The Day Of The Update

Once upon an Update …

Itzik Kotler
Tomer Bitton

Update? I already donated

- Ability to delivery bug fixes or new features to existing customers of applications

- Natural inhibitors:
  - Punch Cards
  - BBS/Modem
  - Floppies/CD’s
  - Internet

What’s The Big Update?

- Updates are usually a background tasks, thus draw little attention from the user
- Most updates are binaries that gets executed on the updater machine
- An update can be used to manipulate sensitive data such as anti-virus rules
- Update can be silently tampered with it, leaving almost no trace behind

Catching an Update

- Feasible over a variety of MITM Attacks:
  - Wi-Fi via Open/Weak Cryptography
  - LAN via ARP Poisoning
  - WAN via DNS Cache Attack (Thanks Dan!)
- Wi-Fi is our favorite choice, common in Airports/McDonalds/Café shops and etc.

Subverting The Update Procedure

- Client asks Server whether it’s up to date
  - Replied with Negative Answer
- Client asks Server for Download Sites
  - Replied with Malicious Sites

OR

- Client downloads from a Known Site
  - Redirected into a Malicious Site

Subverting The Update Connection

- Spoofing Server Reply:
  - IP:
    - Invert source and destination addresses
  - TCP:
    - Invert source and destination ports
    - SEQ is received ACK
    - ACK SEQ is received DATA + SEQ
    - One Shot, One Kill Flags: PUSH + ACK + FIN
- FIN flag is muting the Server, and possibly causing the Client to disconnect afterward

Subverting The Update Agent

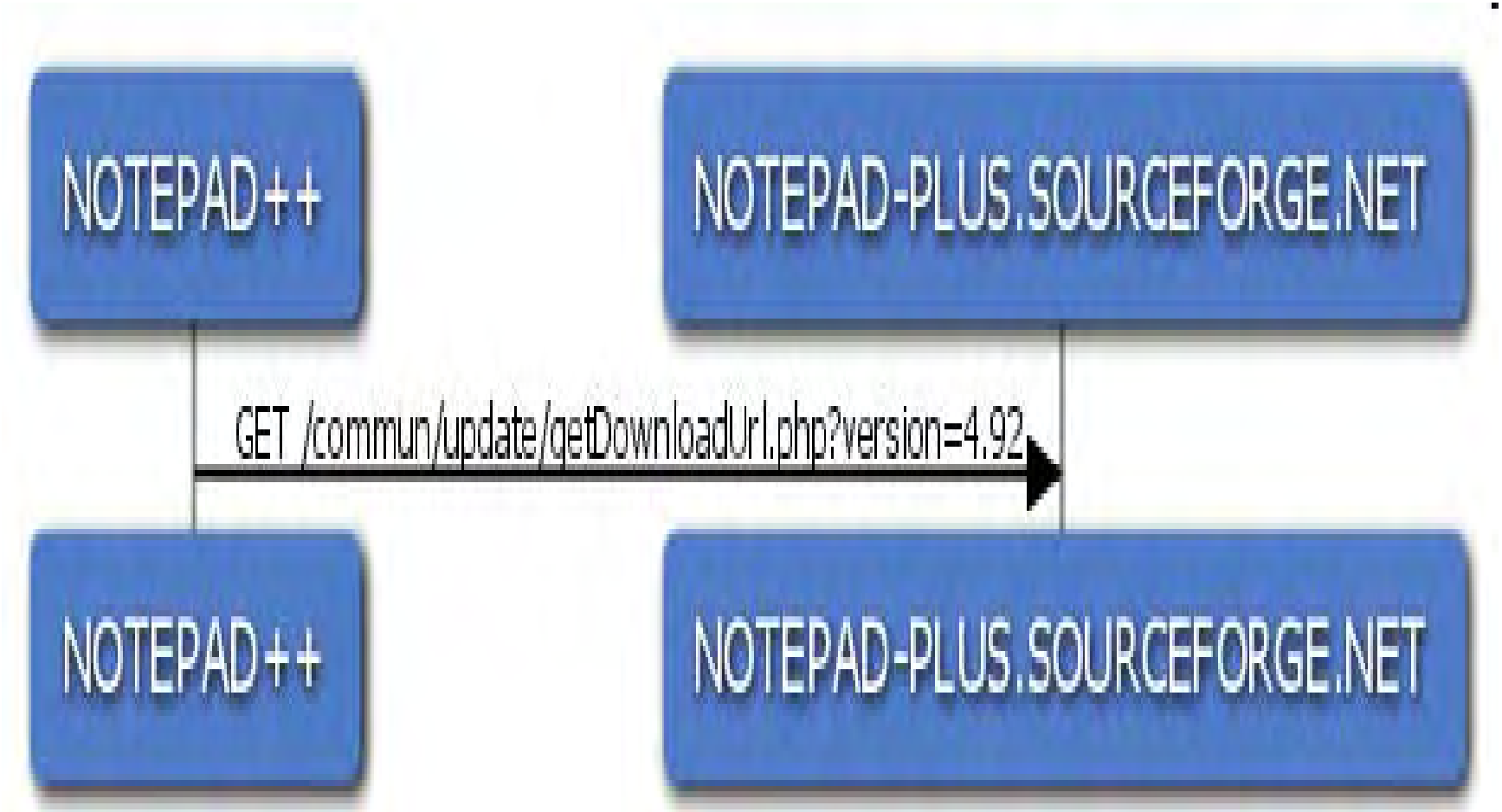
- Client accesses a Document (XML/INI/...)
  - Reply w/ 200 OK (Cooked Data)
    - Document contains Malicious Binary Sites
- Client downloads a File
  - Reply w/ 302 (Redirection)
    - Redirection to Malicious Binary Site
- Server
  - Will be Ignored (muted at Connection Level)

Attack Walkthrough:

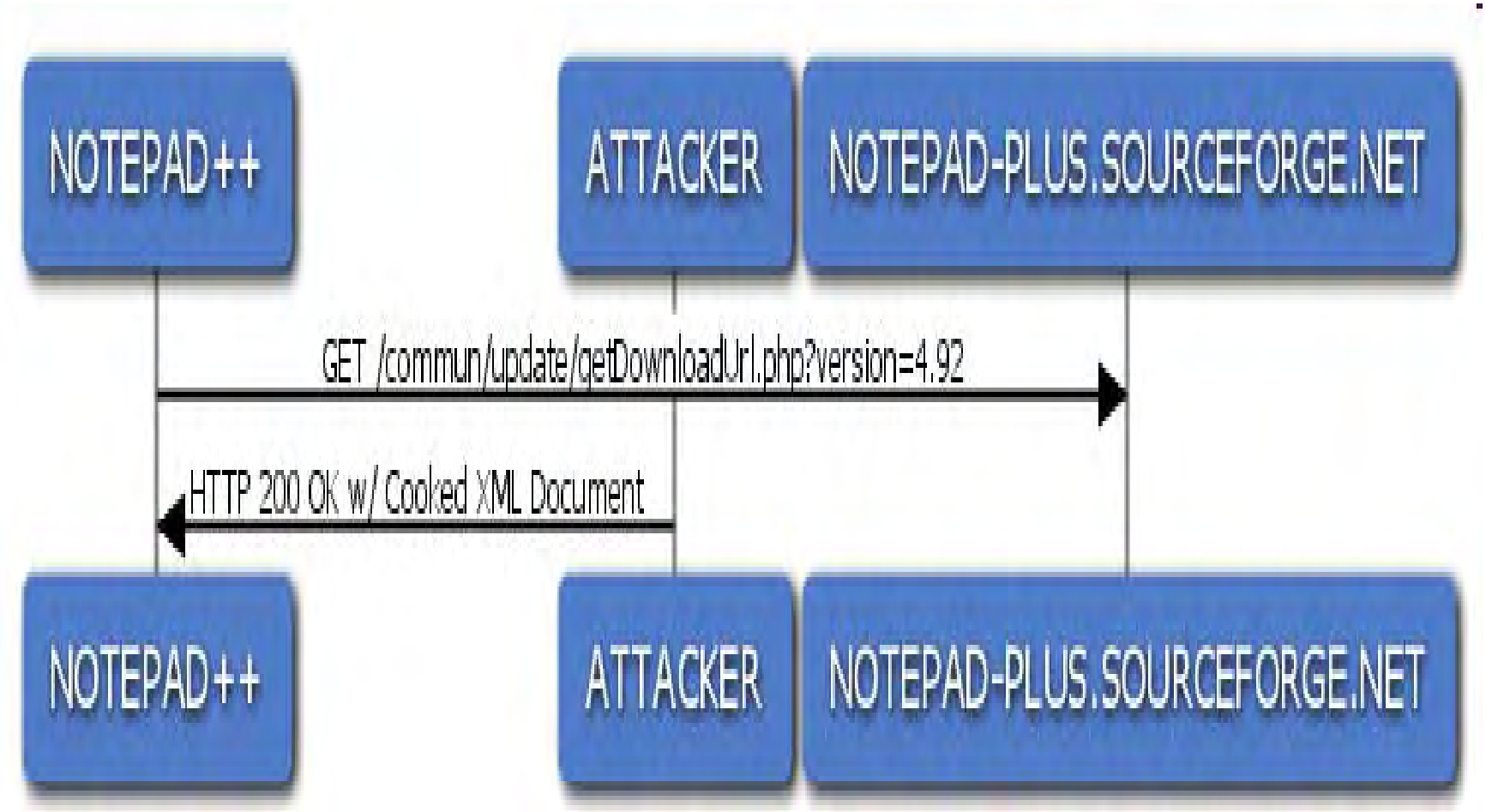
200 OK w/ Cooked Data

Target Application: Notepad++

Notepad++
Checks For a New Version



Replied w/ 200 OK (Cooked Data)



200 OK w/ Cooked Document

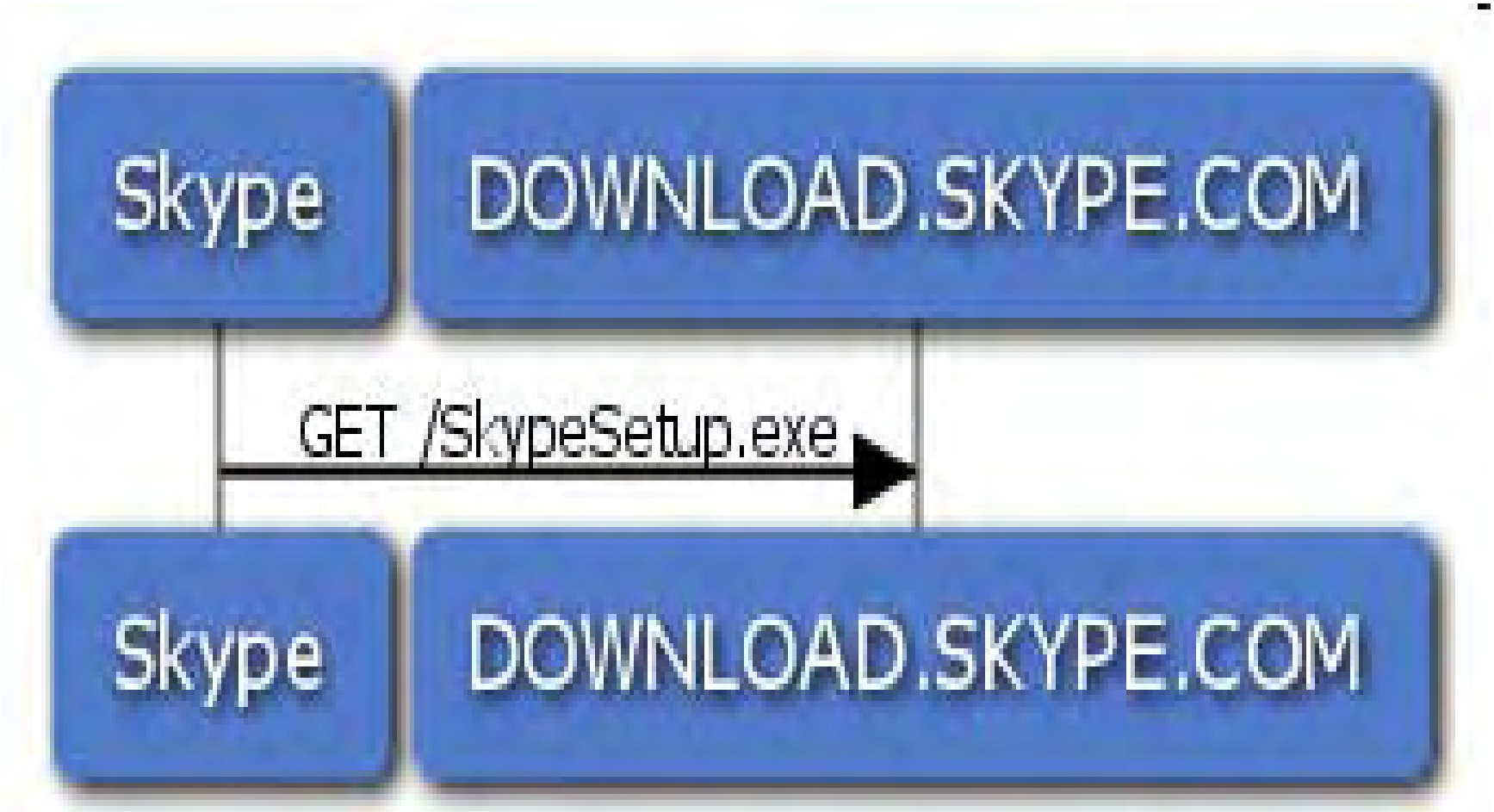
- Update expects:
  - List of Sites for Downloads
    - Upcoming downloads will go to our sites
  - Is There A Newer Version Available?
    - There’s always a “newer” version for you
- Summary:
  - Update will take place on our provided sites
  - One Shot, One Kill!

Attack Walkthrough:

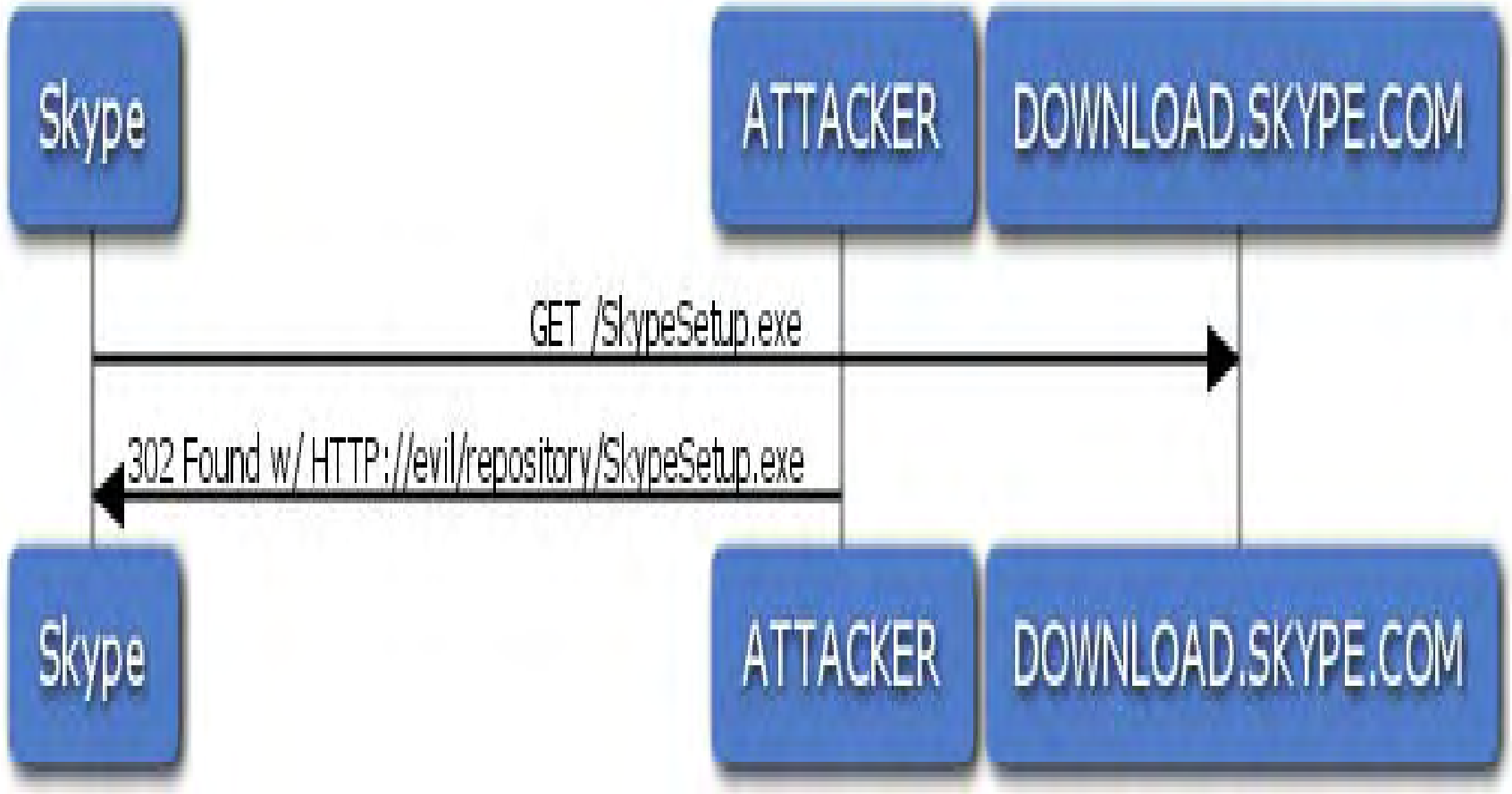
302 Found w/ Malicious Site

Target Application: Skype

Skype Downloads a Newer Version



Replied w/ 302 Found (M. URL)



302 Found w/ Malicious URL

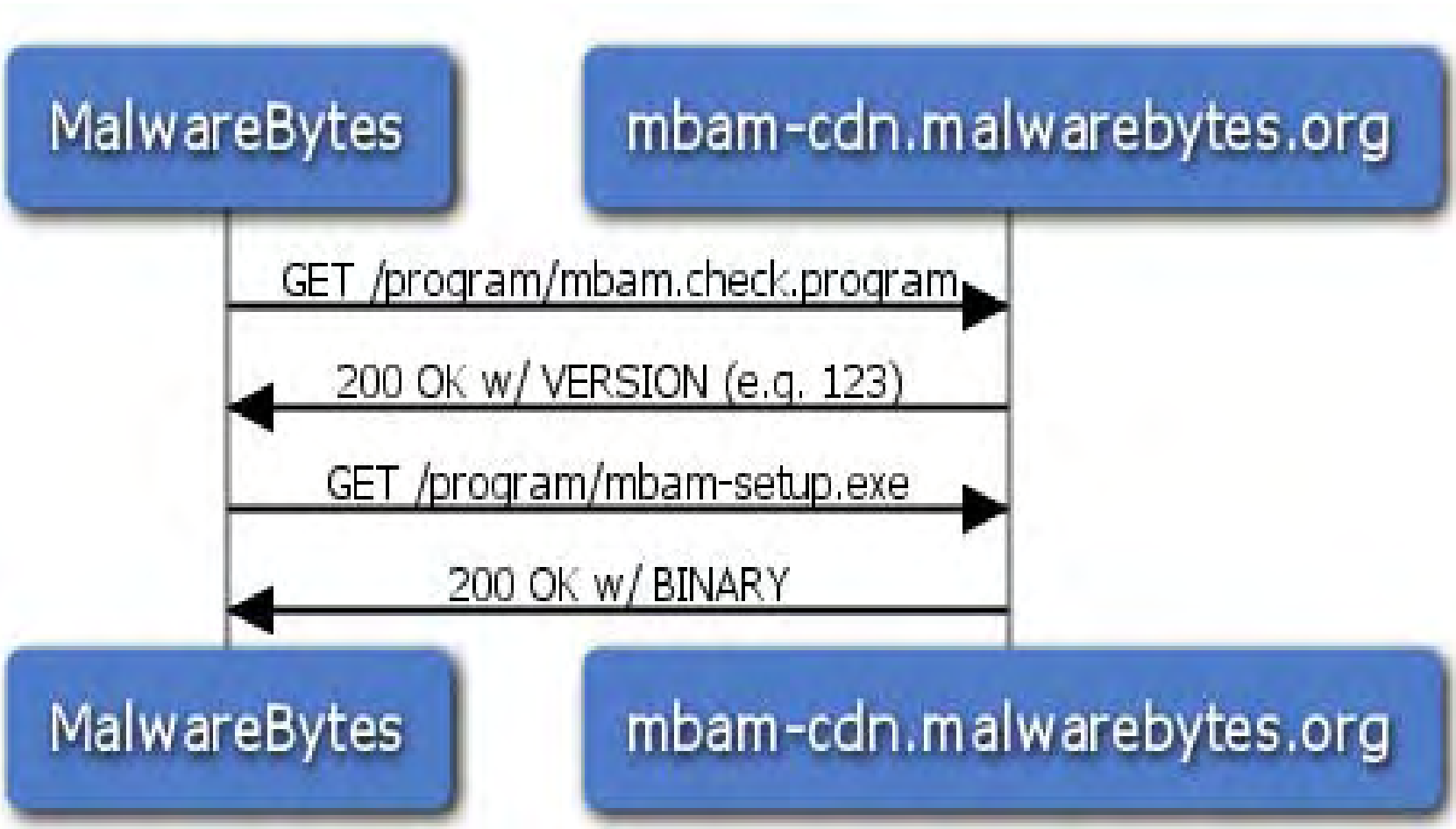
- Update expects:
  - 200 OK on SkypeSetup.exe
- Update receives:
  - 302 Found w/ SkypeSetup.exe
    - This download will go to our site
- Summary:
  - Pre-programmed URLs bypassed
  - One Shot, One Kill!

Attack Walkthrough:

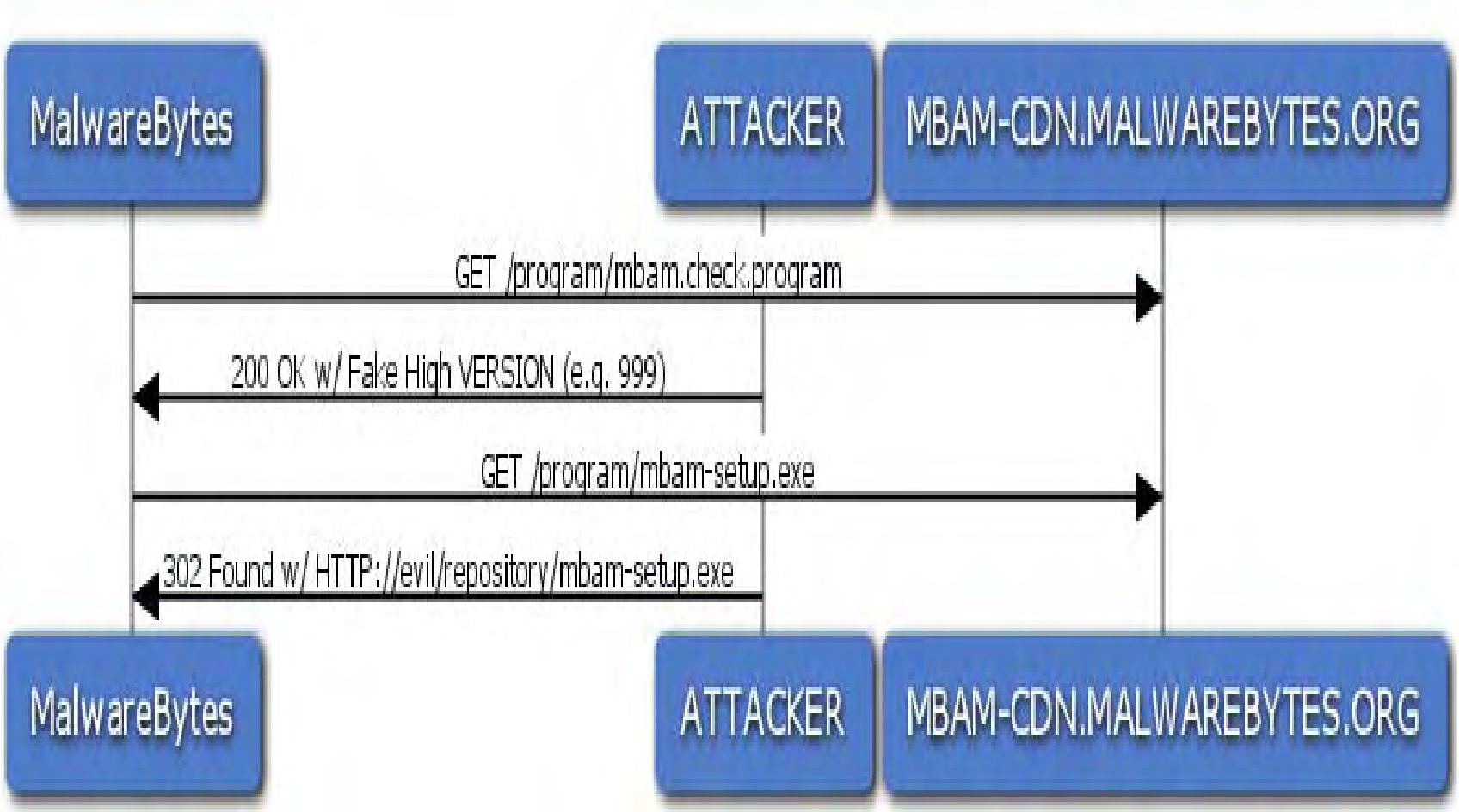
200 OK + 302 Found

Target Application: MalwareBytes

MalwareBytes Update Flow



Replied w/ 200 and 302



Combo Attack (200 + 302)

- Update document don’t contains sites
  - 200 OK only contains a positive update answer, no sites or other parameters defined
- Update has a pre-defined URL
  - 302 Found redirects the upcoming download to our own site

Time for an Update Check!

- Who's also Vulnerable?
  - *Alcohol 120*
  - *GOM Player*
  - *iMesh*
  - *Skype*
  - *Hex Workshop*
  - *Adobe PDF Reader*
  - *…*
- Let's see IPPON taking them down!

IPPON Targets Maintenance

- IPPON takes it’s targets from an XML file that contains triggers and responses

- IPPON Target specifics:
  - Response which is either static, dynamic (on the fly) or a redirection attempt
  - Trigger which is made of a given HOST, URL and can be equal to ANY

SSL Can Update Me Better?

- Generally yes, but surprisingly common implementations of it in Updaters not.
- SSL is expensive resource-wise, thus it’s not fit for an entire download session
- Update takes place in the background, there’s no little golden lock so not everybody puts the efforts

Update w/ Self Signed Certificate

- For an effective SSL the Server must present a valid, verifiable Certificate that costs money.
- Cheap SSL Solutions:
  - Update w/ Self Signed Certificate
  - Update w/ Third-Party Certificate (certificate validity not verified)
- Result:
  - Vulnerable, only provides looks ‘n feel!

Update w/ NULL Cipher

- SSL Server gets to pick Cipher Suite
- It’s possible to race condition ServerHello or ClientHello messages to gain visibility
- If Cipher is set to NULL, there’s little benefit for SSL
- Minimum Cipher Suite Strength should be set in advance to avoid such tampering

Update, for a better future

- Digital Signature
  - Update agent holds a public key, and can verify the download directly, or indirectly throughout a file that contains an md5/sha1
- SSL (The Right Way):
  - Must be Valid/Verifiable Certificate
  - Only needs to exchange an MD5/SHA1 of the upcoming download

Nothing but an Update Party!

- Proprietary Update Attack:
  - Playing w/ Anti Virus Rules
    - Anti Virus Attacks Legitimate Applications
    - Anti Virus Attacks Itself
    - Anti Virus Protects Virus
- Hit ‘n Run Mode:
  - If application saves, or maintains a list of latest download sites and you’ve managed to slip one – you’ve got an returning customer ☺
- Contagious Mode:
  - Embedding IPPON and run it on updater, so they could in turn infect their insecure environment wherever they go

Questions?

IPPON Project:

http://code.google.com/p/ippon-mitm/

Get your latest version and targets!

Happy Updating! ☺

./ippon.py –w –i <INTERFACE> targets.xml -u <MALWARE SITE>