ÖN BİLGİ

Bu belge

- https://www.bgasecurity.com/makale/apt-saldirilari-karsisinda-guvenlik-sistemlerin-yetersiziligi/

resmi adresindeki veya linkin kırık olması ihtimaline karşın alternatif olarak

- https://www.includekarabuk.com/kitaplik/indirmeDeposu/Siber_Guvenlik_Teknik_Makaleler/Teori/BaskalarinaAitMakaleler/APT%20Sald%C4%B1r%C4%B1lar%C4%B1%20Kar%C5%9F%C4%B1s%C4%B1nda%20G%C3%BCvenlik%20Sistemlerin%20Yetersizili%C4%9Fi.pdf

adresindeki makaleye çalışılarak elde edilen notlarımı kapsamaktadır. Bu çıkarılan notlar belgemde alıntılar ve/veya kişisel ilavelerim mevcuttur.

1)

Günümüz güvenlik problemlerinin temelini oluşturan son kullanıcıların farkındalık eksikliği ve zararlı yazılımlar karşısında Firewall, IPS, Antivirus gibi klasik siber güvenlik sistemlerinin yetersizliği anlaşılmıştır.

(Page 3)

2)

Geleneksek Güvenlik Yaklaşımı
- Bu yaklaşımda Router, Firewall, IPS, IDS sistemleri kullanılır.
- Bütçelerin tamamına yakını standart (geleneksel) savunma sistemlerine harcanır.
- Kullanıcılara yönelik tehditler genellikle es geçirilir. Çünkü biz onun zaten farkındayız yaklaşımı sergilenmektedir.
- Gerçekleştirilen güvenlik testleri (pentest'ler) firmaların yapılacaklar listesindeki bir maddeyi daha geçebilmek için geçiştirilen şey olarak görülmektedir.

(Page 6)

3)

Güvenliğin artması para harcama ile doğru orantılı değildir.

(Page 7)

4)

Birçok kişi/kurum son bir yıl içerisinde APT benzeri sofistike saldırılara maruz kaldılar.

(Page 8)

5)

APT Nedir?
The term APT (Advanced Persistent Threat) was first named by the US Air Force in 2006 to describe the complex (i.e. “Advanced”) cyber attacks against specific targets over a longer period of time (i.e. “persistent”).

(Page 9)

6)

APT (Advanced Persistent Threat) 2010 yılında gündemimize girmiş göreceli olarak yeni bir konudur.

(Page 9)

7)

APT ile Mücadele
APT kolay tanımlanabilir bir konu olmadığı için mücadelesi de zordur. Tanımlanabilir tehditleri engellemek ise kolaydır.

(Page 11)

8)

APT Yaşam Döngüsü

| Aşama | Eylem | Detaylar |
|---|---|---|
| I. Faz | Keşif ve Hedef Belirleme | Hedefin ve hedefe ulaşılabilecek yollar tespit edilir. |
| II. Faz | Oltalama Epostasını Gönderilmesi | Genellikle bu yöntem tercih edilir (kolay, zahmetsiz ve az teknik detay gerektirdiğinden) |
| III. Faz | Hedefle İrtibata Geçebilme | Hedef sisteme arka kapı yüklemesi yapılır. |
| IV. Faz | Hak Yükseltme ve Hedef Alanını genişletme | Hedef sistemde daha yüksek yetkili kullanıcı haklarına geçiş ve farklı ağları keşif yapılır. |
| V. Faz | Veri Kaçırma | Hedef sistemden ilgili verilerin şifrelenerek (?) dışarı çıkartılması |
| VI. Faz | Erişimi Kalıcı Kılma | İstenildiğinde tekrar bağlanılabilecek bir yapıyı kurup logların ve diğer delillerin silinmesi |

(Page 12)

9)

Saldırganın motivasyonuna göre APT saldırısı 1 gün de sürebilir 4 yıl da sürebilir.

(Page 13)

10)

APT'ye Hatalı Yaklaşımlar
- Saldırgan bula bula bizi mi bulacak görüşüne sahip olmak
- Sadece ürün bazlı bu sorunu çözmeye çalışmak
- Sadece ağ trafiğini dinleyerek bu sorunu çözmeye çalışmak

(Page 15)

11)

Klasik güvenlik korumaları tıpkı Aspirin gibidir. Yani bilinen basit durumlar için işe yarar.

(Page 22)

12)

Örneğin APT saldırısı sonrası saldırgan elde ettiği FTP account'ı ile sunucuya bağlanır ve FTP sunucudaki sık kullanılan dosyaları inceleyerek orjinallerini arka kapılı sürümleriyle değiştirir. Üç gün sonra IP adresi X.Y.Z.T'li bir istemci ilgili sayfaya bağlanır ve sonrasında saldırgan hızlıca istemcinin bilgisayarına erişim sağlar. Bellek dökümü ile de parolasının açık halini elde edebilir.

(Page 27)

13)

Bir APT Örneği
Saldırgan çok bilinen bir blog sisteminin Türkiye sistesini hack'ler. Blog sisteminin bir sonraki sürümü için zaman sayar ve yeni sürüm çıktığında siteye eklenen bu yeni sistemin Türkçe sürüm dosyaları içerisine bir adet arka kapı barındıran php dosyası ekler. Bir hafta sonra ilgili dosyanın download sayısı 173 bin olmuştur. Saldırgan tek bir hareketi ile 173 bin sisteme arka kapı bırakabilmiş olur. Daha sonra saldırgan blog sistemini yayınlayan sunucunun log'larından ilgili dosyaları indren IP adreslerini tespit eder. Böylece istemciler (kurbanlar) indirdikleri arka kapılar üzerinden ele geçirilebilir.

(Page 28)

14)

Türkiye'den Örnek APT Testi
Firmanın ismi hariç hiçbir bilgi alınmamıştır. Sosyal ağ sitelerinden araştırma yapılarak hedef firmaya ait 50 kişi belirlenir (linkedin). Firmanın twitter/facebook sayfaları takip edilerek kampanya/duyuru zamanı beklenir. Kampanya ile ilgili siteye benzer bir alan adı alınarak MX kayıtları girilir ve sahte eposta'lar hazırlanır. 50 çalışana eposta gönderilir ve beklemede kalınır. İlk 10 dakika içerisinde 7 kullanıcı epostada belirtilen sisteme erişmeye çalışır. Saldırgan bunun üzerine elde personellerin hesap bilgilerini elde eder. Farklı kimlikle görünmek adına VPN kurmak için gece 03:00 beklenir. VPN kurulur ve RDP ile elde edilen hesap bilgileri kullanılarak kurbanların bilgisayarına bağlanılır. Antivirus'leri durdurulur. Kalıcı bir arka kapı yüklenir. Kuruma bir hafta içerisinde gerçekleştirilen siber saldırı simulasyonu sonucunda elde edebildikleri bulgular soruldu. IPS log'ları hariç elle tutulur hiçbir bilgi elde edemediklerin söylediler. Kısacası kurum yaptığı milyon dolarlık yatırımın gerçek bir APT saldırısı karşısında kendisini savunamayacağını gördü.

(Page 30-32)

15)

Sonuç
İnternet üzerinden elde edilen veya yerel ağda dolaşımda olan her türlü çalıştırılabilir dosya kontrolden geçmelidir.

(Page 33)

16)

APT teknik bir problemden öte iş dünyasını ilgilendiren hassas bir konudur.

(Page 33)