CYBER KILL CHAIN

HAZIRLAYAN: UMUT EMRE KARACAER
TARİH: 07.02.2025

İÇERİK

GİRİŞ:

Siber güvenlik dünyasında saldırıları daha iyi anlamak, tespit etmek ve engellemek amacıyla çeşitli modeller geliştirilmiştir. Bu modellerden biri olan **Cyber Kill Chain**, Lockheed Martin tarafından ortaya konulmuş ve siber saldırıların aşamalarını sistematik bir şekilde analiz ederek güvenlik önlemlerinin etkin bir şekilde planlanmasına olanak sağlamıştır.

Askeri terminolojiden esinlenerek oluşturulan bu model, saldırganların hedef sistemlere ulaşmak için izledikleri adımları belirlemekte ve her adımda savunma stratejileri geliştirilmesini önermektedir. Bu rapor, **Cyber Kill Chain** modelinin aşamalarını, savunma mekanizmalarını ve SOC analizi ile ilişkisini inceleyerek siber güvenlikteki kritik rolünü ele almaktadır.

CYBER KILL CHAIN NEDİR?

Siber saldırıları analiz edebilmek amacıyla çeşitli modellerden birisi olan ve Locheed Martin firması tarafından geliştirilen cyber kill chain keşif aşamasından saldırı aşamasına kadar tanımlayan ve bu saldırıyı gerçekleştirmek veya önlemek amacıyla oluşturulan 7 aşamalı bir modeldir.

Siber güvenlik modeli, siber saldırıların aşamalarını belirleyerek savunma stratejilerini daha etkin şekilde planlamaya yardımcı olur. Cyber Kill Chain, askeri terminolojiden esinlenerek siber saldırıları çeşitli aşamalarda tanımlayarak her aşamada saldırganın faaliyetlerini tespit edip durdurmak için savunma mekanizmaları oluşturulmasını önerir. Cyber Kill Chain, güvenlik ekiplerinin saldırıları daha iyi anlamalarına, önlemelerine veya karşılık vermelerine yardımcı olur.

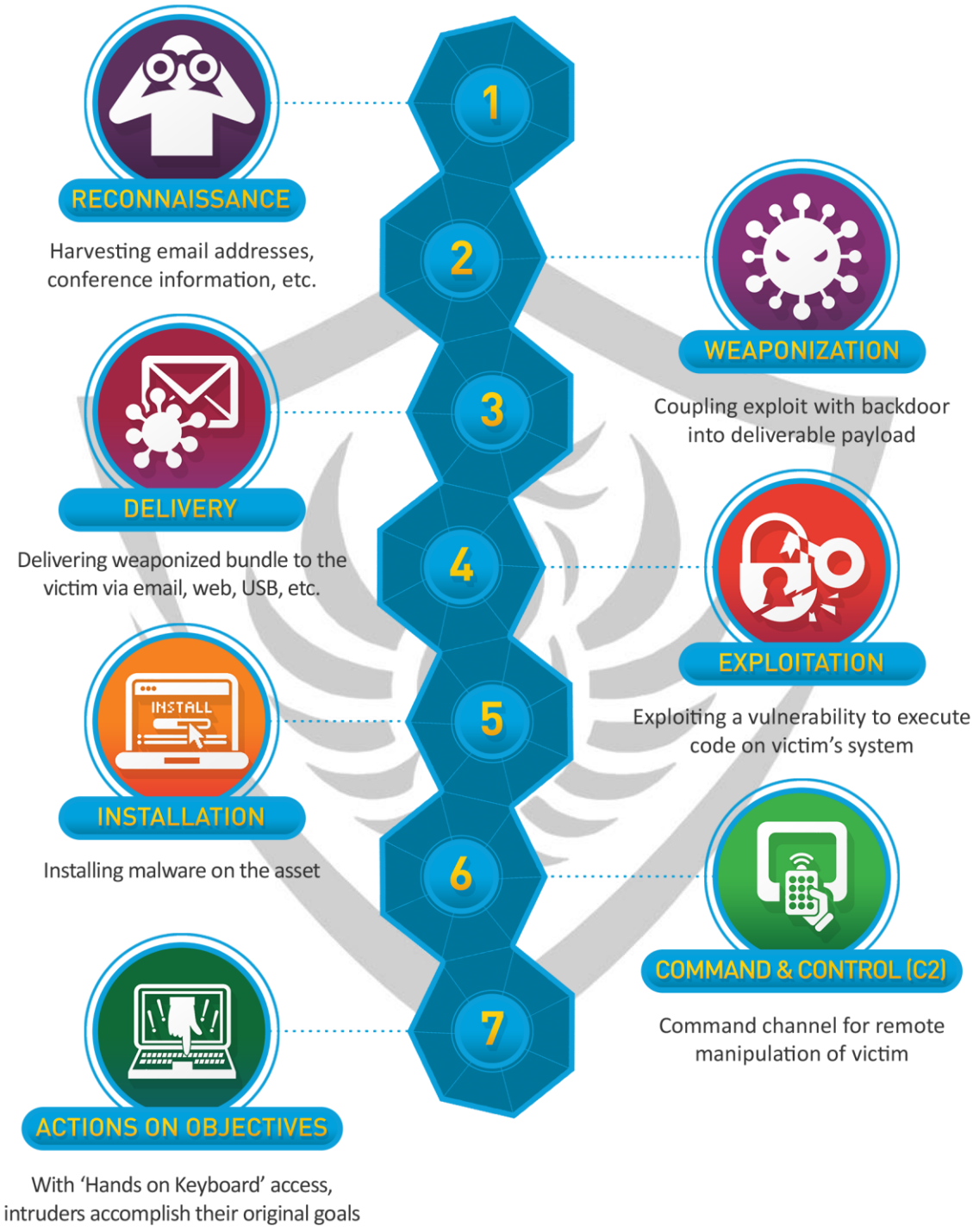
CYBER KILL CHAIN NASIL ÇALIŞIR?

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

CYBER KILL CHAIN AŞAMALARI:

Cyber Kill Chain son derece dikkatle planlanmış aşamalardan oluşur. Cyber Kill Chain aşamaları şu şekilde sıralanabilir:

1. **Reconnaissance (Keşif)**
2. **Weaponization (Silahlanma)**
3. **Delivery (İletme)**
4. **Exploitation (Sömürme)**
5. **Installation (Yükleme)**
6. **Command and control,c2 (Komuata Kontrol)**
7. **Actions on objectives (Eylem)**


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

Reconnaissance (Keşif):

Saldırı gerçekleşmeden veya bir istismar yaratılmadan önce keşif ve bilgi toplama aşamasıdır. Saldıran taraf; hedef sistem veya sistemler üzerinde çeşitli taramalar gerçekleştirerek zafiyetleri tespit etmeye çalışır ayrıca çalışanların isimleri, görevleri, e-mail adresleri, ip adresleri, ağ haritası çıkarma gibi eylemleri aktif ve pasif bilgi toplama araçlarıyla yapabildiği gibi, iş ilanları, linkedln, twitter, facebook, instagram gibi sosyal medya aracılığıyla hedef hakkında sosyal mühendislik yöntemleri ile bilgiler toplayabilir.

- **Pasif Bilgi Toplama:**
  Hedef ile direkt olarak temasa geçilmeden bilgi toplama çeşitidir. (Shodan vb)

- **Aktif Bilgi Toplama:**
  Hedef ile direkt olarak temasa geçilen bilgi toplama çeşitidir. (Port scan vb.)

Weaponization (Silahlanma):

Keşif sırasında bulunan zafiyetlerin sömürülmesi için kullanılacak yöntemlerin belirlenmesi ve uygun araçları hazırlama olarak tanımlanan aşamadır. Bu aşamada zafiyete uygun exploitler, zafiyetin istismar edilmesi için kullanılabilecek payloadlar olabileceği gibi zararlı dosyalar ve dokümanlar, oltalama saldırısında kullanılabilecek sahte epostalar gibi birçok yöntem kullanılarak sızma işlemi gerçekleştirilebilir.

Delivery (İletme):

Hazırlanan zararlının ve belirlenen yöntemle hedefe iletilmesi bu aşamadadır. Çeşitli açık kaynak kodlu yazılımlar, phishing, sosyal networkler veya tünellemeler gibi yöntemler kullanılabileceği gibi, güvenlik olarak çalışanların sosyal mühendisliklere veya phishing saldırılarına karşı farkındalıkları, çalışanların hangi donanımların kurum ağına bağlanabildiği veya bağlanamadığı konusunda bilgilendirmesi, bilinen zararlı veya şüpheli web sitelerinin erişim bloklarının kontrol edilmesi bu aşamayı önleyebilir.

Exploitation (Sömürme):

Oluşturulan zararlı ve belirlenen atak vektörünü kullanarak hedefin zafiyetinin sömürüldüğü aşamadır. Exploit hazırlanıp hedefe iletildikten sonra bu aşamada zararlı kod çalıştırılır. Bunu önlemek amacıyla yazılımlar ne sıklıkla güncellendiği , sistemdeki zafiyetlerin tespit edilmesi için güvenlik denetimleri yapılıp yapılmadığı kontrol edilebilir.

Installation (Yükleme):

Hedefin sömürülmesi ardından, kalıcı bir tehdit haline gelmek, güvenlik sisteminin ötesinde sistem başarılı bir şekilde kontrol edilebilmesi için hedefe asıl zararlı yazılımın indirilmesi, zararlı yazılımın sistemde kalacağı süreyi mümkün olduğunca arttırmayı hedefleyen aşamadır. Sistemde çalışan bilgisayarlarla yüklenen yazılımların denetlenmesi, kullanıcıların istedikleri yazılımları bilgisayarlara yükleyebilirlikleri, whitelisting ve blacklisting oluşturma bu aşamayı önleyebilir.

Command and Control, c&c (Komuata Kontrol):

Sisteme yerleşmiş olan zararlının çalışması uzaktan kontrol edilebildiği ve sistemin ele geçirildiği aşamadır. Bu aşama için saldırıyı engelelyebilircek firewall ve ips'in devrede olup olmadığı iyi konfigüre edilip edilmediği ve güvenlik cihazlarının monitör edilebiliriliği bu aşamayı aksatmak için önemli unsur taşımakta.

Actions on objectives (Eylem):

Bütün aşamaları gerçekleştiren saldırgan kuruma erişim sağlamıştır ve bu aşamada, veri çalma, veri değiştirme , veri silme , veri şifreleme, sisteme zarar verme gibi eylemleri gerçekleştirebilir. Önlem olarak iç ağdan dışarı yapılan veri akışı sınırlandırılması, sadece bilinen sunuculara veri akışını sağlama (whitelisting) oluşturulduğunda saldırı engellenebilir. Bu süreçte tehdit altındaki verilerin yedeklerinin önceden alınması, bir sistem devre dışı kaldığında hizmet verebilecek yedek sistemin olması bu saldırının etkilerini azaltabilir.

CYBER KILL CHAIN KULLANARAK TEHDİTLERİ ÖNLEME:

Cyber Kill Chain modelini 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 VE DİĞER GÜVENLİK MODELLERİ:

Cyber Kill Chain, Lockheed Martin tarafından geliştirilmiş bir siber güvenlik modeli olarak siber saldırıların aşamalarını anlayıp tespit ederek durdurmak için kullanılır. Cyber Kill Chain modeli, saldırganların faaliyetlerini keşif, silahlandırma, teslimat, istismar, kurulum, komuta üzerinde faaliyetler olmak üzere yedi aşamaya ayırır. Bu modelin amacı, saldırganların her aşamada faaliyetlerini durdurarak saldırıyı önlemektir. Diğer popüler güvenlik modelleri arasında MITRE ATT&CK ve NIST Cybersecurity Framework bulunur. MITRE ATT&CK, çeşitli saldırı teknikleri ile taktiklerini sistematik olarak kataloglayarak savunma stratejilerini geliştirmeye yardımcı olur. NIST Cybersecurity Framework ise siber güvenliği geliştirmek için beş temel fonksiyona dayalı yaklaşım sunar. Her iki model de Cyber Kill Chain gibi kuruluşların güvenlik duruşlarını değerlendirip iyileştirmelerine yardımcı olur.

CYBER KILL CHAIN İLE İLGİLİ EN İYİ UYGULAMALAR:

Cyber Kill Chain modelini etkin şekilde kullanmak için en iyi uygulamalardan bazıları şunlardır:

Proaktif Tehdit Avcılığı (Proactive Threat Hunting): Saldırıların erken aşamalarında keşif faaliyetlerini tespit etmek için ağ ve uç nokta güvenliği çözümlerini kullanabilirsiniz.

Güvenlik Farkındalığı Eğitimleri (Security Awareness Training): Çalışanlara kimlik avı gibi sosyal mühendislik saldırılarını tanımaları için düzenli eğitimler vermeniz tavsiye edilir.

Olay Müdahale Planları (Incident Response Plans): Siber saldırılara hızlı ve etkili bir şekilde yanıt vermek için olay müdahale planları oluşturup bu planları düzenli olarak test etmelisiniz.

Ağ Segmentasyonu (Network Segmentation): Saldırganların hareket alanını sınırlayıp kritik sistemleri korumak için ağ segmentasyonu uygulayabilirsiniz.

Tehdit İstihbaratı (Threat Intelligence): Güncel tehdit istihbaratı kaynaklarını kullanarak saldırganların yeni teknik ve taktiklerini öğrenip savunma stratejilerinizi buna göre güncellemelisiniz.

CYBER KILL CHAIN VE SOC ANALİSTİ:

SOC analistleri, Cyber Kill Chain'i kullanarak saldırıların yaşam döngüsünün her aşamasında tespit ve müdahale stratejileri geliştirebilirler. Bu model, SOC analistlerine olayların hangi aşamada olduğunu anlamaları ve hızlı müdahale etmeleri için bir rehber sunar. Örneğin, "Reconnaissance" aşamasında anormal bilgi toplama faaliyetleri tespit edilip engellenebilirken, "Delivery" aşamasında zararlı dosyaların analiz edilmesi gerekebilir. Cyber Kill Chain sayesinde saldırıların erken tespiti, daha az zarar ve etkin savunma stratejileri ile sonuçlanır. Ayrıca, her aşamanın analiz edilmesi, saldırı sonrasında adli bilişim çalışmalarına da katkı sağlar.

SONUÇ:

Cyber Kill Chain modeli, güvenlik ekiplerine saldırı yaşam döngüsünü anlamak ve her aşamada uygun savunma mekanizmaları oluşturmak için önemli bir yapı sunmaktadır. Bu modelin etkin kullanımı, erken tespit ve müdahale ile saldırıların engellenmesini sağlar.

Raporda ele alınan aşamalar, saldırganların faaliyetlerini her adımda analiz etmenin ne denli önemli olduğunu göstermektedir. SOC analistleri için Cyber Kill Chain modeli, hem saldırılara proaktif olarak müdahale etmeyi hem de olay sonrası adli analiz süreçlerini desteklemeyi mümkün kılar.

Sonuç olarak, Cyber Kill Chain'in sistematik yaklaşımı, siber güvenlik stratejilerinin geliştirilmesinde ve tehditlere karşı dirençli bir savunma mekanizması oluşturulmasında önemli bir rehber olarak kabul edilmektedir.

KAYNAKÇA:

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://berqnet.com/blog/cyber-kill-chain
https://bbsteknoloji.com/cyber-kill-chain-nedir/
https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/cyber-kill-chain/
https://www.microsoft.com/en-us/security/business/security-101/what-is-cyber-kill-chain