

Rapor Başlığı: Cyber Kill Chain

Hazırlayan: İlayda Hörgüşlüoğlu

Tarih: 07.02.2025

1. Cyber Kill Chain Nedir?

Cyber Kill Chain, siber saldırıların aşamalarını anlamak, tespit etmek ve önlemek için kullanılan bir güvenlik modeli olup Lockheed Martin tarafından geliştirilmiştir. Bu model, saldırganların hedeflerine ulaşmadan önce durdurulmasını sağlamak amacıyla yedi temel aşamadan oluşur.

1. Keşif (Reconnaissance)

Saldırganlar, hedef organizasyon hakkında bilgi toplar. Bu aşamada kullanılan yöntemler:

* Açık kaynak araştırmaları (OSINT)
* Sosyal mühendislik teknikleri
* Güvenlik açıklarını belirlemek için pasif ve aktif taramalar

1. Silahlandırma (Weaponization)

Saldırganlar, ele geçirilen bilgileri kullanarak zararlı yazılımlar veya saldırı vektörleri hazırlar. Yaygın teknikler:

* Zararlı yazılım (malware) oluşturma
* Kimlik avı (phishing) sahte dosyaları hazırlama
* Exploit kitlerinin kullanımı

1. Teslimat (Delivery)

Hazırlanan zararlı içerik hedef sisteme iletilir. Kullanılan yaygın yöntemler:

* Kimlik avı e-postaları
* USB gibi fiziksel cihazlar
* Web siteleri üzerinden zararlı yazılım yayılması

1. İstismar (Exploitation)

Saldırganlar, teslim edilen zararlı içeriği çalıştırarak sistemde bir güvenlik açığından yararlanır. Bu aşamada:

* Yazılım ve işletim sistemi zafiyetlerinden yararlanma
* Kötü amaçlı kod çalıştırma
* Yetkisiz erişim sağlama

1. Kurulum (Installation)

Saldırganlar, hedef sistemde kalıcı erişim sağlamak için zararlı yazılımları yükler. Bu aşamada kullanılan teknikler:

* Rootkit ve arka kapılar (backdoor) oluşturma
* Keylogger ve trojan yükleme
* Kalıcılık sağlamak için sistem yapılandırmalarını değiştirme

1. Komuta ve Kontrol (Command & Control - C2)

* Saldırganlar, hedef sistemi uzaktan kontrol etmeye başlar. Bu aşamada:
* Bulaşan cihazlarla bağlantı kurulması
* Şifreli veya gizli komut kanalları oluşturulması
* Botnet ağlarına entegrasyon sağlanması

1. Hedeflere Ulaşma (Actions on Objectives)

Saldırganların nihai hedeflerine ulaştığı aşamadır. Yaygın kötü niyetli eylemler:

* Veri sızdırma ve çalma
* Sistemleri bozma veya şifreleme (ransomware saldırıları)
* Ağ içinde yatay hareket ederek daha fazla sistem ele geçirme

1. Cyber Kill Chain’e Karşı Savunma

Siber güvenlik ekipleri, Cyber Kill Chain modelini kullanarak her aşamada saldırıları engellemek için önlemler alabilir:

* Keşif aşamasına karşı: Ağ trafiği izleme, OSINT analizi yapma, güvenlik farkındalığı eğitimi verme.
* Silahlandırma aşamasına karşı: Uç nokta güvenliği artırma, dosya ve yazılım analiz araçları kullanma.
* Teslimat aşamasına karşı: E-posta filtreleme sistemleri, güvenli DNS kullanımı.
* İstismar aşamasına karşı: Sistemleri güncel tutma, güvenlik açıklarını hızla giderme.
* Kurulum aşamasına karşı: Davranışsal analiz sistemleri, antivirüs ve EDR çözümleri kullanma.
* Komuta ve kontrol aşamasına karşı: Ağ segmentasyonu, zararlı C2 trafiğini tespit eden çözümler.
* Hedeflere ulaşma aşamasına karşı: Veri şifreleme, veri kaybı önleme (DLP) çözümleri, olay müdahale planları oluşturma.

SONUÇ

Cyber Kill Chain, siber saldırıların sistematik bir şekilde analiz edilmesini ve saldırganların durdurulmasını sağlayan kritik bir modeldir. Her aşamada uygun güvenlik önlemlerinin alınması, SOC ekiplerinin tehditleri etkili bir şekilde yönetmesine ve saldırıları önlemesine yardımcı olur. Modern tehdit ortamında Cyber Kill Chain modeli, yapay zeka destekli güvenlik sistemleri ve tehdit istihbaratı ile entegre edilerek daha etkin bir hale getirilebilir.