Cyber Kill Chain

Hazırlayan
Burak Ali DÜZÜN

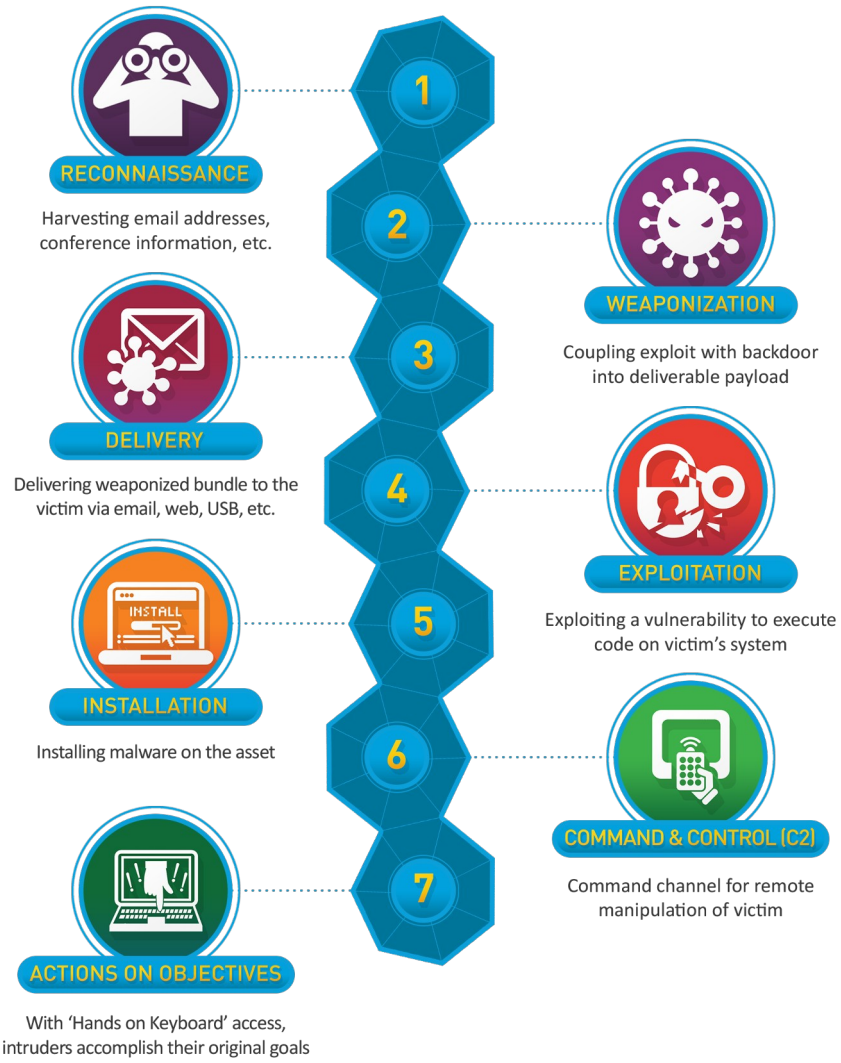
07.02.2025

İÇİNDEKİLER

Cyber Kill Chain Raporu

Siber güvenlik alanında organizasyonların tehditlere karşı etkili bir savunma stratejisi geliştirmesi hayati önem taşır. Lockheed Martin tarafından geliştirilen "Cyber Kill Chain" modeli, siber saldırıların yaşam döngüsünü sistematik bir şekilde anlamaya olanak tanır. Bu model, bir saldırganın hedef sisteme ulaşma sürecini ve bu süreçteki aşamaları tanımlar. Özellikle SOC (Security Operations Center) analistleri ve siber güvenlik uzmanları için rehber niteliği taşıyan bu model, hem saldırıları tespit etmek hem de bu saldırılara zamanında müdahale etmek amacıyla kritik bilgiler sunar.

Bu raporda, Cyber Kill Chain kavramı detaylı olarak ele alınacak, modelin aşamaları tek tek incelenecek ve gerçek dünya senaryolarında bu bilgilerin uygulama alanları üzerinde durulacaktır.



Cyber Kill Chain modeli toplam yedi aşamada ele alınır. Bu aşamalar, siber saldırganın hedef sisteme ulaşma yolculuğunu detaylı bir şekilde açıklar ve her bir aşama, saldırganı durdurmak için bir fırsat sunar.

1. **Reconnaissance (Keşif):**

Bu aşamada saldırgan, hedef sistemi ve sistemdeki zayıflıkları araştırır. Amaç, hedef hakkında mümkün olan en fazla bilgiyi toplamaktır. Bu bilgiler ağ yapısı, kullanılan yazılımlar, çalışan e-posta adresleri ve ağ cihazları gibi unsurlar olabilir. Keşif genellikle sosyal mühendislik ve açık kaynak araştırma (OSINT) teknikleri ile gerçekleştirilir. Örnek olarak, saldırganın LinkedIn gibi platformlardan çalışan bilgilerini toplaması veya Shodan kullanarak ağ cihazlarını taraması gösterilebilir.

2. **Weaponization (Silahlandırma):**

Toplanan bilgiler kullanılarak siber saldırı aracı oluşturulur. Bu, zararlı bir yazılımın (malware) geliştirilmesi veya mevcut bir zararlı yazılımın hedefe uygun hale getirilmesi anlamına gelir. Örneğin, saldırgan bir fidye yazılımı (ransomware) oluşturabilir ve bu yazılımı, hedef organizasyona yönelik bir phishing e-postasına ekleyebilir. Bu aşamada siber saldırı aracını tespite yönelik antivirüs yazılımları kritik rol oynar.

3. **Delivery (Teslimat):**

Hazırlanan siber saldırı aracı hedefe ulaştırılır. Bu, genellikle e-posta ekleri, zararlı linkler, USB cihazları veya sahte web siteleri yoluyla gerçekleştirilir. Örneğin, saldırgan hedef bir şirket çalışanına sahte bir iş teklifini içeren e-posta gönderip zararlı bir belge ekleyebilir. Bu aşamada e-posta filtreleme sistemleri ve güvenli internet geçitleri, tehditlerin yakalanmasında etkilidir.

4. **Exploitation (Sömürülme):**

Teslim edilen zararlı yazılım, hedef sistemdeki bir açığı kullanarak çalışmaya başlar. Örneğin, güncellenmemiş bir yazılımın zafiyetinden faydalanılarak zararlı kod çalıştırılabilir. Örnek olarak, WannaCry zararlı yazılımı "EternalBlue" zafiyetinden faydalanmıştır. Bu aşamada sistemlerin güncel tutulması ve çok faktörlü kimlik doğrulama kullanımı önemlidir.

5. **Installation (Kurulum):**

Zararlı yazılım, hedef sisteme tamamen kurulur ve kalıcı hale gelir. Bu aşamada arka kapılar (backdoor) oluşturulur veya rootkit gibi teknikler kullanılarak sistemde gizlenir. Örneğin, bir sistemin dosya yapısına fark edilmeden yerleştirilen bir zararlı yazılım, daha sonra saldırganın komutlarını yerine getirebilir. Kurulum aşamasında davranış analizi yapan antivirüsler etkili olabilir.

6. **Command and Control (Komuta ve Kontrol):**

Saldırgan, hedef sisteme uzaktan erişim sağlar ve sistemi yönetmek için bir komuta ve kontrol kanalı oluşturur. Örneğin, saldırgan hedef sistemden veri çekmek için DNS veya HTTP tabanlı bir iletişim kanalı kurabilir. Bu aşamada anormal trafik davranışlarını tespit eden izleme sistemleri tehditlerin önünü kesebilir.

7. **Actions on Objectives (Amaçlara Yönelik Hareketler):**

   Saldırgan, nihai amacını gerçekleştirir. Bu, verilerin çalınması, sistemin sabote edilmesi veya fidye talep edilmesi gibi eylemleri içerebilir. Örneğin, bir bankacılık sistemi saldırıya uğradıysa, saldırgan müşteri bilgilerini çalarak fidye talep edebilir. Bu aşamada, olay müdahale ekipleri saldırının etkisini sınırlamak için devreye girmelidir.

Her bir aşamada saldırıyı engelleme fırsatı bulunmaktadır. Örneğin, erken uyarı sistemleri veya e-posta filtreleme yazılımları ile "Delivery" aşamasında tehdit durdurulabilir.

Sonuç olarak; Cyber Kill Chain, siber saldırıların detaylı bir şekilde analiz edilmesine ve savunma mekanizmalarının bu aşamalara uygun olarak geliştirilmesine olanak tanır. Her bir aşama, saldırganın nerede olduğunu anlamak için kritik ipuçları sunar.

Bir saldırının hangi aşamada olduğunu anlamak için izlenecek bazı adımlar şunlardır:

1. **Ağ Trafiği Analizi:**

   Eğer sistemde anormal ağ hareketlilikleri veya bilinmeyen IP adreslerine veri gönderimi tespit edilirse, saldırgan muhtemelen "Command and Control" aşamasına geçmiş olabilir.

2. **Kullanıcı Davranış İzleme:**

   Kullanıcıların beklenmedik dosyaları açması veya bilinmeyen kaynaklardan yazılım çalıştırması "Delivery" ya da "Exploitation" aşamalarının işaretleri olabilir.

3. **Log Analizleri:**

   Sistem logları, "Reconnaissance" aşamasındaki ağ taramaları veya yetkisiz giriş denemelerini tespit etmek için kritik bir kaynak sağlar.

4. **Saldırı İmza Tespiti:**

   Antivirüs veya IDS/IPS sistemleri, bilinen saldırı kalıplarını tespit ederek "Weaponization" veya "Installation" aşamalarında tehditleri ortaya çıkarabilir.

5. **Veri Bütünlüğü Kontrolleri:**

   Sistem dosyalarında beklenmedik değişiklikler tespit edilirse, "Installation" aşamasında bir zararlı yazılımın kurulum aşamasında olduğu anlaşılabilir.

Cyber Kill Chain modeli, hem savunma hem de olay müdahale ekiplerine rehberlik ederek proaktif bir siber güvenlik stratejisi oluşturulmasını sağlar. Özellikle, her aşama için uygun güvenlik önlemlerinin uygulanması, saldırıları erken aşamalarda durdurmayı ve zararı en aza indirmeyi mümkün kılar. Bu nedenle, SOC analistlerinin bu modeli iyi anlaması ve gerçek zamanlı olay müdahale süreçlerinde etkin bir şekilde kullanması kritik öneme sahiptir.

KAYNAKÇA

- https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
- https://www.gaissecurity.com/blog/cyber-kill-chain-bir-siber-saldirinin-yasam-dongusu
- https://berqnet.com/blog/cyber-kill-chain
- https://www.microsoft.com/en-us/security/business/security-101/what-is-cyber-kill-chain
- https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/cyber-kill-chain/
- https://cyberartspro.com/en/cyber-kill-chain-nedir/