Dr.WEB®
since 1992

Defend what you create

DWCERT 030-12

Modern threats to mobile devices

Course outline

1. The criminal industry of malware production
2. Malware for Android
3. Mobile malware in the wild—does it exist?
4. Points of intrusion into mobile devices
5. An anti-virus isn't enough to protect a mobile device
6. Information resources about 'mobile' threats

1. The criminal industry of malware production

In the past, the creators of malicious software were lone programmers. Today's malware is developed by professional virus writers. This is a well-organized criminal business involving qualified system and application developers.

Structural elements of some criminal organizations

In some cases, the roles of the attackers inside criminal organizations can be subdivided as follows:

1. **Organizers:** people who organize and guide the process of creating and using malicious software. Malicious software can either be used directly or sold to other criminals or their associations.
2. **Participants:**
   - Malware developers
   - Malware testers
   - Researchers who look for vulnerabilities in operating systems and application software for criminal purposes
   - 'Experts' on the use of virus packers and encryption
   - Malware distributors and social engineering experts
   - System administrators who ensure that the operating environment is safe within a criminal association and control botnets

Such a working arrangement lets criminal organizations test their malware to ensure that current versions of anti-virus software cannot detect it. This allows criminals to bypass anti-virus protection and deploy viruses and Trojans onto PCs and mobile devices. Any anti-virus program, however good it is in tests for detection by heuristic procedures, will be powerless.

As a result, with ever increasing frequency, criminal organizations are creating 'targeted' threats – malicious programs developed to infect specific, relatively small groups of PCs or mobile devices (customers of the same bank, for example). Typically, these are malicious programs that don't have much impact on an infected PC and go undetected at the moment of **penetration**. Such circumstances let malicious programs go undetected for a long time.

The switch to 'industrial' methods of spreading malware in the wild has meant that only those malicious programs that are not detected by anti-virus software, even when heuristic mechanisms are utilized between updates, are being released. This has led to an increase in the number of malicious programs remaining undetected at the time of penetration.

2. Malware for Android

Most malware is created to infect Android-powered devices. The Android platform is the most attractive for criminals because:

- This platform is widespread: statistics show that in 2013, 80% of all mobile devices run the Android platform;
- It has an open code, allowing criminals to find vulnerabilities;
- It's possible to install applications from spontaneous (not always trusted) sources;
- Mobile device manufacturers do not always update software and firmware in a timely manner.

Threats to Android

Modern handhelds, running OSs with great possibilities, are attractive targets for hacker attacks. This is evidenced by the steady growth in the number of mobile-targeted malicious programs being received by the Dr.Web anti-virus lab.

- Mobile devices provide cybercriminals with more opportunities for spying than PCs do. Many of them are equipped with cameras, and all of them have microphones. Some devices have a GPS navigator. All of these are helpful in different situations so long as the owner maintains control of the device. If that control is intercepted by criminals, mobile devices take on other possibilities. For example:
- **Confidential information stored on your device can be accessed:** passwords (e.g., online banking system passwords or social network account passwords), bank account numbers and many other details. This opens up opportunities for criminals to blackmail users, collect and sell their information, or swap out their data for bogus information. (Android.AntaresSpy.1, Android.SmsSpy).

People use mobile devices in both their private and professional lives. Employees working at home or travelling on business use their personal devices to store corporate information and enter company websites. **That's why the theft of confidential information and passwords from personal devices is so dangerous.**

- **Some mobile device functions can be blocked or managed remotely** – criminals can intercept inbound short messages in order to harm users or their business competitors at just the right moment. (Android.Wukong, Android.SmsSpy, Android.Gongfu).
- **SMS messages can be sent and calls to premium-rate numbers made without user consent**, resulting in direct monetary damage (Android.SmsSend, Android.SmsBot).
- **Criminals can steal money**—from user bank accounts and from online payment systems.
- **Criminals can spy on users** —they can eavesdrop on conversations (toggle on the microphone), receive data from a GPS navigator on a user's location (to see whether they are present or absent in certain locations), take pictures of a user's location (turn on a camera and video recorder); and track what websites a user has visited, as well as incoming and outgoing calls, messages, and SMS.

Banking Trojans for mobile devices

Today, programs that intercept SMS containing mTAN codes, which many banking institutions use to confirm online banking transactions, are the most dangerous.

Examples

- **The banking Trojan** Android.SpyEye.1 **and its new version for PCs.** When users visit a bank website whose address is present in the Trojan horse's configuration file, this malicious program inserts texts or web forms into web pages, so customers loading a page of the bank's site into their browsers will see a message stating that a new bank security policy has been introduced and that in order to access their account (online banking system) they need to install a special application on their mobile device that will supposedly prevent the interception of their short messages, but will actually contain the Trojan horse SpyEye.
- **The malicious program** Android.Pincer **which can intercept short messages.** This malicious program is spread as a security certificate that supposedly must be installed onto an Android device. If a careless user installs the program and attempts to launch it, Android.Pincer will display a fake notification about the certificate's successful installation. Having launched successfully at startup, Android.Pincer will connect to a remote server belonging to criminals and send it information about the mobile device. Android.Pincer makes it possible for a malicious program to be used for targeted attacks and to steal specific messages, for example, those containing mTAN codes sent by banks.
- Android.Fakealert — a representative of the malware family that passes itself off as an anti-virus application for Android. It informs users of viral threats and states the price for their removal.
- Android.Spy — a multifunctional Trojan spy that has the ability to read and write contacts, receive and send SMS messages, define GPS coordinates, read and write browser bookmarks, and obtain information about a mobile device's IMEI and phone number. It possesses functionality for implementing special web searches and for navigating through specific browser links.
- Android.DownLoader — Trojan programs that download and install another malicious application on Android-powered devices.
- Android.Backdoor — is a family of Trojan programs that infects Android-powered mobile devices. These programs carry out attackers' commands'.
- Android.Basebridge — representatives of this Trojan family can send and intercept inbound short messages, send information about mobile devices to a remote server and install other malicious applications.

To familiarize yourself more thoroughly with mobile phone viruses, refer to Android threats in 2012, an overview prepared by Doctor Web specialists.

3. Mobile malware in the wild—does it exist?

Unfortunately, malicious programs for Android do exist and constitute a real threat for users in different countries of the world.

According to statistics acquired using the Dr.Web anti-virus for Android:

- **In September 2013**, users performed scans about 17 million times, though the presence of malicious or dubious software was recorded more than 4 million times.
- The anti-virus monitor for Android detected 11 million threats **in October 2013**, and more than 4 million threats to Android were discovered by the scanner.

The most common threats to Android are:

- The Trojan family Android.SmsSend;
- The Trojan family Android.SmsSpy;
- The Trojan spy Android.Spy.

Also very common are the Trojans Android.DownLoader, Android.Backdoor, Android.Gingersploit, Android.Basebridge and Android.Fakealert, as well as such adware as 'not a virus Tool.SMSSend', 'not a virus Tool.Rooter' and 'not a virus Adware.Airpush'.

4. How do malicious programs penetrate mobile devices?

1. **Through software vulnerabilities.** A vulnerability is a flaw in an operating system or application software that can be exploited by a virus to corrupt data and interfere with its operation.. Theoretically, any error in program code can be used to cause harm to the system in general.

   All software has vulnerabilities.

   Most are in Windows, affecting PCs and laptops, and in Android, affecting mobile devices.

   Software developers do their best to close vulnerabilities, especially critical ones, but sometimes virus writers find them before that happens (i.e., zero-day exploits that are still only known to virus writers or have not yet been closed by the software vendor).

   To eliminate vulnerabilities (close the gap in defence), users should **update their mobile software in a time manner**— all the programs, not just the anti-virus.

2. **Through the Internet.** Many websites, regardless of the content, can be infected with viruses or malicious scripts. **Infection occurs when users visiting infected sites and are made to** download and launch files with the extension .apk.

Astonishing fact

Websites that are more likely to be sources of malware and phishing attacks

- Sites related to technologies and telecommunications
- Business websites: business media, business news portals, accounting-related sites and forums, online courses/lectures, services to improve business efficiency
- Adult content websites and resources for downloading free programs

Through these sites, the criminals who compromised them can watch for victims and redirect them to infected sites. Pirated distributions can also carry viruses or Trojans.

3. **Through mobile redirects.**

   Even if you are confident that you use your mobile device to visit only well-known, completely safe sites, this misconception may result in significant financial losses. The majority of websites are controlled via CMSs (Content Management Systems) which are used to edit and publish content and promptly change a site's design and structure. Most modern CMSs are distributed under the terms of open source licenses, i.e., for free, which means anyone can become familiar with their back code. This enables attackers to analyze the structure of the CMS components, find vulnerabilities and exploit them to compromise sites administered using such a program.

   With the help of compromised websites, cybercriminals can spread various malware programs, the most «popular» being the various modifications of Android.SmsSend. Trojans of this family are designed to send SMS messages to premium numbers and to subscribe users to various services with chargeable content so that a fee can be debited from the subscriber's account.

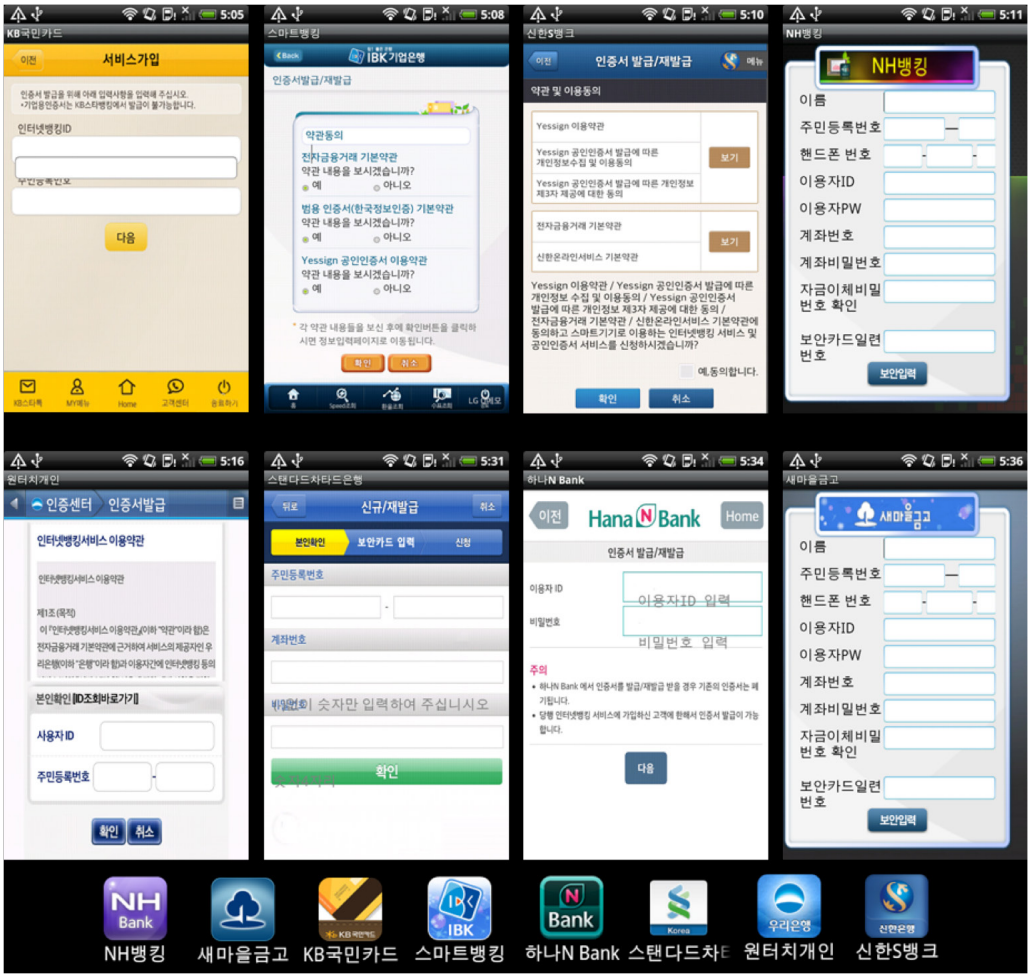
   According to Doctor Web's analysts, about 3% of the websites in the Russian segment of the Internet redirect users of Android smartphones and tablets to malicious sites that spread dangerous software. This means that more than 45,000 sites can infect a variety of Android-powered devices with Trojans. Including fraudulent and phishing sites, the total number may be as high as 100 thousand to 200 thousand.

   The special free service Dr.Web URLologist lets users check links for mobile redirects and warns of any lurking danger. This is particularly useful for users whose mobile devices lack anti-virus software.

4. **Through phishing and social engineering.** Phishing attacks pose a serious danger to users of Android-powered devices. Through such attacks, cybercriminals try to trick their victims into turning over confidential information (logins, passwords, phone numbers, etc.), engaging in precarious activities, transferring money from their bank cards or installing malicious programs. The attackers can use:
   - Sites that simulate the look and functionality of true resources (postal services, banks, online stores, and social networks);
   - SMS, sent supposedly on behalf of banks, major companies, and government institutions;
   - Trojan applications that are similar to authentic programs but under false pretenses demand that users enter confidential information.

Having fallen for the tricks of network criminals, users can not only lose access to their favorite online-services but also get ripped off!

Examples of phishing sites



5. **Through the unwitting actions of users.** Even if a malicious program can't exploit a vulnerability to penetrate a system/software, users are always ready to help.

   Most modern malicious programs aren't viruses—because they can't self-proliferate. They are created in the hope that users will distribute them.

   Using different tricks (social engineering techniques), criminals make their victims install malicious programs, open malicious files, visit compromised sites, etc.

For example, Android.Plankton, which collects and transmits information about compromised devices, was downloaded manually more than 150,000 times (!) from the official application store Android Market (formerly known as Google Play).

5. An anti-virus isn't enough to protect a mobile device

An anti-virus offers protection against viruses and malicious programs, particularly Trojans. **But today this level of protection isn't enough.**

Only comprehensive protection, such as Dr.Web for Android, can protect against any type of malware used by fraudsters for cybercrimes. Such protection should include an anti-virus, anti-spam, anti-theft and an URL filter like Dr.Web Cloud Checker.

- **Anti-spam** – shields against unwanted calls and SMS messages.
- **Anti-theft** – helps find lost or stolen mobile devices, blocks them and, if necessary, remotely deletes private information from them. Information on lost or stolen mobile devices (including access passwords and logins) can be stolen by hackers. A single anti-virus can't protect information if the violator or the person who found the device wants to examine it.
- **URL-Filter Cloud Checker** – limits access to potentially dangerous sites. It is especially useful for children who don't understand the danger of some websites.

IMPORTANT!

Some anti-virus vendors claim to have a Parental Control component in their Android protection products.

However, a product possessing full control over this operating system is IMPOSSIBLE to create at present.

The setup default for the Android browser and the Google Chrome browser for Android does not allow true parental control to be employed since any user can open a page anonymously, and no software can trace that user's steps.

Therefore, unlike its competitors, Doctor Web does not position its URL-Filter Dr.Web Cloud Checker as a parental control tool.

6. Information resources about 'mobile' threats

- News about threats to mobile devices
- Dr.Web URLologist – checking Internet links for 'mobile redirects'
- Virus library

Doctor Web

125124, Russia, Moscow, 3d street Yamskogo polya 2-12A
Phone: +7 (495) 789-45-87 (multichannel), Fax: +7 (495) 789-45-97

www.drweb.com