Analyzing network traffic file

Guilherme S. Mazzariol
Bachelor of Science in Computer Science
Campinas/SP - Brazil
g138466@g.unicamp.br

I. Introduction

Using Wireshark program, it is possible to read a lot of information about traffic in a network on the fly, or from a capture file (*.pcap). Besides Wireshark, tshark[1] is another tool used to read traffic in a network, listening to what is happening in it. This paper uses those programs to read traffic from file *traffic1.pcap* and get more information about it.

A. Discovering the involved Systems and their Geographical Location

Using tshark command:

tshark -r traffic1.pcap -qnz ip_hosts,tree

We can figure the IP address in the *traffic1.pcap* file:

```
===================================
IP Statistics/IP Addresses:
Topic / Item      Count
-----------------------------------
IP Addresses      1762
 192.168.115.238  1762
 200.149.77.224   1276
 66.7.200.69      424
 189.126.11.82    36
 66.7.200.72      18
 8.8.4.4          8
```

Some operational systems have, in their packets, a specific TTL and Windows Size, as shown in this table [2]:

Operating System (OS)	IP Initial TTL	TCP window size
Linux (kernel 2.4 and 2.6)	64	5840
Google's customized Linux	64	5720
FreeBSD	64	65535
Windows XP	128	65535
Windows 7, Vista and Server 2008	128	8192
Cisco Router (IOS 12.4)	255	4128

So, comparing the information from each packet in Wireshark to the information on the table, we can say which is the Operating System from each IP:

192.168.115.238 - Windows XP:

No.	Time	Source	TTL	Window Size	Protocol
17	1.608908	192.168.115.238	128	65535	TCP

200.149.77.224 - FreeBSD:

No.	Time	Source	TTL	Window Size	Protocol
18	1.609022	200.149.77.224	53	18760	TCP

66.7.200.69 - Linux:

No.	Time	Source	TTL	Window Size	Protocol
1279	23.217210	66.7.200.69	50	5840	TCP

66.7.200.72 - FreeBSD:

No.	Time	Source	TTL	Window Size	Protocol
1724	36.651354	66.7.200.72	50	6432	TCP

189.126.11.82 - Linux:

No.	Time	Source	TTL	Window Size	Protocol
1728	37.224479	189.126.11.82	53	5840	TCP

To know where are geographically located the attacking hosts, it's necessary to import and enable GeoIp on Wireshark. All database used for GeoIp was downloaded from MaxMind Developer Site [3].

Using this information, it was possible to identify the locations of hosts:

192.168.115.238

Local IP - Not possible to Locate

200.149.77.224 - Brazil:

No.	Time	Source	Protocol	SRC_Country
1745	63.889321	200.149.77.224	TCP	Brazil

66.7.200.69 - United States:

No.	Time	Source	Protocol	SRC_Country
1714	30.655506	66.7.200.69	TCP	United States

66.7.200.72 - United States:

No.	Time	Source	Protocol	SRC_Country
1724	36.651354	66.7.200.72	TCP	United States

189.126.11.82 - Brazil:

No.	Time	Source	Protocol	SRC_Country
1728	37.224479	189.126.11.82	TCP	Brazil

B. Identifying the TCP Sessions

To show the TCP sessions, you just need to access Wireshark Expert Info (*Wireshark >> Analyze >> Expert Info*). This tool gives us a resume of what is happening in the TCP sessions:

Protocol	Summary
TCP	Connection establish request (SYN): server port 80
TCP	Connection establish acknowledge (SYN+ACK): server port 80
HTTP	GET /DATA-FILES/ARQUIVO12.XLS HTTP/1.1\r\n
TCP	TCP window update
HTTP	GET /images/get_wabs.jpg HTTP/1.1\r\n
HTTP	HTTP/1.1 200 OK\r\n
TCP	Connection finish (FIN)
HTTP	GET /logs/logs.txt HTTP/1.1\r\n
HTTP	POST /images/procopspro.php HTTP/1.0\r\n

Counting the rows, it is possible to identify 9 TCP sessions in the *traffic1.pcap* file. To save each TCP session in a file to analyze the actions in sessions, it was used a specific filter in Wireshark:

tcp.stream eq $Number

where *$Number* must be replaced by the session number (0,1,2,...,8).

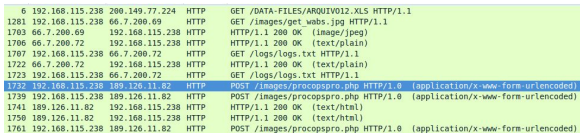
C. Analyzing the attack

By now, we know that there are 9 TCP sessions in the *traffic1.pcap* file, but it's interesting to know how much time each session took, to identify more information about what is happening in that specific attack. To do that, we used the Wireshark Statistics (*Wireshark >> Statistics >> Conversions >> TCP*), that gives us the time per session:

Address A	Port A	Address B	Port B	Duration
192.168.115.238	1126	200.149.77.224	80	65,7965
192.168.115.238	1127	66.7.200.69	80	7,7395
192.168.115.238	1128	66.7.200.72	80	0,7188
192.168.115.238	1129	189.126.11.82	80	9,9025
192.168.115.238	1130	66.7.200.72	80	0,7514
192.168.115.238	1131	189.126.11.82	80	36,5656
192.168.115.238	1132	189.126.11.82	80	24,0238
192.168.115.238	1133	189.126.11.82	80	8,9377
192.168.115.238	1136	189.126.11.82	80	0,1064

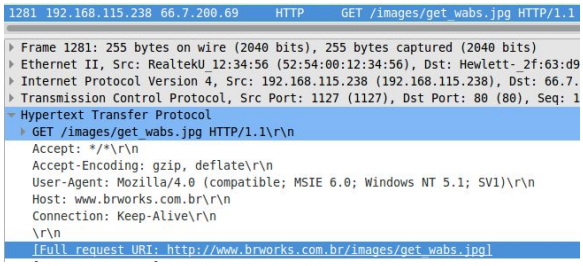
With this information, we can look for the session from IP 192.168.115.238 and 200.149.77.224 which took longer compared to all other sessions: 65,7965 seconds. This is probably the attack session, if we think only about time. But it is necessary to take a look in TCP sessions.

Session 3 has a HTTP GET request, so look deeper in this session. Putting protocols in order by name, we can find that:



Two POST requests (packets 1732 and 1739, in order) so, looking further into these packets with Wireshark:

Packet 1281 gets file ***get_wabs.jpg***



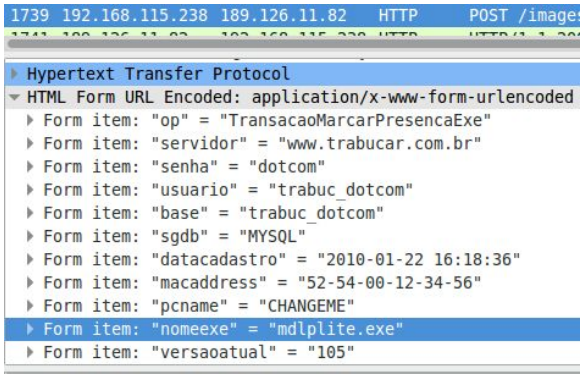
Searching for this file in web, we found a web page Remove get_wabs[1].jpg [4] that said get_wabs.jpg is able to detect system vulnerabilities and then lead off an attack. So the attack starts here.

Packet 1707 gets the file ***http://brdotcom.com.br/logs/logs.txt***

Searching for this file in web, we found the page "*How to Remove Win32.TrojanSpy.Bancos*" [6] telling about a trojan downloading that file, so attack continues.

Packet 1732 has the file ***emplite.exe***

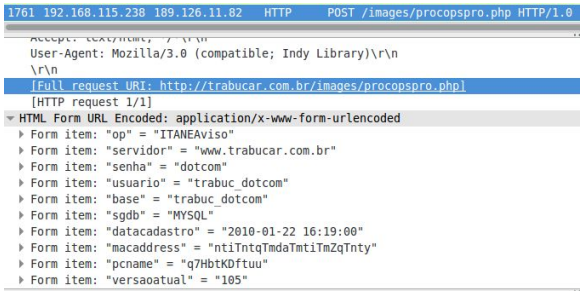
Packet 1739 has the file ***mdlplite.exe***



Searching online for the files *emplite.exe* and *mdlplite.exe*, we found a page from trend micro telling about the "*TROJ_THINSTAL.RN - Threat Encyclopedia - Trend Micro AU*" [7]. In that point we found the proof that the attack involved the malware ***"TROJ_THINSTAL.RN"***.

Looking further, we found that:

Packet 1761 has the file procopspro.php



Searching in web for that file we found a page from trend micro: ***"TROJ_BANKER.LMQ - Threat Encyclopedia - Trend Micro US"***[8], saying:

"This Trojan monitors the Internet Explorer (IE) activities of the affected system, specifically the address bar. It recreates a legitimate Web site with a spoofed login page if a user visits banking sites with certain strings in the address bar."

At this point we can find the trojan: he was spoofing the page from some banks in victims machines.

The packet 1761 identifies the attacker who has the IP 189.126.11.82 locating in Brazil.

The attack starts on packet 1281 and ends on packet 1761, so if we search for this packets on TCP sessions, we find packet 1281 in session 4, packet 1707 in session 7 and packets 1732-1739-1761 in session 8, so the time spent on attacks was the sum of the time from each session, totalizing 9,7955 seconds.

References

[1] tshark(1) - Linux man page, https://linux.die.net/man/1/tshark

[2] Passive OS Fingerprinting - NETRESEC Blog http://www.netresec.com/?page=Blog&month=2011-11&post=Passive-OS-Fingerprinting

[3] GeoLite Legacy Downloadable Databases, MaxMind Developer Site, http://dev.maxmind.com/geoip/legacy/geolite/

[4] Remove get_wabs[1].jpg http://www.completelyuninstallprogram.com/get-wabs-1-jpg/

[5] Analysis #totalhash , https://totalhash.cymru.com/analysis/?4dfe09415724bac695735af2b85b443cae69ebfd

[6] How to Remove Win32.TrojanSpy.Bancos, https://www.securitystronghold.com/gates/win32.trojanspy.bancos.html

[7] “TROJ_THINSTAL.RN - Threat Encyclopedia - Trend Micro AU”, https://www.trendmicro.com/vinfo/au/threat-encyclopedia/malware/troj_thinstal.rn

[8] “TROJ_BANKER.LMQ - Threat Encyclopedia - Trend Micro US”, https://www.trendmicro.com/vinfo/us/threat-encyclopedia/archive/malware/troj_banker.lmq