# The Rise of Agent Tesla: Understanding the Notorious Keylogger

Archived: 2026-04-05 19:14:51 UTC

By: James Arndt

## What is Agent Telsa?

Agent Tesla is a keylogger written in .NET. It can monitor keystrokes, take screenshots, steal passwords from a variety of applications, and exfiltrate this data back to the threat actor through common protocols. Though it has been regularly used by threat actors over the past eight years, its usage soared in late 2020 and early 2021. Due to the relatively low price compared to other malware families and the high functionality it possesses, we have no reason to believe it will be going away any time soon.

## The History of Agent Tesla

Agent Tesla first appeared in 2014 and has been a staple in the malware landscape ever since. This keylogger was originally advertised on a Turkish website as a remote access tool to monitor your own personal computer. It could compile your personal passwords, monitor your keystrokes, and avoid being caught by your endpoint's anti-virus.

As early as 2016, Agent Tesla's (now defunct) website started offering a tiered support structure for customers.

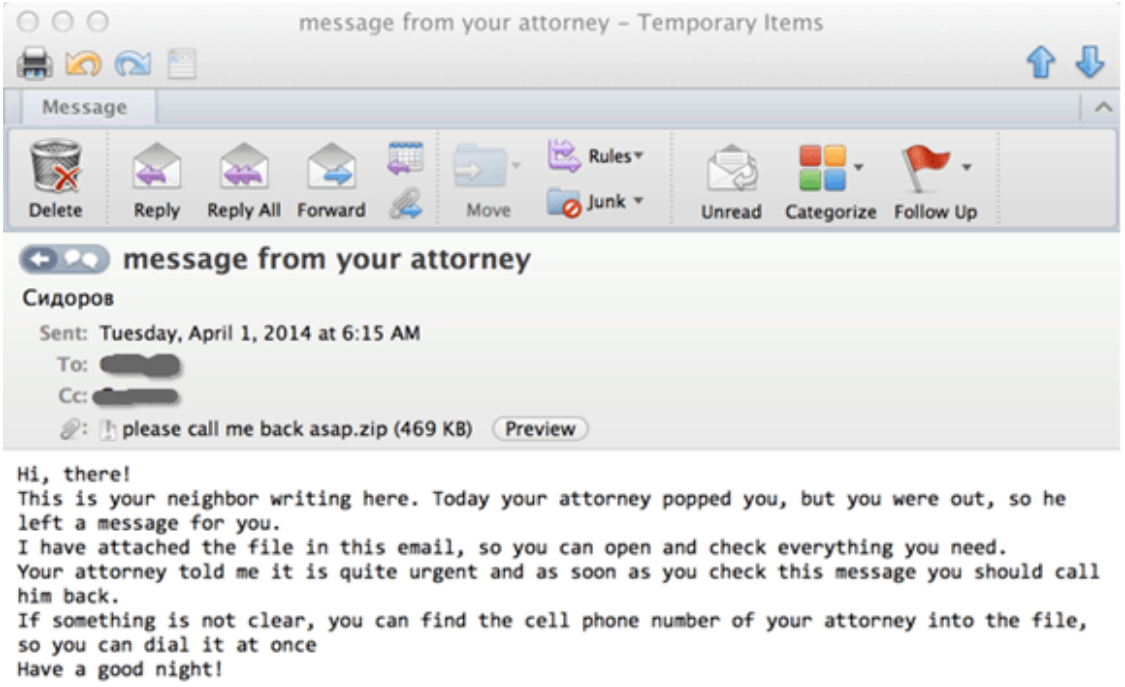


*Figure 1: Tiered support offerings in 2017.*

The website also hosted web panels for customers to access the data sent from infected endpoints. The people behind the website had to stop hosting the Web Panel service in September of 2016 due to legal issues and

CloudFlare banning their IP addresses. Customers were then given the files needed to host their own Web Panels.

Agent Tesla has gone through a variety of upgrades over the years. Besides changes intended to ensure that every new release can bypass anti-virus scans, it now advertises the ability to steal credentials from over 55 applications including web browsers, VPN applications, FTP applications, and mail clients. It has also continually improved its ability to circumvent or avoid sandbox technologies. While at first it only used SMTP to communicate back to the attacker, it now also supports communication over HTTP, FTP, and Telegram.

## Notable Uses

Agent Tesla Keylogger was originally sold as a remote access tool, and it could be argued that it functions no differently from legitimate remote access tools like GoToMyPC or LogMeIn. However, U.S. federal prosecutors have argued when someone is selling a tool and instructs users how to "install the product in ways that are arguably deceptive (such as through the use of software exploits, spam, or disguising the tool as another program), the proprietor has crossed the legal line and can be criminally prosecuted under computer misuse laws."(https://krebsonsecurity.com/2018/10/who-is-agent-tesla/). Similar remote access tools have been sold in this manner and the sellers have been prosecuted and sent to prison.

In March 2020, during the beginning of worldwide lockdowns due to COVID-19, threat actors used COVID-19-themed phishing lures to spread Agent Tesla Keylogger. Its popularity surged in the third and fourth quarters of 2020 and the first two quarters of 2021. Office documents with macros and malicious .rtf documents exploiting CVE-2017-11882 were often used to download and execute Agent Tesla Keylogger.

## File-Originating Delivery and Exfiltration Methods

As shown in Figure 2, an Agent Tesla Keylogger executable is typically delivered via a direct attachment to an email. The CVE-2017-11882 vulnerability, attached DotNET Loaders, and embedded URLs follow as popular delivery methods. The chief exfiltration method over the past year remains SMTP. Telegram traffic is a popular choice as well.

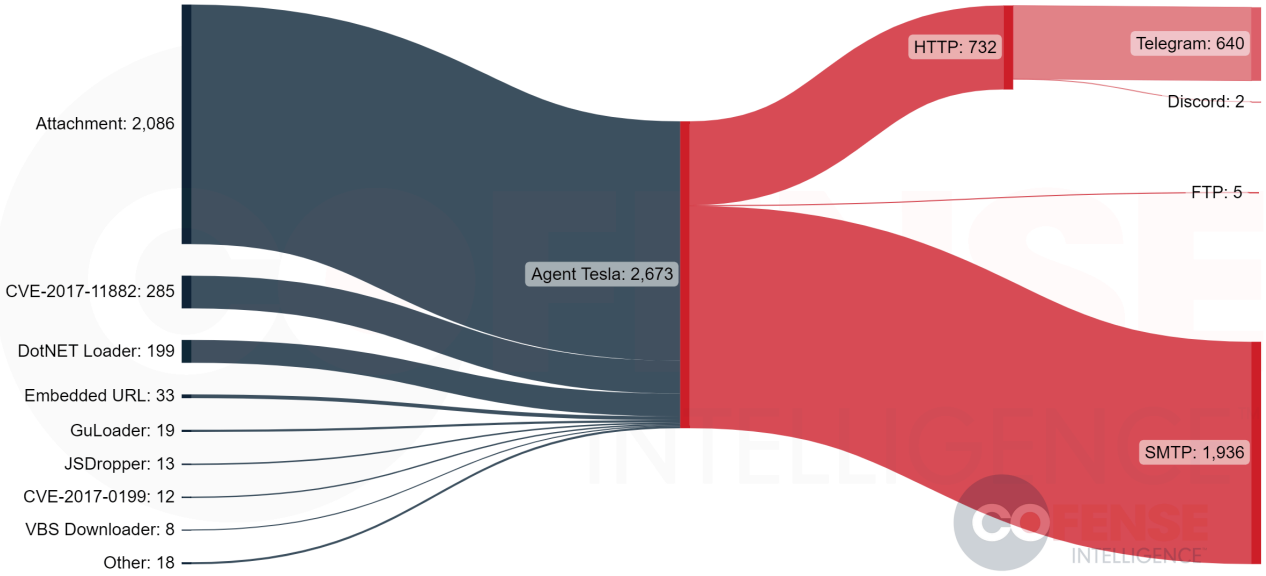


*Figure 2: Agent Tesla's most common delivery mechanisms and exfiltration methods in 2022.*

## Capabilities

The Agent Tesla builder has allowed for a variety of configurations. Early versions only allowed exfiltration via SMTP, but exfiltration was expanded to both SMTP and FTP in 2017. Current versions have added HTTP and Telegram exfiltration. Figure 3 shows the progression of these exfiltration capabilities as advertised by the authors between 2016 and 2017.

*Figure 3: Agent Tesla exfiltration options from 2016 and 2017.*

The ‘password recovery’ feature has expanded significantly from its early iterations. Figure 4 shows two examples of the builder from 2016 and 2017. Agent Tesla Keylogger currently attempts to harvest and exfiltrate passwords from over 55 applications.

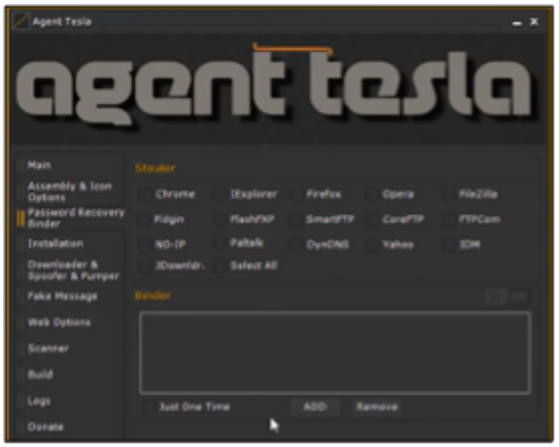


*Figure 4: Expansion of password recovery options from 2016 and 2017 respectively.*

Figure 5 shows how the web panel in 2019 displayed exfiltrated data to the attacker.

```
remnux@remnux:~$ httpd start
Starting web server: thttpd.
remnux@remnux:~$ fakedns
pyminifakeDNS:: dom.query. 60 IN A 172.16.80.128
```

*Figure 5: Web panel from 2019 showing keystrokes that were sent back to the attacker.*

## In The Wild

Agent Tesla Keylogger accounts for about 20% to 30% of the malware-based Active Threat Reports

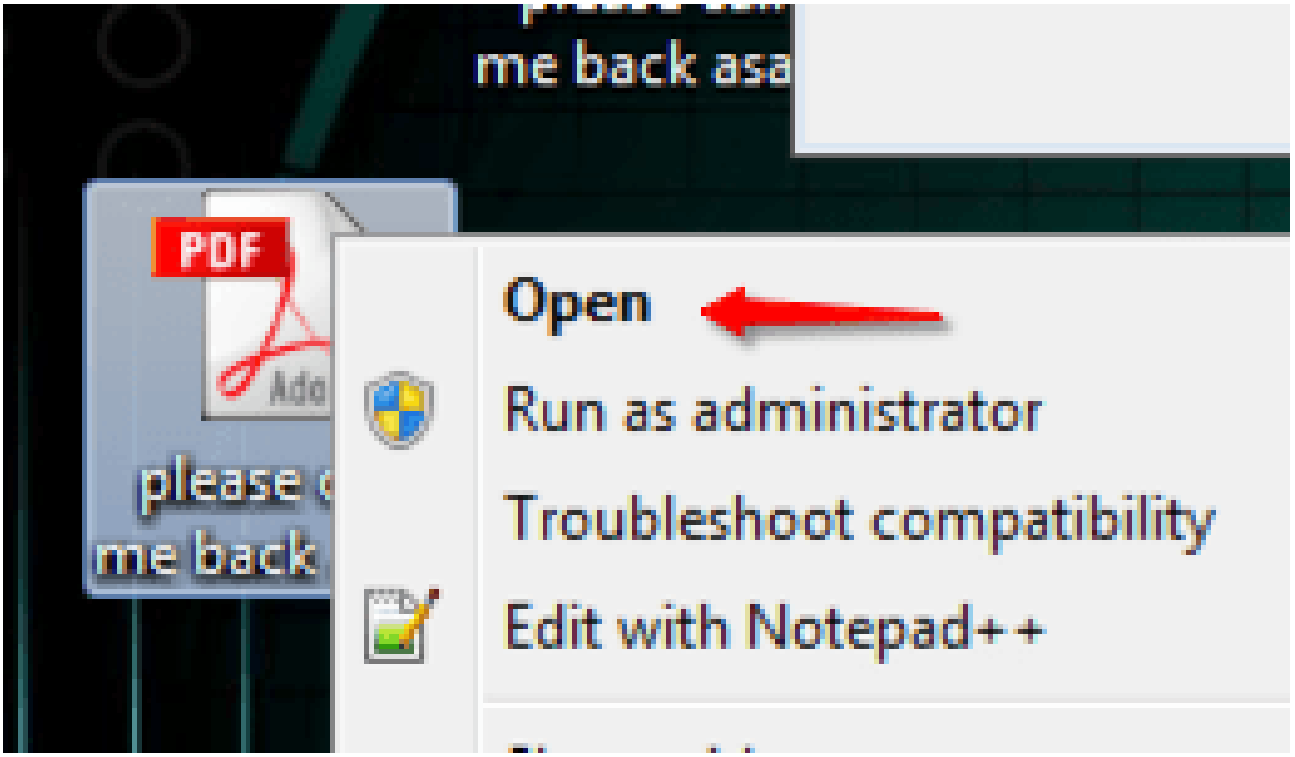

*Figure 6: Agent Tesla Keylogger reports over the past year as a percentage of total malware-based reports seen by Cofense Intelligence.*

## Behavior

Stage one of an Agent Tesla Keylogger infection typically begins with either a packed PE file or one that has been written in .NET. In either case, the first step is to unpack or decode a large chunk of data before stage two can be executed. Figure 7 below is an example of the PE file being written in .NET. The resource *String1* contains a long string of characters. The code replaces certain characters with others and stores the result in an array. This array becomes the second stage of the infection process when it is executed.

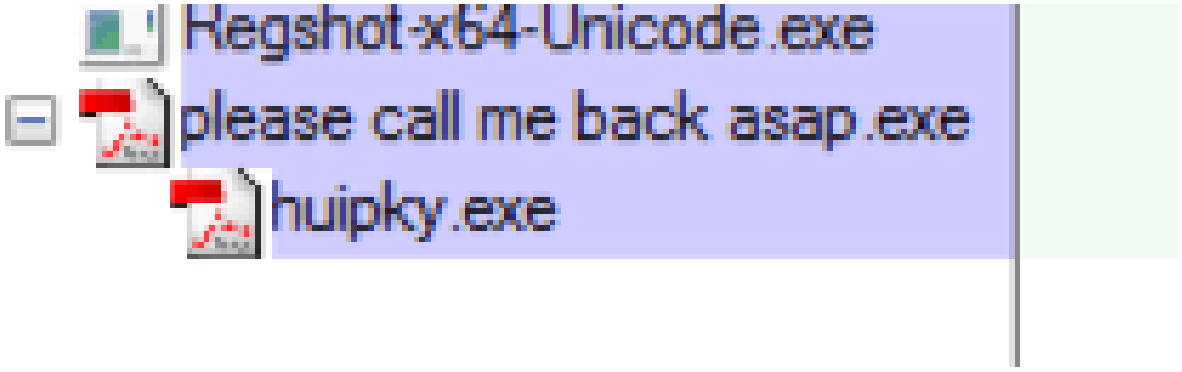


*Figure 7: .NET executable replacing characters to create and execute the second stage.*

Once the second stage is running, it performs some basic checks to see if it is running in a debugger, to determine whether it is being scrutinized by a security analyst. If it determines that it is not being analyzed, it then gathers information about the infected endpoint, such as the MAC address, processor information, and motherboard serial number. This information is sent back to the attacker. Based upon how it was originally configured (Figure 3), Agent Tesla will start monitoring keystrokes, check for the existence of applications from which to steal passwords, and exfiltrate screenshots at regular intervals.

The more recent versions of Agent Tesla Keylogger rely heavily on a large byte array (Figure 8) for functionality. References to this byte array are seen throughout the second stage. Rather than items like registry keys and file paths being in plain text, the code will select certain bytes from this array and decode them on the fly as they are needed.

```
internal static byte[] <<EMPTY_NAME>> = new byte[]
{
    144, 139, 148, 203, 144, 244, 140, 145, 141, 193,
    158, 129, 154, 197, 154, 248, 134, 148, 218, 135,
    158, 151, 149, 251, 211, 223, 195, 212, 205, 245,
    245, 246, 193, 246, 243, 200, 194, 219, 167, 217,
    195, 193, 253, 250, 199, 203, 208, 174, 220, 175,
    229, 226, 202, 222, 222, 224, 233, 214, 195, 210,
    235, 236, 195, 252, 132, 150, 147, 170, 175, 191,
    191, 161, 173, 160, 171, 156, 192, 146, 133, 151,
```

*Figure 2: The beginning of the encoded byte array.*

For example, Figure 9 below shows part of a function which exfiltrates data via FTP. The value for the *ftpWebRequest.Method* can be found inside the encoded byte array. The function is instructed to start at the 1336th byte and select the next four bytes. Those bytes are decoded to produce the string “STOR”, a command used by the FTP protocol to upload files to a remote server.


*Figure 3: Example of the decoding function.*

By decoding the entire byte array in the same way, we can see a variety of commands, registry settings, URLs, and targeted applications that will be used by the Agent Tesla Keylogger in some way.


*Figure 4: Decoded strings reveal a Telegram URL, registry keys, and application paths.*

## Detection and Hunting

Phishing emails that deliver Agent Tesla through both attachments and links have been seen reaching enterprise users in environments protected by some of the leading secure email gateways (SEGs). However, Agent Tesla Keylogger's behavior on an endpoint should be detectable by modern endpoint security suites and network activity.

### Network Traffic

Agent Tesla can exfiltrate data via FTP, SMTP, HTTP, and Telegram messaging. Opportunities for detection include monitoring outbound web traffic on port 20 or 21 (FTP) and port 25 or 587 (standard SMTP ports) from client devices to unknown servers. Since Telegram's popularity for exfiltration has risen over the past year, it may also be beneficial to monitor and/or create policies to regulate outbound traffic to api.telegram.org.

### Endpoint Activity

Identifying unusual network traffic may point to a certain endpoint for further investigation. Modern endpoint security suites should be able to tie network activity to its corresponding process. Investigate those unusual processes and their corresponding parent processes.

Figure 10 above showed evidence of how Agent Tesla Keylogger is using the *CurrentVersionRun* and *StartupApprovedRun* registry keys to establish persistence. Changes to those and other common registry keys used for malware persistence should be monitored.



---