



CRIMEWARE ([HTTPS://WWW.SENTINELONE.COM/LABS/CATEGORY/CRIMEWARE/](https://www.sentinelone.com/labs/category/crimeware/))

## Agent Tesla | Old RAT Uses New Tricks to Stay on Top

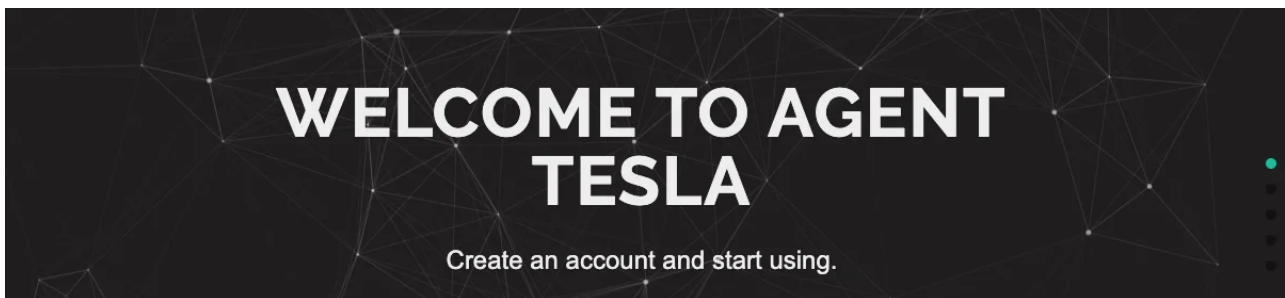
JIM WALTER ([HTTPS://WWW.SENTINELONE.COM/BLOG/AUTHOR/JIMW/](https://www.sentinelone.com/blog/author/jimw/)) / AUGUST 10, 2020  
([HTTPS://WWW.SENTINELONE.COM/BLOG/2020/08/](https://www.sentinelone.com/blog/2020/08/))

As other researchers have recently noted

(<https://blog.checkpoint.com/2020/05/11/april-2020s-most-wanted-malware-agent-tesla-remote-access-trojan-spreading-widely-in-covid-19-related-spam-campaigns/>), the Agent Tesla RAT (Remote Access Trojan) has become one of the most prevalent malware families threatening enterprises in the first half of 2020, being seen in more attacks than even TrickBot or Emotet and only slightly fewer than Dridex. Although the Agent Tesla RAT has been around for at least 6 years, it continues to adapt and evolve, defeating many organizations' security efforts. During the COVID-19 pandemic new variants have been introduced with added functionality, and the malware has been widely used in Coronavirus-themed phishing campaigns.

(<https://www.sentinelone.com/labs/>).

2014, there has been steady growth in the use of Agent Tesla over the last 1-2 years. The malware was initially sold in various underground forums and marketplaces, as well as its very own AgentTesla.com site (now defunct) Agent Tesla, like many of its contemporaries, offered both the malware itself as well a management panel for administration and data collection and management. Information harvested from infected devices quickly becomes available for the attacker via the panel interface.



When originally launched, various ‘packages’ were available for purchase. Each package was basically differentiated by the license duration and build/update access. At the time, pricing was quite competitive with a 1 month license selling for \$12.00 USD all the way up to 6 month licenses going for \$35.00. It is also worth noting that, like many other tools of this nature, cracked and leaked versions of Agent Tesla were quick to appear.

Early versions of Agent Tesla also touted the full suite of features as one would expect to find in a modern RAT, including:

- Multi Language Support
- PHP Web Panel
- Automatic Activation upon payment (for direct customers)
- 24/7 support
- Stable and Fast execution
- Multiple delivery methods for keystroke logs, screenshots, and clipboard pulls
- Support for multiple Windows versions (XP upward)

BRONZE

\$12

1 Month License  
7/24 Support  
Web Panel  
Advanced Keylogger  
FUD Crypter  
doc/xls Converter  
1 Month Updates  
1 Month Builds

Payment Method:  
Perfect Money

Buy Now

SILVER

\$25

3 Month License  
7/24 Support  
Web Panel  
Advanced Keylogger  
FUD Crypter  
doc/xls Converter  
3 Months Updates  
3 Months Builds

Payment Method:  
Perfect Money

Buy Now

GOLD

\$35

6 Month License  
7/24 Support  
Web Panel  
Advanced Keylogger  
FUD Crypter  
doc/xls Converter  
6 Months Updates  
6 Months Builds

Payment Method:  
Perfect Money

Buy Now

## CONTACT US

Still have Questions? Contact Us using the Form below.

## Delivery Mechanism

Like many other threats, the primary delivery mechanism for Agent Tesla is email (phishing messages). Attackers are often timely with their social engineering lures, and the current pandemic is not off limits to the attackers. In the last few months, attackers have been observed spreading Agent Tesla via COVID-themed messages, often masquerading as information information or updates from the WHO (World Health Organization)

(<https://www.sentinelone.com/labs/>)

```
Date: [REDACTED]
From: "WORLD HEALTH ORGANIZATION (WHO)" <healthcaresupport@who.int>
To: [REDACTED]

Subject: URGENT INFORMATION LETTER: FIRST HUMAN COVID-19 VACCINE
TEST/RESULT
UPDATE

FIRST HUMAN COVID-19 VACCINE TEST / RESULT UPDATE .doc 35 KB
Download All Attachment for Vaccine Update (in .iso file) Download All
Attachment for Vaccine Update (in .iso file)

RELATED

* Novel coronavirus (2019-nCoV) outbreak [1]
* Situation reports [2]
* Travel advice [3]
* Protect yourself [4]
* Myth-busters [5]

MEDIA CONTACTS

Tarik Jasarevic

Spokesperson / Media Relations
WHO

EMAIL: jasarevic@who.int

Christian Lindmeier
```

Actors behind Agent Tesla campaigns have also used malicious Office documents to facilitate first-stage delivery. Specially-crafted documents, exploiting Office vulnerabilities such as CVE-2017-11882 (<https://nvd.nist.gov/vuln/detail/CVE-2017-11882>) and CVE-2017-8570 (<https://nvd.nist.gov/vuln/detail/CVE-2017-8570>), have been leveraged, even in present day campaigns. These and similar exploits allow for quick delivery and execution with minimal user interaction (beyond opening the malicious documents and allowing active content to proceed)

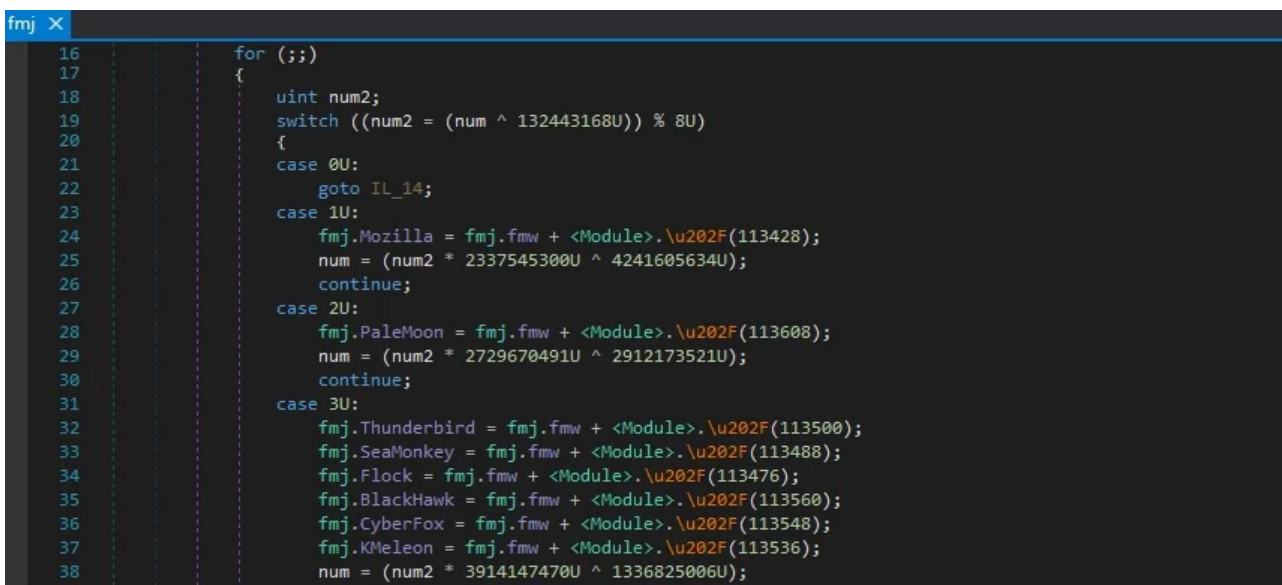
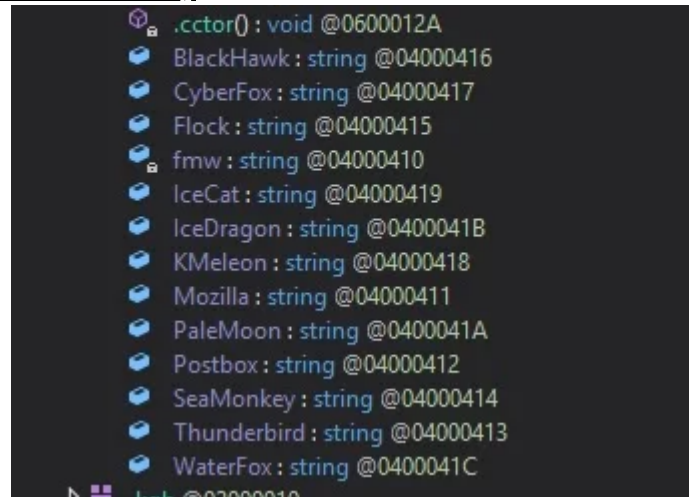
## Feature Set of New Agent Tesla Variants

Over time, additional features have been added to Agent Tesla. These improvements include more robust spreading and injection methods as well as discovery and theft of wireless network details and credentials.

Currently, Agent Tesla continues to be utilized in various stages of attacks. Its capability to persistently manage and manipulate victims' devices is still attractive to low-level criminals. Agent Tesla is now able to harvest configuration data and credentials from a number of common VPN clients, FTP and Email clients, and Web Browsers. The malware has the ability to extract credentials from the registry as well as related configuration or support files. Our analysis of a swatch of current Agent Tesla samples reveals the

# LABS

(<https://www.sentinelone.com/labs/>)



- 360 Browser
- Apple Safari
- Becky! Internet Mail
- BlackHawk
- Brave
- CentBrowser
- CFTP
- Chedot
- Chromium (general)
- Citrio
- Claws Mail
- Coccoc

# LABS

(<https://www.sentinelone.com/labs/>).

- ~~CyberFox~~
- Elements
- Epic Privacy
- FileZilla
- FlashFXP
- Flock
- Google Chrome
- IceCat
- IceDragon
- IncrediMail
- Iridium
- KMeleon
- Kometa
- Liebao
- Microsoft IE & Edge
- Microsoft Outlook
- Mozilla Firefox
- Mozilla Thunderbird
- OpenVPN
- Opera
- Opera Mail
- Orbitum
- PaleMoon
- Postbox
- QIP Surf
- Qualcomm Eudora
- SeaMonkey
- Sleipnir 6
- SmartFTP
- Sputnik
- Tencent OOBrowser

(<https://www.sentinelone.com/labs/>).

- Titan Messenger

- UCBrowser
- Uran
- Vivaldi
- WaterFox
- WinSCP
- Yandex

Harvested data is transmitted to the C2 via SMTP or FTP. The transfer method is dictated per the malware's internal configuration, which also includes credentials (FTP or SMTP) for the attacker's C2.

Current variants will often drop or retrieve secondary executables to inject into, or they will attempt to inject into known (and vulnerable) binaries already present on targeted hosts.

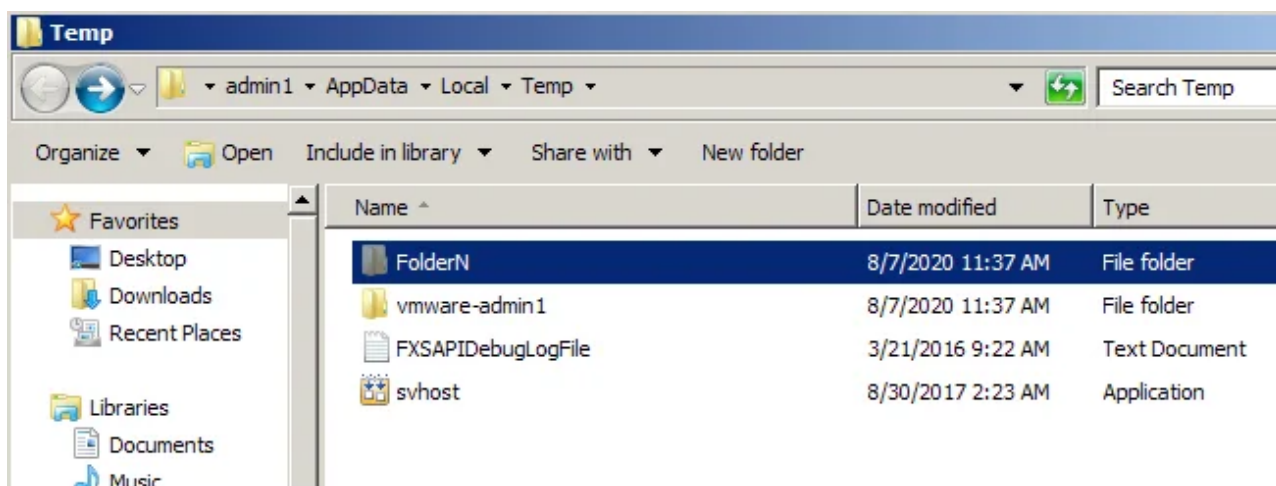
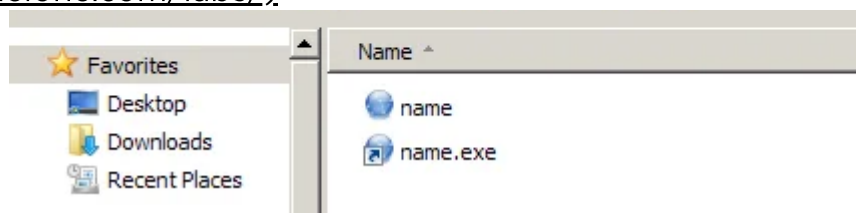
For example, as we see in sample

4007480b1a8859415bc011e4981f49ce2ff7a7dd7e883fe70d9f304cbfefedea , a copy of RegAsm.exe (dropped into %temp%) is subsequently injected into. That new instance of RegAsm.exe is then responsible for handling the brunt of the malicious activity (data harvesting, exfiltration). We can also see frequent use of 'Process Hollowing (<https://attack.mitre.org/techniques/T1055/012/>)' as an injection method. Process Hollowing allows for the creation or manipulation of processes through which sections of memory are unmapped (hollowed) with that space then being reallocated with the desired malicious code.

Some examples get a little less creative with regards to process creation and subsequent injection. For example, in sample

b74bcc77983d587207c127129cfda146644f6a4078e9306f47ab665a86f4ad13 , we can observe it creating hidden folders and processes in %temp%, and using those hidden process instances for the primary infection routines, and as the persistent process (set via Registry)





## Execution Behavior

Upon launch, the malware will begin to gather local system information, install the keylogger module, as well as initializing routines for discovering and harvesting data. Part of this process includes basic WMI queries. Examples include:

```
start iwbemservices::execquery - select * from win32_operatingsystem
```

```
start iwbemservices::execquery - select * from win32_processor
```

Recent samples, with the ability to discover wireless network settings and credentials will spawn an instance of netsh.exe after a brief sleeping period (after launch). The syntax utilized initially is:

```
Netsh.exe wlan show profile
```

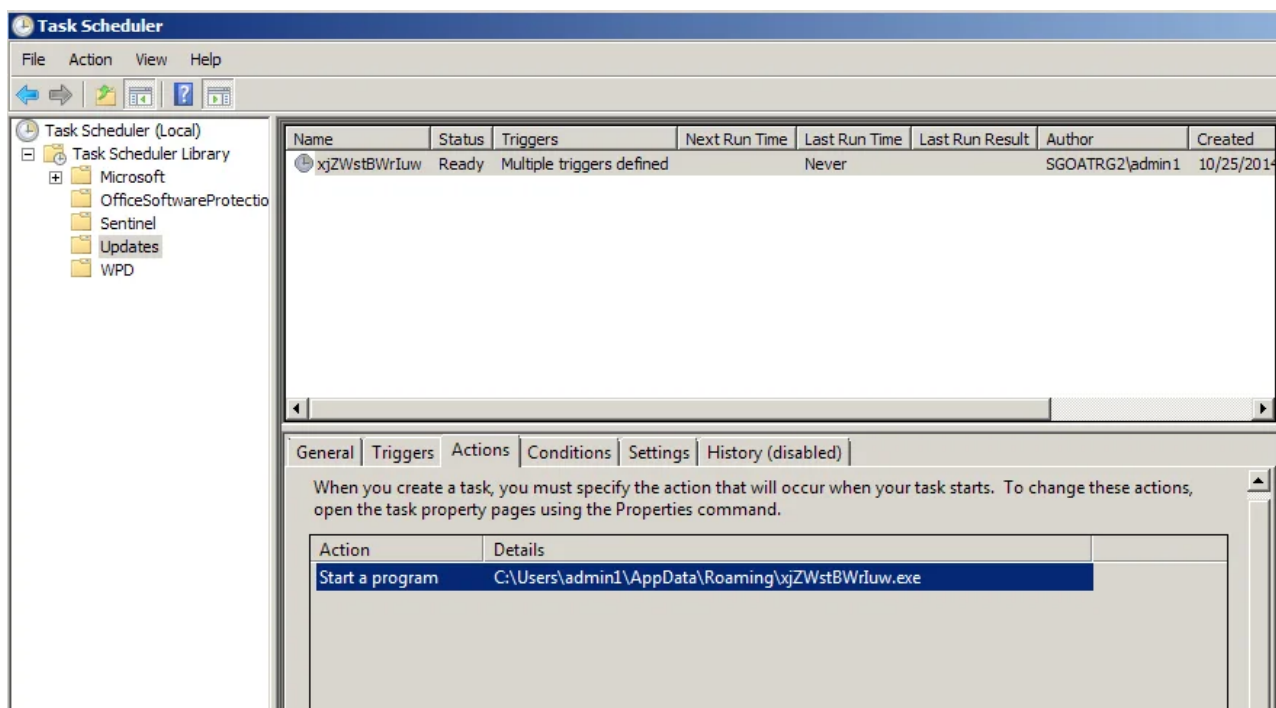
Persistence is typically achieved via registry key entry or scheduled task.



(<https://www.sentinelone.com/labs/>)

executable file is dropped into ~AppDataLocal\temp, and targeted w/ the following syntax to generate the persistent task:

```
Schtasks.exe /Create /TN "UpdatesxjZWstBWrIuw" /XML C:\Users\xxxxxxx\AppData\Local\Temp\UpdatesxjZWstBWrIuw.xml
```



In the sample `b74bcc77983d587207c127129cfda146644f6a4078e9306f47ab665a86f4ad13`, we see an example of establishing persistence via the registry. Upon launch, an instance of the malware is dropped into %temp% as a hidden file, in a hidden folder.

```
/c copy "C:/Users/admin1/Desktop/tes_10.exe" "%temp%\FolderName.exe" /Y
```

The following command is then used to create the Autorun registry key:

```
/c reg add "HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows" /v Load /t REG_SZ /d "C:\Users\admin1\AppData\Roaming\xjZWstBWrIuw.exe"
```

## Conclusion

Agent Tesla has been around for several years now, and yet we still see it utilized as a commodity in many low-to-mildly sophisticated attacks. Attackers are continually evolving and finding new ways to use tools like Agent Tesla successfully while evading detection. For more information, visit <https://twitter.com/LabsSentinel> or <https://www.linkedin.com/company/sentinelone>.

(<https://www.sentinelone.com/labs/>)

engineering tires, these non-sophisticated attacks continue to be successful. Detection and prevention are key to reducing exposure to these threats. The SentinelOne platform (<https://www.youtube.com/watch?v=mhJGzfzymME&feature=youtu.be>) is fully capable of detecting and preventing Agent Tesla-based malware campaigns.

## Indicators & IOCs

### MITRE ATT&CK

Modify Registry (T1112 (<https://attack.mitre.org/techniques/T1112/>))

Subvert Trust Controls: Install Root Certificate (T1553.004

(<https://attack.mitre.org/techniques/T1055/012/>))

Hide Artifacts: NTFS File Attributes (T1564.004

(<https://attack.mitre.org/techniques/T1564/004/>))

Hijack Execution Flow: DLL Search Order Hijacking (T1574.001

(<https://attack.mitre.org/techniques/T1574/001/>))

Process Injection: Process Hollowing (T1055.012

(<https://attack.mitre.org/techniques/T1055/012/>))

Data from Information Repositories (T1213

(<https://attack.mitre.org/techniques/T1213/>))

Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001

(<https://attack.mitre.org/techniques/T1547/001/>))

Process Injection (T1055 (<https://attack.mitre.org/techniques/T1055/>))

Unsecured Credentials: Credentials In Files (T1552.001

(<https://attack.mitre.org/techniques/T1552/001/>))

System Information Discovery (T1082 (<https://attack.mitre.org/techniques/T1082/>))

Query Registry (T1012 (<https://attack.mitre.org/techniques/T1012/>))

OS Credential Dumping (T1003 (<https://attack.mitre.org/techniques/T1003/>))

Scheduled Task (T1053 (<https://attack.mitre.org/techniques/T1053/>))

### SHA256

70aecc29ffb60caf068e4d8107f4d53fcdbd333bed7ac6fb3a852b00e86ded31

7d1bcec8a3f71910e15cbb3adae945cd5096b7de259b51aef8f2e229hd4b40e2

<https://twitter.com/LabsSentinel>) **in**(<https://www.linkedin.com/company/sentinelone>)

# LABS

(<https://www.sentinelone.com/labs/>)

a040e1a15d1ac0b5505105ea0da70a1305070da000100a130ea/00047102/4123  
aa08d96a25908ce76e07475aefbbe192bd812665a5600dc30600688510dd033e  
be26ad023b732078c42b4f95067fb9107fe88aebd7ebbf852e7e968e50eee8a0  
1abf66ab839c550bc77d97d1644c1225935a86b9591e9a95bcd606ebec6bbc19  
b74bcc77983d587207c127129cfda146644f6a4078e9306f47ab665a86f4ad13  
f44c6c8c1c81f9990f11a0f70e6517c358fc1ee00a78b32461d4a2594b48e47d  
9fee57918672137160499dcd1a099670ef8f9a787f3a1ad6d8123df26cddbc3b  
4007480b1a8859415bc011e4981f49ce2ff7a7dd7e883fe70d9f304cbfefedea  
590c19542f6959d6424107eb4f2998b04d035575341b1f23a40dea6d82aecadd  
648261052662b044dc233349ccdfa9dfd6853ec9a21ced386f8f172b2568b0d1  
f24018dead69b0f899d33e73f72f5c3ef6f3c391850484b06b042f36dbc08cac  
7ce7bf11f6285621381b80027c488e9b5009205131a89738975ccc89574a1533  
e2473526523180f460af4d8e164df9060c9f328cc7c0bae5846d51b28c12febe  
7adc0e8236262080e62c4bfb97e745880247f9e244ae8718e60cc217a3ae773b  
0107fadc185fd6b53dc033d4a79e53ef1621ae623917de029b6c02eeae2021c1  
388386f3361138514c561dcf6169e8f9e8726c91e2dc66663efb07bf21ece052  
507b63c73ba3bee19c8c8afb40526c1196240376277f4b49e25bedc5d866b980

## SHA1

a2ad3ec4cd2d70edf2bc9089c493f898b7da44a5  
8f841e8f7d2c3334145c8c9f89c8cd6929a06b2a  
3390272bb793ad15a45d647c3e5a716145fd262a  
8cd26c88b74f913f6e1c9d71a8d1e9aa53b7c6f6  
160c5583f9ba3d11e94a0dd8c9a64936981e8194  
859f498f0ba963e468a3912d936ad8e7ec01dbcd  
90fc8a737a7030db2e3583cbccb3156bb0a8ff12  
683efb5746e85867b5d613dc07a116a80becce58  
6c2d55f7fcedcae779b148f0060b8ab4062e0a9  
7617dc78df626d5df43e38506fa7c577baef4bc5  
05d74461b2a63b75f319ef2c5c4aa074af4e97c3  
9e9c8ef7f20677795684b2749a59367cf5c3ec0a

# LABS

(<https://www.sentinelone.com/labs/>)

50744ce5d3cccu556u00704u0i0ue00zeay20027  
94277994af62de5948d6de134edac0089a54b71e  
3ce8f4bfeb99fa2fb8898c7664ad3838ce4a4fcf  
4ffa900d7cf3ae6414bf90f6c9a4667cedfd57dd  
83be2722b7adc91bc3ee219b75e9176bc7ce8e6e  
72d3d907d7502c383ffc8239d255882838a5a6e4

AGENT TESLA ([HTTPS://WWW.SENTINELONE.COM/BLOG/TAG/AGENT-TESLA/](https://www.sentinelone.com/blog/tag/agent-tesla/))

INFO STEALER ([HTTPS://WWW.SENTINELONE.COM/BLOG/TAG/INFO-STEALER/](https://www.sentinelone.com/blog/tag/info-stealer/))

KEYLOGGER ([HTTPS://WWW.SENTINELONE.COM/BLOG/TAG/KEYLOGGER/](https://www.sentinelone.com/blog/tag/keylogger/))

RAT ([HTTPS://WWW.SENTINELONE.COM/BLOG/TAG/RAT/](https://www.sentinelone.com/blog/tag/rat/))

## SHARE

 Facebook

 Twitter

 LinkedIn

 Reddit

 Mail

PDF (<https://www.sentinelone.com/wp-content/uploads/pdf-gen/1630592806/agent-tesla-old-rat-uses-new-tricks-to-stay-on-top.pdf>)



**JIM WALTER** (<https://www.sentinelone.com/blog/author/jimw/>)

Jim Walter is a Senior Threat Researcher at SentinelOne focusing on evolving trends, actors, and tactics within the thriving ecosystem of cybercrime and crimeware. He specializes in the discovery and analysis of emerging cybercrime "services" and evolving communication channels leveraged by mid-level criminal organizations. Jim joined SentinelOne following ~4 years at a security start-up, also focused on malware research and organized crime. Previously, he spent over 17 years at McAfee/Intel running their Threat Intelligence and Advanced Threat Research teams.

<https://twitter.com/LabsSentinel>) **in**(<https://www.linkedin.com/company/sentinelone>)