Windows Event ID Cheat Sheet

by codeluu (codeluu) via cheatography.com/26083/cs/8500/

Windows Olay Kimlikleri

Event ID	Açıklama
4624	Başarılı Login
4625	Başarısız Login
4672	Admin Hesabı Logini
4634,4647	Başarılı Logoff
4771	Etki alanında ön kimlik doğrulama başarısız oldu
4768	Kerberos Ticket istemi
4776	Etki alanında başarılı ya da başarısız login
7034	Servis beklenmedik bir şekilde çöktü
7035	Servis, başlatma veya durdurma komutu gönderdi
7036	Servis durdu veya başladı
7040	Servis başlangıç tipi değiştirildi (Başlangıçta, elle vs.)
5140	Ağ paylaşımı planlandı
4778	RDP oturum isteği
4779	RDP oturumu kapandı

Farklı ID'leri birbirleriyle ilişkilendirmek de önemlidir. Örneğin 4624 akabinde görülen 4634/4647 ID'leri tamamlanmış bir oturum fikri verebilir. Çok fazla 4625 ID'si görmek bir sözlük saldırısının ya da bir zararlı yazılımın işareti olabilir.

Yerel Login

4624	DC'ye bağlı değil (Yerel)
4625	DC'ye bağlı değil (Yerel)
4771	Etki Alanı üzerinde
4768	Etki Alanı üzerinde
4776	Etki Alanı üzerinde

4624 ve 4625 in 4776 ID lerinin birbirinden farkları net olarak ortaya konmalıdır. Özellikle 4624 ve 4625 lokal makine üzerinde alınan ve DC'ye erişilemediğinde üretilen ID'lere örnektir. Makine DC'ye bağlıysa ise 4771, 4768 ve 4776 ID'leri üretilir.

Windows Oturum Türleri

2	Yerel login (Örn: Klavye ile)
3	Network Logini
4	Batch Login- zamanlanmış görevler için kullanılır
5	Windows servis login – (Görünür/Interaktif olmayacaktır)
7	Kilit ekranını açmak/kapatmak için kimlik bilgileri kullanıldı
8	Ağ üzerinden kimlik bilgileri clear text olarak gönderildi
9	Şu anki oturumu açan haricinde "run as" komutuyla (Yönetici vs. olarak çalıştır) yeni kimlik bilgileri kullanıldı
10	RDP (Uzak Masaüstü)
11	Login kimliği cachten getirildi
12	Cachten RDP yapıldı
13	Cachten kilit açıldı (oturum zaten açık)

Önemli bir olay örneğin 7 numaralı login tipi ile 11 numaralı login tipinin farklarıdır. 7 numaralı login bilgileri DC'den eşleştirilirken, 11 nolu login tipi makine DC'ye erişilemediğinde görülür. Windows o makineye oturum açmayı başaran son 10 kimlik bilgilerini (kullanıcı adı ve şifre) hash olarak saklar. Buradaki son 10 kimlik bilgisinden kasıt birbirinden farklı olan değil, aynısı veya farklısı da olsa son 10 oturum açılmış kimlik bilgileridir.

Zamanlanmış Görevler

106	Görev zamanlandı
200	Görev başlatıldı
201	Görev tamamlandı
141	Görev silindi

Windows içerisinde "zamanlanmış görev" logları bilgisayarımızın ele geçirilip geçirilmediği hususunda bize fikir verebilir. Örneğin bir servisin günün belli saatlerinde oturum açılması için görev zamanlaması gerçekleştirmesi şüpheli bir harekettir.

Malware Hareketleri

1. Zararlı; önce sızılmış sistem üzerinden ağa yayılmak için 4624 olay kimliğini 3 nolu oturum türüyle kullanacaktır. Burada zamanı bi kenara not edin.
2. O zamana yakın diğer sistemlerde 4672 ile oturum açılıp açılmadığına bakın.
3. Bulunursa o sistem üzerinde artık zararlı kod yönetici hakları ile çalıştığından kendisini diğer sistemlere bulaştırmak için 5140 olay kimliğini kullanarak ağ paylaşımı planlayacaktır. Sistemdeki bu çatlaktan zararlının bağlantı sağlanmış olduğu C&C sunucusunun IP bilgileri gibi kritik bilgilere dahi ulaşılabilir.
4. Sistemdeki bu çatlak ile çalıştırabilir kodlar ağı ele geçirecektir.
5. Olay kimliklerinde zamanlanan, başlatılan, tamamlanan, silinen görevler fikir vermelidir. İş tamamlandıktan sonra kendisini ve logları silmek isteyecektir. Zararlı dosyanın ismi ile birlikte zamanlanmış 200 kodlu bir log silme işlemi varsa önemlidir.
6. Logları da temizleyen zararlı son olarak kendi oturumunu 4634 olay kimliği ile kapatacaktır.

RDP Hareketleri

4778 nolu RDP oturumu talebi ile bir uzak masaüstü oturumu isteği gelir. Ancak bu başlamış bir oturum olarak yorumlanmamalıdır. Burada görülen IP adres ve sistem adı gibi bilgiler işe yarayabilir.4778 in akabinde görülen 4624 olay kodu ve 10 nolu oturum tipi oturumun artık RDP ile açıldığı kesin bilgisini verecektir.Bu kısımdan sonra bir önceki bölümün 3. Maddesindeki ağ paylaşımı ya da 5. Maddesindeki görev zamanlama şeklinde bir senaryo ile karşılaşılabilir.Oturumun 4634/4647 kodlarından sonra 4779 RDP'in sonlandırıldığında dair bir bilgi verecektir. Tek başına 4778 ve 4779 RDP istek ve kapanmalarına aldanmamak gerekir. RDP oturumunun açıldığına emin olmak için mutlaka 4778-4624..4634-4779 sıralaması ile görmek gerekir. 4778 ve 4779'un ayrıntılarına bakılabilir

By **codeluu** (codeluu)
cheatography.com/codeluu/
code0day.wordpress.com

Published 20th October, 2016.
Last updated 20th October, 2016.