Detecting Malware Initiating Traffic on Mobile Devices
Marián Kühnel, Ulrike Meyer

Motivation
• Android is the most popular mobile OS
• Easy to install and write new apps with any functionality
• Anti-malware solutions are still insufficient [1]
• Mobile malware is on the rise [2]

Mobile Malware Analysis
• We analyzed over 30 malware families targeting Android platform
• Samples found in the official Android google play market or alternative 3rd markets [3]
• We identified four categories:
  • Premium calls
  • SMS only
  • Premium SMS
  • SMS bombers - send many identical SMSs with intent to spam or DDOS a victim
  • Mobile spyware - reveal and monitor the identity of the user by obtaining IMEI, IMSI, model, product ID, operator name, location information, etc…
  • Botnets - remotely controllable apps
  • HTTP only - connect to a remote server via the Internet
  • RAT (mobile Remote Access Tool) - malware operating in userspace layer, attackers have full control of an infected device

Android Architecture
The filtering component responsible for network analysis is located in the userspace layer [4] and can be controlled via a Sensor App.

Our MITM for sending an SMS
Rild Filter Classifier Modem
AT+CMGS=Y\r
> \r PDU message \r\n
+CMGS: Z\r\n\n0\r
result

Classifier
• List-based filtering is very efficient but easily avoidable
  • Blacklist
  • Whitelist
• Rule-based filtering checks regular call modes
  • Pattern-based filtering is suitable for detecting constant botnets’ commands
  • Regex matching
  • Machine learning techniques help recognize unknown patterns
  • Support Vector Machine
• Challenge-response protocol ensures that a response has been generated by a person.

The Sensor App
• Inform a user about suspicious traffic
• Provide GUI
  • List all events from a local database
  • Whitelist calls, send blocked SMSs
  • Change blocking preferences

Conclusion
• Mobile malware has evolved considerably over time
• Filtering ingoing and outgoing traffic alone suffices for detection of relevant mobile malware
• Real-time approach with 95% detection rate
• For very low false positive rates is user interaction inevitable

Future Work
• Detect malware communicating over the Internet - block sending sensitive information to a remote server
• Support reputation based filtering - create trusted chains and buddy lists from user feedback
• Add security measures to protect the sensor

References