Bezpečnost mobilních systémů

Erika Čížová, CIZ0031

Zajištění bezpečnosti systému

- Izolace procesů – sandboxing
- Povolení přístupu – permissions
- Ochrana paměti zařízení – šifrování dat

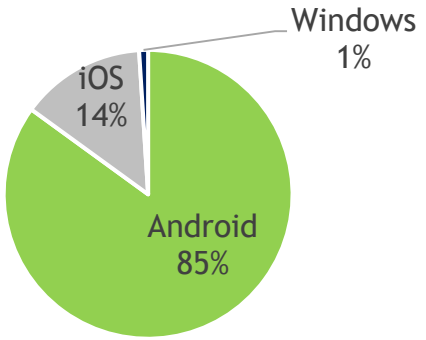
- Monitorování zdrojů -> detekce malware
  - Baterie, paměť, síť

- Software pro ochranu zařízení
  - Antivirus a firewall, tzv. Turing test, biometrická identifikace

Zajištění bezpečnosti systému

- Opatrnost uživatele
  - Povolení přístupu aplikace
  - Šifrování zařízení a SD karet
- Pokročilá nastavení zařízení
  - Debug mode, detekce podezřelých aplikací
- OS přizpůsobený výrobci zařízení
- Sledování sítě
  - Filtrování spamu, šifrování informací

Srovnání bezpečnosti OS

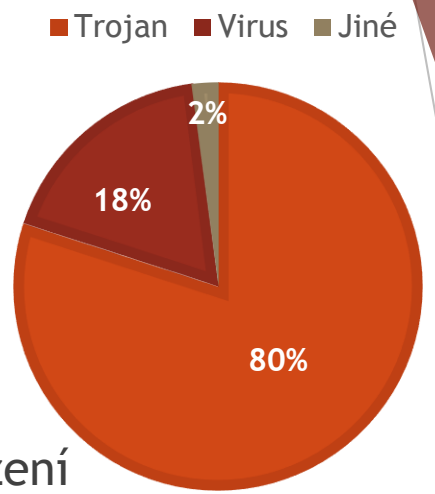


- **iOS**
  - Pouze na zařízení od Apple
  - Přísné požadavky na aplikace, které budou nahrány na AppStore
  - Testování aplikací
  - Uzavřený OS

- **Android**
  - Open source code
  - OS na mnoha různých zařízení + výrobci upravují OS podle svých požadavků
  - Akceptovatelnost aplikací na Google Play Store

- **Windows mobile**
  - Uzavřený OS, omezená možnost individualizace -> nižší riziko zavirování

Mobilní malware



- Trojský kůň – umožňuje externím uživatelům připojení k zařízení
- Virus – připojení sebe sama do legitimních programů a provádění procesů paralelně s programem
- Worm – program reprodukující sám sebe do jiných zařízení v síti
- Spyware - program, který využívá internetové stránky k odesílání dat bez vědomí uživatele

- **Fáze útoků**
  - Infekce
  - Dosažení stanoveného cíle
  - Šíření sebe sama dál

Možné cíle útoků a hrozby

- Data
  - čísla kreditních karet, ověřovací informace, soukromé informace, hesla …
- Identita
- Dostupnost
- Vytvoření backdoor pro další malware

- Škodlivé aplikace, odkazy na sociální sítě

Jak se malware šíří?

- Oficiální app store
- Third-party app store
- SMS
- QR kód
- Bluetooth
- Sociální sítě
- Reklamy
- USB

Úprava aplikace na malware

1. Download jakékoliv aplikace ze storu
2. Dekompilace
3. Stažení/napsání malware kódu
4. Zkopírování souboru s malware kódem do složky obsahující existující zdrojový kód aplikace
5. Provedení změny v manifestu pro spuštění kódu malware před zbytkem aplikace
6. Úprava oprávnění
7. Kompilace modifikované aplikace
8. Upload aplikace do store

Ukázka kódu

```
if (packageName.startsWith("com.skype") && settings.isSkypeEnabled())
{
    injectView(MonitoredProcess.SKYPE);
}
private void injectView(final MonitoredProcess process) {
    Intent intent = new Intent(getApplicationContext(),
    OverlayActivity.class);
    intent.putExtra("package", process);
}
```

https://github.com/geeksonsecurity/android-overlay-malware-example/tree/master/app/src/main/java/com/geeksonsecurity/malwaredemo