CYBER KILL CHAIN

BİR SİBER SALDIRININ YAŞAM DÖNGÜSÜ

07.02.2025

MEHMET MERMER

ALTAY SİBER VATAN

İÇİNDEKİLER

GİRİŞ **3**
CYBER KILL CHAIN NEDİR? **4**
CYBER KILL CHAIN TARİHİ **5**
CYBER KILL CHAIN NASIL ÇALIŞIR? **5**
CYBER KILL CHAIN AŞAMALARI **6**
1) Reconnaissance (Keşif) 6
2) Weaponization (Silahlanma) 7
3) Delivery (İletim) 9
4) Exploitation (Sömürme) 12
5) Installation (Yükleme) 14
6) Command And Control (Komuta & Kontrol) 17
7) Actions On Objectives (Eylem) 19
CYBER KILL CHAIN KULLANARAK TEHDİTLERİ ÖNLEME **22**
CYBER KILL CHAIN MODELİNE ÖRNEK SALDIRI **23**
SONUÇ **25**
KAYNAKÇA **25**

GİRİŞ

Günümüzde siber tehditler giderek karmaşık hale gelmekte ve kurumların güvenliğini tehdit eden siber saldırılar her geçen gün artmaktadır. Bu tehditlere karşı etkin bir savunma mekanizması oluşturmak için, siber saldırıların nasıl gerçekleştirildiğini ve hangi aşamalardan oluştuğunu anlamak büyük önem taşımaktadır.

Bu noktada, Lockheed Martin firması tarafından geliştirilen Cyber Kill Chain Modeli, siber saldırıların yedi temel aşamasını tanımlayarak tehditleri daha iyi analiz etmeye ve savunma stratejileri oluşturmaya yardımcı olmaktadır. Bu model, siber saldırıların başlangıcından hedef sistemin ele geçirilmesine kadar olan süreci detaylı bir şekilde ele almaktadır.

Bu raporda, Cyber Kill Chain Modeli'nin temel aşamaları olan Reconnaissance (Keşif), Weaponization (Silahlandırma), Delivery (Teslimat), Exploitation (Sömürme), Installation (Kurulum), Command & Control (Komuta ve Kontrol) ve Actions on Objectives (Amaçlar Doğrultusunda Hareket) detaylı olarak incelenerek ve her bir aşamanın siber olaylara yönelik tehdit algılama ve müdahale sürecindeki önemi vurgulanmaktadır. Ayrıca, SOC (Security Operations Center) analistlerinin bu modeli kullanarak siber olaylara nasıl daha etkin müdahale edebileceği de ele alınmaktadır.

Bu raporun amacı, Cyber Kill Chain Modeli'ni tanımak, anlamak ve siber saldırıların hangi aşamada olduğunu analiz ederek etkili savunma stratejileri geliştirmeye katkı sağlamaktır.

CYBER KILL CHAIN NEDİR?

Bir Siber Saldırının Yaşam Döngüsü, Siber Ölüm Zinciri Lockheed Martin firması tarafından geliştirilen bir güvenlik modeli olup, saldırganların bir hedef sisteme yönelik gerçekleştirdiği siber saldırıların aşamalarını sistematik bir şekilde analiz etmek, bu aşamaları tespit etmek ve etkili savunma stratejileri geliştirerek saldırıları engellemek amacıyla kullanılan bir çerçevedir. Bu model, saldırı sürecini yedi temel aşamaya ayırarak güvenlik uzmanlarının her aşamada olası tehditleri belirlemesine, erken müdahale etmesine ve saldırının ilerlemesini durdurmasına yardımcı olur. Aynı zamanda, güvenlik ekiplerine tehdit aktörlerinin davranışlarını anlama ve saldırı yüzeyini minimize etme konusunda rehberlik ederek daha proaktif bir siber savunma yaklaşımı sunar.

CYBER KILL CHAIN TARİHİ

2011 yılında Lockheed Martin firması, öldürme zinciri adı verilen askeri bir kavramı siber güvenlik sektörü için uyarladı ve buna siber öldürme zinciri adını verdi. Öldürme zinciri gibi,siber öldürme zinciri de bir saldırının aşamalarını tanımlar ve savunuculara, her aşamada rakiplerinin tipik taktikleri ve teknikleri hakkında fikir verir. Her iki model de saldırganların her aşamayı sırayla takip etmesi beklentisiyle doğrusaldır.

Siber öldürme zincirinin ilk ortaya çıkışından bu yana, siber tehdit aktörleri taktiklerini geliştirdiler ve her zaman siber öldürme zincirinin her aşamasını takip etmiyorlar. Buna karşılık güvenlik sektörü yaklaşımını güncelledi ve yeni modeller geliştirdi. MITRE ATT&CK matrisi, gerçek saldırılara dayanan ayrıntılı bir taktik ve teknik listesidir. Siber öldürme zincirine benzer aşamaları kullanır ancak doğrusal bir sıra izlemez.

2017'de Paul Pols, Fox-IT ve Leiden Üniversitesi ile işbirliği içinde, hem MITRE ATT&CK matrisinin hem de siber öldürme zincirinin unsurlarını 18 aşamalı bir modelde birleştiren birleşik öldürme zinciri adlı başka bir çerçeve geliştirdi.

CYBER KILL CHAIN NASIL ÇALIŞIR?

Siber ölüm zinciri, siber saldırının çeşitli aşamalarını belirleyerek çalışan, saldırganların faaliyetlerini analiz etmeye ve engellemeye yönelik bir güvenlik modelidir. Her aşama, saldırganın belirli bir hedefe ulaşmak için izlediği adımları sistematik bir şekilde ortaya koyar ve bu sürecin anlaşılması, savunma ekiplerinin saldırıyı erken tespit edip engellemesine olanak tanır.

Bu model, saldırının yalnızca gerçekleştiği anda değil, saldırganın keşif aşamasından itibaren tüm süreç boyunca takip edilmesini amaçlar. Siber güvenlik ekipleri, bu aşamaları analiz ederek saldırganın izlediği yöntemi anlamaya, saldırının ilerlemesini durdurmaya ve gelecekte benzer saldırılara karşı daha güçlü savunma mekanizmaları geliştirmeye çalışır.

Siber ölüm zincirinin temel çalışma prensibi, saldırganın faaliyetlerini mümkün olan en erken aşamada tespit edip durdurarak saldırının tamamlanmasını önlemektir. Bunu yaparken, ağ trafiği izleme, anomali tespiti, tehdit istihbaratı ve güvenlik olaylarını ilişkilendirme gibi yöntemler kullanılarak saldırı zincirinin kırılması hedeflenir. Böylece, güvenlik uzmanları saldırganların sistemlere sızmasını önleyebilir, veri sızıntılarını engelleyebilir ve saldırının daha ileri aşamalara taşınmasını engelleyerek kurumun güvenliğini koruyabilir.

CYBER KILL CHAIN AŞAMALARI

1) Reconnaissance (Keşif)

Siber saldırının ilk ve en kritik aşamalarından biri olan Reconnaissance (Keşif), saldırganın hedef aldığı sistem veya organizasyon hakkında bilgi topladığı süreçtir. Bu aşama, saldırının başarılı olabilmesi için gerekli olan zafiyetlerin, sistem yapılandırmalarının ve insan faktörüne dayalı güvenlik açıklarının belirlenmesini içerir. Saldırganlar, keşif sürecinde aktif ve pasif bilgi toplama tekniklerini kullanarak hedefin güvenlik yapısını anlamaya çalışır.

Pasif Keşif (Passive Reconnaissance):

Pasif keşif yöntemleri, saldırganın doğrudan hedef sistemle etkileşime girmeden, mevcut açık kaynaklardan (OSINT - Open Source Intelligence) bilgi toplamasını içerir. Bu yöntemlerde hedef sistemde herhangi bir iz bırakılmadığı için tespit edilmesi daha zordur. Pasif keşif sırasında saldırganlar şunları yapabilir:

- **Sosyal Medya Analizi:** LinkedIn, Twitter, Facebook, Instagram gibi platformlardan çalışanların isimleri, görevleri, e-posta adresleri, ilgi alanları ve iş yerindeki faaliyetleri hakkında bilgi toplanır.
- **İş İlanları İncelemesi:** İş ilanları, kurumun kullandığı yazılım, donanım ve güvenlik sistemleri hakkında kritik bilgiler içerebilir. Örneğin, belirli bir güvenlik duvarı veya veritabanı yönetim sisteminden bahsediliyorsa, saldırganlar bu sistemlere özel saldırı vektörleri geliştirebilir.
- **Alan Adı ve DNS Bilgileri:** Whois sorgulamaları ve pasif DNS kayıtları üzerinden kurumun sahip olduğu IP adresleri, alt alan adları (subdomain) ve kullanılan hizmetler belirlenebilir.
- **Dark Web ve Hacked Database Araştırması:** Daha önce gerçekleştirilen saldırılar sonucu sızdırılan veri tabanları incelenerek hedef sistemin zayıf noktaları veya eski kullanıcı bilgileri elde edilebilir.

Aktif Keşif (Active Reconnaissance):

Aktif keşif, saldırganın doğrudan hedef sistem veya ağ ile etkileşime girerek daha detaylı bilgi toplamasını sağlar. Bu süreç, tespit edilme riskini artırsa da, daha spesifik ve güncel veriler elde edilmesini sağlar. Aktif keşif yöntemleri şunlardır:

- **Ağ Tarama (Network Scanning):** Nmap, Masscan gibi araçlar kullanılarak açık portlar, çalışan servisler ve kullanılan işletim sistemleri hakkında bilgi toplanır.
- **Zafiyet Tarama (Vulnerability Scanning):** Nessus, OpenVAS veya Burp Suite gibi araçlarla sistemlerdeki güvenlik açıkları belirlenmeye çalışılır.
- **E-posta ve Çalışan Bilgileri Toplama:** Harvester gibi OSINT araçları ile kuruma ait e-posta adresleri tespit edilerek hedefli phishing saldırıları için hazırlanabilir.
- **Sosyal Mühendislik Testleri:** Telefon görüşmeleri, sahte e-postalar veya kimlik avı (phishing) siteleri ile çalışanlardan hassas bilgilerin alınması hedeflenir.

Keşif Aşamasının Önemi

Bu aşama saldırının temelini oluşturduğu için, hedef organizasyonlar tarafından dikkatle takip edilmeli ve mümkün olduğunca erken tespit edilmelidir. **Keşif aşamasında saldırıyı önlemek için alınabilecek bazı önlemler şunlardır:**

- **Güvenlik farkındalık eğitimleri düzenlemek**, çalışanların sosyal mühendislik saldırılarına karşı daha bilinçli olmalarını sağlamak.
- **Ağ izleme sistemleri (IDS/IPS) kullanmak**, şüpheli tarama faaliyetlerini tespit etmek.
- **Siber istihbarat servislerini kullanarak**, dark web ve diğer platformlarda kuruma ait hassas verilerin olup olmadığını düzenli olarak kontrol etmek.
- **Minimal veri paylaşımı politikası benimsemek**, sosyal medya ve iş ilanlarında gereksiz teknik detayların paylaşılmasını engellemek.

Reconnaissance aşaması saldırganların hedef belirleme ve saldırı planlama sürecinde kritik bir rol oynar. Bu aşamanın erken fark edilmesi, saldırının gerçekleşmeden durdurulması için büyük bir avantaj sağlar.

2) Weaponization (Silahlanma)

Weaponization (Silahlanma) aşaması, saldırganın keşif aşamasında elde ettiği bilgiler doğrultusunda hedefe yönelik saldırı araçlarını hazırladığı kritik bir süreçtir. Bu aşamada, saldırganın belirlediği güvenlik açıklarını istismar etmek için gerekli olan **exploitler, payloadlar ve zararlı yazılımlar** hazırlanır. Hedef sistemlere sızmak ve kalıcı bir erişim sağlamak amacıyla çeşitli teknikler ve araçlar kullanılarak saldırının etkinliği artırılır.

Saldırganlar bu aşamada genellikle otomatikleştirilmiş araçlardan veya özel olarak hazırlanmış kötü amaçlı yazılımlardan faydalanarak saldırının başarılı olmasını sağlamaya çalışırlar. Silahlanma aşaması, genellikle hedef sisteme doğrudan bir saldırı içermediği için, tespit edilmesi zor olan aşamalardan biridir.

Weaponization Aşamasında Kullanılan Teknikler ve Yöntemler

1. Exploit Geliştirme ve Kullanımı

Keşif aşamasında belirlenen güvenlik açıkları, saldırının başarısını garanti altına almak için istismar edilir.

- **Metasploit, ExploitDB gibi araçlar ve veri tabanları** kullanılarak ilgili zafiyete uygun istismar kodları (exploitler) belirlenir veya geliştirilir.
- **Buffer Overflow, SQL Injection, Remote Code Execution (RCE), Cross-Site Scripting (XSS), Zero-Day Exploit gibi teknikler** hedef sistemin egeçirilmesini sağlar. Eğer hedef sistemde güncellenmemiş bir yazılım varsa, o yazılıma özel bir exploit kullanılarak saldırı gerçekleştirilir.

2. Payload Geliştirme ve Entegrasyonu

Bir güvenlik açığını istismar etmek tek başına yeterli değildir. **Payload**, saldırının tamamlanmasını sağlayan kötü amaçlı kod veya komut setidir.

- **Reverse Shell veya Bind Shell** kullanılarak saldırganın hedef sisteme uzaktan erişimi sağlanır.
- **Meterpreter, Cobalt Strike gibi gelişmiş frameworkler** kullanılarak daha karmaşık saldırı senaryoları uygulanabilir.
- Eğer saldırı sosyal mühendislik ile yapılacaksa, kötü amaçlı yazılım şifrelenerek antivirüs sistemlerinden kaçması sağlanabilir.

3. Kötü Amaçlı Yazılımlar (Malware) ve Dosya Manipülasyonu

Silahlanma sürecinde, saldırganlar zararlı yazılımlar kullanarak hedef sistemleri ele geçirmek için farklı yöntemler uygular:

- **Truva atları (Trojan):** Masum gibi görünen fakat zararlı kod içeren yazılımlar hedef sisteme bulaştırılır.
- **Makro Virüsler:** Microsoft Office veya PDF belgelerine gizlenen kötü amaçlı komut dosyalarıyla sistemlere sızılır.
- **Keylogger ve RAT (Remote Access Trojan):** Kullanıcı giriş bilgilerini veya sistemde yapılan işlemleri kaydetmek için zararlı yazılımlar kullanılır.

4. Sosyal Mühendislik İçin Kullanılan Teknikler

Saldırganlar, hedefi kandırmak ve kötü amaçlı dosyaları açmasını sağlamak için çeşitli sosyal mühendislik yöntemlerini kullanır.

- **Oltalama (Phishing) E-postaları:**
  - Sahte fatura, banka bildirimi veya güvenlik uyarısı gibi görünen kötü amaçlı e-postalar gönderilir.
  - Kurbanın merakını veya korkusunu tetikleyecek sosyal mühendislik içerikleri hazırlanır.
  - E-postalara zararlı bağlantılar veya kötü amaçlı ekler yerleştirilir.

- **Sahte Web Siteleri ve Kimlik Avı (Credential Harvesting):**
  - Kurumun resmi sitesine benzeyen sahte giriş panelleri oluşturularak kullanıcı bilgileri ele geçirilir.
  - Örneğin, sahte bir banka giriş sayfası oluşturularak kullanıcıların şifreleri çalınabilir.
- **USB Rubber Ducky ve Kötü Amaçlı Donanımlar:**
  - USB bellek gibi görünen kötü amaçlı cihazlar hedef sisteme takıldığında zararlı kod çalıştırabilir. RFID ve NFC istismarları ile fiziksel ortamlarda da sızma işlemi gerçekleştirilebilir.

Weaponization Aşamasında Savunma Yöntemleri

Weaponization aşamasında saldırgan doğrudan sisteme müdahale etmediği için tespit edilmesi zor olabilir. Ancak bazı güvenlik önlemleri alınarak bu aşamada saldırıyı engellemek mümkün olabilir:

- **Güvenlik Açıklarının Düzenli Olarak Yamalanması (Patch Management):** Güncel olmayan sistemler saldırganlar için kolay bir hedef haline gelir, bu nedenle işletim sistemleri ve yazılımlar sürekli olarak güncellenmelidir.
- **E-posta Güvenliği ve İçerik Filtreleme:** Oltalama saldırılarına karşı güvenlik duvarları ve spam filtreleri ile zararlı e-postalar engellenebilir.
- **Antivirüs ve EDR (Endpoint Detection and Response) Kullanımı:** Zararlı yazılımlar yüklenmeden önce tespit edilerek sistemde çalıştırılmaları engellenebilir.
- **Çalışanlara Sosyal Mühendislik Farkındalık Eğitimi Verilmesi:** Oltalama saldırıları ve zararlı eklere karşı bilinçli kullanıcılar, saldırganların başarılı olma ihtimalini düşürebilir.

Weaponization Sürecinin Önemi

Bu aşama, saldırının planlanmasının tamamlandığı ve hedef sistemin nasıl istismar edileceğinin belirlendiği kritik bir evredir. Eğer bu aşamada saldırganın faaliyetleri tespit edilirse, saldırının gerçekleşmesi engellenebilir. Güvenlik ekipleri, tehdit istihbaratı ve anomali analizlerini kullanarak saldırganların izlediği yöntemleri önceden belirleyip önlem alarak sistemlerini daha güvenli hale getirebilir.

3) Delivery (İletim)

Delivery (İletim) aşaması, saldırganın hazırladığı zararlı yazılımı, istismar edilecek aracı veya kötü amaçlı komutu hedefe ulaştırdığı kritik bir süreçtir. Bu aşamada, saldırının başarıya ulaşması için belirlenen yöntemler kullanılarak hedef sistemlere zararlı bileşenler iletilir. **Etkili bir saldırının gerçekleştirilebilmesi için, saldırganın hazırladığı kötü amaçlı içerik hedef kullanıcı, sistem veya ağ ile başarılı bir şekilde buluşturulmalıdır.**

Saldırganlar, bu aşamada genellikle **oltalama (phishing), zararlı e-postalar, sosyal medya tuzakları, kötü amaçlı USB cihazları, tünelleme teknikleri veya açık kaynaklı yazılımlar** gibi çeşitli yöntemler kullanarak hedef sisteme sızmayı amaçlar. Teslimat yöntemleri genellikle doğrudan bir saldırı içermez, bunun yerine kurbanın zararlı içeriği çalıştırmasını sağlamak için **ikna veya kandırma (sosyal mühendislik) teknikleri** devreye girer.

Delivery Aşamasında Kullanılan Saldırı Teknikleri ve Yöntemler

1. E-Posta ve Mesajlaşma Yoluyla Teslimat (Phishing & Spear Phishing)

- **Genel Oltalama (Phishing):**
    - Saldırgan, büyük bir kullanıcı kitlesine kötü amaçlı bağlantılar veya ekler içeren sahte e-postalar gönderir.
    - Kurbanların bir kısmının bu e-postalara tıklaması ve zararlı dosyayı indirmesiyle saldırı başlatılır.
    - Örneğin, **"Faturanızı görüntüleyin"** veya **"Şifreniz sıfırlandı"** gibi mesajlarla kullanıcıyı kandıran sahte bildirimler oluşturulabilir.
- **Hedefli Oltalama (Spear Phishing):**
    - Belirli bir birey veya kuruluş için özel olarak hazırlanmış, kişiye özel bilgiler içeren oltalama saldırılarıdır.
    - Sosyal mühendislik teknikleriyle kişinin güvenini kazanarak, sahte bir e-posta veya mesajın açılması sağlanır.
- **CEO Fraud (Business Email Compromise - BEC):**
    - Saldırganlar, şirket içindeki yöneticilerin kimliğine bürünerek çalışanlara sahte emirler veya talepler gönderebilir.

2. Zararlı Dosya ve Belgelerle Teslimat

- **Makro Virüsler ve PDF Zararlıları:**
    - Microsoft Word, Excel veya PDF dosyaları içerisine gömülen kötü amaçlı makrolar, kullanıcı tarafından açıldığında çalıştırılır.
    - **Makro içeren belgeler, hedef sistemde komut dosyaları çalıştırarak zararlı yazılımların indirilmesine ve çalıştırılmasına neden olabilir.**
- **İmza Taklidi Yapılmış Dosyalar:**
    - Dijital olarak güvenilir gibi görünen ancak aslında kötü amaçlı olan dosyalar, kullanıcıları kandırmak için kullanılabilir.
    - Örneğin, bir PDF veya EXE dosyası resmi bir şirket tarafından imzalanmış gibi gösterilebilir.

3. Sosyal Mühendislik ve Sosyal Ağlar Yoluyla Teslimat

- **Sosyal Medya Tuzağı (Social Engineering Traps):**
    - LinkedIn, Facebook, Twitter ve Instagram gibi platformlarda sahte profiller veya hesaplar oluşturularak hedef kişilerle etkileşim kurulabilir.
    - Örneğin, bir saldırgan sahte bir iş teklifi veya güvenilir bir firma gibi davranarak hedefi zararlı bir bağlantıya yönlendirebilir.
- **Sahte Destek ve Yardım Masası Saldırıları:**
    - Saldırganlar, güvenilir bir teknik destek ekibi gibi davranarak hedefi yönlendirir ve zararlı yazılımları yüklemesini sağlar.
    - Örneğin, sahte bir **"Bilgisayarınızı hızlandırmak için bu aracı yükleyin"** gibi mesajlar gönderilebilir.

4. USB ve Fiziksel Cihazlarla Teslimat

- **USB Rubber Ducky ve Kötü Amaçlı USB'ler:**
    - Kötü amaçlı bir USB belleğin kurban tarafından bilgisayara takılmasıyla otomatik olarak zararlı yazılımlar yüklenebilir.

- **Wi-Fi Pineapple veya Rogue Access Points (Sahte Kablosuz Ağlar):**
    - Saldırganlar, halka açık alanlarda güvenilir gibi görünen sahte Wi-Fi ağları oluşturarak kullanıcıların giriş bilgilerini ele geçirebilirler.
    - Kullanıcıların trafiği izlenerek şifreler, oturum bilgileri ve hassas veriler çalınabilir.

Delivery Aşamasında Savunma Yöntemleri

Saldırganlar bu aşamada hedefin güvenlik önlemlerini aşarak zararlı içeriği başarılı bir şekilde iletmeye çalışırlar. Ancak çeşitli önlemlerle bu aşama büyük ölçüde önlenebilir:

1. **Oltalama Saldırılarına Karşı Farkındalık Eğitimleri:**
    - Çalışanlar, sahte e-postalar, sahte giriş sayfaları ve sosyal mühendislik saldırılarını tanıyabilmelidir.
    - Özellikle "acil" veya "önemli" gibi görünen, şüpheli bağlantılar içeren e-postalar dikkatle incelenmelidir.
2. **E-posta ve Web Filtreleme:**
    - E-posta güvenlik sistemleri ve içerik filtreleme araçları kullanılarak, kötü amaçlı ekler ve sahte bağlantılar engellenebilir.
3. **Güvenlik Politikaları ve Cihaz Yönetimi:**
    - **USB cihazlarının kontrol edilmesi:** Şirket ağlarına bağlanabilecek cihazların kısıtlanması gereklidir.
    - **Uygulama beyaz listeleri:** Sadece güvenilir yazılımların çalıştırılmasına izin verilmelidir.
4. **Sandbox Teknolojileri ile Zararlı Yazılım Analizi:**
    - Gelen e-postalardaki şüpheli ekler, sandbox ortamlarında çalıştırılarak zararlı olup olmadığı tespit edilebilir.
5. **DNS ve IP Bloklama:**
    - Bilinen zararlı veya şüpheli web sitelerinin erişim blokları düzenli olarak güncellenmeli ve ağ trafiği analiz edilmelidir.

Delivery Sürecinin Önemi

Cyber Kill Chain modelindeki **Delivery aşaması**, saldırının hedef sistemlere ulaştırılmasını sağlayan en kritik adımlardan biridir. Eğer saldırganın teslimat yöntemleri güvenlik ekipleri tarafından önceden tespit edilir ve engellenirse, saldırının ilerleyen aşamalara ulaşması büyük ölçüde önlenebilir. **Bu nedenle, e-posta güvenliği, kullanıcı farkındalığı, içerik filtreleme ve ağ güvenliği çözümleri bu aşamada hayati önem taşır.**

4) Exploitation (Sömürme)

Exploitation (Sömürme) aşaması, saldırganın hedef sisteme zararlı içeriği başarıyla iletmesinin ardından, belirlenen güvenlik açığını istismar ederek sistem üzerinde yetkisiz erişim elde etmeye çalıştığı kritik bir adımdır. Bu aşamada, saldırganın daha önce keşif sürecinde belirlediği zafiyetler ve teslim ettiği kötü amaçlı bileşenler etkin hale getirilir. Temel amaç, hedef sistemde saldırganın kontrolü sağlayabileceği bir açık kapı oluşturmaktır.

Zafiyetin başarıyla sömürülmesi, hedef sistemde kötü amaçlı komutların yürütülmesi veya sistemde daha fazla ayrıcalık elde edilmesiyle sonuçlanabilir. Sömürme işlemi genellikle işletim sistemi, yazılımlar, web uygulamaları, ağ servisleri veya insan faktörüne bağlı olarak gerçekleşir. Bu aşamanın başarılı olması durumunda saldırgan, sisteme derinlemesine sızma imkânı bulur ve saldırının bir sonraki aşamalarına geçiş yapabilir.

Exploitation Aşamasında Kullanılan Yöntemler

1. Yazılım ve İşletim Sistemi Açıklarından Yararlanma (Software Vulnerabilities)

- **Zero-Day (Sıfırıncı Gün) Saldırıları:**
  - Henüz üretici firma tarafından keşfedilmemiş veya bir güvenlik yaması yayınlanmamış güvenlik açıklarının istismar edilmesidir.
  - Bu tür açıklar genellikle siber suç pazarlarında yüksek fiyatlarla satılır ve devlet destekli tehdit aktörleri tarafından kullanılır.
- **Güncellenmemiş Sistemlere Karşı Saldırılar:**
  - Eski ve güncellenmemiş yazılımlar, kötü amaçlı kodların kolayca çalıştırılmasına neden olabilir.
  - Örneğin, WannaCry fidye yazılımı, güncellenmemiş Windows sistemlerindeki SMB protokolündeki zafiyeti kullanarak yayıldı.
- **Web Uygulama Açıkları (OWASP Top 10):**
  - SQL Injection, Cross-Site Scripting (XSS), Remote Code Execution (RCE) gibi yaygın web güvenlik açıkları bu aşamada kullanılır.
  - Örneğin, bir XSS saldırısı ile kullanıcının oturum bilgileri çalınabilir ve sisteme yetkisiz erişim sağlanabilir.

2. İnsan Faktörüne Dayalı Zafiyetlerin Sömürülmesi (Social Engineering Exploits)

- **Kullanıcı Hatasından Yararlanma:**
  - Çalışanların farkında olmadan zararlı dosyaları açması veya şüpheli bağlantılara tıklaması, saldırının gerçekleşmesini sağlar.

    - Örneğin, Microsoft Office belgeleri içine gizlenmiş kötü amaçlı makrolar ile sistemde zararlı komutlar çalıştırılabilir.
- **Yetki Yükseltme (Privilege Escalation):**
    - Düşük yetkili bir kullanıcı hesabı ile sisteme giriş yapıldıktan sonra, daha fazla erişim hakkı elde etmek için güvenlik açıklarından yararlanılır.
    - Örneğin, sistemde çalışan bir süreçteki zafiyet kullanılarak admin/root yetkileri ele geçirilebilir.

3. Hafıza ve Çalışma Sürecine Yönelik Saldırılar (Memory Exploitation)

- **Buffer Overflow (Arabellek Taşması):**
    - Belirli bir yazılımın hafızada işleyeceği verinin sınırları aşılır ve zararlı kod yürütülmesi sağlanır.
    - Bu teknik, genellikle kritik sistem süreçlerine sızmak için kullanılır.
- **Heap Spraying & Return Oriented Programming (ROP):**
    - Sistem belleğinde zararlı kodu önceden belirlenmiş bir adrese yerleştirerek, uygulamanın yanlışlıkla bu kodu çalıştırmasını sağlamaya yönelik saldırılardır.

Exploitation Aşamasında Savunma Yöntemleri

Exploitation aşamasının başarılı olmasını engellemek için proaktif güvenlik önlemleri ve düzenli güvenlik testleri uygulanmalıdır.

1. **Sistem ve Yazılım Güncellemeleri:**
    - İşletim sistemleri, üçüncü taraf yazılımlar ve kritik güvenlik yamaları sürekli güncellenmelidir.
    - Otomatik güncelleme sistemleri ve yama yönetimi politikaları uygulanmalıdır.
2. **Güvenlik Açıklarını Önceden Tespit Etme (Vulnerability Management):**
    - Düzenli olarak sızma testleri (penetration testing) ve güvenlik taramaları yapılarak sistemdeki olası zafiyetler belirlenmelidir.
    - Saldırı simülasyonları ve Red Team tatbikatları ile organizasyonun savunma yetenekleri test edilmelidir.

3. **Davranış Analizi ve Anomali Tespiti:**
    - Ağ trafiği ve sistem aktiviteleri izlenerek, olağan dışı veya şüpheli davranışlar tespit edilmelidir.
    - Gelişmiş tehdit algılama sistemleri (IDS/IPS, EDR/XDR çözümleri) kullanılarak saldırılar daha erken aşamada engellenebilir.
4. **Memory Protection ve Exploit Mitigation Araçları:**
    - Data Execution Prevention (DEP) ve Address Space Layout Randomization (ASLR) gibi teknikler, bellek tabanlı sömürme saldırılarını engelleyebilir.

5. **Kullanıcı Farkındalığı Eğitimleri ve Sıfır Güven Modeli (Zero Trust Security):**
    - Çalışanlar, şüpheli e-postalar, sosyal mühendislik saldırıları ve güvenlik açıkları konusunda bilinçlendirilmelidir.
    - Yetkilendirme ve erişim denetimleri sıkılaştırılarak saldırganların lateral hareket etmesi önlenmelidir.

Exploitation Sürecinin Önemi

Cyber Kill Chain modelindeki Exploitation aşaması, saldırının hedef sistem üzerinde etkisini göstermeye başladığı kritik bir noktadır. Bu aşama başarılı olduğunda, saldırgan hedef sistem üzerinde kod çalıştırabilir ve kontrol sağlayabilir. Ancak, düzenli güvenlik yamaları, proaktif tehdit avcılığı ve siber farkındalık eğitimleri ile bu aşamanın gerçekleşme ihtimali büyük ölçüde azaltılabilir.

5) Installation (Yükleme)

Installation (Yükleme) aşaması, saldırganın hedef sistemi başarıyla sömürdükten sonra **kalıcı bir tehdit** oluşturmak için zararlı yazılımı yüklediği ve sistemde uzun süre boyunca gizli kalmasını sağlamaya çalıştığı kritik bir süreçtir. Bu aşamada saldırgan, sistem üzerinde kalıcılık elde etmek ve siber güvenlik önlemlerini atlatmak için çeşitli teknikler kullanır. **Hedef, sisteme tam erişim sağlamak ve saldırının ilerleyen aşamalarında saldırganın kontrolü elinde tutmasını garanti altına almaktır.**

Saldırgan, zararlı yazılımı yükledikten sonra sistemi yeniden başlatmalara, antivirüs taramalarına veya kullanıcı farkındalığına rağmen sistemde varlığını sürdürebilir. Bu aşama başarıyla gerçekleşirse, saldırgan **arka kapılar (backdoor), rootkitler, trojanlar veya kötü amaçlı botlar** gibi araçları kullanarak sistemde kalıcı bir sızma gerçekleştirebilir.

Installation Aşamasında Kullanılan Yöntemler

1. Kalıcılığı Sağlama Teknikleri (Persistence Mechanisms)

- **Boot-Time Persistence:**
    - Zararlı yazılımın her sistem açılışında otomatik olarak çalışmasını sağlamak için **Windows Registry**, **Startup Folder**, **Scheduled Tasks** veya **macOS Launch Agents** gibi yöntemler kullanılır.
    - **Örnek:** Saldırgan, zararlıyı **Windows Başlangıç Programları** arasına ekleyerek her açılışta çalışmasını sağlar.

- **System Service Manipulation:**
    - Zararlı yazılım, hedef sistemin hizmetleri (services) içerisine entegre edilerek arka planda sürekli çalışır.
    - **Örnek:** Windows'ta **svchost.exe** gibi meşru görünen hizmetlerin içerisine zararlı kod enjekte edilerek tespit edilmesi zorlaştırılır.
- **DLL Hijacking & Code Injection:**
    - Meşru bir uygulamanın, kötü amaçlı bir **DLL (Dynamic Link Library)** dosyasını yüklemesini sağlayarak sistemde uzun süre gizlenebilir.
    - **Örnek:** Windows uygulamalarının beklediği DLL dosyaları yerine, zararlı DLL'ler yerleştirilerek kod çalıştırılabilir.
- **BIOS / Firmware Persistence:**
    - Gelişmiş saldırılar, zararlıyı işletim sisteminden bağımsız olarak **BIOS, UEFI veya firmware** seviyesinde saklayarak, sistem formatlansa bile varlığını sürdürebilir.

2. Zararlı Yazılım Türleri ve Kullanım Amaçları

- **Backdoor (Arka Kapılar):**
    - Saldırganın sisteme uzaktan erişmesini sağlamak için açılan gizli giriş noktalarıdır.
    - Örneğin, Meterpreter veya Cobalt Strike gibi araçlar kullanılarak **uzaktan komut çalıştırma ve sistem üzerinde tam kontrol sağlanabilir.**
- **Rootkitler:**
    - Sistemin derinliklerine gizlenerek antivirüs ve güvenlik yazılımlarını atlatmaya yardımcı olan zararlılardır.
    - **Örnek:** Kernel seviyesinde çalışan rootkitler, işletim sisteminin çekirdeğine yerleşerek saldırganın tespit edilmesini engeller.

- **RATs (Remote Access Trojans):**
    - Saldırganın sisteme uzaktan erişmesini sağlayan trojan türüdür.
    - Örneğin, **njRAT, DarkComet, Remcos RAT** gibi zararlılar, saldırganın sistemi canlı olarak kontrol etmesine olanak tanır.
- **Botnet Enfeksiyonları:**
    - Ele geçirilen cihazlar, saldırgan tarafından yönetilen büyük botnet ağlarına dahil edilir.
    - **Örnek:** Mirai botneti, yüzbinlerce IoT cihazını kontrol altına alarak büyük ölçekli DDoS saldırıları gerçekleştirmiştir.

Installation Aşamasında Savunma Yöntemleri

1. **Uygulama ve Yazılım Denetimi (Application Whitelisting & Blacklisting):**
    - Kullanıcıların sadece güvenilir yazılımları yükleyebilmelerini sağlamak için **Uygulama Beyaz Listeleme (Whitelisting)** kullanılmalıdır.
    - **Şüpheli veya zararlı yazılımlar kara listeye (Blacklist) alınarak sistem tarafından çalıştırılması engellenebilir.**
2. **İleri Seviye Tehdit Algılama ve Davranış Analizi:**
    - **EDR (Endpoint Detection & Response) ve XDR (Extended Detection & Response)** çözümleri, şüpheli aktiviteleri tespit ederek zararlıyı daha yükleme aşamasında engelleyebilir.
    - Sistem üzerindeki anormal dosya değişiklikleri, ağ trafiğindeki olağandışı hareketlilik gibi belirtiler incelenmelidir.
3. **İmza Tabanlı ve Heuristik Zararlı Yazılım Analizi:**
    - Geleneksel antivirüs yazılımları, bilinen zararlıları tespit edebilir.
    - Ancak, polimorfik (kendini değiştirebilen) zararlılar için **heuristic ve davranışsal analiz** yöntemleri uygulanmalıdır.
4. **Yetkilendirme ve Kullanıcı Kontrolleri:**
    - Kullanıcıların yetkisiz uygulamalar yüklemesini engellemek için **minimum yetki prensibi (Least Privilege Principle)** uygulanmalıdır.
    - **Örneğin, normal kullanıcıların sistem dosyalarına erişim izni kısıtlanmalıdır.**
5. **Yama Yönetimi ve Yazılım Güncellemeleri:**
    - Saldırganların sömürebileceği açıklıkları kapatmak için sistem, uygulama ve üçüncü taraf yazılımlar düzenli olarak güncellenmelidir.
    - **Örneğin, WannaCry saldırısı, güncellenmemiş Windows sistemlerindeki SMB protokolü açığını kullanarak yayıldı.**
6. **Ağ Seviyesinde Zararlı Yazılım Dağıtımını Engelleme:**
    - **Firewall, IDS/IPS, Proxy ve DNS Filtreleme** gibi güvenlik çözümleri, zararlı yazılımların internet üzerinden indirilmesini engelleyebilir.
    - Bilinen kötü amaçlı domainler ve IP adresleri engellenerek saldırganların sistemle iletişim kurması önlenebilir.

Installation Sürecinin Önemi

Cyber Kill Chain modelinde **Installation aşaması, saldırının kalıcı hale gelmesini sağlayan en kritik noktalardan biridir.** Saldırgan, bu aşamayı başarıyla tamamlarsa sistem üzerinde sürekli bir erişime sahip olur ve gelecekteki saldırılarını planlamak için bir üs elde eder. **Ancak, sıkı güvenlik politikaları, ağ izleme sistemleri, güvenlik farkındalığı eğitimleri ve gelişmiş tehdit algılama yöntemleri ile bu aşama büyük ölçüde engellenebilir.**

6) Command And Control (Komuta & Kontrol)

Command and Control (C2 veya C&C) aşaması, saldırganın hedef sistemi başarıyla ele geçirmesinin ardından **uzaktan kontrol mekanizmasını oluşturduğu ve yönetmeye başladığı** kritik bir aşamadır. Saldırganın, ele geçirdiği sistemle sürekli bir bağlantı kurabilmesi ve komutlarını hedef sisteme iletebilmesi için bir **haberleşme kanalı (C2 kanalı)** oluşturulur.

Bu aşama sayesinde saldırgan, zararlı yazılımı yönlendirir, sistem üzerindeki dosyalara erişir, veri çalar, komutlar çalıştırır veya saldırının sonraki aşamalarını gerçekleştirir. **Eğer bir saldırgan, C2 bağlantısını sürdürebilirse, saldırı etkili bir şekilde yönetilebilir ve genişletilebilir.**

Command and Control Aşamasında Kullanılan Yöntemler

1. C2 Kanalı Türleri

Saldırganlar, sistem ile güvenli iletişim kurmak ve tespit edilmeden kalmak için farklı yöntemler kullanır:

- **HTTP/S C2 (Web Tabanlı Komut Kontrolü):**
  - Saldırgan, ele geçirilen sistem ile **HTTP veya HTTPS üzerinden haberleşerek** komutlar gönderir ve veri alır.
  - **Örnek:** Zararlı yazılım, saldırganın kontrol ettiği bir web sunucusuna belirli aralıklarla HTTP istekleri göndererek komutları çeker.
- **DNS Tünelleme (DNS Tunneling):**
  - Normalde web sitelerini çözümlerken kullanılan **DNS protokolü** üzerinden saldırgan, veri iletimi yapabilir.
  - **Örnek:** Ele geçirilen sistem, DNS sorguları gibi görünen mesajlarla saldırganın kontrol sunucusuyla iletişim kurar.
- **Peer-to-Peer (P2P) C2:**
  - Merkezi bir sunucuya bağlı kalmak yerine, ele geçirilen cihazlar birbirleriyle doğrudan haberleşerek komutları yayabilir.
  - **Örnek:** Saldırganın bir botnet ağı oluşturup, farklı sistemlerin birbirleriyle iletişim kurmasını sağlaması.
- **E-posta C2:**
  - Zararlı yazılım, **Gmail, Outlook veya Yandex gibi e-posta hizmetlerini kullanarak** saldırganla iletişim kurar.
  - **Örnek:** Ele geçirilen sistem, bir saldırgan tarafından yönetilen e-posta hesabına belirli aralıklarla mesaj göndererek talimatları alır.
- **Sosyal Medya ve Bulut Hizmetleri:**
  - Saldırgan, **Twitter, Telegram, Google Drive veya GitHub gibi platformları** bir C2 kanalı olarak kullanabilir.
  - **Örnek:** Bir zararlı yazılım, Twitter'da belirli bir hesaptan gönderilen gizli mesajları okuyarak saldırganın komutlarını alabilir.

2. C2 Bağlantısının Güçlendirilmesi ve Gizlenmesi

C2 bağlantısının keşfedilmemesi için saldırganlar aşağıdaki teknikleri kullanabilir.

- **Şifrelenmiş Trafik Kullanımı:**
  - HTTPS, AES veya RSA gibi şifreleme yöntemleriyle veri trafiği gizlenir.
  - **Örnek:** Komutlar şifrelenmiş paketler içinde gizlenerek tespit edilmesi zorlaştırılır.
- **Mimari Bölme (Proxy ve Relay Sunucuları):**
  - Trafik, doğrudan saldırganın kontrol ettiği bir sunucuya gitmek yerine, farklı sunucular üzerinden yönlendirilerek izlenmesi zorlaştırılır.
  - **Örnek:** TOR ağı veya VPN kullanarak saldırganın gerçek IP adresini gizlemesi.
- **Steganografi Kullanımı:**
  - Zararlı yazılım, **görseller, ses dosyaları veya videolar içerisine şifrelenmiş komutlar gömerek** C2 bağlantısını gizleyebilir.
  - **Örnek:** Bir saldırgan, Instagram'da paylaşılan bir görselin içine gizli bir mesaj gömerek zararlının bu mesajı okumasını sağlayabilir.

Command and Control Aşamasında Savunma Yöntemleri

1. Ağ Trafiği Analizi ve Anormal Davranış Tespiti

- **IDS/IPS (Intrusion Detection & Prevention Systems) kullanımı:**
  - Anormal trafik desenlerini ve C2 bağlantılarını tespit etmek için ağ izleme çözümleri kullanılmalıdır.
- **Örnek:** Normal internet trafiği HTTP/HTTPS kullanırken, sistemin beklenmedik şekilde **DNS üzerinden büyük veri transferleri yapması** anormal bir aktivite olarak değerlendirilebilir.

2. Güvenlik Duvarı ve Proxy Kullanımı

- Çıkış trafiğini kısıtlamak ve sadece yetkilendirilmiş servislerin dış dünyayla iletişim kurmasına izin vermek, C2 kanallarını engelleyebilir.
- **Örnek:** Bir güvenlik duvarı, yalnızca belirli IP'lere izin vererek bilinmeyen dış sunuculara bağlantıyı engelleyebilir.

3. C2 Alan Adlarının Kara Listeye Alınması

- Bilinen kötü amaçlı **C2 sunucularına ait alan adlarını** engellemek için sürekli güncellenen **Threat Intelligence** listeleri kullanılmalıdır.
- **Örnek:** Saldırganlar tarafından kullanılan Command and Control sunucularının IP adresleri IDS/IPS sistemlerine eklenerek engellenebilir.

4. EDR/XDR Kullanımı (Endpoint Detection and Response)

- **Gelişmiş uç nokta güvenlik çözümleri (EDR & XDR),** şüpheli bağlantıları ve anormal işlemleri tespit ederek saldırının ilerlemesini durdurabilir.
- **Örnek:** Bir zararlı yazılımın, beklenmeyen saatlerde dış sunuculara bağlantı kurmasını tespit ederek güvenlik ekibini uyarabilir.

5. Güvenlik Farkındalığı ve Çalışan Eğitimi

- Kullanıcılar, **sosyal mühendislik saldırıları, oltalama (phishing) e-postaları ve şüpheli bağlantılar** konusunda eğitilmelidir.
- **Örnek:** Bir çalışanın, sahte bir e-posta yoluyla zararlı bir dosya indirip çalıştırması, C2 bağlantısının kurulmasına sebep olabilir.

Command and Control Sürecinin Önemi

Command and Control aşaması, saldırganın sistem üzerindeki **nihai kontrolünü sağladığı ve saldırıyı yönettiği** aşamadır. Eğer bir saldırgan bu aşamayı başarıyla tamamlayabilirse:

- Sistemi uzaktan yönetebilir.
- Veri hırsızlığı gerçekleştirebilir.
- Fidye yazılımları çalıştırabilir.
- Yeni saldırılar için sistemin kullanılmasını sağlayabilir.

Ancak, **güçlü ağ izleme, güvenlik duvarı kuralları, anormal trafik tespiti ve güvenlik farkındalığı** gibi yöntemlerle bu aşama büyük ölçüde engellenebilir.

7) Actions On Objectives (Eylem)

Actions on Objectives, saldırının nihai hedefinin gerçekleştirildiği aşamadır. Saldırgan, sistem üzerindeki kontrolünü kullanarak önceden belirlediği **hedeflere ulaşmak** için çeşitli eylemler gerçekleştirir. Bu aşama, saldırının başarısına doğrudan etki eden en kritik evredir.

Bu aşamada saldırganın amacı **bilgi çalmak, verileri değiştirmek, sistemleri devre dışı bırakmak veya başka sistemlere saldırı düzenlemek** olabilir. Önceki tüm aşamalar, saldırganın bu noktaya ulaşmasını sağlamak için birer basamaktır. Eğer önceki aşamalarda saldırı tespit edilmez veya durdurulmazsa, saldırgan **hedefine ulaşmış olur ve kurum için ciddi zararlar ortaya çıkabilir.**

Actions on Objectives Aşamasında Gerçekleştirilen Eylemler

1. Veri Hırsızlığı (Data Exfiltration)

- Hedef sistemden hassas veriler ele geçirilir ve saldırganın kontrolündeki bir sunucuya aktarılır.
- **Örnek:** Şirketin müşteri bilgileri, finansal kayıtları veya hassas dokümanları dışarıya sızdırılabilir.

2. Sistem Manipülasyonu ve Sabotaj

- Saldırgan, sistemleri bozarak veya verileri değiştirerek operasyonları aksatabilir.
- **Örnek:** Bir bankanın veri tabanındaki hesap bakiyeleri değiştirilerek finansal sistem zarar görebilir.

3. Veri Şifreleme ve Fidye Yazılımı (Ransomware Attack)

- Saldırgan, sistemdeki verileri şifreleyerek erişimi engeller ve fidye talep eder.
- **Örnek:** Kurban, şifrelenen verileri geri almak için Bitcoin ile ödeme yapmak zorunda kalabilir.

4. İleri Seviye Kalıcılık (Advanced Persistence Threat - APT)

- Saldırgan, sistemde uzun süre fark edilmeden kalabilmek için çeşitli yöntemler kullanır.
- **Örnek:** Yeni kullanıcı hesapları oluşturulması, zararlı servislerin eklenmesi veya rootkitlerin yerleştirilmesi.

5. Diğer Sistemlere Sıçrama (Lateral Movement)

- Ele geçirilen sistem bir sıçrama noktası olarak kullanılarak **kurum içindeki diğer sistemlere saldırılar başlatılabilir.**
- **Örnek:** Bir çalışanın bilgisayarı ele geçirildikten sonra, kurum içindeki sunuculara erişim sağlanarak daha geniş çaplı saldırılar düzenlenebilir.

6. Botnet'e Katılım ve Daha Büyük Saldırılar İçin Kullanım

- Saldırgan, ele geçirilen sistemleri **bir botnet ağına dahil ederek DDoS saldırıları gibi daha büyük ölçekli saldırılarda kullanabilir.**
- **Örnek:** Bir kurumun sunucusu ele geçirilerek, başka bir hedefe büyük ölçekli DDoS saldırısı yapılabilir.

Actions on Objectives Aşamasında Savunma Yöntemleri

Bu aşamaya ulaşılmadan önce saldırının engellenmesi idealdir. Ancak saldırganın başarılı olması durumunda **zararı en aza indirmek ve hızlı müdahale etmek için aşağıdaki güvenlik önlemleri alınmalıdır:**

1. Veri Sızıntısı Önleme (DLP - Data Loss Prevention) Sistemleri Kullanımı

- Hassas verilerin sistem dışına çıkmasını önlemek için **DLP çözümleri** uygulanmalıdır.
- **Örnek:** Şirketin müşteri bilgilerini içeren dosyalar dışarıya kopyalanmaya çalışıldığında sistem bunu tespit edip engelleyebilir.

2. Güvenlik Olay Yönetimi (SIEM - Security Information and Event Management)

- Güvenlik olaylarının anlık olarak izlenmesi ve anormal aktivitelerin belirlenmesi sağlanmalıdır.
- **Örnek:** SIEM sistemleri, bir kullanıcının büyük miktarda veri aktardığını tespit edip uyarı verebilir.

3. Saldırı Sonrası Adli Bilişim ve Müdahale (Incident Response & Digital Forensics)

- Olay müdahale ekipleri, saldırının kaynağını tespit edip saldırının yayılmasını önlemelidir.
- **Örnek:** Bir saldırı gerçekleştiğinde sistem günlükleri (logs) incelenerek saldırının nasıl gerçekleştiği analiz edilebilir.

4. Yedekleme ve Kurtarma Planları

- Veri kaybını önlemek için düzenli olarak yedekleme yapılmalı ve **hızlı geri yükleme planları oluşturulmalıdır.**
- **Örnek:** Fidye yazılımı saldırısı sonrasında verilerin yedeklerden geri yüklenmesi sayesinde kurumun iş sürekliliği sağlanabilir.

5. Sıfır Güven Modeli (Zero Trust Architecture - ZTA)

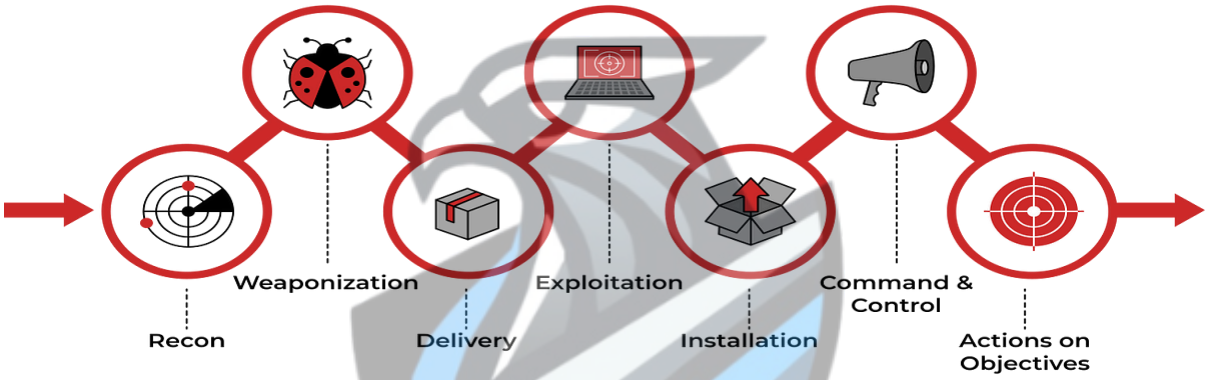
- Her kullanıcı ve cihazın sürekli doğrulama gerektirdiği **Zero Trust** modeli uygulanmalıdır.
- **Örnek:** Çalışanlar yalnızca ihtiyacı olan verilere erişebilir, her erişim sürekli kontrol edilir.

<u>Actions on Objectives Aşamasının Önemi</u>

Bu aşama, saldırganın hedeflediği **nihai amacı gerçekleştirdiği aşamadır.** Önceki aşamalarda saldırı engellenmezse, bu aşamada:

- Kurumun kritik verileri çalınabilir veya satılabilir.
- Operasyonel süreçler durabilir veya zarar görebilir.
- Güvenlik açıkları kullanılarak daha büyük saldırılar gerçekleştirilebilir.
- Kurum, finansal ve itibari kayıplarla karşı karşıya kalabilir.

Bu yüzden **her aşamada güçlü bir güvenlik önlemi almak ve saldırıları erken tespit edip engellemek kritik öneme sahiptir.**



CYBER KILL CHAIN KULLANARAK TEHDİTLERİ ÖNLEME

Siber ölüm zincirini kullanarak tehditleri önlemek, her aşamada uygun savunma mekanizmaları oluşturarak mümkündür. Model, güvenlik ekiplerinin saldırının farklı aşamalarında saldırganın faaliyetlerini tespit ederek durdurmasına yardımcı olur. Ağ trafiği izleme ve analiz araçları kullanarak saldırganların bilgi toplama faaliyetlerini tespit edebilirsiniz. Şüpheli etkinlikleri belirlemek için anormal trafiği izlemeniz yeterlidir. E-posta filtreleme ve kötü amaçlı yazılım analiz araçları, zararlı içerikleri tespit edip engellemek için kullanılabilir.

Kimlik avı eğitimleri ile çalışanlarınızı bilinçlendirebilirsiniz. Güvenlik duvarları ile ağ güvenliği çözümleri, zararlı yazılımların ve araçların hedef sisteme ulaşmasını engelleyebilir. Güvenlik yamaları ile güncellemeleri, sistemlerinizi bilinen güvenlik açıklarına karşı koruyabilir. Zararlı yazılımların tespit edilmesi için antivirüs ve anti-malware yazılımları da kullanabilirsiniz. Sistemlerinizdeki anormal etkinlikleri tespit etmek için uç nokta koruma çözümlerini kullanabilirsiniz. Ağ trafiğini izleyerek şüpheli komuta ile kontrol trafiğini tespit edip engelleyebilirsiniz. Veri kaybı önleme çözümleri, kritik verilerin izinsiz olarak dışarı sızmasının önüne geçebilir.

CYBER KILL CHAIN MODELİNE ÖRNEK SALDIRI

1) Reconnaissance (Keşif Aşaması)

Saldırgan, hedef şirket hakkında bilgi toplamak için çeşitli yöntemler kullanır:

- Açık kaynak istihbaratı (OSINT) ile LinkedIn, Twitter, Facebook gibi sosyal medya platformlarında çalışanlar hakkında bilgi toplar.
- Şirketin web sitesi ve iş ilanlarını analiz ederek kullanılan teknolojileri ve potansiyel güvenlik açıklarını belirler.
- Passive DNS ve WHOIS sorguları yaparak şirketin alan adı, IP adresleri ve ağ altyapısı hakkında bilgi edinir.
- Shodan ve Censys gibi araçlarla açık portlar ve çalışan hizmetleri tespit eder.

Bu aşamada saldırgan, bir çalışanın LinkedIn profili üzerinden e-posta adresini tespit eder.

2) Weaponization (Silahlanma Aşaması)

Saldırgan, keşif aşamasında elde ettiği bilgileri kullanarak hedefe uygun bir saldırı yöntemi belirler:

- Çalışanın Microsoft Outlook kullandığını belirleyerek bir Microsoft Word makro zafiyeti içeren zararlı dosya (malware) hazırlar.
- Dosyaya, açıldığında PowerShell üzerinden ters bağlantı başlatan bir backdoor ekler.

Zararlı dosya, oltalama saldırısında kullanılmak üzere hazır hale getirilmiştir.

3) Delivery (İletim Aşaması)

Saldırgan, zararlı dosyayı hedefe ulaştırmak için sosyal mühendislik yöntemleri kullanır:

- Çalışana, gerçeğe çok benzeyen bir sahte e-posta gönderir.
    - Konu: “Acil! Güncellenmiş Finans Raporları”
    - Gönderen: finance@bigcompany.com
    - Ekli dosya: Finance_Report.docm
- E-posta içeriğinde, "Bu belgedeki verileri görebilmek için içeriği etkinleştirmeniz gerekmektedir." şeklinde bir mesaj bulunur.
- Çalışan dosyayı açarak makroyu etkinleştirir ve zararlı kod çalıştırılmış olur.

Bu aşamada saldırganın zararlı yazılımı hedef sisteme ulaştırılmış olur.

4) Exploitation (Sömürme Aşaması)

- Çalışan, Finance_Report.docm dosyasını açar ve makroyu etkinleştirir.
- Zararlı makro, PowerShell üzerinden ters bağlantı başlatır ve saldırganın kontrolündeki bir sunucuya bağlantı kurar.
- Saldırgan, çalışanın bilgisayarına uzaktan erişim sağlar.

Bu aşamada saldırgan, sistemde zararlı kod çalıştırabilme yetkisi elde etmiştir.

5) Installation (Yükleme Aşaması)

Saldırgan, sistemde kalıcı kalmak ve fark edilmemek için çeşitli yöntemler uygular:

- Sistem açıldığında otomatik çalışacak bir PowerShell betiği oluşturur.
- Windows görev zamanlayıcısını (Task Scheduler) kullanarak ters bağlantıyı düzenli aralıklarla yeniden başlatır.
- Mimikatz aracıyla sistemdeki kimlik bilgilerini çalar ve yönetici yetkileri kazanır.

Bu aşamada saldırgan, sistem üzerinde kalıcılık sağlamıştır.

6) Command and Control (Komuta & Kontrol Aşaması)

Saldırgan, ele geçirilen sistem üzerinden komutlarını çalıştırmaya başlar:

- Zararlı yazılım, saldırganın uzaktaki komuta ve kontrol (C2) sunucusuna bağlanarak yeni komutlar alır.
- Saldırgan, ağ üzerindeki diğer sistemleri keşfetmek için çeşitli komutlar çalıştırır.
- Ele geçirilen sistem üzerinden şirket ağına yayılmak için ek saldırılar gerçekleştirir.

Bu aşamada saldırgan, sistemi uzaktan kontrol etmeye başlamıştır.

7) Actions on Objectives (Eylem Aşaması)

Saldırgan, nihai amacını gerçekleştirmeye başlar:

- Çalışanların müşteri bilgilerini içeren Excel dosyalarını toplar ve kendi sunucusuna yükler. Fidye yazılımı saldırısı başlatarak şirketin kritik dosyalarını şifreler ve fidye talebinde bulunur.

SONUÇ

Bu raporda Cyber Kill Chain modeli detaylı bir şekilde incelenmiş ve siber saldırıların yaşam döngüsü üzerine kapsamlı bir anlayış geliştirilmiştir. Cyber Kill Chain'in aşamaları olan **Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control (C2) ve Actions on Objectives** aşamaları ele alınarak, bir saldırının hangi noktada olduğunu analiz etme becerisi kazanılmıştır.

Ayrıca, bu modelin **SOC analistleri** için nasıl bir rehber niteliği taşıdığı, olayları tespit etme ve müdahale süreçlerini nasıl desteklediği açıklanmıştır. Gerçek dünya saldırı senaryoları incelenerek, bu bilgilerin **proaktif savunma mekanizmaları geliştirmede nasıl kullanılabileceği** konusunda yetkinlik kazanılmıştır.

Sonuç olarak, Cyber Kill Chain modeli siber tehditlerle mücadelede **stratejik bir bakış açısı** kazandırmakta ve siber güvenlik uzmanlarının saldırıları erken aşamada tespit edip engellemesine yardımcı olmaktadır. Bu çerçevede, modelin doğru bir şekilde anlaşılması ve uygulanması, siber güvenlik alanında etkili savunma stratejileri oluşturmak için kritik bir öneme sahiptir.

KAYNAKÇA

- https://berqnet.com/blog/cyber-kill-chain
- https://docs.yavuzlar.org/web-guvenligi/cyber-kill-chain
- https://www.splunk.com/en_us/blog/learn/cyber-kill-chains.html
- https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
- https://www.gaissecurity.com/blog/cyber-kill-chain-bir-siber-saldirinin-yasam-dongusu
- https://www.microsoft.com/en-us/security/business/security-101/what-is-cyber-kill-chain