ALTAY TAKIMI

CYBER KILL CHAIN RAPORU

HAZIRLAYAN:GÜRKAN PARLAK
7.02.2025

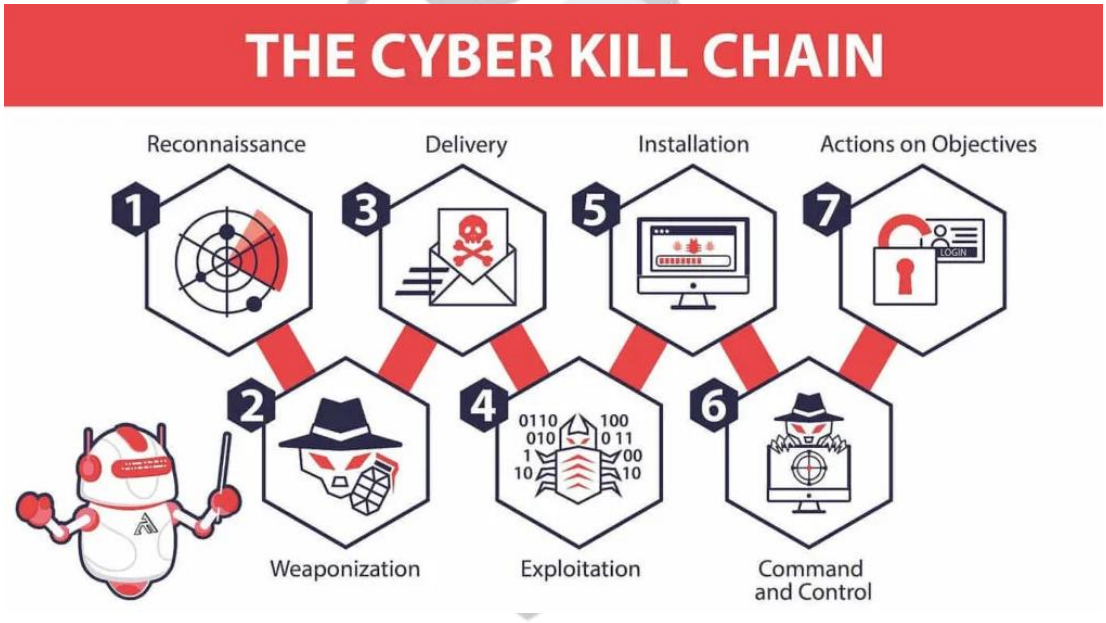
İçindekiler

Cyber Kill Chain

Gelişen teknolojiyle birlikte siber güvenliğin önemi artmış ve dünya genelinde bir ihtiyaç haline gelmiştir. Bu noktada savunma stratejilerine önemli bir katkı sağlayan "Cyber Kill Chain" adlı model ortaya çıkmıştır.

Cyber Kill Chain, Türkçesi "Siber Ölüm Zinciri" anlamına gelir ve başlangıçta askeri alanda geliştirilmiştir. Bu model, saldırganların siber saldırı adımlarının hangi aşamada nasıl engellenebileceği konusunda sistem yöneticilerine önemli bilgiler sağlar. Lockheed Martin şirketi tarafından ortaya konulan bu model, dijital tehditlere karşı etkili bir savunma stratejisi oluşturmak amacıyla kullanılmaktadır. Bu makale, Cyber Kill Chain modelinin yedi aşamasının detaylı bir analizini sunarak, siber güvenlikte etkili bir strateji geliştirmek isteyenlere rehberlik etmeyi amaçlamaktadır.

Bir sistemi savunmanın en etkili yolu, saldırının hangi aşamalardan geçeceğini belirlemektir. Cyber Kill Chain modeli, bu aşamaları anlamak ve bu noktalarda etkili savunma tedbirleri almak için değerli bir çerçeve sunar.



Cyber Kill Chain genellikle şu aşamalardan oluşur:

1.Reconnaissance (Keşif): Saldırgan, hedef sistem veya organizasyon hakkında bilgi toplar. Bu, sosyal mühendislik, ağ taramaları, açık kaynak araştırmaları gibi yöntemlerle yapılır. Amaç, hedefin zayıf noktalarını ve potansiyel giriş noktalarını belirlemektir.

2.Weaponization (Silahlandırma): Saldırgan, hedef sistemi veya ağı hedef almak için gerekli araçları ve teknikleri geliştirir. Bu aşamada, zararlı yazılım (malware) ve çeşitli exploitler hazırlanır.

3.Delivery (Teslimat): Saldırgan, geliştirdiği zararlı yazılımı veya exploit'i hedefe ulaştırır. Bu, e-posta ekleri, sosyal mühendislik saldırıları, kötü amaçlı bağlantılar gibi yöntemlerle yapılabilir.

4.Exploitation (Sömürü): Zararlı yazılım veya exploit, hedef sistemdeki bir zayıflıktan yararlanarak çalıştırılır. Bu aşamada, saldırgan hedef sistem üzerinde yetki kazanır.

5.Installation (Kurulum): Saldırgan, hedef sistemde kalıcı bir varlık oluşturur. Bu, genellikle arka kapı (backdoor) veya başka bir kalıcı zararlı yazılım kurulumunu içerir.

6.Command and Control (C2) (Komut ve Kontrol): Saldırgan, hedef sistemle iletişim kurarak kontrolü sağlar. Bu, genellikle zararlı yazılımın komutları almak ve veri göndermek için kullandığı bir kontrol kanalı oluşturmayı içerir.

7.Actions on Objectives (Hedeflere Yönelik Hareketler): Saldırgan, hedeflerin asıl amacına ulaşır. Bu, veri çalma, sistemi bozma veya diğer zararlı eylemleri içerebilir.

Cyber Kill Chain modelinin amacı, her aşamayı analiz ederek ve savunma stratejileri geliştirerek, bir saldırının başarılı bir şekilde tamamlanmasını engellemektir. Bu model, savunma stratejilerini geliştirmek için saldırganın davranışlarını ve yöntemlerini anlamak açısından faydalıdır.

Cyber Kill Chain Aşamaları

1.Aşama Keşif:

Keşif (Reconnaissance) aşaması, siber saldırıların ilk adımıdır ve saldırganların hedef hakkında bilgi toplamak için kullandığı çeşitli yöntemleri içerir. Bu aşama, hedef sistem veya organizasyon hakkında derinlemesine bilgi edinmeyi amaçlar.

Keşif Aşamasının Alt Aşamaları:

1.Açık Kaynak Araştırması (Open Source Intelligence - OSINT):
- Web Siteleri ve Sosyal Medya: Hedef organizasyonun web sitesi, sosyal medya hesapları, bloglar ve forumlar gibi açık kaynaklardan bilgi toplanır. Çalışanlar hakkında bilgiler, organizasyon yapısı, kullanılan teknolojiler ve güvenlik açıkları hakkında ipuçları elde edilebilir.
- Dizinler ve Kayıtlar: WHOIS bilgileri, DNS kayıtları, IP adresi blokları, SSL sertifikaları ve diğer açık kaynaklardan hedefin ağ yapısı hakkında bilgi edinilebilir.

2.Sosyal Mühendislik:
- Phishing (Oltalama): Hedef kişilere sahte e-postalar veya mesajlar gönderilerek kişisel bilgiler veya giriş bilgileri toplanabilir.
- Pretexting: Saldırganlar, belirli bir amaçla kişisel bilgi toplamak için sahte kimlikler veya hikayeler kullanabilirler.

3.Ağ Tarama ve Analizi:
- Port Tarama: Hedef sistem üzerindeki açık portlar ve servisler belirlenir. Nmap gibi araçlarla bu portlar taranabilir.

- Yazılım ve Versiyon Bilgisi: Açık portlar üzerinden çalışan servislerin yazılım ve sürüm bilgileri toplanarak potansiyel zayıflıklar belirlenebilir.
- Ağ Haritalama: Hedef ağının yapısı, bağlı cihazlar ve IP adresleri gibi bilgiler elde edilir. Bu, hedefin altyapısını anlamak için önemlidir.

4.Sistem Bilgisi Toplama:
- Banner Grabbing: Hedef sistemlerin servisleri tarafından sağlanan bilgi başlıkları toplanır. Bu başlıklar genellikle yazılım türü ve sürüm bilgilerini içerir.
- Güvenlik Duyarlılığı Analizi: Bilinen açıklar ve güvenlik zayıflıkları hakkında bilgi toplanarak hedef sistemlerin potansiyel zayıflıkları belirlenir.

5.Çalışan ve Organizasyon Yapısı Bilgisi:
- Çalışan Bilgileri: Şirket çalışanlarının adları, görevleri ve iletişim bilgileri toplanır. Bu bilgiler, sosyal mühendislik saldırıları için kullanılabilir.
- Organizasyon Şeması: Organizasyon yapısı, departmanlar ve hiyerarşik ilişkiler hakkında bilgi edinilir. Bu, hedef kişilere yaklaşımı kolaylaştırabilir.

Araçlar ve Teknikler:
- Nmap: Ağ tarama ve port keşfi için kullanılır.
- Recon-ng: OSINT toplama için kapsamlı bir framework'tür.
- Shodan: İnternete bağlı cihazların keşfi için kullanılır.
- Maltego: Veri madenciliği ve sosyal mühendislik araştırmaları için kullanılan bir araçtır.

SOC İçin Tespit Yöntemleri
- Güvenlik duvarı ve IDS/IPS loglarını izleme (Nmap gibi taramalar tespit edilebilir).
- Web sunucularında anormal istekleri takip etme (HTTP logları üzerinden).
- Çalışanlara yönelik sosyal mühendislik saldırılarını fark etmek için e-posta loglarını analiz etme.

Proaktif Savunma Mekanizmaları
- OSINT verilerini sınırlandır (örn. çalışanların e-posta adreslerini herkese açık paylaşmamak).
- Web uygulamalarını ve ağları sürekli tarayıp açıkları kapat.
- Güvenlik farkındalık eğitimleri düzenle (phishing saldırılarına karşı).

Keşif Aşamasının Önemi:
- Hedef Belirleme: Saldırganların hangi sistemleri hedef alacağı ve hangi yöntemleri kullanacağı konusunda karar vermesine yardımcı olur.
- Zayıflık Analizi: Hedef sistemlerdeki potansiyel zayıflıklar belirlenir ve bu zayıflıklardan yararlanmak için stratejiler geliştirilir.
- Saldırı Planı Oluşturma: Toplanan bilgiler doğrultusunda etkili bir saldırı planı hazırlanabilir.

Bu aşamada yapılan detaylı bilgi toplama, sonraki adımların başarılı bir şekilde yürütülmesi için kritik öneme sahiptir. Savunma tarafında ise bu aşamanın farkında olmak ve gerekli önlemleri almak, siber güvenliği artırabilir.

2.Aşama Silahladırma

Silahlandırma (Weaponization) aşaması, siber saldırının ikinci adımıdır ve bu aşamada saldırganlar, keşif aşamasında topladıkları bilgilere dayanarak saldırı için uygun araçları ve teknikleri hazırlarlar. Bu aşamanın amacı, hedef sistem veya ağa zarar verebilecek etkili bir saldırı vektörü oluşturmak ve bu vektörü kullanmak için gerekli araçları hazırlamaktır.

Silahlandırma Aşamasının Alt Aşamaları:

1.Zararlı Yazılım (Malware) Geliştirme:
- Özel Yazılım: Saldırganlar, hedefe özgü zararlı yazılımlar geliştirirler. Bu yazılımlar, hedef sistemde çalışarak saldırganın kontrolünü sağlar veya sistemde zarar verir.
- Zararlı Kodlar: Genellikle çeşitli açık kaynaklı veya ticari zararlı yazılım kodları modifiye edilir. Saldırganlar, bu kodları hedef sistemlere uygun hale getirebilirler.

2.Exploit (Sömürü) Geliştirme:
- Güvenlik Açıkları: Keşif aşamasında belirlenen güvenlik açıklarından yararlanmak için özel exploitler hazırlanır. Bu exploitler, hedef sistemdeki bir zayıflıktan yararlanarak zararlı yazılımı veya komutları çalıştırabilir.
- Exploit Kitleri: Saldırganlar, çeşitli exploitlerin bir araya getirildiği kitler oluşturabilirler. Bu kitler, hedef sistemde farklı açıkları hedef alabilir.

3.Zararlı Dosya veya Link Oluşturma:
- Şirket İçi E-posta ve Belgeler: Saldırganlar, hedef organizasyondan alınan bilgileri kullanarak inandırıcı e-posta ekleri veya belgeler oluşturabilirler. Bu belgeler, zararlı yazılımı içerir ve genellikle sosyal mühendislik ile birlikte kullanılır.
- Zararlı Web Siteleri veya Linkler: Zararlı bağlantılar veya web siteleri oluşturulur. Bu bağlantılar, hedefin kötü amaçlı yazılımı indirmesi veya zararlı içerikle etkileşimde bulunmasını sağlar.

4.Komut ve Kontrol (C2) Kanalı Kurma:
- İletişim Kanalları: Saldırganlar, zararlı yazılımın hedef sistemle iletişim kurabilmesi için bir komut ve kontrol (C2) kanalı oluştururlar. Bu, genellikle internet üzerinden veya başka bir iletişim yöntemiyle yapılır.
- Şifreleme ve Gizleme: C2 iletişimi, güvenlik önlemlerini aşmak için şifrelenebilir veya gizlenebilir. Bu, zararlı yazılımın tespit edilmesini zorlaştırabilir.

5.Zararlı İçerik ve Arka Kapı Kurulumu:
- Arka Kapı (Backdoor): Saldırganlar, hedef sistemde kalıcı bir erişim sağlamak için arka kapılar kurabilirler. Bu, saldırganın gelecekte sisteme tekrar erişim sağlamasını kolaylaştırır.
- Zararlı Kod Enjeksiyonu: Sistemlere zararlı kodların yerleştirilmesi, bu kodların çalıştırılmasını ve hedef sistem üzerinde kontrol sağlanmasını mümkün kılar.

Araçlar ve Teknikler:
- Metasploit: Güvenlik açıklarını test etmek ve exploitler geliştirmek için kullanılan popüler bir araçtır.
- Cobalt Strike: Zararlı yazılım geliştirme ve komut ve kontrol (C2) kanalları kurma için kullanılan bir araçtır.

- Veil Framework: Güvenlik testleri için zararlı yazılımın tespit edilmesini zorlaştıran araçlar sağlar.
- Empire: PowerShell tabanlı bir komut ve kontrol (C2) aracı olarak kullanılabilir.

SOC İçin Tespit Yöntemleri
- Zararlı yazılım imzalarını ve hash değerlerini tespit eden tehdit istihbaratı kullanma.
- C2 sunucularına yapılan anormal bağlantıları IDS/IPS ile analiz etme.
- Sandbox ortamlarında şüpheli dosyaları çalıştırarak dinamik analiz yapma.

Proaktif Savunma Mekanizmaları
- EDR/XDR sistemlerini kullanarak dosya içeriği analizi yap.
- E-posta filtreleme sistemleriyle zararlı ekleri engelle.
- Network Traffic Analysis (NTA) ile bilinmeyen zararlı trafiği belirle.

Silahlandırma Aşamasının Önemi:
- Etkili Saldırı: Bu aşama, saldırının başarılı olması için gerekli araç ve tekniklerin hazırlanmasını sağlar. Hedef sistemin güvenlik açıklarından yararlanmak için doğru araçların kullanılması kritik öneme sahiptir.
- Saldırı Planı: Silahlandırma aşaması, hedef sistem için özel olarak tasarlanmış bir saldırı planı oluşturur. Bu plan, zararlı yazılımın etkili bir şekilde çalışmasını sağlar.
- Zararı Artırma: Saldırganlar, bu aşamada zarar verme potansiyelini artıran araçlar ve teknikler geliştirirler.

Silahlandırma aşamasında dikkatli bir hazırlık yaparak, saldırganlar, hedef sistem üzerinde etkili bir şekilde saldırı gerçekleştirebilirler. Bu aşama, saldırının başarısını doğrudan etkiler ve genellikle hedefin zayıf noktalarına uygun olarak özelleştirilir.

3.Aşama Teslimat

Teslimat (Delivery) aşaması, siber saldırının üçüncü adımıdır ve bu aşamada saldırganlar, silahlandırma aşamasında hazırladıkları zararlı yazılımı veya exploit'i hedefe ulaştırır. Bu aşama, saldırının aktif bir şekilde hedefe iletilmesi ve çalıştırılmasını sağlamak için kritik öneme sahiptir.

Teslimat Aşamasının Alt Aşamaları:

1.E-posta Tabanlı Teslimat:
- Phishing (Oltalama) E-postaları: Saldırganlar, hedef kişilere sahte e-postalar gönderir. Bu e-postalar, genellikle zararlı ekler veya bağlantılar içerir. E-postalar, hedefin dikkatini çekmek ve zararlı yazılımın indirilmesini veya çalıştırılmasını sağlamak için tasarlanır.
- İkna Edici İçerik: E-postalar, genellikle hedefe çekici gelebilecek içerikler (örneğin, önemli güncellemeler, şüpheli ödüller veya iş teklifleri) içerir.

2.Kötü Amaçlı Web Siteleri ve Bağlantılar:
- Zararlı Web Siteleri: Saldırganlar, zararlı yazılımın indirilebileceği veya çalıştırılabileceği sahte web siteleri oluştururlar. Bu siteler, genellikle hedefin ilgisini çeken konularda içerik sunar.
- Zararlı Bağlantılar: E-posta veya sosyal medya gibi kanallarla hedefe zararlı bağlantılar gönderilir. Bu bağlantılar, zararlı yazılımı indirir veya hedef sistemi zararlı bir web sitesine yönlendirir.

3.Fiziksel Teslimat:
- Kötü Amaçlı Donanım: Saldırganlar, fiziksel medya (USB bellek, CD, vb.) kullanarak zararlı yazılımı hedef sisteme ulaştırabilirler. Bu yöntem, genellikle hedefe fiziksel erişim sağlandığında kullanılır.
- Kişisel Teslimat: Saldırganlar, zararlı yazılım içeren fiziksel cihazları doğrudan hedefe teslim edebilirler.

4.Sosyal Mühendislik:
- Yalan İçerikler: Sosyal mühendislik teknikleri kullanılarak, hedef kişilere zararlı yazılımın çalıştırılması için kandırılmaları sağlanabilir. Örneğin, hedefin kötü amaçlı bir yazılımı indirmesi için bir "güncelleme" uyarısı verilebilir.
- Destek Talepleri: Saldırganlar, teknik destek gibi görünümlerle zararlı yazılımı yüklemeleri için hedef kişileri ikna edebilirler.

5.Ağ ve Sistem Üzerinden Teslimat:
- Ağ Tarayıcıları ve Exploitler: Saldırganlar, hedef ağ üzerinden doğrudan exploitler kullanarak zararlı yazılımı dağıtabilirler. Bu, genellikle ağda bulunan açık portlar veya zayıflıklardan yararlanılarak yapılır.
- Sistem İçindeki Güvenlik Açıkları: Hedef sistemlerdeki güvenlik açıklarından yararlanarak zararlı yazılımın uzaktan yüklenmesi veya çalıştırılması sağlanabilir.

Araçlar ve Teknikler:
- E-posta Gönderici Araçları: E-posta tabanlı saldırılar için kullanılır. Örneğin, Evilginx, e-postaları zararlı bağlantılarla gönderir.
- Web Shells ve Exploit Kitleri: Zararlı yazılımın hedef sistemlere gönderilmesi için kullanılır. Örneğin, Metasploit, exploit ve payloadları içerir.
- Fiziksel Teslimat Araçları: USB bellekler veya diğer fiziksel medya için kullanılan araçlar ve yazılımlar.

SOC İçin Tespit Yöntemleri
- E-posta loglarında sahte alan adlarını ve şüpheli ekleri inceleme.
- Web proxy loglarını tarayarak zararlı URL bağlantılarını tespit etme.
- Honeytoken kullanarak sahte verilerle saldırganın hareketlerini izleme.

Proaktif Savunma Mekanizmaları
- Güçlü e-posta filtreleme politikaları uygula (DMARC, SPF, DKIM).
- Güvenlik farkındalık eğitimleri ile çalışanları bilinçlendir.
- USB erişim politikalarını sınırla ve denetle.

Teslimat Aşamasının Önemi:
- Erişim Sağlama: Teslimat aşaması, zararlı yazılımın hedef sisteme ulaşmasını ve çalışmasını sağlar. Bu aşamada başarılı olmak, saldırının etkili bir şekilde gerçekleştirilmesi için kritik öneme sahiptir.
- Savunma Stratejileri: Savunma tarafında, teslimat aşamasına yönelik stratejiler geliştirmek, zararlı yazılımların ve exploitlerin hedefe ulaşmasını engelleyebilir. Bu, e-posta filtreleme, ağ güvenlik çözümleri ve kullanıcı eğitimi gibi yöntemlerle sağlanabilir.
- Saldırı Başarısı: Bu aşamanın başarısı, saldırının ilerleyen aşamalarında zararlı yazılımın etkinliğini ve sistem üzerindeki etkisini doğrudan etkiler.

Teslimat aşaması, saldırının aktif bir şekilde hedefe iletilmesini sağlar ve genellikle saldırganın hedef sistemi ele geçirme veya zararlı yazılımı çalıştırma amacıyla gerçekleştirdiği kritik bir adımdır. Bu aşamada kullanılan yöntemler, hedefin savunma mekanizmalarını aşmak ve zararlı yazılımın etkili bir şekilde çalışmasını sağlamak için tasarlanmıştır.

4.Aşama Sömürü

Sömürü (Exploitation) aşaması, siber saldırının dördüncü adımıdır ve bu aşamada saldırgan, hedef sistemdeki bir güvenlik açığından yararlanarak zararlı yazılımı veya exploit'i çalıştırır. Sömürü aşaması, hedef sistem üzerinde yetki kazanmak ve saldırının ilerleyen aşamalarını gerçekleştirmek için kritik bir adımdır.

Sömürü Aşamasının Alt Aşamaları:

1.Güvenlik Açığının Kullanılması:
- Zayıflık Analizi: Saldırgan, keşif aşamasında veya silahlandırma aşamasında belirlenen güvenlik açıklarını kullanır. Bu açıklar, yazılım hataları, konfigürasyon hataları veya bilinen güvenlik açıkları olabilir.
- Exploit Kullanımı: Saldırgan, hedef sistemdeki zayıflığı kullanarak exploit çalıştırır. Bu exploit, genellikle hedef sistemdeki güvenlik açığını kullanarak zararlı kodun çalıştırılmasını sağlar.

2.Yetki Kazanma:
- Sistem Yetkileri: Saldırgan, exploit'i kullanarak hedef sistem üzerinde yetki kazanır. Bu, genellikle kullanıcı seviyesindeki veya yönetici seviyesindeki (root veya admin) yetkileri içerir.
- Kullanıcı Hakları: Bazı durumlarda, saldırganlar hedef sistemdeki normal kullanıcı haklarıyla sınırlı kalabilir, ancak bu hakları yükseltmek için ek adımlar atabilirler.

3.Zararlı Yazılımın Çalıştırılması:
- Kötü Amaçlı Kod: Saldırgan, exploit aracılığıyla zararlı yazılımı çalıştırır. Bu zararlı yazılım, hedef sistemde çeşitli eylemleri gerçekleştirebilir, örneğin arka kapılar kurma, veri çalma veya sistemleri bozma.
- İzleme ve Kontrol: Saldırgan, zararlı yazılımı çalıştırarak hedef sistemde izleme ve kontrol sağlar. Bu, genellikle zararlı yazılımın C2 (Komut ve Kontrol) sunucusuyla iletişim kurmasını içerir.

4.Zafiyetlerin Kullanımı:
- Köprüleme (Pivoting): Saldırgan, bir güvenlik açığını kullanarak hedef ağ üzerinde daha geniş bir erişim sağlar. Bu, bir sistemi ele geçirdikten sonra diğer sistemlere erişim sağlamak için yapılır.
- Kısayol Kullanımı: Saldırgan, sistemde mevcut olan güvenlik açıklarını kullanarak daha fazla yetki kazanabilir veya daha fazla zararlı eylem gerçekleştirebilir.

Araçlar ve Teknikler:
- Metasploit: Güvenlik açıklarını kullanmak ve exploitler geliştirmek için yaygın olarak kullanılan bir framework'tür. Hedef sistemdeki güvenlik açıklarını kullanarak zararlı kodları çalıştırabilir.

- BeEF (Browser Exploitation Framework): Tarayıcı tabanlı güvenlik açıklarını hedef alarak zararlı kod çalıştırabilir.
- Cobalt Strike: Zararlı yazılımın yanı sıra exploitleri kullanarak hedef sistemde kontrol sağlar.

SOC İçin Tespit Yöntemleri
- Log analiz sistemleri ile anormal sistem çağrılarını (syscall) takip etme.
- SIEM kullanarak exploit araçlarının karakteristik imzalarını belirleme.
- HoneyPot kullanarak saldırganı kandırıp analiz etme.

Proaktif Savunma Mekanizmaları
- Tüm sistemleri güncel tut (patch management).
- EDR ile şüpheli PowerShell ve komut çalıştırmalarını engelle.
- İşletim sistemi ve uygulama izinlerini minimum seviyeye indir.

Sömürü Aşamasının Önemi:
- Başarı Şansı: Bu aşama, saldırının başarılı bir şekilde ilerlemesi için kritik bir adımdır. Hedef sistemde etkili bir şekilde exploit kullanmak, saldırının diğer aşamalarına geçişi sağlar.
- Yetki Yükseltme: Sömürü aşamasında başarılı bir şekilde yetki kazanmak, saldırganın hedef sistemde daha geniş bir kontrol sağlamasına ve daha fazla zararlı eylem gerçekleştirmesine olanak tanır.
- Savunma Stratejileri: Savunma tarafında, güvenlik açıklarının belirlenmesi ve kapatılması, bu aşamanın etkisini azaltabilir. Bu, düzenli güvenlik taramaları, güncellemeler ve yamanın uygulanmasını içerir.

Sömürü aşaması, saldırganların hedef sistem üzerindeki kontrolünü sağlamak için kritik bir adımdır ve etkili bir şekilde gerçekleştirilmesi, saldırının başarılı olmasını doğrudan etkiler. Bu aşama, hedef sistemin güvenlik açıklarından yararlanarak zararlı yazılımın çalıştırılmasını sağlar ve saldırının ilerleyen aşamaları için zemin hazırlar.

5.Aşama Kurulum:
Kurulum (Installation) aşaması, siber saldırının beşinci adımıdır ve bu aşamada saldırgan, hedef sistemde kalıcı bir varlık oluşturur. Bu, hedef sistemde sürekli bir erişim sağlamak ve saldırının uzun vadede etkili olmasını sağlamak için yapılan bir adımdır. Kurulum aşaması, zararlı yazılımın veya arka kapının (backdoor) hedef sistemde kalıcı hale gelmesini ve zamanla sistemden silinmesini veya tespit edilmesini zorlaştırmayı amaçlar.

Kurulum Aşamasının Alt Aşamaları:

1.Arka Kapı (Backdoor) Kurulumu:
- Kalıcı Erişim Sağlama: Saldırgan, hedef sistemde arka kapılar kurarak sürekli bir erişim sağlar. Bu arka kapılar, saldırganın sistemi gelecekte de erişmesini sağlar ve genellikle sistemdeki güvenlik duvarlarını veya izleme sistemlerini geçmek için tasarlanmıştır.
- Otomatik Başlatma: Arka kapılar, sistem her yeniden başlatıldığında otomatik olarak çalışacak şekilde yapılandırılabilir. Bu, hedef sistemde kalıcı bir varlık oluşturur.

2.Zararlı Yazılımın Yüklenmesi:

- Kötü Amaçlı Modüller: Saldırgan, hedef sisteme çeşitli zararlı yazılım modülleri yükleyebilir. Bu modüller, veri çalma, anahtar kaydedici, ağ dinleme veya diğer zararlı faaliyetler için kullanılabilir.
- Gizleme Teknikleri: Zararlı yazılım, hedef sistemde tespit edilmesini zorlaştırmak için çeşitli gizleme teknikleri kullanabilir. Bu teknikler arasında kod şifreleme, bellek içi çalıştırma veya anti-virüs yazılımlarını atlatma yer alabilir.

3.Yetki Yükseltme (Privilege Escalation):
- Sistem Yetkilerini Artırma: Saldırgan, başlangıçta elde ettiği düşük yetkileri artırmak için çeşitli teknikler kullanabilir. Bu, sistemde daha fazla kontrol sağlamak ve daha fazla zararlı eylem gerçekleştirmek için önemlidir.
- Yönetici Hakları: Yetki yükseltme, saldırganın yönetici hakları elde etmesine ve hedef sistemde tam kontrol sağlamasına yardımcı olabilir.

4.Kalıcı Komponentler ve Başlangıç Kayıtları:
- Otomatik Başlatma: Zararlı yazılım, hedef sistemdeki başlangıç kayıtlarına, hizmetlere veya planlanmış görevler gibi mekanizmalara eklenerek sistem her başlatıldığında çalışmasını sağlar.
- Sistem Dosyalarına Gizlenme: Zararlı yazılım, sistem dosyalarına veya geçici dosyalara gizlenerek fark edilmesini zorlaştırabilir.

5.İzleme ve Raporlama:
- Geri Bildirim ve Güncellemeler: Saldırgan, zararlı yazılımın performansını izleyebilir ve gerekli güncellemeleri yapabilir. Bu, hedef sistemden veri toplama ve komutları güncelleme için yapılır.
- Komut ve Kontrol (C2) İletişimi: Zararlı yazılım, sürekli olarak komut ve kontrol (C2) sunucusuyla iletişim kurarak saldırganın hedef sistem üzerindeki kontrolünü sürdürmesini sağlar.

Araçlar ve Teknikler:
- Metasploit Framework: Arka kapılar ve zararlı modüller oluşturmak ve yüklemek için kullanılır.
- Cobalt Strike: Kalıcı arka kapılar kurma ve yetki yükseltme teknikleri için kullanılır.
- Empire: PowerShell tabanlı zararlı yazılım ve kalıcı komponentler kurma için kullanılan bir araçtır.

SOC İçin Tespit Yöntemleri
- Yeni hizmetlerin, görevlerin veya cron işlerinin analiz edilmesi.
- Registry değişikliklerini izleyerek anormal girişleri tespit etme.
- Yüksek izinle çalışan yeni süreçleri izleme (SIEM üzerinden).

Proaktif Savunma Mekanizmaları
- Beyaz liste yaklaşımı kullanarak sadece izin verilen uygulamaların çalışmasına izin ver.
- Anormal süreç başlatmalarını ve uzaktan erişim trafiğini engelle.
- Host-based firewall ile şüpheli bağlantıları sınırla.

Kurulum Aşamasının Önemi:

- Sürekli Erişim: Bu aşama, saldırganın hedef sistemde sürekli bir erişim sağlamasını ve gelecekteki saldırılar veya veri çalma eylemlerini kolaylaştırmasını sağlar.
- Savunma Zorlukları: Kalıcı zararlı yazılımlar ve arka kapılar, savunma sistemlerinin tespit etmesini zorlaştırabilir ve hedef sistemdeki güvenlik açıklarını uzun vadeli bir tehdit haline getirebilir.
- Güvenlik Önlemleri: Savunma tarafında, zararlı yazılımların ve arka kapıların tespitini ve kaldırılmasını kolaylaştırmak için sistem taramaları, davranışsal analizler ve sürekli izleme gibi önlemler alınabilir.

Kurulum aşaması, siber saldırının başarılı bir şekilde uzun vadeli etkilerini sağlamak için kritik öneme sahiptir. Bu aşamada kurulan arka kapılar ve zararlı yazılımlar, saldırganın hedef sistemde kalıcı bir kontrol sağlamasını ve bu kontrolü sürdürmesini sağlar.

6.Aşama: Komut ve Kontrol:

Komut ve Kontrol (Command and Control - C2) aşaması, siber saldırının altıncı adımıdır ve bu aşamada saldırgan, hedef sistemdeki zararlı yazılım veya arka kapı aracılığıyla kontrol sağlar. Bu aşama, saldırganın hedef sistem üzerinde etkili bir şekilde komut göndermesi ve veri alması için gerekli olan iletişim kanallarını kurmayı ve sürdürmeyi içerir.

Komut ve Kontrol Aşamasının Alt Aşamaları:

1.İletişim Kanalı Kurma:
- C2 Sunucusu: Saldırgan, hedef sistemle iletişim kurmak için bir komut ve kontrol (C2) sunucusu kurar. Bu sunucu, genellikle zararlı yazılımın komutları aldığı ve sonuçları raporladığı bir merkez olarak işlev görür.
- Protokoller ve Portlar: İletişim, genellikle HTTP, HTTPS, FTP, DNS veya özel protokoller aracılığıyla yapılır. C2 sunucusu, bu protokolleri kullanarak hedef sistemle veri alışverişi yapar.

2.Zararlı Yazılımın İletişimi:
- Komut Gönderimi: Saldırgan, zararlı yazılıma belirli komutlar gönderir. Bu komutlar, veri toplama, dosya ekleme, şifreleri çalma veya diğer zararlı faaliyetleri içerir.
- Veri Toplama: Zararlı yazılım, hedef sistemdeki verileri toplayarak C2 sunucusuna iletebilir. Bu veri, kullanıcı bilgileri, dosyalar veya diğer hassas bilgiler olabilir.

3.Geri Bildirim ve Güncellemeler:
- Durum Raporları: Zararlı yazılım, sistemin durumunu ve gerçekleştirilen eylemleri raporlamak için düzenli geri bildirimler gönderir. Bu, saldırganın sistem üzerindeki etkinliğini izlemesine olanak tanır.
- Güncellemeler ve Yamanlar: Saldırgan, zararlı yazılımın güncellemelerini yapabilir veya yeni modüller ekleyebilir. Bu, zararlı yazılımın yeteneklerini artırmak veya savunma mekanizmalarını aşmak için yapılır.

4.Gizleme ve Şifreleme:
- Şifreleme: İletişim, genellikle şifreleme yöntemleri kullanılarak gizlenir. Bu, zararlı yazılımın ve C2 sunucusunun tespit edilmesini zorlaştırır.

- Gizli Kanallar: Saldırganlar, zararlı iletişim trafiğini gizlemek için çeşitli teknikler kullanabilirler, örneğin, HTTP trafiği gibi görünmesi için şifrelenmiş veriyi saklamak.

5.Erişim Yönetimi:
- Yetki Yönetimi: Saldırgan, hedef sistemdeki erişim haklarını yönetir. Bu, yeni kullanıcılar eklemek veya mevcut kullanıcı haklarını değiştirmek anlamına gelebilir.
- Ağ Üzerinde Pivoting: Saldırgan, C2 kanalı aracılığıyla ağda başka sistemlere erişim sağlamak için pivoting teknikleri kullanabilir.

Araçlar ve Teknikler:
- Metasploit: Komut ve kontrol işlevleri sağlayan çeşitli modüller içerir ve zararlı yazılımların yönetimini sağlar.
- Cobalt Strike: Zararlı yazılımlar ve C2 sunucuları ile kapsamlı bir komut ve kontrol işlevi sunar.
- Empire: PowerShell tabanlı C2 işlevleri sunarak zararlı yazılımın yönetilmesini sağlar.
- Weevely: Web tabanlı C2 aracı olarak kullanılabilir ve zararlı yazılımın yönetimini sağlar.

SOC İçin Tespit Yöntemleri
- DNS tünelleme veya uzun süreli bağlantıları izleme.
- SIEM üzerinden anormal trafik paternlerini belirleme.
- Yabancı veya bilinmeyen IP adreslerine yapılan bağlantıları analiz etme.

Proaktif Savunma Mekanizmaları
-Egress filtering uygulayarak sistemin dış dünya ile gereksiz bağlantı kurmasını engelle.
- SSL/TLS denetimi yaparak zararlı şifreli trafiği çözümle.
- Tehdit istihbaratı ile C2 sunucu IP'lerini önceden belirleyerek erişimi engelle.

Komut ve Kontrol Aşamasının Önemi:
- Saldırı Yönetimi: Bu aşama, saldırganın hedef sistem üzerindeki kontrolünü sürdürmesi ve saldırının etkilerini yönetmesi için kritik öneme sahiptir. Komut ve kontrol, saldırının etkinliğini ve kapsamını artırabilir.
- Savunma Stratejileri: Savunma tarafında, komut ve kontrol iletişimini tespit etmek için ağ trafiği analizleri, anomali tespiti ve davranışsal analizler kullanılabilir. Ayrıca, zararlı iletişim kanallarını engellemek için güvenlik duvarları ve ağ izleme çözümleri uygulanabilir.
- Gizlilik ve Güvenlik: İletişim kanallarının gizlenmesi ve şifrelenmesi, saldırganların tespit edilmesini zorlaştırır. Bu nedenle, savunma stratejileri sürekli güncellenmeli ve tehditlere karşı proaktif önlemler alınmalıdır.

Komut ve kontrol aşaması, zararlı yazılımın etkili bir şekilde yönetilmesi ve hedef sistem üzerindeki faaliyetlerin kontrol edilmesi için kritik bir adımdır. Bu aşama, saldırganın hedef üzerindeki etkisini sürdürmesini ve saldırının uzun vadeli başarısını sağlamasını mümkün kılar.

7.Aşama Hedeflere Yönelik Hareketler:

Hedeflere Yönelik Hareketler (Actions on Objectives) aşaması, siber saldırının yedinci adımıdır ve bu aşamada saldırgan, hedef sistemdeki veya ağdaki belirli amaçlara ulaşmak için çeşitli eylemleri gerçekleştirir. Bu aşama, saldırganın saldırının hedeflerine yönelik nihai amaçlarına ulaşmayı hedefler ve genellikle verilerin çalınması, sistemlerin bozulması veya diğer zararlı faaliyetleri içerir.

Hedeflere Yönelik Hareketler Aşamasının Alt Aşamaları:

1.Veri Çalma:
- Bilgi Toplama: Saldırgan, hedef sistemden hassas bilgiler toplar. Bu bilgiler kişisel veriler, finansal bilgiler, ticari sırlar veya kurumsal veriler olabilir.
- Veri Sızıntısı: Toplanan veriler, saldırganın kontrolündeki bir sunucuya veya başka bir hedefe sızdırılır. Bu, genellikle komut ve kontrol (C2) kanalı üzerinden yapılır.

2.Sistemleri Bozma veya Şifreleme:
- Şifreleme ve Fidye Yazılımı: Saldırganlar, hedef sistemdeki verileri şifreleyebilir ve fidye yazılımı (ransomware) kullanarak verilerin geri alınması için fidye talep edebilir.
- Sistem Bozma: Hedef sistemlerin işleyişini bozmak veya verileri silmek amacıyla zararlı yazılım kullanılabilir. Bu, hedefin operasyonlarını etkileyebilir.

3.Yetki Yükseltme ve Erişim Sağlama:
- Yüksek Yetkiler Elde Etme: Saldırganlar, hedef sistemde yönetici veya yüksek yetkili hesaplara erişim sağlamaya çalışır. Bu, sistemde daha fazla kontrol sağlamalarına olanak tanır.
- Kritik Sistemlere Erişim: Hedef ağdaki kritik sistemlere veya sunuculara erişim sağlanabilir. Bu, saldırının etkisini artırabilir ve daha fazla zararlı faaliyet gerçekleştirilmesini sağlayabilir.

4.Ağda Hareket:
- Pivoting (Köprüleme): Saldırgan, bir sistemden diğerine geçiş yaparak hedef ağda daha geniş bir erişim sağlar. Bu, ağdaki diğer sistemlere veya hizmetlere erişim sağlamak için yapılır.
- Zararlı Yazılım Dağıtımı: Saldırgan, hedef ağda zararlı yazılımın yayılmasını sağlar. Bu, ağdaki diğer sistemlere bulaşma ve etki alanını genişletme amacı taşır.

5.Gizli İşlemler ve İzleme:
- İzleme: Saldırgan, hedef sistemdeki etkinlikleri izleyebilir. Bu, hedefin faaliyetlerini veya güvenlik yanıtlarını değerlendirmek için yapılır.
- Gizli Aktiviteler: Saldırgan, hedef sistemde gizli işlemler gerçekleştirir. Bu, diğer eylemleri gizlemek ve sistemde uzun süre kalıcı bir varlık oluşturmak için yapılır.

Araçlar ve Teknikler:
- Mimikatz: Yetki yükseltme ve kimlik doğrulama bilgilerini çalmak için kullanılan bir araçtır.
- Metasploit: Hedef sistemlerde zararlı yazılım çalıştırmak ve ağda hareket etmek için kullanılan bir framework'tür.
- Cobalt Strike: Hedef sistemlerde hareket etmeyi ve veri çalmayı sağlayan kapsamlı bir komut ve kontrol aracıdır.

- Ransomware (Fidye Yazılımı): Verileri şifreleyerek fidye talep eden zararlı yazılımlar kullanılır.

SOC İçin Tespit Yöntemleri

- Büyük hacimli veri transferlerini SIEM ile izleme.
- Anormal dosya değişikliklerini takip etme (DLP sistemleri).
- Çıkış trafiğinde şifrelenmiş veya bilinmeyen protokolleri analiz etme.

Proaktif Savunma Mekanizmaları
- DLP (Data Loss Prevention) çözümleri ile veri sızıntılarını önle.
- Ransomware karşı yedekleme ve hızlı geri yükleme planları oluştur.
- Kullanıcı erişim izinlerini minimuma indirerek iç tehditleri engelle.

Hedeflere Yönelik Hareketler Aşamasının Önemi:
- Nihai Amaçlara Ulaşma: Bu aşama, saldırının nihai hedeflerine ulaşmayı sağlar. Verilerin çalınması, sistemlerin bozulması veya diğer zararlı faaliyetler, saldırının amacına hizmet eder.
- Savunma Stratejileri: Savunma tarafında, veri sızıntılarını önlemek, sistemlerin güvenliğini artırmak ve ağ içi hareketleri izlemek için çeşitli stratejiler uygulanabilir. Bu, veri şifreleme, ağ segmentasyonu ve düzenli güvenlik izleme ile sağlanabilir.
- Etkilenen Alanların Yönetimi: Bu aşamada yapılan eylemler, genellikle büyük etkilere yol açabilir ve hedef organizasyon üzerinde kalıcı zararlara neden olabilir. Bu nedenle, etkili bir yanıt ve iyileşme planı önemlidir.

Hedeflere yönelik hareketler aşaması, saldırganların siber saldırının nihai amacına ulaşmasını sağlar ve genellikle büyük ölçekte veri çalma, sistem bozulması veya diğer zararlı eylemleri içerir. Bu aşama, saldırının etkilerini artırmak ve hedef organizasyon üzerinde uzun vadeli etkiler bırakmak için kritik öneme sahiptir.

Örnek Senaryo

Faz	Açıklama
Keşif	Hedefe ait e-posta adresleri tespit edilir.
Silahlanma	Zararlı doc dosyası hazırlanır.
İletme	E-Posta yolu ile zararlı doc dosyası hedefe gönderilir
Sömürme	CVE-2017-8570 zafiyeti istismar edilir.
Yükleme	Zararlı kendini registry dosyasına ekler. `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run`
Komuta & Kontrol	HTTPS ile xx.77.87 ile haberleşir
Eylem	Kurumsal veri içeren dosyaları komuta kontrol merkezine gönderir.

Cyber Kill Chain aşamalarına örnekler

Bir siber saldırgan, kurumsal veri içeren dosyaları ele geçirmek amacıyla Y isimli kurumu hedef alır. Öncelikle motivasyonunu belirledikten sonra kurum hakkında keşif çalışmaları yapmaya başlar. Bu süreçte, hedef kurumun çalışanlarının sosyal medya hesaplarında kurumsal e-posta adreslerini kullandıklarını tespit eder ve bir e-posta havuzu oluşturur.

Daha sonra, sosyal mühendislik saldırısında kullanacağı atak vektörünü belirleme aşamasına geçer. Keşif sürecinde, hedef kurumun Windows işletim sistemi kullandığını tespit ettiğinden CVE-2017–8570 kodlu Microsoft Office uzaktan kod çalıştırma zafiyetini istismar etmenin etkili olacağını düşünür. Bu doğrultuda, güvenlik açığını sömürebilecek bir makro kodu oluşturur ve zararlı kod içeren ".doc" uzantılı bir atak vektörü hazırlar.

Hazırladığı zararlı dosyayı, oluşturduğu e-posta havuzundaki çalışanlara oltalama (phishing) e-postaları aracılığıyla iletir ve dosyanın açılmasını bekler. Hedef kurum çalışanlarından bazıları, e-postada bulunan dosyayı açtığında, zararlı kod çalıştırılır ve sistemlere bulaşır. Bu aşamadan sonra zararlı yazılım, hedef sistemde bulunan zafiyeti istismar ederek işletim sisteminin başlangıcına yüklenir ve kalıcılık sağlar.

Zararlı yazılım, xx.77.87 (geçerli olmayan bir domain adresidir) üzerinden saldırganın komuta ve kontrol (C2) sunucusuyla bağlantı kurar ve saldırganın hedef sistemi uzaktan kontrol etmesine olanak tanır. Sistemi ele geçiren saldırgan, motivasyonunu sağlayan kurumsal dokümanları arar ve tespit ettiği verileri komuta kontrol sunucusuna çıkarmayı başarır.

Cyber Kill Chain'in Önemi

Siber saldırılar giderek daha karmaşık ve sofistike hale gelirken, savunma mekanizmalarının da aynı ölçüde gelişmesi gerekmektedir. Cyber Kill Chain, bir saldırının aşamalarını sistematik bir şekilde analiz ederek saldırganın niyetini ve yöntemlerini anlamaya yardımcı olan kritik bir çerçevedir. Bu model sayesinde, saldırılar erken tespit edilerek proaktif savunma önlemleri alınabilir ve saldırı zinciri henüz tamamlanmadan kesintiye uğratılabilir. Özellikle SOC analistleri, bu modeli kullanarak olayları hızlı bir şekilde sınıflandırabilir, saldırının hangi aşamada olduğunu belirleyebilir ve uygun müdahale stratejileri geliştirebilir. Cyber Kill Chain, tehdit istihbaratı, zafiyet yönetimi, saldırı tespiti ve olay müdahalesi gibi güvenlik süreçlerini iyileştirerek kurumların siber tehditlere karşı daha güçlü bir savunma mekanizması oluşturmasını sağlar.

Sonuç

Cyber Kill Chain, siber güvenlik dünyasında stratejik bir yaklaşım sunarak tehditlerin daha iyi anlaşılmasını ve yönetilmesini sağlar. Saldırı zincirinin her aşamasında uygulanacak doğru güvenlik kontrolleri, saldırının başarılı olmasını engelleyebilir veya etkisini minimize edebilir. Günümüz tehdit ortamında, yalnızca reaktif savunma yöntemleri yeterli olmayıp, proaktif ve katmanlı güvenlik önlemleri almak büyük önem taşımaktadır. Bu nedenle, Cyber Kill Chain modelini anlamak ve uygulamak, SOC ekipleri ve siber güvenlik uzmanları için kritik bir beceri olup, kurumların siber dirençliliğini artırmada önemli bir rol oynar.

Kaynakça

https://oguzcanpamuk.medium.com/bir-siber-saldırı-yaşam-döngüsü-cyber-kill-chain-ed207df69586

https://cybershieldcommunity.com/cyber-kill-chain-nedir/

https://www.gaissecurity.com/blog/cyber-kill-chain-bir-siber-saldirinin-yasam-dongusu

https://bbsteknoloji.com/cyber-kill-chain-nedir/

https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf