Smishing campaign in NL spreading Cabassous and Anatsa

threatfabric.com/blogs/smishing-campaign-in-nl-spreading-cabassous-and-anatsa.html

May 2021

Introduction

In early December 2020 ThreatFabric discovered Cabassous, which was later renamed by PRODAFT to FluBot. This is a classic Android bot, equipped with credential stealing capabilities such as the use of overlays (fake login screens) for crypto-currency wallet apps and Android banking apps. Besides harvesting credentials, the bot also gathers all contact information (phone numbers) from a victim's device to spread itself using SMS messages (smishing).

Another banking trojan named Anatsa was discovered by ThreatFabric analysts in January 2021. It should be considered a stronger threat compared to Cabassous, due to its more extensive and advanced set of features. Anatsa's functionalities include the classic credential-stealing overlay attacks, which are first downloaded and stored on the device, and then launched locally. Other features include keylogging, contact information and device information exfiltration, and accessibility logging. This last feature is very advanced and very dangerous for victims. It grants information to the malicious actors about everything displayed in the device's screen, allowing the bot to interact with the UI elements and record all the information that is displayed in them. We also covered this threat in our latest blog.

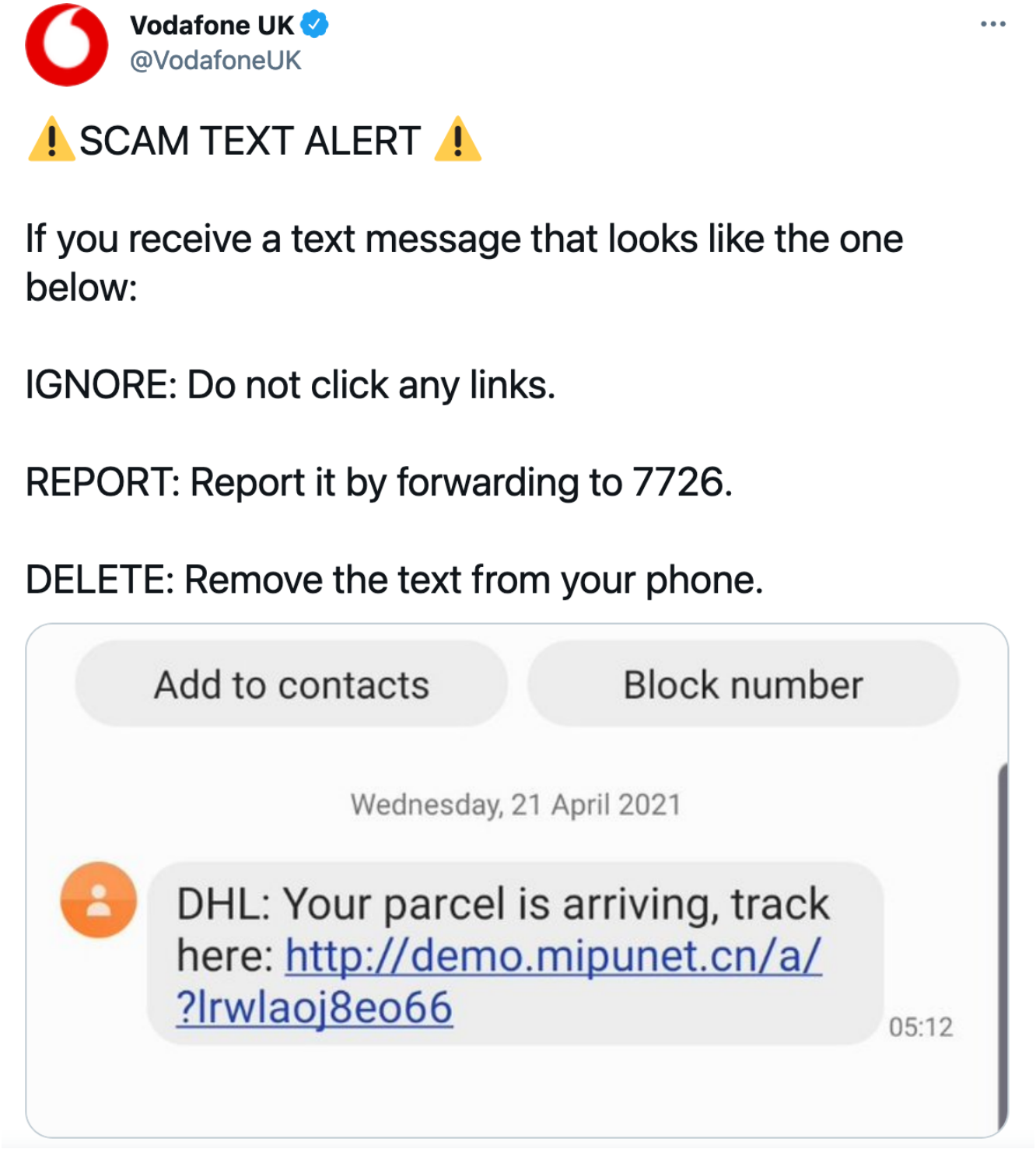
Anatsa has been relatively quiet in the first months of the year, but it has recently increased its activity now including Dutch banks in its target list.

With this threat update we want to inform the users about a new SMS phishing campaign we spotted in the Netherlands masquerading as UPS apps and distributing both Cabassous and Anatsa.

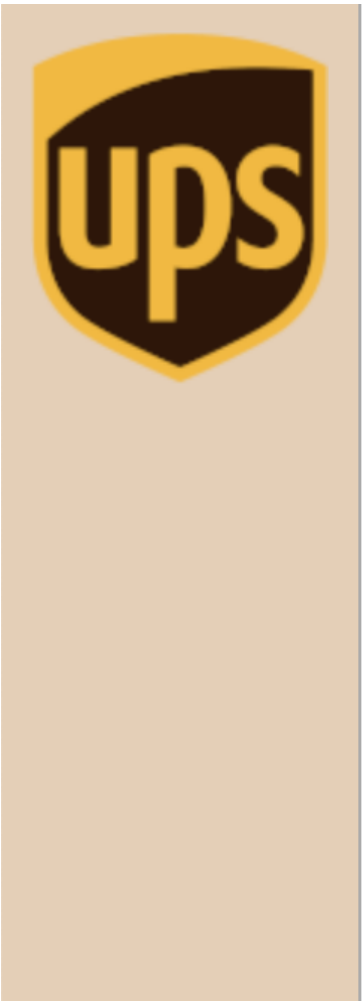
Previous campaigns

On April 18th, Cabassous began to use multiple DGA seeds in every sample allowing it to be more scalable: the Trojan generates corresponding C2 server address to receive the overlay target list specific for the victim's country. This means that every botnet can have its own overlay specific to country of the targeted banking and wallet apps.

As reported by ThreatFabric, enormous SMS phishing campaigns reported by major telecom operators have been observed in multiple new targeted countries, including the UK, Norway, Sweden, Finland, Denmark, Netherlands, and Japan. This also matches with the current smishing campaign reported in the UK masquerading as UPS and DHL apps.



Usually, the SMS contains some link that claims to provide the information about your parcel from DHL or UPS. The link leads to the page with a localized text corresponding to the region defined by the victim's IP location. The text contains instructions to download and install an application, which is the Cabassous Trojan itself.



Latest developments

On May 5th, ThreatFabric analysts spotted a new smishing campaign in the Netherlands masquerading as UPS apps. That is a common MO for Cabassous that has been described above.

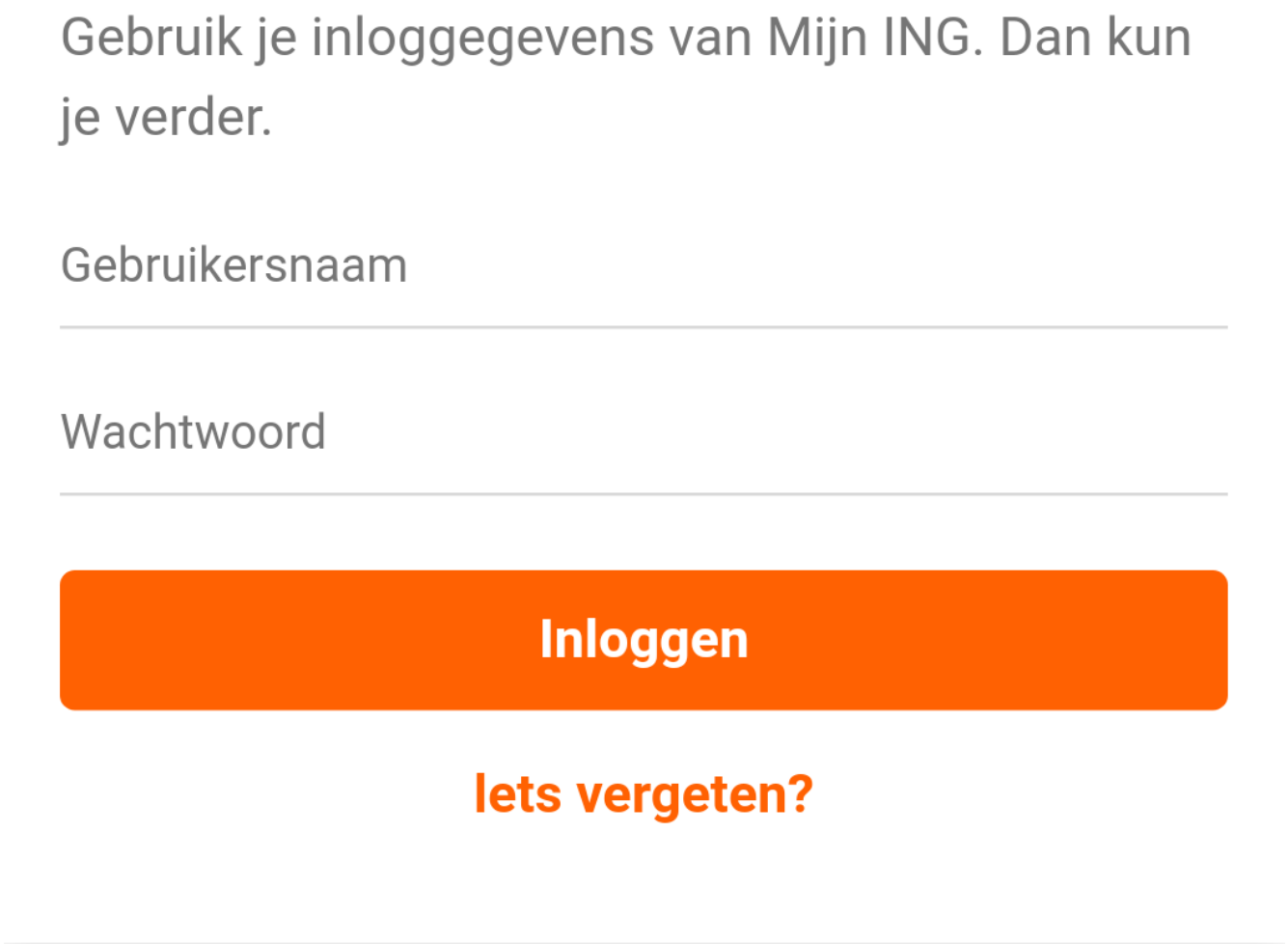
However, besides Cabassous, ThreatFabric analysts were able to obtain the Anatsa Trojan from the same links. That means that at the moment of writing this blog, Anatsa and Cabassous are distributed side-by-side in the Netherlands both masquerading as UPS apps. Nevertheless, there is no solid proof that the actor(s) behind these families are the same.

At the moment of writing Cabassous does not target any application of Netherlands banks, the C2 responsible for the campaign targeting Norway, Sweden, Finland, Denmark, Netherlands and Poland only serves the target list for banking apps in Poland. Anatsa however does have the banking apps from the Netherlands in its target list. The following images are examples of overlays used for the Dutch banks:

X

Particulier Zakelijk

Log je in?



The full lists of targeted applications used by Anatsa and Cabassous can be found in the Appendix.

The danger of Anatsa

When comparing Cabassous with Anatsa, the more dangerous of the two appears to be Anatsa due to its RAT capability. The Trojan can receive a command called “start_client” from the C2 and initiate a connection to a specified IP and port. This connection is used to send and receive data that enables actor(s) to do the following:

- Observe the screen of the victim’s device on a real-time basis
- Perform clicks and actions on behalf of the victim
- Open applications (like banking application or web-browser)
- Manipulate text input

This capability leads to another type of fraud - so called on-device fraud, when actor(s) perform the actual fraud from the device of the victim. The following code snippet represents the actor(s) ability to manipulate text input:

```
while (counter < numberOfActions) {
    int leftBound = byteBuffer.getShort();
    int bottomBound = byteBuffer.getShort();
    byteBuffer.getShort();
    byteBuffer.getShort();
    int length = byteBuffer.getShort();
    byte[] textBytes = new byte[length];
    byteBuffer.get(textBytes, 0, length);
    String setText = new String(textBytes, StandardCharsets.UTF_8);
    AccessibilityNodeInfo rootNodeInfo =
MainAccessibilityService.service.getRootInActiveWindow();
    if (rootNodeInfo != null) {
        for(Object editTextNode: Utils.getAllNodes(rootNodeInfo, "EditText")) {
            AccessibilityNodeInfo accNodeInfo = (AccessibilityNodeInfo)editTextNode;
            Rect v9_1 = new Rect();
            accNodeInfo.getBoundsInScreen(v9_1);
            if (v9_1.left != leftBound || v9_1.bottom != bottomBound) {  // check position
                continue;
            }
            Bundle bundle = new Bundle();
            bundle.putString("ACTION_ARGUMENT_SET_TEXT_CHARSEQUENCE", setText);
            accNodeInfo.performAction(0x200000, bundle);
        }
    }
    ++counter;
}
```

Bot commands

The Anatsa bot supports the following commands:

Command	Description
activate_screen	Enables the screen
app_delete	Uninstalls application
ask_syspass	Shows the request for device password/PIN/gesture
ask_perms	Trigger the bot to request for permissions
stop_pers	Stops persistence mechanisms for 40 seconds

Command	Description
get_accounts	Triggers stealing the list of accounts on the device
kill_bot	Removes the bot from the infected device
mute_phone	Mutes the device
swipe_down	Performs a swipe down gesture
open_inject	Triggers the overlay attack for specified application
open_activity	Opens the specified application
change_pass	Prompts the user to change the password
reset_pass	Clears cached device password (in the bot's runtime)
start_client	Starts RAT client
grab_google_auth	Triggers stealing of google authenticator codes

Getting rid of the malware

In general, we recommend doing a factory reset when your device is infected with malware. This will put the device back to the state it was in when it was first turned on. For Anatsa and Cabassous it is also enough to uninstall the malware apps from the device (through the Android Settings menu), assuming you know which app is the malware (in this campaign the app name "UPS" is used).

Because both malware variants prevent removing the app through the Android Settings menu, you will have to boot the phone into safe mode (preventing the malware from running) to be able to uninstall the app. Another option, for tech-savvy users, is to use ADB (Android Debug Bridge) to connect to the device via USB and run the command `adb uninstall <malware_package_name>`.

Anatsa makes it even more difficult to remove it, because in addition to preventing the app to be uninstalled through the Android Settings, it also prevents rebooting or shutting down the device (required for safe mode). If you can't use ADB, the easiest option is to simply wait until the device turns off because it runs out of power (optionally in the meantime turning off Wi-Fi and data connections to stop the RAT from communicating with its C2) and then boot into safe mode and perform the actions described above.

Client Side Detection

ThreatFabric CSD can be used to detect customers infected with such threats in real-time, therefore avoiding fraud and keeping the risk under control.

Appendix

Cabassous

One of the latest Cabassous samples found in the wild:

App name	Package name	SHA-256 hash
UPS Mobile	kit.stem.iron	83ac4c915546ff9c7bda78cf9cbbc23c7f6f5b1d33967d2040ce8f0f22031a2b

The list of targeted applications contains 30 applications:

App name	Package name
Pibank	es.pibank.customers
Banca Móvil Laboral Kutxa	com.tecnocom.cajalaboral
EVO Banco móvil	es.evobanco.bancamovil
Ibercaja	es.ibercaja.ibercajaapp
BBVA Spain	com.bbva.bbvacontigo
PeoPay	softax.pekao.powerpay
Bankinter Móvil	com.bankinter.launcher
Cajasur	com.cajasur.android
Bank Millennium	wit.android.bcpBankingApp.millenniumPL
ruralvía	com.rsi
imaginBank - Your mobile bank	com.imaginbank.app
Binance - Buy & Sell Bitcoin Securely	com.binance.dev
Santander	es.bancosantander.apps
Blockchain Wallet. Bitcoin, Bitcoin Cash, Ethereum	piuk.blockchain.android
IKO	pl.pkobp.iko
Openbank – banca móvil	es.openbank.mobile
BNP Paribas GOMobile	com.finanteq.finance.bgz
Santander mobile	pl.bzwbk.bzwbk24
Bankia	es.cm.android
Gmail	com.google.android.gm
Banca Digital Liberbank	es.liberbank.cajasturapp
Moje ING mobile	pl.ing.mojeing
Grupo Cajamar	com.grupocajamar.wefferent
UnicajaMovil	es.univia.unicajamovil

App name	Package name
Idea Bank PL	pl.ideabank.mobilebanking
Coinbase – Buy & Sell Bitcoin. Crypto Wallet	com.coinbase.android
CA24 Mobile	com.finanteq.finance.ca
Alior Mobile	pl.aliorbank.aib
Kutxabank	com.kutxabank.android
ING España. Banca Móvil	www.ingdirect.nativeframe

Anatsa

One of the latest Anatsa samples found in the wild:

App name	Package name	SHA-256 hash
UPS	brave.crowd.home	c8dbba4ff6c71e7cdb6637f59694d96398b5da4aed50b5d650b0b532f1b07682

The list of targeted applications contains 39 applications:

App name	Package name
Deutsche Bank Mobile	com.db.pwcc.dbmobile
La Mia Banca	com.db.pbc.miabanca
Knab Bankieren	bvm.bvmapp
VR Banking Classic	de.fiducia.smartphone.android.banking.vr
ING Bankieren	com.ing.mobile
Ibercaja	es.ibercaja.ibercajaapp
ABN AMRO Mobiel Bankieren	com.abnamro.nl.mobile.payments
BBVA Spain	com.bbva.bbvacontigo
myAlpha Mobile	com.mobileloft.alpha.droid
Commerzbank Banking - The app at your side	de.commerzbanking.mobil
Rabo Bankieren	nl.rabomobiel
Cajasur	com.cajasur.android
Banco Sabadell App. Your mobile bank	net.inverline.bancosabadell.officelocator.android
Triodos Bankieren NL	com.triodos.bankingnl
ruralvía	com.rsi

App name	Package name
HVB Mobile Banking	eu.unicreditgroup.hvbapptan
Binance - Buy & Sell Bitcoin Securely	com.binance.dev
Santander	es.bancosantander.apps
SpardaSecureApp	de.sdvrz.ihb.mobile.secureapp.sparda.produktion
Blockchain Wallet. Bitcoin, Bitcoin Cash, Ethereum	piuk.blockchain.android
Postbank Finanzassistent	de.postbank.finanzassistent
Openbank – banca móvil	es.openbank.mobile
Bankia	es.cm.android
Banca Digital Liberbank	es.liberbank.cajasturapp
ING Banking to go	de.ingdiba.bankingapp
ASN Mobiel Bankieren	nl.asnbank.asnbankieren
UnicajaMovil	es.univia.unicajamovil
Grupo Cajamar	com.grupocajamar.wefferent
Santander Banking	de.santander.presentation
comdirect mobile App	de.comdirect.android
WiZink, tu banco senZillo	app.wizink.es
Coinbase – Buy & Sell Bitcoin. Crypto Wallet	com.coinbase.android
Sparkasse Ihre mobile Filiale	com.starfinanz.smob.android.sfinanzstatus
RegioBank - Mobiel Bankieren	nl.regiobank.regiobankieren
Kutxabank	com.kutxabank.android
CaixaBank	es.lacaixa.mobile.android.newwapicon
tractorpool	de.traktorpool
Vivid: Investments & Banking & Crypto	vivid.money
ING España. Banca Móvil	www.ingdirect.nativeframe