SİBER ÖLDÜRME ZİNCİRİ

Sebahattin Gökcen Özden

07/02/2025

GİRİŞ

Bu çalışmada siber güvenliğin temellerinden biri olan ve siber saldırının aşamalarını şematik şekilde algılamamız sağlayan “Siber Ölüm Zinciri” üzerine hazırlanmış bir yazıdır. Çoğu siber saldırganın başarılı saldırıları gerçekleştirmek için bir dizi benzer aşama kullandığını ortaya koyan saldırılarının hassasiyeti üzerine yapılan çalışmalar yapılmıştır. (1) Bu disiplin bütününe ve olaya saldırganın bakış açısından bakmamıza olanak tanıyan bu siber ölüm zinciridir.

Bu raporun amacı bu zinciri daha yakından anlayıp bu siber olarak ölümcül sonuçları olabilecek saldırıyı anlamaktır.

Keywords: Cyber Kill Chain, Siber Ölüm Zinciri, siber güvenlik, siber atak,

SİBER ÖLÜM ZİNCİRİNİ ANLAMAK

Siber Öldürme Zinciri, saldırılarını öngörerek, stratejik olarak meşgul ederek ve durdurarak hedefleri etkili bir şekilde etkisiz hale getirmek için kullanılan bir askeri modelden türetilen Lockheed Martin'e atfedilir. Kulağa ne kadar süslü gelse de, gerçekte Cyber Kill Chain, bilgisayar korsanlarının nasıl saldırdığının sadece adım adım bir açıklamasıdır.Model, saldırının başlangıç aşamalarından bir sistem istismar edilene kadar düşmanların adımlarını açıklar, bu adımlar şunları içerir:

1.Keşif : Saldırgan hedef hakkında bilgi toplar

2.Silahlanma : Saldırgan hedefe göndermek için bir istismar oluşturur

3.Teslimat : Kullanılan silah hedefe mail gibi bir yöntem ile iletilir

4.İstismar : Silahın oluşturduğu istismar yürütülür

5.Kurulum : Hedef'e kötü amaçlı yazılım yada arka kapı kurulur

6.Komut ve Kontrol : Hedef'in uzaktan kontrolü bir komut kontrol kanalı ile sağlanır

7.Eylem : Saldırgan bilgi hırsızlığı gibi kötü amaçlı eylemler gerçekleştirir

veya Kill Chain aşamalarında tekrar çalışarak ağdaki diğer cihazlara ek saldırılar gerçekleştirir.

Öldürme Zincirine karşı savunmak için, Öldürme Zinciri aşamalarında ağ güvenlik savunmaları tasarlanır. Siber Öldürme Zincirine dayanan bir şirketin güvenlik savunmaları hakkında bazı sorular şunlardır:

• Öldürme Zincirinin her aşamasındaki saldırı göstergeleri nelerdir?

• Her aşamada saldırı göstergelerini tespit etmek için hangi güvenlik araçlarına ihtiyaç vardır?

• Şirketin bir saldırıyı tespit etme yeteneğinde boşluklar var mı?

Lockheed Martin'e göre, Kill Chain'in aşamalarını anlamak, savunma engelleri koymalarını, saldırıyı yavaşlatmalarını ve sonuçta veri kaybını önlemelerini sağladı. Şekil, Öldürme Zincirinin her aşamasının saldırıları engellemek ve düzeltmek için çaba ve maliyet miktarındaki artışa nasıl eşit olduğunu göstermektedir.(2)

1.Keşif

Bu, bilgisayar korsanlarının saldırıya karşı savunmasız olabilecek zayıf noktaları belirlemek için bir hedef hakkında olabildiğince fazla bilgi topladığı öldürme zincirinin ilk adımıdır. Keşif için ana odak alanları şunlardır:

1. Ağ bilgileri: Ağ türü, güvenlik zayıflıkları, alan adı ve paylaşılan dosyalar hakkında ayrıntılar (diğerlerinin yanı sıra)

2. Ana bilgisayar bilgileri: IP adresleri, MAC adresleri, işletim sistemi, açık bağlantı noktaları ve çalışan hizmetler (diğerlerinin yanı sıra) dahil olmak üzere bir ağa bağlı cihazlarla ilgili ayrıntılar

3. Güvenlik altyapısı: Güvenlik politikaları, kullanılan güvenlik mekanizmaları ve güvenlik araçları ve politikalarındaki zayıflıklar hakkında ayrıntılar (diğerlerinin yanı sıra)

4. Kullanıcı bilgileri: Bir kullanıcı, ailesi, evcil hayvanları, sosyal medya hesapları, takılma noktaları ve hobileri (diğerlerinin yanı sıra) hakkında özel bilgiler

Keşif sırasında bir tehdit aktörünün geçeceği üç alt aşama vardır: ayak izi, numaralandırma ve tarama.

1.1 Ayak İzi

Ayak izi, öldürme zincirinin keşif aşamasında kritik bir adımdır. Keşifin bu aşamasında mümkün olan maksimum süre harcanmaktadır. Bu aşama, daha sonra hedef

sistemi hacklemek için kullanılabilecek hedef sistemle ilgili verilerin toplanmasını gerektirir. Bu noktada toplanan bazı bilgi örnekleri şunları içerir:

*IP adresi

*VPN

*Ağ Haritası

*URL'ler

Tehdit aktörü, ayak izi elde etmek için çeşitli araçlar ve teknikler kullanacaktır.

1.2 Numaralandırma

Numaralandırma, müşteri adları, makine adları, ağ varlıkları ve hedef sistemlerde kullanılan farklı yönetimler gibi ayrıntıları çıkarmak için kullanılır. Bu noktada toplanan veriler, bilgisayar korsanının bir kuruluşun varlıklarındaki çeşitli zayıflıkları belirlemesini ve daha sonra ayırt etmesini sağladığı için çok önemlidir. Ayrıca, kuruluşun bilgi varlıklarını korumak için kullandığı güvenlik türü gibi bilgilerin belirlenmesine yardımcı olur. Bu noktada odak noktası, kuruluşun daha sonra sömürülebilecek zayıf güvenlik uygulamalarını kullandığı noktalardır.

1.3 Tarama

Bu, keşif aşamasında saldırganlar (ve öldürme zincirini kopyalayan etik bilgisayar korsanları) tarafından kullanılan en popüler metodolojidir. Bu metodoloji, hedef sistem içinde istismar edilebilecek veya kötüye kullanılabilecek hizmetleri belirlemek için kullanılır. Tarama işlemi, bir ağa bağlı tüm makineler, tüm açık bağlantı noktaları ve bir ağa bağlı diğer bilgi varlıkları gibi ayrıntıları ortaya çıkarmaya yardımcı olur.Tarama kullanılarak ortaya çıkan diğer önemli ayrıntılar şunları içerir:

- Sistem tarafından yürütülen hizmetler
- Sistem içinde çeşitli yönetimlere sahip müşteriler
- Sistemin herhangi bir gizli giriş yapıp yapmadığı
- Kuruluş için doğrulama gereksinimleri

Tarama çeşitli teknikler kullanılarak yapılabilir, ancak üç ana tarama türü vardır:

- **Port Tarama**: Bu tür bir tarama, canlı bağlantı noktaları, açık bağlantı noktaları, canlı çerçeveler ve sistemde kullanılan farklı yönetimler gibi sistemle ilgili bilgileri ortaya çıkarmaya yardımcı olur.
- **Ağ Tarama:** Bu tür bir tarama, sistem tarafından kullanılan ağla ilgili ayrıntıları ortaya çıkarmayı amaçlamaktadır. Bu noktada toplanan bilgiler arasında ağ anahtarları, yönlendiriciler, ağ topolojisi ve kullanımda olan ağ güvenlik duvarları bulunur (eğer bir güvenlik duvarı kullanılıyorsa). Erişilen veriler daha sonra bir organizasyonel grafik çizmek için kullanılabilir.
- **Zaafiyet Tarama:** Bu tür bir tarama, etik bilgisayar korsanlarının veya saldırganların daha sonra sistemi istismar etmek için kullanabilecekleri hedef sistemin eksikliklerini belirlemelerine yardımcı olur. Bu tür bir tarama normalde otomatik yazılım kullanılarak yapılır.

Ayak izi, numaralandırma ve tarama yapıldığında, bir tehdit aktörü keşiften öldürme zincirindeki bir sonraki aşamaya geçmeye hazırdır. İlk adım genelde en önemli adımdır. Evet diğer adımlarda karşılaşılacak bir sorun, çıkılan bu yolculuğu anlamsız kılabilir bir nedenle . Ancak ilk adım her zaman yeniden başlayacağımız ve nereye bakmamız gerektiğini gösteren bir pusuladır.

2.Silahlanma

Bir saldırgan keşif yaptıktan ve hedefinin zayıflıklarını bulduktan sonra, hangi silahın belirli hedeflerinde en iyi şekilde çalışacağı konusunda çok daha iyi bir fikir sahibi olacaklardır. Silahlaştırma, kurbanlarına saldırmak için araçların oluşturulduğu veya kullanıldığı aşamadır, örneğin kurbana göndermek için virüslü bir dosya oluşturmak. Hedefe ve saldırganın niyetine bağlı olarak, bir tehdit aktörünün seçtiği silah büyük ölçüde farklılık gösterebilir. Silahlandırma, kesinlikle belirli bir sıfır gün istismarına odaklanan kötü amaçlı yazılım yazmaktan bir kuruluş içindeki birden fazla güvenlik açığından yararlanmaya kadar her şeyi içerebilir.

3.Teslimat

Kulağa geldiği gibi, teslimat sadece silahı kurbana teslim etmektir. Mağdurun sistemlerine erişebilmek için saldırganlar genellikle erişim elde etmek için içeriklerine "kötü amaçlı yazılım" enjekte eder ve ardından kötü amaçlı içerik, kimlik avı, sistemleri tehlikeye atma ve hatta içeriden kullanıcıları kullanma gibi farklı şekillerde kurbana "teslim edilir".

4.İstismar

Bu, siber saldırının silahlaştırma aşamasında oluşturulan kötü amaçlı yazılım tarafından başlatıldığı aşamadır. Kötü amaçlı yazılım, hedefin güvenlik açığından/güvenlik açıklarından yararlanmak için kurbanın sisteminde etkinleştirilecektir.

Bu, ana saldırının başladığı aşamadır. Bir saldırı bu aşamaya ulaştığında, başarılı olduğu kabul edilir. Saldırgan normalde kurbanın ağında hareket etme ve tüm sistemlerine ve hassas verilerine erişme konusunda engelsiz bir özgürlüğe sahiptir. Saldırgan, bir kuruluştan hassas verileri çıkarmaya başlayacaktır. Bu, ticari sırları, kullanıcı adlarını, şifreleri, kişisel olarak tanımlanabilir verileri, çok gizli belgeleri ve diğer veri türlerini içerebilir.

Ek olarak, günümüzde birçok şirket hassas erişim kimlik bilgilerini paylaşılan dosyalarda tutuyor. Bu, personel üyelerinin çağrı merkezi kayıtları gibi paylaşılan hesaplara kolayca erişmelerine yardımcı olmayı amaçlamaktadır. Bununla birlikte, bir saldırgan bir ağı ihlal ettikten sonra, paylaşılan dosyalara gidebilir ve çalışanların herhangi bir hassas dosyayı paylaşıp paylaşmadığını öğrenebilir.

Tehdit aktörleri, bu aşamanın etkisini ilerletmek için sömürü sırasında genellikle ayrıcalık yükseltmesi de yapacaklardır.

4.1 Yetki Yükseltme

İlk ihlalleri sırasında, bilgisayar korsanları yalnızca hedeflerine atanan yönetici ayrıcalıklarına sahip bilgisayarlara veya sistemlere doğrudan erişim elde edeceklerdir. Bu nedenle, yönetici hakları kazanmak ve aynı kuruluştan daha da fazla veri çıkarmak için genellikle çeşitli ayrıcalık yükseltme tekniklerini kullanacaklardır. Bu nedenle, sömürü aşamasında bilgisayar korsanları ayrıcalık yükseltmeyi deneyebilir.

Ayrıcalık yükseltme dikey ve yatay olarak iki şekilde yapılır. İkisi arasındaki farka kısaca değinecek olursak:

Dikey Yetki Yükseltme	**Yatay Yetki Yükseltme**
Saldırgan, daha yüksek bir yetki seviyesine sahip bir hesaptan diğerine geçer.	Saldırgan aynı hesabı kullanır, ancak ayrıcalıklarını yükseltir.
Araçlar ayrıcalıkları yükseltmek için kullanılır.	Orijinal hedefin kullanıcı hesabı, ayrıcalıkları yükseltmek için kullanılır.

Tablo 1:Dikey ve yatay ayrıcalık yükseltmesinin karşılaştırılması

Her iki ayrıcalık yükseltme biçimi de, saldırgana bir sistemdeki yönetici düzeyinde işlevlere veya hassas verilere erişim sağlamak için gerçekleştirilir.

4.1.1 Dikey Ayrıcalık Yükseltme

Dikey ayrıcalık yükseltme, daha düşük ayrıcalıklı bir noktadan başlayan ve ardından ayrıcalıklı kullanıcının seviyesine ulaşana veya hedeflediği işleme kadar ayrıcalıkları yükselten bir saldırıdır. Kullanıcının erişim haklarını yükseltmek için bazı çekirdek düzeyinde işlemler gerçekleştirmesi gerektiğinden karmaşık bir prosedürdür.

İşlemler tamamlandıktan sonra, saldırgan herhangi bir yetkisiz kodu çalıştırmasına izin veren erişim hakları ve ayrıcalıkları ile kalır. Bu yöntem kullanılarak elde edilen haklar, bir yöneticiden daha yüksek haklara sahip bir süper kullanıcının haklarıdır.

Bu ayrıcalıklar nedeniyle, bir saldırgan bir yöneticinin bile durduramayacağı çeşitli zararlı eylemler gerçekleştirebilir.

4.1.2 Yatay Ayrıcalık Yükseltme

Öte yandan yatay ayrıcalık yükseltmesi, bir kullanıcının ilk erişimden elde edilen aynı ayrıcalıkları kullanmasına izin verdiği için daha basittir.

İyi bir örnek, bir saldırganın bir ağ yöneticisinin oturum açma kimlik bilgilerini çalabildiği yerdir. Yönetici hesabı, saldırganın eriştikten hemen sonra üstlendiği yüksek ayrıcalıklara zaten sahiptir.

Yatay ayrıcalık yükseltmesi, bir saldırgan normal bir kullanıcı hesabı kullanarak korunan kaynaklara erişebildiğinde de gerçekleşir. İyi bir örnek, normal bir kullanıcının yanlışlıkla başka bir kullanıcının hesabına erişebilmesidir. Bu normalde oturum ve çerez hırsızlığı, siteler arası komut dosyası oluşturma, zayıf şifreleri tahmin etme ve tuş vuruşlarını kaydetme yoluyla yapılır.

Bu aşamanın sonunda, saldırgan normalde bir hedef sisteme iyi kurulmuş uzaktan erişim giriş noktalarına sahiptir. Saldırganın birkaç kullanıcının hesaplarına da erişimi olabilir. Saldırgan ayrıca, hedefin sahip olabileceği güvenlik araçlarından algılamadan nasıl kaçınacağını da bilir.

5.Kurulum

Yükleme sırasında, saldırganlar bir ağ içinde serbestçe dolaşır, değerli olduğunu düşündükleri tüm verileri kopyalar ve tespit edilmemesini sağlarlar. Veriler zaten çalındığında ve yayınlanabileceği veya satılabileceği bir önceki aşamada saldırıyı sona erdirme seçeneği vardır. Bununla birlikte, bir hedefi tamamen bitirmek isteyen yüksek motivasyonlu

saldırganlar saldırıya devam etmeyi tercih ediyor. Saldırganlar, istedikleri zaman kurbanın bilgisayarlarına ve sistemlerine erişmelerini sağlayan bir arka kapı kurarlar.

Bu aşamaya girmenin temel amacı, sömürüden başka ve hatta daha zararlı bir saldırı gerçekleştirmek için zaman kazanmaktır. Saldırgan, geçmiş verileri ve yazılımları taşımak ve bir kuruluşun donanımına saldırmak için motive olur. Kurbanın güvenlik araçları, bu noktada, saldırının devam etmesini tespit etmede veya durdurmada etkisizdir. Saldırgan normalde kurbanlara birden fazla erişim noktasına sahiptir, böylece bir erişim noktası kapalı olsa bile erişimleri tehlikeye girmez.

6.Komuta ve Kontrol

Bu aşama, kurulum aşamasında kurulan arka kapı üzerine kuruludur. Komuta ve Kontrol aşamasında, saldırgan hedefini uzaktan manipüle etmek için arka kapısını sisteme kullanır. Tehdit aktörü, mağdur bilgisayarından uzaklaşana kadar bekler ve saldırılarında ona yardımcı olacak eylemleri gerçekleştirir.

7. Eylemler

Hedefler Üzerine Eylemler, herhangi bir siber saldırının en korkulan aşamasıdır. Saldırganın veri ve yazılımı aşan hasar verdiği yerdir. Bir saldırgan, kurbanın donanımının işleyişini kalıcı olarak devre dışı bırakabilir veya değiştirebilir. Saldırgan, ele geçirilmiş sistemler ve bilgi işlem cihazları tarafından kontrol edilen donanımı yok etmeye odaklanır.

Bu aşamaya gelen bir saldırıya iyi bir örnek, İran'ın nükleer istasyonuna Stuxnet saldırısıdır. Fiziksel kaynaklara hasara yol açmak için kullanılan ilk kaydedilen dijital silahtı. Tıpkı diğer saldırılar gibi, Stuxnet daha önce açıklanan aşamaları takip etti ve bir yıldır tesisin ağında ikamet ediyordu. Başlangıçta Stuxnet, nükleer tesisteki valfleri manipüle etmek için kullanıldı ve basıncın birikmesine ve tesisteki birkaç cihaza zarar vermesine neden oldu. Kötü amaçlı yazılım daha sonra daha büyük bir hedefe, santrifüjlere saldırmak için değiştirildi. Bu üç aşamada elde edildi.

Kötü amaçlı yazılım, internete bağlı olmadıkları için USB flaş sürücüler aracılığıyla hedef bilgisayarlara iletildi. Hedef bilgisayarlardan birine bulaştığında, kötü amaçlı yazılım kendini çoğalttı ve diğer bilgisayarlara yayıldı. Kötü amaçlı yazılım, Siemens'in mantık denetleyicilerinin programlanmasını kontrol etmek için kullanılan Step7 adlı bazı yazılımlarına bulaştığı bir sonraki aşamaya geçti. Bu yazılım ele geçirildikten sonra, kötü amaçlı yazılım nihayet program mantık denetleyicilerine erişim sağladı. Bu, saldırganların nükleer santraldeki çeşitli makineleri doğrudan çalıştırmasına izin verdi. Saldırganlar, hızlı dönen santrifüjlerin kontrolden çıkmasına ve kendi başlarına parçalanmasına neden oldu.

Stuxnet kötü amaçlı yazılımı, bu aşamanın ulaşabileceği yükseklikleri gösterir. Saldırganlar çoktan erişim elde ettiği, ayrıcalıklarını yükselttiği ve güvenlik araçlarının gözden uzak durduğu için İran nükleer tesisinin kendini koruma şansı yoktu. Tesis operatörleri, bilgisayarlarda birçok özdeş hata aldıklarını, ancak tüm virüs taramalarının enfekte

olmadıklarını gösterdiğini söyledi. Saldırganların, vanalarla ele geçirilmiş tesis içinde solucanın birkaç test çalışması yaptığı açıktır. Etkili olduğunu öğrendiler ve santrifüjlere saldırmak ve İran'ın nükleer silah beklentilerini düşürmek için ölçeklendirmeye karar verdiler.

Esasen, bu aşama, bilgisayar korsanının ele geçirilmiş bir sisteme gerçek zarar verdiği yerdir. Hedeflere İlişkin Eylemler, ağların, sistemlerin ve verilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini tehlikeye atmayı amaçlayan tüm faaliyetleri içerir. Örneğin, Hedeflerde Eylemler aşamasında gerçekleştirilebilecek bir saldırı türü veri sızmasıdır.

7.1Veri sızması

Veri sızması, bir tehdit aktörü bir kuruluşun verilerini çaldığında meydana gelir. Bu, aşağıdaki yollardan herhangi biriyle gerçekleşebilir:

- E-posta - bilgisayar korsanlarının sadece internet üzerinden e-posta yoluyla gönderdikleri sızma için kullandıkları uygun yöntemlerden biri. Kurbanın makinesindeki tek kullanımlık e-posta hesaplarına hızlı bir şekilde giriş yapabilir ve verileri başka bir atılabilir hesaba gönderebilirler.

- İndirme - kurbanın bilgisayarı bilgisayar korsanının bilgisayarına uzaktan bağlandığında, verileri doğrudan yerel cihazlarına indirebilir.

- Harici sürücüler - bilgisayar korsanları ele geçirilmiş sisteme fiziksel erişime sahip olduklarında, verileri doğrudan harici sürücülerine sızdırabilirler.

- Bulut sızması - bir bilgisayar korsanı bir kullanıcının veya kuruluşun bulut depolama alanına erişim elde ederse, buluttan gelen veriler indirmeler yoluyla sızdırılabilir. Öte yandan, bulut depolama alanları sızma amacıyla da kullanılabilir. Bazı kuruluşların, bilgisayar korsanlarının e-posta adreslerine veri gönderemeyeceği kadar katı ağ kuralları vardır. Bununla birlikte, çoğu kuruluş bulut depolama alanlarına erişimi engellemez. Bilgisayar korsanları bunları veri yüklemek ve daha sonra yerel cihazlarına indirmek için kullanabilir.

- Kötü amaçlı yazılım - bu, bir bilgisayar korsanının kurbanın bilgisayarına kurbanın bilgisayarından veri göndermek için özel olarak tasarlanmış kötü amaçlı yazılım bulaştırdığı yerdir. Bu veriler tuş vuruşu günlüklerini, tarayıcılarda depolanan şifreleri ve tarayıcı geçmişini içerebilir.

Saldırganlar normalde sızma sırasında büyük miktarda veri çalar. Bu veriler ya istekli alıcılara satılabilir ya da halka sızdırılabilir.

7.2 Gizleme

Bu, bazı saldırganların görmezden gelmeyi seçebileceği saldırının son aşamasıdır. Buradaki asıl amaç, saldırganların çeşitli nedenlerle izlerini kapatmalarıdır. Saldırganlar tanınmak istemiyorlarsa, bir siber saldırıyı takip eden adli soruşturma sürecini karıştırmak, caydırmak veya yönlendirmek için çeşitli teknikler kullanırlar. Bununla birlikte, bazı saldırganlar, isimsizce çalışırlarsa veya istismarlarıyla övünmek istiyorlarsa, izlerini maskesiz bırakmayı tercih edebilirler.

Gizleme çeşitli şekillerde yapılır. Saldırganların düşmanlarının onlara yetişmesini engellemenin yollarından biri de kökenlerini gizlemektir; bir diğeri de olaydan sonra izlerini gizlemektir. Bu aşamada tehdit aktörleri tarafından kullanılan bazı yaygın teknikler şunlardır:

- Şifreleme - siber izinsiz girişlerle ilgili tüm kanıtları kilitlemek için bilgisayar korsanları, eriştikleri tüm sistemleri şifrelemeyi seçebilir. Bu, meta veriler gibi herhangi bir kanıtı adli müfettişler için etkili bir şekilde okunamaz hale getirir. Buna ek olarak, mağdurun bilgisayar korsanlarının bir sistemi tehlikeye attıktan sonra gerçekleştirdiği kötü niyetli eylemleri farketmesi önemli ölçüde zorlaşır.

- Steganografi - bazı olaylarda, bilgisayar korsanları mağdur kuruluşlarda içeriden gelen tehditlerdir. Hassas verileri bir ağ dışına gönderirken, verileri sızdırırken tespit edilmemek için steganografi kullanmayı tercih edebilirler. Bu, gizli bilgilerin görüntüler gibi gizli olmayan verilerde gizlendiği yerdir. Görüntüler, önemsiz göründükleri için kuruluşlara ve dışına serbestçe gönderilebilir.

Bu nedenle, bir bilgisayar korsanı herhangi bir alarm vermeden veya yakalanmadan steganografi aracılığıyla çok sayıda hassas bilgi gönderebilir.

- Günlükleri değiştirme - saldırganlar, yakalanan şüpheli erişim olayları olmadığını göstermek için sistem erişim günlüklerini değiştirerek bir sistemdeki varlıklarını silmeyi seçebilirler.

- Tünel açma - burası, bilgisayar korsanlarının kurbanın ağından başka bir konuma veri gönderdikleri güvenli bir tünel oluşturduğu yerdir. Tünel açma, tüm verilerin uçtan uca şifrelenmesini ve aktarım sırasında okunamamasını sağlar. Bu nedenle, kuruluş şifreli bağlantılar için izleme ayarlamadığı sürece veriler güvenlik duvarları gibi güvenlik araçlarından geçecektir.

- Soğan yönlendirme - bilgisayar korsanları verileri gizlice sızdırabilir veya soğan yönlendirme yoluyla birbirleriyle iletişim kurabilir. Soğan yönlendirmesi birden fazla şifreleme katmanı içerir ve veriler hedefe ulaşana kadar bir düğümden diğerine sıçranır. Araştırmacıların bu tür bağlantılar aracılığıyla veri izlerini takip etmeleri zordur, çünkü her bir şifreleme katmanını kırmaları gerekir.

- Sürücüleri silmek - gizlemenin son yöntemi kanıtları yok etmektir. Bilgisayar korsanları, mağdurların bilgisayar korsanları tarafından gerçekleştirilen kötü niyetli faaliyetleri

tanımasını imkansız hale getirmek için ihlal ettikleri bir sistemin sabit sürücüsünü silebilir. Temiz mendiller sadece veri silinerek yapılmaz. Sabit sürücü içerikleri kurtarılabildiğinden, bilgisayar korsanları verilerin üzerine birkaç kez yazacak ve diski temizleyecektir. Bu, sürücünün içeriğinin kurtarılmasını zorlaştıracaktır.

3.Siber Öldürme Zincirini Durdurmak İçin Kullanılan Güvenlik Kontrolleri

Bir kuruluşun siber öldürme zincirinin farklı aşamalarını durdurmak için kullanabileceği birkaç yöntem vardır. Bunu çeşitli güvenlik kontrolleri uygulayarak yapabilir. Belirlenen etkili güvenlik kontrollerinden bazıları şunlardır:

1.Algıla: Bu güvenlik kontrolünde, bir kuruluş saldırganların sisteme erişmeye yönelik tüm girişimlerini belirleyecektir. Bu, bir sistemin potansiyel güvenlik açıklarını belirlemek için dışarıdan gelenler tarafından sistemin taramaya çalışılmasını içerir.

2. Engelle: Saldırıları devam ederken engellemek. Güvenlik ekibi, olası herhangi bir saldırıyla ilgili bilgi aldıklarında herhangi bir saldırıyı durdurmak için hızla hareket etmelidir.

3. Bozma: Bu, güvenlik ekibinin saldırganlar ve sistem arasındaki herhangi bir iletişimi engelleme ve bu iletişimi kesme çabalarını içerir. İletişim, saldırganların saldırılarını gerçekleştirmeden önce sistemin çeşitli öğelerini belirlemek için sistemde yaptıkları sorgular hakkında geri bildirim olabilir.

4. Bozulma: Bu, saldırıların bu saldırıların zararını sınırlama gücünü azaltmayı amaçlayan çeşitli önlemlerin geliştirilmesini ve uygulanmasını içerir.

5. Aldatma: Bu, saldırganlara organizasyondaki varlıklar hakkında yanlış bilgiler sağlayarak kasıtlı olarak yanıltacak çeşitli önlemlerin uygulanmasını içerir.

Siber öldürme zinciri aşamalarının her birinde, yukarıda belirtilen güvenlik kontrollerini uygulamak için güvenlik araçları kullanılabilir. Bunlar:

- Keşif aşaması: Tespit, web analizi, ağ izinsiz giriş algılama sistemleri ve tehdit istihbaratı aracılığıyla yapılır. Reddetme, güvenlik duvarı erişim kontrol listeleri ve bilgi paylaşım politikalarının uygulanması yoluyla yapılır.

- Silahlaştırma aşaması: Algılama, tehdit istihbaratı ve ağ izinsiz giriş tespit sistemleri kullanılarak mümkün kılınır. Reddetme, ağ izinsiz giriş önleme sistemleri kullanılarak yapılır.

- Teslimat aşaması: Teslim aşamasında, algılama uç nokta kötü amaçlı yazılım koruması kullanılarak yapılır; de- nying proxy filtreleri ve ana bilgisayar tabanlı izinsiz giriş önleme kullanılarak yapılır; kesinti satır içi bir antivirüs ile yapılır; bozma kuyruklama ile yapılır; içerme, uygulama farkında güvenlik duvarları ve bölgeler arası ağ izinsiz giriş algılama sistemleri tarafından yapılır.

- Sömürü aşaması: Algılama, uç nokta kötü amaçlı yazılım koruması ile yapılır; reddetme yama yönetimi ile yapılır; veri yürütme önleme ile bozulma mümkündür; içerme, güven bölgeleri ve bölgeler arası ağ izinsiz giriş algılama sistemleri tarafından yapılır.

- Kurulum aşaması: Algılama, güvenlik bilgileri ve olay yönetim sistemleri kullanılarak yapılır; reddetme, güçlü şifreler ve ayrıcalık ayrımı kullanılarak yapılır; kesinti, yönlendirici erişim kontrol listeleri tarafından yapılır; içerme, güven bölgeleri ve bölgeler arası ağ izinsiz giriş algılama sistemleri tarafından yapılır.

- Komut ve kontrol aşaması: Algılama, ana bilgisayar tabanlı izinsiz giriş algılama sistemleri kullanılarak yapılır; reddetme, güvenlik duvarı erişim kontrol listeleri ve ağ segmentasyonu kullanılarak yapılır; kesinti, ana bilgisayar tabanlı izinsiz giriş önleme sistemleri tarafından yapılır; bozma bir tarapı tarafından yapılır; aldatma, bir Alan Adı Sistemi yönlendirmesi ile yapılır; içerme, Alan Adı Sistemi çukurları tarafından yapılır.

- Hedefler aşamasındaki eylemler: Uç nokta kötü amaçlı yazılım koruması ve Güvenlik Bilgileri ve Olay Yönetimi (SIEM) kullanılarak tespit mümkündür; reddetme, dinlenmedeki veri şifrelemesi ve çıkış filtrelemesi yoluyla yapılır; kesinti, uç nokta kötü amaçlı yazılım koruması ve bir veri kaybını önleme sisteminin kullanımı ile yapılır; bozulma, hizmet kalitesiyle yapılır; aldatma, bir honeypot kullanılarak elde edilir; olay müdahale programları ve güvenlik duvarı erişim kontrol listeleri kullanılarak içerme mümkün kılınır.

Bu güvenlik kontrollerine ek olarak, kuruluşlar öldürme zincirini kullanarak saldırganları engellemek için KVDA (Kullanıcı ve Varlık Davranış Analizi) ve personel için güvenlik farkındalığı eğitimi gibi başka yöntemler de kullanabilir.

Siber Öldürme Zinciri Raporu Değerlendirmesi ve Sonuçlar

Bu rapor, **Siber Öldürme Zinciri (Cyber Kill Chain)** kavramını ayrıntılı bir şekilde ele alarak siber saldırganların saldırı süreçlerini ve bunlara karşı savunma stratejilerini incelemektedir. Lockheed Martin tarafından geliştirilen bu model, siber saldırıların belirli aşamalar halinde gerçekleştiğini ortaya koyar ve savunma ekiplerine saldırıları önlemek için sistematik bir bakış açısı sunar.

Araştırmada Kazanılan Bilgiler ve Önemli Çıkarımlar

1. **Siber Saldırıların Sistematik Aşamaları:**
    - **Keşif, Silahlanma, Teslimat, İstismar, Kurulum, Komut & Kontrol, Eylem** gibi aşamalardan oluşan **Siber Öldürme Zinciri**, saldırganların izlediği metodolojiyi anlamamıza yardımcı olmaktadır.
    - İlk aşama olan **Keşif** (Reconnaissance), saldırganların sistem hakkında bilgi topladığı kritik bir süreçtir ve başarılı saldırıların temelini oluşturur.
2. **Yetki Yükseltme ve Aşamalar Arası Geçişler:**
    - **Dikey Yetki Yükseltme** (PrivEsc) ve **Yatay Yetki Yükseltme** süreçleri saldırganlara sistem içinde genişleme imkanı sunar.
    - Kurulum aşaması ile saldırganlar kalıcılık elde eder ve tespit edilmelerini zorlaştıran teknikler kullanırlar.
3. **Gerçek Dünya Örnekleri:**
    - **Stuxnet** saldırısı gibi tarihsel olaylar, Siber Öldürme Zinciri'nin nasıl etkili bir saldırı stratejisi sunduğunu göstermektedir.
    - Saldırganlar, **kimlik avı, kötü amaçlı yazılım, zero-day exploitler** gibi yöntemleri kullanarak sistemlere giriş sağlarlar.
4. **Savunma Stratejileri ve Güvenlik Kontrolleri:**
    - **Tespit, Engelleme, Bozma, Aldatma** gibi yöntemlerle saldırı zinciri kırılabilir.
    - Güvenlik ekipleri, **IDS/IPS, SIEM, Honeypots, ağ segmentasyonu, uç nokta koruması, şifreleme** gibi araçlarla saldırıları engelleyebilir.
    - **KVDA (Kullanıcı ve Varlık Davranış Analizi)** ve **personel farkındalık eğitimi** gibi önlemler, sosyal mühendislik saldırılarını önlemekte kritik rol oynar.

Sonuç

Bu rapor, **siber saldırıların nasıl gerçekleştirildiğini ve siber güvenlik önlemlerinin nasıl geliştirilebileceğini** derinlemesine ele almaktadır. Siber Öldürme Zinciri modelinin anlaşılması, **tehdit avcılığı (threat hunting), saldırı tespiti ve olay müdahalesi (incident response)** açısından büyük önem taşır.

Referanslar:

(1)CİSCO network akademisi siber güvenlik makaleleri https://www.netacad.com/

(2) CyberSecurity Attack and Defense Strategies Dr. Erdal Özkaya

(3) Çeşitli internet kaynakları ve editöryal yardım için ChatGPT.