ANKARA ÜNİVERSİTESİ

MÜHENDİSLİK FAKÜLTESİ

BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ

BLM 445 BİLGİ SİSTEMLERİ

Mirai Botnet

Armağan KESKİN

15290038

Emre DOLU

14290032

İrem Nur ECEMİŞ

15290018

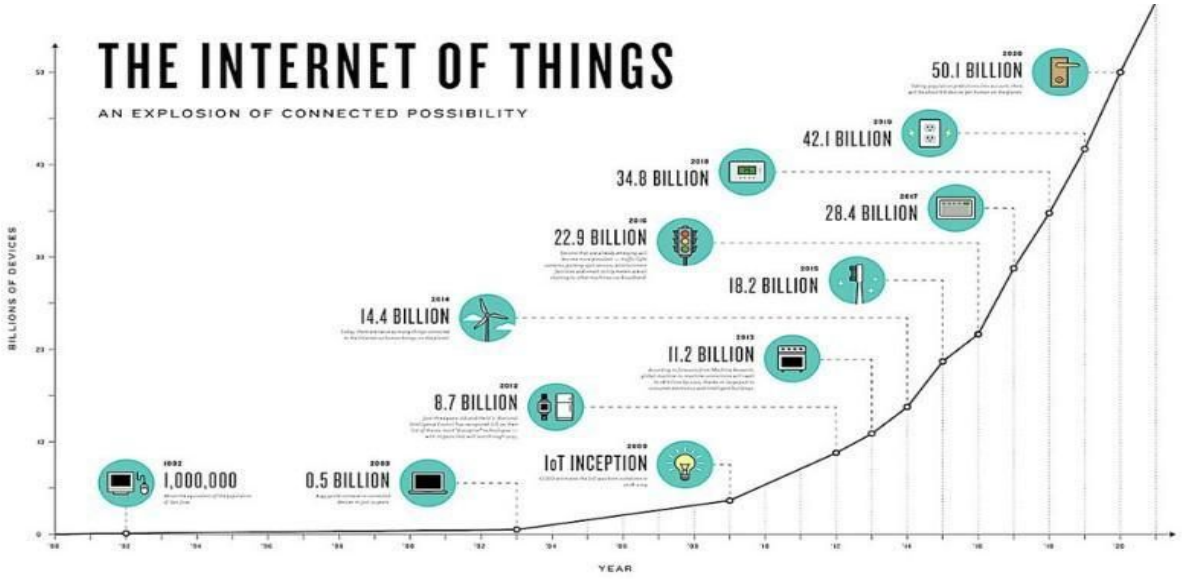
Emin Emrah ÖZSAVAŞ

25.11.2019

Nesnelerin İnternetinde Mirai Saldırıları ve Boyutları

Teknolojinin hayatımıza yerleşmesiyle birlikte günlük hayatta kullandığımız mekanik aletlerin yerini elektronik cihazlar ve otomasyon sistemleri almıştır. Bu sürecin devamında ise kullanılan cihaz ve sistemlerin büyük bir çoğunluğu artık WIFI teknolojisi ile internete bağlanabilir hale gelmiştir ve *IoT (Internet of Things)* terimi ortaya çıkmıştır. IoT, cihazların birbirleriyle belirli bir haberleşme protokolü sayesinde veri üretimi ve paylaşımı, sistem güncellemesi, insan-cihaz etkileşimi gibi birçok önemli işlemi gerçekleştirilen bir ağ-cihaz sistemidir.

IoT'nin kullanım alanları incelendiğinde geniş bir alana yayılmış olduğu görülür. Örnek olarak akıllı ev ve şehir sistemleri, otomatik tarım ve sulama sistemleri, akıllı arabalar, akıllı telefonlar gibi birçok cihazdan bahsedilebilir.



IoT cihazları, hayatımızın birçok alanında bize kolaylık sağlayarak vazgeçilemeyecek bir hale gelmeye başlamıştır. Ancak güvenlik boyutu çok fazla hesaba katılmadan geliştirilen ve kullanılan IoT sistemleri yararlarıyla birlikte bazı zararlarını da beraberinde getirmektedir. Karşılaşılabilecek bu güvenlik sorunlarının daha iyi anlaşılması için öncelikle "*Botnet*" kavramı açıklanmalıdır:

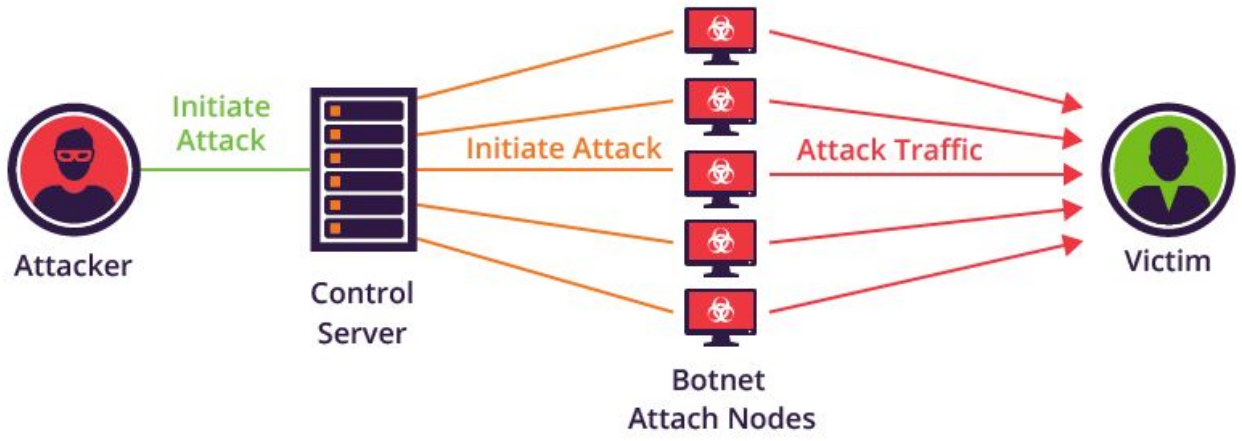
Botnet, siber saldırılarla ele geçirilen, internete bağlanabilen nesneler kümesi olarak tanımlanabilir. Sistemdeki cihaz sayısı arttıkça yapılan saldırıların gücü de aynı oranda artmaktadır. Botnetler yaygın olarak DDoS saldırılarında kullanılır. Botnet aygıtının bulunduğu ağdaki her cihaz tehlike altındadır.

Botnet saldırılarının ciddi etkileri olabilmektedir. Bunun en önemli örneklerinden birisi de 2016'da gerçekleşen *"Mirai"* botnet saldırısıdır. Mirai, IoT cihazlarını Brute-Force yöntem ile ele geçirmeyi hedefleyen kötü amaçlı bir yazılımdır.

Eylül 2016'da, Mirai'nin yazılımcıları tarafından, tanınmış web sitelerine (Twitter, Netflix, Reddit ve GitHub) DDoS saldırısı başlatıldı. Saldırı altındaki siteler saatlerce kullanılamaz hale getirildi. Saldırıdan bir hafta sonra, saldırı kökeninin gizlenmesi amacıyla kaynak kod, yazılımcılar tarafından kamuoyuna sunuldu. Kaynak kodlarının açıklanmasıyla Mirai yazılımının gelişimi farklı boyutlara taşındı. Mirai'deki kodların açık kaynaklı olması, alınabilecek güvenlik önlemlerini arttırdığı halde güvenlik önlemleri açısından elde edilen sonuçlar yazılımın gelişimi karşısında yetersiz kalındığının göstergesidir.

Mirai’nin Saldırı Adımları

İlk olarak IoT cihazlarının dahil olduğu ağlar taranarak kullanıcı adı ve şifresi değiştirilmemiş cihazlara Brute-Force yöntemi ile sızılmaya çalışılır. Erişimin sağlanması ile cihazın bilgileri alınır. Botnet haline gelen cihazın saldırıya uygunluk durumu – internet erişim durumu, komut kabulü ve bulunduğu ağdaki cihaz sayısı- kontrol edilir. Botmaster, bir yandan sık sık yeni potansiyel kurbanlar ararken diğer yandan rapor sunucusuyla iletişim kurarak botnetin güncel durumunu kontrol eder. Hangi korumasız cihazlara bulaşacağına karar veren botmaster, yükleyiciye IP adresi, donanım mimarisi gibi gerekli tüm detayları içeren bir bulaşma komutu gönderir.



Daha sonra yükleyici, hedef cihaza giriş yapar ve cihaza zararlı yazılımın kodunu indirme ve çalıştırma komutu verir. Zararlı yazılım, yüklenir yüklenmez Telnet ve Güvenli Kabuk (SSH) cihazları gibi giriş noktalarını kapatarak kendisini diğer zararlı yazılımlardan korumaya çalışır. Botmaster, sunucu üzerinden tüm bot oluşumlara saldırı tipi ve süresi ile hedef sunucunun IP adresleri gibi gerekli parametreleri ileterek bir saldırı komutu oluşturur. Son olarak ise bot oluşumlar Jeneric Yönlendirici Kapsülleme ve HTTP akını gibi 10 farklı saldırı türünden biriyle hedef sunucuya saldırmaya başlar.

Mirai’nin Çeşitleri ve Gelecekteki Durumu

Mirai’nin kaynak kodlarının yayınlanmasından sadece iki ay sonra botnet sayısı 2 katına çıkmıştır ve geliştirilerek çeşitlenmiştir. Mirai saldırılarının çoğu, 23 ve 2323 numaralı TCP bağlantı noktalarından meydana gelmesine rağmen, Kasım 2016'da tanımlanan Mirai çeşitleri, diğer ISP'lerin cihazlarına (örneğin, ISS'lerin müşterilerin genişbant yönlendiricilerini uzaktan yönetmek için kullandığı 7547 numaralı bağlantı noktasına) dayanmaktadır. Aynı ay, böyle bir Mirai çeşidi saldırısıyla birlikte yaklaşık bir milyon Deutsche Telekom abonesi çevrimdışı kalmıştır. Mirai saldırısında kullanılan cihazların sayısına ilişkin tahminler ise 800.000 virüslü cihazdan 2,5 milyon cihaza kadar değişmektedir.

Mirai zararlı yazılımının meydana getirdiği etki ile birlikte IoT kümesinin güvenlileştirme çabaları artmıştır. Bazı ülkeler güvenlik açığı bulunan cihazların satışını engellemek amacıyla yasal düzenlemeler yayınlamıştır. Bir kısım üreticiler zafiyetli cihazlarını geri toplamış veya bu cihazlara yönelik güncelleme yayınlamıştır. Örnek olarak, Kaliforniya’da kabul edilen ve 2020 yılında yürürlüğe girecek yasada, IoT cihazlarının güvenlik özelliklerinin üst düzeyde olması gerektiği vurgulanmış olup bu özelliği taşımayan cihazlarının satışının kesinlikle yasaklanacağı söylenmiştir.

Diğer Botnetler

Mirai botnet saldırısının ardından, bu yazılımın geliştiricileri tarafından yapılacak diğer saldırılar için daha karmaşık mekanizmalar araştırıldı. Yapılan araştırmalar sonucunda ortaya çıkan ilk IoT botnet Lua programlama dilinde yazıldı – LuaBot- ve 2016 yılında MalwareMustDie tarafından rapor edildi. Botnet ordusunun çoğu ARM CPU ve Linux işletim sistemi kullanan kablolu modemlerden oluşuyordu. Kötü amaçlı yapılmış bu yazılım, DDoS saldırılarının klasik şeklinden farklılaştırılarak kullanılmıştı ve çok fazla karmaşık özelliğe sahip değildi. Ayrıca Lua dilinde yazılmış olması araştırmacıların botnetin asıl amacını anlamalarını engellemişti. Virüslü aygıtları korumak için şifrelenen yazılım, "Komuta et ve Fethet" (Command & Conquer) iletişim kanalına ve her cihaz için özel hale getirilmiş IP tablolarına sahipti.

2016 yılının Ekim aydında Rapidity Networks tarafından Mirai benzeri olan "Hajime" adında bir botnet keşfedildi. Hajime, IPv4 adreslerini tarayan bir düğüm enfeksiyonu başlatarak Telnet servisi için belirlenen 23 portuna TCP bağlantı kabul eden bir cihaz keşfediyordu. Saldırı yapan Hajime düğümü, önceden yazılmış kimlik bilgilerinden Brute-Force şekilde farklı kullanıcı adları ve şifreler deneyerek sisteme giriş yapmaya çalışmaktaydı. Girişten sonra sistem inceleniyor ve sisteme bulaşmaya devam ediliyordu. İlk aşamada dosya transfer programı ve sonrasında tarama programıyla sistemlere bulaşma yaşam döngüsünü devam ettirmekteydi.

Hajime'nin aşamalarında gönderilen her mesaj RC4 şifreli olup, genel ve özel anahtarlar kullanılarak imzalanmıştır. Günümüze kadar Hajime tarafından zarar verici davranış sergilenmemiştir ve Mirai benzeri botnetlerin IoT cihazlardaki güvenlik açıklarını bulabilmek amacıyla oluşturulduğuna dair iddialar vardır.

Bir diğer botnet ise BusyBoz tabanlı IoT botnetidir. 2017 Nisan ayında Radware araştırmacıları tarafından ortaya çıkarılmıştır. Bu botnet SSH servisinin varsayılan kimlik bilgilerini, önceden tanımlanan güvenlik açıklıklarını kullanarak cihazlara PDoS saldırısı denemektedir. Bu yazılımın amacı hedef sistemin donanım bileşenlerine farklı yönlerden zarar vermektir. Cihazın yazılımını geçersiz kılma, bellekteki dosyaları silme ve ağ parametrelerini yeniden yapılandırma işlemlerini yapabilmeyi amaçlamaktadır.

IoT'da Güvenlik Ne Durumda? Firmalar ve Kullanıcılar Hangi Önlemleri Almalı?

IoT cihazlarının satıcılar ve kullanıcılar tarafından yeterli güvenlik önlemleri olmadan çevrimiçi durumda bulunması gibi birçok nedenden ötürü, IoT cihazlar Mirai veya diğer botnetlerin saldırılarına açık hale gelmiştir. Daha önce de bahsedildiği gibi saldırılar cihazın kontrolünü ele geçirip giderek büyüyen bir zombi ordusu yaratabilir durumdadır. Ayrıca "2019 IoT Tehdit Raporu" araştırmasına göre dikkat çeken bir diğer nokta ise kötü amaçlı yazılım bulaşan IoT cihazının bir başka IoT cihazına da virüs bulaştırmak için kullanıcı adı ve şifrelerin bir listesini oluşturması olmuştur.

IoT cihazlarının hedef olarak seçilmesinde rol oynayan sebepleri ve bu durumlara karşı üretici ve tüketici tarafından alınabilecek tedbirler şöyle sıralanabilir:

- Dizüstü ve masaüstü bilgisayarların aksine web kameraları ve kablosuz yönlendiriciler gibi pek çok IoT aygıtı 7/24 çalışır haldedir. Böylesi sık kullanıma rağmen ağ trafiği akışı çoğunlukla izlenilmez. Kontrolü sağlayabilmek adına cihazların ağ erişimine müdahale etmeden IoT kullanımının tespit edilmesi ve engellenmesi için bir izinsiz giriş önleme sistemi kullanılabilir.

- Firmaların ve kullanıcıların yaptığı diğer bir hata ise cihazlarını en yeni yazılım ve güvenlik yamaları ile güncellememeleridir. Bunun yanı sıra üretici firmanın düzenli aralıklarla sızma testi uygulayıp sistemlerini kullanıcının karşılaşabileceği tehditlere karşı güçlendirmesi gerekmektedir. Kısacası ürettiği ürünü kullanıcıya ulaştırdıktan sonra da takip edip güvenliği için sorumluluk alan üreticiler tercih edilmelidir.

- Kullanıcılar tarafından yapılan en büyük hatalardan birisi ise cihazı aldıktan sonra konfigürasyon ayarlarını (erişimi sınırlandırma, bilgileri filtreleme vb.) gözden geçirmemek ve kişisel bir kullanıcı adı - parola kombinasyonu oluşturmamaktır. Bunun yanı sıra IoT cihazının hesabına giriş yapmak için iki faktörlü kimlik doğrulaması kullanılması izinsiz erişime karşı ek bir güvenlik önlemi olarak alınabilir.

Sonuç olarak güvenli bir IoT altyapısı sağlamak adına IoT güvenliği şirketleri verileri, cihazları ve bağlantıları korumak için üç aşamalı bir yaklaşım kullanılmasını önermektedir:

- Cihazların güvenli bir üreticiden temin edilmesi,
- Cihazlarla bulut arasındaki bağlantının güvenliğinin sağlanması ve
- İşleme ve depolama sırasında buluttaki verilerin güvenliğinin sağlanmasıdır.

Siber korsanlar, IoT cihazlarını kolayca ele geçirerek DDoS saldırılarında kullanabilmektedir. Önümüzdeki yıllarda internete bağlı cihaz sayısının artmasıyla birlikte bu saldırıların da artacağı düşünülmektedir. 2020 yılında yaklaşık 20 milyar IoT cihazının kullanımda olacağı tahmin ediliyor. Bu yüzden bahsedilen yaklaşımlarla önlem alınması ve güvenliğin her zaman üst düzeyde tutulması büyük önem arz etmektedir. IoT cihazların sayısının artmasıyla Mirai ve diğer botnet çeşitlerinin saldırı boyutları da gün geçtikçe daha tehlikeli hale gelmektedir.

KAYNAKÇA

Makale: [URL:

https://www.researchgate.net/publication/318288727_DDoS_in_the_IoT_Mirai_and_other_botnets]

Nesnelerin İnterneti [URL: https://proente.com/nesnelerin-interneti-nedir/]

Mirai Botnet [URL: https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/]

Botnet
[URL:https://www.ebi.com.tr/blog/mirai-botnetin-yeni-cesidi-kurumsal-sistemleri-hedefliyor/]

IoT'da Güvenlik [URL: https://www.autodesk.com.tr/redshift/iot-guvenlik-sorunlari/]

Siber Güvenlik [URL:
https://azure.microsoft.com/tr-tr/overview/internet-of-things-iot/iot-security-cybersecurity/]

Yüksek Güvenlikli Cihazların Özellikleri [URL:
https://www.microsoft.com/en-us/research/wp-content/uploads/2017/03/SevenPropertiesofHighlySecureDevices.pdf]

Hajime [URL: http://security.rapiditynetworks.com/publications/2016-10-16/hajime.pdf]

Busybox [URL: https://blog.radware.com/security/2016/10/busybox-botnet-mirai/]

DDoS [URL: https://tr.geekmarkt.com/what-is-ddos-attack]