VIPRE
SECURITY GROUP

Email Threat Trends Report: 2024:Q3

An Expert Look at Email-Based Threats

Content

Introduction

Staying Ahead in the Battle Against Email-Based Threats. Every year, email infiltrators step up their game. In this never-ending game of cat-and-mouse, we have reached a point where the security industry has successfully created email security tools that can detect foul play when it crosses the inbox threshold.

However, today's attackers are finding clever ways to slip new ills over the line undetected, and while those ways aren't necessarily sophisticated, the tools required to fight – or find – them need to be.

VIPRE's Q3 2024 Email Threat Trends report aims to bring those tactics to light.

At VIPRE, we are committed to robust email security. We offer this quarterly report to the cybersecurity community in the hope that no organization will be left vulnerable to evolving threats.

Having been in the industry for over 25 years, we dedicate ourselves to the highest level of email threat security, creating our own tools and innovations just to stay one step ahead of the curve. Our dedication to staying ahead ensures our customers benefit from the most advanced threat intelligence available.

We are eager to share our unique insights into the evolving email threat landscape with organizations that are, or soon will be, navigating similar challenges—fostering a stronger, more resilient cybersecurity ecosystem.

Key Trends

Before we dive into specifics, here is an investigative profile into the types of malicious emails we caught; their origins, types, and destinations.

We typically process about 1.8 billion emails per quarter, and this quarter was no exception. Roughly 208 millions of those were malicious, and 12.3 million were caught by our proprietary sandboxing software, Link Isolation. As more email attackers seek to obfuscate their tactics, the number of emails caught in this manner has increased (up from 11 million this time last year).

Content vs. Links

While we usually see a 50/50 split between how the nefarious emails were caught (content vs. links), the ratio was flipped from Q3 2023 as well. This year:

- **107 million were caught due to content (about the same as last year).**
- **98 million due to links (20 million fewer than Q3 2023).**

Attachments and Behavior-Only Detection

Attackers are aware that email security solutions are constantly evolving to detect malicious links and attachments.

As a result, they now employ more intricate methods to bypass defenses, often appearing harmless at first but exhibiting malicious behavior later. To counter these tactics, organizations must be equipped to identify and respond to subtle behavioral anomalies.

Additionally, attachments are getting sneakier, posing as voice mails for download, or even security updates, although the most common forms were Microsoft PDFs and .DOCX files. It could be because Microsoft is a trusted name, and those are trusted formats.

This quarter:

- **2.18 million emails were detected due to malicious attachments.**
- **141,000 were caught by DeepLink, our webpage behavioral detection solution, alone (malicious attachments never seen before).**

We have seen the number of malicious attachments drop significantly in the last year, falling from over 5 million to just over 2 million.

Caught At Click Time

There's one more feature that deserves mentioning.

In the world of email security, it's rarely black-and-white; many malicious links are not seen for what they are until it's too late. That's why it's important to have a defense mechanism at click time.

In Q3 of this year, VIPRE labs protected customers from over 68,000 nefarious links that had somehow made it past previous defenses and were only detected at the time the user clicked. Nine in ten of those were flagged due to dangerous content, and the other ten percent were caught by next-generation behavioral detection.

Without this additional real-time defensive capability, many organizations would feel completely protected only to fall victim to what appears to be a "vetted, safe" link, but is anything but.

Types of Spam

The top three forms of favored spam are still the top three from Q3 2023, though with slightly different ratios:

- **Scam (34%)**
- **Commercial (30%)**
- **Phishing (20%)**

Malware accounts for (11%) of threats, followed Others (5%). This highlights an intriguing phenomenon: while much of the cybersecurity industry focuses on well-known threats like ransomware and malware, these methods make up less than 20% of email attacks. The greater concern lies in the more subtle tactics, such as scams and phishing emails, which pose a much larger threat.

And what does this mean? **It means that our email security solutions – which can catch malware and ransomware – are doing their jobs.** And that we as users have been weighed in the balance and found to be the far easier line to break through. If we can't educate the working masses overnight, then at least we can continue to bolster security with Security Awareness Training (SAT) and ever-stronger, savvier phishing and scam detection solutions: click time detection, behavioral detection, sandboxing, and the like. **If users are going to click anyway, our email solutions need to acknowledge that and be prepared.**

Where Do They Come From, Where Do They Go?

That is the question. Unsurprisingly, the United States retains its perennial top spot (accountable for "sending out" 74% of the world's spam), followed by the UK (the nation with the third highest number of data centers), and Ireland (not even in the top ten by the data center metric).

While the US and UK are typical contenders, there is often an unexpected wildcard, and this quarter, it was Ireland. Even then, it only accounted for a paltry 3%. However, China, Russia, and Italy were tied at fourth place (making up 2% together).

As we're always quick to mention, attackers from all over the world can disguise themselves as an attacker from another country. Trusted, server-rich nations like the US and UK are often coveted locales, while regularly suspect countries that often get caught for such crimes – possibly Russia and China among them – are not.

Interestingly, while most email plagues seem to stem from the US and Great Britain, they also seem to target the US and Great Britain as well. Those two countries share the top two spots for "receiving the greatest number of email attacks," respectively. **Either both countries are making a point of fighting primarily against themselves, or there are other factors at play.**

Sectors in the Crossfire

Among different industries, critical infrastructure seemed to be at the most risk, a growing trend over the past several years.

As the US Department of Homeland Security states on their website, “Nation-states and their proxies, transnational criminal organizations, and cyber criminals use sophisticated and malicious tactics to undermine critical infrastructure, steal intellectual property and innovation, engage in espionage, and threaten... democratic institutions.”

As evidence, the sectors most targeted by BEC, phishing, and malspam emails this quarter (worldwide) were:

- **Manufacturing (27%)**
- **Energy (23%)**
- **Retail (10%)**
- **Utilities (7%)**
- **Real Estate (6%)**

Followed, shockingly, by Finance, which typically ranks highly on that list. One reason that Manufacturing continues to pop up in breach and cybersecurity attack headlines is the ongoing quest to combine OT with IT. It needs to be done, but the introduction of vulnerable on-premises systems that have never seen the light of day to the uber-connected, cloud-centric world of modern IT leaves some security considerations to be desired.

Network security specialists are still working on that, and in the meantime, organizations can cut down on one of the largest vectors of attack – email – **by implementing sophisticated email security solutions capable of catching many of these threats at their genesis.**

The Calm Before the Storm

One thing we noted overall was that malicious email submissions were quieter this quarter—a bit too quiet.

Our samples were down by a full 16.48% compared to Q2. This could be because email threat actors have decided to pursue a more honest line of work (one can only hope).

Or, and possibly more likely, it might be attributable to the possibility that they’re gearing up for the holiday season. After all, this is when they do their best work: Black Friday, Thanksgiving, Christmas, and New Year’s. We might simply find ourselves in the middle of “vacation time” for the hardworking cybercrime sector, and doesn’t everyone deserve some time off?

If nothing else, it gives us more time to prepare for the barrage of treacherous ploys to come in the quarter ahead.

The Lucrative Business of BEC

As Business Email Compromise (BEC) continues to be a highly profitable threat, we expect it will remain a significant focus in our quarterly reports.

Many are familiar with the FBI's IC3 report highlighting that BEC accounted for over $2.9 billion in adjusted losses—nearly 49 times the losses from ransomware. This disparity exists largely because companies have more substantial funds available to transfer (and lose) than individuals.

Well, our real estate allotment was wisely provisioned as the majority of our scam emails arose from BEC. **The numbers went from under half in Q2, to comfortably over half (58%) in Q3, an increase of roughly 3%. While that doesn't sound like much, a three percent increase in a quarter, if repeated amounts to a 12% hike within a year – a significant escalation in an already thriving market.**

BEC and Manufacturing

A number-one target? Manufacturing (of course).

And we uncovered an uncomfortable trend; BEC emails targeting this sector have risen steadily since January:

- **2% in Q1**
- **4% in Q2**
- **10% in Q3**

We'd hate to see where it goes next. Manufacturing firms are often targeted for financial gain through social engineering campaigns that redirect vendor payments to fraudulent accounts. **They can also serve as a pivot for downstream attacks, where unauthorized email access is used to phish other clients, such as by sending fake document requests to vendors in order to steal credentials.**

These attacks may be increasing because the industry relies heavily on mobile sign-ins at worksites, making employees more likely to fall for phishing attempts while "on the go" and anxious to meet manufacturing deadlines.

The Weapon of Choice

The weapon of choice in most of these cases was impersonation, with this strategy accounting for 89% of total BEC attempts.

The most-impersonated individuals are:

- **CEOs and Executives (57%)**
- **Directors, Managers, and Supervisors (26%)**
- **IT Personnel (9%)**

With Human Resources and School Heads accounting for an accumulated 9%. The main takeaway is double and triple-check emails from your higher-ups, especially when it has to do with money or credentials, and even – or especially – when their email directs you to another site. A good rule of thumb is to compose a new message to them directly (as their "email address" may be a closely-resembled fake) or, better yet, reach out to them on another platform or in-person.

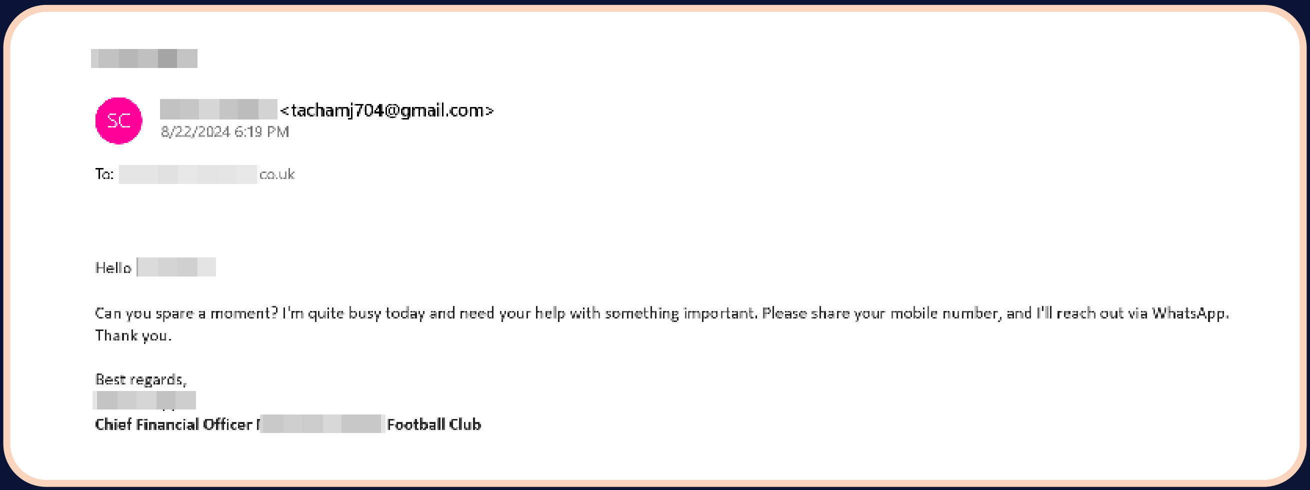
If anything, it will show your conscientiousness about security and possibly save your organization from public humiliation.

Feature: BEC Impersonation

BEC (Business Email Compromise) impersonation is a type of cyberattack where attackers impersonate high-level executives, IT personnel, HR staff, or other known individuals within an organization.

The goal is typically to deceive employees into taking actions such as making unauthorized payments, transferring sensitive information, or granting access to systems. Attackers craft these emails to appear legitimate by mimicking the tone, language, and email structure of the impersonated person, often targeting employees who may not suspect foul play.

Here is an example of a BEC scam found in an employee’s inbox:



[redacted]

[redacted] <tachamj704@gmail.com>
8/22/2024 6:19 PM

To: [redacted] co.uk

Hello [redacted]

Can you spare a moment? I'm quite busy today and need your help with something important. Please share your mobile number, and I'll reach out via WhatsApp. Thank you.

Best regards,
[redacted]
Chief Financial Officer [redacted] Football Club

By leaning into the casual (and flattering) intimacy of a C-Suite executive tossing you a quick email—with an urgent need—from their personal cell phone, threat actors prove their skill at their craft: manipulating human nature. These are essentially social engineering threats at their core, so keep your critical thinking cap on and consider not only the source but also the method, the circumstances, and the ask.

And for those times when we all fall short and click anyway, organizations need to back up their employees’ best efforts with click time protection, link and attachment sandboxing, and behavioral-driven email threat analysis.

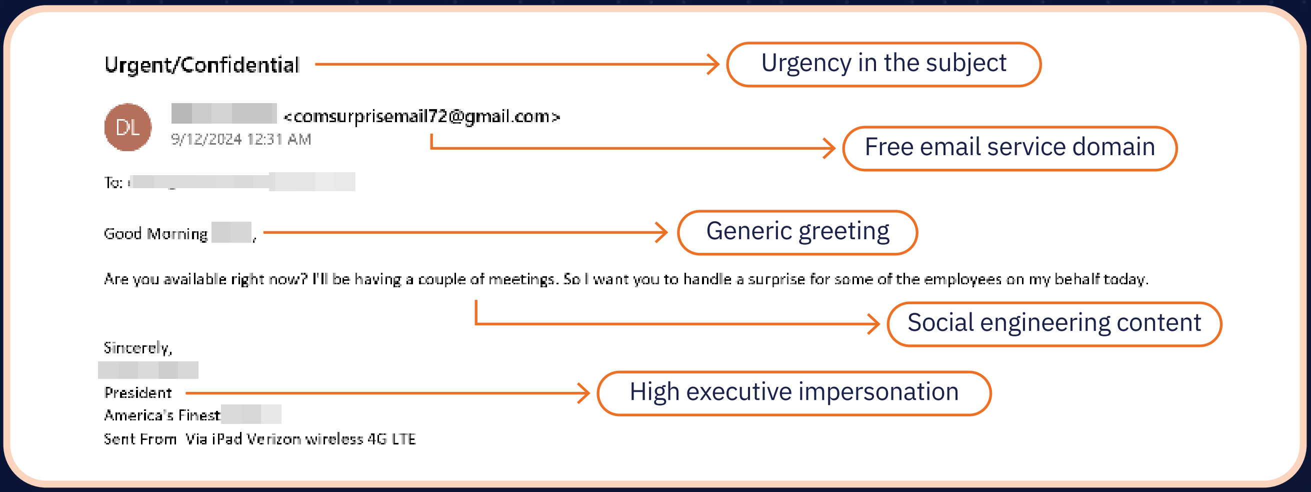
BEC an AI: A Disastrous Duo

Using AI detector tools, we discovered that 36% of the BEC samples in Q3 were crafted by AI. Threat actors are still utilizing Generative AI to generate BEC-related content, and there seems little apparent reason for them to stop. With the word-perfect capabilities of generative-AI and the ability to take on a certain (and convincing, or casual, or friendly tone), many threat actors are experimenting with letting AI do their dirty work.

The fact that the number of AI-created BEC threats just tops one-third shows both that cybercriminals are trying it out with gusto – but not putting all their eggs in one basket just yet. After all, in such a lucrative business, you can’t afford to take too many chances with what works.

Feature: Anatomy of a BEC Attack

If you encounter something like this in the inbox, make sure to report it immediately.



Urgent/Confidential

DL [redacted] <comsurprisemail72@gmail.com>
9/12/2024 12:31 AM

To: [redacted]

Good Morning [redacted],

Are you available right now? I'll be having a couple of meetings. So I want you to handle a surprise for some of the employees on my behalf today.

Sincerely,
[redacted]
President
America's Finest[redacted]
Sent From Via iPad Verizon wireless 4G LTE

Urgency in the subject

Free email service domain

Generic greeting

Social engineering content

High executive impersonation

Note the non-personal greeting (how many people do you reach out to with a formal Good Morning?), the play to the real world (a ”couple of meetings”), the important-sounding subject (”Urgent/Confidential”), and the impressive – or intimidating – resume at the end (”President”).

Also note the fact that there is no link included. This allows the still nefarious email to get past traditional email defenses undetected, and, in the subsequent emails, will probably try to get the employee off the corporate network (where the email security protections may still be too strong). Once the user is safely on a personal device – or on an unsecured app, even better – the “President” will send over a link (ostensibly for the “surprise” mentioned in this case), which will then detonate on the employee’s phone.

In the best-case scenario for the attacker, that personal device will also be used for work, and the threat actor will infiltrate and pivot to the corporate network from there.

The Good News

As of now, 98% of the BEC emails received in Q3 of 2024 have been detected by our in-house AV Labs using the newly crafted and maintained “New Heuristic Rules.” These rules are curated and maintained by VIPRE’s AV Labs to enhance detection and keep up with the latest email threats.

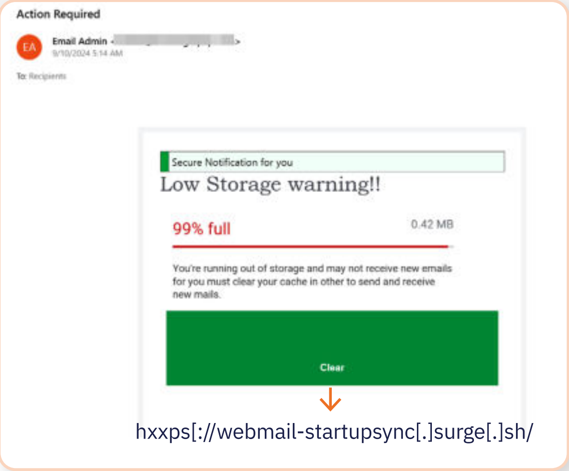
In updating our spam campaign tracking, we have been focusing on a more generalized approach to our heuristics policies. **Thanks in part to the changes, our aggregated AV Labs Expert Rules detected a total of over 2.3 million spam emails in Q3 alone.**

Phishing in the Dark

In the ever-present war between links and attachments, the gap is widening. Compared to last quarter, threat actors are using more attachments in their malicious campaigns (30% compared to Q2's 21%), and slightly fewer links and QR codes as a result.

Phishing with Links

Among phishing emails with links, some can include an action perceived to be beneficial to the user, as in these examples:



Action Required

EA Email Admin <[redacted]>
9/10/2024 5:14 AM

To: Recipients

Secure Notification for you

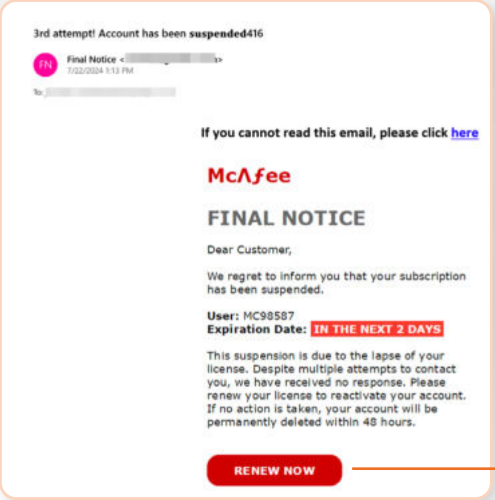
Low Storage warning!!

99% full 0.42 MB

You're running out of storage and may not receive new emails for you must clear your cache in other to send and receive new mails.

Clear

hxxps[://webmail-startupsync[.]surge[.]sh/



3rd attempt! Account has been **suspended416**

FN Final Notice <[redacted]>
7/22/2024 1:13 PM

To: [redacted]

If you cannot read this email, please click here

McAfee

FINAL NOTICE

Dear Customer,

We regret to inform you that your subscription has been suspended.

User: MC98587
Expiration Date: IN THE NEXT 2 DAYS

This suspension is due to the lapse of your license. Despite multiple attempts to contact you, we have received no response. Please renew your license to reactivate your account. If no action is taken, your account will be permanently deleted within 48 hours.

RENEW NOW

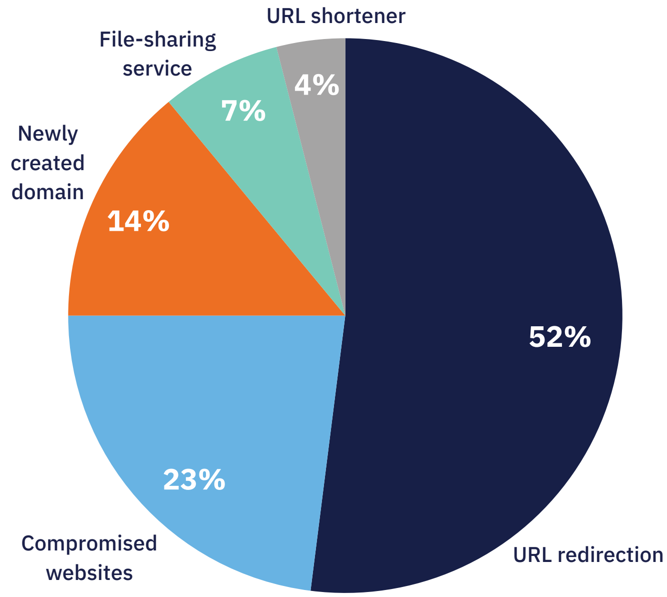
hxxps[:}/marionette[.]blob||core[./
windows.net/website/
LMaispd#offer/00209/570/
cn3fs/20em/41/77

In both cases, these seem like nice things to do (clear storage or renew your antivirus subscription), but the over-exerted urgency with which those two "companies" reached out should be a red flag.

The types of links commonly sent this quarter favored URL redirection by a landslide, a tactic especially effective at evading security controls as the ploy utilizes a "clean" URL within the body of the email, and then redirects the user to a malicious one once inside. For this reason, an email security solution with the power to safely try out those links and detect malicious content on the page before the user navigates (sandboxing) is crucial.

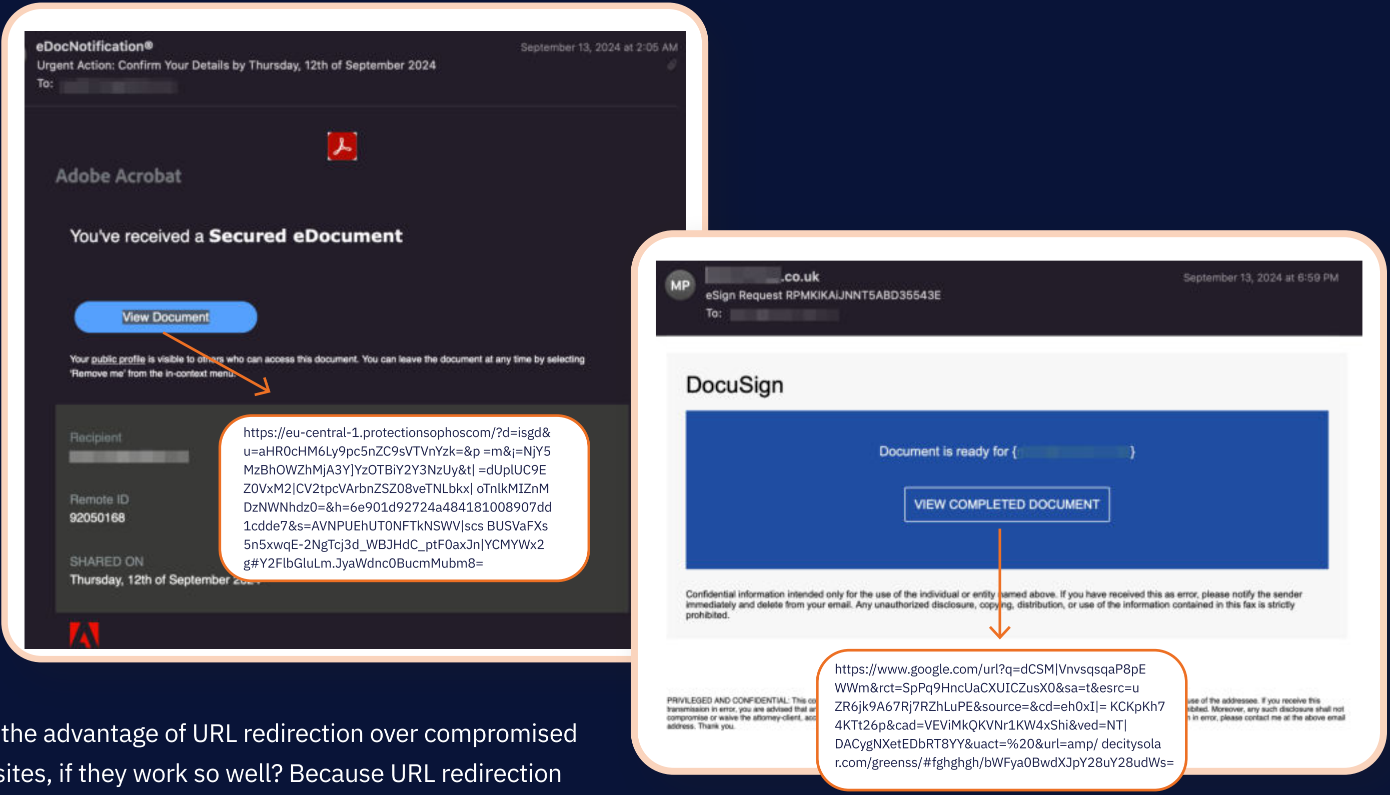
Last quarter, URL redirection was followed by file-hosting services (26%), now replaced by compromised websites (23%). Compromised websites look like "the real deal," earning the users' trust. There might be more chance for advertising (and therefore clicks) on these sites, whereas with file-hosting services, a threat actor would need to convince the user that there was a good reason to be there, and to take action on an asset (download, open, etc.). Leaving the clicks up to the users' pliable interests may garner more success – or at least cybercriminals thought so this quarter.

Phishing links



Feature: URL Redirection

The following are examples of phishing emails utilizing URL redirection to spoof users. Notice that the sites victims are being redirected to are well-known sources, allaying concerns.



eDocNotification®
Urgent Action: Confirm Your Details by Thursday, 12th of September 2024
To: [redacted]
September 13, 2024 at 2:05 AM

Adobe Acrobat

You've received a **Secured eDocument**

Your public profile is visible to others who can access this document. You can leave the document at any time by selecting 'Remove me' from the in-context menu.

Recipient
[redacted]

Remote ID
92050168

SHARED ON
Thursday, 12th of September 2024

https://eu-central-1.protectionsophoscom/?d=isgd&u=aHR0cHM6Ly9pc5nZC9sVTVnYzk=&p =m&¡=NjY5MzBhOWZhMjA3Y]YzOTBiY2Y3NzUy&t| =dUplUC9EZ0VxM2|CV2tpcVArbnZSZ08veTNLbkx| oTnlkMIZnMDzNWNhdz0=&h=6e901d92724a484181008907dd1cdde7&s=AVNPUEhUT0NFTkNSWV|scs BUSVaFXs5n5xwqE-2NgTcj3d_WBJHdC_ptF0axJn|YCMYWx2g#Y2FlbGluLm.JyaWdnc0BucmMubm8=

MP
[redacted].co.uk
eSign Request RPMKIKAJNNT5ABD35543E
To: [redacted]
September 13, 2024 at 6:59 PM

DocuSign

Document is ready for {[redacted]}

Confidential information intended only for the use of the individual or entity named above. If you have received this as error, please notify the sender immediately and delete from your email. Any unauthorized disclosure, copying, distribution, or use of the information contained in this fax is strictly prohibited.

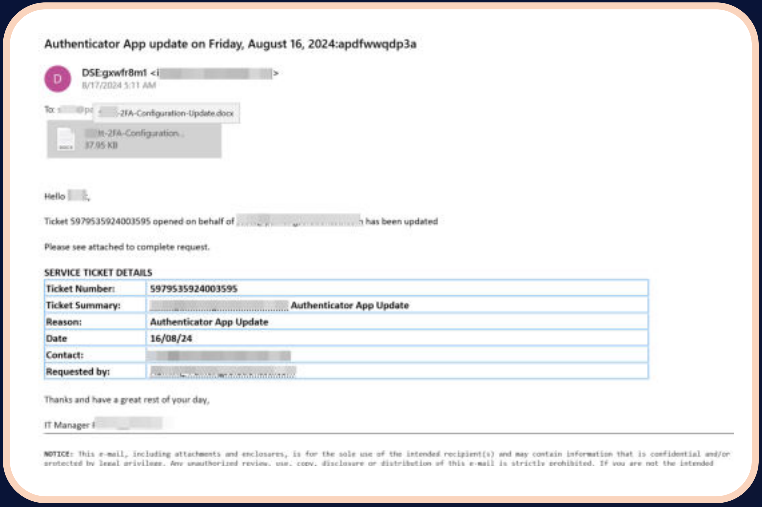
PRIVILEGED AND CONFIDENTIAL: This co… transmission in error, you are advised that ar… compromise or waive the attorney-client, acc… address. Thank you. …use of the addressee. If you receive this …ibited. Moreover, any such disclosure shall not …n in error, please contact me at the above email

https://www.google.com/url?q=dCSM|VnvsqsqaP8pEWWm&rct=SpPq9HncUaCXUICZusX0&sa=t&esrc=uZR6jk9A67Rj7RZhLuPE&source=&cd=eh0xI|= KCKpKh74KTt26p&cad=VEViMkQKVNr1KW4xShi&ved=NT|DACygNXetEDbRT8YY&uact=%20&url=amp/ decitysolar.com/greenss/#fghghgh/bWFya0BwdXJpY28uY28udWs=

Why the advantage of URL redirection over compromised websites, if they work so well? Because URL redirection employs a perfectly clean link that directs one to a compromised website as a second step. Starting out with a compromised website in the body of theemail increases the risk of being caught by email security solutions.

Phishing with Attachments

In the following example of a phishing email with a malicious attachment, the payload is in the form of an "update" to an authenticator app. These threat actors are masquerading as concerned security professionals – while actively striving to undermine your network security.



Authenticator App update on Friday, August 16, 2024:apdfwwqdp3a

D
DSE:gxwfr8m1 <i[redacted]>
8/17/2024 5:11 AM

To: [redacted] [redacted]-2FA-Configuration-Update.docx
[redacted]-2FA-Configuration...
37.95 KB

Hello [redacted],

Ticket 5979535924003595 opened on behalf of [redacted] has been updated

Please see attached to complete request.

SERVICE TICKET DETAILS

Ticket Number:	5979535924003595
Ticket Summary:	[redacted] Authenticator App Update
Reason:	Authenticator App Update
Date	16/08/24
Contact:	[redacted]
Requested by:	[redacted]

Thanks and have a great rest of your day,

IT Manager [redacted]

NOTICE: This e-mail, including attachments and enclosures, is for the sole use of the intended recipient(s) and may contain information that is confidential and/or protected by legal privilege. Any unauthorized review, use, copy, disclosure or distribution of this e-mail is strictly prohibited. If you are not the intended

Trends in Malspam

It may help to define the difference between a malspam email and a phishing email.

While both have the same nefarious intentions, malspam is seen as an unsolicited message from anyone with malicious content involved. Phishing, on the other hand, at least pretends to be nice as threat actors seek to disguise their messages as legitimate sources you may know and trust.

Malspam Links vs. Attachments

While links may be the fairly consistent favorite method of attack in phishing ploys, all bets are off when it comes to malspam.

During Q3, the vast majority of malspam efforts were centered on malicious attachments (64%), while only 36% employed a link. However, just a quarter ago, links were the tool of choice by a factor of nearly nine-to-one (86% links to 14%). **The reason for this pendulum swing is unclear, but it seems malspam actors are still trying to find their stride.**

Malspam Links: Compromised Websites Take Top Spot

We noticed three general trends when analyzing malspam emails this quarter, and that was the propensity to deliver their payloads in one of three ways:

- **Compromised websites (41%)**
- **Cloud storage (33%)**
- **Newly Registered Domains (26%)**

Last quarter, cloud-based software development platforms were the favorite (37%), with compromised websites as a close second (35%). Maybe not everyone wants to develop software this quarter, or perhaps the trick was used widely enough to garner suspicion, forcing threat actors to go to Plan B.

Compromised websites are a hearty option for attackers as they look and read like the real thing and can even contain value-adding content, making the ruse more complete.

Malware Attachments

One year ago, the top malspam attachments were ZIP (62%), DOC/DOCX (16%), and HTML (12%) files. Now, they are:

- **LNK (38%)**
- **ZIP (34%)**
- **DOCX (20%)**

A lot can change in a year. One possible reason that the previously unlisted LNK file flourished this quarter is the same reason URL redirects are so popular. In fact, a parallel can be drawn between them, with LNK files operating (maliciously, anyway) as the URL redirects of the malspam attachment world. LNK files are Windows Shortcuts that point users to open a folder, file, or application. So, while the end file might be malicious, the LNK typically will not be – and will thereby avoid detection.

Feature: Malware Family of the Quarter

And the winner is – drumroll - RedLine. And although there have been other so-named malware families in-between, RedLine was interestingly the top malspam family in Q3 of 2023, as well.

Here was a differing trend: When we stacked up all the malware that made the list in Q3, we noticed something interesting: it all appeared to be Windows-based. To illustrate, here are the top seven:

1. RedLine
2. Remcos
3. AgentTesla
4. Formbook
5. Pikabot
6. AsyncRAT
7. Amadey

Redline: What you Need to Know

RedLine Stealer is malware designed to steal sensitive information from web browsers, such as credentials and payment data. It features a customizable file-grabber to target specific file types.

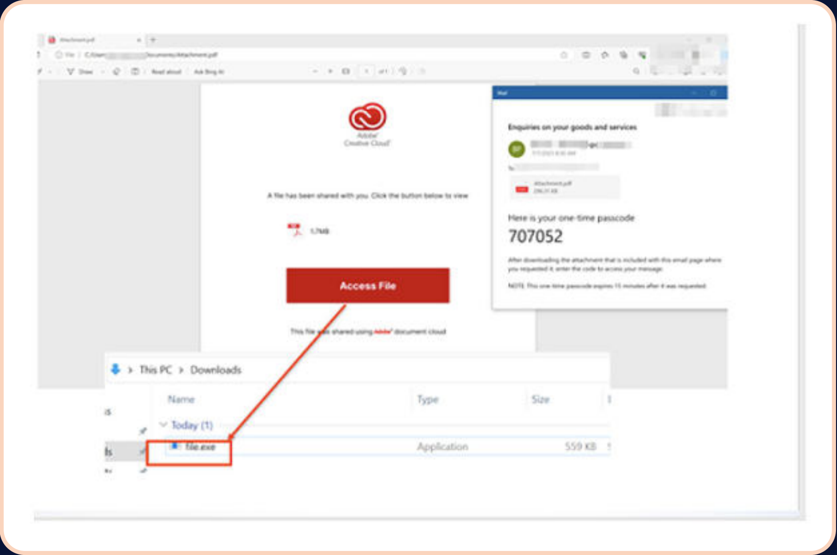
Typically distributed via phishing emails or malicious websites, it sends stolen data to a command- and-control server controlled by the attacker.

Like we mentioned in our Q3 2023 report, RedLine "can be spread via innocuous phishing emails and can appear in various formats such as PDFs, executable files, and Office Suite documents"

and they have the potential to do some serious damage, such as:

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

RedLine has the ability to completely take over a compromised machine and uses multiple methods of infiltration. In this instance, a malicious PDF attachment directs users to click an equally malicious link, resulting in the download of a malicious executable (the RedLine malware, formatted as file.exe).



A file has been shared with you. Click the button below to view

This file was shared using Adobe document cloud

Enquiries on your goods and services

Here is your one-time passcode

707052

After downloading the attachment that is included with this email page where you requested it, enter the code to access your message.

NOTE: This one-time passcode expires 15 minutes after it was requested.

This PC > Downloads

Name	Type	Size
Today (1)		
file.exe	Application	559 KB

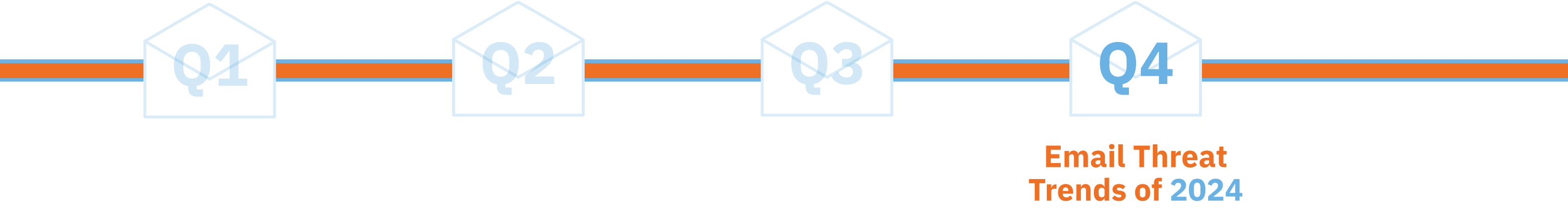
Conclusion

For nearly three decades, VIPRE Email Security has been dedicated to the highest level of email threat security, pioneering our own tools and techniques just to stay one step ahead of the curve.

Our solutions empower customers with the confidence that their security is not only equipped to handle current threats but is also informed by the latest intelligence and designed to proactively address emerging risks. By staying at the forefront of email security, we ensure that our clients are always prepared for whatever tactics cybercriminals deploy next, fostering a future-ready defense strategy.

For more information about VIPRE Email Security - who we are, or what we do schedule a demo today.

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



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

VIPRE
SECURITY GROUP

North America	UK and other regions	DACH Sales	Nordics Sales
sales@vipre.com	uksales@vipre.com	dach.sales@vipre.com	nordic.sales@vipre.com
+1 855 885 5566	+44 (0)800 093 2580	+49 30 2295 7786	+45 7025 2223