Spam trends campaigns senior superlatives 2023

By Ole Villadsen, Golo Mühr

Published: 2024-02-28 · Archived: 2026-04-06 00:46:36 UTC

Authors

Ole Villadsen

Cyber Threat Hunt Analyst

IBM Security

The 2024 IBM X-Force Threat Intelligence Index revealed attackers continued to pivot to evade detection to deliver their malware in 2023. The good news? Security improvements, such as Microsoft blocking macro execution by default starting in 2022 and OneNote embedded files with potentially dangerous extensions by mid-2023, have changed the threat landscape for the better. Improved endpoint detection also likely forced attackers to shift away from other techniques prominent in 2022, such as using disk image files (e.g. ISO) and HTML smuggling.

Of course, with these security improvements, attackers are forced to find successful entry points into organizations, and in 2023, X-Force observed attackers—in particular, initial access brokers—increasingly shift to placing malicious links within emails to download subsequent payloads or attach PDF files containing malicious links. Other key observations for 2023 include:

- An increase in the use of Nullsoft Scriptable Install System (NSIS) executables and .NET-based obfuscators and packers in executable files used to deliver commodity malware.
- The continued prominence of ZIP files as the most observed archive. More advanced threat actors introduced new file types within archives such as Internet shortcut (.URL) files, whose overall use increased significantly in 2023.
- An increase in the exploitation of older vulnerabilities such as CVE-2017-11882, the most prolific exploit in email campaigns.
- The adoption of increasingly complex execution chains likely designed to reduce detection rates and filter out security researchers and automated sandboxes.

This article describes high-level shifts X-Force observed in threat actors' email campaigns in 2023 and leverages the tradition of United States High School "Senior Superlatives" to highlight noteworthy campaigns and trends that X-Force observed last year along with examples. The article concludes with a look at what to expect in 2024 and what organizations can do to detect and improve their defenses.

Bye bye malicious macros?

The 2023 X-Force Threat Intelligence Index highlighted how threat actors were forced to change tactics in 2022 when Microsoft began to block macro execution by default in documents received through email or from the internet. The move away from malicious macros became even more apparent with Office documents containing malicious Visual Basic Application (VBA) macros and Excel Macro (XLM) files observed in a few campaigns early in 2023. Year over year X-Force saw a 93% reduction in email spam containing maldocs leveraging VBA macros with close to no activity since late March, when X-Force observed their use with Emotet and Hive0133 campaigns.

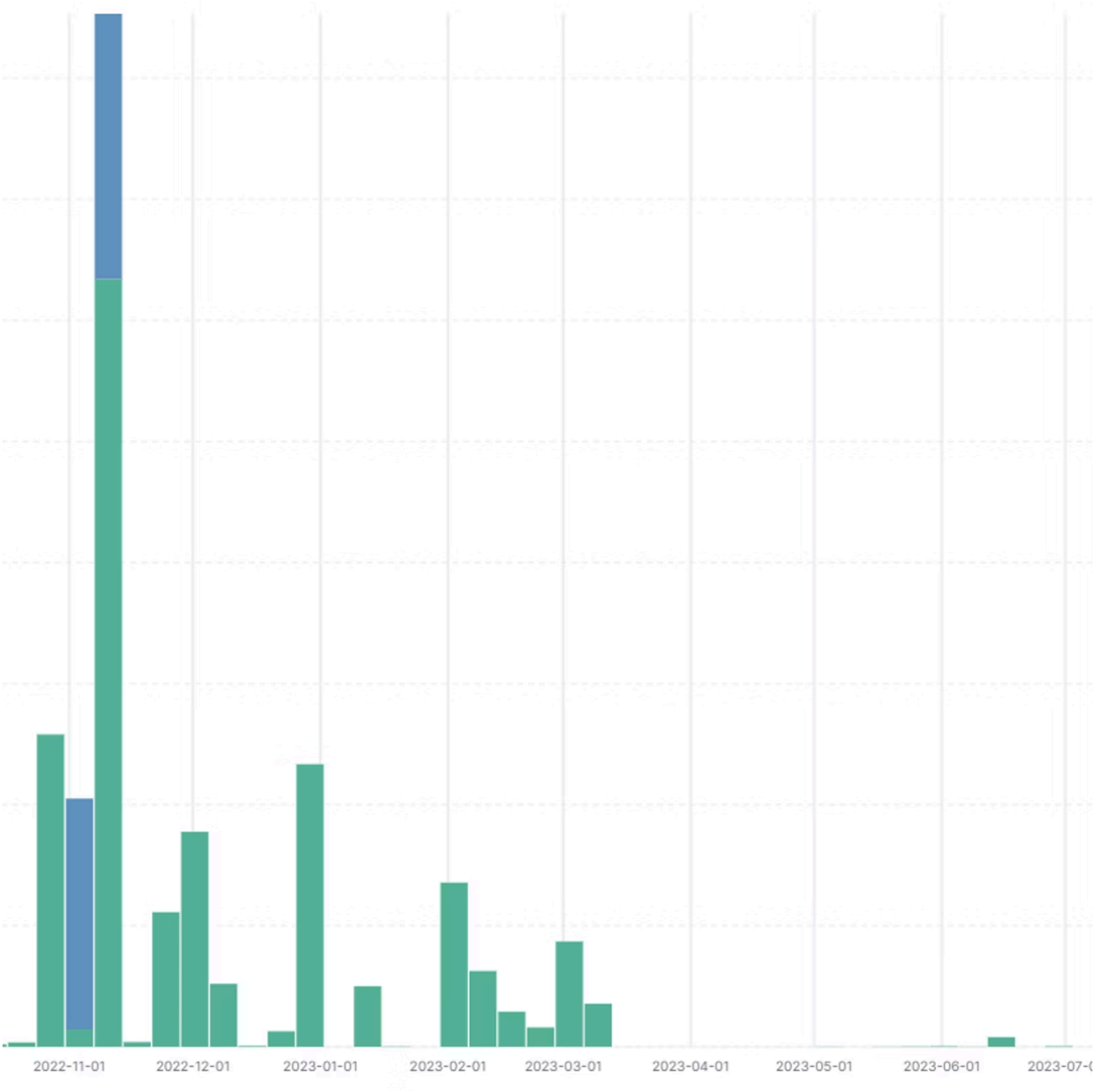


Figure 1: Volume of emails with VBA and XLM documents in 2023. Source: X-Force

This dramatic reduction in attackers' use of malicious macros is a positive reflection of how implementing certain changes to an environment can practically shut down what would have otherwise been fruitful opportunities for

malicious actors. However, as discussed later in this article, when one door closes for an attacker, they attempt to find their way in through another door.

Short-lived campaigns: HTML smuggling and OneNote

As in 2022, X-Force identified Qakbot and other activities last year that used HTML smuggling to compromise victims. This evasive technique allows the attacker to use HTML 5 and JavaScript running in the browser to dynamically decode or decrypt a payload embedded within the HTML and drop it to the victim's system. While the majority of HTML smuggling activity took place in March, activity was also observed in January, April, and May. Year-over-year HTML smuggling activity is down 96%. X-Force assesses this is the case because endpoint detection continues to improve. A local HTML file triggering the browser to "download" something without web traffic is suspicious. Additionally, HTML files are very large if they bear an encoded payload – another opportunity to detect this activity.

In early 2023, X-Force also observed multiple groups leveraging OneNote attachments in their campaigns to include the initial access brokers TA570 and TA577—known for delivering Qakbot, and TA551, whose campaigns primarily delivered IcedID. Other groups using OneNote attachments included Emotet and Hive0126 (which overlaps with TA581), with the latter attempting to deliver IcedID and Bumblebee malware.

Figure 2: Volume of OneNote emails in 2023. Source: X-Force

The short-lived but large OneNote campaigns by these threat actors occurred in the first three months of the year. Notably, X-Force has observed very little activity using OneNote attachments since March 2023. This is likely because Microsoft took steps to block embedded files with "dangerous extensions" in April.

Containers/Archives: Disk images down; NSIS and .URL up

In 2022, X-Force observed an increase in the use of malicious disk images (ISO, IMG) with Windows shortcut files (LNK) to deliver malware. This landscape shifted in 2023, with the use of ISO files dropping to only 3% of container/archive deliveries and IMG files similarly down to 1.39%. This is likely due to email detections adjusting to the previous year's threats. There is minimal legitimate use of disk images in emails, making it easy to identify as suspicious.

In 2023, ZIP files were again by far the most common delivery mechanism among archives (54.07%), followed by RAR files (20.13%).

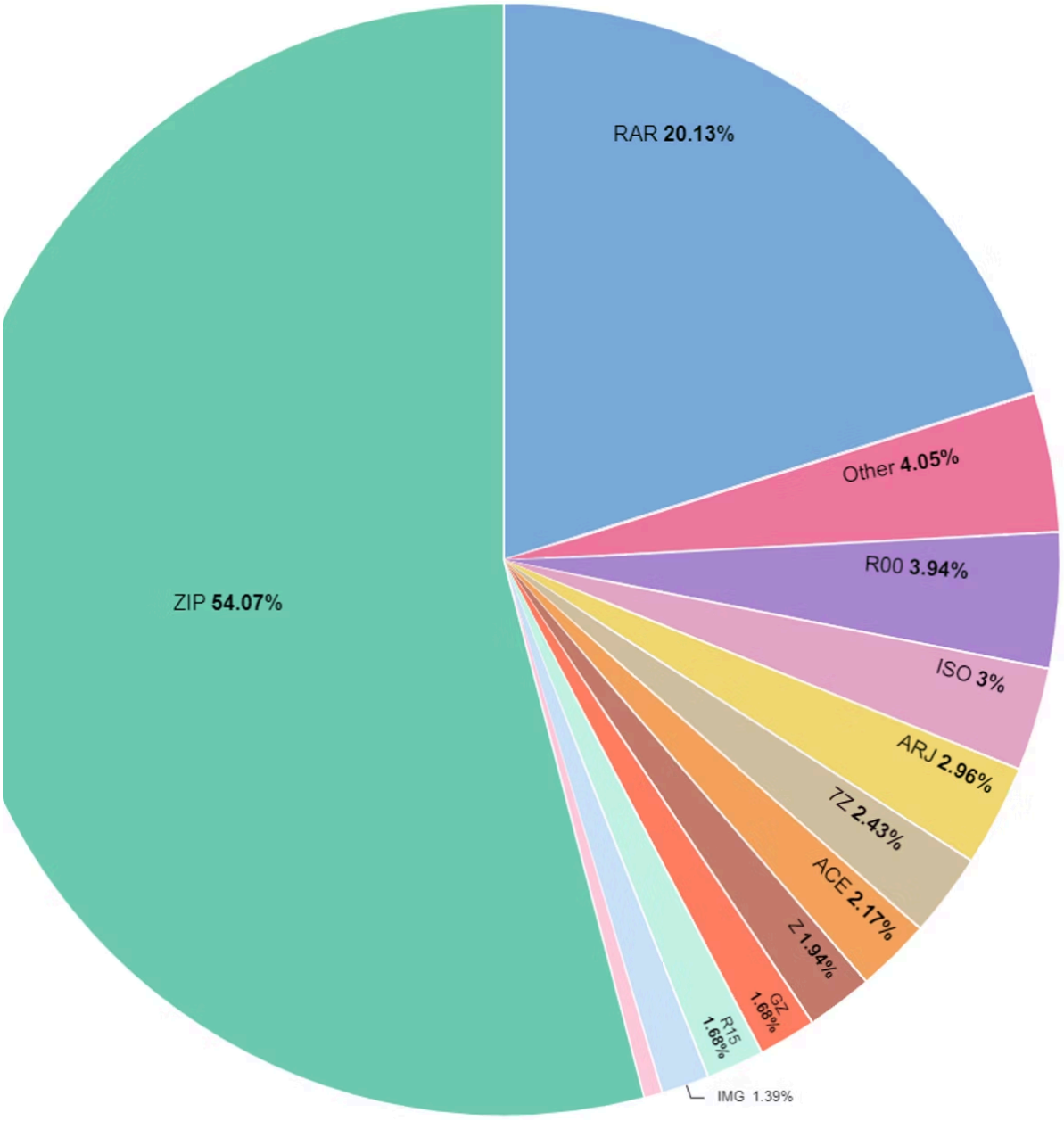


Figure 3: 2023 top archive extensions. Source: X-Force

The majority of file types contained within container or archive attachments – greater than 80% – were Windows executables, which are mainly used to deliver commodity Stealers and RATs such as Agent Tesla, the "Most Common Malware" X-Force observed in 2023. Attackers pivot though, where they can, to evade detection: X-Force saw a notable increase in Nullsoft Scriptable Install System (NSIS) executables—likely because NSIS is more difficult to scan since it works as a self-extracting archive. These installers were found mostly in 7z, RAR, and ZIP files and make up more than 25% of executables observed in 2023 spam emails. Another common technique is the use of . NET-based obfuscators and packers such as Eazfuscator, .NET-Reactor, Crypto-Obfuscator and the Roboski packer – which were used in more than 60% of the executables X-Force observed.

More advanced threat actors have also switched to less common filetypes within archives such as Internet shortcut (.URL) files, which were used in several large campaigns, as seen in Figure 4 below, including from Hive0126. The use of .URL files in general—whether within an archive, directly attached to emails, or as part of complex execution chains—increased dramatically in 2023.

Other examples of file types used for malspam include various script files such as Batch, JavaScript, Windows Script Files or Visual Basic. X-Force also observed the use of .PIF and .COM extensions on Windows executables, which are less common but also result in automatic execution if opened by a Windows user.

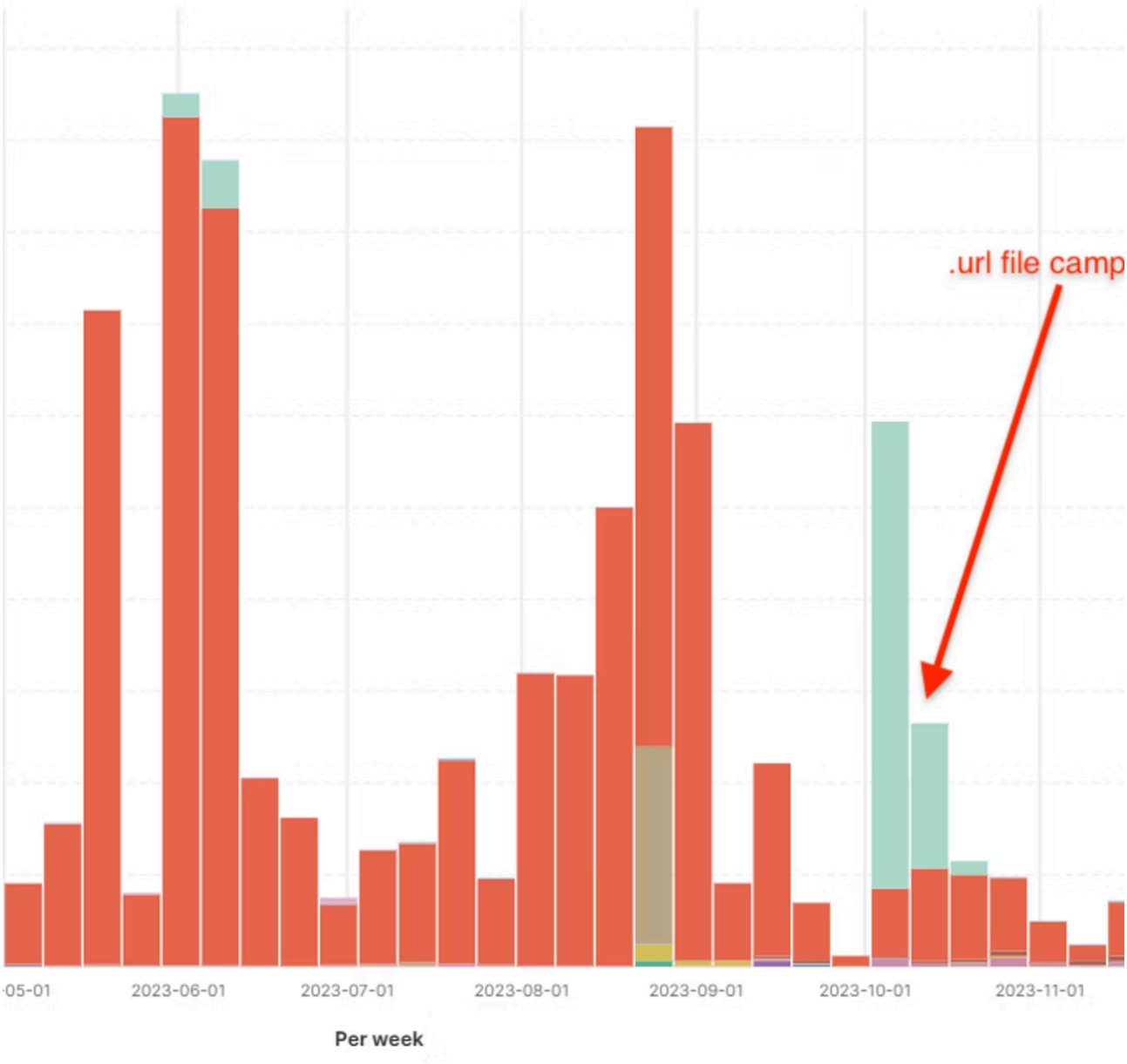


Figure 4: Volume of emails leveraging less common file types within archives in 2023. Source: X-Force

URLs and PDF files take the stage

Coinciding with the decline in Macros, disk images and HTML smuggling files, X-Force has observed threat actors—including initial access brokers such as TA570, TA577, and Hive0133—shift increasingly to using URLs placed directly within emails or within attached PDF files to download malicious payloads. X-Force also has observed Latin American distributors regularly employ these techniques to deliver banking trojans such as Ousaban and Grandoreiro. Threat actors likely have adopted these techniques because it would not be feasible for network defenders or security solutions to block emails wholesale with URLs or PDF attachments given their prevalent use with legitimate communication. Other security researchers have also identified the trend towards increased use of PDFs early last year.

This dynamic forces network defenders into a game of "whac-a-mole" to identify and either flag or block potentially malicious URLs and PDF attachments before they can lead to dangerous infections, including ransomware attacks. X-Force has also observed threat actors require passwords provided within the email to open encrypted PDFs, impeding the ability to scan these PDFs for malicious URLs or other content. In other cases, threat actors have adopted several evasion techniques unique to PDF files to obfuscate or otherwise conceal URLs, making it more difficult to identify and extract embedded links for review and enabling them to pass through security solutions. The "Senior Superlatives" section below for "Most Dangerous Campaigns" provides an example of a TA577 campaign using a malicious PDF attachment.

High schools in the United States practice a tradition in which graduating seniors are awarded "superlatives" for being the best example of a given category, such as "Most Likely to Succeed", "Most Outspoken", or "Most Popular". Leveraging such superlatives provides an effective way to highlight interesting campaigns, trends, and statistics for 2023 from X-Force telemetry, as detailed below.

Most Common Malware

The winner of 2023's "Most Common Malware" goes to Agent Tesla, a popular information stealer active since 2014 and available for sale on underground markets. Rounding out the top five most common malware are the information stealers Formbook and Lokibot, the remote access tool Remcos, and Snake Keylogger. These malware were typically delivered within archives or downloaded by malicious office documents, including those exploiting CVE-2017-11882 (see below).

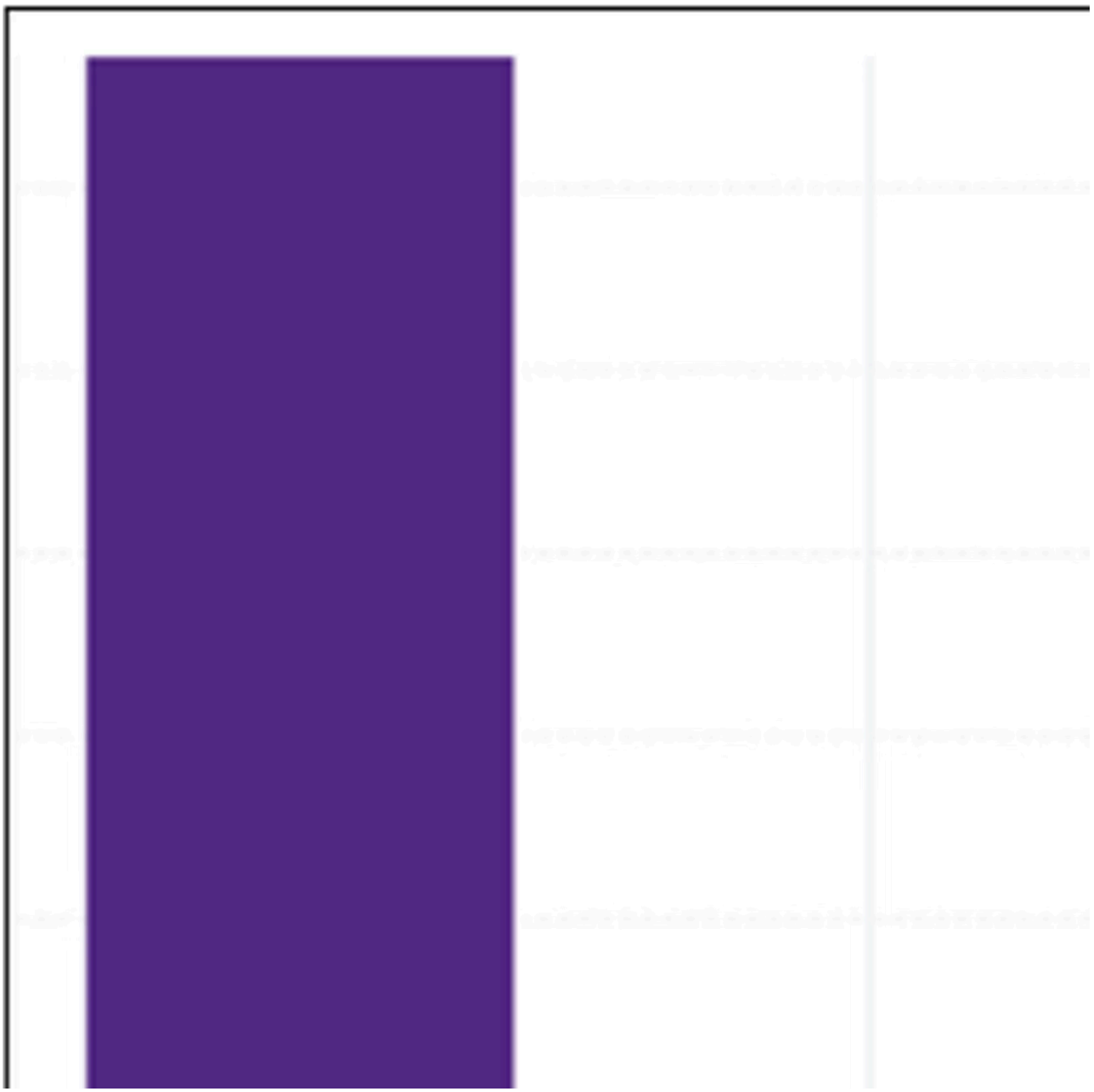
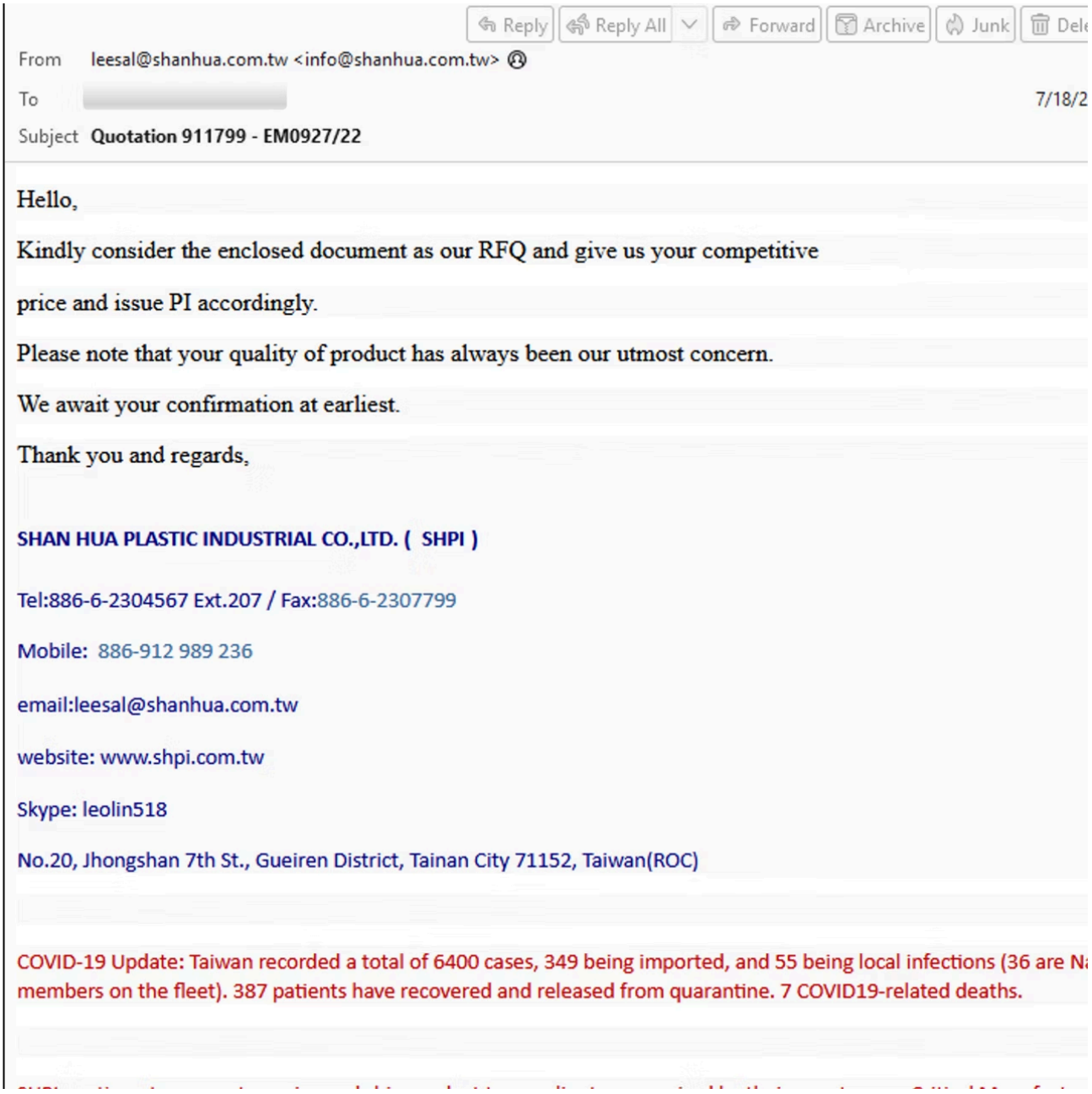


Figure 5: Most common malware observed in email spam for 2023. Source: X-Force

Figure 6 provides an example of an email campaign delivering Agent Telsa using an NSIS installer delivered within a ZIP archive. As mentioned above, X-Force has also observed an increase in the use of NSIS installers to deliver commodity malware.


Reply Reply All Forward Archive Junk Dele

From leesal@shanhua.com.tw <info@shanhua.com.tw>

To

Subject **Quotation 911799 - EM0927/22**

7/18/2

Hello,

Kindly consider the enclosed document as our RFQ and give us your competitive

price and issue PI accordingly.

Please note that your quality of product has always been our utmost concern.

We await your confirmation at earliest.

Thank you and regards,

SHAN HUA PLASTIC INDUSTRIAL CO.,LTD. (SHPI)

Tel:886-6-2304567 Ext.207 / Fax:886-6-2307799

Mobile: 886-912 989 236

email:leesal@shanhua.com.tw

website: www.shpi.com.tw

Skype: leolin518

No.20, Jhongshan 7th St., Gueiren District, Tainan City 71152, Taiwan(ROC)

COVID-19 Update: Taiwan recorded a total of 6400 cases, 349 being imported, and 55 being local infections (36 are N
members on the fleet). 387 patients have recovered and released from quarantine. 7 COVID19-related deaths.

Figure 6: Email delivering Agent Tesla infostealer using an NSIS installer. Source: X-Force

Most observed exploit

The winner of the “Most observed exploit” category goes to CVE-2017-11882. Now that the easy way in through the use of macros has been mitigated, many threat actors are focusing on creating and weaponizing exploits for older and potentially vulnerable versions of MS Office. Notably, X-Force observed a significant increase in the use of files exploiting the vulnerability CVE-2017-11882 – a remote code execution vulnerability in the Microsoft Office Equation Editor tool. Campaigns exploiting this vulnerability to deliver commodity malware such as Agent Tesla, Remcos, Formbook, Lokibot, Xworm and AsyncRAT (to name a few) came in large waves in 2023, with spikes in activity observed in March, May, and July, resulting in this exploit being the most observed in spam documents in 2023.

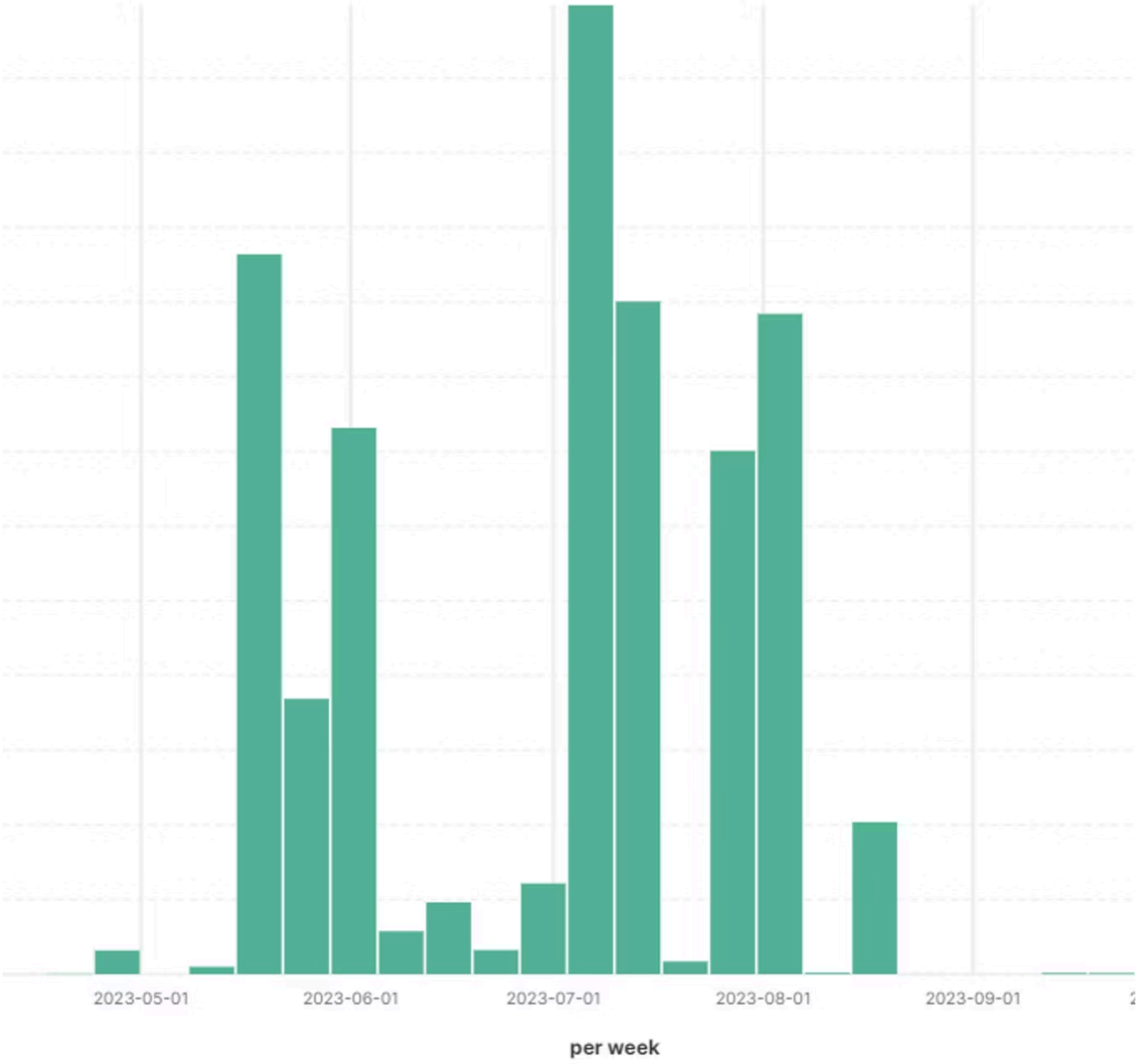


Figure 7: Volume of emails exploiting CVE-2017-11882 in 2023. Source: X-Force

Although a patch has been available since November 2017, attackers bank on organizations not having applied the security update and are therefore potentially vulnerable to their exploit. In fact, attackers often take advantage of organizations overwhelmed by the task of identifying, prioritizing and remediating vulnerabilities. Vulnerability management services can help organizations handle this task effectively ensuring high-risk vulnerabilities, like CVE-2017-11882, are found and remediated.

Figure 8: Malicious email leveraging CVE-2017-11882 to download Formbook. Source: X-Force

Most dangerous campaigns

The “Most dangerous campaigns” category goes to the initial access broker TA577, also known as “TR” and tracked by X-Force as Hive0118. TA577 campaigns in 2023 delivered Qakbot until it was disrupted in August, after which they switched to DarkGate, IcedID, and Pikabot. X-Force observed several TA577 email campaigns last year result in successful Qakbot infections, which have been observed leading to BlackBasta ransomware attacks. TA577 combines high-volume campaigns with email “thread hijacking”, in which attackers add malicious URLs or attachments to a stolen email to make it appear more legitimate. The majority of TA577 campaigns since last spring have leveraged malicious URLs or PDFs containing a malicious URL. The example below took place on 22 December and delivered Pikabot.

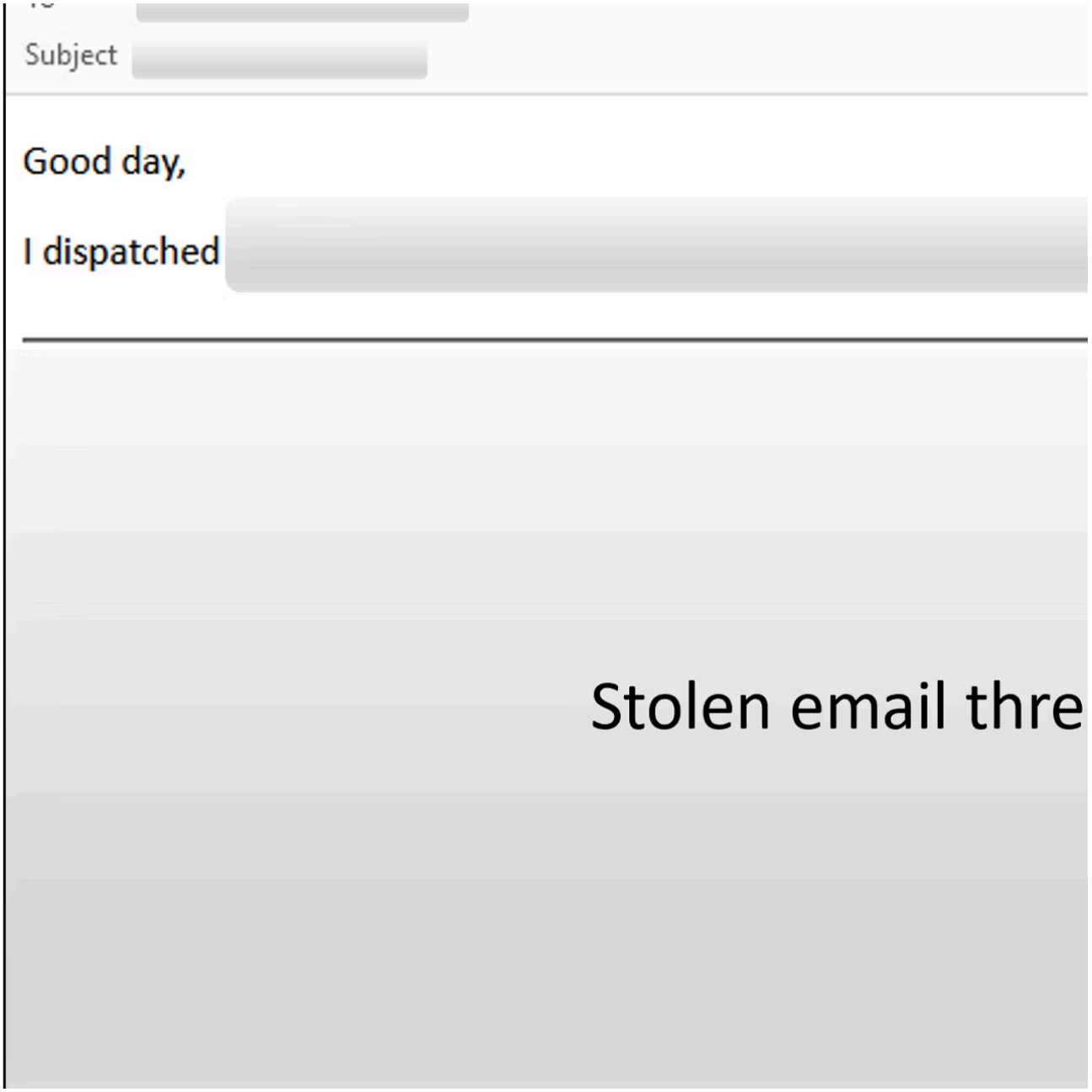


Figure 9: TA577 Thread-hijacking email delivering a malicious PDF attachment. Source: X-Force

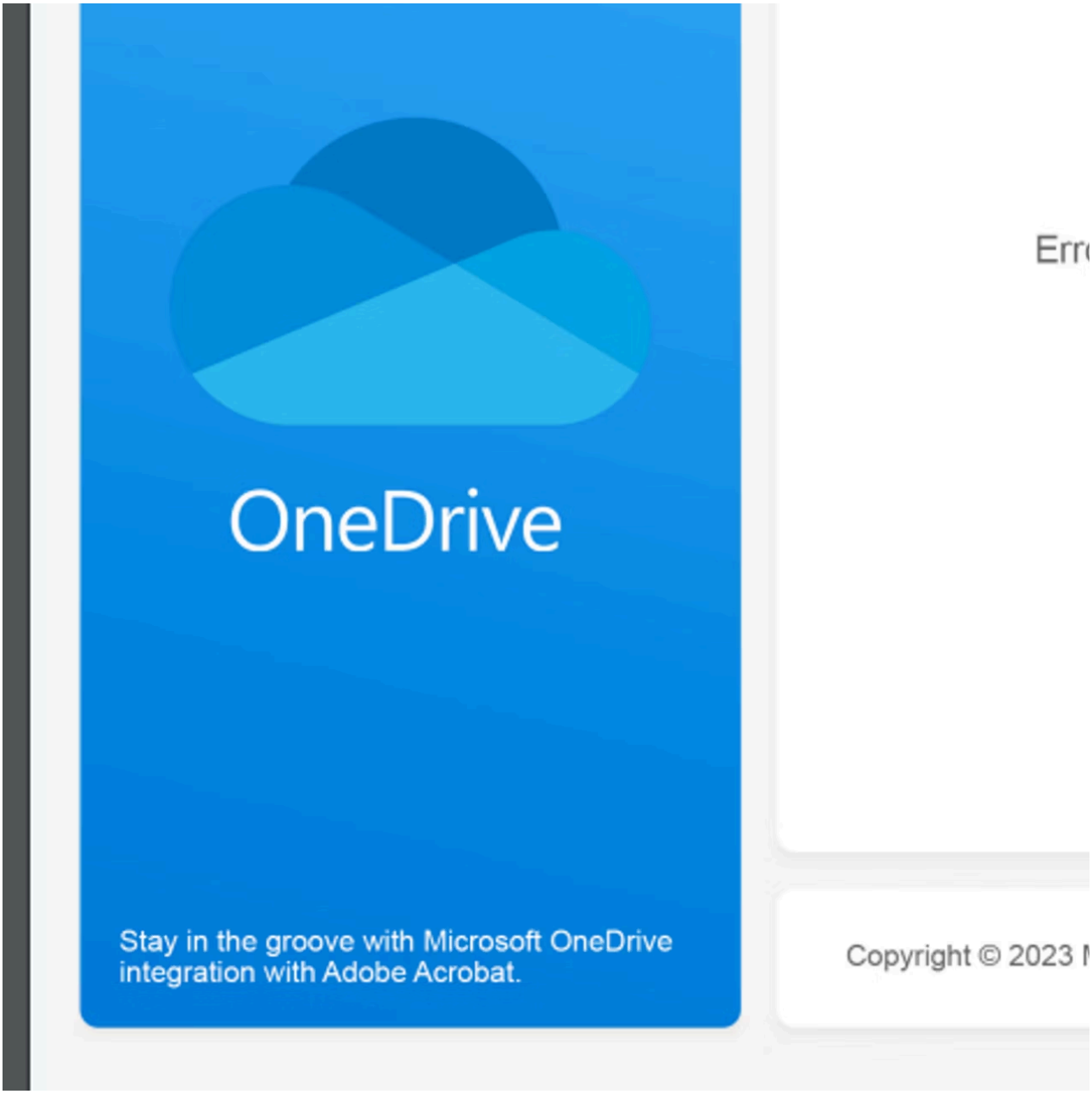


Figure 10: PDF containing a malicious URL, delivered by the TA577 campaign in Figure 9. Source: X-Force

Most complex infection chain

The “Most complex infection chain” goes to a campaign from mid-December 2023 delivered by a distributor tracked as Hive0137. Over the past year, threat actors have increasingly employed complex execution chains. The use of several consecutive stages makes individual components and their behavior less prone to detection and allows attackers to implement checks at several different points throughout the infection to filter out security researchers and automated sandboxes.

Hive0137 has been active since at least October delivering emails containing malicious PDF attachments or URLs which have led to DarkGate, NetSupport and a new loader dubbed “T34 Loader.” Hive0137 campaigns overlap with Proofpoint’s BattleRoyal cluster, which also noted the complexity of their email campaigns. During a

Hive0137 campaign taking place on 19 December 2023, X-Force identified an extraordinarily complex infection chain delivering the T34 Loader. X-Force has previously observed the T34 Loader downloading the Rhadamanthys stealer.

To download and install the T34 loader, this campaign leveraged an Open Redirect URL, the Keitaro traffic distribution system (TDS), remote configuration data and four distinct files, including two .URL files, a downloader PE file, the Snow crypter, and the T34 Loader DLL. Of note, the Snow crypter was developed by former members of the Trickbot/Conti syndicate (aka ITG23), suggesting a relationship between threat actors developing or using T34 Loader and ITG23.

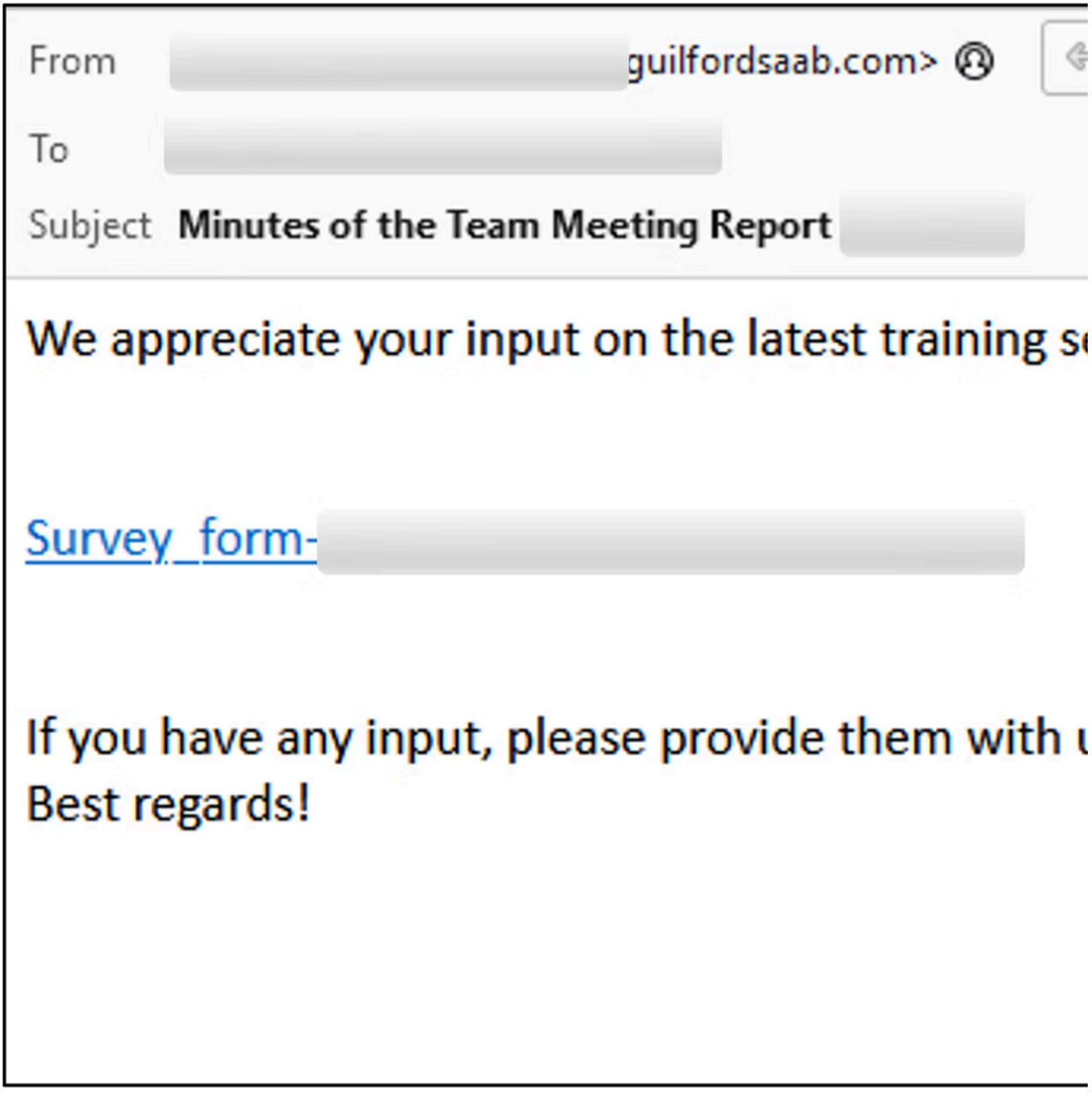


Figure 11: Hive0137 email with a malicious URL commencing an elaborate execution chain. Source: X-Force

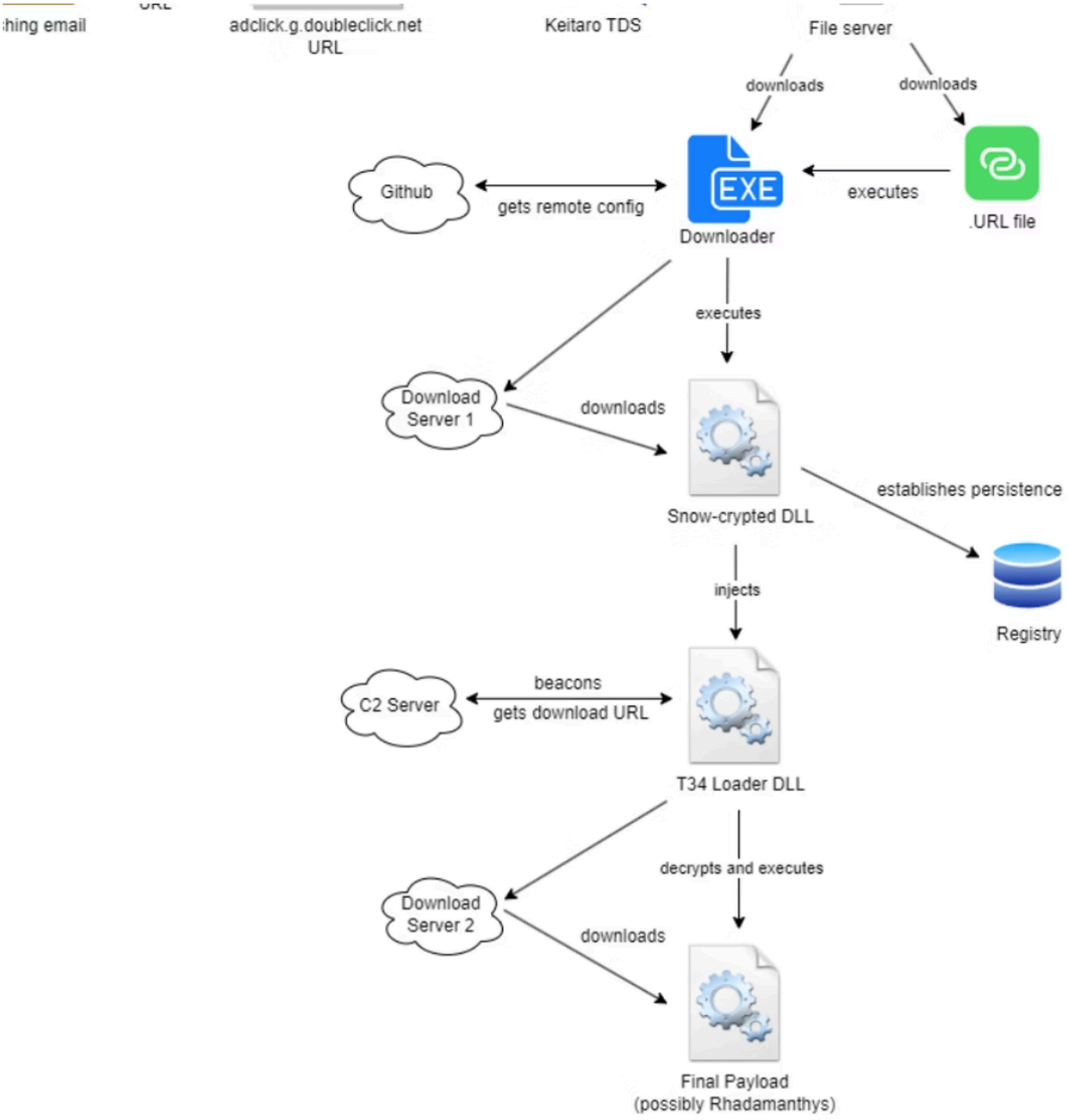


Figure 12: Hive0137 campaign using a complex execution chain to deliver the final payload.

Moving forward in 2024, X-Force anticipates email spam distributors will continue to adopt new tactics, techniques, and procedures (TTPs) to bypass security solutions and network defenses and convince users to execute email attachments and links. In particular:

- Threat actors will continue to use URLs within emails and PDF attachments to commence execution chains. An email with a PDF attachment looks far less suspicious than an email with a disk image. Threat actors understand this and will use these methods to get past the first line of defense.
- Email distributors will increasingly embrace artificial intelligence and Large Language Models (LLMs) to create more convincing email content that pushes users to click on links or execute attachments. Spam emails can often be spotted quickly if they use poor grammar, broken English, or simplistic messages. This will change as actors leverage AI to help them create professional and polished emails.

- Increasingly complex infection chains with multiple stages will also likely increase. Already there are regular email campaigns that make use of multiple stages before delivering the final payload, with the goal of deflecting security researchers and sandboxes and minimizing behavior to pass through security defenses. Attackers will likely turn to unusual file types to support these execution chains, such as .URL attachments or script files e.g. Javascript or batch files.

Good cyber-hygiene will continue to play a critical role in preventing the success of email-based attacks e.g., regularly updating and patching applications, ensuring anti-virus software and associated files are working and up to date, and maintaining vigilance for any suspicious activity.

Organizations should also train users to exercise extreme caution with email links and PDF attachments and to refrain from executing unusual file types that they may have never seen before or trigger their sixth sense that something is wrong, e.g. .URL attachments or script files. To limit the danger from script files, organizations should also consider changing the default application for Javascript/JScript/VBScript files to Notepad.

Policy and procedure changes in the form of multi-factor authentication implementation, monitoring for leaked enterprise credentials and review of policies for disk image auto-mounting can also help mitigate the risk of email spam attacks.
