SECURİTY EVENT ANALİST REPORT

Project : ACME-Security analist

Reporter : Onur Karakoç

Date : 2025.11.07

Part 1: Event Analyst

Time Schedule

2024-10-15 06:46:30 JWT Token erişimi 1523 ID li kullanıcıya ait token kullanılarak yetkisiz girişim denemesi 203.0.113.45 IP adresinden yapılmıştır

2024-10-15 06:47:15 JWT Token erişimi 1523 ID li kullanıcıya ait token kullanılarak yetkisiz girişim denemesi 203.0.113.45 IP adresinden yapılmıştır

2024-10-15 06:47:18 JWT Token erişimi 1523 ID li kullanıcıya ait token kullanılarak yetkisiz girişim denemesi 203.0.113.45 IP adresinden yapılmıştır

2024-10-15 06:47:21 JWT Token erişimi 1523 ID li kullanıcıya ait token kullanılarak yetkisiz girişim denemesi 203.0.113.45 IP adresinden yapılmıştır

2024-10-15 06:47:24 JWT Token erişimi 1523 ID li kullanıcıya ait token kullanılarak yetkisiz girişim denemesi 203.0.113.45 IP adresinden yapılmıştır

2024-10-15 06:47:27 JWT Token erişimi 1523 ID li kullanıcıya ait token kullanılarak yetkisiz girişim denemesi 203.0.113.45 IP adresinden yapılmıştır

2024-10-15 06:47:30 JWT Token erişimi 1523 ID li kullanıcıya ait token kullanılarak yetkisiz girişim denemesi 203.0.113.45 IP adresinden yapılmıştır

2024-10-15 06:47:33 JWT Token erişimi 1523 ID li kullanıcıya ait token kullanılarak yetkisiz girişim denemesi 203.0.113.45 IP adresinden yapılmıştır

2024-10-15 06:47:36 JWT Token erişimi 1523 ID li kullanıcıya ait token kullanılarak yetkisiz girişim denemesi 203.0.113.45 IP adresinden yapılmıştır

2024-10-15 06:47:39 JWT Token erişimi 1523 ID li kullanıcıya ait token kullanılarak yetkisiz girişim denemesi 203.0.113.45 IP adresinden yapılmıştır

2024-10-15 06:47:42 JWT Token erişimi 1523 ID li kullanıcıya ait token kullanılarak yetkisiz girişim denemesi 203.0.113.45 IP adresinden yapılmıştır

2024-10-15 06:47:45 JWT Token erişimi 1523 ID li kullanıcıya ait token kullanılarak yetkisiz girişim denemesi 203.0.113.45 IP adresinden yapılmıştır

2024-10-15 06:47:48 JWT Token erişimi 1523 ID li kullanıcıya ait token kullanılarak yetkisiz girişim denemesi 203.0.113.45 IP adresinden yapılmıştır

2024-10-15 06:47:51 JWT Token erişimi 1523 ID li kullanıcıya ait token kullanılarak yetkisiz girişim denemesi 203.0.113.45 IP adresinden yapılmıştır

2024-10-15 06:47:54 JWT Token erişimi 1523 ID li kullanıcıya ait token kullanılarak yetkisiz girişim denemesi 203.0.113.45 IP adresinden yapılmıştır

2024-10-15 06:47:57 JWT Token erişimi 1523 ID li kullanıcıya ait token kullanılarak yetkisiz girişim denemesi 203.0.113.45 IP adresinden yapılmıştır

```
2024-10-15 06:46:30,1523,/api/v1/portfolio/1523,GET,1523,200,156,203.0.113.45,Acme-Mobile-Android/3.2.0,jwt_token_1523_stolen
2024-10-15 06:47:15,1523,/api/v1/portfolio/1524,GET,1524,200,143,203.0.113.45,Acme-Mobile-Android/3.2.0,jwt_token_1523_stolen
2024-10-15 06:47:18,1523,/api/v1/portfolio/1525,GET,1525,200,138,203.0.113.45,Acme-Mobile-Android/3.2.0,jwt_token_1523_stolen
2024-10-15 06:47:21,1523,/api/v1/portfolio/1526,GET,1526,200,147,203.0.113.45,Acme-Mobile-Android/3.2.0,jwt_token_1523_stolen
2024-10-15 06:47:24,1523,/api/v1/portfolio/1527,GET,1527,200,141,203.0.113.45,Acme-Mobile-Android/3.2.0,jwt_token_1523_stolen
2024-10-15 06:47:27,1523,/api/v1/portfolio/1528,GET,1528,200,139,203.0.113.45,Acme-Mobile-Android/3.2.0,jwt_token_1523_stolen
2024-10-15 06:47:30,1523,/api/v1/portfolio/1529,GET,1529,200,144,203.0.113.45,Acme-Mobile-Android/3.2.0,jwt_token_1523_stolen
2024-10-15 06:47:33,1523,/api/v1/portfolio/1530,GET,1530,200,142,203.0.113.45,Acme-Mobile-Android/3.2.0,jwt_token_1523_stolen
2024-10-15 06:47:36,1523,/api/v1/portfolio/1531,GET,1531,200,148,203.0.113.45,Acme-Mobile-Android/3.2.0,jwt_token_1523_stolen
2024-10-15 06:47:39,1523,/api/v1/portfolio/1532,GET,1532,200,145,203.0.113.45,Acme-Mobile-Android/3.2.0,jwt_token_1523_stolen
2024-10-15 06:47:42,1523,/api/v1/portfolio/1533,GET,1533,200,140,203.0.113.45,Acme-Mobile-Android/3.2.0,jwt_token_1523_stolen
2024-10-15 06:47:45,1523,/api/v1/portfolio/1534,GET,1534,200,146,203.0.113.45,Acme-Mobile-Android/3.2.0,jwt_token_1523_stolen
2024-10-15 06:47:48,1523,/api/v1/portfolio/1535,GET,1535,200,143,203.0.113.45,Acme-Mobile-Android/3.2.0,jwt_token_1523_stolen
2024-10-15 06:47:51,1523,/api/v1/portfolio/1536,GET,1536,200,149,203.0.113.45,Acme-Mobile-Android/3.2.0,jwt_token_1523_stolen
2024-10-15 06:47:54,1523,/api/v1/portfolio/1537,GET,1537,200,141,203.0.113.45,Acme-Mobile-Android/3.2.0,jwt_token_1523_stolen
2024-10-15 06:47:57,1523,/api/v1/portfolio/1538,GET,1538,200,147,203.0.113.45,Acme-Mobile-Android/3.2.0,jwt_token_1523_stolen
```

Kimlik Hırsızlığı

/api/v1/portfolio/1523 isteğinde JWT kullanımına dair kayıtlar görülmeye başlanmıştır. Takip eden kısa süre içerisinde 15 ayrı API çağrısı gerçekleştirilmiş ve jwt_token_1523_stolen etiketiyle izler kaydedilmiştir. Bu zaman aralığında security-acme-finance.com hesabına etkileşim talepleri gönderilmiş, bunlardan bazılarına “yes” (evet) yanıtı alınmıştır.

Analiz

Saldırının aynı kaynak IP adresinden (203.0.113.45) gönderildiği tespit edilmiştir. Bu IP üzerinden çapraz biçimde kaba kuvvet (brute-force) yöntemiyle erişim sağlanmaya çalışıldığı görülmüştür.

JWT token hırsızlığı ve yeniden kullanım (token replay) saldırısı, MITRE ATT&CK çerçevesinde T1552 – Credentials from Web Browsers tekniğiyle ilişkilendirilebilir. OWASP tarafında ise A07: Identification and Authentication Failures kategorisiyle örtüşmektedir. Bu tür hatalar, kullanıcı kimliğinin doğrulanması ve oturum yönetimi süreçlerinin zayıf tasarlanmasından kaynaklanır ve kritik öneme sahiptir.

Ayrıca bu tür phishing saldırıları, SQL Injection gibi saldırılara zemin hazırlayabilmektedir.

Aynı IP adresinden (203.0.113.45) yapılan bir diğer erişim girişiminde index.php dosyasına yönelik talepler görülmüş, sonrasında “multiple auth error” (birden fazla kimlik doğrulama hatası) kaydedilmiştir. Bu durum, ilgili hesaba kimliği belirsiz kişiler tarafından erişim sağlandığı şüphesini güçlendirmektedir.

Ayrıca sistem loglarında, Windows NT 10.0 sisteminden giriş gözükmekte bu windows sürümü işlemciden bağımsız, çoklu işlem ve çoklu kullanıcı desteği sunan bir işletim sistemidir.

2024-10-15 09:18:30,1523,/login,,200,3421,203.0.113.45,Mozilla/5.0 (Windows NT 10.0	Win64	x64) Chrome/118.0	
2024-10-15 09:19:15,1523,/dashboard,,200,8934,203.0.113.45,Mozilla/5.0 (Windows NT 10.0	Win64	x64) Chrome/118.0	
2024-10-15 09:20:30,1523,/dashboard/search,ticker=AAPL' OR 1=1--,403,567,203.0.113.45,Mozilla/5.0 (Windows NT 10.0	Win64	x64) Chrome/118.0	
2024-10-15 09:21:15,1523,/dashboard/search,ticker=AAPL'	DROP TABLE users--,403,567,203.0.113.45,Mozilla/5.0 (Windows NT 10.0	Win64	x64) Chrome/118.0
2024-10-15 09:22:00,1523,/dashboard/search,ticker=AAPL' UNION SELECT * FROM users--,403,567,203.0.113.45,Mozilla/5.0 (Windows NT 10.0	Win64	x64) Chrome/118.0	
2024-10-15 09:23:45,1523,/dashboard/search,ticker=AAPL' /*!50000OR*/ 1=1--,200,156789,203.0.113.45,Mozilla/5.0 (Windows NT 10.0	Win64	x64) Chrome/118.0	
2024-10-15 09:24:10,1523,/dashboard/export,format=csv,200,892341,203.0.113.45,Mozilla/5.0 (Windows NT 10.0	Win64	x64) Chrome/118.0	
2024-10-15 09:30:00,1523,/dashboard/home,200",200,8934,203.0.113.45,Mozilla/5.0 (Windows NT 10.0	Win64	x64) Chrome/118.0	

```
2024-10-15 09:00:23,950107,HIGH,DETECT,203.0.113.45,/verify-account.php,Suspicious Link Pattern,no
2024-10-15 01:30:15,920420,LOW,DETECT,192.168.1.100,/api/v1/portfolio/1000,Multiple Failed Auth,no
2024-10-15 01:30:19,920420,LOW,DETECT,192.168.1.100,/api/v1/portfolio/1004,Multiple Failed Auth,no
```

203.0.113.45 IP adresine erişim engeli uygulanmalı.

İlgili hesaplara verilen izinler kısıtlanmalı, geçici olarak askıya alınmalı.

Gerekirse **bant daraltma** işlemi uygulanarak sistemden veri giriş-çıkışı kontrol altına alınmalı.

Erişim logları detaylı şekilde incelenmeli ve olayın zaman çizelgesi çıkarılmalı.

Çalışanlara **phishing farkındalık eğitimi** verilmelidir. Bu tür saldırılar süreklilik gösterebileceğinden, kullanıcıların bilinçli davranması büyük önem taşır.

VİDEO LİNK: https://youtu.be/_AF6CN7WBQI