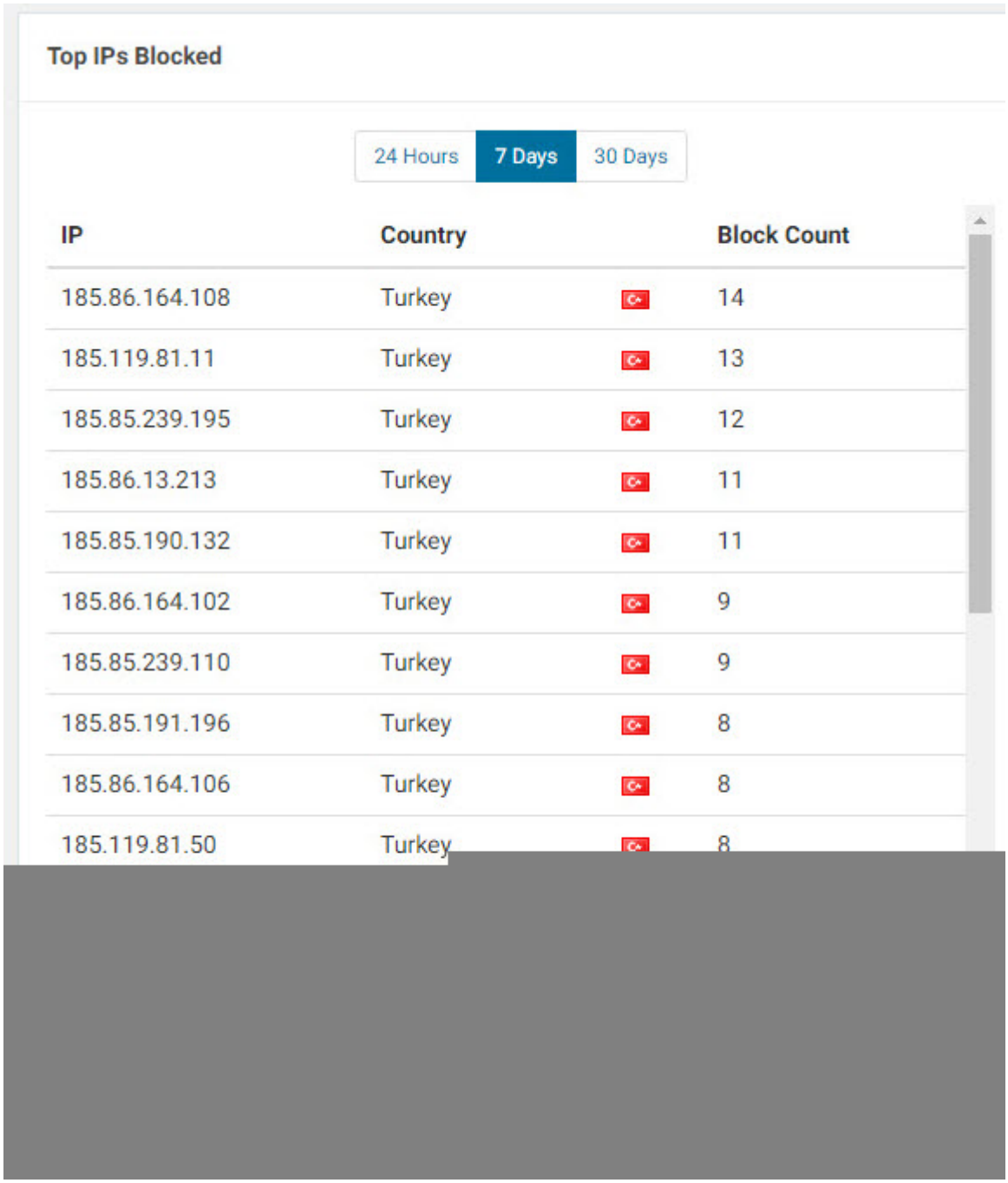
TLS Parmak İzi

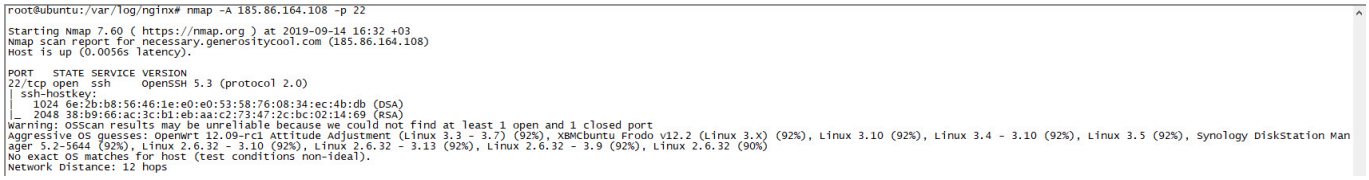
written by Mert SARICA | 1 June 2020

If you are looking for an English version of this article, please visit here.

WordPress Güvenliği başlıklı blog yazımı okuyanlarınız, blogumun yönetici sayfasına 20'den fazla ip adresinden yıllardır (Mayıs 2020 sonuna kadar devam etti) süren sözlük saldırısı yapıldığını ve bununla nasıl mücadele ettiğimi görmüşlerdir. Siber saldırı girişimlerini tespit etmek kadar saldırıların arkasındaki grupları, kullanılan araçları tespit etmek de bu saldırılarla mücadele adına DoS ile Mücadele başlıklı blog yazımda ortaya koyduğum gibi büyük bir öneme sahiptir. Önceki tecrübelerimden yola çıkarak bu araştırmamda bloguma gerçekleştirilen sözlük saldırısı ile ilgili olarak ne tür bilgiler elde edebileceğime bakmaya karar verdim.



İlk olarak web sunucumun kayıtlarından sözlük saldırısını gerçekleştiren ip adreslerinin kayıtlarına baktığımda, HTTP trafiğini gerçekleştiren işletim sistemine, internet tarayıcısına ve kullanılan araca dair bilgi veren User Agent alanında Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36 bilgisinin yer aldığını gördüm. Teoride sözlük saldırısını gerçekleştiren işletim sistemi Windows 10 gibi görünse de bu ip adresinin 22. bağlantı noktasına yönelik Nmap aracını -A parametresi (-A: Enable OS detection, version detection, script scanning, and traceroute) ile çalıştırarak hedef işletim sisteminin büyük bir olasılıkla Linux işletim sistemi olduğunu kolay bir şekilde öğrenmiş oldum.



Ardından 20 tane farklı ip adresinden sözlük saldırısını gerçekleştiren araçların aynı mı yoksa farklı mı (botnet olma ihtimali) olduğu sorusu aklımı kurcalamaya başladı. Bunu nasıl bulabileceğime dair hindi gibi düşünürken bir anda aklıma daha önce teknik bir makalede okuduğum ve siber tehdit istihbaratında da kullanılan JA3 metodu geldi!

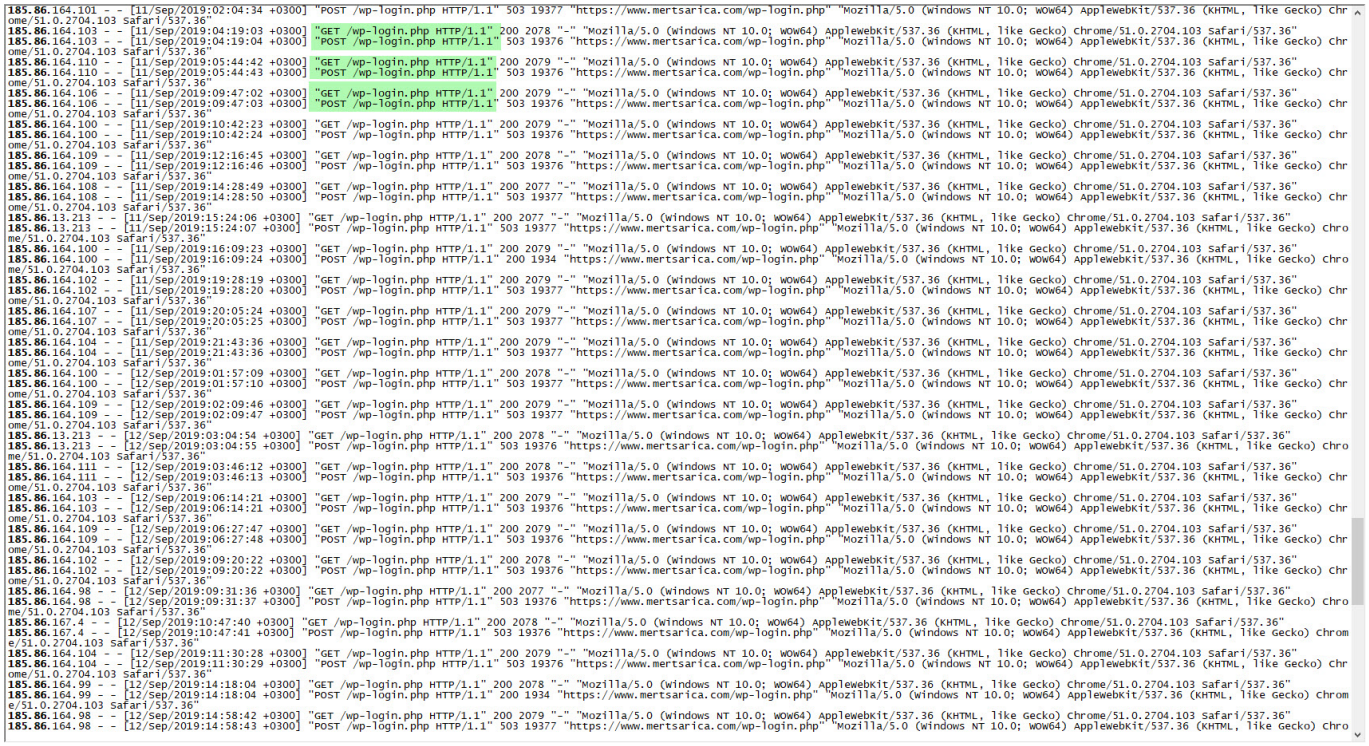
JA3 metoduna göre TLS bağlantı esnasında istemci uygulaması tarafından üretilen "Client Hello" paketinde yer alan bilgilerden (Version, Accepted Ciphers, List of Extensions, Elliptic Curves, Elliptic Curve Format) elde edilen md5 özet değerinin aynı olduğu görülmüş. Örnek vermek gerekirse komuta kontrol merkezi ile TLS üzerinden haberleşen x sürüm Emotet bankacılık zararlı yazılımı 4d7a28d6f2263ed61de88ca66eb011e3 md5 özet değerine sahipmiş. Bu bilgiden yola çıkarak kayıt altına alınan TLS ağ trafiğinde (full packet capture) bu değeri aratarak Emotet zararlı yazılımının bulunduğu sistemleri ağınızda tespit etmek mümkün olabiliyor.

Tabii blogum Cloudflare'in arkasında olduğu ve TLS trafiği istemci ile Cloudflare ile sağlandığı için web sunucum üzerinden TLS bağlantılarını kayıt altına almam pratikte mümkün değildi. Ne yapmalı ne etmeli diye düşünürken çalışmamı bir sonraki adıma taşımak için bir yandan CPU, bellek ve disk anlamında çok daha iyi bir sunucuya ihtiyacım olduğunu da anladım. Fiyat ve performans açısından nasıl bir VDS (Virtual Dedicated Server) sunucusu almam gerektiğine dair bir tweet attıktan kısa bir süre sonra bilişim ve teknoloji dünyasının fenomeni, bloggerı sevgili Hamza ŞAMLIOĞLU (@TEAkolik) imdadıma yetişerek beni Hosting.com.tr yetkilileri ile bir araya getirdi. Kendileri ile görüştükten kısa bir süre sonra güvenlik araştırmalarıma sponsor olmayı kabul ederek bana iki tane canavar gibi VDS verdiler!

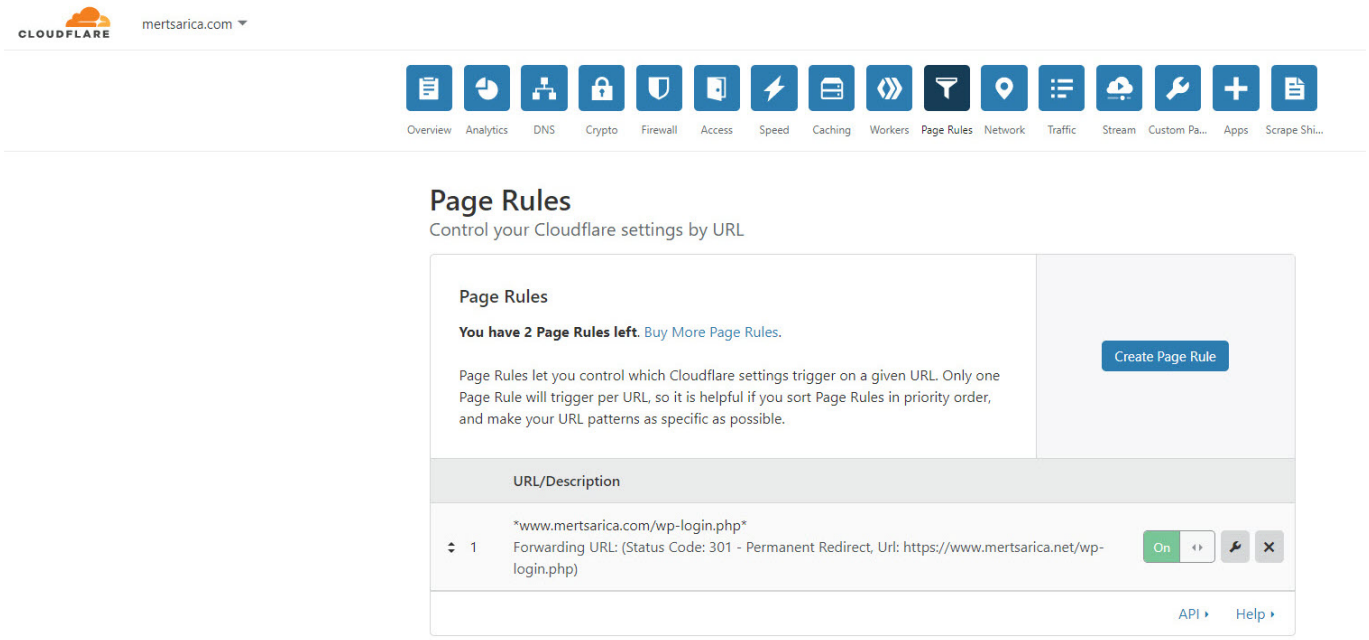
Hosting.com.tr, bulut hosting, bulut sunucu, fiziksel sunucu ve ek hizmetlerin olduğu ürün portföyü ile Türkiye'de güvenilir, hızlı ve kesintisiz internet hizmetleri ile müşteri protföyünü her geçen gün arttırmaktadırlar. 2015 yılında kurumsal kimlik, web altyapısı ve teknik altyapılarını yenileyerek tamamen responsive (mobil uyumlu) yeni web siteleri ve yönetim panelleri ile hizmet alımı ve tüm kontrol panel işlemlerini daha sade, daha hızlı yönetilebilir hale getirmişlerdir.

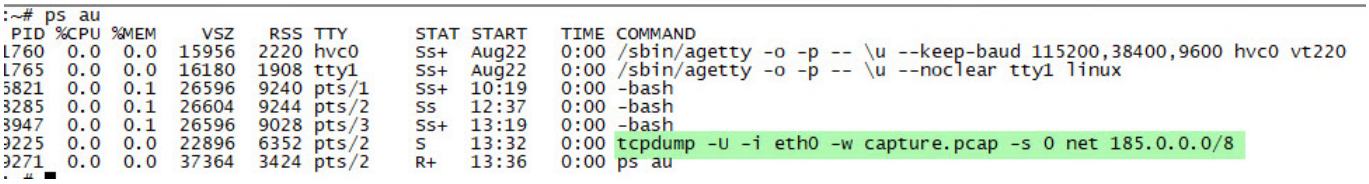
Yenilenen teknik altyapıları ile tüm sunucuları SSD diskler üzerine bulut sunucu mimarisine geçmiştir. Hosting.com.tr, klasik hosting hizmeti fiyatları ile SSD disklerde hizmet vermektedir. Bu çerçevede kaliteden ödün vermeden, koşulsuz müşteri memnuniyeti odaklı prensipleri ile sürekli ve mutlu müşteri portföyünü her geçen gün büyütmek için çalışmaktadırlar.

VDSlerime kavuştuktan sonra sözlük saldırısına dair HTTP trafiğine göz atmaya devam ettim ve /wp-login.php sayfasına önce GET ardından POST isteği yapıldığını gördüm. Bu durumda yapılan ilk GET isteğinde saldırganı yeni VDS'imde barındırdığım www.mertsarica.net adresine yönlendirerek POST isteğini oraya yapmasını sağlayarak JA3 md5 özet değerini elde edebilir miydim ?



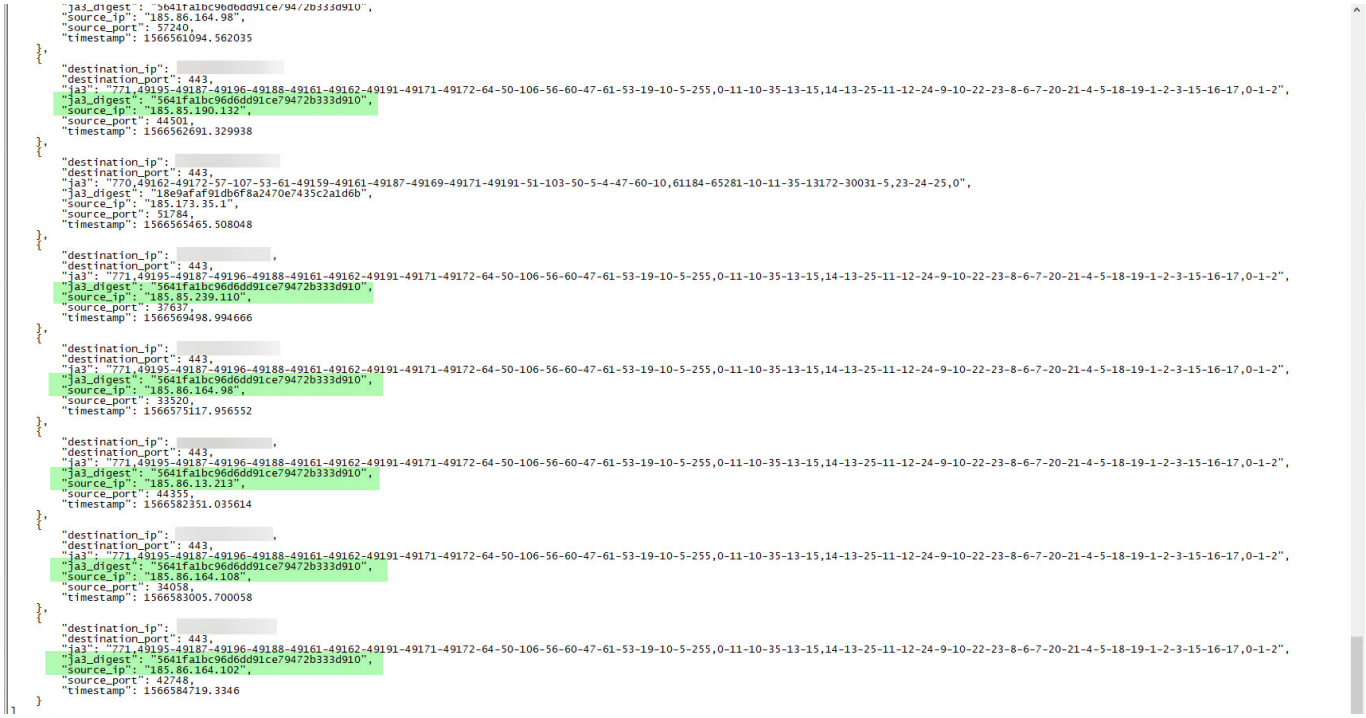
Vakit kaybetmeden ilk iş olarak www.mertsarica.net alan adımı Hosting.com.tr altyapısında barındırdığım VDS'e yönlendirdim. Daha sonra Cloudflare'nin yönetim panelinden www.mertsarica.com/wp-login.php sayfasına yapılan tüm isteklerin www.mertsarica.net/wp-login.php sayfasına yönlendirilmesini sağladım. Salesforce firması tarafından geliştirilen JA3 aracını VDS'e kurduktan sonra tcpdump aracı ile www.mertsarica.net web sunucusuna yapılan bağlantıları kayıt altına almaya başladım.





```
:~# 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
```

Aradan bir gün geçtikten sonra tcpdump aracının çıktısına baktığımda sözlük saldırısını gerçekleştiren 6 farklı ip adresinin JA3 md5 özet değerinin (5641fa1bc96d6dd91ce79472b333d910) aynı olduğunu gördüm. Bu bilgiden yola çıkarak saldırıyı gerçekleştiren tüm sistemlerde aynı aracın kullanıldığını öğrenmiş oldum. Sıra hangi araç ile bu saldırının gerçekleştirildiğini öğrenmeye geldiğinde hemen bu md5 özet değerini JA3 parmak izi bilgilerinin tutulduğu JA3 SSL Fingerprint web sayfasında arattım ancak herhangi bir kayıt bulamadım. Bir gün bu md5 özet değerine dair bilginin JA3 SSL Fingerprint web sitesine ekleneceğini ümit ederek güvenlik araştırmamı burada sonlandırdım.



Kıssadan hisse, sizler de JA3 metodundan faydalanarak ağınızda gerçekleştirilen şüpheli, zararlı aktiviteleri tespit edebilir, benim gibi gerçekleştirilen siber saldırılara dair aklınızı kurcalayan sorulara yanıt bulabilirsiniz. Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.