

# Flubot: Android-Malware verbreitet sich über Fake-Patches

Moritz Rupp

Hochschule Albstadt-Sigmaringen

WS 21/22

Android-Malware Flubot ist zurück

## Flubot: Android-Malware verbreitet sich über Fake-Patches



Flubot: Der Banking-Trojaner ist mit einer neuen Masche zurück – Vorsicht ist geboten!

1

# Inhalt

- 1 Trivia
- 2 Funktionsweise
- 3 Verbreitung
  - Phishing
- 4 Technische Analyse
- 5 Conclusion
- 6 Quellen

# Terminologie

## Malware

Software zu ausführung unerwünschter bzw. schädlicher Funktionen.

## Banking Trojaner

Vermeintlich harmlose Anwendung dringt in System ein und greift Daten ab. ⇒ Banking Login Daten.

## Phishing

Vortäuschung von Diensten zu erlangung von Login Informationen.

## Botnetze

Große Anzahl an Geräten(Bots) die über Netzwerke automatisiert Malware betreiben.

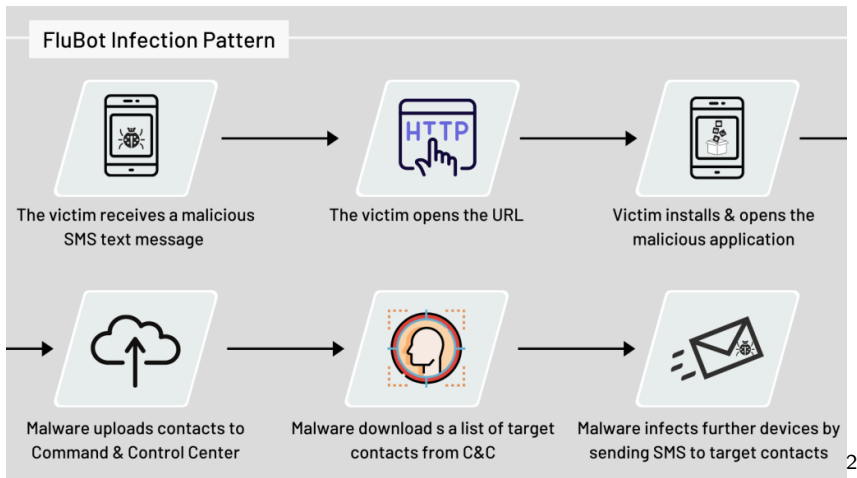
# Was ist Flubot?

- Android Malware
- Banking Trojaner
- Verbreitung über SMS Nachrichten
- Nutzung von Botnetzten und Phishing Methoden
- Nach wie vor im Umlauf

- Erstes Auftreten Ende 2020 in Spanien
  - Frühjahr 2021 in Deutschland
- Weltweite Verbreitung im Laufe des Jahres 2021
- ~13 Millionen infizierte Geräte
- Finanzieller Schaden schwer feststellbar ~ 8-stelligem Bereich!

- Opfer erhält eine SMS mitsamt Link.
- Der Link führt zu einer Webseite auf der ein APK Download bereit steht.
- Durch Download der APK wird das betroffene Gerät infiziert.
- Die Malware durchsucht nun die Kontaktliste und schickt über diese weitere Phishing Nachrichten!
- Nun werden über ausgewählte Apps Phishing Overlays gelegt  
⇒ Jegliche Eingaben werden nun an Angreifer weitergeleitet

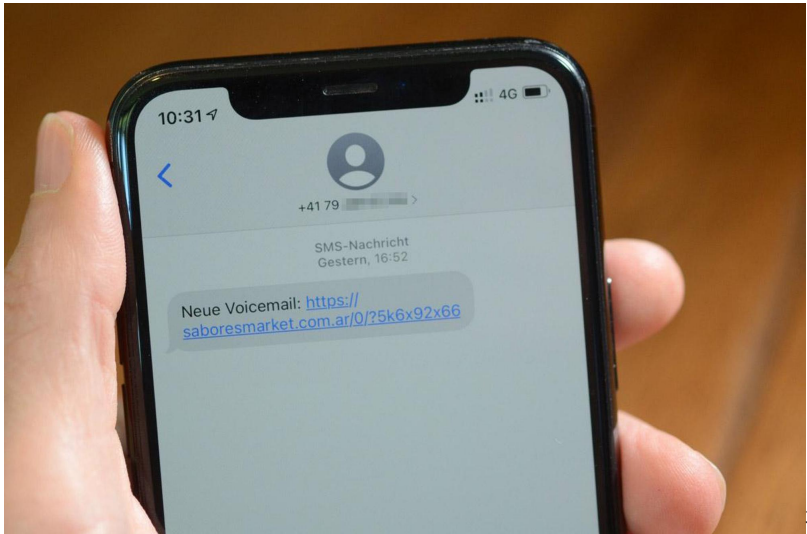
# Verbreitung

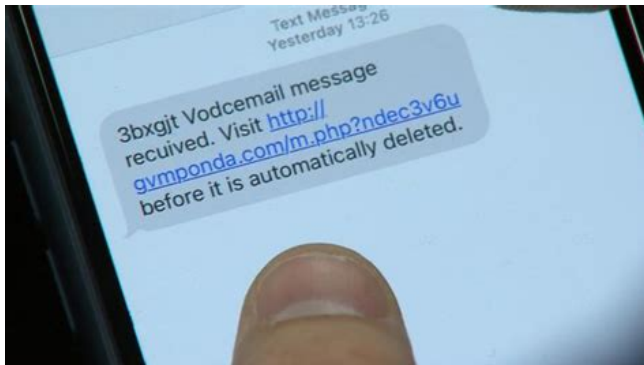




# Phishing Methoden

- Anfangs wird eine vermeintliche Voicemail als Köder verwendet
- Seit Frühjahr 2021 vermehrt Packerlieferdienste
- Ab mitte 2021 'Fake security patches' gegen Flubot selbst
- Anfang 2022 nun Adobe Apps
- Flubot variiert und wechselt häufig Phishing Köder!





4

Hallo [REDACTED],  
Ihr Paket steht noch aus.  
Bestatigen Sie Ihre Angaben hier:  
[http://  
www.\[REDACTED\].de/  
id/?\[REDACTED\]](http://www.[REDACTED].de/id/?[REDACTED])  
Deutsche Post

Hallo [REDACTED],  
Der Kurier nahm das Paket  
ab.  
Track:  
[http://\[REDACTED\].com/  
trck/?\[REDACTED\]](http://[REDACTED].com/trck/?[REDACTED])

Das Paket mit ID #2 [REDACTED] ist  
unterwegs.  
Wir benötigen Ihre Informationen  
[https://  
www.\[REDACTED\].com/t/?\[REDACTED\]](https://www.[REDACTED].com/t/?[REDACTED])

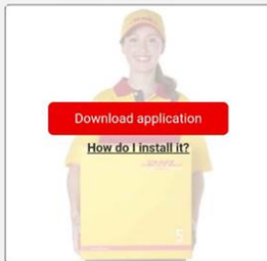
Bestellung 24 [REDACTED] versandt.  
Lieferung: 3-5 Werktag/e.  
Paketverfolgung  
[https://\[REDACTED\]/track/  
?\[REDACTED\]](https://[REDACTED]/track/[REDACTED]?[REDACTED])

Ihr paket wird heute zum Absender  
zuruckgesendet. Letzte Moglichkeit es  
abzuholen  
[http://\[REDACTED\].com.ua/track/  
?\[REDACTED\]](http://[REDACTED].com.ua/track/[REDACTED]?[REDACTED])

5



Download our application to track your parcel



6

# Post-Infection

- Verbindungsaufbau zum Command and Control Server

## Command and Control Server

Hauptzentrale des Botnetzes! Hier wird die Malware gesteuert!

- Gerät schickt alle Kontakte und installierten Apps an den C&C Server!
- Dieser antwortet mit einer neuen Liste neuer Kontakte  
⇒ Über diese werden weitere Phishing SMS versendet!
- Zudem wird eine Liste der gezielten Anwendungen geschickt
- Über diese Anwendungen wird nun das eigentliche Phishing Overlay gelegt!

**ING**

**Acceso para Ti**

Número de documento  
DNI o Tarjeta de residencia

Fecha de nacimiento Identifícame con Pasaporte

DD MM AAAA

Clave de seguridad

Entrar

**ruralvía**

**Acceso Banca Internet**

Usuario

NIF / NIE

Contraseña

Cancelar Iniciar sesión

**GRUPO COOPERATIVO CAJAMAR**

USUARIO

Contraseña

**imagin** banca

**Welcome**

User

Password

Log in

Unirse to enter?

**Acceso clientes**

Usuario

Contraseña

Recordar usuario

ENTRAR

**Buenos Días**

NIF

Número de documento

Clave de acceso

Recordar usuario en este dispositivo

ENTRAR

**Openbank** Open

**TIPO DE DOCUMENTO Y NUMERO**

NIF Ingresa número de documento

**CLAVE DE ACCESO**

Acceder

**Liberbank**

ID USUARIO

CONTRASEÑA

¿Has olvidado tu clave?

Entrar

**Acceso para Ti**

Número de documento  
DNI o Tarjeta de residencia

Fecha de nacimiento Identifícame con Pasaporte

DD MM AAAA

Clave de seguridad

Entrar

**Acceso para Ti**

Número de documento  
DNI o Tarjeta de residencia

Fecha de nacimiento Identifícame con Pasaporte

DD MM AAAA

Clave de seguridad

Entrar

Nº Documento

Clave de acceso

Correo electrónico

Entrar

Olvidé mi clave

Solicitar claves

**BINANCE**

Email

Password

Login

Forgot your password?

Don't have an account yet? Register

**k** bank

NIF/Usuario

Clave

Fecha de nacimiento

DD MM AAAA

Recordar usuario implica que este dispositivo recibirá notificaciones dirigidas al usuario vinculado. Puedes configurarlo desde "Ajustes".

Entrar

¿Has olvidado tu clave?

**pibank**

Hazte cliente

NIF/NIE

7

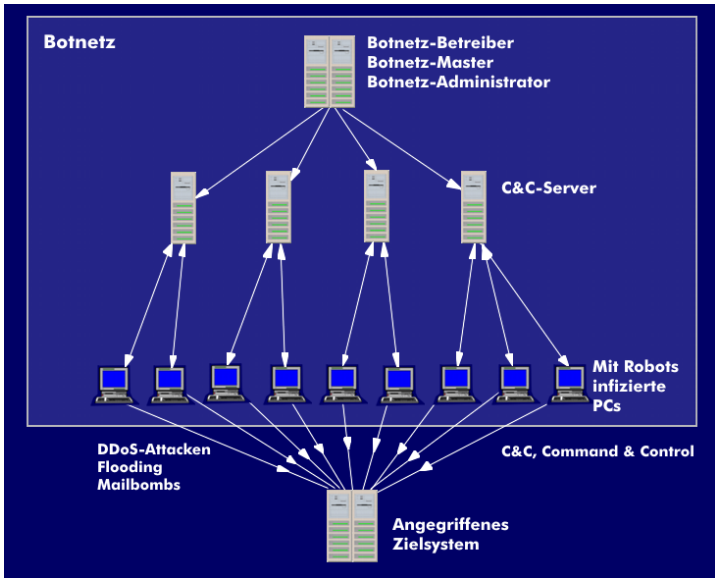
# Technische Analyse

- Die Malware APK ist komplett in Java geschrieben
- Läuft ab Android Version 4.1.2
- Wird stetig weiterentwickelt
- Verwendung von String Obfuscation um Reverse Engineering zu erschweren!
- Über 30 Kommandos für Kommunikation zwischen Gerät und C&C möglich!



# Command and control Server

- Hauptzentrale der Malware Infrastruktur
- Bietet Angreifern Administration
- Server - Client model
- Über 20 Kommandos zwischen Gerät und C&C möglich
- Zugreifbar über Weboberfläche
- Liegt in einem verteilten System



8

#Kommandos von dem C&C Server an das Gerät  
GET\_CONTACTS - Schicke Kontakte an den Server.  
RETRY\_INJECT - Versuche erneut die Anwendung zu infizieren  
BLOCK - Jegliche Kommunikation blocken  
UNINSTALL\_APP - Deinstalltion der Malware  
SEND\_SMS - Versenden von SMS  
DISABLE\_PLAY\_PROTECT - Den Virenschutz des Google Play stores  
deaktivieren<sup>9</sup>

---

<sup>9</sup><https://raw.githubusercontent.com/prodaft/malware-ioc/master/FluBot/FluBot.pdf>

- Flubot verwendet gekappte Webseiten als Hosts für C&C
- Mehrere hundert betroffene Instanzen
  - meist Wordpress Blogs
  - stetig wachsend
- Keine feste Domain oder IP
- Stattdessen Domaingenerierung anhand des Domain-Generation-Algorithmus
  - Auflösung über DNS über HTTPS
  - Nutzt Services wie dns.google

# Domain Generation Algorithmus

## Algorithmus zu Domain Generierung

- Kombiniert randomisiert Top-Level-Domain mit Second-Level-Domain
- Liste 1 enthält Top-Level-Domains

*.de, .com, .net, .org, .io*

- Liste 2 enthält Second-Level-Domains

*test, hallowelt, Albstat, Lirum, Ipsum*

- Aus diesen Listen werden nun vollständige Domains aufzulösen

- Für die Domainauflösung werden Dienste von google oder cloudflare genutzt  
⇒ dns.google, cloudflare.dns
- Teilweise werden bis zu 10 DNS Requests benötigt

34974	https://dns.google	GET	/resolve?name=ewnwoysvaefmdpm.su&type=A	✓
34973	https://cloudflare-dns.com	GET	/dns-query?name=hoacuennuwscmsk.su&type=A	✓
34972	https://cloudflare-dns.com	GET	/dns-query?name=ycligamdesovkuj.su&type=A	✓
34971	https://dns.alidns.com	GET	/resolve?name=bqocuxxqwchdrkp.cn&type=A	✓
34970	https://dns.alidns.com	GET	/resolve?name=pccytxvsyvlfky.cn&type=A	✓
34969	https://dns.alidns.com	GET	/resolve?name=cytcfvjgyciuxiu.su&type=A	✓
34968	https://dns.google	GET	/resolve?name=iwqeudyiwqdxotc.su&type=A	✓
34967	https://dns.google	GET	/resolve?name=kauvuvrfoybvgci.ru&type=A	✓

# Lösungsansätze

- Entfernung der Malware durch Rücksetzung zum Werkszustand möglich
- Verlust der Persönlichen Daten zur Folge
- Open-Source tools wie paranoid bieten ALternative
- Gegen Phishing Angriffe kaum technische Lösungen vorhanden
- Zwei-Faktor-Authentifizierung bietet gewissen Schutz
- Bildung bietet größte Chance
  - ⇒ Informatik in Schulen kaum Schwerpunkt
- Umgang mit digitalen Medien sollte Flächendeckend gelehrt werden



# Conclusion

- Phishing nach wie vor eine der größten Bedrohungslagen
- Meist in Verbindung mit weiterer Malware eingesetzt
- Android häufigstes Zielsystem
- 'Internet of things' vergrößert Angriffsziele
- Technologien wie nfts, smartcontracts könnten abhilfe schaffen
- Nachhaltiger Schutz bzw. Bekämpfung nur durch bessere Aufklärung und Bildung möglich

# Quellen

computerbild | 07.11.2021, <https://www.computerbild.de/artikel/cb-News-Sicherheit-Flubot-Gefaehrliche-Android-Malware-verbreitet-sich-ueber-Fake-Patches-30863335.html>

threatmark | 07.01.2022,  
<https://www.threatmark.com/flubot-banking-malware>

threadmonit | 06.01.2022,  
<https://www.threadmonit.io/flubot-android-malware-technical-analysis>  
heise | 02.01.2022, <https://www.heise.de/news/Smishing-BSI-warnt-vor-neuen-Betrugsmaschen-bei-SMS-Phishing-6220072.html>

bsi | 03.01.2022,  
<https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Botnetze/Steckbriefe-aktueller-Botnetze/Steckbriefe/Flubot.html>

<https://de.statista.com/statistik/daten/studie/1235321>

<https://de.statista.com/themen/1355/android/>

<https://www.telekom.com/en/blog/group/article/flubot-under-the-microscope-636368>

<https://www.telekom.com/en/blog/group/article/flubot-under-the-microscope-636368>

<https://www.computerbild.de/artikel/cb-News-Sicherheit-Flubot-Gefaehrliche-Android-Malware-verbreitet-sich-ueber-Fake-Patches-30863335.html>

<https://computerwelt.at/news/android-malware-flubot-stuermt-top-ten>

<https://www.telekom.com/en/blog/group/article/flubot-under-the-microscope-636368>