

dn

Systems

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

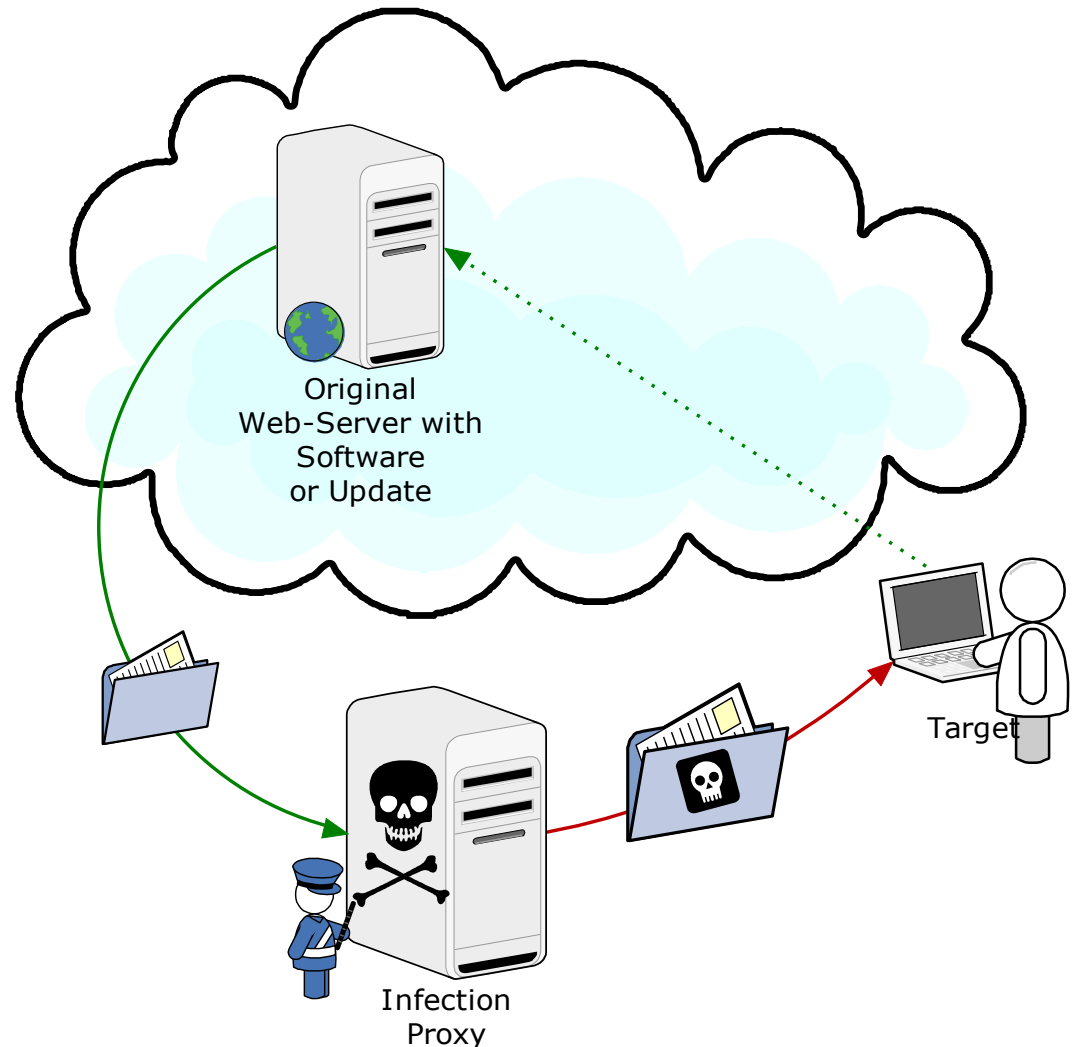
- DNS Spoofing to redirect to a forge server
- Transparent infection Proxy
 - Can sit on the wire, or as Trojan on the system
 - Drive By Exploits
 - Fake-Downloads from 3rd Party Download Sites
 - Google Search poisoning

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

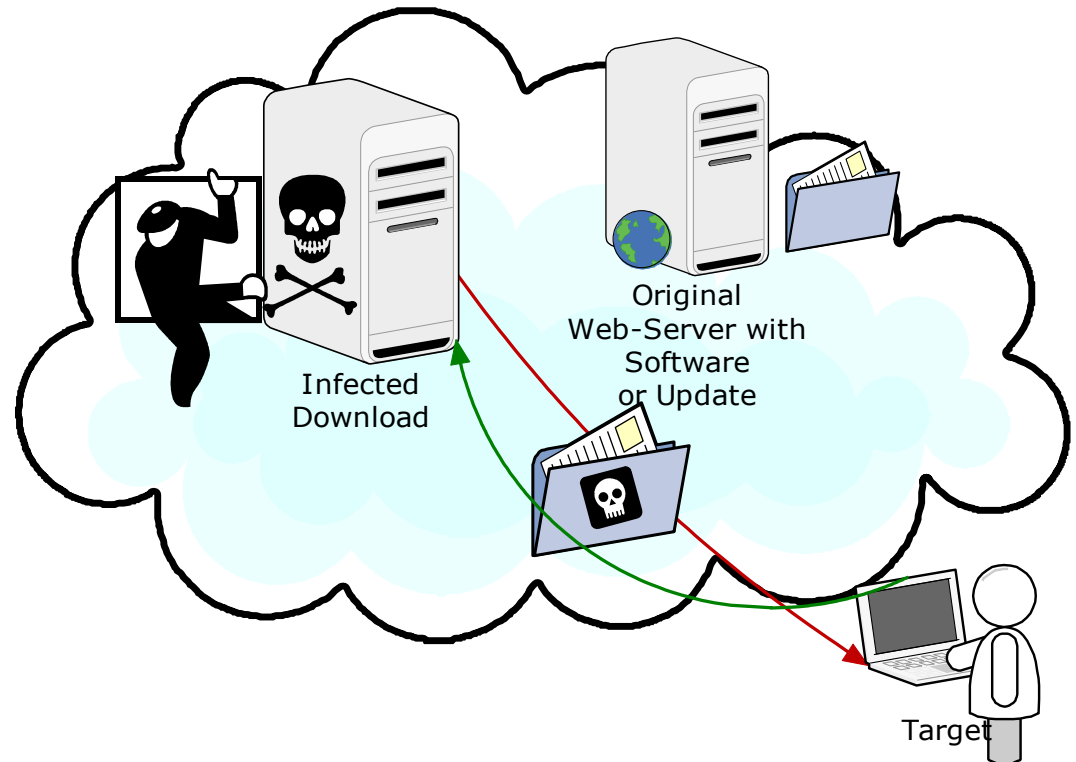
Poisoned Update Inband

- 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

The screenshot shows a 'Follow TCP Stream' window with the following content:

```
Stream Content
GET /manifest/60/win/AdobeUpdater.upd HTTP/1.1
Accept: *
User-Agent: Adobe Update Manager 6
Host: swupmf.adobe.com

HTTP/1.1 200 OK
Server: Apache
Last-Modified: Tue, 20 Jan 2009 18:56:28 GMT
ETag: "1030a00-dc4-49761e5c"
Accept-Ranges: bytes
Content-Length: 3524
Content-Type: text/plain
Date: wed, 03 Mar 2010 17:48:32 GMT
Connection: keep-alive

.....Y...T....maRCS+JeENrM7t7iVo3ImMOFAsEryGVOHS8tFC1XfsbhL1BjmJGbvJF5shQPhyUESFZhcADKD774B1toM5t5
+viqJwfq3wys716nvOLLge+9LtONS PRI4aP/rpn7GqYMNvUS9yGYqFEQwophMdqAMQ1N7UrmvtQDvDJCCvHUq+c=<Manifest auVersion="5.0">
<Component category="AUIM" name="AdobeUpdater">
  <DisplayName default="en_US">
    <en_US>Adobe Updater Install Manager Update 6.2</en_US>
  </DisplayName>
  <Description default="en_US">
    <en_US>This update installs the 6.2 version of Adobe Updater Install Manager</en_US>
  </Description>
  <File>
    <Url>http://swupd1.adobe.com/updates/60/AdobeUpdater/win/AdobeUpdaterInstallMgr.exe</Url>
    <Size>93048</Size>
    <FileInfo>
```

At the bottom of the window, there are buttons for 'Find', 'Save As', and 'Print'. A dropdown menu shows 'Entire conversation (207914 bytes)'. To the right are radio buttons for 'ASCII', 'EBCDIC', 'Hex Dump', 'C Arrays', and 'Raw' (which is selected). At the bottom right, there are buttons for 'Filter Out This Stream' and 'Close'. A 'Help' button is located at the bottom left.

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

The screenshot shows a 'Follow TCP Stream' window with the following content:

```
Stream Content
GET /content/catalogs/others/index-windows-1.sucatalog HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; officeLiveConnector.1.3;
OfficeLivePatch.0.0; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; .NET CLR 1.1.4322)
Host: swcatalog.apple.com
Connection: Keep-Alive
Cookie: s_vi=[CS]v1|4312252A000034C9-A000C7100000001[CE]

HTTP/1.1 200 OK
Last-Modified: Fri, 19 Feb 2010 01:23:59 GMT
ETag: "6475385-161aa-4b7de82f"
Accept-Ranges: bytes
Content-Length: 90538
Content-Type: text/plain
Server: Apache/1.3.33 (Darwin)
Cache-Control: max-age=11
Expires: wed, 03 Mar 2010 17:55:57 GMT
Date: wed, 03 Mar 2010 17:55:46 GMT
Connection: keep-alive

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple Computer//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
.<key>ApplePostFreq</key>
.<string>100</string>
.<key>ApplePostURL</key>
.<string>http://swquery.apple.com/webobjects/softwareupdatesstats</string>
.<key>IndexDate</key>
.<date>2010-02-19T01:23:58Z</date>
.<key>Products</key>
.</dict>
```

At the bottom of the window, there are buttons for 'Find', 'Save As', 'Print', and a dropdown menu showing 'Entire conversation (91293 bytes)'. To the right of these buttons are radio buttons for 'ASCII', 'EBCDIC', 'Hex Dump', 'C Arrays', and 'Raw' (which is selected). At the bottom right, there are buttons for 'Filter Out This Stream' and 'Close'. A 'Help' button is located at the bottom left.

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

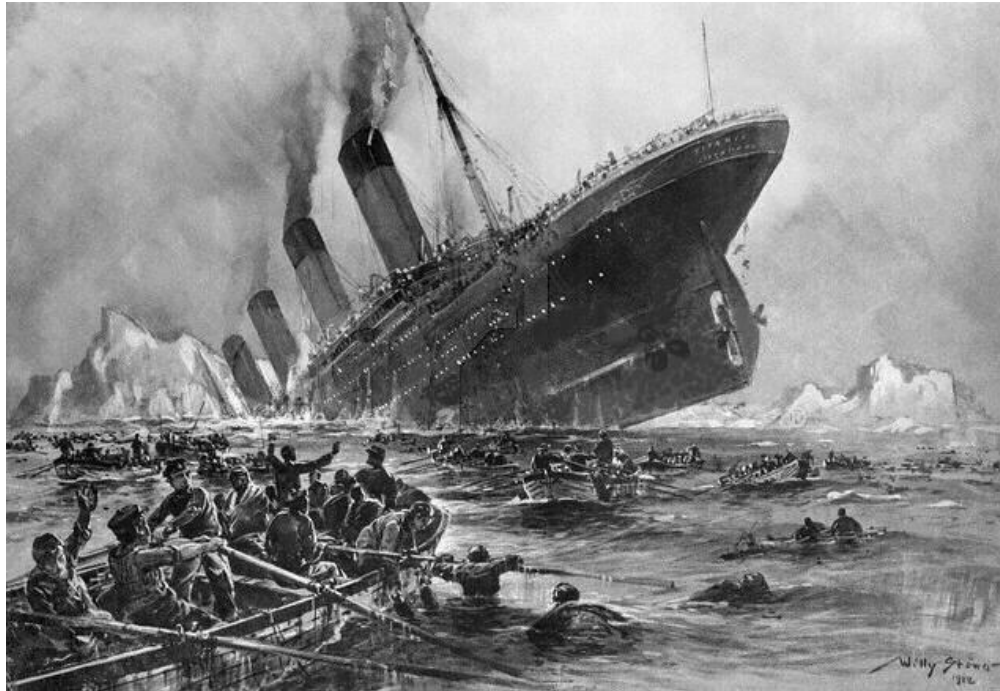
Microsoft Update

- Update is using CRL correct
 - Lost certificate is not fatal
 - Software segments are signed
 - 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