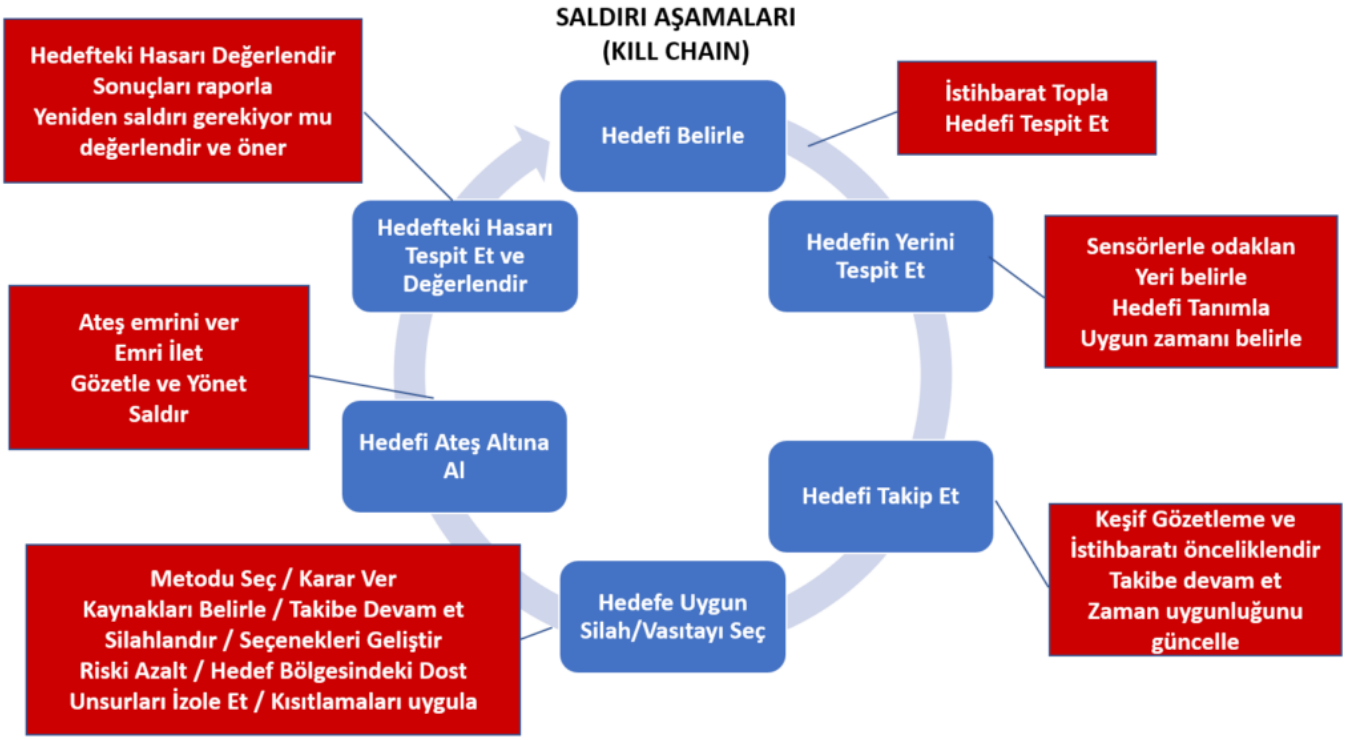
"Cyber Kill Chain" modellemesi ifadesi, önceden beri kullanılan ve "Kill Chain (Ölüm Zinciri-Saldırı Aşamaları) olarak bilinen askerî konseptin siber güvenlik alanına yansıtılmasıyla elde edilmiştir. "Siber Saldırı Aşamaları"na geçmeden, konuyu daha iyi anlayabilmek ve askerî konseptlerin ticari firmaları nasıl yönlendirdiğine dair bir örnek olması bakımından, önce bu Ölüm Zinciri-Kill Chain konseptinden kısaca bahsedelim. *Serdar Gülsoy*



Ölüm Zinciri (Saldırı Aşamaları) – "Kill Chain" Nedir?[1]

Serdar Gülsoy

"Kill Chain" ölüm zinciri ya da "saldırı aşamaları" olarak tanımlanabilecek bir askerî

konsepttir. Bu tanımlama ile bir saldırının yapısı ve aşamaları anlatılmaya çalışılmıştır.

Bir saldırının aşamaları olarak;
– Hedefin belirlenmesi / tanımlanması
– Hedefe kuvvet sevkiyatı
– Hedefe saldırının başlatılması
– Hedefin imhası, safhaları düşünülmüştür.

Bu saldırı aşamaları değişik modellemeler ile geliştirilmiştir. Örneğin, çokça bilinen ve maddelerin baş harflerinin akrostişi ile kısaltılan **"F2T2EA Modeli"** şöyledir;

Find : Hedefi ne olduğunu keşif gözetleme ve istihbarat ile belirle.
Fix : Hedefin yerini / koordinatlarını belirle.
Track : Hedefin hareketlerini takip et.
Target : Hedefin üzerinde oluşturmak istediğin etkiye uygun nitelikteki silah/vasıtayı belirle.
Engage : Silahı hedef üzerinde kullan.
Assess : Hedefte oluşan hasarı istihbarat vasıtalarınla tespit et ve değerlendir.

Bu modelleme, bir zincir bütünü olarak tanımlanmaktadır. Çünkü safhaların herhangi bir aşamasındaki bir halkanın gerçekleştirilememesi bütün işlemi sonlandırmak için yeterlidir.

SİBER SALDIRI AŞAMALARI (SİBER ÖLÜM ZİNCİRİ) – "CYBER KILL CHAIN"

F-16', F-35'ten C-130 uçaklarına, Sikorsky Black Hawk, Apache Helikopterlerinden ANTPQ radarlarına kadar, her türlü kara/hava/deniz silah yelpazesinde ürünü bulunan, ABD merkezli, Lockheed Martin (LM) Şirketi, gelişen bunca teknoloji ve yazılımın korunması maksadıyla, 2011 yılında, bilgisayar ağlarını savunmak için yeni bir "saldırı/öldürme zinciri-Kill Chain" çerçevesi veya modeli tanımladı.

LM bilgisayar bilimcileri, siber savunmanın sağlıklı olarak gerçekleştirilebilmesi için öncelikle saldırganın taktik ve tekniklerini ve uyguladığı yöntemleri tanımlamayı ve safhalandırmayı düşündüler. Bilgisayar bilimcileri bu saldırıların aşamalar halinde gerçekleşebileceğini ve her aşamada kurulan kontroller aracılığıyla bu saldırıların engellenebileceğini yazdılar. **2011 yılından beri, siber saldırıların aşamalarını tanımlamak için, "Siber Saldırı/öldürme Zinciri – Cyber Kill Chain" bilgi güvenliği firmaları ve organizasyonları tarafından benimsenmiştir.**

Peki bu aşamalar nelerdir?[2]

1. **Keşif :** Saldırgan, hedefi seçer, hedefin özelliklerini araştırır ve hedefin bilgi ağı içindeki zafiyetlerini bulmaya çalışır. Yani, sessizce **hedef hakkında bilgi toplar.**
2. **Silahlandırma:** Saldırgan, bir veya daha fazla güvenlik açığına göre uyarlanmış, virüs veya solucan gibi uzaktan erişim amaçlı zararlı yazılım/silahını oluşturur. Yani kurbana **ulaştıracağı silahı/yükü hazırlar.**
3. **Ulaştırma (İletim):** Saldırgan, e-posta ekleri, web sitesi linkleri, harici disk (usb) gibi iletim vasıtalarıyla, silahı/zararlı yazılımı hedefe iletir. Yani, **hazırladığı yükü/silahı kurbana gönderir.**
4. **İstismar (Sömürme):** Kötü amaçlı yazılım/silahın program kodu hedef sistemi içinde tetiklenir ve bu kodlar güvenlik açığından yararlanmak için hedef ağ üzerinde işlem yapar. Yani, gönderilen yük kurbanın network-ağına dahil olur.
5. **Yükleme:** Zararlı yazılım/silah, ağ içerisinde, saldırgan tarafından kullanılabilen ve "arka kapı" denen bir erişim noktası oluşturur. Yani, kurbanın bilgi ağlarında tutunma noktaları inşa eder.
6. **Komuta ve Kontrol:** Zararlı yazılım, saldırganın hedef ağ içerisinde kalıcı erişime sahip olmasını sağlar. Yani, saldırgan kurbanın ağlarında uzaktan kontrol etme erişimine sahip olur.
7. **İcra (eylem):** Saldırgan, veri hırsızlığı, veri imhası ya da fidye talebi için dosyaların kilitlenmesi gibi hedeflerine ulaşmak için harekete geçer. Yani, kurbanın ağındaki verileri çalmak için icraya başlar.

Cyber Kill Chain önemli bir modelleme sunarken bazı eleştirilerle de karşılaşmıştır. Bu modellemedeki en önemli açık, birinci safhadaki (keşif) olayların savunulan ağın dışında gerçekleştiriliyor olmasıdır.**[3]**

Bir diğer eleştiri de geleneksel siber öldürme zincirinin, içeriden gelen tehdidi (insider threat) modellemek için uygun olmadığı yönündedir. Yani tehdit, şirket/organizasyon içinden gelirse, bu saldırı aşamalarının tanımlanması yetersiz kalmaktadır.

Cyber Kill Chain modellemesi yukarıda sunulan saldırganın saldırı aşamalarına karşılık olarak karşı savunma maksadıyla şu hareketleri önermektedir:

1. **Algıla**: Sisteminizde bir saldırgan olup olmadığını belirleyin. Bunun için geliştirilmiş anti-virüs sitemleri denilen EDR (Endpoint Detection and Response – Son Kullanıcı Tespit ve Yanıtlama) çözümleri ve SIEM (Security Information and Event Management – Güvenlik Bilgileri ve Olay Yönetimi) yönetimi kullanılmaktadır.

2. **Reddet:** Bilginin açığa çıkmasını ve sisteminize yetkisiz erişimleri önleyin.
3. **Saldırıyı Boz:** Sistemden dışarı (saldırgana) giden trafiği durdurun veya değiştirin.
4. **Tehdidin seviyesini düşür:** Komuta ve kontrol ile karşı atak (karşı taarruz) yapın.
5. **Aldatma sağla**: Komuta ve kontrol ile müdahale edin.
6. **Muhafazaya al**: Ağ bölümlerinde etkilenmeyi azaltmak için değişiklikler yapın.

Lockheed Martin'in siber saldırılara yönelik saldırıyı anlamak ve kötü maksatlı kişi/grupların taktiklerini modellemek için geliştirdiği Siber Saldırı Aşamaları-Cyber Kill Chain modelinden sonra, diğer büyük bilgi güvenliği firmaları da bu modele yöneltilen eleştirileri de göz önüne alarak, daha kapsamlı modelleri geliştirmiştir. Bunlardan en önemlilerinden biri MITRE ATT&CK diye bilinen modellemedir.

Bir sonraki yazıda MITRE ATT&CK'i inceleyelim mi?

Çizgi Ötesi'ni izlemeye devam edin.

[1] https://www.jcs.mil/Portals/36/Documents/Doctrine/training/jts/jts_studentguide.pdf?ver=2017-12-29-171316-067

[2] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

[3] https://en.wikipedia.org/wiki/Kill_chain