Threat Bulletin

Flubot Banker Trojan

24 May 2021

Introduction

Flubot has had a devastating impact on Android users in several European countries over the last few months. The latest Banker Trojan spreads via SMS messages that appeared to be from well-known shipping companies (FedEx, DHL, etc.) to trick users into clicking to download the malicious app onto their mobile device, ostensibly to track a package delivery. Once downloaded, Flubot completely takes over the phone, hiding itself from antivirus detection and removal, gathering and exfiltrating personal banking data, and propagating itself further by sending out the SMS to the phone's contacts. The cybercriminals behind the attack use stolen banking and browsing history data to identify which ecommerce sites or banking/payment apps the phone's owner habitually uses, so that the next time they try to login to their account the Flubot command & control server reroutes them to a targeted overlay that looks identical and steals login credentials.

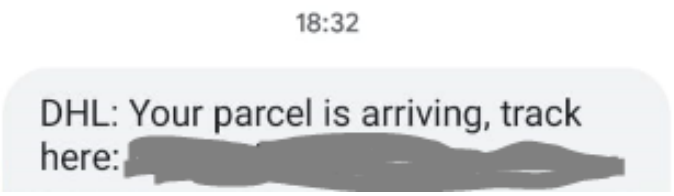
During March and April 2021 Allot Secure prevented Flubot Banker Trojan connecting to its command & control server 106,612,889 times.

Flubot Steals Money

Flubot is a Banker Trojan. A Trojan, named after the Trojan Horse of Greek mythology, is a type of malware that disguises itself as legitimate software, in this case delivery tracking software, to sneak its way onto your device and gain access to the system. A Banker Trojan steals money by intercepting sensitive personal information and credentials for accessing ecommerce or online banking/payment accounts.

Parcel Delivery SMS Tricks People into Downloading Flubot App

This Banker Trojan uses social engineering to spam mobile subscribers with a simple SMS message that appears to be from a large, well-known shipping service such as FedEx, DHL, Amazon, Correos (Spain), etc. The familiar-looking message states a package is on its way and instructs you to download the branded company app to track the delivery. This is such a common activity, especially since the Covid-19 crisis has boomed the delivery industry. Once the user clicks on the innocent looking link, the malicious app is installed. Everything about the download and installation process precisely mimic the real company's real app. Flubot can then access the phone's contacts to send SMS messages to more victims. Flubot targets Android uses with a malicious android app, but this time even iOS users are not spared. If an iPhone user receives the SMS and clicks on the link, the device is recognized as iOS and redirected to a regular web-based phishing page. Flubot can also be spread to PCs via an email message with a download or phishing link.



URLs Recently Used by Flubot Banker Trojan

The recent campaign used dozens of different URLs, with localized content for each target market hit. Some URLs are purely malicious, others are of real legitimate organizations that have been hacked and used to host the Banker Trojan without the permission or knowledge of the website owner.

```
ailnoir.com/app/
amzstudy.com/pack/
blog.sidmach.com/app/
buguilou.com/p/ computin
chevychasefarmersmarket.
clone.app.home-cost.com/
colegioaugustoribeiro.co
contornosdesign.pt/pkg/
dclifechanging.com/fedex
dgeneration.in/pack/
diamondcup.gr/fedex/
dibae.blog/fedex/
dilalla.com.ar/web/
ekremakin.org/pack/
elonatheexplorer.com/fed
erbiltursu.com/app/
fallenjewellery.com/fede
illuminate.org/info/
kidimy.org/pkg/ malware-
lacasa-dh.nl/pack/
lavozislamica.com/www/
magicboximportados.com.b
mir2018.mrororr.ru/fedex
mmcamping.com/app/
nbkangxi.com/pack/
njzmfcls.com/fedex/
nuevocalor.com/fedex/
offx.link/info/ malware-
ouyangpengcheng.xyz/p/
raeloficial.com/pkg/
rishipes.co.nz/pack/
ryansa.com/pkg/ phishing
smcsme.com/fedex/
spave.com.pk/p/ malware-
tacloban.gov.ph/info/
testtaglabel.com/web/
```

Evading Antivirus Detection

Once installed, Flubot makes itself undetectable by modifying the registry. It also blocks access the Google Play Store so that the user is unable to download new antivirus applications. This means that not only is it almost impossible to protect yourself from infection, even once you realize your device is infected, it is very difficult to remove. Advanced users can follow the removal instructions in this video (https://youtu.be/dIIDh1AqUKQ). Most users will need to do a factory reset, which wipes clean all the apps and information on the phone. Android Factory Reset instructions: https://support.google.com/android/answer/6088915?hl=en

Reconnaissance, Data Exfiltration, and Banking Overlay

Like the name suggests, once inside a Banker Trojan quickly begins gathering reconnaissance for its ultimate mission – stealing money. When the malware is installed in the terminal, it uses the banking/payment app's internal name to detect the moment it is opened. Next it sends this information to the C&C server, which then sends the matching overlay that identically mimics that apps login page to intercept account login details. Once this stage is complete, the criminals can begin emptying funds from the account or making malicious purchases.

Flubot Internal App Identifiers

```
hostname:vloxaloyfmdqxti[.]ru
payload:GET_INJECTS_LIST,alior.banking[...]zebpay.Application
Response:com.bankinter.launcher,com.bbva.bbvacontigo,com.binance.dev
,com.cajasur.android,com.coinbase.android,com.grupocajamar.wefferent
,com.imaginbank.app,com.kutxabank.android,com.rsi,com.tecnocom.cajal
aboral,es.bancosantander.apps,es.cm.android,es.evobanco.bancamovil,e
s.ibercaja.ibercajaapp,es.liberbank.cajasturapp,es.openbank.mobile,e
s.pibank.customers,es.univia.unicajamovil,piuk.blockchain.android,ww
w.ingdirect.nativeframe
```

Allot Secure Flubot Connection Blocks

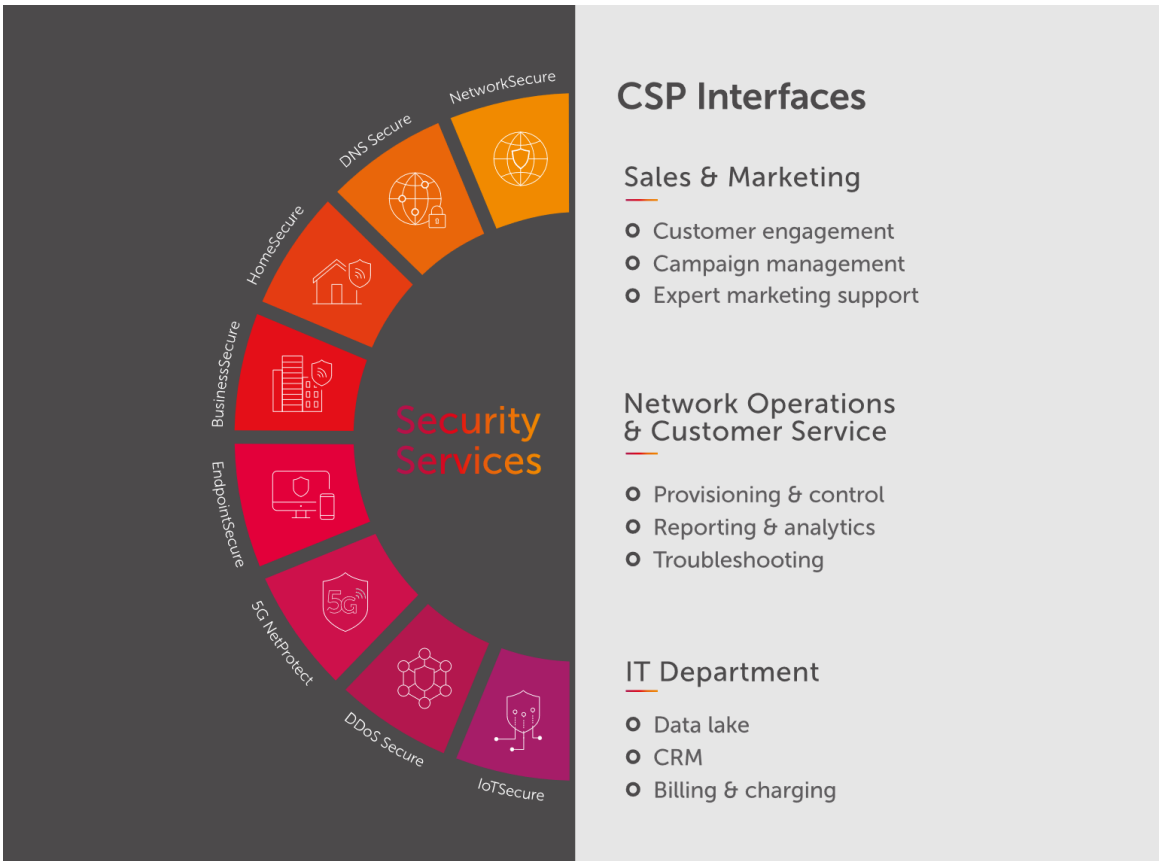
During March and April 2021 Allot Secure protected users from Flubot Trojan Banker connecting to its command & control server 106,612,889 times.

Conclusion

Protect Subscribers with Allot Secure

Allot Secure allows CSPs to protect their subscribers from all types of cyberthreats by offering security as a service (SECaaS) from the network. Up-to-date threat intelligence and in-line anti-virus scanning protects users from connecting to C&C servers, malicious browser trackers, and all types of malware, banking Trojans, crypto jacking, ransomware, and IoT specific attacks such as Mirai and its variants.

Allot Secure unifies network-based security, home and business gateway security and security clients into the CSP's own branded security service. It delivers a seamless customer experience through a single interface for policy setting, reporting, and event handling.



To learn more about how service providers can increase customer satisfaction, NPS and ARPU by offering Allot Network Security Solutions, download the Telco Security Trends Report:

How Effective are CSP Security Services for the Mass Market?
or watch this video: **How Allot NetworkSecure Works**.