2020-09-25 - TRAFFIC ANALYSIS EXERCISE ANSWERS

Link to exercise: https://www.malware-traffic-analysis.net/2020/09/25/index.html

Links to some tutorials I've written that should help with this exercise:

- Customizing Wireshark - Changing Your Column Display
- Using Wireshark: Identifying Hosts and Users
- Using Wireshark - Display Filter Expressions
- Using Wireshark: Exporting Objects from a Pcap

ENVIRONMENT:

- LAN segment range: 10.0.0.0/24 (10.0.0.0 through 10.0.0.255)
- Domain: pascalpig.com
- Domain controller: 10.00.10 - Pascalpig-DC
- LAN segment gateway: 10.0.0.1
- LAN segment broadcast address: 10.0.0.255

INCIDENT REPORT:

Executive summary:

On Thursday, 2020-09-24 at approximately 22:41 UTC, a Windows host used by Ronaldo Paccione was infected with Agent Tesla malware.

Victim details:

IP address: 10.0.0.179
MAC address: 00:0c:6e:34:b2:d0 (ASUSTekC_34:b2:d0)
Host name: DESKTOP-M1JC4XX
User account name: ronaldo.paccione

Indicators of compromise (IOCs):

SHA256 hash: 1e4b7d7868d25071db67da87392fd5dafab344a9fa6dc040f7afb0699152fc13

- File size: 326,080 bytes
- File type: PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
- File location: http://198.12.66.108/jojo.exe
- File description: EXE file for AgentTesla malware

2020-09-25 - TRAFFIC ANALYSIS EXERCISE ANSWERS

Malicious HTTP traffic:

- 198.12.66.108 port 80 - 198.12.66.108 - GET /jojo.exe
- 185.61.152.63 port 587 - mail.big3.icu - SMTP traffic with data stolen from the infected Windows host

Suspicious domains using HTTPS traffic:

- 37.120.174.218 port 443 - paste.nrecom.net - HTTPS address check probably related to the infection
- port 443 - api.ipify.org - probably IP address check by the infected Windows host

NOTES

AgentTesla is an information stealer. There are two categories of AgentTesla:

- AgentTesla that uses SMTP to send stolen data
- AgentTesla that uses FTP to send stolen data

The AgentTesla seen from this infection is the type that uses SMTP. Even though it's over TCP port 587 (normally used for encrypted SMTP), the traffic is unencrypted.

You can use ***File --> Export Objects --> IMF*** to export the 5emails sent over SMTP from the pap.

There were 4 subject lines in 5 emails sent out:

- Subject: PW_ronaldo.paccione/DESKTOP-M1JC4XX
- Subject: CO_ronaldo.paccione/DESKTOP-M1JC4XX
- Subject: SC_ronaldo.paccione/DESKTOP-M1JC4XX (sent twice)
- Subject: KL_ronaldo.paccione/DESKTOP-M1JC4XX

The two-letter prefix breaks out as follows:

- PW - passwords found on the infected host.
- CO - cookie data from the web browsers

- SC - screen capture, has jpeg attachment with picture of the
- KL - keylogger data

Feel free to export these emails from the pcap and view them in a text editor or an email client like Thunderbird. If this were a real-life situation, you could show the infected user exactly what was stolen from their computer.

A lot of AgentTesla malware uses encrypted SMTP, so we were lucky that this one used unencrypted SMTP, which makes it easier to identify due to the alert:

ET TROJAN AgentTesla Exfil Via SMTP

Which had 58 hits starting at 22:43 UTC

The domain ***paste.nrecom.net*** is associated with the EXE from the pcap. We can't see what the URL is, because it's HTTPS.

But HTTPS traffic to this domain is called by the initial EXE, where we'd see something like:

https://paste.nrecom.net/view/raw/b44fe71a

The above returned a base64 encoded hex string when I checked it. I converted the hex string into a binary, and in the above case, I XOR-ed each with 0x02 to find an EXE that seems to be malicious.

Of note, I don't think the domain ***paste.nrecom.net*** is inherently malicious. It's just another Pastebin-like service that malware authors for AgentTesla have been utilizing in the past week or so as I write this.