openHPI Course: Cyberthreats by Malware

Advanced Persistence Threats

Daniel Köhler
Prof. Dr. Christoph Meinel
Hasso Plattner Institute
University of Potsdam, Germany

Hack of the German Bundestag (2015)

07/2015

Hacked: Computersystem of the Bundestag offline for several days

https://www.heise.de/newsticker/meldung/Nach-Hack-Computersystem-des-Bundestags-wird-tagelang-abgeschaltet-2734034.html

- Cyberattack against IT-Systems of the Bundestag
  - Social-Engineering Email to the representatives
  - Initial access by compromised passwords
  - Further spread through use of self-developed Command & Control Server
  - Spread to further computers
  - Retrieval of all „new" documents

```
for %%G in (.pdf, .xls, .xlsx, .doc, .docx) do (
   forfiles /P F:\[…] /m *%%G /s /d +01.05.2015 /c
"cmd /c copy @path
C:\ProgramData\[…]\d\@file" )
```

APTs as Highly Specialized Attacks

Advanced Persistence Threats (APTs) are highly dangerous and specialized attacks

- Targeted Attack against highly sensible targets such as Government, Military or Industry

Motivation

- Wide-Spread information retrieval / Eavesdropping
- Deactivation / Destruction of critical infrastructure
- Political goals

What is special about APTs?

Advanced Persistence Threat

Advanced

- Highly developed, unobtrusive, secret attack methods
- Often using **Social Engineering** methods
- Excessive use of known and (currently) unknown weaknesses (so-called **0-Day-Exploits**)
- Attack often consisting of multiple steps

Persistent / Persistence

- Spanning over a long timeframe (months – years)
- Attackers attempt to stay onrecognized
- Attackers often have a very specific goal / target

Advanced Persistence Threat

Threat (dt. Bedrohung)

- Attackers are often organized teams
- Attackers often own (basically) unlimited resources
- Attacks are constantly observed and controlled by experts

Phases of an APT-Attack

Reconnaissance
- Information Retrieval
- Social Media, Internet, …

First Access
- Without attracting attention
- Often Social Engineering

Secure Access
- Usage of Remote-Access-Tools
- Command & Control Server

Lateral Movement
- Reconnaissance of further targets
- Spread to more computer

Achieve the Target
- Data Exfiltration, Sabotage…

Example: Stuxnet

Malware which has been detecten on the computer systems of iranian uran enrichment plants in 2010

- Abuse of various, formerly unknown **vulnerabilities**
  - 4 Security Vulnerabilities in Windows
  - Various vulnerabilities in control-software (SCADA) for uranium-centrifuges
- Attacks on control-systems have previously been only fiction from research papers
- Initial access through **Social Engineering**
  - USB-Stick containing Stuxnet malware was used in the factory

Example: Stuxnet

Expected Goal of the Attack:

- Sabotage of the iranian Nuclear program
- First variation of the Stuxnet worm has been seen in 2009
  - At that point in time it wasnt referred to as Stuxnet
  - Until July 2010 without broader discovery

Attackers had massive amounts of resources

- Early guess: attacker probably with access to **infrastructures of a state / country**
- According to insights from whistleblower Edward Snowden, the USA & Israel might be the creators of Stuxnet.