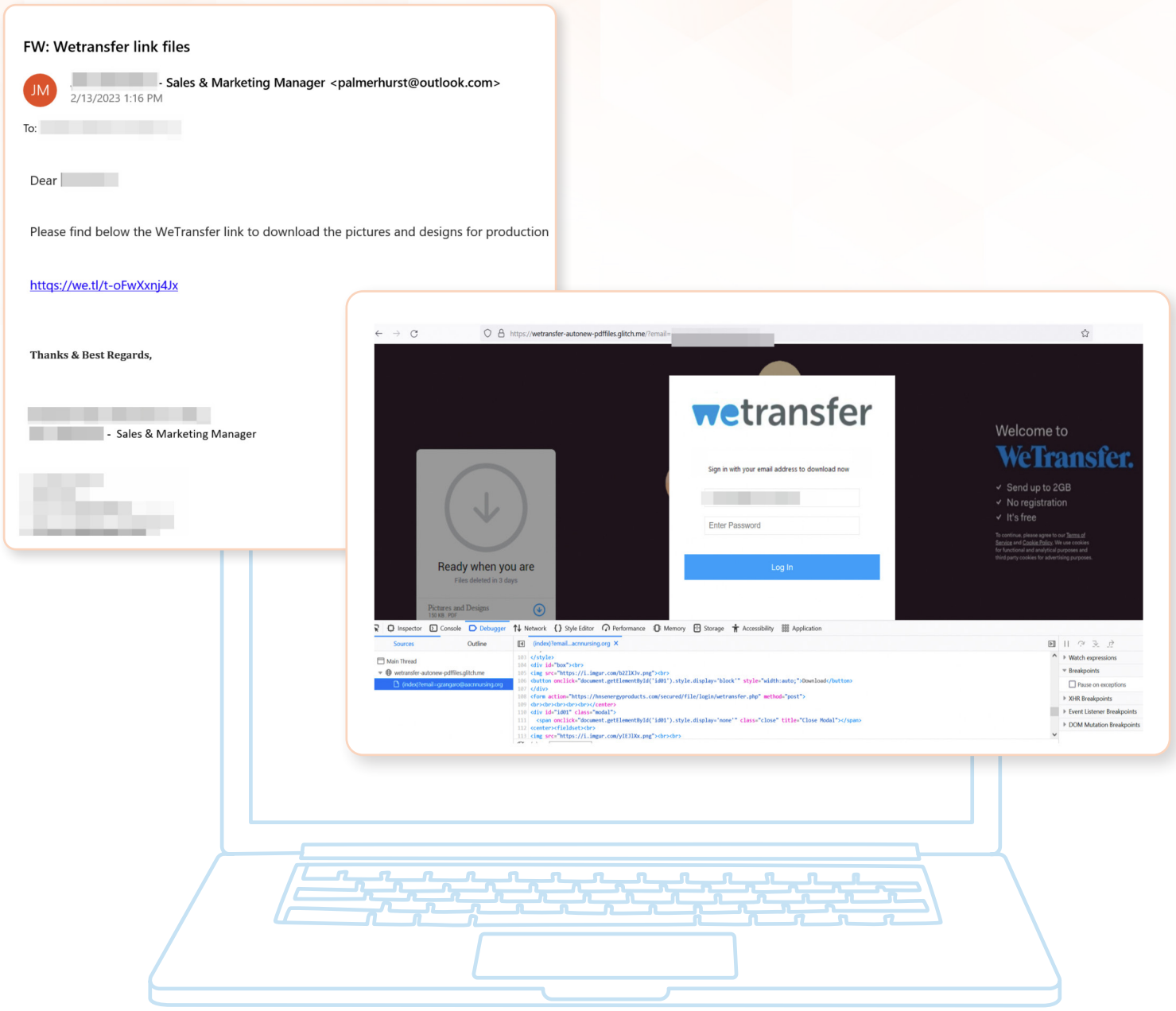


A typical phishing email from our Q1 subset will employ a sense of urgency as it prompts the user to upgrade a service or update their information.

Some examples include:



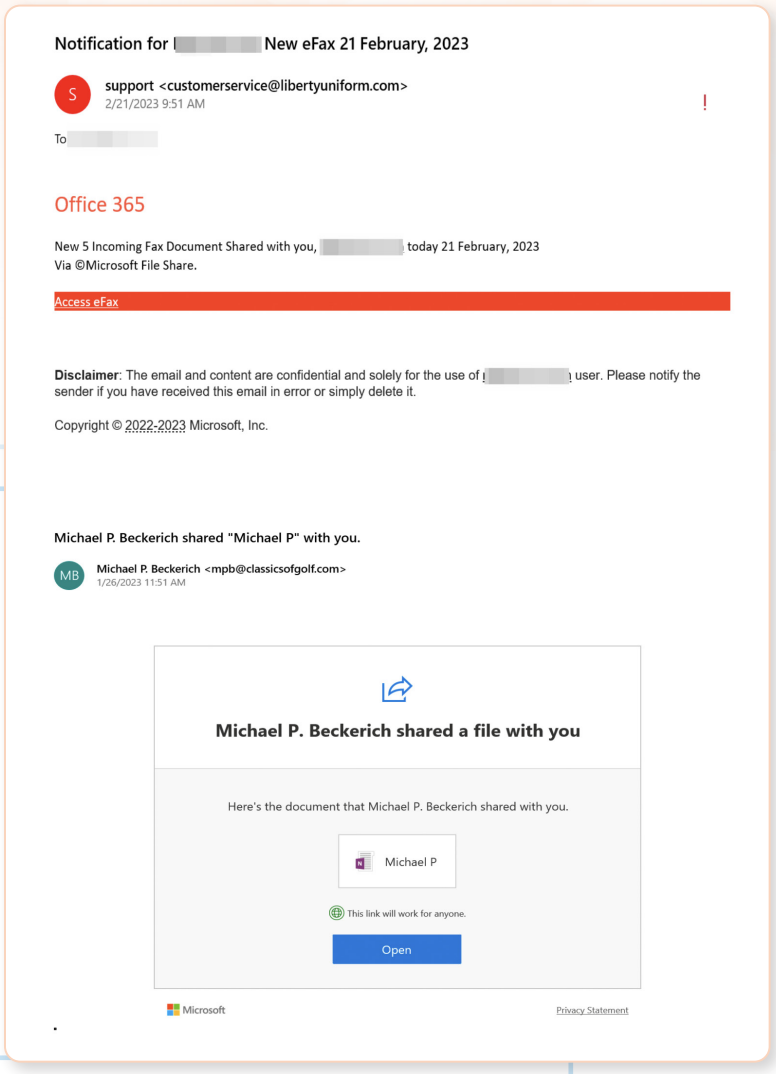
Others will mimic a service already in use and intercept the awaiting customer before the legitimate company can get to them. Consider another real-world example from a "WeTransfer" spoofed email:



Microsoft

Once again, with a combination of both links and attachments, Microsoft was the most impersonated brand of our Q1 2023 dataset. It had nearly three times the use of the next most popular candidates; DHL, WeTransfer, and Apple.

Posing as anything from Microsoft File Share (to bait users with a link) to a benign voice message (an attachment), and displaying Microsoft branding within the emails, can be convincing, and potentially fool the user that the email is actually from Microsoft.



When sending these emails, we found (again, unsurprisingly) that **cybercriminals in Q1 favor the top-level domain (TLD) ".com".** This took the overwhelming share; the next most popular TLDs - ".ca" and ".net" - received less than a fourteenth of the traffic. What was notable, however, was the fact that phishers are resorting to country code top-level domains such as ".ca", ".jp", ".uk", ".de" and ".it".

Malicious Links

Within a phishing email, most malicious links were attributed to compromised websites.

Tactics can include embedding malicious scripts into forms on the site (injection attacks), causing a malware agent to download upon clicking (drive-by download), and swapping legitimate hyperlinks for malicious ones.

The next most common phishing links were newly created URLs specifically designed for phishing, and cloud storage URLs, an ever more popular market in a growing digital economy. The trick to phishing is to blend in with the scenery, and with so many people accessing cloud storage sites on a regular basis – either for work, collaboration, or personal use – sites of that nature commonly deceive users.

The data differs slightly from last year's, but much is the same. Compromised websites and phishing maintain the top one and two positions, but subdomain cybersquatting was the popular third choice of 2022. This year, that was traded for cloud storage URLs. This indicates that criminals are adapting their tactics to the most relevant online searches and services in use, emphasizing the need for constant vigilance on the part of organizations and users.

Malicious Attachments

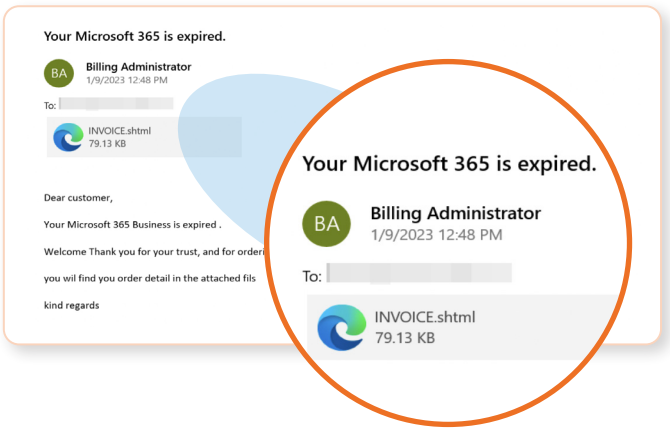
The number one most favored file type for malicious attachments this past quarter was ".html", accounting for 88% of the total share. Contents of these attachments can be coded, obfuscated, and fall under the category of HTML smuggling. This lines up with the data from Q1 2022, although total attachment use has declined from 49% in 2022 to 23% this year. As we noted in last year's report, threat actors usually hide their payload inside of an HTML file by encoding it using base64. They then leverage JavaScript blob and other JavaScript features to assemble the malicious file on the victim's computer.

Other file types in use this past quarter are **".pdf" (7%), ".eml" (4%),** and **".zip" (1%).**

Some examples of names used in all the top malicious attachments are:

File Attachment	File Name
HTML/HTM	• AuthorizationRequest.xls.html • Current Balance_(date).htm • ecomFax.htm • InvoiceCredit.htm • Payment_Reciept_(date)html • PaymentAdvice Note-(randomNnumber).html • Play Audio Attachment.html • Redemption_statement_(randomnumber).html • Remit(randomNumber).html • Remittance Advice.html • Remittance_(randomNumber).html • SOP_Invoice.html
EML	• (Target Name) shared a folder (random phrase) with you.eml • Fee Assigned.html
PDF	• ElecRemittanceAdvice_(randomnumber).pdf • Gloves Collect Remit.pdf • Invoice#(randomnumber).pdf • Rcpt#(randomNumber).pdf

However, the most popular attachment ploy utilizes the term "invoice":



Deep Dive: Malspam

While attachments may have taken a back seat in phishing emails, they certainly took the lead when it came to malspam emails.

In Q1, a staggering 97% employed attachments as their primary tactic. Only 3% utilized malicious links, and of those, all were compromised websites.

Here, the most popular attachment type belonged to a Microsoft OneNote file (".one"), with 64% of the total percentage.

DOC/DOCX files came next at 17%, followed by ISO files (9%), and the remaining 10% attributable to ".zip", ".xls", ".jse" and others.

Some sample attachments names within the malspam spread include:

File Attachment	File Name
ONE	• account_statement.one • adocu(randomNumber).one • Invoice#(randomNumber).one • Invoice_due.one • Iremittanceadv.one • shared_document.one • Invoice#(randomNumber).one • Shipment Document.one • wiz.one
DOC/DOCX	• document(randomNumber).doc • Delivery-report(date).docx • invoice.docx • invoicecerec(randomnumber).docx • reference_shipment.doc • req#(randomNumber.docx
ISO	• packageUpdater.iso • PO(randomNumber).iso • ref.iso • Shipment-(date).iso
XLS/XLSM	• (adv_reciept(date).xlsm • REQ(randomNumber).xls • (ship#(randomnumber).xls
JSE	• airfreeMachine.jse • zoom.jse
ZIP	• Document#(randomNumber)_PO.zip • PO_att(randomNumber).zip

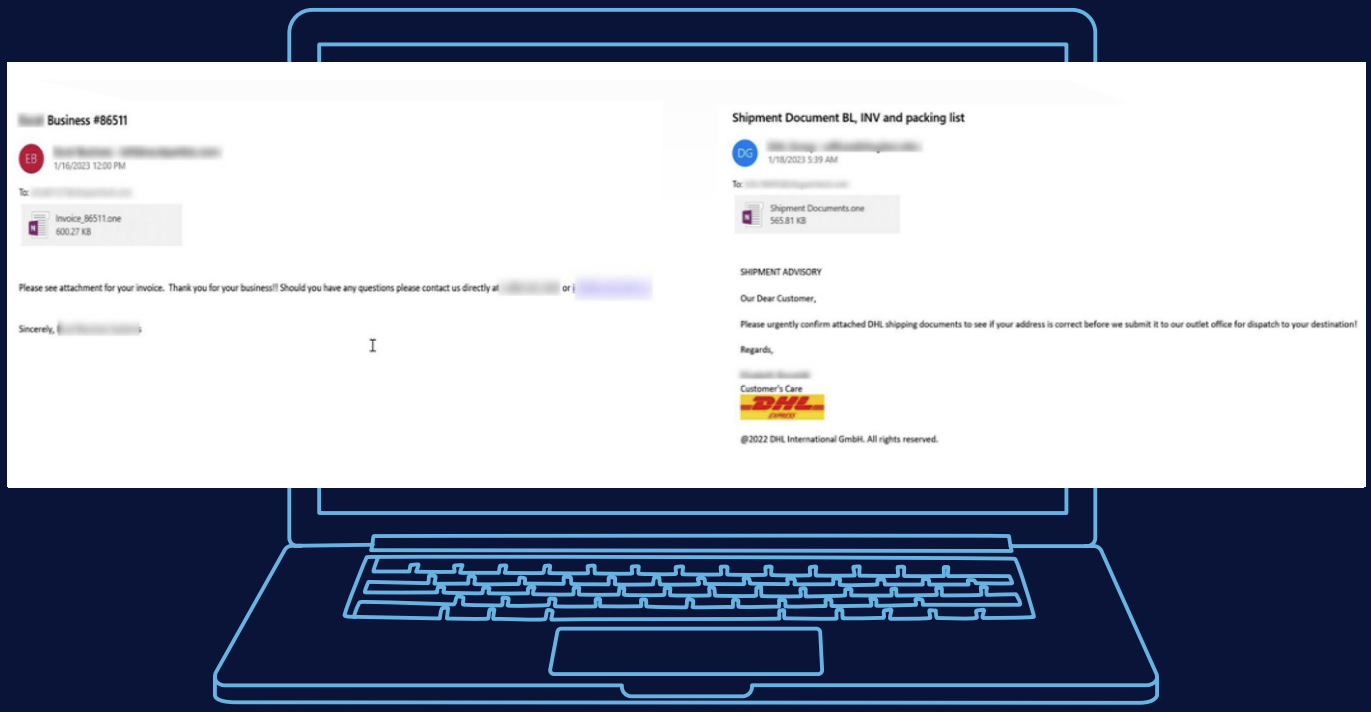
One interesting development is that QBot, last year's most popular malware family, was replaced by this year's AsyncRAT. In fact, most malspam exploits in Q1 2023 are related to Remote Access Trojans, or RATS. Following were more malware strains recently stuffed into .doc files. They are, in order, RedLine, Agent Tesla, Netwire RAT, and several down the list – QBot.

RATs are malware specifically designed to allow an attacker to control a host machine remotely. Once the remote access trojan is embedded within the target, it can start sending commands back and exfiltrating data. This is a popular way to control a machine remotely, and allows attackers to easily steal passwords, screenshots, keystrokes, files, and other sensitive data.

Feature: Spotlight on Microsoft OneNote and AsyncRAT

Ever since Microsoft disabled Macros by default, criminal hackers have been on the hunt for new ways to exploit the Microsoft Office Suite. They found one in Microsoft OneNote. The innocuous .one file can hide embedded malicious files like .exe, .vbs, .bat, .cmd, and .lmk, which in turn deliver malware payloads like QBot, RedLine, and AsyncRAT.

Malspam emails containing Microsoft OneNote can look like this:

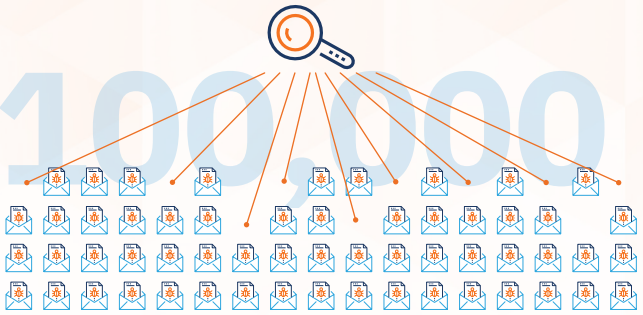


Speaking of malicious payloads, let's dig deeper into AsyncRAT, the top malware family of 2023 per our report. First active in 2016, the AsyncRAT malware is known for its ability to remotely monitor and control an infected system. It was originally introduced on Git Hub as a legitimate open-source tool for remote administration, but it has since been leveraged as a powerful hacking tool by bad actors. Its most recent version evades detection with a specially designed .bat loader, much like URSA and other trojans. AsyncRAT uses the .bat loader to take advantage of different load stages, and with a lot of obfuscated code, manages to bypass AV/EDR detection. With the RAT installed on the system, tools like VirusTotal will render a clean bill of health. As researchers explain, "the file not being detected is likely due to a long string added in the file multiple times (more than 100) by the attacker." **Ultimately, security solutions need to be able to spot signs of threat behavior, not just threat signatures.**

Never-Before-Seen Email Threats Found with Behavioral Detection

Ultimately, there were several instances in particular that really pulled our focus this past quarter.

Of all the malicious emails that were detected, over 100,000 were discovered due to behavioral detection techniques: They were new to the wild and had no known signatures. The scary fact is that a company with basic signature-based email security would have missed all of these.



These are **never-before-seen malicious attachments** that classical AV engines do not catch. However, with an email security platform that supports behavioral-based detection for attachments, customers can keep these attacks on their radar. Otherwise, they will slip through.

Secondly, there were **over 10 million links protected by Link Isolation.** Of those, 74,000 were detected at click time. At the point-of-click, a link that once registered as safe could have been compromised only minutes before. Link Isolation provides dynamic link protection by scanning, rewriting malicious links, or preventing access.

10 MILLION
links protected by Link Isolation

Along with those figures, another **10,000 bad sites were detected by DeepLink, another behavioral-driven tool.** These are, again, never-before-seen malicious links that were not recognized on any blocklist-based detection engine. To be aware of them, customers would need to have behavioral-driven tools primed to spot indicators of bad behavior. Without them, these emerging exploits would have had a clean entryway into an unsuspecting system. By the time they were detected, it would have been too late.

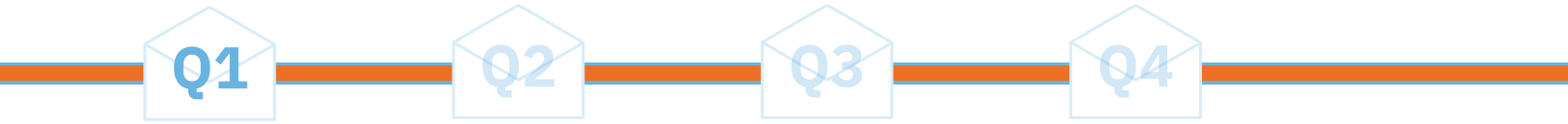
Conclusion

Cybercriminals are expanding their email warfare tactics while sticking with a few tried-and-true methods. Bad links are here to stay. Attachments have not fallen out of style, and HTML is still the preferred tool of use. However, as traditional email security solutions increase in strength, savvy bad actors are changing schemes.

Now, advanced **behavioral-driven email security detection is required to keep up with the emerging threat trend** increasing across the board. Tools like XDR, EDR, and NDR have cropped up to handle the influx of similar threats across endpoints and ecosystems, and the time has arrived when dedicated email solutions require the same AI-powered detection capabilities. Waiting for signatures is not enough when hundreds of thousands of emerging threats no longer have one.

VIPRE's Q1 2023 Email Threat Bulletin is designed to educate organizations on the most to-the-minute criminal tactics of email exploiters. Staying ahead of today's most prominent exploits and emerging risks requires best-in-class email security solutions that can scale to whatever email threats may lie on the horizon – known or unknown.

Stay up to date and look out for the next installment of the Q2 VIPRE Email Threat Bulletin



Email Threat Trends of 2023

Sign up today for your FREE 14 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