Malware #2: Das Verhalten von Malware

Mag. Lukas Feiler, SSCP
lukas.feiler@lukasfeiler.com
http://www.lukasfeiler.com/lectures_malware

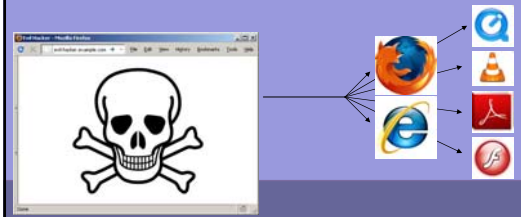
Übersicht

Malware #1: Die Kompromittierung von Computern durch Malware

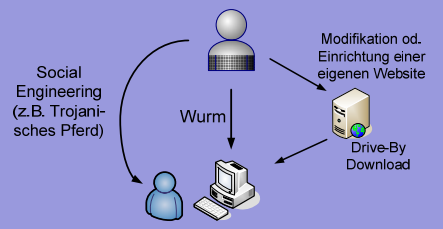
Malware #2: Das Verhalten von Malware

Technische Angriffe über den Browser: „Drive-By Downloads“

- Die Browser-Software (z.B. Mozilla Firefox, IE)
- Plugins (insbesondere Adobe Flash, Adobe Reader, Quicktime, VLC Media Player)



Zusammenfassung der Angriffsarten



Das Verhalten von Malware

Zu welchem Zweck wird Malware geschrieben?

- Um User auszuspionieren: Spyware
- Um Werbung an den Mann/die Frau zu bringen: Adware
- Um Spam versenden zu können: Spamware
- Um Distributed Denial of Service (DDoS)-Angriffe auszuführen
- Aus Spaß & Neugier (=Dummheit)

Spyware

Arten von Spyware:

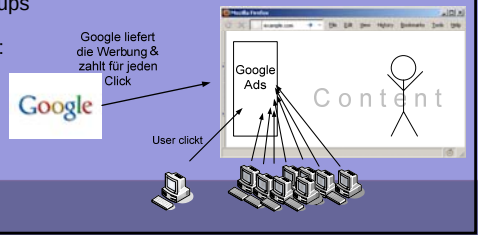
- Keylogger 
- Screen-Grabber 
- Sniffer 

Adware

Arten von Adware:

- Traditionelle Adware
  → Werbeunternehmen zahlen für jede angeklickte/angezeigte Werbeeinschaltung
  → idR Popups

- Click-Fraud:



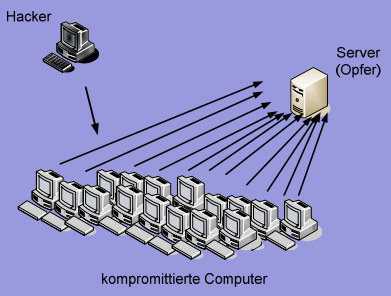
Spamware

Was ist SPAM?

→ Unaufgeforderte Werbe-E-Mails

→ mehr als die Hälfte aller Spam-Mails wird über kompromittierte Systeme versendet!

Distributed Denial of Service (DDoS)



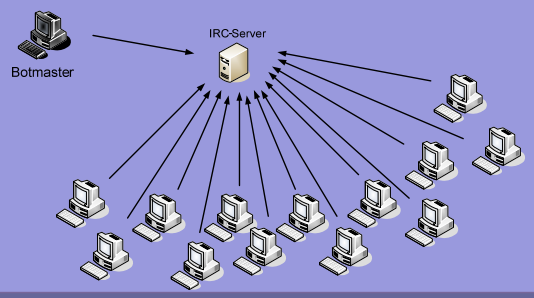
Wie schützt sich Malware vor Entdeckung?

Rootkits: Manipulation des Kernel

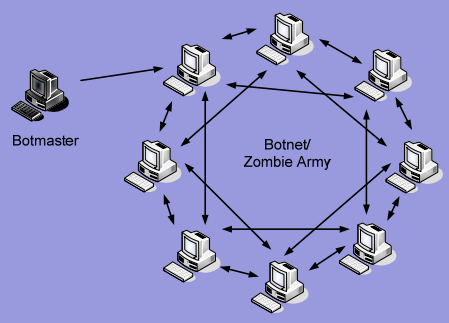
Welche Dateien gibt es in einem Verzeichnis?
Welche Prozesse laufen gerade?

→ Bei diesen Antworten vertraut man immer auf den Kernel

Wie kontrolliert der Hacker die kompromittierten Computer: Botnets



Dezentrale Botnet-Architekturen (P2P)



lukas.feiler@lukasfeiler.com
http://www.lukasfeiler.com/lectures_malware

Danke für die Aufmerksamkeit