



CYBER ATTACKS JUST AHEAD



Ivan Bütler, Compass Security

Compass Security AG
www.csnc.de
www.hacking-lab.com



Ivan Bütler

Penetration Testing

Forensic Analysis

APT Detection

National Cyber Security **Strategy**

National Cyber Security **Challenge**

Hackerangriff auf Angela Merkel: "CyberBerkut" bekennt sich

08.01.2015, 10:02 Uhr | dpa

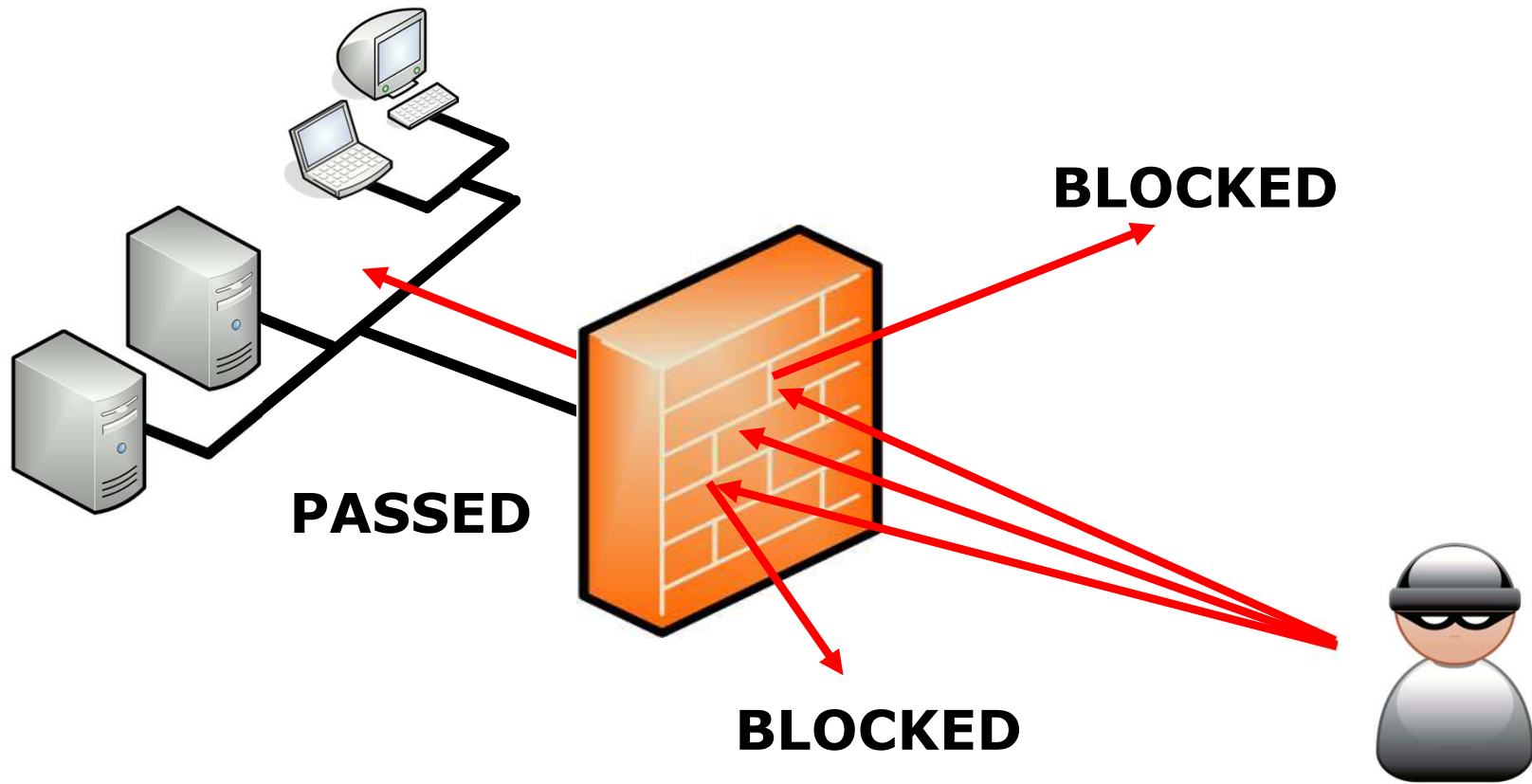


- Einführung "Direkte versus Indirekte Attacken"
- Was ist ein APT Angriff?
- Welche Schutzkonzepte bieten sich an?
- Braucht Deutschland Cyber Security Spezialisten?
- Wie sieht der Penetration Test NG aus?
- Zusammenfassung

- **Einführung "Direkte versus Indirekte Attacken"**
- Was ist ein APT Angriff?
- Welche Schutzkonzepte bieten sich an?
- Braucht Deutschland Cyber Security Spezialisten?
- Wie sieht der Penetration Test NG aus?
- Zusammenfassung

Direkte Angriffe

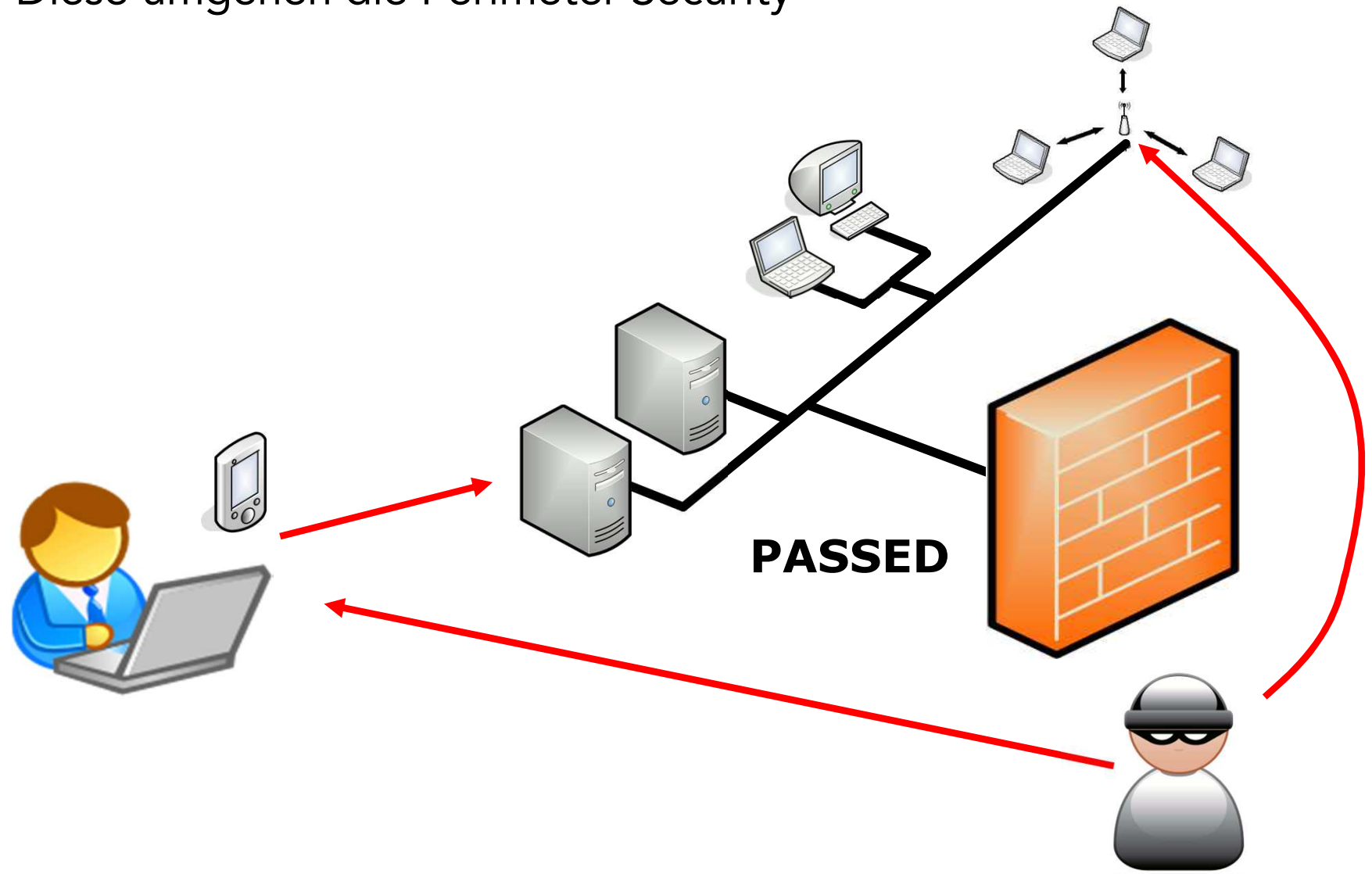
Hacker Attacken auf Web Anwendungen (Internet Facing)



Indirekte Angriffe



Diese umgehen die Perimeter Security



Der USB Stick als Waffe



Stuxnet basierte auf USB Stick



Der Stick enthält ein Trojanisches Pferd

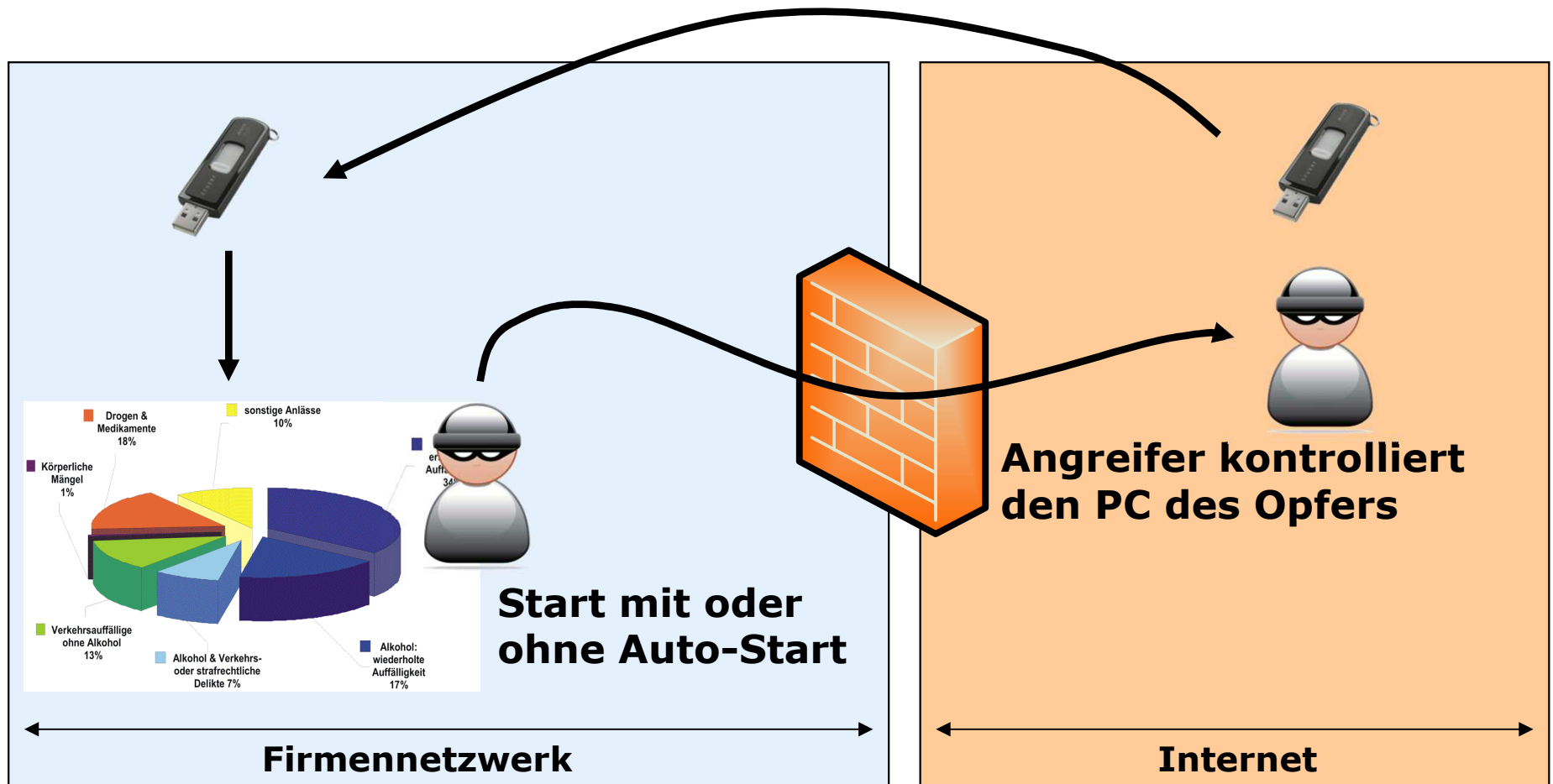


Wie macht es Compass in Pentests?

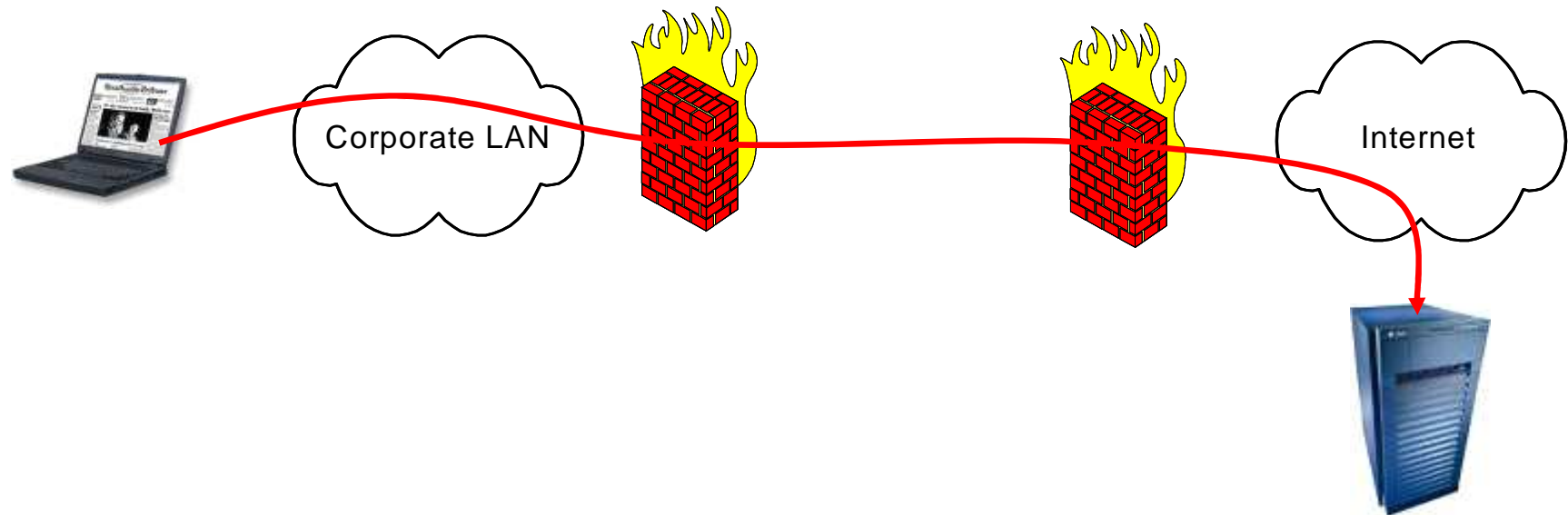


Covert Channels

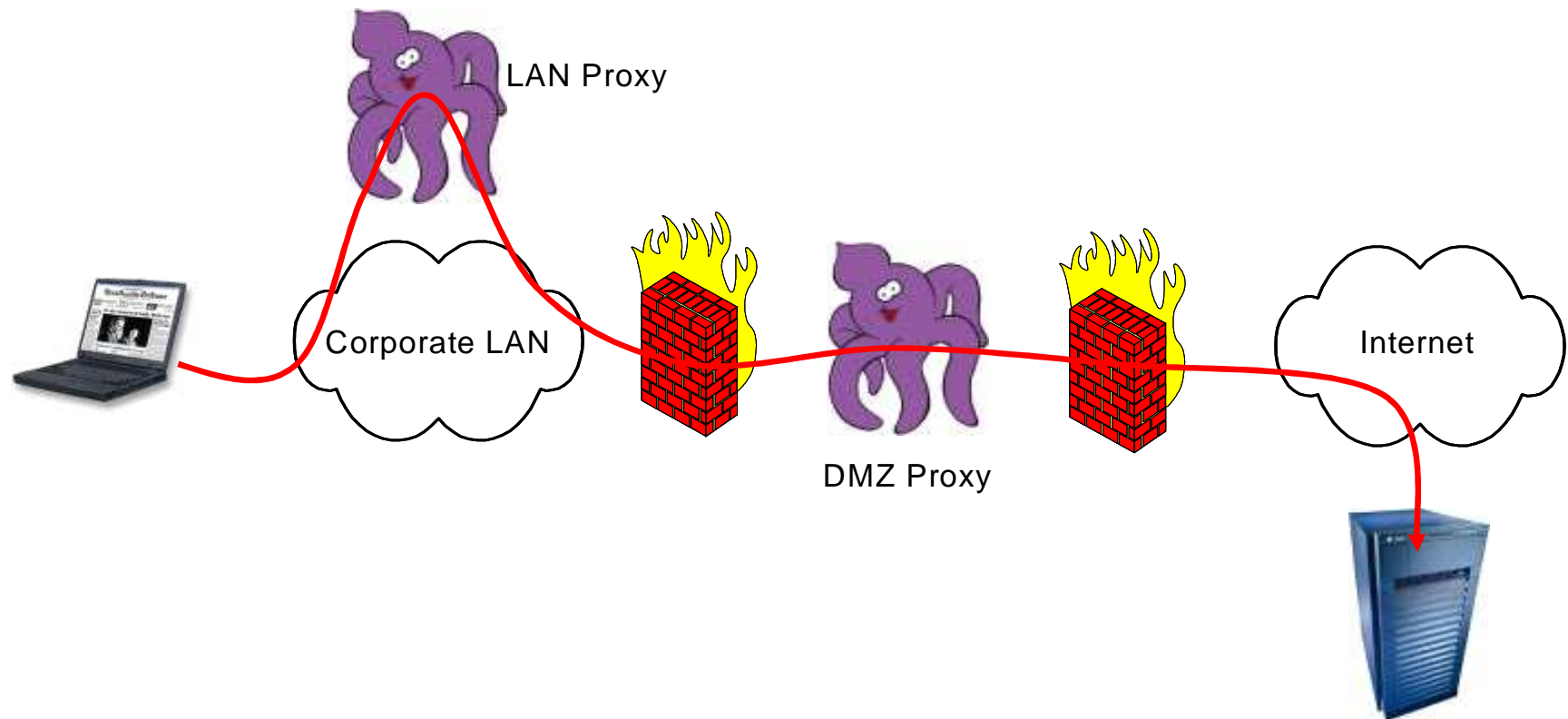
Lieferung als USB Stick



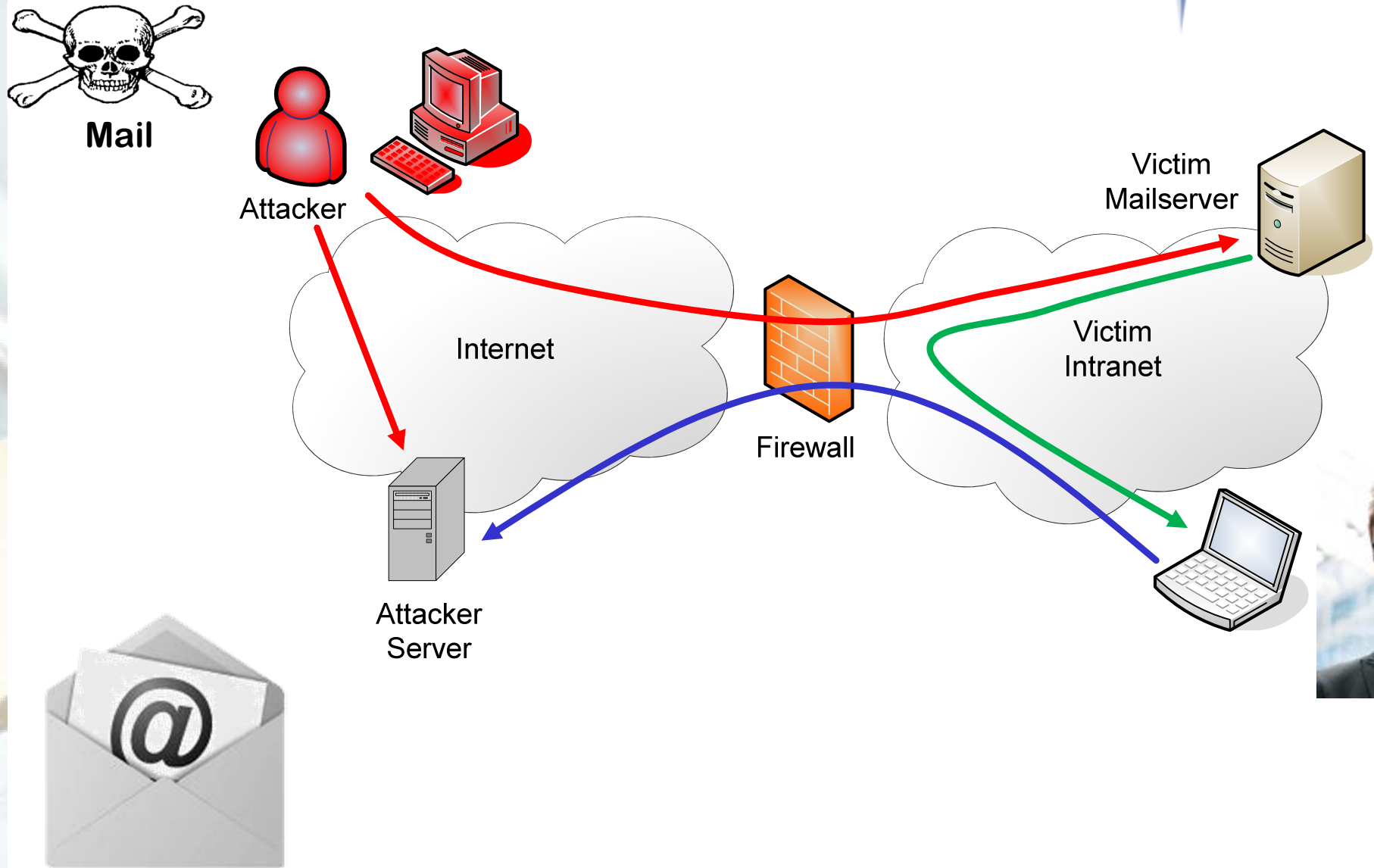
Einfache Exfiltrierung (Home Systeme)



Exfiltrierung aus Firmen heraus (Proxies)



Word Virus





Hardware Bot Clients



**GPRS/UMTS
Covert Channel**



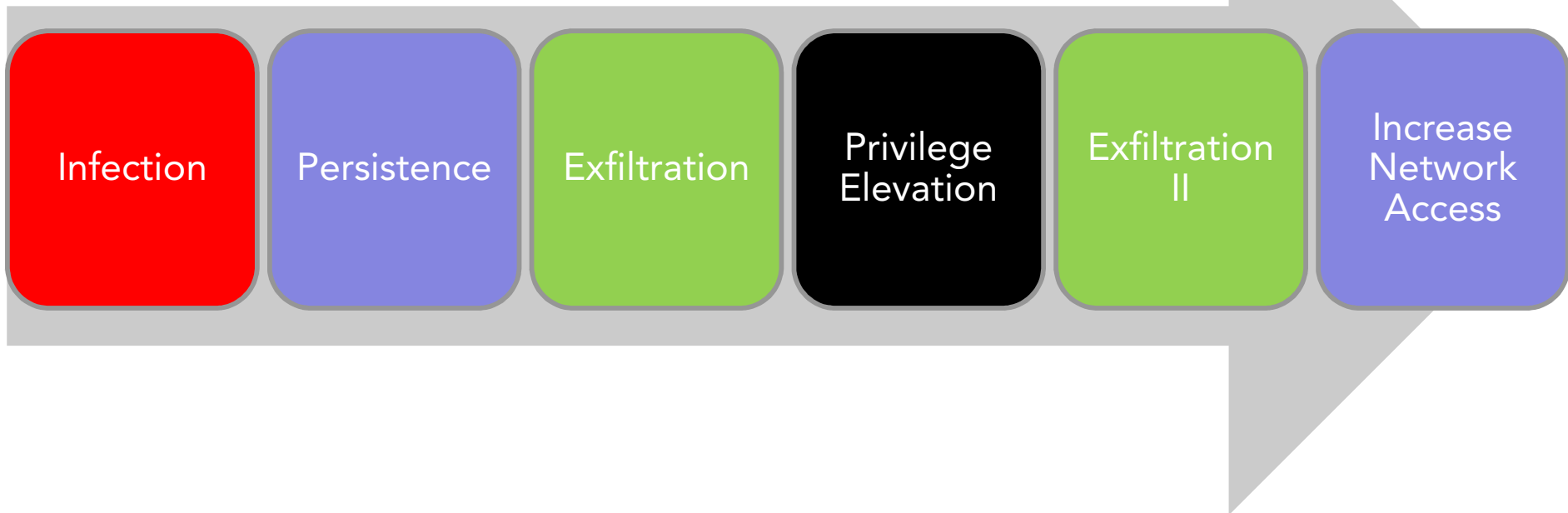
Central Command

- Einführung "Direkte versus Indirekte Attacken"
- **Was ist ein APT Angriff?**
- Welche Schutzkonzepte bieten sich an?
- Braucht Deutschland Cyber Security Spezialisten?
- Wie sieht der Penetration Test NG aus?
- Zusammenfassung

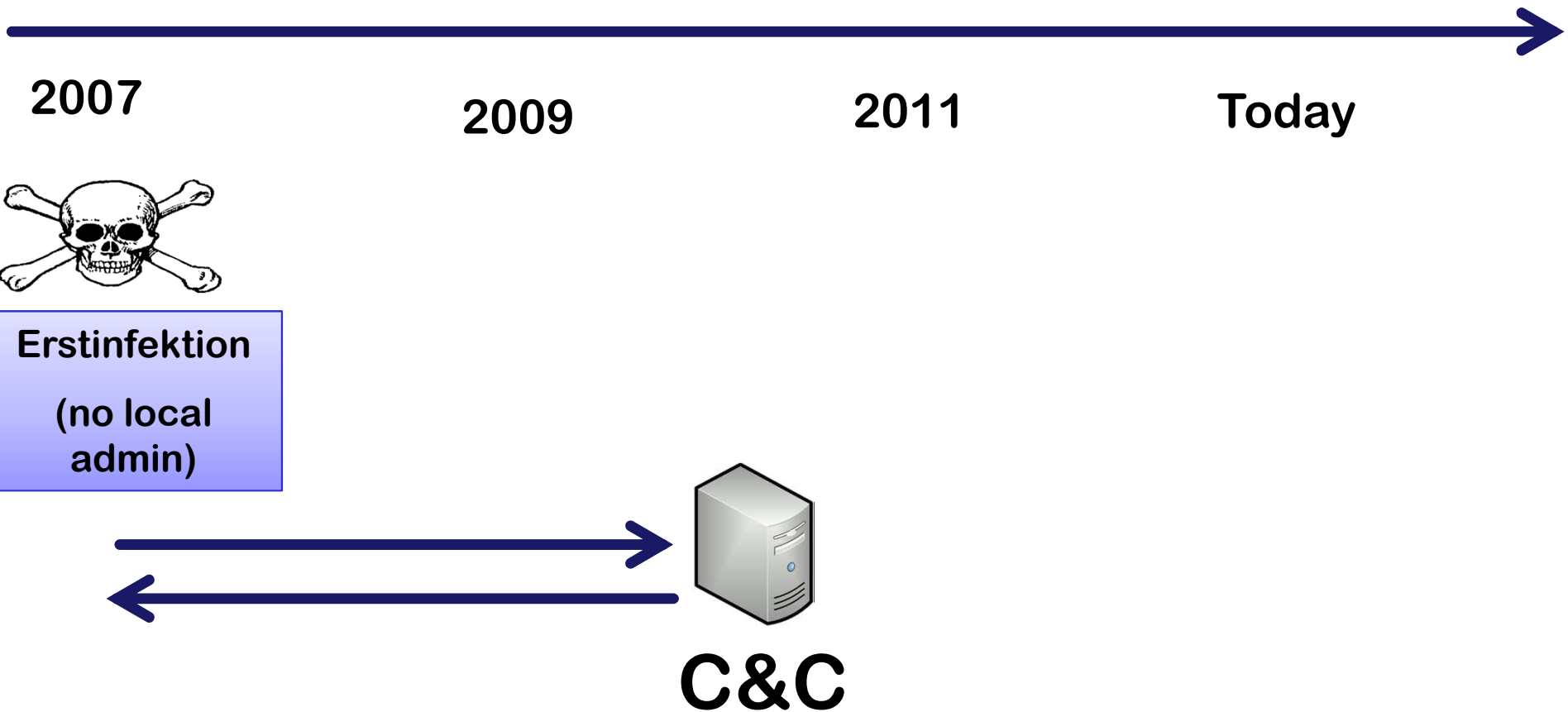
Hackerangriff auf Angela Merkel: "CyberBerkut" bekennt sich

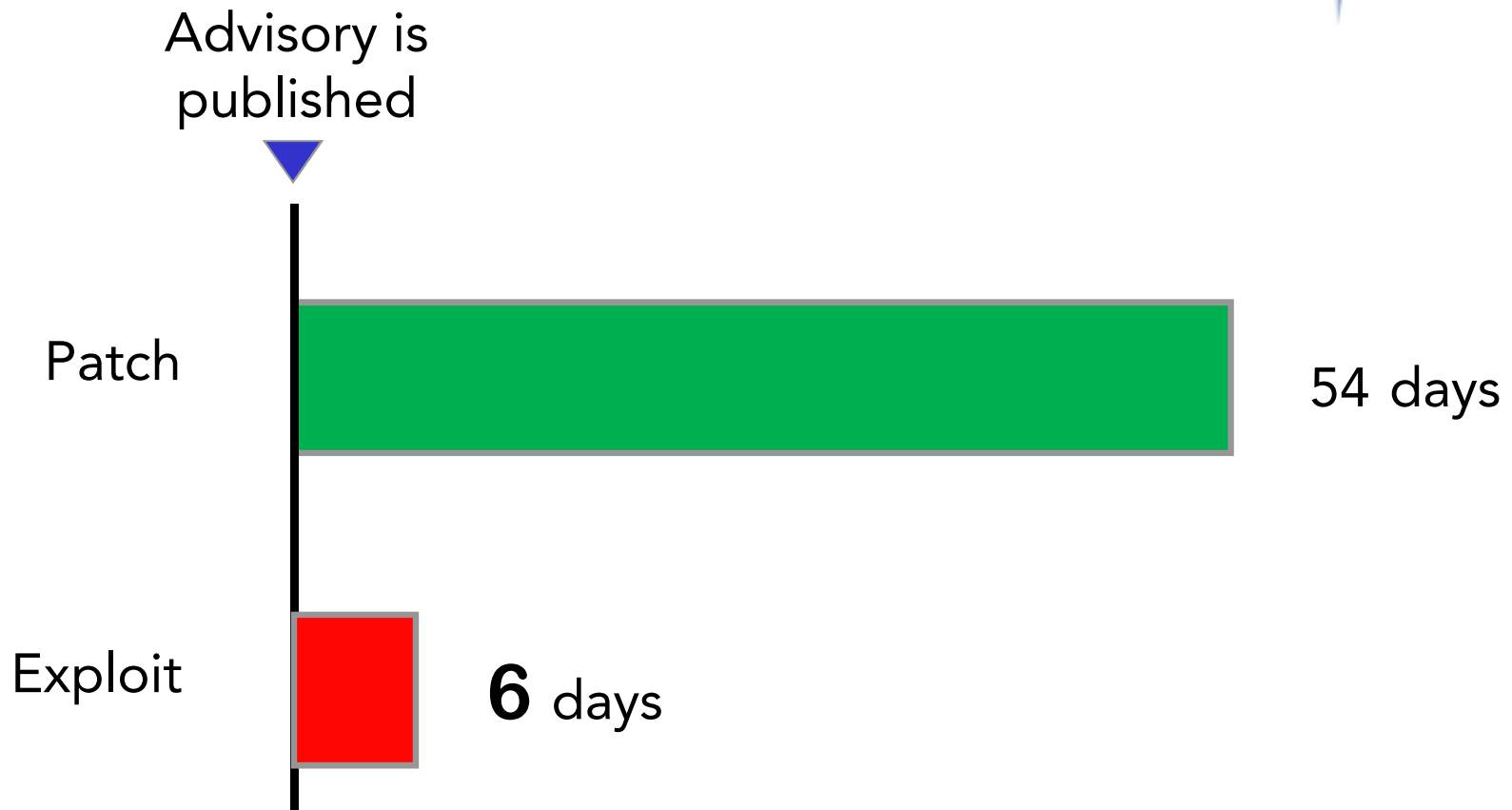
08.01.2015, 10:02 Uhr | dpa





Advanced Persistent Threat





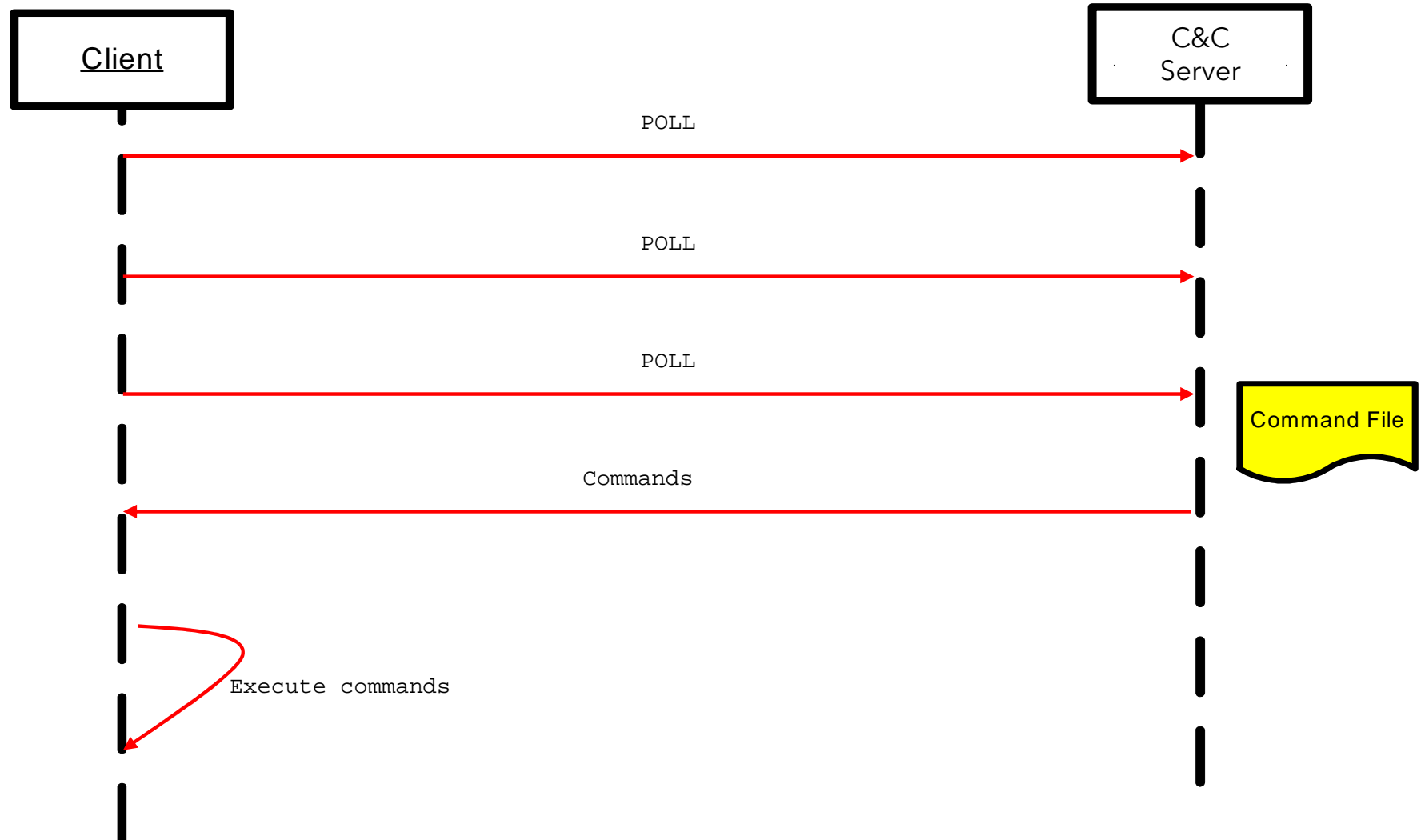
[3] ETHZ Stefan Frei 2009 (Dissertation): We found that exploit availability consistently exceeds patch availability since 2000

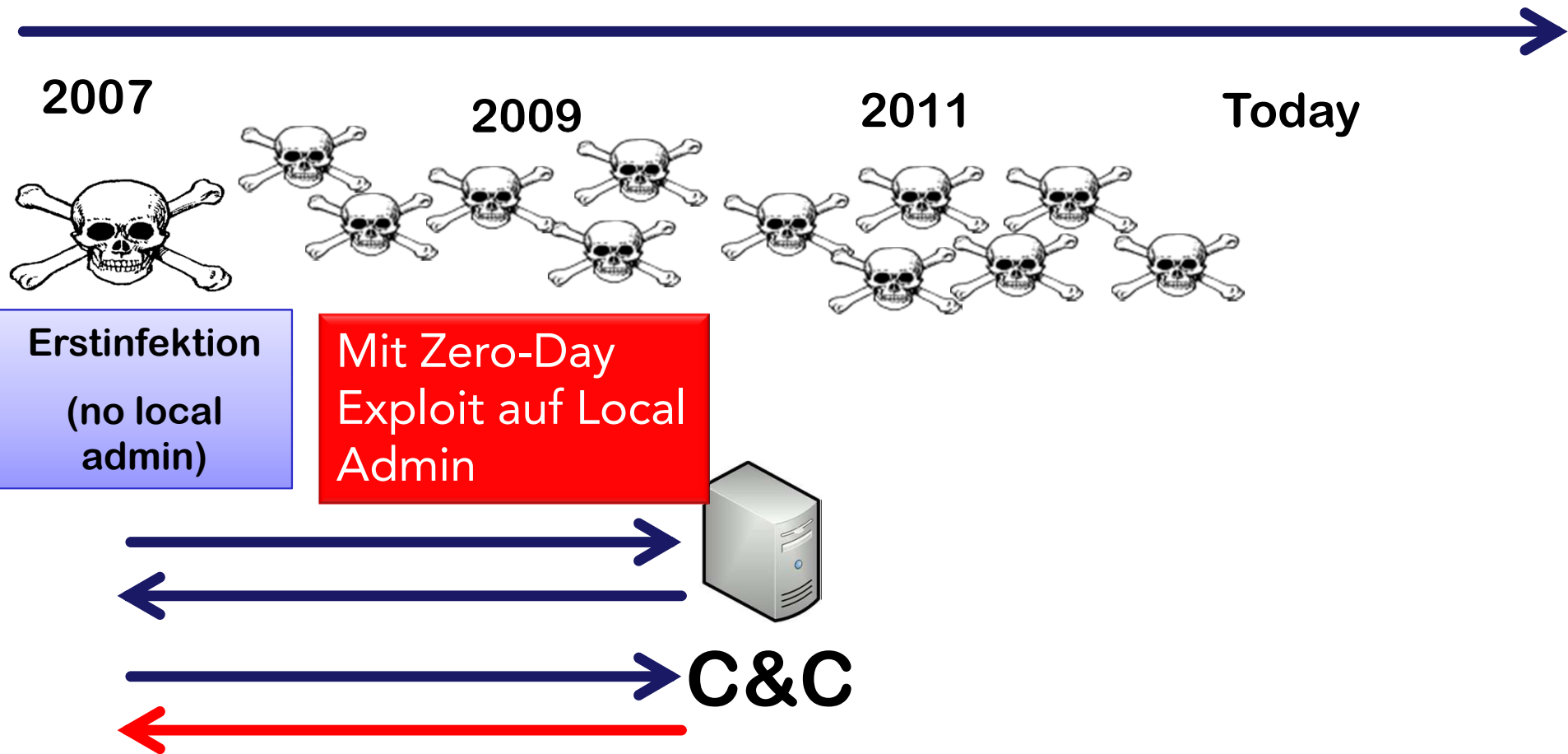
A vertical decorative image on the left side of the slide shows a close-up of a computer keyboard with a yellow padlock resting on one of the keys.

Die Macht der **48 Tage**

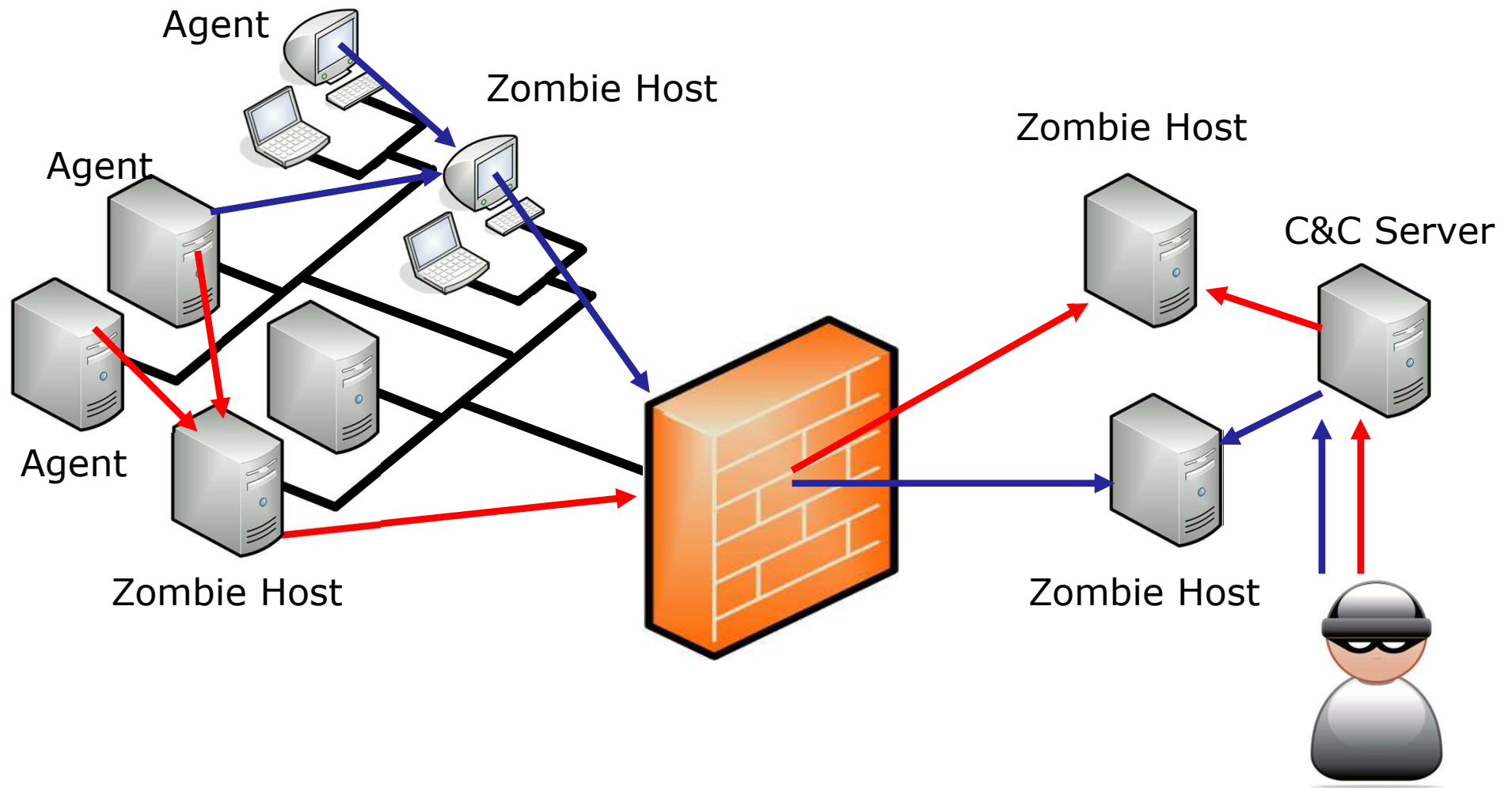
Statistisch gesehen sind alle Firmen regelmässig während 48 Tagen verwundbar und diesen Zustand nützen die APT Angreifer aus!

Command & Control Communication



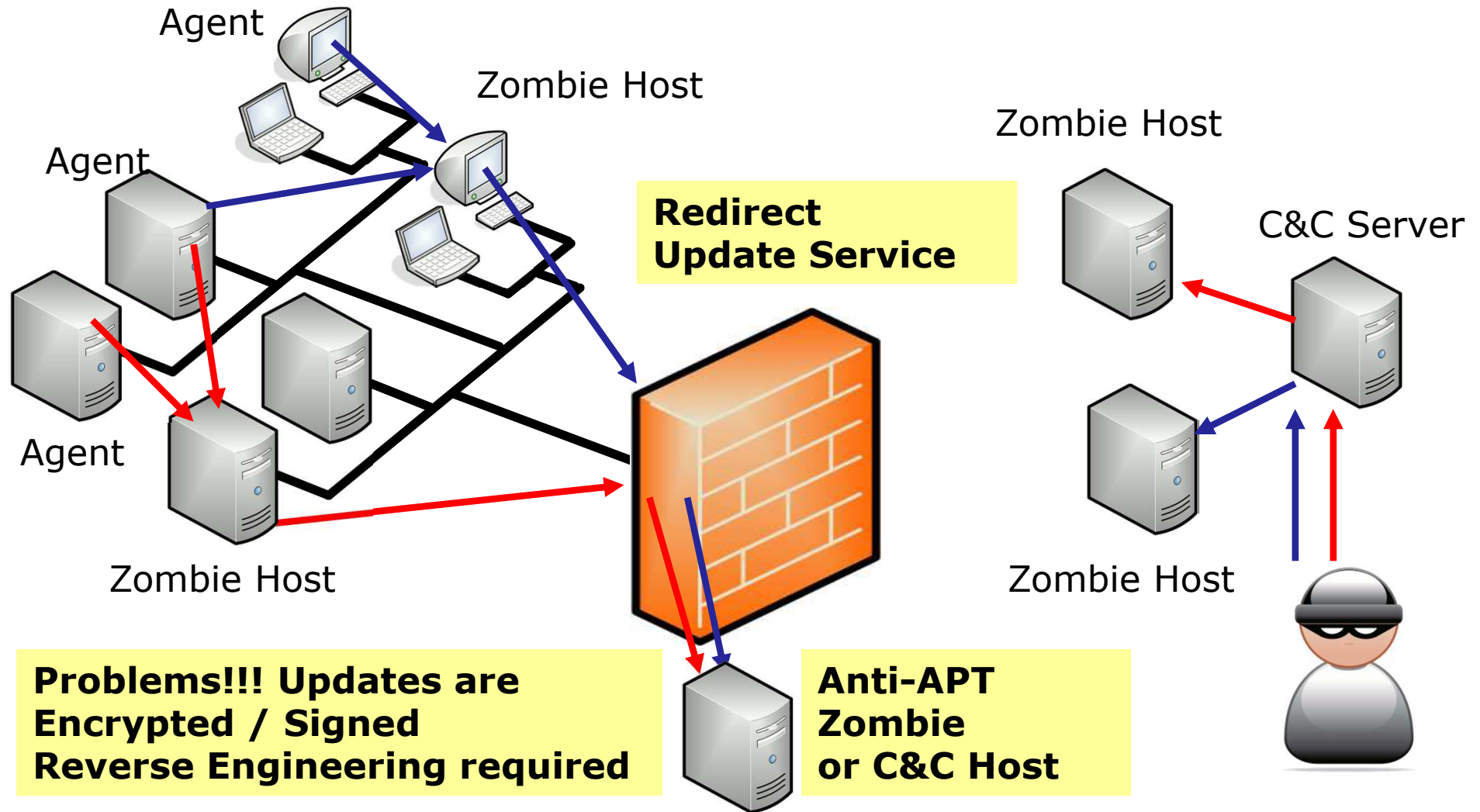


Advanced Persistent Threat



- Einführung "Direkte versus Indirekte Attacken"
- Was ist ein APT Angriff?
- **Welche Schutzkonzepte bieten sich an?**
- Braucht Deutschland Cyber Security Spezialisten?
- Wie sieht der Penetration Test NG aus?
- Zusammenfassung

Reaktion auf APT ? – C&C Traffic Redirection





Beten und nichts machen. Wird schon nichts passieren



Versicherung abschliessen. Versicherung verlangt jedoch Nachweis, dass man Best Practice umgesetzt hat.



Trennung vom Internet der kritischen Systeme. Will man nicht wirklich, weil es aktuell so cool und geekig ist.



Monitoring mit IDS/IPS Next Generation



APT Detection mit Splunk

FireEye basiert auch auf Splunk



- Home
- About
- Security Events
- Dashboard
- Reference Projects
- How it Works
- Chat
- Global Scoring
- Mobile Services
- Download
- Research
- Support
- Login / Sign up

Don't have an account?
Create a free account
now!

CTF Statistics

Swiss Qualifying

Swiss Cyber Storm



Running

Germany Qualifying

Cyber Security Challenge Germany



Running

Austria Qualifying

Cyber Security Austria



Running

OWASP AppSec EU



Hacky Easter



Running

European Cyber Security Challenge



Countdown to Start

147 07:40:51

News [see more](#)

Date	Title
05.02.2015	Cyber Security Challenge Germany 2015
23.12.2014	OWASP AppSec EU 2015 University Challenge
23.12.2014	Germany CTF - Join Now
27.10.2014	Swiss Cyber Storm 2014 is history!

Social Media



Follow us on
Twitter



Like us on
Facebook



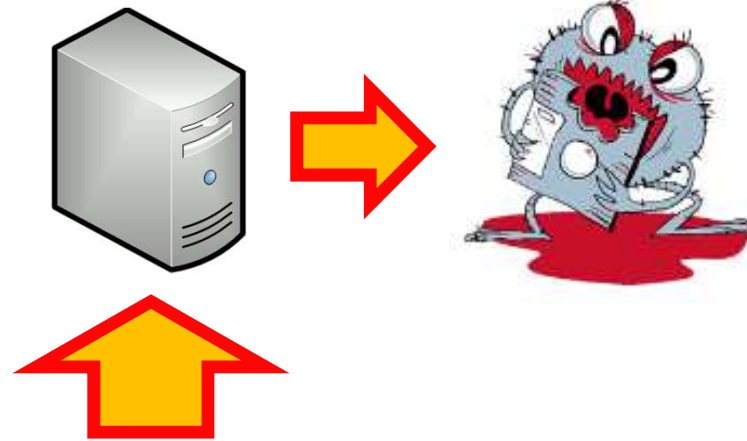


splunk™ >



APT Intelligence Engine

Splunk Installation in Hacking-Lab



Lookup Database

Splunk Screenshot



Search Verbose Mode

```
source="mandiant-apti-indicators.csv" | fields MANDIANIAPT_DOMAIN | lookup malwaredomains domain
```

4,094 matching events Save Create



0 selected fields Edit

1 interesting fields

- MANDIANIAPT_DOMAIN (>100)

Only 1 field available

4,094 events over all time

Export Options

« prev 1 2 3 4 5 6 7 8 9 10 next » 10 per page

1	3/20/13 11:36:12.000 AM	*ztl.firefoxupdate.com*,****
2	3/20/13 11:36:12.000 AM	*zone.todayusa.org*,****
3	3/20/13 11:36:12.000 AM	*zone.searchforca.com*,****
4	3/20/13 11:36:12.000 AM	*zone.usnhome.org*,***
5	3/20/13 11:36:12.000 AM	*zone.companyinfosite.com*,****

Malware Domains (DNS Source)

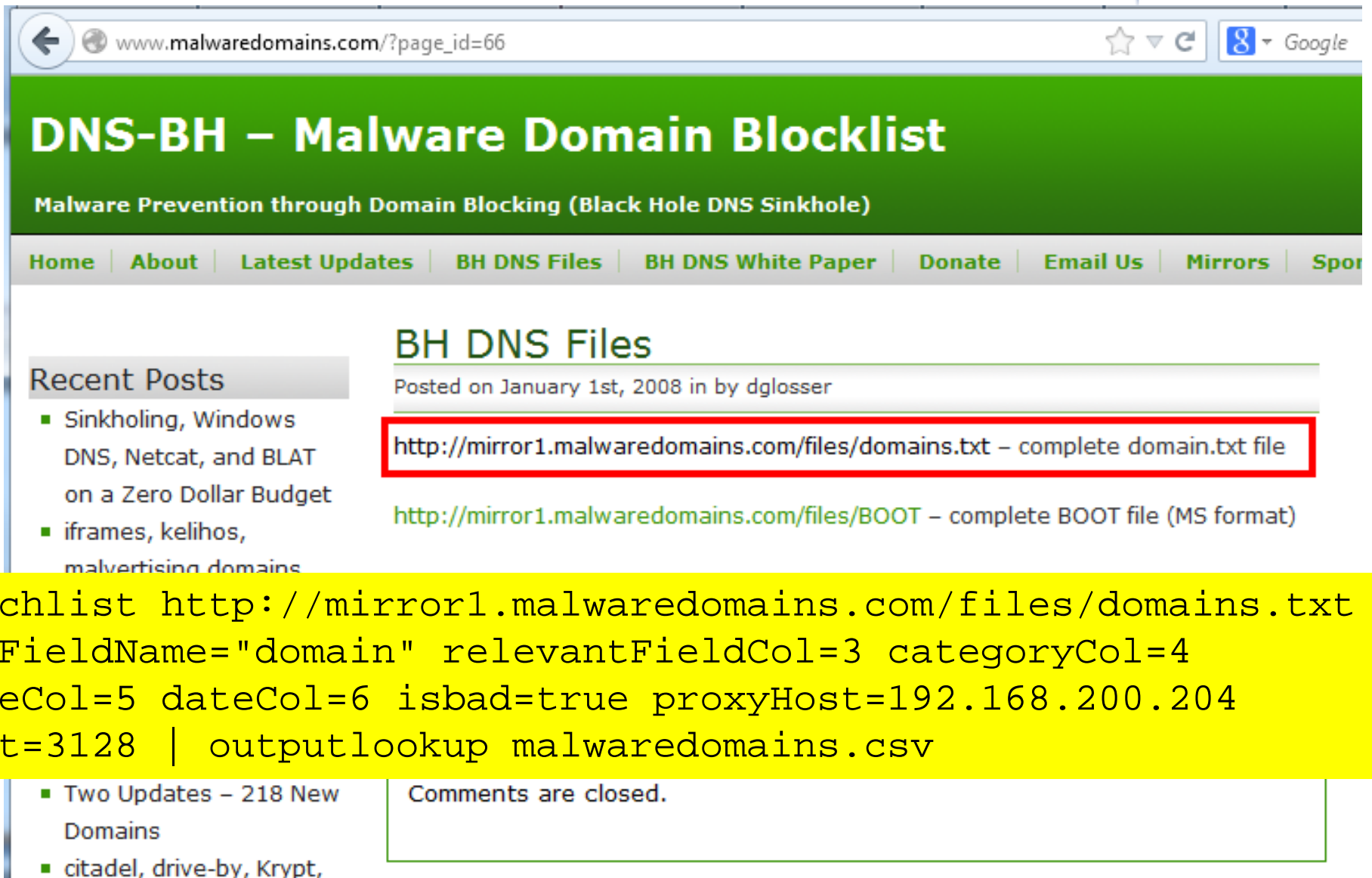
- ✦ Malware Domains <http://malwaredomains.com/>
- ✦ | **getwatchlist** <http://mirror1.malwaredomains.com/files/domains.txt>
relevantFieldName="domain" relevantFieldCol=3 categoryCol=4
referenceCol=5 dateCol=6 isbad=true | **outputlookup** malwaredomains.csv

Mandiant Sources

- ✦ <http://www.joshd.ca/sites/default/files/mandiant-apt1-indicators-list.txt>
- ✦ sourcetype=dns_query OR sourcetype=proxy [| **inputlookup mandiant-apt1-indicators.csv** MANDIANT-APT1-DOMAIN | fields + \$MANDIANT-APT1-DOMAIN]

Zeus Tracker, Dshield, Spamhaus

- ✦ Zeus tracker IP list <http://www.abuse.ch/zeustracker/>
- ✦ DShield recommended block list <http://dshield.org/>
- ✦ Spamhaus DROP list <http://www.spamhaus.org/drop/>



www.malwaredomains.com/?page_id=66

DNS-BH – Malware Domain Blocklist

Malware Prevention through Domain Blocking (Black Hole DNS Sinkhole)

Home | About | Latest Updates | BH DNS Files | BH DNS White Paper | Donate | Email Us | Mirrors | Spor

BH DNS Files

Posted on January 1st, 2008 in by dglosser

<http://mirror1.malwaredomains.com/files/domains.txt> – complete domain.txt file

<http://mirror1.malwaredomains.com/files/BOOT> – complete BOOT file (MS format)

Recent Posts

- Sinkholing, Windows DNS, Netcat, and BLAT on a Zero Dollar Budget
- iframes, kelihos, malvertising domains

Two Updates – 218 New Domains

- citadel, drive-by, Krypt,

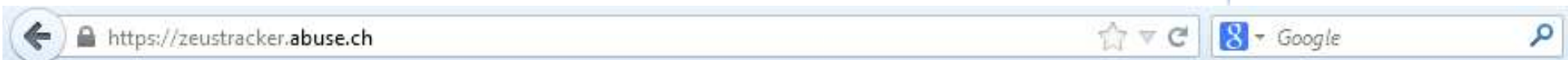
Comments are closed.

```
| getwatchlist http://mirror1.malwaredomains.com/files/domains.txt  
relevantFieldName="domain" relevantFieldCol=3 categoryCol=4  
referenceCol=5 dateCol=6 isbad=true proxyHost=192.168.200.204  
proxyPort=3128 | outputlookup malwaredomains.csv
```

← www.joshd.ca/sites/default/files/mandiant-apt1-indicators-list.txt ☆ ▾ ↻ Google

MANDIANT-APT1-DOMAIN, MANDIANT-APT1-MD5SUM, MANDIANT-APT1-FILENAME, MANDIANT-APT1-FILESIZE, MANDIAN
advanbusiness.com, *001dd76872d8080169211942308c84e6*, *121.exe*, *10233*, *!@#*\$ %&!*
aoldaily.com, *002325a0a67fded0381b5648d7fe9b8e*, *162.exe*, *10240*, *@***@*#####
aolonline.com, *00dbb9e1c09dbdafb360f3163ba5a3de*, *1.dll*, *102912*, *2010QBP*
applesoftupdate.com, *00f24328b282b28bc39960d55603e380*, *1.exe*, *104448*, *3DC76854-C328-43D7-9
arrowservice.net, *0115338e11f85d7a2226933712acaae8*, *1.jpeg*, *104449*, *6k6Gpms*
attnpower.com, *0141955eb5b90ce25b506757ce151275*, *1.jpg*, *10752*, *-----
aunewsonline.com, *0149b7bd7218aab4e257d28469fddb0d*, *1.rar*, *110592*, *Abrot*
avvmail.com, *016da6ee744b16656a2ba3107c7a4a29*, *204.exe*, *11264*, *AFX_Ideas_H*
bigdepression.net, *01e0dc079d4e33d8edd050c4900818da*, *2.dll*, *113664*, *bdzkt*
bigish.net, *024fd07dbdacc7da227bede3449c2b6a*, *4.exe*, *1220608*, *c2x1ZXA=*
blackberrycluter.com, *0285bd1fbdd70fd5165260a490564ac8*, *66.exe*, *12507*, *Can not open file o
blackcake.net, *02a2d148faba3b6310e7ba81eb62739d*, *a1.dll*, *126976*, *cmd.exe*
bluecoate.com, *02c65973b6018f5d473d701b3e7508b2*, *abc.gif*, *12800*, *C:\Ocean\Project-VS2008\E
booksonlineclub.com, *034374db2d35cf9da6558f54cec8a455*, *acrod32.exe*, *12801*, *C:\Ocean\Projec
bpyoyo.com, *03ae71eba61af2d497e226da3954f3af*, *AcroRd32.exe*, *13068*, *Create cmd shell failed
businessconsults.net, *0469a42d71b4a55118b9579c8c772bb6*, *acrord32.exe*, *131072*, *cXVpdA==*
businessformars.com, *0496e3b17cf40c45f495188a368c203a*, *acrord32ram.exe*, *13312*, *D:\M tools\
basketball.com, *04a7b7dab5ff8ba1486df9dbe68c748c*, *a.dat*, *13824*, *d:\My Documents\Visual Stu
canadatvsite.com, *04e83832146034f9797d2e8145413daa*, *adobearm.exe*, *13825*, *DreateRemoteThrea
canoedaily.com, *04f481d6710ac5d68d0eacac2600a041*, *adobere.exe*, *142848*, *dW5zdXBwb3J0*
chileexe77.com, *0501bb10d646b29cab7d17a8407010d9*, *adobe_sl.exe*, *14336*, *E:\4xjq\Eclipse_A1.

Zeus Tracker



abuse.ch Zeus Tracker

[Home](#) | [FAQ](#) | [Zeus Blocklist](#) | [Zeus Tracker](#) | [Submit C&C](#) | [Removals](#) | [ZTDNS](#) | [Statistic](#) | [RSS Feeds](#) | [Contact](#) | [Links](#)

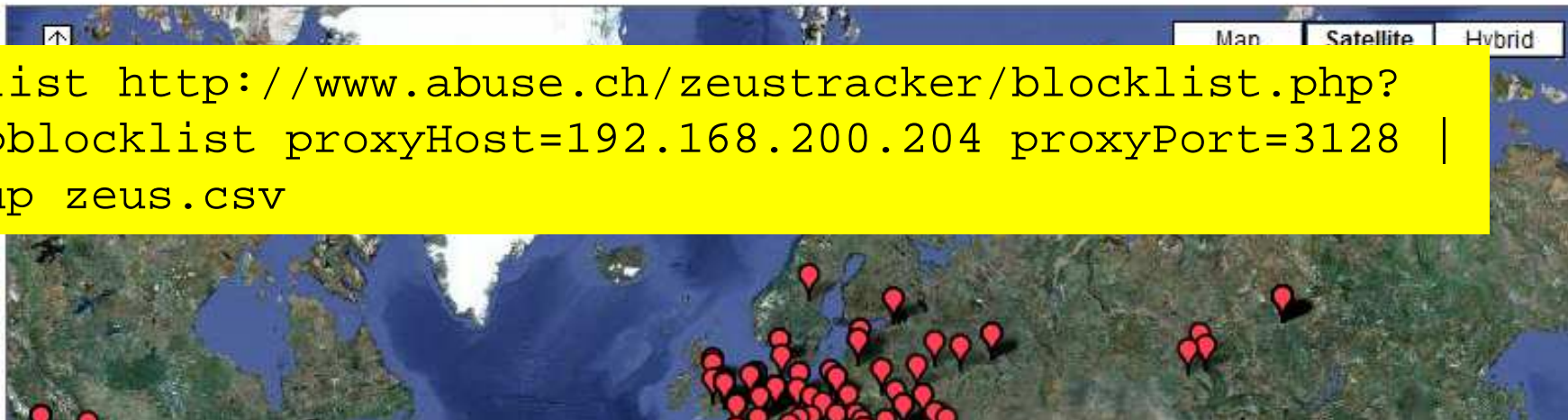
Welcome to the Zeus Tracker

Zeus Tracker tracks Zeus Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist. If you have any questions please take a look into the [FAQ](#) or send me a email ([contact](#)).

Here are some quick statistics about the Zeus crimeware:

- Zeus C&C servers tracked: **967**
- Zeus C&C servers online: **569**
- Zeus C&C servers with files online: **41**
- Zeus FakeURLs tracked: **2**
- Zeus FakeURLs online: **1**
- Average Zeus binary Antivirus detection rate: **38.32%**

You can find more interesting statistics about the Zeus crimeware on the [Zeus Tracker statistic page](#). The map below shows a dot for each Zeus Command&Control server (ip or domain).



```
| getwatchlist http://www.abuse.ch/zeustracker/blocklist.php?  
download=ipblocklist proxyHost=192.168.200.204 proxyPort=3128 |  
outputlookup zeus.csv
```


Malware Sample Acquisition Cycle

- ✦ **Malware.lu** hashes -> **VirusTotal** behavioral information -> **custom parser**, DNS/ssdeep hashes extraction -> **Splunk Source**





Improvement through modified samples

- ✦ ssdeep (<http://ssdeep.sourceforge.net/>) hashes for fuzzy detection of modified malware samples
- ✦ May be used for automatic generation of OpenIOC indicators (<http://www.openioc.org/>)

openioc.org/iocs/ea3cab0c-72ad-40cc-abbf-90846fa4afec.ioc



Google



This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
- <ioc id="ea3cab0c-72ad-40cc-abbf-90846fa4afec" last-modified="2011-11-04T19:35:05">
```

```
  <short_description>STUXNET VIRUS (METHODOLOGY)</short_description>
```

```
  - <description>
```

Generic indicator for the stuxnet virus. When loaded, stuxnet spawns lsass.exe in a suspended state. The malware then maps in its own executable section and fixes up the CONTEXT to point to the newly mapped in section. This is a common task performed by malware and allows the malware to execute under the pretense of a known and trusted process.

```
  </description>
```

```
  <keywords>methodology</keywords>
```

```
  <authored_by>Mandiant</authored_by>
```

```
  <authored_date>0001-01-01T00:00:00</authored_date>
```

```
  <links/>
```

```
  - <definition>
```

```
    - <Indicator operator="OR" id="73bc8d65-826b-48d2-b4a8-48918e29e323">
```

```
      - <IndicatorItem id="b9ef2559-cc59-4463-81d9-52800545e16e" condition="contains">
```

```
        <Context document="FileItem" search="FileItem/PEInfo/Sections/Section/Name" type="mir"/>
```

```
        <Content type="string">.stub</Content>
```

```
      </IndicatorItem>
```

```
      - <IndicatorItem id="156bc4b6-a2a1-4735-bfe8-6c8d1f7eae38" condition="contains">
```

```
        <Context document="FileItem" search="FileItem/FileName" type="mir"/>
```

```
        <Content type="string">mdmcpq3.PNF</Content>
```

```
      </IndicatorItem>
```

IP Reputation (Honeypot DB)



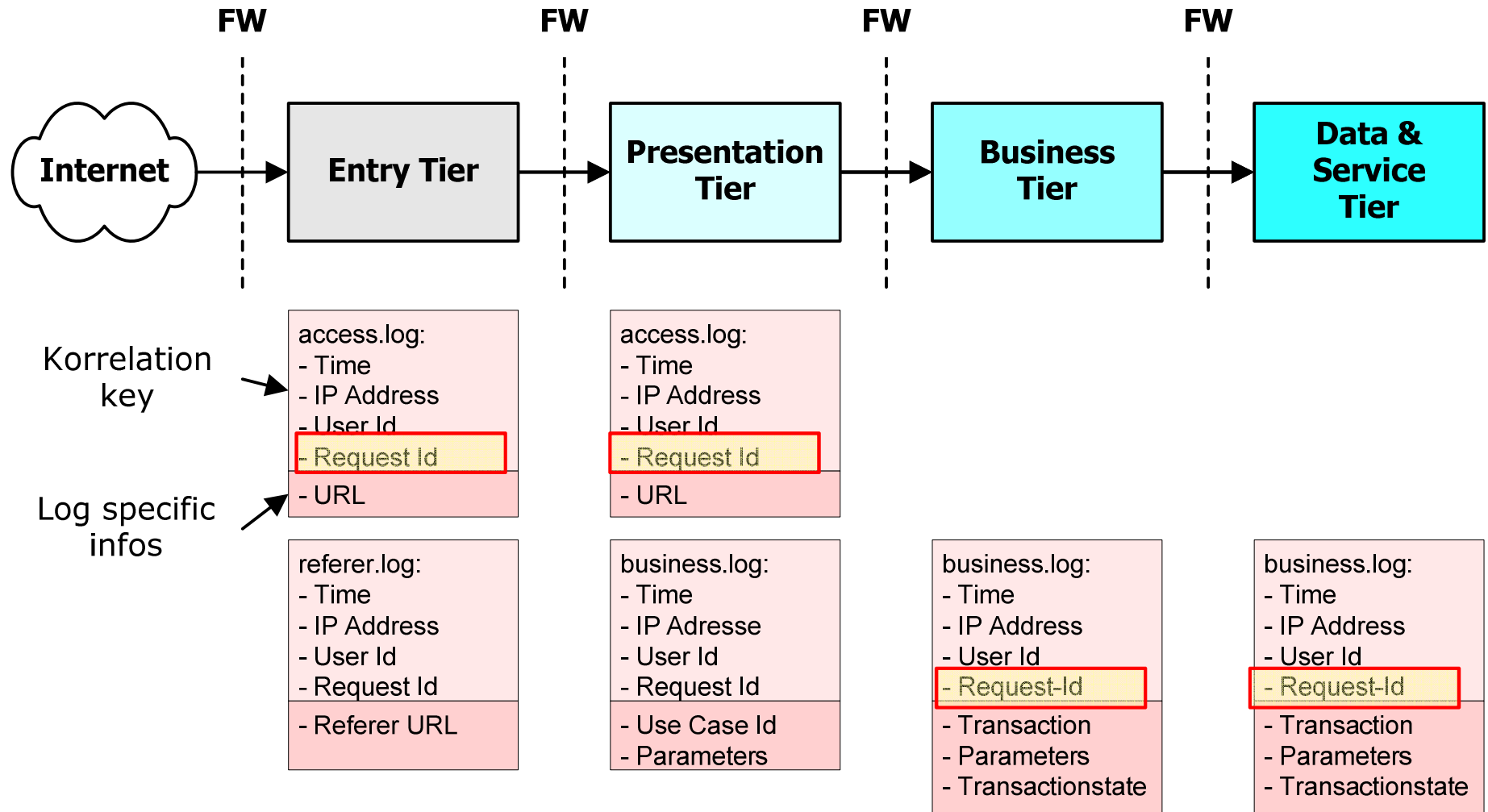
Description

This app allows you to enrich your IP Data with realtime threat information by contacting the Project Honey Pot database via DNS-Blacklist requests.

A vertical image on the left side of the slide showing a close-up of a computer keyboard with a yellow padlock resting on one of the keys.

Voraussetzungen für diese
Analysen sind 'gute' Logfiles

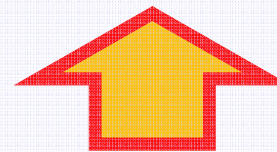
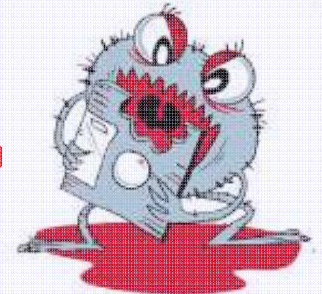
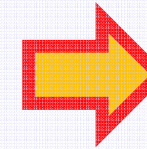
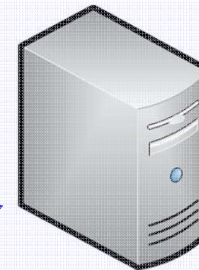
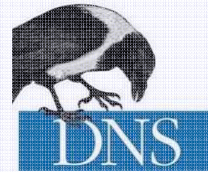
Correlation across tier (Simplified illustration)



Attachments



Sandbox
Infrastructure



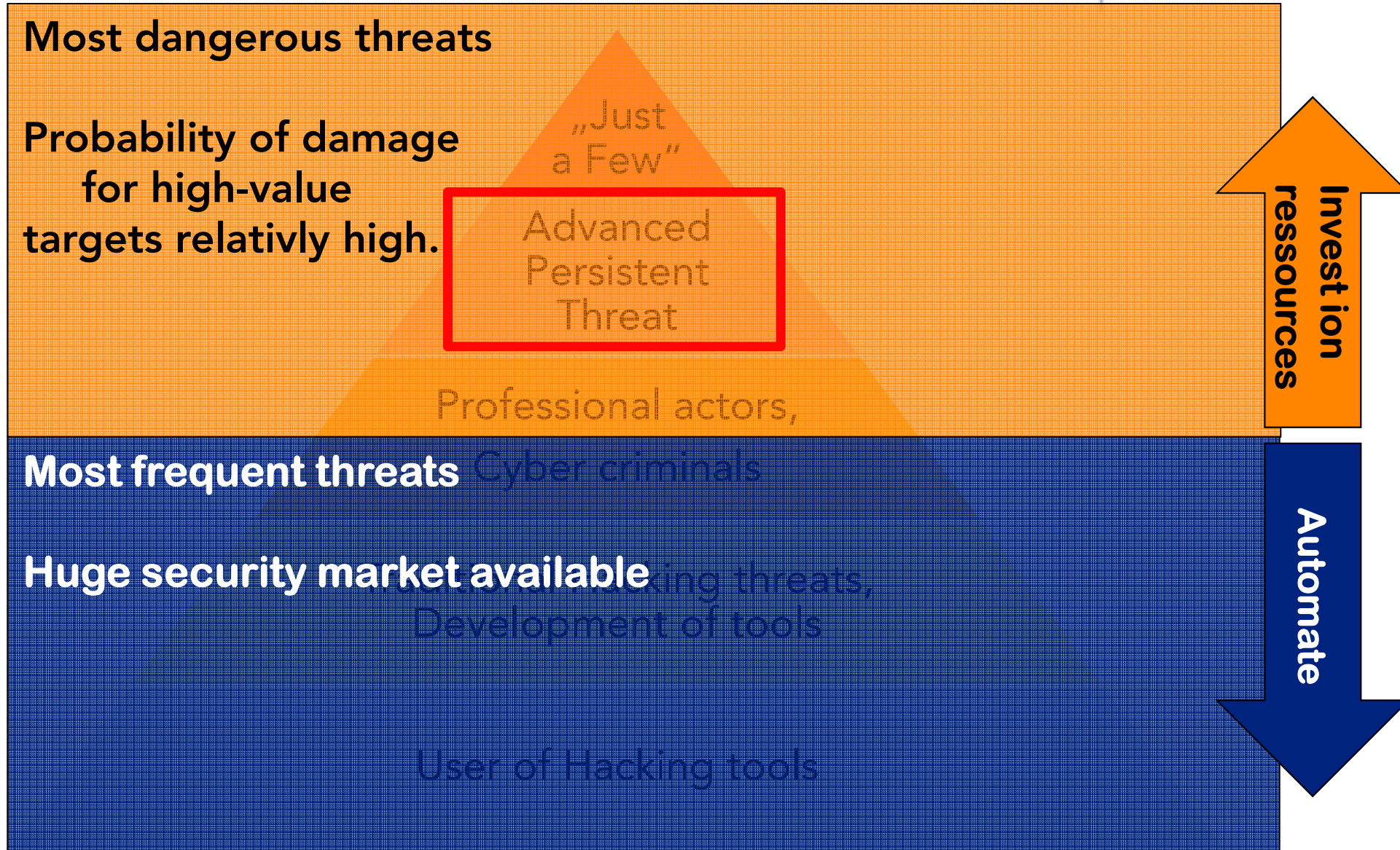
Lookup Database

Cuckoo Sandboxing Analysis

- Do I want to analyze PDF exploits?
- Do I want to analyze Office exploits?
- Do I want to analyze PHP and Perl scripts?
- Do I want to analyze browsers' exploits?
- What else do I want to analyze?
- Do I want it to communicate with the outside?

<http://blog.rootshell.be/2012/06/20/cuckoomx-automating-email-attachments-scanning-with-cuckoo/>

- Einführung "Direkte versus Indirekte Attacken"
- Was ist ein APT Angriff?
- Welche Schutzkonzepte bieten sich an?
- **Braucht Deutschland Cyber Security Spezialisten?**
- Wie sieht der Penetration Test NG aus?
- Zusammenfassung





Cyber Security
Challenge

GERMANY



Jetzt anmelden –
Neue Challenges ab Mai

[Aktuelles](#)

[Challenge](#)

[Konferenz](#)

[Sponsoring](#)

[Download-Bereich](#)

[Galerie](#)

[Archiv](#)

© April 22, 2015

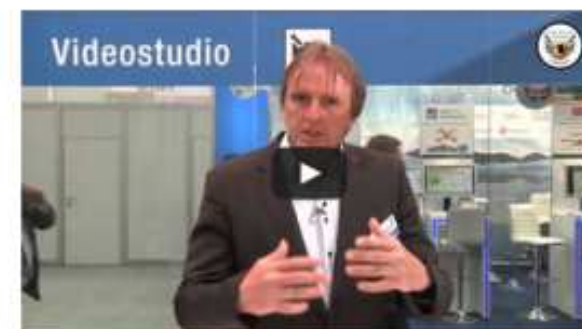
Für die gute Seite entschieden – Hackingtalent hilft Unternehmen, sicherer zu werden



Bei der vergangenen Cyber Security Challenge Germany nahmen rund 800 Nachwuchshacker an der Qualifikationsphase teil, ins Finale nach Berlin schafften es schließlich zehn SchülerInnen und zehn Studierende. Einer von ihnen ist der 19-jährige Robert Kugler aus Welzheim bei Stuttgart, Schüler an einem technischen Gymnasium. Mit seinem Team belegte er in Berlin den zweiten Platz und musste sich lediglich einem Studenten-Team geschlagen geben.

In den vergangenen Jahren hat sich...

[Weiter zum kompletten Beitrag](#)



© April 9, 2015

Hacking-Talente können sich erneut beweisen – Online-Challenges der CSCG starten ab Mai



Bald ist es wieder soweit: Die besten Nachwuchs-Hacker Deutschlands können sich ganz legal an das Aufspüren von Schwachstellen machen und in zwölf schwierigen Challenges ihr Können unter Beweis stellen. Ab Mai beginnen die Online-Qualifikationen für die kommende Cyber Security

■ Kooperationspartner



■ Förderer



Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

- Einführung "Direkte versus Indirekte Attacken"
- Was ist ein APT Angriff?
- Welche Schutzkonzepte bieten sich an?
- Braucht Deutschland Cyber Security Spezialisten?
- **Wie sieht der Penetration Test NG aus?**
- Zusammenfassung



- Testing von APT ohne "Schadware"
- Unabhängig von Metasploit und allfälliger Viren Erkennung
- Unterstützung vieler verschiedener Covert Channels

Compass APT Testing Framework



The screenshot shows the Malware Builder v. 0.0.1 BETA interface. The top menu bar includes "Malware" and "C&C Server". Below the menu is a toolbar with icons for Save, Open Config, Preview, Add, Remove All, Anti-Debug, Anti-VM, Enable, TRACE, Kernel Rootkit, Build Configuration, Release, Graph Layout Algorithm (set to Circular), Process Name (MalwareToolkit.WinMain), and Kill. The main area is split into two panes. The left pane displays a JSON configuration for components:

```
{
  "components": [
    {
      "Type": "ConfigManager",
      "Supertype": [
        "ConfigManager"
      ],
      "Description": null,
      "Id": "configmanager",
      "constructor-params": null,
      "module-params": null,
      "IsSingleton": false,
      "IsConfigured": true,
      "IsPayload": false
    },
    {
      "Type": "StreamerCrypto",
      "Supertype": [
        "IStreamerEncryptor"
      ],
      "Description": "Handles streamer encryption/decryption",
      "Id": "streamercrypto",
      "constructor-params": [
        {
          "value": "configmanager",
          "name": "ConfigManager",
          "type": "ConfigManager",
          "reference": true,
          "list": false,
          "configured": false,
          "MultipleIds": ""
        },
        {
          "value": "streamercrypto",
          "name": "Id",
          "type": "string",
          "reference": false,
          "list": false,
          "configured": false,
          "MultipleIds": ""
        }
      ]
    }
  ]
}
```

The right pane shows a dependency graph with nodes: commanddispatcher, ccontroller, sectionalbuffer, smarttrigger, dropboxstreamer, configmanager, httpnetworkstreamer, and streamercrypto. Arrows indicate dependencies between these components.

Step Up Funktion

- ✦ Non-Admin zu Admin Erhöhung

C&C Server

- ✦ Mit oder ohne Verschlüsselung

Malware Client

- ✦ Anti Reverse Engineering
- ✦ Anti VM (Vmware, VirtualBox)
- ✦ Code Obfuscation

Covert Channel

- ✦ HTTP Tunnel
- ✦ ICA Tunnel (Citrix)
- ✦ DNS Tunnel

- Einführung "Direkte versus Indirekte Attacken"
- Was ist ein APT Angriff?
- Welche Schutzkonzepte bieten sich an?
- Braucht Deutschland Cyber Security Spezialisten?
- Wie sieht der Penetration Test NG aus?
- **Zusammenfassung**

- Wir befinden uns aktuell in einem Cyber Wettrüsten
- Wir können uns nicht 100% schützen
- APT Detection Framework bieten den nächsten Schutzlevel an
- Funktionieren diese auch wie geplant?
- Compass Security bleibt für Sie am Ball (Angewandte Forschung)
- Wir unterstützen Sie bei **professionellen Security Tests**
- Wir entwickeln unsere Tests laufend weiter
- Wir freuen uns nun auf das **kühle Bier!**