Cyber Kill Chain

Hazırlayan: Berra SÖYLER

Tarih: 07.02.2025

İçindekiler

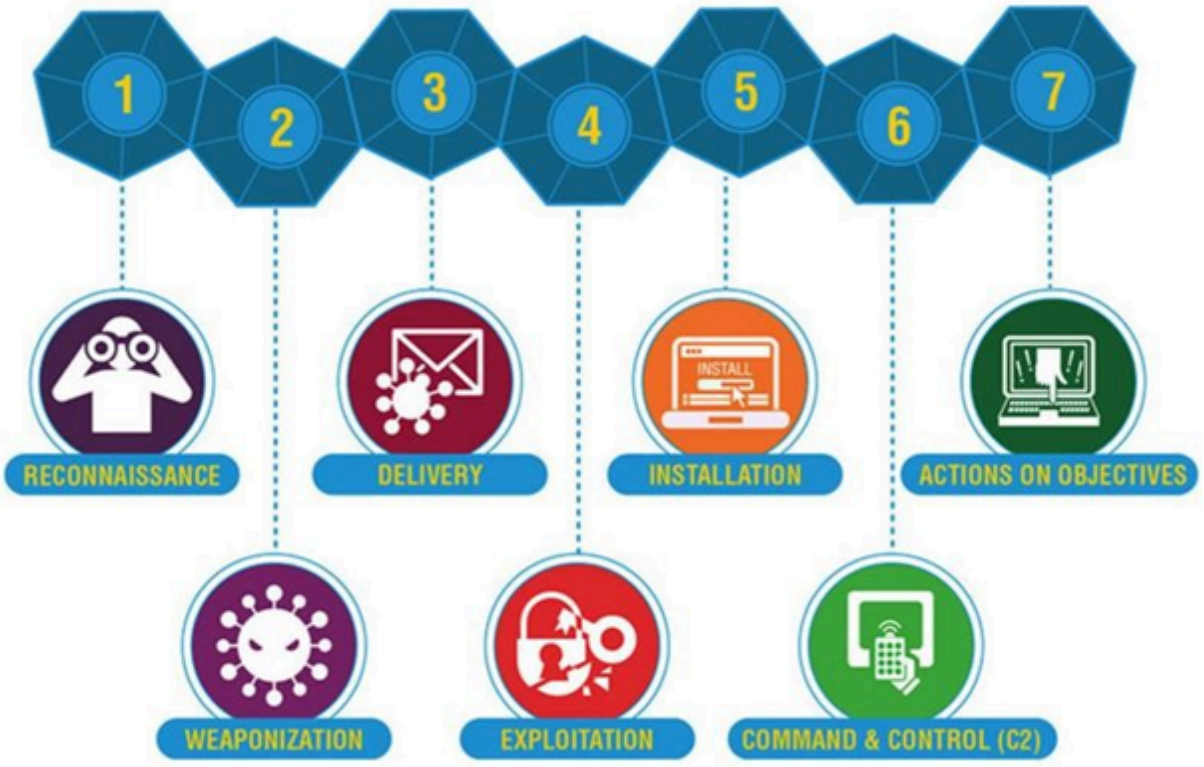
Giriş

Siber güvenlik dünyasında, saldırganların yöntemlerini ve saldırı süreçlerini anlamak, etkili savunma stratejileri geliştirmek için kritik öneme sahiptir. Bu bağlamda, Lockheed Martin tarafından geliştirilen Cyber Kill Chain modeli, siber saldırıların aşamalarını sistematik bir şekilde analiz ederek, savunma ekiplerine rehberlik etmektedir. Bu raporda, Cyber Kill Chain modelinin detaylı bir incelemesi yapılacak, her bir aşama açıklanacak ve SOC (Security Operations Center) ekiplerinin bu modeli nasıl kullanabileceği ele alınacaktır.

1.Cyber Kill Chain Nedir?

Cyber Kill Chain, Lockheed Martin tarafından geliştirilen ve saldırganların bir siber saldırıyı nasıl planlayıp uyguladığını aşamalara ayıran bir modeldir. Bu çerçeve, saldırı sürecinin sadece son aşamasını değil, başlangıcından itibaren tüm evrelerini detaylı bir biçimde analiz eder. Böylece, savunma ekipleri saldırının hangi noktasında müdahale ederek zararı en aza indirebileceklerini belirleyebilir.

Cyber Kill Chain, saldırganların izlediği adımları sistematik hale getirir ve her aşamada ortaya çıkan zayıf noktalara yönelik önlemler alınmasını sağlar. Model, saldırı sürecinde gerçekleştirilen faaliyetlerin anlaşılmasına ve bu faaliyetlerin erken tespit edilerek durdurulmasına yardımcı olur. Bu sayede, organizasyonlar saldırıların gerçekleşme olasılığını düşürürken, başarılı bir saldırı durumunda bile etkilerini sınırlamayı başarır.



2. Cyber Kill Chain Aşamaları

1. **Reconnaissance (Keşif):** Saldırgan, hedef sistem veya kuruluş hakkında bilgi toplayarak güvenlik açıklarını belirler.
2. **Weaponization (Silahlandırma):** Saldırgan, keşif aşamasında elde ettiği bilgilere göre zararlı yazılım veya saldırı araçları hazırlar.
3. **Delivery (Teslimat):** Saldırgan, hazırladığı zararlı yazılımı hedefe ulaştırmak için e-posta, sahte web sitesi veya güvenlik açığı içeren bir dosya gibi yöntemler kullanır.
4. **Exploitation (İstismar):** Teslim edilen zararlı yazılım veya saldırı kodu, hedef sistemdeki bir güvenlik açığını kullanarak saldırının aktif hale gelmesini sağlar.
5. **Installation (Kurulum):** Zararlı yazılım, hedef sistemde kalıcılığını sağlamak için kendini kurar ve saldırganın erişimini sürdürmesine olanak tanır.
6. **C2 (Komuta & Kontrol):** Saldırgan, ele geçirilen sistemle uzaktan bağlantı kurarak saldırıyı yönetir ve ek komutlar gönderir.
7. **Actions on Objectives (Son Hedefler):** Saldırgan, verileri çalmak, sistemleri şifrelemek, hizmetleri devre dışı bırakmak veya diğer zararlı eylemleri gerçekleştirmek gibi nihai amacına ulaşır.

Bu aşamaların her biri, saldırı sürecinin kritik bir parçasını oluşturur ve savunma stratejilerinin hangi aşamada etkin olabileceğini anlamamıza yardımcı olur. Böylece, Cyber Kill Chain modeli sayesinde organizasyonlar, saldırının erken evrelerinde müdahale ederek saldırının başarısız olmasını sağlayabilirler.

3. Cyber Kill Chain'in Aşamalarıyla Saldırı Örnekleri

Cyber Kill Chain modeliyle her saldırının belirli aşamalardan geçtiğini bilmek, saldırının hangi noktada durdurulabileceğini anlamamıza yardımcı olur. Aşağıda, farklı saldırı türlerini Cyber Kill Chain aşamalarıyla eşleştirerek, saldırının nasıl ilerlediği detaylıca açıklanmıştır.

a. Brute-Force Saldırısı

Brute-force saldırıları, saldırganın bir hesaba veya sisteme yetkisiz erişim sağlamak için sürekli farklı şifreler denediği bir saldırı türüdür.

Saldırının Cyber Kill Chain Aşamalarına Göre İncelenmesi

Reconnaissance (Keşif):
- Saldırgan, hedef sistemin giriş noktalarını analiz eder.
- SSH, RDP veya VPN gibi dışa açık giriş arabirimlerini tespit etmek için port taraması yapar.

Weaponization (Silahlandırma):
- Saldırgan, kaba kuvvet saldırısı için bir parola listesi (wordlist) oluşturur veya var olan bir veri sızıntısından elde edilen kimlik bilgilerini kullanır.

- Delivery (Teslimat) (Bu saldırıda doğrudan bir teslimat aşaması yoktur.)

Exploitation (İstismar):
- Saldırgan, hedef sisteme sürekli olarak farklı şifreler deneyerek yetkisiz erişim elde etmeye çalışır.
- Eğer şifre kırılırsa, saldırgan sisteme giriş yapar.

Installation (Kurulum):
- Saldırgan, ele geçirdiği hesap üzerinden kalıcılığını sağlamak için arka kapılar (backdoor) oluşturur.
- Mevcut kullanıcıların şifrelerini değiştirerek erişimi kontrol altına alır.

C2 (Komuta & Kontrol):
- Saldırgan, ele geçirilen hesabı bir C2 sunucusuna bağlayarak uzaktan yönetmeye başlar.

Actions on Objectives (Son Hedefler):
- Saldırgan, sistemde yeni kullanıcı hesapları oluşturarak kalıcılığını artırır.
- Hassas verilere erişim sağlarsa, bu verileri çalabilir veya değiştirebilir.

b. Ransomware (Fidye Yazılımı) Saldırısı

Ransomware saldırıları, saldırganların sistemleri zararlı yazılımlarla sisteme yerleşip şifreleyerek kullanılamaz hale getirmesi ve fidye talep etmesi ile gerçekleşir.

Saldırının Cyber Kill Chain Aşamalarına Göre İncelenmesi

Reconnaissance (Keşif):
- Saldırgan, hangi şirketlerin güvenlik açıkları olduğunu araştırır.
- Dark web üzerinde, zayıf VPN erişimleri veya eski sistemler hakkında bilgi toplayabilir.

Weaponization (Silahlandırma):
- Fidye yazılımını (ransomware) özel olarak hedeflenen işletim sistemi ve ağ yapısına göre özelleştirir.

Delivery (Teslimat):
- Saldırgan, fidye yazılımını hedefe ulaştırmak için bir e-posta eki, sahte web sitesi veya USB belleğe gizlenmiş zararlı dosya kullanabilir.

Exploitation (İstismar):
- Kullanıcı, sahte e-postayı açıp zararlı dosyayı çalıştırdığında fidye yazılımı etkinleşir.

Installation (Kurulum):
- Fidye yazılımı, sistem içinde yayılmaya başlar ve ağdaki diğer sistemlere bulaşır.
- Yanal hareket (lateral movement) yaparak diğer cihazları etkiler.

C2 (Komuta & Kontrol):
- Fidye yazılımı, saldırganın sunucusuna bağlanarak saldırıyı yöneten kişiye rapor verir.
- Şifreleme anahtarları saldırganın kontrol ettiği bir sunucuda saklanır.

Actions on Objectives (Son Hedefler):
- Tüm dosyalar şifrelenir ve saldırgan fidye ödenmesini talep eden bir mesaj bırakır.
- Eğer fidye ödenmezse, veriler kalıcı olarak silinebilir.

c. Phishing Saldırısı (Phishing Attack)

Phishing saldırıları, saldırganların sahte e-postalar, mesajlar veya web siteleri aracılığıyla hedef kullanıcıları aldatıp kimlik bilgilerini, finansal verileri veya diğer hassas bilgileri ele geçirmeye yönelik sosyal mühendislik teknikleridir. Cyber Kill Chain modeli çerçevesinde incelendiğinde, phishing saldırılarında saldırganların izlediği aşamalar şu şekilde sıralanabilir:

Saldırının Cyber Kill Chain Aşamalarına Göre İncelenmesi

Reconnaissance (Keşif):
-Saldırgan, hedef organizasyona ait çalışanların e-posta adreslerini, sosyal medya profillerini ve kamuya açık diğer bilgileri toplar.
-Bu aşamada, hedef kullanıcıların ilgi alanları, görevleri ve iletişim alışkanlıkları gibi veriler de elde edilir.

Weaponization (Silahlandırma):
-Toplanan bilgiler doğrultusunda, saldırgan gerçek bir kurumdan geliyormuş gibi görünen sahte e-postalar ve/veya web siteleri oluşturur.
-Bu içeriklerde, kullanıcının dikkatini çekecek ve güvenini kazanacak mesajlar, görseller veya belgeler yer alır.

Delivery (Teslimat):
-Hazırlanan sahte e-postalar, SMS veya sosyal medya mesajları aracılığıyla hedef kullanıcılara gönderilir.
-Bu mesajlar, kullanıcıyı sahte web sitesine yönlendirecek bağlantılar veya ekler içerir

Exploitation (İstismar):
-Kullanıcı, gelen sahte e-postayı açıp içindeki bağlantıya tıkladığında ya da ek dosyayı indirip açtığında, sahte web sitesi veya içerik aracılığıyla giriş bilgilerini, kişisel verilerini ya da finansal bilgileri girmesi istenir.
-Bu aşamada, sosyal mühendislik etkisiyle kullanıcı, bilgilerini asılsız bir güvenlik talebi kapsamında vermeye ikna edilir.

Installation (Kurulum):
-Kullanıcının kimlik bilgilerini veya diğer hassas verileri girdikten sonra, saldırgan bu bilgileri ele geçirir.
-Bazı durumlarda, phishing saldırısı sonrasında zararlı yazılımın (malware) yüklenmesi de gerçekleşebilir; böylece saldırgan, hedef sistemde daha kalıcı bir varlık elde eder.

C2 (Komuta & Kontrol):
-Ele geçirilen kimlik bilgileri ve diğer veriler, saldırganın kontrolündeki sunuculara aktarılır.
-Bu sayede saldırgan, ele geçirilen hesaplar üzerinde uzaktan kontrol sağlayarak daha fazla bilgi toplama ya da ileri düzey saldırılar gerçekleştirme imkanına kavuşur.

Actions on Objectives (Son Hedefler):
-Saldırgan, ele geçirdiği bilgileri kullanarak yetkisiz erişim elde eder, finansal işlemler gerçekleştirebilir, veri hırsızlığı yapabilir veya bu bilgileri dark web'de satabilir.
-Nihai hedef, elde edilen bilgileri kullanarak daha fazla zarar vermek ya da gelir elde etmektir.

4. Cyber Kill Chain'in SOC'ta Rehber Alınması

SOC ekipleri için Cyber Kill Chain modeli, saldırı sürecini daha iyi anlamalarını ve olaylara zamanında müdahale etmelerini sağlayan güçlü bir rehberdir. Bu model, saldırganların izlediği bu temel adımları detaylandırarak, SOC'nin hangi aşamada hangi log ve uyarıları yakalaması gerektiğini belirlemede yardımcı olur. Böylece, SOC analistleri saldırının hangi evresinde olduklarını saptayarak, uygun ve zamanında olay müdahalesi (incident response) gerçekleştirebilirler. Örneğin, her saldırı türü Cyber Kill Chain'in farklı aşamalarında izlenebilecek belirli göstergeler sunar:

a. Brute Force Saldırısı:

SOC analistleri, SIEM veya IDS/IPS araçları aracılığıyla bir IP adresinden çok sayıda başarısız giriş denemesine ait logları tespit ederse, bu durum saldırının "Exploitation" aşamasında gerçekleştiğini işaret eder. Bu aşamada, sistem yöneticileri IP adresini engelleyerek ve erişim politikalarını güncelleyerek müdahaleye geçebilir. Böylece saldırının ilerlemesi önlenmiş olur.

Eğer SOC analistleri, bir saldırganın sadece başarısız denemelerle kalmayıp sisteme eriştiğini fark ederse, bu durum saldırının Exploitation aşamasının başarıyla tamamlandığını ve sistemin artık Installation aşamasına geçtiğini gösterir. Yani saldırgan, mevcut güvenlik açığından yararlanarak sisteme giriş yapmış ve artık kalıcı bir iz bırakmak için zararlı yazılım (backdoor, rootkit vb.) yüklemeye ya da başka kötü niyetli bileşenleri devreye sokmaya başlamıştır. Bu durumda SOC analistleri Installation Aşamasını engelleyerek zararlı yazılımın veya kalıcı arka kapıların sisteme yüklenmesi engellemeye çalışır.

b. Ransomware Saldırısı:

Saldırgan, zararlı ek dosya veya bağlantı aracılığıyla ransomware'i hedef sisteme gönderir. SOC, şüpheli e-posta trafiği veya zararlı dosya ekleri loglarını inceleyerek bu aşamayı "Delivery" aşamasında tespit edebilir.

Kullanıcı, zararlı ek dosyayı açıp ransomware'ı çalıştırdığında, saldırı "Exploitation" aşamasını tamamlamış olur. SOC, bu aşamada anormal dosya erişim ve işlem aktivitelerini loglardan fark edebilir.

Ransomware, sisteme girdikten sonra kalıcı hale gelmek üzere kendisini yükler ve dosyaları şifrelemeye başlar. SOC, özellikle dosya şifreleme aktivitelerindeki ani artış, sistem performansında düşüş ve ilgili uyarı loglarını tespit ederek, saldırının "Installation" aşamasında olduğunu belirler.

Eğer ransomware'ın yüklenme ve dosya şifreleme aktiviteleri fark edilirse, SOC analistleri etkilenen uç noktaları hızla izole ederek ve ağdaki lateral hareketi engelleyerek saldırının C2 (Komuta & Kontrol) ve Actions on Objectives (Son Hedefler) aşamalarına ilerlemesini durdurmaya çalışır.

c. Phishing Saldırısı:

Saldırgan, sahte e-posta veya mesajlar aracılığıyla hedef kullanıcılara kimlik avı (phishing) içerikleri gönderir. SOC, e-posta trafiği ve ilgili log kayıtlarını izleyerek bu aşamadaki olağandışı aktiviteleri "Deliverye" aşamasında tespit edebilir.

Kullanıcı, sahte e-postadaki bağlantıya tıkladığında veya kimlik bilgilerini girdiğinde saldırı "Exploitation" aşamasını başarıyla tamamlamış olur. Bu durum, SOC'nin kimlik doğrulama loglarında ve erişim kayıtlarında, beklenmeyen giriş aktiviteleri şeklinde ortaya çıkar.

Eğer phishing saldırısı sonucunda bir kullanıcının kimlik bilgileri ele geçirilmişse, SOC analistleri bu durumu tespit ederek, ilgili hesabı geçici olarak devre dışı bırakma, şifre sıfırlama ve ek kimlik doğrulama önlemleri uygulama yoluna gider. Böylece, saldırganın daha ileri aşamalara (örneğin, Installation veya C2 aşamalarına) geçişi önlenmiş olur.

Dolayısıyla Cyber Kill Chain'in her aşamasına yönelik olarak SOC'nin topladığı loglar ve uyarılar, olay müdahale sürecinin hangi evresinde olduğunu belirlemede kritik rol oynar. Bu sayede, SOC ekipleri olayları doğru şekilde sınıflandırıp önceliklendirebilir. Bu da SOC ekibinin olaylara hızlı ve etkili yanıt vererek, organizasyonun genel siber güvenlik duruşunu güçlendirmesine yardımcı olur.

5. Cyber Kill Chain Modelinin Avantajları ve Sınırlılıkları

Cyber Kill Chain modeli, siber saldırıların yedi aşamasını tanımlayarak (keşif, silahlandırma, teslimat, istismar, kurulum, komuta ve kontrol, hedeflere ulaşma) güvenlik ekiplerinin saldırıları daha iyi anlamalarına ve erken tespitle önlemelerine yardımcı olmasının yanı sıra bazı gelişmiş kalıcı tehditler (APT'ler gibi), geleneksel saldırı aşamalarını atlayabilir veya farklı teknikler kullanabilir, bu da modelin bu tür tehditleri tespit etmede yetersiz kalmasına neden olabilir. Ayrıca saldırganlar, tespit edilmekten kaçınmak için sürekli olarak yeni teknikler geliştirmektedir. Bu dinamik doğa, sabit aşamalara dayanan modellerin etkinliğini azaltabilir. Dolayısıyla, bu model siber saldırıların anlaşılması ve önlenmesinde değerli bir çerçeve sunarken güvenlik ekiplerinin gelişmiş ve dinamik tehditlere karşı daha esnek ve kapsamlı stratejiler geliştirmesi gerekliliğini de ortaya koymaktadır. MITRE ATT&CK gibi diğer yöntemlerin de araştırılıp öğrenilmesi ve sürekli güncel olunmasıyla saldırılara karşı etkili bir savunma mekanizması geliştirmek SOC ekipleri için vazgeçilmezdir.

6. Sonuç

Bu raporda, Cyber Kill Chain modeli ve SOC (Security Operations Center) ekiplerinin bu modeli nasıl kullanabileceği detaylı bir şekilde incelenmiştir. Cyber Kill Chain, siber saldırıların aşamalarını sistematik olarak tanımlayarak, savunma stratejilerinin hangi noktalarda etkili olabileceğini göstermektedir. SOC ekipleri, bu model sayesinde saldırıların erken evrelerinde tespit ve müdahale imkânı bulabilirler.

Özellikle brute-force, fidye yazılımı (ransomware) ve phishing gibi saldırı türlerinin Cyber Kill Chain aşamalarına göre analiz edilmesi, saldırıların hangi noktada durdurulabileceğini anlamamıza yardımcı olur. Bu analizler, SOC ekiplerinin log ve uyarıları doğru yorumlayarak, olay müdahale süreçlerini daha etkili yönetmelerini sağlar.

Sonuç olarak, Cyber Kill Chain modeli, siber güvenlik savunmasında kritik bir araç olup, saldırıların erken aşamalarda tespit edilmesi ve etkili müdahale stratejilerinin geliştirilmesi için SOC ekiplerine rehberlik etmekle beraber diğer yöntemlerin de öğrenilmesinin gerekliliği belirtilmiştir.

7. Kaynakça

https://www.gaissecurity.com/blog/cyber-kill-chain-bir-siber-saldirinin-yasam-dongusu
https://berqnet.com/blog/cyber-kill-chain
https://www.splunk.com/en_us/blog/learn/cyber-kill-chains.html
https://www.datapalladium.com/understanding-cyber-kill-chain-model/?utm_source=chatgpt.com
https://www.lepide.com/blog/cyber-kill-chain-vs-mitre-attck-what-are-the-key-differences/