Sanal Obruk

written by Mert SARICA | 1 March 2014

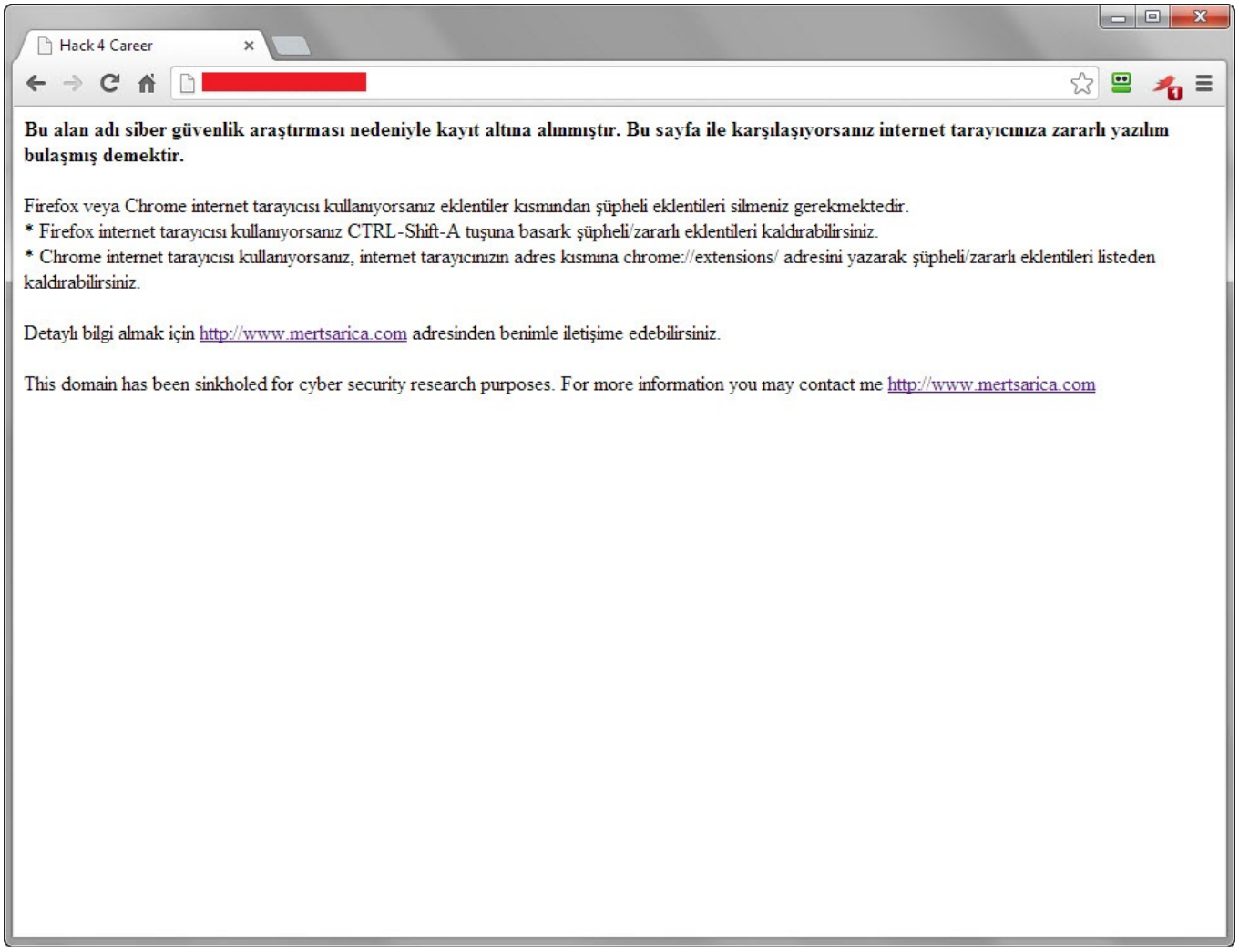
Obruk, yatay veya yataya yakın tabakalı kireçtaşlarında bulunan yeraltı nehirlerinin veya aktif mağara tavanlarının çökmesi sonucu oluşmuş baca veya kuyu görüntüsü veren derin çukurluklardır. Sanal obruk (sinkhole) ise zararlı yazılımlarla yapılan mücadelede, zararlı yazılım salgınını (özellikle solucanlar) durdurmak, zararlı yazılım bulaşan sistemlerin sayısını tespit etmek ve zararlı yazılım hakkında bilgi toplamak için güvenlik firmaları, güvenlik araştırmacıları ve zararlı yazılım analistleri tarafından komuta kontrol merkezini ele geçirmeye yönelik kullanılan bir yöntemdir.

Bu yöntemde öncelikle zararlı yazılımın haberleştiği komuta kontrol merkezi tespit edilir. Ardından alan adını kayıt eden firma ile iletişime geçilerek alan adının güvenlik firmasına transfer edilmesi sağlanarak sunucu üzerine gelen trafik güvenlik firması tarafından analiz edilmektedir. Bunun dışında zararlı yazılım içinde gömülü olan DGA (domain generation algorithm) analiz edilerek, zararlı yazılımın ilerleyen zamanlarda haberleşeceği muhtemel alan adları tespit edilerek kayıt altına alınmakta ve trafiğin analiz edilmesi sağlanmaktadır. Bunlara ilave olarak komuta kontrol merkezi olarak kullanılan alan adları, zaman aşımına uğramaya yakın bir zamanda, salgında, aktif olarak kullanılmaya başlanmış ise zaman aşımına uğraması beklenerek tekrar kayıt altına alınarakta trafik analiz edilebilmektedir.

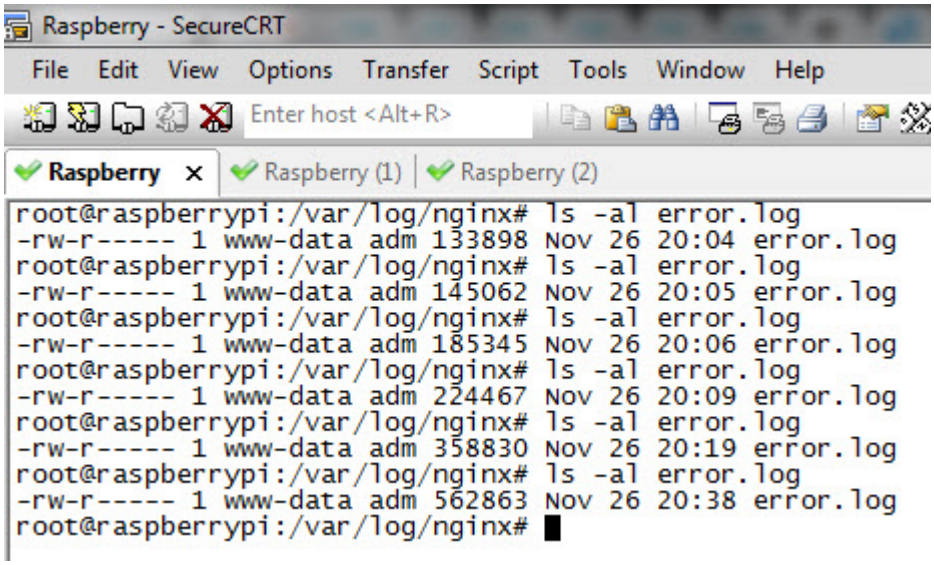
2013 yılında, sahte, zararlı Flash Player uygulaması ile insanları kandırarak internet tarayıcılarına bulaşan ve sosyal medya hesaplarını ele geçirip reklam ve dolandırıcılık yapmaya çalışan çok sayıda zararlı yazılım ile karşılaştık ve hemen hemen her salgında zararlı yazılımların farklı alan adları ile haberleştiğini gördük. Bu salgınlarda dikkatimi çeken, yeni kayıt edilen her alan adının en fazla bir senelik alınması olmuştu. Bunu fırsat bilerek daha önce analiz ettiğim bir zararlı yazılım tarafından kullanılan ve zaman aşımı nedeniyle kaydı düşmüş olan bir alan adını kayıt ederek (sinkhole), 1.5 sene sonunda bu zararlı yazılımın ne kadar aktif olduğunu trafiği analiz ederek anlamaya çalıştım.

Bunun için zararlı yazılım tarafından kullanılan ve kayıt altına aldığım alan adını, üzerinde Raspbian ve Nginx kurulu olan Raspberry Pi cihazına yönlendirerek, zararlı yazılım bulaşmış sistemlerden gelen trafiği 14 saat boyunca izlemeye başladım. Tabii kazara veya bilinçli bir şekilde bu alan

adına bağlananları, bu alan adının bir güvenlik araştırması nedeniyle kayıt altına alındığı konusunda da bilgilendirmeyi ihmal etmedim.



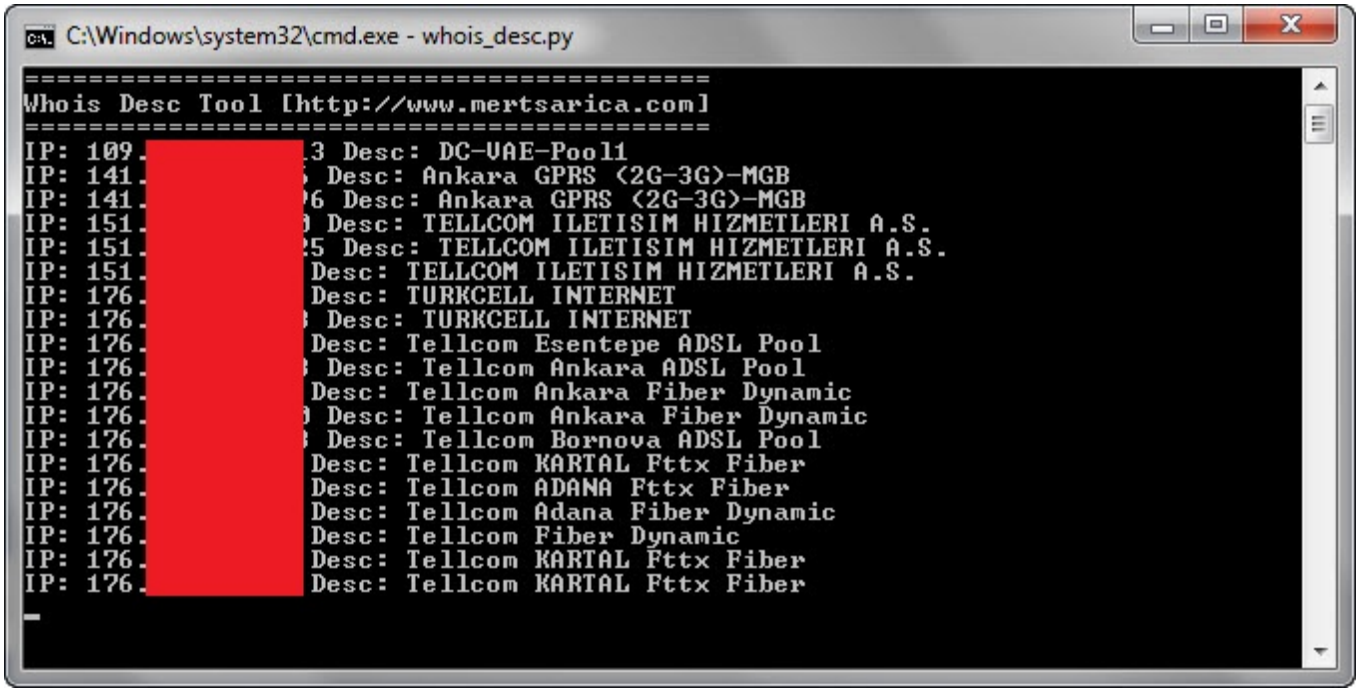
Trafiği izlemeye başladıktan 35 dakika sonra access.log dosyasının 400 KB olduğunu gördüm ve bu durum bana 1.5 sene sonra dahi zararlı yazılım bulaşmış sistemlerin halen aktif olduğunu göstermiş oldu.

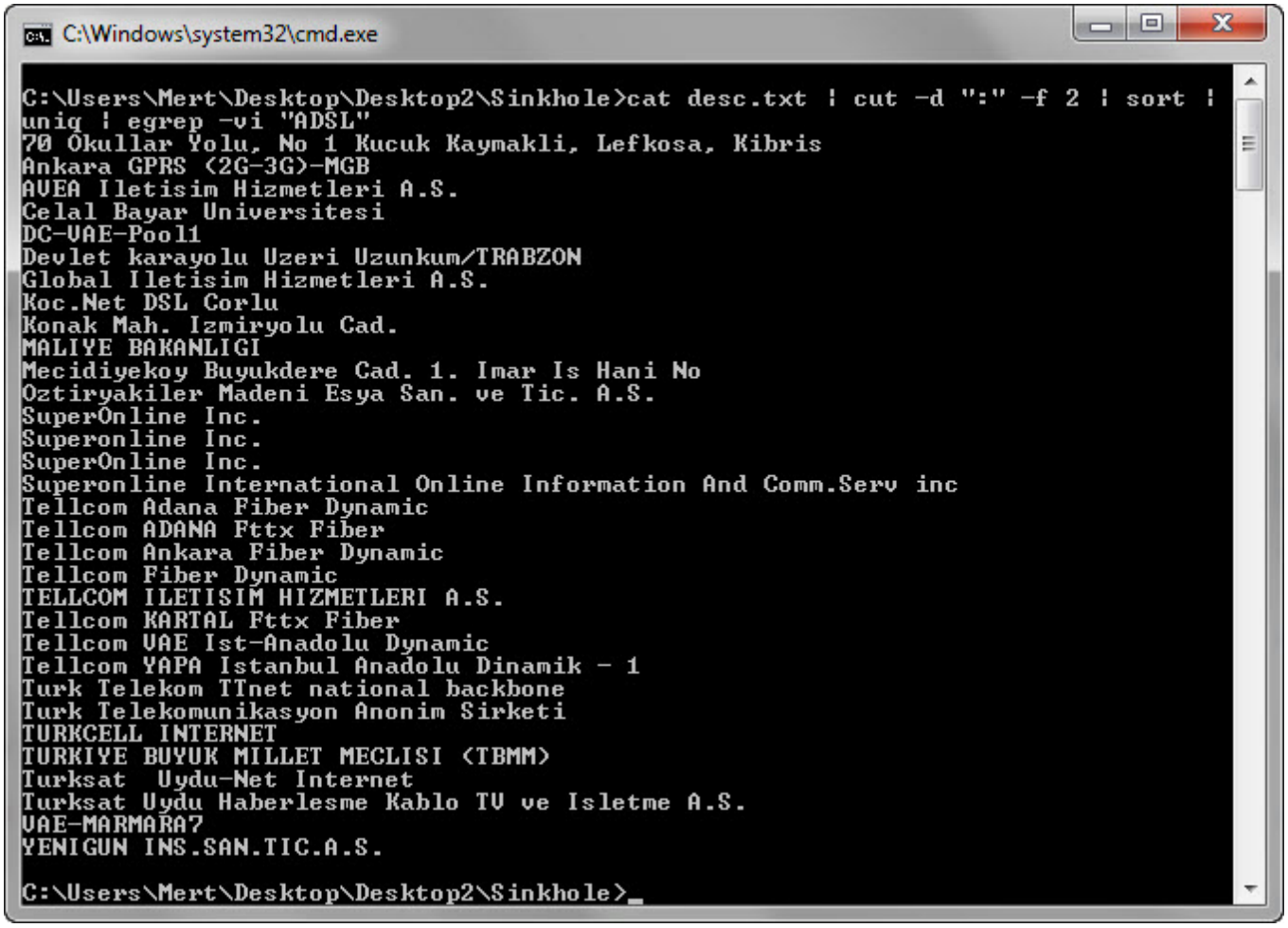


14 saatin sonunda access.log dosyasını, en son yıllar yıllar önce kullandığım

Sawmill aracı ile incelemeye başladım ve alan adını bu zaman zarfında 274 kişinin ziyaret etmiş olduğunu ve 40.300 hit aldığını gördüm.

274 ip adresinin IP blok bilgilerini daha önce Python ile geliştirmiş ve yayınlamış olduğum WHOIS DESC aracı ile topladığımda, çoğunun ADSL kullanıcıları olduğunu gördüm fakat bu zararlı yazılımın TBMM, Maliye Bakanlığı IP bloklarında kullanılan sistemlere bulaşmış olduğu da dikkatimden kaçmadı. (Yetkililer dilerlerse ilgili IP adresleri hakkında bilgi almak için benimle iletişime geçebilirler.)





Zararlı yazılım, Javascript dosyası çağırdığı için normal olarak en çok çağırılan dosya uzantısı JS olmuştu. Ziyaretçilerin kullandığı internet tarayıcıları sıralamasında Firefox'un en üst sırada yer alması da bu zararlı yazılımdan en çok ve kalıcı olarak Firefox kullanıcılarının etkilendiğini gösteriyordu. Bu zararlı eklenti, ziyaret edilen her siteden gelen yanıt paketine, komuta kontrol merkezinden bir javascript dosyası çağıracak şekilde programlandığı için ziyaret edilen her siteye ait kayıtlar, komuta kontrol merkezinde de yer almaktaydı dolayısıyla referrers kayıtları, sisteminde zararlı yazılım bulunanların ziyaret ettiği siteleri gösteriyordu.

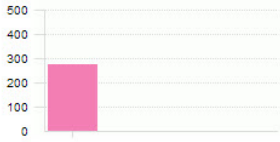
Overview

Hits	Visitors	Size	Page views	Sessions	Session duration	Bounces	Bounce Rate
40,300 Avg/day —	274 Avg/day —	10.28 M Avg/day —	22 Avg/day —	10 Avg/day —	00:12:51 Avg/day —	4 Avg/day —	40.00% Avg/day —

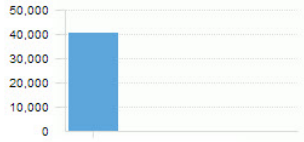
Traffic

Page views

Visitors

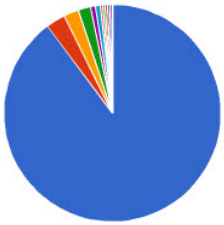


Hits



Country

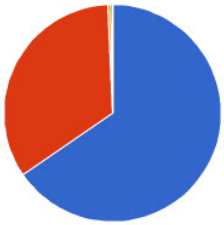
Visitors *(descending)*



89.8 %	Turkey
2.9 %	Azerbaijan
2.2 %	United States
1.8 %	Morocco
0.7 %	Belgium
0.7 %	Germany
0.4 %	India
0.4 %	Vietnam
0.4 %	Netherlands
0.4 %	China

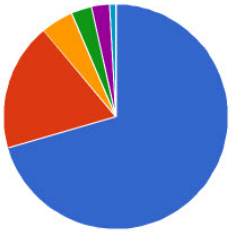
Device Category

Visitors *(descending)*



65.4 %	Non-mobile (desktop, laptop, server)
33.8 %	Unknown
0.5 %	Mobile (phone, tablet)
0.2 %	Spider

Hits *(descending)*



70.5 %	28,410	Firefox
18.4 %	7,405	Internet Explorer
4.7 %	1,896	unspecified
2.9 %	1,185	Mozilla
2.6 %	1,055	Chrome
0.8 %	338	Opera
0.0 %	6	unknown (possible spider)
0.0 %	4	Safari
0.0 %	1	(spider)

	Web browser	↓ Hits		Visitors	Size	Page views	Sessions	Session duration	Bounces	Bounce Rate
1	Firefox	28,410	70.5 %	119	5.20 M	3	2	00:00:00	1	50.00%
2	Internet Explorer	7,405	18.4 %	108	4.19 M	12	6	00:12:51	1	16.67%
3	unspecified	1,896	4.7 %	138	1.44 K	5	1	00:00:00	0	0.00%
4	Mozilla	1,185	2.9 %	37	221.63 K	0	0	00:00:00	0	0.00%
5	Chrome	1,055	2.6 %	11	611.98 K	0	0	00:00:00	0	0.00%

	Referrer	↓ Hits		Visitors	Size	Page views	Sessions	Session duration	Bounces	Bounce Rate
1	(no referrer)	8,679	21.5 %	158	1.25 M	17	6	00:12:51	3	50.00%
2	http://www.milliyet.com.tr/(omitted)	5,028	12.5 %	16	1.11 M	0	0	00:00:00	0	0.00%
3	http://googleads.g.doubleclick.net/(omitted)	3,554	8.8 %	93	866.42 K	0	0	00:00:00	0	0.00%
4	http://www.sahibinden.com/(omitted)	1,726	4.3 %	19	532.87 K	0	0	00:00:00	0	0.00%
5	http://ts7.travian.com.tr/(omitted)	1,043	2.6 %	6	195.56 K	0	0	00:00:00	0	0.00%
6	http://reklam.milliyet.com.tr/(omitted)	647	1.6 %	9	121.31 K	0	0	00:00:00	0	0.00%
7	http://www.youtube.com/(omitted)	604	1.5 %	63	168.60 K	0	0	00:00:00	0	0.00%
8	http://eu-u.openx.net/(omitted)	526	1.3 %	10	99.80 K	0	0	00:00:00	0	0.00%
9	http://ng2.virgul.com/(omitted)	453	1.1 %	6	85.33 K	0	0	00:00:00	0	0.00%
10	http://ext.ciceksepeti.com/(omitted)	427	1.1 %	1	247.69 K	0	0	00:00:00	0	0.00%
11	http://ads.milliyet.cubecdn.net/(omitted)	399	1.0 %	8	74.81 K	0	0	00:00:00	0	0.00%
12	http://www.gittigidiyor.com/(omitted)	367	0.9 %	7	212.89 K	0	0	00:00:00	0	0.00%
13	http://tr.msn.com/(omitted)	355	0.9 %	15	76.38 K	0	0	00:00:00	0	0.00%
14	http://ib.adnxs.com/(omitted)	311	0.8 %	22	96.00 K	0	0	00:00:00	0	0.00%
15	http://static.adhood.com/(omitted)	250	0.6 %	10	48.05 K	0	0	00:00:00	0	0.00%
16	http://www.girlsgogames.com.tr/(omitted)	223	0.6 %	1	41.81 K	0	0	00:00:00	0	0.00%
17	http://tr.adsplats.com/(omitted)	222	0.6 %	2	113.86 K	0	0	00:00:00	0	0.00%
18	http://cm.g.doubleclick.net/(omitted)	222	0.6 %	30	68.71 K	0	0	00:00:00	0	0.00%
19	http://platform.linkedin.com/(omitted)	219	0.5 %	8	121.93 K	0	0	00:00:00	0	0.00%

Görüldüğü üzere internet tarayıcılarına eklenti olarak bulaşan bu ve benzer zararlı yazılımlar kolay kolay temizlenememekte ve komuta kontrol merkezi olarak kullanılan alan adları, zaman aşımına uğradıktan sonra bile sistemde var olmaya devam etmektedir. Her ne kadar sistemde bu zararlı eklentiler var olmaya devam etse de, komuta kontrol merkezleri olarak kullanılan bu alan adlarının, zaman aşımı nedeniyle bir tehdit oluşturmadığını düşünülebilir fakat art niyetli kişilerin zaman aşımına uğramış alan adlarını tekrar kayıt ederek, kendisine gelen tüm istekleri istismar kiti yüklü olan sitelere yönlendirme ve/veya Beef gibi bir araca yönlendirme ihtimali asla göz ardı edilmemelidir.

Zararlı yazılım ihtimaline karşı belli aralıklarda internet tarayıcınızın eklentilerini kontrol etmenizi önerir, bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.