CYBER KILL CHAIN

HAZIRLAYAN

ADI: AYŞE

SOYADI: BALCI

TARİH:05/02/2025

İçindekiler Tablosu

GİRİŞ

Siber saldırılar günümüzde giderek daha karmaşık hale gelirken, savunma stratejileri de aynı oranda gelişmek zorundadır. Siber Ölüm Zinciri (Cyber Kill Chain), saldırı süreçlerini anlamak ve etkili savunma mekanizmaları oluşturmak için kullanılan bir modeldir. Lockheed Martin tarafından geliştirilen bu model, bir saldırının aşamalarını sistematik bir şekilde analiz ederek, tehditlerin tespit edilmesine ve önlenmesine yardımcı olur.

Bu dökümanda, modelin aşamalarını inceleyerek saldırganların yöntemlerini ve güvenlik ekiplerinin alabileceği önlemleri ele alacağız. Ayrıca MITRE ATT&CK ile karşılaştırmalar yaparak farklı güvenlik yaklaşımlarını değerlendirecek ve gerçek saldırı senaryoları üzerinden modelin nasıl uygulandığını göstereceğiz.

CYBER KILL CHAIN NEDİR?

Siber Ölüm Zinciri (Cyber Kill Chain), ilk olarak askeri alanda ortaya çıkan ve bir siber saldırının aşamalarını tanımlayarak önlem almak için gerekli strateji ve taktiklerin geliştirilmesine yönelik bir metodolojidir. Bu model, saldırganın hedefe ulaşmak için geçmesi gereken aşamaları belirler ve siber savunmada saldırganın perspektifinden düşünerek sistemlerin güvenliğini artırmaya yardımcı olur.

Siber ölüm zinciri, siber olaylara müdahale ekipleri(SOME) ve zararlı yazılım analistlerinin işbirliği yapması için bir çerçeve sunar. Saldırganın izleyeceği yolları ve yöntemleri detaylı inceleyerek potansiyel açıklar hakkında bilgi sağlar. Bu metodoloji, siber saldırıların karmaşık yapısını basitleştirerek analiz etmeyi sağlar. Lockheed Martin tarafından geliştirilmiş olup, bilgi toplama aşamasından sızma eylemine kadar tüm süreçleri kapsamaktadır.

Şekil 1 Cyber kill chain

SİBER GÜVENLİKTE CYBER KILL CHAIN

Cyber kill chain, siber güvenlikte bir siber saldırının aşamalarını anlamak için kullanılan önemli bir kavramdır. Saldırıyı keşif aşamasından nihai hedefe kadar belirgin aşamalara ayırarak, organizasyonlara tehditlerle başa çıkmak için yapılandırılmış bir çerçeve sunar.

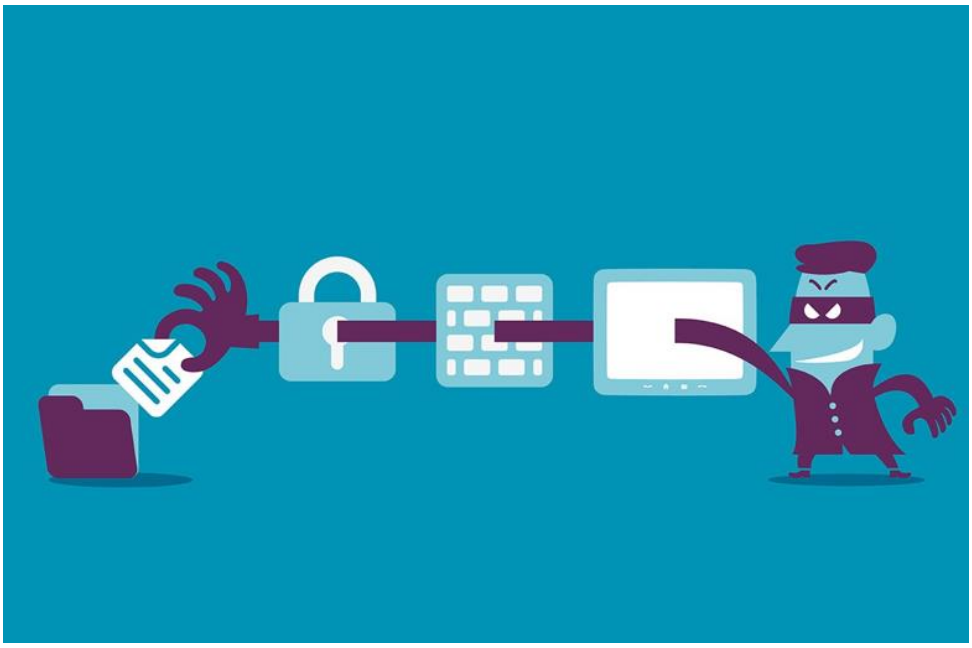
Siber Ölüm Zinciri'ni anlamanın önemli nedenleri arasında aktif savunma, olay yanıtı, kaynak tahsisi ve tehdit istihbaratı yer alır. Saldırının erken aşamalarında tehdit göstergelerini tanımak, aktif olarak önlemler almayı sağlar. Herhangi bir saldırı durumunda saldırı aşaması belirlenerek önlem almada yardımcı olur. Saldırı anında gerçekleşen aşamaların savunma düzeyleri belirlenerek önlem şekli buna göre belirlenebilir. Ayrıca geçmiş saldırılar analiz edilerek saldırganların taktikleri hakkında çıkarımlar yapılabilir.

CYBER KILL CHAIN AŞAMALARI NELERDİR?

Cyber Kill Chain'in temelinde, siber saldırıların genellikle aşamalar halinde gerçekleştiği ve her aşamada oluşturulan kontrollerle bu saldırıların engellenebileceği fikri yatmaktadır. Bu fikre dayanarak 7 adımdan oluşur. Bu adımlar:

KEŞİF(RECONNAISSANCE):

Siber Ölüm Zinciri'nin ilk aşaması olan keşif aşaması, saldırganın hedef hakkında bilgi topladığı süreçtir. Bu aşamada, teknik ve teknik olmayan yöntemlerle sistemlere giriş için hassas noktalar belirlenir. Aktif ve Pasif bilgi toplama yöntemleri kullanılarak, hedef firmanın IP adresleri, çalışan bilgileri, güvenlik sistemleri ve ifşa olmuş parolalar tespit edilir. Sosyal mühendisli teknikleriyle LinkedIn, Instagram gibi sosyal medya platformları incelenebilir ve hatta çöplerden bilgi toplama (Dumpster Diving) gibi yöntemler uygulanabilir. Süreç, genellikle pasif saldırı olarak değerlendirilir ve esas amacı hedefin güvenlik yapısını anlamak ve bir saldırı profili çıkarmaktır.



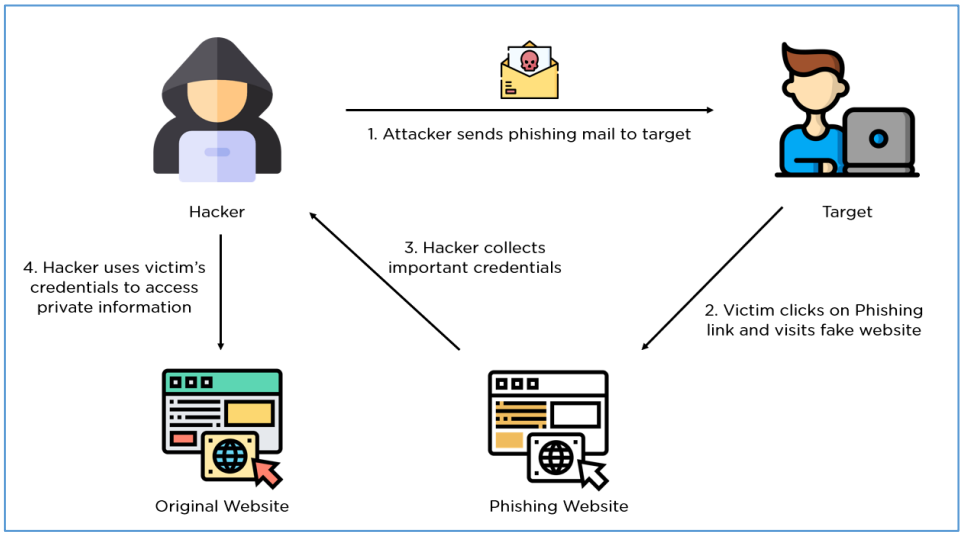
Şekil 2 Keşif aşaması temsili

Pasif Bilgi Toplamada; Hedef sistem hakkında bilgi toplanırken, sunucu ile direkt iletişime geçmeden yapılan bilgi toplama yöntemidir. Pasif bilgi toplama araçları olarak, whois sorguları, archieve.org, theHarvester, recon-ng, maltego, shodan, sosyal medya platformları kullanılabilir.

Aktif Bilgi Toplamada; Hedef sistem hakkında bilgi toplanırken sunucu veya sistem ile direkt olarak iletişime geçilerek yapılan bilgi toplama yöntemidir. Burada ise, nmap, dirb, dmitry gibi araçlar kullanılabilir.

SİLAHLANMA (WEAPONIZATION):
Keşif aşamasında elde edilen bilgiler doğrultusunda saldırgan, henüz saldırıyı gerçekleştirmeden sistemdeki zafiyetlerin sömürülmesi için izlemesi gereken yolu belirler ve buna göre hazırlıklarını yapar. Bu süreçte, işletim sistemindeki veya internette açık bir uygulamadaki eksik yamalar (patch), açık olmaması gereken portlar veya güvenlik açıkları analiz edilir. Saldırgan, keşfedilen güvenlik açıklarına özel olarak hazırlanmış zararlı yazılımlar (malware) geliştirebilir veya zararlı web siteleri oluşturabilir. Bu aşama, saldırganın kullanacağı araç ve yöntemleri belirlediği aşamadır. Saldırganın saldırı gücü bu aşamada artar ve elde edilen güvenlik açıklarını istismar etmek için exploitler, payloadlar, zararlı dosyalar, oltalama e-postaları gibi yöntemler üzerinde çalışılır. Sürecin tamamlanmasıyla birlikte saldırgan, hedef sisteme sızmak için phishing gibi tekniklerle hedef sisteme sızmaya çalışır.

İLETME (DELIVERY):
Cyber Kill Chain üçüncü aşaması, saldırganın zararlısını hedef sisteme ilettiği aşamadır. Phishing delivery aşamasında kullanılan en yaygın yöntem olup, zararlı genellikle e-posta ekleri veya USB gibi taşınabilir medyalar aracılığıyla hedefe ulaştırılır. 2018 Verizon Veri İhlali Raporu, ağ saldırılarının büyük ölçüde çalışanlara yönelik phishing saldırılarından kaynaklandığını göstermektedir. Spear Phishing, hedef odaklı bir saldırı türü olup, Microsoft Word veya PDF belgeleri gibi ekler içerebilir. Dökümanlar içerisinde zararlı kodlar gömülür ve kurum ağına ilk erişimi sağlayabilir. Saldırgan, bilgi toplama aşamasında belirlediği en zayıf halkayı hedef alarak, sosyal mühendislik ve tünelleme gibi yöntemlerle saldırısını gerçekleştirir.



Şekil 3 Phishing temsili

SÖMÜRME (EXPLOTATION):

Explotation, saldırganın hedef sistemde keşfettiği güvenlik açıklarını istismar ederek zararlı yazılımını çalıştırdığı süreçtir. Bu aşamada, daha önce belirlenen zafiyetler kullanılarak sisteme yetkisiz erişim sağlanır. Saldırgan, hazırladığı exploit(istismar kodu) ve belirlenen atak vektörünü kullanarak, hedef sistemin güvenlik açıklarını sömürür ve zararlı yazılımını çalıştırır.

Bu aşamada saldırgan, APT (Gelişmiş Kalıcı Tehdit) kötü amaçlı yazılımını uzaktan veya otomatik olarak yürütür ve hedeflenen bilgi sistemine erişim sağlar. Exploit'in başarılı olması durumunda, saldırgan yetki yükseltme (Privilege Escalation) tekniklerini kullanarak sistemdeki erişim seviyesini artırabilir.

YÜKLEME (INSTALLATION):

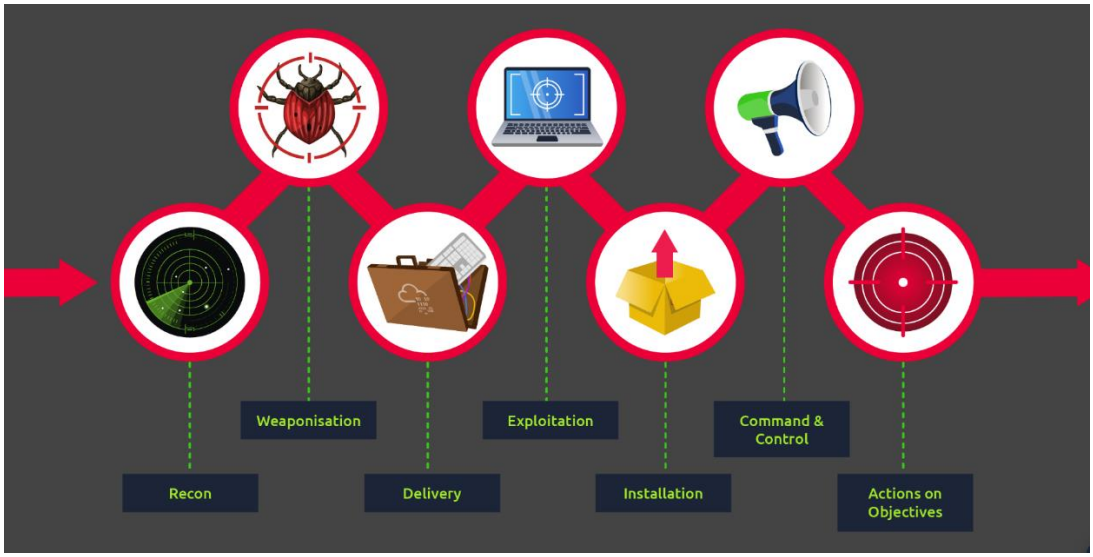
Hedefin sömürülmesi ardından, kalıcı bir tehdit haline gelmek, güvenlik sisteminin ötesinde sistem başarılı bir şekilde kontrol edilebilmesi için hedefe asıl zararlı yazılımın indirilmesi, zararlı yazılımın sistemde kalacağı süreyi mümkün olduğunca arttırmayı hedefleyen aşamadır. Elbette bu aşamada hedef bir şeylerin ters gittiğini görüp zafiyeti kapatabilir, hesap şifrelerini güncelleyebilir. Bu durumda saldırgan, client makinasında kalıcılık sağlamak için yeni bir servis oluşturabilir, kullanıcının yetkilerini değiştirebilir, logon script yazabilir, yeni bir kullanıcı oluşturulduğunda zararlı yazılımının çalışması için registryde değişiklik vs yapabilir. Amaç daha yetkili bir hesap ele geçirmek, kritik kullanıcıların bilgisayarlarına erişmek ki bu hassas doküman ve verileri bulmak anlamına geliyor.

KOMUTA VE KONTROL (COMMAND AND CONTROL):

Bu aşamada saldırgan, ele geçirdiği sistemle uzaktan iletişim kurarak tam kontrol sağlamayı amaçlar. Komuta ve kontrol altyapısı genellikle C2 sunucuları üzerinden çalışır ve saldırgan, zararlı yazılım aracılığıyla hedef sisteme komutlar gönderebilir, veri sızdırabilir veya saldırıyı genişletebilir. DNS tünelleme, HTTPS şifreleme, gizli kanallar ve meşru servisler üzerinden veri akışı gibi yöntemler kullanılarak tespit edilmesi zor hale getirilebilir.

EYLEME GEÇME (ACTIONS ON OBJECTIVES):

Eyleme Geçme aşaması, saldırganların hedeflerine ulaşmak için gerçekleştirdiği eylemleri ifade eder. Bu aşamada, saldırganlar veri hırsızlığı yapabilir, sistemleri ele geçirip kontrol altına alabilir, hedeflere zarar verebilir (örneğin fidye yazılımı ile şifreleme) veya faaliyetlerinin izlerini silerek tespit edilmesini engellemeye çalışabilirler. Bu aşama, saldırının sonuçlarını belirleyerek saldırganın nihai amacına ulaşmasını sağlar.



Şekil 4 Cyber Kill Chain

CYBER KILL CHAIN İLE TEHDİTLERİ ÖNLEME

Cyber Kill Chain modelini kullanarak tehditleri önlemek için, her aşamada uygun savunma önlemleri almak mümkündür. Model, güvenlik ekiplerinin saldırganın faaliyetlerini tespit edip durdurmasına yardımcı olur. Ağ trafiği izleme ve analiz araçları, bilgi toplama faaliyetlerini belirlemek için kullanılabilir. E-posta filtreleme ve kötü amaçlı yazılım analiz araçları, zararlı içerikleri tespit edip engeller. Çalışanlara kimlik avı eğitimleri vererek bilinçlendirme sağlanabilir. Güvenlik duvarları ve ağ güvenliği çözümleri, zararlı yazılımların sisteme ulaşmasını engellerken, güvenlik yamaları sistemleri bilinen açıklar karşısında korur. Antivirüs yazılımları zararlı yazılımları tespit ederken, uç nokta koruma çözümleri anormal etkinlikleri belirler. Ayrıca, veri kaybı önleme çözümleri kritik verilerin izinsiz sızmasını önler.

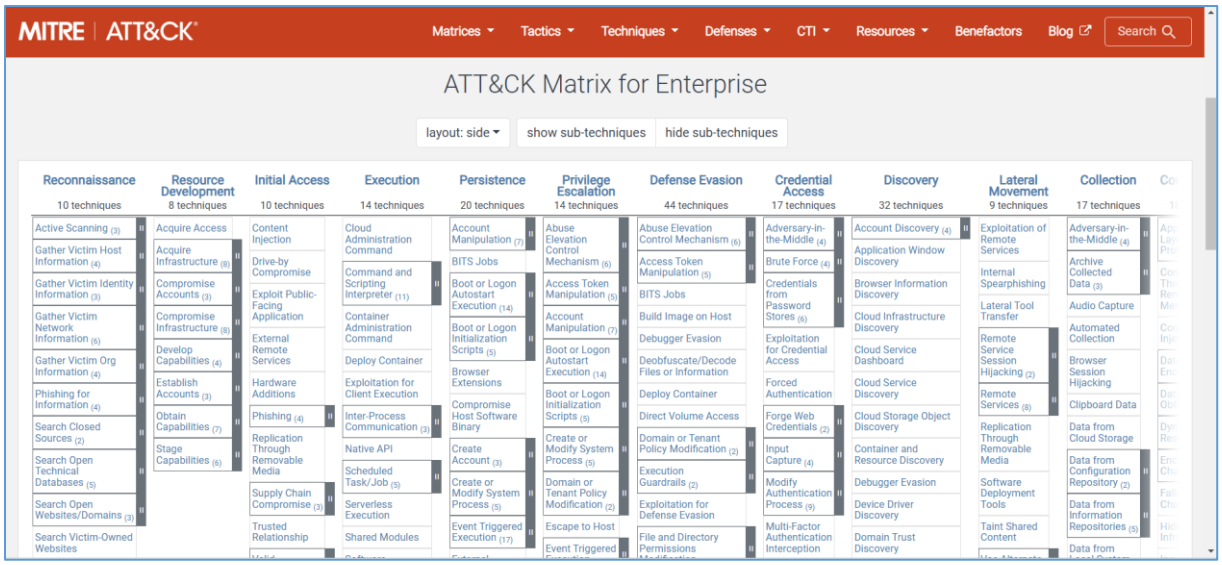
Cyber Kill Chain modelini etkin şekilde kullanmak için en iyi uygulamalardan bazıları şunlardır:

- 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 verilebilir.
- 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 edilebilir.
- Ağ Segmentasyonu (Network Segmentation): Saldırganların hareket alanını sınırlayıp kritik sistemleri korumak için ağ segmentasyonu uygulanabilir.
- Tehdit İstihbaratı (Threat Intelligence): Güncel tehdit istihbaratı kaynaklarını kullanarak saldırganların yeni teknik ve taktikleri öğrenilip buna uygun savunma yöntemleri geliştirilebilir.

CYBER KILL CHAIN VS MITRE ATT&CK

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) Framework, siber güvenlik alanında saldırganların kullandığı taktikleri, teknikleri ve ortak bilgiyi tanımlamak için kullanılan bir bilgi tabanıdır. MITRE Corporation tarafından geliştirilmiştir.

MITRE ATT&CK Framework'un temel amacı, savunma taraflarının saldırganların kullanabileceği taktikleri ve teknikleri anlamalarına ve siber saldırılarla mücadele ederken daha etkili olmalarına yardımcı olmaktır. Bu şekilde, güvenlik uzmanları ve kurumlar, siber saldırılara karşı daha iyi savunma stratejileri geliştirebilir ve olası saldırıları tespit ve önleme konusunda daha proaktif bir tutum alabilirler.



Şekil 5 MITRE ATT&CK

Cyber Kill Chain ve MITRE ATT&CK, siber güvenlikte farklı yaklaşımlar sunar. Cyber Kill Chain, saldırıların aşamalarını belirlerken, MITRE ATT&CK, saldırganların kullandığı taktik ve teknikleri detaylandırarak daha esnek bir çerçeve sağlar. Temel farklarını incelemek gerekirse:

Cyber Kill Chain	**MITRE ATT&CK**
Yedi aşamalı bir modeldir ve saldırıların belirli bir sırayla gerçekleştiğini varsayar. Bu aşamalar: Keşif, Silahlandırma, İletim, Yükleme, Sömürme, Komuta ve Kontrol, Eyleme Geçme'dir.	Daha kapsamlı bir çerçeve sunar ve saldırganların taktiklerini, tekniklerini ve prosedürlerini (TTP'ler) detaylandırır. 14 taktik içerir ve her taktik altında birden fazla teknik bulunur.
Daha katı bir yapıya sahiptir ve modern siber saldırıların her zaman bu aşamaları takip etmediği göz önüne alındığında sınırlayıcı olabilir.	Esnek bir yapı sunar ve farklı saldırı senaryolarına uyum sağlayarak saldırgan davranışlarını daha iyi anlamaya yardımcı olur.
İlk algılama ve yanıt planlaması için etkilidir. Her aşamada güvenlik kontrolleri uygulayarak saldırıyı kesintiye uğratmayı hedefler.	Saldırgan taktikleri ve teknikleri hakkında detaylı bilgiler sunarak algılama ve yanıtı geliştirir.
Genel bir savunma stratejisi oluşturmak için faydalıdır, ancak detaylı tehdit istihbaratı ile entegrasyonu zayıftır.	Tehdit istihbaratının entegrasyonunu kolaylaştırarak, ortaya çıkan tehditleri öngörmeye ve karşı koymaya yardımcı olur.

CYBER KILL CHAIN VE GERÇEK SALDIRI İNCELEMELERİ

WannaCry Fidye Yazılımı Saldırısı (2017)

- Reconnaissance: Saldırganlar, hedef sistemlerin zayıf noktalarını belirlemek için geniş bir bilgi toplama süreci yürüttü.
- Weaponization: Microsoft'un SMB protokolündeki zafiyeti kullanarak zararlı yazılım geliştirildi.
- Delivery: Zararlı yazılım, hedef sistemlere ağ üzerinden yayıldı.
- Exploitation: Saldırganlar, zayıf sistemleri hedef alarak zararlı yazılımı çalıştırdı.
- Installation: WannaCry, sistemlere kurularak dosyaları şifrelemeye başladı.
- Command and Control: Saldırganlar, şifrelenmiş dosyalar için fidye talep etmek üzere kontrol sunucularıyla iletişim kurdu.
- Actions on Objectives: Kullanıcıların dosyalarını şifreleyerek fidye talep ettiler.

Şekil 6 Wannacry zararlı yazılımı

Equifax Veri İhlali (2017)

- Keşif (Reconnaissance): Saldırganlar, Equifax'ın web uygulamalarındaki zayıflıkları belirlemek için bilgi topladı.
- Silahlandırma (Weaponization): Apache Struts zafiyetini kullanarak zararlı yazılım geliştirildi.
- Teslimat (Delivery): Zararlı yazılım, hedef sistemlere sızdı.
- İstismar (Exploitation): Saldırganlar, zayıf sistemleri hedef alarak zararlı yazılımı çalıştırdı.
- Kurulum (Installation): Zararlı yazılım, sistemlere kurularak kalıcı bir varlık oluşturdu.
- Komut ve Kontrol (Command and Control): Saldırganlar, çalınan verileri dışarı aktarmak için iletişim kanalları kurdu.
- Hedeflerdeki Eylemler (Actions on Objectives): 147 milyon kişinin kişisel bilgileri çalındı.

SONUÇ

Siber Ölüm Zinciri (Cyber Kill Chain), saldırı süreçlerini analiz ederek siber tehditlere karşı etkili savunma mekanizmaları oluşturmayı sağlayan güçlü bir modeldir. Bu metodoloji, saldırganların izlediği adımları anlamayı ve her aşamada proaktif önlemler almayı mümkün kılar.

Cyber Kill Chain, MITRE ATT&CK gibi modern çerçevelerle birlikte kullanıldığında, organizasyonlara tehdit istihbaratını daha iyi değerlendirme ve olay müdahale süreçlerini güçlendirme imkanı sunar. Gerçek saldırı senaryolarında görüldüğü gibi, doğru uygulamalarla siber tehditler erkenden tespit edilip engellenebilir.

Sonuç olarak, siber güvenlik ekiplerinin saldırgan perspektifini benimsemesi, güvenlik farkındalığını artırması ve savunma stratejilerini sürekli geliştirmesi gerekmektedir. Cyber Kill Chain modelini etkili bir şekilde kullanmak, siber tehditlere karşı daha dayanıklı bir güvenlik yapısı oluşturmanın anahtarıdır.

KAYNAKÇA

1. https://berqnet.com/blog/cyber-kill-chain
2. https://www.exabeam.com/explainers/information-security/cyber-kill-chain-understanding-and-mitigating-advanced-threats/
3. https://www.researchgate.net/figure/Cyber-Kill-Chain-Anatomy-of-WannaCry-17_fig5_379583763
4. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf
5. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
6. https://www.defenceturk.net/gelismis-siber-saldirinin-7-evresi-siber-olum-zinciri-cyber-kill-chain
7. https://en.wikipedia.org/wiki/Cyber_kill_chain
8. https://bbsteknoloji.com/cyber-kill-chain-nedir/
9. https://www.proofpoint.com/us/threat-reference/cyber-kill-chain
10. https://www.safebreach.com/blog/equifax-breach-three-data-breach-protection-measures-learned/
11. https://www.sentinelone.com/cybersecurity-101/threat-intelligence/cyber-kill-chain/