Mobile Infrastrukturen
Studiengang Informatik

- Dipl.-Inf., Dipl.-Ing. (FH) Michael Wilhelm
- Hochschule Harz
- FB Automatisierung und Informatik
- mwilhelm@hs-harz.de
- Raum 2.202
- Tel. 03943 / 659 338

Inhalt

- **Rechnerstrukturen ohne Tablets (Hardware / Software)**
  - Ebenen der IT-Infrastruktur
  - Rechenzentrum (Desktop-Rechner)
- **Erweiterung auf „Mobile Infrastrukturen“**
  - Rechenzentrum + Mobile Infrastrukturen
- **Komponenten_mobiler_Infrastrukturen**
- **Gesetze**
- **Sicherheitsprobleme bei Smartphones und Tablets**
- **Mobile Device Management**

Mobile Computing bedeutet

- Mobilität von **Diensten und Programmen**
  - Email, Whats‘App, FileTransfer
- Mobilität von **Daten**
  - Mit unterschiedlichen Geräten wird von überall auf der Welt mittels Cloud auf Daten zugegriffen
- Mobilität der **Endgeräte**
  - Die Geräte müssen bequem portabel und unabhängig von einer Stromversorgung funktionieren.
  - Die Benutzung sollte einfach sein (Anmeldung).
- Mobilität der **Netzanbindung**
  - Die Verbindung zum Unternehmensnetz soll über drahtlose Netze mit Zugriffspunkten oder Mobilfunknetzen von überall auf der Welt sicher möglich sein.
- **Peripherie**
  - Speicherkarten, Headsets, USB-Sticks, SD-Karten

Mobile Computing bedeutet

- **Anforderung an die Hersteller**
  - Die Bedienung sollte für nicht geschulten Personal einfach sein.
  - Mobilität: Einzelkämpfer
  - Auch ein IT-Administrator!
  - Ohne Unterstützung von Software und IT-Abteilungen nicht möglich.
- **Mobile Device Management**
  - Mobile Device Management sorgt für eine Grundkonfiguration der Geräte.
  - Update erst mit der Aufforderung der Software.

Sicherheitsprobleme

- **Zugriff auf die Daten Verlust oder Diebstahl**
  - Man benutzt die Geräte immer und überall. Man kann sie leicht vergessen oder verlieren.
  - „Offen“ in der Hosentasche ist es eine Einladung an Diebe.
  - Zugriffskarten sind klein, haben aber eine große Kapazität. Man „verleiht“ kurz das Handy und schnell ist die SD-Karte ausgebaut.
  - CEO‘s sind vom „Whaling“ bedroht.
    - Angriff per Emails, Fake Websites, Social Accounts
    - Man in the middle attack
- **Nach dem Verlust**
  - Ist ein Backup vorhanden
  - Gibt es Restore-Möglichkeiten
  - Gibt es auf dem geklauten Gerät voreingestellte Anmeldungen?
  - Wie sicher war die Gerätesperre?
  - Kann man das Gerät ausschalten?

- https://phoenixite.com/what-is-whaling-in-cyber-security/
- https://us.norton.com/internetsecurity-emerging-threats-whaling-attack.html

Passwortlänge

- **Die Top 20 der beliebtesten Passwörter 2021**

1. 123456
2. 123456789
3. 12345
4. qwerty
5. Kennwort
6. 12345678
7. 111111
8. 123123
9. 1234567890
10. 1234567
11. qwerty123
12. 000000
13. 1q2w3e
14. aa12345678
15. abc123
16. Kennwort1
17. 1234
18. qwertyuiop
19. 123321
20. passwort123

- Experten empfehlen die mehrstufige Authentifizierung.
- Konzerne wie Apple oder Google bieten dies an und schlagen auch sichere Passwörter vor, die sich dann in der Cloud speichern lassen. Oder Sie nutzen Passwort-Manager.

Sicherheitsprobleme

- **Nach kurzen Suchen wiedergefunden**
  - Hier ist Vorsicht angebracht.
  - Die Daten auf dem mobilen Gerät können manipuliert sein.
  - Es kann Spyware installiert worden sein.
    - Es dient jetzt als Wanze.
    - Per Email und GPS wird der Ort des CEO bekannt.
    - Etc.

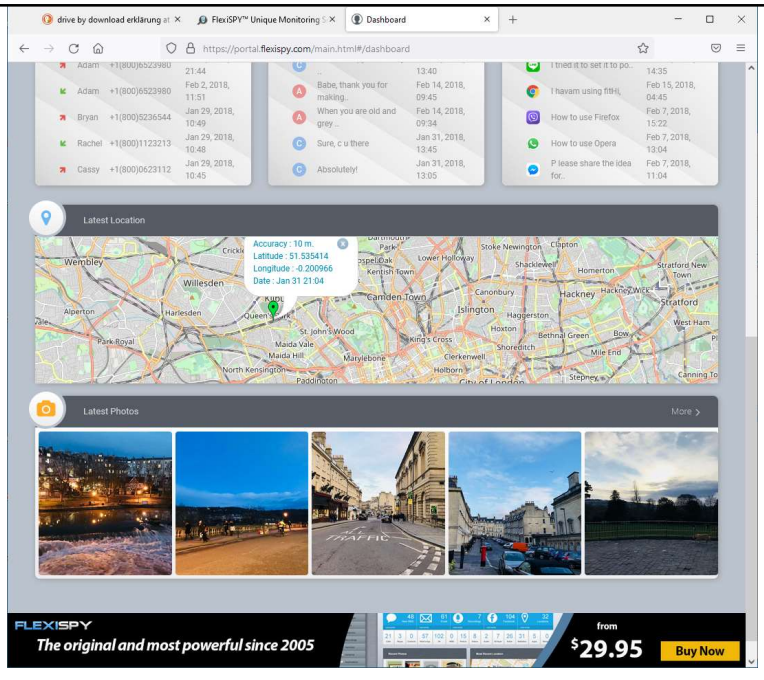
Sicherheitsprobleme

- **Schadsoftware**
  - Verbreitet per E-Mail, Bluetooth, WLan
  - Verbreitet durch schadhafte App im Store
    - Abhilfe: Signature
    - Aber:
    - Bekannte Apps, Candy Crush, werden mit Viren infiziert und im AppStore angeboten.
    - Verbot des Downloads von App (MDM).
  - Auf der Messe:
    - Geschenkte USB-Sticks
    - Geschenkte SD-Karten.
  - Drive by download
    - In vielen Fällen werden von Angreifern gezielt Webseiten ohne Wissen der Betreiber manipuliert, indem etwa bekannte Schwachstellen bei verbreiteten Webanwendungen ausgenutzt werden.
    - Diese manipulierten Webseiten führen dann in Verbindung mit offenen Sicherheitslücken im Browser oder im Betriebssystem zur unbemerkten Ausführung von Schadsoftware auf dem Computer des Benutzers.

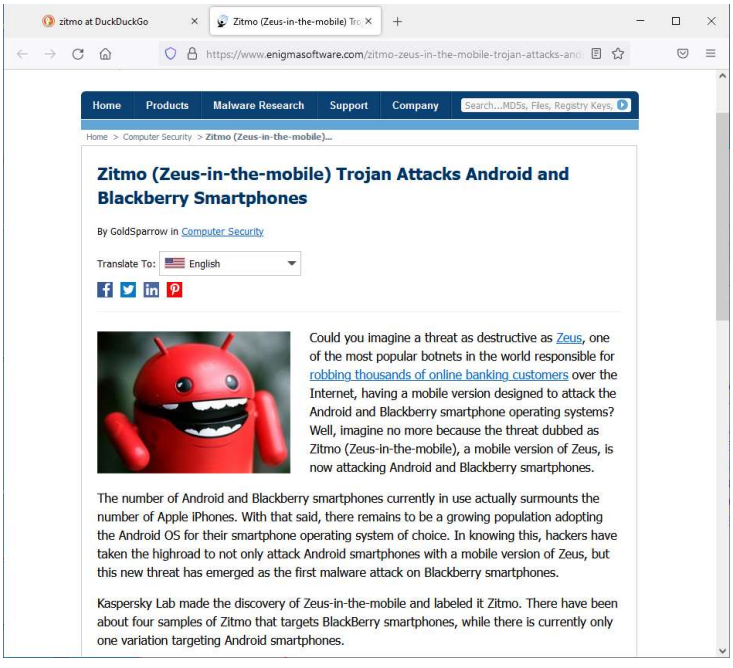
Sicherheitsprobleme

- **Schadsoftware**
  - Spy-Apps
    - Diese Spy-Apps werden kommerziell angeboten und dienen der Überwachung.
    - Sinnvoll für Firmen?
    - Diese App können aber auch gezielt installiert werden, um Bankdaten etc. abzugreifen.
  - Bekannte Trojaner (botnet)
    - ZeuS
    - ZitMo (Zeus in the mobile, umgeht Tan-Verfahren)

- https://www.flexispy.com/
- https://www.enigmasoftware.com/zitmo-zeus-in-the-mobile-trojan-attacks-android-blackberry-smartphones/




FLEXISPY
24/7 +1 213 810 3122
PRODUCTS
FEATURES
COMPATIBILITY
REVIEWS
WHY FLEXISPY?
MORE
PREINSTALLED PHONES
Family Phone Bundles Savings
From $1,119
The World's Most Powerful Monitoring So
for Computers, Mobile Phones and Tablet
Know Everything That Happens on A Computer or Smartphone, No Matter Where You Are
Monitor all Android and iPhone digital and audio communications
Monitor everything that happens on a PC or Mac
More monitoring features than any other product
No Hassle Remote Installation Service
FREE Mobile Viewer App for Android and iPhone
Used for Parental Control and Employee Monitoring
My Dad's not here. Meet me at 10.
View Demo
Buy Now
FlexiSPY is monitoring software that you install on your computer or mobile device.
It takes complete control of the device, letting you know everything, no matter where you are.
We're Online!
How may I help you today?


Home
Products
Malware Research
Support
Company
Home > Computer Security > Zitmo (Zeus-in-the-mobile)...
Zitmo (Zeus-in-the-mobile) Trojan Attacks Android and Blackberry Smartphones
By GoldSparrow in Computer Security
Translate To: English
Could you imagine a threat as destructive as Zeus, one of the most popular botnets in the world responsible for robbing thousands of online banking customers over the Internet, having a mobile version designed to attack the Android and Blackberry smartphone operating systems? Well, imagine no more because the threat dubbed as Zitmo (Zeus-in-the-mobile), a mobile version of Zeus, is now attacking Android and Blackberry smartphones.
The number of Android and Blackberry smartphones currently in use actually surmounts the number of Apple iPhones. With that said, there remains to be a growing population adopting the Android OS for their smartphone operating system of choice. In knowing this, hackers have taken the highroad to not only attack Android smartphones with a mobile version of Zeus, but this new threat has emerged as the first malware attack on Blackberry smartphones.
Kaspersky Lab made the discovery of Zeus-in-the-mobile and labeled it Zitmo. There have been about four samples of Zitmo that targets BlackBerry smartphones, while there is currently only one variation targeting Android smartphones.

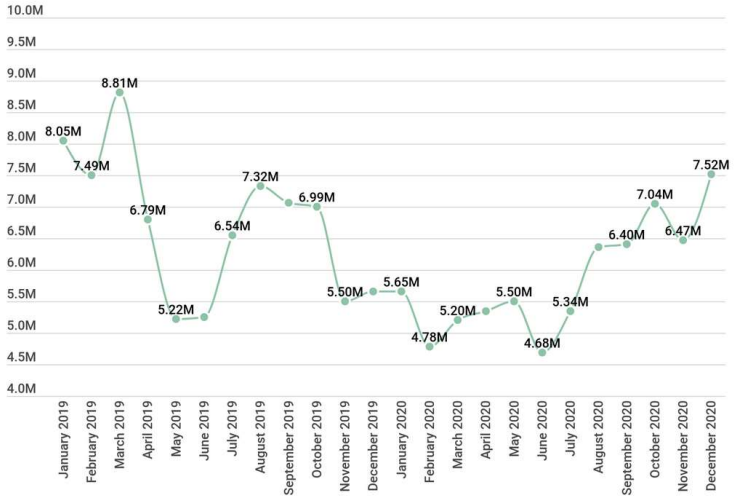
Sicherheitsprobleme

- **Schadsoftware**
  - Schadsoftware mittels Social Engineering
    - Red Browser läuft auf jedem mobilen Gerät.
    - Es gaukelt dem Anwender vor, ein Browser zu sein, der kostenlos eine SMS verschickt.
    - Diese SMS muss vom Anwender explizit mit einem Bankkonto genehmigt werden.
    - Dann wird eine teure Premium-SMS verschickt.
    - Werden heute noch SMS verschickt?

Sicherheitsprobleme

- **Schadsoftware pro Plattform**
  - Meistens sind es Android-Geräte
  - Auf Apple Geräte kommt es sehr selten vor
- **MDM**
  - Es sollten also Einschränkungen gegenüber App getroffen werden.
- **Schutz vor Malware**
  - Es sollten also Einschränkungen gegenüber App getroffen werden.

Report der mobilen Attacken (nur 1% Anteil an den gesamten Attacken



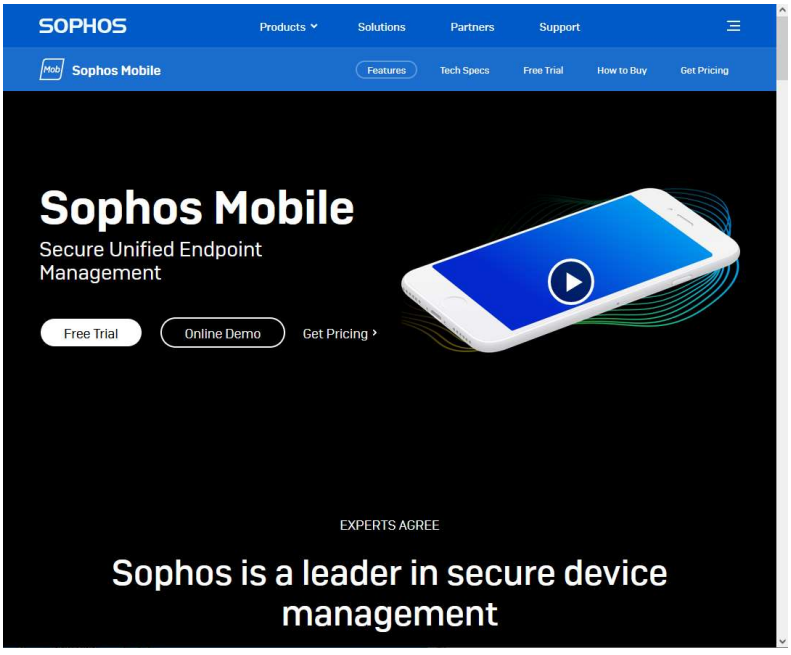
- https://securelist.com/mobile-malware-evolution-2020/101029/

https://www.cybertalk.org/2022/06/10/10-eye-opening-mobile-malware-statistics-to-know/

- The NSO group's Pegasus spyware remains as the most notorious of commercial phone malware/spyware varieties, but new findings indicate that Predator spyware could target tens of thousands of Android phones.
- Banking malware threats on Android devices have increased by **80%**, meaning that strong phone security is more important than ever before.
- Last year, Adware accounted for 42% of new mobile malware worldwide. How's your adware protection?
- **47% of free Android antivirus programs can't effectively detect malware**. Are your BYOD employees relying on free antivirus programs?
- There are 50× more Android mobile malware infections than iOS infections. 50×!
- Mobile malware apps that provide backdoors into phones are currently spreading via SMS or text messaging.
- Some cyber criminals are paying a monthly fee of $5,000 to rent an app that steals access credentials from hundreds of other fraudulent apps.
- 97% of organizations have contended with malware threats that leverage various attack vectors.
- Cyber security researchers recently devised a malware threat that can persist on iPhones even when the devices run in low-power mode.
- During Q1 of 2022, security programs successfully blocked 6,463,414 mobile malware, adware and riskware attacks.

Arten von Malware auf mobilen Geräten

- Bank trojans. This malware type commonly masquerades as a legitimate application. It tends to affect users who are just going about their personal banking activities from mobile devices. Banking trojans generally aim to steal credentials.
- Remote Access Tools (Fernwartung). These are typically used for intelligence collection purposes. RATs can gather installed application information, call history data, address books, web browsing history and SMS data. Further, RATs can be used to send SMS messages, to enable device cameras and to log GPS data.
- Adware. This type of malware enables an attacker to hijack a device in order to generate income via fake ad clicks. Adware ist eine Form von Schadsoftware, die sich auf Ihrem Gerät verbirgt und Werbungen einblendet. Einige Adware-Varianten überwachen auch Ihr Online-Verhalten, damit Ihnen gezielte Anzeigen präsentiert werden können.
- Cryptomining Malware. This type of malware allows attackers to execute calculations on a victim's device – enabling them to generate cryptocurrency. Cryptomining is often conducted via Trojan code that's surreptitiously lurking in legitimate-seeming applications.



Sicherheitsprobleme

- **Pishing**
  - Durch gefälschte Webseiten, E-Mails, Kurznachrichten versucht man an sensible Daten zu kommen.
    - Mit Bankdaten werden dann Waren bestellt.
    - Der Bildschirm eines mobilen Geräts ist relativ klein.
    - Man ist meistens in einer „Stress-Situation“.
    - Man berührt ohne Nachzudenken den Link.
    - Einige E-Mail-Clients zeigen nur den Title-Tag und nicht die gesamt URL.
    - **Mobile Nutzer sind immer online.** Damit sind „Pishing-Angriffe“ noch unbekannt. Ein Benutzer eines Desktop-Rechner öffnet die E-Mail erst später und deshalb kann der Filter den Angriff erkennen (vielleicht).
    - Nach einer Statistik sind iPhone-Benutzer am meistens von Pishing betroffen.
    - Eine Ursache: Bei iPhone wird ein Link OHNE Nachfrage gestartet.
    - Ein MDM sollte alle möglichen Gegenmaßnahmen eingebaut haben.

Sicherheitsprobleme

- **Direkte Beobachtung (Shoulder Surfing)**
  - Durch Sitznachbarn oder „Hintermänner“ wird der Bildschirm und die Tastatur abgelesen. Oder es wird mit einer Videokamera aufgezeichnet.
    - Orte:
      - Zugabteil
      - Flugzeug
      - Gaststätten
      - Abflughallen
    - Gegenmaßnahmen
      - Ein gesundes Mistrauen gegenüber der Umgebung
      - Polarisationsfilter (von der Seite nun schwerer zu lesen)
      - Keine einfachen Passwörter/Pins verwenden (an den Finger abzulesen)
      - Verzicht auf „Arbeiten“ in unsicherer Umgebung
    - MDM
      - Zwang zu längeren Passwörter
      - Häufigere Wechsel

Sicherheitsprobleme

- **Unsichere Datenablage im mobilen Gerät**
  - Durch Sitznachbarn oder „Hintermänner“ wird der Bildschirm und die Tastatur abgelesen. Oder es wird mit einer Videokamera aufgezeichnet.
    - Cache des Betriebssystems
      - Zahlungsdaten
      - Passwörter
      - Originalfotos beim Scannen
      - Wortvervollständigungen
    - Wichtig
      - Der aktuelle Datenbestand muss immer protokolliert sein.
      - Welche Gefahr droht durch den Verlust.
    - Gegenmaßnahmen
      - Verschlüsselung der Daten (AES 256). Sicherheitslücken?
        - Schlüsselverwaltung
        - Alle daten oder nur einzelne Dateien?
      - Schärfere Zugangs- und Zugriffsbeschränkung von sensiblen Daten. Zwei-Faktor-Authentisierung
    - MDM
      - Zwang zu längeren Passwörter
      - Häufigere Wechsel

Sicherheitsprobleme

- **Unsichere Datenablage im mobilen Gerät**
  - **iOS**
    - Es gibt eine transparente Verschlüsselung der Systempartition, wenn das Gerät gesperrt ist.
    - Ist es entsperrt, so kann man auf alle daten zugreifen!.
    - **Bei einem Fernlöschbefehl wird nur die FAT gelöscht!**
    - Eine App muss eine permanente Verschlüsselung einer Datei explizit anfordern.
    - Im iPhone das “Secure Enclave” Modul
    - E-Mails werden verschlüsselt, aber mit einem Jailbreak sind Zugriffe möglich.
    - Der Passwortschutz per App ist sehr gut. Nach dreimaliger Fehleingabe ist es vorbei.
    - Mit einem Jailbreak kann man die Systempartition als externe Festplatte anschließen. Nun kann man mit einem Bruce-Force das Passwort rausfinden.
    - MDM
      - Keine 4 stelligen Zahlen
      - Besser sechs bis achtstellige alphanumerische Eingaben.

Sicherheitsprobleme

- **Unsichere Datenablage im mobilen Gerät**
  - **Android**
    - Es gibt ab Version 3,0 eine Unterstützung von Crypto-Chips.
    - Abfrage der Telefon-Pin und der Pin der Sim-Karte
    - Die Sperrung ist leicht zu durchbrechen
      - Die Datei /data/system/gesture.key enthält die Daten als SHA1-Hash und sind von rooted-Android auslesbar.
    - Eine sinnvolle Verschlüsselung ist nur durch externe Apps (MDM) möglich.
    - Auch hier gilt: Was ist die Quelle (Trojaner)

Sicherheitsprobleme

- **Schwachstellen drahtloser Kommunikation**
  - GSM / UMTS / 5G
  - WLAN (Evil Twin als Access Point)
  - Blutooth

Sicherheitsprobleme

- **Apps mit unerwünschtem Datenabfluss**
  - App versuchen Daten abzugreifen (Zeus)
  - App versuchen den Benutzer zu teuren Handlungen zu bewegen (teuere Telefonnummern, SMS etc.)
  - App‘s telefonieren nach Hause. Extremer Datenverkehr, der außerdem meist unverschlüsselt ist. Die Daten dienen zum Erstellen persönlicher Profile und werden dann an Werbefirmen verkauft.
    - GPS-Daten
    - Kontaktdaten
    - Bilder/Videos
  - .

Sicherheitsprobleme

- **iOS-Apps mit unerwünschtem Datenabfluss**
  - App‘s laufen in einer Sandbox
    - Abgeschottet. Kein Zugriff auf die Daten anderer Apps.
    - Aber die Apps müssen mit den Betriebssystem oder anderen Apps kommunizieren.
      - Inter-Process Communication
    - Wie genau wird diese Kommunikation überwacht?
  - .Unter iOS haben die Apps keinen Zugriff auf Daten anderer Apps.
  - Apps von Drittanbietern dürfen ohne Rückfragen:
    - WLAN kommunizieren.
    - Auf das Adressbuch, E-Mail, Notizen, Kalender, Musik etc. zugreifen
    - Die UUID des Gerätes auslesen
    - Historie des Browser lesen
    - Die eigene Telefonnummer auslesen
    - Die Liste der angeschauten YouTube Videos auslesen
    - Wortvervollständigungsliste auslesen
    - Log-datei der WiFi-Verbindungen
    - Mikrofon und Kamera

Sicherheitsprobleme

- **iOS-Apps mit unerwünschtem Datenabfluss**
  - Der Schweizer Softwareentwickler Nicholas Seriot hat eine BeispielApp entwickelt, die alle Daten ausliest und per E-Mail versendet.
  - Software SpyPhone
    - http://seriot.ch/resources/talks_papers/iPhonePrivacy.pdf
  - Quellcode der App
    - http://github.com/nst/spyphone

Sicherheitsprobleme

- **Android-Apps mit unerwünschtem Datenabfluss**
  - Android ist eine Kombination aus einem Linux-System und einer Java-Plattform
    - Dalviks Virtual Maschine
  - Unter Android laufen die Apps in ihrer eigenen JVM
  - Ausnahmen:
    - Apps können eine Liste aller installierten Apps einschließlich ihrer Programmlogik einsehen
    - Apps dürfen alle Inhalte einer SD-Karte lesen aber nicht ändern.
    - Apps dürfen andere Apps aufrufen (WebBrowser etc.)
    - Weitere Rechte nach Nachfrage:
      - Bei einigen Samsung Geräten kann man das Nachfragen einstellen. Aber manchmal auch nur Ja/Nein.
    - Bei Rechten gilt: alles oder nichts