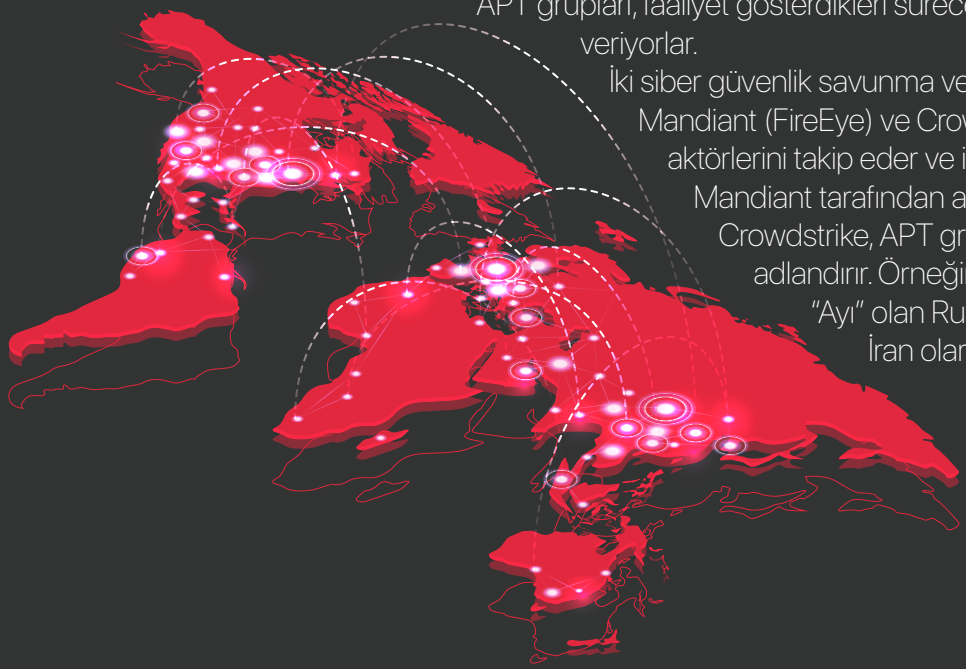
Advanced Persistent Threat

Advanced persistent threat (APT) gelişmiş kalıcı tehdit demektir. Gelişmiş Kalıcı Tehditler (APT'ler) keşfedilmeden mümkün olduğunca değerli verilere sızmak ve / veya dışarı sızmak için tasarlanmış uzun vadeli operasyonlardır. Terimin genel olarak devletler sponsorluğu ile ilişkilendirilse de birkaç yıldır , belirli hedefler için büyük ölçekli hedeflenmiş müdahaleler yapan ulus dışı devlet gruplarının birden fazla örneği görülmektedir.

APT'ler genellikle uluslar veya çok büyük kuruluşlar tarafından desteklenmektedir. Genel amaçları diğer hack olaylarından farklı olarak uzun soluklu sistem içerisinde kalma ve uzun süreli bilgi çalmakdır. Yani APT'leri diğer siyah şapkalı hackerlardan veya bilgisayar korsanlarından ayıran çabuk olarak ayrılmaması ve amacı için uzun soluklı bir saldırı gerçekleştirmesidir. Bu da diğerlerinden çok daha zararlı ve tehlikeli olduğunun en büyük göstergesi olarak karşımıza çıkıyor.

APT, her yerdeki işletmeler için radarda olması gereken bir saldırı yöntemidir.
APT saldırganları, büyük hedeflere erişim kazanmanın bir yolu olarak nihai hedeflerinin tedarik zincirini oluşturan küçük şirketleri giderek daha fazla kullanıyor.
Tipik olarak daha az savunulan şirketleri basamak taşları olarak kullanıyorlar.

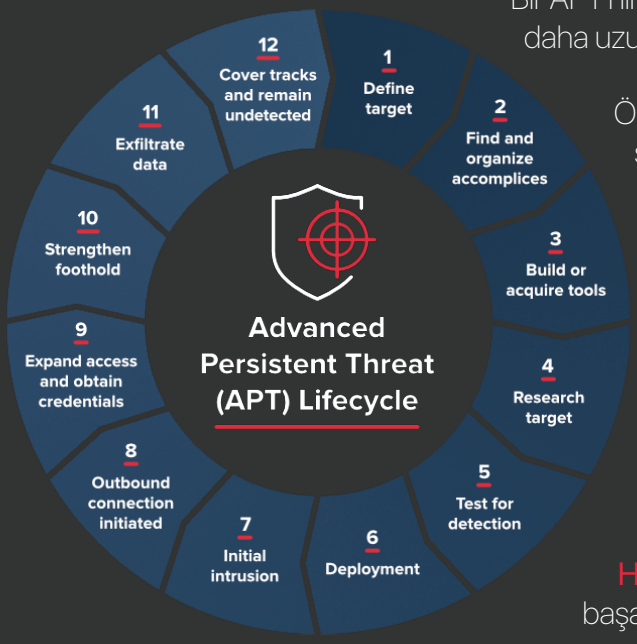
MITRE ATT & CK , APT operasyonları olarak kaydedilmiş 107 farklı gruba sahiptir. Bu gruplar tüm dünyaya yayılmıştır ve büyük ölçüde finanse edilen devlet destekli grupları ve siber güvenlik dünyasında büyük bir göçük yapan paçavra etiketli takımları içerir.



APT grupları, faaliyet gösterdikleri sürece kendilerine şifreli takma adlar veriyorlar.
İki siber güvenlik savunma ve araştırma organizasyonu - Mandiant (FireEye) ve Crowdstrike - dünyadaki tehdit aktörlerini takip eder ve izler. APT grupları sayısal olarak Mandiant tarafından adlandırılır ve ülkeye bağlı olarak Crowdstrike, APT gruplarını hayvanlara göre adlandırır. Örneğin, bir Çin APT grubu "Panda", "Ayı" olan Rus grupları ve "Yavru Kedi" ile İran olarak adlandırılmıştır.

https://github.com/abdullahcicekli https://www.linkedin.com/in/cicekliabdullah/ https://www.instagram.com/cicekli_abdullah/

İleri Kalıcı Tehdit (APT) Yaşam Döngüsü



Bir APT'nin yaşam döngüsü, diğer saldırı türlerinden çok daha uzun ve daha karmaşıktır.

Örneğin Stuxnet, yüksek değerli bir hedefe stratejik bir saldırıya yol açtı: programcılar, İran'ın uranyum zenginleştirmek için kullandığı belirli bir üretici tarafından belirli bir kontrol panosuna saldırmak için kod yazdı. Ve bunu bulmak zor olacak şekilde yazdılar, bu yüzden mümkün olduğunca çok hasar vermek için çok zaman vardı. Bir APT'nin yaşam döngüsü diğer saldırı türlerinden çok daha uzun ve karmaşıktır.

Hedefi Tanımlayın : Kimi hedeflediğinizi, neyi başarmayı umduğunuzu ve nedenini belirleyin.

İştirakçiler Bulun ve Düzenleyin : Ekip üyelerini seçin, gerekli becerileri belirleyin ve içeriden erişim sağlayın.

Araç Oluşturma veya Edinme : Şu anda mevcut olan araçları bulun veya iş için doğru araçları almak üzere yeni uygulamalar oluşturun.

Araştırma Hedefi : İhtiyacınız olan erişimi, hedefin hangi donanımı ve yazılımı kullandığını ve saldırıyı en iyi şekilde nasıl tasarlayacağınızı keşfedin.

Algılama Testi : Yazılımınızın küçük bir keşif sürümünü dağıtın, iletişimleri ve alarmları test edin, zayıf noktaları belirleyin.

Konuşlandırma : Dans başlar. Tam paketi dağıtın ve sızmaya başlayın.

İlk Saldırı : Ağın içine girdiğinizde, nereye gideceğinizi öğrenin ve hedefinizi bulun.

Giden Bağlantı Başlatıldı : Hedef alındı, tahliye talebinde bulundu. Hedeften veri göndermeye başlamak için bir tünel oluşturun.

Erişimi Genişletin ve Kimlik Bilgilerini Alın : Hedef ağın içindeki denetiminiz altında bir "hayalet ağ" oluşturun ve daha fazla hareket elde etmek için erişiminizi kullanın.

Ayak Dayanağını Güçlendirin : Daha fazla zombi oluşturmak veya diğer değerli yerlere erişiminizi genişletmek için diğer güvenlik açıklarından yararlanın.

Verileri Genişletme : Aradığınızı bulduğunuzda, tekrar temel alın.

İzleri Örtün ve Fark Edilmeden Kalın : Tüm işlem ağda gizli kalma yeteneğinize bağlıdır. Gizli kontrollerinizde yuvarlanmaya devam edin ve kendinizden sonra temizlediğinizden emin olun.

https://github.com/abdullahcicekli https://www.linkedin.com/in/cicekliabdullah/ https://www.instagram.com/cicekli_abdullah/

Gelişmiş Kalıcı Tehditler (APT) Nasıl Yönetilir ?

Kendinizi APT'lerden korumak katmanlı bir güvenlik yaklaşımı gerektirir :

Her Şeyi İzleyin : Verileriniz hakkında yapabileceğiniz her şeyi toplayın.

Verileriniz nerede ?
Bu verilere kimler erişiyor ?
Güvenlik duvarında kimler değişiklik yapar ?
Kimlik bilgilerinde kim değişiklik yapabilir ?
Hassas verilere kimler erişiyor ?
Ağınıza kim erişiyor ve nereden hizmet alıyorsunuz ?

Ağınızda ve verilerinizde gerçekleşen her şeyi bilmelisiniz. Dosyaların kendisi hedeftir. Dosyalarınıza ne olduğunu biliyorsanız APT'lerin kuruluşunuza zarar vermesine tepki verebilir ve bunları engelleyebilirsiniz.

Veri Güvenliği Analizlerini Uygulama : Temel davranışlarla dosya ve kullanıcı etkinliğini karşılaştırın; böylece neyin normal neyin şüpheli olduğunu bilirsiniz. Bir tehdidi çok geç olmadan durdurabilmeniz için olası güvenlik açıklarını ve şüpheli etkinlikleri izleyin ve analiz edin . Uyarıları alırken tehditleri yönetmek için bir eylem planı oluşturun. Farklı tehditler için farklı bir müdahale planı gerekir: ekiplerinizin her bir tehdit ve güvenlik olayını nasıl ilerleteceklerini ve araştıracaklarını bilmeleri gerekir.

Çevreyi Koruyun : Güvenlik duvarına ve fiziksel alana erişimi sınırlayın ve denetleyin. Herhangi bir erişim noktası APT saldırısına potansiyel giriş noktalarıdır. İşlenmemiş sunucular, açık WIFI yönlendiriciler, kilitsiz sunucu odası kapıları ve güvenli olmayan güvenlik duvarı güvenlik zaafiyeti oluşturabilir.

Kaynaklar :

https://attack.mitre.org/groups/
https://www.cybereason.com/
https://www.kaspersky.com/
https://www.varonis.com/