trends in mobile malware and importance of network based user protection

Sicherheitsnetzwerk München: Praxisforum „Anwender und Anbieter im Dialog“
Mobile Sicherheit im Unternehmen

Joachim Lüken, Nokia Networks, 04-12-2014
Threat landscape

Subscribers are unaware

- Not aware of security threats (Trojans, …)
- Do not install a mobile AV client

Operators are at risk

- Increased claims
- Increased churn
- Brand erosion
- Threats to the network

Growing security threats

- Total mobile malware grew 614% from 03/12 to 03/13

Mobile phones are attractive targets

- Personal information
- Device location
- Billing possibilities

Telco fraud loss

- $46.3 B in 2013
- $4.73 B due to Premium Rate Services

New opportunities

- Security is top concern for new services
- Security is pre-condition and enabler for new business

1) Juniper Networks Third Annual Mobile Threats Report 2013, 2) Communication Fraud Control Association estimation, 3) Nokia Acquisition and Retention Study 2013
Trends in mobile malware

less families ... more variants

Android Mobile Malware Families | Average Number of Variants Per Family
---|---
103 | 38

2012 | 2013

-45% | +50%

more intelligent ... customizable ... configurable

The malware can also intercept incoming messages and can receive commands from command-and-control servers to send specific text messages to particular phone numbers.
Anti-virus is dead?

… most modern antivirus programs don’t really do that great a job, only around 45 percent of attacks.

New concepts are needed!

... focus on ... tracking attacks as they take place, mitigating them, giving advice and investigating who’s doing attacking.

antivirus software ... are the random unsophisticated attacks - the "background radiation" of the Internet.

Symantec declared anti-virus dead, and it's right. Anti-virus won't protect you if someone designed to bypass antivirus software manages to get out there. The "background radiation" of the Internet.
Best-in-class protection = Network traffic pattern detection + device Anti-Virus

Client-based approach

> Signature-based detection
> Protects only if AV client is installed
> Device-dependent limitations
> Time gap for new malware detection

Network-based approach

> Analysis of traffic pattern behavior
> Protects all subscribers against fraud
> Device-independent
> Immediate detection of new malware
> Signatures but same behavior

Nokia approach

Traffic patterns

Signatures

detection rate

time
Mobile Malware detection, mitigation and prevention
Levels of Defense

External Analysis (offline)

Mobile Guard: Orchestration

Detection Mitigation Prevention Analysis

3 Prevent malicious activity (Fraud, final attack) Solutions for specific frauds, e.g. P-SMS sending and MTAN stealing use cases

2 Prevent intra Malware / Botnet Communication Detect and optionally block Malware and Botnet setup and configuration

1 Prevent attempt to infect UE Filter out Malware Code

Learn! Detect new malware and add to covered cases.
Network based real-time intelligence

Mobile Guard: Real-time monitoring / detection / mitigation

Content security: In-line web and e-mail filtering
Network based malware detection

**Detect:** Identify devices and subscribers, visualize event details and related threats and provide statistics.

**Monitor:** Correlate traffic patterns from telco network with malware patterns from:
- Malware intelligence database
- Self-learned patterns

**Clean:** Device AV client cleans malware on the device

**Mobile Guard**
- Security Insight (Dashboard)
- Action Engine (automated actions)
- Malware intelligence DB
- Correlation of traffic patterns

**Mitigate:** Minimize impact by applying automated actions, e.g.:
- Inform subscriber
- Block value added services

System intelligence is located here: smart detection of malware behaviour allows to close the gap …

**Radio**
- GSM/3G/LTE

**Core**
- SGSN
- GGSN
- SMSC
Detection taking advantage of mobile network data

Integration with GTP context data (IMEI, MSISDN, etc.)
- Native device-based view
- Visibility of internal traffic (also attacks against infrastructure)

Blacklists
- IP addresses, domains, URLs, packet payload signatures of CnC servers, dropzones, etc.
- SMS numbers and content signatures

Extended detection intelligence
- Failed DNS queries reveal Bots and Botnet structure using domain generation algorithms (DGA)
- Suspicious DNS results using round robin DNS, potentially with short TTL
- Characteristic communication patterns (e.g. ratio of numerical characters in the DNS names, ...)

Mobile network context data
- Geo location correlation
- Device type and usage expectation

Advanced Correlation
- Cross-interface correlation (e.g. Gn vs. SMS)
Nokia Security Center Berlin

Own and partner products solutions testing
→ On-site testing of miscellaneous scenarios.
→ Interoperability testing
→ Integration testing

Offering of deep insights in 3G/4G/LTE threat scenarios
→ NSC offers insights in latest threat scenarios and is furnished with real equipment which provides chances for hands-on enabling to eliminate security issues.

Platform for exchange
→ NSC serves as a platform for open exchange between several stakeholders about security solutions that protect mobile networks infrastructure, services and end-users.
Security you can rely on

Security in networks
- Radio access transport security
- Core network security
- Network operation security

Security in cloud
- Secured cloud architecture
- Professional security services

Security for end user
- Malware monitoring and detection
- Web content filtering

Security in future
- Backdoor detection
- Security trends and vision
- Air interface security
**Sensors**

**GTP sensor**

> Gn and Gp reference points are supported with GTP-C and GTP-U v1 protocols

> For LTE S5 and S8 reference points are required with GTP-C v2, or, in case of a combined S/PDN GW S1-U and S11 instead of S5.

Note: In case of a combined S/PDN GW (where S5 is internal) S1-U and S11 will be monitored instead of S5.
Malware classification according to MNO’s needs
Nokia’s Threat Classification Schema

Severity level

- high
  - Premium SMS Fraud
  - Premium Phone Call Fraud
  - App Purchase Fraud
- medium
  - SMS Fraud
  - SMS Spam
  - E-mail Spam
  - Phone Call Fraud
  - Wangiri
- low
  - No threats here
  - No threats here

MNO Services

- MNO Infrastructure
- Assets

- Subscriber Privacy and Security

- mTAN Stealing
- Phone Calls Spy
- SMS Spy
- Private Data Theft
- Media Theft

- Device Data Theft
- Location Tracking
- Browser History Collection
- Unwanted App Install and De-installation
- Browser Bookmark Collection and Modification
- Scam/Hoax App Purchase
- Settings Modification
- Fake Application
- Links to insecure App Stores
- Aggressive Advertisement
- Device Home Screen Modification

© Nokia Solutions and Networks 2014
Confidential
P-SMS trojans

- Trojan:Android/OpFake.M:
  - Fake Opera Mini browser secretly sends SMSes to premium numbers.

- Trojan:Android/Fakeinst variants:
  - Steal private data on phones, send SMSes to premium numbers.

- Trojan:Android/SmsSend.AC:
  - Sends SMSes to premium numbers.

- Trojan:Android/Mseg.A:
  - Steal private data on phones, secretly send SMSes to premium numbers.

- Android Vidro / EClips:
  - Fake video player application secretly sends SMSes to premium numbers.

Severity: High
Trojans stealing device data

- Trojan:Android/Fakeinst variants:
  - Appears as a downloader application, but secretly steals contact information from the infected phones

- Trojan:Android/Mseg.A:
  - Secretly sends contact list and other private information from the infected phones to a remote server

- Trojan:Android/GinMaster variants:
  - Secretly steals device specific data and submits them to a remote server

- Trojan:Android/FakeBattScar variants:
  - Hoax battery life optimiser program secretly tracks and submits phone location data

  - Secretly steals device specific data and submits them to a remote server

- Trojan:Android/Vdloader.A
  - Secretly steals device specific data and submits them to a remote server

- Trojan:Android/GoldDream.C
  - Secretly steals device specific data and submits them to a remote server

Severity: High
Copyright and confidentiality

The contents of this document are proprietary and confidential property of Nokia Solutions and Networks. This document is provided subject to confidentiality obligations of the applicable agreement(s).

This document is intended for use of Nokia Solutions and Networks customers and collaborators only for the purpose for which this document is submitted by Nokia Solution and Networks. No part of this document may be reproduced or made available to the public or to any third party in any form or means without the prior written permission of Nokia Solutions and Networks. This document is to be used by properly trained professional personnel. Any use of the contents in this document is limited strictly to the use(s) specifically created in the applicable agreement(s) under which the document is submitted. The user of this document may voluntarily provide suggestions, comments or other feedback to Nokia Solutions and Networks in respect of the contents of this document ("Feedback"). Such Feedback may be used in Nokia Solutions and Networks products and related specifications or other documentation. Accordingly, if the user of this document gives Nokia Solutions and Networks Feedback on the contents of this document, Nokia Solutions and Networks may freely use, disclose, reproduce, license, distribute and otherwise commercialize the feedback in any Nokia Solutions and Networks product, technology, service, specification or other documentation.

Nokia Solutions and Networks operates a policy of ongoing development. Nokia Solutions and Networks reserves the right to make changes and improvements to any of the products and/or services described in this document or withdraw this document at any time without prior notice.

The contents of this document are provided "as is". Except as required by applicable law, no warranties of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose, are made in relation to the accuracy, reliability or contents of this document. NOKIA SOLUTIONS AND NETWORKS SHALL NOT BE RESPONSIBLE IN ANY EVENT FOR ERRORS IN THIS DOCUMENT or for any loss of data or income or any special, incidental, consequential, indirect or direct damages howsoever caused, that might arise from the use of this document or any contents of this document.

This document and the product(s) it describes are protected by copyright according to the applicable laws.

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

© Nokia Solutions and Networks 2014