# CYBER KILL CHAIN

**MELİKE TAŞDELEN**

**07.02.2025**

# GİRİŞ

Günümüzde siber saldırılar giderek daha karmaşık hale gelmekte ve saldırganlar her geçen gün yeni teknikler geliştirmektedir. Bu durum, güvenlik ekiplerinin saldırıları erken aşamada tespit etmesi ve etkili müdahale mekanizmaları oluşturmasını zorunlu kılmaktadır. İşte bu noktada, Lockheed Martin tarafından geliştirilen Cyber Kill Chain modeli, saldırıların nasıl ilerlediğini anlamak ve savunma stratejileri geliştirmek için önemli bir çerçeve sunmaktadır.

Cyber Kill Chain, bir siber saldırıyı aşamalar halinde tanımlayan bir modeldir. Bu model, saldırıların erken tespit edilmesini ve etkili müdahale edilmesini sağlayarak organizasyonların güvenlik operasyonlarını güçlendirmeye yardımcı olur.

Bu raporda, Cyber Kill Chain aşamaları ele alınmıştır.

# İÇİNDEKİLER

## CYBER KILL CHAIN NEDİR?

Siber saldırı zinciri olarak da bilinen siber öldürme zinciri, karmaşık siber saldırıları kesintiye uğratmaya ve engellemeye yardımcı olmak için tasarlanmış bir siber güvenlik modelidir. Lockheed Martin tarafından 2011 yılında geliştirilmiştir. Siber saldırıları yedi ayrı aşamaya bölerek, bir siber saldırının yaşam döngüsünü anlamaya yönelik bir yaklaşım sunar.

## NEDEN KULLANILIR?

Siber Öldürme Zinciri, saldırganların siber saldırıları nasıl planlayıp gerçekleştirdiğini anlamak için bir çerçeve sunar. Savunma stratejilerini belirlemek ve geliştirmek için kullanılır. Her aşamada alınan önlemler, saldırıları tespit etmeye ve etkilerini azaltmaya yardımcı olabilir.

## NERELERDE KULLANILIR?

Siber Öldürme Zinciri, siber saldırı riski altında olan herhangi bir kuruluş veya birey için geçerlidir. İster büyük bir şirket, ister bir devlet kurumu veya küçük bir işletme olsun, bir siber saldırının aşamalarını anlamak etkili bir savunma için önemlidir.

## NEDEN ÖNEMLİDİR?

Siber Öldürme Zinciri, savunmacıların siber saldırıların planlamanın ilk aşamalarından son aşamalara kadar nasıl gerçekleştiğini anlamalarına yardımcı olur. Siber Öldürme Zinciri, siber tehdit yaşam döngüsünün tüm aşamalarında önemlidir. Saldırganların kullandığı taktikleri anlayarak savunmacılar siber tehditlere karşı daha iyi hazırlanabilir ve onları azaltabilir.

## CYBER KILL CHAIN' in SOC EKİPLERİ İÇİN ÖNEMİ

Cyber Kill Chain, SOC (Security Operations Center) ekipleri için siber saldırıları tespit etmek, analiz etmek ve etkili bir şekilde müdahale etmek adına kritik bir rehberdir. SOC analistleri ve güvenlik mühendisleri, Cyber Kill Chain modelini kullanarak saldırı yaşam döngüsünü anlamlandırabilir ve tehditlere proaktif olarak yanıt verebilir.

SIEM, IDS/IPS, SOAR ve tehdit istihbaratı gibi araçlarla entegre edilerek güçlü bir savunma mekanizması oluşturulabilir.

## CYBER KILL CHAIN NASIL ÇALIŞIR?

Cyber Kill Chain, siber saldırının çeşitli aşamalarını belirleyerek çalışır. Her aşama, saldırganın belirli bir hedefe ulaşmak için gerçekleştirdiği adımları temsil eder. Saldırı aşamalarını anlamak, savunma ekiplerinin saldırganı erken tespit ederek saldırıyı engellemesine olanak tanır. Cyber Kill Chain'in temel çalışma prensibi, saldırganın faaliyetlerini erken aşamalarda durdurarak saldırının tamamlanmasını önlemektir.

# CYBER KILL CHAIN'in AŞAMALARI

Siber öldürme zinciri, siber saldırganların zihniyetini, motivasyonlarını, araçlarını, yöntemlerini ve tekniklerini, nasıl karar aldıklarını ve tespitten nasıl kaçtıklarını anlama amacıyla bir dizi siber saldırı aşamasını tanımlar.

### RECONNAISSANCE(KEŞİF)

Saldırgan, hedef sistem hakkında bilgi toplar. Bu aşamanın amacı sisteme sızma yöntemini belirlemektir. Saldırgan, oturum açma kimlik bilgilerini toplayabilir veya e-posta adresleri, kullanıcı kimlikleri, fiziksel konumlar, yazılım uygulamaları ve işletim sistemi ayrıntıları gibi diğer bilgileri toplayabilir; bunların hepsi kimlik avı veya kimlik sahtekarlığı saldırılarında yararlı olabilir. Bu süreç, saldırganın hedef sistemdeki güvenlik zayıflıklarını istismar etme stratejilerini belirlemesini sağlar. Keşif aşamasında kullanılan iki ana yöntem bulunmaktadır: Aktif ve pasif keşif.

### AKTİF KEŞİF:

Aktif keşifle,bilgisayar korsanları doğrudan bilgisayar sistemiyle etkileşime girer ve otomatik tarama veya manuel test gibi teknikler kullanılarak bilgi toplamaya çalışır.

### PASİF KEŞİF:

Pasif keşif, hedefle doğrudan temas olmadan, herkese açık bilgilerin taranmasıyla gerçekleşen, iz bırakmayan bir bilgi toplama sürecidir.

### WEAPONIZATION(SİLAHLANDIRMA)

Keşif sırasında elde edilen bilgiler kullanılarak hedef alınan organizasyonun zayıflıklarından en iyi şekilde yararlanmak için kötü amaçlı yazılımlar oluşturulur. Bu aşama sırasında saldırgan, orijinal giriş noktası ağ yöneticileri tarafından tanımlanıp kapatılırsa sisteme erişmeye devam edebilmek için arka kapılar da kurabilir. Saldırganın saldırıdan önce son hazırlıklarını tamamladığı aşamadır.

### DELIVERY(TESLİMAT)

Hazırlanan zararlının belirlenen yöntemle hedefe iletilmesi bu aşamadadır. İletim; e-posta, kötü amaçlı bağlantılar veya güvenlik açıklarından yararlanma yoluyla gerçekleştirilir. Aynı zamanda, saldırgan açısından riskli bir aşamadır çünkü iz bırakma riski taşır.

### EXPLOITATION(İSTİSMAR)

Oluşturulan zararlı ve belirlenen atak vektörünü kullanarak hedefin zafiyetinin sömürüldüğü aşamadır. Exploit hazırlanıp hedefe iletildikten sonra bu aşamada zararlı kod çalıştırılır. Düzenli güvenlik açığı değerlendirmeleri ve zamanında yama yönetimi istismarı önleyebilir.

### INSTALLATION(KURULUM)

Hedefin sömürülmesi ardından, kalıcı bir tehdit haline gelmek, güvenlik sisteminin ötesinde sistem başarılı bir şekilde kontrol edilebilmesi için hedefe asıl zararlı yazılımın indirilmesi, zararlı yazılımın sistemde kalacağı süreyi mümkün olduğunca arttırmayı hedefleyen aşamadır. Bu evrede, saldırgan

başarılı bir şekilde sistemi kontrol etme yeteneğine sahip olur ve istediği aktiviteleri gerçekleştirmek için gerekli olan kontrolü elinde bulundurur.

**COMMAND AND CONTROL(KOMUTA VE KONTROL)**

Sisteme yerleşmiş olan zararlının çalışması uzaktan kontrol edilebildiği ve sistemin ele geçirildiği aşamadır. Saldırgan, hedef sistemi uzaktan kontrol etmek için komuta ve kontrol kanallarını oluşturup hedef sistemle kontrol sunucusu arasında iletişim sağlar.

**ACTIONS ON OBJECTIVES(HEDEFLERDEKİ EYLEMLER)**

Bu aşama saldırganın eyleme geçtiği aşamadır. Bütün aşamaları gerçekleştiren saldırgan kuruma erişim sağlamıştır ve bu aşamada, veri çalma, veri değiştirme , veri silme , veri şifreleme, sisteme zarar verme gibi eylemleri gerçekleştirebilir. Sonunda saldırgan hedeflerine ulaşır.

Bu 7 aşama bir zincir gibi birbirine bağlıdır. Her aşamadaki başarı bir sonraki aşamayı etkileyecektir**.**

# SONUÇ

Cyber Kill Chain modeli, saldırıların her aşamasını ayrıntılı bir şekilde analiz etmeye ve saldırılara proaktif olarak yanıt vermeye yardımcı olan güçlü bir çerçeve sunmaktadır.

Bu raporda, Cyber Kill Chain'in temel aşamaları incelenmiş ve açıklanmıştır. Siber tehditlerle mücadelede Cyber Kill Chain gibi sistematik yaklaşımlar benimseyerek organizasyonların daha güvenli bir dijital altyapı oluşturması mümkündür.

Sonuç olarak Cyber Kill Chain, yalnızca saldırıları analiz etmek için değil, aynı zamanda organizasyonların siber güvenlik stratejilerini daha güçlü hale getirmek için de kritik bir araçtır. SOC ekipleri bu modeli kullanarak erken aşamada tehditleri tespit edebilir, saldırıları önleyebilir ve olay müdahale süreçlerini iyileştirebilir.

# KAYNAKÇA


https://berqnet.com/blog/cyber-kill-chain

https://cyberartspro.com/en/cyber-kill-chain-nedir/

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://medium.com/@felixmomodebe/understanding-the-cyber-kill-chain-a-brief-overview-7e46774c35b3

https://burak-vural.medium.com/a-strategic-analysis-tool-what-is-cyber-kill-chain-944190d88bea

https://anticitizenone.medium.com/the-cyber-kill-chain-984358c79628

https://medium.com/@princep49036142/cyber-kill-chain-a-tryhackme-room-write-up-21d850b30b9c