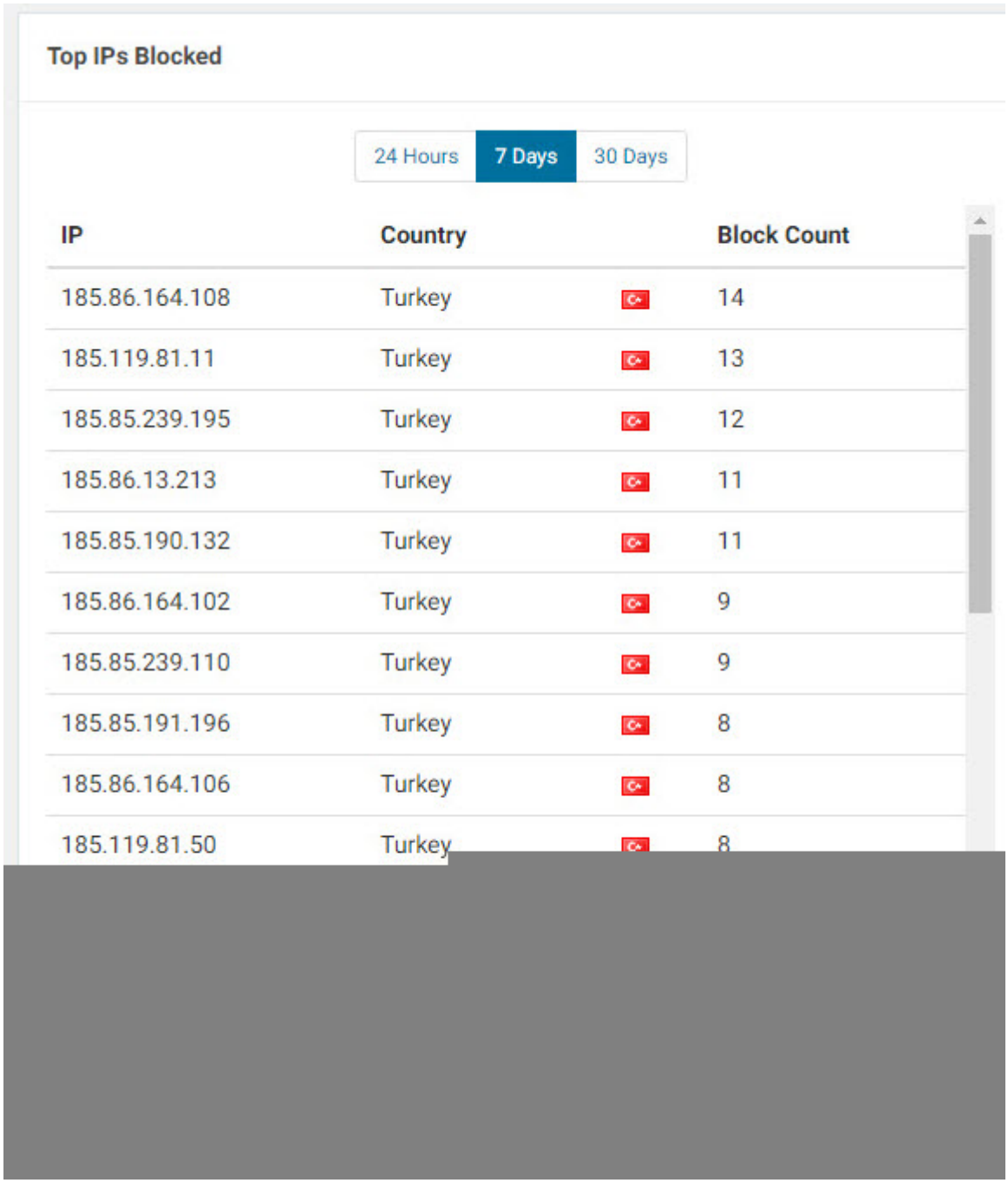
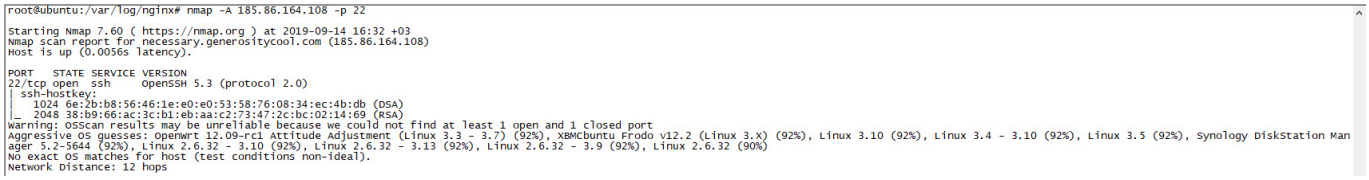
TLS Fingerprinting

written by Mert SARICA | 1 June 2020

For those of you who read my blog post on WordPress Security, you would have seen in the administrator page of my blog that there was a dictionary attack that was conducted for years (up until May 2020) from more than 20 IP addresses, and how I fought against it. It is important to not only detect cyber attack attempts but also to identify the groups behind the attacks, the tools they use. As I demonstrated in my blog post “Fighting Against DoS,” it is crucial in the fight against these attacks. Based on my previous experiences, I decided to investigate what kind of information I could gather about the dictionary attack on my blog in this research.



First, when I looked at the records of the IP addresses that conducted the dictionary attack in the logs of my web server, I saw that the User Agent field, which gives information about the operating system, internet browser and the tool used, contains the information Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36 Safari/537.36. While the operating system that theoretically conducted the dictionary attack appeared to be Windows 10, by running the Nmap tool with the -A parameter (Enable OS detection, version detection, script scanning, and traceroute) targeting the 22nd connection point, I easily found out that the target operating system was most likely a Linux operating system.



Then the question of whether the tools that conducted the dictionary attack from 20 different IP addresses were the same or different (the possibility of a botnet) began to bother me. While I was thinking about how I could find out, the JA3 method, which I had read about in a technical article before and is also used in cyber threat intelligence, suddenly came to my mind!

According to the JA3 method, it is found that the md5 hash value obtained from the information (Version, Accepted Ciphers, List of Extensions, Elliptic Curves, Elliptic Curve Format) in the “Client Hello” packet produced by the client application during the TLS connection is the same. For example, if you give command to the command and control center, the x version of Emotet banking malware that communicates over TLS has a md5 hash value of 4d7a28d6f2263ed61de88ca66eb011e3. Based on this information, it is possible to detect systems where Emotet malware is present in your network by searching for this value in the TLS network traffic recorded (full packet capture).

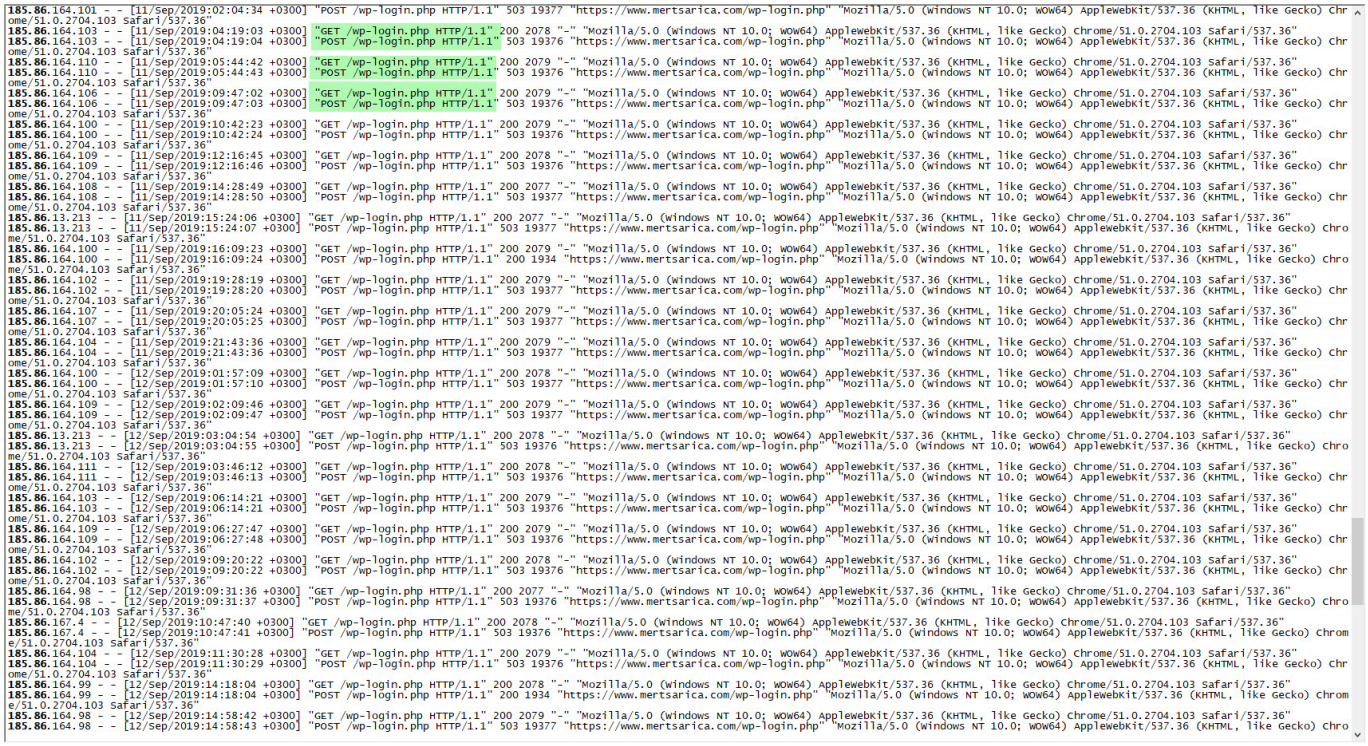
Of course, since my blog is behind Cloudflare and the TLS traffic is provided by the client and Cloudflare, it is not practically possible to record TLS connections from my web server. While thinking about what to do, I also realized that I need a much better server in terms of CPU, memory and disk for my next step. I tweeted about what kind of VDS (Virtual Dedicated Server) I should buy in terms of price and performance, and shortly after, Hamza ŞAMLIOĞLU (@TEAkolik), an information and technology influencer and a blogger, came to my aid and brought me together with Hosting.com.tr officials. After talking to them, they accepted to sponsor my security research and gave me two VDS!

Hosting.com.tr is a trusted, fast, and uninterrupted internet service provider in Turkey with a product portfolio including cloud hosting, cloud servers, physical servers, and additional services. They are constantly increasing their customer portfolio with their reliable, fast, and uninterrupted internet services. In 2015, they renewed their corporate identity, web infrastructure, and technical infrastructure, and with the new responsive website and management panels, they made the purchase of services

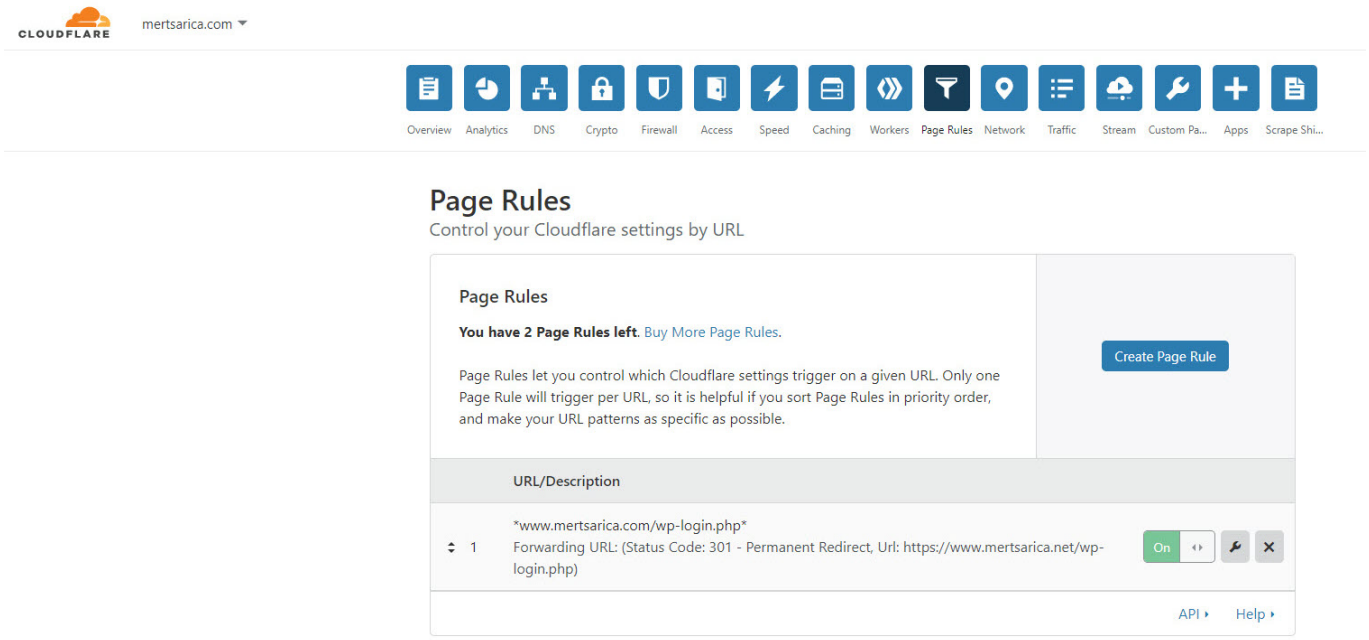
and all control panel operations simpler and more manageable.

With their renewed technical infrastructure, they have transitioned all servers to the cloud server architecture on SSD disks. Hosting.com.tr offers SSD disk services at classic hosting service prices. Within this framework, they work to constantly and happily increase their customer portfolio without compromising quality, focusing on unconditional customer satisfaction principles.

After I got my VDS, I continued to look at the HTTP traffic related to the dictionary attack and saw that the /wp-login.php page was first requested by a GET and then by a POST. In this case, could I have obtained the JA3 md5 summary value by redirecting the attacker to the www.mertsarica.net address that I hosted on my new VDS in the first GET request, and then making the POST request there?

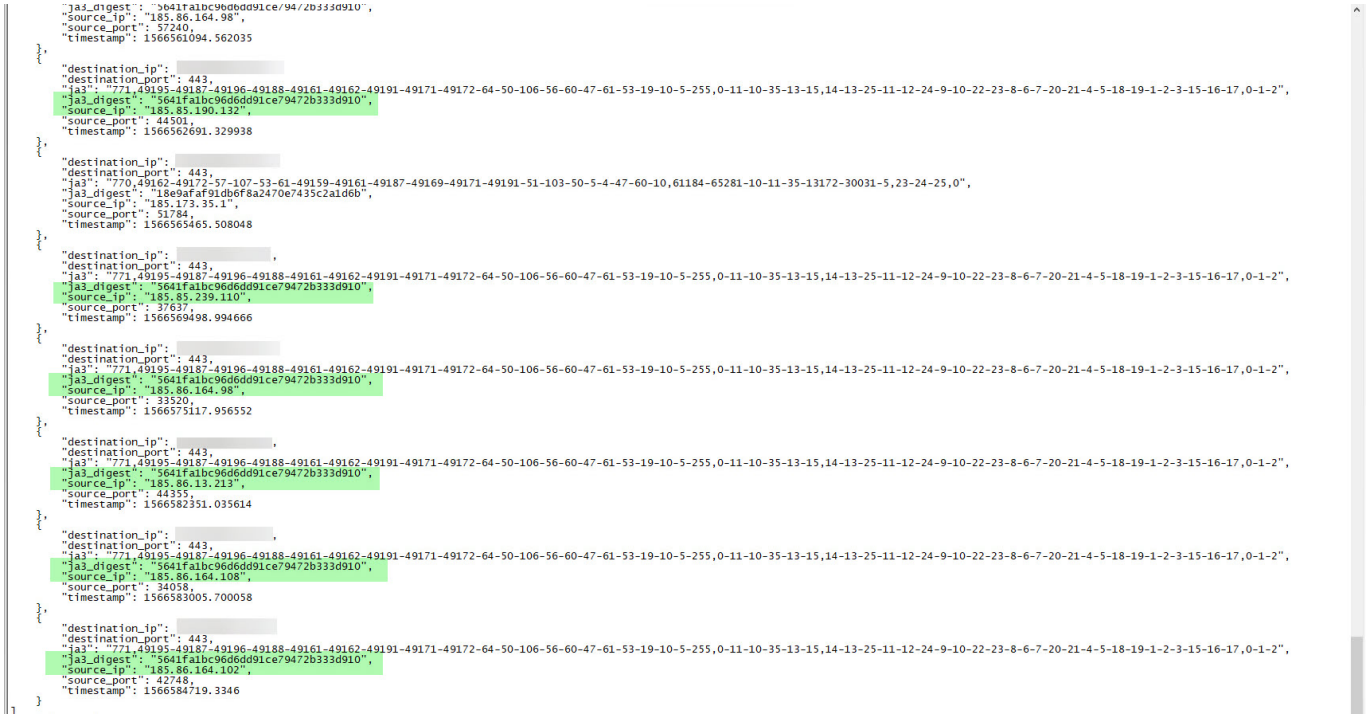


Without wasting time, I first redirected the www.mertsarica.net domain name to the VDS hosted on the infrastructure of Hosting.com.tr. Later, I set up Cloudflare's management panel so that all requests to www.mertsarica.com/wp-login.php would be redirected to www.mertsarica.net/wp-login.php. After installing the JA3 tool, developed by Salesforce, on the VDS, I began to record all connections to the www.mertsarica.net web server using the tcpdump tool.




```
:~# ps au
  PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
 1760  0.0  0.0  15956  2220 hvc0     Ss+  Aug22   0:00 /sbin/agetty -o -p -- \u --keep-baud 115200,38400,9600 hvc0 vt220
 1765  0.0  0.0  16180  1908 tty1     Ss+  Aug22   0:00 /sbin/agetty -o -p -- \u --noclear tty1 linux
 5821  0.0  0.1  26596  9240 pts/1    Ss+  10:19   0:00 -bash
 8285  0.0  0.1  26604  9244 pts/2    Ss   12:37   0:00 -bash
 8947  0.0  0.1  26596  9028 pts/3    Ss+  13:19   0:00 -bash
 9225  0.0  0.0  22896  6352 pts/2    S    13:32   0:00 tcpdump -U -i eth0 -w capture.pcap -s 0 net 185.0.0.0/8
 9271  0.0  0.0  37364  3424 pts/2    R+   13:36   0:00 ps au
:~#
```

A day later, when I looked at the output of the tcpdump tool, I saw that the JA3 md5 summary value (5641fa1bc96d6dd91ce79472b333d910) of 6 different IP addresses that carried out the dictionary attack was the same. From this information, I learned that the same tool was used on all systems that carried out the attack. As it came to finding out which tool was used for this attack, I immediately searched for this md5 summary value on the JA3 SSL Fingerprint website where JA3 fingerprint information is stored, but I couldn’t find any record. I ended my security research here, hoping that one day information about this md5 summary value would be added to the JA3 SSL Fingerprint website.



In summary, by utilizing the JA3 method, you can detect suspicious, malicious activities on your network, and find answers to the questions that plague your mind about cyber attacks, just like I did. I wish everyone safe days and hope to see you in the following articles.