Flubot: Android-Malware verbreitet sich über Fake-Patches !WIP!

Moritz Rupp

Hochschule Albstadt-Sigmaringen

tobedated - WS 21/22

Inhalt

Leitartikel

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!

Trivia

- Banking Trojaner - Phishing Malware
- Erstes Auftreten Ende 2020 in Spanien - Frühjar 2021 in Deutschland
- 80 tausend Infizierte Geräte
- im Umlauf
- Schaden in höhe von 10 Mio €

Was ist Flubot?

- Verbreitung über SMS
- kurzer Text mit Link
- vermeintlicher Dienst wie Voicemail etc.
- Nur durch herunterladen der apk nutzbar

Banking Trojaner

Vermeintlich harmlose Anwendung dringt in System ein und greift Daten ab.
- In diesem Fall Banking Apps

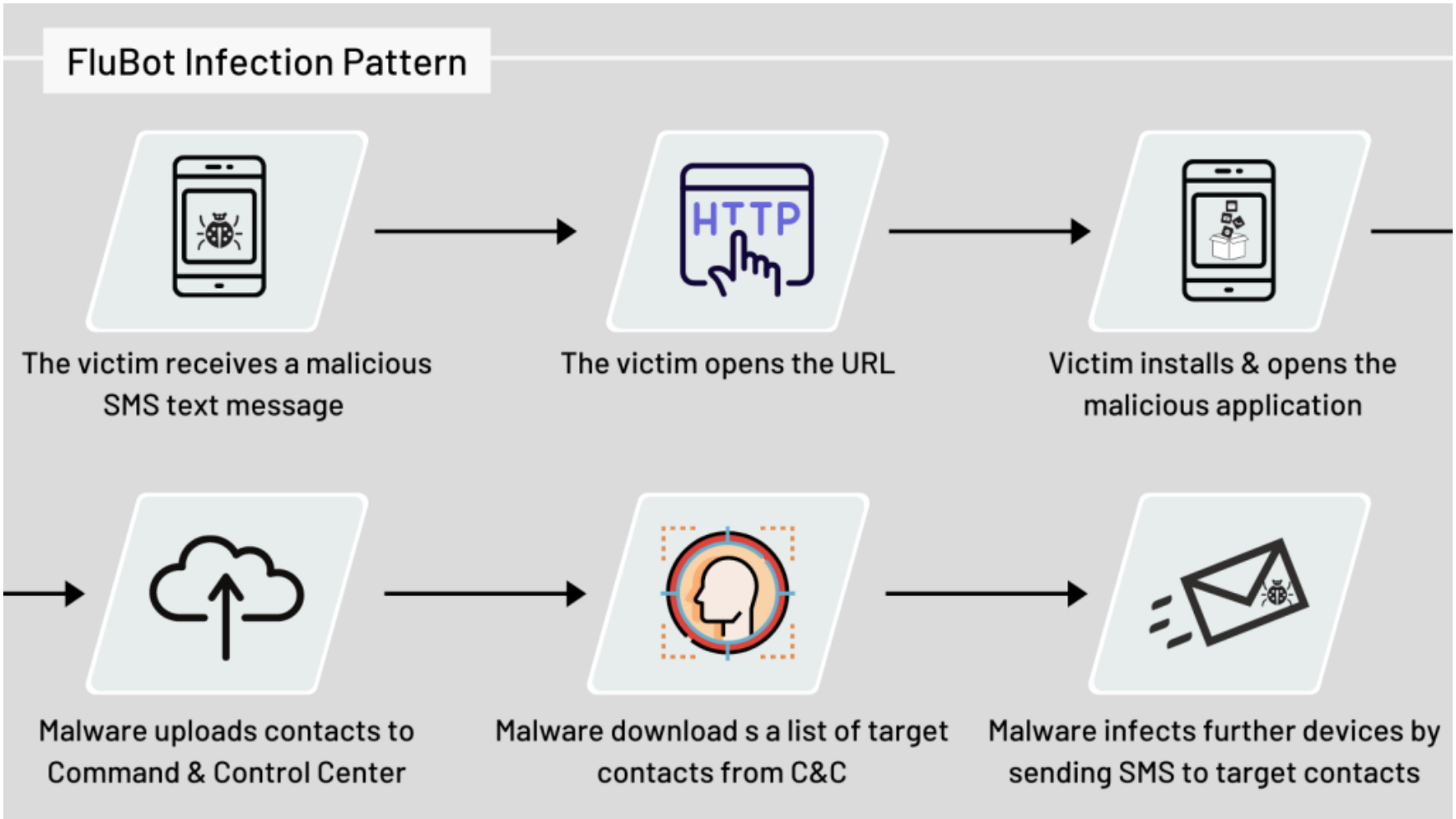
Botnetze

Große Anzahl an Infizierten Geräten die automatisiert Malware betreiben und sich verbreiten

Funktionsweiße

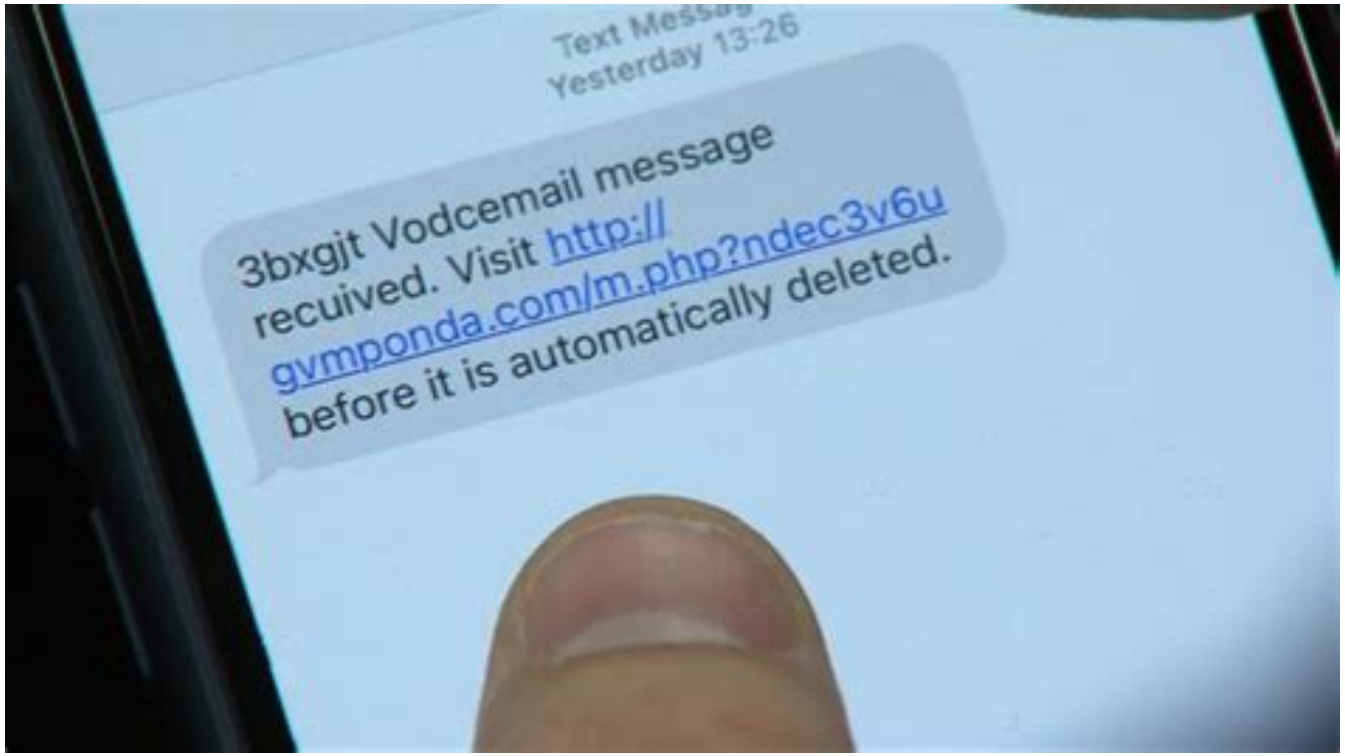
-Opfer erhählt eine SMS mitsamt Link!
-Der Link führt zu einer Webseite auf der ein APK Download zu verfügung gestellt wird.
- Durch Download der APK wird das betroffene Gerät infiziert!
- Die Malware durchsucht nun die Kontaktliste und schickt über diese weitere Phishing Nachrichten!
- Des weiteren werden über Banking Apps Phishing Overlays gelegt!
$\Rightarrow$ Jegliche Eingaben werden nun seitens der Angreifer mitgelesen!

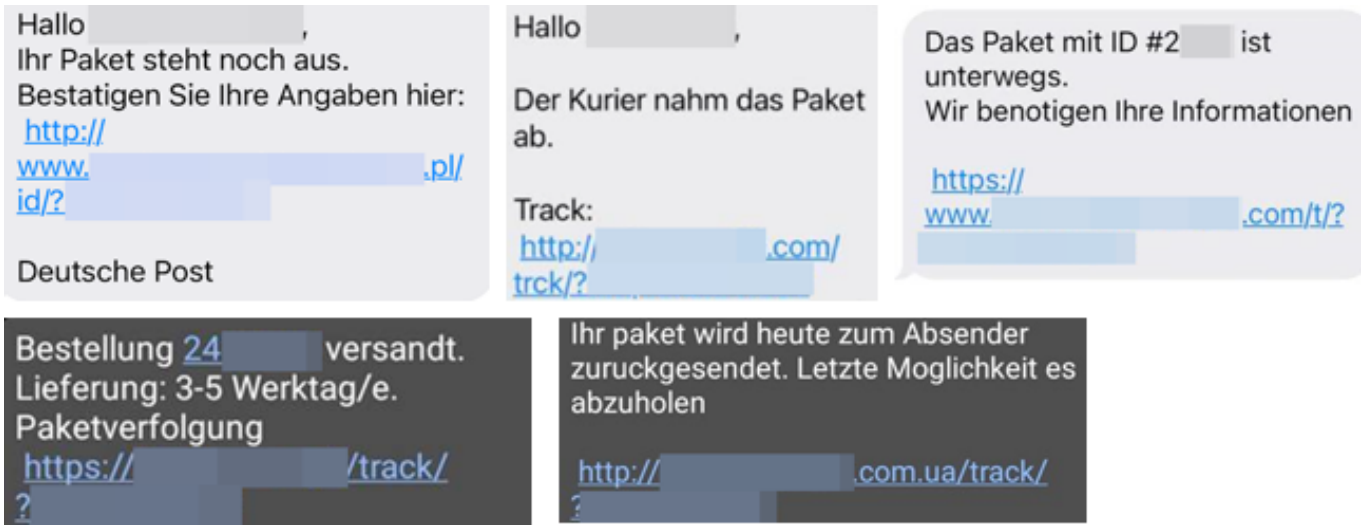
Verbreitung

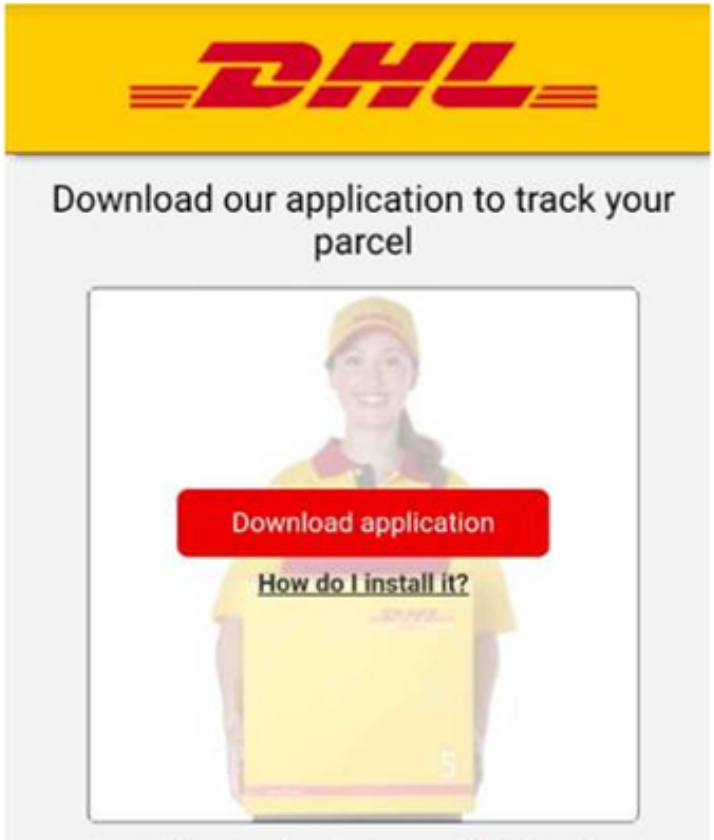


Phishing

- Anfangs wird eine vermeintliche Voicemail als Köder verwendet!
- Seit Anfang 2021 Packetlieferdienste!
- Seit mitte 2021 Fake security update gegen Flubot selbst!


Yesterday 13:26
3bxgjt Vodcemail message
recuived. Visit http://
gvmponda.com/m.php?ndec3v6u
before it is automatically deleted.


Hallo ,
Ihr Paket steht noch aus.
Bestatigen Sie Ihre Angaben hier:
http://
www. .pl/
id/?
Deutsche Post
Hallo ,
Der Kurier nahm das Paket ab.
Track:
http:/ .com/
trck/?
Das Paket mit ID #2 ist unterwegs.
Wir benotigen Ihre Informationen
https://
www. .com/t/?
Bestellung 24 versandt.
Lieferung: 3-5 Werktag/e.
Paketverfolgung
https:// /track/
?
Ihr paket wird heute zum Absender zuruckgesendet. Letzte Moglichkeit es abzuholen
http:// .com.ua/track/


DHL
Download our application to track your parcel
Download application
How do I install it?

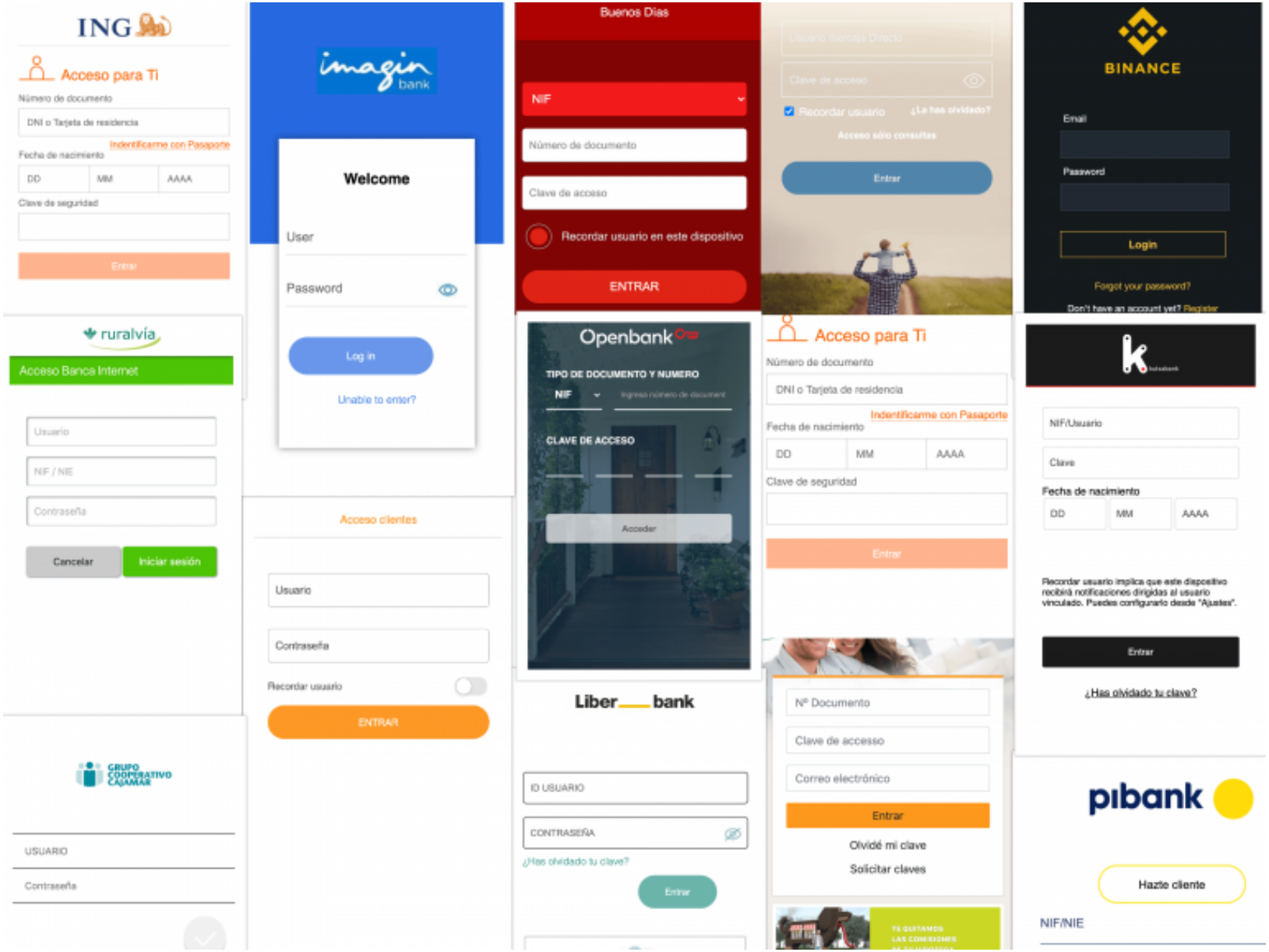
Post-Infection

- Verbindungsaufbau zum Command and Control Server!

Command and Control Server

Hauptzentrale des Botntzes! Hier wird die Malware gesteuert!

- Infiziertes Gerät schickt alle Kontakte und installierten Apps an den C&C Server!
- Dieser Antwortet mit einer neuen Liste Kontakte!
- Über diese wird die Malware nun weiter verbreitet!
- Auch wird eine Liste der gezielten Anwendungen geschickt!


ING
Acceso para Ti
Número de documento
DNI o Tarjeta de residencia
Identifícarme con Pasaporte
Fecha de nacimiento
DD
MM
AAAA
Clave de seguridad
Entrar
imagin bank
Welcome
User
Password
Log in
Unable to enter?
Buenos Días
NIF
Número de documento
Clave de acceso
Recordar usuario en este dispositivo
ENTRAR
Recordar usuario
¿La has olvidado?
Acceso sólo consultas
Entrar
BINANCE
Email
Password
Login
Forgot your password?
Don't have an account yet? Register
ruralvía
Acceso Banca Internet
Usuario
NIF / NIE
Contraseña
Cancelar
Iniciar sesión
Acceso clientes
Usuario
Contraseña
Recordar usuario
ENTRAR
Openbank
TIPO DE DOCUMENTO Y NUMERO
NIF
CLAVE DE ACCESO
Acceder
Acceso para Ti
Número de documento
DNI o Tarjeta de residencia
Identifícarme con Pasaporte
Fecha de nacimiento
DD
MM
AAAA
Clave de seguridad
Entrar
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?
GRUPO COOPERATIVO CAJAMAR
USUARIO
Contraseña
Liberbank
ID USUARIO
CONTRASEÑA
¿Has olvidado tu clave?
Entrar
Nº Documento
Clave de acceso
Correo electrónico
Entrar
Olvidé mi clave
Solicitar claves
pibank
Hazte cliente
NIF/NIE

Technische Analyse

- Die Apk ist komplett in Java geschrieben
- Läuft ab Android Version 4.1.2
- Verwendet String Obfuscation um Reverse Engineering zu erschweren!
- Über 30 Kommandos kann der C&C Server mit dem Gerät Kommunizieren!

#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[1]

[1] https://raw.githubusercontent.com/prodaft/malware-ioc/master/FluBot/FluBot.pdf

Netzwerkstrukur

- Flubot verwendet gekapperte Webeiten als Hosts.
- Über 200 betroffene Blogs!
- Keine Feste Domain oder IP!
- Domaingenerierung anhand des DGA
- Auflösung über DNS über HTTPS
- Nutzt Services wie dns.google

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=yciigamdesovkuj.su&type=A	✓
34971	https://dns.alidns.com	GET	/resolve?name=bqocuxxqwchdrkp.cn&type=A	✓
34970	https://dns.alidns.com	GET	/resolve?name=pccytxvsyvlifky.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	✓

Conclusion

- Pishing nach wie vor größte Bedrohungslage
- Keine technische Lösung!
- Geringer schutz durch 2FA möglich!
- Nachhaltiger Schutz bzw. Bekämpfung nur durch bessere Aufklärung und Bildung möglich!

Quellen

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