

Flubot: Android-Malware verbreitet sich über Fake-Patches

Cybersecurity

Moritz Rupp

Wintersemester 2021/22

Inhaltsverzeichnis

1	Abstract	3
2	Einführung	4
3	Funktionsweise	5
3.1	Infektion und Verarbeitung	5
3.2	Post Infection	6
4	Technische Analyse	7
4.1	Netzwerkstruktur	7
4.2	Payload	8
5	Lösungsansätze	11
6	Conclusion	11
7	Eigentständigkeitserklärung	12
8	Quellen	13

1 Abstract

Die tägliche Nutzung von Smartphones ist seit nunmehr über 10 Jahren in der breiten Gesellschaft angekommen. Egal ob Kurznachrichtendienste, Soziale Medien, Online Banking oder shopping. In allen Bereichen des sozialen und geschäftlichen Lebens findet das Smartphone Anwendung. Auch neuere Erscheinungen wie der Online-Handel mit Kryptowährungen findet größtenteils über mobile Endgeräte statt.

Derzeit sind laut statista¹ über 4 Milliarden mobile Geräte im Umlauf. Davon nutzen über 70 Prozent² das Betriebssystem Android. Diese enorme Anzahl an ähnlichen Geräten auf denen sensitive Daten laufen bietet eine große Menge an Angriffsmöglichkeiten für Cyberkriminelle! Hierbei gilt Phishing seit Jahren als eine der größten Bedrohungen. Meist werden versucht Login Daten durch imitation eines Anbieters oder Dienstes abzugreifen. Des weiteren stellen Botnetze eine große Gefahr dar. Diese können sich automatisiert in kurzer Zeit auf tausende Geräte ausbreiten.

Der Banking Trojaner Flubot kombiniert Phishing Methoden und Botnetze um sich großflächig zu verbreiten und sensitive Daten abzufischen.

Diese Arbeit beleuchtet die Funktionsweise und technischen Hintergründe der Malware.

¹<https://de.statista.com/statistik/daten/studie/1235321/>

²<https://de.statista.com/themen/1355/android/>

2 Einführung

Die Android-Malware 'Flubot' trat das erste mal Ende des Jahres 2020 auf.³ Anfangs hunderte, später tausende von Android Nutzern berichteten über eine Vielzahl von verdächtigen SMS Nachrichten. Zwar unterschieden sich die Mitteilungen in gewissen Details, jedoch war der Kernaufbau der Nachricht immer der gleiche. Ein kurzer Text, gefolgt von einem Link. In dem Nachrichtentext wurde der Empfänger auf einen Dienst hingewiesen der über den Link zu erreichen sei. Öffnete man diesen wurde man auf eine Webseite weitergeleitet. Hier sollte der jeweilige Dienst über ein Download nutzbar gemacht werden. Durch Installation dieses Downloads infizierte sich das Gerät mit Flubot. In folge dessen durchläuft die Malware das Adressbuch und verbreitet sich daraufhin namesgebend wie ein Flohefall über private Kontakte!

Anfangs stellte der Köder eine vermeintlich verpasste Voicemail dar. Im weiteren Verlauf der Angriffe wurden zudem Packetlieferdienste imitiert die auf ein bald eintreffendes Packet aufmerksam machen sollten.⁴ Seit Mitte des Jahres 2021 wird nun versucht mit Sicherheitsupdates gegen Flubot selbst zu täuschen.⁵

Für Branchenkenner war schnell klar das dass ganze eine groß Angelegte Phishing Kampagne darstellte!

Aufgrund der Tatsache das Flubot nach wie vor im Umlauf ist lässt sich schwer einschätzen wie viele Geräte derzeit infiziert sind. Nach Schätzungen des IT Dienstleisters Computerwelt betrug die globale Verbreitung von Flubot im August 2021 0.33 Prozent.⁶ Dies entspricht über 13 Millionen infizierten Geräten. Auch finanziell ist die Schadenssumme derzeit nicht präzise zu bestimmen.

Durch die Ausmaße führte Flubot zu einem neuen bewusstsein von Phishing Malware. Gegenstand dieser Arbeit ist es die Bedrohungslage von solch Angriffen zu verstehen und Lösungsansätze zu finden.

Dafür wird anfangs die Funktionsweise genauer untersucht und erleutert. Anschließend wird durch eine Technische Analyse die eigentliche Anwendung hinter Flubot aus Angreifersicht beleuchtet.

Darauf aufbauend werden nun verschiedene Lösungsansätze diskutiert und vorgeschlagen. Abschließend werden die neu erlernten Kenntnisse zusammengeführt und ein Ausblick in zukünftige Bedrohungslagen und Lösungen gewagt.

³<https://www.telekom.com/en/blog/group/article/flubot-under-the-microscope-636368>

⁴<https://www.telekom.com/en/blog/group/article/flubot-under-the-microscope-636368>

⁵<https://www.computerbild.de/artikel/cb-News-Sicherheit-Flubot-Gefaehrliche-Android-Malware-verbreitet-sich-ueber-Fake-Patches-30863335.html>

⁶<https://computerwelt.at/news/android-malware-flubot-stuermt-top-ten/>

3 Funktionsweise

3.1 Infektion und Verbreitung

Flubot lässt sich terminologisch als 'Banking Trojaner' einordnen. Das heißt Hauptintension der Schadware besteht darin als nützliches Programm getarnt in Geräte einzudringen und Banking Informationen abzugreifen. Die Infektion und Verbreitung von Trojanern werden häufig mithilfe von Botnetzen betrieben. Diese bestehen aus oftmals tausenden Geräten die automatisiert die Malware betreiben und sich zudem über das befallene Gerät weiter ausbreiten. Erste Handlung von solch Angriffen ist es also eine große Anzahl an potenziellen Opfern zu kontaktieren um das Botnetz zu vergrößern. Im Falle von Flubot wird davon ausgegangen das ein Großteil der ersten Mobilfunknummern durch einen Datenleak von Facebook stammen. Mitte 2020 war es Angreifern gelungen persönliche Profil-Daten mitsamt Handy Nummern von über 11 Millionen Britischen Facebook Konten abzugreifen.⁷ Des weiteren wurden höchstwahrscheinlich weitere Datenleaks der letzten Jahre genutzt!

Durch die Länder Vorwahl ist Flubot in der Lage aus einer Liste von Phishing Ködern zu wählen die zu Sprache und Region des Opfers passen. Eine Phishing SMS setzte sich anfangs lediglich aus einer kurzen Nachricht und einem Link zusammen.

voice message received: hxxp://tantawy-group[.com/z.php?REDACTED⁸

Nachdem jedoch viele dieser Nachrichten durch SMS-Filter seitens der Mobilfunkanbieter geblockt wurden, passte sich das Botnetz durch komplexere Meldungen an. Nun wurde ein prefix aus zufälligen Zahlen und Buchstaben vor der eigentlich Nachricht eingefügt. Auch im Nachrichtentext wurden teilweise einzelne Buchstaben geflipt. Im Verlauf der Angriffe wechselten die Köder Nachrichten sehr häufig. So wurde vorallem im deutschsprachigen Raum mit Packet Tracking Mitteilungen von DHL gearbeitet. In den USA meist mit Lieferdiensten wie Fedex und UPS. Zuletzt nun mit Sicherheitsupdates gegen Flubot selbst. Diese Nachrichten gaben vor eine Infektion des Gerätes erkannt zu haben die nur durch Installation externer Software entfernt werden könne.

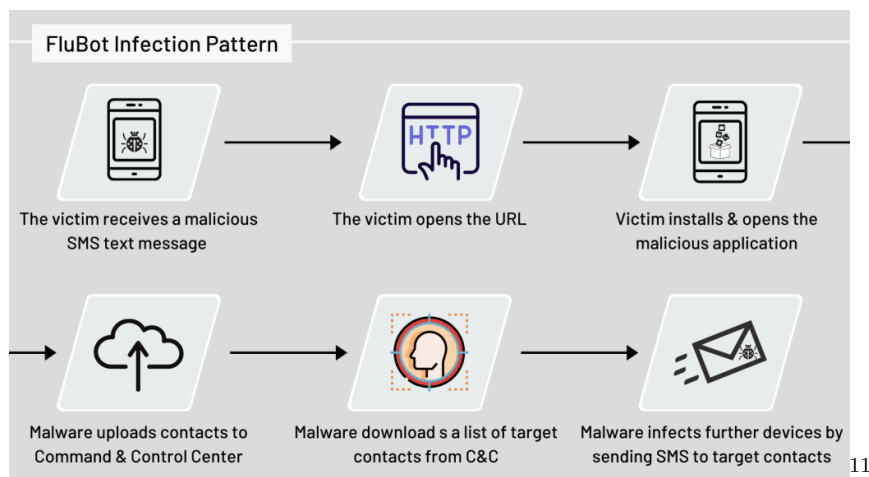
asdljNew voice-message jecoived: hxxp://fyqz[.vip/m.php?REDACTED
Ihr Packet kommt an, folgen sie es hier: https:prouthouseporpery:/64asdasd
DHL: Your parcel is arriving track here: asdadsajldadskjlkaйда⁹

In allen Fällen führt der Link auf eine Webseite. Auf dieser wird aufgefordert ein Android Package Kit herunterzuladen dass den jeweiligen Dienst nutzbar macht. Anhand einer kurzen Anleitung wird zudem gezeigt wie externe App Installationen zugelassen werden können. Nach Installation dieser APK ist das betroffene Gerät endgültig infiziert und Teil des Botnetzes.

⁷<https://wa.rner.me/2021/04/09/major-data-breach.html>

3.2 Post Infection

Erste Handlung der Malware ist es nun eine Verbindung zu dem Command and Control Server aufzubauen. Dieser ist eine Art Hauptzentrale der Malware Infrastruktur und steuert viele Abläufe der Angriffe. Auch gekappte Daten werden hier in Datenbanken verschlüsselt gespeichert und weiterverarbeitet. Ist die Verbindung hergestellt durchsucht Flubot das komplette Adressbuch des infizierten Gerätes und sendet die Kontakte an den C&C Server. Dieser antwortet erneut mit einer Liste von Handynummern die bereits durch andere Bots gesichert wurden. Über diese wird nun die Verbreitung der Malware fortgesetzt. Um eine Mustererkennung und Blockierung vorzubeugen verbreitet sich das Botnetz meist nur über neue Kontakte des C&C Servers.¹⁰



Des Weiteren schickt das infizierte Gerät eine Liste der installierten Applikationen an den Command and Control Server. Dieser antwortet wiederum mit einer Liste von Apps die kompromenttiert werden sollen. Größtenteils konzentriert sich Flubot auf Banking Apps, aus denen Login Informationen ausgelesen werden. Weitere Ziele sind Dienste für Kryptowährungen. Darunter auch sogenannte 'Multi-Asset-Broker'. Also Dienstleister die den Handel mehrerer Vermögenswerte wie Aktien, ETFs oder auch Kryptowährungen anbieten. In allen Fällen werden die ausgewählten Anwendungen injiziert. Öffnet ein Opfer nun eine der betroffenen Apps liegt ein Phishing Overlay des Login Screens als Maske über der eigentlichen Anwendung. Jegliche Eingaben werden nun an den C&C Server weitergeleitet. Weitere schädliche Aktionen beinhalten das deinstallieren von Apps, die Unterbindung von Benachrichtigungen und das Auslesen von Kreditkarten Informationen. Durch die Möglichkeit über den Command and Control Server immer wieder auch neue Angriffe zu steuern bietet Flubot über den ursprünglichen Nutzen hinaus die Möglichkeit Profit aus dem infizierten Gerät zu generieren.

¹⁰<https://www.threatmark.com/flubot-banking-malware/>

¹¹<https://www.threatmark.com/flubot-banking-malware/>

4 Technische Analyse

4.1 Netzwerkstruktur

Hinter Flubot steckt eine großflächige Infrastruktur. Kern des ganzen bildet bekanntlich der Command and Control Server. Dieser liegt nicht fest auf einem Webspaces sondern arbeitet als verteiltes System auf mehreren hundert Instanzen. Kompromitierte Webseiten wie Wordpress Blogs dienen hierbei als Hosts. In früheren Botnetzen lag der C&C Server fest auf einer dedizierten Domäne. Dies war einfach zu bekämpfen, da nach Ermittlung der IP Adresse der Internet-Service Provider diese blockieren konnte und somit die Verbreitung des Botnetzes stoppte. Flubot löst dies einmal durch die große Menge an Host-Servern und anhand des Domain Generation Algorithm.¹² Dieser Algorithmus generiert dynamisch neue Domännennamen und versucht diese aufzulösen. Grob beschrieben bedient sich der Algo aus einer Liste mit möglichen Top level Domains und generiert durch eine weitere Liste potenzielle second level Domains. Analysiert man den ausgehenden Netzwerkverkehr eines infizierten Gerätes, so ist auffällig, dass teilweise bis zu 10 DNS Requests benötigt werden, bis eine auflösbare Domäne gefunden ist. Derzeit wird DNS über HTTPS für die Domäinauflösung verwendet. Dafür werden unter anderem Services wie dns.google oder cloudflare-dns.com genutzt.¹³

34974	https://dns.google	GET	/resolve?name=ewnwoysvaefmdpm.su&type=A	✓	200	820	JSON
34973	https://cloudflare-dns.com	GET	/dns-query?name=hoacuennuwsmsk.su&type=A	✓	200	611	JSON
34972	https://cloudflare-dns.com	GET	/dns-query?name=ycligamdesovkuj.su&type=A	✓	200	611	JSON
34971	https://dns.alidns.com	GET	/resolve?name=bqocuxxqwchdrkp.cn&type=A	✓	200	407	JSON
34970	https://dns.alidns.com	GET	/resolve?name=pccytxsvylify.cn&type=A	✓	200	407	JSON
34969	https://dns.alidns.com	GET	/resolve?name=cytcfvjgyluxiu.su&type=A	✓	200	419	JSON
34968	https://dns.google	GET	/resolve?name=iwqeudyiwqdxotc.su&type=A	✓	200	861	JSON
34967	https://dns.google	GET	/resolve?name=kauvuvrfyobvgci.ru&type=A	✓	200	860	JSON

14

Der gesamte Source Code der dies möglich macht liegt in der heruntergeladenen APK. In späteren Versionen wurde der eigentliche Payload in Form der Phishing Malware erst nachträglich über den C&C geladen. Hierbei wird ein GET Request für die benötigten Dateien gestellt. Jegliche Kommunikation zwischen Gerät und Server wird zudem anhand von RSA verschlüsselt.

¹²<https://www.threatmonit.io/flubot-android-malware-technical-analysis/>

¹³[incibe-certflubotanalysisstudy2021v1.pdf](#)

¹⁴<https://www.threatmark.com/flubot-banking-malware/>

4.2 Payload

Die Payload als auch die restliche APK von Flubot sind komplett in JAVA geschrieben. Sie enthält den benötigten Source Code um Kontakt zu dem C&C Server herzustellen, die benötigten Berechtigungen einzufordern und die Phishing Malware auf ausgewählte Applikationen anzuwenden. Auch die RSA Keys für die verschlüsselte Kommunikation sind enthalten. Die gepackte APK welche den Payload trägt ist anhand MD5 gehashed und wird erst auf dem Gerät entpackt. Derzeit sind Geräte ab Android-Version 4.1.2 betroffen.¹⁵

Genauer betrachtet ist ein Android Application Package die Installations Datei für eine Android App. In ihr befinden sich alle benötigten Dateien für die Installation und Ausführung der Anwendung. In Grunde genommen ist eine Apk eine Komprimierte zip Datei die auch mit bekannter Software wie Winrar geöffnet werden kann. Das gleiche gilt für Flubot. Um Sicherheitsanalysen jedoch zu erschweren verwendet die Malware sogenannte String Obfuscation. Dies ist ein Konzept dessen Hauptaufgabe darin besteht Programmcode zu verschleiern bzw. unleserlich zu machen. Dies wird beispielweise durch Variablensubstitution erreicht. Teilweise werden auch komplette Codeabschnitte verschlüsselt.¹⁶ Für die Obfuscation verwendet Flubot das Open Source tool paranoid!¹⁷ Durch Reverse Engineering gelang es den Code zu Deobfuscieren also wieder leserlich zu machen. Die Datei AndroidManifest.xml enthält alle Berechtigungen die eine APK benötigt. Flubot hat über 40 Einträge die unter anderem Internet Zugriff und das versenden von SMS autorisieren.

```
#Berechtigungen in der Datei AndroidManifest.xml
android.permission.READ_CONTACTS
permission.WRITE_SMS
permission.INTERNET
android.permission.READ_PHONE_STATE
android.permission.QUERY_ALL_PACKAGES
android.permission.WAKE_LOCK
android.permission.FOREGROUND_SERVICE
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS18
```

¹⁵<https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Botnetze/Steckbriefe-aktueller-Botnetze/Steckbriefe/Flubot.html>

¹⁶<https://raw.githubusercontent.com/prodaft/malware-ioc/master/FluBot/FluBot.pdf>

¹⁷<https://github.com/MichaelRocks/paranoid>

Des weiteren ist es gelungen die Kommunikationskommandos zwischen Malware und des Command and Control Servers zu erfassen. Derzeit sind über 20 Kommandos möglich, wobei Flubot stetig weiterentwickelt und um Funktionalitäten ergänzt wird.¹⁹

```
#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 deaktivieren20
```

```
# Kommandos von Gerät an Server
GET_SMS Get the phishing SMS text including phone number
GET_INJECTS_LIST Get the list of targeted applications by sending all package names.
GET_INJECT Fordert den Html code für das jeweilige Phishing overlay an.
GET_INJECTS_LIST - Liste der zu attackierenden Apps anfordern!
SMS_RATE - Festlegung der zu verschickenden Phishing SMS!21
```

¹⁹<https://raw.githubusercontent.com/prodaft/malware-ioc/master/FluBot/FluBot.pdf>

Die eigentliche Phishing Attacke welche ein Overlay über die betroffene Anwendung legt, wird mittels Webview umgesetzt. Das heißt bei Öffnung der infizierten App wird das Overlay mittels Html Code im Browser dargestellt und über die Anwendung gelegt.²²

```
private void LoadHtml() {  
    String GetInject = Bot.GetInject(packagename);  
    #package name wird durch die gezielte Application ersetzt.  
    if (GetInject==0) {  
        finishandRemovetask();  
    } else {  
        this.webView.loadDataWithBaseURL(null, GetInject,  
        Deobfuskator$app$Release.getString(-225216466544654L);  
        Deobfuskator$app$Release.getString(-225216466544654L);  
        null;  
    )  
    }  
}
```

23

Flubot wird stetig weiterentwickelt und gewinnt zunehmend an Komplexität. Technisch ist die Malware auf dem neuesten Entwicklungsstand und auch aufgrund der Größe höchstwahrscheinlich von einem größeren Team professionell entwickelt worden.

²²<https://www.scamwatch.gov.au/news-alerts/missed-delivery-call-or-voicemail-flubot-scams>

5 Lösungsansätze

Flubot hat einige Mechanismen implementiert um nicht erkannt und entfernt zu werden. So wird die Anwendung nicht unter installierter Software gelistet und ist auch in einigen Taskmanagern nicht als Prozess sichtbar. Findet man die Installationsdatei doch, blockiert Flubot den Android deinstaller. Des weiteren ist Flubot in der Lage 'Play protect' zu deaktivieren. Dennoch ist die Entfernung der Malware durch Rücksetzung zum Werkzustand recht einfach.²⁴ Dies hat allerdings ein Verlust der persönlichen Daten zur Folge. Eine Entfernung ohne Datenverlust ist beispielweise durch das Open-Source tool 'malninstall'²⁵ möglich. Dieses Tool wurde speziell für die Entfernung von Flubot entwickelt.

Grundsätzlich gibt es keine generelle technische Lösung gegen Phishing Malware. Da solch Angriffe in erster Linie Social Engineering nutzen ist es schwierig ein technisches Mittel dagegen zu entwickeln. Der Mensch ist immer der anfälligste Teil eines Sicherheitsrelevanten Systems. Ein gewisser Schutz bietet jedoch Zwei Faktor Authentifizierung, der wenn möglich in allen Anwendungen aktiviert sein sollte!

Das größtmögliche Potential stellt eine bessere Bildung und Aufklärung da! Informatik sollte in Schulen deutlich stärker gewichtet werden und auch IT Sicherheitsrelevante Themen lehren!

6 Conclusion

Phishing ist nach wie vor die meist verwendete Methode um Sicherheitsrelevante Daten abzugreifen. Solange der Endnutzer nicht über die notwendige Expertise verfügt um solch Angriffe zu erkennen und abzuwehren wird Phishing Malware auch in Zukunft eine Rolle spielen!

Durch neue Technologien wie das 'Internet der Dinge' wird die Menge der angreifbaren Ziele immer weiter steigen. Die einzige Möglichkeit nachhaltig dem Problem entgegenzuwirken stellt eine ausreichende Bildung dar!

Die Drahtzieher hinter Flubot wurden im Herbst 2021 in Spanien festgesetzt.²⁶ Zum stand dieser Arbeit verbreitet sich das Botnetz allerdings nach wie vor!

²⁴<https://www.threatmonit.io/flubot-android-malware-technical-analysis/>

²⁵<https://github.com/linuxct/malninstall>

²⁶<https://therecord.media/despite-arrests-in-spain-flubot-operations-explode-across-europe-and-japan/>

7 Eigentständigkeitserklärung

Eigentständigkeitserklärung Hiermit bestätige ich, dass ich die vorliegende Arbeit selbstständig verfasst und keine anderen Publikationen als die Angegebenen benutzt habe. Alle Teile meiner Arbeit, die wortwörtlich oder dem Sinn nach anderen Werken entnommen sind, wurden unter Angabe der Quelle kenntlich gemacht. Gleiches gilt für von mir verwendete Internetquellen. Die Arbeit ist weder von mir noch von einem Kommilitonen in einem anderen Seminar vorgelegt worden.

Moritz Rupp, Albstadt, 27.11.2021

8 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>
<https://wa.rner.me/2021/04/09/major-data-breach.html>
<https://www.threatmark.com/flubot-banking-malware-incibe-certflubotanalysisstudy2021v1.pdf>
<https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Meinungen-der-Cyber-Kriminalitaet/Botnetze/Steckbriefe-aktueller-Botnetze/Steckbriefe/Flubot.html>
<https://raw.githubusercontent.com/prodaft/malware-ioc/master/FluBot/FluBot.pdf>
<https://www.scamwatch.gov.au/news-alerts/missed-delivery-call-or-voicemail-flubot-scams>