Unsichere Software-Updates und Infection proxys

Lukas Grunwald

DN-Systems GmbH Germany

CeBIT 2010- iX Forum

2010 Hannover

Software update cures it all

- Vendors publish security patches via Software Updates
- Adobe plans to install / update software for the Acrobat Reader autonomously
  - No user control any more
  - Background process while user is online
- Apple updates Safari and iTunes with Apple Update
- Microsoft updates in Background
  - (XP, Vista, W7, Server)
- How trusted are this update mechanism ?

Update via Internet

1. DNS Resolve of update cluster / hosts
2. Connect to the update server
3. Get a index of actual version
4. Calculate the needed patches / updates
5. Download the patch / updates
6. Install them on the target system

Attacks to updates

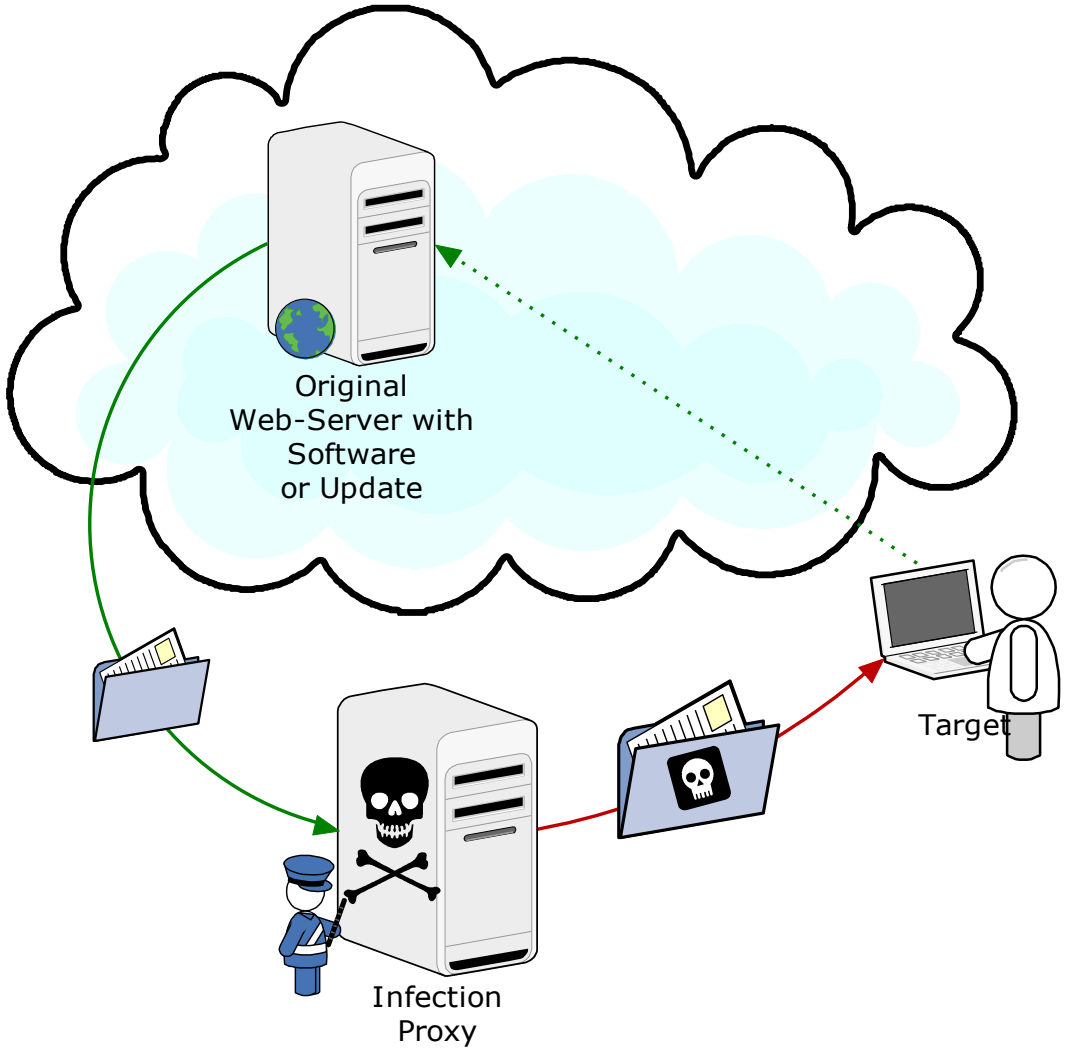
- DNS Spoofing to redirect to a forge server
- Transparent infection Proxy
  - Can sit on the wire, or as Trojan on the system
  - Drive By Exploits
  - Fake-Downloads from 3rd Party Download Sites
    - Google Search poisoning

Motivation for Poisoning

- Lawful Interception / Offensive Forensic
- Criminal Intention
  - Attack Home Banking
  - Zombie infection to get a Bot-Net Node
  - Referrer Poisoning go get sales margin
- Private Investigation
- Corporate Intelligence

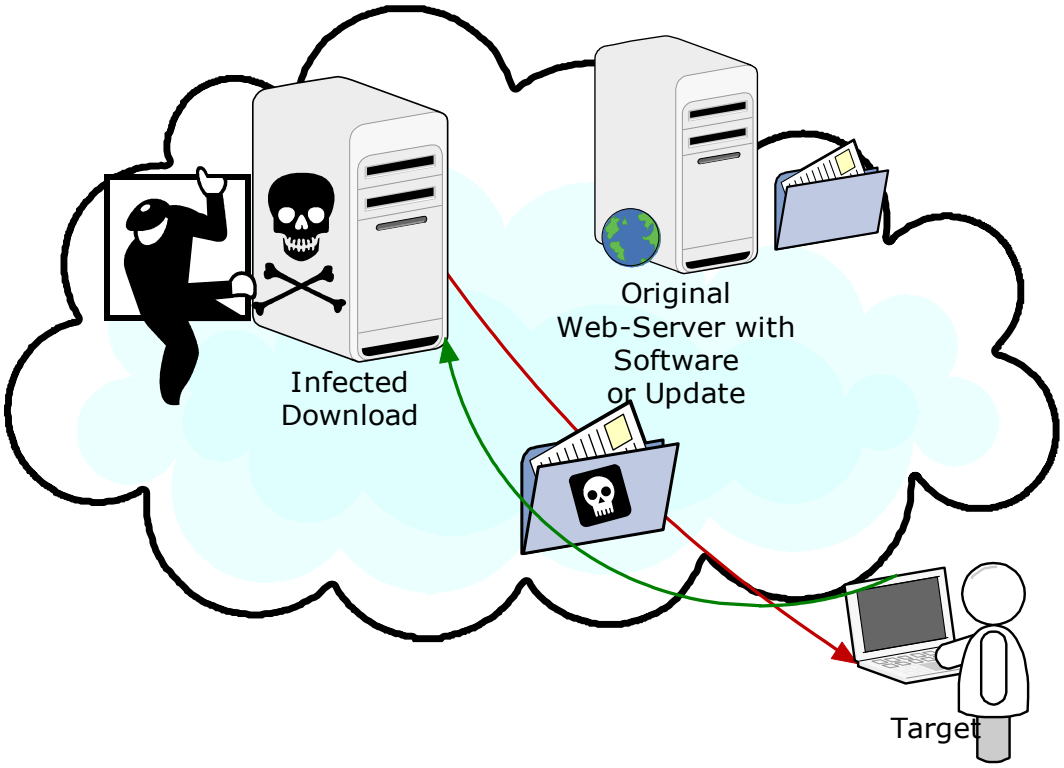
Poisoned Update Inband

- In-band Infection
- Download is diverted via transparent proxy
- Used for remote forensics
- Support from software industry will make it easy
- Possible with every software download / upload



Poisoned Downloads

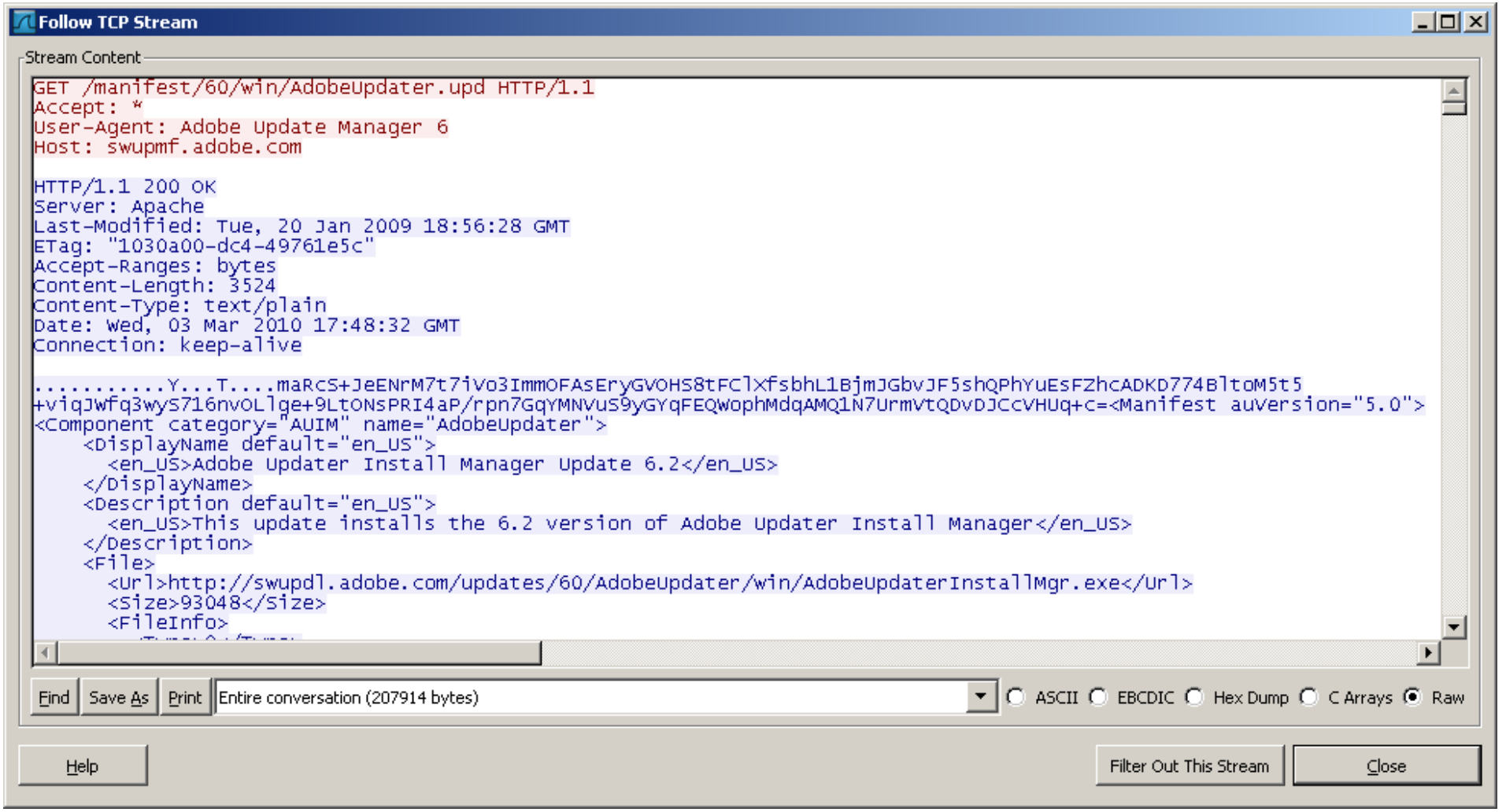
- DNS-Redirection
- Download from rouge server
- Mostly exploits
- Standard method for trojan infection
- Possible with every software download / upload



Some Updates as example

- Adobe Download Manager
  - Critical Security Flaw
  - Browser Plugin (DLM)
  - Any software could be injected and executed
- Adobe Acrobat is responsible for 80% of all known attacks over the last year

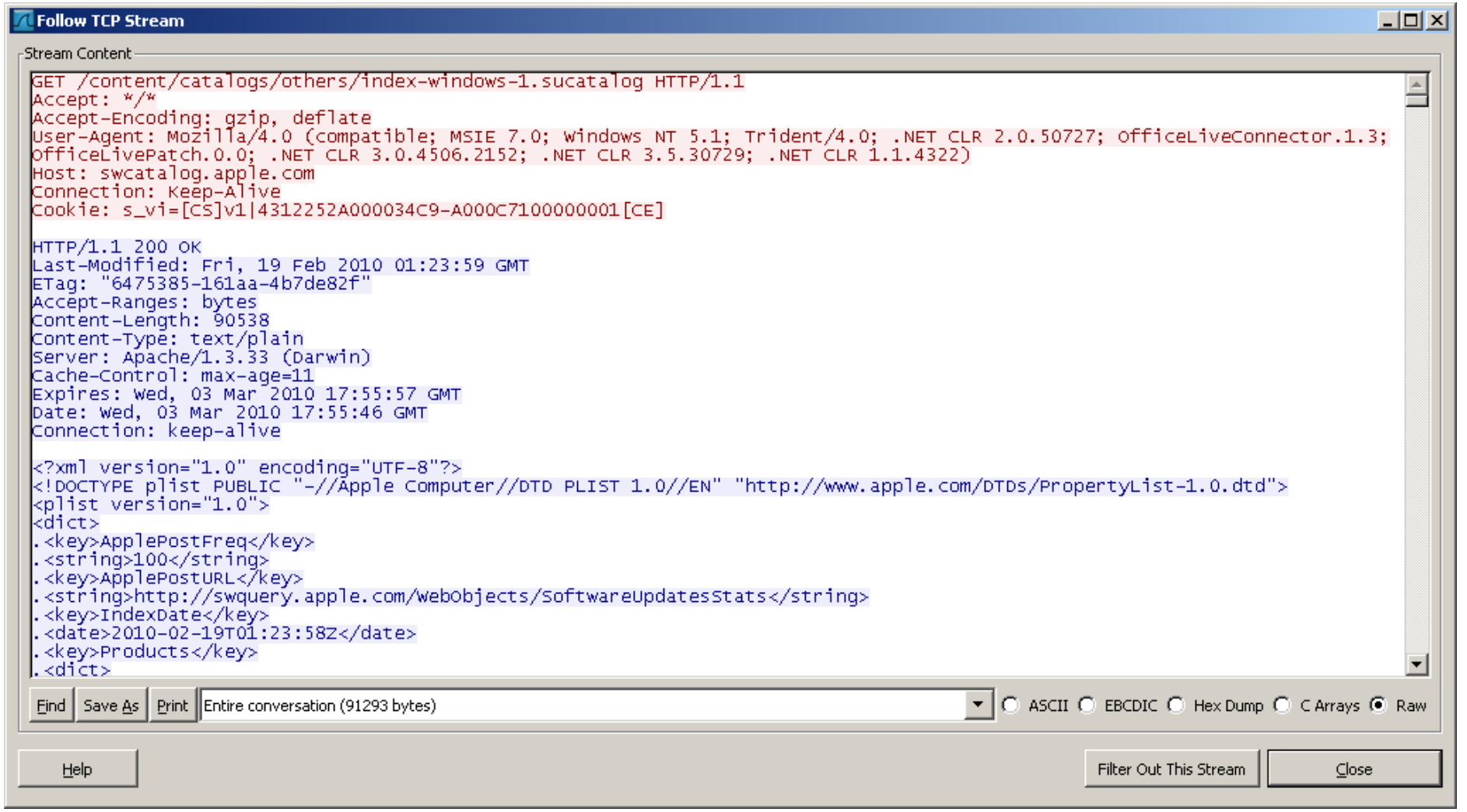
Adobe Update



Adobe Update

- Uses Signed Files
- CRL is implemented and updated before update
  - Lost Certificate is not fatal
- Update uses unencrypted HTTP
- Whole security depends on Adobe Certificates
- NO SSL or Secure Channel

Apple Update



Apple Update

- No CRL used lost certificate is fatal
- Uses Scripts during Updates
- Security depends only on URL
- No secure channel is used
- Software Distribution / Update is XML Based

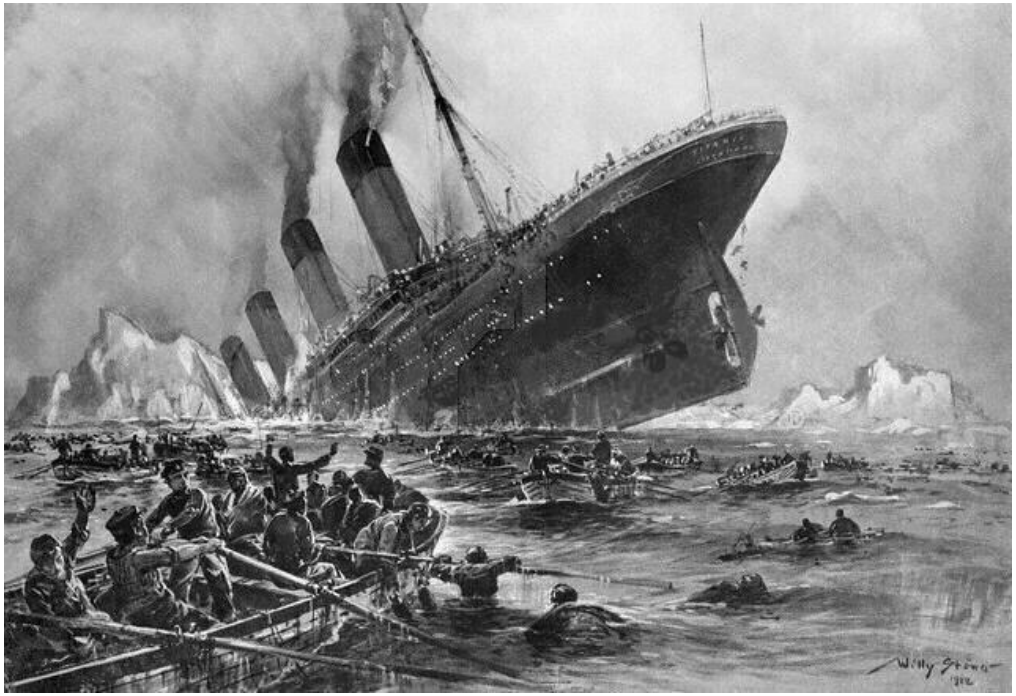
Microsoft Update

- Update is using CRL correct
  - Lost certificate is not fatal
  - Software segments are singed
  - Update uses HTTP (not HTTPS)
  - **Microsoft Update V6 is secure** as long no valid Signing Certificate is shared with Law-Enforcement or Criminals (Insider Attacks)

Avoiding Infection Proxys

- Verify MD5/SHA-1 hashes of downloaded software before installation
- Dangerous co-operation of system and software vendors
  - Trusted software signatures for LEAs
  - Creation of poisoned system software or operating systems
  - Installation via signed Vista system driver possible
- Open Source operating systems
- Self-compilation of software and system using publicly available source code (BSD / Linux / …)

Thank you, keep in mind …



High-tech ≠ High-security