Exfiltration over Telegram Bots: Skidding Infostealer Logs

By André Tavares

Published: 2024-10-16 · Archived: 2026-04-06 01:31:06 UTC

- Telegram has become a popular platform among cybercriminals, not only for messaging but for a wide range of illicit activities, including serving as a data exfiltration server for infostealer malware as well as a marketplace of victim data, including user/employee credentials.

- Credentials are increasingly utilized as the initial attack vector to infiltrate corporate environments. Therefore, companies should monitor underground markets to mitigate potential risks as early as possible.

- Bitsight’s visibility over infostealer malware which exfiltrates over Telegram suggests that the most infected countries are the USA, Turkey, and Russia, followed by India and Germany.

In recent years, Telegram has emerged as a popular messaging platform among cybercriminals, driven by its combination of simplicity, security, and efficiency. Telegram's encrypted messaging capabilities, real-time communication, and the ability to send large data files make it an ideal platform for cybercriminal activities, making it an attractive alternative to traditional underground forums. Another advantage is the seamless communication across different levels—private messages, groups, and channels—without the delays and security risks associated with forum-based messaging.

Currently, Telegram is leveraged by a wide range of threat actors to conduct a plethora of illicit activities. The activity this blog post concerns is related with infostealer malware, where Telegram is used as a data exfiltration server and a marketplace for victim data. This type of malware steals all kinds of data from the system it infects, including credentials (passwords and cookies) for VPNs, RDP, business services, banking and social media, stored by a variety of apps (including popular browsers like Chrome and Firefox). Other kinds of highly sensitive data that infostealers often collect are screenshots, keylogs, clipboard, cryptocurrency wallets and autofill data, the latter occasionally containing credit card info. All of this data is referred to by cybercriminals as “logs”.

These logs are then fed into autoshop marketplaces, some of them known as "clouds of logs". For a relatively small fee or, in many cases, free of charge (as a sort of promotion), they allow all kinds of threat actors, including less-skilled ones, to access all of this data. In some of these logs it’s possible to find credentials to corporate environments, allowing threat actors to bypass the typical initial stages of an attack. Even outdated credentials can be valuable because they can be used in "credential stuffing" attacks, taking advantage of password reuse by the victim.

Looking at the bigger picture, Figure 1 provides a great overview on how the infostealer ecosystem works. Let’s focus on the three main types of attackers, which often are the most direct threat to companies, by leveraging the stolen data. First we have script-kiddies, bored young individuals seeking quick cash or simply looking to cause chaos. Second, there are Initial Access Brokers (IABs), which use stolen credentials to establish footholds in corporate networks, and then sell the access to other threat actors, such as ransomware gangs. Third, the highly

skilled threat actors, including APTs, which also use these credentials for more sophisticated, targeted attacks on organizations. The infamous Lapsus$ group is a notable example, although not fully fitting one single category, since their reasons swing between gaining notoriety, financial gain and in some cases just juvenile amusement. They have targeted high-profile companies such as Uber, Okta, and T-Mobile by exploiting compromised credentials as their initial attack vector.

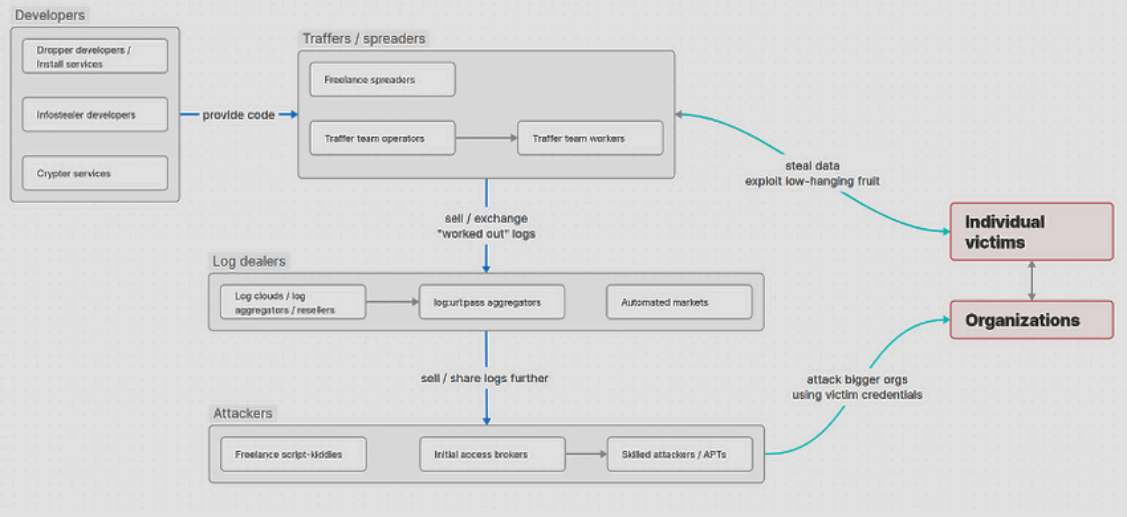

Figure 1 - Overview of the Infostealer ecosystem.
(source: https://thehackernews.com/2024/07/10000-victims-day-infostealer-garden-of.html)

This blog post focuses on analyzing logs exfiltrated by infostealers, specifically to Telegram, through their Bot API. Unlike logs present in "clouds of logs", which can come from a variety of different places, the ones we analyzed were obtained directly from threat actors' Telegram bots. These logs were uploaded in an automated way by malware running on infected systems. This means that there's a higher degree of confidence in the data, in terms of freshness, and it's also more unlikely that the data has been modified. We started collection in October 2024 and so far, out of about 1,800 Telegram bots, we could observe a total of **5 million** logs containing victim IP addresses or domain names related to credentials, with timestamps starting from 2020, but mostly from 2022 onwards. For this research, only credentials (passwords and cookies) and basic system information was collected. Figure 2 shows the logs collected over time by each malware family. It's evident that Telegram usage is showing a significant upward trend, both in terms of volume and also family diversity.

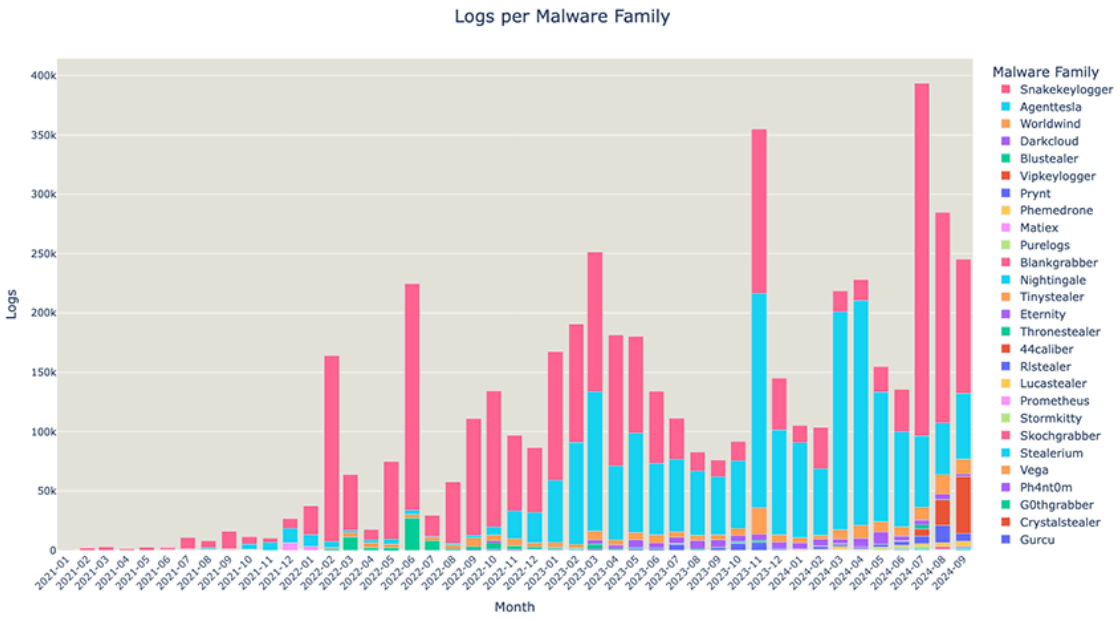

Figure 2 - Number of logs by malware family over time.

So far, we've parsed logs generated by 27 infostealer families. We've also observed some RAT families, such as XWorm and AsyncRAT, but these are yet to be parsed. Regarding infostealers, the majority of the logs were uploaded by SnakeKeylogger (pink) and AgentTesla (blue), two very popular infostealer families. Another interesting fact is that many of the malware families discovered are actually open source, such as Worldwind, Prynt and Phemedrone, as well as the mentioned RATs.

From July onwards, the chart reveals a shift on the top families, with a sharp decline in AgentTesla and a substantial rise in SnakeKeylogger, which has now clearly taken the lead. Added to that, a new family showed up, VipKeylogger (orange), which is actually a variant of SnakeKeylogger. On Snake's telegram channel, they advertise both products (Figure 3) and they also have a sales website in the clearweb, at hxxps://snaketools.xyz/. Both families account for the majority of logs we've observed recently.

The appearance of VipKeylogger coincides with the major decline of AgentTesla, also known as OriginLogger. The threat actors behind OriginLogger posted on their sales Telegram channel explaining that they have lost access to their server and backups, which led to their decision to retire (Figure 4).

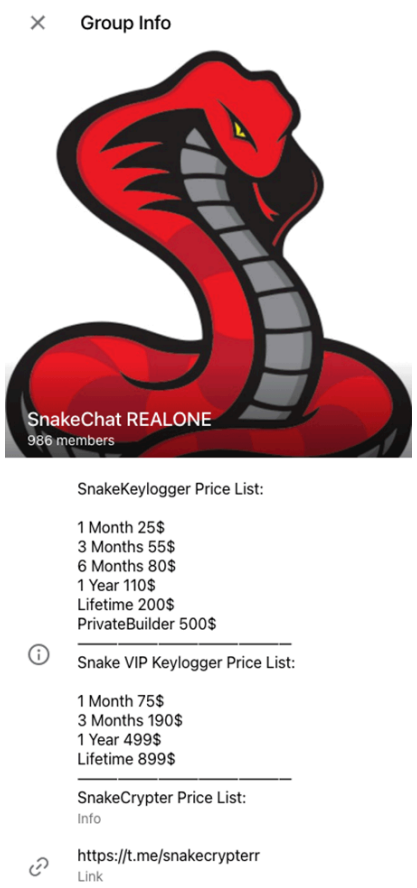

Figure 3 - SnakeKeylogger group info with prices for buying access to the malware.

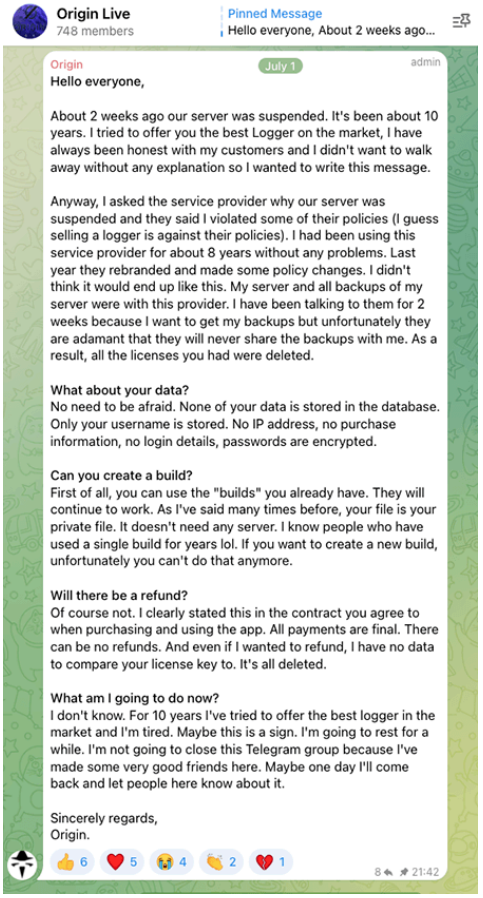

Figure 4 - AgentTesla/OriginLogger actors explaining the shutdown of the service.

It’s important to note that the chart in Figure 2 is probably biased in at least three ways. First, by the sources, which are the Telegram bot tokens we could find, extracted from malware samples we’ve collected. Second, the data parsers, mainly due to parser completeness but also due to missing parsers for malware families we aren’t covering yet or are yet to be discovered. Third, some threat actors might have deleted bot messages, thus making visibility gaps in the collection. The absence of popular infostealer families from this dataset, such as StealC, Lumma, Redline, and Vidar, can be explained by the fact that generally the groups behind them use Telegram mainly for selling the stolen data rather than for exfiltrating it.

Figure 5 illustrates the global distribution of infected systems, based on more than 100,000 system IP addresses found in some of the logs. It’s worldwide spreaded as expected, since infostealer malware is widely accessible, and the top 5 most infected are the USA (16%), Turkey (12%) and Russia (9%), followed by India (5%) and Germany (4%). Turkey's high infection rate can be attributed to the prevalence of AgentTesla and SnakeKeylogger, two malware families seen being used in attacks targeting Turkish industries, and the fact that AgentTesla itself originated in Turkey may be related as well.

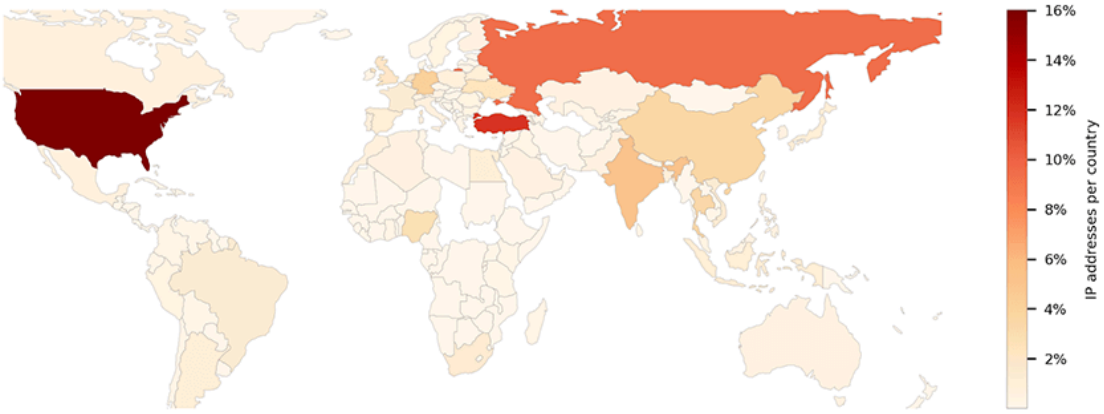

Figure 5 - World distribution of systems infected with telegram-based infostealers.

Within 5 million logs, we've found **2.8 million credentials**, from which 400,000+ unique domains and 10,000+ unique IP addresses were extracted. In this relatively small dataset, we could find credentials associated with almost 60,000 organizations, which says a lot about the diversity of the data. It's important to note that there are two major classes of credentials: user/customer and **employee credentials**. The latter can be the most critical for companies, from a defensive perspective, as previously highlighted.

Figure 6 shows the top domains and corresponding sectors by number of credentials. Most of the credentials are related to the Technology sector, such as email and social media accounts, but there are all kinds of credentials, related to all sectors. Some of the top sectors are the Government and Finance sectors, accounting for 5% and 6% of all credentials, respectively. For instance, we've found 0.2% or 56,000+ paypal credentials. The amount of Turkish domains is in accordance with the seen geographic distribution of infections.

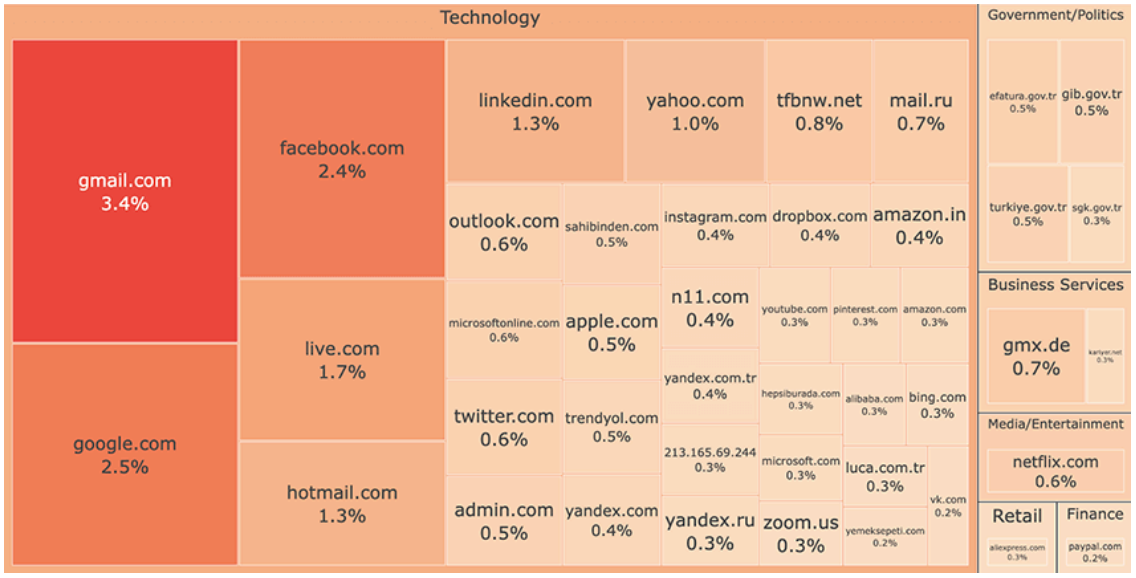

Figure 6 - Top domains and corresponding sectors by number of credentials found.

Although this seems quite a lot of data, we are only seeing the tip of the iceberg. For instance, HudsonRock infostealer reports show many thousands of compromised systems per week. According to one of their reports, the

number of compromised users increased by a factor of six in 2022, a trend also evident in the data we collected. This reinforces the growing perception that the infostealer market is becoming increasingly popular.

The 2024 Data Breach Investigations Report by Verizon reveals that stolen credentials were the single biggest initial attack vector in 2023. Credentials, not exotic malware or zero-day exploits, were the most common way hackers breach systems and wreak havoc. For instance, a widely covered attack this year was the Snowflake incident, where a financially motivated threat actor stole a significant volume of records from Snowflake customer environments, using stolen customer credentials, and advertised victim data for sale on cybercrime forums, as well as attempted to extort many of the victims.

Data breaches resulting from these attacks can lead to severe financial losses for organizations. Therefore, organizations can benefit significantly from monitoring credential leakage, including reducing the risk of data breaches, increasing compliance with industry and privacy laws, and saving costs by mitigating the impact of security incidents.

This research is a “relatively” small sample of the volume of data stolen by infostealers and emphasizes that cybercriminals in general and the infostealer ecosystem in particular are increasingly taking advantage of legitimate services, in this case Telegram (Discord is also being leveraged), to conduct illicit activities and monetize system and data access as much as possible. As such, companies should care about this threat and enhance protection in their corporate environments. One possibly critical step that can be done, specifically regarding Telegram, is blocking access to the Telegram API (api.telegram.org), if there isn’t a business use case for it. This single action can prevent Telegram based infostealers from exfiltrating data. Additionally, implementing multi-factor authentication (MFA) across all company accounts is essential. Finally, regular monitoring for compromised credentials may enable swift responses to potential breaches.
