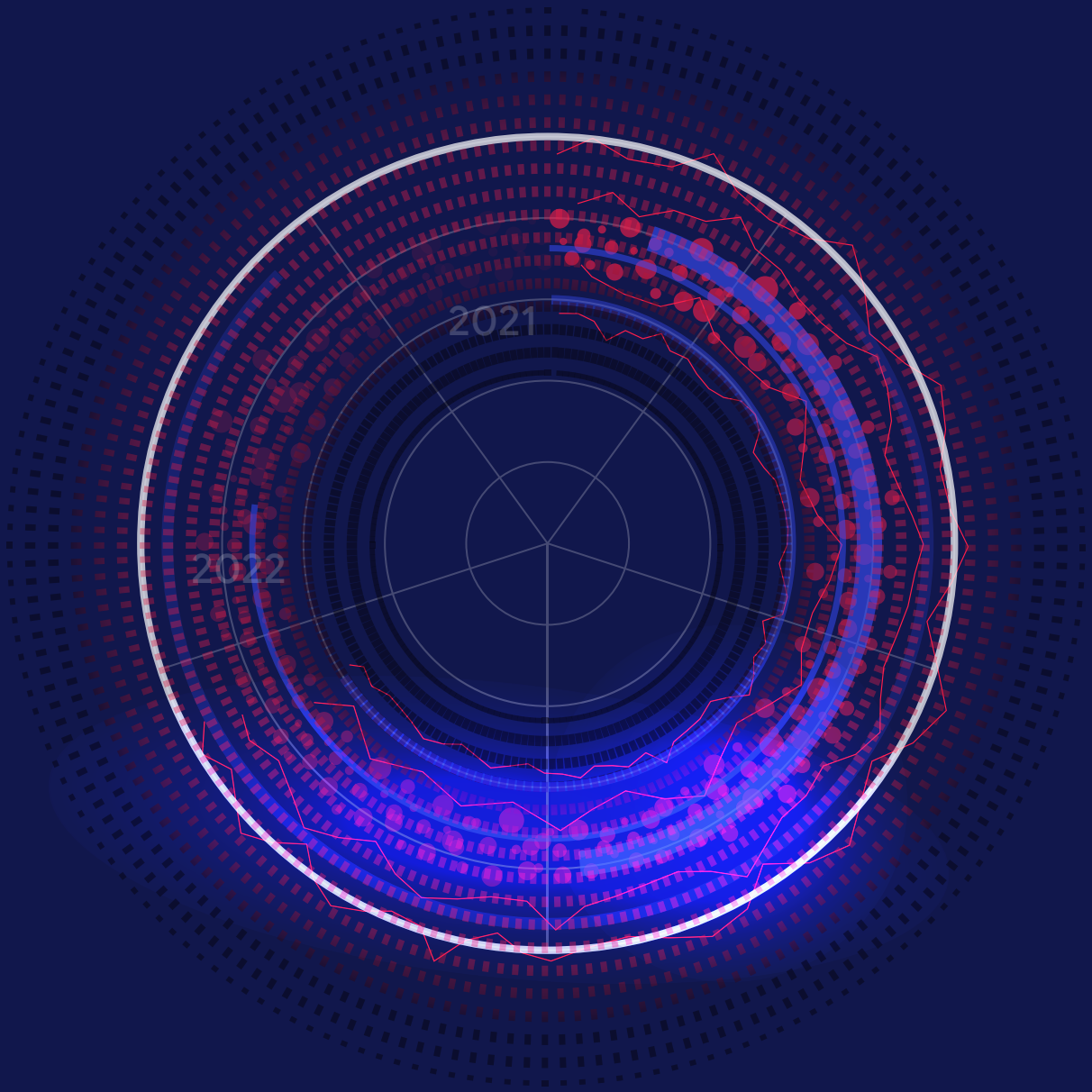
VIRUSTOTAL'S 2021 MALWARE TRENDS REPORT



VIRUSTOTAL

March 2022

Welcome

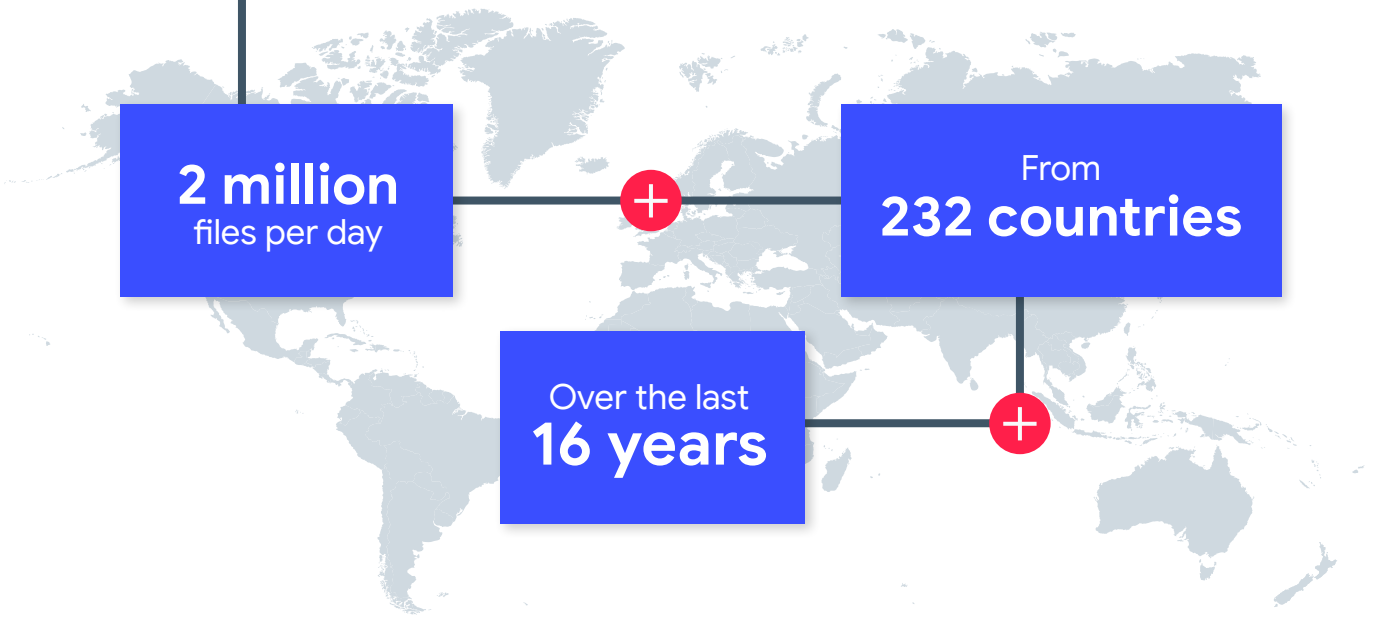
Welcome to "VirusTotal's 2021 Malware Trends Report" research report. We hope that by sharing our visibility into the threat landscape that we can help researchers, security practitioners, and the general public better understand the evolution of malware attacks in 2021.

When facing online threats as complicated as those we face today, defenders naturally struggle to see the whole picture. This partial view makes it difficult to condense and analyze significant and rich data in a single place and creates blind spots for defenders.

VirusTotal is in a unique position to provide a source of comprehensive visibility. Over the last 16 years, we have processed more than 2 million files per day across 232 countries. VirusTotal also harnesses the continuous contribution 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.

This report continues in the direction of what we hope will become an ongoing community effort to discover and share actionable information on malware trends.

Methodology: VirusTotal relies on crowdsourced contributions, providing a valuable picture of how different attacks spread and evolve. All the data in this report is based on a representative subset of submissions from our users. To be clear, the relevance of the raw number of samples observed and detected as malicious varies throughout the course of the year. Small changes in malicious samples driven by variances in contributors, polymorphism, and external crawlers can result in significantly more unique detections.



Executive Summary

Attackers' use of **malware with built-in exploits increased by 27%** in 2021.

The average time it took for the most popular vulnerabilities to be exploited dropped from 93 days in 2020 to **0 days in 2021** because many were being exploited before their public announcement.

There was a more than **37% increase in the number of droppers used** in malware distribution. These increases were accompanied by a **20% increase in infrastructure hosting malware**, often on legitimate domains.

Attackers transitioned from **Microsoft Word DOCX files to Microsoft Excel XLSX files** for malware distribution, largely due to increased usage of Excel malicious spreadsheets with macros.

The overall number of **malicious Android samples decreased**. However, for the first time we found a few Android samples among the most submitted and researched samples of the year. We also observed an 146% increase in the number of samples targeting Linux systems.

Log4j had a very noticeable impact both on attackers and defenders. Even though the log4j vulnerability was not publicly revealed until December, it shot to the top of the list of those vulnerabilities most often abused by attackers in 2021. Four malware samples related to log4j attacks were found in the **top 10 for most looked up samples** during the last quarter of the year.

The number o**f fresh CobaltStrike samples grew by 155%**, mainly during the first quarter of 2021, to be followed by a wave of VirusTotal users looking those samples up for the rest of the year.

Families such as Dridex (1,306% increase in number of samples in 2021 compared to 2020) and Gozi (37% increase) bloomed, while others such as Emotet (66% decrease), Qakbot (76% decrease) and Smokeloader (73% decrease) greatly reduced the number of fresh samples during 2021.

We detected attackers rotating their RATs (Remote Access Trojans) and backdoors of choice. Padodor/Berbew (2,111% increase in number of samples in 2021 compared to 2020) is a clear outlier given its polymorphic nature and its (suspected) code reuse by other malware families. AsyncRAT (+139%) and Flyagent (+118%) increased in popularity among attackers. On the other hand, the presence of Gravity RAT dropped 99% in 2021.

At a Glance

In general, we didn't observe any anomaly in the timeline for new samples received and detected as malicious during 2020 and 2021. If anything, the timeline is generally constant and reaches a plateau by the end of 2021.

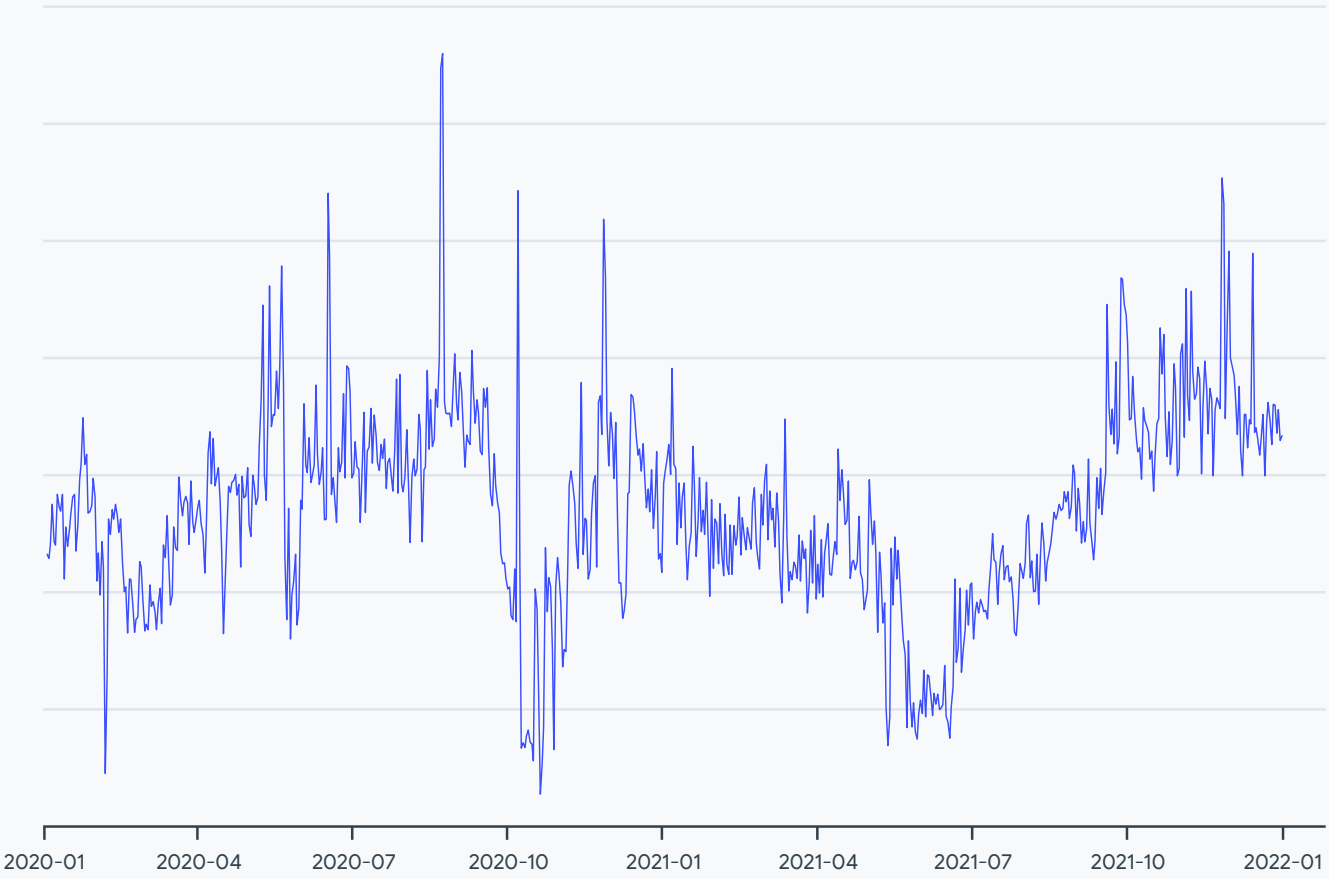


Fig 1.
Malware submission timeline.

The number of potentially malicious samples (detected as such by five or more different antivirus engines) first seen during the year is almost the same between 2020 (45.86%) and in 2021 (46.12%). When checking the percentage of malicious samples generating new malware clusters (by similarity), which can provide clues to researchers as to how new malware samples are different, we also find almost the same ratio (0.43% vs 0.44%).

We saw unexpected differences crop up, however, when we compared samples of malicious files as explained in the section below.

How malware distribution evolved in 2021

In 2021 we observed the following distribution changes (compared to 2020) for file types used by malicious samples:

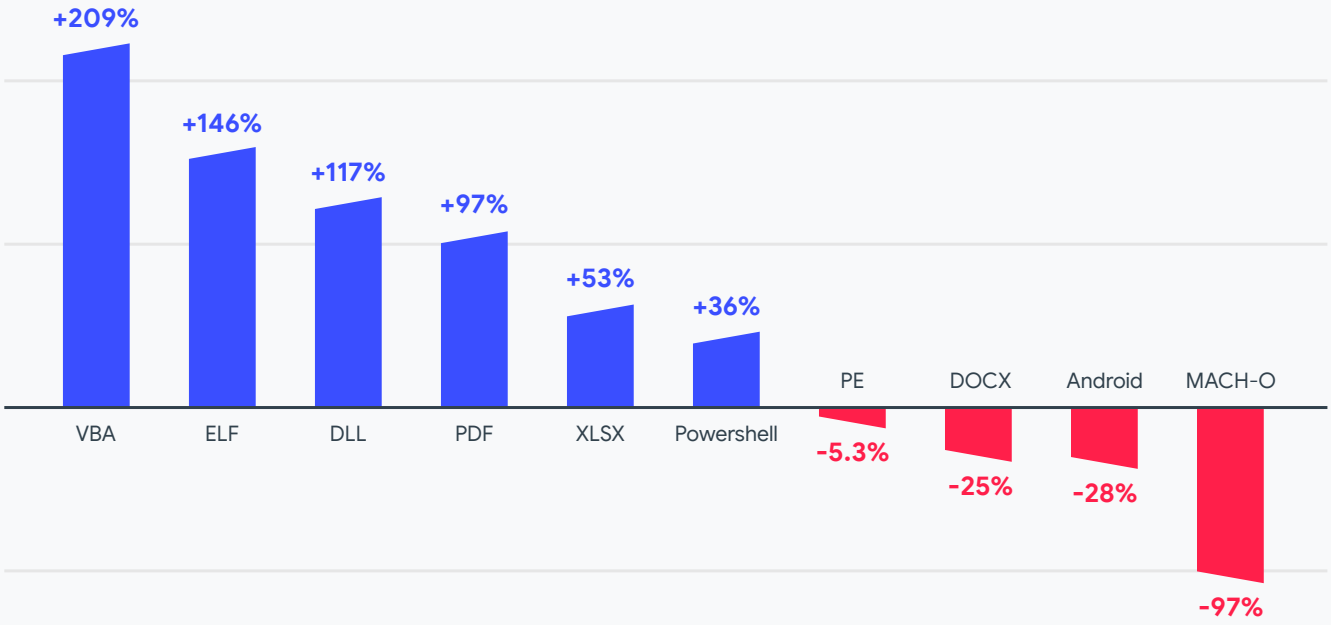


Fig 2.
2021 distribution changes for file types used by malicious samples.

Below we provide some ideas to explain these changes.

Windows executable files represent the vast majority of files considered as malicious in VirusTotal. The percentage decrease of PE files in 2021 is compensated by the combined increase in other formats. In particular, the increase of DLL files might be read as a technicality to replace PEs in some malware families. Interestingly, the percentage of PE samples implementing any kind of exploit increased by 131%.

We also found a dramatic decrease (97%) in the number of macOS-based MACH-O malicious files. In this case, the explanation can be found in the peak of ransomware "polymorphic" samples belonging to the EvilQuest family distributed aggressively for macOS in mid-2020 and described in our 2021 report "Ransomware in a global context". EvilQuest is no longer active and there was no similar campaign in 2021, which explains the decrease in the number of samples, but naturally there were new malware families for macOS such as Macma, Xloader, and XcodeSpy.

Threat actors in 2021 changed from deploying malicious DOCX files to malicious XLSX files. Both are some of the most common formats for malware distributed as attachment. Many different campaigns in 2021 such as Emotet, Qakbot, Dridex, Zloader, and Trickbot relied on malicious XLSX files to infect their victims. However, the number of files implementing exploits in 2021 for both formats increased only for DOCX, which seems counterintuitive.

We couldn't find any technical reason for the transition, although we can speculate that attackers might have decided to abuse formats victims are less used to seeing in social engineering attacks. Finally, the increase in VBA files corresponds to the high use of both formats for malware distribution embedding malicious macros.

ELF files implementing exploits increased 135%

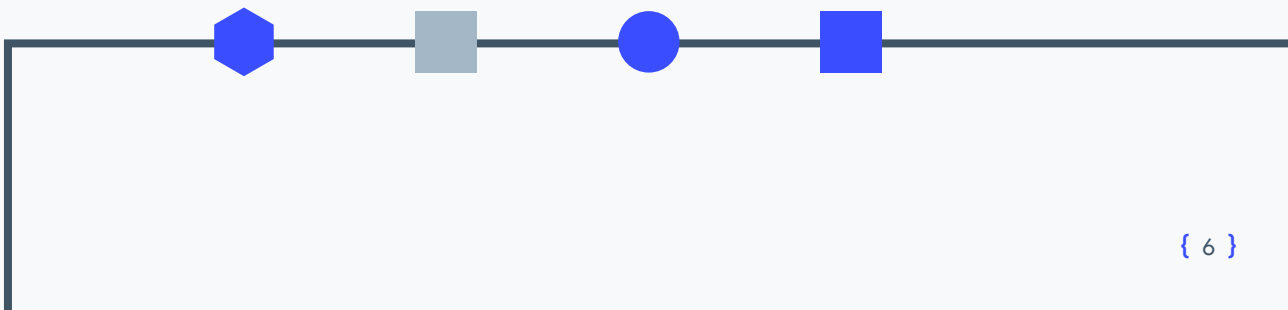
The big increment in ELF malware seems to be mainly related to Mirai, Tsunami and different coin miners. Notably, the number of ELF files implementing exploits increased 135% in 2021, including the exploitation of the Log4j vulnerability CVE-2021-44228.

The 97% increase of PDF files seems to be mainly related to phishing attacks, often hosted in URLs in-the-wild. On the other hand, we detected a decrease of 63% in the number of PDF files implementing exploitation techniques.

Although there is a decrease in the percentage of Android malicious samples found in 2021, there are two Android samples in the top 10 most submitted malware of 2021, as well as an Android sample (in this case, a banker) in the top 10 most searched malware in VirusTotal during the last quarter of 2021. We detected a moderate increase (12%) in the percentage of Android malware implementing some kind of exploit.

282% increase in the number of PowerShell files implementing exploits

The use of scripting languages for malware distribution is nothing new, but it seems to keep gaining traction. Malicious PowerShell files are popular for this purpose, and in addition to an increase in the adoption by attackers of this format, we observed a whopping 282% increase in the number of PowerShell files implementing exploits. This can be circumstantial depending on the ease to exploit some vulnerabilities with this format. In 2021 alone, we found PowerShell scripts exploiting at least 9 different CVEs.



Most submitted samples in 2021

The list of most submitted malware for the year consists of, not surprisingly, widespread samples such as Adware and PUAs with half of them sharing similarity clusters and infrastructure. An extended list also includes generic trojans and samples both for Windows and Android.

When checking the most looked up samples in VirusTotal during the last quarter of 2021, we find all kinds of riskware. When excluding them (as well as coin miners - also for Linux), we get a much more interesting top 10:

Top looked up samples
Ransomware.Blackmatter
Trojan Danabot
Ransom:MSIL/Khonsari.A
Win64/Exploit.CVE-2021-40449.A
Ransom.Win32.Sabsik
Linux/Mirai
Mirai.Linux
Android.Banker, Bankbot
Danabot, Upatre
Linux/Mirai

Not surprisingly, several of the top positions are filled with ransomware. The exploit for CVE-2021-40449 (Elevation of Privilege Vulnerability in win32k) does not appear in our list of top exploits for 2021 in terms of samples abusing it. However, it seems this particular sample was very widespread among victims.

Danabot is also present in two positions of the top 10, as well as Mirai - in this case, this might be a reflection of the increase on ELF malware we already discussed. Finally, we see Android makes it to this list with a Banker.

Malware Distribution

While we observed no significant difference in the level of phishing artifacts detected in VirusTotal between 2020 and 2021, other distribution mechanisms such as the use of exploits or distribution through URLs greatly varied. In terms of malware droppers, we observed a 37% increase in the number of samples.

Usage of Exploits

57 0-day exploits were found being used in the wild in 2021 - that's a new all time record, and almost twice as much as the year before. These exploits covered a wide range of software, starting with usual targets such as popular browsers but also server-side software such as Microsoft Exchange and devices such as SonicWall Email Security appliances.

During 2021 we observed a 24% jump in the number of samples exploiting vulnerabilities as compared to 2020. Adding exploit kits to this set of samples bumped the increase to 30%.

The following chart shows the distribution of samples implementing any kind of exploit in 2021.

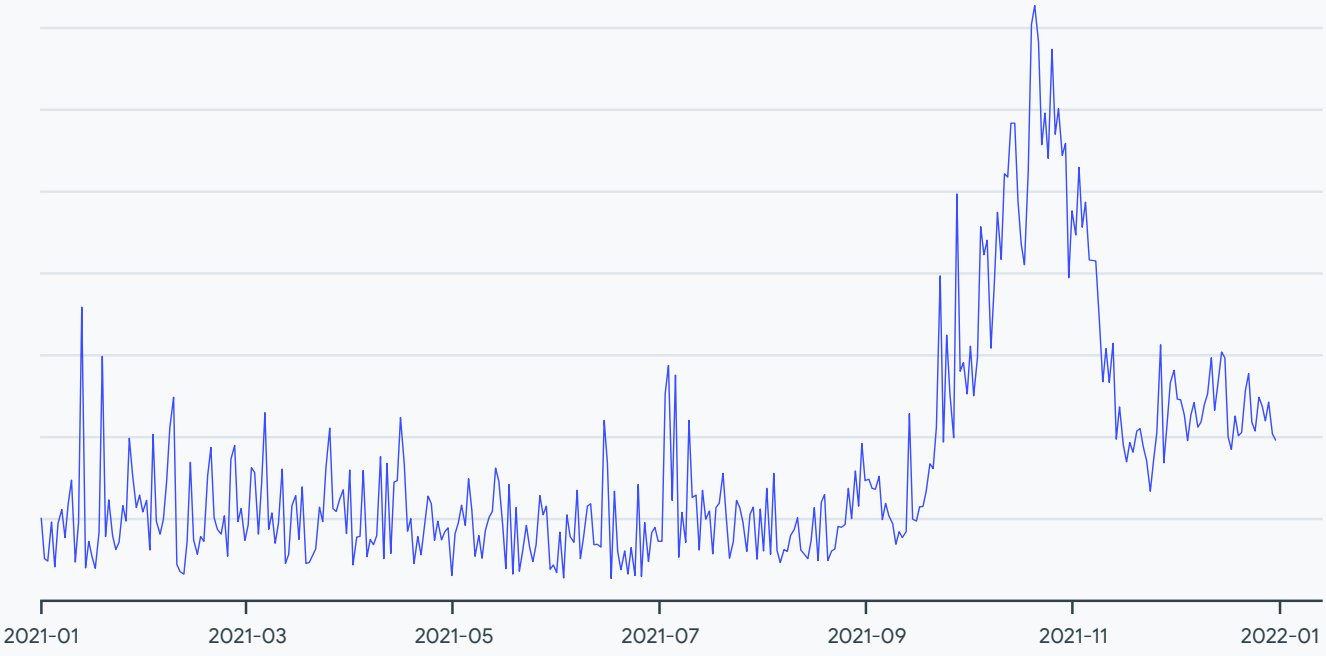


Fig 3.
Malware implementing exploits timeline.

There are still a huge number of samples weaponized to abuse vulnerabilities more than 5 years old, which is a gentle reminder as to why we should keep systems up-to-date. We decided to focus on how quickly attackers adopted new vulnerabilities. The following chart shows the timeline for samples first seen in 2021 that exploit vulnerabilities published in 2020 or 2021.

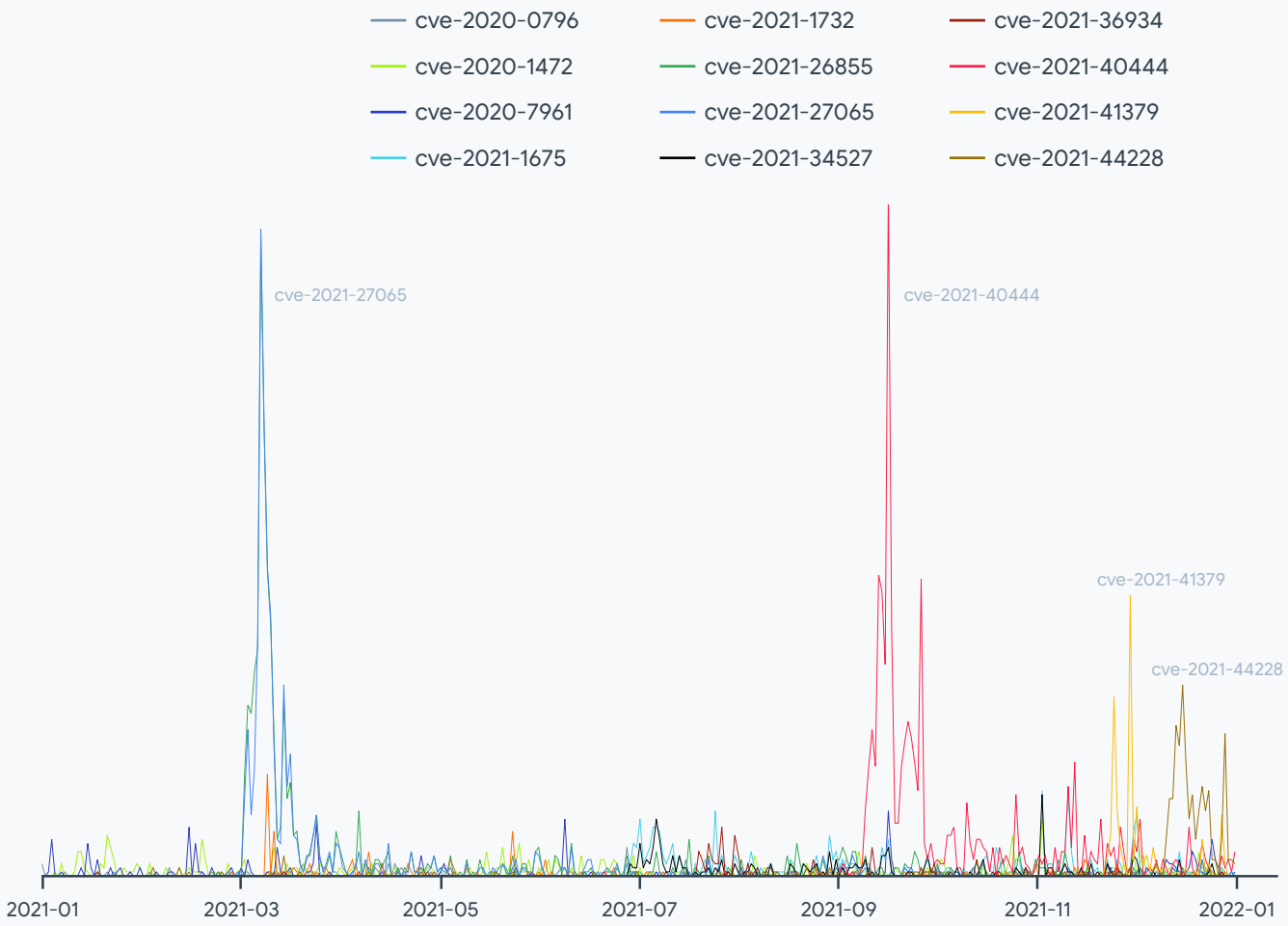


Fig 4.
Timeline for malware exploiting 2020 and 2021 vulnerabilities.

There are several interesting points to consider. First, peaks occur when vulnerabilities gain traction for malware distribution. This often happens shortly after a write-up or a Proof-of-Concept is uploaded to a public repository. After the peak, attackers decide whether the exploit becomes part of their toolset and stays, or if it simply is not useful anymore. We can also see some overlap between exploits where attackers decide to use them together, either because they need two vulnerabilities for the exploitation or simply to make samples more likely to infect the victim.

We found an interesting peak in March where CVE-2021-26855 and CVE-2021-27065, both targeting Microsoft Exchange Server, were part of an attack chain and distributed together. There is another smaller peak for CVE-2021-1732 at the time when the researcher uploaded a PoC to GitHub. We found a peak in September for CVE-2021-40444 (remote code execution in MSHTML). The peak in November seems to be related to CVE-2021-41379 (Windows Installer escalation of privileges) and in December (surprise) we have Log4j CVE-2021-44228.

How are these vulnerabilities being exploited?

CVE-2021-40444 had 3-4 weeks peak, and was mainly implemented by malicious documents detected as Donoff/Wacatac/Cryxos. Afterwards, the number of samples slowly decays.

Log4j's CVE-2021-44228 was one of the most impactful public vulnerabilities in 2021. The timeline below shows detections all year along, but this is because there are plenty of false positives detecting Apache Log4j source code itself as the exploit.

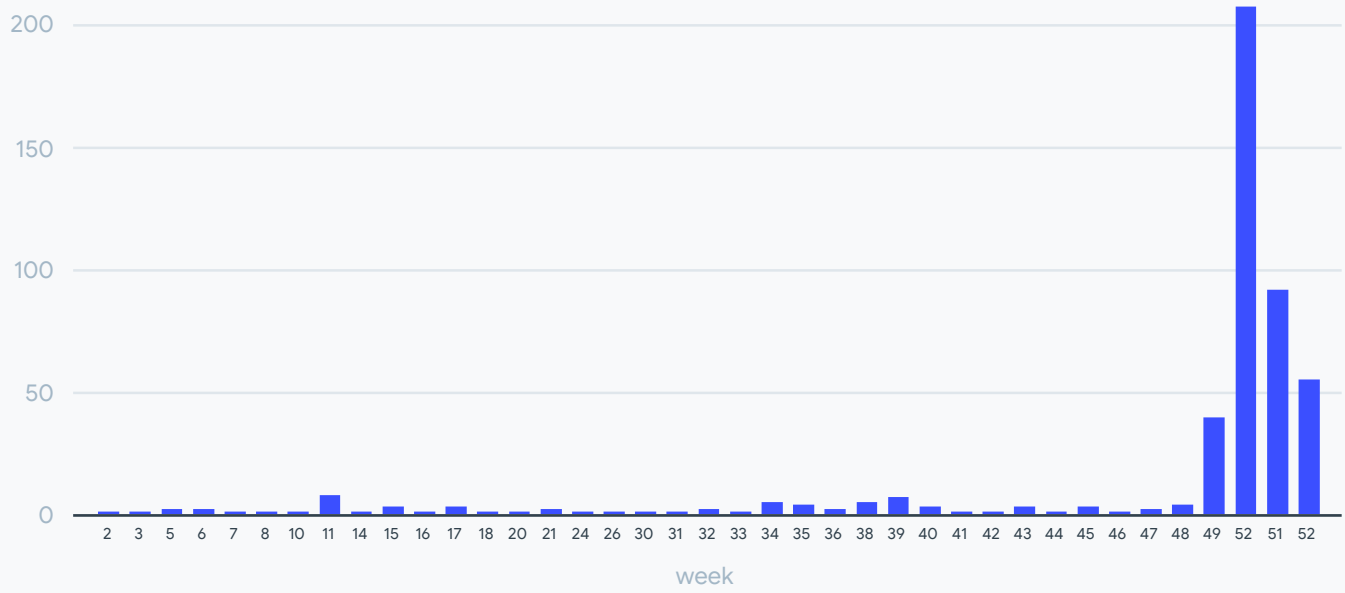


Fig 5.
Samples exploiting Log4j CVE-2021-44228.

The peak in week 11 (March 2021) corresponds to Tsunami samples used as payloads by Mirai in Log4j attacks and wrongly detected as exploiting the vulnerability. Other than that, Mirai and several coin miners seem to have been heavy adopters of this exploit.

Pattern analysis indicates that attackers are increasing the speed at which exploits are being adopted. The following chart shows this time difference (in days) for the most exploited vulnerabilities found in 2020 and 2021 in VirusTotal:

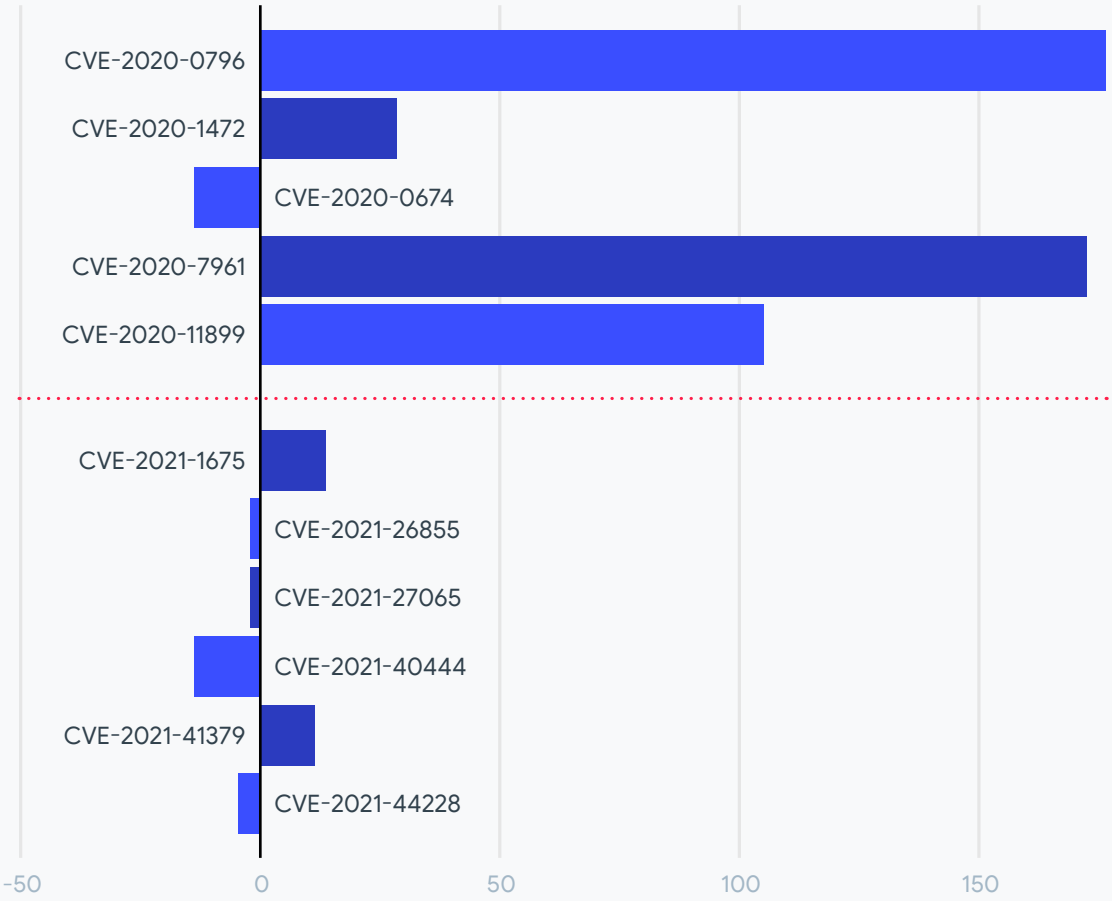


Fig 6.
Days from release until exploitation for most exploited 2020/21 vulnerabilities.

We found multiple instances of attackers exploiting vulnerabilities in the wild before details were made public, which we think of as negative days (as relative to 0-days, when the vulnerability is first revealed to the public.) When averaged with vulnerabilities which we found were exploited after a public announcement, or positive days, the number of days since a vulnerability was published until we found samples exploiting it plummeted between 2020 and 2021. In 2020, it took an average of 93 days for the most exploited, published vulnerabilities to be used in a cyberattack. In 2021, it took an average of 0 days for the most exploited, published vulnerabilities to be used in a cyberattack, because so many of them were being exploited before their public announcement.

The selection of vulnerabilities in the previous chart is based on their popularity in numbers of samples exploiting them found in VirusTotal. Publication date for vulnerabilities is provided by CVEdetails,it is possible that some vulnerabilities get officially published after being discovered in the wild.

Malware distribution in the wild

Compared to 2020, we observed a very slight increase in the number of malware samples being distributed in the wild (ITW). However, the number of URLs where ITW malware was found increased by 20%. This means that malware samples that were distributed using this method were more widely spread, and the generation of unique URLs for their distribution became more common. Factors that contributed to this increase include the usage of legitimate cloud storage and file-sharing services.

The chart below shows the top ten URLs used for malware distribution during 2021.

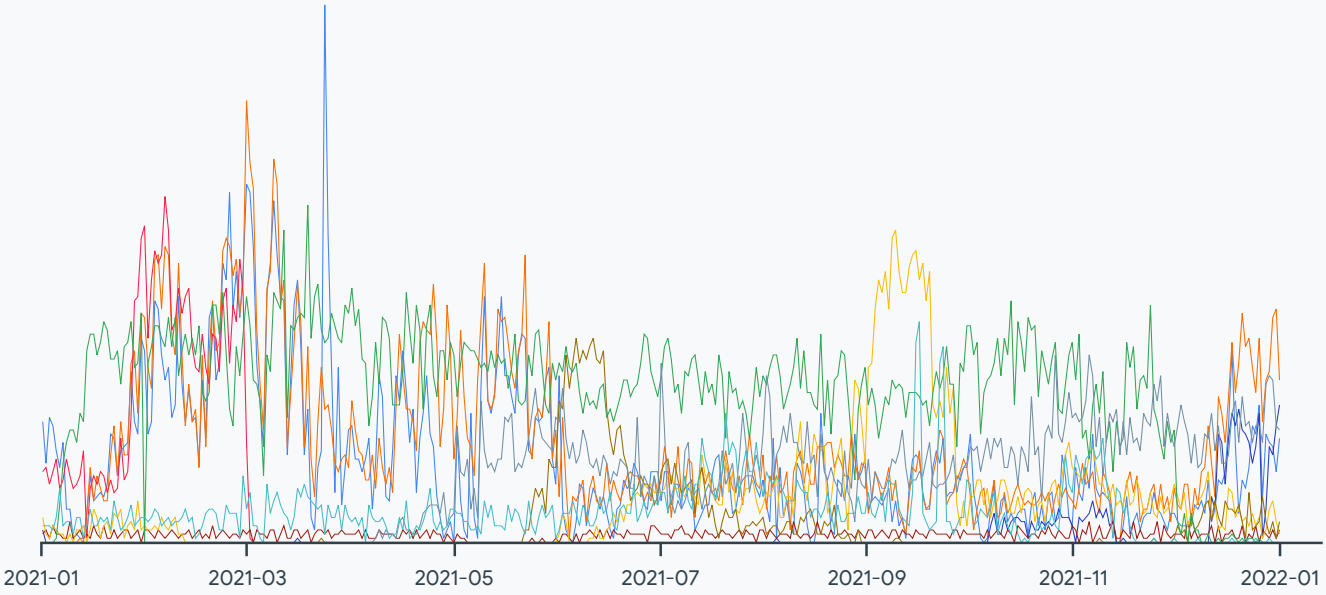


Fig 7.
Top 10 URLs distributing malware in 2021.

Notably, some of them were consistently distributed during the year while others go up and down depending on how they are used in different campaigns. If we isolate domains used for malware distribution, it looks as follows:

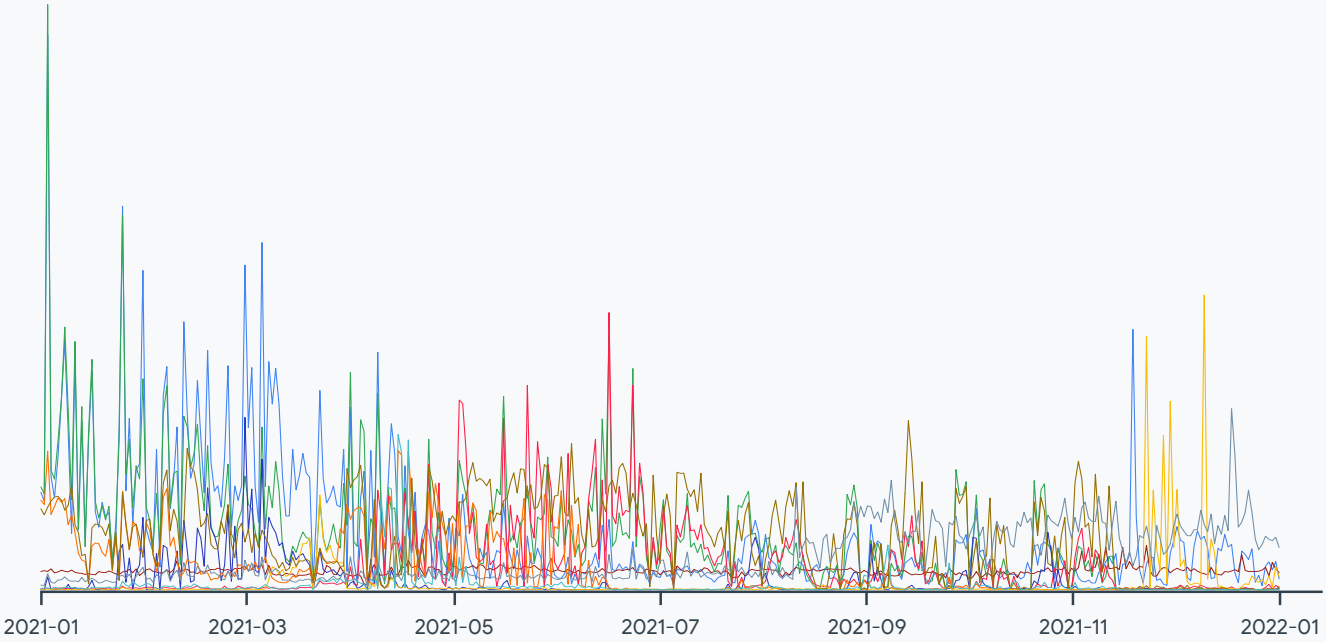


Fig 8.
Top 10 domains distributing malware in 2021.

Here, the usage of domains look a bit more distributed in different campaigns for a certain period of time. The biggest campaigns for the first half of 2021 correspond to malware (mostly PDFs used in phishing attacks) distributed through legitimate domains such as Amazonaws. However, in the second half of the year, distribution through both domains is almost non-existent. Another top 10 domain used for malware distribution is discordapp, which seems to have been gaining popularity during the last months.

There are several families that used hundreds of ITW URLs for distribution during 2021, including Mirai, Azorult, and Glupteba. Phishing attacks also greatly abused this kind of distribution vector.

Malware Trends

Footholding and Lateral movement

There are a number of artifacts potentially used by attackers for lateral movement, many of which are not necessarily malicious. It is common to use the same toolset that pentesters and system administrators do. There are also several malware families from the following section (RATs) that implement the capabilities needed in the first stages of an attack. Having said that, in this section we want to provide insights into how several tools traditionally used by attackers in the first stages of all kinds of attacks evolved during the year according to our visibility.

CobaltStrike

This is one of the favorite tools used both by pentesters and attackers. We observed an increase of 155% of fresh samples seen in 2021 for this artifact, with submissions peaking during the first quarter of the year.

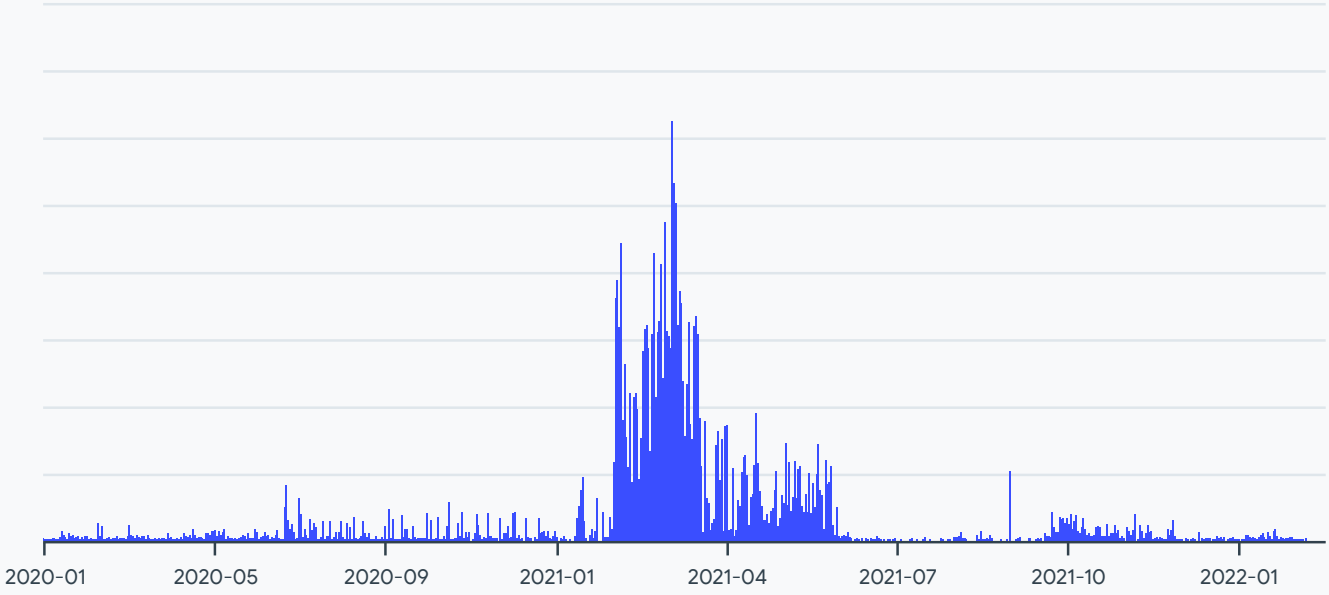


Fig 9.
CobaltStrike submission timeline.

Despite the new samples being first seen during that first Q, the interest from VirusTotal users searching for them in our platform is quite constant during the year, reflecting how these freshly created samples were later reused in different attacks.

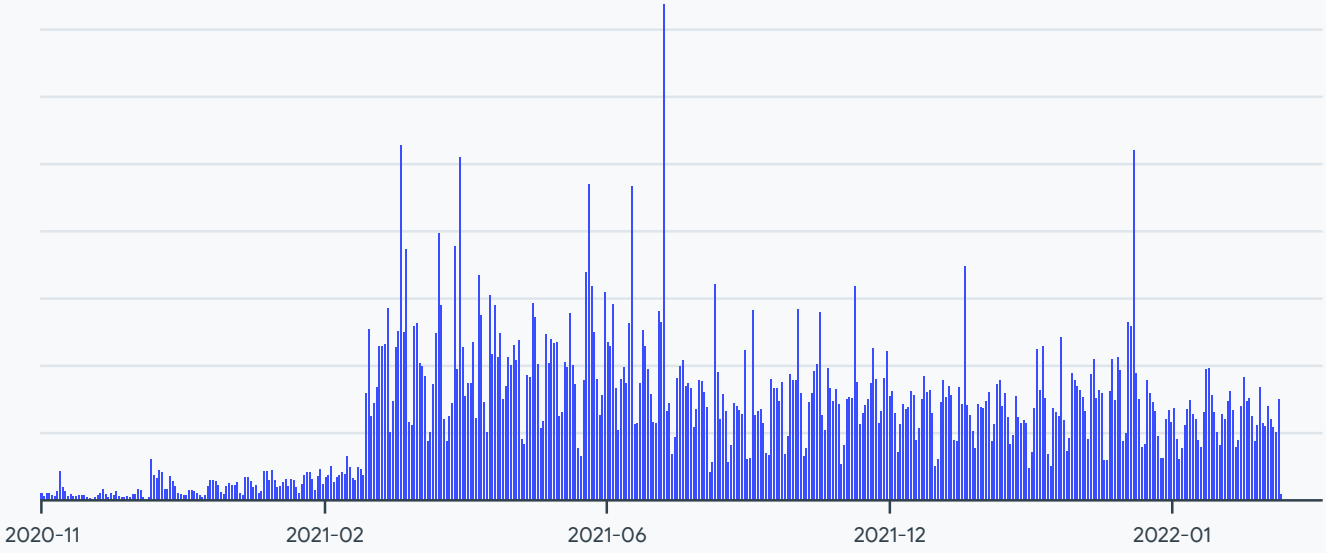


Fig 10.
CobaltStrike lookup timeline.

Meterpreter

Similar to CobaltStrike, this is one of the most popular choices by pentesters and attackers, enabling similar functionalities. During 2021, the number of first seen samples was 23% lower than in the previous year. However, the number of submissions is incredibly constant during the last two years. We can observe a peak in the number of lookups in February-March 2021.

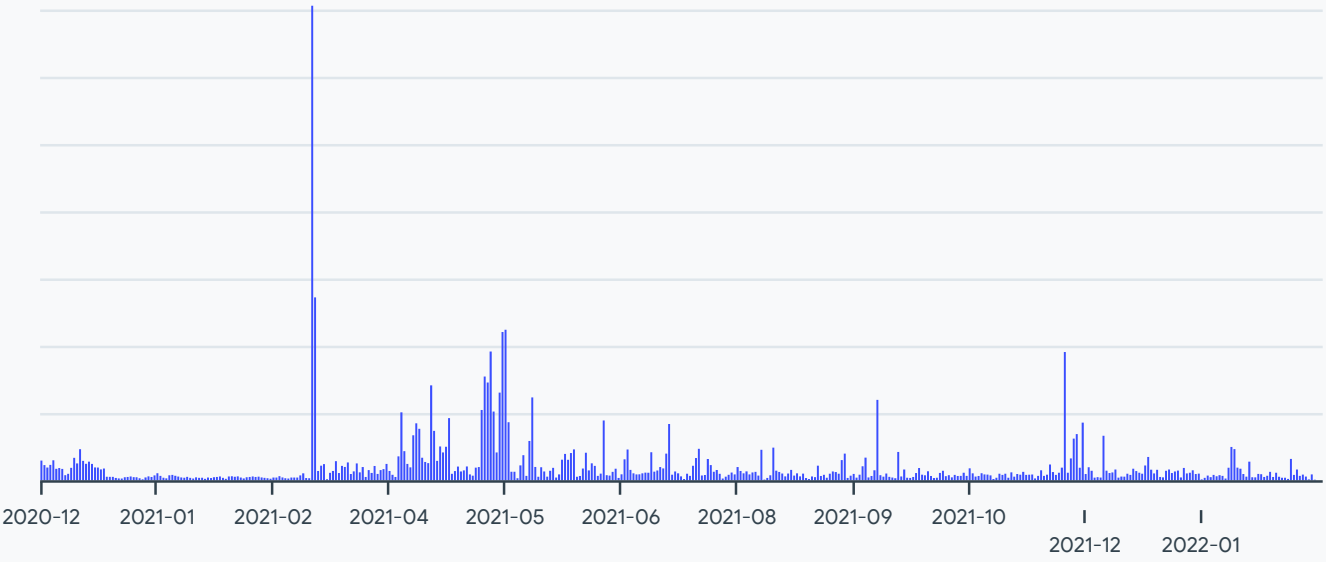


Fig 11.
Meterpreter lookup timeline.

Mimikatz

Although there is a 75.5% decrease in the number of fresh samples seen in 2021, in this case the freshness of the sample is probably not as significant as it could be for other malware families. Despite that, we observe the biggest historical peaks of submissions for this artifact between August and October 2021:

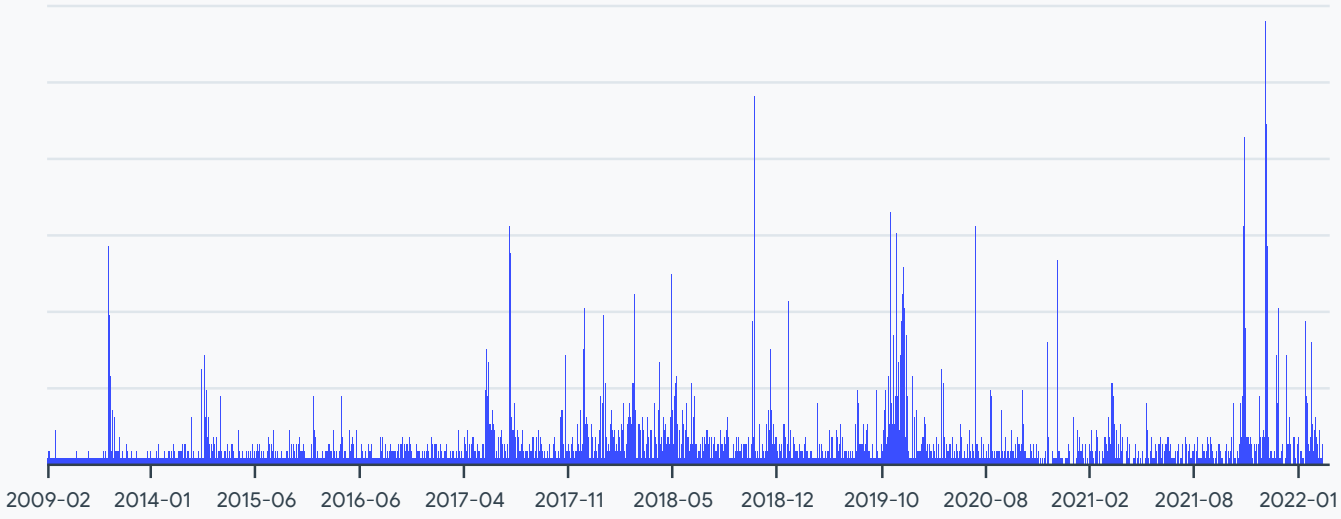


Fig 12. **Mimikatz submission timeline.**

We also can see a record number of lookups by VirusTotal users around March-April of 2021:

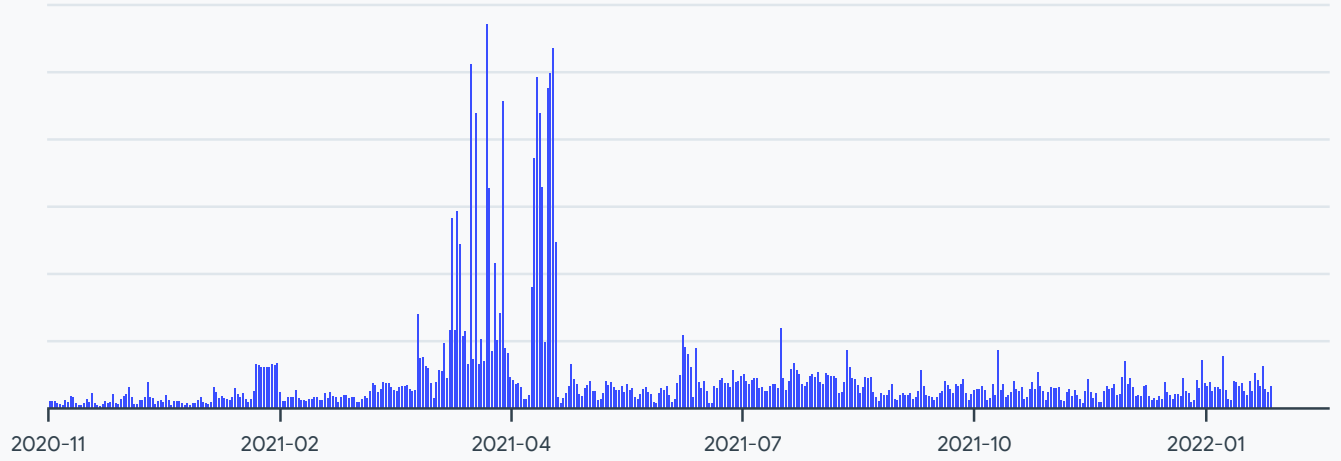
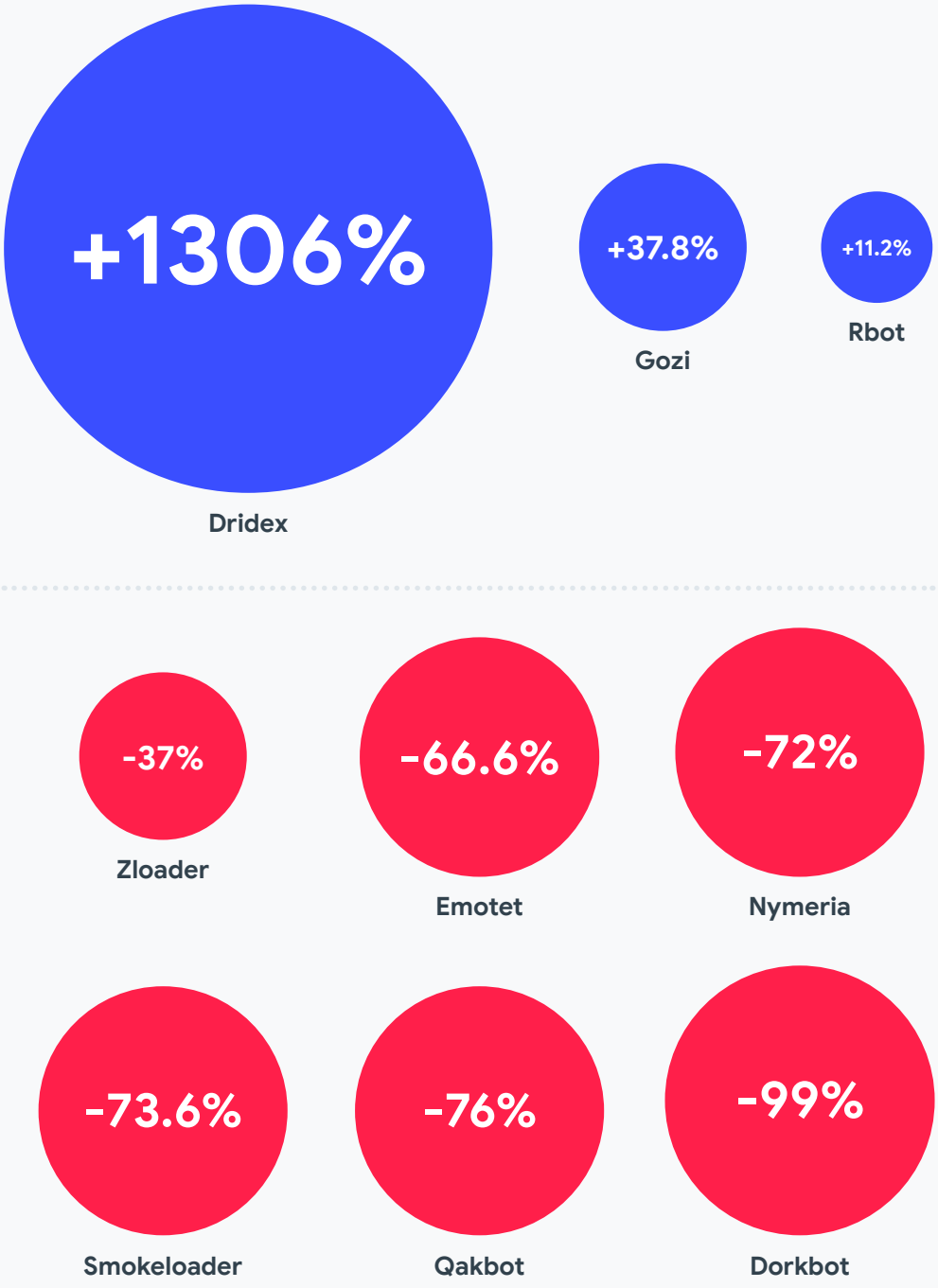


Fig 13. **Mimikatz lookup timeline.**

In addition we looked at some of the most traditional bots. In reality, this kind of malware should be considered as multi-purpose as it is still an excellent option for many attacks that leverage the existing victim base and the basic capabilities as the first stage for more sophisticated attacks. The evolution for some of the most well-known bots during 2021 is as follows:



Given the incredible increase in 2021, we did a more detailed analysis of Dridex.

Dridex

We observed a huge number of fresh Dridex samples during 2021 as well as submissions, where we registered two historical peaks of submissions for this kind of malware during the year despite being a veteran malware family.

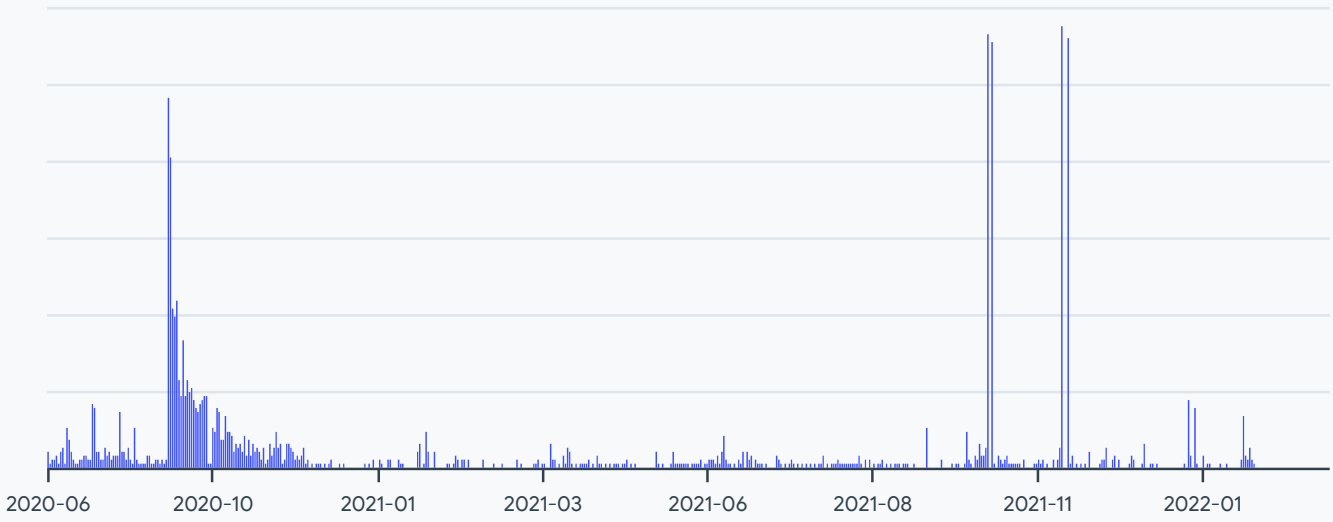


Fig 14. **Dridex submission timeline.**

The spike in the number of lookups by VirusTotal users reflects their interest in these samples, most likely motivated by their wide distribution.

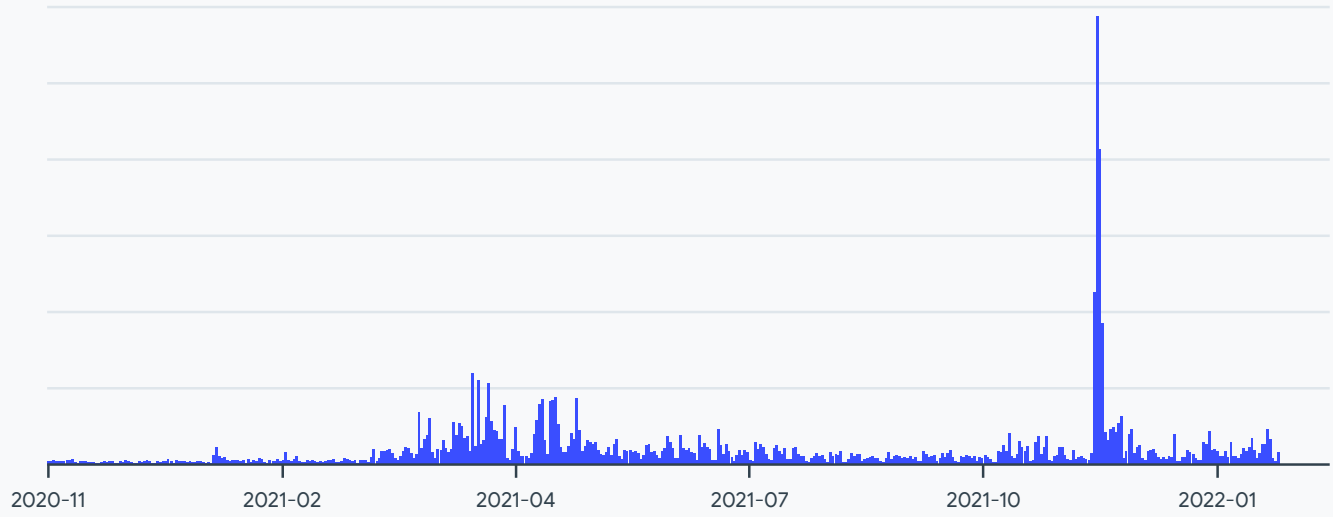


Fig 15. **Dridex lookup timeline.**

Several public sources discussed Dridex campaigns spreading through Excel documents during 2021.

Remote Access Trojans (RATs) and Backdoors

RATs are one of the most used malicious tools by attackers for all kinds of operations, especially in the first stages of an attack – regardless of the attack's sophistication. They are part of every attacker's toolbox, and for the last few years attackers have chosen widely available RATs over in-house development except in very specific cases (mostly by APT actors). RATs allow attackers to perform reconnaissance, deploy other malicious tools as needed, and avoid attribution. That's why it is important to keep an eye on what RATs and backdoors are the most commonly chosen by attackers for their operations.

The choice of RATs for attacks changed quite a bit during the year according to the number of samples found in VirusTotal. Here is the ranking of families that dramatically increased their presence in 2021:

Families	% increase
PADODOR/BERBEW	+2,111%
ASYNCRAT	+139%
FLYAGENT	+118%
ORCUSRAT	+102%
NOANCOOE	+102%

There is a large number of samples (including polymorphic families) that trigger Padodor/Berbew detections as they share some execution characteristics, including the use of the same Mutex. Speculatively, this could be explained by some code reuse, or maybe these families are designed to trigger this detection on purpose.

We also observed a growth in Crowdsourced Yara rules detecting AsyncRAT, which is the second fastest growing family. Flyagent made it to the top three and is one of the most significant families by total number of samples at the time of writing this report.

In addition, Yara rules detecting DCRat, SystemBC, and Blackshades RAT malware were among the ones showing most significant growth in 2021.

On the other hand, the following list shows families whose usage decreased last year – in some cases having almost no new fresh samples in 2021:

Families	% decrease
GRAVITYRAT	-99%
SHIZ	-93%
NETWIREDRC	-82%
REMCOSRAT	-82%
XTREMERAT	-74%

Despite having a usage decrease, Bladabindi and Darkcomet still are in the top five by total number of samples first seen by VirusTotal in 2021. The top five RAT families in absolute numbers first seen in VirusTotal in the last two years is as follows:

Top 5 RAT Families
PADODOR/BERBEW
BLADABINDI
SHIZ
REMCOSRAT
DARKCOMET

Crowdsourced data

In this section, we checked samples belonging to different Crowdsourced Yara rules and VirusTotal Collections in order to understand which ones had relevant changes during the year.

In terms of fast-growing Yara rules, other than the ones described in the previous section (DCRat, AsyncRAT, SystemBC and Blackshades RAT), there are several generic ones based on detecting invalid certificates or packers. Additionally, we also found several fast-growing Collections tracking different RATs, such as SystemBC, Sakula RAT or buteRAT. One of the rules with a bigger growth during the year detects a tool used for large scale DDoS attacks.

During the first half of the year we also observed remarkable growth of rules detecting CobaltStrike and BazarLoader. For the second half, the fastest growing rules detect Quantum Locker, Ryuk, Moonwind and FatDuke. We also saw Collections for Moonwind and Ryuk growing at a similar rate for the same period of time.

Final thoughts

Analyzing two years worth of threat intelligence data can be overwhelming to digest. Our main goal is to apply VirusTotal's unique visibility to share useful data points. Below are the main report takeaways and what they mean:

Attackers are faster in adopting exploits for new vulnerabilities. This includes the exploitation of 0-days as well as adoption of published ones.

There is an increase of malware distribution through droppers as well as an increase in the infrastructure used for malware hosting, often using legitimate domains.

The total number of samples for Android decreased but, at the same time, some specific samples were among the most searched by VirusTotal users. The number of malicious ELF files increased.

Some malware families (like Dridex, Gozi or AsyncRAT) skyrocketed in 2021, while the usage of others (like Emotet or Quakbot) severely decreased.

Log4j vulnerability had a noticeable impact translated into different malware families adopting it and security practitioners monitoring its evolution. This tells us about the relevance of such vulnerabilities in the security ecosystem.

Based on all the above, here are some considerations for including this insight in an effective security strategy:

Vulnerability patching is critical. Consider using environments that provide effective and agile patching strategies.

Monitoring the usage and spreading of malware families is crucial to prioritize effective defenses.

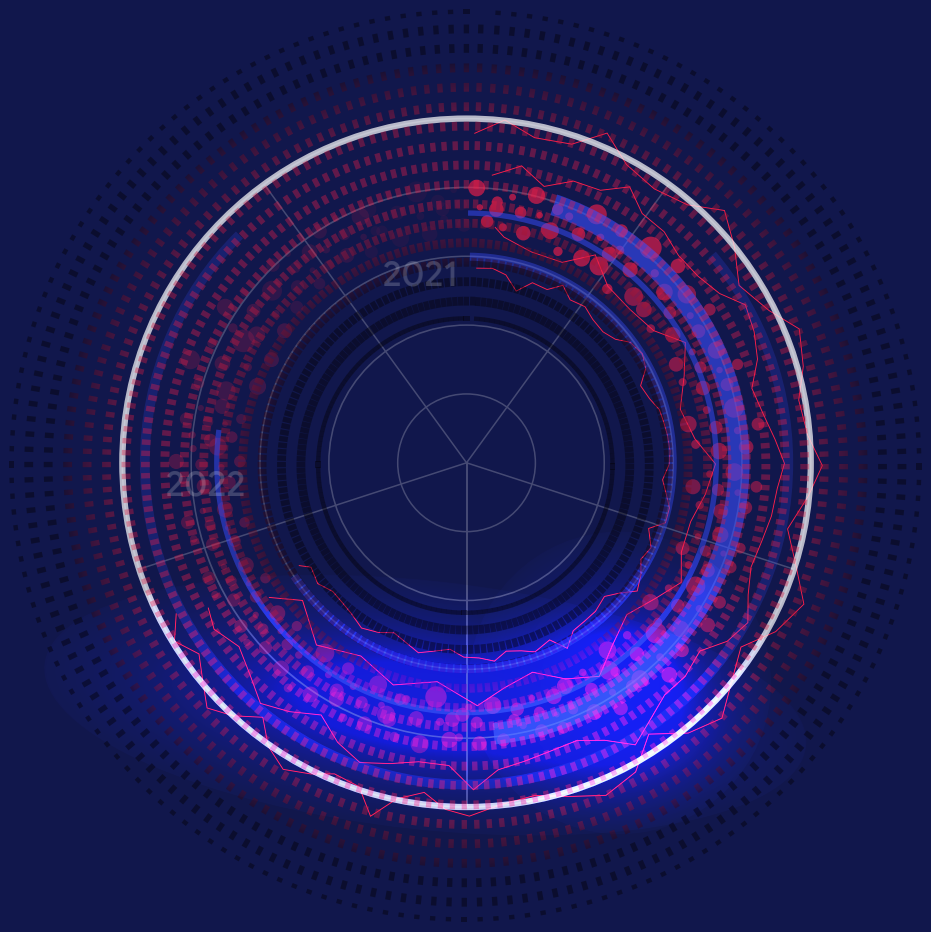
Transformative security events, such as the Log4j vulnerability (CVE-2021-44228), quickly change the security ecosystem. Effective monitoring and remediation is critical.

Do not underestimate the presence of well-known malware families (such as Dridex) in your systems, as they can be first stagers for serious attacks.

Educate your staff against phishing and social engineering, no matter the format of the attachment, the domain hosting the file, or the channel used for distribution.

We hope this data is a first step to an open, healthy discussion that can help researchers understand how to better protect against these threats. We trust the information shared in this report will prove useful - and that it will keep our world a little bit safer.

Join the discussion @virustotal



VIRUSTOTAL

Find out more at: virustotal.com