Turkey targeted by Cerberus and Anubis Android banking Trojan campaigns

By BushidoToken

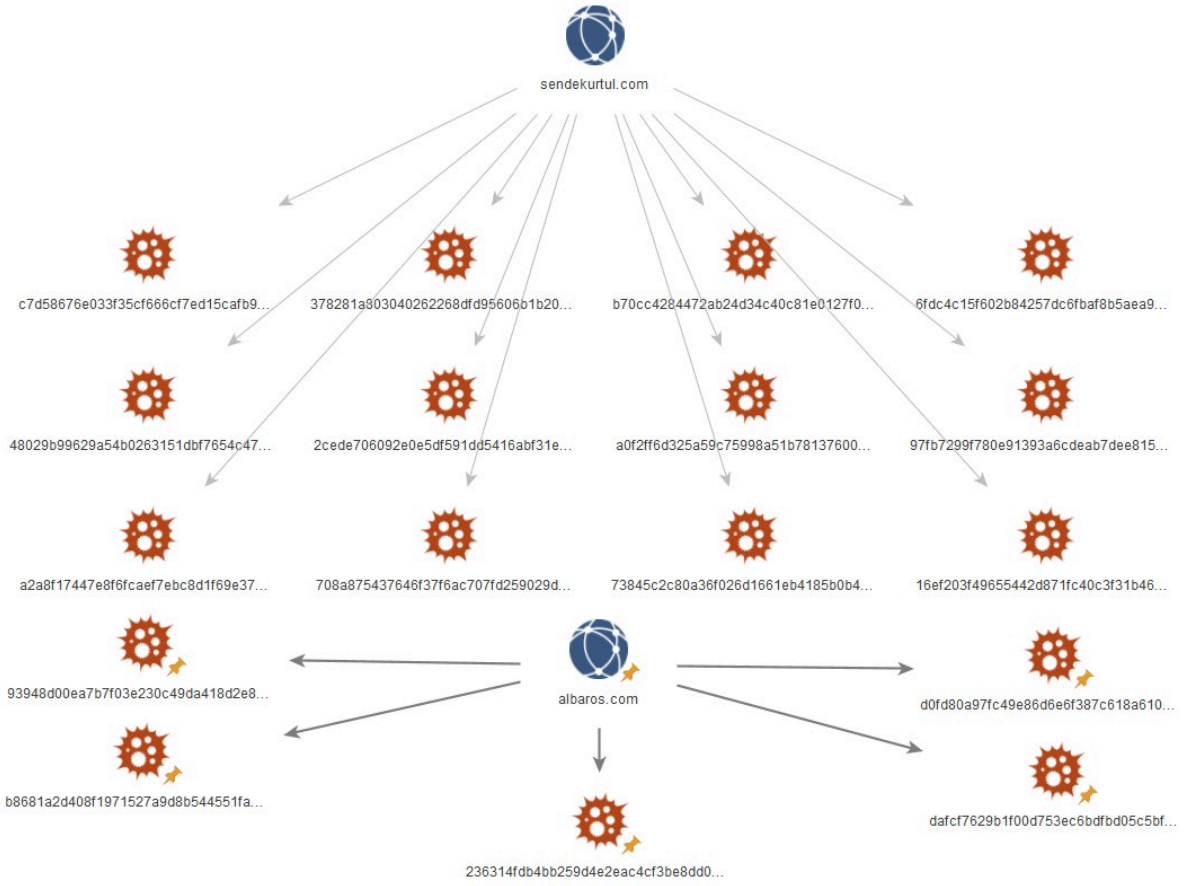
Published: 2020-05-09 · Archived: 2026-04-05 23:10:35 UTC

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.

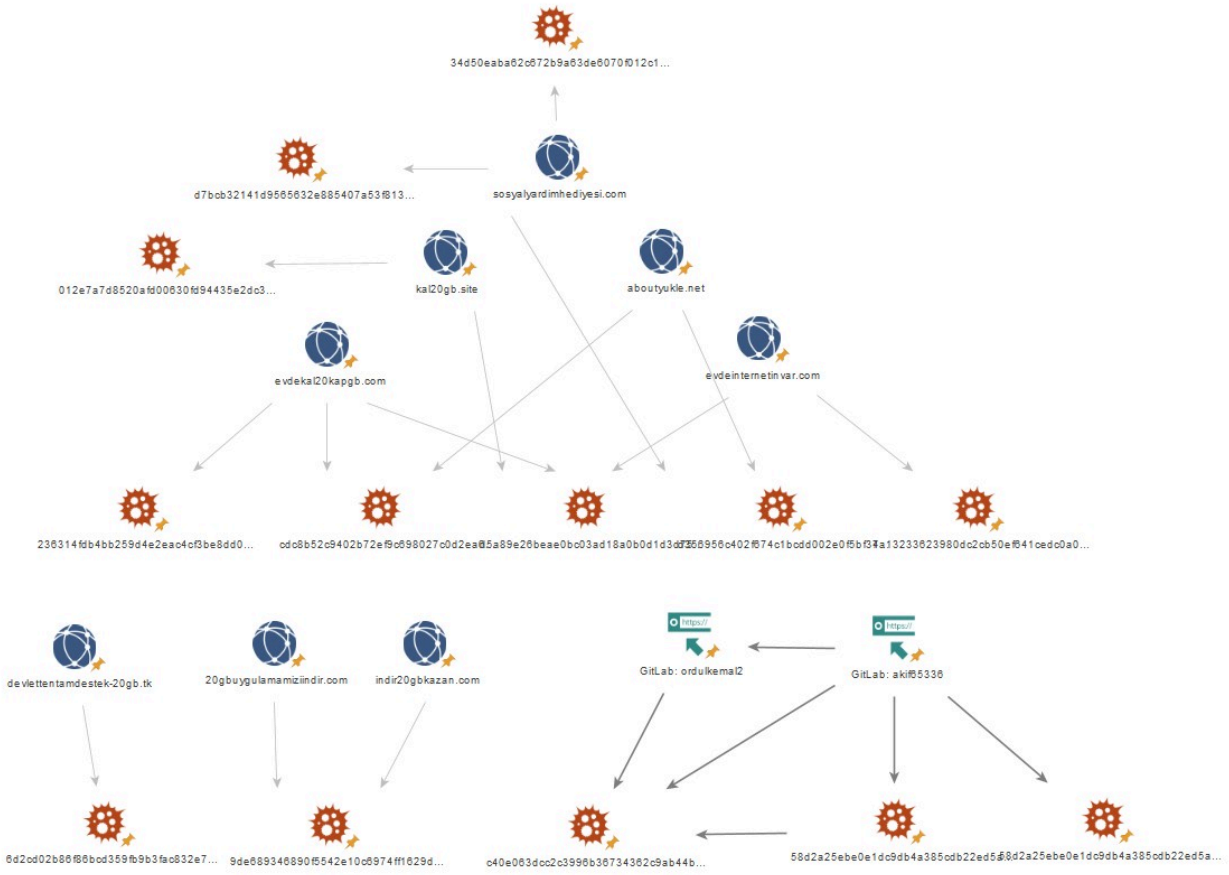
Security researchers such as @MalwareHunterTeam, @ReBensk, @pr3wtd, and @mertcangokgoz, and others have all recently shared new samples of Cerberus and Anubis targeting users in Turkey with mobile data “gifts” that are offered from their mobile carriers due to COVID-19. Various websites are registered 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.

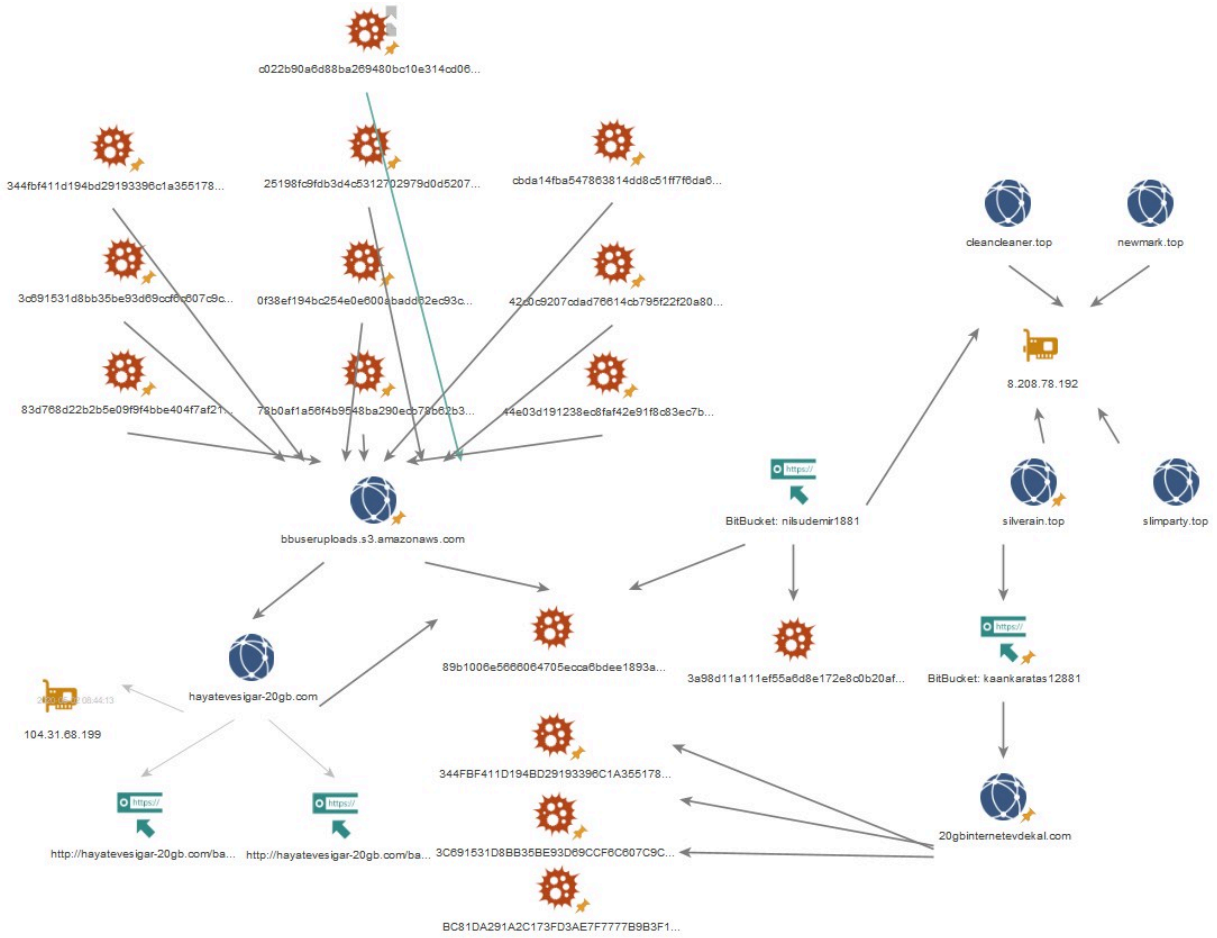
Multiple Anubis campaigns:



Cerberus GitLab campaign:



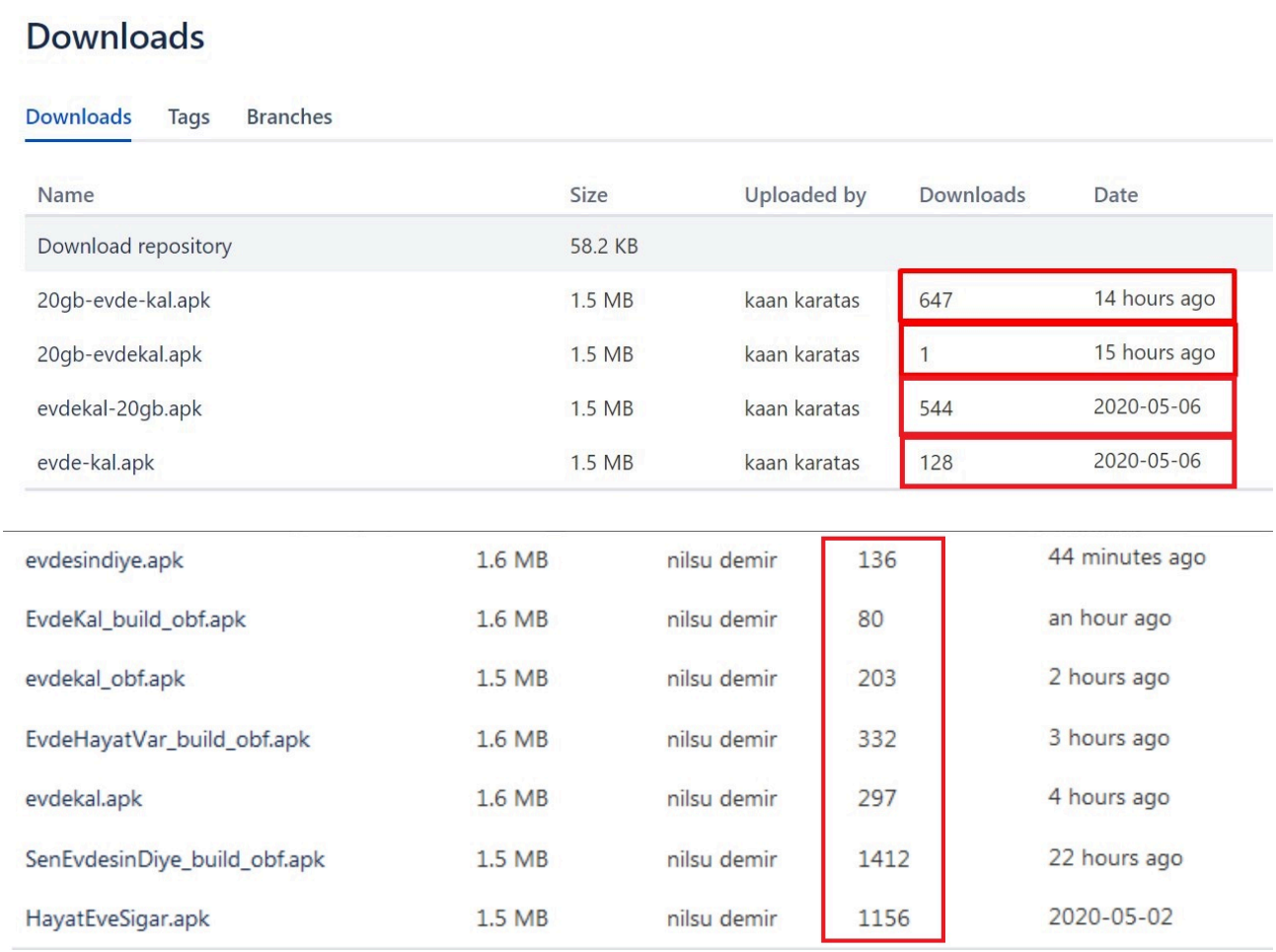
Cerberus BitBucket campaign:



Phishing lures:


#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.
Hemen indirin
Google play
TURKCELL
Türk Telekom
vodafone

Number of people targeted in these campaigns:



Downloads

Downloads Tags Branches

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:
