

ABCD BANKASI ADLİ BİLİŞİM İNCELEME RAPORU

ADLİ BİŞİLİM İNCELEME RAPORU

RAPORU HAZIRLAYAN: TUNAHAN GÖKGÖZ

16 MAYIS 2025

BÜTÜN HAKLARI SAKLIDIR.

BU BELGE "GİZLİ" BİLGİLER İÇERMEKTEDİR. SAHİPLİĞİ VE MÜLKİYET HAKLARI BUSİBER'E AİTTİR. RAPORUN BÜTÜNÜ VEYA HERHANGİ BİR PARÇASI, BUSİBER BOĞAZICI SİBER GÜVENLİK AŞ'İN YAZILI ŞEKİLDE İZİN OLMDAN HERHANGİ BİR ŞEKİLDE AÇIKLANAMAZ, GÖSTERİLEMEZ, KOPYALANAMAZ VEYA ÇÖĞALTILAMAZ.

Önsöz:

Adli Analiz ve Siber Olay Müdahale işlemi uzlaşma göstergelerini (indicators of compromise) tespit etme süreçlerini tanımlar.

Adli analiz ve siber olay müdahale süreci, bir sistemde gerçekleşmiş olası siber saldırıların teknik izlerini (Indicators of Compromise - IoC) tespit ederek saldırının türünü, kapsamını ve etkisini belirlemeyi amaçlar. Bu süreçte ağ trafiği, zararlı yazılım izleri ve sistem davranışları analiz edilerek saldırının kaynağı ve yöntemi ortaya çıkarılır.

Ağ adli bilişimi, ağ üzerinden geçen paketlerin incelenmesiyle tehditlerin analiz edilmesini içerirken; bilgisayar adli bilişimi, bireysel sistemlerin (masaüstü, dizüstü vb.) iç yapısındaki kayıtların (log, RAM, disk vb.) incelenmesini kapsar. Bu iki yaklaşım, siber saldırıların tam anlamıyla aydınlatılmasında birlikte çalışarak etkin sonuçlar üretir.

Özetle siber olay müdahale ve adli analizinin özü, sistemdeki olağandışı durumları aramaya dayanır. Burada hafıza analizi önemli bir rol oynar. Bu çalışmada siber saldırıda bulunan sunuculara yönelik ram analiz, yapılmış sonuçları rapor olarak sunulmuştur.

SİZİN HAKKINIZDA KISA CV

Boğaziçi Üniversitesi Yönetim Bilişim Sistemleri öğrencisiyim. Siber güvenlik alanına özel ilgi duyuyor ve EC-Council Certified Cybersecurity Technician (C|CT) eğitimini aktif olarak tamamlıyorum. Pentest uygulamaları, Wireshark, Brim ve virustotal gibi analiz araçlarıyla pratik deneyim sahibiyim. Bu raporda yer alan analizleri kendi sanal laboratuvar ortamımda gerçekleştirdim.

İÇİNDEKİLER

1. TESPİT TALEBİ ve TESPİTİ İSTENEN HUSUSLAR.....	3
1.1. Dijital Materyaller.....	3
1.2. Analizlerde kullanılan araçlar:	3
1.3. İncelemenin yapıldığı bilgisayar ve özellikleri	3
2. Bahse konu olan “c09a3019ada7ab17a44537b069480312” md5 özet değerli dijital materyalin incelenmesi.....	4
2.1 Ağ Trafik Analizi ile Elde Edilen Bulgular	4
2.2. DNS ve Alan Adı Tabanlı İletişim	5
2.3. Virustotal Tabanlı Zararlı Yazılım İncelemesi.....	7
2.3.1 q.jar – Java Exploit Dosyası (CVE-2012-1723)	7
2.3.2 sdfg.jar – Java Exploit Dosyası (Bytverify)	8
2.3.3 loading.php – PE32 Zararlı Yürütülebilir Dosya (SpyEye).....	9
2.4 Saldırı Zinciri Zaman Çizelgesi ve Şüpheli Aksiyonların Kronolojisi.....	10
3. SONUÇ VE DEĞERLENDİRME	11

1. TESPİT TALEBİ ve TESPİTİ İSTENEN HUSUSLAR

Tarafıma tevdi edilen **ağ trafiği kayıtlarının** incelenerek, “içerisindeki bilgilerin teknik analizinin gerçekleştirilmesi” amacıyla rapor hazırlanması talep edilmiştir. Dijital delillere ait bilgileri ve teknik incelemesi aşağıda paylaşılmıştır.

1.1. Dijital Materyaller

MD5 Özet Değeri	c09a3019ada7ab17a44537b069480312
Sha1 Özet Değeri	0a7549eba016de22e4f6f65c960743f92679f29b
Dosya Adı	infected-c09.pcap
Alınma Tarih-Saati (UTC)	2025-14-05 20:43:34
Bilgisayar Adı	TICKLAB

1.2. Analizlerde kullanılan araçlar:

- Wireshark
- Brim IDS
- <https://virustotal.com>
- <https://any.run>
- IP geolocation servisleri (ipapi.is, ip2location.com)
- Hash hesaplama araçları (md5sum, sha1sum)

1.3. İncelemenin yapıldığı bilgisayar ve özellikleri

Cihaz: MacBook Air M1 (2020)

RAM: 8 GB

İşlemci: Apple Silicon (ARM64)

İşletim Sistemi: macOS

2. Bahse konu olan “c09a3019ada7ab17a44537b069480312” md5 özet değerli dijital materyalin incelenmesi

2.1 Ağ Trafiği Analizi ile Elde Edilen Bulgular

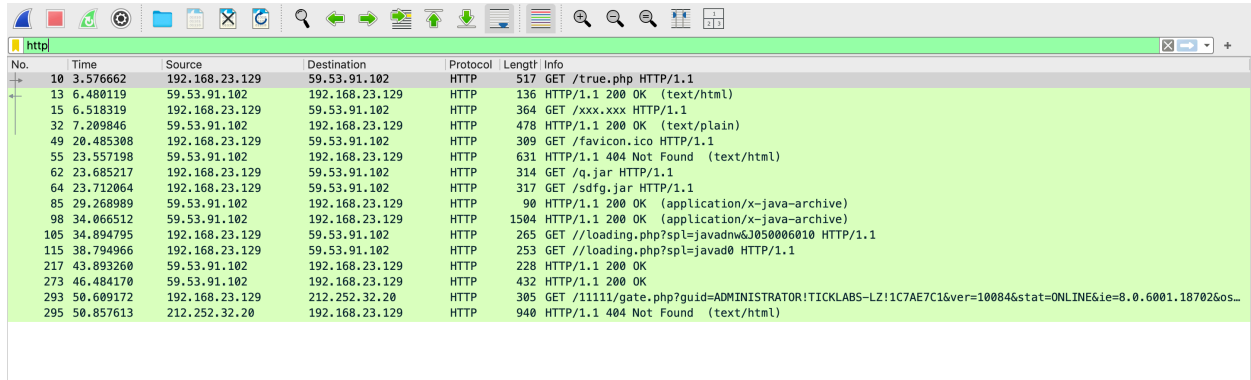
Adli bilişim kapsamında ağ trafiği analizi, bir sistemin dış dünya ile kurduğu bağlantıların detaylı olarak incelenmesini sağlar. Bu analiz yöntemiyle, kötü niyetli bir yazılımın hedef sisteme nasıl ulaştığı, hangi adımlar üzerinden bulaştığı ve saldırgan ile nasıl iletişim kurduğu ortaya çıkarılabilir. Ağ trafiği tipik olarak OSI modelinin katmanları boyunca gerçekleşen veri alışverişlerinin, özellikle de uygulama katmanındaki protokollerin (HTTP, DNS, FTP, SMTP vb.) analiz edilmesiyle değerlendirilir.

Bu çalışmada analiz edilen .pcap dosyası, HTTP protokolü üzerinden gerçekleşen zararlı bağlantıların açık izlerini taşımaktadır. Paketler arasında yapılan sıralı analizde, kurban sistemin belirli IP adreslerine gerçekleştirdiği HTTP GET istekleri dikkat çekmiştir. Bu istekler, sırasıyla bir giriş noktasına (true.php), iki Java exploit dosyasına (q.jar, sdfg.jar) ve sonrasında bir PE32 yürütülebilir dosya içeren .php URI'sine yönelmiştir. HTTP trafiğinin detaylı incelenmesiyle, bu bağlantıların zararlı içerik taşımak üzere yapılandırıldığı anlaşılmıştır.

Trafik analizinde dikkat çeken bir diğer nokta da, hedef IP adreslerinin sabit olması ve DNS üzerinden çözümlenmiş olmalarıdır. Bu durum, saldırganın sabit ve önceden yapılandırılmış bir altyapı (exploit kit veya C2 paneli) üzerinden saldırı gerçekleştirdiğini düşündürmektedir. Wireshark kullanılarak elde edilen bu ağ izleri, saldırının çok katmanlı olduğunu ve exploit kit üzerinden çalıştığını ortaya koymuştur. Analiz sürecinde filtreleme, paket takibi (Follow TCP Stream), içerik tiplerinin kontrolü (Content-Type), dosya transfer boyutları ve User-Agent gibi HTTP başlıkları değerlendirilmiş; saldırı zinciri bütünsel olarak ortaya konmuştur.

Sonuç olarak, ağ trafiği analizi yoluyla saldırının ilk teması, dosya aktarım sıralaması ve potansiyel komuta ve kontrol iletişimi başarılı şekilde tespit edilmiş ve raporlanmıştır.

Zaman (sn)	İstek Türü	Hedef IP / Alan Adı	URI	Açıklama
3.57	GET	59.53.91.102	/true.php	Exploit kit giriş noktası
23.68	GET	59.53.91.102	/q.jar	Java exploit (CVE-2012-1723)
23.71	GET	59.53.91.102	/sdfg.jar	Java exploit
34.89	GET	59.53.91.102	/loading.php?...	PE32 zararlısı (SpyEye)
50.60	GET	212.252.32.20	/11111/gate.php?...	Olası C2 bağlantısı



No.	Time	Source	Destination	Protocol	Length	Info
10	3.576662	192.168.23.129	59.53.91.102	HTTP	517	GET /true.php HTTP/1.1
13	6.480119	59.53.91.102	192.168.23.129	HTTP	136	HTTP/1.1 200 OK (text/html)
15	6.518319	192.168.23.129	59.53.91.102	HTTP	364	GET /xxx.xxx HTTP/1.1
32	7.209846	59.53.91.102	192.168.23.129	HTTP	478	HTTP/1.1 200 OK (text/plain)
49	20.485308	192.168.23.129	59.53.91.102	HTTP	309	GET /favicon.ico HTTP/1.1
55	23.557198	59.53.91.102	192.168.23.129	HTTP	631	HTTP/1.1 404 Not Found (text/html)
62	23.685217	192.168.23.129	59.53.91.102	HTTP	314	GET /q.jar HTTP/1.1
64	23.712064	192.168.23.129	59.53.91.102	HTTP	317	GET /sdfg.jar HTTP/1.1
85	29.268989	59.53.91.102	192.168.23.129	HTTP	90	HTTP/1.1 200 OK (application/x-java-archive)
98	34.066512	59.53.91.102	192.168.23.129	HTTP	1504	HTTP/1.1 200 OK (application/x-java-archive)
105	34.894795	192.168.23.129	59.53.91.102	HTTP	265	GET //loading.php?spl=javaadm6j050006010 HTTP/1.1
115	38.794966	192.168.23.129	59.53.91.102	HTTP	253	GET //loading.php?spl=java0 HTTP/1.1
217	43.893260	59.53.91.102	192.168.23.129	HTTP	228	HTTP/1.1 200 OK
273	46.484170	59.53.91.102	192.168.23.129	HTTP	432	HTTP/1.1 200 OK
293	50.609172	192.168.23.129	212.252.32.20	HTTP	305	GET /11111/gate.php?guid=ADMINISTRATOR!TICKLABS-LZ!1C7AE7C1&ver=10084&stat=ONLINE&ie=8.0.6001.18702&os=...
295	50.857613	212.252.32.20	192.168.23.129	HTTP	940	HTTP/1.1 404 Not Found (text/html)

Resim 1: "http" filtresi ile wireshark analizi

2.2. DNS ve Alan Adı Tabanlı İletişim

İncelenen .pcap dosyasında, saldırıya maruz kalan sistem tarafından yapılan DNS sorguları ve karşılık gelen IP yanıtları aşağıdaki gibi tespit edilmiştir. Bu sorgular sonucunda elde edilen IP'lere HTTP üzerinden bağlantılar gerçekleştirilmiştir.

Sorgulanan Alan Adı	Yanıtlanan IP	Açıklama
nrtjo.eu	59.53.91.102	HTTP trafiğinin yoğunlaştığı adres
freeways.in	212.252.32.20	Son bağlantının yapıldığı adres

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.23.129	192.168.23.2	DNS	68	Standard query 0xfa1c A nrtjo.eu
2	0.988900	192.168.23.129	192.168.23.2	DNS	68	Standard query 0xfa1c A nrtjo.eu
3	1.987301	192.168.23.129	192.168.23.2	DNS	68	Standard query 0xfa1c A nrtjo.eu
4	2.909144	192.168.23.2	192.168.23.129	DNS	162	Standard query response 0xfa1c A nrtjo.eu A 59.53.91.102 NS ns2.vnmhab.com NS ns1.vnmhab.com A 59.53.9...
6	2.929185	192.168.23.2	192.168.23.129	DNS	162	Standard query response 0xfa1c A nrtjo.eu A 59.53.91.102 NS ns1.vnmhab.com NS ns2.vnmhab.com A 59.53.9...
7	2.930238	192.168.23.2	192.168.23.129	DNS	162	Standard query response 0xfa1c A nrtjo.eu A 59.53.91.102 NS ns1.vnmhab.com NS ns2.vnmhab.com A 59.53.9...
43	19.900252	192.168.23.129	192.168.23.2	DNS	68	Standard query 0x5b1d A nrtjo.eu
44	19.971014	192.168.23.2	192.168.23.129	DNS	162	Standard query response 0x5b1d A nrtjo.eu A 59.53.91.102 NS ns1.vnmhab.com NS ns2.vnmhab.com A 59.53.9...
90	29.821145	192.168.23.129	192.168.23.2	DNS	85	Standard query 0xe78a PTR 102.91.53.59.in-addr.arpa
93	30.666108	192.168.23.2	192.168.23.129	DNS	143	Standard query response 0xe78a No such name PTR 102.91.53.59.in-addr.arpa S0A ns.jxncptt.net.cn
288	50.210596	192.168.23.129	192.168.23.2	DNS	71	Standard query 0xbca3 A freeways.in
289	50.310134	192.168.23.2	192.168.23.129	DNS	235	Standard query response 0xbca3 A freeways.in A 212.252.32.20 NS ns3.everydns.net NS ns1.everydns.net N...

Resim 2: “dns” filtresi ile wireshark analizi

DNS sorgularının Wireshark üzerindeki dns filtrelemesiyle tespit edildiği görülmüştür. Özellikle nrtjo.eu alan adı, saldırı zincirinin başlatıcısı olan /true.php URI'si ile doğrudan ilişkilidir. Aynı şekilde, freeways.in adresi üzerinden gerçekleştirilen gate.php isteği, saldırının son aşamasında kullanılmıştır.

IP Adresi	Ülke	Şehir	ISP
59.53.91.102	Çin	Nanchang	CHINANET Jiangxi Province Network
212.252.32.20	Türkiye	İstanbul	Tellcom ISP (Türk Telekom altyapısı)

DNS sorgularıyla elde edilen IP adreslerinin fiziksel lokasyonları ve hizmet sağlayıcıları, farklı coğrafi veri servislerinden (ipapi.is, ip2location.com) alınan bilgiler ışığında aşağıdaki gibidir: Coğrafi analizde her iki IP adresi için de lokasyon bilgisi genel olarak uyumludur. Özellikle 59.53.91.102 adresi, zararlı yazılım dağıtımı yapılan ilk HTTP bağlantılarının gerçekleştiği noktadır ve **Çin'e ait geniş ISP bloklarında** yer almaktadır. Bazı servislerin şehir/koordinat düzeyinde farklılık göstermesi, IP coğrafi konum verilerinin %100 kesinlikte olmamasından kaynaklanmaktadır. Ancak ülke düzeyinde tespitler oldukça güvenilir sayılmaktadır.

212.252.32.20 ise Türkiye kaynaklı bir sunucuya aittir. Trafikte bu IP'ye yapılan bağlantı, saldırının ilerleyen aşamalarında gerçekleştirilmiş olup, olası komuta ve kontrol (C2) sunucusu işlevi gördüğü değerlendirilmektedir.

2.3. Virustotal Tabanlı Zararlı Yazılım İncelemesi

Bu bölümde, .pcap dosyası üzerinde tespit edilen HTTP bağlantıları ile indirilen dosyaların hash değerleri hesaplanmış ve Virustotal üzerinde analiz edilmiştir. Bu analiz sayesinde indirilen içeriklerin zararlı yazılım içerip içermediği değerlendirilmiş, tehdit tipi, istismar ettiği zafiyetler (CVE), davranış kalıpları ve saldırının amacı hakkında çıkarımlar yapılmıştır. İncelenen 3 dosya da yüksek oranda zararlı yazılım olarak işaretlenmiş, tehdit sınıflandırmaları ve AV motorlarının yorumları bu bölümde detaylı biçimde sunulmuştur.

Dosya Adı	Bağlantı URI	Dosya Türü	Tespit Oranı (AV)	Etiketler / CVE Bilgisi	Açıklama
q.jar	/q.jar	Java JAR	38 / 63	Trojan.Java.GenericGB , Exploit.CVE-2012-1723	Java applet ile RCE sağlayan exploit dosyası
sdfg.jar	/sdfg.jar	Java JAR	44 / 65	Trojan.Java.Bytverify , Exploit.Java.Generic	Java runtime içindeki güvenlik açıklarını sömüren JAR
loading.php	/loading.php? spl=...	PE32 EXE	66 / 72	Trojan.Spy.SpyEye , SpyBot , Banking Trojan	Zararlı yürütülebilir dosya, keylogger ve C2 iletişimi içeriyor

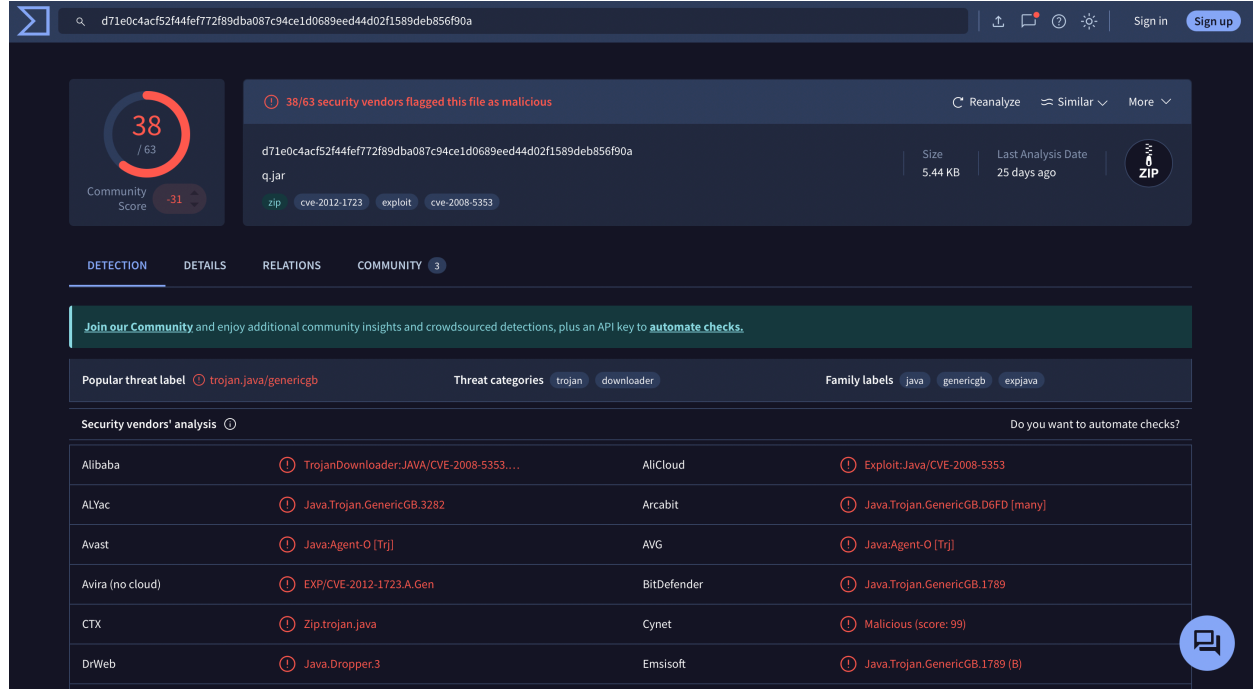
2.3.1 q.jar – Java Exploit Dosyası (CVE-2012-1723)

Bu dosya 59.53.91.102 adresine yapılan bir GET isteğiyle (/q.jar) indirilmiştir. Java tabanlı bir .jar uzantılı arşiv dosyasıdır. SHA256 değeri üzerinden Virustotal’da yapılan analizde 38 farklı antivirüs motoru tarafından zararlı olarak işaretlenmiştir. Etiketlemeler ağırlıklı olarak Trojan.Java.GenericGB ve Exploit.Java.CVE-2012-1723 biçiminde gerçekleşmiştir. Bu CVE, Java’nın 7 sürümüne ait bir güvenlik açığı olup, tarayıcı üzerinden Java Applet çalıştırılarak kurban sistemde uzaktan kod çalıştırılmasına olanak tanır.

Bu tür .jar dosyaları genellikle exploit kitlerin ilk aşamasında kullanılır. Kullanıcı sisteme bir şekilde bu Applet’i yüklediğinde, arka planda sessizce başka zararlı içerikler indirilip çalıştırılır.

SHA256: d71e0c4acf52f44fef772f89dba087c94ce1d0689eed44d02f1589deb856f90a

MD5: 0cf8b61b5c26d1eaa3f6bfe9246c45a7



Şekil 3 : q.jar virüstenalizi

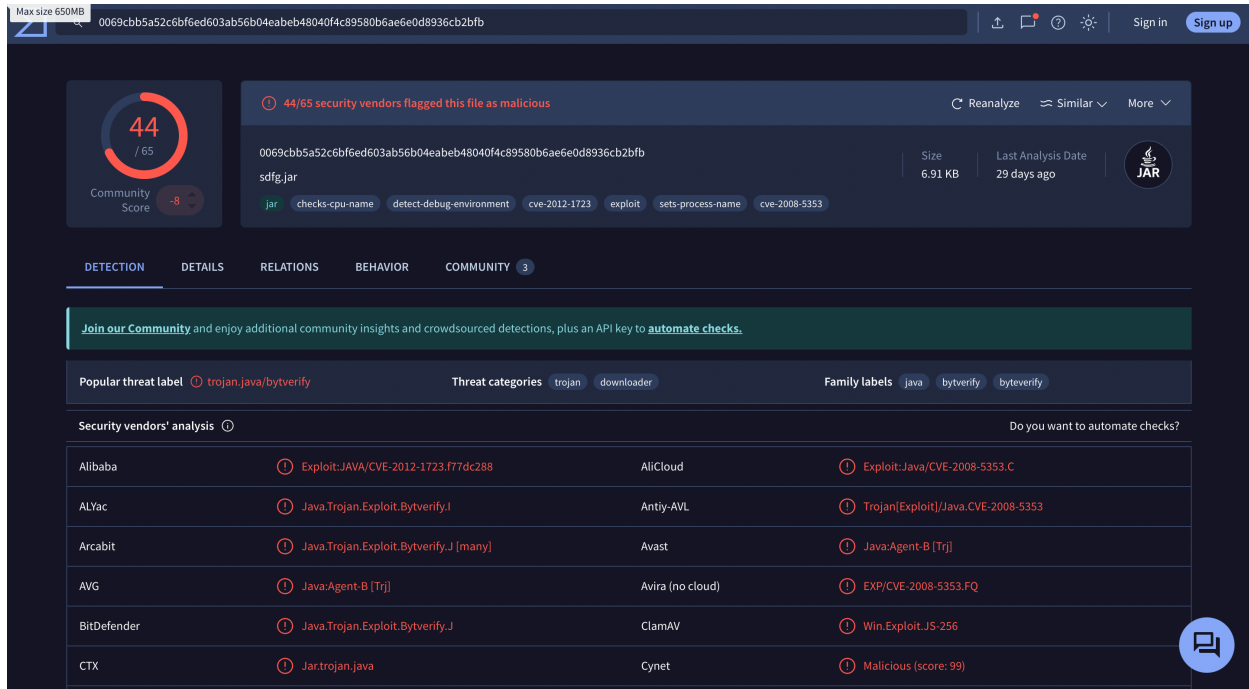
2.3.2 sdfg.jar – Java Exploit Dosyası (Bytverify)

59.53.91.102 adresinden /sdfg.jar URI'siyle indirilen bu dosya, yine Java tabanlı bir JAR arşividir. 44/65 AV motoru tarafından zararlı olarak işaretlenmiştir. Bu dosya özellikle Trojan.Java.Bytverify etiketi ile tanımlanmış ve Exploit.Java.Generic sınıfına dahil edilmiştir. Bytverify exploitleri, Java sınıflarının derlenmiş versiyonları üzerinde çalışarak kod bütünlüğünü bozan veya kodu manipüle eden saldırılar içerir.

Yapılan analiz sonucunda bu dosyanın da tıpkı q.jar gibi bir exploit kit parçası olduğu ve hedef sistemde ilk erişimi sağlamak üzere tasarlandığı değerlendirilmiştir.

SHA256: 0069cbb5a52c6bf6ed603ab56b04eae648040f4c89580b6ae6e0d8936cb2bfb

MD5: b0d5d52b514c9f1ed60bcfd5f3f5e0d5



Şekil 4: sdfg.jar virüstopal analizi

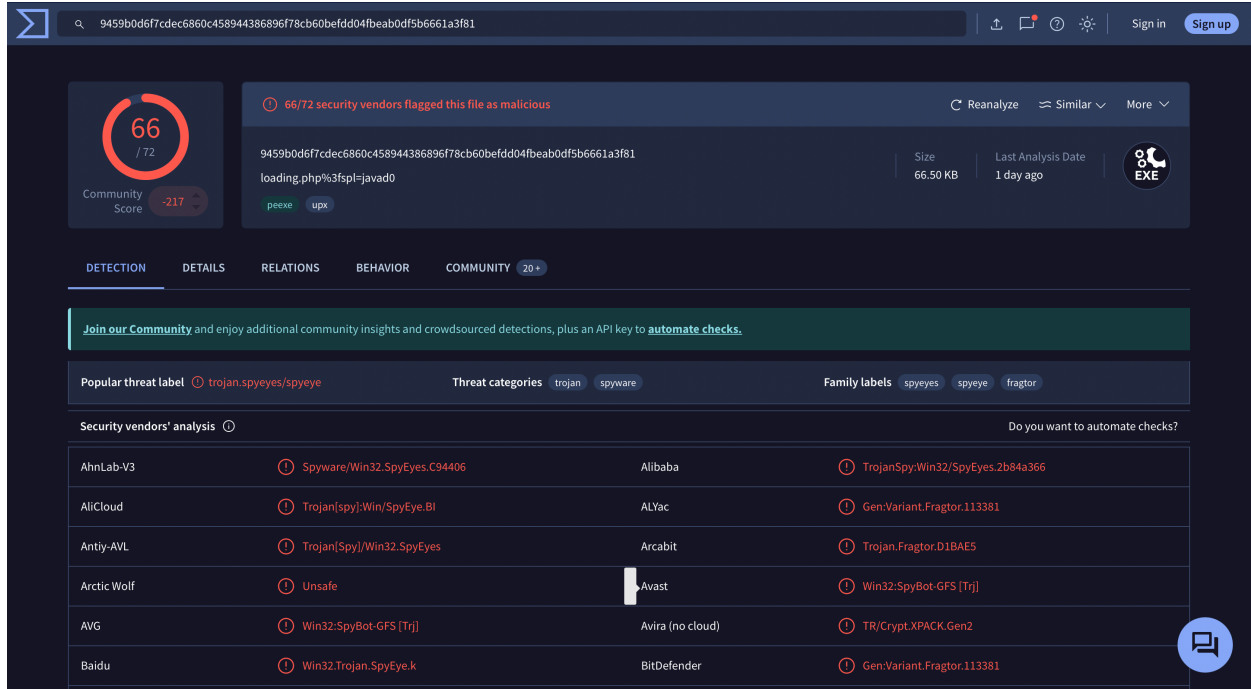
2.3.3 loading.php – PE32 Zararlı Yürütülebilir Dosya (SpyEye)

Bu dosya yine 59.53.91.102 adresine yapılan /loading.php?spl=... şeklindeki bir GET isteği ile indirilmektedir. Bu bağlantıdan dönen içerik bir PE32 formatlı EXE dosyasıdır ve sistem üzerinde doğrudan çalıştırılabilir yürütülebilir bir yapıdadır. Dosyanın hash değeri üzerinden yapılan analizde 66/72 AV motoru tarafından zararlı olarak işaretlenmiş, yaygın biçimde Trojan.Spy.SpyEye, Win32.SpyBot gibi etiketlerle tanımlanmıştır.

SpyEye, özellikle finansal bilgileri hedef alan, tarayıcı üzerinden kredi kartı verisi, oturum bilgisi ve şifre çalan bir trojan olarak bilinir. Ayrıca C2 sunucusuyla iletişim kurarak, saldırganın kurban sistemi uzaktan kontrol etmesini sağlar. Persistence özellikleri sayesinde sistem her açıldığında yeniden çalışır ve temizlenmesi zordur.

SHA256: 9459b0d6f7cdec6860c45894438696f78cb60befdd04fbeb0df5b6661a3f81

MD5: 33e5f8d0280f4c1f9b12edcf7ad53c3d



Şekil 5 :loading.php virüstopal analizi

2.4 Saldırı Zinciri Zaman Çizelgesi ve Şüpheli Aksiyonların Kronolojisi

İncelenen ağ trafiğinde gerçekleşen zararlı aktiviteler, zaman damgalarına göre analiz edilmiştir. Bu analiz ile saldırının hangi aşamada hangi bileşeni yüklediği ve bu bileşenlerin sistem üzerinde ne şekilde bir sırayla tetiklendiği belirlenmiştir. Zaman çizelgesi, saldırının gelişimini anlamak, olay yanıtı planlamak ve sistemin ne kadar sürede ele geçirildiğini tespit etmek açısından kritik öneme sahiptir.

Zaman (sn)	Kaynak IP	Hedef IP	Olay Tanımı	Açıklama
3.57	192.168.23.129	59.53.91.102	GET /true.php	İlk temas, saldırı yönlendirmesi başlıyor
23.68	192.168.23.129	59.53.91.102	GET /q.jar	Java exploit dosyası indiriliyor
23.71	192.168.23.129	59.53.91.102	GET /sdfg.jar	İkinci Java exploit iniyor
34.89	192.168.23.129	59.53.91.102	GET /loading.php? spl=...	Zararlı EXE (SpyEye) dosyası indiriliyor
50.60	192.168.23.129	212.252.32.20	GET /11111/gate.php?..	Olası C2 sunucusuna bağlanılıyor

Bu çizelgeye göre saldırı **yaklaşık 50 saniyelik bir zaman dilimi** içinde gerçekleşmiştir. Bu da saldırının otomatikleştirilmiş bir araç (muhtemelen exploit kit) tarafından gerçekleştirilmiş olabileceğini güçlü biçimde desteklemektedir. Kullanıcı etkileşimi gerekmeksizin indirilen dosyaların tetiklenmesi, saldırının “drive-by download” özelliği taşıdığını düşündürmektedir.

3. SONUÇ VE DEĞERLENDİRME

Yapılan ağ trafiği analizi sonucunda, kurban sisteme yönelik planlı ve çok aşamalı bir siber saldırı gerçekleştiği tespit edilmiştir. İlk olarak, 192.168.23.129 IP adresine sahip istemci cihaz tarafından 59.53.91.102 adresine yapılan HTTP bağlantıları, saldırının başlangıç noktasını oluşturmuştur. Bu bağlantılar aracılığıyla Java tabanlı zararlı içerikler (q.jar, sdfg.jar) ve sonrasında bir PE32 yürütülebilir dosya (loading.php üzerinden) sisteme indirilmiştir.

İndirilen dosyalar üzerinde yapılan hash tabanlı analizler, dosyaların exploit kit kaynaklı olduğunu ve **yüksek tespit oranına sahip zararlı yazılımlar içerdiğini** açıkça ortaya koymuştur. Özellikle loading.php ile ulaşılan EXE dosyasının, finansal verileri hedefleyen ve sistem üzerinde kalıcılık sağlayan **SpyEye trojanı** olduğu belirlenmiştir.

DNS sorgularında tespit edilen alan adları (nrtjo.eu, freeways.in), saldırının yönlendirme ve C2 altyapısını temsil etmektedir. Bu alan adlarının çözümlendiği IP adresleri ise farklı coğrafi konumlardaki saldırgan altyapılara işaret etmektedir (Çin ve Türkiye).

Zaman çizelgesine göre, saldırı zinciri yaklaşık **50 saniye gibi kısa bir sürede** tamamlanmış, bu da saldırının manuel değil, tam otomatik bir yapı üzerinden yürütüldüğünü göstermektedir.

Tüm bulgular değerlendirildiğinde, bu saldırının yalnızca sistem ele geçirme değil, aynı zamanda **bilgi çalma, sistem üzerinde kontrol kurma ve olası C2 haberleşmesi sağlama** amacı taşıdığı anlaşılmıştır. Elde edilen veriler, kurumun bilgi güvenliği yapısında önemli zafiyetler bulunduğunu ve özellikle dışa açık servislerde kullanıcıya yönelik browser tabanlı tehditlerin kritik risk oluşturduğunu göstermektedir.