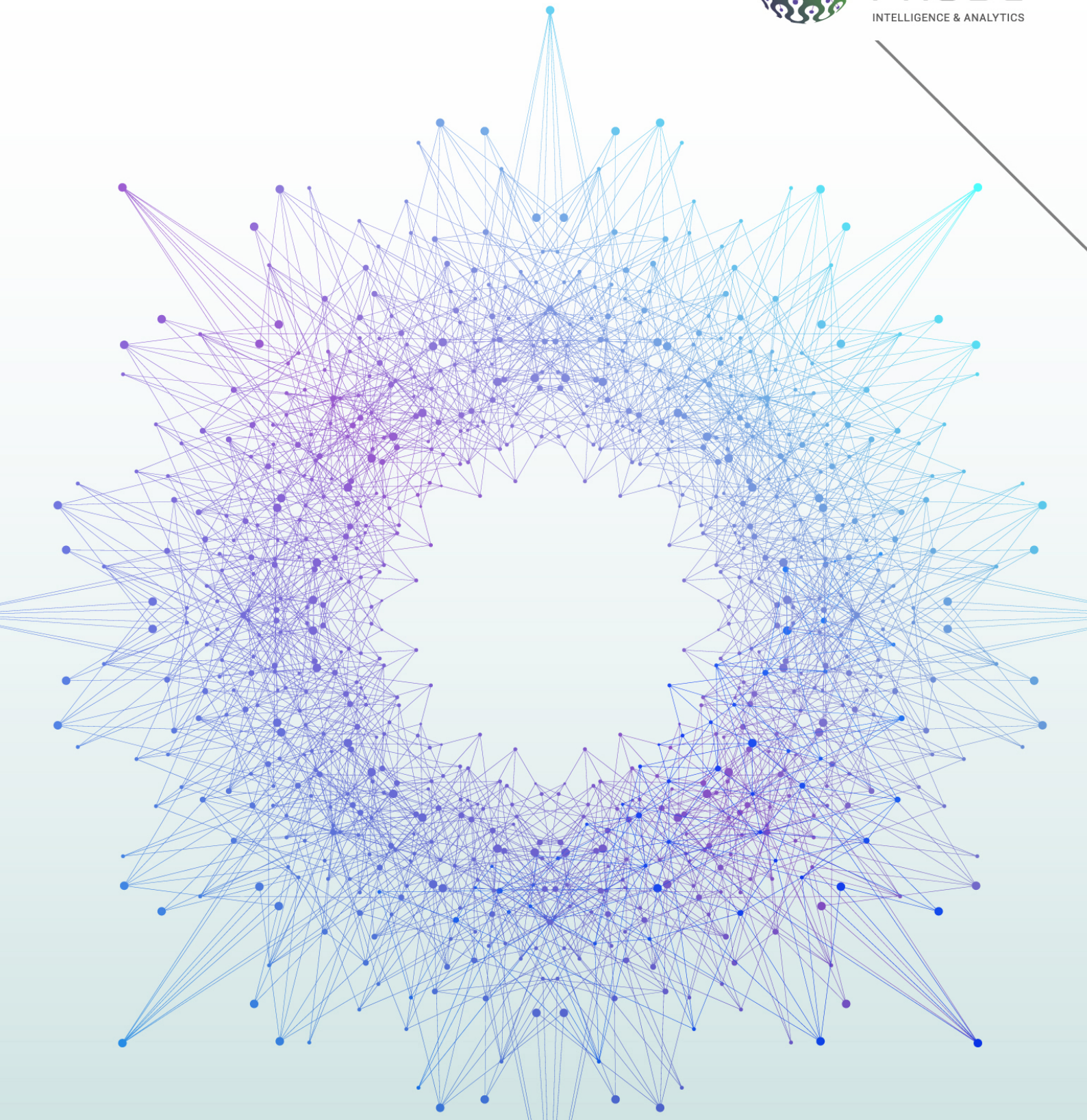
INTEL PROBE
INTELLIGENCE & ANALYTICS



# **Corona**(Covid-19)

## Mobil Tehdit İstihbaratı Raporu

5 Nisan 2020

# Corona/Covid-19 Mobil Tehdit Raporu

Bu rapor Corona/Covid-19 virüsü salgınının, dijital dünya üzerindeki etkilerinin incelenmesi sonucu oluşturulmuştur. Aralık 2019 tarihinde Çin Halk Cumhuriyeti'nin Wuhan kentinde başlayan ve kısa sürede tüm dünyaya yayılan Corona tipi Covid-19 virüsü tüm dünya üzerinde yankı uyandırmıştır.

Pek çok alanda kendisine yer bulan Corona virüsü bilişim ve teknoloji dünyasında da tehlikeli bir dijital salgına neden olmuştur. Saldırganların Corona virüs teması kullanarak sahte mobil uygulamalar aracılığı ile hedef odaklı ya da gelişi güzel saldırılar düzenlediği gözlemlenmiştir.



## Yönetici Özeti

Corona/Covid19 virüsünün ortaya çıkışından itibaren dijital ortamlarda da ilgi giderek artmış kullanıcıların çevrimiçi olarak ilgili haberler, vaka sayısı ve içeriklere ulaşabileceği web ve mobil uygulamalar ortaya çıkmıştır. Oluşturulan uygulamaların sayısının giderek artması saldırganların Corona/Covid19 temasını kullanmasına zemin oluşturmuştur. CatchProbe Siber Tehdit İstihbaratı platformu ile elde ettiğimiz veriye göre özellikle Mart ayı içerisinde ilgili tema ile pek çok sayıda alan adı kayıt edildiği görülmüştür. Alan adı kayıtlarının detaylı bilgilerine "Dijital Corona Virüs Siber Tehdit İstihbaratı İnceleme Raporu-2" üzerinden ulaşılabilir.

Yapılan tespitler sonucu benzer popülaritenin mobil uygulamalar üzerinde de olduğu Mart ayı içerisinde Corona/Covid19 temalı birçok mobil uygulamanın çeşitli platformlar üzerinden yayımlandığı görülmüştür. IntelProbe uzmanları tarafından gerçekleştirilen teknik incelemeler ve gözlemler sonucu sahte mobil uygulamalarının varlıkları tespit edilmiş, gerçekleştirilen analizler sonucunda bazı mobil uygulamaların Corona/Covid19 ile ilgili bilgi sunarken arka tarafta zararlı işlemler gerçekleştirdiği görülmüştür. Gerçekleştirilen işlemler ile son kullanıcının istismar edilmeye çalışıldığı tespit edilmiştir. Kullanıcıların özellikle aktif ve devam eden oturum bilgileri çalınarak, kullanıcılar adına işlem yapılması hedeflenmiştir. Özellikle evden çalışılmanın yaygınlaşması, siber saldırganları iştahlandırdığı düşünülmektedir.

IntelProbe uzmanları tarafından gerçekleştirilen tespit, analiz ve değerlendirmeler ile içerisinde yerli bankalarının mobil uygulamalarının da hedef alındığı Türkçe içerikli kampanyalar görülmüştür. İlgili mobil tehdit detaylarına raporun teknik analiz kısmından ulaşılabilir.

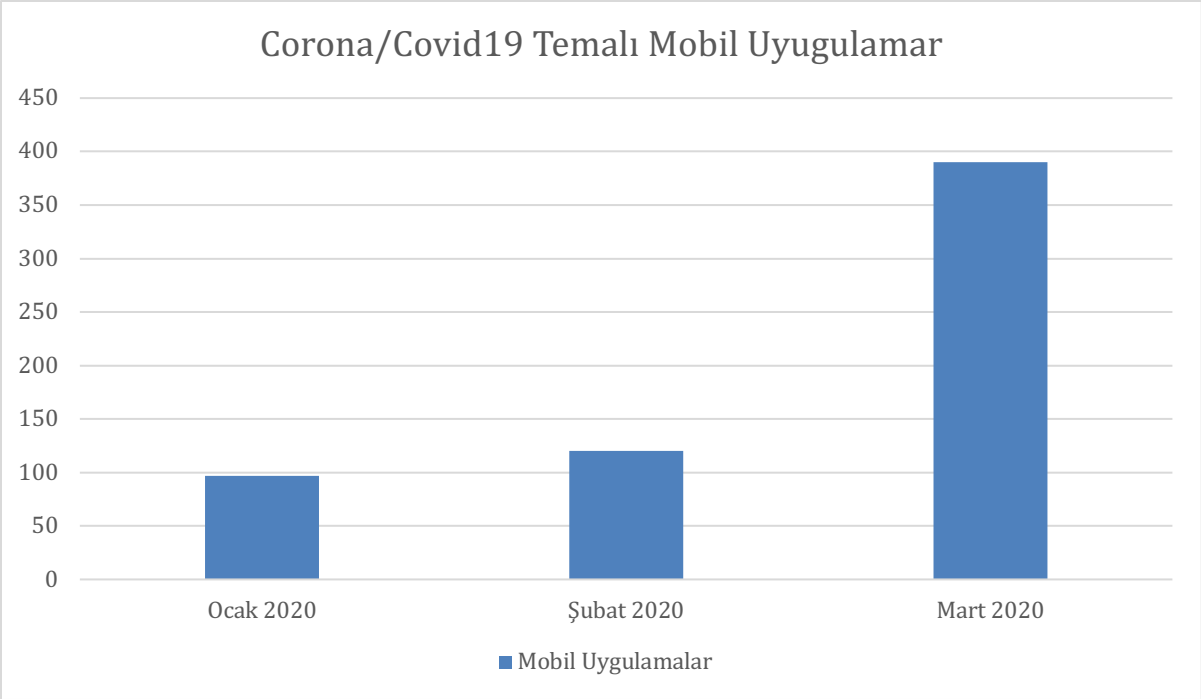
## Mobil Tehditler

Gerçekleştirilen istihbarat çalışmaları sonucu mobil uygulamalar üzerinde Corona/Covid19 ile ilgili birçok tehdit görülmüştür. Saldırganların bu temayı kullanarak mobil kullanıcıların kişisel bilgilerini çalmak için RAT zararlılarının sıkça kullanıldığı görülmüştür. Zararlının bulaştığı cihaza uzaktan erişim yapılabilmesi için kullanıldığı bilinmektedir.

Yapılan araştırmalar ve değerlendirmeler sonrasında sahte mobil uygulamaları kullanılarak kullanıcıların mobil cihazları üzerindeki önemli bilgilerin şifrelenerek fidye talep edildiği ve bu trendin 2020 yılı içerisinde önemli ölçüde devam edeceği öngörülmektedir. Tespit edilen ve önemli olarak görülen bazı zararlı mobil uygulamalar aşağıda tablo ile verilmiştir.

| | | |
|---|---|---|
| | Covid Tracker | 8e28ae16f571101f4029a04e3d10b759e32023dc8cee2076836051538dfef6a5 |
| | V-Alert COVID-19 | b1323c8e514a255b7f61c544ecdfe4cc9fff2eee922131c50ce9af7c7b95d892 |
| | V-Alert COVID-19 | f092a594f615678099a25c28f7abfd8d95749abdcec83e43d1306ecb066ef3dc |
| | Covid 19 Tracker | 19b331b79cdd95a13b68ab5e8b4eb69102878fce1c81071cb7c17cbc24900c15 |
| | Covid-19 Tracker | 19b331b79cdd95a13b68ab5e8b4eb69102878fce1c81071cb7c17cbc24900c15 |
| | Corona Safety Mask | d7d43c0bf6d4828f1545017f34b5b54c |
| | Corona Takip | b7070a1fa932fe1cc8198e89e3a799f3<br>64ebe4ecfb242019ee590d80740e6a46 |

Gerçekleştirilen değerlendirme sırasında Corona Tracker / Corona Takip isimli mobil uygulamanın içerisinde özellikle bankaların hedef alındığı zararlı aktiviteler tespit edilmiştir. İçerisinde Türkiye Bankacılık uygulamalarının da bulunduğu pek çok şüpheli ve zararlı işlem için izin ve yetki isteyen mobil uygulamalar birçok ülkeyi hedef almıştır. Amerika Birleşik Devletleri, Rusya, Almanya, İtalya, Fransa, Ukrayna olarak tespit edilmiştir.

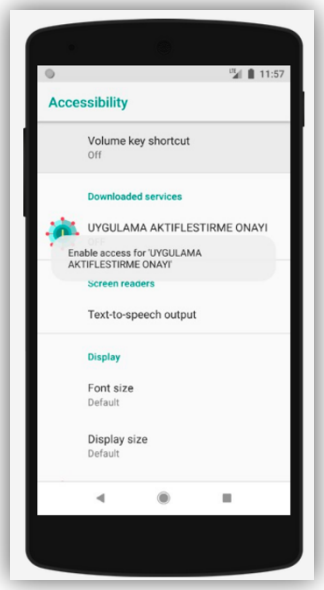


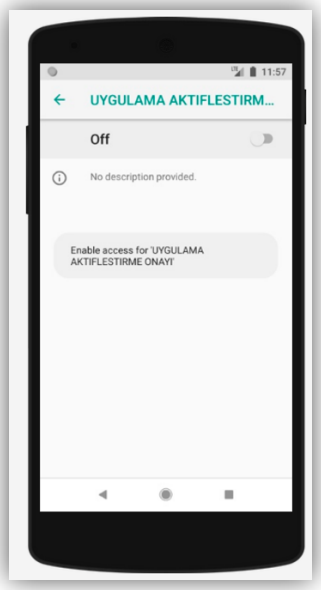

Yapılan tespitler sırasında mobil uygulamaların ortaya çıkma işlemleri arasında "Corona Virüs" temalı kayıt işlemlerinin giderek arttığı görülmüştür. İlgili mobil uygulamalarının tamamının olası siber saldırılar ile alakalı olmadığı fakat Corona/Covid-19 virüs temasının popülaritesinin giderek arttığı görülmüşüdür. Covid-19 salgını dolayısı ile kullanıcıların uzaktan/evden çalışma koşullarının ve mobil çalışma durumunun da hedef alınacağı tahmin edilmektedir.

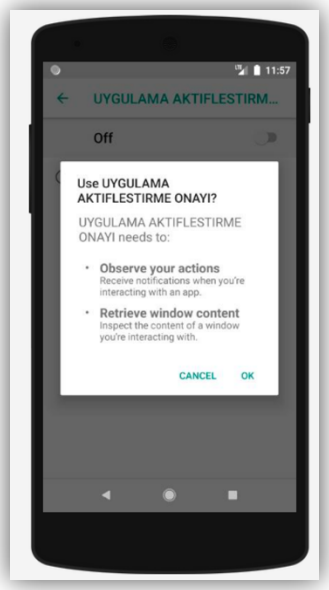
## Teknik Analiz

| | | |
|---|---|---|
| | **Corona Takip** (com.turenak.ch) | b7070a1fa932fe1cc8198e89e3a799f3 (MD5)<br>c3b72c0c59f7f072e6d425c7026b35e6749893b5 (SHA1)<br>dfb54d6c468271c73865d45e54b9dd942a18e716d608cf9233f1122cf79bab8c |

Gerçekleştirilen Corona/Covid-19 temalı mobil uygulamaların analizleri sırasında "Corona Takip" isimli uygulama üzerinde zararlı aktivitelerin olduğu görülmüştür. Uygulama açılır açılmaz kullanıcıdan "UYGULAMA AKTIFLESTIRME ONAYI" adı altında önemli izinler istemektedir. İlgili mobil uygulama incelemeleri sonrasında saldırganların son kullanıcıları hedef aldığı ve belirli bir gelir elde etme amacının olduğu düşünülmektedir. Corona/Covid-19 temasının kullanılması doğrultusunda başarının arttırılması hedeflenmiştir.




Kullanıcı üzerinden ilgili izinlerin beklenmesi sırasında döngü halinde **http://aymyapi[.]com/o1o/a4.php** ve **http://aymyapi[.]com/o1o/a14.php** adresleri ile iletişimi beklenmektedir.

| | |
|---|---|
| http://aymyapi.com/o1o/a4.php | (pending) |
| http://aymyapi.com/o1o/a14.php | (pending) |
| http://aymyapi.com/o1o/a4.php | (pending) |
| http://aymyapi.com/o1o/a14.php | (pending) |
| http://aymyapi.com/o1o/a4.php | (pending) |
| http://aymyapi.com/o1o/a14.php | (pending) |
| http://aymyapi.com/o1o/a4.php | (pending) |
| http://aymyapi.com/o1o/a14.php | (pending) |

İlgili adrese (C&C) POST işlemlerinin gerçekleştirildiği görülmüştür. Bu aktivitelerin zararlı olduğu ve bilgi göndermek amacı ile yapıldığı gözlemlenmektedir.

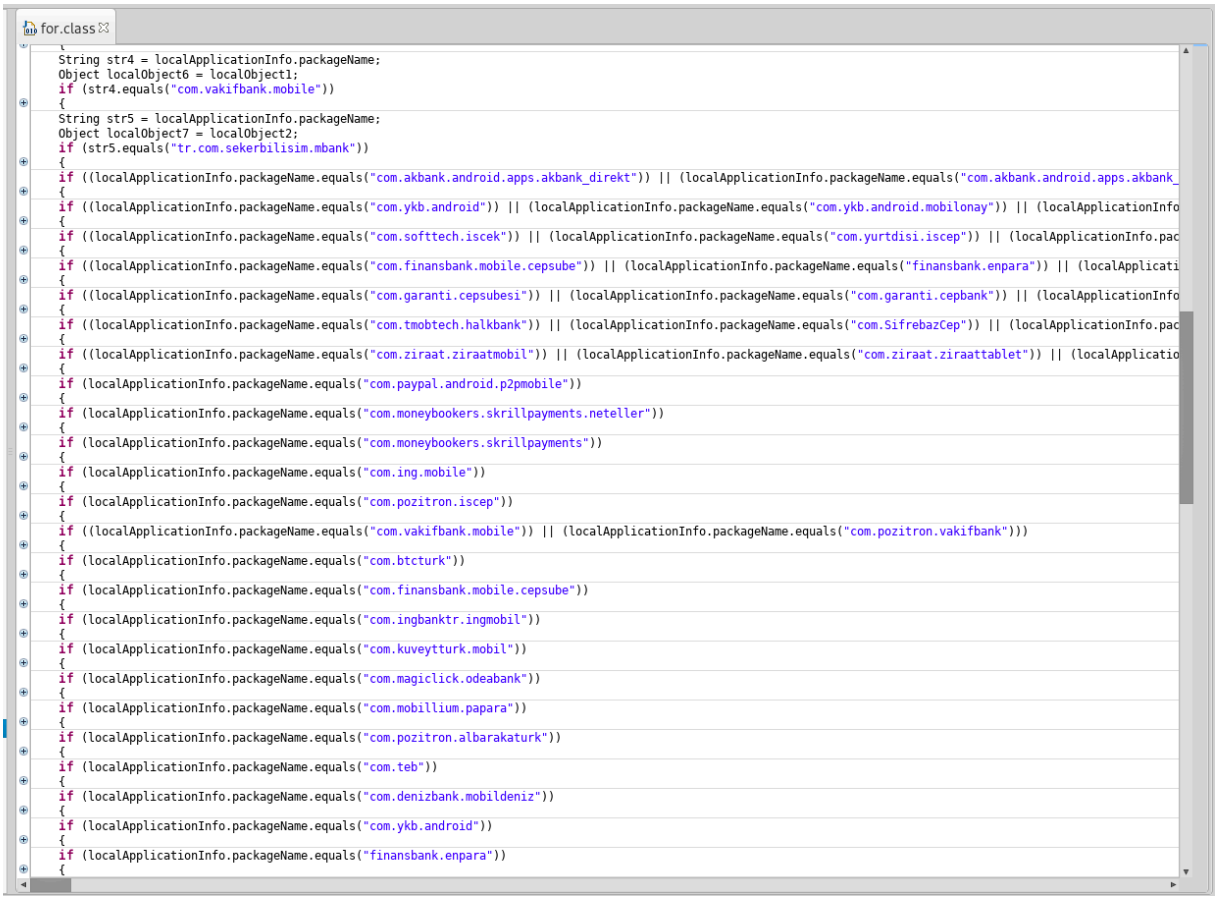
**Request status:**
`POST http://aymyapi.com/o1o/a4.php`

**Request headers:**
Content-Length: `108`
Content-Type: `application/x-www-form-urlencoded`
User-Agent: `Dalvik/2.1.0 (Linux; U; Android 8.1.0; Android SDK built for x86 Build/OSM1.180201.031)`
Host: `aymyapi.com`
Connection: `Keep-Alive`
Accept-Encoding: `gzip`

**Response headers:**

**Content:**
`not available`

Gerçekleştirilen diğer incelemeler sırasında uygulama "decompile" edilmiş ve içerisinde pek çok yerli bankanın yer aldığı bir hedef listesi tespit edilmiştir.




Vakıfbank, Finansbank, Garanti BBVA, Akbank gibi bankaların bulunduğu tüm mobil erişim listesi aşağıdaki gibidir. Zararlı mobil uygulaması erişim listesinde bulunan uygulamaları takip etmekte ve bu uygulamalar üzerinden kişisel bilgileri çalmak için işlem gerçekleştirmektedir. Gerçekleştirilen işlemler içerisinde kişisel bilgileri çalmak için sahte ekran görüntüleme yeteneğinin mevcut olması da tespit edilmiştir.

Uygulama çalışıp, gerekli izinleri kullanıcı tarafından aldıktan sonra liste içerinde bulunan uygulamaları aramakta ve kullanıcıları kullandıkları ilgili uygulama üzerinden hedef almaktadır.

- es.cm.android
- es.cm.android.tablet
- apps.com.app.utils
- com.DijitalSahne.EnYakinHalkbank
- com.Plus500
- com.SifrebazCep
- com.akbank.android.apps.akbank_direkt
- com.akbank.android.apps.akbank_direkt_tablet
- com.akbank.android.apps.akbank_direkt_tablet_20
- com.akbank.softotp
- com.albarakaapp
- com.albarakaapp
- com.amazon.mShop.android.shopping
- com.android.chrome
- com.android.settings
- com.android.system
- com.android.systemui
- com.android.vending
- com.bankia.wallet
- com.bestbuy.android
- com.binance.dev
- com.binance.odapplications
- com.bitcoin.ss.zebpayindia
- com.bitfinex.bfxapp
- com.bitmarket.trader
- com.blockfolio.blockfolio
- com.btcturk
- com.coin.profit
- com.coinbase.android
- com.coins.bit.local
- com.coins.ful.bit
- com.crypter.cryptocyrrency
- com.db.mm.norisbank
- com.db.pwcc.dbmobile
- com.denizbank.mobildeniz
- com.ebay.mobile
- com.edsoftapps.mycoinsvalue
- com.finansbank.mobile.cepsube
- com.fragment.akbank
- com.garanti.cepbank
- com.garanti.cepsubesi
- com.garantibank.cepsubesiro
- com.garantiyatirim.fx
- com.twitter.android
- com.ing.mobile
- com.ingbanktr.ingmobil
- com.jackpf.blockchainsearch
- com.jamalabbasii1998.localbitcoin
- com.kryptokit.jaxx
- com.kuveytturk.mobil
- com.localbitcoins.exchange
- com.localbitcoinsmbapp
- com.magiclick.FinansPOS
- com.magiclick.odeabank
- com.mal.saul.coinmarketcap
- com.matriksmobile.android.ziraatTrader
- com.mobillium.papara
- com.moneybookers.skrillpayments
- com.moneybookers.skrillpayments.neteller
- com.monitise.isbankmoscow
- com.mycelium.wallet
- com.paypal.android.p2pmobile
- com.paypal.android.p2pmobile
- com.plunien.poloniex
- com.portfolio.coinbase_tracker
- com.pozitron.albarakaturk
- com.pozitron.albarakaturk
- com.pozitron.iscep
- com.pozitron.vakifbank
- com.redrockdigimark
- com.softtech.isbankasi
- com.softtech.iscek
- com.targo_prod.bad
- com.teb
- com.thunkable.android.manirana54.LocalBitCoins_unblock
- com.tmobtech.halkbank
- com.tnx.apps.coinportfolio
- com.unocoin.unocoinmerchantPoS
- com.unocoin.unocoinwallet
- com.vakifbank.mobile

- com.veripark.ykbaz
- com.vipera.ts.starter.QNB
- com.vkontakte.android
- com.ykb.android
- com.ykb.android.mobilonay
- com.ykb.androidtablet
- com.ykb.avm
- com.yurtdisi.iscep
- com.ziraat.ziraatmobil
- com.ziraat.ziraatmobil
- com.ziraat.ziraattablet
- tr.com.hsbc.hsbcturkey
- tr.com.sekerbilisim.mbank
- tr.com.tradesoft.tradingsystem.gtpmobile.halk
- wos.com.zebpay
- mobile.santander.de
- finansbank.enpara
- finansbank.enpara.sirketim
- tr.com.hsbc.hsbcturkey
- tr.com.sekerbilisim.mbank
- tr.gov.turkiye.edevlet.kapisi
- eu.unicreditgroup.hvbapptan
- io.getdelta.android
- de.schildbach.wallet
- piuk.blockchain.android
- info.blockchain.merchant
- zebpay.Application
- xmr.org.freewallet.app
- com.matriksdata.finansyatirim
- com.matriksdata.ziraatyatirim.pad

## Sonuç

Corona/Covid-19 virüsü nedeni ile tüm dünya üzerinde acil durumda olan kullanıcılar, kurumlar ve organizasyonlar bilgiye dijital ortam üzerinden ulaşma eğilimindedir. Özellikle salgından korunmak amacı ile uzaktan çalışan kullanıcıların mobil olarak çalışmasından yararlanmaya çalışan saldırganlar, mobil uygulamalara yönelmiştir. Gerçekleştirilen işlemler ile kullanıcılıların istismar edilmeye çalışıldığı tespit edilmiştir. Kullanıcıların özellikle aktif ve devam eden oturum bilgileri çalınarak, kullanıcılar adına işlem yapılması hedeflenmiştir. Özellikle evden çalışılmanın yaygınlaşması, siber saldırganları iştahlandırdığı düşünülmektedir.

Saldırganlar oluşturdukları sahte mobil uygulamalar ile cihaz üzerindeki önemli bilgileri şifreleyerek fidye talep ettiği görülmüştür. Bu trendin 2020 yılı içerisinde önemli ölçüde devam edeceği öngörülmektedir.

Kullanıcılar mobil cihazları ile işlem yaparken bu tehditlere karşı dikkatli olmalıdırlar. Kullanıcıların korku, heyecan ve sevinç duygularının sömürülmesi için oluşturulan haber ve uygulamalara karşı dikkat edilmelidir. Güvenilir olmayan kaynaklardan temin edilen mobil uygulamalar kullanılmamalıdır.


**Adres :**
Mutlukent Mah.
Fesleğen Sk. No:9
Çankaya - ANKARA

**Tel :**
+90 312 225 10 93

**Fax:**
+90 312 225 10 99