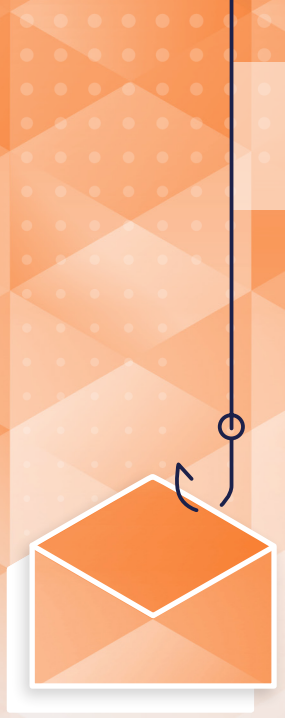
VIPRE SECURITY GROUP



Email Threat Trends Report: 2024: Q1

An Expert Look at Email-Based Threats

Content

Introduction

VIPRE's Email Threat Trends Report - Q1 2024: PikaBot Malware, Up Coming Elections, and The Clever Phisherman.

We come out of Q1 swinging with tales of new phishing campaigns, horror stories of emerging malware, and warnings of all the email troubles an election year can bring. Here at VIPRE, we make it our business to tell you the attacks we see on the horizon – so you know them when you see them in your inbox.

We've been around for nearly three decades, offering over 25 years' worth of malware protection to our over 50,000 clients globally. The VIPRE Security Group secures over one million endpoints, has over four thousand active channel partners, and processes billions of emails every quarter. We offer our clients cutting-edge machine learning, real-time behavioral monitoring, and one of the largest threat intelligence clouds on the planet. Every day, VIPRE is pushing the boundaries in email protection as we continue to perfect proprietary protection techniques few others offer.

As we do every quarter, we make our proprietary email security findings available to the global cybersecurity community. We feel it is important to know, with real-world examples, what our adversaries are up to. But we're not here to scare you – at VIPRE, our mission is to arm you.

YoY Email Threat Trends of 2024

In the first quarter of the year, VIPRE processed 1.8 billion emails, 234 million of which were spam (12 million more than last year), and 11 million of which could only be caught by Link Isolation, our proprietary behavioral-based detection technology.

We drilled down into 20,374 email samples for our analysis, discovering that an overwhelming 95% of them were spam, in keeping with our findings from a year ago. And just like Q1 2023, we saw spam messages spike for one month, but this year it was March (not February), due to two phishing and one email spam campaign.

What did the emails contain? Aside from the 3% that were work-related or otherwise legitimate, the spam category broke down into commercial emails, scams, phishing emails, and malware, by volume. Different from last year, scams overtook phishing emails in popularity this first quarter.

Again, the US was the main source of spam emails, but not by as high a margin as this time last year. In Q1 2023, the US accounted for 76% - this quarter, 66%. The runners-up also changed; from Germany and Turkey to Great Britain, Ireland, and Japan. Possible socioeconomic factors could contribute to the sway, or it could be nothing more than criminal hackers bouncing from place to place as analysts get wise to their geo-specific tricks. It's good to keep in mind that many threat actors use servers based in other countries (predominantly North America) but they themselves live elsewhere.

As for countries that were the targets of email-based attacks, the list looks very much the same as those apparently sourcing it; the US (76%), Great Britain (11%), and uniquely, Canada (9%) are the top three.

In Q1 2024

66% OF SPAM

Originated in the US

The main targets of email-based attacks were (Top 3):

US - 76%
Great Britain - 11%
Canada - 9%

The good news?

VIPRE Email Security Link Isolation, one of our features, detected and protected over 41.9 million links clicked by users in 2023.

We're pretty proud of that.

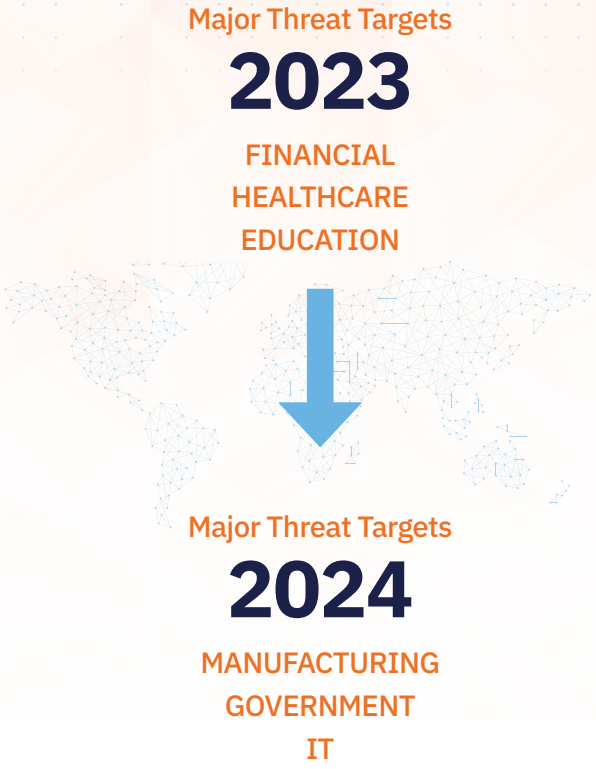
YoY Email Threat Trends of 2024

One thing that perhaps changed the most between this year and last was the sectors being targeted. In Q1 2023, the most victimized industries were:

- Financial (25%)
- Healthcare (22%)
- Education (15%)

In Q1 2024, the sectors most hit by malicious emails were:

- Manufacturing (43%)
- Government (15%)
- IT (11%)



With an obvious landslide in favor of manufacturing. While manufacturing's click rates aren't necessarily higher than other industries' they are on track to achieve over $15 million value-added this year and have been experiencing steady growth. Deloitte notes that because of recent tax incentives to the US manufacturing sector "the IIJA, CHIPS, and IRA have already spurred record private sector investment in the manufacturing industry." Cybercriminals know this and are likely riding the wave.

And finally, election-related email scams are rearing their ugly heads again. While we'll cover the issue more in-depth later in the report, suffice it to say that it's an unwelcome surprise to nobody that the US 2024 presidential election is driving up fraudulent emails of this sort. However, the worst part is that they not only endanger individuals or companies, but an entire democratic process. Some copy-and-pasted examples we've included can help voters stay wary.

Feature: What Only VIPRE Can Do: Proprietary Techniques

Link Isolation

We spoke of pushing the edge. VIPRE Email Security Link Isolation, "like URL sandboxing for your email," caught over 11 million emails that would have gone undetected otherwise.

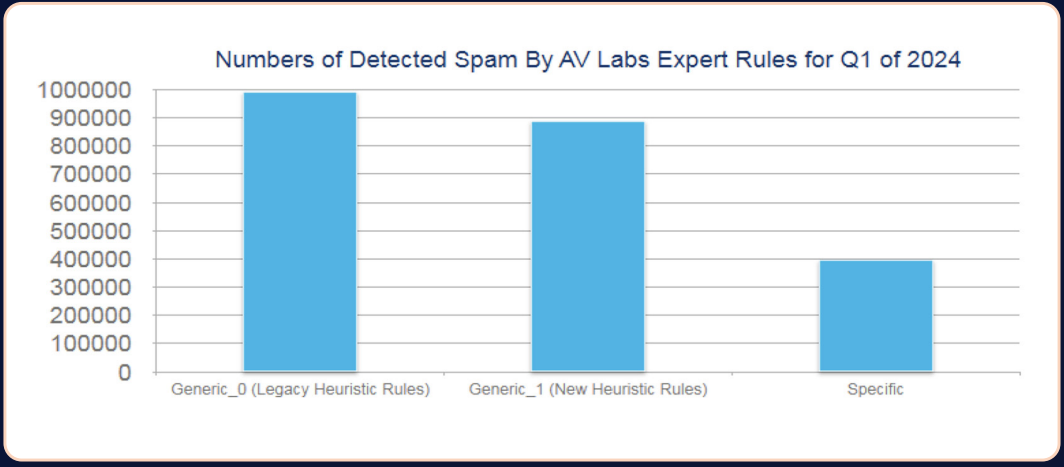
What other tools can't catch is what's on the webpage *before* it's opened. With Link Isolation, users can. And then, Link Isolation rescans the link every time the user clicks on it, in case the site has been compromised in the meantime. It's living, breathing email security that works just the way the criminals do.

Of those 11 million emails caught in the Link Isolation net, 72,000 were detected at click time. Of those, 84% were flagged due to content and the other 16% were caught by enabling Deeplink, an option that allows Link Isolation to analyze malicious URLs using deep, cloud-based scanning.

VIPRE Expert Rules

These rules are curated and maintained by VIPRE AV Labs to enhance detection and keep up with the latest email threats.

The generic rules (Generic 0 and Generic 1) detected over 1.8 million spam emails in Q1 of 2024. Specific rules refer to signature-based detection, leveraging mostly strings or phrases of known spam emails. Our proprietary rules collectively detected nearly a quarter million spam instances in the first quarter alone.



Feature: XSS Flaw Exploited for Phishing

This past quarter, VIPRE AV Labs observed a notable sample exploiting a web application vulnerability called Reflected Cross-Site Scripting (XSS) focusing on the tag attribute "href". To circumvent detection, the attacker resorted to various tactics, including:

- Using images as the entire content of the email
- Encoding the URL to conceal the XSS vulnerability attempt
- Directing the victim through multiple URLs

Before landing on the phishing website. Additionally, the format of the URL containing the XSS is uncommon for business emails. See the example below:

Encoded URL:

```
hxxps[:]//www[.]lawlibrary[.]ie/find-a-barrister/search-results/?r=49&member-
type=barristers&KeyW=%22%3E%3Cscript%3Ewindow%5B%27location%27%5D%5B%27replace%27%5D(%
5B%27%68%27%2C%27%74%27%2C%27%74%27%2C%27%70%27%2C%27%73%27%2C%27%3A%27%2C%27%2F%27%2C
%27%2F%27%2C%27%63%27%2C%27%75%27%2C%27%74%27%2C%27%74%27%2C%27%2E%27%2C%27%6C%27%2C%2
7%79%27%2C%27%2F%27%2C%27%39%27%2C%27%77%27%2C%27%47%27%2C%27%31%27%2C%27%52%27%2C%27%
34%27%2C%27%74%27%2C%27%68%27%5D%5B%27join%27%5D(%27%27)),document%5B%27body%27%5D%5B%
27style%27%5D%5B%27opacity%27%5D=0x0;%3C/script%3E
```

Decoded URL:

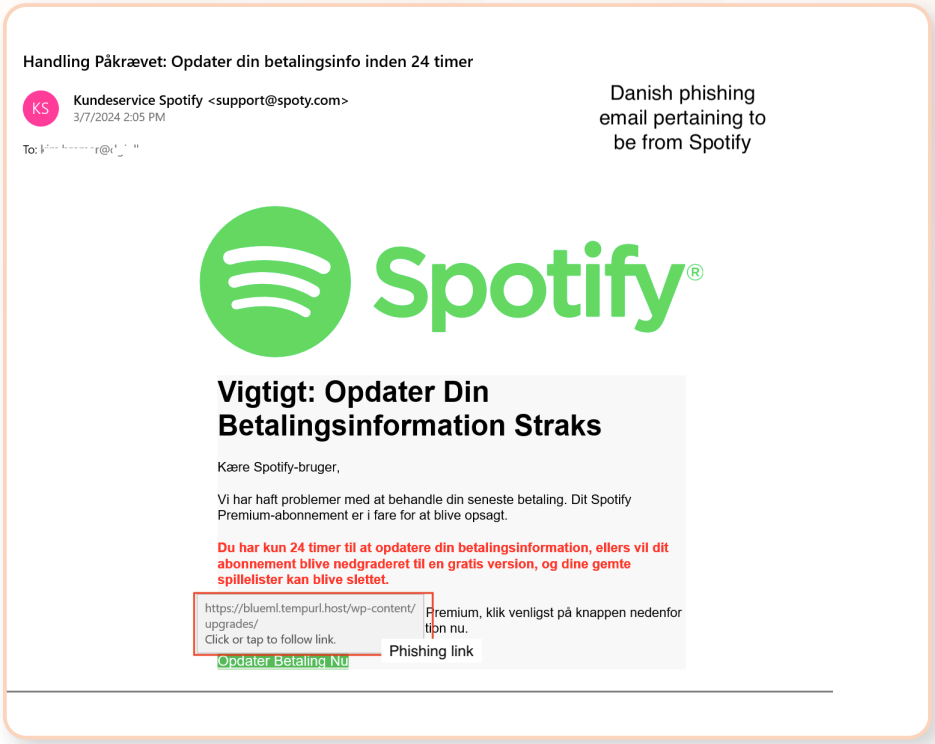
```
hxxps[:]//www[.]lawlibrary[.]ie/find-a-barrister/search-results/?r=49&member-
type=barristers&KeyW= "><script>window['location']'replace',document['body']['style']
['opacity']=0x0;</script>"
```

For a more in-depth review, see our article on the exploit here.

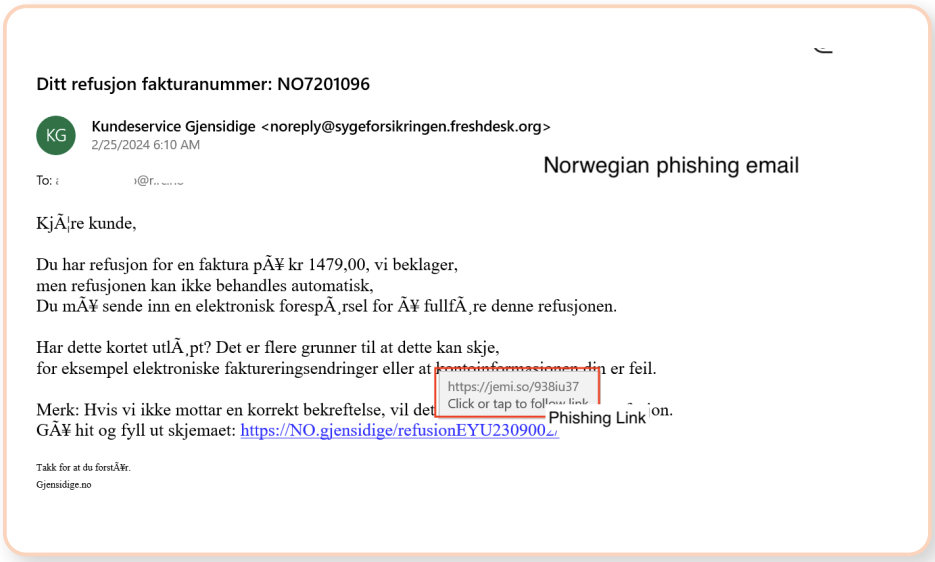
Phishing Trends

Caught in the Wild

Here are a few examples of real-world phishing scams caught in the act by VIPRE in Q1 of 2024.



Norwegian phishing email



Phishing Trends

Caught in the Wild

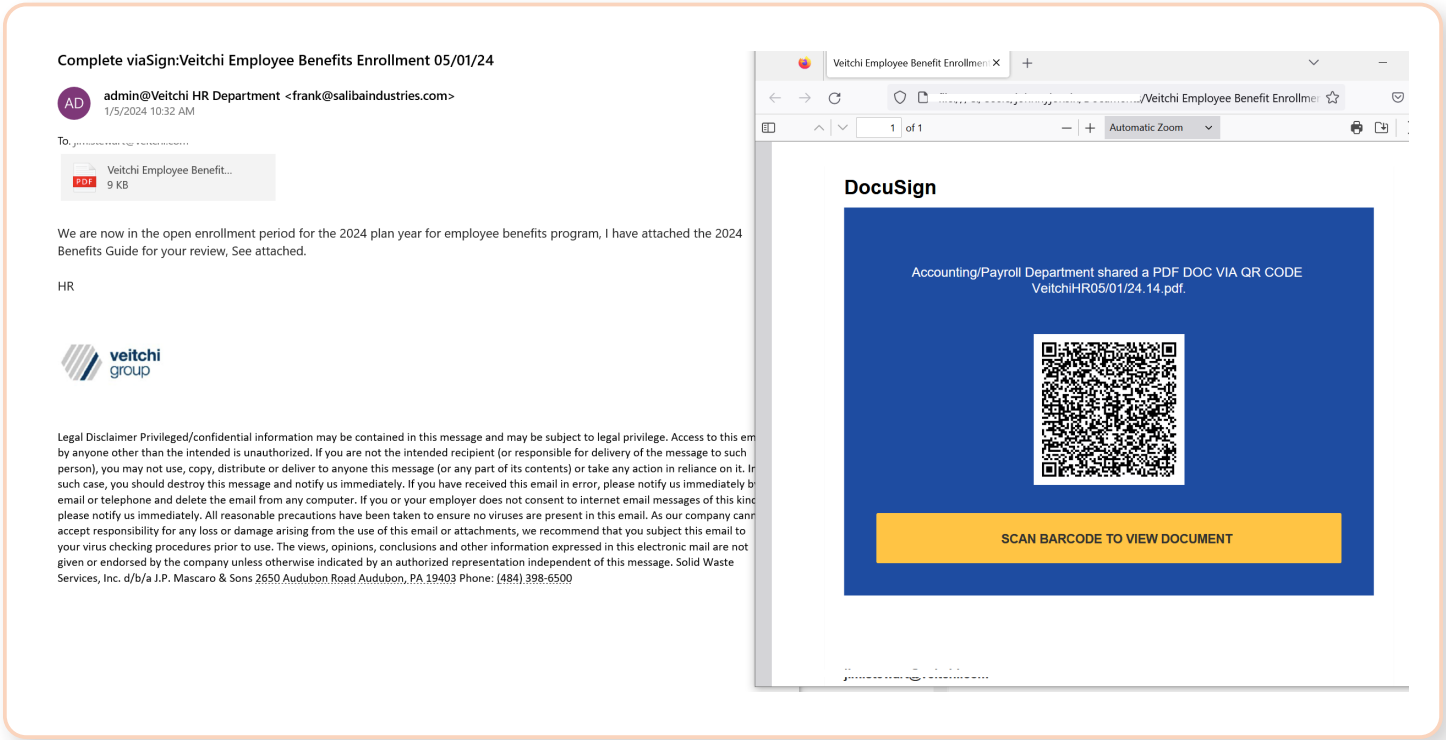
Thanks to the advent of generative AI technologies like ChatGPT, highly convincing phishing emails can now be sent in virtually any language.

However, there's often no more chance of telling whether ChatGPT wrote the email than there is of finding out the link is malicious – until it's too late. Without a tool like VIPRE that can scan links before they're opened, many users are forced to find out the hard way.

HR is Calling, It's for You

Beyond well-known brands, our observations for Q1 of 2024 indicate a notable increase in phishing emails masquerading as communications from human resources.

These emails often falsely claim to relate to employee benefits, compensation, or insurance within a company. Upon opening the attachment, typically in .html or .pdf format, recipients encounter a phishing QR code. Scanning this code redirects users to a phishing website. See the example below and be careful not to scan.



Phishing Trends

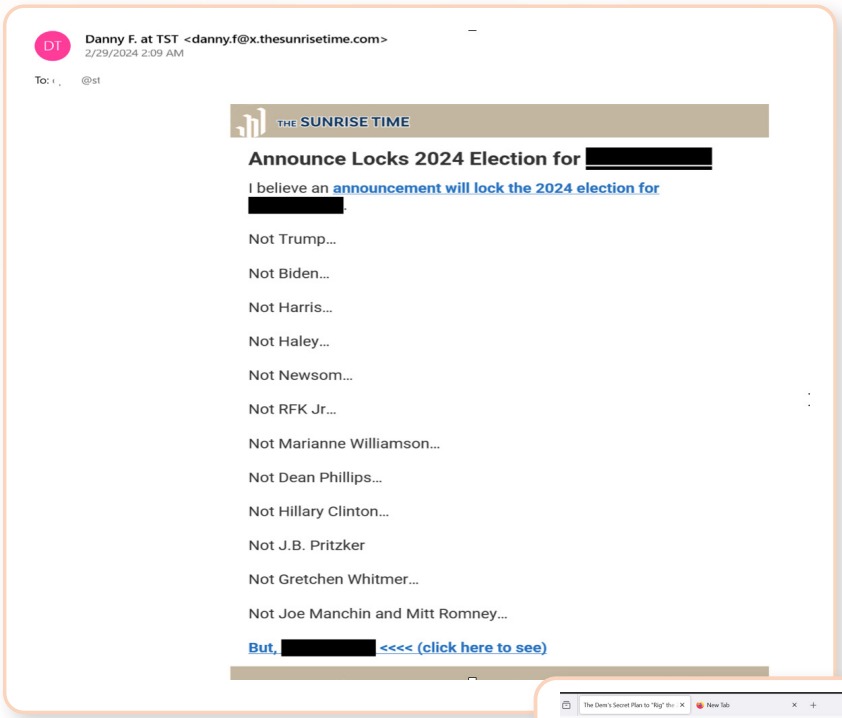
Election Scams: They're Back

Phishers are opportunists, and there is perhaps no bigger wave this coming year, or one that will garner more online attention, than the 2024 US presidential election.

With so much curiosity abounding, threat actors have already been quick to capitalize, and will likely only increase their efforts as election day draws nearer.

Here are some examples caught by VIPRE that highlight their various forms.

Some, amazingly in this post-ChatGPT world, employ poor grammar:

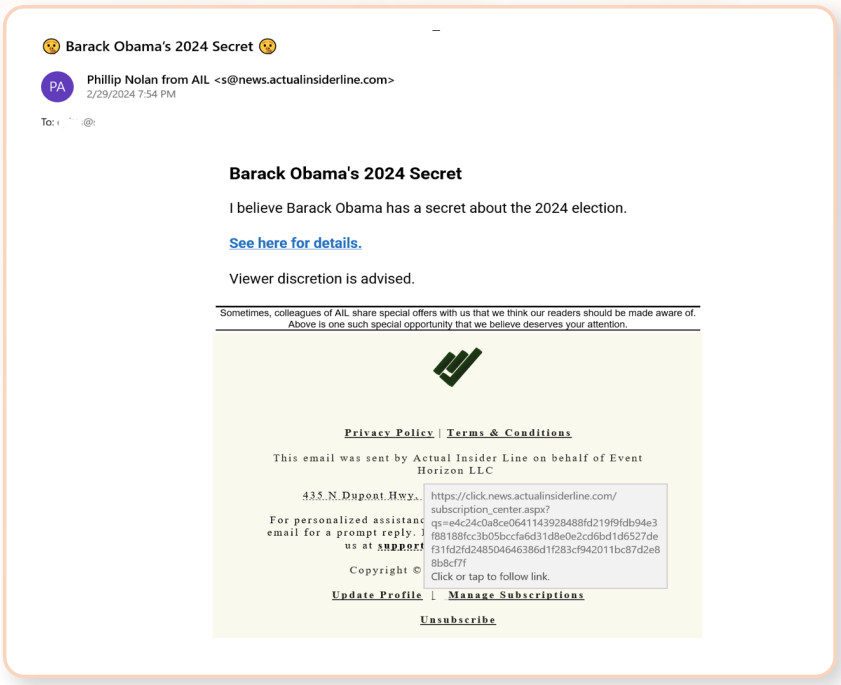


Some play on sensationalism and divisiveness:

Phishing Trends

Election Scams: They're Back

And some seem outright scammy:



Barack Obama's 2024 Secret

PA Phillip Nolan from AIL <s@news.actualinsiderline.com>
2/29/2024 7:54 PM

To: [redacted]

Barack Obama's 2024 Secret

I believe Barack Obama has a secret about the 2024 election.

See here for details.

Viewer discretion is advised.

Sometimes, colleagues of AIL share special offers with us that we think our readers should be made aware of. Above is one such special opportunity that we believe deserves your attention.

Privacy Policy | Terms & Conditions

This email was sent by Actual Insider Line on behalf of Event Horizon LLC

435 N Dupont Hwy.

For personalized assistanc
email for a prompt reply.
us at support

Copyright ©

https://click.news.actualinsiderline.com/subscription_center.aspx?qs=e4c24c0a8ce064114392848fd219f9fdb94e3f88188fcc3b05bccfa6d31d8e0e2cd6bd1d6527def31fd2fd248504646386d1f283cf942011bc87d2e88b8cf7f
Click or tap to follow link.

Update Profile | Manage Subscriptions

Unsubscribe

With so much hanging in the balance the best-case scenario is that a few unsuspecting persons get scammed. When it comes to misinformation, microtargeting, and government elections, we all know the worst. It is extremely important that US voters have their critical thinking caps on throughout the campaign season and get their information from a reputable source – and preferably from its official site (as typed into a search bar, if necessary) and not unbidden from a salacious email.

Common Phishing Phrases

Now it's time to test your knowledge. How well would you recognize a common phishing phrase if you saw one? Here are some commonly used ones that should raise a red flag:

- 2FA Authentication is outdated
- Benefit payroll
- Changes for upcoming payroll enrollment
- Clear your cache to free space
- Email quarantined
- Password expiration notice
- Review and update your subscription details
- Statement of account review

Many of these offer legitimate services, which is exactly their aim and their weak spot. If you really do require aid in one of these areas, you can search out the service directly through a front-door channel (contacting your HR department directly, for example) and not risk replying to an unsolicited message with a convenient link.

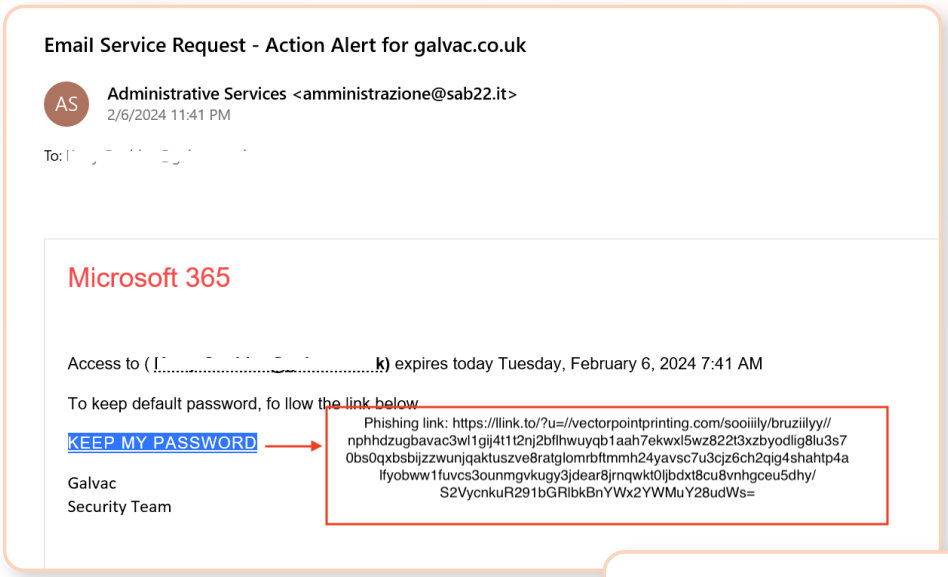
Phishing Statistics

Links vs. Attachments vs. QR Codes

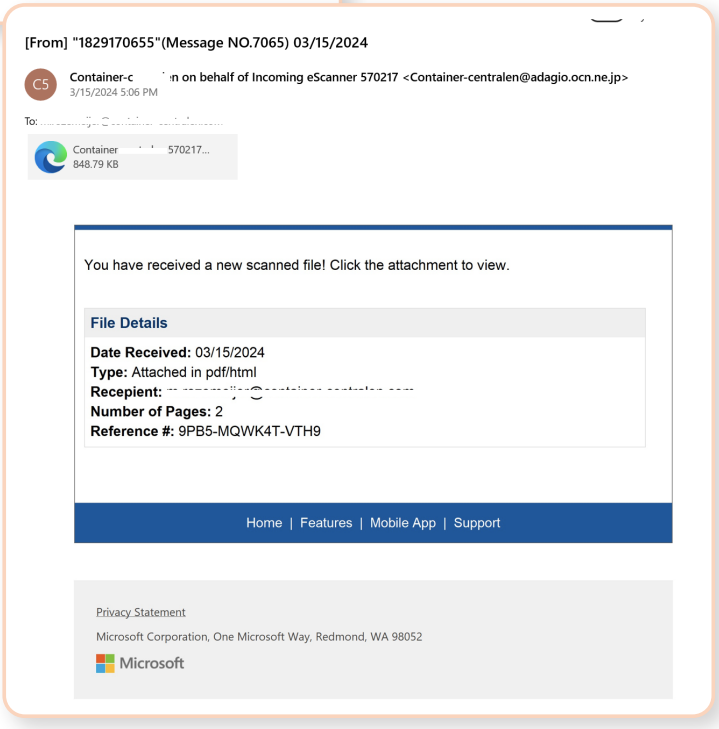
Three years ago, it was a 50/50 split between phishing emails utilizing links versus attachments.

Last year, that ratio changed drastically in favor of links, and that lead has held into 2024. In Q1, VIPRE AV Labs analysis revealed that 75% of phishing emails leverage links, while 24% favor attachments and 1% are using QR codes (quishing). This is in tune with our findings which indicate that phishers are leaning into emails which encourage users to update or change their passwords – an innocuous enough ask in a climate of data privacy and hygiene.

Microsoft-themed phishing email with link



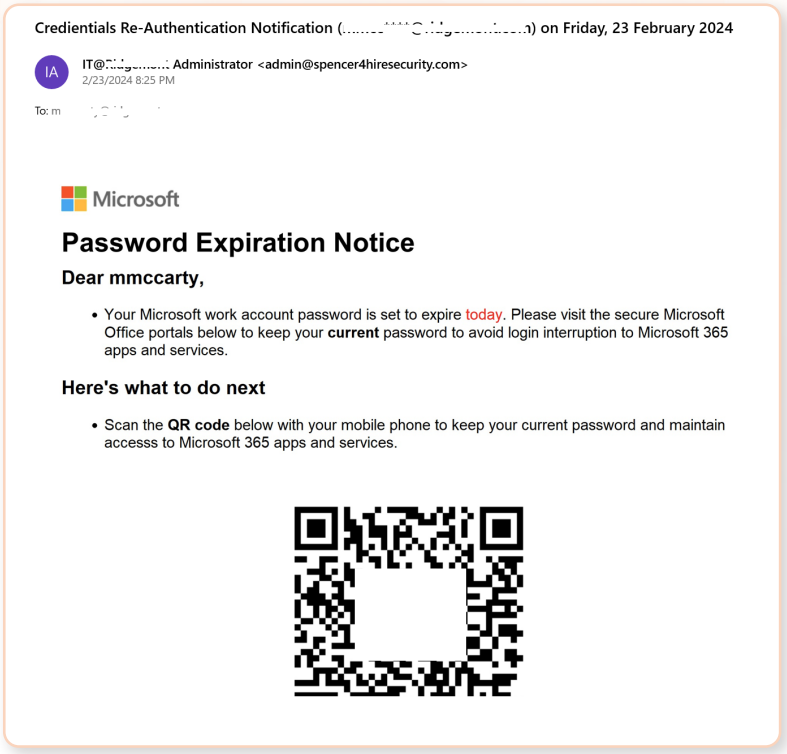
Microsoft-themed phishing email with attachment



Phishing Statistics

Links vs. Attachments vs. QR Codes

Microsoft-themed phishing email with QR code (please, don't scan)



Most Spoofed Brand

Historically, Microsoft has been the most spoofed brand, and this quarter was no different. And why not? Investing.com notes that Microsoft users increased by 894% in 2020 alone, and four out of five Fortune 500 companies use Microsoft Office 365. It's a safe bet for scammers.

However, this quarter's runners-up did change. Here's a side-by-side comparison:

Q1 2023

- Microsoft
- DHL
- WeTransfer
- Apple

Q1 2024

- Microsoft
- DocuSign
- eFax
- PayPal

Last year, it was physical packages, file sharing, and anything Apple. This year, phishers are baiting users with ways to digitally send faxes (perhaps hoping to catch an older, less cybersecurity-savvy crowd), the now less-popular PayPal (again, perhaps hoping for an older user who wouldn't have opted for Venmo or Cash App), and DocuSign, the all-too-familiar online signing agent used to ink important documents like loans, insurance papers, and other legal documents. The common thread that could run through each of these services is, perhaps, a generational gap that criminal hackers hope belies a gap in security knowledge as well.

Phishing Statistics

Most Common Top-Level Domain (TLD)

While the fact that ".com" was again the most favored TLD by attackers is no new news, the runners-up again are. In Q1 2023, ".ca" and ".net" took second and third place, respectively, but this year the lineup looked like:

1 .com
2 .org
3 .uk
4 .cloud
5 .fr

And .jp, .net, and .se trailing behind. Possible reasons? ".Org"s inspire trust, ".uk" may not be viscerally associated with scams (although that might be changing), ".cloud" emails are becoming ever more common in a society that's all but migrated to it, and ".fr" might share the same neutral or positive – or perhaps, simply "as yet unsullied" - online reputation to oft-targeted Americans as the UK.

Favored Phishing Link Strategies

The malicious phishing emails employing links were categorized into five basic categories to highlight the methods most preferred by attackers. They are as follows:

1 .URL redirection (54%)
2 Compromised websites (22%)
3 Newly created domains (15%)
4 File storage links (6%)
5 XSS vulnerability links (4%)

In Q1 of last year, compromised websites and newly created domains retained the two top spots. This year, they were both bumped down in a big way by URL redirection, a technique that opens a different web page when the desired web page is clicked – essentially, a bait-and-switch. The benefit of this, as threat actors have apparently seen in large numbers, is that the legitimate URL will avoid detection by most email security tools and users alike, while back-end, a malicious link is doing its dirty work.

Without a tool like VIPRE's Link Isolation that safely sandboxes the URL before opening, users may ignorantly click the link and regret it later.

Malicious Attachments

Unlike Q1 last year, the most used attachment file type wasn't .html at a whopping 88%, but .pdf at a more moderate 51%. Following this quarter was .html (30%), .eml (7%), and .zip (2%). We also saw some new additions not detected on our radars last year, such as:

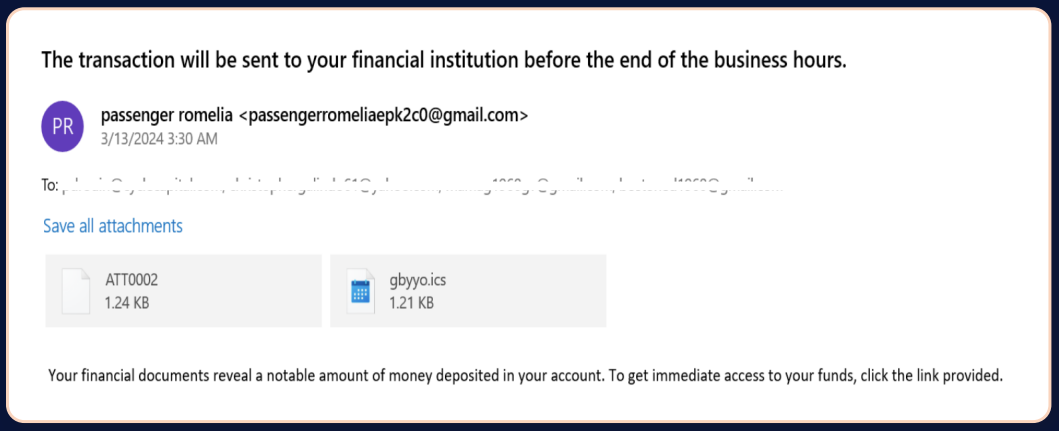
- .rtf
- .ics
- .txt

Feature: ICS and RTF Attachments

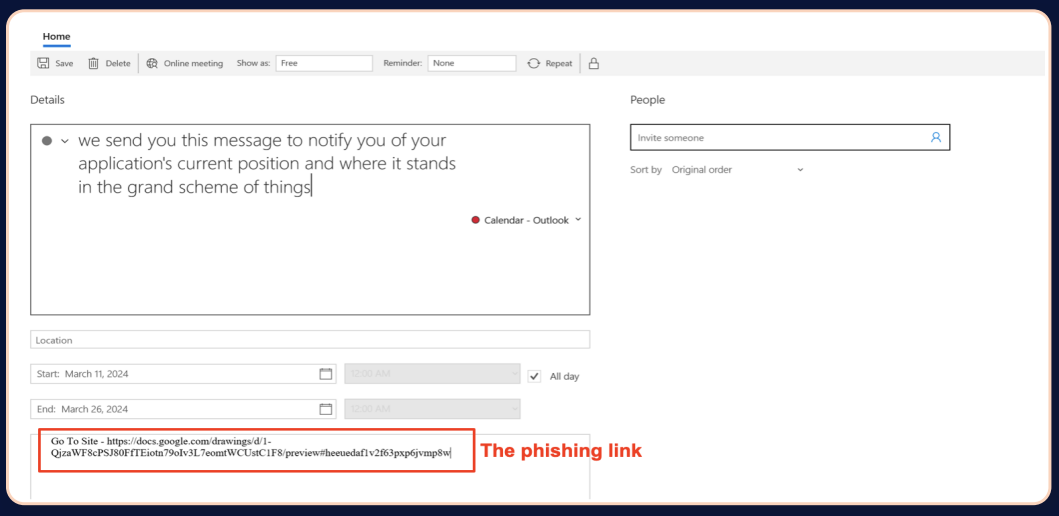
Threat actors are known for their persistent efforts to devise new methods for delivering malicious or phishing attacks to unsuspecting victims.

During our Q1 detections, we uncovered a recent trend involving the use of less common file formats in phishing attacks, Specifically, attachments in formats such as .ics (calendar file format) and .rtf (rich text file format). Although not many EML samples are currently found to be related to this trend, we predict that it may become more prevalent in the following months of this year.

ICS phishing email: This phishing email does not contain a link; instead, it includes a .ics attachment with a random filename.



Note the sense of urgency induced by the use of words like 'immediate.' Additionally, the email may originate from a free email service provider, such as Gmail, which is often a red flag for suspicious emails. Also, the use of colloquialisms and cliches, especially in a context where business-level writing is expected, can provide additional clues (note the use of "in the grand scheme of things"):



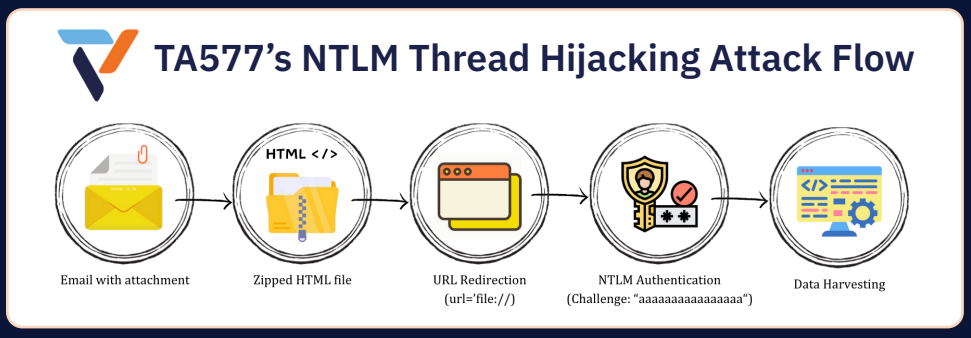
Feature: NTLM Phishing Attack

In a notable incident observed by VIPRE AV Labs before the end of February, a series of deceptive messages emerged, masquerading as replies to previous emails.

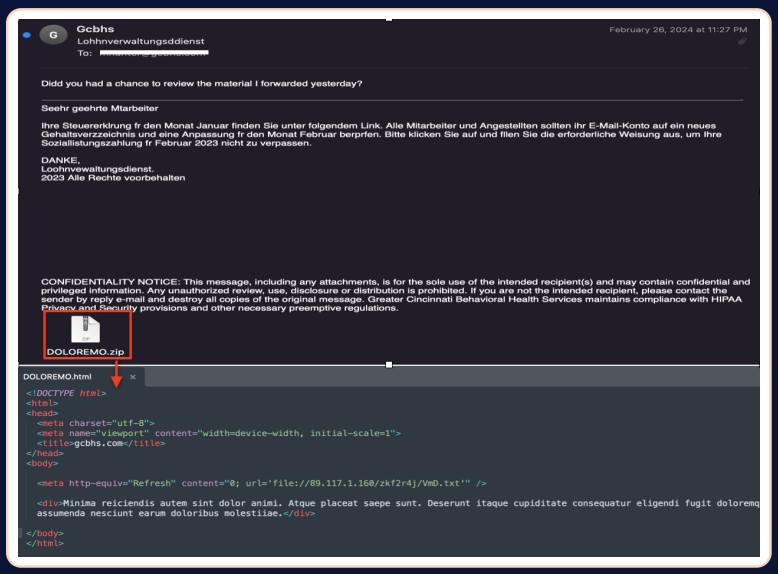
These messages utilized a technique known as thread hijacking and contained zipped HTML attachments, effectively concealing their malicious intent within unsuspecting inboxes.

- ***NTLM (NT LAN Manager) is a security protocol used by Microsoft Windows operating systems for authentication purposes. SMB (Server Message Block) is a network communication protocol primarily used for providing shared access to files, printers, and other resources on a network.***

By hijacking the authentication thread, attackers can extract NTLM challenge-response hashes from legitimate SMB sessions, enabling them to impersonate authenticated users and gain unauthorized access.



When recipients open the zipped HTML attachment, they unknowingly set off a chain of events that compromise their system's security. The HTML file serves as a passage for exploitation, redirecting the user's system to a file hosted on an external server via the Server Message Block (SMB) protocol. Also, it's important to note that each HTML file has its own distinct hash. This detail makes it challenging for detection purposes, adding another layer of complexity to efforts aimed at uncovering them.



Despite its harmless appearance, this redirection hides a malicious intent, allowing threat actors to gain unauthorized access to sensitive data within the victim's system such as username, IP address, computer name and domain name.

Malspam Statistics

Perhaps the biggest difference between this quarter's malspam statistics and this time last year comes in comparing the ratio of links to attachments in malspam usage. In Q1 2023, a "staggering 97%" of malware-based emails employed attachments; only 3% used links.

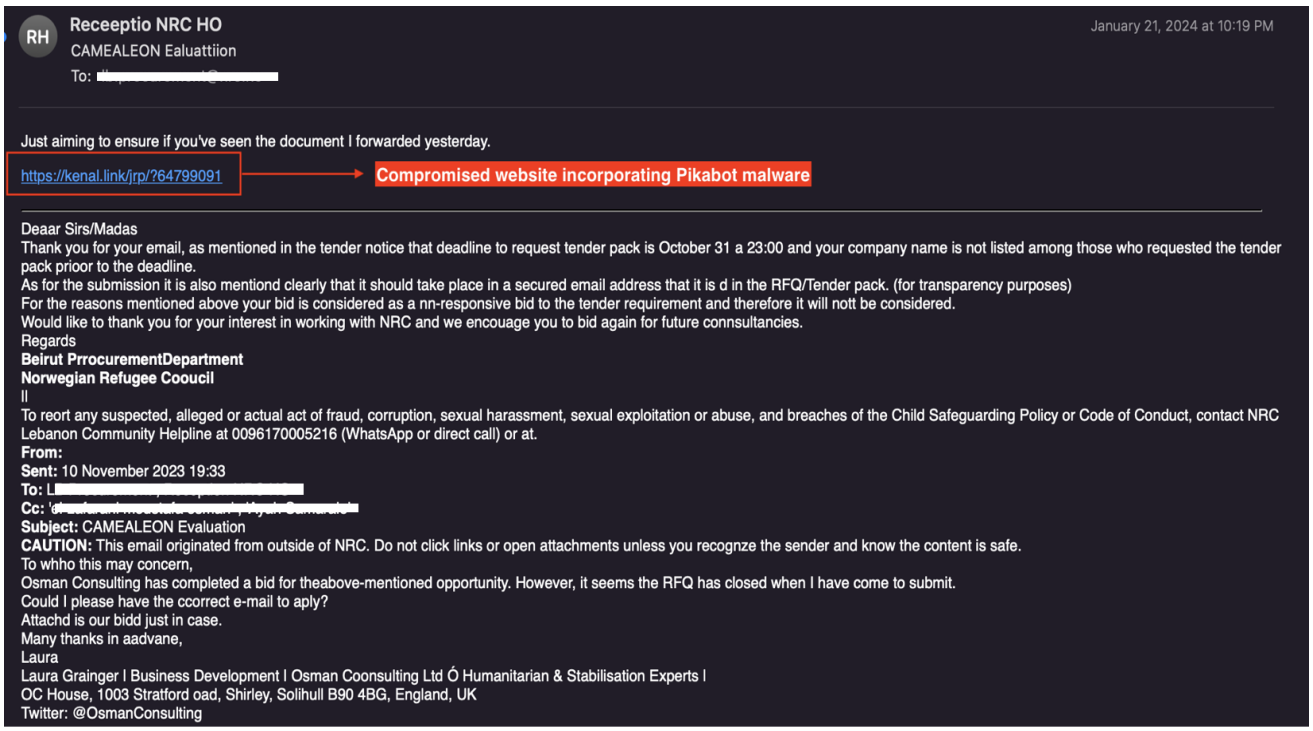
This year, a drastically lower 78% of malspam emails used attachments, with 22% opting instead for malicious links. Given the popularity (and supposed success) of password-oriented phishing emails, all leveraging links, perhaps the theme and popularity has spread.

Malspam Links

When we dug into the link-related malspam emails, we discovered that threat actors employ three primary methods:

1. Compromising legitimate websites to host and distribute the malware
2. Creating newly registered domains that evade detection by standard email security tools
3. Hiding malware in widely unsuspected cloud storage platforms like Google Drive

Here is one example we found of a malspam email using a compromised legitimate website (note the use of Pikabot):


RH Receeptio NRC HO
CAMEALEON Ealuattiion
To: [redacted]
January 21, 2024 at 10:19 PM

Just aiming to ensure if you've seen the document I forwarded yesterday.

https://kenal.link/jrp/?64799091 → Compromised website incorporating Pikabot malware

Deaar Sirs/Madas
Thank you for your email, as mentioned in the tender notice that deadline to request tender pack is October 31 a 23:00 and your company name is not listed among those who requested the tender pack prioor to the deadline.
As for the submission it is also mentiond clearly that it should take place in a secured email address that it is d in the RFQ/Tender pack. (for transparency purposes)
For the reasons mentioned above your bid is considered as a nn-responsive bid to the tender requirement and therefore it will nott be considered.
Would like to thank you for your interest in working with NRC and we encouage you to bid again for future connsultancies.
Regards
Beirut PrrocurementDepartment
Norwegian Refugee Cooucil
ll
To reort any suspected, alleged or actual act of fraud, corruption, sexual harassment, sexual exploitation or abuse, and breaches of the Child Safeguarding Policy or Code of Conduct, contact NRC Lebanon Community Helpline at 0096170005216 (WhatsApp or direct call) or at.
From:
Sent: 10 November 2023 19:33
To: [redacted]
Cc: [redacted]
Subject: CAMEALEON Evaluation
CAUTION: This email originated from outside of NRC. Do not click links or open attachments unless you recognze the sender and know the content is safe.
To whho this may concern,
Osman Consulting has completed a bid for theabove-mentioned opportunity. However, it seems the RFQ has closed when I have come to submit.
Could I please have the ccorrect e-mail to aply?
Attachd is our bidd just in case.
Many thanks in aadvane,
Laura
Laura Grainger I Business Development I Osman Coonsulting Ltd Ó Humanitarian & Stabilisation Experts I
OC House, 1003 Stratford oad, Shirley, Solihull B90 4BG, England, UK
Twitter: @OsmanConsulting

Malspam Statistics

Malspam Attachments

When we analyzed the vast majority of malspam emails that still rely on attachments, we discovered that the most used attachment in malicious spam emails for Q1 of 2024 are .pdf files, having 51% of the total amount. The breakdown is as follows:

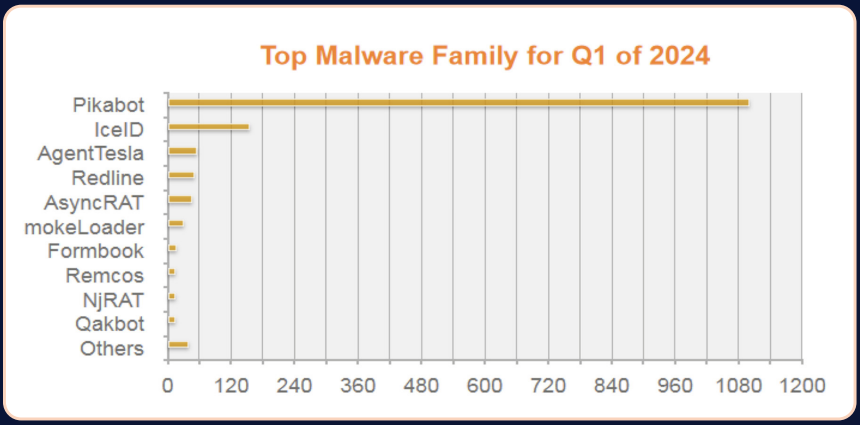
- **.pdf (51%)**
- **.docm/.docx (27%)**
- **.html (14%)**
- **.xlsm/.xlsx (6%)**
- **.zip (2%)**

Interestingly, all of the malicious .pdf files are related to the Pikabot malware we encountered primarily in January of this year.

Feature: Pikabot: Top Malware Family of Q1 2024

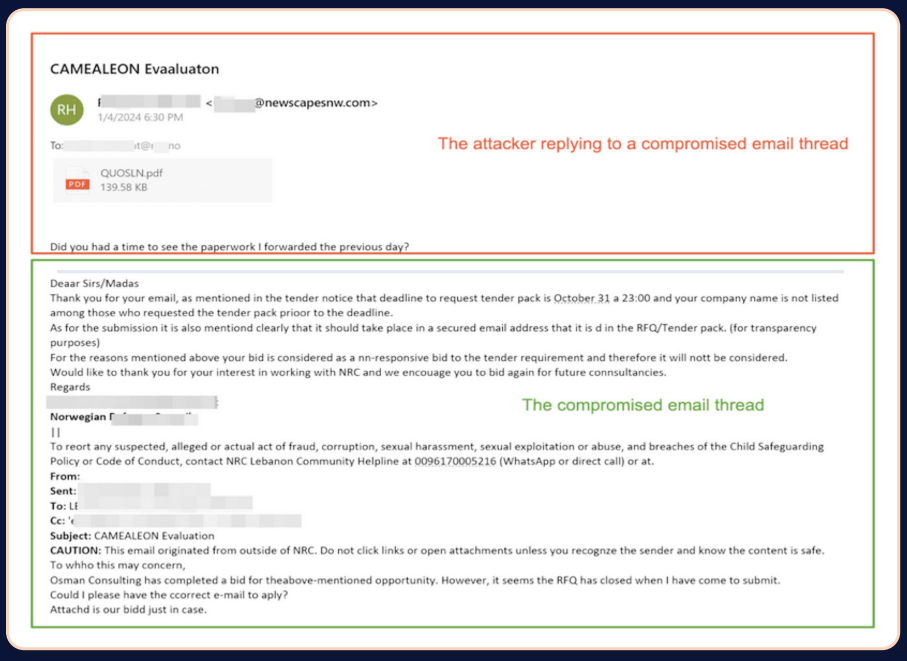
Since early 2023, malicious backdoor Pikabot has been slipped into a growing number of emails via PDF files.

One year later, it has overtaken Q1 2023's Qakbot as the most pernicious threat of the first quarter. Based on our research, it focused most of its attacks on users in the United Kingdom and Norway. It is followed by the following malware families, though only distantly:



How It Works

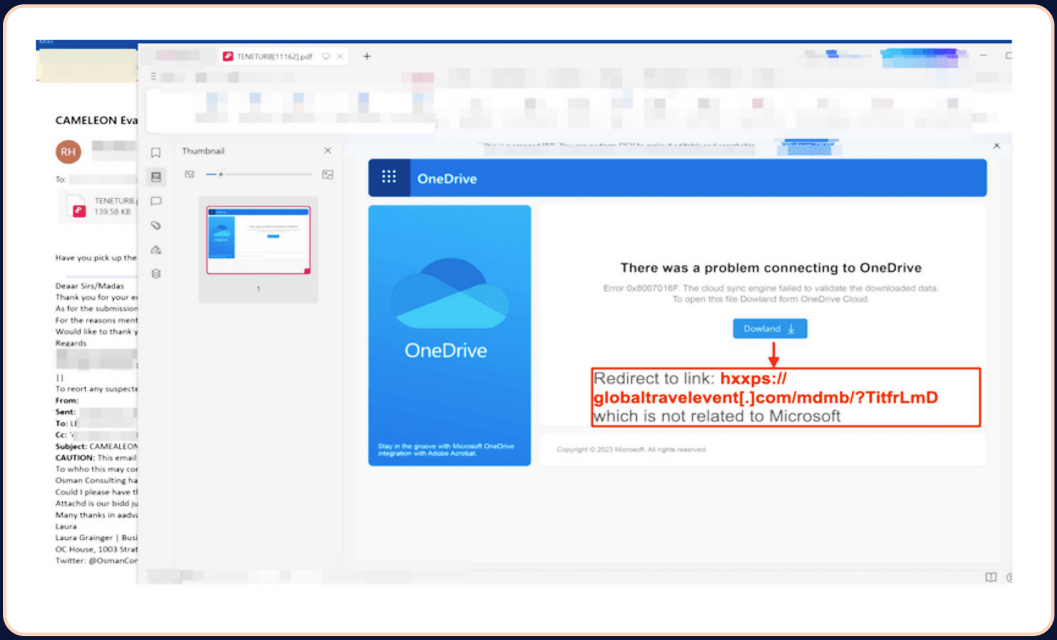
Step 1: Step 1: Social Engineering | Attackers reply to an old email thread they had previously compromised, "following up" and changing the subject to look legitimate. See the example below and note the typo in the middle of the page, among other red flags.



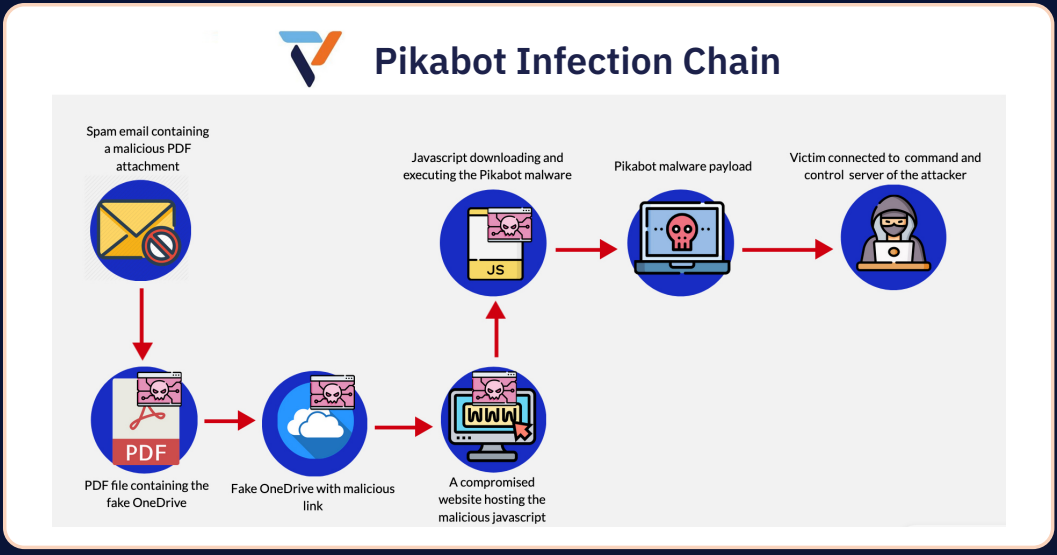
Feature: Pikabot: Top Malware Family of Q1 2024

Step 2: Malicious PDF | The user opens a PDF file attachment which takes them to a spoofed OneDrive page, which urges a download.

Step 3: Obfuscated Download | The download button redirects them to a compromised website where the Pikabot malware downloads upon execution. Note the example below and see our Pikabot blog for a more detailed analysis.



The visual below serves to illustrate the flow of the Pikabot infection chain:›



Feature: Pikabot: Top Malware Family of Q1 2024

What It Does

Pikabot not only grants unauthorized access to threat actors but can also be leveraged to perform a range of other malicious activities, such as stealing sensitive information, crypto-mining, enabling remote control over compromised systems, and deploying ransomware.

The New Qakbot?

There are observations that Pikabot might be filling the void left by the dismantled Qakbot malware. Notable similarities have been identified between Pikabot and the Qakbot trojan, including patterns in email thread hijacking, unique URL structures, almost identical infection chains, and similar loader capabilities.

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 Q1 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 malicious infections 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.

Conclusion

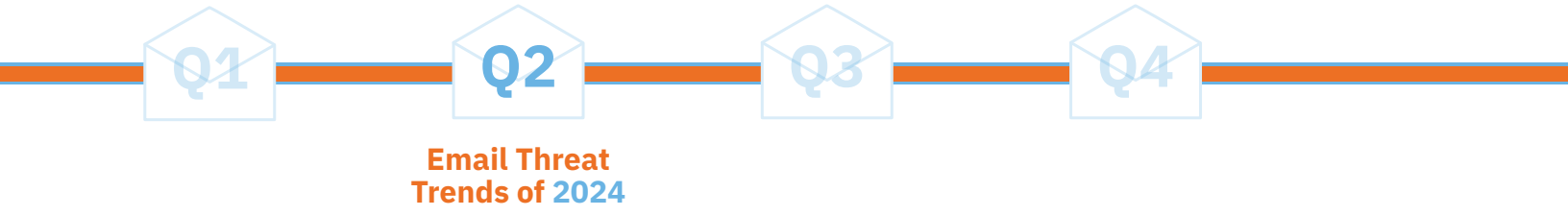
The email threat landscape is always changing.

As attackers start to favor malicious links for their capability to come across “clean,” our Link Isolation tool and VIPRE Expert Rules are even more vital for helping our customers catch what traditional email solutions can’t. The general trend - be it manifested in new XSS attempts, code hidden in calendar files, or phishing emails that bait the user to call – is to lean away from technical trickery and target the end-user instead.

This is why traditional email security services are becoming increasingly irrelevant, and cutting-edge techniques like attachment sandboxing, link isolation, and even employee awareness training are taking the lead as our best defense against inbox crime. As the cybersecurity industry shoots high, attackers shoot low and seek to circumvent email security defenses not with might, but with wit. Inserted links come out clean because it’s the second link that’s corrupted; emails don’t warrant a red flag because the only thing malicious is the invitation to call a vendor back; and clean .html attachments lead to nefarious QR codes.

As cybercriminals get sneakier, email defense solutions need to follow the trail. VIPRE’s email security platform stays ahead of emerging threats, quarter by quarter, and remains adaptable enough to respond to the latest tactics and powerful enough to block 234 million threats en masse. For more information about VIPRE email security technology, request 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