CYBER KİLL CHAİN

ALTAY TAKIMI

HAZIRLAYAN:**MUHAMMED ALİ ZENGİN**
22.02.2025

İçindekiler

1.GİRİŞ

Günümüzde kurumlar ve bireyler, siber saldırganların sürekli evrilen yöntemlerine karşı güçlü bir savunma mekanizması geliştirmek zorundadır. Bu bağlamda, Lockheed Martin tarafından geliştirilen Cyber Kill Chain modeli, bir siber saldırının aşamalarını sistematik bir şekilde analiz ederek, tehditlerin erken tespit edilmesi ve engellenmesi için kapsamlı bir çerçeve sunmaktadır.

Bu sunumda, Cyber Kill Chain modelinin aşamalarını detaylı bir şekilde ele alarak, siber saldırganların izlediği yöntemleri ve bu tehditlere karşı alınabilecek önlemleri inceleyeceğiz. Siber güvenliğin her geçen gün daha kritik hale geldiği günümüzde, etkili bir savunma stratejisi oluşturmanın temel unsurlarını birlikte değerlendireceğiz.

2.Cyber Kill Chain Nedir?

İlk olarak 2011 yılında Lockheed Martin tarafından geliştirilen siber öldürme zinciri, yaygın siber saldırıların çeşitli aşamalarını ve dolayısıyla bilgi güvenliği ekibinin saldırganları önleyebileceği, tespit edebileceği veya engelleyebileceği noktaları ortaya koyar.

Bu model, bir saldırının genellikle yedi temel aşamadan oluştuğunu varsayar. Bu aşamaların her biri, saldırının ilerleyişini durdurmak için kritik müdahale noktaları sunar. Amaç, saldırıyı mümkün olduğunca erken aşamada tespit ederek saldırganın ilerlemesini engellemektir.

3.Cyber Kill Chain 7 Aşaması

3.1.Reconnaissance (keşif)

Bu aşama, saldırganın hedef sistem hakkında bilgi topladığı aşamadır. Buradaki amaç, sisteme sızmak için en uygun yöntemi belirlemektir. Saldırgan; hedef sistemin IP adreslerini, çalışan bilgilerini ve kullanılan güvenlik sistemlerini tespit eder. Temel amacı, istismar edebileceği güvenlik açıklarını bulmaktır.

3.2.Weaponization (silahlanma)

Bu aşamada saldırgan, hedef sistem hakkında topladığı bilgileri kullanarak hangi saldırı vektörünü kullanacağına karar verir. Zararlı yazılımlar (malware) da bu aşamada oluşturulur.Saldırgan ayrıca, ağ yöneticileri tarafından orijinal giriş noktası tespit edilip kapatılırsa sisteme erişimini sürdürebilmek için arka kapılar da kurabilir.

3.3.Delivery (iletme)

Bu aşama, saldırının hedef sisteme ulaştırılmasını içerir. Saldırgan, zararlı yazılımı e-posta, USB, kötü amaçlı web siteleri veya sosyal mühendislik teknikleri ile hedef sisteme iletir.
Burada en yaygın saldırı yöntemi oltalama saldırısıdır (phishing). Saldırgan, sistemdeki en zayıf halkayı hedef alarak saldırıyı gerçekleştirir.

3.4.Exploitation (sömürme)

Bu aşamada, kötü amaçlı kod, kurbanın sistemi içerisinde yürütülür.

3.5.Installation (yükleme)

Bu aşamada saldırgan, hedef sistemde zararlı yazılımı çalıştırdıktan sonra kalıcılık sağlamak için çeşitli yöntemler kullanır. Sistemde daha uzun süre gizlenebilmek için arka kapılar (backdoor) veya rootkitler yükleyebilir.
Saldırgan bu aşamada başarıyla sisteme yerleşmiş olur ve sistemi kontrol edebilir

3.6.C2 (Command & Control)

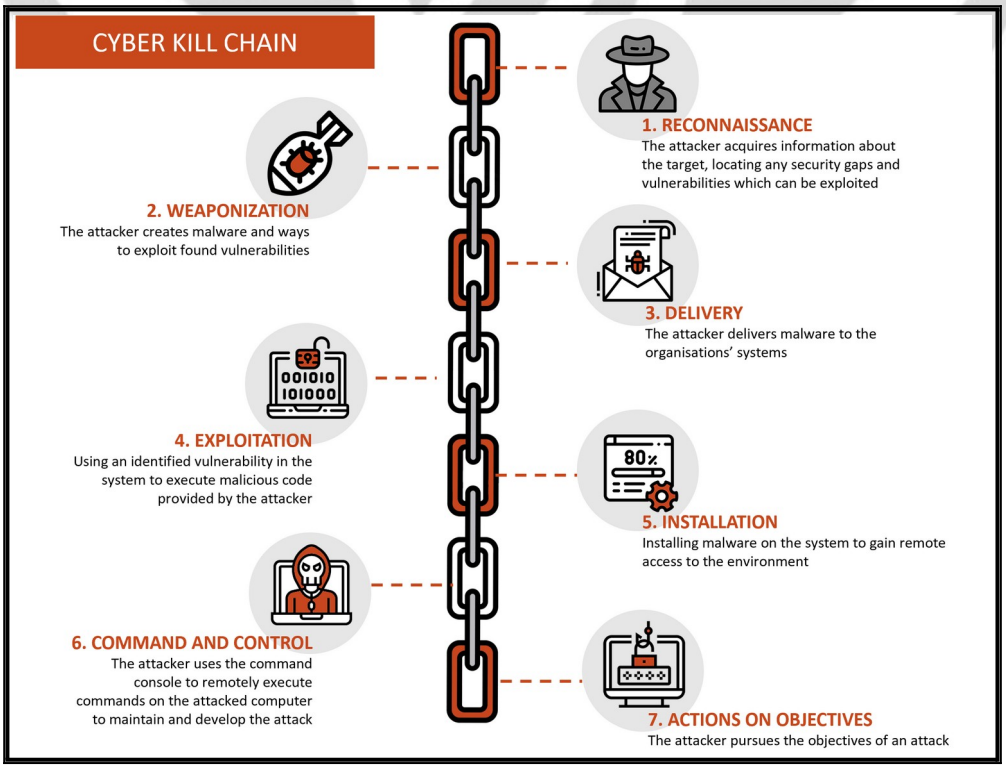
Bu aşama, saldırganın hedef sistemle uzaktan bağlantı kurduğu aşamadır. Hedef sistemin kontrolü tamamen saldırganın eline geçer.

3.7.Actions On Objectives (eylem)

Bu aşamada, saldırgan hedeflediği amaçları gerçekleştirmek için adımlar atar. Bu amaçlar arasında veri hırsızlığı, yok etme, şifreleme veya dışarıya sızdırma bulunabilir.

3.8.Monetization(Gelir elde etme)

Lockheed Martin'in orijinal siber öldürme zinciri modeli yalnızca yedi adımdan oluşsa da, birçok siber güvenlik uzmanı bunu sekiz adıma genişletmiştir. Bu ek adım, saldırganların saldırıdan gelir elde etmek için gerçekleştirdiği faaliyetleri kapsar. Örneğin, saldırganlar kurbanlarından fidye almak amacıyla fidye yazılımı kullanabilir veya hassas verileri dark web üzerinde satarak kazanç sağlayabilir.



4.Cyber Kill Chain Sınırlamaları ve Eksiklikleri

Lockheed Martin'in Cyber Kill Chain modelini ilk kez tanıttığı 2011 yılından bu yana, teknoloji ve siber tehditler büyük ölçüde değişti. Birçok siber saldırı, öldürme zincirinde özetlenen sekiz aşamayı takip etse de, bazı saldırılar bu süreci atlayabilir veya birkaç adımı tek bir eylemde birleştirebilir. Bu durum, tehditleri yalnızca bu modele göre analiz eden kuruluşların bazı saldırıları gözden kaçırmasına neden olabilir.

Bunun yanı sıra, Cyber Kill Chain modeli genellikle dış tehditlere odaklanmıştır. Ancak, halihazırda sistemlere erişimi olan içeriden gelen tehditleri tespit etmek bu modelle daha zordur. Ayrıca, model kötü amaçlı yazılımlara ağırlık vermekte olup, sosyal mühendislik, kimlik avı ve güvenlik açıklarının suistimali gibi farklı saldırı türlerini yeterince kapsamamaktadır.

Tüm bu eksikliklere rağmen, Cyber Kill Chain hâlâ siber güvenlik dünyasında önemli bir araç olmaya devam etmektedir. Kuruluşların saldırganların bakış açısını anlamalarına yardımcı olurken, güvenlik stratejilerini daha etkili bir şekilde oluşturmalarına da katkı sağlamaktadır.

5.Sonuç

Cyber Kill Chain modeli, siber saldırıların aşamalarını anlamak ve savunma stratejileri geliştirmek için güçlü bir çerçeve sunmaktadır. Özellikle tehditlerin tespit edilmesi ve erken aşamada durdurulması konusunda kuruluşlara rehberlik eder
Cyber Kill Chain siber güvenlik dünyasında önemli bir yer tutmaya devam etse de, kuruluşların MITRE ATT&CK çerçevesi, Zero Trust güvenlik yaklaşımı ve davranışsal analiz gibi modern güvenlik stratejilerini de benimsemeleri gerekmektedir.

6.Kaynakça;

https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/cyber-kill-chain/
https://www.microsoft.com/en-us/security/business/security-101/what-is-cyber-kill-chain
https://cyberartspro.com/en/cyber-kill-chain-nedir/
https://en.wikipedia.org/wiki/Cyber_kill_chain