The Hasty Agent: Agent Tesla Attack Uses Hastebin

By Bar BlockThreat Intelligence Researcher

Published: 2020-10-29 · Archived: 2026-04-05 16:21:55 UTC

Earlier this week, we stumbled across a new malware sample in one of our production sites, that caught our attention. During our analysis, we came to the conclusion that we were dealing with a new Agent Tesla variant, that is loaded from a pastebin service which hadn't been seen in use by prominent malware families in the past, "hastebin.com".

Background

Pastebins

A Pastebin is an online content storage site that allows users to store plain texts, from source codes to grocery lists. Paste sites have been around since the 1990s, when "pastebin.com" was founded, and have been in use ever since. Like with anything popular, malware authors chose to take advantage of these services to store their own data, such as source codes and stolen information. Different paste services sometimes operate differently from one another- some offer features like protecting pastes with passwords or "burning" them after they are read. Some offer APIs to make it easy to transfer code from a console into a paste site. Others enforce different policies regarding types of content that are not allowed, for example- stolen user credentials, and policies regarding pastes' "life expectancy", meaning for how long a paste page will stay up.

One of these services is "hastebin.com", a simple paste service, that can also work from a console using an API. Recently, this domain, which hasn't previously been known to host malware families, was observed by Deep Instinct's Threat Intelligence team to host new Agent Tesla payloads.

Agent Tesla

Agent Tesla is infamous spyware with extensive data harvesting and keylogging capabilities. It has been active since 2014 and is marketed in dark-web forums as a commercial project, to which subscription licenses can be bought on the malware's official website. Throughout the years, tweaks and changes have been made to maintain the malware's evasiveness from new security measurements and to help it remain one of the most common malware in the wild.

The New Sample

The Loader

Infection Vector

As with most malware campaigns, the attack most likely started with the attackers going phishing. One of the samples' names, which we found on its Virus Total page, was "PACKING LIST - TJ20070006 CHINA-pdf.exe". The name, the fact that many users don't turn off the default option "Hide extensions for known file types" and the

executable's logo (which appears to be a page from a document), all suggest that the sample was made to appear far more benign. In this case as a PDF that lists recommendations for packing supplies when traveling to China, and was probably accompanied by a suitable text when delivered to potential victims.

Loading the Payload

Once an unsuspecting user opens the file, it connects to pastes hosted on "hastebins.com", from which it gets the Agent Tesla payload, which it then runs. The loader also tries to connect to two "pastebin.com" paste pages, but they have been down since the beginning of the month because they were identified as malicious.

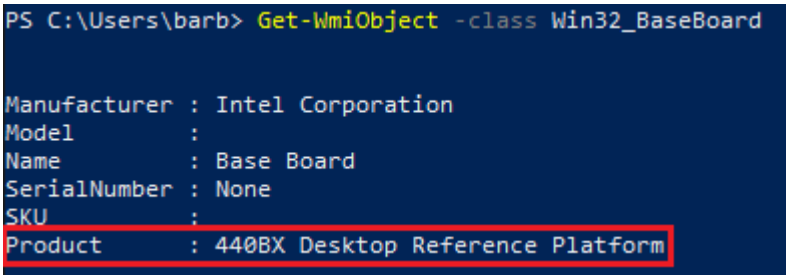
Once Agent Tesla is loaded and ready, the fun part begins.

The Payload

The malware uses a few copies of itself, as well as conhost, PowerShell, and Chrome to perform all its tasks. It even uses timeout.exe to time some of the activities.

Evasion Techniques

Unsurprisingly, one of the sample's first actions is to detect if it's running in a virtual environment. It does this with the use of WMI commands that help it query the system for network and BIOS details. For example, it uses Win32_BaseBoard to check if there's a VM related key. In the screenshot below, the product key's value is "440BX Desktop Reference Platform", which refers to a motherboard model used by VMware- "Intel Corporation 440BX Desktop Reference Platform".



Agent Tesla also checks for the presence of Wine APIs and the Sandboxie DLL "SBIEDLL.DLL". If the sample's suspicions are proven right- it will avoid performing any more malicious activities.

To keep protecting itself from analysis, even while running, the spyware hides its threads from the debugger. It also uses PowerShell to prevent the loader from being scanned by Windows Defender, using the command "Add-MpPreference". The malware also uses the parameter 'Force', as can be seen below, to avoid prompting a warning that the user needs to sign off on in order to add the exclusion.

```
C:\Users\bar.b>'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\
AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\qsavjmf9A0.exe' -Force
```

Persistence

If the malicious logic concludes that it isn't being analyzed, it ensures the loader's persistence by copying it ("qsavjmf9A0.exe") into the startup folder "C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup" and adding it to the uncommonly used registry key "HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\shell". The payload also creates two keys under "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run" – "<Unknown>" and "qsavjmf9A0.exe", both, as well as the previously mentioned key, point to the sample's initial location, e.g. "C:\Users\username\Downloads".

Credential Harvesting

Its persistence and evasion are nice features, but the point of the infection is stealing data, which is what this spyware is all about. The sample tries to harvest credentials from web browsers, specifically from their cookies and login files, for example- "C:\Users\username\AppData\Local\Google\Chrome\User Data\Default\Login Data" and "C:\Users\username\AppData\Roaming\Mozilla\Firefox\Profiles\qkye9m34.default\cookies.sqlite".

It also tries to steal mail credentials from services like "Microsoft Outlook", "Thunderbird" and even the recently shutdown "IncrediMail". The attempts take place both in the file system and in the registry. If that wasn't enough, the greedy malware also tries to obtain WinSCP session credentials from "HKEY_CURRENT_USER\SOFTWARE\Martin Prikryl\WinSCP 2\Sessions" and installs a keyboard hook to capture keystrokes.

The gathered loot is sent via SMTP (port 857) to "smtp.privateemail.com", which translates into "199.193.7.228".

The Use of "hastebin.com"

As mentioned earlier, the Agent Tesla payload is loaded from "hastebin.com". This provides the malware capabilities that otherwise may have been more difficult to implement. The use of a remote payload may decrease the chances of the malware being caught by certain security products, which will perform a static analysis only on the loader, that doesn't have many malicious capabilities of its own. Moreover, "hastebin.com" provides an easy-to-use API, that lets attackers post their malware from the comfort of their own console and since it's less popular among malware families- it may be deemed as less suspicious.

The service is also less supervised than other paste sites, like "pastebin.com", which has a security team that works to detect malicious pastes and take them down. The Agent Tesla sample, mentioned earlier, was taken down by this team.

"hastebin.com" has been up for over eight years, but in July 2019, its popularity increased to 300 hits a day, predominantly, but not exclusively, from the US. Other hits came from various countries, including the UK, India, Germany and Spain.

Conclusion

If a prominent malware family such as Agent Tesla is hosted on and deployed from “hastebin.com”, others may follow suit and do the same, especially since the service is easy to use and offers some advantages.

Deep Instinct’s customers are protected from Agent Tesla thanks to our product’s deep learning-based protection.

IoCs

The Analyzed Loader- SHA256

01fa75f6d9aace12a225c5cb93c306b22968f6ba44a431595fbee38cab275179

Similar Samples- SHA256

2adb3505038e73bc83e5c5d9a60b725645fb65a7b0a781a5aadde50c942d13dc

378911a0ffd090bc26b1bb981abe1c5bb8dec098e3138ef0b9a7f1ce88747fbd

d5bb27d8c7efd36c62458d3dfca74de7c517108e32bf8c1bc68c8152a351003f

“hastebin.com” Contacted Pastes

https://hastebin[.]com/raw/edutecikus

https://hastebin[.]com/raw/esoqaxeqag

https://hastebin[.]com/raw/noqivebupe

The SMTP Domain and IP

smtp[.]privateemail[.]com

199.193.7.228
