Tarih 4/02/2025

Cyber Kill Chain

Hazırlayan

Kaan Akdeniz

İçindekiler

Giriş

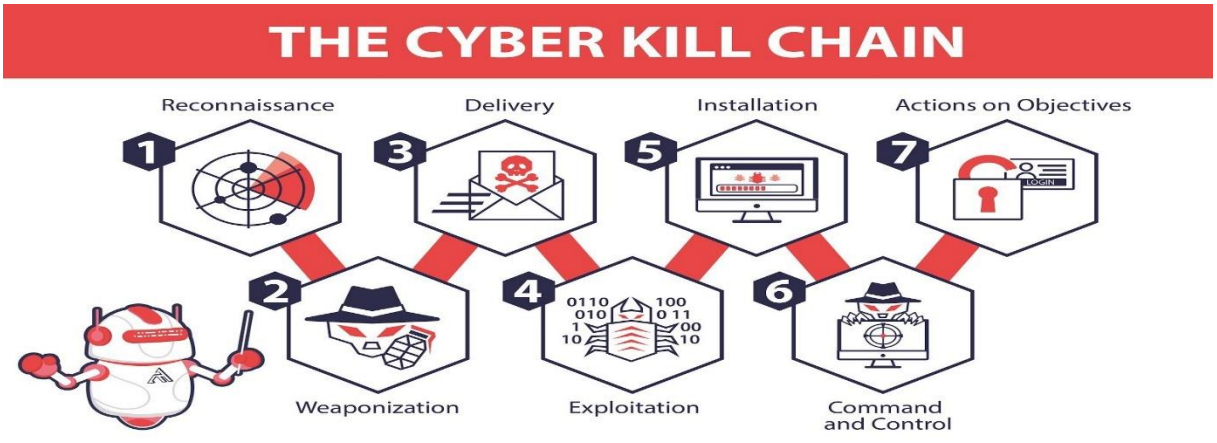
Siber tehditlerin giderek daha sofistike hale gelmesi, kurumların güvenlik stratejilerini geliştirmesini zorunlu kılmıştır. Siber saldırganlar, hedeflerine ulaşmak için belirli aşamalardan geçer ve bu süreçlerin anlaşılması, etkili savunma önlemleri almak için kritik bir gerekliliktir. Lockheed Martin tarafından geliştirilen Cyber Kill Chain Modeli, bir saldırının aşamalarını tanımlayarak, savunma mekanizmalarının güçlendirilmesine yardımcı olur. Bu model, saldırganların nasıl hareket ettiğini anlamamızı sağlarken, aynı zamanda proaktif güvenlik önlemleri almamıza olanak tanır. Bu çalışmada, Cyber Kill Chain Modeli detaylı olarak ele alınarak, her aşamada kullanılan saldırı ve savunma stratejileri incelenecektir.

Cyber Kill Chain Modeli

Cyber Kill Chain, Lockheed Martin tarafından geliştirilmiş bir siber saldırı yaşam döngüsünü analiz eden bir modeldir. Bu model, saldırganların gerçekleştirdiği aşamaları belirleyerek, savunma mekanizmalarının güçlendirilmesine yardımcı olur. Yani bu döngü saldırganların benzer şekilde bir yol izlemesi sonucu bu benzerliklerin belirlenip bir yol haritası olarak Lockheed Martin tarafından geliştirilmiştir.

1. Cyber Kill Chain Aşamaları

1. **Keşif (Reconnaissance)**
2. **Silahlandırma (Weaponization)**
3. **Teslimat (Delivery)**
4. **Sömürme (Exploitation)**
5. **Kurulum (Installation)**
6. **Komuta ve Kontrol (Command & Control)**
7. **Hedef Gerçekleştirme (Actions on Objectives)**



1.1 Keşif (Reconnaissance)

Bu aşamada saldırgan, hedef sistem veya kuruluş hakkında bilgi toplar. Açık kaynak araştırmaları (OSINT), phishing saldırıları ve sosyal mühendislik teknikleri kullanılarak sistemdeki zafiyetler belirlenmeye çalışılır.

Saldırı Stratejisi:

- Sosyal medya ve açık kaynaklardan bilgi toplama (OSINT)
- E-posta veya sahte web siteleri ile phishing saldırıları düzenleme
- Ağ taramaları ve güvenlik açıklarını keşfetme

Savunma Stratejisi:

- Ağ trafiği izleme ve anomali tespiti
- Çalışanların siber güvenlik farkındalığını artırma
- Hassas bilgilerin açık kaynaklardan kaldırılması

1.2 Silahlandırma (Weaponization)

Saldırgan, topladığı bilgilere dayanarak zararlı yazılımlar veya kötü amaçlı komut dosyaları hazırlar. Bu aşamada, zararlı yazılımın nasıl dağıtılacağı belirlenir.

Saldırı Stratejisi:

- Zero-day açıklarını kullanarak özel zararlı yazılım geliştirme
- Kimlik avı saldırıları için özel olarak hazırlanmış kötü amaçlı ekler oluşturma
- Açık kaynak güvenlik araçlarıyla saldırı teknikleri geliştirme

Savunma Stratejisi:

- Tehdit istihbaratı analizi
- Güvenli yazılım geliştirme
- Zararlı yazılım analiz araçlarının kullanımı

1.3 Teslimat (Delivery)

Saldırgan, zararlı yazılımı hedefe ulaştırır. Bu genellikle phishing e-postaları, kötü amaçlı ekler, USB aygıtları veya güvenlik açıkları üzerinden gerçekleştirilir.

Saldırı Stratejisi:

- Kötü amaçlı e-posta ve ekler gönderme (Phishing, Spear Phishing)
- Zararlı yazılım içeren USB bellekler bırakma
- Web sitelerine zararlı kod yerleştirme (Drive-by Download)

Savunma Stratejisi:

- E-posta filtreleme ve phishing tespiti
- USB ve harici cihaz kullanım kısıtlamaları
- Güvenlik açıklarının düzenli olarak yamalanması

1.4 Sömürme (Exploitation)

Saldırgan, hedef sistemdeki bir güvenlik açığını kullanarak zararlı yazılımı çalıştırır. Genellikle işletim sistemi veya uygulamalardaki zafiyetler sömürülür.

Saldırı Stratejisi:

- İşletim sistemlerindeki veya yazılımlardaki güvenlik açıklarını kullanma
- Web uygulamalarındaki açıkları sömürerek yetkisiz erişim sağlama
- Kötü amaçlı komut dosyalarını çalıştırarak arka kapılar oluşturma

Savunma Stratejisi:

- Güncel yama ve güvenlik güncellemelerinin uygulanması
- Güvenlik duvarı ve antivirüs sistemlerinin aktif kullanımı

1.5 Kurulum (Installation)

Bu aşamada saldırgan, zararlı yazılımı sisteme yerleştirir ve saldırının devamlılığını sağlar. Bu, genellikle rootkit veya arka kapılar (backdoor) ile gerçekleştirilir.

Saldırı Stratejisi:

- Rootkit veya trojan yükleyerek sistem üzerinde kalıcılık sağlama
- Arka kapılar (Backdoor) oluşturarak uzaktan erişim sağlama
- Kendi izlerini silerek tespitten kaçınma

Savunma Stratejisi:

- Davranışsal analiz tabanlı güvenlik sistemleri
- Sistem dosyalarındaki değişikliklerin izlenmesi

1.6 Komuta ve Kontrol (C2 - Command & Control)

Saldırgan, ele geçirilen sisteme uzaktan erişim sağlar. Genellikle botnet veya uzaktan komut sistemleri kullanılır.

Saldırı Stratejisi:

- Zararlı yazılımın saldırganın kontrol sunucusuna bağlanmasını sağlama
- Şifrelenmiş C2 kanalları kullanarak veri transferi yapma

- Tespit edilmemek için normal ağ trafiği gibi görünmesini sağlama

Savunma Stratejisi:

- Ağ trafiği analizi ve şüpheli bağlantıların engellenmesi
- DNS sorgularının izlenmesi

1.7 Hedef Gerçekleştirme (Actions on Objectives)

Saldırgan, sistemdeki verileri çalar, siler veya şifreler. Bu aşama, saldırının nihai amacına ulaşmasını sağlar.

Saldırı Stratejisi:

- Hassas verileri çalarak finansal veya ticari avantaj sağlama
- Fidye yazılımları kullanarak verileri şifreleme (Ransomware)
- Sistemi tamamen çökertmek için zararlı kod çalıştırma

Savunma Stratejisi:

- Veritabanı şifreleme
- Yedekleme sistemlerinin düzenli test edilmesi

2. Teknik Yönleri

Cyber Kill Chain Modeli, her aşamada farklı teknikler ve savunma mekanizmalarını kapsar:

- **Keşif:** OSINT (Açık Kaynak İstihbarat), domain sorguları ve sosyal mühendislik ile bilgi toplanır.
- **Silahlandırma:** Remote Access Trojan (RAT) ve exploit kitleri kullanılarak zararlı yazılımlar geliştirilir.
- **Teslimat:** Phishing, drive-by download ve USB taşıyıcılar üzerinden zararlı yazılım bulaştırılır.
- **Sömürme:** Zero-day exploit'ler ve yetki yükseltme teknikleri kullanılır.
- **Kurulum:** Rootkit ve arka kapı yöntemleriyle kalıcılık sağlanır.
- **Komuta ve Kontrol:** Merkezi veya P2P tabanlı C2 sunucuları kullanılır.

- **Hedef Gerçekleştirme:** Veri çalma, sabotaj veya fidye yazılımları çalıştırma gibi işlemler uygulanır.

Sonuç

Cyber Kill Chain Modeli, siber güvenlik alanında saldırıları daha iyi anlamak ve etkili savunma mekanizmaları geliştirmek için önemli bir çerçeve sunmaktadır. Modelin her aşaması, hem saldırganların kullandığı yöntemleri hem de bu tehditlere karşı alınabilecek önlemleri ortaya koymaktadır. Günümüzün dijital dünyasında, şirketlerin ve kuruluşların güvenlik operasyon merkezleri (SOC) aracılığıyla proaktif güvenlik önlemleri alması giderek daha kritik hale gelmektedir. Siber tehditlerin sürekli evrildiği göz önüne alındığında, Cyber Kill Chain Modeli gibi yapıların güvenlik stratejilerinin merkezinde yer alması gerekmektedir. Böylece, organizasyonlar saldırılara karşı daha dayanıklı hale gelir ve olası tehditleri en aza indirebilir.

Kaynakça

1-) Cyber Kill Chain: Definition & Examples

2-) Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2015). *Technical aspects of Cyber Kill Chain*. ResearchGate. https://www.researchgate.net/publication/281148852_Technical_Aspects_of_Cyber_Kill_Chain