Flubot:
Android-Malware verbreitet sich über Fake-Patches

Moritz Rupp

Hochschule Albstadt-Sigmaringen

WS 21/22

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!

1

[1] computerbild.de

Inhalt

Terminologie

Malware

Software zu ausführung unerwünschter bzw. schädlicher Funktionen.

Banking Trojaner

Vermeintlich harmlose Anwendung dringt in System ein und greift Daten ab. $\Rightarrow$ 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

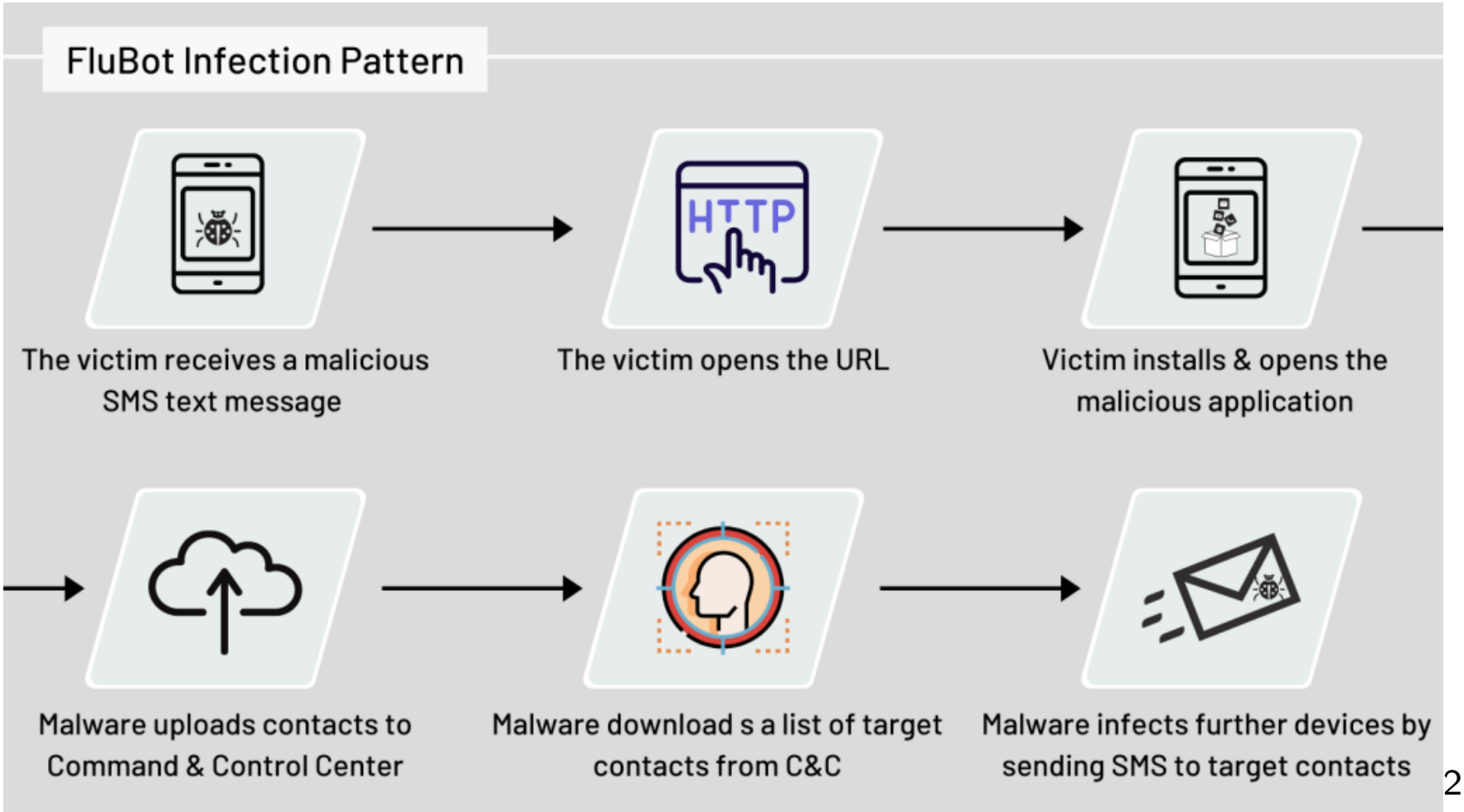
Trivia

- Erstes Auftreten Ende 2020 in Spanien
  - Frühjar 2021 in Deutschland
- Weltweite Verbreitung im laufe des Jahres 2021
- ~13 Millionen Infizierte Geräte
- Finanzieller Schaden schwer festellbar ~ 8 stelligem Bereich!

Funktionsweiße

- 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
  $\Rightarrow$ Jegliche Eingaben werden nun an Angreifer weitergeleitet

Verbreitung

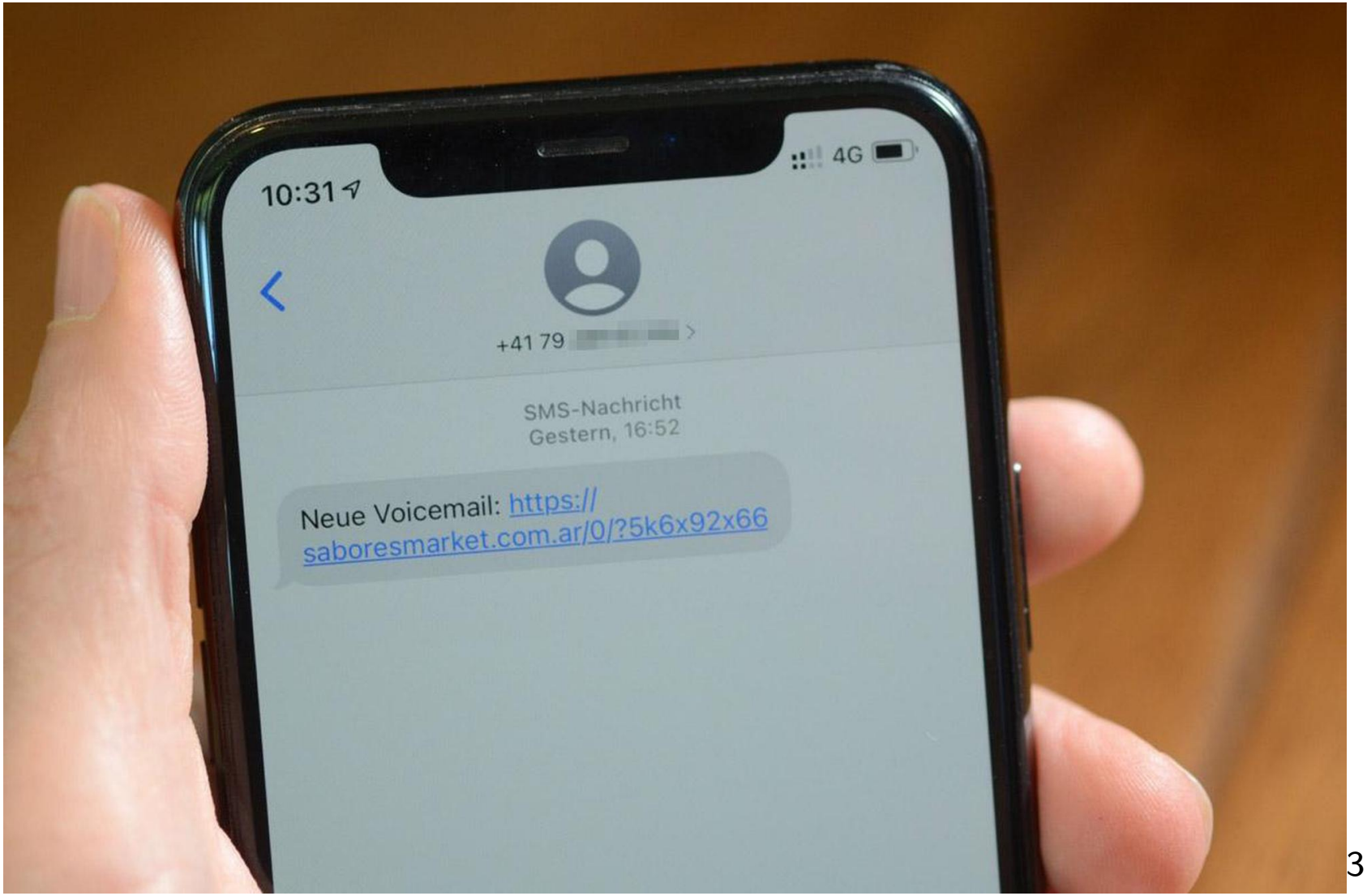


[2]

[2] threatmark.com

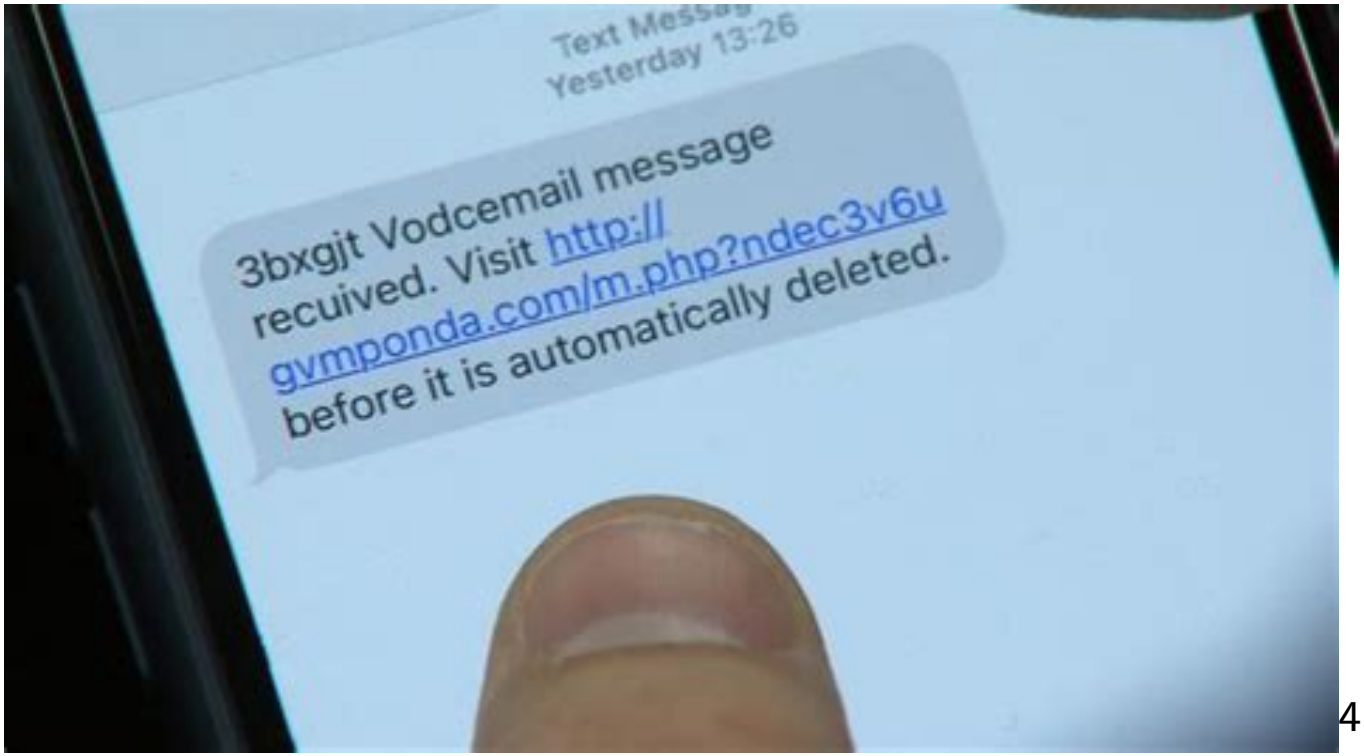
Phishing Methoden

- 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 variert und wechselt häufig Phishing Köder!

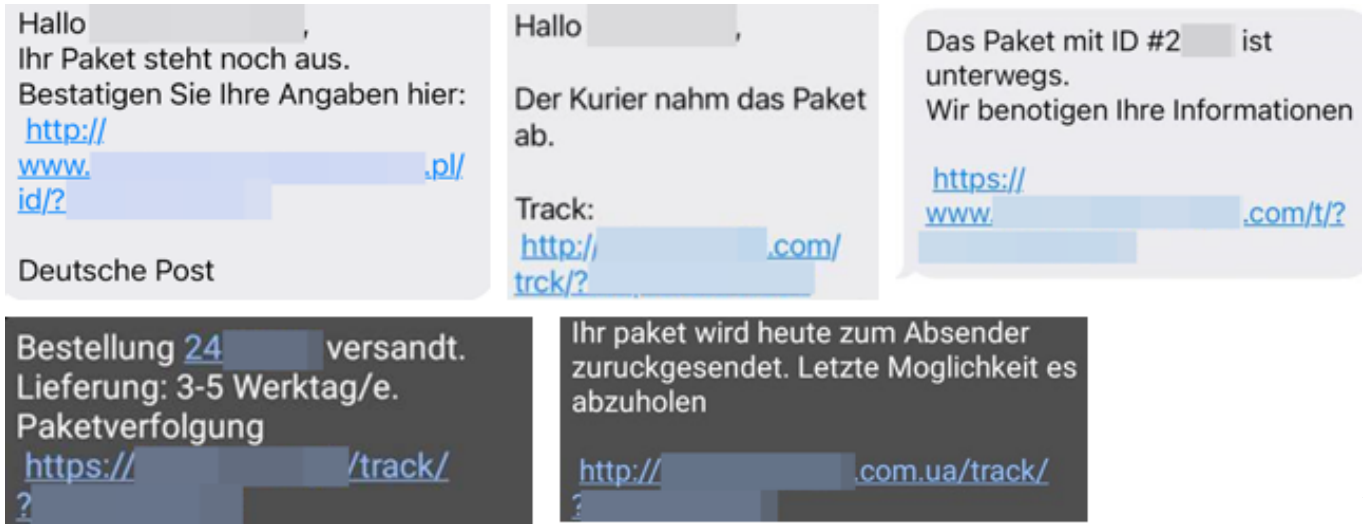


[3]

[3] threatmark.io

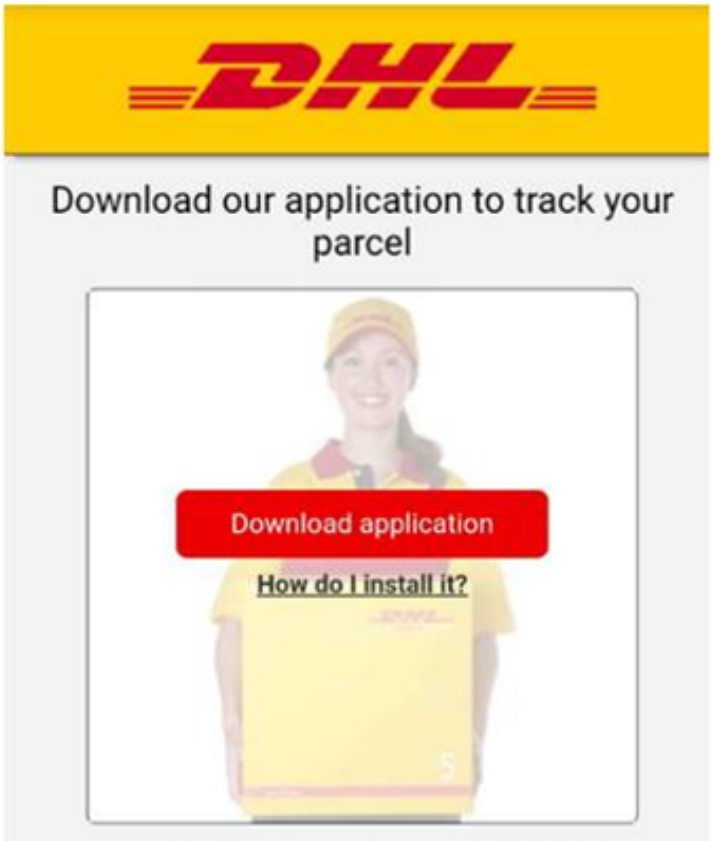

Yesterday 13:26
3bxgjt Vodcemail message
recuived. Visit http://
gvmponda.com/m.php?ndec3v6u
before it is automatically deleted.
[4]

[4] bsi.de



5

[5] computerbild.de



[6]

[6] threatmonit.io

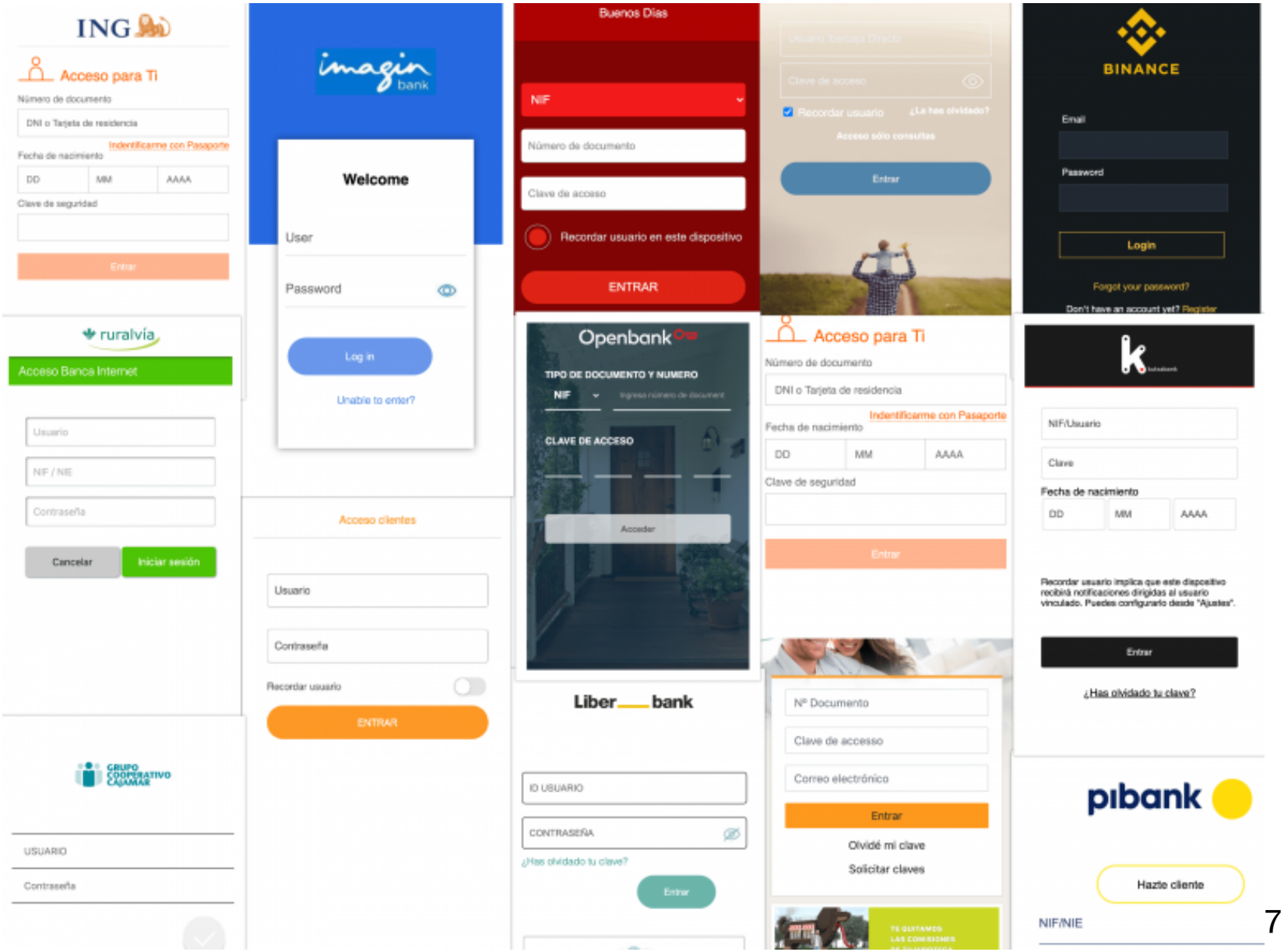
Post-Infection

- 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
  $\Rightarrow$ Über diese werden weitere Phishing SMS versendet!
- Zudem wird eine Liste der geziehlten Anwendungen geschickt
- Über diese Anwendungen wird nun das eigentliche Phishing Overlay gelegt!



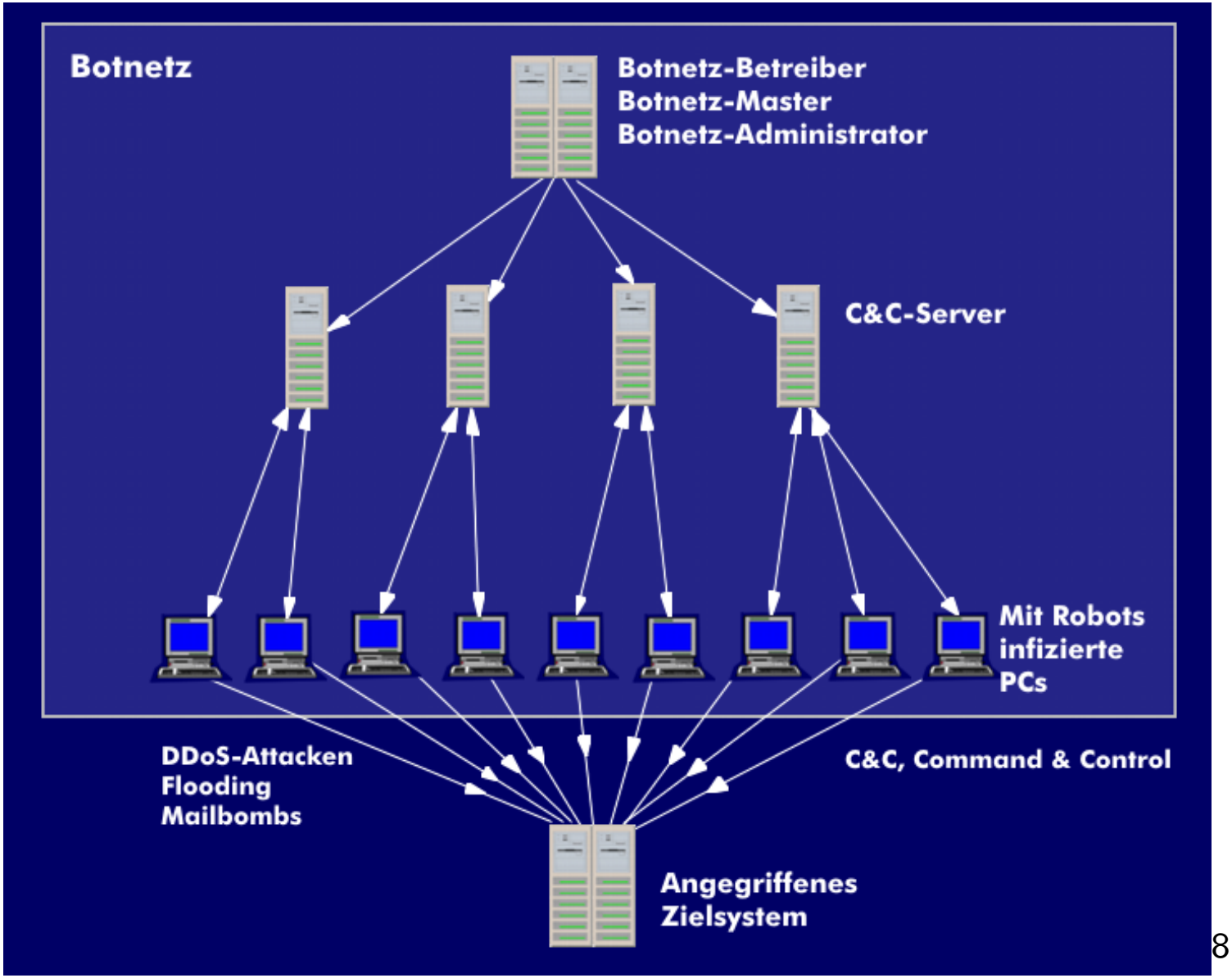
[7] threatmark.io

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


Botnetz
Botnetz-Betreiber
Botnetz-Master
Botnetz-Administrator
C&C-Server
Mit Robots
infizierte
PCs
DDoS-Attacken
Flooding
Mailbombs
C&C, Command & Control
Angegriffenes
Zielsystem
[8]

[8] heise.de

#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[9]

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

Netzwerkstrukur

- Flubot verwendet gekapperte Webeiten 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 versucht vollständige Domains aufzulösen

- Für die Domainauflösung werden Dienste von google oder cloudflare genutzt
  $\Rightarrow$ 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=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	✓

[10] threatmark.io

Lösungsansätze

- Enfernung 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
  $\Rightarrow$ Informatik in Schulen kaum Schwerpunkt
- Umgang mit digitalen Medien sollte Flächendeckend gelehrt werden

Conclusion und Ausblick

- 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.threatmonit.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