
openHPI Course: Cyberthreats by Malware

# Adware and Spyware

**Prof. Dr. Christoph Meinel**
Hasso Plattner Institute
University of Potsdam, Germany

# Adware

**Adware** – malware that display **advertisments** (**ads**) in addition to their actual functionality

- Most often installed within the web browsers disguising as genuine or legitimate program/plug-in
- Shows deceptive, flashing, pop-up advertisements on any website to the users
- Could trick users to
  - install malware or unwanted software
  - go to fake phishing website
- In most cases harmless and easy to remove however it could be **very annoying** for the users

# Adware
# **Example: Fireball**

- In 2017, Fireball infected 250 million computers and devices, and 20% corporate networks worldwide
- Spread mostly by unknowingly installing the adware alongside a genuine program
- Hijacked web browsers
  - change default search engine to fake malicious search engines
  - track user's web activities
- Capable of executing malicious codes on victim machines
  - dropping additional malware
  - steal victim's credentials

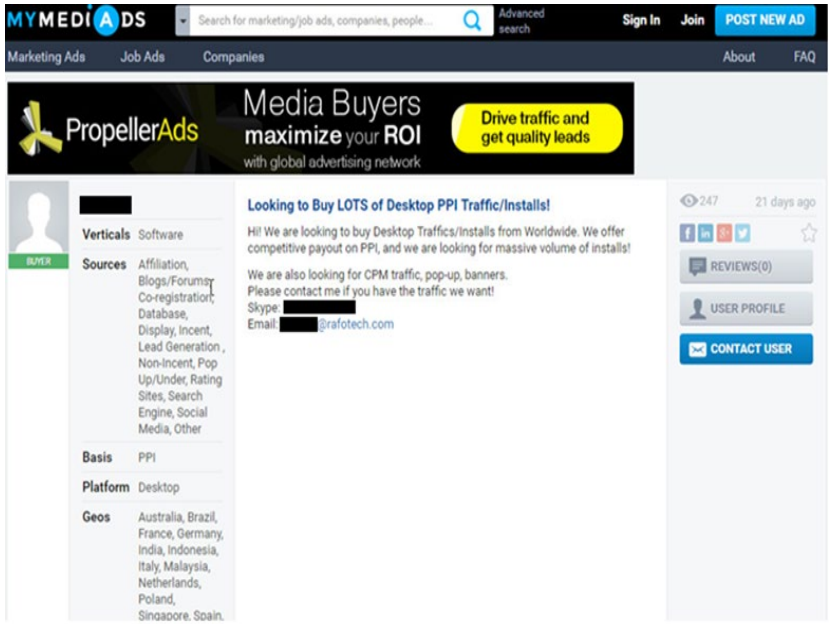


Figure 4: Bundling in Action

Source: https://blog.checkpoint.com/2017/06/01/fireball-chinese-malware-250-million-infection/

# Spyware

**Spyware** – malware that records and steals confidential information of the victims

- Could be installed when installing a seemingly legitimate software or by exploiting vulnerabilities in the system
- Run quietly on the background process that gather information about the users
  - emails
  - banking details
  - username and password
  - …
- Collected data about the victims could be misused or sold to third-party without their consent, e.g., in the Darknet or to data vendors

# Spyware
# **Example: DarkHotel**

- Targeting high-profile people staying in a hotel, such as business executives or government leaders
- Attackers first inject malware to the hotel’s server before the victim arrives at the hotel
- As soon as the victim connects to the hotel’s WiFi, attacker performs a spear-phishing attack to mislead the victim to install the spyware
- Uses several malware components to gain access to the system and steal sensitive information of the victim
- Finally, attackers delete the malware from the hotel‘s server and network to avoid getting dedected

# Adware and Spyware
# **Protective Measures**

- Pay attention to what you **click** and **download**
  - do not install programs from unknown sources
  - do not click on the links from suspicious emails
  - in case of doubt, inform yourself beforehand whether the program is legitimate and genuine
- When installing programs, make sure that no unwanted **"free tools"** are installed at the same time
  - can often change during the installation process be voted out
- Use **Anti-Virus** and **Anti-Malware scanner** to detect and remove malware
- Use **Adblocker** in the web browser to stop showing unwanted advertisements