Università di Roma Tor Vergata

V CONFERENZA NAZIONALE

Partenariato cybersecurity privacy

Cybersecurity: stato dell'arte, sistemi di difesa e resilienza

Roma, Palazzo Wedekind, Piazza Colonna 366, 4 aprile 2022

Online authentication and Social Engineering

Francesco Buccafurri

Simple Password

- Dictionary attacks, or… Password spraying
- Keylogger (or other Trojan)
- (Spear) Phishing or Pharming attacks
- Weakness of password recovery
- Exploiting passwords sold in the Dark Web (after data breaches)

Double-factor authentication (2FA)

- **How does it work?**
  - True random sent to the smartphone
    - *Through an SMS*
    - *Through an encoded call*
  - Pseudo-random number generated by a token or by a smartphone app:
    - *With no input (only a state, with a validity time)*
    - *Dependent on the input (as required by EU PSD2)*

Double-factor authentication (2FA): Attacks

- True random sent to the smartphone
  - *Through an SMS*
  - *Through an encoded call*
    - ✓ **SMS/Call Hijacking,**
    - ✓ **SIM swap,**
    - ✓ **Man-in-the-middle,**
    - ✓ **Remote Access Trojan (RAT)**

Double-factor authentication (2FA): Attacks (2)

- Pseudo-random number generated by a token or by a smartphone app:
  - *With no input (only a state, with a validity time)*
    - ✓ **Man-in-the-middle,**
    - ✓ **Remote Access Trojan (RAT)**
  - Dependent on the input (as required by EU PSD2)
    - ✓ **Remote Access Trojan (RAT)…but…**

- **Recent RATS:**
  - **Xenomorph**
  - ***GravityRAT (Android, but also Windows and MacOS)***

…Social Engineering+Smartphone+Procedure Vulnerabilities…

- **Phishing for RAT**
- **Vishing to force the installation of a malicious app**
  - *Awareness, discipline*

- **SIM SWAP and reinstalling the remote-banking app**
  - ***Fortify procedures:*** *AGCOM n. 86/21/CIR,*
  - ***Anomaly-detection:*** *BankItalia&AGCOM initiative (involving CERTFin and Mobile operators for API inteorperability)*

Conclusions

- ***Even with MFA (coompliant with PSD2) social engineering can be successuful***
- ***The smartphone plays a crucial role***
- ***Awarenss and Education are fundamental***