Log Analiz Raporu

Okan UZUN

22.09.2025

Table of Contents

Giriş

Bu raporda, Graylog üzerinde tespit edilen üç güvenlik alarmının oluşum süreçleri incelenmiştir. İnceleme kapsamında **“A member was added to a security-enabled global group”**, **“Path Travel Detected”** ve **“Root Authentication Failed”** alarmlarının nasıl oluştuğu analiz edilerek ortaya konulmuştur.

Alarmlar

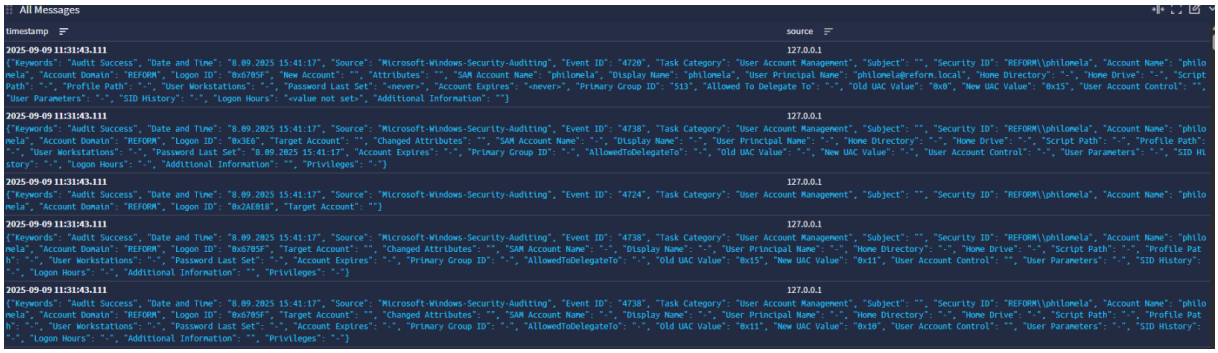
A Member Was Added To A Security-enabled Global Group

Logon aşaması

İncelenen zaman diliminde ilk tespit edilen kritik olay, Event ID 4625(Unknown user name or bad password) Başarısız giriş deneme kaydıdır. Bu kayıt Graylog üzerinde “**09.08.2025 16:44:30**” zaman damgasına denk gelirken Windows event logunda “**08.09.25 15:42:52**” zamanına denk gelmektedir.

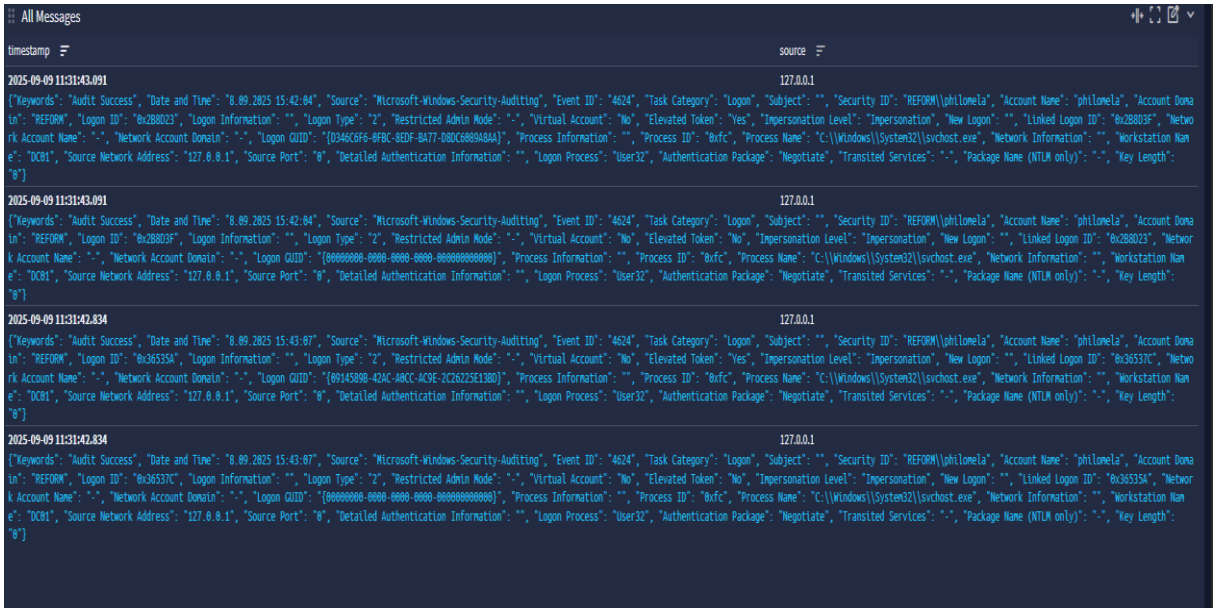
Hatalı Giriş

Daha sonra kullanıcı, **philomela,** hesabı **“09.09.25 11:31:42”** zaman damgasında oluşturulmuştur(Event ID 4720). Oluşturulan hesap üzerinde parola reset girişimi yapılmış(Event ID 4724). Daha sonra hesap üzerinde değişiklik yapılmış(Event ID 4738) ancak “Changed Attributes” alanı boş görülmektedir. Kritik değişiklik logda gözlemlenmemiştir.



Account oluşturulmuş

Bu noktada ise **“09.08.2025 15:42:07”** zaman damgasında **philomela** kullanıcısı ile başarılı bir oturum açma gerçekleşmiştir (Event ID 4624). Logon Type:3 olması sisteme ağ üzerinden erişildiği göstermektedir. Uzak masaüstü bağlantısı olan RDP protokolüyle bağlanmış olabileceğini gösterir. Oturum açma işleminde ise svchost.exe çalışmıştır. Svchost.exe bu windows içindeki hizmet işlemleri düzenleyen bir .



Logon

Privilage Escalation

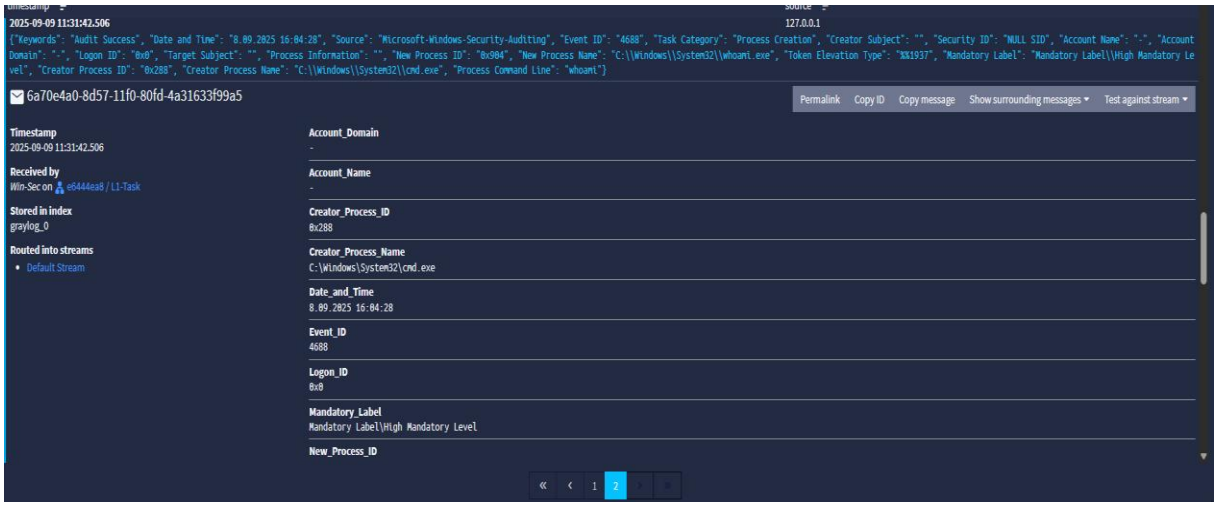
Bu noktada saldırgan **“2025-09-09 11:31.42”** zaman damgasına Creator Process ,svchost.exe, ardından Runtimebroker.exe çalışıyor. Bu olağan dışı davranış, saldırganın Windows servislerini istismar ederek yetkili bir RuntimeBroker işlemi oluşturduğunu

göstermektedir. Bu yöntem, privilege escalation ve defense evasion amacıyla kullanılan LOLBin (Living off the Land Binaries) tekniklerinden biridir.

Svchost.exe -> RuntimeBroker.exe

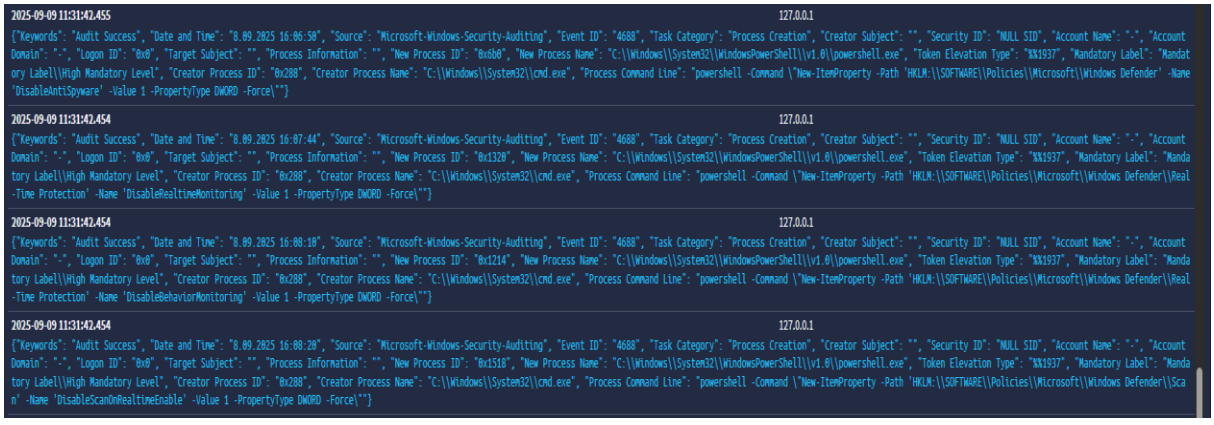
Bu noktada ise process zinciri devam etmektedir. Çalışan RuntimeBroker "**2025-09-09 11:31:42"** zaman damgasında cmd.exe'yi çalıştırmaktadır. Ayrıca olay High Mandatory Level (yükseltilmiş yetki) ile gerçekleşmiştir. Bu durum saldırganın, privilege escalation sonrasında RuntimeBroker üzerinden yönetici haklarına sahip bir komut satırı açtığını ve bunu kötüye kullandığını göstermektedir. Ayrıca bu esnada whoami sorgusu yapmıştır bu da loglarda gözlemlendi.

RuntimeBroker.exe -> cmd.exe



whoami

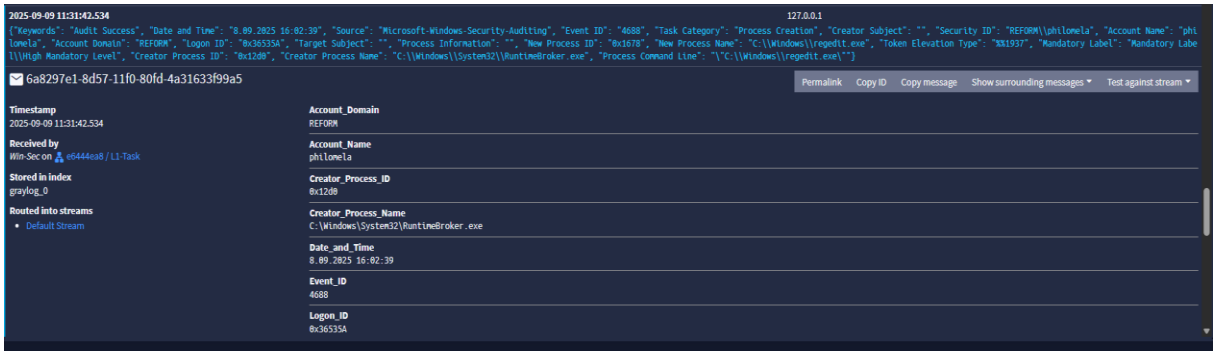
“09.09.2025 11:31:42’de powershell.exe üzerinden Windows Defender’ın registry anahtarları değiştirilerek güvenlik modülleri kapatılmıştır. Bu değişiklikler arasında antispyware modülünün, gerçek zamanlı taramanın, davranışsal analiz motorunun ve realtime tetikleyici taramalarının devre dışı bırakılması yer almaktadır. Value değerlerinin 1 olması bu araçların devre dışı bırakıldığını göstermektedir.



cmd.exe -> powershell.exe

İşlem aralığı “**09.09.2025 11:31:42 – 11:31:43”** zaman damgalarında ise saldırganın başlattığı ek süreçler de tespit edilmiştir.

Regedit.exe, Windows kayıt defteri üzerinde değişiklik yapılmasına izin veren güçlü bir yönetim aracıdır. Yetkisiz şekilde çalıştırılması, saldırganın sistem ayarlarını değiştirme, güvenlik kontrollerini devre dışı bırakma veya kalıcılık sağlamak için başlangıç girdilerini manipüle etme amacıyla kullanılmış olabileceğini göstermektedir.

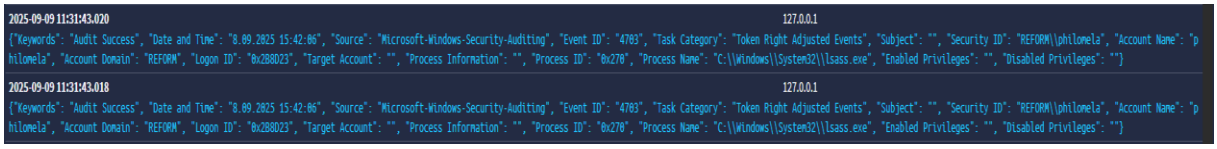


Regedit.exe

Bir diğer kayıtta PowerShell.exe (PID: 0x4c4) tarafından auditpol.exe (PID: 0x1550) aracının çalıştırıldığı tespit edilmiştir. Saldırgan tespit edilmekten kaçınma ve hangi faaliyetlerin kayıt altına alındığını görmek isteyebilir.

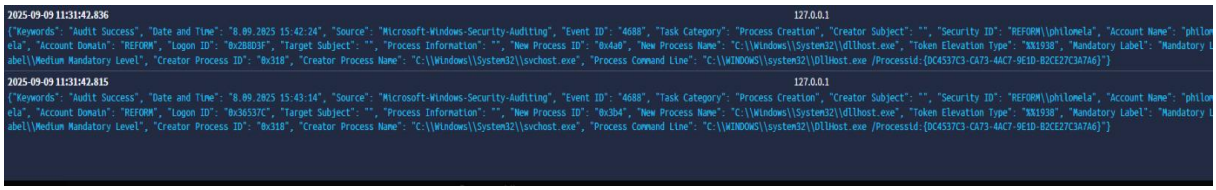
Auditpol.exe

Kayıtlarda lsass.exe (PID: 0x270) süreci için Event ID 4703 (Token Right Adjusted Events) üretilmiştir. LSASS windows içindeki kimlik bilgileri yönetimini yapan kritik bir yapıdır. Bu noktada kimlik bilgilerini çıkarmaya çalıştığı söylenebilir.



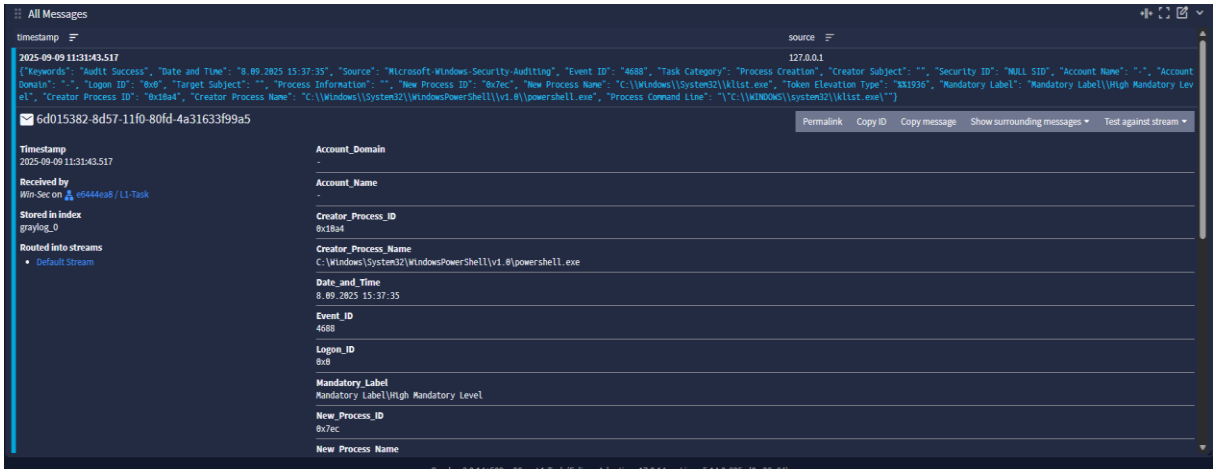
Lsass.exe

Son olarak kayıtlarda svchost.exe (PID: 0x318) tarafından başlatılan dllhost.exe süreçleri gözlenmiştir. Normalde bu işlem meşru olabilir ama saldırgan tarafından manipüle edilmeye çalışılmış olabilir.



Scvdll.exe

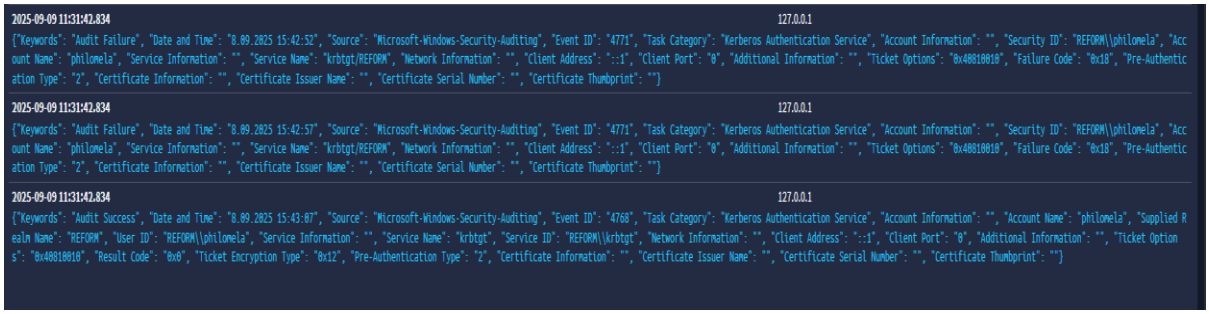
Zaman damgası “**2025-09-09 11:31:43”** anında log kaydı incelendiğinde, saldırganın PowerShell üzerinden klist.exe aracının ,high mandatory(%%1936), yani yönetici ayrıcalıklarıyla çalıştırdığı görülmektedir. Bu aracın amacı kerberos ticket bilgilerini görmek, yeniden istemek ve yönetmektir. Bundan sonra Kerberos ticket talebi veya pass-the-ticket saldırısı gerçekleşebilir.



Klist.exe

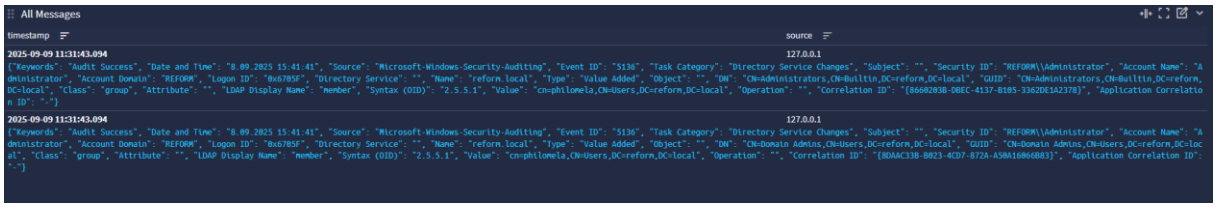
İnceleme sırasında Event ID 4771 (Kerberos authentication failure) kaydı tespit edilmiştir. Bu logda kullanıcının Kerberos kimlik doğrulama isteği gönderdiği, ancak Failure Code: 0x18 değeri ile başarısız olduğu görülmektedir. Kısa bir süre sonra ise Event ID 4768 (Kerberos Authentication Service – Success) logu oluşmuş ve aynı kullanıcı için Kerberos Ticket Granting Ticket (TGT) başarıyla alınmıştır. Log içerisinde Result Code: 0x0 ve Ticket Encryption

Type 0x12 değerleri görülmektedir. Bu da şifrelenmenin AES256 ile gerçekleşip doğrulamanın tamamlandığını gösterir.

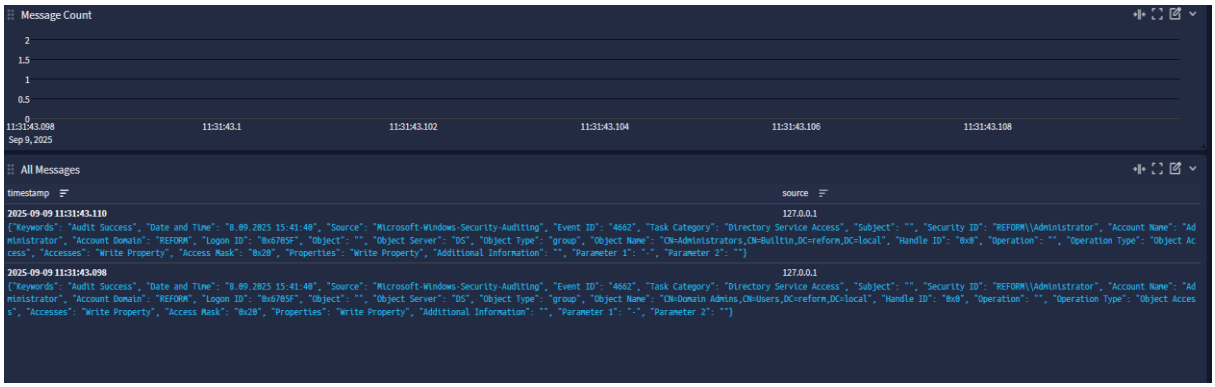


Kerberos İşlemleri

Administrator hesabı üzerinden Active Directory'de kritik bir işlem gerçekleştirilmiş ve **"Write Property"** erişim tipi kullanılarak hem Builtin\Administrators hem de Domain Admins grupları üzerinde yazma yetkisi kullanıldığı tespit edilmiştir. Domain Admins grubu, Active Directory ortamında en yüksek yetki seviyesini temsil eder ve bu gruba üye olan kullanıcılar tüm domain üzerindeki kaynaklar üzerinde tam kontrol hakkına sahip olur. Özellikle dikkat çeken alanlardan biri Object Name kısmıdır. Burada önce CN=Administrators, CN=Builtin daha sonra da CN=Domain Admins, CN=Users gruplarında Write Property işlemleri kaydedilmiştir(Event ID 5136). Bu, philomela kullanıcısının hem local sistem yöneticisi grubuna hem de domain yöneticileri grubuna eklendiğini kanıtlamaktadır.

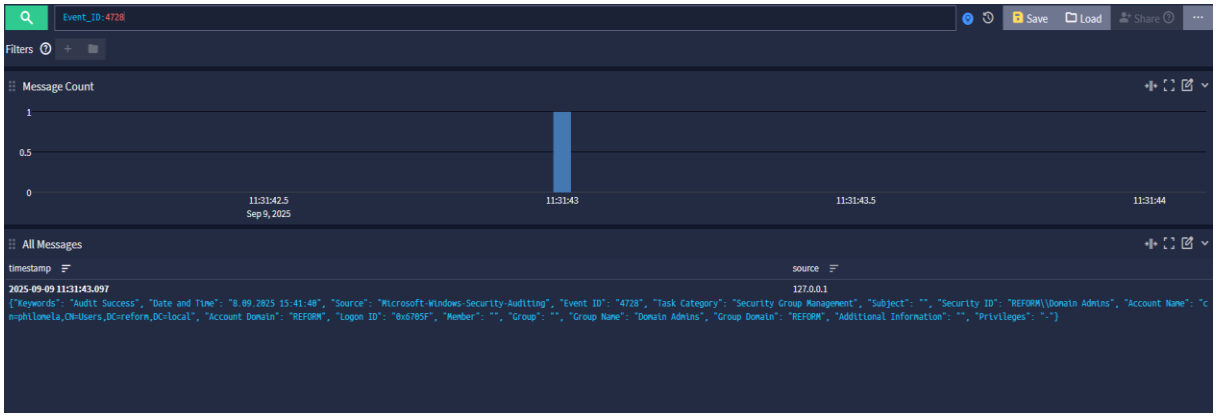


Event ID 5136



Write property

Event ID 4732



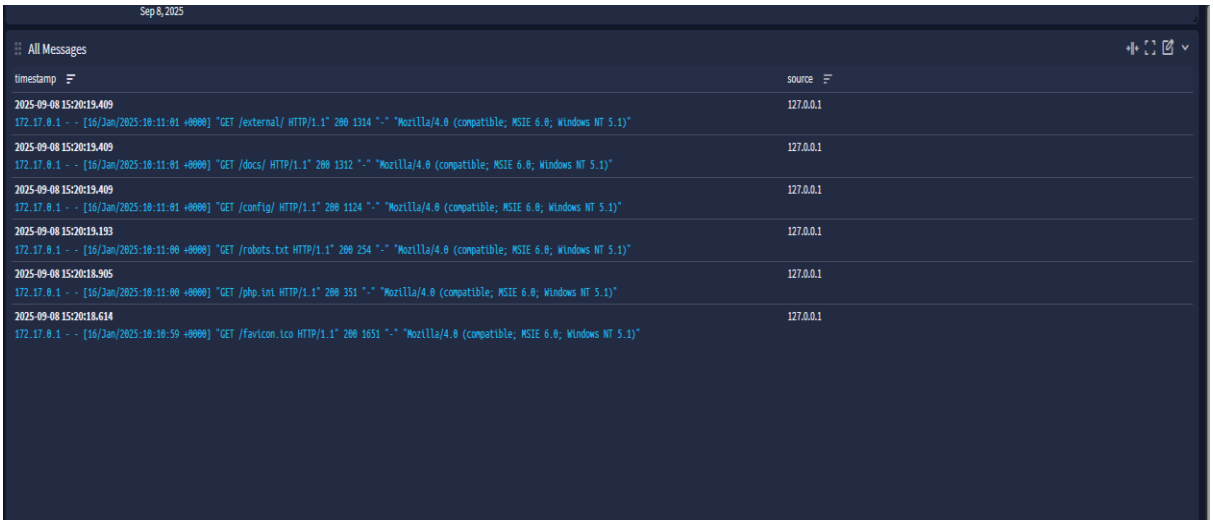
Event ID 4728

Path Travel Detected

Bu alarm, sistem üzerinde gerçekleştirilen dosya veya dizin erişimlerinde olağan dışı bir davranış tespit edildiğinde tetiklenmektedir. Özellikle directory traversal olarak bilinen bu durum saldırganın yetkisiz klasörlere erişmeye çalışması ya da normalde izin verilmeyen dizinler arasında geçiş yapmasıyla ilişkilidir. Bu noktada web isteklerine dikkat edildi ve response kodu 200 olanlar filtrelendi ve istekler bulundu.

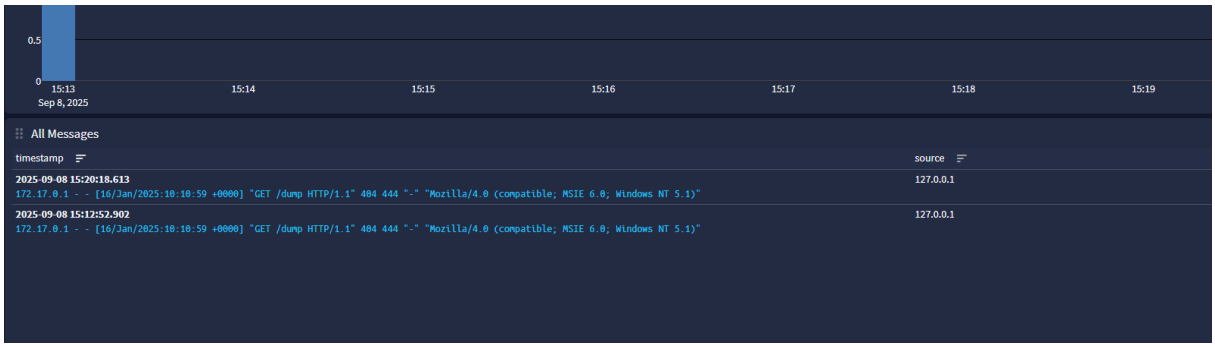
Web dizin sorgusu

Öncelikle /external/, /docs/ ve /config/ gibi kritik dizinlere istek gönderilmiş ve sunucu her defasında **200 OK** cevabı döndürmüştür. Bu durum, saldırganın yapılandırma ve dokümantasyon klasörlerine doğrudan erişebildiğini göstermektedir. Ardından robots.txt dosyası istenmiş bu da genellikle gizlenmek istenen dizinlerin açığa çıkmasına neden olabilmektedir. Daha kritik olarak php.ini dosyası da çağrılmış ve erişim sağlanmıştır bu dosya sistemin PHP yapılandırmasını içerdiği için veritabanı bağlantıları, hata logları veya kısıtlı fonksiyonlar gibi hassas bilgilerin sızmasına yol açabilir

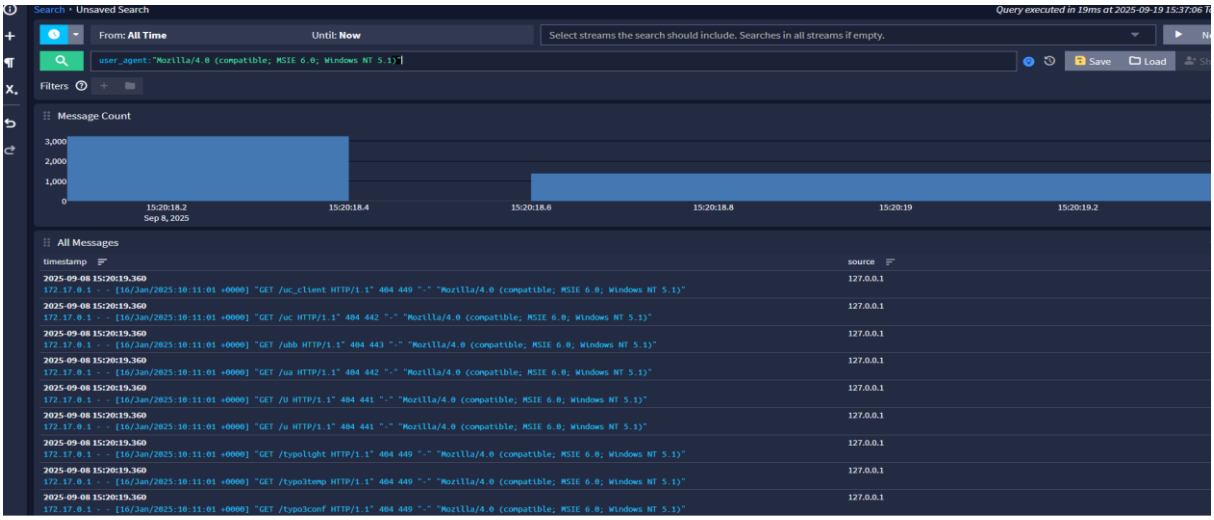


Mozilla

Ayrıca çok fazla sayıda da response 404 kodlu istek de bulunmaktadır. Burada saldırgan doğrudan **“dump”** isimli bir dosya veya dizin talep etmiş. Ancak yanıt **HTTP 404 (Not Found)** dönüyor. Yani orada dizinin bulunmadığını gösteriyor. Bu arama ,dump, çoğu zaman servis dökümü ve hata çıktılarının tutulduğu yerdir.



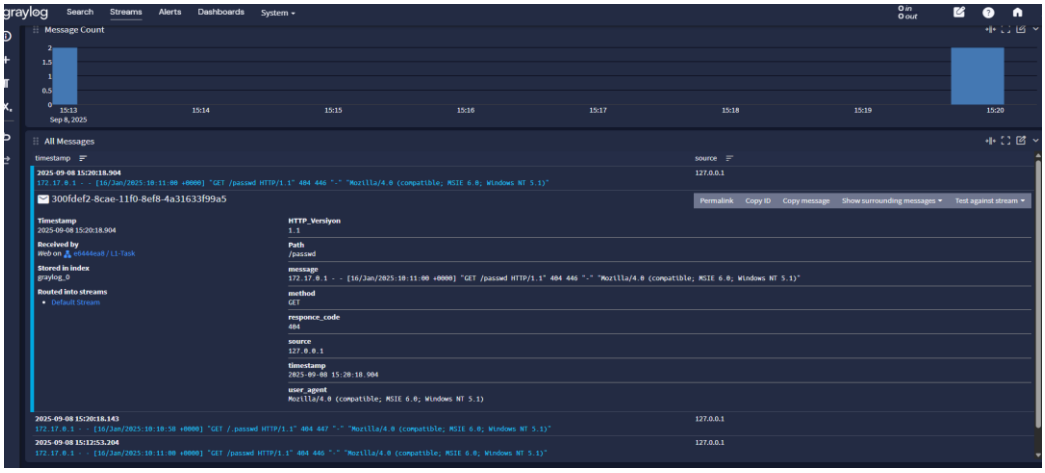
dump



Response 404

Passwd sorgusu

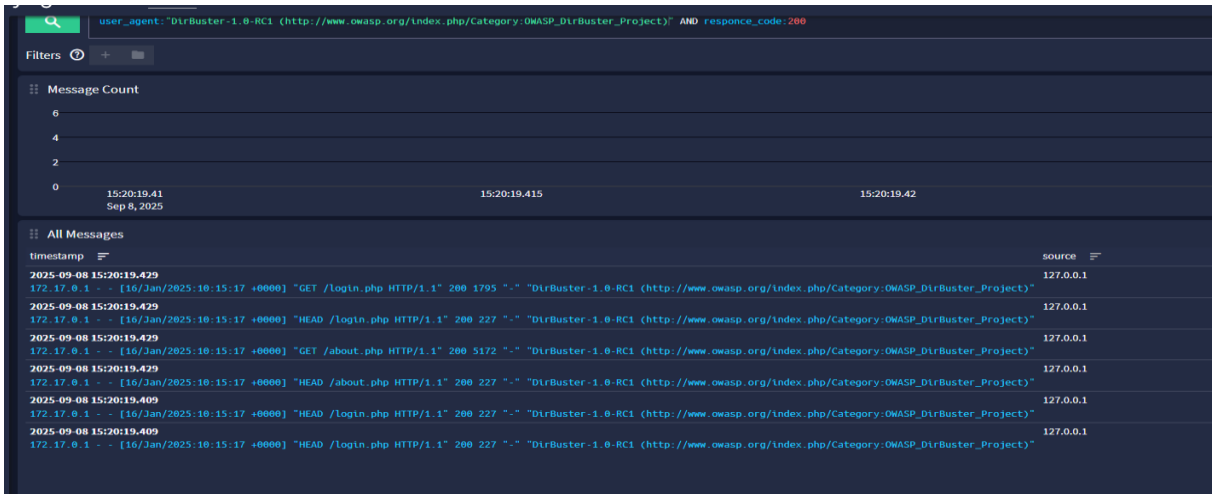
Bu esnada ise /passwd dizini ya da dosyası mevcut değil bunu response koduna(404) bakarak gözlemleyebiliriz. Saldırganın denediği path **"/passwd"** Unix/Linux sistemlerinde kritik şifre bilgilerini barındıran /etc/passwd dosyasına gönderme yapar. Genellikle path traversal saldırılarında saldırganlar "../../../etc/passwd" ya da encode şeklinde, "%2e%2e%2f%2e%2e%2fetc%2fpasswd", gibi denemeler yapar ama burada doğrudan /passwd olarak ilkel bir şekilde denenmiş.



Passwd

Dirbuster

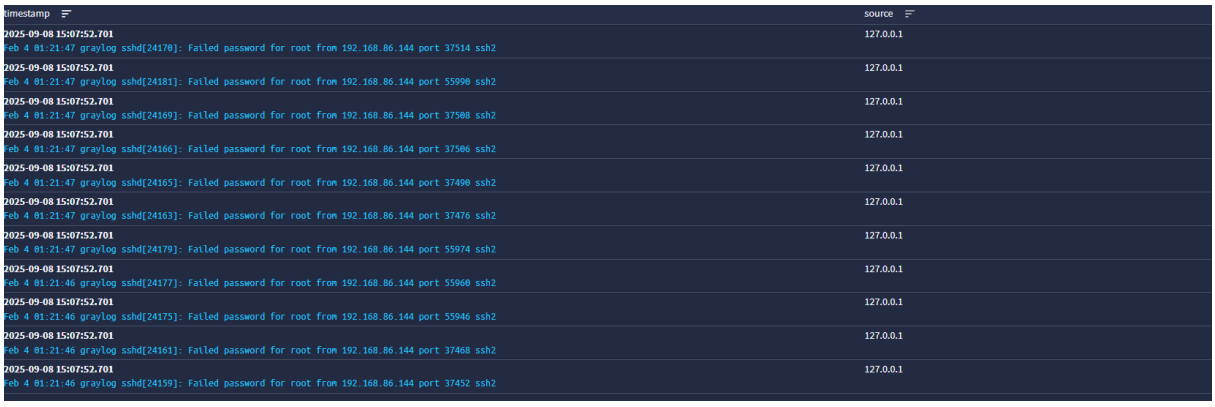
DirBuster logları incelendiğinde açıkça DirBuster-1.0 kullanımı var. Bu da saldırganın OWASP DirBuster aracıyla web dizin taraması yaptığını doğruluyor. Loglarda /Login.php, /about.php gibi istekler art arda geliyor ve çoğu **HTTP 200 (OK)** dönüyor.



Dirbuster

Root Authentication Failed

Bu log çıktısına göre aynı IP adresinden (192.168.86.144) çok kısa süre içerisinde defalarca **root** kullanıcısı için başarısız oturum açma denemesi yapılmış. Her deneme farklı portlardan (37514, 55990, 37508, 37476, 55974 vs.) geliyor ama **ssh2 protokolü** üzerinden gerçekleşiyor. Log satırları "Failed password for root" şeklinde ardışık biçimde kaydedilmiş. Önleme için /etc/ssh/sshd_config dosyasında "PermitRootLogin no" yapılarak direkt olarak root kullanıcısıyla doğrudan giriş yapılması engellenebilir.



Root Authentication Failed

MITRE ATT&CK Analizi

Tactic	Technique	ID	Açıklama
Defense Evasion	Impair Defenses: Disable or Modify Tools	T1562.001	PowerShell üzerinden Defender'ın kapatılması
Credential Access	OS Credential Dumping: LSASS Memory	T1003.001	lsass.exe erişimi / dump girişimi
Discovery / Evasion	System Information Discovery / Modify Registry	T1082	regedit.exe çalıştırılması
Credential Access	Kerberos Tickets: TGT Abuse	T1558.001	klist.exe ile ticket'ların listelenmesi
Privilege Escalation	Create Account / Add to Group	T1136.002	Event ID 4728 / 4732 – Kullanıcıların "Domain Admins" grubuna eklenmesi
Discovery	Path Traversal	T1006	/etc/passwd, /dump gibi path traversal denemeleri
Reconnaissance	Active Scanning	T1595	DirBuster User-Agent ile Login.php, about.php taramaları
Credential Access	Brute Force: Password Guessing	T1110.001	"Failed password for root" denemeleri
System Binary Proxy Execution	Defense Evasion(LOLBIN)	T1218	RuntimeBroker->cmd.exe->powershell.exe

Sonuç-Öneri

Analiz edilen log kayıtları, sistem üzerinde hem privilege escalation (yetki yükseltme) hem de defense evasion (savunma atlatma) girişimlerinin başarıyla gerçekleştirildiğini göstermektedir. Özellikle Windows Defender'ın registry üzerinden devre dışı bırakılması, LSASS sürecine erişim sağlanması, Kerberos ticket manipülasyonları ve Domain Admins grubuna kullanıcı eklenmesi saldırganın sistem üzerinde tam kontrol elde ettiğini işaret etmektedir. Ayrıca path traversal, DirBuster ile dizin keşfi ve SSH brute force denemeleri gibi aktiviteler, saldırganın yalnızca iç ağda değil, dışa açık servislerde de aktif keşif ve saldırı faaliyetlerinde bulunduğunu kanıtlamaktadır.

Active Directory ortamında en az ayrıcalık prensibi uygulanmalı, kullanıcıların erişim hakları düzenli olarak gözden geçirilmeli ve gerekli durumlarda güncellenmelidir. Güvenliği artırmak için çok faktörlü kimlik doğrulama (MFA) devreye alınmalıdır. Hizmet hesaplarının ayrıcalıkları en düşük seviyede tutulmalı ve kaba kuvvet saldırılarını zorlaştırmak amacıyla en az 25 karakter uzunluğunda, karmaşık parolalar kullanılmalıdır. RC4 şifreleme algoritması bilinen zafiyetleri nedeniyle güvenilirliğini yitirmiştir ve saldırganlar bu zafiyetleri kullanarak şifreli trafiği çözebilir. Bu nedenle devre dışı bırakılarak yerine AES gibi modern ve güçlü algoritmalar tercih edilmelidir. LSA (Yerel Güvenlik Yetkilisi) Koruması, LSASS sürecine yönelik yetkisiz erişimleri engelleyerek kimlik bilgisi hırsızlığına karşı güçlü bir savunma sağlar. Bu koruma, bellekten parola özetlerinin veya kimlik doğrulama belirteçlerinin çekilmesini zorlaştırır.

Kaynakça

1- https://www.ultimatewindowssecurity.com/ (Event loglarının detaylı olarak analiz edildiği site)
2- https://www.techtarget.com/searchsecurity/definition/Kerberos (Kerberos hakkında detaylı açıklama yapıldığı site)
3- https://blog.netwrix.com/ (Genel AD yapısının açıklandığı site)
4- https://www.semperis.com/blog/ (Özellikle AD güvenliği konusunda çözümleri olan bir şirketin blog sitesi)
5- https://chatgpt.com/ (Loglar incelenirken anlam bütünlüğü oluşturulması adına kullanıldı.)