Android Malware Intercepts SMS 2FA: We have the Logs!

securityboulevard.com/2018/09/android-malware-intercepts-sms-2fa-we-have-the-logs/

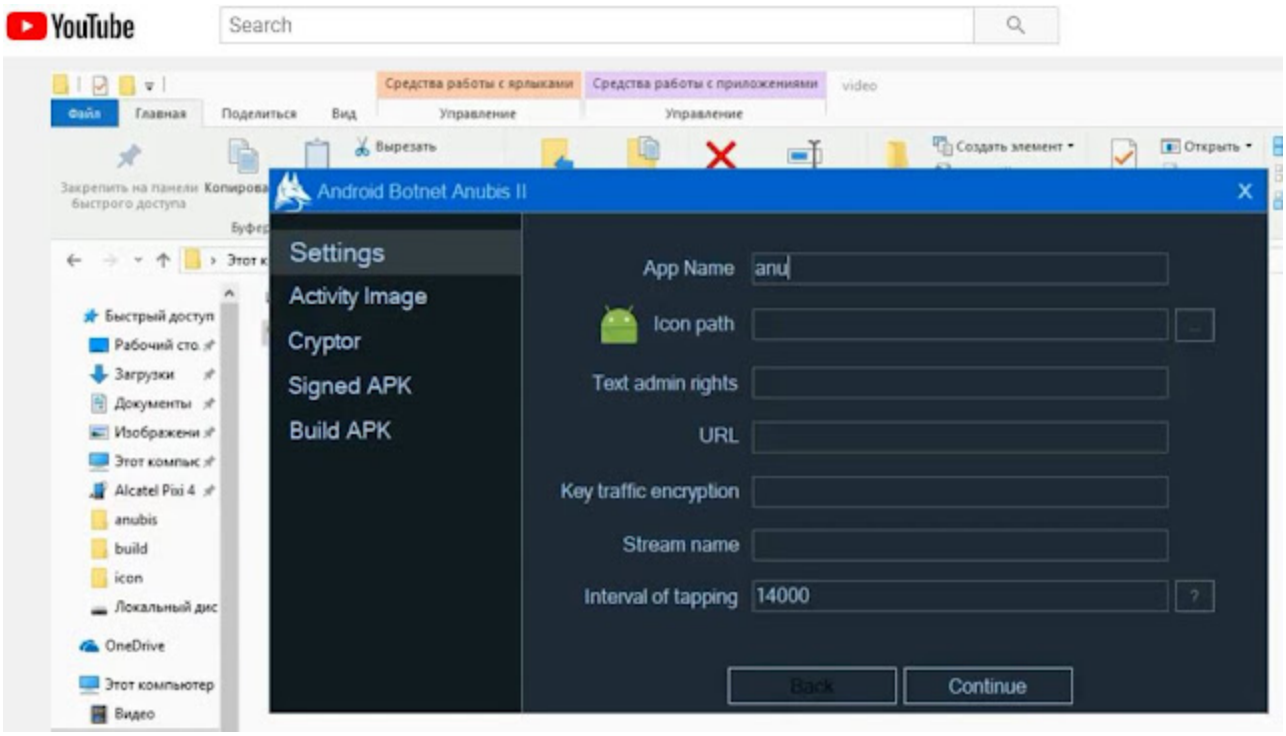
by Gary Warner, UAB on September 10, 2018 September 10, 2018

A couple years ago I was doing some phishing investigations training at the Police School in Santiago, Chile. One module in my training was called “Logs Don’t Lie” which pointed out that in most cases we have everything we need to prioritize a phishing response just by looking at the log files, either on the compromised phishing server, or in the Financial Institutions own logs.

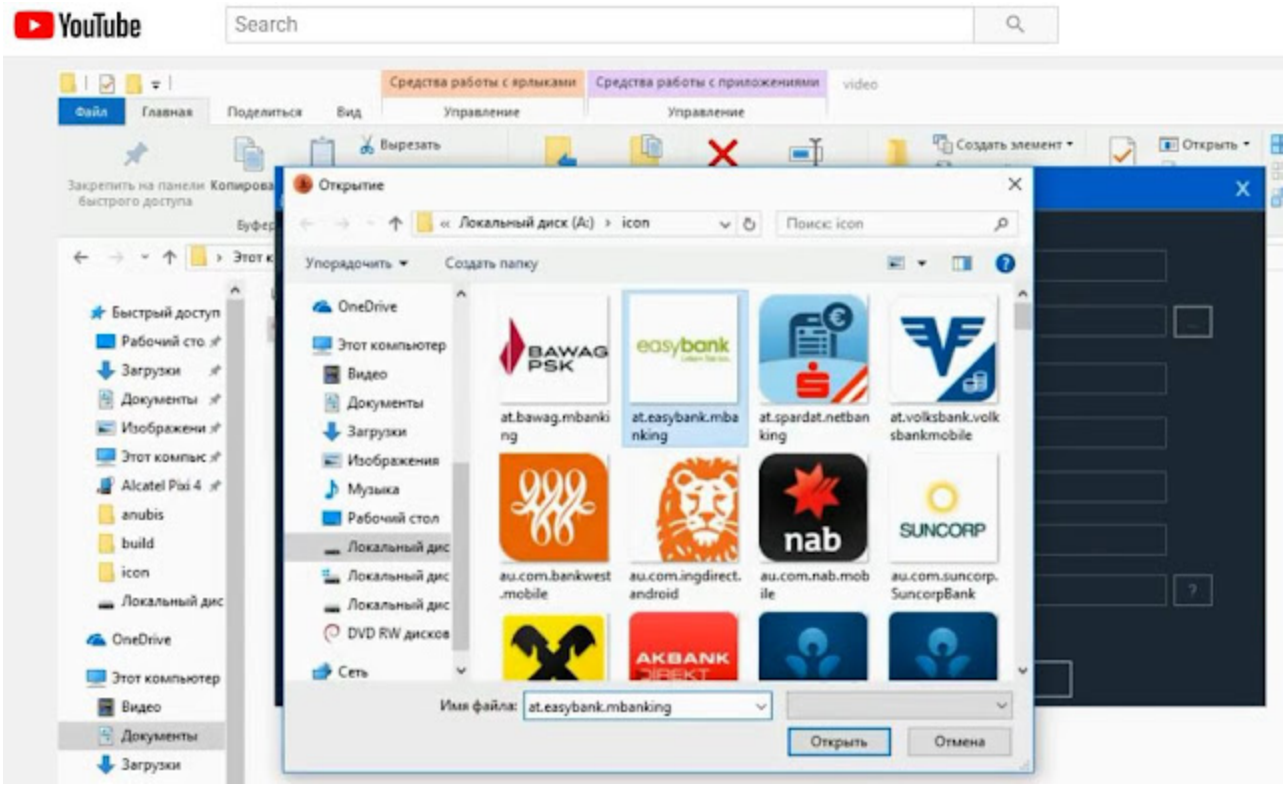
Malware C2 servers are another great place to apply the rule “Logs Don’t Lie.” Most security researchers realize that there is a great cloud of fellow researchers on Twitter sharing little tips and glimpses of their investigations. @LukasStefanko and @nullcookies and I have been looking at a C2 server for a piece of Android malware. And the Logs are AMAZINGLY helpful at understanding just what kind of damage such a trojan can do!

(Sidenote: *@nullcookies is a monster for finding fresh and interesting phish (and often related tools), while @LukasStefanko is an awesome malware analyst for ESET, specializing in Android-based malware. You should follow both on Twitter if you care about such things. Thanks to them both for the pointer that leads to what follows.)*

In this case, the malware is believed to be called “Anubis II” and likely uses the “Builder” that is depicted in this YouTube video, titled “Builder Android Bot Anubis 2“

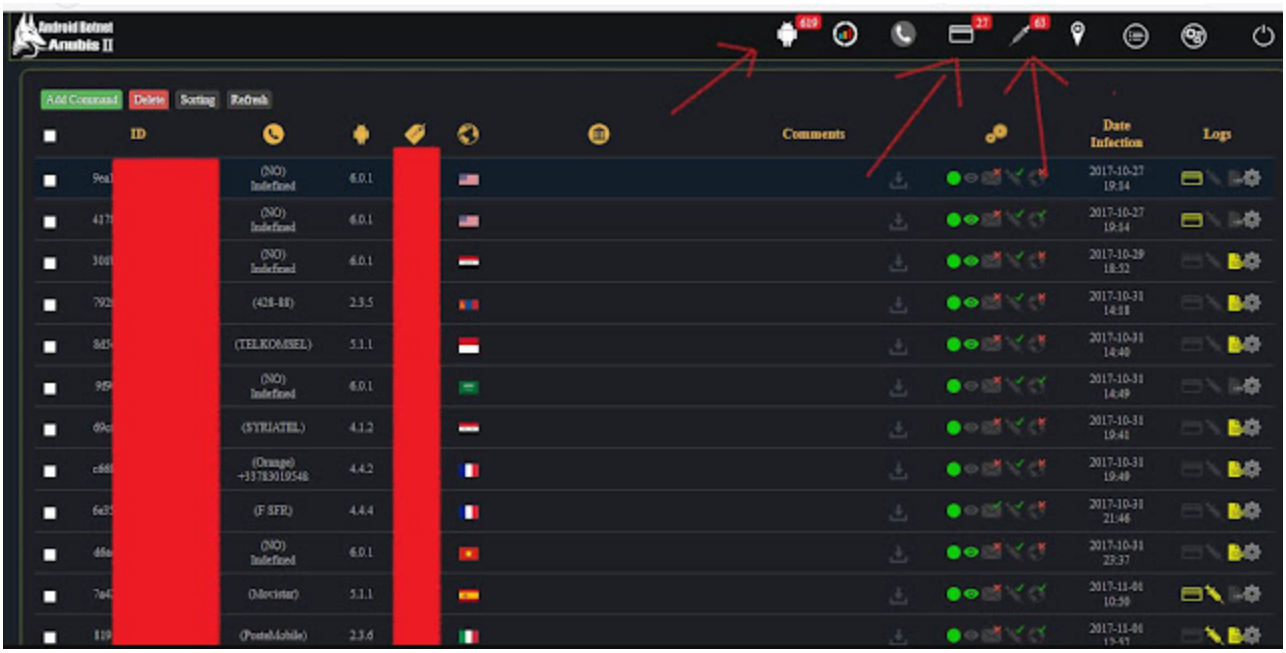


Launcher the APK Builder “Android Botnet Anubis II”



Malware actor chooses from his list of banking targets

In the comments section of the video, someone has shared a screen shot of the botmaster's control panel. In this case it is demonstrating that 619 Android phones can be controlled from the botnet:



Phones that can be controlled from Anubis II control panel

In the particular instance referred to by Lukas and NullCookies, the malware seems to have been active primarily in June of 2018. The server hosting the Anubis II panel has a list of banks that it can present.

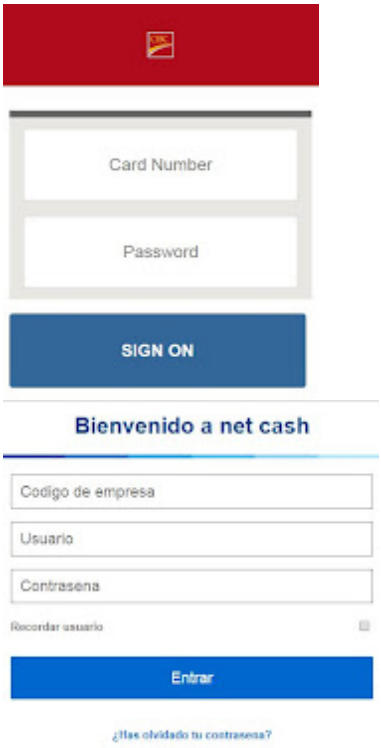
The targets which have custom web inject (or phone inject) content include:

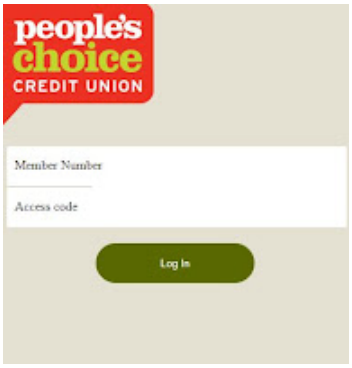
- 7 Austrian banks
- 18 Australian banks
- 5 Canadian banks
- 6 Czech banks
- 11 German banks
- 11 Spanish banks
- 11 French banks
- 8 Hong Kong banks
- 11 Indian banks
- 6 Japanese banks
- 1 Kenyan bank
- 4 New Zealand banks
- 32 Polish banks
- 4 Romanian banks
- 9 Turkish banks

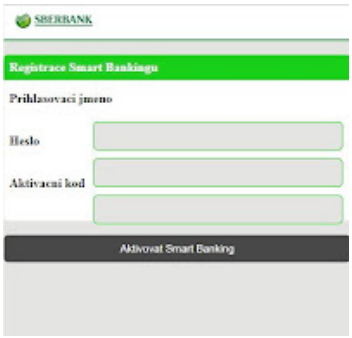
- 10 UK banks (Bank of Scotland, Barclays, CSGCSDNMB, Halifax, HSBC, Natwest, Royal Bank of Scotland, Santander, TSB, Ulster)
- 10 US banks (Bank of America, Capital One, Chase, Fifth Third, NetTeller, Skrill, SunTrust, USAA, US Bank, Wells Fargo Mobile)

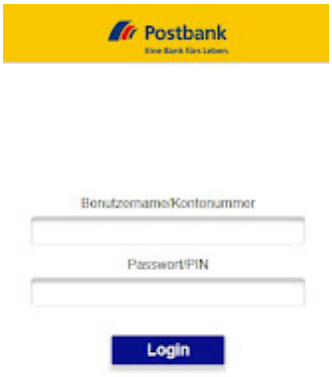
Fake Android Login Pages for Banks

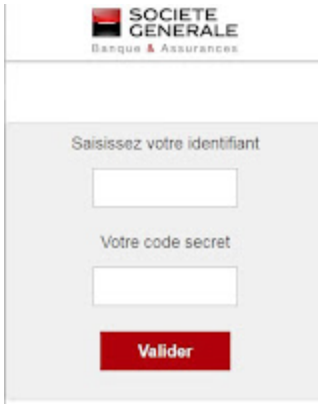
While each of the 190 sites has a fake login page available, we thought we would show a sampling from banks around the world . . .

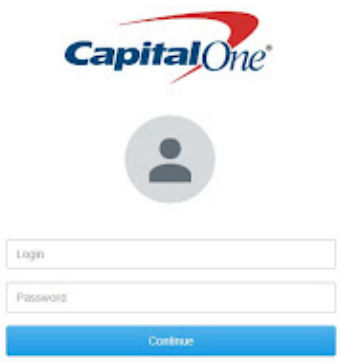


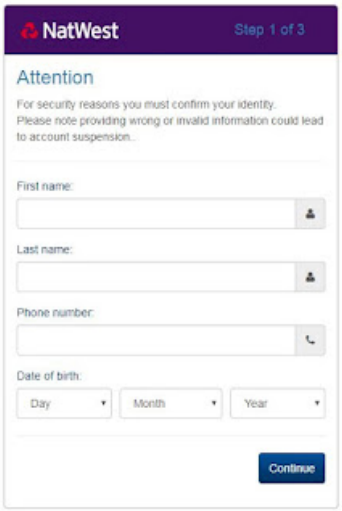












There are also several Crypto Currency organizations listed:

- blockchaine
- coinbase
- localbitcoin
- unocoin

As well as some Online Payment, Email, and Social Media sites:

- eBay
- Facebook

- Gmail
- PayPal
- ZebPay

Each bank on the list has the equivalent of a phishing page that can be presented if the owner of the android phone attempts to log in to the given bank.

Some of them have silly typographical errors that will hopefully reduce success, such as this Wells Fargo content, inviting the phone owner to “Sing In” to the bank. Perhaps there is a Wells Fargo Choir? Hopefully that will cause victims to NOT fall for this particular malware!

The Wells Fargo Choir? Sing On!

The SMS Intercepts

One of the main benefits of having access to the server was to see so many examples of successful SMS message intercepts! At the time of the server dump, this one contained 32,900+ unique “keylog” entries and 52,000+ logged SMS messages from at least 47 unique devices.

Here’s an example showing a Bank Two Factor Authentication request being forward to the criminals:

Text: Bank of Redacted: 819881 is your authorization code which expires in 10 minutes. If you didn’t request the code, call 1.800.xxx.xxxx for assistance.

Keylogging was also enabled, allowing the criminal to see when a bank app was being used:

*06/14/2018, 09:07:34 EDT|(FOCUSED)|[From:, REDACTED BANK, Account Number:, ******6680, Date:, May 30, 2018 10:10:42 AM EDT, Status:, Canceled, Amount:, $100.00, Type:, Deposit, Transfer ID:, 25098675]*

In this example, an online payment company is sharing a message:

06/29/2018, 15:28:46 EDT|(CLICKED)|[Friendly reminderThis is Mr. XXXXXXX from REDACTED. This is a friendly reminder that you have a payment due today by 6pm If you have any questions or need to make a payment via phone call 804-999-9999 or we have a new payment processing system that allows , for your convenience, to simply text in the last 4 digits of a card you've previously used and the security code and we're able to process your payment. Feel free to call REDACTED with any questions at 804-xxx-xxxx]

Hundreds of Gmail verification codes were found in the logs:

06/14/2018, 00:19:33 EDT|(FOCUSED)|[G-473953 is your Google verification code., 1 min ago]

Quite a few Uber codes were also found in the logs:

Text: [#] 9299 is your Uber code. qlRnn4A1sbt

Paypal, Quickbooks, LinkedIn, Facebook, Stash, and Stripe all had 2FA codes make appearances in the logs:

Text: FREE PayPal: Your security code is: 321842. Your code expires in 10 minutes. Please don't reply.

Text: [Your QuickBooks Self-Employed Code is 952708, 1 min ago]

Text: 383626 is your Facebook password reset code or reset your password here: https://fb.com/l/9wBUVuGxxxx5zC

Text: Your LinkedIn verification code is 967308.

Text: 103-667 is your Stripe verification code to use your payment info with Theresa.

Text: Your Stash verification code is 912037. Happy Stashing!

Text: Cash App: 157-578 is the sign in code you requested.

Text: Your verification code for GotHookup is: 7074
In a directory called "/numers/" there were also examples of address book dumps from phone contacts. The small number of these seem to indicate this would be a "triggered" request, where the botnet operator would have to request the address book. In the example we found, with seven area code (404) numbers, four (770) numbers and four (678) numbers, it is likely an Atlanta, Georgia based victim.

The Keylogging feature also seems to be something that is turned on or off by request of the botnet operators. There were far fewer devices for which keylogs were found. Example keylog entries looked like this:

A telephone prompt looked like this:

- *06/15/2018, 14:38:55 EDT|(CLICKED)|[Call management, •, 10m, 4 missed calls, Ashley Brown (3), Mom]*
- *06/15/2018, 14:38:59 EDT|(CLICKED)|[Call Ashley Big Cousin, Quick contact for Ashley Brown]*
- *06/15/2018, 14:39:01 EDT|(CLICKED)|[1 804-999-9999, Mobile, Call Ashley Brown]*

Responding to a message looked like this:

- *06/15/2018, 16:02:34 EDT|(CLICKED)|[Messaging, •, now, Expand button, (804) 999-9999 , Hey Terry can you send the address, REPLY]*
- *06/15/2018, 16:02:37 EDT|(FOCUSED)|[Aa]*
- *06/15/2018, 16:02:46 EDT|(CLICKED)|[Copy, Forward, Delete]*
- *06/15/2018, 16:02:50 EDT|(FOCUSED)|[]*
- *06/15/2018, 16:02:54 EDT|(CLICKED)|[Messaging]*
- *06/15/2018, 16:02:57 EDT|(CLICKED)|[Enter message]*
- *06/15/2018, 16:05:11 EDT|(CLICKED)|[Answer]*
- *06/15/2018, 16:05:29 EDT|(CLICKED)|[]*
- *06/15/2018, 16:10:50 EDT|(FOCUSED)|[]*
- *06/15/2018, 16:10:52 EDT|(CLICKED)|[Enter]*
- *06/15/2018, 16:11:01 EDT|(FOCUSED)|[2007 Their Address Ct North CityTheyTyped OK 11111]*
- *06/15/2018, 16:11:03 EDT|(FOCUSED)|[]*

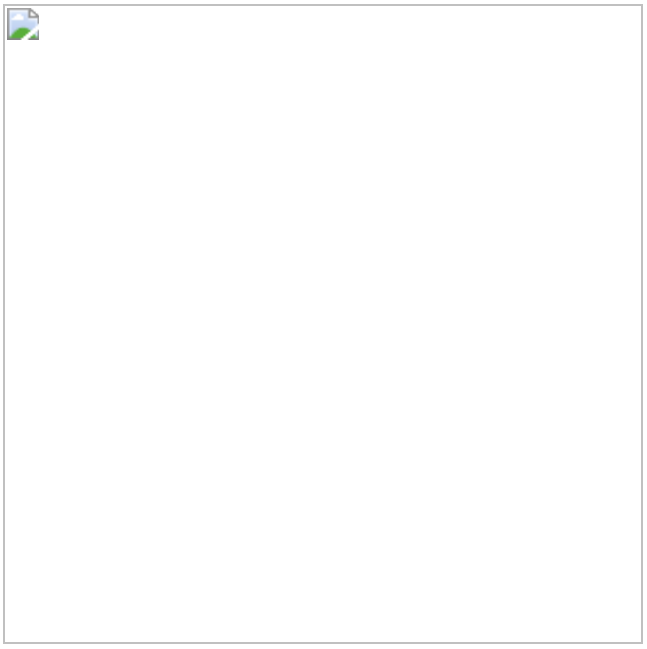
A YouTube session looked like this:

- *06/27/2018, 15:23:36 EDT|(CLICKED)|[YouTube]*
- *06/27/2018, 15:23:46 EDT|(CLICKED)|[Pause video]*
- *06/27/2018, 15:41:19 EDT|(FOCUSED)|[14:46, Go to channel, FINDING OUT THE GENDER!!!, Menu, The Rush Fam · 26K views4 hours ago, 6:12, Go to channel, TRY NOT TO CRY CHALLENGE REACTION WITH KID (SHE ACTUALLY CRIED), Menu, CJ SO COOL · 2.5M views · 1 year ago, SUBSCRIBED]*
- *06/27/2018, 15:46:38 EDT|(FOCUSED)|[]*
- *06/27/2018, 15:46:41 EDT|(CLICKED)|[Enter]*
- *06/27/2018, 15:46:53 EDT|(CLICKED)|[Play video]*
- *06/27/2018, 15:48:06 EDT|(CLICKED)|[· 0:11]*
- *06/27/2018, 15:48:09 EDT|(CLICKED)|[· 0:09]*
- *06/27/2018, 15:48:10 EDT|(CLICKED)|[· 0:08]*

- *06/27/2018, 15:54:30 EDT\(CLICKED)\[Suggested: "BREAKING UP IN FRONT OF COMPANY!!" PRANK ON PANTON SQUAD!!!]*

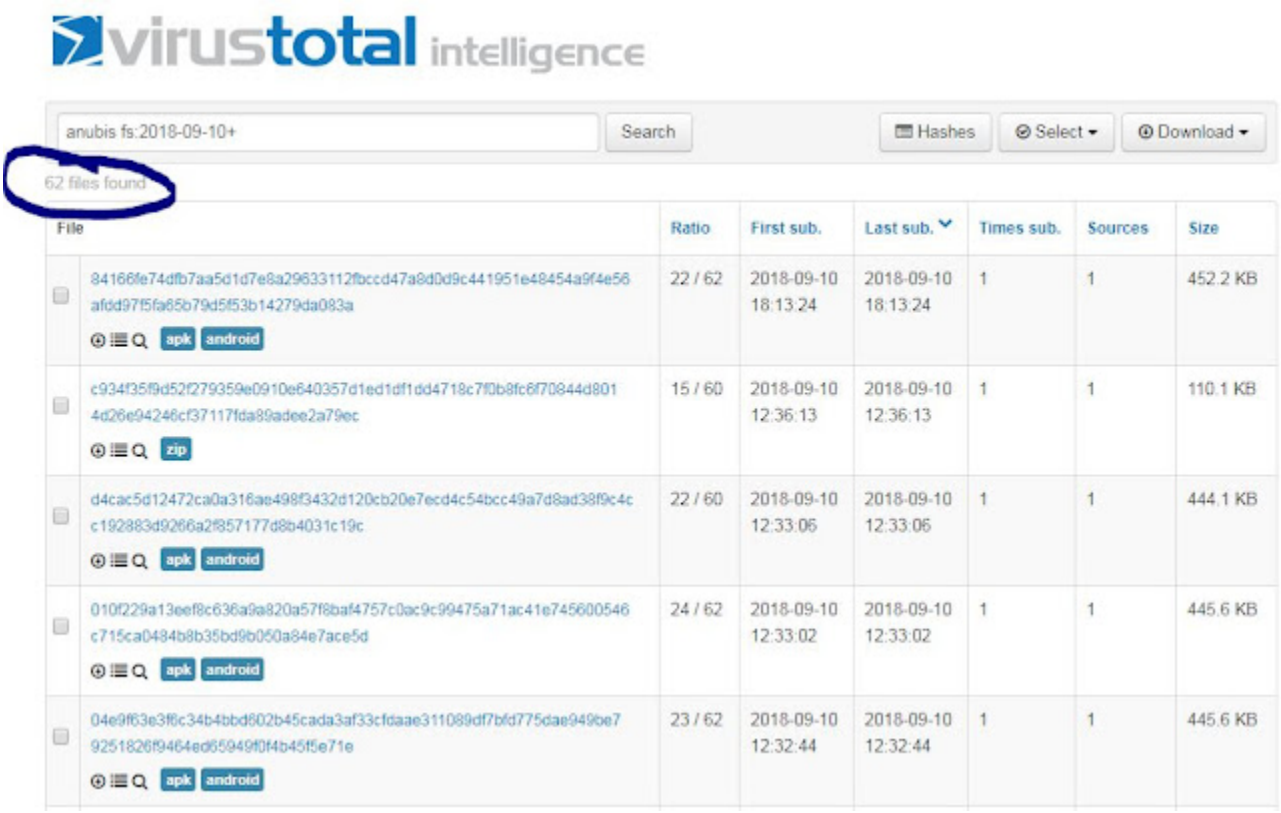
Distribution

From looking for this malware in various collections, such as Virus Total Intelligence, it seems that the malware is fairly common. Many new versions of the malware show up in their collection every day. The most common point of distribution seems to be from the Google Play Store.
A popularly reported stream of such apps was reported on by, well, just about everyone in July 2018. Some of the headlines included:
Anubis Strikes Again: Mobile Malware continues to plague users in Official App Stores – from IBM X-Force Research's Security Intelligence blog
Best graphic goes to Secure Computing Magazine:
BankBot Anubis campaign targets Turkish Android users with fake apps in Google Play store

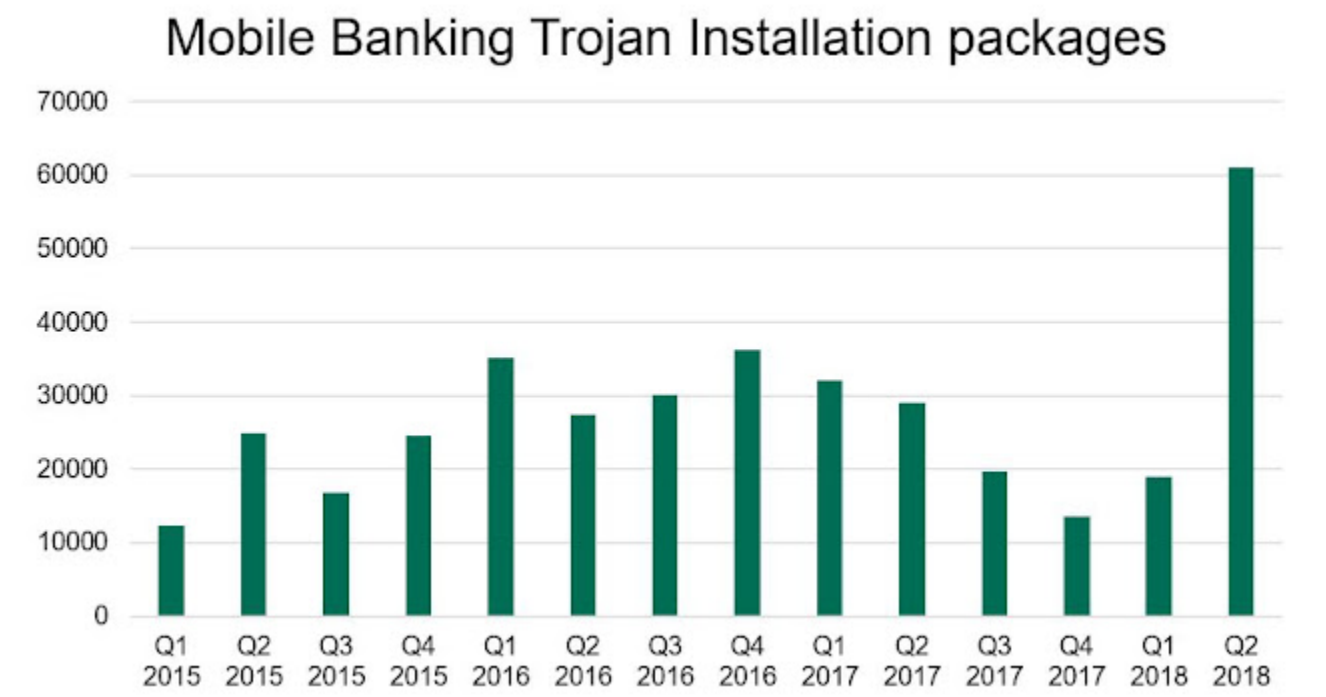


https://www.scmagazine.com/

Medium.com had "Hackers Distributing Anubis Malware via Google Play Store to Steal Login credentials, E-wallets, and Payment Cards Details"
A more recent post, from AlienVault, (20 days ago): "Anubis Android Malware in the Play Store"
A search in VirusTotal Intelligence reveals 62 new filehashes ONLY FROM TODAY (September 10, 2018) that match a definition name of "Anubis". Some of the more popular names for the trojan on VirusTotal include:
DrWeb: Android.BankBot.1679
Ikarus: Trojan-Banker.AndroidOS.Anubis
Kaspersky: HEUR:Trojan-Dropper.AndroidOS.Hqwar.bbSophos: Andr/BankSpy-AH



Kaspersky authored a special article on this banking trojan, which they call “HQWar” back in April under the headline “Phantom menace: mobile banking trojan modifications reach all-time high: Mobile banking Trojans hit the list of cyber-headaches in Q2 2018” In that article they said they have documented 61,000 versions!



Kaspersky: Phantom Menace

As I mentioned Lukas at the beginning of this blog, ESET has produced an amazing number of articles on Android banking trojans lurking in the Google Play store. Here are a few of them:

Jul 26, 2018 – Fake banking apps on Google Play leak stolen credit card data
Dec 11, 2017 – Banking malware on Google Play targets Polish banks
Nov 21, 2017 – New campaigns spread banking malware through Google Play
Sep 25, 2017 – Bankbot trojan returns to Google Play with new tricks
Nov 15, 2017 – Multi-stage malware sneaks into Google Play

Apr 19, 2017 – Turn the light on and give me your passwords!

*** This is a Security Bloggers Network syndicated blog from CyberCrime & Doing Time authored by Gary Warner, UAB. Read the original post at: http://garwarner.blogspot.com/2018/09/android-malware-intercepts-sms-2fa-we.html