

# Mobile Banküberfälle:

Die globale wirtschaftliche  
Bedrohung



# Index

|                                                                                             |           |
|---------------------------------------------------------------------------------------------|-----------|
| <b>1:1 Einführung</b>                                                                       | <b>2</b>  |
| <b>1:2 Was sind Trojaner?</b>                                                               | <b>3</b>  |
| <b>1:3 Zentrale Erkenntnisse</b>                                                            | <b>3</b>  |
| <b>1:4 Zentrale Erkenntnisse</b>                                                            | <b>4</b>  |
| <b>1:5 Highlights der globalen Bedrohungen</b>                                              | <b>5</b>  |
| <b>2:1 Die am meisten betroffenen Finanz-Apps</b>                                           | <b>6</b>  |
| <b>2:2 Trojaner-Fähigkeiten im Mobile Banking</b>                                           | <b>7</b>  |
| <b>2:3 Die Verbraucher als Betrugsoffer</b>                                                 | <b>8</b>  |
| <b>2:4 Die Risiken von unzureichenden Sicherheitsmaßnahmen für mobile Finanzanwendungen</b> | <b>9</b>  |
| <b>2:5 Command-and-Control-Standorte</b>                                                    | <b>10</b> |
| <b>3:1 Banking-Trojanerfamilien</b>                                                         | <b>11</b> |
| • BianLian                                                                                  | 11        |
| • Cabassous                                                                                 | 12        |
| • Coper                                                                                     | 13        |
| • EventBot                                                                                  | 14        |
| • ExobotComact.D/Octo                                                                       | 15        |
| • FluBot                                                                                    | 16        |
| • Medusa                                                                                    | 17        |
| • Sharkbot                                                                                  | 18        |
| • Teabot                                                                                    | 19        |
| • Xenomorph                                                                                 | 20        |
| <b>3:2 Zimperium - Immer Einen Schritt Voraus</b>                                           | <b>21</b> |
| <b>3:3 Zimperium vs. Digitale Räuber</b>                                                    | <b>21</b> |
| <b>3:4 Zimperium sichert mobile Finanz- und Zahlungsanwendungen</b>                         | <b>21</b> |
| <b>3:5 Wie Zimperium Laufzeit-Exploitation verhindert und Banking-Malware stoppt</b>        | <b>22</b> |
| <b>4:1 Schlussfolgerung</b>                                                                 | <b>23</b> |
| <b>4:2 Anhang</b>                                                                           | <b>24</b> |
| <b>4:3 Impressum</b>                                                                        | <b>43</b> |

# Einführung

Im Jahr 2006 hatten die Banken von Chicago ein Problem. Ein Problem mit Banküberfällen, um genau zu sein. Während die Finanzinstitute der Stadt daran arbeiteten, Sicherheit und Zugriff für ihre Kunden mit mehr Zugangspunkten, neuen Filialen und anderen kundenfreundlichen Dienstleistungen in Einklang zu bringen, wurden die Bankräuber aufmerksam. Laut FBI ging die Zunahme dieser kundenfreundlichen Zugangspunkte über mehrere Jahre hinweg mit einem Anstieg der Überfälle einher und führte zu mehr Diebstählen als in den Jahren zuvor.

Jede neue Bank, von den bekanntesten Marken bis hin zu den kleinsten Startups, hatte es mit jedem physischen Standort auf das Vermögen ihrer Kunden abgesehen, aber es gab nur sehr wenig, was sie tun konnten, um die Zunahme der Diebstähle zu stoppen. Seitdem hat sich die Bankenwelt erheblich verändert. Im Jahr 2021 schlossen Berichten zufolge allein in den USA über 2.900 Banken ihre Türen.

**„Es gibt einfach mehr Ziele, die Bankräuber angreifen können.“**

**-Frank Bochte, FBI**

Auch die Art und Weise, wie wir heute Bankgeschäfte abwickeln, hat sich verändert, vor allem durch den Fortschritt der mobilen Technologie. Aber Banküberfälle gibt es immer noch. Unabhängig von diesen Schließungen haben Finanzkunden heute mehr Zugang zu ihrem Geld und ihren Finanzanlagen als je zuvor. Bankfilialen auf der ganzen Welt haben sich von der Ecke der Main Street in die Hände der Kunden verlagert, wo sie per Fingerdruck sofort auf ihre Finanzen zugreifen und Vermögenswerte bewegen können. Aber auch die Betrüger haben sich weiterentwickelt und nehmen dies zur Kenntnis.

Die Anzahl potenzieller Angriffsvektoren für mobile Banking-Apps ist endlos und nimmt jedes Jahr weiter zu. Die Risiken und Gefahren, die von Banküberfällen vor Ort ausgehen, haben abgenommen. Böswillige Akteure ziehen keine Masken mehr an, sondern wenden sich ihren Computern und bösartigem Code zu, um den nächsten digitalen Raub zu planen. Anstelle der bisherigen Banküberfälle gibt es jetzt harmlos aussehende Anwendungen, die eine bösartige Nutzlast enthalten: den Banking-Trojaner. Diese digitalen Bankräuber lassen sich leicht und massenhaft verbreiten. Sie verstecken sich im Verborgenen und warten auf den richtigen Moment und das passende Betrugsoffer. Da nun jede Bank einen bequemen, mobilen Zugang anbietet, ist jeder Kunde dem Risiko des ultimativen digitalen Bankraubs ausgesetzt.

**„Die Banken befinden sich in einer Art Zwickmühle. Indem Sie den Kunden den Zugang zu ihren Bankgeschäften erleichtern, erleichtern Sie es gleichzeitig auch den Räubern.“**

**- J. Branch Walton, Präsident der Nationalen Vereinigung für Bankensicherheit**

Achtzehn Jahre nach der Reaktion von J. Branch Walton auf die Banküberfälle in Chicago befindet sich die Finanzbranche in der gleichen Lage, allerdings an der digitalen Front. Die Ermöglichung des weltweiten Zugriffs auf die Finanzen der Kunden über einfach zu bedienende mobile Anwendungen erweiterte die Angriffspunkte im Finanzbereich und erhöhte das Risiko für die Kunden und ihre finanzielle Sicherheit.

Diese harmlos aussehenden Anwendungen, bzw. „Trojaner“, sind nicht neu. Vielmehr stellen sie eine besonders schädliche Form von Malware dar, die mobile Anwendungen, Unternehmen und Kunden plagt. Der Name geht auf die Legende vom Trojanischen Pferd zurück. Die Geschichte besagt, dass das Trojanische Pferd, ein großes hölzernes Gebilde, der Stadt Troja als Geschenk überreicht wurde, doch im Inneren verstecken sich Feinde. Nachdem das Pferd vor die Stadttore gebracht worden war, ließen die Soldaten mehr ihrer Kämpfer herein und führten einen Angriff innerhalb der Stadttore durch.



# Was sind Trojaner?

Dies ist eine passende Analogie für moderne Cyber-Bedrohungen, welche nun deshalb „Trojaner“ genannt werden. Trojaner sind bösartige Anwendungen, die in irgendeiner Weise getarnt sind, um einem potenziellen Betrugsoffer vorzugaukeln, sie seien legitim. Sie können in Anwendungen wie Produktivitäts-Tools oder Spielen versteckt sein und auf den richtigen Zeitpunkt warten, um eingesetzt zu werden. Sobald sich diese Software auf einem Zielgerät befindet, kann sie verschiedene Taktiken verfolgen, z. B. die Kontrolle über ein System erlangen, Malware auf andere Systeme verbreiten, Gerätedaten beschädigen oder sensible Informationen, Zugangsdaten oder andere Werte sammeln.

Es gibt eine Vielzahl von Trojanern, darunter Remote-Access-Trojaner (RAT), Backdoor-Trojaner, Short Message Service (SMS)-Trojaner und viele mehr. Die Verwendung von Trojanern reicht bis in die 1970er Jahre zurück, als ANIMAL entwickelt wurde. Seitdem haben die Varianten und Verwendungszwecke weiter zugenommen.<sup>1</sup> Der erste mobilspezifische Trojaner tauchte 2004 auf, infizierte Symbian-Geräte und verbreitete sich über Bluetooth.<sup>2</sup>

Der Banken- und Finanzdienstleistungssektor sieht sich immer raffinierteren Angriffen durch Trojaner ausgesetzt, die bei ihren Kunden finanziellen Schaden anrichten. Banking-Trojaner sind speziell für mobile Finanzanwendungen entwickelt worden. Banken, Investmentfirmen, Kryptowährungs-Wallets und mehr sind Angriffen von Banking-Trojanern ausgesetzt, die versuchen, Geld direkt von den Betrugsopfen zu stehlen.

So wie Bankräuber in der Vergangenheit physische Bankfilialen überfielen, hat der weit verbreitete Zugriff auf die Finanzen der Benutzer über mobile Geräte Möglichkeiten für größere Gewinne und geringere physische Risiken eröffnet.

**Die böswilligen Akteure, die hinter Banking-Trojanern stecken, setzen auf mobile Anwendungen und Endgeräte, denen es an umfassenden Sicherheitslösungen fehlt, um ihre Aktionen zu erkennen und zu verhindern.** Die Zahl der mobilen Finanzanwendungen, die den Nutzern zur Verfügung stehen, wächst und jeden Tag kommen neue Ziele hinzu.

Mobile Nutzer und ihre Finanzen sind zunehmend dem Risiko ausgesetzt, von diesen digitalen Betrügern, die hinter Banking-Trojanern und Finanzdienstleistungen stecken, bestohlen zu werden. Keine Region ist vor diesen Angriffen gefeit, und da Banking-Trojaner immer wieder mit neuen Funktionen und Fähigkeiten aktualisiert werden, sind sowohl die Benutzer als auch die Finanzinstitute weiterhin dieser globalen wirtschaftlichen Bedrohung ausgesetzt.

***Haftungsausschluss:** Dieser Bericht befasst sich mit Banking-Trojanern, die mehrere Entwicklungs- und Aktualisierungszyklen durchlaufen haben. Die in diesem Bericht enthaltenen Daten basieren vollständig auf den heutigen Varianten der einzelnen Familien. So wie die Banking-Trojaner aktualisiert werden, so werden auch die Zielbanken für jede Variante aktualisiert. Die Anzahl der betroffenen Unternehmen könnte jedoch aufgrund älterer Varianten der Banker-Trojaner, die nicht Gegenstand dieses Berichts sind, anders ausfallen.*

*Die Informationen in diesem Bericht und seine Schlussfolgerungen beruhen auf der Überprüfung und den Informationen, die dem Forschungsteam von Zimmerium zur Verfügung stehen.*

***Haftungsausschluss:** Als wichtiges Mitglied der Google App Defense Alliance scannt Zimmerium Anwendungen, bevor sie veröffentlicht werden, und bietet eine laufende Analyse der Android-Apps im Google Play Store*

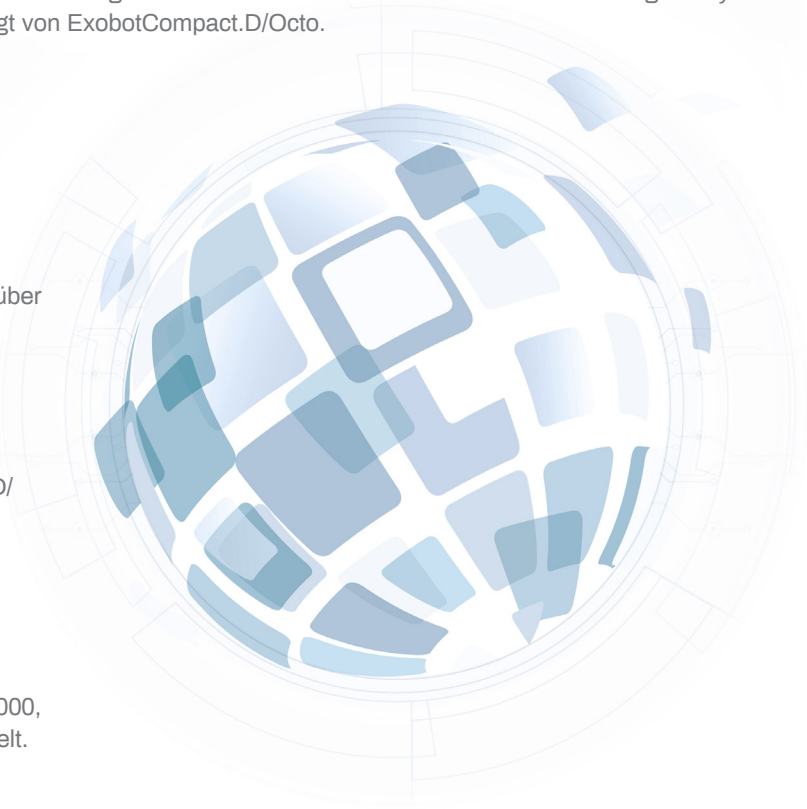
## Über diesen Bericht

Das Forschungsteam von Zimmerium analysiert täglich mehrere hunderttausend Anwendungen mit modernsten maschinellen Lernmodellen und anderen proprietären Techniken. Die in diesem Bericht behandelten Proben wurden nach dieser Methode gesammelt und klassifiziert.

In diesem Bericht untersuchen wir 10 weit verbreitete Banking-Trojaner, die es auf die mobilen Android-Apps von Nutzern weltweit abgesehen haben, und erläutern ihre Funktionen und Möglichkeiten. **Die in diesem Bericht untersuchten Finanzanwendungen sind im Google Play Store erhältlich.** Wir gehen auch detailliert darauf ein, was die einzelnen Malware-Familien voneinander unterscheidet, und heben die einzigartigen und fortschrittlichen bösartigen Funktionen hervor, welche die einzelnen Banking-Trojaner-Familien einzigartig machen. Eine vollständige Liste aller 639 Finanzanwendungen, die Bank-, Anlage-, Zahlungs- und Kryptowährungsdienste abdecken, sowie der verschiedenen Banking-Trojaner-Familien, die auf diese Anwendungen abzielen, finden Sie in **Anhang A**.

# Zentrale Erkenntnisse

- **Investmentanwendungen:** Von den 639 Anwendungen, die in diesem Bericht behandelt werden, beziehen sich 50 auf das Investieren in Aktien, Kryptowährungen oder die Portfolioverwaltung. Diese 50 Anwendungen machen über 285.000.000 Downloads im Google Play Store aus. Die meisten davon wurden von Teabot anvisiert, gefolgt von ExobotCompact.D/Octo.
- **Teabot** hat 410 der 639 verfolgten Anwendungen im Visier.
- **ExobotCompact.D/Octo** zielt auf 324 der 639 untersuchten Anwendungen ab und ist der Einzige, der es auf beliebte, nicht-finanzielle Anwendungen abgesehen hat.
- Die in diesem Bericht aufgeführten Apps für mobiles Banking, Investitionen, Zahlungen und Kryptowährungen wurden weltweit über **1.012.452.500** Mal aus dem Google Play Store heruntergeladen.
- Die meistgenutzte mobile Banking-Anwendung ist **BBVA Spain | Online Banking** mit über 10 Millionen Downloads. Diese eine Anwendung ist das Ziel von sechs der zehn bekannten Banking-Trojaner. (Medusa, Xenomorph, Coper, Flubot, ExobotCompact.D/Octo, und Sharkbot)
- Die **indische Handy-App PhonePe** bietet mit über 100.000.000 Downloads im Google Play Store die größte Angriffsfläche für Banking-Trojaner. Teabot
- **Sharkbot** zielt nur auf vier Finanzanwendungen mit über 70.500.000, darunter zwei der größten Kryptowährungshandelsdienste der Welt.



# Highlights der globalen Bedrohungen

**Australien:** 26 der 53 australischen Banken verwalten 34 mobile Banking-Apps mit über 12.752.000 Downloads im Google Play Store. Vierzehn dieser Banking-Apps sind von drei oder mehr Banking-Trojanern betroffen.

**Neuseeland:** Während Banking-Trojaner nur auf 1 von 5 neuseeländischen Bank-Apps abzielen, machen diese Apps 2.605.000 Downloads aus, mehr als die Hälfte der Bevölkerung des Landes.

**Vereinigte Staaten:** Mit mehr als 286.753.500 Downloads aus dem Google Play Store sind 121 US-amerikanische Finanzanwendungen, darunter Blockchain-Wallets und Zahlungs-Apps, Ziel von Banking-Trojanern.

**Vereinigtes Königreich:** Mit mehr als 106.260.000 Downloads sind 55 mobile Finanzanwendungen mit Sitz in Großbritannien, darunter Kryptobörsen und Investmentanwendungen, Ziel von Banking-Trojanern. Dies ist die höchste Anzahl von anvisierten Finanzanwendungen eines einzelnen Landes in ganz Europa.

**Frankreich:** 31 französische Finanzanwendungen mit über 51.390.000 Downloads aus dem Google Play Store werden stark von den Banking-Trojanern ExobotCompact.D/Octo und Teabot anvisiert.

**Vereinigte Arabische Emirate:** Von den 22 lokalen Institutionen in den Vereinigten Arabischen Emiraten sind neun Banken mit 13 Anwendungen direkt von Banking-Trojanern bedroht.

**Deutschland:** 15 in Deutschland ansässige Finanzanwendungen mit über 12.510.000 Downloads werden von ExobotCompact.D/Octo, Bianlian Botnet und Teabot angegriffen.

**Spanien:** ABANCA Corporacion Bancaria, S.A. hat sechs Apps mit 1.140.000 Downloads, die alle von ExobotCompact.D/Octo betroffen sind, die Hälfte davon von Xenomorph und Medusa.

**Türkei:** Mit mehr als 95.760.000 Downloads sind 33 türkische Finanzanwendungen von ExobotCompact.D/Octo betroffen, wobei 30 % auch von Medusa betroffen sind.

**Schweiz:** 19 Schweizer Finanzapplikationen im Bereich Banking und Kryptowährungen machen 9.250.000 Downloads aus. Alle werden exklusiv von Teabot angepeilt. Die am meisten betroffenen.

## Die am stärksten angegriffenen Länder



Vereinigte Staaten  
2 Apps betroffen



Vereinigtes Königreich  
55 Apps betroffen



Italien  
43 Apps betroffen



Türkei  
34 Apps betroffen



Australien  
33 Apps betroffen



Frankreich  
31 Apps betroffen



Spanien  
29 Apps betroffen



Portugal  
27 Apps betroffen



Schweiz  
19 Apps betroffen

## 2.1

# Die am meisten betroffenen Finanz-Apps



**PhonePe**  
Indien  
100.000.000 Downloads



**Binance**  
Malta  
50.000.000 Downloads



**Cash App**  
Vereinigte Staaten  
50.000.000 Downloads



**La Banque Postale**  
Frankreich  
10.000.000 Downloads



**Ma Banque**  
Frankreich  
10.000.000 Downloads



**Caf - Mon Compte**  
Frankreich  
10.000.000 Downloads



**Garanti BBVA Mobile**  
Argentinien  
10.000.000 Downloads



**Postepay**  
Italien  
10.000.000 Downloads

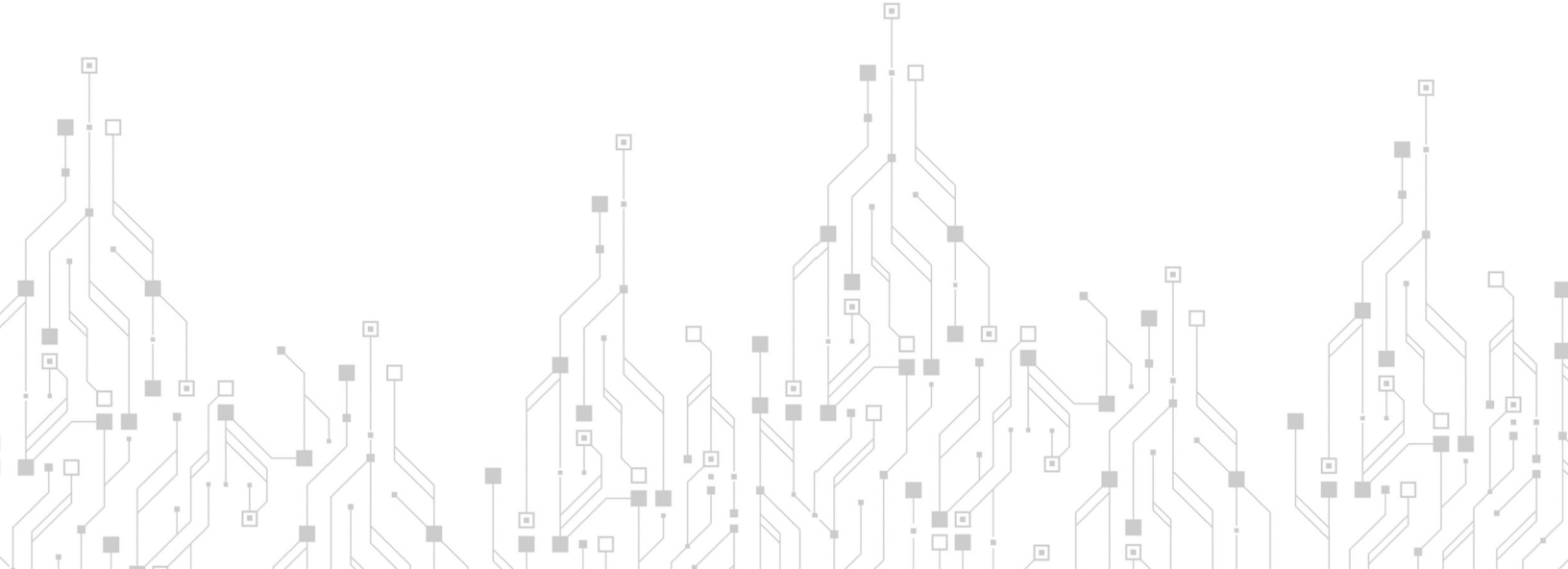


**BBVA Mexico**  
Mexiko  
10.000.000 Downloads

Die Top 9 der zielgerichteten mobilen Finanz-Apps umfassen Banken, Investitionen, Zahlungen und Kryptowährungen mit insgesamt über **260.000.000 Downloads** im Google Play Store.

Drei in Frankreich ansässige Banken (La Banque Postale, Ma Banque, Caf - Mon Compte) sind unter den Top 9 und kommen auf **30.000.000 Downloads**. Die indische mobile Finanz-App PhonePe ist, gemessen an der Anzahl der Downloads, die größte Zielscheibe unter allen verfolgten, anvisierten Anwendungen.

**Die Top 3 der mobilen Finanz-Apps, auf die es Trojaner abgesehen haben, konzentrieren sich auf mobile Zahlungen und alternative Anlagen, wie Kryptowährungen und Gold.** Diese drei Apps zählen weltweit über 200.000.000 Downloads.



# Trojaner-Fähigkeiten im Mobile Banking

Bei den heute verbreiteten Banking-Trojanern handelt es sich in der Regel um eine Mischung aus alten und neuen Methoden. Cyber-Angreifer bieten eine Reihe von Kernfunktionen, die die meisten Trojaner gemeinsam haben. Sie fügen jedoch auch eine Reihe einzigartiger Fähigkeiten hinzu, um ihre Ziele effektiver zu verfolgen, sei es, um einer Entdeckung besser zu entgehen, mehr Leute zu täuschen oder ihren Fokus besser auf eine bestimmte Bank, eine bestimmte Region oder ein bestimmtes Ziel zu richten.

Viele Banking-Trojaner haben gemeinsame Merkmale und Fähigkeiten:

- **Verbreitung.** Viele Trojaner werden über App-Stores verbreitet, darunter der Google Play App-Store und App-Stores von Drittanbietern. Andere werden über SMS-Nachrichten verbreitet, die vorgeben, von einer anerkannten Organisation zu stammen.
- **Täuschung.** Um potenzielle Opfer zu täuschen, nutzen Cyber-Angreifer die Vertrautheit und das Vertrauen der Verbraucher in bekannte Marken aus. Sie versuchen oft, ihre Nachrichten und Webseiten so aussehen zu lassen, als ob sie von Banken, Versendern, Anbietern von Kommunikations-Apps und Unterhaltungsseiten stammen würden. Sie nutzen diesen Trick, um ahnungslose Opfer dazu zu verleiten, auf bösartige Links zu klicken und Malware herunterzuladen.
- **Ausbeutung.** Nach der Installation zielen viele Trojaner auf Zugriffsdienste ab, die dazu verwendet werden können, Anmeldedaten durch Keylogging zu stehlen oder bösartigen Anwendungen automatisch die Erlaubnis zu erteilen. Sie können Overlay-Angriffe einsetzen, bei denen ein Betrugsoffer auf eine gefälschte Bankanmeldeseite geleitet wird, um die eingegebenen Anmeldedaten zu stehlen.
- **Kommunikation und Kontrolle.** Trojaner interagieren häufig mit Command-and-Control-Servern, auch um gestohlene Daten auszutauschen und die Fernsteuerung von Geräten zu übernehmen. Trojaner können auch Bildschirmfreigaben in Echtzeit mit Servern durchführen. Sie können SMS-Nachrichten erstellen und empfangen, Kontakte lokalisieren und Spam versenden und vieles mehr.
- **Umgehung.** Um sich der Entdeckung zu entziehen, verstecken Trojaner oft das Anwendungssymbol im Startmenü des Betriebssystems, so dass es unwahrscheinlicher ist, dass die Benutzer die Existenz des Trojaners entdecken. Sie können auch Maßnahmen deaktivieren oder ergreifen, um die Erkennung durch Anti-Malware-Anwendungen zu verhindern. Eine kleine Anzahl von Trojanern ergreift auch Maßnahmen, um zu verhindern, dass sie deinstalliert werden, wenn sie vom Betrugsoffer entdeckt werden.



# Die Verbraucher als Betrugsoffer

Mit Banking-Trojanern zielen Cyber-Kriminelle auf Finanzdienstleister oder einzelne Bankkunden, die mobile Banking-Apps nutzen. Die Zunahme des mobilen Bankings hat den Weg für eine viel größere und weniger gesicherte Angriffsfläche für den modernen Bankräuber geebnet.

**Drei von vier Amerikanern (193 Millionen)<sup>3</sup> nutzen Banking-Apps, um ihre täglichen Bankgeschäfte zu erledigen, z. B. Schecks einzureichen, Kontostände abzurufen oder finanzielle Vermögenswerte zu überweisen, und sind damit ein aktives Ziel für Banking-Trojaner.** Und fast die Hälfte der Teenager (48 %)<sup>4</sup> verwenden Mobiltelefone oder Websites, um ihr Geld zu verwalten, und setzen damit ihre persönlichen Daten (PII) einem Risiko aus, ohne dass sie oder ihre Erziehungsberechtigten es je erfahren. 71 % der Jugendlichen in derselben Umfrage gaben an, dass sie sich Sorgen um ihre Kreditwürdigkeit machen, was ein bemerkenswertes Finanzbewusstsein in einem so jungen Alter zeigt. Sie sind sich nicht bewusst, dass Cyber-Kriminelle ihre Kreditwürdigkeit leicht zerstören können, bevor sie überhaupt ins Berufsleben eintreten.

Es gibt zwei Arten von Banking-Trojanern, die es auf Mobile Banking-Nutzer weltweit abgesehen haben. Der erste ist Teil einer größeren Angriffskette mit Funktionen, die darauf abzielen, Bankdaten und Zugangsdaten zu infiltrieren und Sicherheitskontrollen wie die Multifaktor-Authentifizierung in Verbindung mit dem Konto des Kontoinhabers zu beeinträchtigen.

Bei der zweiten Variante kommen Funktionen wie Screen Scraper und Keylogger zusammen mit Dateneingabefunktionen hinzu, die darauf abzielen, Geld direkt über die App zu stehlen, wenn sich ein Benutzer anmeldet.

Banking-Trojaner zielen zwar auf die Nutzer mobiler Apps ab, aber auch die Auswirkungen auf das Institut können erheblich sein. Banken haben die Aufgabe, die Finanzen ihrer Kunden zu sichern. Doch im Falle eines Betrugs durch Banking-Trojaner ist nicht nur der Verbraucher betroffen, auch die Auswirkungen auf die Bank können schwerwiegend sein: Rufschädigung, Verlust des Kundenvertrauens, Umsatzeinbußen, erhöhte Kosten, Schadensersatz und Geldbußen.

Wie andere Malware auf Android setzen auch viele Banking-Trojaner auf Social Engineering und das Vertrauen des Betrugsoffers, um der App Zugriff und Berechtigungen zu erteilen, so dass sie als Administrator des Geräts agieren kann. Diese Schritte ermöglichen es den Banking-Trojanern, die Sicherheitskontrollen zu manipulieren, den Bildschirm und die Texteingaben zu überwachen und schließlich den Werksreset zu veranlassen, nachdem das Geld des Betrugsoffers gestohlen wurde. Dank dieser Kontrolle und Fähigkeit können fortschrittliche Banking-Trojaner auch alle Nachrichten und Eingaben zur Multi-Faktor-Authentifizierung abfangen und so die Sicherheitskontrollen und die Eingaben der Nutzer umgehen.



# Die Risiken von unzureichenden Sicherheitsmaßnahmen für mobile Finanzanwendungen

Die Risiken für die Anbieter von Finanzanwendungen sind vielfältig und wirken sich noch lange nach dem ersten Angriff negativ auf ein Unternehmen aus. Hier sind einige der schädlichsten Folgen eines erfolgreichen Fintech-Sicherheitsverstoßes.



## Datendiebstahl

Sensible personenbezogene Daten und andere wertvolle Daten, einschließlich Namen, Passwörter und Zahlungskartendetails, können über kompromittierte Finanz-Apps leicht zugänglich gemacht werden. Mobile Banking-Trojaner wie Sharkbot und Medusa sowie andere mobile Malware verwenden verschiedene Techniken zur Datenexfiltration, darunter Keylogger, Overlay-Bildschirme und die Ausnutzung von Zugriffsdiensten.



## Bußgelder und Schadensersatzzahlungen

Eine Reihe globaler Gesetze zur Datensicherheit legt die Strafen für Verstöße gegen die Sicherheit von Finanz-Apps fest. So kann ein Unternehmen **nach der EU-Datenschutzgrundverordnung mit einer Geldstrafe von bis zu 4 % seines weltweiten Umsatzes belegt werden.**<sup>5</sup> Zusätzlich zu den Bußgeldern müssen betroffene Unternehmen möglicherweise erhebliche Entschädigungen an die betroffenen Nutzer zahlen. Ein bemerkenswertes Beispiel ist der Entschädigungsfonds in Höhe von 300 Millionen USD (der möglicherweise auf 425 Millionen USD ansteigt), den Equifax einrichten musste, nachdem das Unternehmen bei der Sicherung seiner Kundendaten nachlässig war.<sup>6</sup>



## Verlust des Kunden-vertrauens

Kunden verlieren das Vertrauen in Unternehmen, bei denen die Cybersicherheit verletzt wurde. Untersuchungen zeigen, dass **83 % der US-Verbraucher**<sup>7</sup> zumindest für einige Monate keine Geschäfte mehr mit einem betroffenen Unternehmen machen würden. In Großbritannien gaben über 40 % der Kunden an, dass sie mit einem solchen Unternehmen nie wieder Geschäfte machen würden. Außerdem ist es teurer, neue Kunden zu gewinnen. Diese Kosten entstehen durch die zusätzlichen Marketingausgaben, die erforderlich sind, um den Ruf der Marke wiederherzustellen, und durch Änderungen des Geschäftsmodells, wie z. B. höhere Produktrabatte oder niedrigere Servicegebühren.



## Gestohlene Vermögenswerte, die für Betrug verwendet werden

Banking-Apps enthalten verschiedene Elemente von direktem monetärem Wert, darunter die Möglichkeit, Geld zu überweisen, Aktien und Kryptowährungen zu kaufen und zu verkaufen und sogar Zahlungs-Token, die für mobile Transaktionen verwendet werden. Der Diebstahl dieser Vermögenswerte führt direkt zu Betrug und Schaden für die Verbraucher und Banken. Laut einem kürzlich erschienenen Bericht der Federal Trade Commission **meldeten die Verbraucher einen Anstieg der Betrugsfälle um 70 % von 2020 bis 2021**, was einem Wert von mehr als 5,8 Milliarden Dollar entspricht.<sup>8</sup> Eine weitere Studie ergab, dass betrügerische mobile Transaktionen 29 % der Kosten ausmachen, die Finanzinstituten nach einem Betrug entstehen. Dazu gehören angefallene Zinsen, Bußgelder und Rechtskosten, Arbeits- und Ermittlungskosten sowie Kosten für die Wiederbeschaffung von Vermögenswerten.<sup>9</sup>

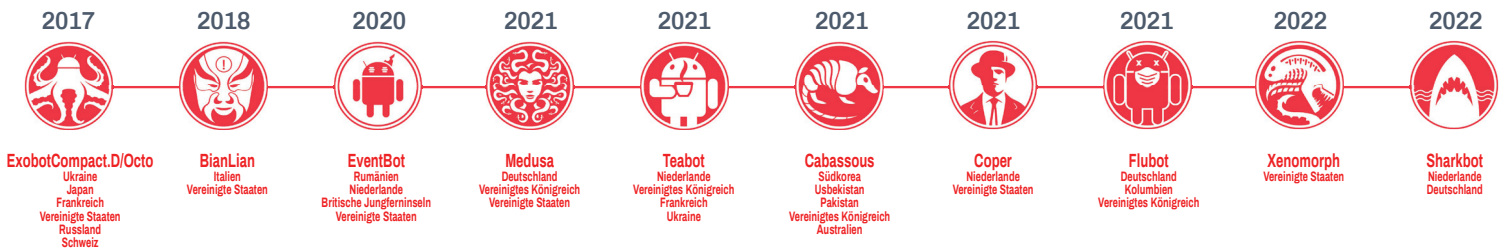
# Command-and-Control-Standorte

Finanzkriminalität ist ein globaler Wirtschaftszweig. Böswillige Akteure nutzen global zugängliche Ökosysteme, um ihre Command-and-Control (C&C)-Einrichtungen zu hosten. Es gibt zwar einige Beweise für einen Zusammenhang zwischen der Entwicklung von Banking-Trojanern und unfreundlichen Nationen, aber die Hosting-Standorte des Command-and-Control-Servers bedeuten nicht, dass die böswilligen Parteien an diesem Ort ansässig sind oder von diesem Ort unterstützt werden. Darüber hinaus neigen böswillige Akteure dazu, Hosting-Dienste zu nutzen, die nicht über strenge Maßnahmen zur Verhinderung illegaler Aktivitäten verfügen, was sie auf bestimmte Standorte verweist.

Die Verbreitung der Command-and-Control-Server-Standorte zeigt die globale Reichweite von Banking-Trojanern. Von den zehn überwachten Banking-Trojanern hostet Kolumbien den einzigen C&C-Standort in der südlichen Hemisphäre, während die Vereinigten Staaten Server für 6 der 10 Banking-Trojaner beherbergen. In Osteuropa hosten Russland, Rumänien und die Ukraine mehrere Server, während Usbekistan, Japan und Südkorea C&C-Hosting in Asien ermöglichen. Obwohl Teabot auf die meisten Finanzanwendungen abzielt, greift es auf weniger C&C-Server zurück als ExobotCompact.D/Octo, während Xenomorph nur einen C&C-Host in den USA nutzt.

Die erste Familie von Banking-Trojanern, auf die in diesem Bericht hingewiesen wird, wurde 2017 entdeckt, während BianLian in 2018 entdeckt wurde. Die Zunahme der Bedrohung wurde jedoch erst im Jahr 2020 deutlich. Seitdem wurden 8 der 10 weiteren Trojaner entdeckt. Dieser sprunghafte Anstieg an Banking-Trojanern deckt sich mit den Daten zur Nutzung und Abhängigkeit von mobilen Endgeräten im Alltag, insbesondere ab 2020, als sich die Welt durch COVID-19 veränderte.

## Zeitleiste / Ort der Entdeckung des Banking-Trojaners



## 3.1

# Banking-Trojanerfamilien

## BianLian



### Entdeckt in 2018

BianLian ist ein Banking-Trojaner, der über den Google Play Store verbreitet wird. Sobald die Malware aktiviert ist, wartet sie auf Anweisungen von Firebase, Googles Plattform für die Erstellung mobiler Apps. Die Angreifer konnten Firebase zum Senden von Befehlen an kompromittierte Geräte nutzen. Dieser Trojaner nutzt viele gängige Techniken, darunter das Abfangen von SMS, die Möglichkeit, das Gerät zu sperren, und Overlay-Angriffe, um Anmeldedaten zu stehlen.

Die früheste Version dieser Malware-Familie wurde im Jahr 2018 entdeckt. Die Entwickler dieses Trojaners sind unter dem Namen Hydra bekannt und haben die Fähigkeiten der Malware weiter verbessert. Im April 2022 wurde eine Trojaner-Version entdeckt, mit der photoTAN – eine Authentifizierungsmethode, die Banken zur Verifizierung von Online-Bestellungen einsetzen – umgangen werden kann. Dieser Trojaner wurde verwendet, um Banken in der Türkei und in Europa anzugreifen.

Er wendet mehrere Methoden an, um sich der Erkennung zu entziehen, darunter:

- Die Malware erkennt, ob eine Anfrage von Google Play Protect stammt. Wenn dies der Fall ist, fungiert der Trojaner als normale App, um der Erkennung zu entgehen.
- In späteren Versionen konnte der Trojaner erkennen, ob Google Play Protect ausgeführt wurde und den Dienst vor der Anfrage deaktivieren.
- Die Angreifer haben den Code verschleiert, um die Untersuchung der Malware zu erschweren.



**Binance: Buy BTC & 600+ Krypto**  
Malta  
50.000.000 Downloads



**Garanti BBVA Mobile**  
Argentinien  
10.000.000 Downloads



**Ziraat Mobile**  
Serbien  
10.000.000 Downloads



**Akbank Mobile Banking**  
Türkei  
10.000.000 Downloads



**QNB Finansbank**  
Türkei  
10.000.000 Downloads



**Halkbank Mobil**  
Türkei  
10.000.000 Downloads



**Cep - Mobile Banking**  
Türkei  
10.000.000 Downloads



**VakıfBank Mobil Bankacılık**  
Türkei  
10.000.000 Downloads



**Yapi Kredi Mobile**  
Türkei  
10.000.000 Downloads

# Cabassous



## Entdeckt in 2021

Cabassous wird über betrügerische SMS-Nachrichten verbreitet. Die Nachrichten sahen so aus, als kämen sie von FedEx, DHL oder einem anderen Zustelldienst. In der Nachricht wird der Empfänger aufgefordert, eine App herunterzuladen, um sein Paket zu verfolgen. Mit Hilfe der Overlay-Angriffsmethode würde der Trojaner versuchen, die Benutzer zur Eingabe ihrer Anmeldedaten aufzufordern.

Die Apps von fast 15 Banken waren betroffen, darunter Bankinter, ING Espana und Santander. Diese Malware wurde erstmals im Januar 2021 entdeckt. Später wurde eine neue Variante identifiziert, die den Namen FluBot erhielt.

Sobald das Zielgerät angegriffen wurde, unternahm die Malware zahlreiche Schritte, darunter das Senden und Empfangen von SMS-Nachrichten, das Versenden von Spam an Kontakte in der Kontaktdatenbank und das Stehlen dieser Kontaktdaten und sogar das Deaktivieren von Google Play Protect.

Dieser Trojaner nutzte außerdem mehrere neuartige Fähigkeiten:

- Der Code verbirgt das App-Symbol vor dem Launcher des Betriebssystems, so dass der Nutzer die App nicht erkennen kann.
- Durch die Auswahl der Adresse des Command-and-Control-Servers verwendeten die Angreifer einen Algorithmus zur Generierung von Domains, um die Erkennung zu umgehen.
- Dieser Trojaner hatte es vor allem auf Banking- und Kryptowährungs-Apps spanischer Kunden abgesehen.



**Barclays Mobile App**  
Vereinigtes  
Königreich  
100.000.000 Downloads



**Commonwealth Bank**  
Australien  
50.000.000 Downloads



**Halifax Mobile Banking**  
Kanada  
50.000.000 Downloads



**Lloyds Bank Mobile**  
Vereinigtes  
Königreich  
50.000.000 Downloads



**Santander  
Mobile Banking**  
Vereinigtes Königreich  
50.000.000 Downloads



**NatWest Mobile  
Banking**  
Vereinigtes Königreich  
50.000.000 Downloads



**ANZ Australia**  
Australien  
10.000.000 Downloads



**St.George Mobile  
Banking**  
Australien  
10.000.000 Downloads



**Westpac Mobile  
Banking**  
Australien  
10.000.000 Downloads

# Coper



## Entdeckt in 2021

Coper wurde zunächst als Banking-App mit dem Namen „Bancolombia Personas“ präsentiert, die sich an Kunden dieser kolumbianischen Bank richtete.

Sobald diese Malware auf dem Gerät des Benutzers installiert ist, nutzt sie Social Engineering und die Funktion der Zugriffsdienste, um Google Play Protect zu deaktivieren und weitere bösartige Apps zu installieren. Coper wurde im Juli 2021 entdeckt und zielt auf 40 Finanz-Apps ab.

Sobald die App gestartet ist, erhält sie eine Reihe von Berechtigungen, darunter Admin-Rechte, die Möglichkeit, SMS-Nachrichten zu senden und abzufangen, Anrufe zu tätigen, das Gerät zu sperren und zu entsperren, Keylogging durchzuführen sowie Anwendungen zu deinstallieren.

Zusätzlich zu den üblichen Trojaner-Funktionen verfügt Coper über weitere neuartige Fähigkeiten wie:

- Die Überwachung der Akku-Optimierungsliste des Geräts ermöglicht es, das Gerät teilweise von den Einstellungen für Dösen und App-Standby zu befreien und den Betrieb fortzusetzen.
- Jede Minute benachrichtigt der Trojaner den Command-and-Control-Server über seine erfolgreiche Infektion des Geräts und wartet auf Anweisungen. Der Server kann Aktualisierungen bereitstellen, z. B. den Wechsel von Servern, die Identifizierung von Apps, die mit einem Phishing-Bildschirm angegriffen werden sollen, die Auswahl von Apps, die gelöscht oder an der Ausgabe von Benachrichtigungen gehindert werden sollen, und vieles mehr.



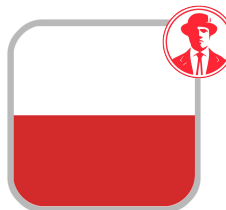
**BBVA Spain |  
Onlinebanking**  
Spanien  
100.000.000 Downloads



**CaixaBankNow  
Mobile Banking**  
Spanien  
100.000.000 Downloads



**Commonwealth Bank**  
Australien  
50.000.000 Downloads



**Santander  
Mobile Banking**  
Polen  
50.000.000 Downloads



**ANZ Australia  
Mobile Banking**  
Australien  
10.000.000 Downloads



**St.George  
Mobile Banking**  
Australien  
10.000.000 Downloads



**ING Australia Banking**  
Australien  
10.000.000 Downloads

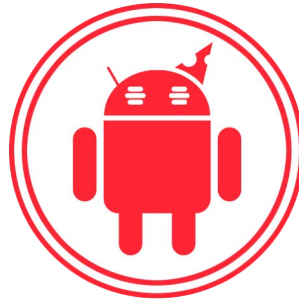


**TSB Mobile Banking**  
Vereinigtes  
Königreich  
10.000.000 Downloads



**NAB Mobile  
Banking**  
Vereinigte Staaten  
10.000.000 Downloads

# EventBot



## Entdeckt in 2020

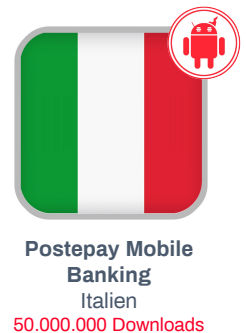
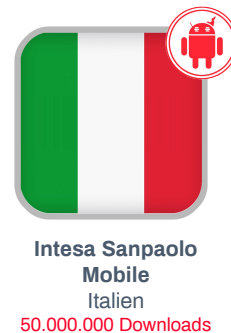
EventBot wurde erstmals im März 2020 entdeckt und wurde vermutlich über App-Stores von Drittanbietern und bösartige Websites verbreitet. Durch den Missbrauch von Zugriffsfunktionen auf dem Android-Gerät kann der Trojaner die Anmeldedaten der Benutzer von Banking-Apps stehlen. Die Malware kann auch die SMS-Nachrichten der Benutzer stehlen und an einen Server senden, um die Multi-Faktor-Authentifizierungssysteme der Bank zu umgehen.

EventBot wurde erstmals im Jahr 2020 entdeckt. Seitdem haben die Angreifer immer wieder neue Versionen des Trojaners mit zusätzlichen Funktionen entwickelt.

Verbraucher in Deutschland, Italien, Spanien und Großbritannien sind betroffen, und 12 Banking-Apps wurden kompromittiert.

Dieser Trojaner verfügt über mehrere neuartige Fähigkeiten, um seine Effektivität zu verbessern:

- Der Trojaner ist in der Lage, Konfigurationsdateien zu aktualisieren und neue Malware-Module herunterzuladen.
- Die in der Malware verwendeten Symbole ähneln denen von bekannten Anwendungen wie Microsoft Word und Adobe Flash.
- Der Trojaner nutzt bewährte Funktionen zur Erstellung von Overlay-Phishing-Seiten, um Anmeldedaten zu stehlen.



# ExobotCompact .D/Octo



## Entdeckt in 2017

Die Angreifer, die hinter Exobot stecken, verbreiten diesen Trojaner über SMS-Nachrichten, die die Benutzer dazu bringen, gefälschte Versionen von häufig genutzten Apps wie WhatsApp, Netflix und Runtastic zu installieren. Anschließend zeigten sie mit Hilfe eines Overlay-Angriffs eine Seite an, die wie die einer Bank aussah. So konnten sie die Zugangsdaten und Details zu Kredit- und Debitkarten des Benutzers stehlen.

Der Trojaner verfügte über eine weitere Täuschungsebene, indem er die aktuell auf dem Bildschirm des Benutzers ausgeführte App überprüfte und dann das Phishing-Overlay an diese App anpasste, so dass der Benutzer nicht auf die Idee kommen konnte, dass es sich um eine bösartige Anwendung handelt. Der Trojaner nutzte die Android Process-Bibliothek, um festzustellen, welche App im Vordergrund läuft. Der Trojaner überprüfte auch das Vorhandensein von Antivirus-Apps und schloss sogar die Antivirus-App, wenn sie den Trojaner entdeckte.

Exobot wurde erstmals im Februar 2017 entdeckt. Mehr als 370 Banking-Apps wurden angegriffen, mit Betrugsopfern in Belgien, Frankreich, Deutschland, Italien und Großbritannien. ExobotCompact.D/Octo wandte viele fortschrittliche Taktiken an und verließ sich dabei auch auf völlig neue Fähigkeiten:

- Bei den entdeckten Exobot-Samples handelte es sich durchweg um sehr kleine Anwendungen, typischerweise um die 700 KB herum.
- Die Listen der anvisierten Banken und die zugehörigen Overlays konnten über einen Command-and-Control-Server aktualisiert werden.
- Die entdeckten Samples enthalten keine nativen Bibliotheken und bestehen nur aus Dalvik-Bytecode, einer nicht mehr weiterentwickelten virtuellen Maschine, die Anwendungen auf der Android-Plattform ausführt.
- Der Trojaner verwendet die AndroidProcess-Bibliothek, die es der Anwendung ermöglicht, den Namen des Android-Pakets zu ermitteln, das gerade im Vordergrund ausgeführt wird. Sie wurde verwendet, um zu erkennen, welche Bankanwendung gerade ausgeführt wird, und zeigt dann das entsprechende Overlay an.



**PayPal - Senden, Kaufen, Verwalten**  
Vereinigte Staaten  
100.000.000 Downloads



**Binance: Buy BTC & 600+ Krypto**  
Malta  
50.000.000 Downloads



**Cash App Mobile**  
Vereinigte Staaten  
50.000.000 Downloads



**Barclays Mobile Banking**  
Vereinigtes Königreich  
10.000.000 Downloads



**BBVA Spain | Onlinebanking**  
Spanien  
10.000.000 Downloads



**CaixaBankNow Mobile**  
Spanien  
10.000.000 Downloads



**Garanti BBVA Mobile**  
Argentinien  
10.000.000 Downloads



**Ziraat Mobile**  
Serbien  
10.000.000 Downloads



**QNB Finansbank**  
Türkei  
10.000.000 Downloads

# Flubot



## Entdeckt in 2021

FluBot ist eine aggressive Variante von Cabassous, die ebenfalls in diesem Bericht behandelt wird. Sie nutzt SMS-Phishing, um ihre Opfer auf der ganzen Welt zu erreichen. Angreifer, die den Trojaner FluBot einsetzen, gaukeln Benutzern mit betrügerischen Nachrichten und Benachrichtigungen vor, dass sie ein Paket verpasst hätten. Diese Nachrichten enthalten einen Link zu einer Seite, die den Benutzer auffordert, Malware zu installieren, die als eine scheinbar legitime Lieferanwendung getarnt ist.

Dieser Trojaner hat viele der Funktionen von TeaBot. Die wichtigste Änderung war die Möglichkeit, direkt auf Push-Benachrichtigungen zu antworten. Mit dieser Fähigkeit kann Malware eine eingehende Benachrichtigung abfangen, sie an den Server des Angreifers weiterleiten sowie eine manipulierte Benachrichtigung an das Betrugsopfer zurücksenden. Der im April 2021 entdeckte Trojaner hat es auf 17 Banking-Apps abgesehen. Dabei wurden die Geräte von Betrugsopfern aus Österreich, Australien, Deutschland, Polen und Spanien kompromittiert.

Zusätzlich zu den gemeinsamen Funktionen bot FluBot weitere neue Möglichkeiten:

- Jede Minute sendet die Malware Statistiken über die eingegangenen Benachrichtigungen an den Server.
- Über die Funktion „Direct Reply“ können Angreifer Push-Benachrichtigungen abfangen, sie an den Server senden und den Benutzern die manipulierte Benachrichtigung anzeigen.



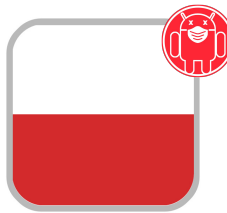
**BBVA Spain | Onlinebanking**  
Spanien  
10.000.000 Downloads



**CaixaBankNow Mobile**  
Spanien  
100.000.000 Downloads



**BBVA Mexico Mobile**  
Mexiko  
100.000.000 Downloads



**Santander Mobile Banking**  
Polen  
50.000.000 Downloads



**Banco Sabadell App**  
Spanien  
10.000.000 Downloads



**Grupo Cajamar**  
Spanien  
10.000.000 Downloads



**Ibercaja Mobile Banking**  
Spanien  
10.000.000 Downloads



**ING Espana. Banca Movil**  
Spanien  
10.000.000 Downloads



**BBVA Net Cash | ES & PT**  
Portugal  
5.000.000 Downloads

# Medusa



## Entdeckt in 2020

Sobald dieser Trojaner installiert ist, wird der Benutzer des Geräts aufgefordert,

ihm Zugriffsdienste zu gewähren, die dazu dienen, der Anwendung weitere Berechtigungen zu erteilen. Der Trojaner verfügte über eine Reihe von Funktionen, darunter Keylogging, Stehlen von Daten aus Zwischenablagen, Screencasting und Senden von Ereignisprotokollen an einen Command-and-Control-Server.

Die Drahtzieher hinter Medusa stammen aus der Türkei und ihre erste Kampagne konzentrierte sich auf die dortigen Banken. Die nachfolgenden Angriffe betrafen jedoch Benutzer in ganz Nordamerika und Europa, und mehr als 76 Banken wurden angegriffen. Medusa wurde erstmals im Juli 2020 entdeckt.

Zusätzlich zu den üblichen Taktiken wie Keylogging und Diebstahl von Daten aus der Zwischenablage hat dieser Trojaner auch andere, neuartige Fähigkeiten eingesetzt:

- Der Trojaner führte die Funktion Semi-ATS (Automatic Transfer System) ein.
- Ein Zugriffsskriptdienst, der eine Reihe von Aktionen im Namen des Opfers ausführen kann. Mechanismus zur Protokollierung von Zugangsereignissen in der Malware.



**BBVA Spain |  
Onlinebanking**  
Spanien  
10.000.000 Downloads



**CaixaBankNow Mobile**  
Spanien  
10.000.000 Downloads



**Garanti BBVA Mobile**  
Argentinien  
10.000.000 Downloads



**BZiraat Mobile**  
Serbien  
10.000.000 Downloads



**Akbank Onlinebanking**  
Türkei  
10.000.000 Downloads



**QNB Finansbank**  
Türkei  
10.000.000 Downloads



**Halkbank Mobil**  
Türkei  
10.000.000 Downloads



**Cep - Mobile  
Banking**  
Türkei  
10.000.000 Downloads



**VakifBank Mobil  
Bankacilik**  
Türkei  
10.000.000 Downloads

# Sharkbot



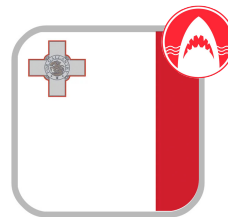
## Entdeckt in 2021

Der Sharkbot-Trojaner zielt in erster Linie auf Geldtransfers ab und versucht, die Technik des automatischen Überweisungssystems (ATS) auszunutzen, mit der die mehrstufigen Authentifizierungsmechanismen einer Bank umgangen werden. Wenn ein Benutzer versucht, Geld auf ein anderes Bankkonto zu überweisen, ändert die Malware die internationale Bankkontonummer (IBAN), die in das Konto des Angreifers eingegeben wurde.

Sharkbot wurde im Jahr 2021 entdeckt und zeigt nach der Installation kein Symbol auf dem App-Launcher des Benutzers an. Nachdem er die Zugriffsdienste eines Geräts missbraucht hat, führt der Trojaner unter der Identität des Betrugsopfers Aktionen aus. Der Trojaner kann auch Overlay-Angriffe einsetzen, um Anmeldedaten und Kreditkarteninformationen zu stehlen.

Zu den üblichen Taktiken wie Keylogging und dem Verstecken des App-Symbols vor dem App-Startprogramm des Benutzers kommen bei diesem Trojaner noch weitere neue Fähigkeiten hinzu: Anti-Analyse-Techniken, einschließlich der Erkennung von Emulatoren, und die Verwendung eines Domain-Generierungs-Algorithmus für seine Netzwerkkommunikation. Die Tatsache, dass der Trojaner von Grund auf neu geschrieben wurde, trägt ebenfalls dazu bei, dass er nicht entdeckt wird.

- Eine Anti-Lösch-Funktion, die Opfer daran hindert, die App zu deinstallieren.
- Die Fähigkeit, andere Apps auf den Geräten des Opfers zu löschen, basierend auf Anweisungen von einem Command-and-Control-Server.
- Die Möglichkeit, per SMS gesendete legitime Bankkommunikation abzufangen.
- Die Verwendung von Verschlüsselung, um die Kommunikation mit dem Command-and-Control-Server zu verbergen.



**Binance: Buy BTC & 600+ Krypto**  
Malta  
50.000.000 Downloads



**BBVA Spain | Onlinebanking**  
Spanien  
10.000.000 Downloads



**Coinbase: Bitcoin & Ether kaufen**  
Vereinigte Staaten  
10.000.000 Downloads



**EVO Banco mobil**  
Spanien  
500.000 Downloads

# Teabot



## Entdeckt in 2021

Teabot ist einer der allgemeineren Banking-Trojaner, der es auf die meisten mobilen Finanzanwendungen mit eher standardmäßigen Funktionen abgesehen hat. Sobald sich der Trojaner auf dem Gerät des Betroffenen befindet, prüft er, welche Anwendungen installiert sind, und sobald er eine gezielte Banking-App entdeckt, lädt er eine Nutzlast speziell für diese App herunter.

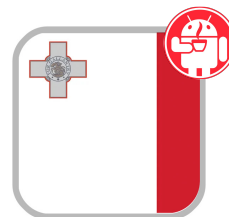
Teabot wurde erst Anfang 2021 entdeckt und war zuvor als Anatsa/Toddler bekannt. Ursprünglich hatte Teapot mehr als 60 Banken in Italien im Visier. Im Laufe der Zeit wurde dieser Trojaner verwendet, um mehr als 400 Banken in einer Reihe von Ländern anzugreifen.

Nebst den gemeinsamen Taktiken mit anderen Trojanern ist Teabot mit weiteren neuartigen Fähigkeiten ausgestattet:

- App-spezifisches Keylogging für Banking-Apps.
- Senden der gesammelten Daten alle 10 Sekunden an einen Command-and-Control-Server.
- Verlässt sich auf GitHub, um die Nutzdaten zu hosten, die letztendlich heruntergeladen wurden.



**PhonePe: UPI, Aufladen, Investition, Versicherung**  
Indien  
100.000.000 Downloads



**Binance: Buy BTC & 600+ Krypto**  
Malta  
50.000.000 Downloads



**Barclays Mobile**  
Vereinigtes Königreich  
10.000.000 Downloads



**Postepay Mobile Banking**  
Italien  
10.000.000 Downloads



**Crypto.com - Buy BTC, ETH**  
Singapur  
10.000.000 Downloads



**Blockchain.com Wallet: Buy BTC**  
Vereinigtes Königreich  
10.000.000 Downloads



**Bank of America Mobile Banking**  
Vereinigte Staaten  
10.000.000 Downloads



**Capital One Mobile**  
Vereinigte Staaten  
10.000.000 Downloads



**Coinbase: Bitcoin & Ether kaufen**  
Vereinigte Staaten  
10.000.000 Downloads

# Xenomorph



## Entdeckt in 2022

Xenomorph wurde über den Google Play App Store vertrieben. Der als „Fast Cleaner“ bezeichnete Trojaner wurde von mehr als 50.000 Benutzern heruntergeladen. Xenomorph setzte viele gängige Trojaner-Taktiken ein, wie z. B. das Stehlen von SMS-Nachrichten, das Abfangen von Benachrichtigungen, das Umgehen der Zwei-Faktor-Authentifizierung sowie Overlay-Angriffe, um Anmeldedaten zu stehlen.

Dieser Trojaner wurde im Februar 2022 entdeckt und es wird vermutet, dass er von einer Akteursgruppe mit dem Namen „ring0“ stammt. RingO war auch der Entwickler eines anderen Trojaners, der als Alien bekannt ist, und Xenomorph hat viele Ähnlichkeiten mit diesem Trojaner. Die Geschädigten kommen aus Belgien, Italien, Portugal und Spanien, und 29 Banking-Apps wurden kompromittiert.

Zusätzlich zu den üblichen Taktiken setzte Xenomorph weitere neue Fähigkeiten ein:

- Der Trojaner fungierte als Dropper für weitere Malware-Apps auf dem Gerät.
- Missbrauch von Zugriffsdiensten zur Protokollierung von Aktivitäten und zum Senden von Protokollen an die Zentrale.



**BBVA Spain |  
Onlinebanking**  
Spanien  
10.000.000 Downloads



**KBC Mobile**  
Belgien  
10.000.000 Downloads



**Belfius Mobile**  
Belgien  
10.000.000 Downloads



**Easy Banking App**  
Belgien  
10.000.000 Downloads



**ING Banking App**  
Niederlande  
10.000.000 Downloads



**Imagin Banking App**  
Spanien  
10.000.000 Downloads



**Caixadirecta  
Mobile Banking**  
Portugal  
10.000.000 Downloads



**MB WAY Mobile**  
Portugal  
10.000.000 Downloads



**Grupo Cajamar**  
Spanien  
10.000.000 Downloads

# Zimperium - Immer Einen Schritt Voraus

## Zimperium vs. Digitale Räuber

Die rasante Ausbreitung von Finanz-Apps und ihr Wert als lukratives Ziel bedeutet, dass die Bedrohungen häufiger und komplexer geworden sind und sich mit einfachen Sicherheitsmaßnahmen nur schwer verhindern lassen. Die Fähigkeiten einiger der in diesem Bericht vorgestellten Banking-Trojaner zeigen, dass böswillige Akteure ein weites Netz auswerfen, um kritische Login- und (Multifaktor-) Authentifizierungsinformationen sowie Kontoinhaber- und Kreditkartendaten zu sammeln, mit dem Ziel des Finanzbetrugs. Die kriminellen Organisationen und böswilligen Akteure, die hinter der Banking-Malware stecken, profitieren von der unzureichenden oder gar nicht vorhandenen Sicherheit der mobilen Banking-Apps.

## Zimperium sichert mobile Finanz- und Zahlungsanwendungen

Heutzutage sind mobile Finanzanwendungen der digitale Kanal für den Zugang zu Vermögenswerten. Sie stellen den Kunden Ressourcen zur Verfügung, die früher an physische Bankstandorte gebunden waren. Allerdings bergen sie auch ungeahnte Sicherheits- und Datenschutzrisiken, wenn sie auf mobilen Endgeräten ausgeführt werden, die normalerweise als unsicher gelten. Und diese Risiken nehmen weiter zu, da Finanz-Apps immer mehr sensible Daten verarbeiten und damit Endnutzer und Finanzinstitute dem Betrug und Diebstahl über mobile Geräte aussetzen.

Von Investitionen bis hin zur Vermögensverwaltung, von Zahlungen bis hin zu Kryptowährungen - mobile Finanz-Apps sind ein leichtes Ziel für sogenannte On-Device-Angriffe, da sie auf Geräten außerhalb der Reichweite und Kontrolle der Bank laufen. Erschwerend kommt hinzu, dass böswillige Akteure uneingeschränkten Zugriff auf die Binärdateien der mobilen Banking-Apps und die für das Reverse Engineering erforderlichen Tools haben, da diese frei verfügbar sind. Dies ermöglicht es den Angreifern, die mobilen Banking-Apps zu analysieren und anschließend gezielte Malware und Phishing-Kampagnen zu erstellen und einzusetzen, um Zugangs- und andere Daten der Kunden direkt von den Apps auf den Endgeräten zu stehlen. Angreifer haben wiederholt bewiesen, dass sie in der Lage sind, mobile Apps auf dem Gerät über Sicherheitslücken, gefälschte Wi-Fi-Netzwerke, Phishing und bösartige Apps auszunutzen, was zu Sicherheitsverletzungen, Betrug und Diebstahl führt.

Schlechte Cyber-Hygiene und immer raffiniertere Angriffe gefährden Daten und den gesamten Markenwert. Und die größte Hürde für Finanzunternehmen besteht heute darin, mit einer stark fragmentierten Reihe von Einzelprodukten zu arbeiten, die nur begrenzten bis gar keinen Einblick und Schutz vor realen Laufzeitbedrohungen wie der Kompromittierung von Endbenutzergeräten, Malware und Phishing bieten.



## 3.5

### Mobile Banküberfälle: Die globale wirtschaftliche Bedrohung

#### Wie Zimperium Laufzeit-Exploitation verhindert und Banking-Malware stoppt

Mobile Banking-Anwendungen sind anfällig für Banking-Malware, da die meisten mobilen Banking-Apps nicht in der Lage sind, Bedrohungen auf den Mobiltelefonen zu erkennen und sich wirksam gegen Angriffe und Malware zu schützen.

**Zimperium** hat die branchenführende **Mobile Application Protection Suite (MAPS)** entwickelt, mit der Unternehmen sichere und konforme mobile Anwendungen erstellen können. Die Plattform ermöglicht es den Entwicklern, risikobewusste Anwendungen zu erstellen, die sich gegen verschiedene Angriffe und Malware auf den Geräten der Endbenutzer verteidigen können. Diese leistungsstarke Plattform kombiniert Schwachstellen-Scans, Anwendungsabschirmung und Schlüsselschutz mit zentralem Einblick in Bedrohungen.



Die Mobile Application Protection Suite schützt nachweislich Apps und ihre sensiblen Daten, mildert Angriffe ab und hilft Entwicklern bei der Einhaltung der Sicherheitsvorschriften der Branche. Unser Team verfügt über umfangreiche Erfahrung im Bereich der Sicherheit von Finanz- und Zahlungsanwendungen.

Mit **Zimperiums zDefend** können mobile Anwendungen proaktiv Bedrohungen und Angriffe während der Laufzeit erkennen und sich davor schützen. Mit dieser einzigartigen **RASP-Funktion (Runtime Application Self-Protection)** können mobile Anwendungen Bedrohungen auf Geräteebene in Echtzeit bewerten und dynamisch den Zugriff verhindern oder Funktionen mit hohem Risiko deaktivieren, um Angriffe zu verhindern und Betrug bei mobilen Banking-Anwendungen zu minimieren. Die Erkennungsfunktionen und die damit verbundenen In-App-Abwehrmaßnahmen von zDefend funktionieren unter allen Umständen, selbst wenn keine Netzwerkverbindung besteht, so dass die Schutzmaßnahmen nur sehr schwer zu umgehen sind.

Zimperiums einzigartiger Ansatz zur Laufzeitverteidigung (RASP) schützt auch vor fortgeschrittenen Kompromittierungs- und Ausbeutungstechniken direkt auf dem Gerät (on-device), selbst im Falle von **0-Day-Schwachstellen**. zDefend nutzt z9™, Zimperiums patentierte, auf maschinellem Lernen basierende Mobile Threat Defense (MTD) Engine. Mit dem eingebetteten zDefend kann die Host-App komplexe Verhaltensanomalien auf dem Gerät erkennen und so einen erweiterten Anti-Malware- und Anti-Phishing-Schutz bieten. Die Erkennungsfunktionen von zDefend können Over-The-Air aktualisiert werden, ohne dass die Anwendung über die App-Stores neu erstellt werden muss. So wird ein kontinuierlicher Schutz gewährleistet, ohne dass sich dies auf die Endbenutzer der mobilen Banking-App auswirkt.

Die Fähigkeit, Bedrohungen und Angriffe direkt auf dem Gerät zu erkennen, bietet den Banken eine einzigartige Möglichkeit, die Telemetrie von Bedrohungen in Echtzeit und unter Wahrung der Privatsphäre zu überwachen. Dieser praktische und skalierbare Ansatz ermöglicht es Finanzinstituten, umgehend auf neu entdeckte Bedrohungen und Schwachstellen zu reagieren. Heute wird zDefend weltweit in mehreren Millionen Banking-Apps für Verbraucher eingesetzt.

zDefend lässt sich als Software Development Kit (SDK) leicht in jede iOS- oder Android-Anwendung einbetten und ermöglicht es App-Teams, Security-by-Design-Ansätze als Teil ihrer DevSecOps-Reise zu übernehmen.

# 4.1

## Mobile Banküberfälle: Die globale wirtschaftliche Bedrohung

Zusätzlich zu Zimperium zDefend besteht MAPS aus drei weiteren Funktionen:

**Zimperium zScan** hilft Entwicklern mobiler Apps dabei, Reputations- und finanzielle Risiken in ihrem App-Binary zu erkennen, indem es Datenschutz-, Sicherheits- und Compliance-Risiken im Entwicklungsprozess automatisch identifiziert, bevor Apps für die Öffentlichkeit freigegeben werden.

**Zimperium zShield** stattet Anwendungen mit Selbstverteidigungsfunktionen aus, so dass sie in Zero-Trust-Umgebungen sicher ausgeführt werden können. Es verwendet mehrere Methoden, darunter Code-Verschleierung und Intrusion Detection in Echtzeit (RASP), um Manipulationen, Reverse Engineering und andere Techniken zu verhindern, die von Cyberkriminellen eingesetzt werden, um Schwachstellen zu entdecken und Zugriff auf sensible Informationen und Ressourcen in Finanzdienstleistungsanwendungen zu erhalten.

**Zimperium zKeyBox** verwendet modernste White-Box-Kryptografie, um geheime kryptografische Schlüssel im Code der Anwendung selbst während der Laufzeit gut zu verstecken. Es ist einfach zu integrieren und zu verwenden und bietet einen umfangreichen Satz von High-Level-Klassen und -Methoden für den Umgang mit den gängigsten kryptographischen Algorithmen auf jeder Plattform. Kryptographische Schlüssel erscheinen nie im Klartext.

# Schlussfolgerung

In den letzten zehn Jahren hat die Finanzbranche ihre Bank- und Zahlungsverkehrsdienstleistungen sowie den Aktienhandel vollständig auf mobile Geräte umgestellt. Diese Umstellung bringt zwar mehr Komfort und neue Optionen für die Verbraucher, aber auch neue Betrugsrisiken mit sich. Da mobile Endgeräte von Natur aus unsicher sind und die meisten aktuellen mobilen Banking-Apps sich als anfällig für Banking-Malware erwiesen haben, ist es von entscheidender Bedeutung, die Sicherheit mobiler Banking- und Zahlungs-Apps so zu verbessern, dass sie in der Lage sind, Bedrohungen und Angriffe während der Laufzeit zu erkennen und sich proaktiv davor zu schützen.



## Quellen

1. <https://www.fourmilab.ch/documents/univac/animal.html>
2. [https://www.cs.virginia.edu/~robbins/Malware\\_Goes\\_Mobile.pdf](https://www.cs.virginia.edu/~robbins/Malware_Goes_Mobile.pdf)
3. <https://www.forbes.com/advisor/banking/digital-banking-survey-mobile-app-valuable-features/>
4. <https://www.cashmatters.org/blog/in-the-usa-80-of-teenagers-paid-allowance-receive-cash-ja-2019>
5. <https://gdpr.eu/fines/>
6. <https://www.csoonline.com/article/3410278/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html>
7. <https://www.businesswire.com/news/home/20190917005012/en/New-Global-Research-Shows-Poor-Data-Security>
8. <https://www.ftc.gov/news-events/news/press-releases/2022/02/new-data-shows-ftc-received-28-million-fraud-reports-consumers-2021-0>
9. <https://risk.lexisnexis.com/insights-resources/research/us-ca-true-cost-of-fraud-study>

Erfahren Sie mehr unter: [zimperium.com](https://zimperium.com)

Kontaktieren Sie uns unter: 844.601.6760 | [info@zimperium.com](mailto:info@zimperium.com)



Zimperium, Inc  
4055 Valley View, Dallas, TX 75244, USA

## 4.2

## Mobile Banküberfälle: Die globale wirtschaftliche Bedrohung

## Anhang

| AppName                          | Developer                                       | Country   | Number of Downloads | Android/BianllanBotnet | Coper | Cabassous.D | Eventbot | ExobotCompa<br>ct.D/Octo | FluBot | Medusa | Sharkbot | Teabot | Xenomorph |
|----------------------------------|-------------------------------------------------|-----------|---------------------|------------------------|-------|-------------|----------|--------------------------|--------|--------|----------|--------|-----------|
| Banco BIC, SA                    | Banco BIC, SA                                   | Angola    | 100000              |                        |       |             |          | X                        |        |        |          |        | X         |
| Garanti BBVA Mobile              | T. Garanti Bankasi A.S.                         | Argentina | 10000000            |                        |       |             |          | X                        |        | X      |          |        |           |
| Greater Bank                     | Greater Bank Ltd                                | Australia | 100000              |                        |       | X           |          |                          |        |        |          |        |           |
| Macquarie Mobile Banking         | Macquarie Bank Limited                          | Australia | 100000              |                        |       | X           |          |                          |        |        |          |        |           |
| My AMP                           | AMP Limited                                     | Australia | 100000              |                        |       | X           |          |                          |        |        |          |        |           |
| myRAMS                           | RAMS Financial Group Pty Ltd                    | Australia | 50000               |                        |       | X           |          |                          |        |        |          |        |           |
| ANZ Transactive - Global         | Australia and New Zealand Banking Group Limited | Australia | 5000                |                        |       | X           |          | X                        |        |        |          |        |           |
| Bank of Melbourne Business App   | St.George Bank                                  | Australia | 1000                |                        |       | X           |          | X                        |        |        |          |        |           |
| BankSA Business App              | St.George Bank                                  | Australia | 1000                |                        |       | X           |          | X                        |        |        |          |        |           |
| CommBiz                          | Commonwealth Bank of Australia                  | Australia | 10000               |                        |       | X           |          | X                        |        |        |          |        |           |
| HSBC Australia                   | HSBC                                            | Australia | 100000              |                        |       | X           |          | X                        |        |        |          |        |           |
| St.George Business App           | St.George Bank                                  | Australia | 5000                |                        |       | X           |          | X                        |        |        |          |        |           |
| Westpac Corporate Mobile         | Westpac Banking Corporation                     | Australia | 10000               |                        |       | X           |          | X                        |        |        |          |        |           |
| Bank Australia App               | Bank Australia Limited                          | Australia | 50000               |                        | X     | X           |          | X                        |        |        |          |        |           |
| Beyond Bank Australia            | Beyond Bank Australia                           | Australia | 100000              |                        | X     | X           |          | X                        |        |        |          | X      |           |
| ANZ Australia                    | Australia and New Zealand Banking Group Limited | Australia | 1000000             |                        | X     | X           |          | X                        |        |        |          | X      |           |
| Bank of Melbourne Mobile Banking | St.George Bank                                  | Australia | 100000              |                        | X     | X           |          | X                        |        |        |          | X      |           |
| BankSA Mobile Banking            | St.George Bank                                  | Australia | 100000              |                        | X     | X           |          | X                        |        |        |          | X      |           |
| Bankwest                         | Bankwest                                        | Australia | 500000              |                        | X     | X           |          | X                        |        |        |          | X      |           |
| Bendigo Bank                     | Bendigo and Adelaide Bank Ltd                   | Australia | 500000              |                        | X     | X           |          | X                        |        |        |          | X      |           |
| BOQ Mobile                       | BOQ                                             | Australia | 100000              |                        | X     | X           |          | X                        |        |        |          | X      |           |
| CommBank                         | Commonwealth Bank of Australia                  | Australia | 5000000             |                        | X     | X           |          | X                        |        |        |          | X      |           |
| St.George Mobile Banking         | St.George Bank                                  | Australia | 1000000             |                        | X     | X           |          | X                        |        |        |          | X      |           |
| Westpac                          | Westpac Banking Corporation                     | Australia | 1000000             |                        | X     | X           |          | X                        |        |        |          | X      |           |
| Great Southern Bank Australia    | Credit Union Australia                          | Australia | 100000              |                        |       | X           |          | X                        |        |        |          | X      |           |
| ME Bank                          | ME Bank                                         | Australia | 100000              |                        |       | X           |          |                          |        |        |          | X      |           |

[illegible]

[illegible]

## Mobile Banküberfälle: Die globale wirtschaftliche Bedrohung

| AppName                                        | Developer                                        | Country        | Number of Downloads | Android/<br>BianlianBotnet | Coper | Cabassous.D | Eventbot | ExobotCompa<br>ct.D/Octo | FluBot | Medusa | Sharkbot | Teabot | Xenomorph |
|------------------------------------------------|--------------------------------------------------|----------------|---------------------|----------------------------|-------|-------------|----------|--------------------------|--------|--------|----------|--------|-----------|
| m-zaba                                         | Zagrebačka banka d.d.                            | Croatia        | 500000              |                            |       |             |          |                          |        |        |          | X      |           |
| mHPB                                           | Hrvatska poštanska banka, dioničko društvo       | Croatia        | 100000              |                            |       |             |          |                          |        |        |          | X      |           |
| PBZ mobile banking application                 | Privredna banka Zagreb d.d.                      | Croatia        | 500000              |                            |       |             |          |                          |        |        |          | X      |           |
| Home Credit SK                                 | Home Credit a.s.                                 | Czech Republic | 50000               |                            |       |             |          |                          |        |        |          | X      |           |
| Oberbank                                       | Oberbank AG                                      | Czech Republic | 100000              |                            |       |             |          |                          |        |        |          | X      |           |
| SmartBanking SK                                | UniCredit Bank Czech Republic and Slovakia, a.s. | Czech Republic | 100000              |                            |       |             |          |                          |        |        |          | X      |           |
| Mobilni Banka                                  | Komerční banka, a.s.                             | Czechia        | 1000000             |                            |       |             |          | X                        |        |        |          |        |           |
| AL-Bank                                        | BEC a.m.b.a.                                     | Denmark        | 100000              |                            |       |             |          |                          |        |        |          | X      |           |
| Jyske Bank                                     | Jyske Bank                                       | Denmark        | 100000              |                            |       |             |          |                          |        |        |          | X      |           |
| Lunar                                          | Lunar A/S                                        | Denmark        | 500000              |                            |       |             |          |                          |        |        |          | X      |           |
| Ringkjøbing Landbobank og Nordjyske Bank       | Ringkjøbing Landbobank                           | Denmark        | 10000               |                            |       |             |          |                          |        |        |          | X      |           |
| Spar Nord Mobilbank                            | BEC a.m.b.a.                                     | Denmark        | 100000              |                            |       |             |          |                          |        |        |          | X      |           |
| Sydbanks Mobilbank Privat                      | Sydbank                                          | Denmark        | 50000               |                            |       |             |          |                          |        |        |          | X      |           |
| Vestjysk Bank                                  | BEC a.m.b.a.                                     | Denmark        | 50000               |                            |       |             |          |                          |        |        |          | X      |           |
| Zonda - crypto exchange                        | BB Trade Estonia                                 | Estonia        | 100000              |                            |       |             |          | X                        |        |        |          |        |           |
| Coop Pank                                      | Coop Pank AS                                     | Estonia        | 10000               |                            |       |             |          |                          |        |        |          | X      |           |
| LHV                                            | AS LHV Pank                                      | Estonia        | 100000              |                            |       |             |          |                          |        |        |          | X      |           |
| SEB Estonia                                    | Skandinaviska Enskilda Banken AB (publ)          | Estonia        | 100000              |                            |       |             |          |                          |        |        |          | X      |           |
| Smart-ID                                       | SK ID Solutions AS                               | Estonia        | 1000000             |                            |       |             |          |                          |        |        |          | X      |           |
| Nordea Mobile - Denmark                        | Nordea Bank Abp                                  | Finland        | 500000              |                            |       |             |          |                          |        |        |          | X      |           |
| Nordea Mobile - Sweden                         | Nordea Bank Abp                                  | Finland        | 1000000             |                            |       |             |          |                          |        |        |          | X      |           |
| Banque de Savoie                               | BANQUE POPULAIRE                                 | France         | 10000               |                            |       |             |          | X                        |        |        |          |        |           |
| Banque Populaire PRO                           | BANQUE POPULAIRE                                 | France         | 100000              |                            |       |             |          | X                        |        |        |          |        |           |
| CMSO suivi de compte et budget                 | Credit Mutuel Sud Ouest                          | France         | 100000              |                            |       |             |          | X                        |        |        |          |        |           |
| Fortuneo, mes comptes banque & bourse en ligne | Fortuneo                                         | France         | 100000              |                            |       |             |          | X                        |        |        |          |        |           |
| La Banque Postale                              | La Banque Postale                                | France         | 10000000            |                            |       |             |          | X                        |        |        |          |        |           |
| La Poste - Services Postaux : colis & courrier | La Poste                                         | France         | 1000000             |                            |       |             |          | X                        |        |        |          |        |           |
| Ma Banque                                      | CREDIT AGRICOLE TECHNOLOGIES ET SERVICES         | France         | 10000000            |                            |       |             |          | X                        |        |        |          |        |           |
| Ma Banque Entreprise                           | BNP PARIBAS                                      | France         | 10000               |                            |       |             |          | X                        |        |        |          |        |           |
| Mes Comptes - LCL                              | LCL - Le Crédit Lyonnais                         | France         | 1000000             |                            |       |             |          | X                        |        |        |          |        |           |
| Oney France : suivez vos achats                | Oney France                                      | France         | 1000000             |                            |       |             |          | X                        |        |        |          |        |           |
| Paiement mobile CA                             | Crédit Agricole S.A.                             | France         | 1000000             |                            |       |             |          | X                        |        |        |          |        |           |
| Pro & Entreprises LCL                          | LCL - Le Crédit Lyonnais                         | France         | 10000               |                            |       |             |          | X                        |        |        |          |        |           |

[illegible]

## Mobile Banküberfälle: Die globale wirtschaftliche Bedrohung

| AppName                                       | Developer                                      | Country | Number of Downloads | Android/BianlianBotnet | Coper | Cabassous.D | Eventbot | ExobotCompa<br>ct.D/Octo | FluBot | Medusa | Sharkbot | Teabot | Xenomorph |
|-----------------------------------------------|------------------------------------------------|---------|---------------------|------------------------|-------|-------------|----------|--------------------------|--------|--------|----------|--------|-----------|
| myAlpha Mobile                                | Alpha Bank                                     | Greece  | 1000000             |                        |       |             |          |                          |        |        |          | X      |           |
| NBG Mobile Banking                            | National Bank of Greece S.A.                   | Greece  | 1000000             |                        |       |             |          |                          |        |        |          | X      |           |
| Viva Wallet                                   | Viva Wallet Holdings - Software Development SA | Greece  | 100000              |                        |       |             |          |                          |        |        |          | X      |           |
| Winbank Mobile                                | Piraeus Bank S.A.                              | Greece  | 1000000             |                        |       |             |          |                          |        |        |          | X      |           |
| CIB Business Online                           | CIB Bank                                       | Hungary | 1000                |                        |       |             |          | X                        |        |        |          |        |           |
| Erste Business MobilBank                      | Erste Bank Hungary Zrt.                        | Hungary | 10000               |                        |       |             |          | X                        |        |        |          |        |           |
| CIB Bank                                      | CIB Bank                                       | Hungary | 100000              |                        |       |             |          | X                        |        |        |          | X      |           |
| K&H mobilbank                                 | K&H Bank Zrt.                                  | Hungary | 500000              |                        |       |             |          | X                        |        |        |          | X      |           |
| MKB Mobil App (ex BB)                         | MKB BANK Nyrt.                                 | Hungary | 100000              |                        |       |             |          | X                        |        |        |          | X      |           |
| MKB Mobilalkalmazás                           | MKB BANK Nyrt.                                 | Hungary | 100000              |                        |       |             |          | X                        |        |        |          | X      |           |
| OTP SmartBank                                 | OTP Bank Nyrt.                                 | Hungary | 1000000             |                        |       |             |          | X                        |        |        |          | X      |           |
| GRÁNIT eBank                                  | GRÁNIT Bank Zrt.                               | Hungary | 10000               |                        |       |             |          |                          |        |        |          | X      |           |
| OTP Bank HU                                   | OTP Bank Nyrt.                                 | Hungary |                     |                        |       |             |          |                          |        |        |          | X      |           |
| OTP mobile banking HR                         | OTP banka powered by Asseco SEE                | Hungary | 100000              |                        |       |             |          |                          |        |        |          | X      |           |
| OTP SZÉP Card                                 | OTP Bank Nyrt.                                 | Hungary | 500000              |                        |       |             |          |                          |        |        |          | X      |           |
| OTP Bank HU                                   | OTP Bank Nyrt.                                 | Hungary | 1000000             |                        |       |             |          |                          |        |        |          | X      |           |
| PhonePe: UPI, Recharge, Investment, Insurance | PhonePe                                        | India   | 100000000           |                        |       |             |          |                          |        |        |          | X      |           |
| Wexopay Crypto Payments                       | WEXO                                           | India   | 50000               |                        |       |             |          |                          |        |        |          | X      |           |
| permanent tsb                                 | permanent tsb                                  | Ireland | 500000              |                        |       | X           |          | X                        |        |        |          |        |           |
| Discount Bank                                 | Israel Discount Bank Ltd.                      | Israel  | 1000000             |                        |       |             |          | X                        |        |        |          |        |           |
| בנק יחב - ניהול חשבון                         | Bank Yahav                                     | Israel  | 100000              |                        |       |             |          | X                        |        |        |          |        |           |
| הבנק הבינלאומי                                | הבנק הבינלאומי                                 | Israel  | 100000              |                        |       |             |          | X                        |        |        |          |        |           |
| לאומי                                         | Bank Leumi                                     | Israel  | 1000000             |                        |       |             |          | X                        |        |        |          |        |           |
| Intesa Sanpaolo Business                      | Intesa Sanpaolo SPA                            | Italy   | 100000              |                        |       |             | X        |                          |        |        |          |        |           |
| Intesa Sanpaolo Private                       | Intesa Sanpaolo SPA                            | Italy   | 100000              |                        |       |             | X        |                          |        |        |          |        |           |
| Inbank                                        | Allitude Spa                                   | Italy   | 500000              |                        |       |             | X        |                          |        |        |          | X      |           |
| RelaxBanking Mobile                           | BCC Sistemi Informatici S.p.A.                 | Italy   | 1000000             |                        |       |             | X        |                          |        |        |          | X      |           |
| Mediolanum                                    | Banca Mediolanum                               | Italy   | 500000              |                        |       |             | X        | X                        |        |        |          | X      |           |
| ING Italia                                    | ING BANK N.V. Milan Branch                     | Italy   | 1000000             |                        |       |             |          | X                        |        |        |          | X      |           |
| Banca MPS                                     | Banca Monte dei Paschi di Siena                | Italy   | 1000000             |                        |       |             | X        | X                        |        | X      |          | X      |           |
| BancoPosta                                    | Poste Italiane S.p.A.                          | Italy   | 5000000             |                        |       |             | X        | X                        |        | X      |          | X      |           |
| Intesa Sanpaolo Mobile                        | Intesa Sanpaolo SPA                            | Italy   | 5000000             |                        |       |             | X        | X                        |        | X      |          | X      |           |
| Bancaperta                                    | Creval S.p.A.                                  | Italy   | 100000              |                        |       |             |          | X                        |        | X      |          | X      |           |
| BNL                                           | BNL S.p.A.                                     | Italy   | 1000000             |                        |       |             |          | X                        |        | X      |          | X      |           |
| Carige Mobile                                 | Gruppo Banca Carige                            | Italy   | 100000              |                        |       |             |          | X                        |        | X      |          | X      |           |
| myCartaBCC                                    | Iccrea Banca SPA                               | Italy   | 500000              |                        |       |             |          | X                        |        | X      |          | X      |           |

[illegible]

## Mobile Banküberfälle: Die globale wirtschaftliche Bedrohung

| AppName                        | Developer                                | Country     | Number of Downloads | Android/<br>BianlianBotnet | Coper | Cabassous.D | Eventbot | ExobotCompa<br>ct.D/Octo | FluBot | Medusa | Sharkbot | Teabot | Xenomorph |
|--------------------------------|------------------------------------------|-------------|---------------------|----------------------------|-------|-------------|----------|--------------------------|--------|--------|----------|--------|-----------|
| BTA Lietuva                    | BTA Baltic Insurance Company             | Latvia      | 5000                |                            |       |             |          |                          |        |        |          | X      |           |
| myTU - Mobile Banking          | Travel Union, UAB                        | Lithuania   | 10000               |                            |       |             |          |                          |        |        |          | X      |           |
| Paysera Mobile Wallet          | Paysera LT, JSC                          | Lithuania   | 1000000             |                            |       |             |          |                          |        |        |          | X      |           |
| Perlas Go                      | Sąskaitų apmokėjimas ir įmokos           | Lithuania   | 100000              |                            |       |             |          |                          |        |        |          | X      |           |
| SEB Lithuania                  | Skandinaviska Enskilda Banken AB (publ)  | Lithuania   | 500000              |                            |       |             |          |                          |        |        |          | X      |           |
| Šiaulių bankas                 | AB Šiaulių bankas                        | Lithuania   | 50000               |                            |       |             |          |                          |        |        |          | X      |           |
| Viena Sąskaita                 | Viena sąskaita                           | Lithuania   | 100000              |                            |       |             |          |                          |        |        |          | X      |           |
| AmOnline                       | AmBank (M) Berhad                        | Malaysia    | 1000000             |                            |       |             |          | X                        |        |        |          |        |           |
| PB engage MY                   | Public Bank Berhad                       | Malaysia    | 1000000             |                            |       |             |          | X                        |        |        |          |        |           |
| Binance: Buy BTC & 600+ Crypto | Binance Inc.                             | Malta       | 50000000            |                            |       |             |          | X                        |        |        | X        | X      |           |
| BBVA México                    | BBVA                                     | Mexico      | 10000000            |                            |       |             |          |                          | X      |        |          |        |           |
| Pocket Bank                    | Banque Centrale Populaire                | Morocco     | 1000000             |                            |       |             |          | X                        |        |        |          |        |           |
| ABN AMRO                       | ABN AMRO Bank N.V.                       | Netherlands | 1000000             |                            |       |             |          |                          |        |        |          | X      |           |
| ASN Mobiel Bankieren           | ASN Bank                                 | Netherlands | 100000              |                            |       |             |          |                          |        |        |          | X      |           |
| Bitvavo   Buy Bitcoin & Crypto | Bitvavo B.V.                             | Netherlands | 500000              |                            |       |             |          |                          |        |        |          | X      |           |
| BLOX Crypto & Bitcoin Trading  | weareblox                                | Netherlands | 100000              |                            |       |             |          |                          |        |        |          | X      |           |
| bunq - bank of The Free        | bunq                                     | Netherlands | 1000000             |                            |       |             |          |                          |        |        |          | X      |           |
| ING Bankieren                  | ING NV                                   | Netherlands | 5000000             |                            |       |             |          |                          |        |        |          | X      |           |
| Knab Bankieren                 | Knab                                     | Netherlands | 100000              |                            |       |             |          |                          |        |        |          | X      |           |
| LiteBit – Buy Bitcoin & crypto | 2525 Ventures BV                         | Netherlands | 100000              |                            |       |             |          |                          |        |        |          | X      |           |
| RegioBank - Mobiel Bankieren   | RegioBank                                | Netherlands | 100000              |                            |       |             |          |                          |        |        |          | X      |           |
| SNS Mobiel Bankieren           | SNS Bank                                 | Netherlands | 500000              |                            |       |             |          |                          |        |        |          | X      |           |
| Triodos Bankieren NL           | Triodos Bank                             | Netherlands | 100000              |                            |       |             |          |                          |        |        |          | X      |           |
| ING Banking                    | ING Belgium NV                           | Netherlands | 1000000             |                            |       |             |          | X                        |        |        |          |        | X         |
| ANZ goMoney New Zealand        | ANZ NZ                                   | New Zealand | 1000000             |                            |       | X           |          |                          |        |        |          | X      |           |
| ASB Mobile Banking             | ASB Bank Limited                         | New Zealand | 1000000             |                            |       | X           |          | X                        |        |        |          | X      |           |
| Kiwibank Mobile Banking        | Kiwibank Ltd.                            | New Zealand | 500000              |                            |       | X           |          |                          |        |        |          | X      |           |
| BNZ Mobile                     | Bank of New Zealand                      | New Zealand | 500000              |                            |       |             |          |                          |        |        |          | X      |           |
| The Co-operative Bank (NZ)     | The Co-operative Bank (NZ)               | New Zealand | 100000              |                            |       |             |          |                          |        |        |          | X      |           |
| Unity Money                    | New Zealand Association of Credit Unions | New Zealand | 5000                |                            |       |             |          |                          |        |        |          | X      |           |
| GTBank                         | Guaranty Trust Bank                      | Nigeria     | 1000000             |                            |       |             |          |                          |        |        |          | X      |           |
| Santander Sverige - Mobilbank  | Santander Consumer Bank AS               | Norway      | 50000               |                            |       |             |          |                          |        |        |          | X      |           |
| BusinessPro Lite               | Alior Bank S.A.                          | Poland      | 100000              |                            |       |             |          | X                        |        |        |          |        |           |
| iBiznes24 mobile               | Santander Bank Polska S.A.               | Poland      | 10000               |                            |       |             |          | X                        |        |        |          |        |           |
| ING Business                   | ING Bank Slaski S.A.                     | Poland      | 100000              |                            |       |             |          | X                        |        |        |          |        |           |

## Mobile Banküberfälle: Die globale wirtschaftliche Bedrohung

| AppName                                       | Developer                              | Country  | Number of Downloads | Android/BianlianBotnet | Coper | Cabassous.D | Eventbot | ExobotCompa<br>ct.D/Octo | FluBot | Medusa | Sharkbot | Teabot | Xenomorph |
|-----------------------------------------------|----------------------------------------|----------|---------------------|------------------------|-------|-------------|----------|--------------------------|--------|--------|----------|--------|-----------|
| iPKO biznes                                   | PKO Bank Polski SA                     | Poland   | 100000              |                        |       |             |          | X                        |        |        |          |        |           |
| Moje ING mobile                               | ING Bank Slaski S.A.                   | Poland   | 1000000             |                        |       |             |          | X                        |        |        |          |        |           |
| Nest Bank                                     | Nest Bank                              | Poland   | 100000              |                        |       |             |          | X                        |        |        |          |        |           |
| Pekao24Makler                                 | Bank Pekao SA                          | Poland   | 500000              |                        |       |             |          | X                        |        |        |          |        |           |
| PekaoBiznes24                                 | Bank Pekao SA                          | Poland   | 50000               |                        |       |             |          | X                        |        |        |          |        |           |
| plusbank24                                    | PLUS BANK S.A.                         | Poland   | 1000000             |                        |       |             |          | X                        |        |        |          |        |           |
| Santander mobile                              | Santander Bank Polska S.A.             | Poland   | 1000000             |                        |       |             |          | X                        |        |        |          |        |           |
| Santander                                     | Banco Santander                        | Poland   | 5000000             |                        | X     |             |          | X                        | X      | X      |          |        |           |
| ABANCA - Mobile Banking                       | ABANCA Corporación Bancaria, S.A       | Portugal | 10000               |                        |       |             |          | X                        |        |        |          |        |           |
| ABANCA Empresas                               | ABANCA Corporación Bancaria, S.A       | Portugal | 10000               |                        |       |             |          | X                        |        |        |          |        |           |
| Banco CTT                                     | Banco CTT, S.A.                        | Portugal | 100000              |                        |       |             |          | X                        |        |        |          |        |           |
| Bankinter Portugal                            | BANKINTER, S.A. - SUCURSAL EM PORTUGAL | Portugal | 100000              |                        |       |             |          | X                        |        |        |          |        |           |
| Best Bank                                     | Banco Best                             | Portugal | 10000               |                        |       |             |          | X                        |        |        |          |        |           |
| Caderneta                                     | Caixa Geral de Depósitos, SA           | Portugal | 50000               |                        |       |             |          | X                        |        |        |          |        |           |
| Caixadirecta Empresas                         | Caixa Geral de Depósitos, SA           | Portugal | 50000               |                        |       |             |          | X                        |        |        |          |        |           |
| EuroBic Mobile App                            | Banco BIC Português, S.A.              | Portugal | 10000               |                        |       |             |          | X                        |        |        |          |        |           |
| MY ATLANTICO                                  | Banco ATLANTICO Europa                 | Portugal | 50000               |                        |       |             |          | X                        |        |        |          |        |           |
| novobanco                                     | NOVO BANCO, S.A                        | Portugal | 100000              |                        |       |             |          | X                        |        |        |          |        |           |
| Oney Portugal                                 | Oney Bank - Sucursal em Portugal       | Portugal | 100000              |                        |       |             |          | X                        |        |        |          |        |           |
| Santander Empresas Portugal                   | Banco Santander Totta S.A.             | Portugal | 100000              |                        |       |             |          | X                        |        |        |          |        |           |
| Santander Particulares                        | Banco Santander Totta S.A.             | Portugal | 1000000             |                        |       |             |          | X                        |        |        |          |        |           |
| Santander Portugal                            | Banco Santander Totta S.A.             | Portugal | 500000              |                        |       |             |          | X                        |        |        |          |        |           |
| Wizink. Um banco. Infinitas possibilidades    | © WiZink Bank, S.A.U.                  | Portugal | 100000              |                        |       |             |          | X                        |        |        |          |        |           |
| WiZink, tu banco senZillo                     | © WiZink Bank, S.A.U.                  | Portugal | 500000              |                        |       |             | X        | X                        |        |        |          |        | X         |
| ABANCA Pay - Paga y envía dinero con el móvil | ABANCA Corporación Bancaria, S.A       | Portugal | 100000              |                        |       |             |          | X                        |        | X      |          |        |           |
| //ABANCA                                      | ABANCA Corporación Bancaria, S.A       | Portugal | 1000000             |                        |       |             |          | X                        |        | X      |          |        |           |
| Pera Algo Wallet                              | Pera Wallet                            | Portugal | 100000              |                        |       |             |          |                          |        |        |          | X      |           |
| Millenniumbcp                                 | Millenniumbcp                          | Portugal | 1000000             |                        |       |             |          |                          |        |        |          |        | X         |
| ABANCA - Portugal                             | ABANCA Corporación Bancaria, S.A       | Portugal | 10000               |                        |       |             |          | X                        |        |        |          |        | X         |
| BBVA Portugal                                 | BBVA                                   | Portugal | 10000               |                        |       |             |          | X                        |        |        |          |        | X         |
| BPI APP                                       | Banco BPI, S.A.                        | Portugal | 500000              |                        |       |             |          | X                        |        |        |          |        | X         |
| CA Mobile                                     | Crédito Agrícola                       | Portugal | 100000              |                        |       |             |          | X                        |        |        |          |        | X         |
| Caixadirecta                                  | Caixa Geral de Depósitos, SA           | Portugal | 1000000             |                        |       |             |          | X                        |        |        |          |        | X         |
| MB WAY                                        | SIBS FORWARD PAYMENT SOLUTIONS         | Portugal | 1000000             |                        |       |             |          | X                        |        |        |          |        | X         |
| NB smart app                                  | NOVO BANCO, S.A                        | Portugal | 500000              |                        |       |             |          | X                        |        |        |          |        | X         |

[illegible]

[illegible]

## Mobile Banküberfälle: Die globale wirtschaftliche Bedrohung

| AppName                                  | Developer                               | Country     | Number of Downloads | Android/BianlianBotnet | Coper | Cabassous.D | Eventbot | ExobotCompa<br>ct.D/Octo | FluBot | Medusa | Sharkbot | Teabot | Xenomorph |
|------------------------------------------|-----------------------------------------|-------------|---------------------|------------------------|-------|-------------|----------|--------------------------|--------|--------|----------|--------|-----------|
| Mobilbank DK – Danske Bank               | Danske Bank                             | Sweden      | 500000              |                        |       |             |          |                          |        |        |          | X      |           |
| Mobile Bank UK – Danske Bank             | Danske Bank                             | Sweden      | 100000              |                        |       |             |          |                          |        |        |          | X      |           |
| Nordnet                                  | Nordnet Bank AB                         | Sweden      | 500000              |                        |       |             |          |                          |        |        |          | X      |           |
| Qliro                                    | Qliro Ab                                | Sweden      | 500000              |                        |       |             |          |                          |        |        |          | X      |           |
| Resurs                                   | Resurs Bank                             | Sweden      | 100000              |                        |       |             |          |                          |        |        |          | X      |           |
| Rocker                                   | Rocker AB (publ)                        | Sweden      | 100000              |                        |       |             |          |                          |        |        |          | X      |           |
| Savings Bank private                     | Sparbankernas Service AB                | Sweden      | 1000000             |                        |       |             |          |                          |        |        |          | X      |           |
| SBAB                                     | SBAB                                    | Sweden      | 100000              |                        |       |             |          |                          |        |        |          | X      |           |
| SEB                                      | Skandinaviska Enskilda Banken AB (publ) | Sweden      | 500000              |                        |       |             |          |                          |        |        |          | X      |           |
| Skandia och Skandiabanken                | Skandiabanken AB (publ)                 | Sweden      | 100000              |                        |       |             |          |                          |        |        |          | X      |           |
| Svea - banken för dig                    | Svea Bank AB                            | Sweden      | 50000               |                        |       |             |          |                          |        |        |          | X      |           |
| Swedbank Eestis                          | Swedbank                                | Sweden      | 500000              |                        |       |             |          |                          |        |        |          | X      |           |
| Swedbank Latvia                          | Swedbank                                | Sweden      | 500000              |                        |       |             |          |                          |        |        |          | X      |           |
| Swedbank Lietuva                         | Swedbank                                | Sweden      | 1000000             |                        |       |             |          |                          |        |        |          | X      |           |
| Swedbank private                         | Swedbank AB (publ)                      | Sweden      | 1000000             |                        |       |             |          |                          |        |        |          | X      |           |
| Bank Cler Zak                            | Bank Cler                               | Switzerland | 100000              |                        |       |             |          |                          |        |        |          | X      |           |
| BCV Mobile                               | Banque Cantonale Vaudoise               | Switzerland | 100000              |                        |       |             |          |                          |        |        |          | X      |           |
| Credit Suisse – CSX                      | Credit Suisse Group AG                  | Switzerland | 100000              |                        |       |             |          |                          |        |        |          | X      |           |
| Credit Suisse TWINT – mobile payment app | Credit Suisse Group AG                  | Switzerland | 100000              |                        |       |             |          |                          |        |        |          | X      |           |
| eBanking Mobile                          | Zürcher Kantonalbank                    | Switzerland | 100000              |                        |       |             |          |                          |        |        |          | X      |           |
| FlowBank App   Online Trading            | FlowBank                                | Switzerland | 50000               |                        |       |             |          |                          |        |        |          | X      |           |
| frankly. Pillar 3a.                      | Zürcher Kantonalbank                    | Switzerland | 100000              |                        |       |             |          |                          |        |        |          | X      |           |
| MyAXA CH                                 | AXA Schweiz                             | Switzerland | 100000              |                        |       |             |          |                          |        |        |          | X      |           |
| neon - your account app                  | neon Switzerland AG                     | Switzerland | 100000              |                        |       |             |          |                          |        |        |          | X      |           |
| Nexo: Buy BTC, ETH, SOL & AVAX           | Nexo Capital Inc                        | Switzerland | 1000000             |                        |       |             |          |                          |        |        |          | X      |           |
| PostFinance App                          | PostFinance AG                          | Switzerland | 1000000             |                        |       |             |          |                          |        |        |          | X      |           |
| PostFinance TWINT                        | PostFinance AG                          | Switzerland | 500000              |                        |       |             |          |                          |        |        |          | X      |           |
| Raiffeisen E-Banking                     | Raiffeisen Schweiz Genossenschaft       | Switzerland | 500000              |                        |       |             |          |                          |        |        |          | X      |           |
| Raiffeisen TWINT                         | Raiffeisen Schweiz Genossenschaft       | Switzerland | 500000              |                        |       |             |          |                          |        |        |          | X      |           |
| SwissBorg: Invest in Crypto              | SwissBorg                               | Switzerland | 100000              |                        |       |             |          |                          |        |        |          | X      |           |
| UBS Access: Secure login                 | UBS AG                                  | Switzerland | 500000              |                        |       |             |          |                          |        |        |          | X      |           |
| UBS Mobile Banking                       | UBS AG                                  | Switzerland | 500000              |                        |       |             |          |                          |        |        |          | X      |           |
| Valora - Crypto Wallet                   | Valora Inc                              | Switzerland | 100000              |                        |       |             |          |                          |        |        |          | X      |           |
| ZKB TWINT                                | Zürcher Kantonalbank                    | Switzerland | 100000              |                        |       |             |          |                          |        |        |          | X      |           |
| Bitfinex: Trade Digital Assets           | Bitfinex                                | Taiwan      | 100000              |                        |       |             |          | X                        |        |        |          |        |           |
| Albaraka Mobile Banking                  | Albaraka Türk Katılım Bankası A.Ş.      | Turkey      | 500000              |                        |       |             |          | X                        |        |        |          |        |           |
| Alternatif Bank Mobil                    | Alternatif Bank                         | Turkey      | 100000              |                        |       |             |          | X                        |        |        |          |        |           |

## Mobile Banküberfälle: Die globale wirtschaftliche Bedrohung

| AppName                                 | Developer                                         | Country              | Number of Downloads | Android/BianlianBotnet | Coper | Cabassous.D | Eventbot | ExobotCompa<br>ct.D/Octo | FluBot | Medusa | Sharkbot | Teabot | Xenomorph |
|-----------------------------------------|---------------------------------------------------|----------------------|---------------------|------------------------|-------|-------------|----------|--------------------------|--------|--------|----------|--------|-----------|
| Anadolubank Mobil                       | Anadolubank                                       | Turkey               | 50000               |                        |       |             |          | X                        |        |        |          |        |           |
| CEPTETEB İŞTE                           | Türk Ekonomi Bankası A.Ş.                         | Turkey               | 100000              |                        |       |             |          | X                        |        |        |          |        |           |
| Enpara.com Şirketim Cep Şubesi          | QNB Finansbank A.Ş.                               | Turkey               | 100000              |                        |       |             |          | X                        |        |        |          |        |           |
| fastPay                                 | fastPay Elektronik Para ve Ödeme Hizmetleri A.Ş.  | Turkey               | 1000000             |                        |       |             |          | X                        |        |        |          |        |           |
| Fibabanka Corporate Mobile              | Fibabanka A. Ş.                                   | Turkey               | 100000              |                        |       |             |          | X                        |        |        |          |        |           |
| HSBC Turkey                             | HSBC                                              | Turkey               | 500000              |                        |       |             |          | X                        |        |        |          |        |           |
| ING Mobil                               | ING Turkey                                        | Turkey               | 5000000             |                        |       |             |          | X                        |        |        |          |        |           |
| ininal                                  | Ininal                                            | Turkey               | 5000000             |                        |       |             |          | X                        |        |        |          |        |           |
| Maximum İşyerim                         | Türkiye İş Bankası A.Ş.                           | Turkey               | 100000              |                        |       |             |          | X                        |        |        |          |        |           |
| Mobile Branch                           | Vakıf Katılım Bankası A.Ş.                        | Turkey               | 100000              |                        |       |             |          | X                        |        |        |          |        |           |
| N Kolay                                 | Aktif Yatırım Bankası A.Ş.                        | Turkey               | 500000              |                        |       |             |          | X                        |        |        |          |        |           |
| Papara                                  | PAPARA                                            | Turkey               | 5000000             |                        |       |             |          | X                        |        |        |          |        |           |
| Param                                   | TURK Elektronik Para A.Ş.                         | Turkey               | 100000              |                        |       |             |          | X                        |        |        |          |        |           |
| Paribu   Bitcoin-Kripto Para Alım Satım | PARIBU                                            | Turkey               | 1000000             |                        |       |             |          | X                        |        |        |          |        |           |
| PeP: Para Transferi Sanal Kart          | Paladyum Elektronik Para ve Ödeme Hizmetleri A.Ş. | Turkey               | 1000000             |                        |       |             |          | X                        |        |        |          |        |           |
| PTTBank                                 | T.C. Posta ve Telgraf Teşkilatı Genel Müdürlüğü   | Turkey               | 1000000             |                        |       |             |          | X                        |        |        |          |        |           |
| ŞEKER MOBİL                             | Şekerbank                                         | Turkey               | 500000              |                        |       |             |          | X                        |        |        |          |        |           |
| Türkiye Finans Mobile Branch            | Türkiye Finans Katılım Bankası                    | Turkey               | 1000000             |                        |       |             |          | X                        |        |        |          |        |           |
| Akbank                                  | AKBANK                                            | Turkey               | 10000000            |                        |       |             |          | X                        |        | X      |          |        |           |
| CEPTETEB                                | Türk Ekonomi Bankası A.Ş.                         | Turkey               | 5000000             |                        |       |             |          | X                        |        | X      |          |        |           |
| Enpara.com Cep Şubesi                   | QNB Finansbank A.Ş.                               | Turkey               | 1000000             |                        |       |             |          | X                        |        | X      |          |        |           |
| Halkbank Mobil                          | T. HALK BANKASI A.S.                              | Turkey               | 10000000            |                        |       |             |          | X                        |        | X      |          |        |           |
| HSBC Türkiye                            | HSBC                                              | Turkey               | 10000               |                        |       |             |          | X                        |        | X      |          |        |           |
| İşCep - Mobile Banking                  | Türkiye İş Bankası A.Ş.                           | Turkey               | 10000000            |                        |       |             |          | X                        |        | X      |          |        |           |
| Katılım Mobil                           | Ziraat Katılım Bankası A.Ş.                       | Turkey               | 500000              |                        |       |             |          | X                        |        | X      |          |        |           |
| Kuveyt Türk Mobile                      | Kuveyt Türk Katılım Bankası A.Ş.                  | Turkey               | 1000000             |                        |       |             |          | X                        |        | X      |          |        |           |
| MobilDeniz                              | DenizBank                                         | Turkey               | 5000000             |                        |       |             |          | X                        |        | X      |          |        |           |
| Odeabank                                | Odeabank A.Ş.                                     | Turkey               | 500000              |                        |       |             |          | X                        |        | X      |          |        |           |
| QNB Finansbank                          | QNB Finansbank A.Ş.                               | Turkey               | 10000000            |                        |       |             |          | X                        |        | X      |          |        |           |
| VakıfBank Mobil Bankacılık              | Türkiye Vakıflar Bankası T.A.O.                   | Turkey               | 10000000            |                        |       |             |          | X                        |        | X      |          |        |           |
| Yapı Kredi Mobile                       | Yapı ve Kredi Bankası A.Ş.                        | Turkey               | 10000000            |                        |       |             |          | X                        |        | X      |          |        |           |
| Mashreq UAE                             | Mashreq                                           | United Arab Emirates | 500000              |                        |       | X           |          |                          |        |        |          |        |           |
| ADCB                                    | Abu Dhabi Commercial Bank                         | United Arab Emirates | 1000000             |                        |       | X           |          |                          |        |        |          | X      |           |
| CBD - Instant digital banking           | Commercial Bank of Dubai                          | United Arab Emirates | 500000              |                        |       | X           |          |                          |        |        |          | X      |           |

## Mobile Banküberfälle: Die globale wirtschaftliche Bedrohung

| AppName                                           | Developer                     | Country              | Number of Downloads | Android/BianlianBotnet | Coper | Cabassous.D | Eventbot | ExobotCompact.D/Octo | FluBot | Medusa | Sharkbot | Teabot | Xenomorph |
|---------------------------------------------------|-------------------------------|----------------------|---------------------|------------------------|-------|-------------|----------|----------------------|--------|--------|----------|--------|-----------|
| Emirates NBD                                      | Emirates NBD                  | United Arab Emirates | 1000000             |                        |       | X           |          |                      |        |        |          | X      |           |
| ADCB Hayyak: Start your banking relationship now! | Abu Dhabi Commercial Bank     | United Arab Emirates | 500000              |                        |       |             |          |                      |        |        |          | X      |           |
| ADIB Mobile Banking App                           | Abu Dhabi Islamic Bank        | United Arab Emirates | 500000              |                        |       |             |          |                      |        |        |          | X      |           |
| DIB MOBILE                                        | DIB Mobility                  | United Arab Emirates | 1000000             |                        |       |             |          |                      |        |        |          | X      |           |
| FAB Mobile                                        | First Abu Dhabi Bank          | United Arab Emirates | 500000              |                        |       |             |          |                      |        |        |          | X      |           |
| Liv. KSA - Digital Banking                        | Emirates NBD                  | United Arab Emirates | 100000              |                        |       |             |          |                      |        |        |          | X      |           |
| Mashreq Neo - Bank easy                           | Mashreq                       | United Arab Emirates | 1000000             |                        |       |             |          |                      |        |        |          | X      |           |
| RAKBANK Digital Banking                           | RAKBANK                       | United Arab Emirates | 500000              |                        |       |             |          |                      |        |        |          | X      |           |
| smartbanking by ADIB                              | Abu Dhabi Islamic Bank        | United Arab Emirates | 50000               |                        |       |             |          |                      |        |        |          | X      |           |
| Nationwide Banking App                            | Nationwide Building Society   | United Kingdom       | 1000000             |                        |       | X           |          |                      |        |        |          |        |           |
| Virgin Money Credit Card                          | Virgin Money                  | United Kingdom       | 500000              |                        |       | X           |          |                      |        |        |          |        |           |
| MBNA Card Services App                            | Lloyds Banking Group PLC      | United Kingdom       | 500000              |                        |       | X           |          | X                    |        |        |          |        |           |
| Royal Bank of Scotland                            | National Westminster Bank PLC | United Kingdom       | 1000000             |                        |       | X           |          | X                    |        |        |          |        |           |
| Tesco Mobile                                      | Tesco Mobile UK               | United Kingdom       | 1000000             |                        |       | X           |          | X                    |        |        |          |        |           |
| TSB Mobile Banking                                | TSB Bank plc.                 | United Kingdom       | 1000000             |                        | X     | X           |          | X                    |        |        |          | X      |           |
| Barclays                                          | Barclays Services Limited     | United Kingdom       | 10000000            |                        |       | X           | X        | X                    |        |        |          | X      |           |
| Metro Bank                                        | Metro Bank PLC                | United Kingdom       | 500000              |                        |       | X           |          | X                    |        |        |          | X      |           |
| NatWest Mobile Banking                            | National Westminster Bank PLC | United Kingdom       | 5000000             |                        |       | X           |          | X                    |        |        |          | X      |           |
| The Co-operative Bank                             | The Co-operative Bank UK      | United Kingdom       | 100000              |                        |       | X           |          | X                    |        |        |          | X      |           |
| TSB Bank Mobile Banking                           | TSB Bank Limited              | United Kingdom       | 100000              |                        |       | X           |          | X                    |        |        |          | X      |           |
| Lloyds Bank Mobile Banking                        | Lloyds Banking Group PLC      | United Kingdom       | 5000000             |                        |       | X           |          |                      |        |        |          | X      |           |
| Santander Mobile Banking                          | Santander UK plc              | United Kingdom       | 5000000             |                        |       | X           |          |                      |        |        |          | X      |           |
| Barclaycard                                       | Barclays Services Limited     | United Kingdom       | 1000000             |                        |       |             | X        |                      |        |        |          |        |           |
| CEX.IO Cryptocurrency Exchange                    | CEX.IO                        | United Kingdom       | 1000000             |                        |       |             |          | X                    |        |        |          |        |           |

[illegible]

## Mobile Banküberfälle: Die globale wirtschaftliche Bedrohung

| AppName                                            | Developer                      | Country        | Number of Downloads | Android/ BianlianBotnet | Coper | Cabassous.D | Eventbot | ExobotCompa ct.D/Octo | FluBot | Medusa | Sharkbot | Teabot | Xenomorph |
|----------------------------------------------------|--------------------------------|----------------|---------------------|-------------------------|-------|-------------|----------|-----------------------|--------|--------|----------|--------|-----------|
| Business Banking                                   | Santander UK plc               | United Kingdom | 100000              |                         |       |             |          |                       |        |        |          | X      |           |
| Oval - Track, save and invest                      | Oval Money                     | United Kingdom | 500000              |                         |       |             |          |                       |        |        |          | X      |           |
| Pocket: A Banking Alternative                      | Pocket Ltd                     | United Kingdom | 100000              |                         |       |             |          |                       |        |        |          | X      |           |
| Revolut                                            | Revolut Ltd                    | United Kingdom | 10000000            |                         |       |             |          |                       |        |        |          | X      |           |
| Revolut Business                                   | Revolut Ltd                    | United Kingdom | 100000              |                         |       |             |          |                       |        |        |          | X      |           |
| Sokin Global Money Transfer                        | Sokin Mobile                   | United Kingdom | 100000              |                         |       |             |          |                       |        |        |          | X      |           |
| Starling Bank - Mobile Banking                     | Starling Bank                  | United Kingdom | 1000000             |                         |       |             |          |                       |        |        |          | X      |           |
| thinkmoney                                         | Think Money Limited            | United Kingdom | 100000              |                         |       |             |          |                       |        |        |          | X      |           |
| TSB Business Mobile                                | TSB Bank plc.                  | United Kingdom | 100000              |                         |       |             |          |                       |        |        |          | X      |           |
| Ulster Bank NI Mobile Banking                      | National Westminster Bank PLC  | United Kingdom | 100000              |                         |       |             |          |                       |        |        |          | X      |           |
| Virgin Money Mobile Banking                        | Clydesdale Bank PLC            | United Kingdom | 500000              |                         |       |             |          |                       |        |        |          | X      |           |
| Wirex: Crypto Exchange & Card                      | Wirex                          | United Kingdom | 1000000             |                         |       |             |          |                       |        |        |          | X      |           |
| Yorkshire Bank Mobile Banking                      | Clydesdale Bank PLC            | United Kingdom | 500000              |                         |       |             |          |                       |        |        |          | X      |           |
| Tomamos impulso - TARGOBANK I AGRUPACIÓ I ATLANTIS | Euro Information               | United Kingdom | 50000               |                         |       |             |          | X                     |        |        |          |        | X         |
| HSBC UK Mobile Banking                             | HSBC                           | United Kingdom | 1000000             |                         |       | X           |          | X                     |        |        |          | X      |           |
| HSBC UK Business Banking                           | HSBC                           | United Kingdom | 100000              |                         |       |             |          |                       |        |        |          | X      |           |
| UBank                                              | NAB                            | United States  | 100000              |                         |       | X           |          | X                     |        |        |          |        |           |
| NAB Mobile Banking                                 | NAB                            | United States  | 1000000             |                         | X     | X           |          | X                     |        |        |          | X      |           |
| ATB Business - Mobile Banking                      | ATB Online                     | United States  | 10000               |                         |       |             |          | X                     |        |        |          |        |           |
| Barclays US Credit Cards                           | Barclays US Bank               | United States  | 1000000             |                         |       |             |          | X                     |        |        |          |        |           |
| Cash App                                           | Square, Inc.                   | United States  | 50000000            |                         |       |             |          | X                     |        |        |          |        |           |
| CitiManager – Corporate Cards                      | Citibank N.A.                  | United States  | 100000              |                         |       |             |          | X                     |        |        |          |        |           |
| Coinbase Wallet: NFTs & Crypto                     | Coinbase Wallet                | United States  | 5000000             |                         |       |             |          | X                     |        |        |          |        |           |
| HSBC Mobile Banking                                | HSBC Technology & Services USA | United States  | 5000000             |                         |       |             |          | X                     |        |        |          |        |           |
| HSBCnet Mobile                                     | HSBC Bank plc                  | United States  | 100000              |                         |       |             |          | X                     |        |        |          |        |           |
| Kraken Pro: Crypto Trading                         | Payward, Inc.                  | United States  | 1000000             |                         |       |             |          | X                     |        |        |          |        |           |
| Mi Banco Mobile                                    | Banco Popular de Puerto Rico   | United States  | 1000000             |                         |       |             |          | X                     |        |        |          |        |           |
| Paxful Bitcoin & Crypto Wallet   Buy BTC ETH USDT  | Paxful                         | United States  | 1000000             |                         |       |             |          | X                     |        |        |          |        |           |

## Mobile Banküberfälle: Die globale wirtschaftliche Bedrohung

| AppName                                         | Developer                      | Country       | Number of Downloads | Android/<br>BianlianBotnet | Coper | Cabassous.D | Eventbot | ExobotCompa<br>ct.D/Octo | FluBot | Medusa | Sharkbot | Teabot | Xenomorph |
|-------------------------------------------------|--------------------------------|---------------|---------------------|----------------------------|-------|-------------|----------|--------------------------|--------|--------|----------|--------|-----------|
| PayPal - Send, Shop, Manage                     | PayPal Mobile                  | United States | 100000000           |                            |       |             |          | X                        |        |        |          |        |           |
| PC Financial Mobile                             | PC Bank                        | United States | 500000              |                            |       |             |          | X                        |        |        |          |        |           |
| WeChat                                          | WeChat International Pte. Ltd. | United States | 100000000           |                            |       |             |          | X                        |        |        |          |        |           |
| Western Union ES - Send Money Transfers Quickly | Western Union Android Apps     | United States | 500000              |                            |       |             |          | X                        |        |        |          |        |           |
| Chase Mobile                                    | JPMorgan Chase                 | United States | 10000000            |                            |       |             |          | X                        |        |        |          | X      |           |
| MetaMask - Blockchain Wallet                    | ConsenSys                      | United States | 10000000            |                            |       |             |          | X                        |        |        |          | X      |           |
| Trust: Crypto & Bitcoin Wallet                  | DApps Platform, Inc.           | United States | 10000000            |                            |       |             |          | X                        |        |        |          | X      |           |
| U.S. Bank Mobile: Bank and Invest               | U.S. Bank Mobile               | United States | 5000000             |                            |       |             |          | X                        |        |        |          | X      |           |
| Union Bank Mobile Banking                       | Union Bank                     | United States | 1000000             |                            |       |             |          | X                        |        |        |          | X      |           |
| Coinbase: Buy Bitcoin & Ether                   | Coinbase Android               | United States | 10000000            |                            |       |             |          | X                        |        |        | X        | X      |           |
| Ally: Banking & Investing                       | Ally Financial                 | United States | 1000000             |                            |       |             |          |                          |        | X      |          |        |           |
| Amex                                            | American Express               | United States | 5000000             |                            |       |             |          | X                        |        | X      |          |        |           |
| Bank of the West Mobile                         | Bank of the West               | United States | 500000              |                            |       |             |          | X                        |        | X      |          |        |           |
| BMO Digital Banking                             | BMO Harris Bank N.A.           | United States | 100000              |                            |       |             |          | X                        |        | X      |          |        |           |
| Compass Savings Bank                            | Compass Savings Bank           | United States | 500                 |                            |       |             |          | X                        |        | X      |          |        |           |
| Discover Mobile                                 | Discover Financial Services    | United States | 5000000             |                            |       |             |          | X                        |        | X      |          |        |           |
| First Citizens Mobile Banking                   | First Citizens Bank & Trust    | United States | 100000              |                            |       |             |          | X                        |        | X      |          |        |           |
| KeyBank - Online & Mobile Banking               | KeyBank, N.A.                  | United States | 1000000             |                            |       |             |          | X                        |        | X      |          |        |           |
| M&T Mobile Banking                              | M&T Bank                       | United States | 1000000             |                            |       |             |          | X                        |        | X      |          |        |           |
| Morgan Stanley Wealth Mgmt                      | Morgan Stanley and Co. LLC     | United States | 100000              |                            |       |             |          | X                        |        | X      |          |        |           |
| People's United Bank Mobile                     | People's United Bank           | United States | 100000              |                            |       |             |          | X                        |        | X      |          |        |           |
| Woodforest Mobile Banking                       | Woodforest National Bank       | United States | 1000000             |                            |       |             |          | X                        |        | X      |          |        |           |
| Zelle                                           | Early Warning Services, LLC    | United States | 10000000            |                            |       |             |          | X                        |        | X      |          |        |           |
| Bank of America Mobile Banking                  | Bank of America                | United States | 10000000            |                            |       |             |          | X                        |        | X      |          | X      |           |
| Capital One Mobile                              | Capital One Services, LLC      | United States | 10000000            |                            |       |             |          | X                        |        | X      |          | X      |           |
| Citi Mobile®                                    | Citibank N.A.                  | United States | 10000000            |                            |       |             |          | X                        |        | X      |          | X      |           |
| Citizens Bank Mobile Banking                    | Citizens Bank, N.A.            | United States | 1000000             |                            |       |             |          | X                        |        | X      |          | X      |           |
| E*TRADE: Invest. Trade. Save.                   | E*TRADE Securities             | United States | 1000000             |                            |       |             |          | X                        |        | X      |          | X      |           |
| Fifth Third Mobile Banking                      | Fifth Third Bank               | United States | 1000000             |                            |       |             |          | X                        |        | X      |          | X      |           |
| Navy Federal Credit Union                       | Navy Federal                   | United States | 5000000             |                            |       |             |          | X                        |        | X      |          | X      |           |
| PNC Mobile                                      | PNC Bank, N.A.                 | United States | 5000000             |                            |       |             |          | X                        |        | X      |          | X      |           |
| Schwab Mobile                                   | The Charles Schwab Corporation | United States | 1000000             |                            |       |             |          | X                        |        | X      |          | X      |           |
| SECU                                            | State Employees' Credit Union  | United States | 500000              |                            |       |             |          | X                        |        | X      |          | X      |           |
| TD Bank (US)                                    | TD Bank, N.A.                  | United States | 5000000             |                            |       |             |          | X                        |        | X      |          | X      |           |
| USAA Mobile                                     | USAA                           | United States | 5000000             |                            |       |             |          | X                        |        | X      |          | X      |           |
| Wells Fargo Mobile                              | Wells Fargo Mobile             | United States | 10000000            |                            |       |             |          | X                        |        | X      |          | X      |           |

[illegible]

[illegible]

# Impressum

**Forscher:**

Aazim Yaswant  
Gianluca Braga  
Adam Wosotowsky  
Vishnu Pratapagiri

**Editoren:**

Richard Melick  
Kasey Hewitt

**Autoren:**

Randy Budde  
Monique Becenti  
Richard Melick  
Tim Hartog

**Leitende Editoren:**

Nico Chiaraviglio  
Andrew Snyder  
Tim Hartog  
JT Keating  
Jon Paterson

**Grafikdesign**

Tom Green



## Über Zimperium

Zimperium basiert auf der Prämisse, dass mobile Sicherheit einen völlig neuen Ansatz erfordert, und schützt sowohl mobile Geräte als auch Anwendungen, damit diese sicher und geschützt auf Daten zugreifen können. Eine einzige, einheitliche Plattform schützt den Endpunkt und sichert den gesamten Anwendungsentwicklungszyklus mit der einzigen gerätebasierten Engine, die auf maschinellem Lernen aufbaut. Zimperium bietet Transparenz und Schutz vor bekannten und Zero-Day-Bedrohungen und Angriffen über Geräte-, Netzwerk-, Phishing- und Anwendungsbedrohungsvektoren auf Android-, iOS- und ChromeOS-Geräte. Zimperium hat seinen Hauptsitz in Dallas, Texas, und wird von Warburg Pincus, SoftBank, Samsung, Sierra Ventures und Telstra Ventures unterstützt.

Weitere Informationen oder Kontakt zu uns finden Sie unter [zimperium.com](https://zimperium.com).