Cyber Kill Chain

Tarih: *06.02.2025*

Hazırlayan: *Muhammed Barış Güven*

Altay

Cyber Kill Chain

Siber saldırı faaliyetlerinin tanımlanması ve önlenmesi için, saldırıları aşamalar halinde inceleyen bir modeldir. Bu modeli her analizcinin bilmesi gerekmektedir, saldırı taktik ve tekniklerini bilmek analiz yapan kişinin, saldırı hakkında alabileceği önlemi artırır. Bu saldırı aşaması yedi adımdan oluşur;

1. Reconnaissance (keşif)

İlk aşama, saldırganın hedef hakkında bilgi toplama aşamasıdır. Bu aşamada saldırgan hedef kişi veya kuruluş hakkında aktif veya pasif yollarla bilgi toplar, topladığı bilgiler hedefin zayıflık gösterdiği durumlardır.

1.1. Aktif Tarama

Aktif tarama, hedef sistemin veya sunucunun açık portlarını, zayıflık gösterdiği alanları gerekli araçlar yardımı ile keşfetme işlemidir.

1.2. Pasif Tarama

Açık kaynakları kullanarak (sosyal medya, forum, sözlük) yapılan tarama işlemidir. OSINT (open-source intelligence) araçları kullanarak, yapılan tarama işlemleri otomatize edilebilir. Bu şekilde hedef hakkında toplanan bilgiler ile saldırı güzergahı az çok belli olur.

2. Weaponization (silahlanma)

Keşif aşamasının tamamlanmasının ardından saldırgan potansiyel hedefler ile bunların güvenlik açıkları hakkında yeterli bilgiyi toplamış bir şekilde, belirli güvenlik açıklıklarını istismar etmek için tasarlanmış kötü amaçlı bir payload oluşturur veya temin eder.

Weaponization süreci, mevcut araçları saldırıda kullanılacak şekilde değiştirmelerini de kapsar. Örnek olarak saldırgan bir fidye yazılımı (ransomware) türü üzerinde küçük değişiklikler yaparak yeni bir araç oluşturabilir. Bu aşamada saldırgan güvenlik çözümlerinden kaçınmaya yönelik önlemleri eklemek için elinden geleni yapar. Bu aşamanın anlaşılması, savunma yapacak analiz ekibinin saldırganların araçlarını nasıl oluşturabileceğini önceden tahmin etmesine yardımcı olur.

Kötü amaçlı yazılımların antivirüs yazılımlarını atlatacak şekilde özelleştirilmesi veya kullanıcıların güvenlik açıklarını istismar etmek amacıyla, zararlı dosya veya belgelerle oltalama (phishing) e-postalarının oluşturulmasını sağlar.

3. Delivery (teslimat)

Saldırgan bu aşamada, hedefe kötü niyetli bir payload iletir. Bu iletiyi, oltalama saldırısı yaparak hedefte bulunan kişilerin e-postalarına zararlı yerleştirilmiş ekler göndererek veya sahte web siteleri tasarlayarak kişinin giriş bilgileri, kredi kartı bilgileri gibi hassas bilgilere ulaşıp hedefte bulunan kişiye zarar verir. Bu tarz saldırı yöntemlerine literatürde, sosyal

mühendislik saldırısı denilir. Birkaç çeşidi olsada Cyber Kill Chain adımlarına en uygun sosyal mühendislik saldırısı spear-phishing (mızrakla oltalama) kullanılır.

3.1. spear-phishing (mızrak-oltalama)

Bu sosyal mühendislik türü, spesifik olarak bir kişiye veya kuruma göre hazırlanmış oltalama tekniğidir. Bu teknik, esas amaç olarak karşı tarafın hassas bilgilerine erişmek veya sistemine bir zararlı yüklemek için manipüle edilmiş ek dosyalar göndermektir. (.pdf, .jpg vb.)

4. Exploitation (sömürmek)

Zararlı virüsü veya hassas bilgileri ele geçiren saldırgan, bu aşamada bu bilgileri veya zararlı virüsünü kullanmak için kollarını sıvar. Saldırgan hedefine ulaşmak için, gerekli araçları[1] kullanarak, aynı ağda bulunan diğer cihazlar arasında yanal olarak hareket[2] ederler. Ağdan sorumlu olan güvenlik ekibi gelecek saldırıların manipülasyon ve aldatma tekniklerine dair önlem almaması durumunda saldırganlar hedeflerine erişebilir.

5. Installation (kurulum)

Siber suçlular hedeflerinin güvenlik açıklarını sömürdükten sonra sistemin kontrolünü ellerine alabilmek adına hedef ağdaki açığı kullanarak, sisteme trojan, backdoor veya scriptler ile zararlı kurabilirler. Bu şekilde sisteme tekrar bağlanarak kendi sistemlerini hedef sistem üzerinde kalıcı hale getirebilirler.

6. Command and Control (komut ve kontrol)

Bu aşamada saldırgan, hedef sistemi uzaktan kontrol etmek için komuta ve kontrol kanallarını yüklediği, trojan, script veya backdoorlarla oluşturur. Bu şekilde hedef sistemle kontrol sunucusu arasında iletişim sağlar.

7. Actions on Objectives (Hedeflerdeki Eylemler)

Artık saldırgan sistem üzerinde tam yetki sahibidir ve artık hedeflediği şeyi yapmak için önünde bir engel kalmamıştır. Bu durumda yapabileceği faaliyetler; veri hırsızlığı, sabotaj, fidye yazılımları sayesinde kilitlenen sistemi açmak adına yapılabilecek şantaj.

---

[1] *araç: ingilizcesi tool olan araç kelimesi, hazır scriptlerden oluşan, zaafiyetleri sömürmek için bize yardımcı olan çalıştırılabilir dosya. Bkz: https://www.webopedia.com/definitions/cyber-security-tools/*

[2] *Saldırganların hedefi, daha yüksek seviyede erişim ve kontrol elde etmektir. Bu nedenle, saldırganlar ağa girdiklerinde, hangi kaynaklara erişebileceklerini ve hangi hesapları ele geçirebileceklerini belirlemek için keşif işlemlerine başlarlar. Yüksek ayrıcalıklı hesapları ve kritik kaynakları hedef alarak, ayrıcalıklarını artırmaya çalışırlar.*

Sonuç

Bu modelin en iyi uygulanma yöntemi, çalışanların oltalama saldırısı gibi sosyal mühendislik saldırılarını tanıyabilecekleri eğitimlerden geçmesini sağlamak, ağ ve uç nokta güvenliği çözümlerini kullanmak, siber saldırılara hızlı ve etkili yanıtlar verebilecek müdahale planları oluşturmak ve düzenli testler ile çalışanları bu planlar doğrultusunda refleks gösterebilecekleri kıvama getirmek, saldırganların hareket alanını sınırlayıp kritik sistemleri korumak için ağ segmentasyonu yapmak ve güncel tehdit istihbaratı kaynaklarını kullanarak saldırganların yeni teknik ve taktiklerini öğrenip savunma stratejilerinizi buna göre güncellemek gerekmektedir.

KAYNAKÇA

https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

https://darktrace.com/cyber-ai-glossary/cyber-kill-chain

https://e-data.com.tr/siber-saldirganlarin-gozunden-yanal-hareket-ve-ayricalik-yukseltme-teknikleri/

https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack/

https://berqnet.com/blog/cyber-kill-chain