Cyber Kill Chain

Hazırlayan: Saliha Polat

Tarih: 07.02.2025

İçindekiler

Kapak Sayfası **1**
İçindekiler **2**
Giriş **3**
Cyber Kill Chain Nedir? **4**
Cyber Kill Chain Aşamaları ve Saldırgan - Savunmacı Hareketleri **4**
Cyber Kill Chain' den Yararlanma **12**
Cyber Kill Chain – Mitre Attack **13**
Sonuç **14**
Kaynakça **15**

Giriş

Siber güvenlik alanında tehditleri anlamak ve savunma stratejileri geliştirmek amacıyla çeşitli modeller kullanılmaktadır. Kurumlar ve bireyler, siber saldırılara karşı daha güçlü önlemler almak zorunda kalırken, güvenlik uzmanları da tehditleri tespit edebilmek ve saldırıları önleyebilmek adına çeşitli yöntemler geliştirmektedir. Cyber Kill Chain modeli, bu çerçevede saldırı süreçlerini daha iyi analiz etmek ve etkili savunma stratejileri oluşturmak için kullanılan yaklaşımlardan biridir. Lockheed Martin tarafından geliştirilen bu model, bir siber saldırının nasıl gerçekleştiğini aşamalar hâlinde açıklayarak saldırganların izlediği yolu sistematik bir şekilde inceleme imkânı sunmaktadır.

Bu bağlamda, Cyber Kill Chain, sadece saldırı sürecini anlamakla kalmayıp, aynı zamanda güvenlik ekiplerine proaktif savunma mekanizmaları geliştirme konusunda yol gösterici olmaktadır. Modelin her bir aşaması, saldırganların hangi adımları takip ettiğini belirlemeye ve uygun karşı önlemleri zamanında almaya yardımcı olmaktadır. Bu çalışmada, Cyber Kill Chain'in temel yapısı, saldırı sürecindeki aşamaları, saldırgan ve savunmacı perspektifinden değerlendirilmesi, modelin MITRE ATT&CK ile olan ilişkisi ve tehdit istihbaratı kapsamında nasıl kullanılabileceği ele alınmaktadır.

Cyber Kill Chain Nedir?

Siber güvenlik dünyasında “Cyber Kill Chain” terimi, bir saldırının aşamalarını ve her aşamada ne yapılabileceğini anlamak için kullanılan bir modeldir. Cyber Kill Chain, Türkçesi “Siber Ölüm Zinciri” anlamına gelir ve başlangıçta askeri alanda geliştirilmiştir. Lockheed Martin tarafından geliştirilmiş olan bu model, saldırganların bir siber saldırı gerçekleştirmek için takip ettiği adımları sistematik bir şekilde tanımlar. Cyber Kill Chain, savunma stratejilerinin geliştirilmesi ve saldırıların önlenmesi için kritik bir çerçeve sağlar.

Cyber Kill Chain’in mantığı, saldırganların her aşamada belirli adımları izleyerek bir saldırıyı gerçekleştirdiklerini varsayar. Bu model, savunucuların saldırının hangi aşamasında olduklarını anlamalarına ve saldırıyı durdurmak için gerekli önlemleri almalarına yardımcı olur. Cyber Kill Chain modeli, siber saldırılara karşı bütüncül bir savunma stratejisi geliştirilmesini sağlar. Her aşama, saldırının durdurulabileceği bir fırsat penceresi sunar. Bu, savunucuların saldırıyı erken aşamalarda tespit edip durdurmasına olanak tanır. Cyber Kill Chain, saldırganların belirli bir düzende hareket ettiğini varsayar. Bu düzen, keşif aşamasından hedeflere ulaşma aşamasına kadar sistematik bir şekilde ilerler. Her aşamanın belirli zayıflıkları ve savunma stratejileri vardır.

Cyber Kill Chain Aşamaları ve Saldırgan – Savunmacı Hareketleri

1)Resconnaissance (Keşif)

Siber Öldürme Zinciri'nin ilk adımıdır ve saldırganın hedef sistemde bilgi toplama sürecini ifade eder. Bu aşamanın temel hedefi, sisteme sızma yöntemlerini tespit etmek ve potansiyel güvenlik açıklarını araştırmaktır. Saldırgan, hedefin IP adresleri, çalışan bilgileri ve kullanılan güvenlik sistemlerini belirleyerek anahtar bilgileri toplar. Keşif aşaması, herhangi bir sızma testi yapılmadan önce potansiyel hedeflerin belirlenmesi, zayıf noktaların tespiti, üçüncü tarafların bağlantıları ve erişebilecekleri verilerin keşfi ile karakterizedir. Bu süreç, saldırganın hedef sistemdeki güvenlik zayıflıklarını istismar etme stratejilerini belirlemesini sağlar. Keşif aşamasında kullanılan iki ana yöntem bulunmaktadır:

Aktif Bilgi Toplama: Bilgisayar korsanları doğrudan bilgisayar sistemiyle etkileşime girer ve otomatik tarama veya manuel test gibi teknikler ve ping ve netcat gibi araçlar aracılığıyla bilgi elde etmeye çalışır. Aktif keşif genellikle daha hızlı ve daha doğrudur ancak daha risklidir çünkü sistem içinde daha fazla gürültü yaratır ve tespit edilme şansı daha yüksektir

Pasif Bilgi Toplama: Hedef ile doğrudan temas olmadan, herkese açık bilgilerin taranmasıyla gerçekleşen, iz bırakmayan bir bilgi toplama sürecidir. İnternetin imkânlarıyla gerçekleştirilen bu süreç, Wireshark, Shodan gibi araçlar ve işletim sistemi parmak izi gibi yöntemlerle sistemlere doğrudan etkileşimde bulunmadan bilgi elde eder.

Saldırgan ve Savunmacı Gözünden Resconnaissance (Keşif) Aşaması

Saldırgan

Saldırgan, "Keşif" süreci sırasında çeşitli yaklaşımlar kullanarak çeşitli kaynaklardan bilgi toplayabilir. Bu aşamada saldırgan aşağıdaki işlemleri gerçekleştirilebilir:

- Hedefe ait sunucuların ve yazılımların sürüm bilgilerinin alınması.
- Hedef hakkında açık kaynaklardan bilgi edinilmesi daha önce serbest bırakılması.
- Kurum çalışanlarının e-posta adreslerinin alınması.
- Sosyal paylaşım platformlarını kullanarak kurum çalışanlarına ait dahili veya kişisel bilgilerin elde edilmesi.
- İnternete bağlı cihazların tespiti.
- İnternet üzerinden erişime açık sunuculardaki güvenlik açıklarının tespiti.
- Kuruluşa ait IP adres bloğunun belirlenmesi.
- Kuruluşun iş birliği yaptığı tedarikçilerin belirlenmesi.

Savunmacı

Blueteam'ler bu aşamada saldırganların girişimlerine yanıt olarak harekete geçebilir. Bu, bir saldırganın elde edebileceği bilgi miktarının azaltır. SOC analistlerinin ve blueteam'lerin uygulayabileceği bazı yöntemler aşağıda listelenmiştir:

- Harici pentest ile bilgi ifşa alanlarının tespiti.
- Tehdit İstihbarat kaynaklarından kuruluş hakkında sızıntı bilgilerinin elde edilmesi.
- Örgütsel bilgi sağlayan belgeleri internette güvenlik duvarı gibi güvenlik çözümleri kurarak trafiğin izlenmesi.
- Yeni güvenlik açıklarının istismar edilmesini önlemek için anında güncelleme.

2)Weaponization (Silahlanma)

Saldırganın keşif aşamasında edindiği bilgilerle sistemdeki potansiyel giriş noktalarını belirlediği ve bu noktalara özel kötü amaçlı yazılımları hazırladığı kritik bir evredir. Bu aşamada, saldırgan saldırı öncesi son hazırlıklarını tamamlar ve siber saldırı için özel bir vektör oluşturur. Bu vektör, uzaktan erişime yönelik kötü amaçlı yazılımları, fidye yazılımlarını veya keşif aşamasında belirlenen güvenlik açıklarından yararlanabilecek virüs veya solucanları içerebilir. Bu süreç, saldırganın saldırısını daha etkili ve hassas hale getirmek için gerekli olan teknik ve taktik planlamayı içerir.,

· **Exploit:** Yazılımların veya bilgisayar sistemlerinin içinde bulunan güvenlik açıklarından faydalanmak için özel olarak tasarlanmış kodları ifade eder**.**

· **Malware:** Bilgisayar sistemlerine zarar veren kötü niyetli yazılımları ifade eder. Genel amacı, zarara yol açmak veya çalışmalarını aksatmaktır.

Saldırgan ve Savunmacı Gözünden Weaponization (Silahlanma) Aşaması

Saldırgan

Saldırgan, “Silahlandırma” süreci sırasında birçok alternatif saldırı tekniği geliştirebilir veya siber saldırı için gerekli bileşenleri hazırlayabilir. Saldırganın bu aşamada kullanabileceği süreçlerden bazıları şunlardır:

- Kötü amaçlı yazılım oluşturma.
- Exploit’leri geliştirmek.
- Kimlik avı girişiminde kullanılmak üzere kötü amaçlı içerik oluşturma (örneğin, bir e-posta şablonu ve kötü amaçlı bir belge).
- Siber saldırı için en iyi aracın belirlenmesi.

Savunmacı

SOC analistlerinin ve Blueteam’lerin saldırganların saldırı hazırlıklarının şu aşamada doğrudan engellenmesi mümkün değildir. Ancak, sınırlı da olsa bazı önlemler alınabilir. Bu önlemlerden bazıları şunlardır:

- Sistemlerin düzenli olarak kontrol edilerek herhangi bir güvenlik açığının tespit edilip edilmediği kontrol edilir.
- Kurumların sistemlerine güvenlik güncellemelerinin en kısa sürede yüklenmesi.

- Bilinen veya yeni üretilen siber saldırı araçlarının sistemler üzerindeki etkisinin, bilinen veya yeni geliştirilen saldırı izlenmesi ve dolayısıyla aracın ne zaman kullanıldığının tespit edilebilmesi yoluyla analiz edilmesi.

3)Delivery (Teslimat)

İletme ve iletim aşaması, saldırganın hazırladığı zararlı yazılımları hedefe ulaştırmaya yönelik kritik bir süreçtir. Bu aşamada, saldırgan çeşitli yöntemler kullanarak zararlı yazılımları iletmeye çalışır. Örneğin, bir USB aracılığıyla bulaştırma veya oltalama (phishing) gibi sosyal mühendislik taktikleriyle kullanıcıyı yanıltma yöntemleri bu aşamada sıklıkla kullanılır. USB aracılığıyla bulaştırma, fiziksel erişim gerektirebilirken, oltalama e-posta yoluyla veya sahte web siteleri aracılığıyla gerçekleştirilebilir. Bu süreç, savunma ekipleri için izleme ve müdahale fırsatları sağlar. Aynı zamanda, saldırgan açısından riskli bir aşamadır çünkü gerekli anonimliği sağlayamazsa iz bırakma riski taşır.

Saldırgan ve Savunmacı Gözünden Delivery (Teslimat) Aşaması

Saldırgan

"Teslimat" aşamasında, saldırgan çeşitli yöntemlerle kurbana çeşitli siber silahlar teslim edebilir. Bu aşamada, saldırgan aşağıdaki işlemleri gerçekleştirebilir:

- Kötü amaçlı bir URL'yi e-posta yoluyla iletmek.
- Kötü amaçlı yazılımı e-posta yoluyla dosya eki olarak iletme.
- Web sitesi aracılığıyla köyü amaçlı yazılım dağıtımı.
- Kötü amaçlı URL'yi sosyal medya aracılığıyla iletmek.
- Sosyal medya aracılığıyla kötü amaçlı yazılım dağıtımı.
- Kötü amaçlı yazılımı doğrudan hedef sunucuya yükleme (Eğer sunucuya doğrudan erişim mümkünse).
- Kötü amaçlı yazılımın doğrudan bir USB aygıtı aracılığıyla hedef sisteme fiziksel kurulması veya kurulmasının etkinleştirilmesi.

Savunmacı

Blueteam'ler ve bireysel kullanımlar bu aşamada pek çok önlem alabilirler. Siber saldırının gerçekleşmesini tamamen engellemeseler de bu önlemler başarılı bir siber saldırı riskini önemli ölçüde azaltabilir. Bu dönemlerde bazıları aşağıda listelenmiştir:

- E-posta içeriğindeki URL'lere karşı şüpheci bir tutum benimsemek ve bunları bir de ortamında görüntülemek.
- E-postanın eklerini antivirüs yazılımını kullanarak tarama.
- Kuruluşlarda e-posta güvenlik çözümü ürünlerinin kullanımı.
- Kullanıcıların/kurum çalışanlarının bilgi güvenliği konusunda eğitim almasını sağlamak.

- Sunucu erişiminin sürekli izlenmesi ve günlüklerin kaydedilmesi.
- Güvenlik Duvarı gibi güvenlik çözümlerinin etkin kullanımı ve yönetimi.
- Gerektiğinde şüpheli faaliyetlerin detaylı analizinin yapılması.
- Anormalliklerin tespiti ve başlangıç nedeninin belirlenmesi.

4)Exploitation (Sömürme)

Sömürme aşaması genellikle kullanıcı sistemlerdeki zafiyetin sömürülmesi aşamasıdır. Hedefin ele geçirilebilmesi ve kontrol altına alınabilmesi için zararlı yazılımın sisteme kurulması ve kullanıcı farkında olmadan uzak erişim sağlanması gerekecektir. Bunun olabilmesi için ilgili kullanıcı makinasındaki işletim sisteminde veya uygulamalarda bir zafiyet olması şarttır. İletme aşaması ile bilgisayara indirilen dosya çalıştırıldığında, sistemdeki zafiyet sömürülerek yükleme aşamasının önü açılmış olur.

Saldırgan ve Savunmacı Gözünden Exploitation (Sömürme) Aşaması

Saldırgan

Saldırgan hedefe istismar edilmesi amaçlanan program veya sistem hakkında bazı temel bilgilere sahiptir ve "Sömürü" aşamasında önceden uygun saldırı araçlarını hazırlamıştır. Bu, saldırganın istismarının veya aracının çalıştırıldığı/test edildiği adımdır. Bu adım, istismar veya araç kurbanın sisteminde kullanılmaya uygun değilse başarısız olabilir. Bu seviyede, saldırgan aşağıdaki işlemleri gerçekleştirebilir:

- Donanım güvenlik açığını istismar eden istismarın yürütülmesi.
- Yazılımın veya işletim sisteminin zafiyetinden yararlanan istismarın yürütülmesi.
- Kötü amaçlı yazılım çalıştırılıyor.

Savunmacı

İstismara karşı savunma, Blueteam'ler diğer aşamalara kıyasla önemli ölçüde daha karmaşık ve emek yoğun bir görev teşkil eder. Bunun başlıca nedeni, daha önce görülmemiş kötü amaçlı yazılımlarla ve istismarlarla karşılaşma olasılığıdır ve bu da savunma sürecine bir karmaşıklık katmanı ekler. Açıklamak gerekirse, sıfır günlük istismarların kullanımı bu aşamada tespit ve önleme prosedürlerini karmaşıklaştırabilir. Kötü amaçlı faaliyetleri tespit etmek ve önlemek için aşağıdaki noktalar dikkate alınabilir:

- Sistemlerde yüklenen bir dosyanın ne zaman açılmasının gerekli/gerekmediği ve hangi hususlara dikkat edilmesi gerektiği konusunda kurum çalışanlarına eğitim verilmesi.
- Kuruma ait varlıklar üzerindeki sistem güvenlik operasyonlarının sürekli izlenmesi ve anormalliklerin tespiti.
- Kuruma ait varlıklarda yayımlanan güvenlik açıklarının takibi, uygun izleme kuralının yazılması ve istismar edildiğinde tespit edilemesin.
- Kuruma ait varlıkların güvenlik güncellemelerinin takibi ve anında kurulumu.

- EDR ürünlerini kullanarak uç noktalardaki faaliyetlerin izlenmesi.
- Yerel olarak geliştirilen uygulamalarda güvenlik açıklarını önlemek amacıyla yazılım geliştiricilere güvenli kodlama eğitimi verilmesi.
- Kuruluşun varlıkları üzerinde düzenli olarak pentestler yapılması.
- Düzenli otomatik güvenlik açığı taraması ve raporların izlenmesi.
- Kuruma ait varlıklar üzerindeki yetkilendirmelerin düzenlenmesi ve her hesaba gereken yetkinin verilmesi.

5)Installation (Kurulum)

Hedef sisteme başarılı bir şekilde sömürme işlemi uygulandıktan sonra, saldırgan, zararlı aktivitelerini gerçekleştirmeye başlar. Sistem üzerine başarılı bir şekilde yerleşen saldırgan, gizlenmek için çeşitli teknikleri bu aşamada kullanır ve sistem üzerinde kalıcılığı sağlamak amacıyla farklı yazılımları da yükleyebilir. Bu evrede, saldırgan başarılı bir şekilde sistemi kontrol etme yeteneğine sahip olur ve istediği aktiviteleri gerçekleştirmek için gerekli olan kontrolü elinde bulundurur.

Saldırgan ve Savunmacı Gözünden Installation (Kurulum) Aşaması

Saldırgan

"Kurulum" adımında, bir saldırgan çok çeşitli işlemler gerçekleştirebilir. Saldırgan, istismar ettiği sistemdeki yetkisiyle sınırlı olduğu sürece çeşitli teknolojik faaliyetleri başarıyla gerçekleştirebilir. Saldırgan bu işlemleri gerçekleştirirken, sistemde mümkün olduğunca az iz bırakmaya ve güvenlik ürünlerinin işlemlere müdahale etmemesini sağlamaya çalışır. Bu şekilde, saldırgan sistemde daha uzun süre tespit edilmeden kalabilir ve saldırıyı gerçekleştirmek için gereken zamanı kazanabilir. Bu aşamada, saldırgan aşağıdaki eylemleri gerçekleştirebilir:

- Kurbanın cihazına kötü amaçlı yazılım yükleyin.
- Kurbanın sistemine Backdoor (Arka Kapı) yerleştirmek.
- Web sunucusuna (eğer web sunucu ise) web kabuğunu yükleyin.
- Mağdur cihazın kalıcılığını sağlamak için bir hizmet, güvenlik duvarı kuralı veya zamanlanmış görev ekleme.

Savunmacı

Blueteams'in bu aşamada saldırganlara uyguladığı operasyonlar Threat Hunting operasyonlarından oluşmaktadır. Bu aşamaya ulaşan bir saldırgan sistemlerde kötü amaçlı faaliyetlerde bulunması, saldırganın tespit edilmeyeceğini gösterir. Bu nedenle saldırganın mevcut olup olmamasına bakılmaksızın SOC ekibi, sistemde her zaman bir saldırganın mevcut olduğu varsayımıyla güvenlik operasyonlarını yönetmeli ve yürütmelidir. Bu seviyede gerçekleştirilebilecek güvelik operasyonları mevcut yapıya bağlı olacaktır. Genel olarak gerçekleştirilebilecek bazı aktiviteler şunlardır:

- Kuruluşun tüm varlıklarında Ağ Güvenliği İzleme işlemlerini yürütmek.
- Her uç noktada uygulanan yapılandırma değişikliklerinden haberdar olmak için EDR güvenlik çözümlerini kullanma.
- Sistemlerdeki kritik dosyalara erişimi kısıtlama ve erişimi izleme.
- Sistemlerdeki kullanıcılar için yetkilendirme düzenlemeleri yapılarak yönetici ayrıcalıklarının sadece zorunlu durumlarda kullanılmasına izin verilmesi.
- Sistemlerde çalışan süreçleri izleyerek kötü amaçlı süreç etkinliklerini tespit etmek.
- Sistemde yalnızca geçerli imzaya sahip yürütülebilir dosyaların çalıştırılmasına izin veriliyor.
- İzlenen tüm sistem faaliyetlerindeki anormallikleri tespit edin ve temel nedeni bulun.

6)Command and Control, c2 (Komuta ve Kontrol)

Uzaktan gerçekleştirilen siber saldırıların önemli bir kısmı Komuta Kontrol (C&C) sistemine dayanmaktadır. C&C sistemi, ele geçirilen makineler üzerinde uzaktan gizli talimatlar vermek için kullanılır ve aynı zamanda tüm verilerin dışarı çıkarılacağı bir yer olarak görev yapar. Bu kanalların mimarisi, yıllar geçtikçe savunma mekanizmalarının gelişmesiyle birlikte evrim geçirmiştir, özellikle antivirüsler, güvenlik duvarları, IDS'ler gibi önlemlerle karşılaşmaktadır.

Temelde üç tür C&C iletişim yapısı bulunmaktadır:

Geleneksel Merkezi Yapı: Geleneksel istemci-sunucu ilişkisine çok benzer şekilde çalışmaktadır. Sadece bir sunucu olduğu için yönetimi kolayca yapılabilmektedir. Ayrıca komuta kontrol sinyallerini iletmek için virüslü makinelere bağımlılık bulunmamaktadır. Bu nedenle, rastgele virüs bulaşmış makinelerin arızalanması C2 mimarisini etkilememektedir. Genel bulut hizmetleri ve içerik dağıtım ağları (content delivery network veya CDN), C2 etkinliğini barındırmak veya maskelemek için sıklıkla kullanılmaktadır. Bilgisayar korsanlarının meşru web sitelerini tehlikeye atarak, sahiplerinin bilgisi olmadan komuta ve kontrol sunucularını barındırmak için kullanması, yaygın bir yöntem olarak bilinmektedir [6].

Merkezi Olmayan Yapı: P2P, yani "peer-to-peer" olarak da adlandırılan, Komuta ve Kontrol (C&C) modelinde kullanılan bir yapıdır. Bu modelde, botnet üyeleri arasında merkezi olmayan bir iletişim sağlanır ve komuta ve kontrol talimatları birbirleri arasında doğrudan iletilir. Bazı botlar hala sunucu olarak işlev görebilir, ancak merkezi veya "ana" bir düğüm bulunmaz. Bu, merkezi bir modele kıyasla kesintiyi zorlaştırır, ancak aynı zamanda saldırganın botnet'in tamamına talimat vermesini de karmaşık hale getirir. P2P ağları, birincil C2 kanalının kesildiği durumlarda geri dönüş mekanizması olarak kullanılabilir

Sosyal Ağ Tabanlı Yapılar: Saldırganlar, nadiren engellendikleri için geleneksel olmayan C2 platformları olarak sosyal medya platformlarını da kapsamlı bir şekilde kullanmaktadırlar. Saldırganlar güvenliği ihlal edilmiş ana bilgisayarlara C2 mesajları göndermek için, Gmail, IRC (İnternet Aktarmalı Sohbet) sohbet odaları gibi sistemleri kullandıkları da bilinmektedir. Saldırganlar, kanal algılamayı ve engellemeyi daha zor hale getirebilmek için normal trafik modellerini taklit eden gizli iletişim mekanizmalarını da kullanmaktadırlar. Örneğin; C2 trafiği, çevrimiçi sosyal ağlar (OSN'ler), gizli DNS trafikleri ve tor gibi anonim iletişim ağlarında bulunan sayfalar ve resimler aracılığıyla da gerçekleşebilmektedir.

Saldırgan ve Savunmacı Gözünden Command and Control (Komuta ve Kontrol) Aşaması

Saldırgan

"Komuta ve Kontrol (C2)" aşamasında, saldırganın yaptığı şey C2 ile hedef sistem arasındaki iletişim kurmaktır. Bu aşama, saldırganın hedeflediği eylemlerin yürütülmesini içermez. C2 iletişimi tamamlandıktan sonra, saldırgan kötü amaçlı faaliyetler yürütmeye devam edecektir.

Saldırganın bu aşamada yaptığı işlemleri kısaca şöyle özetleyebiliriz:

- C2 Server'ın kurbanla iletişim kurması için yapılandırması.
- Mağdurun cihazında C2 ile temasını mümkün kılmak için gerekli işlemlerin uygulanması.

Savunmacı

Bu aşamada mavi takımlar için belirli bir eylem olmasa da C2 iletişimi bağlamında genel güvenlik izleme ve tespit teknikleri ve uygulamaları dikkate alınmalıdır. Mavi takımlar, olası C2 ağ trafiği akışını tanımak ve önlemek için uygun adımları atmalıdır. Atılması gereken bazı adımlar şunlardır:

- Bilinen C2 araçlarının sistemlerde mevcut olup olmadığını belirlemek için.
- Güvenlik Duvarı gibi güvenlik ürünleri aracılığıyla C2 sunucu IP adreslerinin Siber Tehdit İstihbarat kaynaklarından engellenmesi.
- Sistemde Ağ Güvenlik İzleme ile C2 iletişimi olabilecek ağ trafiğini tespit etmek.

7)Actions On Objectives (Hedeflere Yönelik Eylemler)

Bu aşama saldırganın eyleme geçtiği aşamadır. Sistemi ele geçiren saldırgan amacına ulaşmak için çeşitli eylemleri gerçekleştirir. Bu aşamadaki genel amaç, olabildiğince fazla sisteme yayılıp saldırganlar için değerli olan bilgileri ele geçirmektir. Veri çalma, değiştirme ve silme gibi eylemler örnek gösterilebilir. Saldırganlar bu aşamada, izlerini kaybettirmeye çalışır. Bunun örneklerinden biri de ele geçirilen sistemlerin bilinçli olarak bozulması veya hizmet kesintisi yaşatacak saldırılarla hedef şaşırtılmasıdır.

Saldırgan ve Savunmacı Gözünden Actions On Objectives (Hedeflere Yönelik Eylemler) Aşaması

Saldırgan

Saldırganlar bu seviyeye ulaştığında hedeflenen hareketleri farklılaşabilir. Bu aşamada saldırganların eylemleri amaçları ve motivasyonları tarafından belirlenir. Saldırganın birincil amacı sisteme zarar vermekse, örneğin kritik bilgileri silebilir. Saldırganın bu aşamada gerçekleştirebileceği adımlardan bazıları şunlardır:

- Fidye yazılımı yardımıyla sistemdeki dosyaları şifrelemek.
- Sistem içindeki kritik bilgileri/belgeleri sızdırmak.
- Sistemdeki kritik bilgilerin silinmesiyle sisteme zarar verilmesi.

- Yetki yükseltme işlemleri ile daha yetkili işlemleri uygulayabilmek ve ağdaki diğer makinelere erişim sağlayarak siber saldırının kapsamını genişletebilmek.
- Ağdaki başka bir cihaza erişim sağlamak için kullanıcı kimlik bilgilerinin toplanması.
- Sistem içerisinde bilgi toplanması.
- Sistemdeki bilgilerin değiştirilmesi veya manipüle edilmesi.

Savunmacı

Bu aşamada, mavi takımların saldırgan aktivitesini tespit etmek ve durdurmak için her bir belirli işleme göre farklı eylemler gerçekleştirmesi gerekebilir. Öncelikle sistem düzenli olarak izlenmelidir. Bu şekilde sistemde kötü amaçlı aktivite tespit etmek mümkün olabilir. Tespit aşamasından sonra, tespit edilen eylemin ardından uygun eylem uygulanmalıdır. SOC ekiplerinin alabileceği en temel önlemlerden biri, saldırganların verileri kuruluştan dışarı sızdırmasını önlemektir. Çünkü veri sızıntısı günümüzde en yaygın siber saldırı sonuçlarından biridir. Bu aşamada alınması gereken bazı önlemler şunlardır:

- Ağ trafiğindeki anormallikleri tespit etme.
- Dışarıya ağ erişimini kısıtlamak ve sürekli izlemek.
- Kritik bilgiler içeren dosyalara/klasörlere erişimi kısıtlamak ve erişimi düzenli olarak kontrol etmek.
- Kritik bilgilerin yer aldığı veri tabanlarına erişim yetkisinin kısıtlanması ve erişimin sürekli izlenmesi.
- Veri sızıntısını önlemek için DLP ürünlerinin kullanılması.
- Kullanıcıların yetkisiz erişimini tespit etme.

Cyber Kill Chain’ den Yararlanma

Saldırganın hangi aşamada olduğunu bilmek, güvenlik ekiplerinin güvenlik kontrollerini katmanlandırmasına ve olası siber saldırıları önlemesine yardımcı olur. Siber Öldürme Zincirini anlamak ve bu bilgiyi doğru Tehdit İstihbaratı ile güçlendirmek, kuruluşlara güçlü bir tehdit önleme yeteneği kazandırır.

Keşif aşamasında saldırgan araştırma için dışarıdan içeriye bir yaklaşım kullanır ve unuttuğunuz veya farkında olmadığınız varlıkları bulmaya çalışır. Kuruluşların, neyi koruyacaklarını bilmeleri için altyapılarının bütünsel bir görünümünü elde etmeleri gerekir. Ancak bu her zaman yeterli değildir ve Tehdit İstihbaratı tam da burada devreye girer.

Yeni güvenlik açıklarını bilmek önemlidir, çünkü bu şekilde saldırganın neyi hedef alabileceğini bilirsiniz.

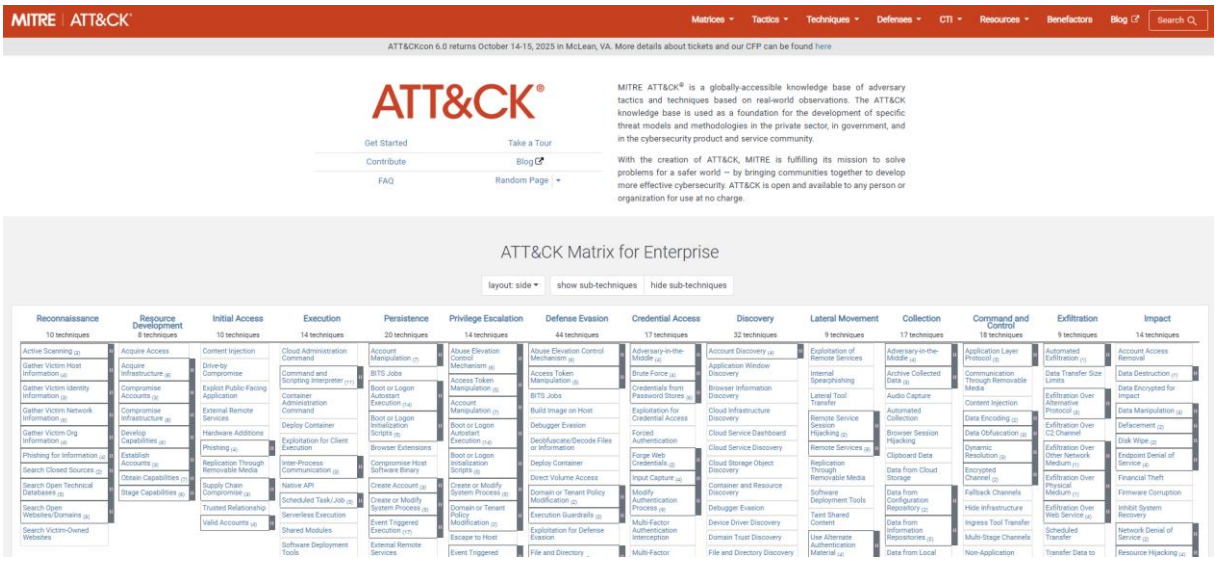
Saldırılar genellikle sisteme erişmek için sıfırıncı gün zafiyetlerini veya birkaç zafiyeti aynı anda kullanır. Ancak her APT grubunun saldırmak için uyguladığı kendi taktikleri, teknikleri ve prosedürleri (TTP'ler) vardır. Farklı APT grupları farklı sektörleri hedefler ve olası saldırganınızı ve onun TTP'lerini bilmek uygun tehdit önleme için önemlidir. APT grupları

sürekli olarak yeni TTP'ler geliştirir, bu nedenle bu değişiklikleri sürekli takip etmek de önemlidir.

Personeli kimlik avı e-postalarına ve kötü amaçlı web sitelerine kurban gitmemeleri konusunda eğitmek, kuruluşu korumanın bir yoludur. Ancak, yeni kayıtlı kimlik avı alan adlarını belirlemek için tehdit istihbaratını kullanmak, izinsiz girişleri önlemenin bir başka yoludur. Güvenlik ekipleri, kimlik avı bilgilerini sisteme gönderebilir ve kuruluşun ağı üzerinden bu alan adlarına erişimi engelleyebilir.

Cyber Kill Chain – Mitre Attack

Siber saldırı zinciri sıklıkla MITRE Corporation'ın bir yaklaşımı olan MITRE ATT&CK çerçevesiyle karşılaştırılır. MITRE ATT&CK benzer şekilde siber saldırının aşamalarını gösterir ve bunların çoğu siber saldırı zinciri modeline benzerdir.



Siber öldürme zinciri ile MITRE ATT&CK arasındaki temel fark, MITRE taktiklerinin belirli bir sıraya göre listelenmemiş olmasıdır; öldürme zincirinin belirli aşama gruplandırması ve doğrusal yapısı buna örnektir.

Bir diğer fark ise, siber öldürme zinciri çerçevesinin siber saldırı sürecini üst düzeyde yedi aşamada ele alması, MITRE ATT&CK'nin ise siber saldırının ayrıntılı ayrıntılarıyla ilgili çeşitli teknik ve prosedürleri araştırmasıdır.

Sonuç

Siber saldırılar, günümüzde giderek artan bir tehdit unsuru hâline gelmiş ve kurumlar için ciddi güvenlik riskleri oluşturmuştur. Bu saldırılara karşı etkili savunma stratejileri geliştirmek, yalnızca saldırılar gerçekleştikten sonra alınan önlemlerle değil, aynı zamanda saldırganların kullandığı yöntemleri önceden tespit edip engellemekle de mümkündür. Bu noktada, Cyber Kill Chain modeli, saldırı süreçlerini belirli aşamalara ayırarak, güvenlik ekiplerinin tehditleri daha erken fark etmesini ve müdahale sürecini daha verimli bir şekilde yönetmesini sağlamaktadır. Modelin sağladığı bu yapı, yalnızca savunma stratejilerinin güçlendirilmesine yardımcı olmakla kalmamakta, aynı zamanda siber tehdit istihbaratının daha etkin bir şekilde kullanılmasına da imkân tanımaktadır.

Özellikle, Cyber Kill Chain'in MITRE ATT&CK gibi saldırgan tekniklerini detaylandıran çerçevelerle birlikte kullanımı, tehdit aktörlerinin taktiklerini daha iyi anlamaya ve savunma süreçlerini buna göre uyarlamaya olanak tanımaktadır. Bu nedenle, kurumların siber güvenlik politikalarını oluştururken bu modeli dikkate almaları, saldırı önleme ve tespit süreçlerini daha etkin hâle getirecektir. Sonuç olarak, siber tehditlerin giderek karmaşıklaştığı günümüz dijital dünyasında, Cyber Kill Chain gibi sistematik modellerin kullanımı, saldırılara karşı daha güçlü ve proaktif bir savunma oluşturmak açısından kritik bir rol oynamaktadır.

Kaynakça

Berqnet. *Cyber kill chain nedir?* Berqnet. https://berqnet.com/blog/cyber-kill-chain

BBS Teknoloji. *Cyber kill chain nedir?* BBS Teknoloji. https://bbsteknoloji.com/cyber-kill-chain-nedir/

CrowdStrike. *Cyber kill chain explained.* CrowdStrike. https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/cyber-kill-chain/

CyberArtsPro. *Cyber kill chain nedir?* CyberArtsPro. https://cyberartspro.com/cyber-kill-chain-nedir/

CyberShield Community. *Cyber kill chain nedir?* CyberShield Community. https://cybershieldcommunity.com/cyber-kill-chain-nedir/

Fordefence. *Cyber kill chain.* Fordefence. https://fordefence.com/cyber-kill-chain/

Proofpoint. *Cyber kill chain.* Proofpoint. https://www.proofpoint.com/us/threat-reference/cyber-kill-chain

ResearchGate. (2015). *Technical aspects of cyber kill chain.* ResearchGate. https://www.researchgate.net/publication/281148852_Technical_Aspects_of_Cyber_Kill_Chain

SecureFors. *Cyber kill chain nedir?* SecureFors. https://www.securefors.com/cyber-kill-chain-nedir/

SOCRadar. *Using cyber kill chain for threat intelligence.* SOCRadar. https://socradar.io/using-cyber-kill-chain-for-threat-intelligence/

Splunk. *Cyber kill chains.* Splunk. https://www.splunk.com/en_us/blog/learn/cyber-kill-chains.html

Varonis. *Cyber kill chain.* Varonis. https://www.varonis.com/blog/cyber-kill-chain

Varonis. *What is C2?* Varonis. https://www.varonis.com/blog/what-is-c2

Zekeriya, S. (2023). *Cyber kill chain nedir?* Medium. https://medium.com/@zekeriyasen412/cyber-kill-chain-nedir-e9a5d89d2b24