Agent Tesla Malspam Campaign Spoofs Bank Correspondence

Author: Nick Sundvall

Overview

From 1 to 6 April, we observed a malspam campaign distributing a TAR file containing Agent Tesla, a remote access trojan (RAT) designed to steal information from a victim. The campaign's email subjects attempted to gain the victims trust by impersonating the British bank Standard Chartered. Some of the emails claimed to offer advice from the bank, as well as notified the recipient of a payment.

Customer Impact

Discovered in 2014,[1] the Agent Tesla RAT has a variety of malicious capabilities such as stealing credentials from browsers, VPNs, FTP and email clients. It can also record the user's screen and log keystrokes. The threat actor can then use these stolen credentials and keystrokes to log into, and potentially take over, the user's accounts to access more of their data.

Agent Tesla is distributed as "malware-as-a-service," reportedly for as little as $12 USD online. This buys a one-month license, an online portal to set up the configuration of the malware, and 24/7 support.[2]

Campaign Analysis

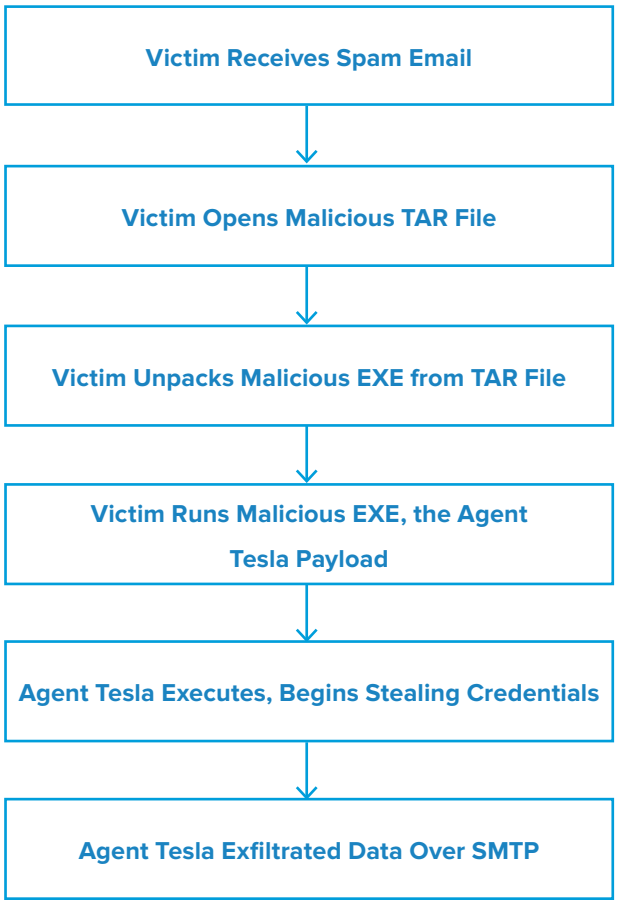
The threat actor behind this campaign used email subjects mimicking correspondence from Standard Chartered, a legitimate British bank. One of the email subject lines was *SUBJECT:Advice from Standard Chartered Bank* and *Confirming - Notice of payment*, with a sender's name of *Standard Chartered Bank*. The sender's address (*AdvicesMY@sc[.]com*) also imitates the real Standard Chartered Bank's website (*sc[.]com*).

All of the emails had a TAR file attachment containing an executable (EXE). TAR files are a kind of archive file, similar to a ZIP or RAR. The EXE was the malicious payload containing Agent Tesla. The file names, such as *Payment Advice.img.tar*, all include .img.tar as the extension in an attempt to disguise themselves as an image (IMG) file. The bodies of the emails are all empty.

Attack Chain

Upon opening the attached TAR file, the victim is able to extract the malicious EXE - *MY08466Q000951.exe* - from the archive. Running the EXE initiates the Agent Tesla RAT. From here, the malware begins stealing the victim's credentials.

Once Agent Tesla has gathered the information, it exfiltrates it over SMTP and then sends the data to the email address *vijay.yadav@mivante[.]com.*



Vulnerabilities & Mitigation

Infoblox recommends the following to reduce the risk of this type of infection:

- Be aware of any attachment's file type, and never open files that could be a script (.vbs, .cmd, .bat), an internet shortcut file, or compression file. Using the latter is a known method for evading detection methods based on file hashes and signatures. Threat actors use them to mask the real malicious file due to email service restrictions on attachment file types.
- Verify important or potentially legitimate attachments with the sender via alternative means (e.g. by phone or in person) before opening them.
- Always be suspicious of vague or empty emails, especially if there is a prompt to open an attachment or click on a link.
- Do not open attachments that are unexpected or from unfamiliar senders.

Endnotes

1. https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/the-many-roads-leading-to-agent-tesla/
2. https://labs.sentinelone.com/agent-tesla-old-rat-uses-new-tricks-to-stay-on-top/

Corporate Headquarters: 2390 Mission College Boulevard, Ste. 501 | Santa Clara, CA | 95054
+1.408.986.4000 | info@infoblox.com | www.infoblox.com