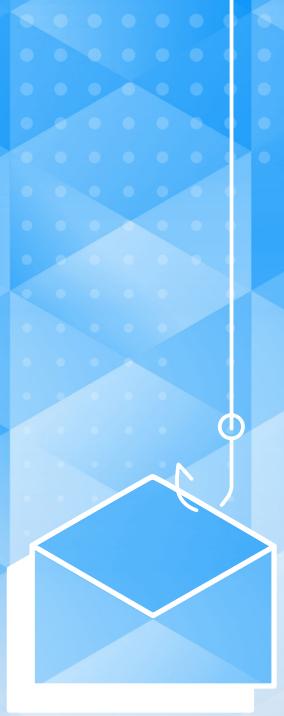
VIPRE SECURITY GROUP



Email Threat Trends Report: 2023: Q2

BEC is on the Rise

Content

Introduction

In the second quarter of this year, we've processed nearly 1.8 billion emails, detected over 230 million malicious ones, and drawn a few conclusions to share with you.

With over 25 years in the malware protection business, VIPRE Security Group is an award-winning global cybersecurity, privacy and data protection company. We service upwards of 50,000 customers worldwide, have a network of over four thousand channel partners, and have secured over one million endpoints. We love what we do, and we feel that good should keep on giving. Which is why we freely offer our findings every three months to the greater security community at large.

What we've learned is valuable, and - it's safe to say - impossible to learn in any other way. **We have an extensive network of sophisticated, AI-driven email security systems in place that catch billions of emails within a twelve-week period and provide us with detailed information and analysis that is second to none.**

We're excited to share our findings with you in this Q2 Email Threat Bulletin.

Email Threat Trends Overview

While it barely scratches the surface, below is an introductory review of some of the key points of this quarter's email threat trend analysis.

200 million malicious emails

58%
(~130 million)
detected due to
content

42%
(~95.7 million)
detected due to
links

5 million
spotted as
malicious attachments

What We Analyzed and How

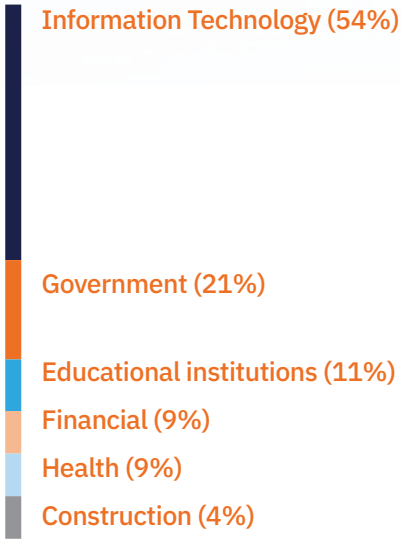
There were some interesting discoveries in our breakdown of over 200 million malicious emails this past quarter. Of the bunch, 58% (~130 million) were detected due to content, and 42% (~95.7 million) were detected due to links. A smaller 5 million were spotted as malicious attachments, with **ninety thousand malicious attachments put on the radar due to behavioral driven monitoring, never having been seen before.**

Basic attachment and link protection are fine but don't do deep enough in protecting your organisation. Sandboxing on attachment and dynamic link crawling to are much deeper and better methods to provide more complete protection.

On that note, there were nearly 10 million malicious links discovered by our Link Isolation solution, an advanced service included within VIPRE Email Security ATP. Link Isolation is a solution that sandboxes a link before allowing you to open it, placing it on an isolated browser away from your users and your network. Once it scans against known bad and AV engines, it puts the link through heuristics and behavior analysis to make sure it isn't bearing any zero-days. Needless to say – all of this was needed.

It took nothing less than that level of advanced behavioral-driven techniques, utilized by our Link Isolation feature DeepLink, to discover the full 10 million malicious threats otherwise hidden from tooling. This figure holds true to our numbers from last quarter's data, but we anticipate that number will steadily rise with time.

Most phishing emails in Q2



Trends in attacks

While content, links, and attachments were still the top players, the presence of email-based attacks that were undiscoverable by traditional means is worth noting. Basic attachment and link protection no longer secures you against the new generation of threats plaguing inboxes. Sandboxing attachments and dynamic link crawling are the techniques that provide the adequate amount of in-depth protection needed today.

Who is Being Attacked

A key difference between Q1 and Q2 is the target of attack. While financial institutions topped the list last quarter, Information Technology (IT) organizations received the most phishing emails in Q2. Next came government (21%) and educational (11%) institutions, followed by the financial (9%), health (9%) and construction (4%) sectors.

These numbers show a **trend towards technology and the public sector**, and away from the finance and healthcare focus of the year's onset. One possibility is that healthcare and finance – having borne the brunt of so many attacks last quarter – have stepped up their game and added increased defenses. And the perennial lack of IT investment in government agencies can be an additional cause for the increased attention; their defenses are well-known, they have large numbers of employees, and their cybersecurity defenses are still in the shoring-up stages.

Content of phishing emails

85%
favor malicious links

15%
favor attachments

Top-Level Domain most in use

.com
.es
.edu
.ca
.net

How They Are Being Attacked

The results are in, and **Content is still King.**

The majority (85%) of phishing emails favor malicious links embedded in the content of the email, while a much smaller minority (15%) slip them into attachments. Threat actors have gotten a lot of mileage out of convincing phishing email content: namely, social engineering ploys, according to our research.

Most emails use some sort of social engineering tactic related to password changing and updating of email accounts. Commonly used phishing phrases we discovered in these emails include:

- **Password expiration**
- **Account locked due to security reason**
- **Verify account within {time} hours**
- **Account will be disabled**
- **Full email storage capacity**
- **Update now!**

The **most spoofed brand among our customers is still Microsoft**, followed by Apple, DocuSign, and (interestingly) SpareBank. Last quarter the tech giant was followed in impersonations by DHL, WeTransfer, and Apple. Large OS providers, file services and financial firms seem to be a constant, and it's safe to say threat actors rotate between the top companies in those fields in order to increase their chances of catching unsuspecting consumers off-guard.

When analyzing the Top-Level Domain (TLD) most in use, **Q2 revealed again that it was ".com"**. This time, however, instead of being tailed by Q1's ".ca" and ".net", we saw a shockingly high influx of ".es", ".edu" and of course, various country codes. The increase in educational TLDs can be attributed to the fact that graduation and the end of the school year – a time when last-minute assignments are plentiful and school-based communications are critical – falls within the second quarter.

URL Redirection and Other Phishing Techniques

Now that we know who is being targeted and how, the question is: where are attackers sending victims once they click the link?

45%
of phishing links lead to compromised websites

Our data shows that 45% of phishing links lead to compromised websites. A not-too-far distant 39% are URL redirection, up from this time last year.

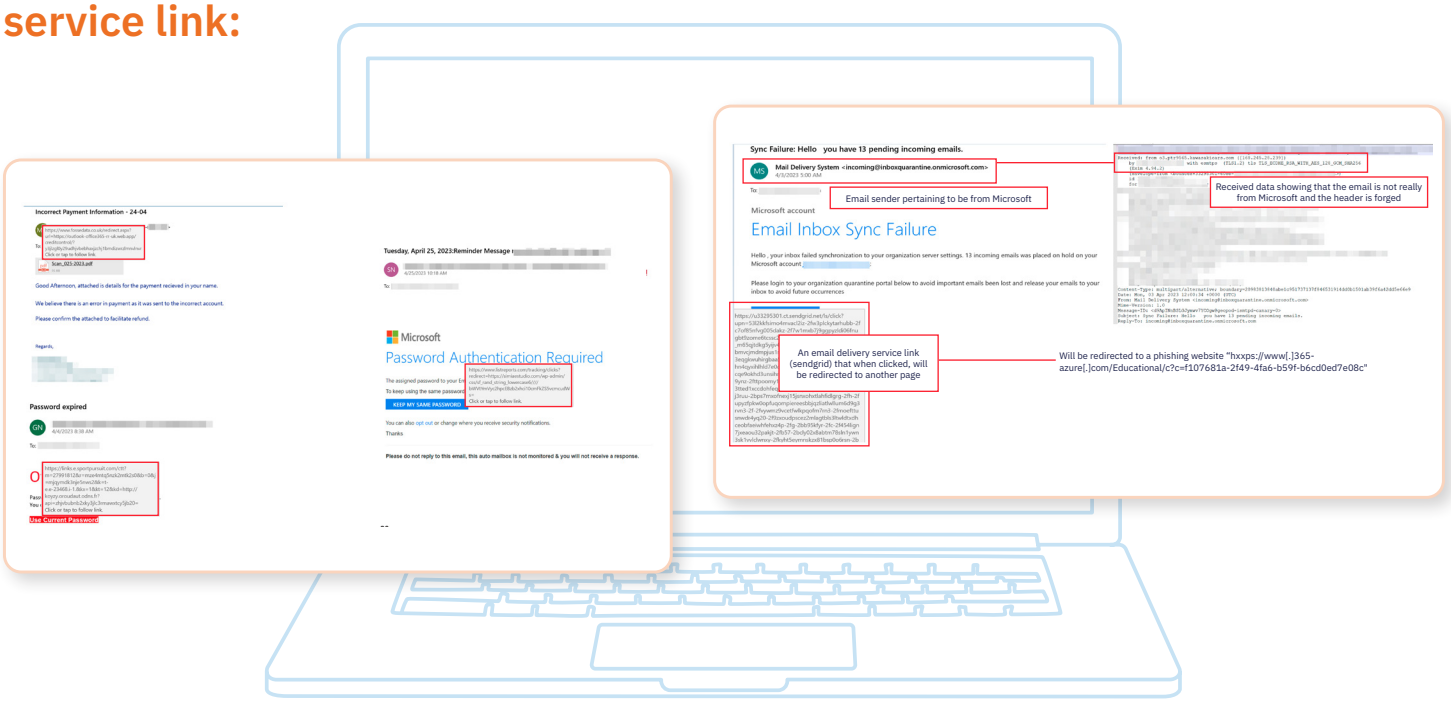
This year, more cybercriminals are using this tactic to hide the actual phishing link (most likely from technology employed to spot it). As malicious hackers get more cunning, heuristics and behavioral-driven email security models will be in ever-higher demand. Tools that can sandbox links, like VIPRE Email Security ATP Link Isolation, go the extra mile of clicking and clearing the link in a safe zone before ever letting the user open it.

39%
of phishing links lead to URL redirection

While not new, URL redirects are now a popular tactic among threat actors.

They get around detection by using an email delivery service like MailChimp or employing an open redirect technique.

Here is an example of a phishing email that uses an email delivery service link:



Feature: BEC Triples in 3 Months

A quick look at the most recent FBI Internet Crime Report will tell you **Business Email Compromise (BEC) losses are seventy-eight times higher than those resulting from ransomware.** The actual figures are $2.7 billion in adjusted BEC losses versus ransomware's $34.3 million.

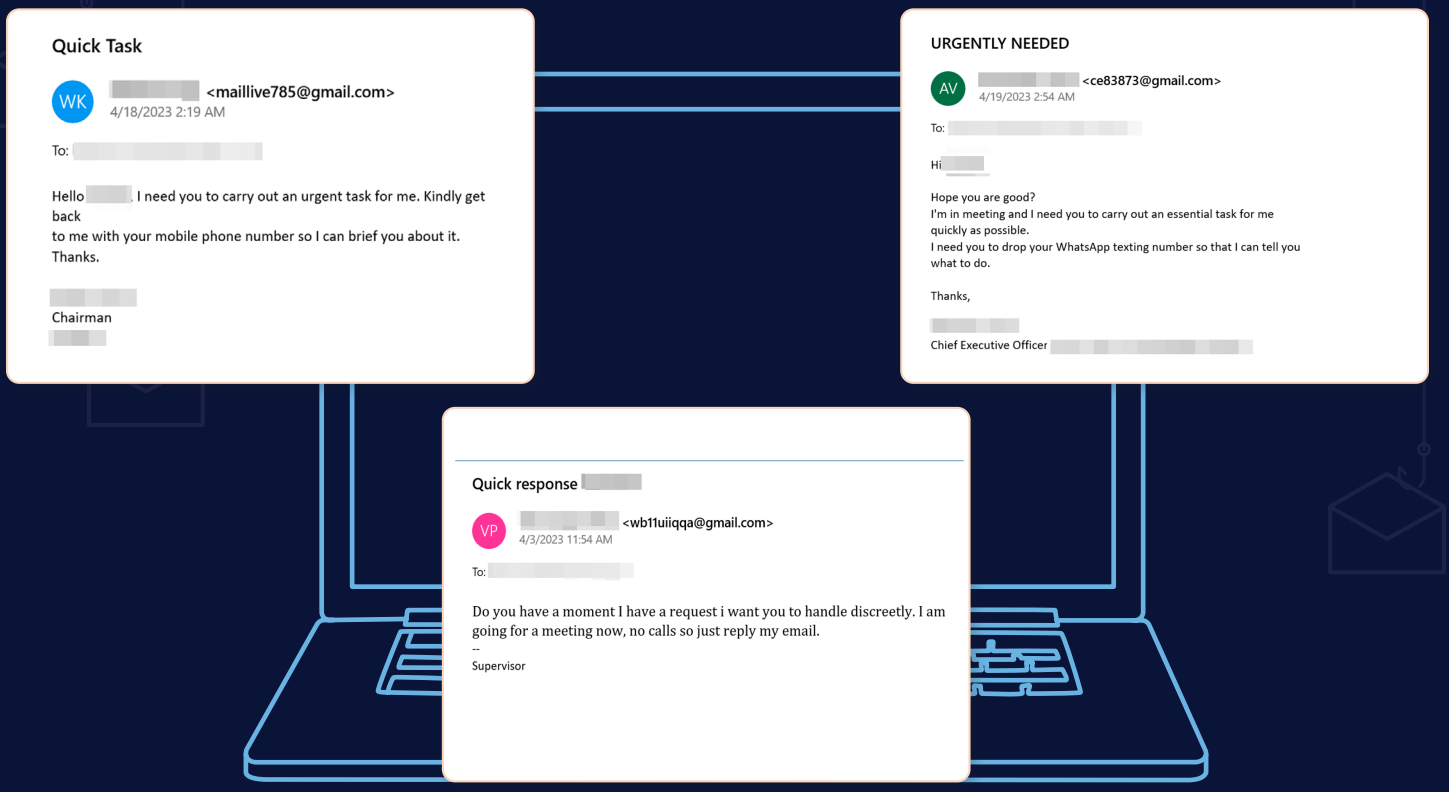
Cyber criminals go where they money goes, and Q2 saw the majority of scam emails (48%) classified as BEC scam. This method of tricking the target to transfer money via a spoof email – typically "from" a high-level executive or trusted partner – has tripled since Q1.

Commonly used BEC phrases include:
- **"Complete an assignment for me."**
- **"Swift email response"**
- **"Confidential"**

Commonly spoofed senders include examples like:
- **presidentOfUSA@gmail.com**
- **ceoexecutive01@gmail.com**
- **privateceo12@gmail.com**

And commonly used domains are those from free email services, such as:
- **Gmail.com**
- **Outlook.com**
- **Yahoo.com**

Business Email Compromise will continue to be a common tactic so long as the dividends continue to pay what they do. To stay vigilant, get familiar with some real cases of BEC caught this past quarter:



More Spam, Overall

There was a sizeable 30% increase in spam emails from Q1 to Q2 of this year. Of the 12,615 email samples submitted to VIPRE AV Labs this quarter for analysis, a staggering 11,610 were analyzed as spam emails (92% of all received). This was up from last quarter's roughly nine thousand.

Diving deeper, April was the biggest spam month and BEC emails were the biggest spam culprit. This could be due to April being the end of the 2022 tax year, and businesses buckling to a sense of urgency – always a useful tactic on the attacker's side.

Also of note in Q2:

- The US accounts for 67% of all spam
- Runners up are Denmark (10%), Ireland (8%) and China (7%)
- A collective 16% is accounted for by 13 other countries (from Singapore to Japan)

Last year the US still topped the list of spam originators, but at a more commanding percentage (76%). Runners up were Germany and Turkey, who this year didn't make the top-three list.

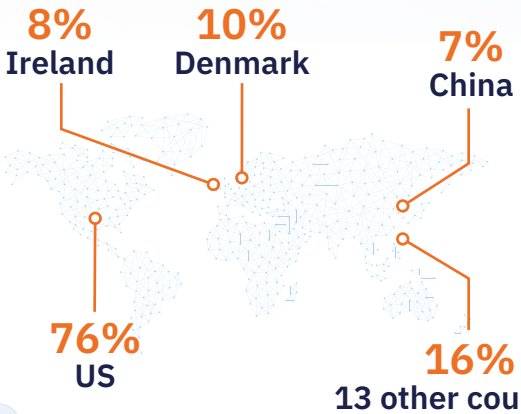
April saw the most scam emails by far, attributable to different kinds of BEC scams. Last quarter, it was February, and the spike was largely due to the Microsoft OneNote malware.

For a cheat sheet of usual file names used in malspam attachments, see the table below:

increase in spam emails

92% of all emails analyzed were spam

Countries accounting for spam



File Attachment	File Name
PDF	• AM.pdf • DM.pdf • EM.pdf • HN.pdf • HO.pdf • MO.pdf • MT.pdf • RO.pdf • TM.pdf • VA.pdf
DOC/DOCX	• InfoDocument_{randomnumber}.docx • Remittance_adv/random number}.docx • Inv{random date}_name.doc • remt#prf{randomCharacter}_{date}.docx • cycheck_{name}_{random number}.docx • Dhlshipmnt{date}.docx
ISO	• Logo extractor.iso • windowsUpdate.iso • Shipment{random number}.iso • Recordstool{randomnumber}.iso
XLS/XLSM	• receiptbill#_{randomnumber}.x|sx • Billingaddr{date}_shipment.x|sx • ad+invoice_document.xls • Invoice {randomnumber}.xIsx
ZIP	• Shipment{date}.zip • Audiorecording by {name}.zip

of phishing attachments are .HTML/HTM files

Malicious Attachments

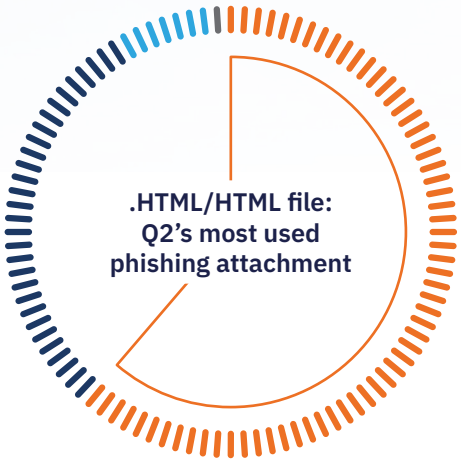
We discovered that Q2's **most used phishing attachment is still the .HTML/HTM file,** having 62% of the total file attachment. While that represents the majority, it signifies a decrease from Q1.

Other file types like .PDF (30%), .EML (7%), and .ZIP (1%) are being utilized in lesser numbers to deliver phishing attempts. Some popular HTML filenames include:

- BILL_OF_LADDING.html ("lading" misspelled)
- COMMERCIAL_INVOICE.html
- EFT Remittance EP8152.html
- Incoming_Wire_{random character}.htm
- Invoice_receipt{random character}.shtm
- Microsoft validation form.htm
- Office365 validation form.htm
- Payroll {date}.html
- Payment_Summary_{date}.html

As a general rule, the filenames of the phishing attachments are most often related to "invoice" and "remittance".

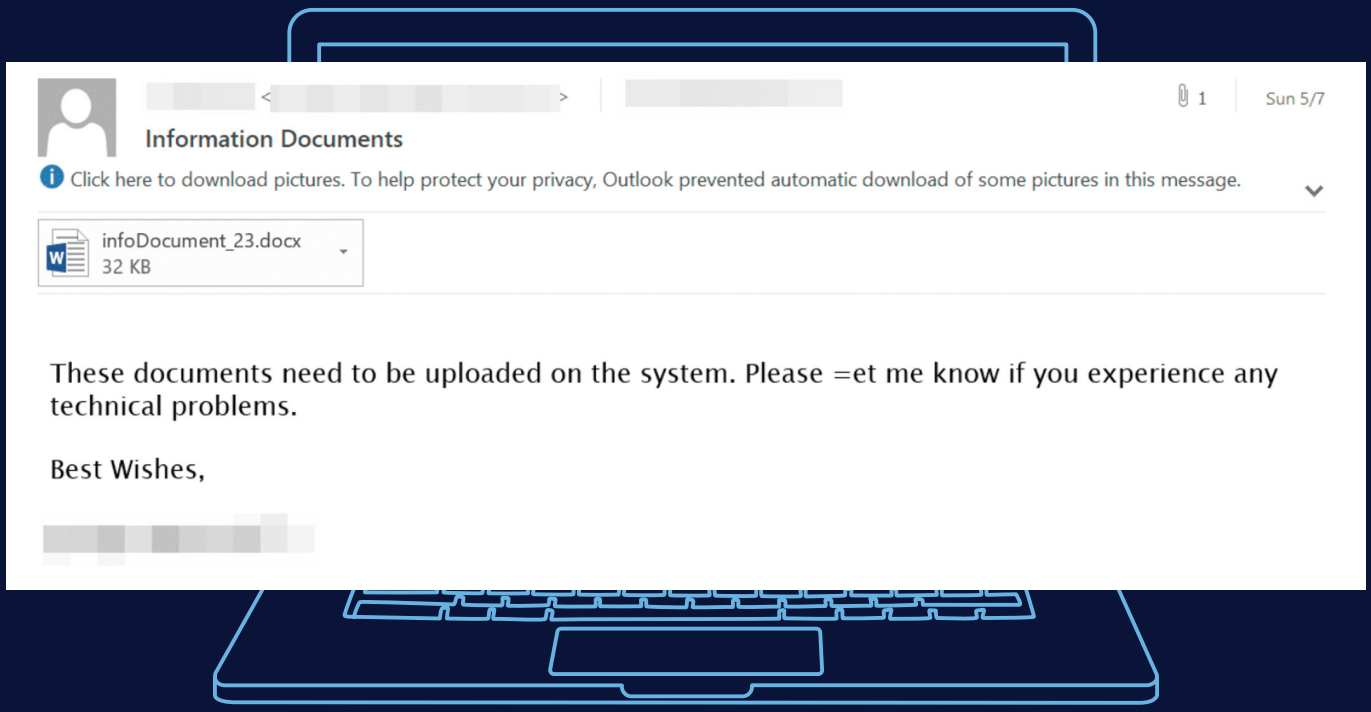
Types of files to deliver phishing



- .HTML/HTM file (62%)
- .PDF file (30%)
- .EML file (7%)
- .ZIP file (1%)

Feature: Macro-less Malspam Attack Trend

VIPRE Labs discovered a new malspam email campaign containing a ".docx" attachment. This specially crafted Microsoft document in turn contained a malicious external resource page that was called when the file was opened.



Exploiting the vulnerability CVE-2022-30190, known as the Follina vulnerability, the discovered malspam campaign allows for remote code execution on the victim's system by leveraging the Microsoft Support Diagnostic Tool (MSDT).

How it works:

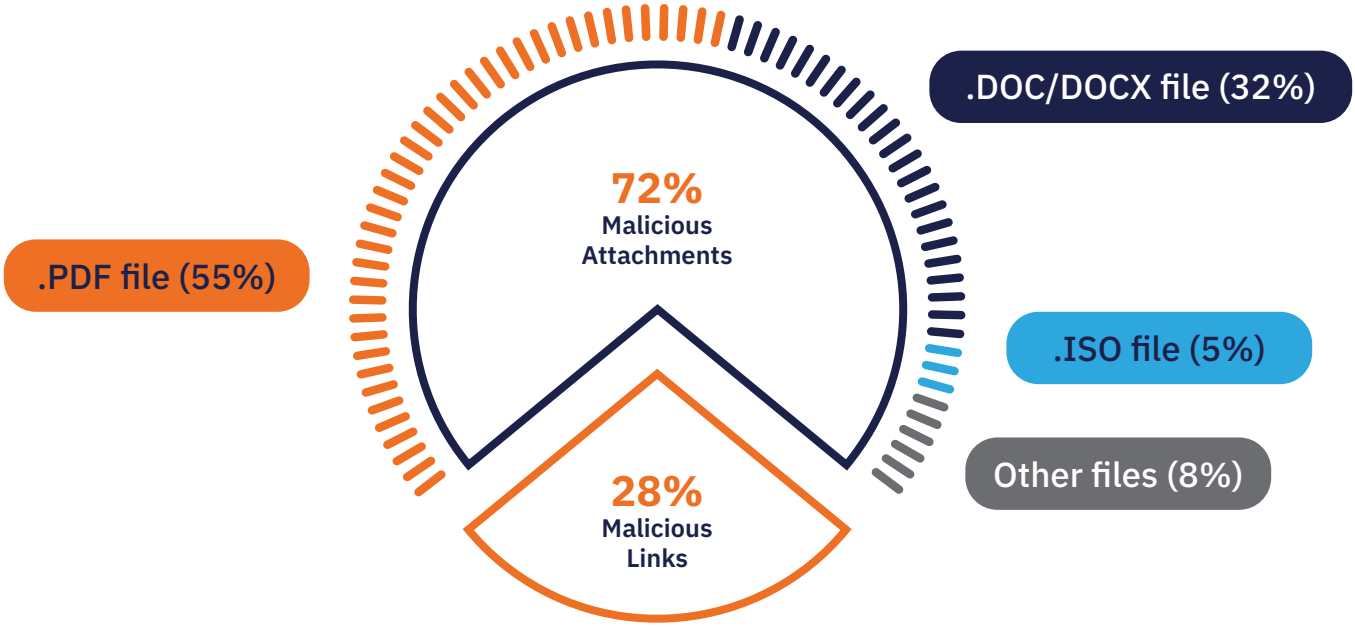
- Once opened, the HTML page contains JavaScript code that invokes MS-MDST, which is the MSDT URI protocol handler, and executes PowerShell scripts.
- The script then downloads the final payload, which has been verified as XWorm malware.
- XWorm is a sophisticated Remote Access Trojan capable of ransomware-like behavior, data theft, surveillance, DDoS attacks, and more.

Malspam

In Q2, the majority of malspam emails used malicious attachments (72%) and the remaining 28% used malicious links. Of the attachments, most (55%) were PDF files, followed by DOC/DOCX files (32%), ISO files (5%), and other files (8%) used to deliver malware like zip and xls.

These numbers differ slightly from Q1, in which a staggering 97% of all malspam employed attachments as their primary tactic, leaving only a paltry 3% to links. This quarter has trended towards more of a balance, though still leaning heavily towards attachments.

Analyzing the content of all the malspam emails we received, we noticed that threat actors mainly used compromised email threads to make the malspam look like a legitimate conversational email.

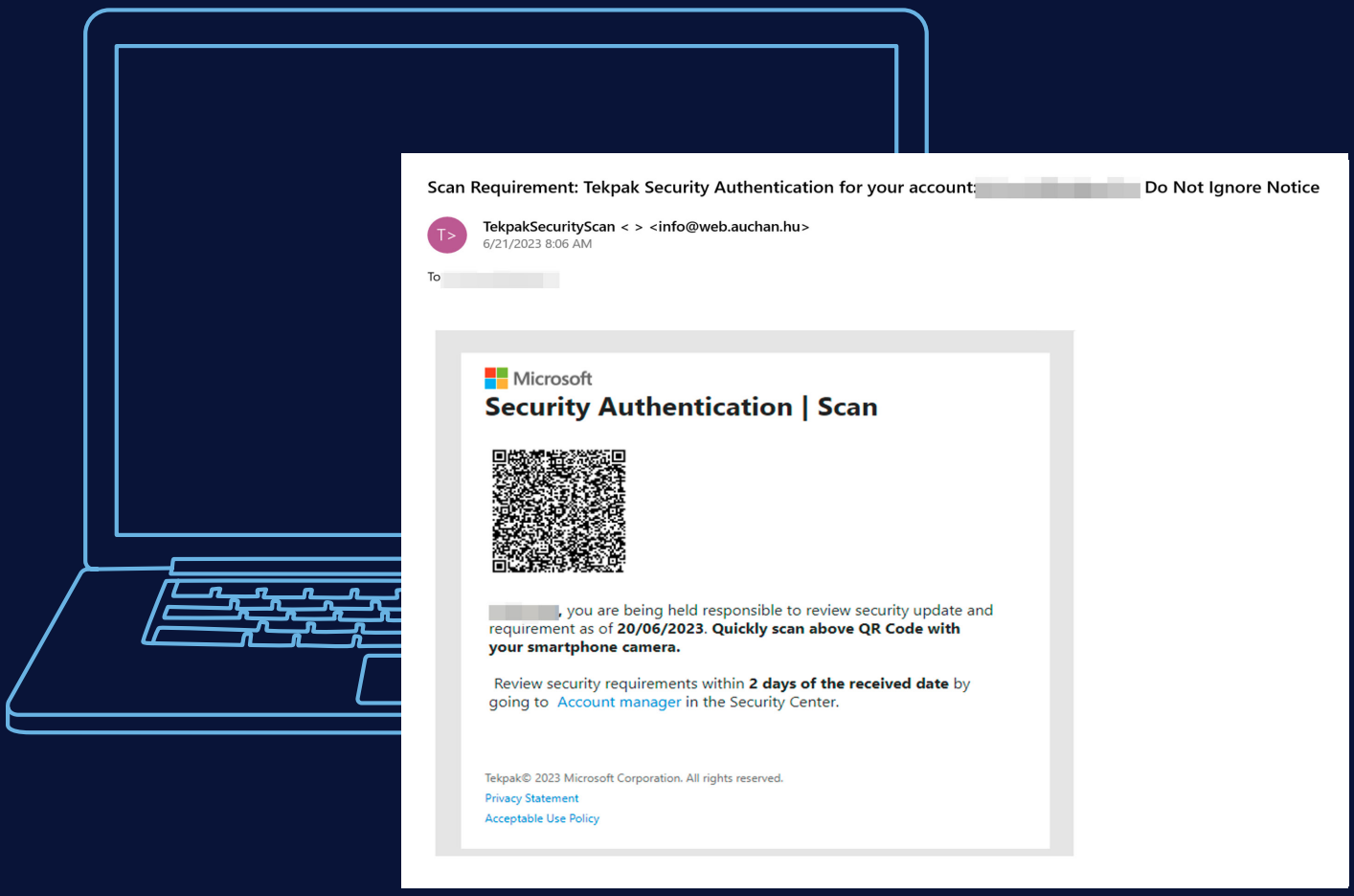


Feature: Phishing Emails with QR Codes

On June 2023, VIPRE AV Labs encountered a large number of phishing emails utilizing QR codes as their primary method of attack.

True to our prediction for the year, threat actors have begun using QR code-related tactics, baiting victims with a code that (when scanned) leads directly to a phishing page.

Be careful what you scan.



Beware: Scanning the QR code will lead to a separate page, where the victim will be redirected to the actual phishing page (hxxps://pioneerbroadcasters[.]org/RCA%2044%20BX%20For%20Sale.htm#M={victim's email address}).

Watch out!

Top Malware Family of the Quarter

The top malware family encountered by VIPRE Labs in Q2 was Qakbot, commonly known as Qbot. While it wasn't accountable for all malware cases, Qbot was related to every single malware link we discovered this quarter, an incredible percentage.

Next (by a wide margin) was XWorm, followed by IceID. Last quarter the top offender was AsyncRAT, although Qbot still held the title of the most popular malware family of last year.

Similarly, however, most of the malware we found in Q2 is some form of Remote Access Trojan, or RAT.

Qakbot: how it works

Deep Dive: QakBot: How It Works

QakBot is a pernicious malware strain that requires a deep dive to know it better.

How is QakBot delivered? Via URL and file attachment.

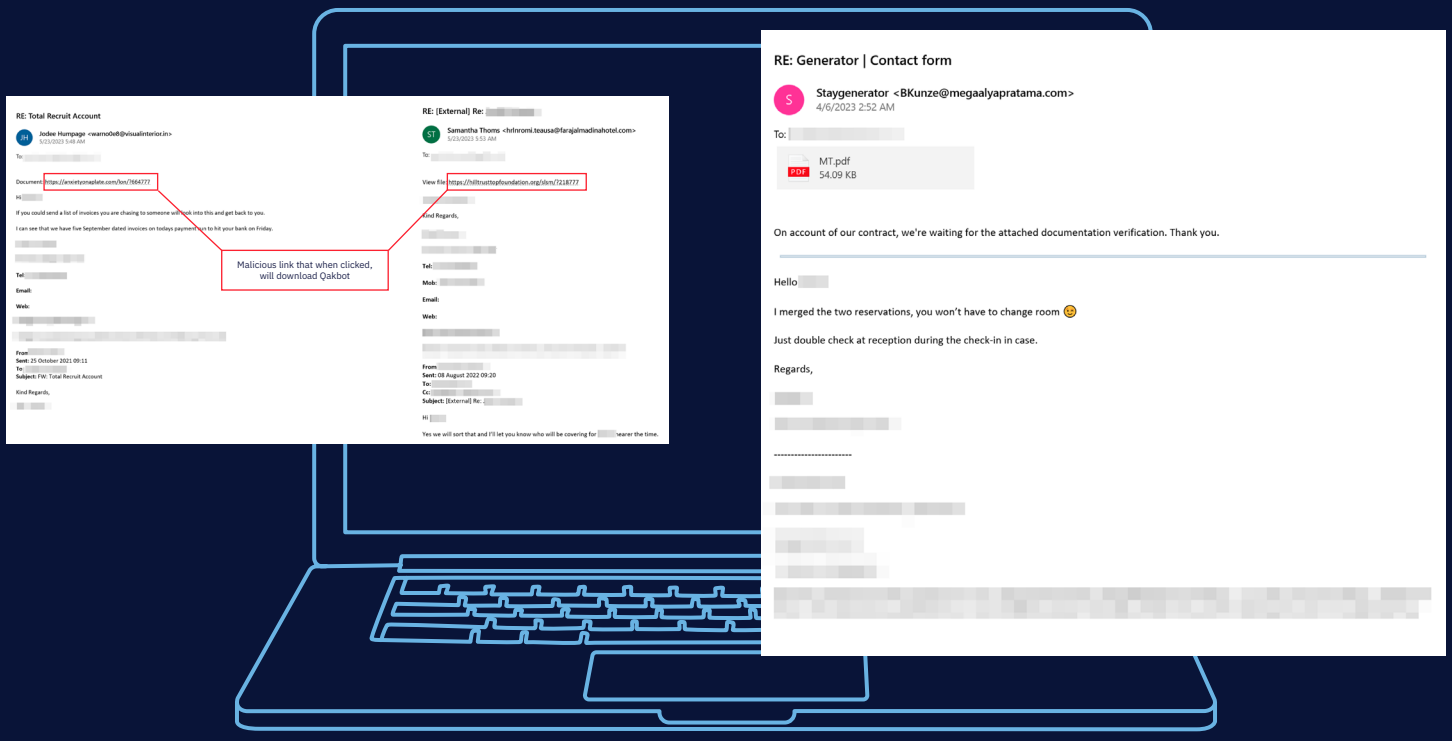
URL - As we saw with malspam, attackers still favor compromised email threads as a form of delivery for QakBot malware. No one expects the person they just emailed to send them back spam. The link is typically a compromised website or newly created domain, in the following format: "https://{domain}/{random letters}/?{random numbers}". However, HTTPS would be modified to HXXP, and "." to "[.]" in order to prevent the link from being clicked, as in:

- hxxps://hilltrusttopfoundation[.]org/slsm/?218777
- hxxps://anxietyonaplate[.]com/lon/?664777
- hxxps://navigatetocanada[.]com/mr/?taugif

Attachment - Most malspam emails with file attachments were also related to QakBot and took the similar form of compromised threads. When delivered via attachment, the PDFs are likely to have a two-letter format.

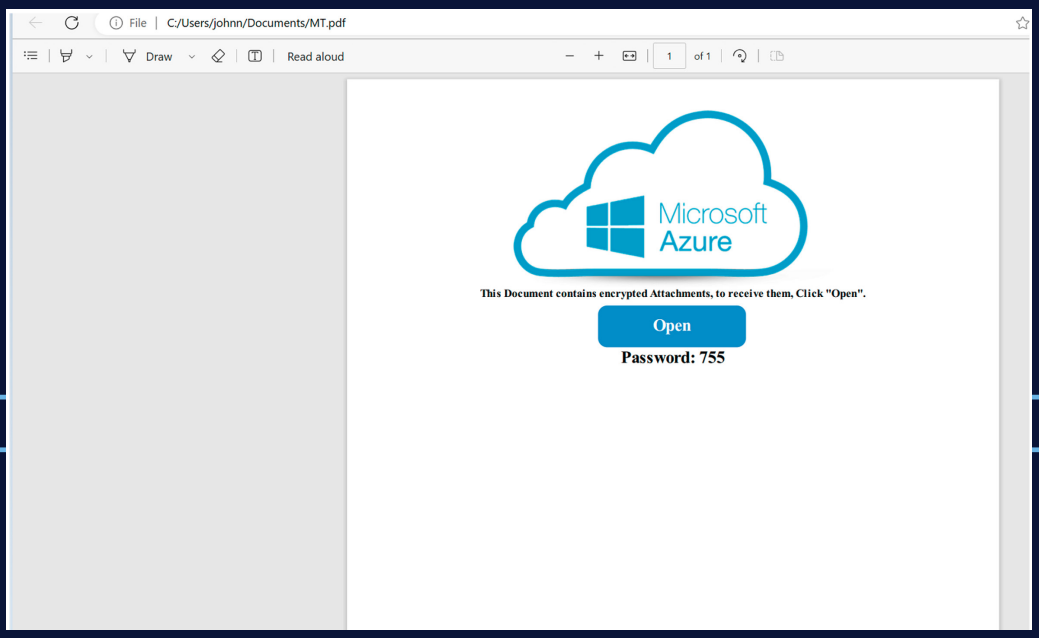
- AM.pdf
- DM.pdf
- EM.pdf
- HN.pdf
- And more.

A typical email with QakBot attachment may look like this:

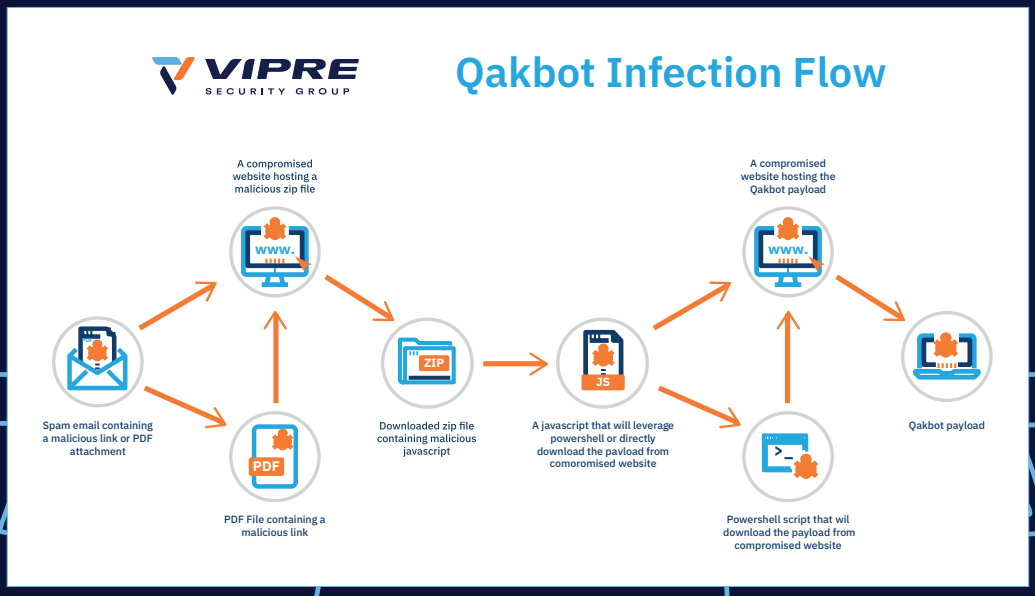


QakBot: How It Works (continued)

A typical email will direct the victim to a disguised QakBot link, like this "Open" button on a fake Microsoft Azure cloud account:



See below for an in-depth view of the QakBot flow, starting from malicious link or PDF attachment:



Q2 Conclusions

As usual, with billions of emails there is a lot to take in. Even analyzing a few thousand can give you an incredible big-picture view, and the data always proves revealing.

In Q2 of 2023:

1. **April saw the biggest spike in email compromise, possibly due to it being the end of the 2022 tax year.**
2. **VIPRE Labs discovered a new malspam campaign that utilizes a macro-less attack.**
3. **QR code-based attacks are on the rise, as we predicted for 2023.**
4. **QakBot is the top malware family of the quarter.**
5. **There were thousands of exploits catchable by behavioral-driven email solutions alone.**

And most malware is still delivered via malicious links embedded in compromised email threads.

VIPRE's Q2 2023 Email Threat Trends Report provides a rare glimpse into the email threat landscape, exposing malicious trends and bringing adversarial email tactics to light. We use our updated threat data to influence our email security solution delivery, customizing our platform to meet the challenges enterprises face today – quarter by quarter.

For more information about VIPRE's best-in-class email security solutions, click here.

Stay up to date and look out for the next installment of the Q3 VIPRE Email Threat Bulletin

Q1 An Expert Look at Email-Based Threats 2023

Q2 BEC is on the Rise 2023

Q3

Q4

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