# DECEPTION AT SCALE: HOW MALWARE ABUSES TRUST

VIRUSTOTAL

JUNE 22

# Welcome

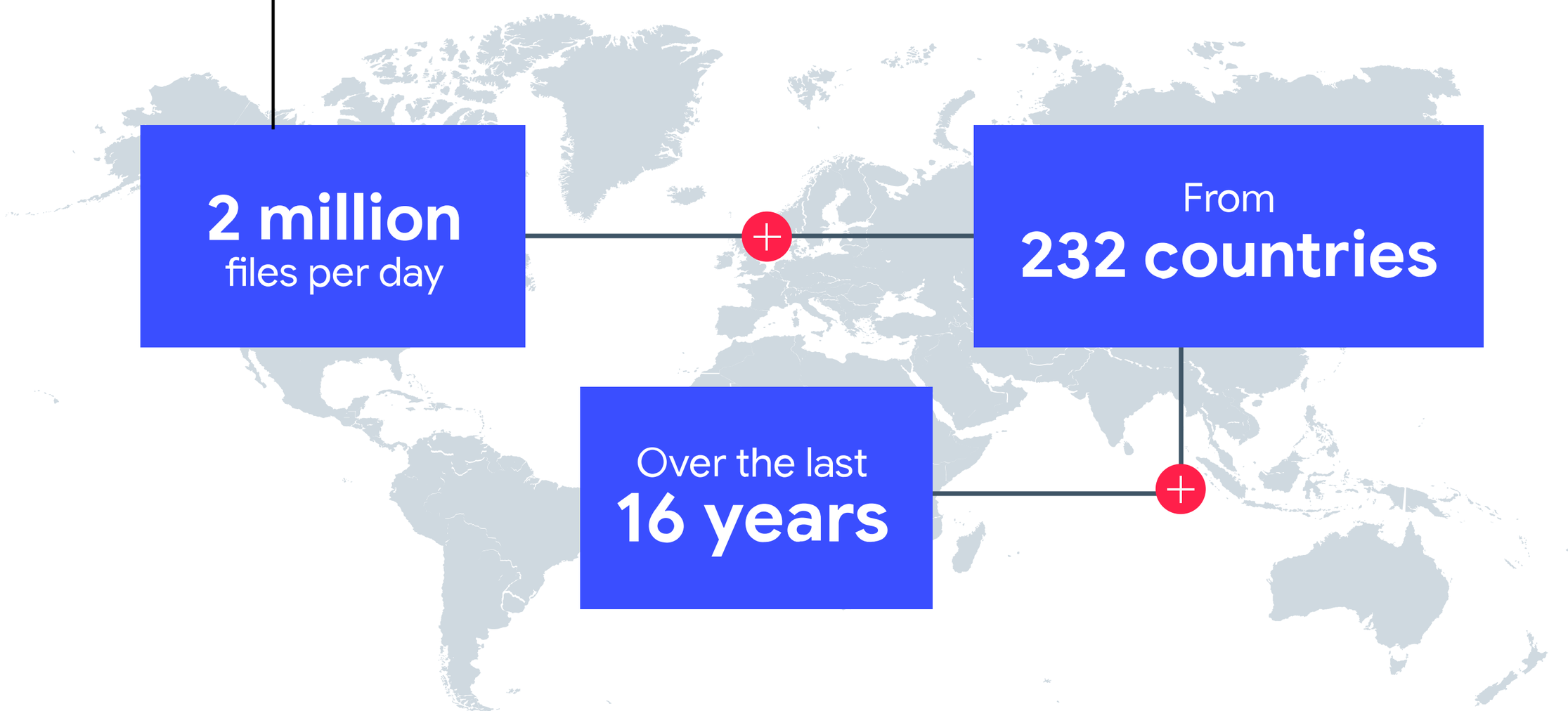
Welcome to the VirusTotal **“Deception at scale: How malware abuses trust”** research report. We hope that by sharing our visibility into the threat landscape we can help researchers, security practitioners, and the public  better understand the evolution of malware attacks.

This report explores different abuse-of-trust approaches used by attackers to spread their malware, avoid defenses, or maximize the success of social engineering attacks. We decided to study this approach following the wave of supply chain attacks witnessed during the last few years. These attacks can be seen as an abuse-of-trust as malware authors often rely on the implicit trust that exists between a reputable software supplier and the user.

We identified different ways attackers use to abuse this implicit trust, including mimicking legitimate applications, using legitimate distribution channels for their malware, and signing their samples. Our goal is to explore the magnitude and evolution for some of these techniques.

VirusTotal is in a unique position to provide a source of comprehensive visibility of the malware landscape. Over the last 16 years, we have processed more than two 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.



# Executive Summary

- **10% of the top 1,000 Alexa domains** have distributed suspicious samples.
- **0.1 % of legitimate hosts** for popular apps have distributed malware.
- Since 2021, we found more than **1 million signed malicious samples, 87%** of them having a valid signature when uploaded to VirusTotal.
- In a growing social engineering trend, **4,000 samples** either executed or were packed with legitimate apps installers.
- There has been a **continuous increase in the number of malware** visually mimicking legitimate applications, with Skype, Adobe Acrobat, and VLC comprising the top three.
- Similarly, WhatsApp, Instagram and Amazon are the **top three most mimicked websites** by using similar favicon.
- **98 % of samples** including legitimate installers in their PE resources, were malicious.

# Methodology

**VirusTotal** relies on crowdsourced contributions, which provide 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 year. Small changes in malicious samples driven by variances in contributors, polymorphism, and external crawlers can result in significantly more unique detections.

# Abuse of trust

We explored some common techniques used by attackers to bypass defenses and make social engineering attacks more effective.

## Distribution through legitimate domains

This is a common technique by which attackers use legitimate domains for malware distribution. It provides different advantages, such as avoiding traditional perimeter defenses and alerts (like domain/IP-based firewalls); avoiding using dedicated infrastructure which can be taken-down or attributed to a particular actor; abusing well-resourced, highly-available hosts for their malware; and to some extent, looking less suspicious for their final victim.

We found around 2 ½ million suspicious files (detected as malicious by at least five different antivirus) downloaded from legit (top 1,000 domains in Alexa) domains. This includes domains regularly used for file distribution and others that could be abused in different ways. We found 101 domains distributing suspicious files which represents 10% of these top 1K Alexa domains.

Using samples received in 2022, we counted the number of legitimate domains involved in malware distribution:

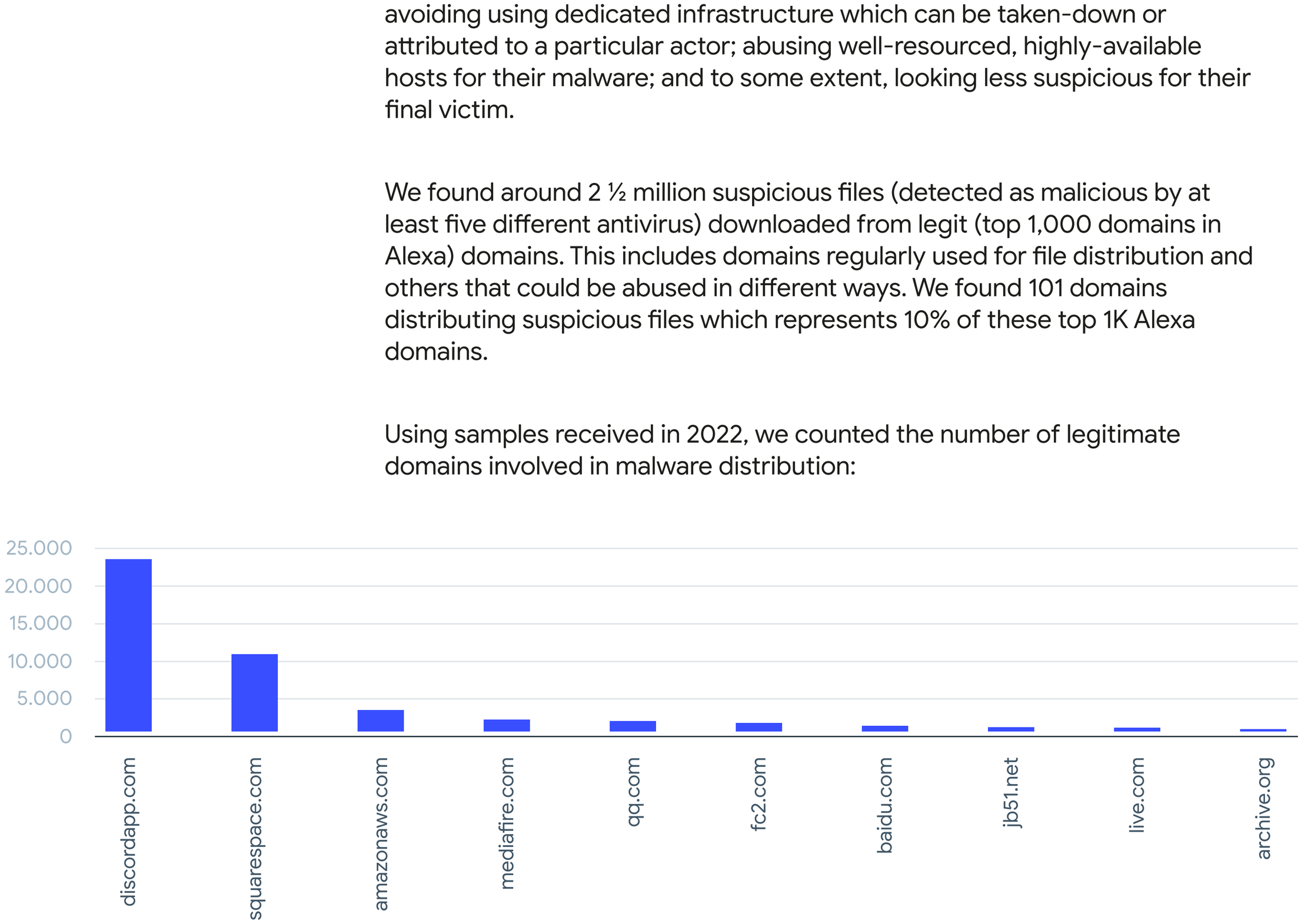



Fig 1.

**Top legitimate domains abused for malware distribution in 2022**

These suspicious samples are not widely distributed across many different, legitimate domains. At most, we observed samples use six legitimate domains for distribution.

# Valid certificates

Samples signed with legitimate certificates were, for a long time, considered safe to use by the operating system and some security solutions. Unfortunately, attackers abused this trust by stealing legitimate signing certificates and using them to sign their malware, making them appear as though they came from legitimate software makers. Our friends at Chronicle conducted some interesting research nearly three years ago exploring this technique. Using a recent example, Nvidia was attacked by the Lapsus$ group who were able to steal their signing certificates. Shortly thereafter, malware samples were observed which were signed by the same stolen certificates.

We explored VirusTotal's database and found that since 2021 **more than one million signed samples** were considered as suspicious (with more than 15% of Antiviruses detecting them as malicious). However, not all samples had a valid signature when they were created as attackers reused revoked or invalid certificates, often the validity of the certification chain is not checked by the victim. In particular, close to 13% of these samples did not have a valid signature when they were uploaded for the first time to VirusTotal. More than 99% of these signed files are Windows Portable Executable or DLL files. The following chart shows the timeline of signed malicious PE samples first seen in VirusTotal. The peak appeared during January 2022 where we saw 80% of samples received were of a WinZip installer flagged as OpenInstall PUA (Potentially Unwanted Application) by Antiviruses and signed by "OI Software, Inc" and "OpenInstall, Inc".

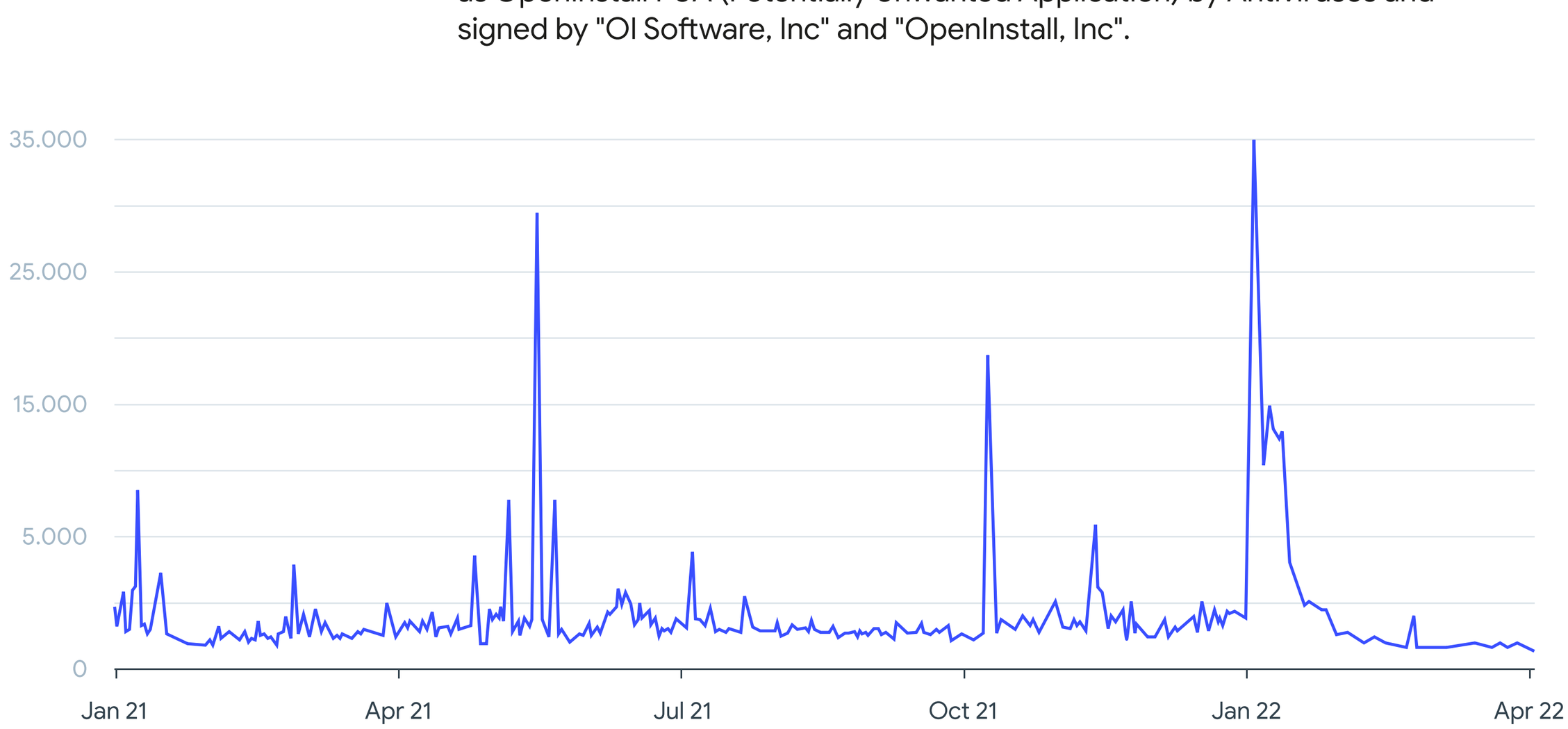



Fig 2.

**Timeline (since 2021) of signed malicious PE samples as first seen in VirusTotal**

Around 950,000 samples were signed with a valid certificate when they were first submitted. The following chart shows the top 10 certification authorities used to sign malicious samples.

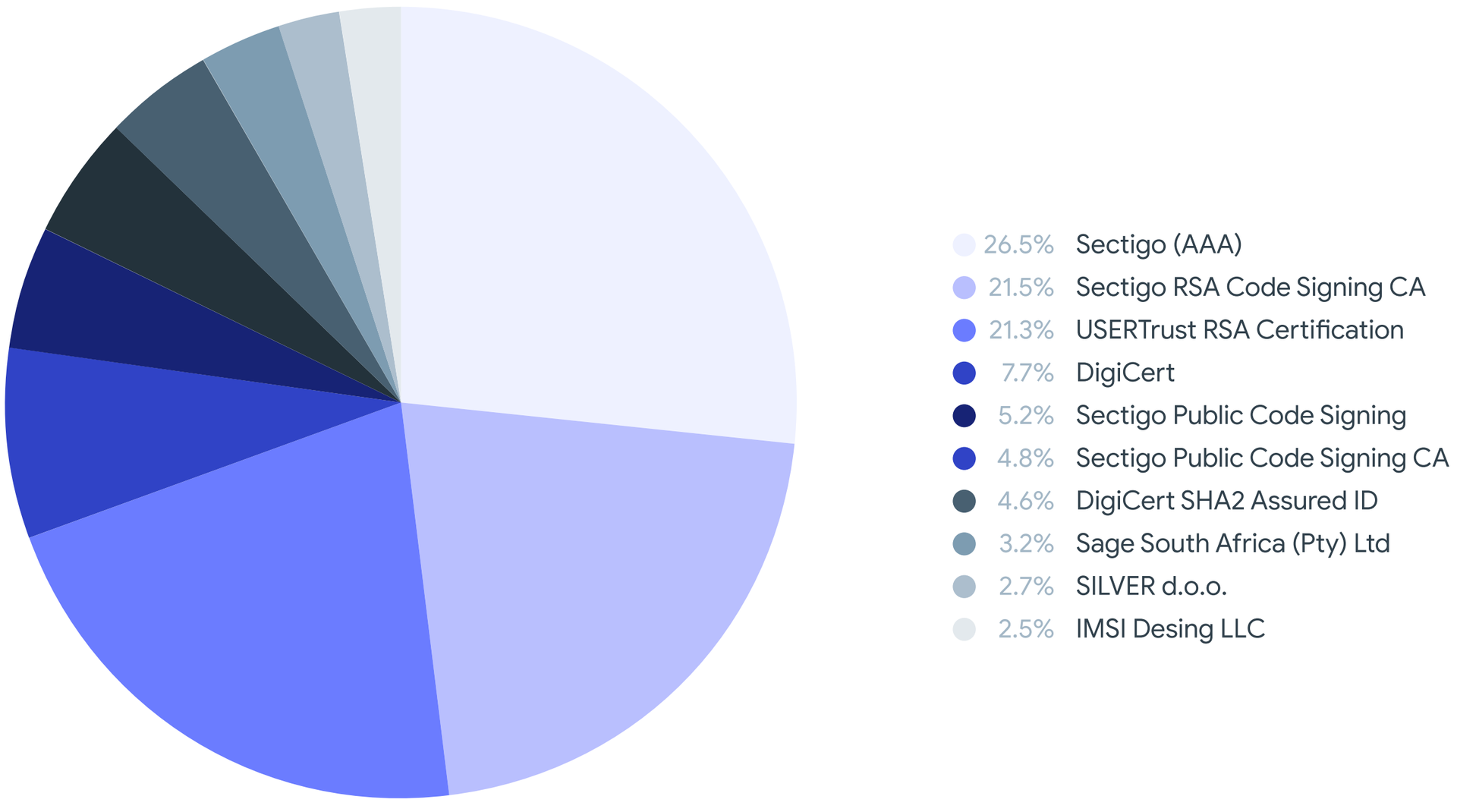



Fig 3.

**Distribution of top 10 CAs used by signed malware samples**

Around 1.1% malicious signed samples signed by certificates that were already revoked when they were first uploaded to VirusTotal.

The chart below shows the timeline of samples signed with revoked certificates (belonging to Nvidia, Softonic, Symantec, BitTorrent and Panda, among others) when they were first uploaded to VirusTotal beginning in 2022. The January / February peak around appears to correspond with the appearance of fake Adobe flash downloaders signed with “Skill on Net”, the most revoked certificate.

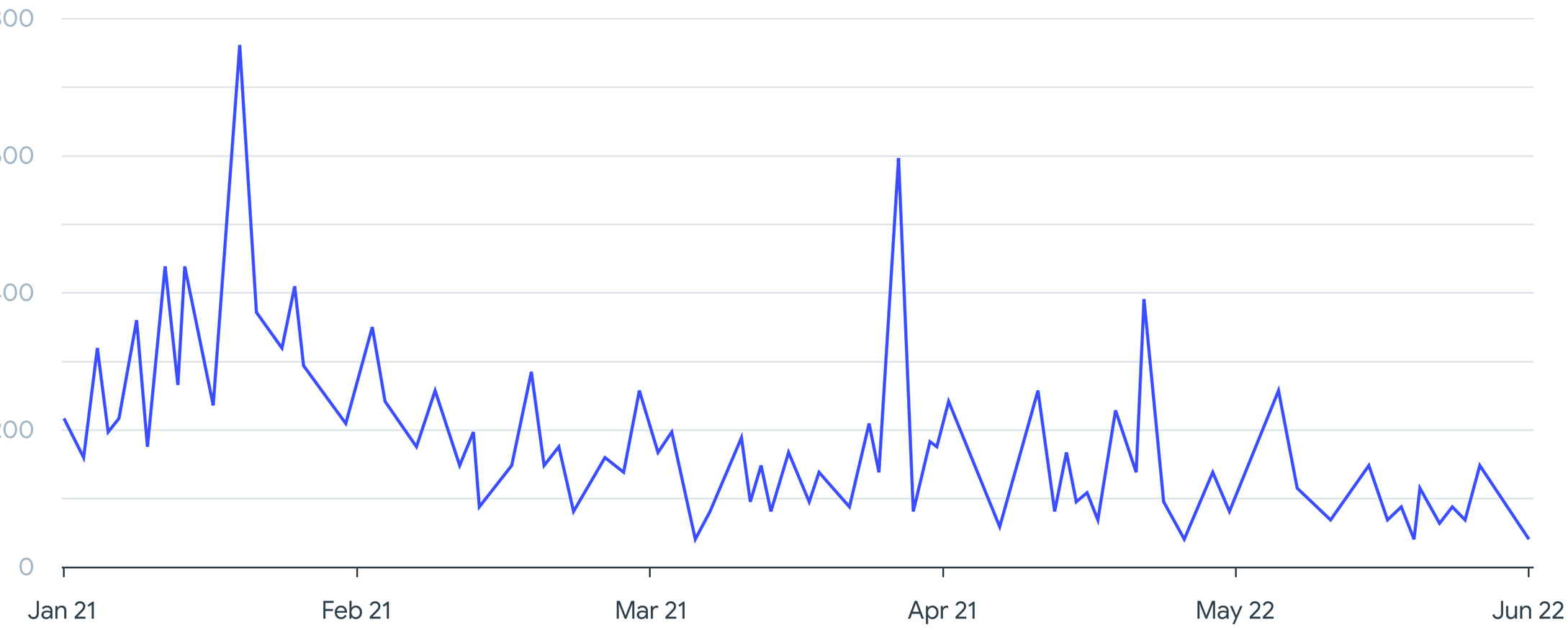



Fig 4.

**Timeline (since 2022) of signed malicious samples with revoked certificates as first seen in VirusTotal**

The following timeline shows the evolution of malware signed with the stolen Nvidia certificates we mentioned at the very beginning, which can provide an idea of the lifecycle of such campaigns. In this particular case, it looks like there were two clear waves, one with first adopters until this information was widespread, and a second still deciding to reuse the revoked certificates.

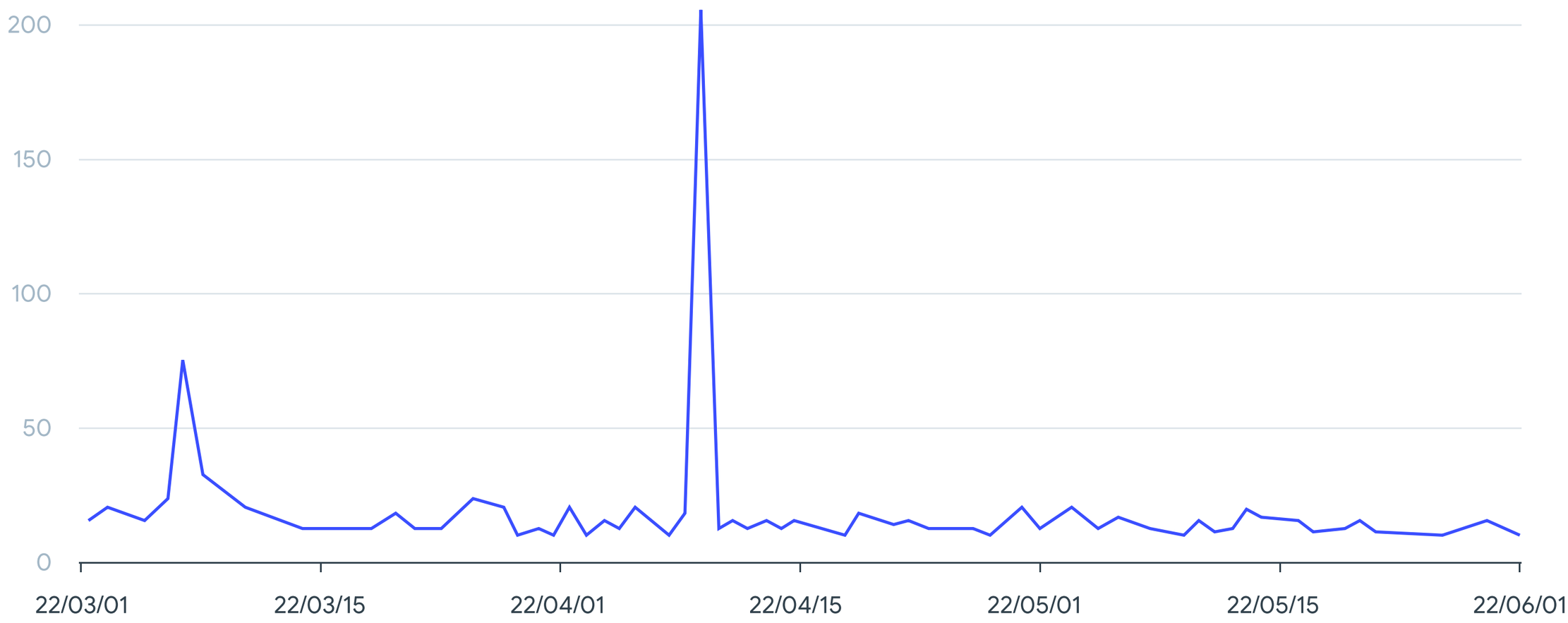



Fig 5.

**Timeline (since march 2022) of signed malicious samples with stolen Nvidia certificates as first seen in VirusTotal**

# Malware disguised as legitimate software

One of the simplest social engineering tricks we've seen involves making a malware sample seem a legitimate program. The icon of these programs is a critical feature used to convince victims that these programs are legitimate.

To demonstrate this we took a set of frequently downloaded Windows software, using fuzzy logic to find suspicious samples (with more than 5 Antiviruses detecting it as malicious) using visually similar icons. This can give us some idea as to how widespread this technique is used. The timeline illustrates the number of samples and when we observed them for the first time in VirusTotal using this technique for our selection of top 25 popular software icons. The timeline appears to indicate increasing use of this technique:

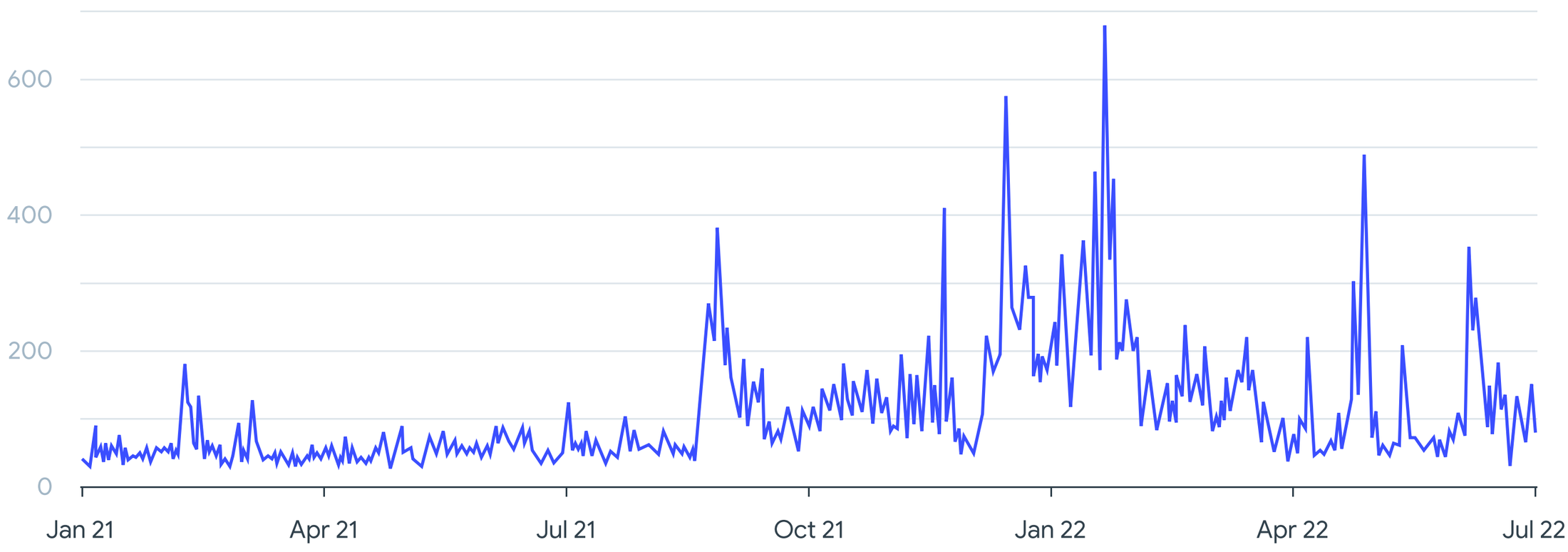



Fig 6.

**Timeline of suspicious samples mimicking icons of popular legitimate software**

From this selection, we also analyzed what application and corresponding icons are most abused by attackers. The chart below shows the applications whose icons were found to be abused the most, according to our data: :

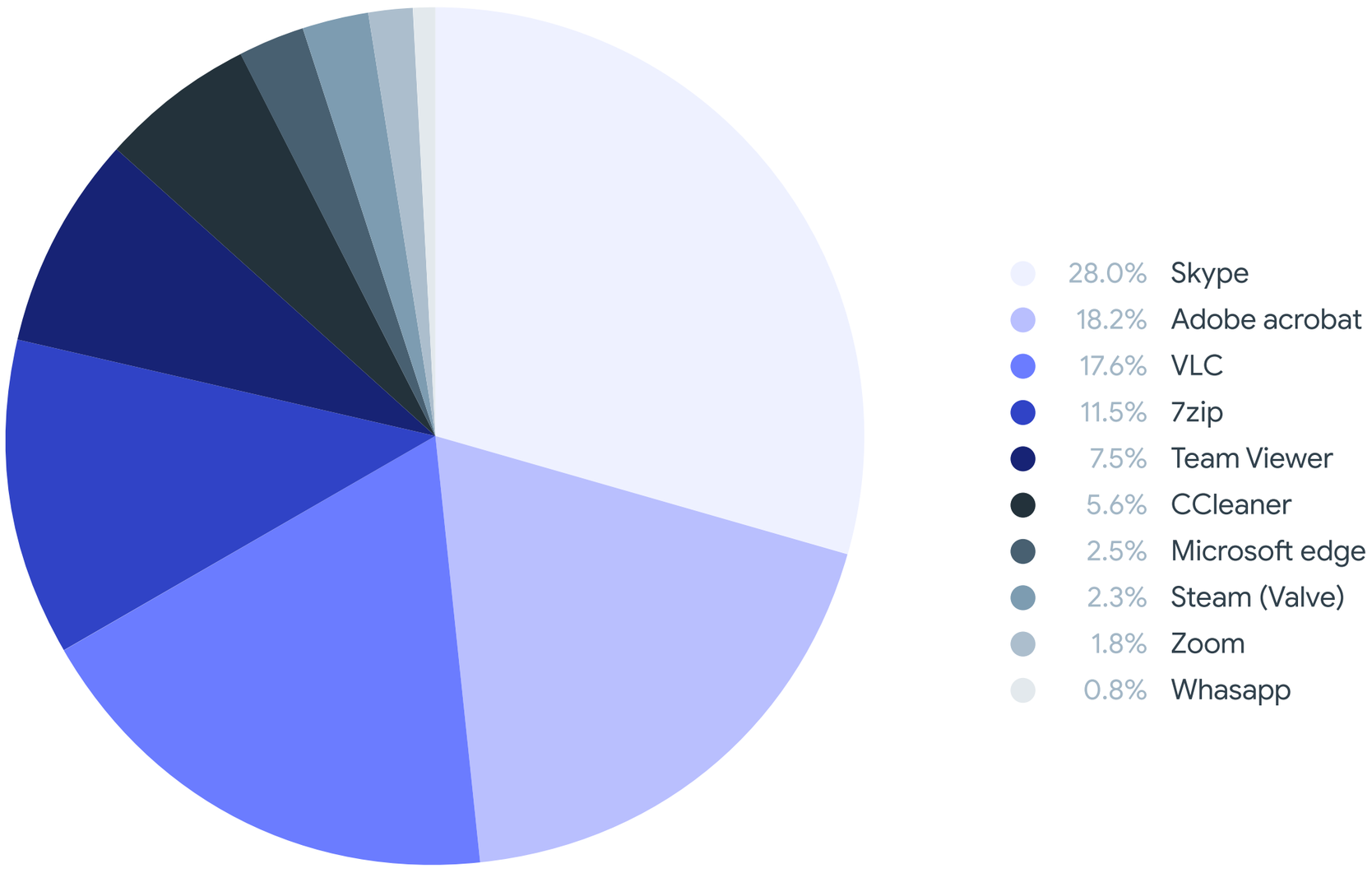



Fig 7.

**Most mimicked legitimate applications (by icon)**

We found it interesting that the infection ratio (or, the number of samples being suspected of being malicious vs total number of samples found using a given icon) greatly differs. We think this  could be an indicator of the attackers' applications of choice for this social engineering technique.

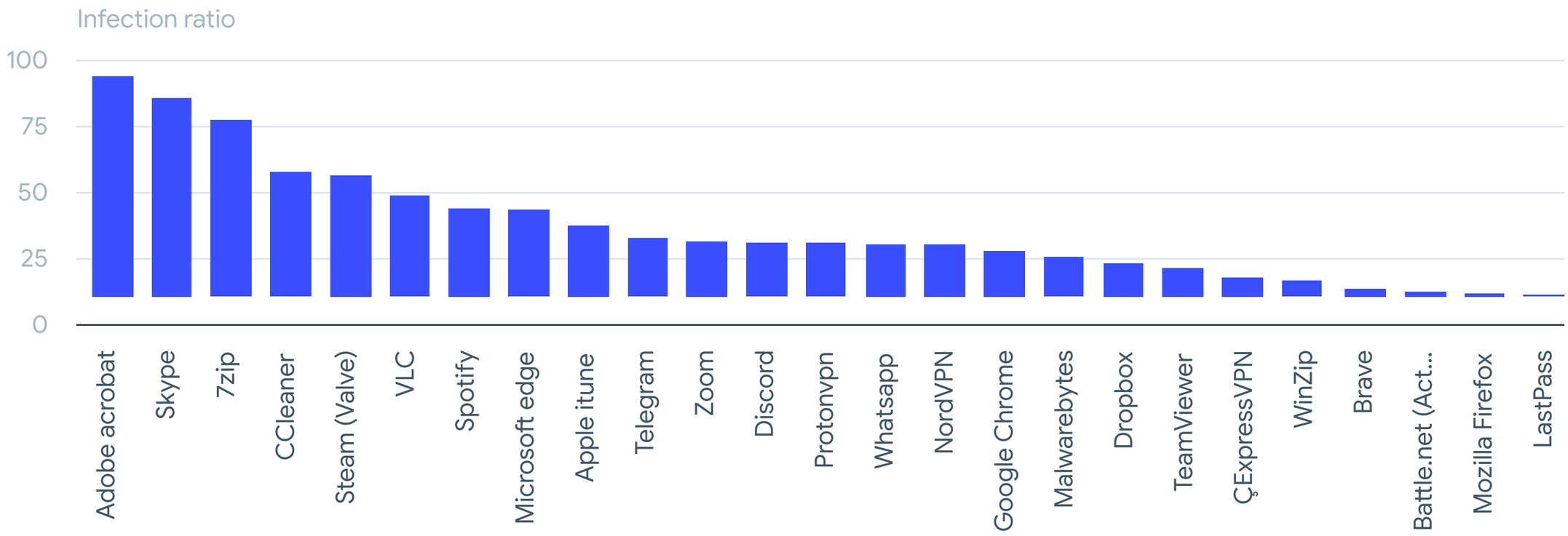



Fig 8.

**Infection ratio (infected vs legitimate apps) using similar icon**

Using Figure 7 and Figure 8, we found Adobe Acrobat, Skype and 7zip are very popular and  have the highest infection ratio, which probably makes them the top three applications and icons to be aware of from a social engineering perspective.

We conducted a similar analysis on URLs using favicon similarity. We found the following to be the most abused websites by a number of different URLs suspected of being malicious:

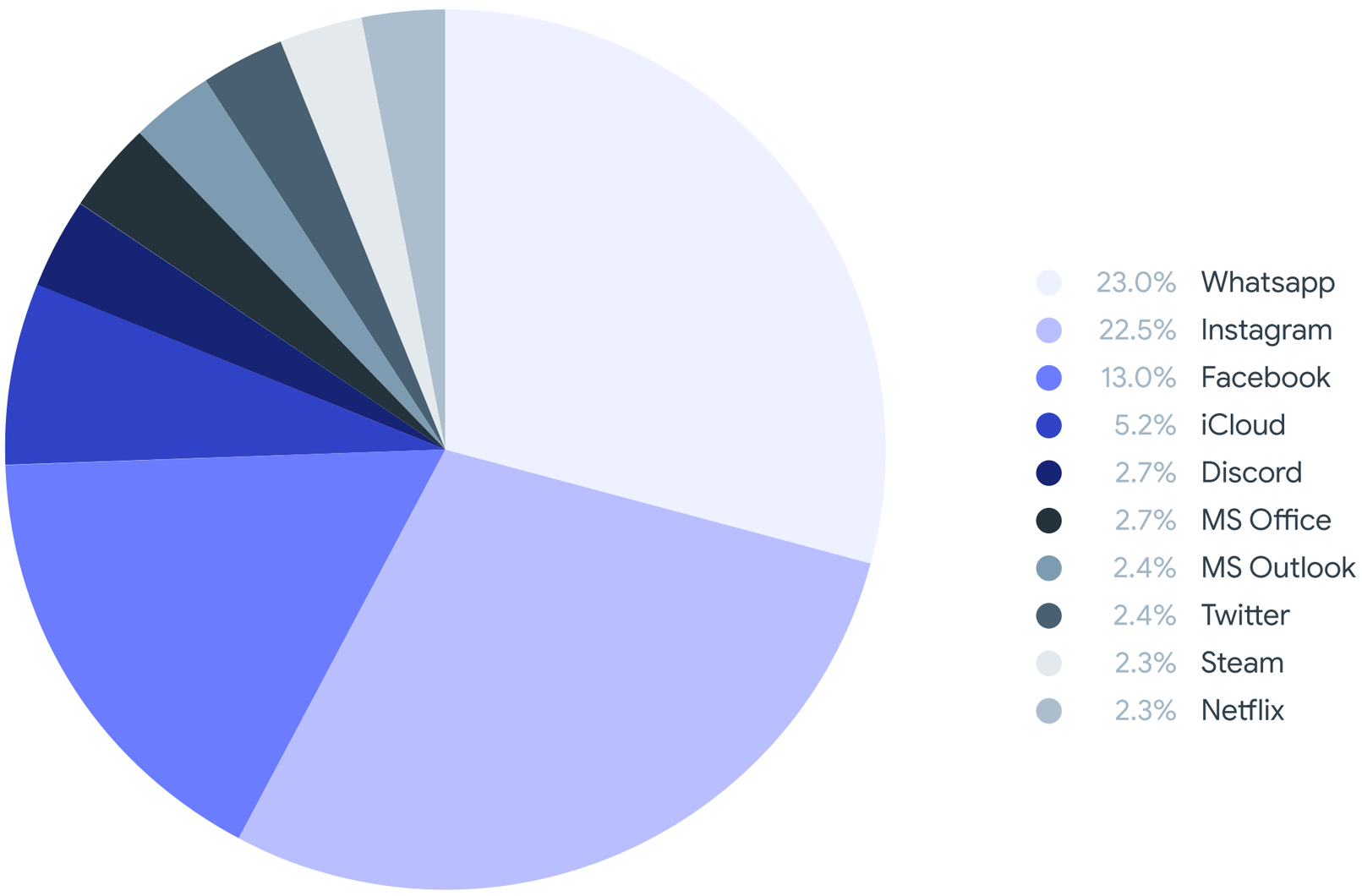



Fig 9.

**Most mimicked legitimate websites (by favicon)**

The infection ratio metric is the percentage of URLs suspected of being malicious vs all the URLs using the specific favicon:




Fig 10.

**Infection ratio (infected vs legitimate URLs) using similar favicons**

# Malware packaged with legitimate software

One of the most effective social engineering techniques consists of masquerading malware as legitimate software by packaging malware in installation packages. These supply chain attacks work when attackers get access to the official distribution server, source code or certificates.

To find potential cases where attackers could be using legitimate hosting servers to distribute malware, we searched in VirusTotal for samples downloaded from a subset of 35 legitimate domains hosting popular software packages. From 2020 until now, we found around 80 suspicious files (with more than 5% Antivirus detecting them as malicious) out of 80 thousand served files (around 0.1%).

In addition to the detection rate, we explored relationships (including execution, compressed, PE resource and PCAP parents) for all served files to understand if they were performing any suspicious activity or being dropped by malware files. This technique allows us to find suspicious “execution parents” or malware that executes legitimate software installers to masquerade their activity.

**Execution Parents**

| Scanned | Detections | Type | Name |
|---|---|---|---|
| 2022-04-13 | 52 / 69 | Win32 EXE | Telegram.exe |
| 2022-04-20 | 23 / 68 | Win32 EXE | Telepon.exe |
| 2022-02-09 | 0 / 59 | RAR | tsetup-x64.3.5.1.rar |
| 2022-04-20 | 26 / 67 | Win32 EXE | 22413d21953743fd956d53926ca20149aac37efc00a294a3725df9e62fa1999a |
| 2022-02-15 | 0 / 57 | RAR | tsetup-x64.3.5.1.rar |
| 2022-03-31 | 32 / 67 | Win32 EXE | TG3-19_se.exe |
| 2022-02-13 | 0 / 58 | RAR | /1/4/3/432a41ff372967c677ed9477106704b5f59d3eeac2f1008b1dd811553cb5f066.file |
| 2022-04-20 | 27 / 60 | Win32 EXE | 556d4dc6dacfbfa54d49c65878b3f88765046c19c926fd6ed27eedc4ccf5c500 |
| 2022-04-13 | 49 / 70 | Win32 EXE | telegram.exe |
| 2022-05-16 | 31 / 66 | Win32 EXE | cnTele.exe |

Fig 11 .

**Execution Parents for a legitimate Telegram installer**

Focusing in on the top legitimate installers executed by malware, we found installers that combined malware with installers for other popular software like Google Chrome, Malwarebytes, Windows Update, Zoom, Brave, Firefox, ProtonVPN, and Telegram amongst others. In total, we found 1816 samples exploiting this condition, distributed through 268 different hosts. The following chart provides a timeline of “malicious execution parents” submitted to VirusTotal:

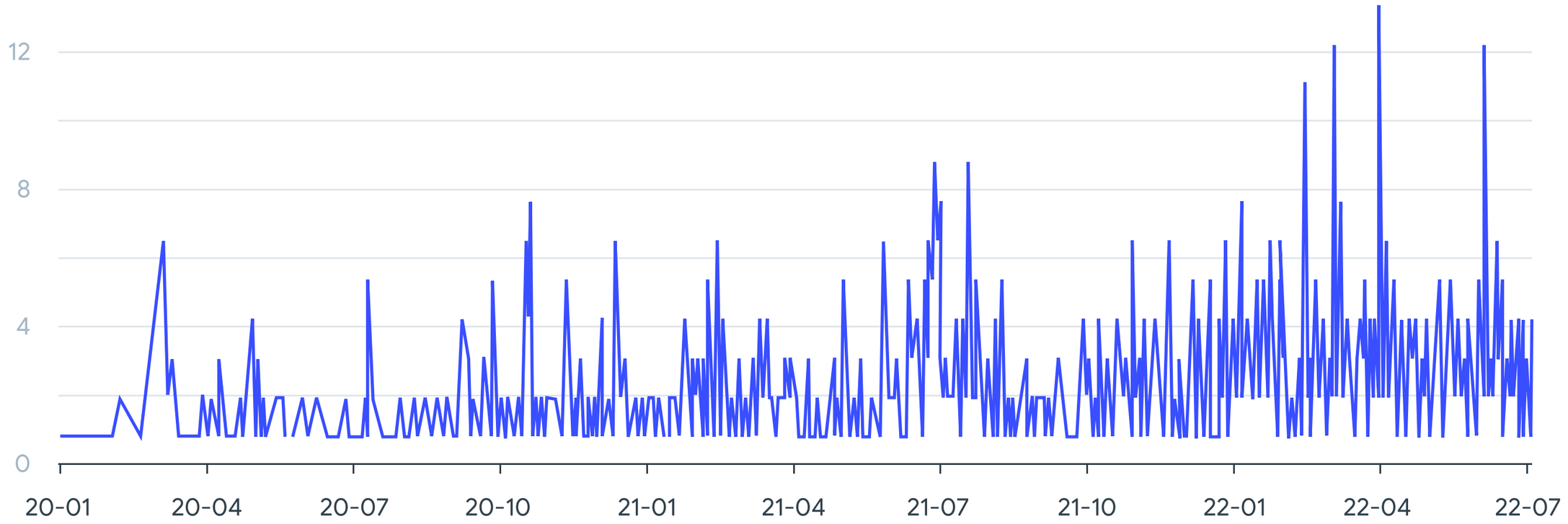



Fig 12.

**Timeline of malicious execution Parents submitted to VirusTotal executing legitimate installers**

The list of top hosts distributing them includes some legitimate domains, as previously discussed:

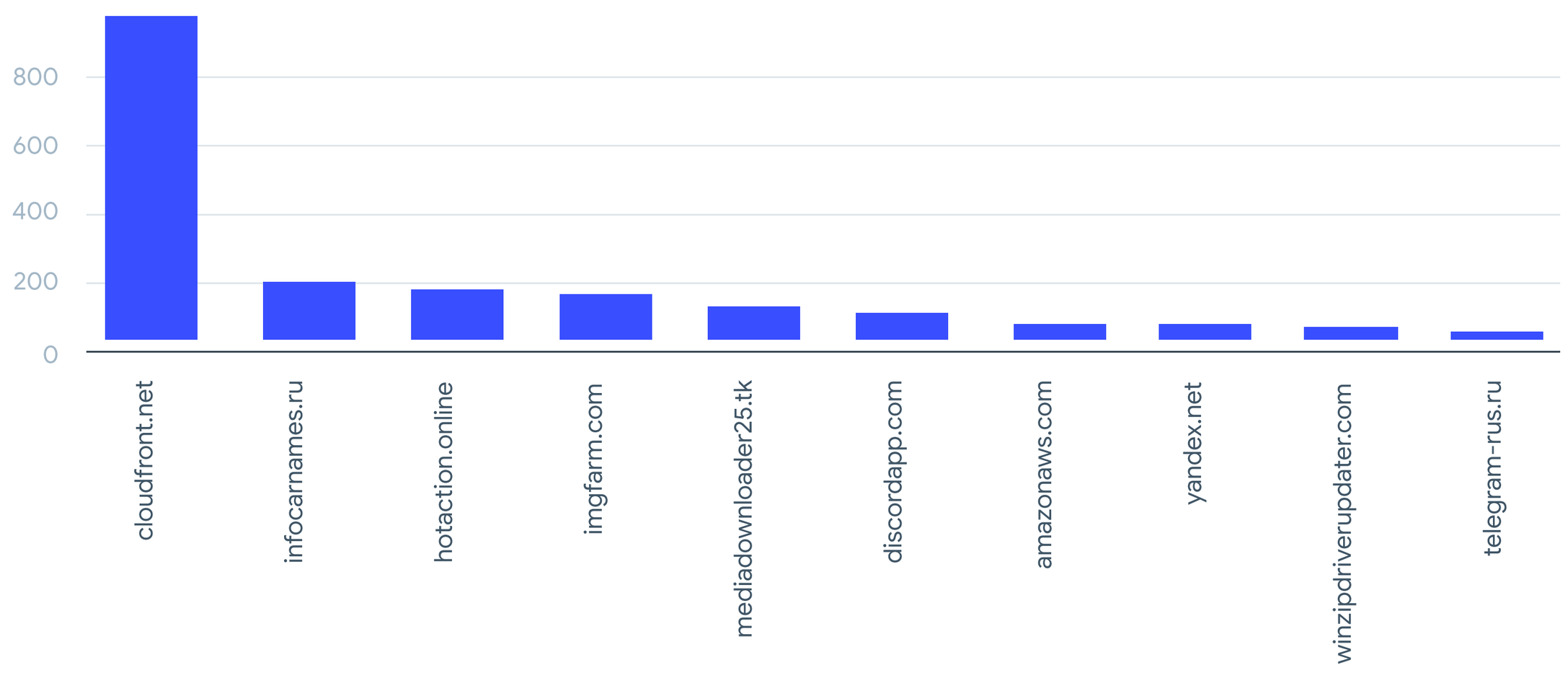



Fig 13.

**Top hosts (some of them legitimate ones) distributing malware packaged with legitimate software**

In other cases, legitimate installers are included in compressed files along with malicious samples. In total, we found 2218 samples abusing this technique being distributed through 180 different domains. The following example shows how a compressed file distributed in-the-wild includes both the legitimate ProtonVPN installer and its what appears to be malware that installs the Jigsaw ransomware.

**Bundled Files**

| Scanned | Detections | File type | Name |
|---|---|---|---|
| 2022-02-28 | 48 / 71 | Win32 EXE | ProtonVPN_win_v1.16.1 - Cracked By PC-RET/CRACK/ProtonVPN.exe |
| 2020-10-28 | 0 / 60 | Text | ProtonVPN_win_v1.16.1 - Cracked By PC-RET/How to....txt |
| 2022-05-06 | 0 / 69 | Win32 EXE | ProtonVPN_win_v1.16.1 - Cracked By PC-RET/ProtonVPN_win_v1.16.1.exe |

Fig 14.

**Compressed file distributing ransomware along legitimate installer**

A more sophisticated technique widely used by attackers consists of including a legitimate installer as a resource (PE Resource) into the malicious sample. In this case, the legitimate file will be executed when the malware runs so the victim thinks everything goes well. We found 452 malicious samples using this technique including in their resources legitimate installers for Zoom, Spotify, Winzip, 7-zip and NordVPN, among others. It is interesting to notice that in 98% of the cases where we observed an executable embedding a legitimate installer in its PE resources, the sample was also malicious.

# Final thoughts

Supply chain attacks are worrisome, for a good reason. The multiple techniques analyzed in this report can have a similar impact on the victim's defenses. While they may seem less sophisticated than other forms of cyber attack, they can be a differentiating factor to succeed in a social engineering attack or bypass many existing security measures used by defenders.

When analyzing these techniques separately, we believe:

- Malware signed by stolen signing keys  likely occurs more frequently than we expected.
- Visually mimicking legitimate apps is a growing trend and targets a number of popular applications. We are still analyzing how this list of the most frequently seen applications will continue to be targeted over time.
- Malware executing legitimate installers, or packing them in the same compressed file within the malware sample, is likely not as common as the other documented  techniques, but seems to be a constant and slightly growing trend.
- Popular domains used by legitimate organizations are used regularly for malware distribution. This includes hosting sites for popular apps, which we would like to analyze in more detail.

When thinking about these techniques as a whole, one could conclude that there are both opportunistic factors for the attackers to abuse (like stolen certificates) in the short and mid term, and routinely (most likely) automated procedures where attackers aim to visually replicate applications in different ways.

Although less sophisticated, the aggregate effect of these techniques could lead to a bigger combined impact than more complex but less voluminous attacks. That's why it seems there are good candidates to monitor at a global level how malware attackers abuse them, which can also help automatically detect suspicious samples before they hit the victim

**Join the discussion @Virustotal**

VIRUSTOTAL

Find out more at virustotal.com