Agent Tesla: The Punches Keep Coming

Archived: 2026-04-05 20:37:11 UTC

By Nathaniel Raymond

Agent Tesla has become a massively popular choice of malware for threat actors since its first appearance in 2014 and for good reasons. This vetted Malware-as-a-Service, MaaS, owes its popularity to many attractive factors that Cofense has broken down in a previous Strategic Analysis which include being an affordable malware service option, easy to use, having multiple capabilities at and during infection time, and being flexible in its exfiltration choices. These features, coupled with Agent Tesla's relatively long life, have led this malware family to become the most widespread malware distributed in email campaigns seen by Cofense. This Strategic Analysis aims to analyze this five-year historical trend in email campaigns delivering Agent Tesla to understand Agent Tesla's recent past trends better and get a glimpse of potential future trends. A quick overview of the trend analysis suggests that Agent Tesla email campaigns continue to rise yearly, with Q3 and Q4 being notably higher in email volume.

Key Points

- Agent Tesla is a popular MaaS that entices threat actors of varying skill degrees through attractive features such as being an affordable malware service with multiple capabilities to exfiltrate and steal users' data.
- Agent Tesla has a long history, dating to its discovery in 2014. Since then, it has only become more popular every year, with most campaigns in Q3 and Q4 of each year.
- Agent Tesla has had a massive surge during the height of the COVID-19 epidemic, that is potentially due to lockdowns and work-from-home mandates. The trend analysis suggests that Agent Tesla has only since grown in popularity.

Recap: What is Agent Tesla?

By now, Agent Tesla needs no introduction. However, a quick overview of Agent Tesla is that it is an affordable MaaS, written using the .NET framework, with multiple capabilities during and after the initial infection. Agent Tesla can be considered a bit of a Swiss army knife. It can play multiple roles as a keylogger and an information stealer and utilizes some RAT-like monitoring functionalities. Agent Tesla can also download other malicious programs after infection. These features, coupled with the malware's ability to use many exfiltration methods such as FTP, SMTP, Web Panels, and even Telegram bots, make this malware an incredibly popular choice among threat actors of varying skill levels.

Trends: Yearly

The overall trends in Figure 1, agree that Agent Tesla has increased yearly, with 2021 having the most volume. The 2021 volume increase was potentially due to mandatory stay-at-home mandates declared during the height of the COVID-19 pandemic which made some users work from home. This was a challenge for many businesses as

employees may not have been accustomed to working at home during this time. Although Agent Tesla increased in 2021, this spike in volume was only one of many threats to increase in 2021, as the FBI (Federal Bureau of Investigation) claimed a 400% increase in cyber-attacks seen during the pandemic. We witness that 2022 and 2023 have increased since 2019 and 2020 with 2023 being the most volume aside from 2021. We also note that if trends continue, this year may see Agent Tesla reaching volumes seen in 2021.

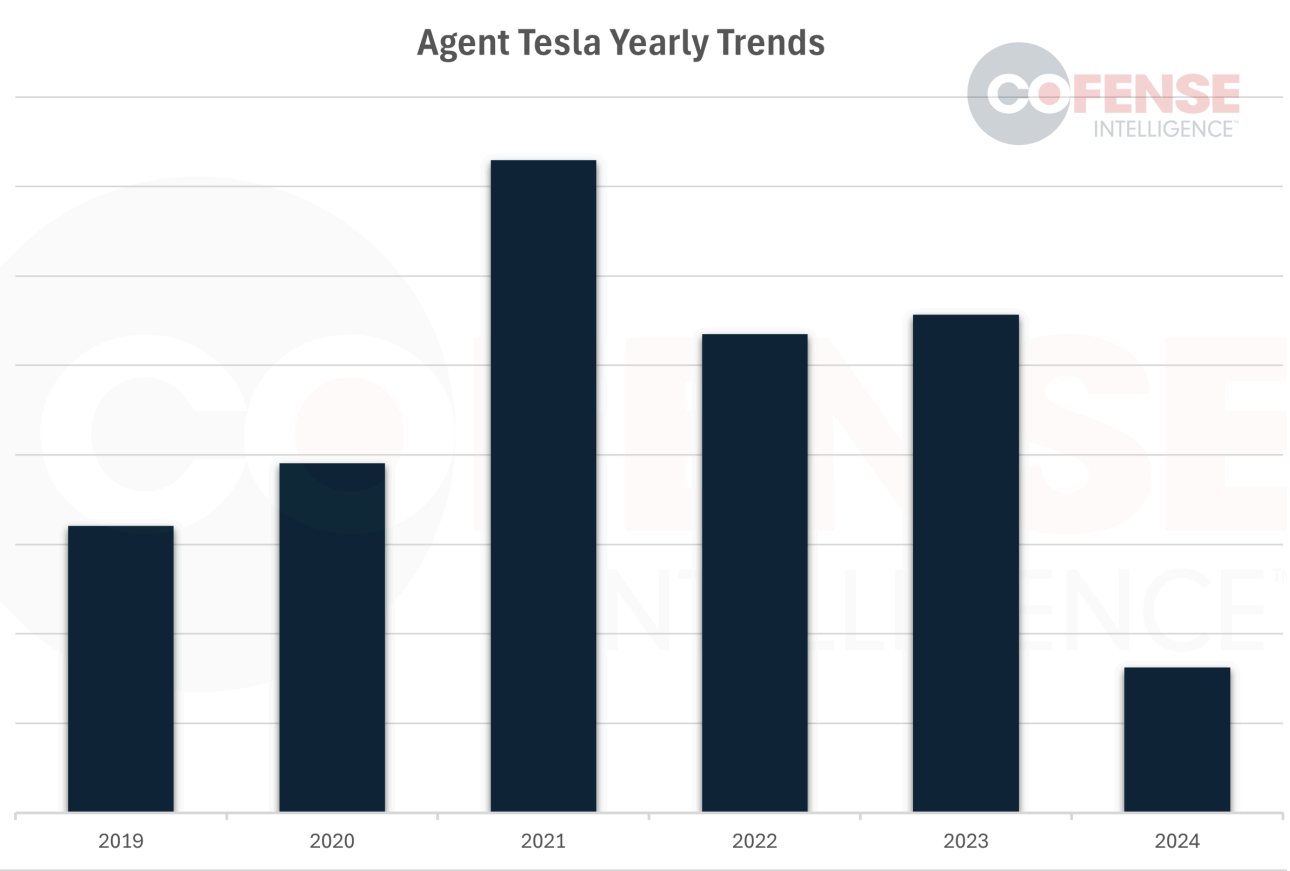

Figure 1: Agent Tesla volumes by year.

Trends: Quarterly

While Agent Tesla or a delivery mechanism(s) that delivers Agent Tesla may potentially reach a user's inbox at any time, Figure 2 suggests that Q3 and Q4 have the highest volume per year marking them as the time Agent Tesla poses a higher chance, simply by volume. In 2024 and unlike other first quarters in the past five years, the first quarter of 2024 saw the most emails delivering Agent Tesla by volume. Not only has Q1 of 2024 beat previous Q1 quarters, but it also has overshadowed many previous quarters in their respective years. This lends credibility to the trends in Figure 1, which show that Agent Tesla volumes are projected to increase yearly.

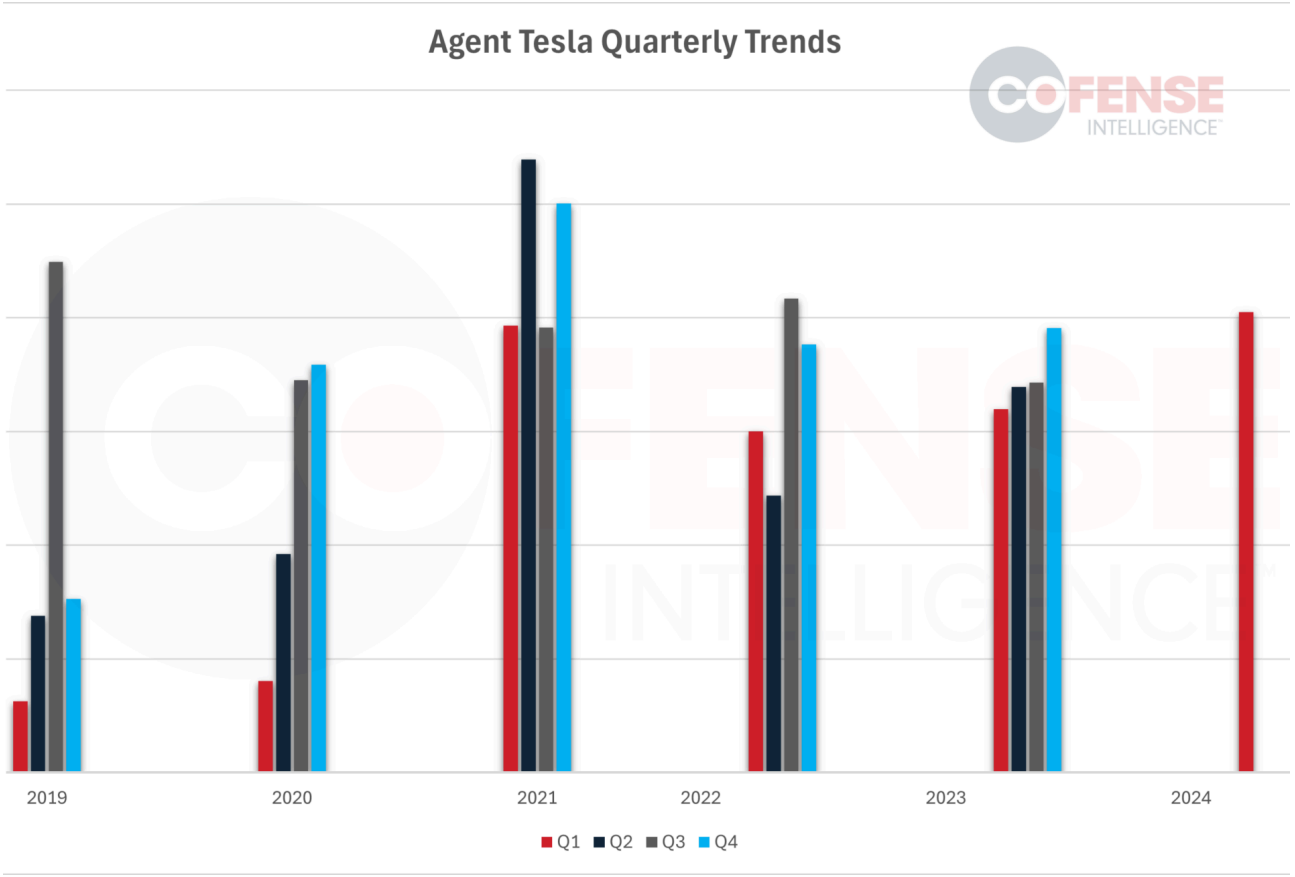

Figure 2: Agent Tesla quarterly trends.

Reaching New Heights

Thanks to the detection improvements made at Cofense, we can see that not only did Q1 of 2024 have more volume than most of the past quarters in the past 5 years, but also has been attributed to increasing weekly volumes and averages. However, it is important to recognize that this observation in Q1 2024 does not necessarily indicate an increase in the distribution of Agent Tesla as a whole. Rather, it reflects the enhancements in our detection capabilities, allowing us to identify a greater extent of the existing instances.

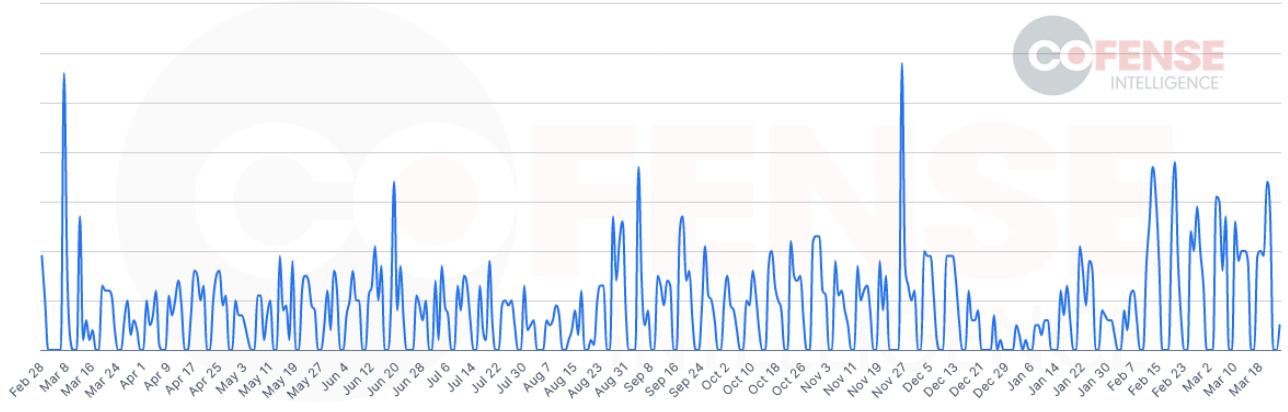

Figure 3: Year-over-year average increase.

Putting It All Together

With enhanced detection capabilities made at Cofense increasing weekly averages and Q1 2024 numbers, 2024 is set to potentially repeat this trend again this year, thus following the increasing volume trend in Figure 1 which is attempting to potentially meet or exceed 2021 email volumes. Q3 through Q4 each year has the most potential that Agent Tesla will be delivered to a user’s inbox simply thanks to increased volumes versus Q1 or Q2 as shown in Figure 2.
