Wireshark Analysis Incident Report

Aaron Gehring

September 26, 2021

1 Executive Summary

On September 24th, 2020, at 5:41 pm CDT, a Windows device was logged in with Ronaldo Paccione's account and then was infected by the Agent Tesla trojan virus. The virus installed a keylogger, captured a picture of the user's desktop, and stole passwords and temporary website login data. The attacker knows about a text file containing passwords in the user's Documents folder. The Agent Tesla virus is typically introduced by convincing the user to run an infected file; it is not clear that this has happened. Further investigation is recommended to discover what initiated the virus download.

2 Victim

- ronaldo.paccione/DESKTOP-M1JC4XX has been infected by the trojan virus "Agent Tesla"
- Infected on 2020-09-24 at approximately 22:41 UTC (17:41 CDT).
- IP address: 10.0.0.179
- Domain: pascalpig.com
- The victim's account appears to have logged in and then started the jojo.exe download within 10 seconds.
- The victim appears to have logged in as "\u2E72\u2E6F\u2E6E\u2E61\u2E6C\u2E64o.paccione". In fact, the session setup has many strange Unicode characters.

3 jojo.exe

- Trojan Virus known as Agent Tesla
- SHA-256 hash: 1e4b7d7868d25071db67da87392fd5dafab344a9fa6dc040f7afb0699152fc13
- jojo.exe: PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
- VirusTotal flagged as trojan virus
- Downloaded via plain HTTP from http://198.12.66.108/jojo.exe

No.	Time	Source	port	Destination	port	Protocol	Length	Info
752	2020-09-24 22:41:33	10.0.0.179	50066	198.12.66.108	80	HTTP	209	GET /jojo.exe HTTP/1.1

- HTTP User Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
  - This is not a user agent of a browser or email client, but of a built-in Windows library. There is a chance that the PC was already infected. Further investigation recommended.
- Downloads payload from paste.nrecom.net, a public pastebin service.

No.	Time	Source	port	Destination	port	Protocol	Length	Server Name
1039	2020-09-24 22:41:38	10.0.0.179	50067	37.120.174.218	443	TLSv1.2	232	paste.nrecom.net

- Contacts ipify.com to collect public IP of infected device, seen reported in exfil.

No.	Time	Source	port	Destination	port	Protocol	Length	Server Name
2128	2020-09-24 22:43:07	10.0.0.179	50083	54.235.98.120	443	TLSv1.2	229	api.ipify.org

4 Exfil

- Virus remotely logs into own email via SMTP and sends emails to itself

No.	Time	Source	port	Destination	port	Protocol	Length
2264	2020-09-24 22:43:13	10.0.0.179	50085	185.61.152.63	587	SMTP/IMF	164

  from: jojo@big3.icu, subject: CO_ronaldo.paccione/DESKTOP-M1JC4XX, (text/html) (application/zip)

- Exfil via email to jojo@big3.icu
- Information sent as attachments
- Passwords, browser/email cookies, screen capture of desktop, keylogger results
- Four emails were sent, each with a prefix denoting the data being sent
  - PW_=list of passwords
  - KL_=keylogger
  - CO_=cookies
  - SC_=screen capture
- Cookie file could have compromised many accounts if the value row were not blanked

5 Compromised Accounts

- ronaldo.paccione, infected PC
- ronaldo.paccione@outlook.com: live.com (via password capture)
- AOL (via keylogger)
- Documents\password-list.txt potentially compromised

6 Domains/IP Addresses

- jojo@big3.icu/mail.big3.icu (185.61.152.63)
- paste.nrecom.net/server3.nrecom.net (37.120.174.218)
- ipify.com (54.235.98.120)
- pascalpig.com (107.182.238.224)
- pascalpig-dc.pascalpig.com (10.0.0.10)
- jojo.exe host (198.12.66.108)

7 Lessons Learned

Agent Tesla is typically the result of phishing, so training employees to identify malicious pages, like spam email, fake web forms, and malicious Microsoft Office documents, would do well to avoid these viruses. The organization should also train their users basic cyber security, such as how it is bad practice to store your passwords in a plain text file in your documents folder. Blocking unsigned software would avoid this scenario, if reasonable for the organization. Blocking access to pastebin services would stop this virus, and is a solution seen implemented at other organizations.

8 Appendix A - Investigation Details

A detailed look at how the investigation was conducted can be viewed in the attached document “notes.pdf”. In addition to the documentation of how the investigation was conducted, a more detailed list of discoveries is built throughout, and completed on the last page.