Mirai Zararlısı Nedir?

Mirai **2016'nın sonlarında** öne çıkan (daha önceki yıllar içerisinde de aktif olduğu düşünülen), linux bazlı internete açık IoT cihazları ele geçiren, ve bu ele geçirilmiş cihazlar ile (bu botnet ile) servis dışı bırakma saldırısı yapan bir zararlıdır (bir malware'dir). Mirai zararlısının ilk hedefi nesnelerin interneti (IoT) diye tabir ettiğimiz güvenlik kamerası, televizyon, buzdolabı, ev router'ı gibi cihazlardır. Mirai zararlısı devamlı olarak internette IoT cihazları tarar ve ele geçirdiklerini botnet'ine katar.

Mirai zararlısının oluşturduğu botnet 2016 yılı Ekim ayında Dyn adlı DNS hizmet sağlayıcısının sunucularına DDOS saldırısı yapmak için kullanılmıştır ve Reddit, Spotify, Pinterest, Neflix, Twitter gibi ünlü web sitelerine erişim engellenmiştir. Bu saldırı akıllı ev cihazlarının kullanıldığı ilk büyük DDOS saldırısı olarak internet tarihine geçmiştir.

Mirai Tam Olarak Nasıl Çalışıyor?

Mirazi zararlısı temelde şu şekilde çalışmaktadır: İnternette linux-based IoT cihazlarını ve bu cihazların telnet servislerini tarar. Tespit ettiği IoT cihazlarda telnet servislerine varsayılan kullanıcı adı ve parolalar sözlük dosyası kullanarak wordlist saldırısı yapar. Cihazın telnet'inde oturum açma denemeleri bu şekide yapılır ve oturumu açılan cihaz ele geçirilmiş olur. Bu sayede botnet oluşur. Ardından ele geçirilen akıllı ev cihazlarının telnet oturumu komut satırından hedef bir web sitesine http request gönderilir (veya hedef bir DNS sunucusuna DNS çözümleme isteği gönderilir) ve DDOS saldırısı gerçekleşir.

Kaynaklar:

https://en.wikipedia.org/wiki/Mirai_(malware)
http://webrazzi.com/2016/10/24/nesnelerin-sucu-neydi-tarihi-ddos-saldirisina-sebep-olan-webcamler-ureticisi-tarafindan-toplatiliyor/
http://www.chip.com.tr/haber/yeni-dunya-hackerlari-bu-sadece-denemeydi_65827.html
https://www.beyondtrust.com/resources/glossary/hardcoded-embedded-passwords