Turkey targeted by Cerberus and Anubis Android banking Trojan campaigns

bushidotoken.blogspot.com/2020/05/turkey-targeted-by-cerberus-and-anubis.html

BushidoToken

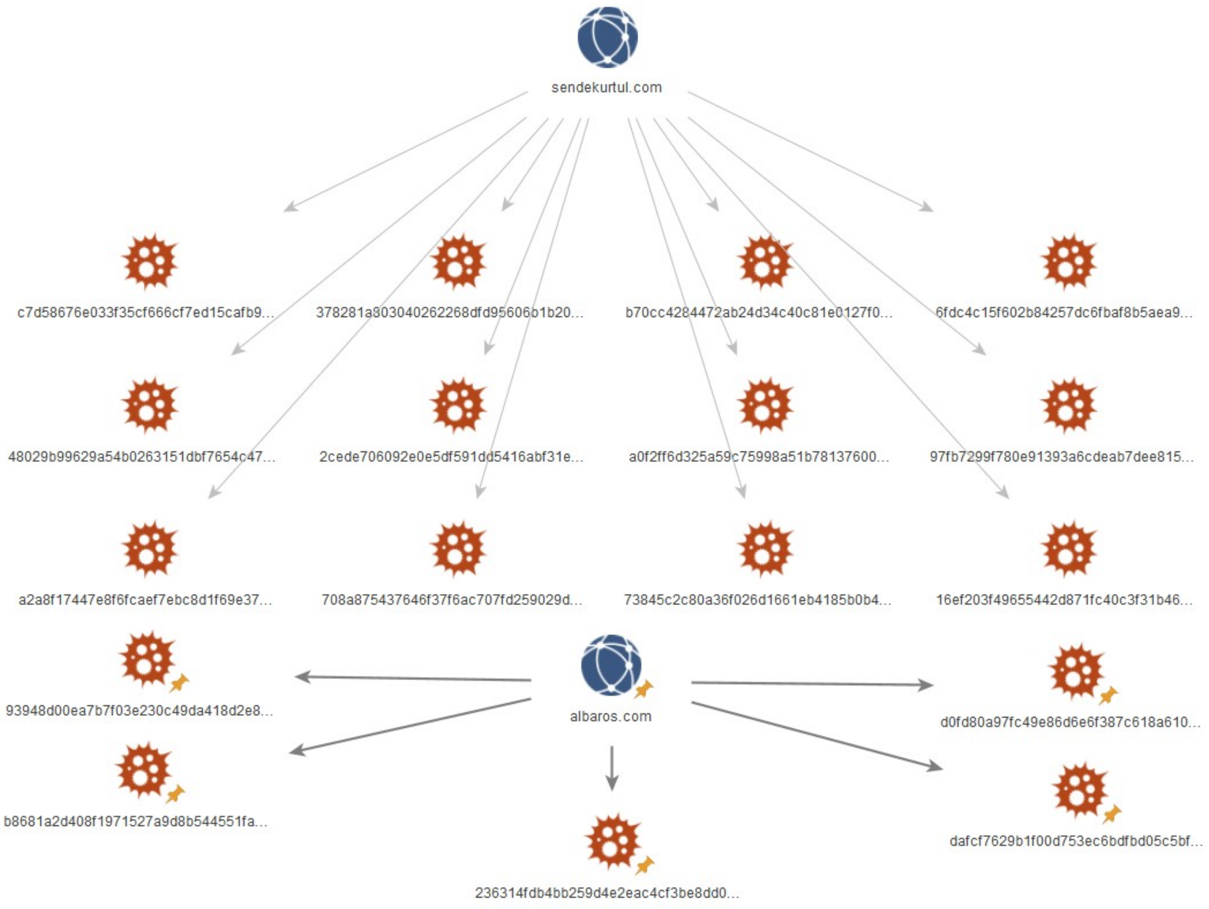
#EVDEKAL
TÜM OPERATÖRLERE 20GB DEVLET HEDİYESİ!
vodafone
TURKCELL
BIM CELL
BİZ BİZE YETERİZ
TÜRKİYEM

I recently set out to become more acquainted with Maltego, a useful program for open-source intelligence (OSINT) and forensics, developed by Paterva. I also noticed there is an ongoing campaign against Turkey using Android banking Trojans such as Anubis and Cerberus. Both are Malware-as-a-Service offerings that supply a builder and mobile remote access Trojan (MRAT) to steal credentials from Android users.

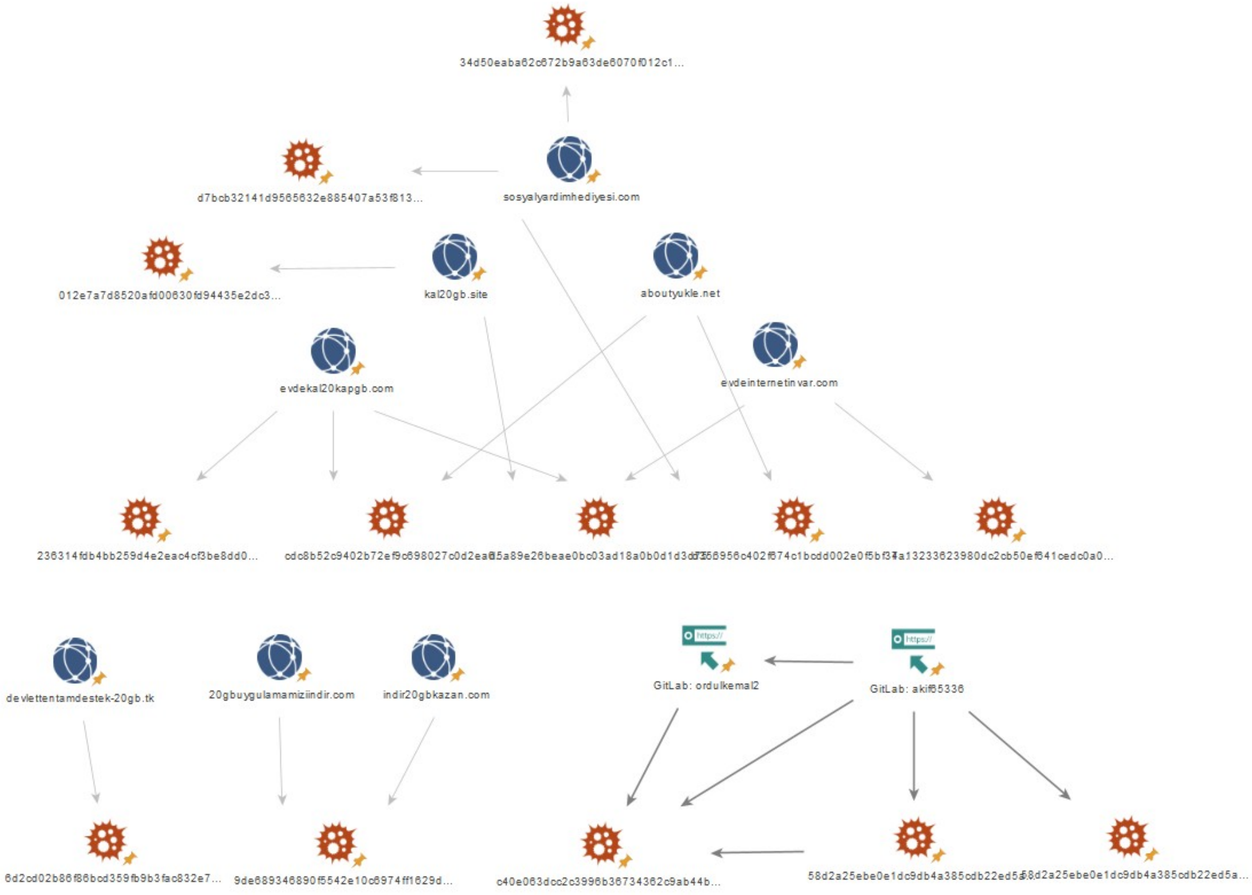
Security researchers such as @MalwareHunterTeam, @ReBensk, @pr3wtd, and @mertcangokgoz, and others have all recently shared new samples of Cerberus and Anubis targeting users in Turkey with mobile data "gifts" that are offered from their mobile carriers due to COVID-19. Various websites are registered hosting links to fake apps, which were downloaded from the threat actor's GitLab or BitBucket repositories. These apps are Android packages (.APK) that can be distributed via SMS, instant messaging app, on Twitter, via email, and other social engineering techniques.

With the Tweets of these security researchers I compiled the indicators of compromise (IOCs) such as file hashes, domains, IP addresses, and any other useful artefacts. I then fired up Maltego and began compiling the IOCs and trying to figure out how it was all connected.

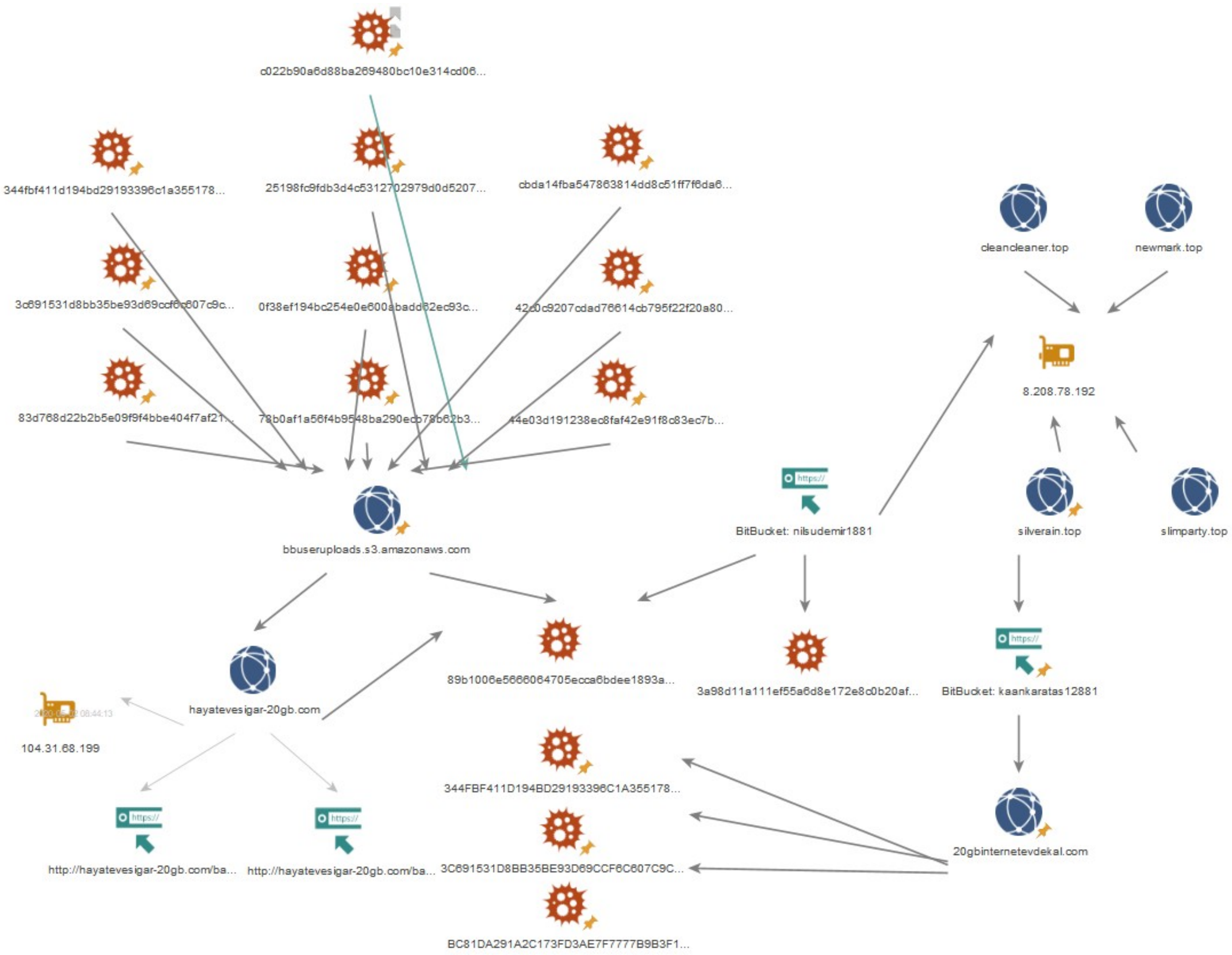
Multiple Anubis campaigns:


sendekurtul.com
c7d58676e033f35cf666cf7ed15cafb9...
378281a803040262268dfd95606b1b20...
b70cc4284472ab24d34c40c81e0127f0...
6fdc4c15f602b84257dc6fbaf8b5aea9...
48029b99629a54b0263151dbf7654c47...
2cede706092e0e5df591dd5416abf31e...
a0f2ff6d325a59c75998a51b78137600...
97fb7299f780e91393a6cdeab7dee815...
a2a8f17447e8f6fcaef7ebc8d1f69e37...
708a875437646f37f6ac707fd259029d...
73845c2c80a36f026d1661eb4185b0b4...
16ef203f49655442d871fc40c3f31b46...
93948d00ea7b7f03e230c49da418d2e8...
albaros.com
d0fd80a97fc49e86d6e6f387c618a610...
b8681a2d408f1971527a9d8b544551fa...
dafcf7629b1f00d753ec6bdfbd05c5bf...
236314fdb4bb259d4e2eac4cf3be8dd0...

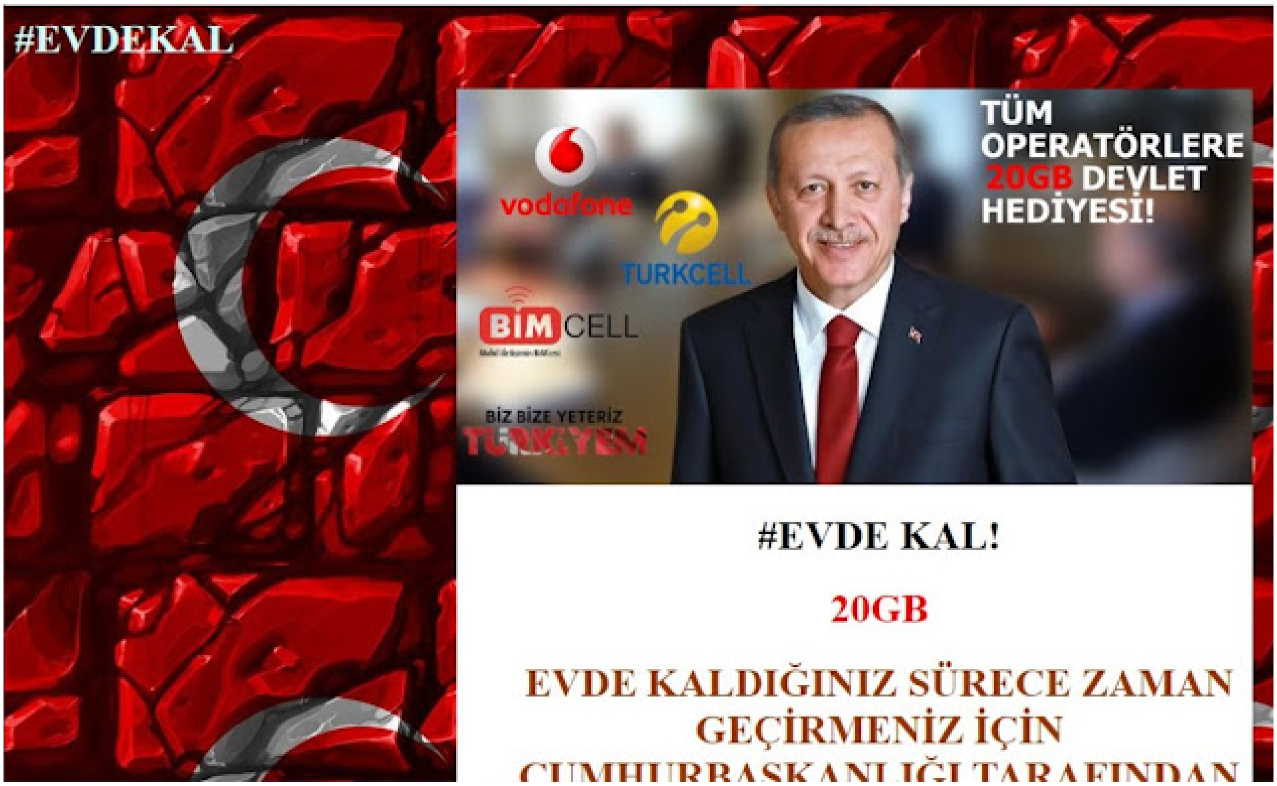
Cerberus GitLab campaign:


34d50eaba62c672b9a63de6070f012c1...
d7bcb32141d9565632e885407a53f813...
sosyalyardimhediyesi.com
012e7a7d8520afd00630fd94435e2dc3...
kal20gb.site
aboutyukle.net
evdekal20kapgb.com
evdeinternetinvar.com
236314fdb4bb259d4e2eac4cf3be8dd0...
cdc8b52c9402b72ef9c698027c0d2ea65a89e26beae0bc03ad18a0b0d1d3df356956c402f674c1bcdd002e0f5bf34a13233623980dc2cb50ef641cedc0a0...
devlettentamdestek-20gb.tk
20gbuygulamamiziindir.com
indir20gbkazan.com
https://
GitLab: ordulkemal2
https://
GitLab: akif65336
6d2cd02b86f86bcd359fb9b3fac832e7...
9de689346890f5542e10c6974ff1629d...
c40e063dcc2c3996b36734362c9ab44b...
58d2a25ebe0e1dc9db4a385cdb22ed5a58d2a25ebe0e1dc9db4a385cdb22ed5a...

Cerberus BitBucket campaign:


c022b90a6d88ba269480bc10e314cd06...
344fbf411d194bd29193396c1a355178...
25198fc9fdb3d4c5312702979d0d5207...
cbda14fba547863814dd8c51ff7f6da6...
3c691531d8bb35be93d69ccf6c607c9c...
0f38ef194bc254e0e600abadd62ec93c...
42c0c9207cdad76614cb795f22f20a80...
83d768d22b2b5e09f9f4bbe404f7af21...
78b0af1a56f4b9548ba290ecb78b62b3...
44e03d191238ec8faf42e91f8c83ec7b...
bbuseruploads.s3.amazonaws.com
cleancleaner.top
newmark.top
8.208.78.192
BitBucket: nilsudemir1881
silverain.top
slimparty.top
hayatevesigar-20gb.com
104.31.68.199
2020-05-02 08:44:13
89b1006e5666064705ecca6bdee1893a...
3a98d11a111ef55a6d8e172e8c0b20af...
BitBucket: kaankaratas12881
344FBF411D194BD29193396C1A355178...
3C691531D8BB35BE93D69CCF6C607C9C...
BC81DA291A2C173FD3AE7F7777B9B3F1...
20gbinternetevdekal.com
http://hayatevesigar-20gb.com/ba...
http://hayatevesigar-20gb.com/ba...

Phishing lures:

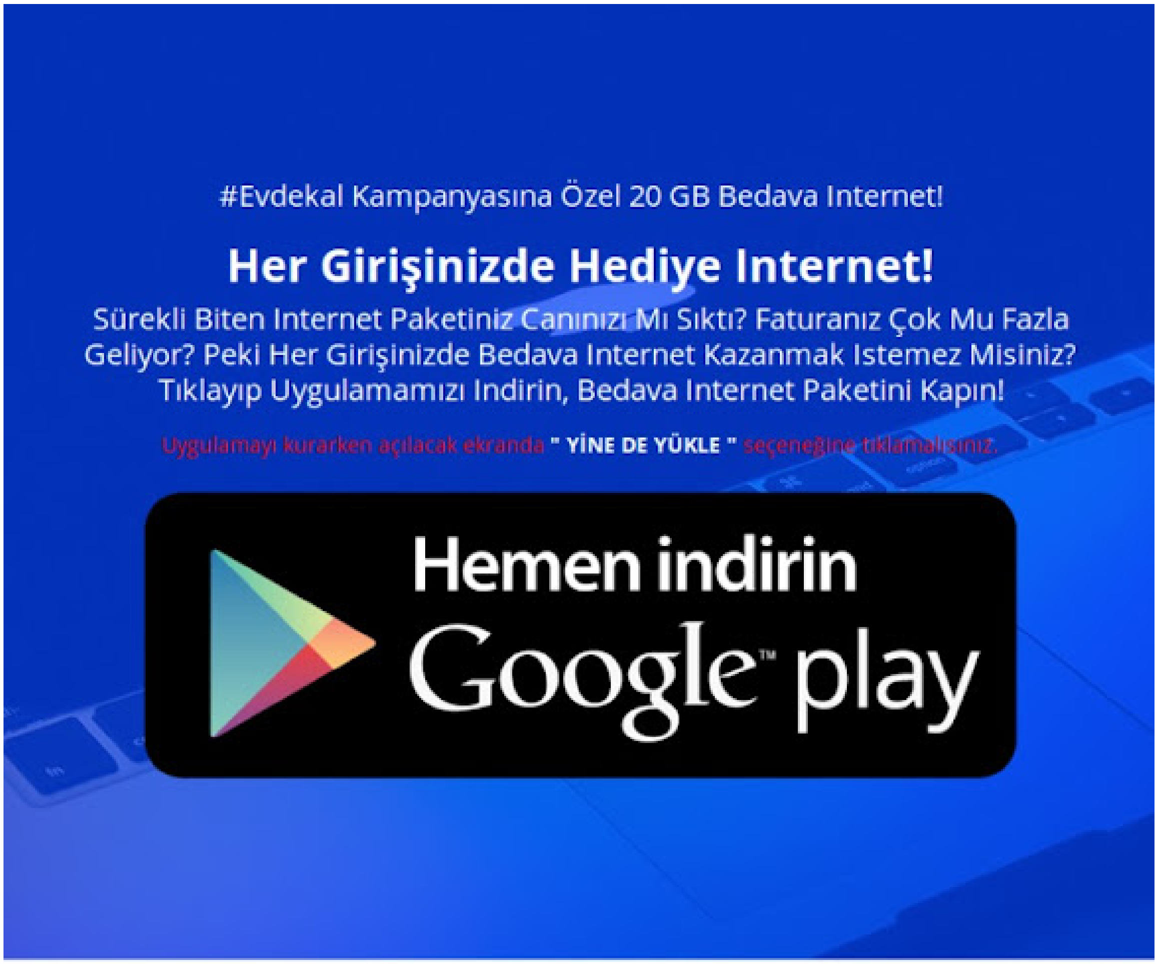


#EVDEKAL

#EVDE KAL!

20GB

EVDE KALDIĞINIZ SÜRECE ZAMAN GEÇİRMENİZ İÇİN CUMHURBAŞKANLIĞI TARAFINDAN

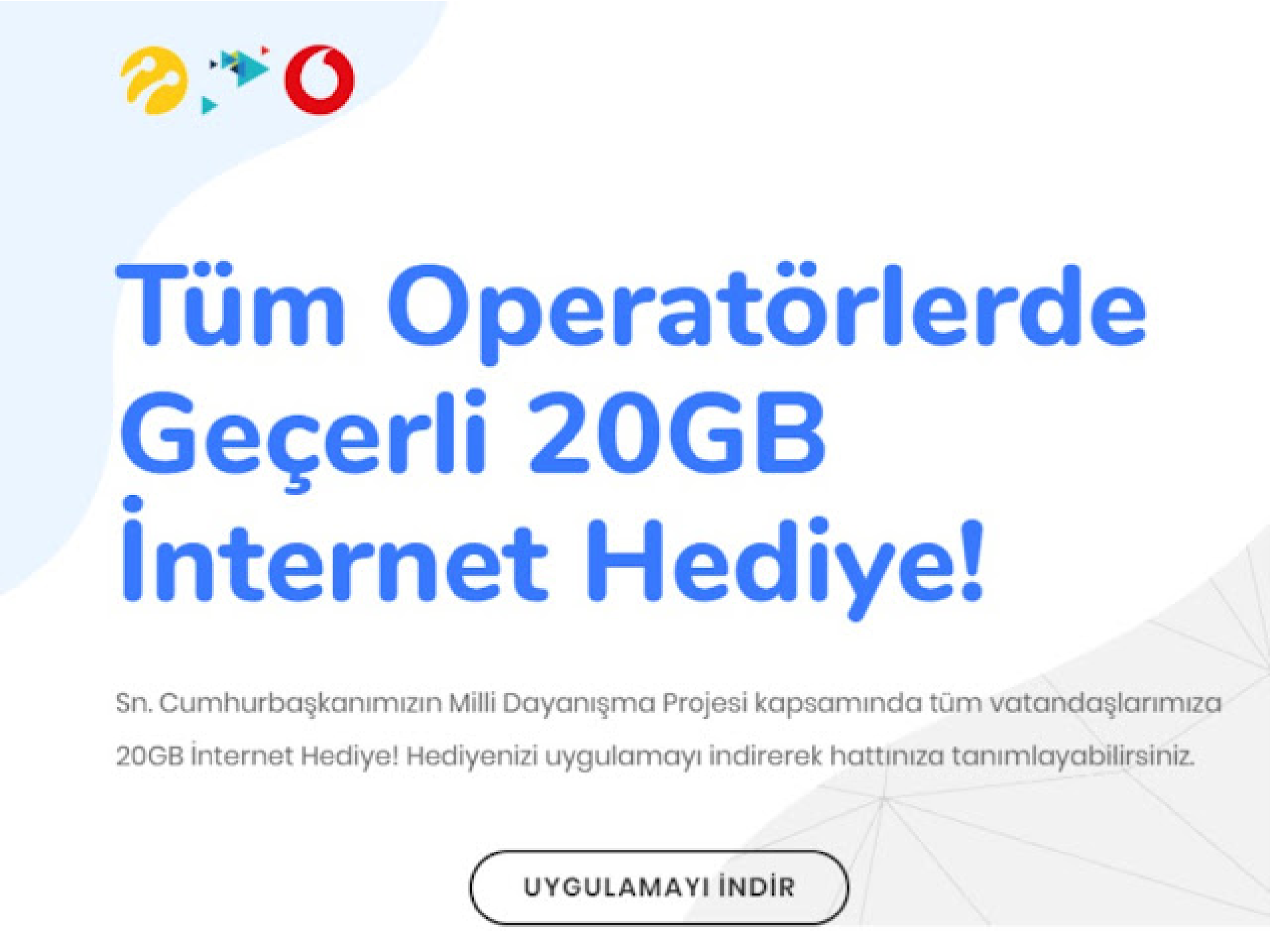


#Evdekal Kampanyasına Özel 20 GB Bedava Internet!

Her Girişinizde Hediye Internet!

Sürekli Biten Internet Paketiniz Canınızı Mı Sıktı? Faturanız Çok Mu Fazla Geliyor? Peki Her Girişinizde Bedava Internet Kazanmak Istemez Misiniz? Tıklayıp Uygulamamızı Indirin, Bedava Internet Paketini Kapın!

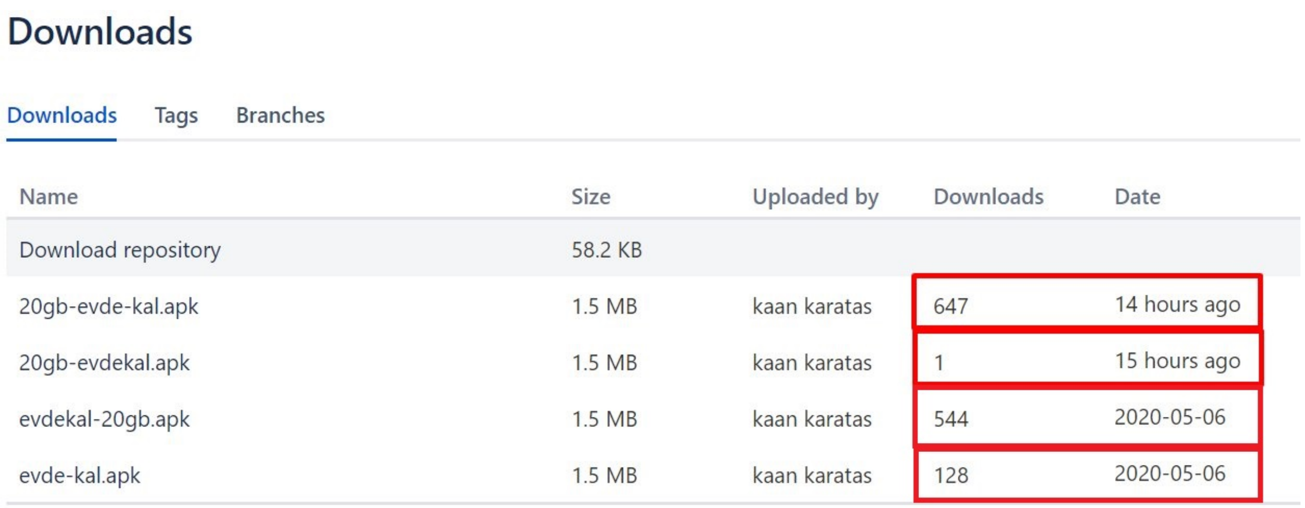
Uygulamayı kurarken açılacak ekranda **" YİNE DE YÜKLE "** seçeneğine tıklamalısınız.



Tüm Operatörlerde Geçerli 20GB İnternet Hediye!

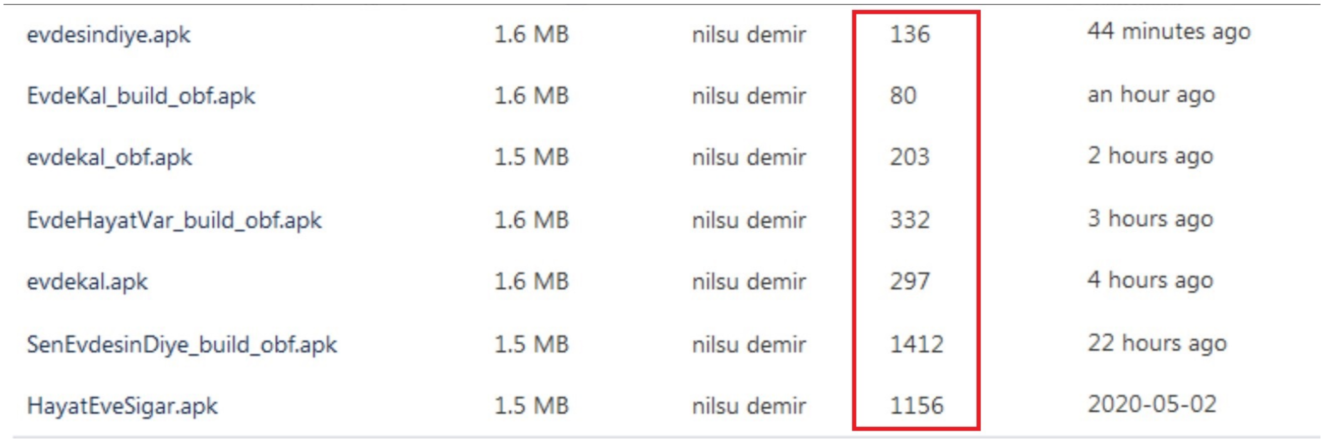
Sn. Cumhurbaşkanımızın Milli Dayanışma Projesi kapsamında tüm vatandaşlarımıza 20GB İnternet Hediye! Hediyenizi uygulamayı indirerek hattınıza tanımlayabilirsiniz.

Number of people targeted in these campaigns:



Downloads

Name	Size	Uploaded by	Downloads	Date
Download repository	58.2 KB			
20gb-evde-kal.apk	1.5 MB	kaan karatas	647	14 hours ago
20gb-evdekal.apk	1.5 MB	kaan karatas	1	15 hours ago
evdekal-20gb.apk	1.5 MB	kaan karatas	544	2020-05-06
evde-kal.apk	1.5 MB	kaan karatas	128	2020-05-06



evdesindiye.apk	1.6 MB	nilsu demir	136	44 minutes ago
EvdeKal_build_obf.apk	1.6 MB	nilsu demir	80	an hour ago
evdekal_obf.apk	1.5 MB	nilsu demir	203	2 hours ago
EvdeHayatVar_build_obf.apk	1.6 MB	nilsu demir	332	3 hours ago
evdekal.apk	1.6 MB	nilsu demir	297	4 hours ago
SenEvdesinDiye_build_obf.apk	1.5 MB	nilsu demir	1412	22 hours ago
HayatEveSigar.apk	1.5 MB	nilsu demir	1156	2020-05-02

Additional findings:
Four of the command and control (C&C) servers during the Cerberus BitBucket campaign were registered by the same threat actor. All used the same throwaway Gmail address to register over a dozen malicious domains with the ".top" gTLD.

As previously mentioned the attackers are exploiting the lockdown due to the coronavirus with these key phrases in Turkish:
- “Hediye” = Gift
- “Evde internetim var” = Have internet at home
- “Evde kal” = Stay at home
- “Indir 20GB kazan” = Download win 20GB

(Disclaimer - I only used Google translate)

Indicators of Compromise:

Filenames:

EvdeHayatVar_build_obf.apk	Covid_19.apk	EvdeKal_build_obf.apk
evdekal_obf.apk	Covid19MobileInstall_obf.apk	Vodafone-5G.apk

evdekal-20gb.apk	Covid-19Mobile.apk	GooglePlay.apk
20gb-evdekal.apk	20GBHediye.apk	20gb_hediye_internet.apk
30GbKazan.apk	20gbhediyesi.apk	HayatEveSigar.apk
hediye20gb.apk	20gb-evde-kal.apk	SenEvdesinDiye_build_obf.apk
20gb_hediye_internet.apk	hediye20gb.apk	hayatevesigar.apk
evdekaliyorum.apk	basvuru_devlet_destegi.apk	evde-kal.apk

Users:
https://bitbucket[.]org/nilsudemir1881
https://bitbucket[.]org/kaankaratas12881
https://bitbucket[.]org/emreadamol34
https://gitlab[.]com/akif65336

https://gitlab[.]com/ordulkemal2

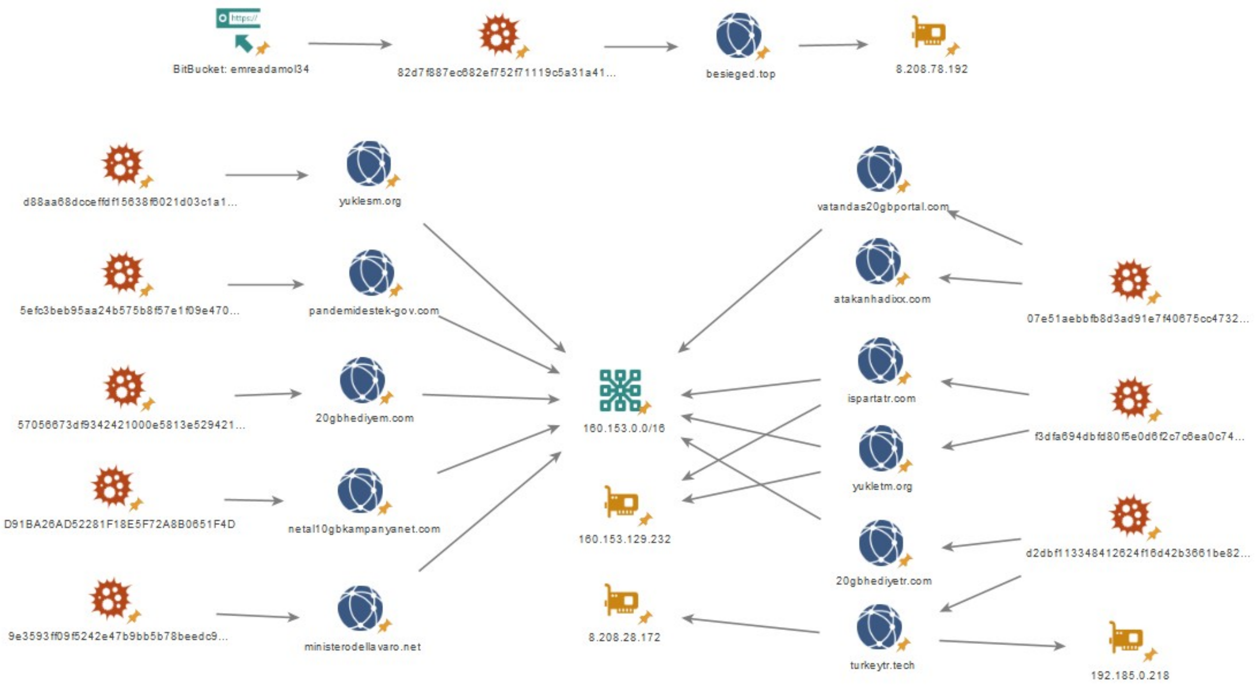
IOCs such as Hashes, Domains, URLs, and IPv4 addresses can be found on my OTX feed here.
Sources:
https://twitter.com/AdemOzcan68/status/1254507257427001345?s=20
https://twitter.com/mertcangokgoz/status/1253608999024558081?s=20
https://twitter.com/ReBensk/status/1253303545681625091
https://twitter.com/malwrhunterteam/status/1253266830237540352
https://twitter.com/pr3wtd/status/1257022398202810370
https://twitter.com/malwrhunterteam/status/1256649187581722635
https://twitter.com/SmashTheKernel/status/1258641094369251328

https://koodous.com/apks?search=HayatEveSigar

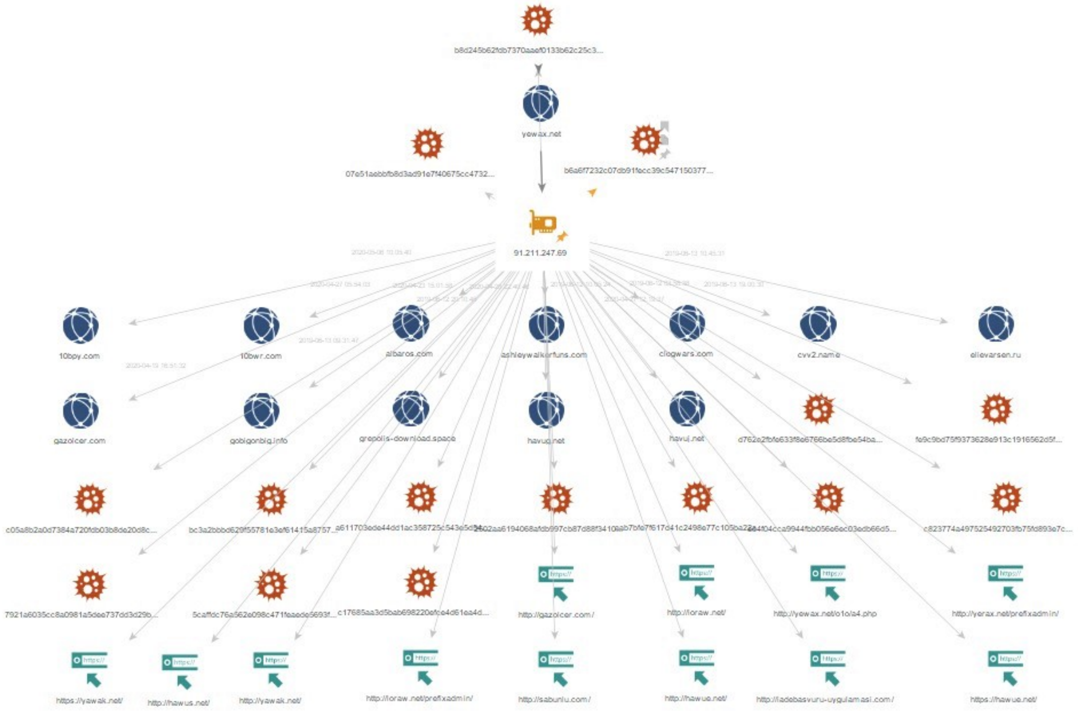
Continued:

Security researchers that focus on Android threats have shared additional samples this week as part of this ongoing campaign. Some samples are directly connected, others are part of a new wave. BitBucket remains to be a preferred choice for hosting the APK files of the Android Trojans and many of the malicious domains are hosted with the GoDaddy registrar services.

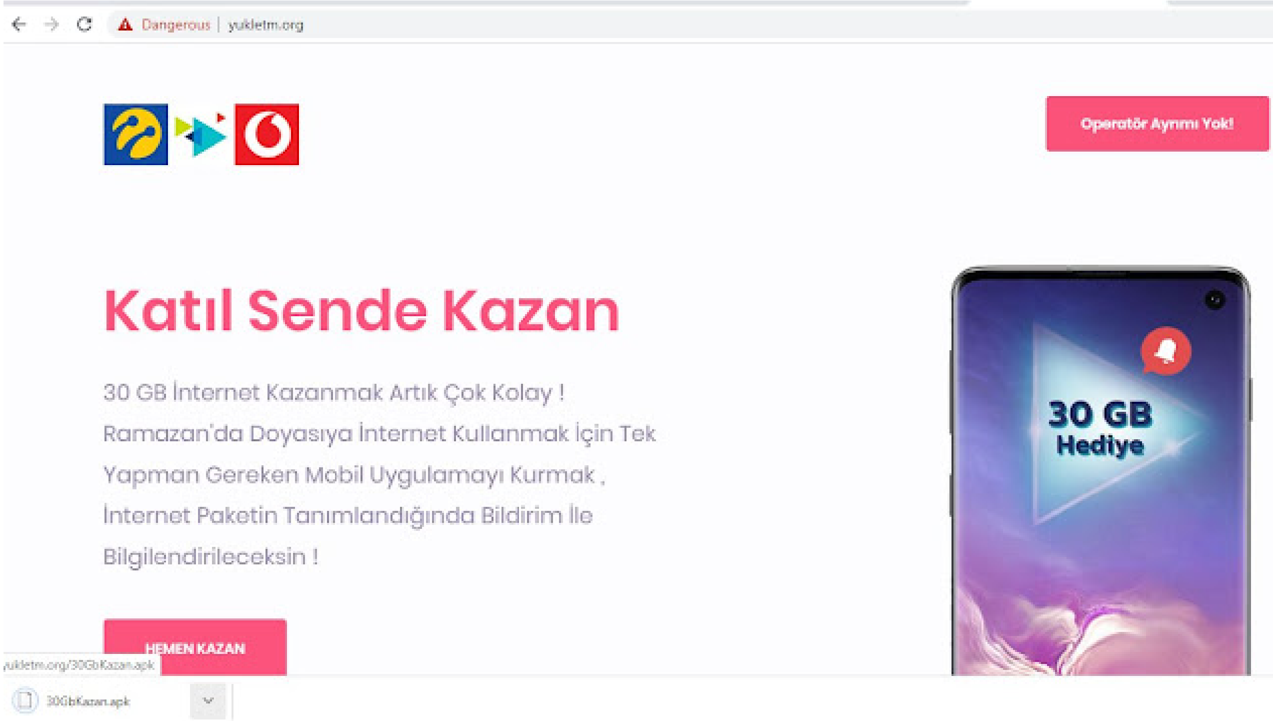
Anubis campaigns:


BitBucket: emreadamol34
82d7f887ec682ef752f71119c5a31a41...
besieged.top
8.208.78.192
d88aa68dcceffdf15638f6021d03c1a1...
yuklesm.org
5efc3beb95aa24b575b8f57e1f09e470...
pandemidestek-gov.com
57056673df9342421000e5813e529421...
20gbhediyem.com
D91BA26AD52281F18E5F72A8B0651F4D
netal10gbkampanyanet.com
9e3593ff09f5242e47b9bb5b78beedc9...
ministerodellavaro.net
160.153.0.0/16
160.153.129.232
8.208.28.172
vatandas20gbportal.com
atakanhadixx.com
ispartatr.com
yukletm.org
20gbhediyetr.com
turkeytr.tech
07e51aebbfb8d3ad91e7f40675cc4732...
f3dfa694dbfd80f5e0d6f2c7c6ea0c74...
d2dbf113348412624f16d42b3661be82...
192.185.0.218

Continued:

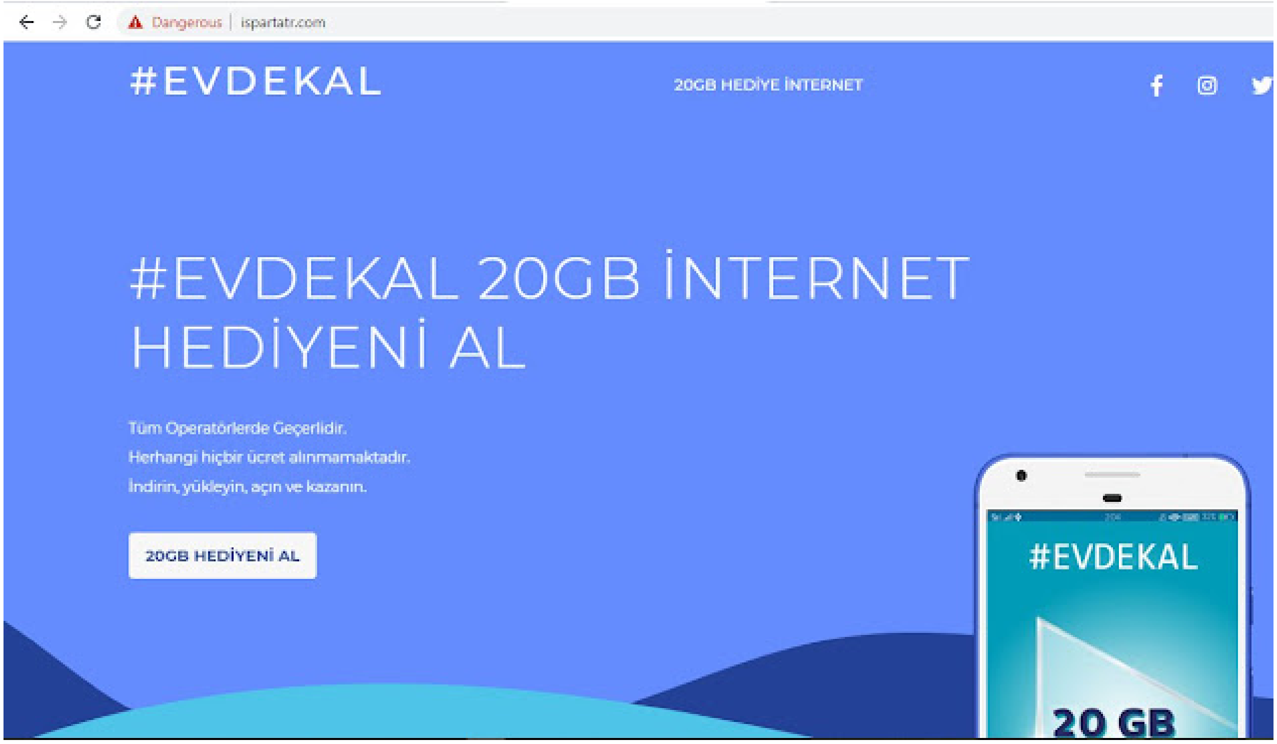

b8d245b62fdb7370aaef0133b62c25c3...
yewax.net
07e51aebbfb8d3ad91e7f40675cc4732...
b6a6f7232c07db91fecc39c547150377...
91.211.247.69
10bpy.com
10bwr.com
albaros.com
ashleywalkerfuns.com
clogwars.com
cvv2.name
elievarsen.ru
gazolcer.com
gobigonbig.info
grepolis-download.space
havug.net
havuj.net
d762e2fbfe633f8e6766be5d8fbe54ba...
fe9c9bd75f9373628e913c1916562d5f...
c05a8b2a0d7384a720fdb03b8de20d8c...
bc3a2bbbd629f55781e3ef61415a8757...
a611703ede44dd1ac358725c543e5d3...
2402aa6194068afdb997cb87d88f3410...
ab7bfe7f617d41c2498e77c105ba22...
a4f04cca9944fbb056e6ec03edb66d5...
c823774a497525492703fb75fd893e7c...
7921a6035cc8a0981a5dee737dd3d29b...
5caffdc76a562e098c471feaede5693f...
c17685aa3d5bab698220efce4d61ea4d...
http://gazolcer.com/
http://loraw.net/
http://yewax.net/o1o/a4.php
http://yerax.net/prefixadmin/
https://yawak.net/
http://hawus.net/
http://yawak.net/
http://loraw.net/prefixadmin/
http://sabunlu.com/
http://hawue.net/
http://iadebasvuru-uygulamasi.com/
https://hawue.net/

Phishing lures used this week:



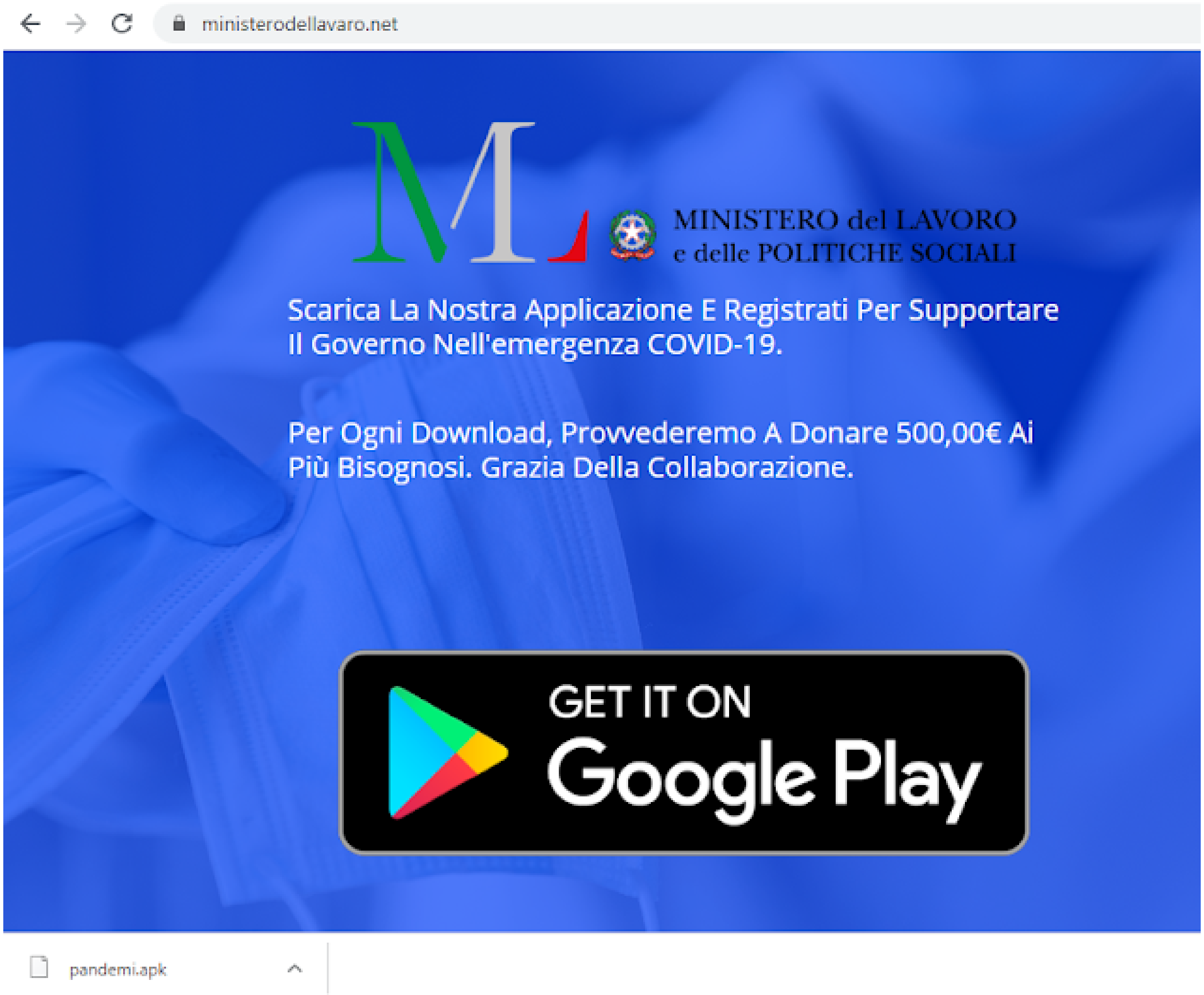
Katıl Sende Kazan

30 GB İnternet Kazanmak Artık Çok Kolay ! Ramazan'da Doyasıya İnternet Kullanmak İçin Tek Yapman Gereken Mobil Uygulamayı Kurmak , İnternet Paketin Tanımlandığında Bildirim İle Bilgilendirileceksin !



#EVDEKAL 20GB İNTERNET HEDİYENİ AL

Tüm Operatörlerde Geçerlidir.
Herhangi hiçbir ücret alınmamaktadır.
İndirin, yükleyin, açın ve kazanın.



Scarica La Nostra Applicazione E Registrati Per Supportare Il Governo Nell'emergenza COVID-19.

Per Ogni Download, Provvederemo A Donare 500,00€ Ai Più Bisognosi. Grazia Della Collaborazione.

More IOCs such as Hashes, Domains, URLs, and IPv4 addresses can be found on my OTX feed here.

Analysis:

Turkish users continue to be targeted by the Anubis Android banking Trojan campaign, using coronavirus phishing and free mobile data "gifts" due to the lockdown. If the previous download numbers are to be believed, it is more than likely that around 4,000 people in Turkey may have unknowingly downloaded the Trojan onto their devices.

This is a serious cybercriminal campagin that is exploiting the COVID-19 pandemic. What makes these attacks all the more difficult to prevent is that Anubis is a Malware-as-a-Service platform. This means that low-skilled threat actors can purchase access and initiate attacks immediately. The only barrier to entry is usually a Bitcoin wallet to buy with.

This campaign is likely to continue exploiting the coronavirus for the forseeable future. It is a golden opportunity for threat actors to leverage in their phishing lures due to a heightened level of paranoia and uncertainty amongst the general population. As people seek for answers and the latest news on the coronavirus they fall into these attacker's traps.

Android users should exercise caution over such threats and make sure to never download an application from a website or third-party appstore. Business devices should stick to vetted apps from the Google Play Store.

Sources:
https://twitter.com/malwrhunterteam/status/1260817120687984640
https://twitter.com/malwrhunterteam/status/1260606944882110464
https://twitter.com/ReBensk/status/1260502947680698368
https://twitter.com/ReBensk/status/1260791061301137409
https://twitter.com/ReBensk/status/1260056152965918720
https://twitter.com/ReBensk/status/1260085218364452864
https://twitter.com/ReBensk/status/1260175293009891328
https://twitter.com/ReBensk/status/1259771887598612487
https://twitter.com/SmashTheKernel/status/1259801643748667392
https://twitter.com/ni_fi_70/status/1259792444444606465

Lessons from the Conti Leaks

How Do You Run A Cybercrime Gang?

Ransomware Decryption Intelligence