VIRUSTOTAL MALWARE TRENDS REPORT: EMERGING FORMATS AND DELIVERY TECHNIQUES

VIRUSTOTAL

JUL 23

Welcome

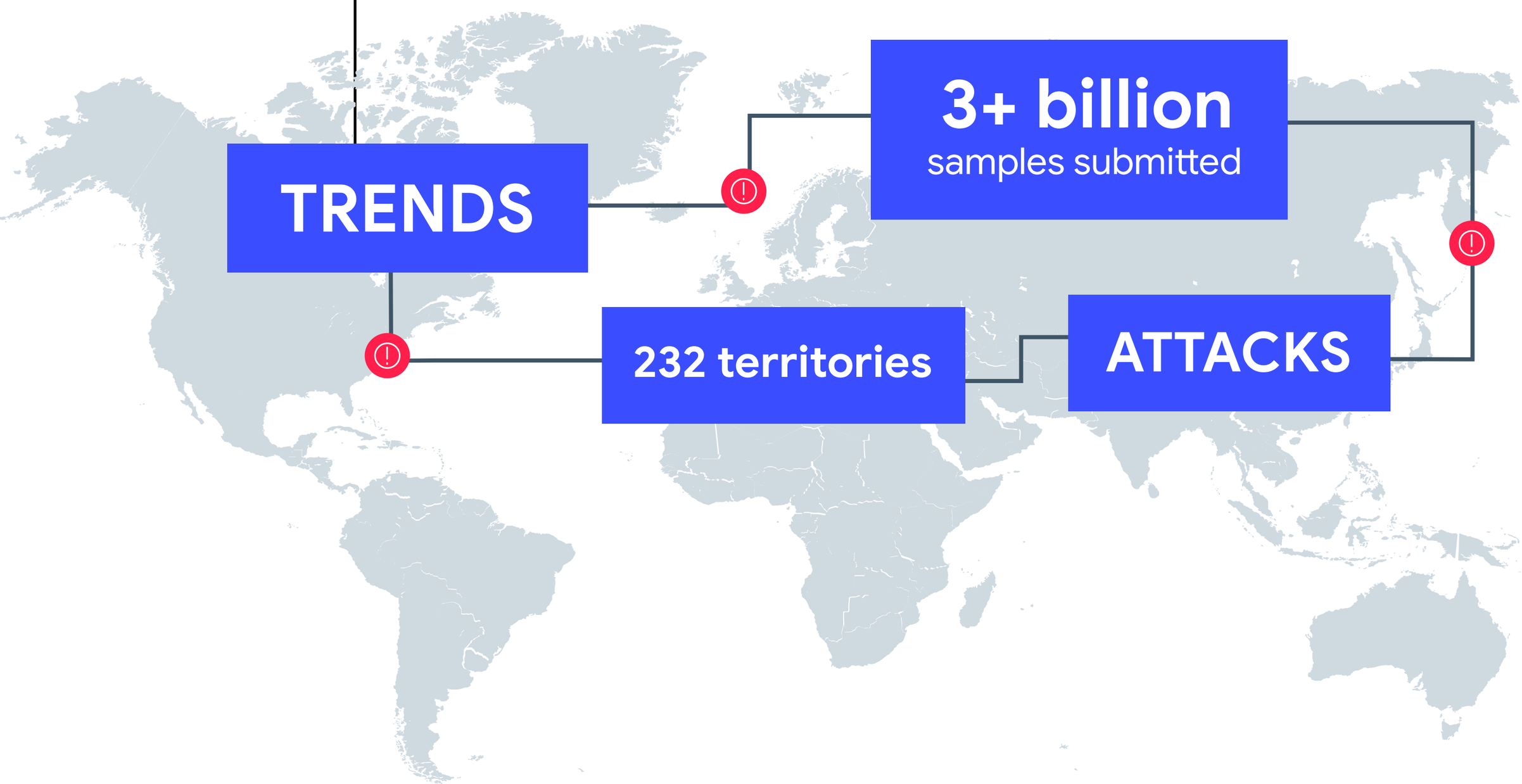
Welcome to the VirusTotal **“Emerging Formats and Delivery Techniques”** research report. We hope that by sharing our visibility into the malware threat landscape, we can help researchers, security practitioners, and the greater public better understand the evolution of malware attacks. This report explores various malware trends, including how delivery methods are evolving, and what file formats are being used to spread malware. In particular, we analyzed more than 3 billion samples submitted to VirusTotal between January 2021 and May 2023 .

Email attachments remain a popular way to spread malware, and recent data shared in this report demonstrates that attackers are increasingly using new file types and techniques to evade detection. In 2023, attackers began using OneNote as a reliable alternative to macros in other Office products, with antivirus (AV) products initially being caught off guard by this new format. We also observed the increase of attackers using ISO files for spreading malware, sometimes using them as heavily compressed attachments that make them difficult to scan by security solutions.

We found these new formats being increasingly used to spread all types of malware families, as well as participate in more targeted attacks.

VirusTotal is in a unique position to provide a source of comprehensive visibility of the malware landscape. Over the last 19 years, we have processed more than two million files per day across 232 territories. VirusTotal also harnesses contributions of its community of users to provide relevant attack context. We use this crowdsourced intelligence to analyze relevant data, share an understanding of how attacks develop, and help inform how they might evolve in the future.

We hope this report contributes to ongoing community efforts to discover and share actionable information on malware trends.



Executive Summary

Key observations:

- Email attachments continue to be a popular way to spread malware, even though this technique is decades old.
- Traditional file types such as Excel, RTF, CAB, and compressed formats are becoming less popular for malware delivery as email attachments.
- Although the use of PDFs slowly decreased for the last few months, with the exception of occasional peaks corresponding to campaigns, in June 2023 we observed the biggest peak in the number of suspicious samples for the last two years.
- New trends such as using OneNote and JavaScript distributed along HTML are the most rapidly growing formats for malware delivery in 2023.
- OneNote emerged in 2023 as a reliable alternative for attackers to the traditional use of macros in other Office products.
- AV products were initially caught off guard by the use of OneNote for malware delivery.
- Attackers increased the use of ISO files for malware spreading, distributing all types of families and participating in targeted campaigns.
- ISO files are also distributed as heavily compressed email attachments. The large size, once decompressed, makes them difficult to scan by some security solutions.
- ISO files are being disguised as legitimate installation packages for a variety of software, including Windows, Telegram, AnyDesk, and malicious CryptoNotepad, among others.

Methodology

VirusTotal relies on crowdsourced contributions, which provides a bigger picture on how different malware spreads and attacks evolve. All data in this report is compiled using a representative subset of submissions from our users from January 2021 until the end of June 2023.

For the realization of this study, we have examined files first seen in VirusTotal over the past three years that also have been identified as malicious by at least 5% of the AV engines we integrate with. Based on these files, we began analyzing relationships with other entities (emails, ISO files and other file types). We focus on both detecting anomalies and examining the evolution of the most common file formats in malware campaigns.

The relevance of the samples observed and detected as malicious varies throughout the year. Small changes in malicious samples driven by variances in contributors, polymorphism, and external crawlers can result in significantly more unique detections.

Malware Distribution Trends

Attackers combine the usage of well-known distribution vectors for their malware campaigns with new formats that help them understand the evolution of defenses, and effectiveness of different social engineering techniques. We have been monitoring samples submitted to VirusTotal since January 2021 to determine how attacker techniques have evolved, specifically their file formats of choice used for malware distribution.

Looking at our data on the evolution of the files attached to malicious emails since the beginning of the year, we observed a significant increase between March and April of 2023. In fact, spreading malware via email attachments, despite being a very old technique, saw an increase in popularity as far back as 2022. We started by analyzing the evolution of traditional file types used as malicious attachments (Figure 1).

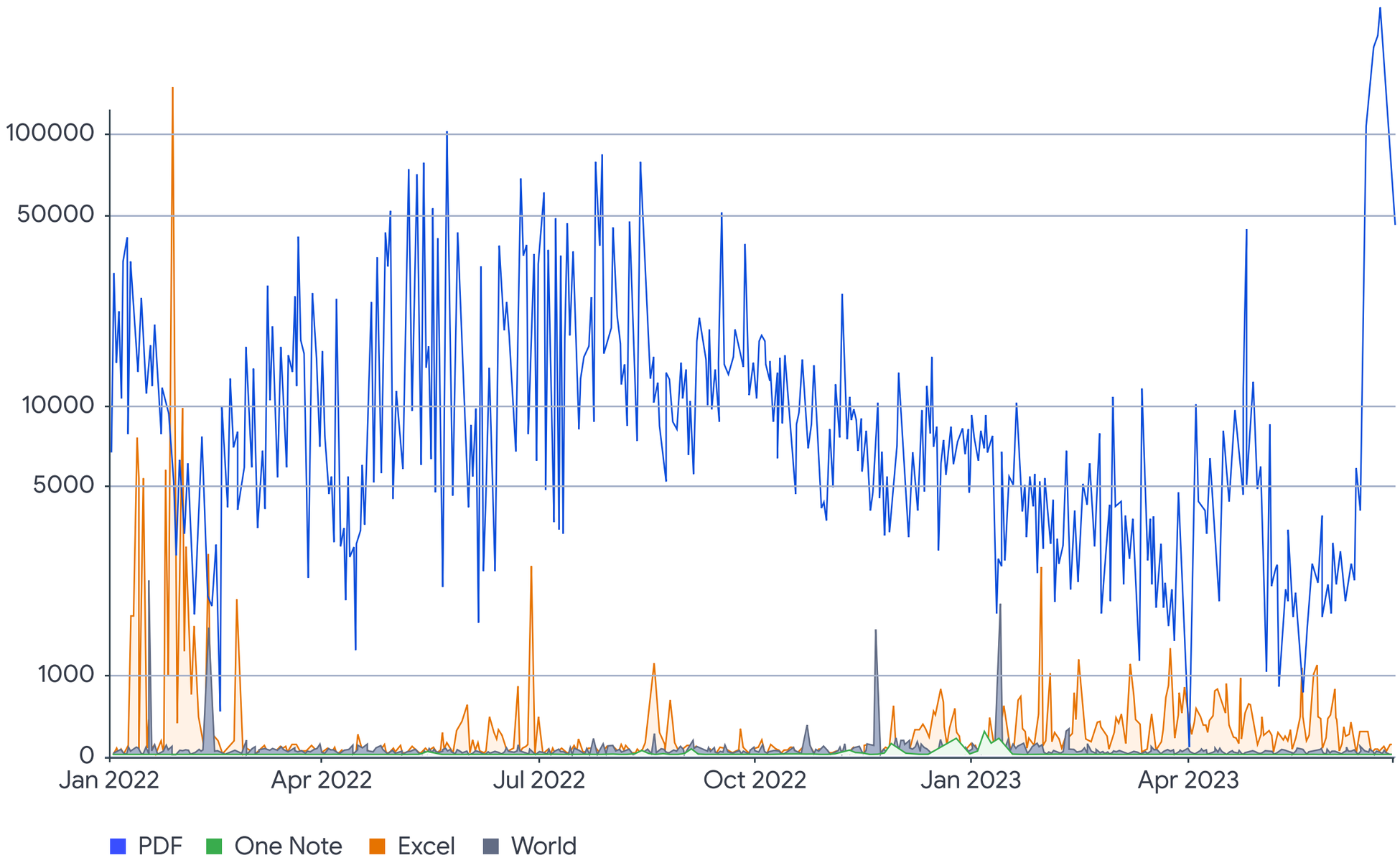


Fig 1.

File types used as malicious attachments since 2022

For the last two years, we have observed peaks of suspicious PDF files linked to campaigns. Although it appears as though the trend has slowly decreased since Q4 2022, we still find fresh campaigns in 2023, including the highest peak of suspicious PDF files seen to date in June 2023. We have observed these PDFs being used for various purposes; for example, they could be “weaponized” to exploit a vulnerability, or simply contain a link to a phishing site that requests information.

In 2022 we observed peaks of suspicious Excel files, many related to Emotet distribution. During this period, Microsoft Word seemed to have had a more constant baseline with fewer smaller peaks, which seems to imply its use for malware distribution is in decline, but not dead. We observed peaks in May 2023 both for Word and Excel, followed by the biggest peak in June 2023. This speaks of the opportunistic usage of both formats depending on the campaign. The peak of both file types (along with PDF files) seems to indicate a remarkable increase in malware distribution efforts by mid-2023.

As seen in Figure 2, OneNote is an emerging format of choice for malware distributed as email attachment in 2023. We describe this OneNote attack flow in the next section. By percentage, it became the strongest newcomer format for malicious attachments in 2023.

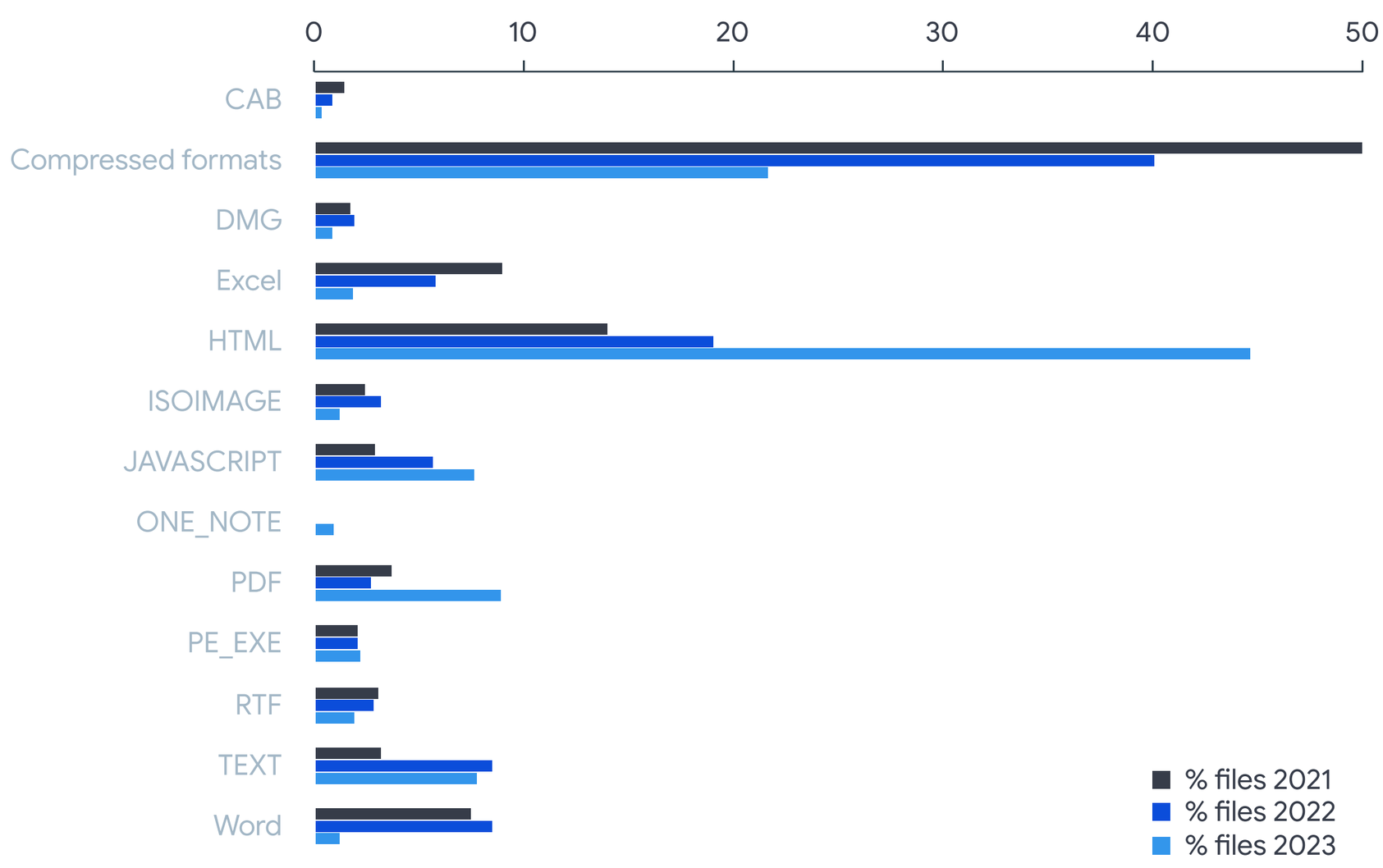


Fig 2

Comparison of different file types distributed as malicious attachments since 2021

We saw a significant increase in 2023 of JavaScript, usually distributed along with HTML, being used in elaborate phishing designed to steal victims' credentials. Excel, RTF, CAB, compressed formats, and Word all seem to be relatively declining in popularity as malicious attachments.

OneNote

OneNote refers to Microsoft OneNote note-taking software, available as part of the Microsoft Office suite and offered for free on all platforms outside the suite. It provides attackers with the ability to include inside the document malicious URLs and different scripting formats, including JavaScript, PowerShell, Visual Basic Script and Windows Script. This makes OneNote extremely flexible and resourceful for attackers, becoming a reliable alternative to the traditional use of macros by attackers in different Office products.

OneNote can be attached to emails for malware distribution, commonly as password-encrypted files. Most of the time, they are used to execute embedded scripts to download additional malware.

Although we observed OneNote increasing in popularity for malware spreading in 2023, even in Q4 2022 we found traces of samples used to distribute NjRAT and AsyncRAT. Most OneNote samples found in 2023 were actively being distributed as malicious email attachments, while samples in 2022 were simply uploaded to VirusTotal. This suggests samples in 2022 were tested to evaluate AV detection, while samples in 2023 were used in real campaigns.

Around December 2022 is when we first started observing more elaborate samples, with convincing messaging that would more likely result in a recipient interacting with the email (Figure 3 shows an example)

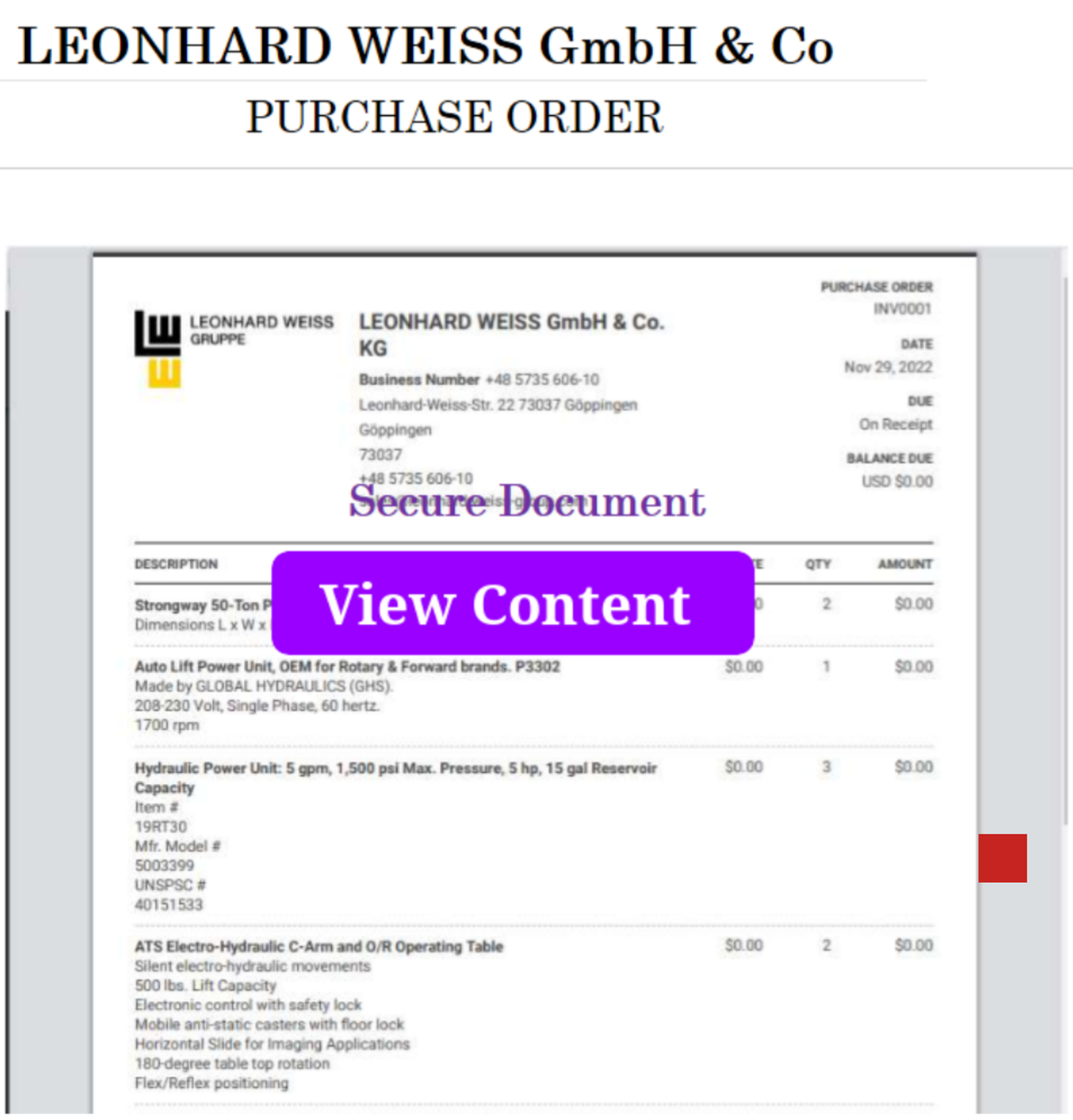


Fig 3

Example of malicious OneNote

The apparent success of these tests (as victims face an unfamiliar format), along with the flexibility of OneNote, is the likely cause behind the snowball effect we are observing. We observed that OneNote files distributed as email attachments used different file extensions, probably to complicate analysis and/or look less suspicious to victims. Figure 4 shows how most of the time they were distributed seemingly as GIF or PNG files, resulting primarily in a DLL being downloaded to the victim after execution.

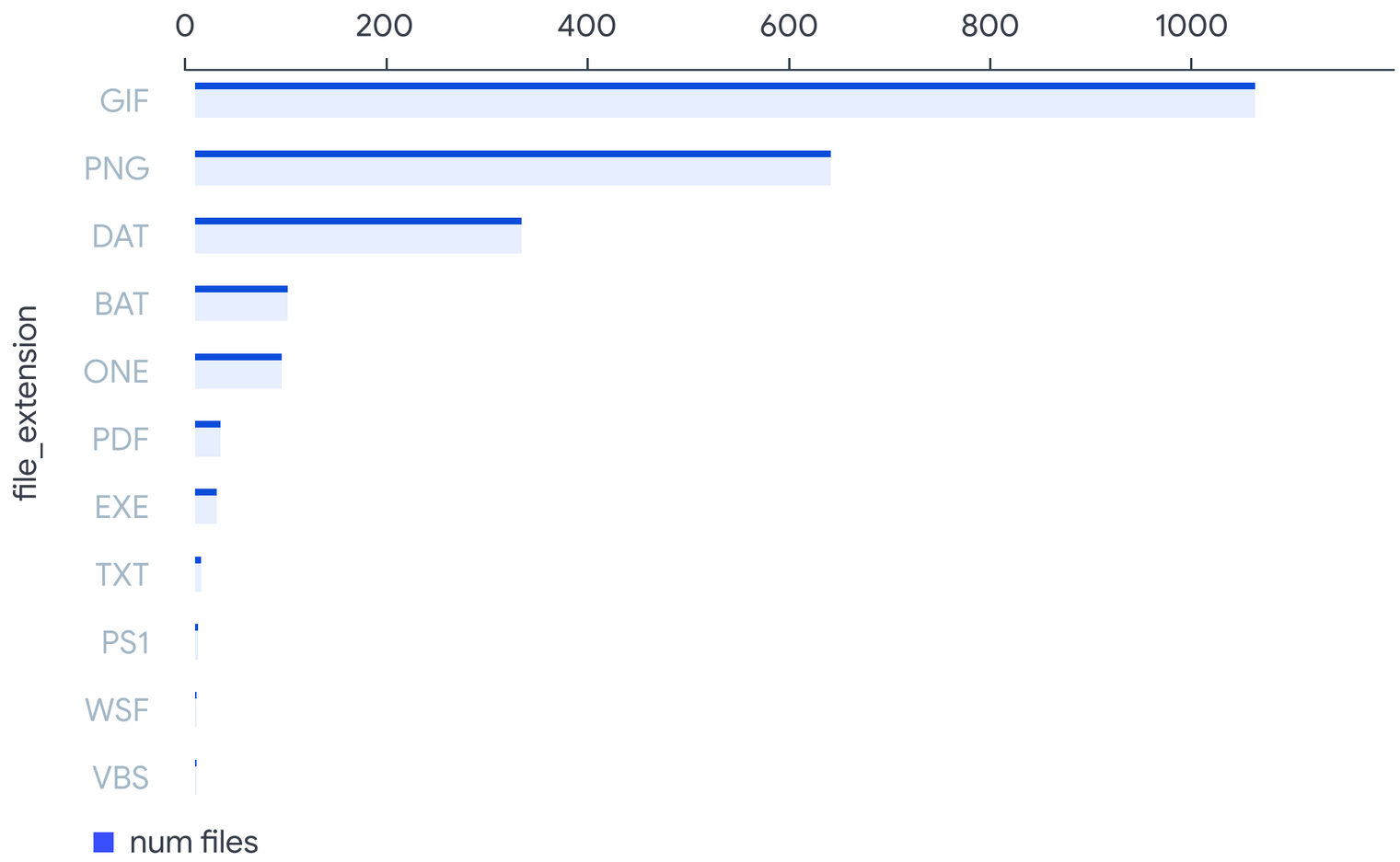


Fig 4

Extensions used by OneNote files when being distributed as malicious attachments

We observed over 70 collections in VirusTotal where OneNote files were used for distribution, 68 of them created in 2023. So far, we observed OneNote used for distributing (at least) Qakbot, IceID, Emotet, AsyncRAT and Redline. It was also observed being used by the threat actor Kimsuky for malware distribution, a subgroup under what our Mandiant colleagues refer to as APT43.

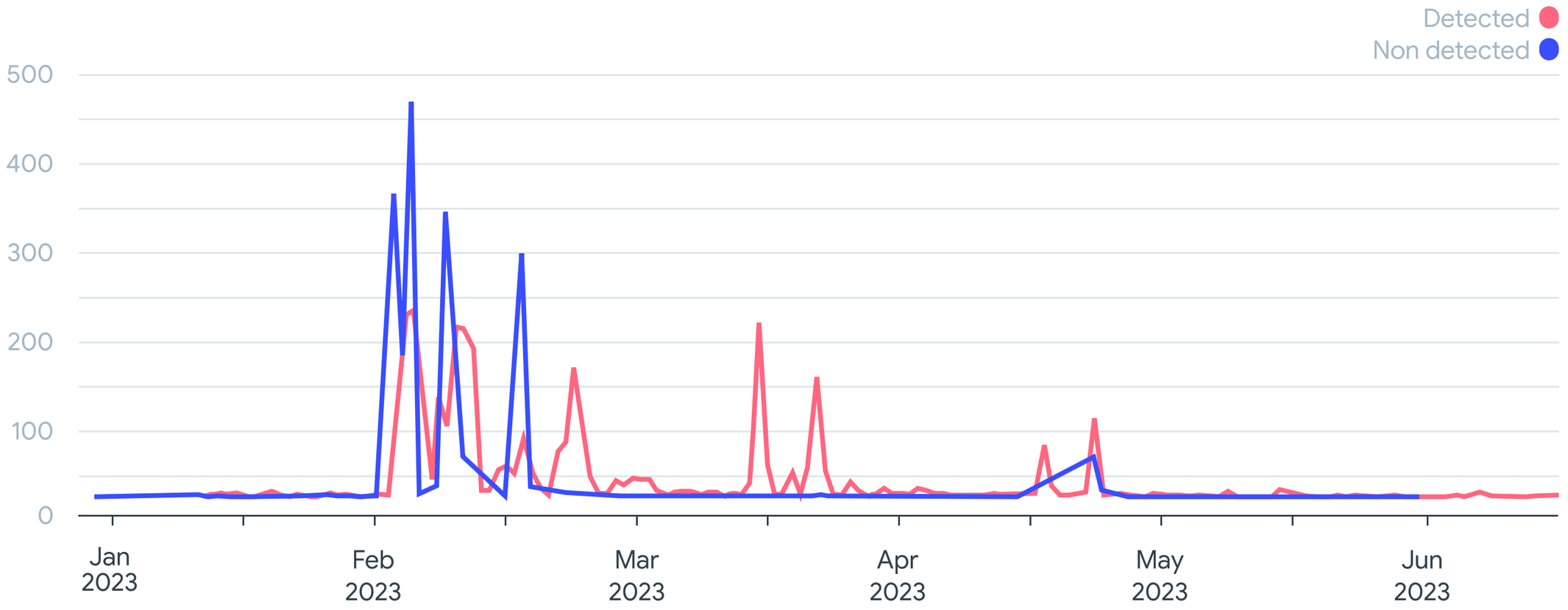


Fig 5

AV detection evolution for OneNote files

Figure 5 shows AV adding detection for a significant group of originally undetected OneNote files weeks after first seen in VirusTotal. Detection for OneNote files first seen in 2023 and publicly discussed as part of malicious campaigns is around 35%, which is reasonably high. Interestingly, detection average falls to 23% when suspicious OneNote files are found as part of active malware distribution campaigns, meaning these samples use better evasion techniques such as obfuscation. This might also show how AV engines incorporate detection for publicly known malicious samples.

ISOs

We observed an increase in the number of suspicious ISO files in 2023 when compared with 2022 (Figure 6). This is a format we find is getting more relevance for malware distribution. Although we already found the presence of ISO files in some 2022 campaigns, in 2023 we have found it distributing different malware families (lockbit, darkbit, Quakbot, AsyncRAT, RemcosRAT, among others), as well as being part of more targeted campaigns involving (according to OSINT) threat actors such as MuddyWater, Dark Pink, Saaiwc, and an unconfirmed suspected Russian threat actor.

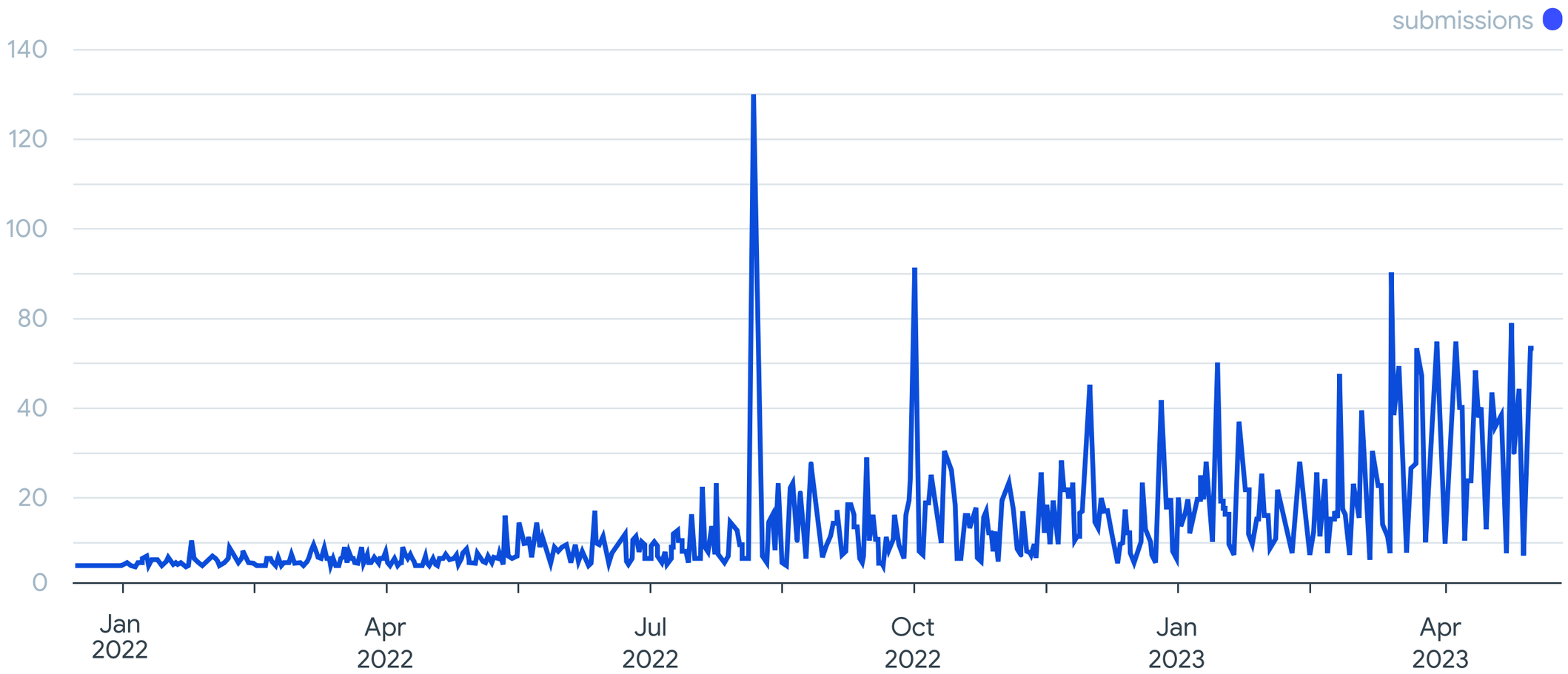


Fig 6

Timeline of suspicious ISO files submitted to VirusTotal since 2022

In this section we want to provide more details on how this format is used by malicious actors in their campaigns, and what characteristics are useful to know from a defender's perspective. We also uncovered some campaigns where ISO files were instrumental for malware distribution.

We started by plotting in a chart all ISO files found in VirusTotal, where X axis is size, and Y axis is detection ratio (Figure 7). Each black dot represents a single ISO file.

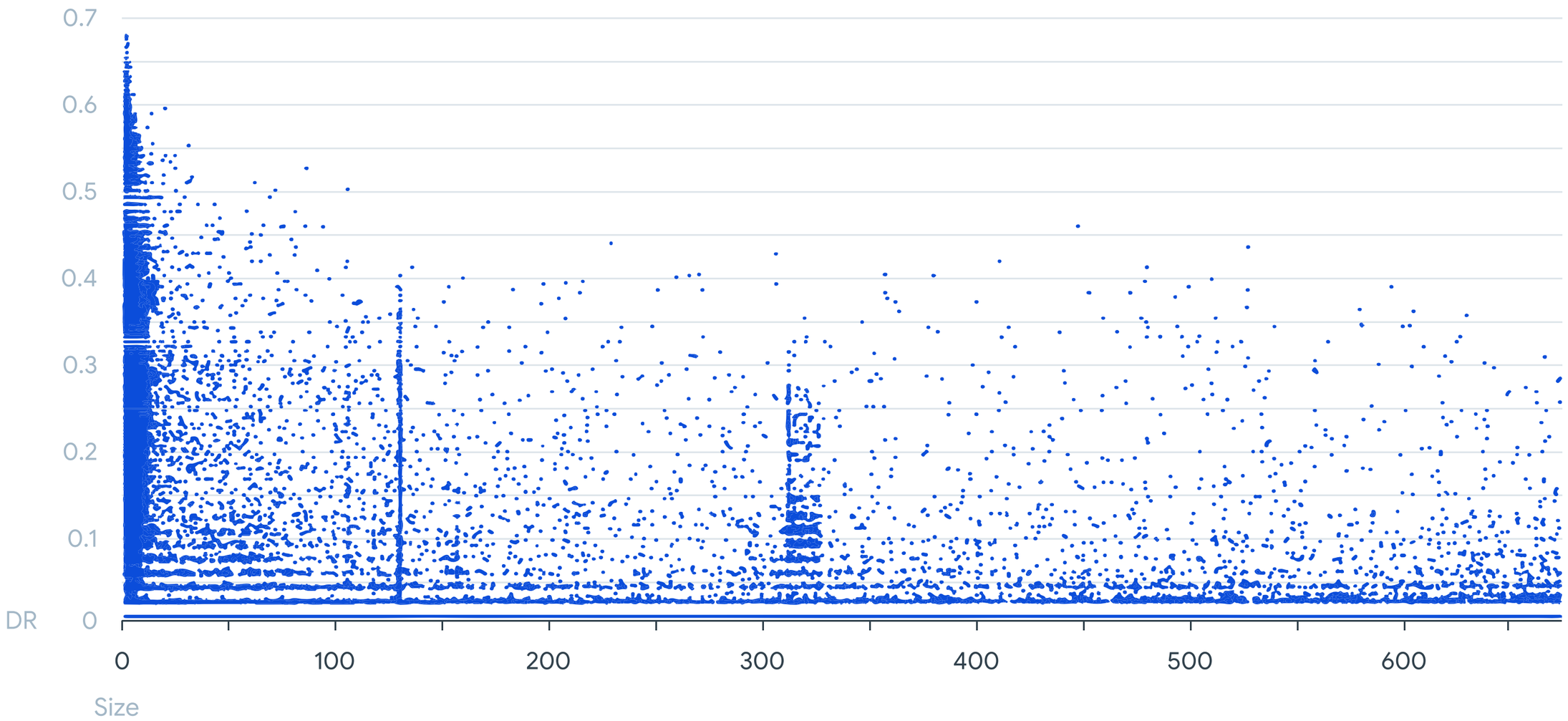


Fig 7

ISO files in VirusTotal plotted by number of detections (Y axis) and size (X axis)

Let's focus on the cluster on the left. This is a cluster of lightweight ISO files (less than 15MB) with 72% of files looking suspicious (meaning AV detection ratio is over 10%). Excluding this cluster, for all other ISO files, the "suspiciousness" ratio is 6% (instead of 72%). In short, according to this data, smaller ISO files are more likely to be malicious than large ones.

When filtering ISO files out using this 10% detection ratio, we can observe smaller clusters that correspond to malicious campaigns, as seen in Figure 8.

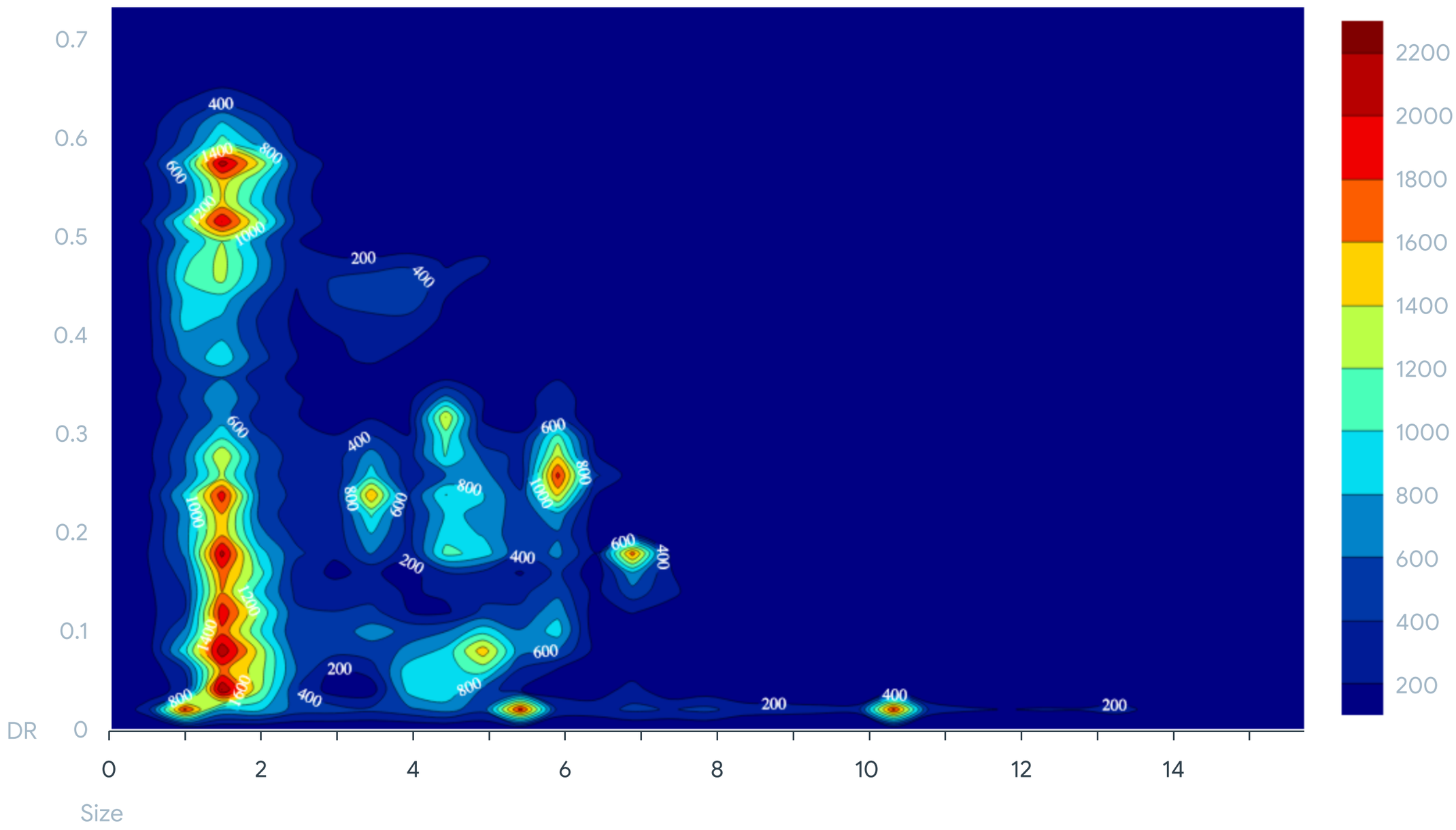


Fig 8

Suspicious clustered ISO files in VirusTotal plotted by number of detections (Y axis) and size (X axis)

We found a cluster of 18,000 files sized between 1.15Mb and 1.2Mb, and with a high detection ratio distributed as email attachments, installing a downloader for LokiBot and AgentTesla (here is a reference).

A second cluster of 7,000 files sized around 125Mb was distributing ChromeLoader samples, most of them undetected by AV engines. According to ISO metadata (such as Volume modification date), we estimate this campaign was active between January and November 2022. There is a clear prevalence among the file names used by attackers:

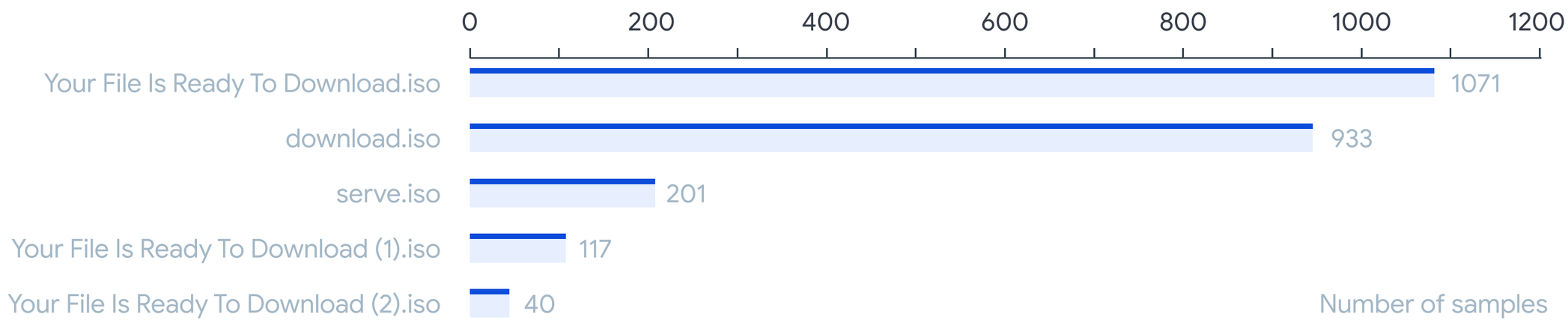


Fig 9

Most common names used for this cluster

We found a third cluster consisting of 1,200 samples with ISO files artificially inflated to 300Mb to 315Mb by appending zero bytes. This allows packing ISOs into 300Kb ZIP files so they can be delivered by mail to the victim. This also allows attackers to avoid some security solutions that limit analysis depending on the file size.

Many samples in this third cluster are disguised as legitimate ISO installers, as shown in Figure 10.

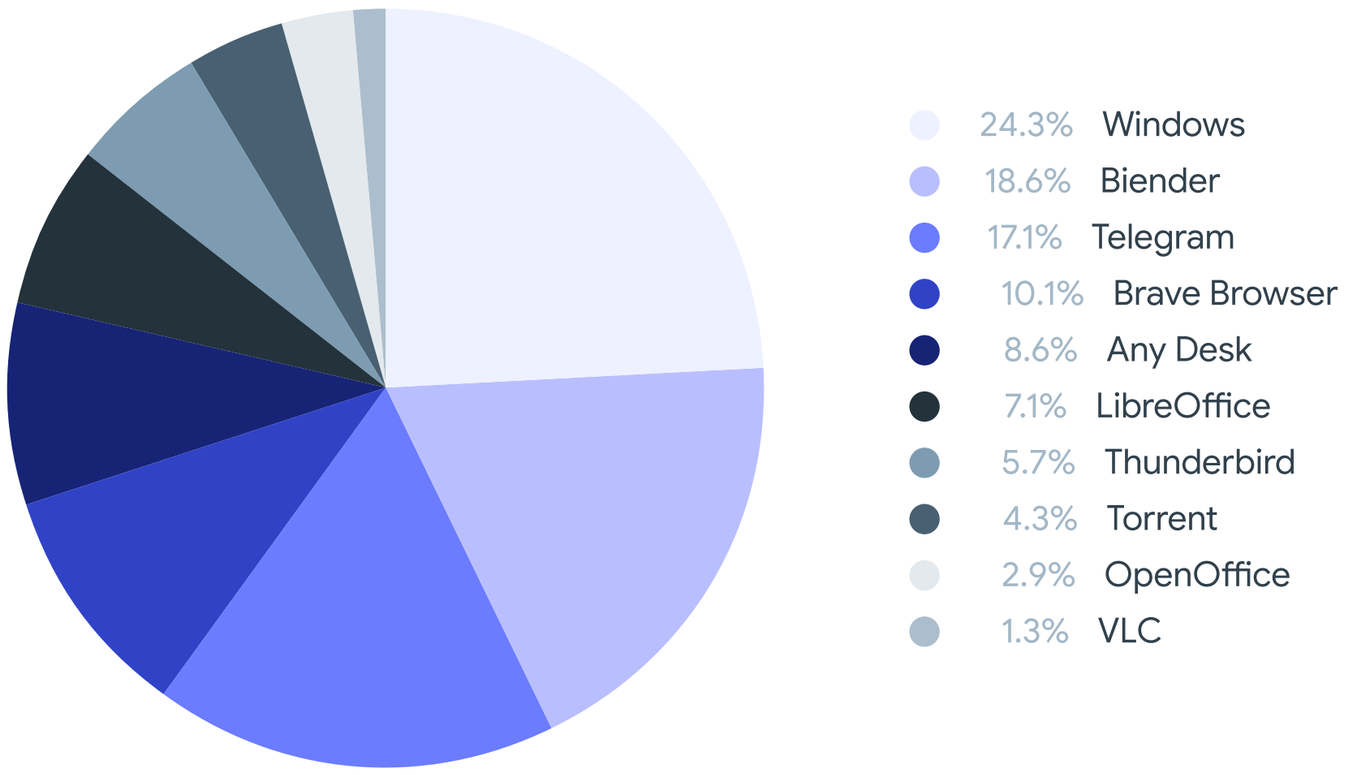


Fig 10

Distribution of malicious ISO installers by software they reflect

We also found a malicious version of Crypto Notepad being distributed in this cluster that, besides installing the expected software, is capable of executing PowerShell scripts hosted in Discord.

Besides the analysis of clusters based on their size, we found a swarm of ISO files containing a single PE executable. Indeed, these types of ISO files seem to be most prevalent, representing 79% of the total. In general, detection ratio for ISO files containing a single malicious executable is lower than detection ratio for the bundled malicious executable. These ISO files are mostly distributed by email (79.6% of samples), either directly attaching the ISO file to it or by using an intermediate archive containing it such as a compressed file. The rest (20.4%) we found being distributed in the wild.

The distribution of top domains we found hosting ISO files is seen in Figure 11, which highlights both the usage of the format for email attachments, and the abuse of legitimate domains such as discordapp, dropbox, catbox, sendspace, onedrive or filetransfer.

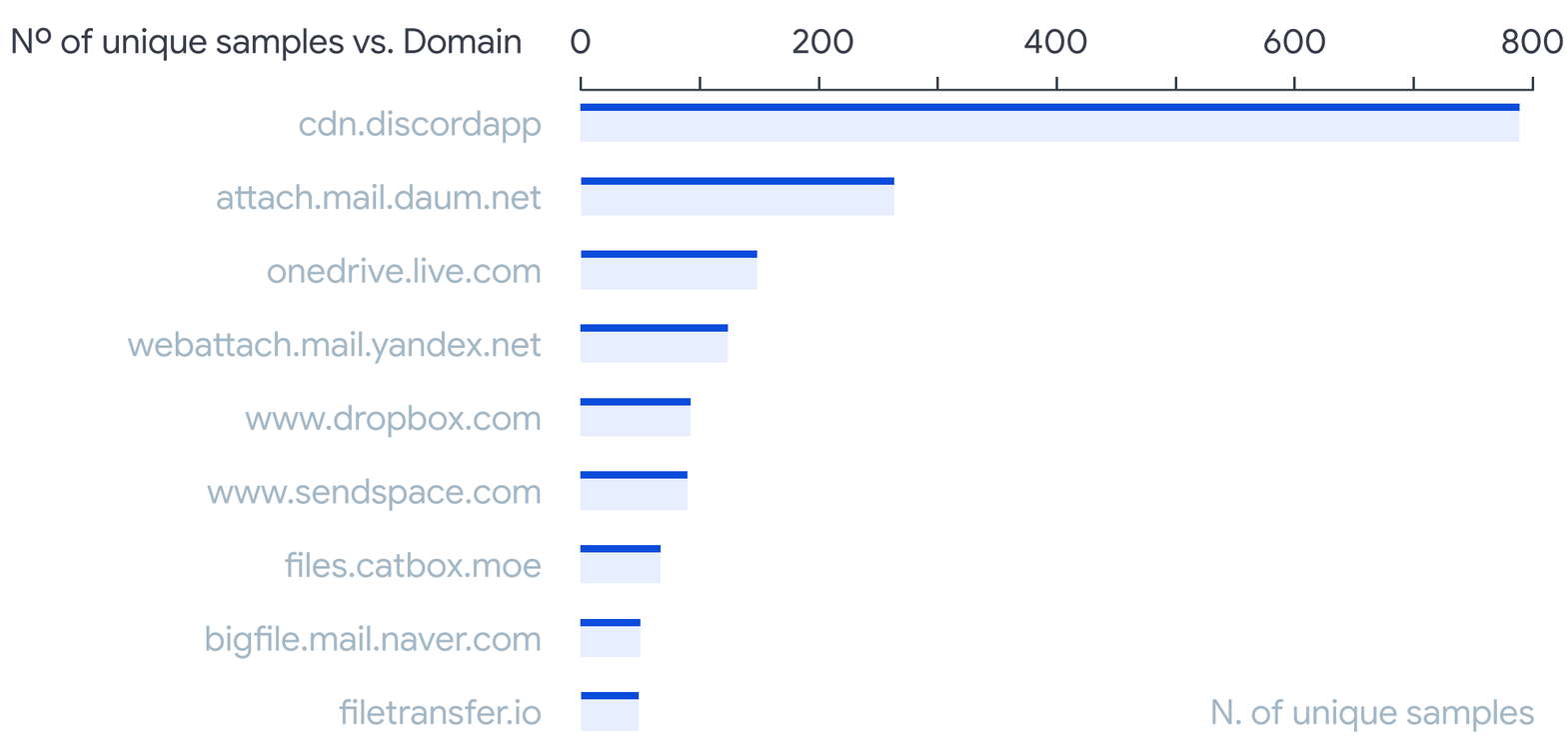


Fig 11

Top domains distributing suspicious ISO files

Final thoughts

The rotation of formats from the attacker's side should be read as a way to increase the effectiveness of their malware spreading campaigns. This includes both the social engineering and the technical side, as well the flexibility of the chosen format to perform actions on the victim's side and to avoid security measures.

Although traditional file types are still often used for malware delivery, it is important to understand how alternative formats gain popularity and how that might represent an advantage for attackers. From the awareness side, we hope this report helps the security community put more resources in making sure to stop these new spreading methods. From the technical side, OneNote seems to be a natural replacement (or addition) for Word, Excel and RTF, offering similar features. ISO might be an alternative for compressed formats.

On the distribution side, it is worth mentioning the continuous use of different legitimate platforms for malware delivery, which we already mentioned in previous reports. This also seems to be an additional advantage to masquerade malware as legitimate software for ISO files. It looks a bit surprising that the fact of simply bundling a malicious sample inside of an ISO file immediately decreases AV detections. We also observed poor detection in the first waves of OneNote malicious files, although improved with time. These techniques are used both for generic malware spreading and targeted attacks.

We suggest several ideas to minimize most common risks:

- Monitor malware spreading trends, and actively check how your security stack responds to them.
- Include in your analysis all logs to/from allowed legitimate sites as they are regularly used for malware distribution, do not exclusively focus your anomaly detection on unknown traffic.
- In addition to format-agnostic security awareness programs, consider implementing a zero-trust architecture.

We consider that the details provided in this report should serve as a heads up towards a better security awareness when it comes to malware spreading. The analysis of the evolution of formats used in malicious campaigns helps defenders and security analysts better understand how to prevent and investigate ongoing attacks. Evolution will continue, likely adding new elements to make social engineering more effective. VirusTotal will keep informing of any **new relevant** trends as we observe them.

Join the discussion @virustotal

VIRUSTOTAL

Find out more at virustotal.com