|  |
| --- |
| ***Cyper Kill Chain*** |
| Kaan Efe Öğüt  *ADLİ BİLİŞİM MÜHENDİSLİĞİ* |
| Siber güvenlik araştırmacıları, siber saldırıları analiz edebilmek amacıyla çeşitli modeller üzerinde çalışmaktadırlar.Bu modellerden biri olan Cyper Kill Chain hakkında bilgi vereceğim. |

**19.08.2021**

***Cyper Kill Chain***

-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.



***1-)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 ve Aktif bilgi toplama olarak ikiye ayrılmaktadır.

-Pasif Bilgi Toplama : Hedef ile direkt olarak temasa geçilmeden bilgi toplama çeşitidir.

-Aktif Bilgi Toplama : Hedef ile direkt olarak temasa geçilen bilgi toplama çeşitidir.

***2-)Weaponization(Silahlanma)***

-Keşif aşamasında sistemde belirlenen giriş noktasını kullanarak;çeşitli kaynak kodlu yazılımlar,phishing gibi yöntemlerden hangisini kullanacağını belirlediği basamaktır.

***3-)Delivery(İletme)***

-Silahlanma basamağında belirlenen yazılımın hedef sisteme iletildiği aşamadır.

-Çeşitli kaynak kodlu yazılımlar,phishing,sosyal networkler veya tünellemeler gibi yöntemler kullanılabilir.Ayrıca kurum üzerinde güvenlik olarak çalışanların sosyal mühendislik ve phishing saldırılarına karşı farkındalıklarını arttırarak önlenebilir.

***4-)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,sistemde ki zafiyetlerin tespit edilebilmesi için güvenlik denetimleri yapılıp yapılmadığı kontrol edilebilir.

***5-)Installation(Yükleme)***

-Sistem üzerinde başarı ile çalışan zararlı yazılım, kalıcı bir tehdit haline gelmek için sisteme kendini yüklemelidir.

-Bu aşamada siber saldırganın başarılı bir şekilde sistemi kontrol etmesinin önü açılır.

-Yükleme aşamasının en önemli amacı, zararlı yazılımın sistemde kalacağı süreyi mümkün oldukça arttırmaktır.

***6-)Command & Control,C2(Komuta & Kontrol)***

-Sisteme yerleşmiş olan zararlının çalışması uzaktan kontrol edilebildiği ve sistemin ele geçirildiği aşamadır.

-Bu aşama için saldırıyı engelleyebilecek Firewall ve IPS‘in devrede olup olmadığı iyi konfigüre edilip edilmediğine bakılmalıdır.

-Bu aşama da haberleşme kaynağı ile genellikle şifreli haberleşme yönteleriyle bağlantı kurulur.

-Bu aşama da hedef sistem ele geçirilmiş olur.

***7-)Actions On Objectives(Eylem)***

-Hedef sistemi ele geçiren saldırgan, bu aşama ile birlikte amacına ulaşmak için çeşitli eylemler gerçekleştirir. Bu eylemlere, veri çıkarma, silme veya başka bir sisteme saldırma örnek olarak verilebilir. Ayrıca, asıl hedefine ulaşabilmek için gerçekleştirdiği tüm eylemler bu basamakta değerlendirilir.

-Önlem olarak iç ağdan dışarı yapılan veri akışı sınırlandırılması,sadece bilinen sunuculara veri akışını sağlama(Whitelisting) oluşturulduğunda saldırı engellenebilir.

-Bu süreçte tehdit altında ki verilerin yedeklerinin önceden alınması,bir sistem devre dışı kaldığında hizmet verebilecek yedek sistemin olması bu saldırının etkilerini azaltabilir.