Data Insights on AgentTesla and OriginLogger Victims

bitsight.com/blog/data-insights-agenttesla-and-originlogger-victims

Written by André Tavares January 09, 2024 Share Facebook Twitter LinkedIn

Bitsight Security Research

Key takeaways

- AgentTesla (also known as OriginLogger) remains a prevalent commodity stealer, being daily distributed, mainly via email attachments;
- The primary method for exfiltrating data remains the usage of mail servers, although Telegram utilization is increasing;
- Available infection telemetry suggests that the most targeted countries are the United States, China and Germany.

Malware as a Service

AgentTesla is a Windows malware written in .NET, designed to steal sensitive information from the victim's system. It’s considered commodity malware given its accessibility and relatively low cost. Commodity malware poses a significant threat as it enables less

sophisticated cybercriminals to conduct various types of cyberattacks without requiring extensive technical knowledge. AgentTesla has been a persistent and widespread threat since its emergence in 2014.

Also known as Negasteal, it was rebranded to OriginLogger (also known as AgentTesla v3 – and beyond) in 2019. This change followed revelations by Krebs on Security in October 2018, spotlighting one of the suspected actors behind the malware, a Turkish individual – while writing this blog post, another suspected author was revealed, a second Turkish individual, which appears to be the actual author of the malware. The first disclosure led to the sudden suspension of AgentTesla sales shortly thereafter. By March 2019, the developers announced via their Discord customer support server that they were shutting down the shop due to legal trouble but also prompted an alternative product, OriginLogger:

"If you want to see a powerful software like Agent Tesla, we would like to suggest you OriginLogger. OriginLogger is an AT-based software and has all the features."

OriginLogger is in fact a variant of AgentTesla, since they share the same code base. Consequently, existing detection methods for AgentTesla are effective for identifying OriginLogger, frequently causing OriginLogger samples to be classified as belonging to the AgentTesla family. Similar to AgentTesla, OriginLogger operates as a licensed-based Malware as a Service (MaaS), maintaining a presence on the clear web, using suggestive websites such as agenttesla[.]com and originpro[.]me. Figure 1 presents the current face of the OriginLogger website.

ORIGIN LOGGER

POWERFUL EASY STABLE

ORIGIN

ABOUT

ORIGIN LOGGER POWERFUL ALGORITHM CAN RECORD EVERYTHING THAT IS TYPED ON THE KEYBOARD, INCLUDING PASSWORDS, REGARDLESS OF THE APPLICATION USED. KEYBOARD, SCREENSHOTS AND SAVED PASSWORDS ARE SENT IN LOG.

YOU CAN RECEIVE YOUR LOGS VIA E-MAIL, DISCORD, TELEGRAM, FTP OR HTTP(WEB PANEL)

FEATURES

POWERFUL KEYBOARD HOOK

DETECTS ALL KEYBOARD STROKES. IT DOES NOT WORK WITH THE TIMER, IT HOOK DIRECTLY. ORIGIN LOGGER HAS SUPPORT ALL LANGUAGES. (CHINESE, GREEK, LATINS ETC..)

WEB PANEL

YOU CAN MONITORING YOUR LOGS ON YOUR HOSTING. WE ARE PROVIDING OUR PANEL SCRIPTS AND WE CAN HELP YOU FOR INSTALLATION.

COLORED LOG

ORIGIN LOGGER SAVES LOGS IN HTML. COLORED TEXTS MAKE READING EASIER.

SMART LOGGER

WITH THIS FEATURE, THE KEYLOGGER STARTS TO WORK ONLY IN THE WINDOWS WHERE THE WORDS YOU SPECIFY ARE DETECTED.

- MULTILANGUAGE SUPPORT
- 5 DIFFERENT DELIVERY: HTTP, SMTP, TELEGRAM, DISCORD AND FTP.
- KEYLOGGER
- COLORED LOG
- SCREENSHOT LOGGER
- MULTI FILE BINDER
- CLIPBOARD LOGGER
- SMARTLOGGER
- PASSWORD RECOVERY
- WEB PANEL
- 7/24 SUPPORT
- FAKE MESSAGE
- AUTOBUY
- STABLE AND FAST
- PURE CODE
- ALL WINDOWS OS SUPPORTED
- UAC BYPASS: WIN 7/8/10.
- ASSEMBLY & ICON OPTION

PASSWORD RECOVERY

- GOOGLE CHROME
- MOZILLA FIREFOX
- OPERA
- YANDEX
- SAFARI FOR WINDOWS
- INTERNET EXPLORER
- SEAMONKEY
- FLOCK BROWSER
- COMODO DRAGON
- COOLNOVO BROWSER
- CHROMIUM
- BLACKHAWK
- CYBERFOX
- K-MELEON
- WATERFOX
- FALKON BROWSER
- ICECAT
- PALEMOON
- COMODO ICE DRAGON
- UC BROWSER
- 7STAR
- AMIGO BROWSER
- CENT BROWSER
- CHEDOT BROWSER
- COCCOC BROWSER
- ELEMENTS BROWSER
- KOMETA BROWSER
- ORBITUM
- SPUTNIK
- BRAVE BROWSER
- CITRIO
- SLEIPNIR 6
- URAN BROWSER
- VIVALDI BROWSER
- EPIC PRIVACY BROWSER
- TORCH
- MICROSOFT OUTLOOK
- THUNDERBIRD
- FOXMAIL
- OPERA MAIL
- EUDORA MAIL
- THE BAT!
- POCOMAIL
- INCREDIMAIL
- POSTBOX
- CLAWS MAIL
- TRILLIAN
- BECKY!
- FILEZILLA
- WINSCP
- FLASHFXP
- COREFTP
- FTPCOMMANDER
- WS_FTP
- SMARTFTP
- FTP NAVIGATOR
- JDOWNLOADER
- INTERNET DOWNLOAD MANAGER
- WI-FI
- PSI/PSI+
- OPENVPN
- AND MORE+

PRICING

1 MONTHS	3 MONTHS	6 MONTHS
50$	75$	90$

Fig. 1 - Image from the OriginLogger website.

The website offers time-limited licenses for purchase, spanning up to six months. These licenses grant customers access to the malware builder, enabling them to customize their own instance of AgentTesla, including the configuration of the data exfiltration method.

With AgentTesla and OriginLogger sharing so many similarities, distinguishing between them individually becomes quite challenging. Throughout this article, we refer to both as AgentTesla for simplicity's sake, except when we are comparing them.

Widespread Infostealer

Since its rebranding, the malware has undergone regular updates, with the most recent one occurring in November. It has been consistently ranked among the top charts for the most widespread and prevalent malware, as evidenced by platforms such as ANY.RUN, Unpac.Me, and MalwareBazaar.

Typically, AgentTesla campaigns involve phishing emails carrying malicious attachments, oftentimes involving malware loaders down the infection chain, such as GuLoader and PureCrypter, or as the initial infection vector, such as PrivateLoader. After all infection stages are executed on the victim's system, the final payload initiates actions to sustain persistence, aiming to harvest credentials, keystrokes, clipboard data, and screenshots for as long as possible. More specifically, it harvests a wide array of sensitive information from browsers, VPN clients, mail clients, FTP clients, VNC clients, Microsoft applications, and social media apps. Further details regarding tactics, techniques, and procedures (TTPs) can be found here, here and here. This exfiltration of data can be accomplished through various protocols: SMTP, FTP, and HTTP – which encompass the Telegram and Discord APIs, both later introduced on the OriginLogger variant in August 2020 and October 2022 respectively. Finally, the data is sent unencrypted to the threat actor’s server and remains there also unencrypted.

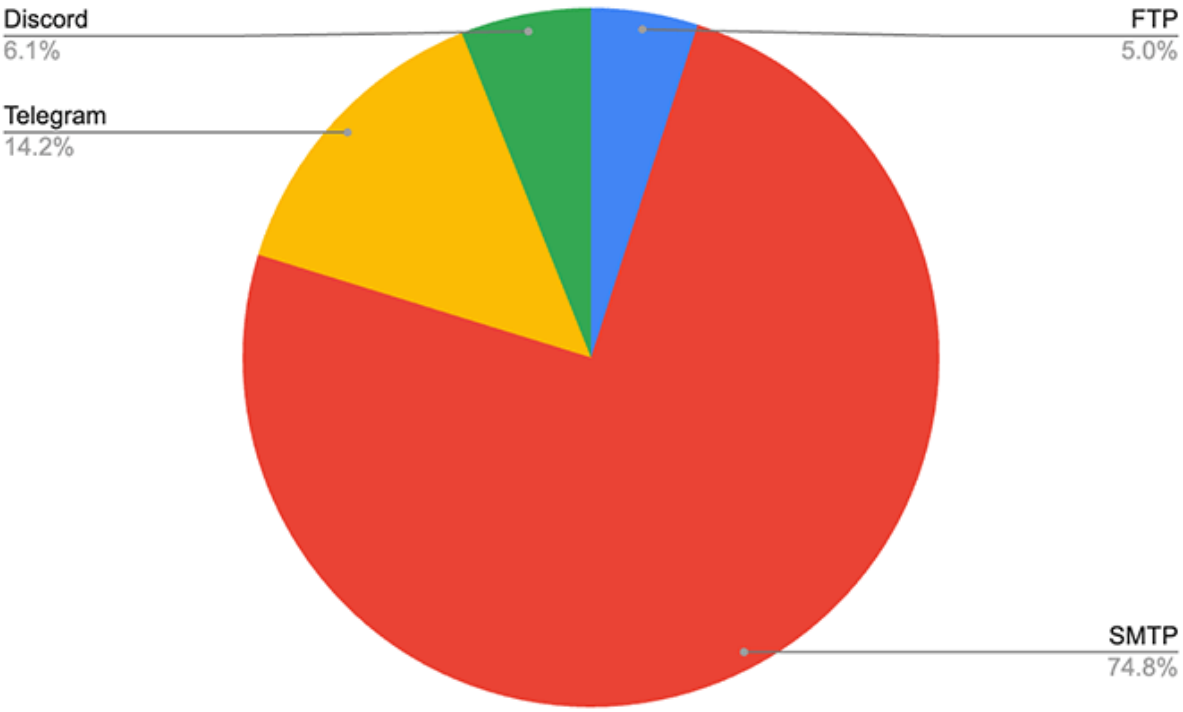

Fig. 2 - AgentTesla exfiltration methods by number of configs.

For the past 3 months, Bitsight identified more than 1500 AgentTesla configurations (which can be roughly translated to campaigns), extracted from samples originating from several diverse sources, including spam campaigns. About 75% of these configurations primarily utilize email accounts for data exfiltration, although the use of the Telegram API holds a significant share, around 14% (Fig. 2). The last observation of a configuration using HTTP exfiltration was in December 2022.

Exfiltrated Data Analysis

Bitsight obtained access to 3 months of victim data from about 210 campaigns of the malware. Between October and December 2023, at least 5300 computers were compromised. From those, we're also able to identify about 2000 IP addresses, which allow us to geographically map their location (Fig. 3) – although these IPs are only OriginLogger victims since IP grabbing functionality was not available in AgentTesla (older versions). The available visibility over infected systems suggests that the most targeted country is by far the United States, followed by China and Germany.

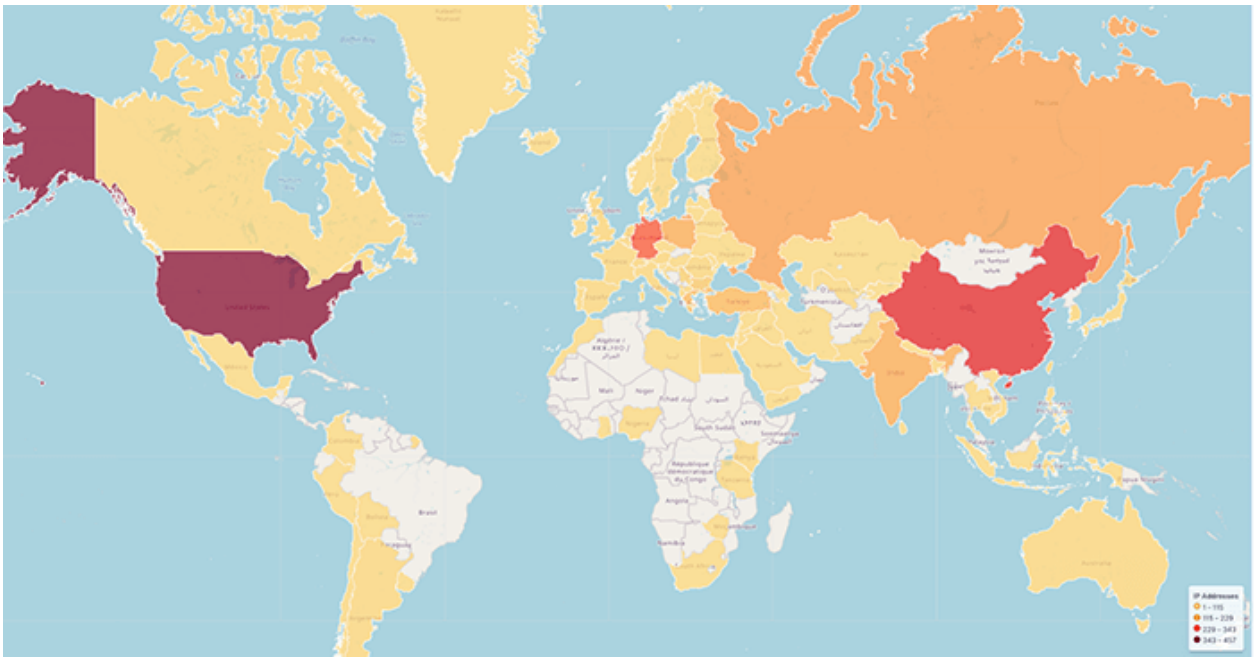

Fig. 3 - Geographic distribution of victims (38% of observed victims).

When looking at the types of data exfiltrated by AgentTesla, passwords were the most commonly collected, with almost all campaigns aiming to harvest it, as figure 4 shows.

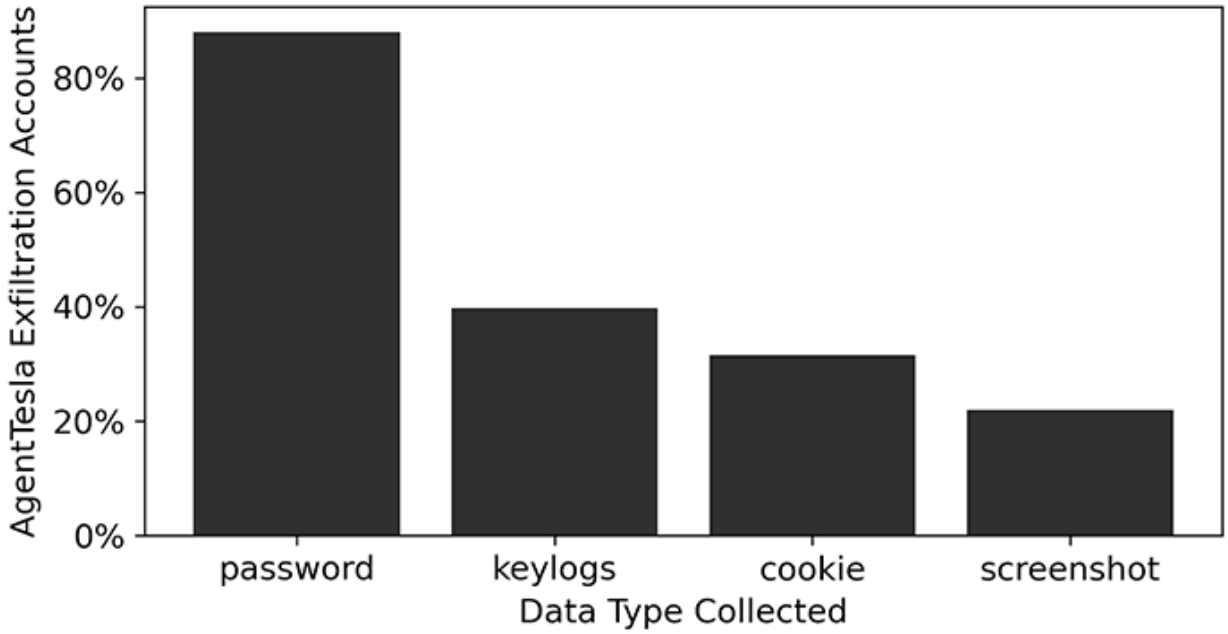

Fig. 4 - Types of data most collected by percentage of active AgentTesla exfiltration accounts.

Figure 5 depicts a word cloud of the top domains for stolen credentials. The results are consistent with expectations given the geographical distribution of infections since the majority are from US companies, some are Chinese, such as qq.com and 163.com, and there are also Russian, Turkish and Greek companies, including government entities.

Fig. 5 - Top domains by number of victim

However, this domain data reveals more the nationality of the victims rather than the country where their computer is connected from. When we look at the most common country top level domains (ccTLD), this data point presents a view (Fig. 6) quite different from the world map view of victims location (Fig. 3), where it suggests that most victims have most likely ties with European countries (Turkey, Italy, Russia, Poland, Greece, Romania, Germany and Spain)

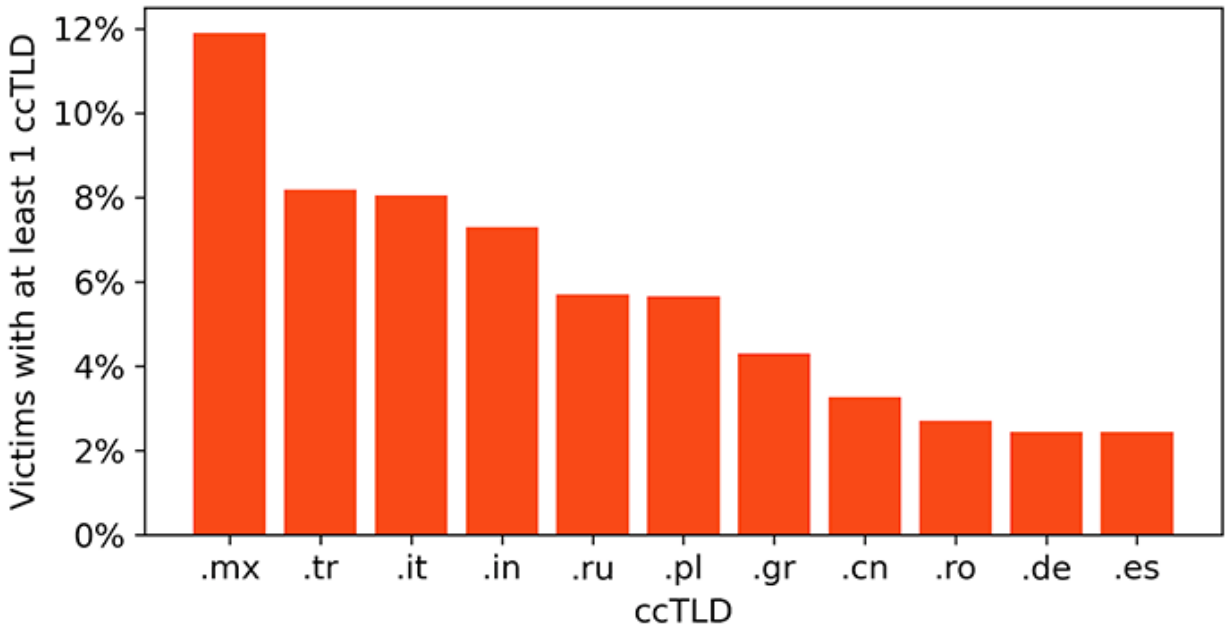

Fig. 6 - Top ccTLDs by percentage of victims with at least 1 credential with ccTLD.

Logs exploitation

When all the mentioned data, also referred to as “logs” in the cybercriminal world, is collected by a financially motivated threat actor, it’s either exploited or sold for further exploitation. For direct exploitation, threat actors generally use authentication information (cookie or password credentials) to transfer money, cryptocurrencies or any other valuable asset from the victims’ accounts to their own. Beyond direct exploitation, these actors use the acquired data for other profit-driven schemes, such as ransomware attacks – often resulting in data breaches, as in the Uber’s case – and business email compromise (BEC) attacks. The latter involves cybercriminals manipulating or impersonating trusted individuals within a company via email to deceive employees into taking actions that compromise security or financial integrity. For instance, the threat actor intercepts an email between two parties involved in a transaction and modifies financial documents to direct funds to their bank accounts. As a matter of fact, AgentTesla malware has been utilized by a syndicate of Nigerian fraudsters to reroute financial transactions from corporate organizations, including oil and gas companies in South East Asia, the Middle East and North Africa.

Wrap-up

In conclusion, AgentTesla, a Windows malware operating under a Malware as a Service model, has proven to be a persistent threat since 2014. Its rebranding as OriginLogger and widespread campaigns highlight its adaptability and pervasiveness. Recent data analysis reveals thousands of victims, primarily in the United States, China, and Germany, with vast amounts of credentials exfiltrated. The stolen data not only poses a direct financial threat but also fuels ransomware and business email compromise attacks. In the landscape of evolving cyber threats, while addressing the threat posed by malware as a service models is an important part of securing digital environments, it's also important to complement efforts against these specific threats with a comprehensive cybersecurity strategy. This strategy should encompass a multi-layered defense approach, proactive threat detection, employee awareness programs, and continuous adaptation to effectively be defended against a spectrum of cyber risks.

Detection

File/Memory detection rules (YARA):
https://github.com/kevoreilly/CAPEv2/blob/master/data/yara/CAPE/AgentTesla.yar

Samples: https://bazaar.abuse.ch/browse/signature/AgentTesla/