openHPI Course: Cyberthreats by Malware

Carberp

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

Carberp

Example of a complex and dangerous malware

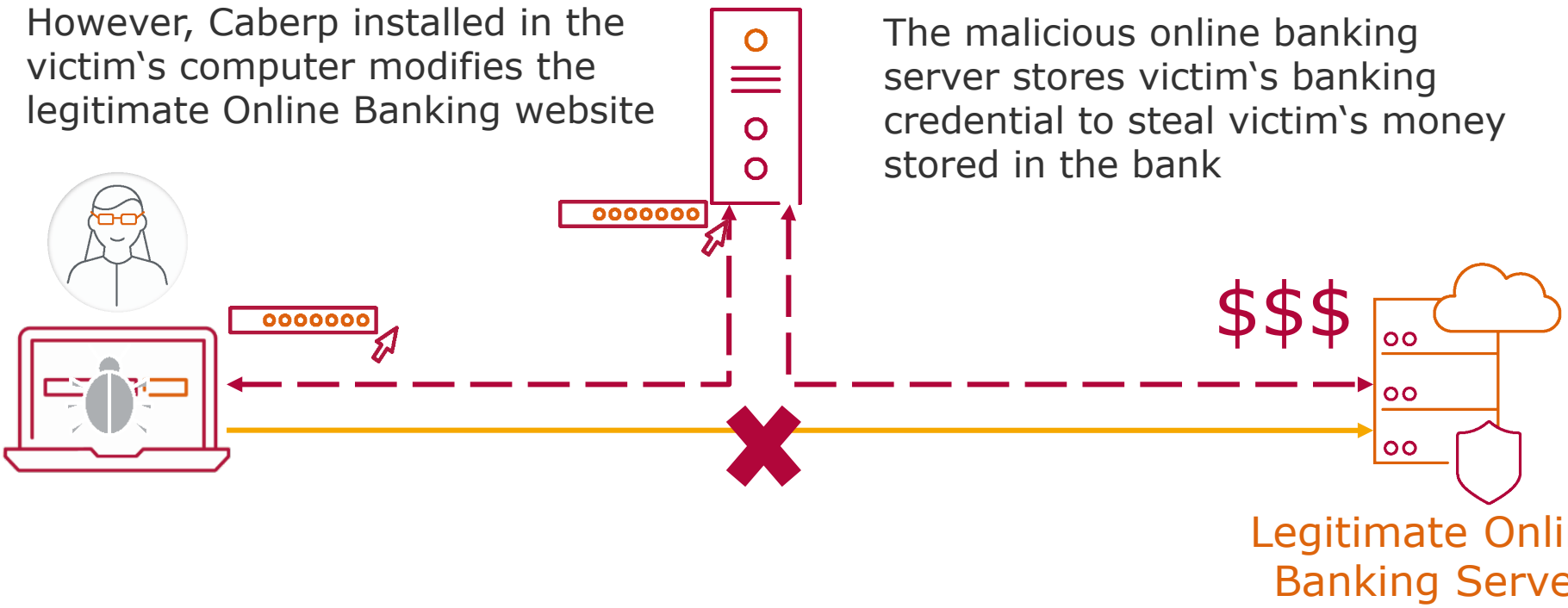
- First discovered in 2009 that stole banking credentials to siphon off millions of dollars from the bank accounts almost exclusively in Russian speaking nations
- Spread by hacking and creating "bookmarks" of the malware on popular and publishing sites
- It records user's keystrokes and spoofs websites that copies itself to locations that do not require administrator privileges
  → **Keylogger + Spoofing Attack**
- It could eliminate other malwares and antivirus programs already running on the infected systems by installing additional programs onto the system
  → **Trojan**

Carberp

Malicious Online Banking Server

However, Caberp installed in the victim's computer modifies the legitimate Online Banking website

The malicious online banking server stores victim's banking credential to steal victim's money stored in the bank



Legitimate Online Banking Server

The victim tries to login to Online Banking website by supplying the username and password

The victim unknowingly sends the banking credential to the cybercriminal's malicious online banking server

Carberp

- Carberp modified the online banking's web page on the fly to trick users to download fake mobile banking application
  → **Phishing Attack**
- This would allow Carberp to send the money to cybercriminal's bank account undetected by capturing transaction authentication number (TAN) necessary to authorize the money transfer
  → **Man-in-the-Middle Attack**

Source: https://securelist.com/carberp-in-the-mobile/57658/

Carberp

- Carberp's source code was leaked online in 2013
  - it was sold for $50.000 before got leaked
  - anyone could rent the malware service ranged from $2.000 to $10.000 per month
- Since then Carberp has
  - infected around 150,000 PCs in Australia between 2012 and 2013
  - been used as the foundation for Carbanak backdoor
  - multiple derivative malwares