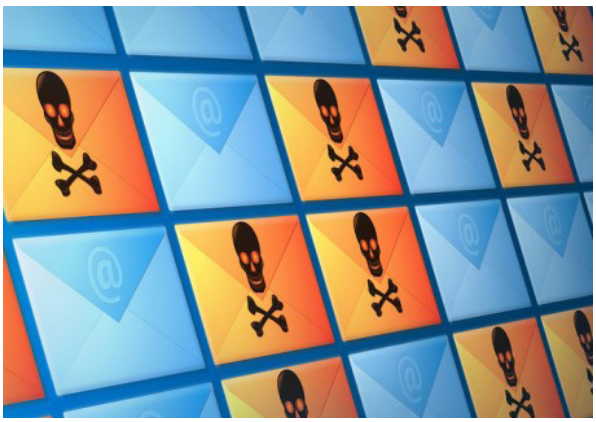
Series of New Agent Tesla Infostealer Campaigns Use Coronavirus Themes



Overview

Since 16 March, we observed a series of campaigns using COVID-19 or Coronavirus-themed spam emails to distribute the Agent Tesla information stealer (infostealer). While we also observed two other large campaigns distributing the Hawkeye keylogger and Predator the Thief, the majority of this report will focus only on Agent Tesla.

As with last week's Cyber Campaign Brief, we will provide representative indicators in the Appendix for each of the campaigns mentioned above.

Customer Impact

Agent Tesla is an easy-to-use, readily available keylogger that can capture and store keystrokes, steal credentials and information from forms, and exfiltrate data to a command and control (C2) server.

Agent Tesla can also steal data from a victim's clipboard, as well as videos and pictures from a connected camera.[1] Threat actors can use newer versions of the malware to execute remote code and potentially download additional malware.[2]

The languages in the message bodies and information in the signature blocks indicate that the targets for this week's campaigns appeared to be from Qatar, Turkey, China, and Brazil or Portugal.

Campaign Analysis

While all of the campaigns we initially observed used a Coronavirus theme in the email subjects, pivoting on one of the sender hostnames allowed us to find several additional campaigns.

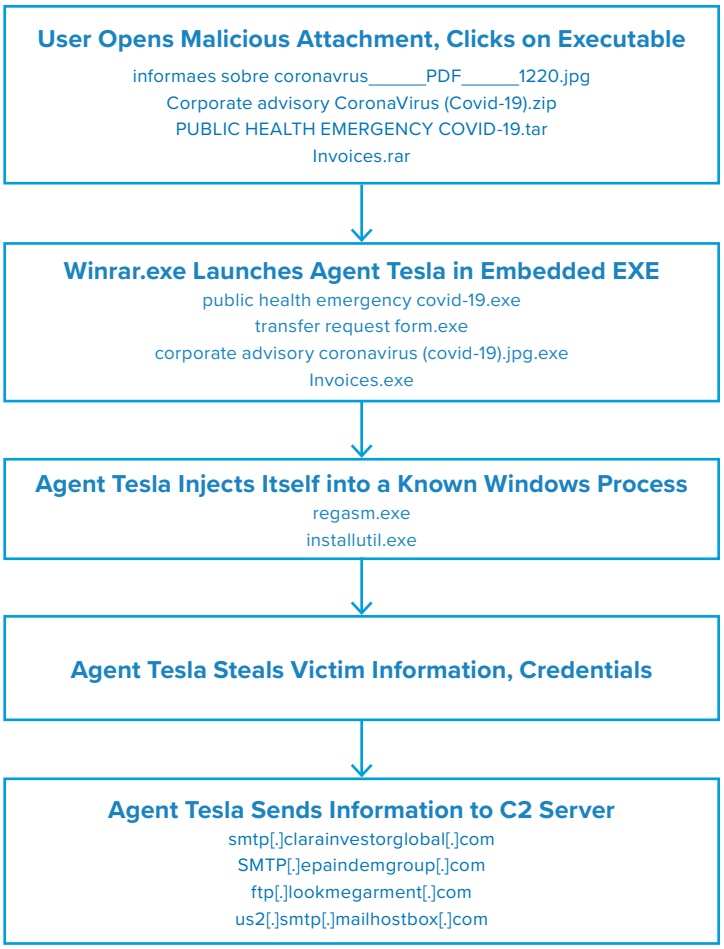
Overall, most campaigns used subject lines mentioning COVID-19, "COVID-19 Supplier Notice," or referencing the "Public Health Emergency" or the "Outbreak of Coronavirus." However, we also found groups of related emails using more typical malspam themes including orders, invoices, bank statements, and project enquiries.

Most of the emails contained message bodies with letters to the recipient about various kinds of updates on the Coronavirus outbreak. Some were all in a single language such as English or Portuguese, while others mixed English with Arabic or Turkish.

All of the messages carried attachments that were a type of archived file: ZIP, RAR, or TAR. Some used file names attempting to portray the file as a JPEG, PDF, GZ, or 7Z rather than a RAR file.

Attack Chain

As with previous Agent Tesla campaigns,[3,4] once the recipient opened the attachment and decompressed the archive file, the executable inside launched the malware, gathered victim information, and then reached out to send the data to an FTP or SMTP server. Some of this week's samples also reached out to Google Drive before attempting to exfiltrate the victim's data to an FTP or SMTP server.



Vulnerabilities & Mitigation

Threat actor(s) continue to take advantage of the high interest in the current status, implications, and future restrictions related to COVID-19 by designing their spam emails with related themes. As such, we recommend the following actions to reduce the risk of this type of infection:

- Regularly train users to be aware of potential phishing efforts and how to handle them properly.
- Always be suspicious of unexpected and vague emails and unknown senders.
- Do not open files attached to emails that are suspicious or from unknown senders.
- Exercise additional caution when unexpected messages or attachments have commonly used themes such as shipping or financial documents or advice.
- Verify important or potentially legitimate attachments with the sender via alternative means such as a phone call or separate email to a known contact.
- Check order statuses by browsing directly to the delivery website, rather than using an embedded link.

Appendix

Representative Indicators of Compromise	Description
RE:(COVID-19). COVID-19 Supplier Notice PUBLIC HEALTH EMERGENCY COVID-19.tar RE: Due to outbreak ofCoronavirus -- Corona Virus Outbreak - INLINE WITH THE PUBLIC HEALTH EMERGENCY COVID-19.(QATAR MINISTRY OF HEALTH MEMO) -- --TNT Express Notification/ Your shipment was returned to our office!!! BECAUSE OF COVID-19 OUTBREAK -- [WARNING: MESSAGE ENCRYPTED]Your Periodic Statement from QNB Mozoon Tower project Enquiry RE: PAYMENT TO BANK DETAILS (CONFIRM BANK DETAILS)	Agent Tesla malspam subject lines (some subjects are two lines long, denoted with "--" at the beginning and end)
informaes sobre coronavrus_____PDF_____1220.jpg -- informaes sobre coronav_PDF_____657473.7z -- -- informaes sobre coronav_PDF_____657473.gz -- Corporate advisory CoronaVirus (Covid-19).zip PUBLIC HEALTH EMERGENCY COVID-19.tar Invoices.rar TNT Express Notification Your shipment was returned.zip ACCOUNT STATEMENT_15-03-2020.zip Mozoon Tower project Enquiry_2020.zip Transfer Request Form.zip	Agent Tesla attachment file names (some file names are multiple lines long, denoted with "--" at the beginning and end)
smtp[.]clarainvestorglobal[.]com SMTP[.]epaindemgroup[.]com ftp[.]lookmegarment[.]com us2[.]smtp[.]mailhostbox[.]com	Agent Tesla C2 servers
5a594c84a1b14e565e06ff0ccb2cab5fb09a8a40f1e1b10a79f56b9422554ce dd455771ee174a203b1525ed64bf75ab55e45d6b080669ee6d71bc03540e466c e845d5dbbc215a3b9d95cb9173e9409360d4882e43c95a72c323c41425310788 20cb79ce821f7adb47eef021858f4d4a687f68da68721649f70b72bbab257a92 73aed7213676bfb02b7b9f99f6a0e3c5ac99ee0c22f39ff9c9e8588f362031a5 408bde2024c8b5840b9301dd0537f67a4aa269c35acd603fa04c8875cea88cc1 62d85f813ab1e0da66027a282aee76197a140afa4c064e3a3143f7e3f5b7b611 56b64e6933f4af99dd94e6dcad231c3372b571a8e899728ba357737864ce6cd6 a0cc35e646db421873923a20afb0a5dc1f52ed1431cb271574002494cae7eb38 4bec37e6d0cc92ae488afffe6bb0dd637413299732dccd5eedea16534e775666	Agent Tesla attachment file SHA256
RE: Coronavirus disease (COVID-19) outbreak prevention and cure update	Hawkeye malspam subject
Coronavirus Disease (COVID-19) CURE.rar Coronavirus Disease (COVID-19) CURE.zip	Hawkeye attachment file names
mail[.]eagleeyeapparels[.]com	Hawkeye C2 server

Representative Indicators of Compromise (Continued)	Description
f3eac3b0b250ae5da352a6d1358e9729e79af9549bc04f53d83283b5b07679fd d4bf55a016c9d5bf28b4945c682e5f998efddbffe5578600a070da12eb985d78	Hawkeye attachment file SHA256s
Coronavirus Disease 2019 (COVID-19) COVID-19 cases in the U.S. Government Response to Coronavirus COVID-19 United States Coronavirus Coronavirus: All 50 States Report Cases Coronavirus updates from March 16, 2020 Information about COVID-19 in the United States Coronavirus in the US US takes more big pandemic response steps	Predator the Thief subjects lines
covid[0-9]{2}_form.zip	Predator the Thief attachment file name regex
show1[.]website	Predator the Thief C2
f9201a2787ec144b0638e22744a074ef168084f94123d1cd8f25f42ef10b7a57 f8620dd6b8fc37fba432728341961a4441ed929ff16cb3f70b80244d70768d7f f33ef99d401431174c55d410148e36394a021729dcc8054e58cf07ebcaefd8ee e9fb57f7f5286e07ef704bac0ddeb098542ee3229a03220a0b7677daf177bf7e e5187acd91e48b18e68ef63093d0368c3a6f24527160d42089071edf5e69139d e1d30614a27ba2da03216dfd98f39077e3a3c08af813710a405748af3b7e96d1 dfdbe5ff6d5ea17ff3ed0b521a0ea6c4b2c95e4702ba4725ff006d507cfc3504 d9db96ab59eaab31009d5facc359e3bc6e915cd6558e339cd94b6c407b3934be d435d18375c78d727f5a30c9363d81a25edea59757b8dd3b8f500e039b05d830 ccc9b3ce71b082c0e81dc8acb8ddbb8d4aa66dfebf3377ca3f2d5d0e47007b3b bc27f858d9ad61c36b95a232e506476de8ebdd85eb712bcbf6b045fbb1c340eb b374c87ae852aa0443eb541f7d4ef4017c4238b10155381b88bb05016caab445	Predator the Thief attachment file SHA256s

Endnotes

1. https://www.em360tech.com/continuity/tech-features-featuredtech-news/agent-tesla/
2. https://cyware.com/news/hackers-employ-a-new-technique-to-hide-behind-anti-virus-programs-and-spread- agent-tesla-info-stealer-1f62f547
3. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--17
4. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--58

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com