Strategic Analysis: Agent Tesla Expands Targeting and Networking Capabilities

cofense.com/strategic-analysis-agent-tesla-expands-targeting-and-networking-capabilities/

Cofense December 15, 2020

A new iteration of the Agent Tesla keylogger has expanded on its data harvesting capabilities and exfiltration efforts in phishing campaigns primarily targeting India and ISPs. Cofense Intelligence recently alerted customers to Agent Tesla's high volume compared to other keylogger families from January to August this year. The newest iteration of the keylogger added to that volume, likely as threat actors moved to adopt the updated version.

Threat actors who transition to this version of Agent Tesla gain the capability to target a wider range of stored credentials, including those for web browser, email, VPN and other services. This may indicate an increased interest in stolen credentials for a more specialized segment of the market or a particular kind of product or service. The update also includes networking capabilities that create a more robust set of exfiltration methods, including the use of the Telegram messaging service—adding to an overall trend of abusing trusted platforms to evade network-based detection. For Cofense Intelligence customers, technical details of these and other updates are available in the full report in ThreatHQ.

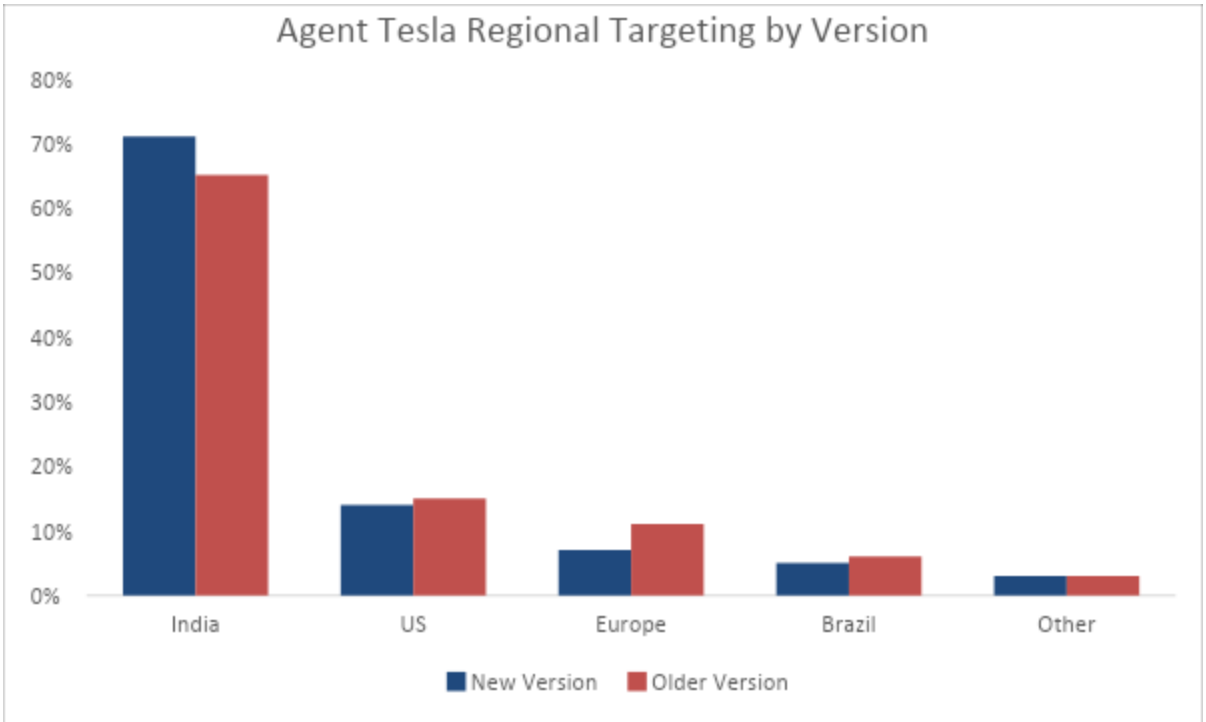

Figure 1: Top regions targeted by the different versions of Agent Tesla.

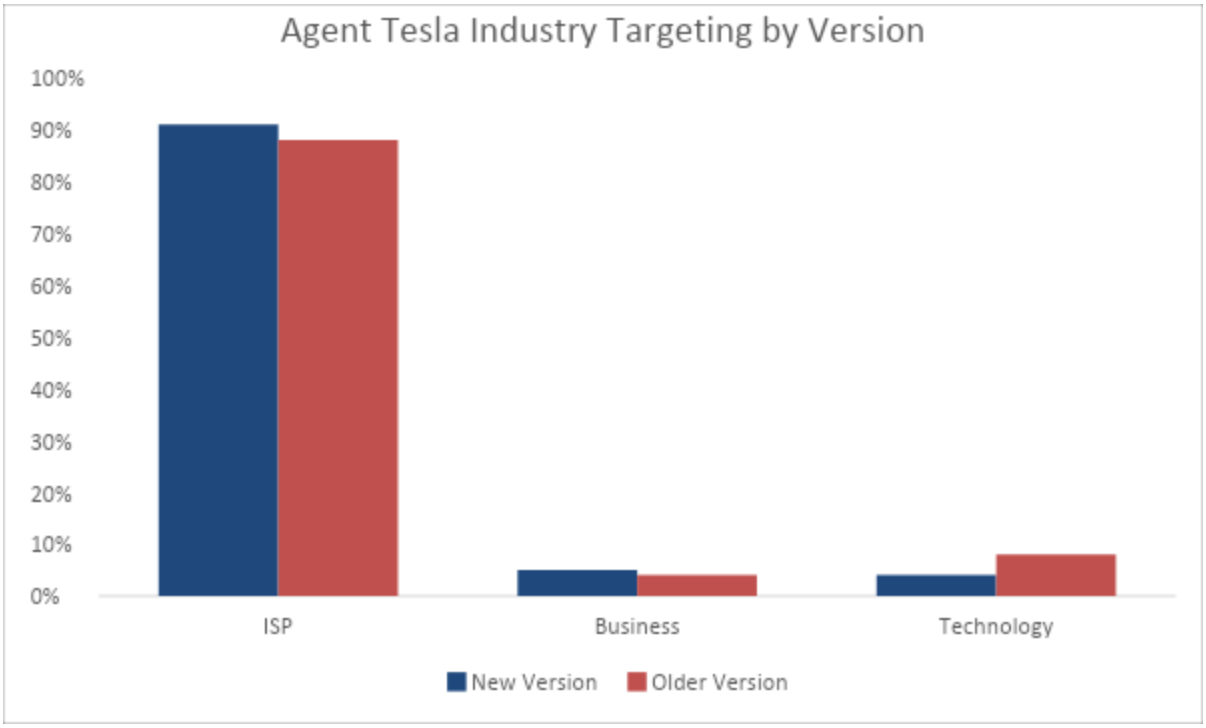

Figure 2: Top industries targeted by the different versions of Agent Tesla.

From August to December of this year, the newest iteration of Agent Tesla largely followed the same pattern as the older version in terms of targeted industries and regions. Figure 1 shows that both versions preferred to target email accounts in India more than any other region. The United States and Brazil were also among the top three most targeted regions.

Figure 2 shows that Agent Tesla overwhelmingly targeted internet service providers (ISPs) over other industries. Utilities and financial services rounded out the top three targeted industries.

ISPs could be considered a major target for threat actors because of the other industry verticals that rely on them for essential functions. A compromised ISP could give threat actors access to organizations that have integrations and downstream permissions with the ISP. Subscribers would also be at risk, as ISPs often hold emails or other critical personal data that could be used to gain access to other accounts and services. In at least one incident, attackers reportedly targeted subscriber data of a compromised ISP in Austria.

Agent Tesla has been a major force within the phishing-threat landscape for years and has steadily evolved, likely in response to threat actors' demands and improvements in network defenses. The variety of infection chains that use this keylogger family as its final payload are too numerous to list, which shows the versatility of this particular family. The fact that older versions of Agent Tesla keylogger are still successful today likely indicates that threat actors will be slow to adopt the newest version. However, once threat actors realize the benefits gained from updating to the newest version, they may transition more quickly as the new features might be necessary. Despite the dangerous capabilities of both versions of Agent Tesla, organizations can protect themselves by educating their employees and keeping proper mitigations in place.