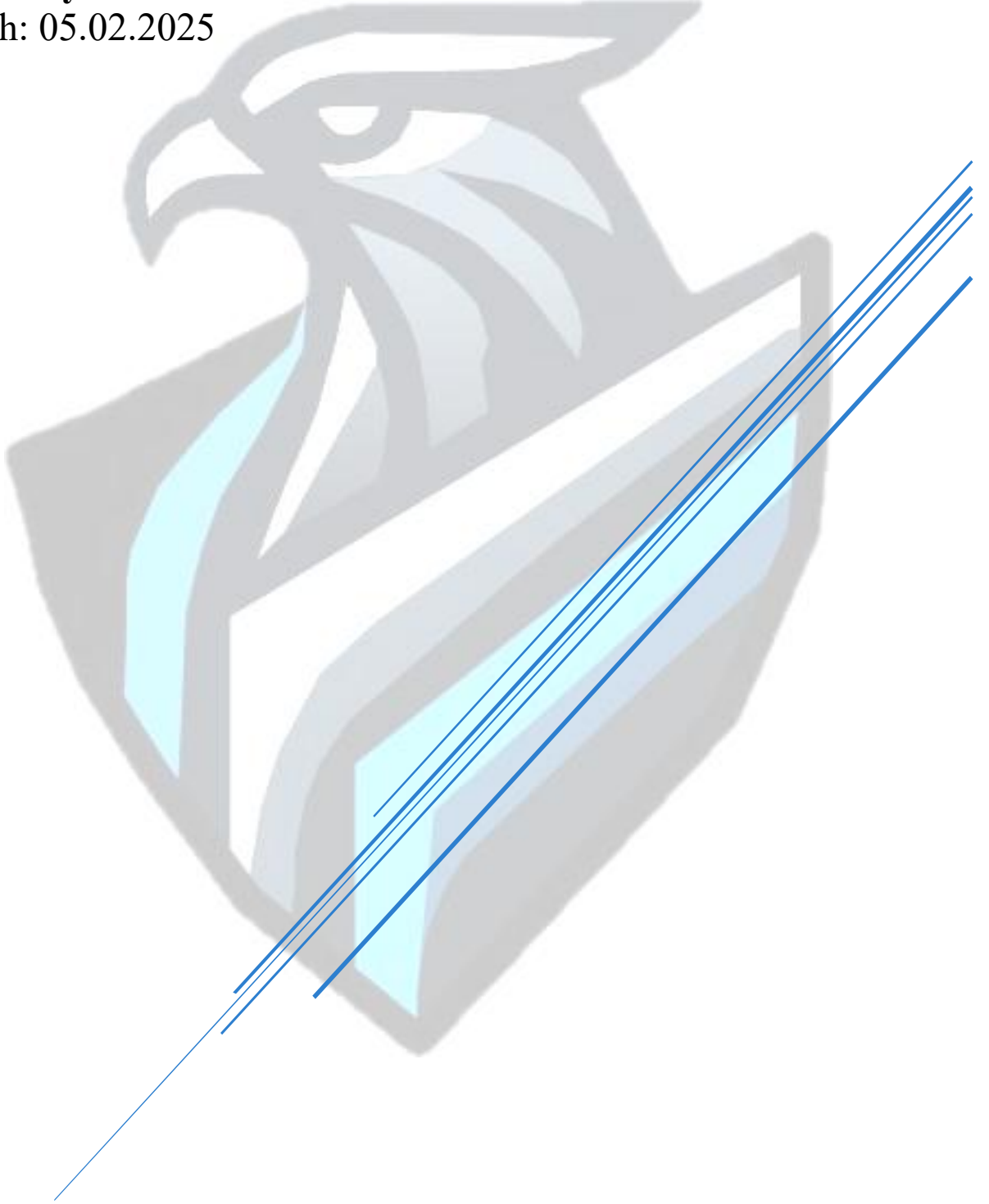


SOC FUNDAMANTELS VE CYBER KILL CHAIN

Hazırlayan: Emrecaan Atlıhan

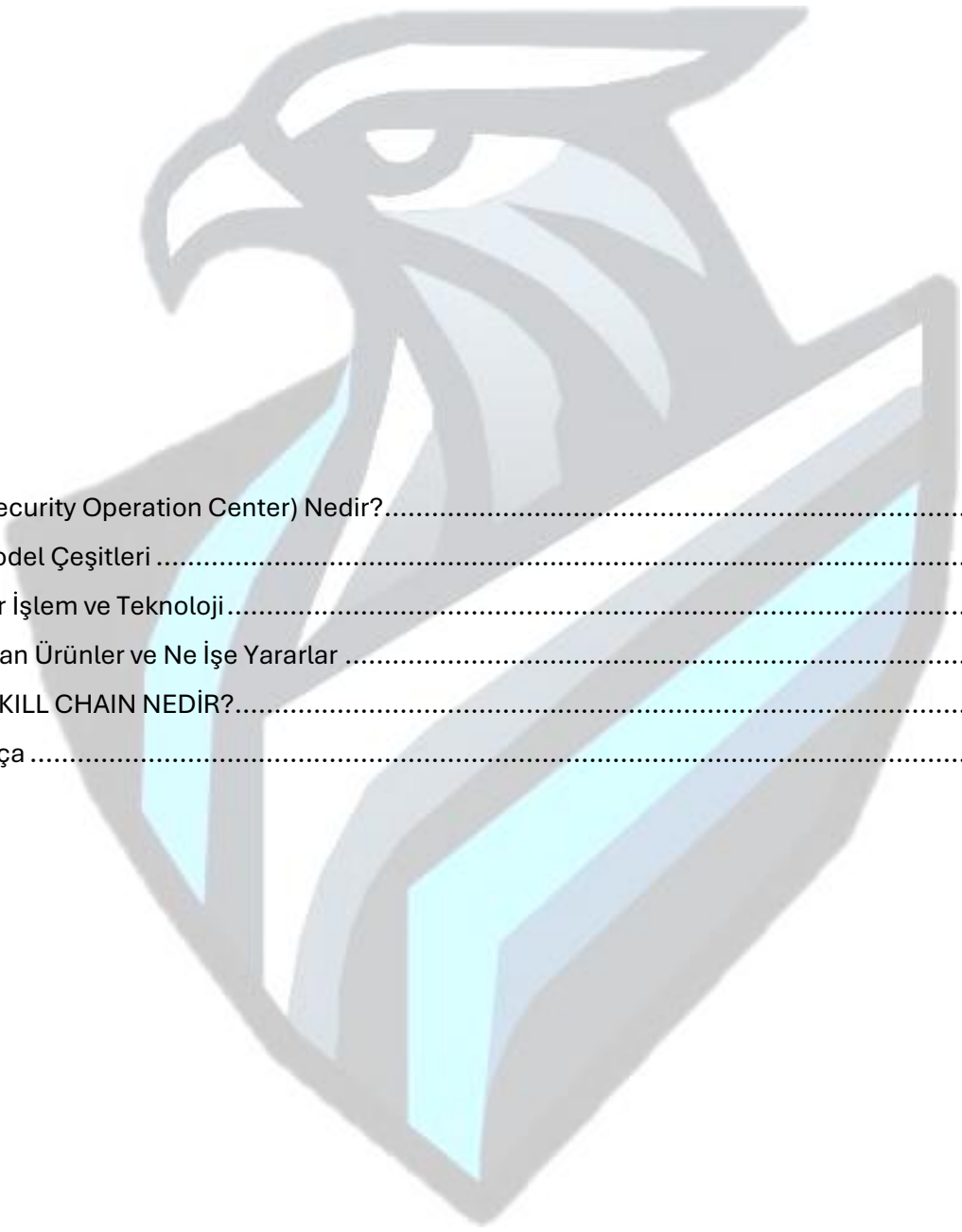
Tarih: 05.02.2025



GİRİŞ

Bu raporun hazırlanış amacı SOC Fundamantels ve Cyber Kill Chain hakkında bilgi vermektir. SOC alanında çalışmak ve bilgilenmek isteyenler için başlangıç rehberi gibi sayılabilir. İçeriğimizde SOC alanındaki görevlerin ve Cyber Kill Chain adımlarının açıklamaları bulunmaktadır. Bunlara ekstra olarak SOC alanında kullanılan birkaç aracın da açıklaması yapılmıştır. Son olarak kaynakça kısmında ise daha fazla bilgilenmek isteyenler için URL'ler bırakılmıştır.





SOC (Security Operation Center) Nedir?.....	3
SOC Model Çeşitleri	3
İnsanlar İşlem ve Teknoloji.....	4
Kullanılan Ürünler ve Ne İşe Yararlar	5
CYBER KILL CHAIN NEDİR?.....	10
Kaynakça	13

SOC (Security Operation Center) Nedir?

Bilgi güvenliği ekibinin bir organizasyonun veya kuruluşun güvenliğini sürekli olarak izleyen ve analiz eden bir grup olarak düşünülebilir. SOC aslında bu grubun toplamına verilen bir isimdir.

SOC takımının görevi aslında tespit etmek ve bu tespitlere uygun cevaplar verebilmektir. Tespit etme kısmı bazı güvenlik çözümleri ile sağlanır. Bu çözümler kontrol edilecek şirkete veya kuruma entegre edildikten sonra SOC takımının elinde kaynak oluşur. Bu kaynaklardan tespit daha da kolaylaşır. SOC takımı 7 gün 24 saat aktif olmak zorundadır. Bu topluluk illaki aynı yerde olma zorunluluğu yoktur.

Birkaç çeşit SOC modeli vardır. Aşağıda bunun açıklaması bulunmaktadır.

SOC Model Çeşitleri

SOC'nin 4 farklı modeli vardır. Bu modeller gereksinimlere göre değişiklik gösterebilir.

1. In-House SOC
2. Virtual SOC
3. Co-Managed SOC
4. Command SOC

1-In-House SOC

Bir kuruluşun siber güvenlik operasyonlarını kendi bünyesinde yürüttüğü bir güvenlik merkezi anlamına gelir. Burada şirket kendi ekibini tutup toplayacağı için bazı dezavantajları ve avantajları olabilir.

2-Virtual SOC

Herhangi bir merkezde bulunma zorunluluğu olmayan çeşitli yerlerde uzaktan çalışabilen SOC modelidir.

3-Co-Managed SOC

Bir kuruluşun kendi içindeki güvenlik operasyonlarını, bir dış siber güvenlik sağlayıcısıyla birlikte yönettiği bir modeldir. Bu yapı, şirketin kendi güvenlik ekibi ile üçüncü taraf bir MSSP (Managed Security Service Provider) arasında iş birliği sağlandığı SOC modelidir.

4- Command SOC

Bu SOC ekibi geniş bir bölgede yayılmış olan daha küçük SOC gruplarını denetler. Büyük bir bölgenin tek bir SOC'ye bağlı olması sorun çıkarabilecekken küçük gruplar halinde küçük bölgelere bakan takımların denetlenmesi daha uygun ve güvenli olacaktır.

İnsanlar İşlem ve Teknoloji

Eğer başarılı olmasını istediğiniz bir SOC takımını kurmak istiyorsanız koordinasyon çok önemlidir. İnsan, işlem ve teknoloji arasında güçlü bir bağ ve ilişki olması lazım. Yukarıda başlık olarak attığım üç madde SOC için gereklidir.

1- İnsanlar

Aslında burada insanlar olarak bahsettiğimiz kısım çalışanlarınızdır. Çalışanlarınızın kendini geliştirmiş olması ve atak senaryolarına güvenlik alarmlarına önceden çalışmış olması gerekiyor. Dünyada her gün yeni bir saldırı metodu çıkıyor. Çalışanlarınızın bu durumlara hızlıca uyum sağlaması gerekiyor. Bu uyum sürecini hızlandırmak için aslında önceden atak senaryolarına ve güvenlik alarmlarına çalışılması gerekiyor.

2- İşlemler

Burada aslında işlemler kısmı yapacağınız işlerin bir standardize olması gerektiğini belirtir. Dünyada NIST (National Institute of Standards and Technology), PCI (Peripheral Component Interconnect) gibi birçok farklı standartlarla uyumlu halde çalışırsanız globalleşebilirsiniz.

3- Teknoloji

Takımınızın birçok farklı görev için ürünlere ihtiyacı olacaktır. Organizasyonunuz için en iyi ürünü bulabilmek için marketi ve teknolojiyi iyi bir şekilde takip etmeniz gerekmektedir.

SOC'de Roller

1- SOC Analisti

Bu rol kendi içinde 3 bölümden oluşur. Asıl amaçları alarmları kategorize etmek, neden oluştuğuna bakmak ve iyileştirme amaçlı tavsiyeler vermektir.

- SOC Seviye 1 Analist

İlk olarak alarmlara tepki veren SOC çalışanıdır. Alarmlar ilk olarak buradan geçer. Zararlı olup olmadığına karar verir ve gerektiğinde uygun kanallar aracılığı ile tespit ettiklerini üstüne raporlar.

- SOC Seviye 2 Analist

Seviye 2 analistler araştırmalarını daha derine inerler ve doğru bir analiz için birden fazla kaynaktan gelen verilerin korelasyonunu sağlarlar.

- SOC Seviye 3 Analist

Seviye 3 analistler tehditlere karşı deneyimli olan profesyonellerdir. Herhangi bir olay müdahalelerde yardımcı olabilecek deneyime sahiptirler. Analist 1 ve 2'den gelen raporları inceleyerek kritik olanlara ayrıntılı müdahale yaparlar.

2- Olay Müdahale Görevlisi (Incident Responder)

Bu kişi tehdit tespitinden sorumludur. Yapılan güvenlik ihlallerinin ilk değerlendirilmesini gerçekleştirir.

3- Tehdit Avcısı (Threat Hunter)

Geleneksel yöntemlerden kaçabilen gelişmiş tehditleri araştıran manuel veya otomatik sistemleri kullanan kurumun altyapısı hakkında bilgi sahibi olan kişidir. Tehditleri işletmeye zarar vermeden veya kesintiye uğramadan önce bulmayı ve önlemeyi amaçlar.

4- Güvenlik Mühendisi (Security Engineer)

Güvenlik mühendisi SIEM, SOAR, EDR, XDR, IDS/IPS gibi ürünlerin kurar yapılandırır ve optimize eder. Olay tespit kurallarını ve alarmlarını oluşturur.

5- SOC Yöneticisi (SOC Manager)

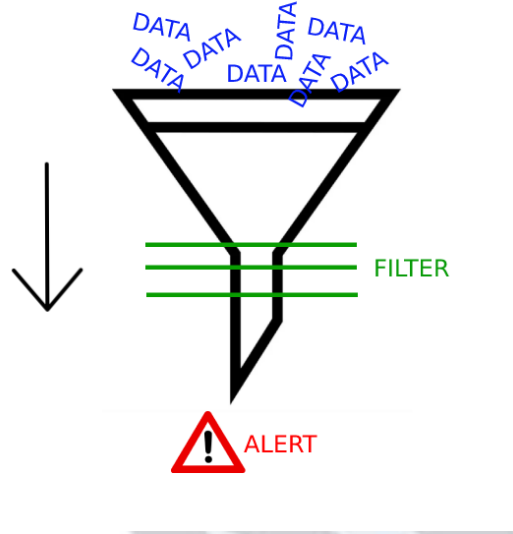
SOC yöneticisi genel olarak bütçe strateji ve yönetim gibi şeylerden sorumludur. Teknik konulardan ziyade operasyonel sorunlar onu daha çok ilgilendirir.

Kullanılan Ürünler ve Ne İşe Yararlar

SIEM

SIEM çözümü aslında güvenlik bilgileri ile olay yönetimini harmanlar. Bu harmanlama sonucu gerçek zamanlı logları izleme fırsatı sunar. Bu loglamanın ana amacı güvenlik tehditlerini tespit etmektir.

SIEM'lerin birçok özelliği vardır. Bizi asıl ilgilendiren kısmı ise toplanan veriyi filtreleyip şüpheli olaylar için uyarılar sağlamasıdır.



En ünlü SIEM ürünleri IBM QRadar, ArcSight ESM, FortiSIEM, Splunk.

EDR ve XDR çözümleri

Günümüz dünyasında siber tehditlerde inanılmaz bir yükseliş var. Bu yükselişte saldırılar organizasyonlar için daha sofistike ve majör bir problem yaşatmakta. Bu noktada EDR ve XDR çözümleri ortaya çıkıyor. Burada EDR ve XDR çözümlerine göz atacağız.

1. EDR (Endpoint Detection and Response) çözümü

EDR çözümleri teknolojiyi kullanarak uç kullanıcının cihazını izleme, tespit etme ve tehditleri bildirme üzerine kuruludur. EDR'lar bilgisayarı veya cihazları izleyerek, yapılan normal olmayan davranışları yakalayarak bunları hızlıca bildirip aksiyon alınır. Peki EDR'larda neler yapılabilir?

- **Dosya ve İşlem İzleme**

Normal olmayan işlemler ve dosyalarda yakalanabilecek virüs işaretleri izlenerek korum sağlanır

- **Davranış Analizleri**

Bir uygulamanın veya kullanıcının normalde yaptığı davranışların dışında bir işlem gerçekleşirse EDR bunu yakalar. Örneğin herhangi bir kullanıcınız dışarıya doğru ping atmaz. Tabii ki de bu her zaman bir normal olmayan bir davranış anlamına geleceğini düşündürmesin size. Sadece saldırganlar ilk olarak erişim sağladığında internete bağlı olup olmadığını makinenin kontrol etmek için ping kullanabilirler. Bunu kullanıcı da atmış olabilir.

- **Zararlı Yazılım Tespiti**

Zararlı yazılımları tespit edip izole eder. Bunlara örnek olarak trojanlar, ransomware'ler olabilir.

- **Güvenlik İhlali Göstergeleri (Indicator of Compromise) Tespiti**

Tehdit istihbaratı kullanılarak bazı zararlı yazılım aktiviteleri tespit edilebilir. Virüslerin hashleri, bağlantı kurulan IP adresleri, e-postalar bunlara örnek olabilir.

- **Log Analizi**

Loglar izlenerek yakalanan normal olmayan davranışlar tanımlanıp önlem alınır.

2. XDR Çözümleri

XDR'lar birden fazla katmandan gelen veriyi harmanlayarak tehdit tespiti yaparlar. Bu veriler uç noktadan, ağdan, sunucudan, bulut ortamlarından ve e postalardan gelir. Sadece uç noktayı değil kurulduğu şirketin tamamını kapsar.

XDR'lar neler yapabilir peki?

- **Otomatik Tehdit Tespiti**

XDR'lar normal olmayan davranışları makine öğrenmesi ve yapay zekâ kullanarak otomatik tespit ederek potansiyel tehditlerden koruma sağlar.

- **Tehdidin İzlediği Yolun Analizi**

XDR olaylar ve ilişkileri inceleyerek tehdidin ilerleyişi ve verebileceği zararı göz önüne serer. Bazen karmaşık saldırılarda bunu kullanarak çözüme daha kısa ulaşabiliriz.

- **Olay Yönetimi ve Analizi**

XDR, farklı güvenlik olaylarını geniş bir bakış açısıyla bakarak değerlendirir ve analiz eder.

XDR ve EDR arasındaki farklar nelerdir?

Özellik	EDR (Endpoint Detection and Response)	XDR (Extended Detection and Response)
Odak Noktası	Yalnızca uç noktalar	Uç noktalar + Ağ + Bulut + E-posta + Sunucular
Veri Kaynağı	Endpoint logları	Çoklu veri kaynakları (ağ trafiği, SIEM, e-posta, vb.)
Tehdit Korelasyonu	Sınırlı	Gelişmiş ve kapsamlı
Görünürlük	Sınırlı	Geniş ve bütünsel görünürlük

Çok Bilinen EDR ve XDR ürünleri

- CrowdStrike Falcon
- Cybereason
- Palo Alto
- Sentinel One

SOAR nedir?

SOAR, Security Orchestration Automation and Response'un kısaltmasıdır. Yapılması gereken bazı işleri otomatik yaparak SOC takımına yardımcı olur. Aslında neredeyse gereken her şeyin bir yerde toplanıp işleri kolaylaştırmasıdır.

SOAR'ın 4 farklı temel bileşeni var diyebiliriz.

- Orkestrasyon
Güvenlik çözümlerinin birbiriyle uyumunu sağlayarak işleme koyar. SIEM'den gelen bir alarmı EDR ile ilişkilendirerek otomatik aksiyon alınabilir.
- Otomasyon
Olaylardaki aksiyon olma eylemlerini otomatik hale getirebilir. Zararlı IP'leri engelleyebilir.
- Yanıt
Tespit edilen tehditlere müdahale otomatik veya manuel şekilde sağlanır.
- Raporlama
Olayın analizi için raporlar sağlanır.

CYBER KILL CHAIN NEDİR?

Cyber Kill Chain bir siber saldırının adımlarını belirten 7 maddeden oluşan bir tablodur. Her saldırı buna benzeyen şekilde adımları bulunur. Bu tablo raporlamada kolaylık sağlar. Saldırganın ilk olarak ne yaptığı hangi metotları kullanarak ilerlediği tabloda belirtilir.

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command and control
- Action

Reconnaissance (Tarama)

Tablomuz ilk olarak tarama ile başlar. Saldırganlar bilgi toplamak amacıyla tekniklerle birlikte kurban hakkında bilgi toplarlar.

Tarama kısmı 2 bölümden oluşur:

1. Aktif Tarama
Bu metotta kurbanla direkt olarak etkileşime geçilir ve hakkında bilgi toplanmaya çalışılır. Buna örnek olarak NMAP taramaları, zafiyet taramaları ve kaba kuvvet saldırıları örnek verilebilir.
2. Pasif Tarama
Kurbanla direkt olarak etkileşime girmeden yapılan taramalardır. Buna örnek olarak web arşiv siteleri kullanılarak şu anda mevcut olmayan site arayüzüne erişim sağlamak sayılabilir.

Weaponization (Silahlanma)

İkinci adıma geldiğimizde ise silahlanma olarak adlandırabileceğimiz bölüm gelir. Saldırgan tarama kısmında topladığı bilgilerle saldırı için gerekli şeyleri yapmaya başlar. Bunlara örnek olarak ise ortalama e postaları, zararlı yazılım yaratmak, açıkları sömürmek, zararlı dosyalar yaratmak olabilir. Zararlı dosyalar olarak MS programları örnek verilebilir. Saldırgan ortalama e postasına ekleyeceği bir Excel dosyasına makrolar ekleyerek gerekli erişimi sağlayabilir. Bundan korunmak için e posta analizleri, gerekli araçları (ole araçları) ile dosya analizleri, tersine mühendislik gibi teknikler gerekebilir.

Delivery (İletim)

Üçüncü adımda iletim gelir. Aslında yukarıda biraz nasıl iletim sağlandığına örnek verdim. Bunlara ek olarak daha farklı iletim yolları da görebiliriz. Bu adım siber saldırının başladığı nokta olarak da sayabiliriz.

- E posta yoluyla zararlı URL gönderimi
- Zararlı yazılımı dosya eki olarak e postadan gönderimi
- Zararlı yazılımı sunucuya yüklemek (eğer erişimi varsa)
- Zararlı yazılımı sosyal medya yoluyla göndermek

Exploitation (Sömürme)

Dördüncü adımda karşımıza sömürü kısmı çıkar. Saldırgan zararlıının kurban makineye geçtiğinden emin olduktan sonra çalışmalara başlar.

Bu adımda saldırı şunları yapabilir:

- Zararlı yazılımın çalışması
- Yazılımın veya işletim sisteminin sömürülmesi

Installation (Kurulum)

Beşinci adımda kurulumla devam ediyoruz. Saldırganlar burada sömürülen sistemde kalıcılık sağlamak için girişimlerde bulunurlar. Bunun sebebi saldırı istediği zamanda erişim sağlamaktır. Bulduğu açık zaman içinde güncelleme alarak düzeltilebilir. Bunun yaşanması durumunda saldırının emekleri boşa gidecektir. Bunu önlemek adına bir zararlı yüklenerek arkakapı (backdoor) indirir. Bu işi tamamlayan saldırı daha rahat dolaşabilmek için yetki yükseltme saldırısı ile yüksek yetkili bir kullanıcı hesabına erişim sağlamayı veya kendi kullanıcısının yetkisini yükseltmeye çalıştığı görülür.

Bu bölümde maddelerle kısaca yapılanlar şunlardır:

- Zararlıının kurban makineye indirilmesi
- Arkakapı oluşturulması
- Web Shell yüklenmesi

- Kurban makinada kalıcılık sağlanması için teknikler kullanılması (servisler, görev zamanlayıcısı, güvenlik duvarında kural değişiklikleri, COM Hijacking, kayıt defterinde değişiklikler)

Komut ve Kontrol (Command and Control)

Saldırgan önemli noktaları tamamladıktan sonra komuta kontrol sunucusunu kullanarak karşı tarafta komut çalıştırmaya başlar.

Aslında bu bölüm bu kadar neredeyse fakat DFIR raporlarından gördüğüm birkaç komut kontrol için kullanılan ürünleri sıralayalım:

- Cobalt Strike
- Havoc
- Sliver
- MsfConsole

Action (Aksiyon)

Saldırgan tüm adımları başarı ile tamamladıktan sonra önünde hiçbir engel kalmadığı için istediğini yapabilir. Bu onun amacına göre değişiklik gösterebilir.

Amaçları şunlar olabilir:

- Bir fidye grubu ise dosyaları şifreleyip para isteyebilir.
- Önemli dosyaları sızdırabilir.
- Kullanıcı verilerini ele geçirerek diğer makinelere erişimde bulunmak için kullanabilir.
- Sistemde bazı değişiklikler yapabilir.

Kaynakça

<https://letsdefend.io/>

<https://tryhackme.com/>

