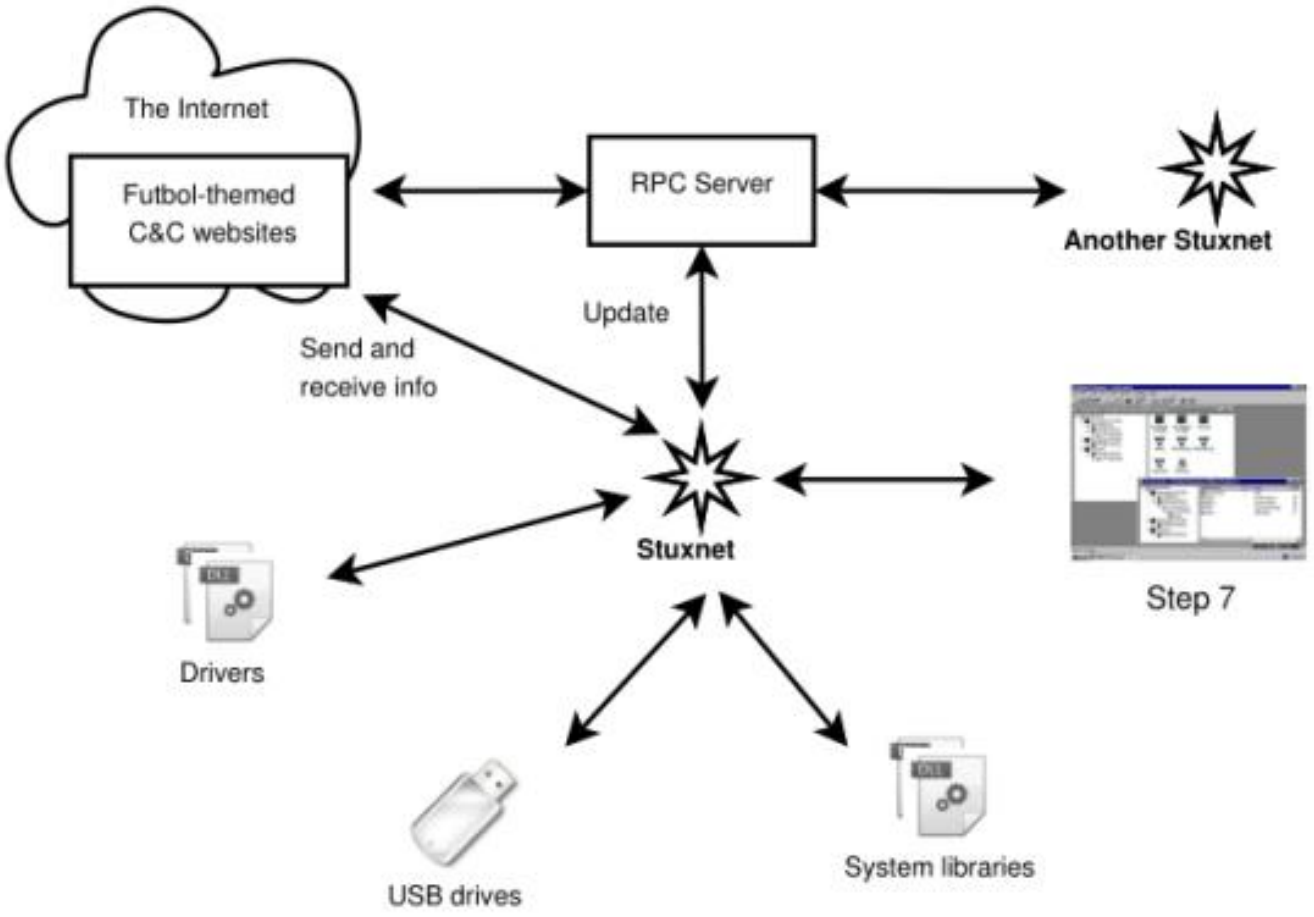
Advanced Persistent Threats

Advanced Persistent Threats (APT)

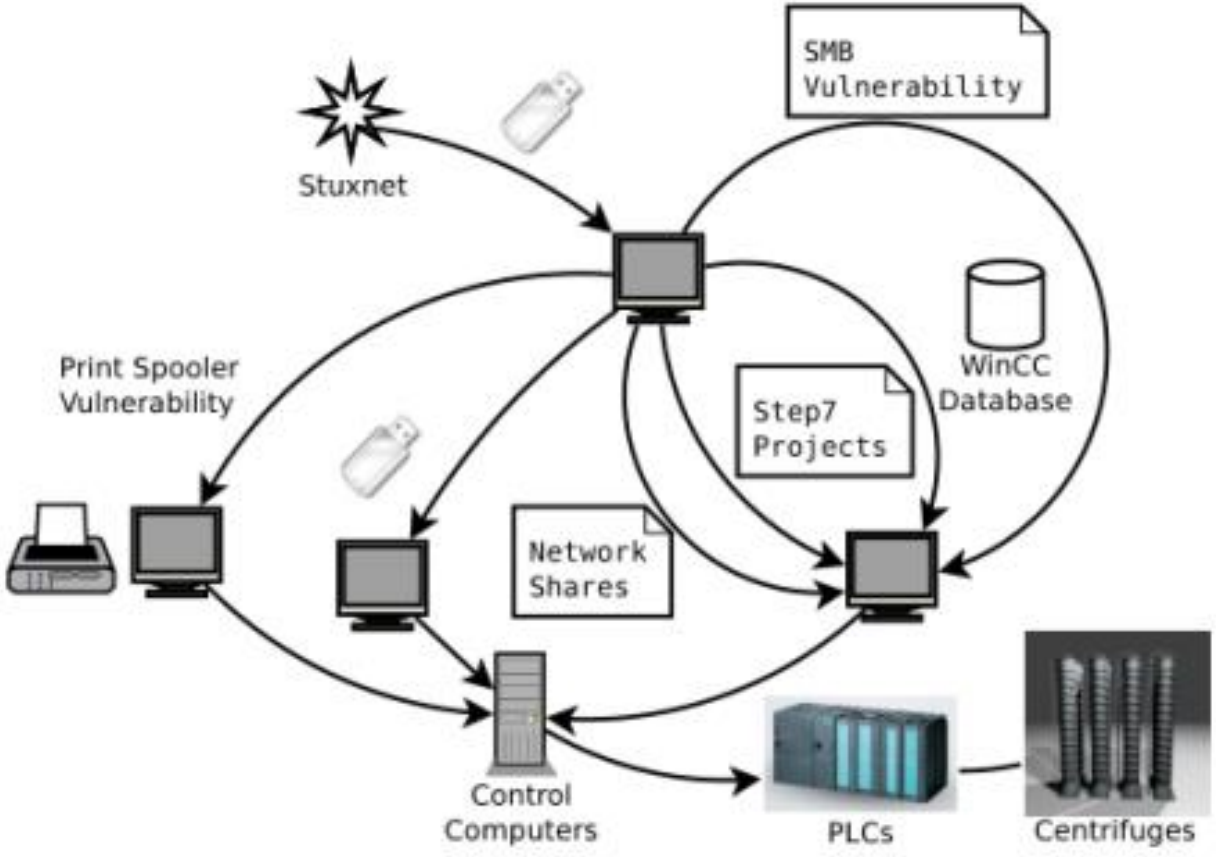
- Usage of the term:
  - Originally (US Air force): well-funded, organized attack groups that have interest in data theft
  - Now: cybercrime directed at business and political targets
- "Advanced" = combining different kind of attacks
  - Multi-vector (*vector* = "*path/method/scenario that can be exploited to break into an IT system*")
  - Multi-stage
- "Persistent" = structured series of attacks with long-term goals
  - Requires stealthiness to avoid early detection
- Requires funding and planning
  - Criminal organizations with financial goals
  - Governments
- Example: Stuxnet

Stuxnet: Components



Source: The Stuxnet Worm. P Mueller & B. Yadegari.

Stuxnet: Attack Paths



Source: The Stuxnet Worm. P Mueller & B. Yadegari.

Equation Group

- "Equation" = name given by Kaspersky lab to a group of "threat actors" because they love encryption algorithms
- Identity unknown
  - Active since 2001, maybe 1996
  - Traces of them seen in several attacks in different countries
  - NSA?

- Developed and used complex attack platforms
  - Many zero-day attacks
    (zero-day = a vulnerability unknown to the software authors/users)
  - Probably also responsible for some of the Stuxnet components (although not its creators)

Lifecycle of an APT

5. Evasion

4. Exfiltrate data

1. Preparation and reconnaissance

3. Spread in system ("Lateral movement") and find target data

Source: Wikipedia

2. Initial compromise

Other attack models (1)

"The Cyber Kill Chain" by Lockheed

Other attack models (2)

- MITRE ATT&CK matrix

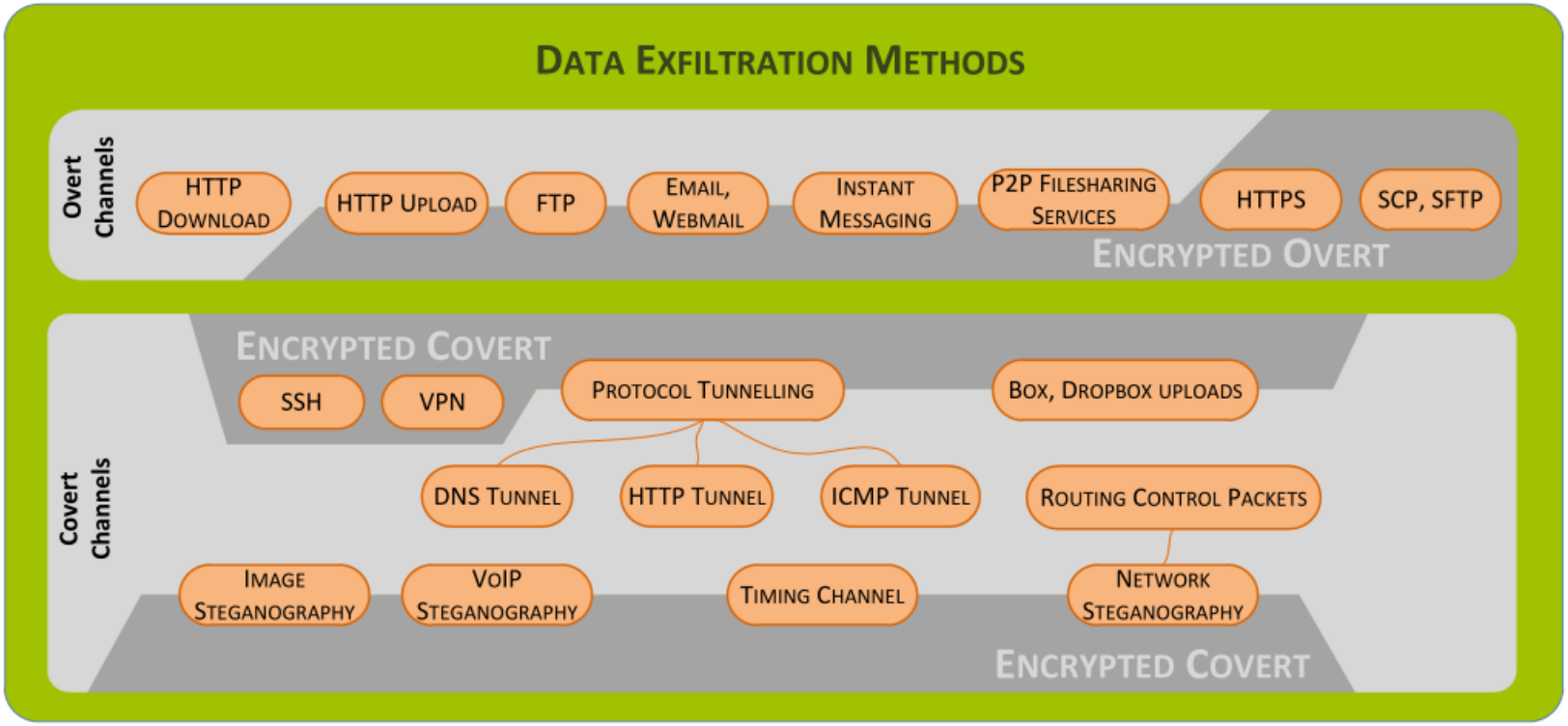
https://attack.mitre.org/matrices/enterprise/

  - Reconnaissance
  - Resource Development
  - Initial Access
  - Execution
  - ...

Initial compromise

- Hardest step
  - Systems are protected against attacks from outside, but weak once you are in (“Eggshell principle”)
  - Sensitive systems are isolated from the Internet (“air gap”)
- We have seen some techniques in the past weeks
  - DNS cache poisoning
  - Web attacks (cross-site scripting, SQL injection, etc.)
  - Buffer overflows
  - ...
- Human level is important: Social engineering!
- APTs often rely on zero-day attacks

Exfiltration



Source:Detecting and Preventing Data Exfiltration – Lancaster University

- Exfiltration traffic should be hidden or look innocent, so it is not noticed by admin or IDS
- Example: DNS tunneling (hiding data in DNS queries)

Evasion

- Requires knowledge of detection techniques used by the target system
- Possible techniques:
  - Slow attacks
  - Hide as normal network traffic
  - Encrypt payload
  - Detect VMs and honeypots! Could be a security expert analyzing you!
  - Delete log files
  - Manipulate the OS (e.g. the process list)
  - …

Lessons learned from APTs

- Requires multi-level defense
  - Deploy different detection and security techniques (“defense in depth”)
  - Defend not only against attacks from outside but also inside
  - Monitor outgoing traffic, too
  - Regular training for employees, e.g., how to detect a phishing mail