CYBER ATTACKS
JUST AHEAD

Ivan Bütler, Compass Security

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

Ivan Bütler, Compass Security

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

Agenda

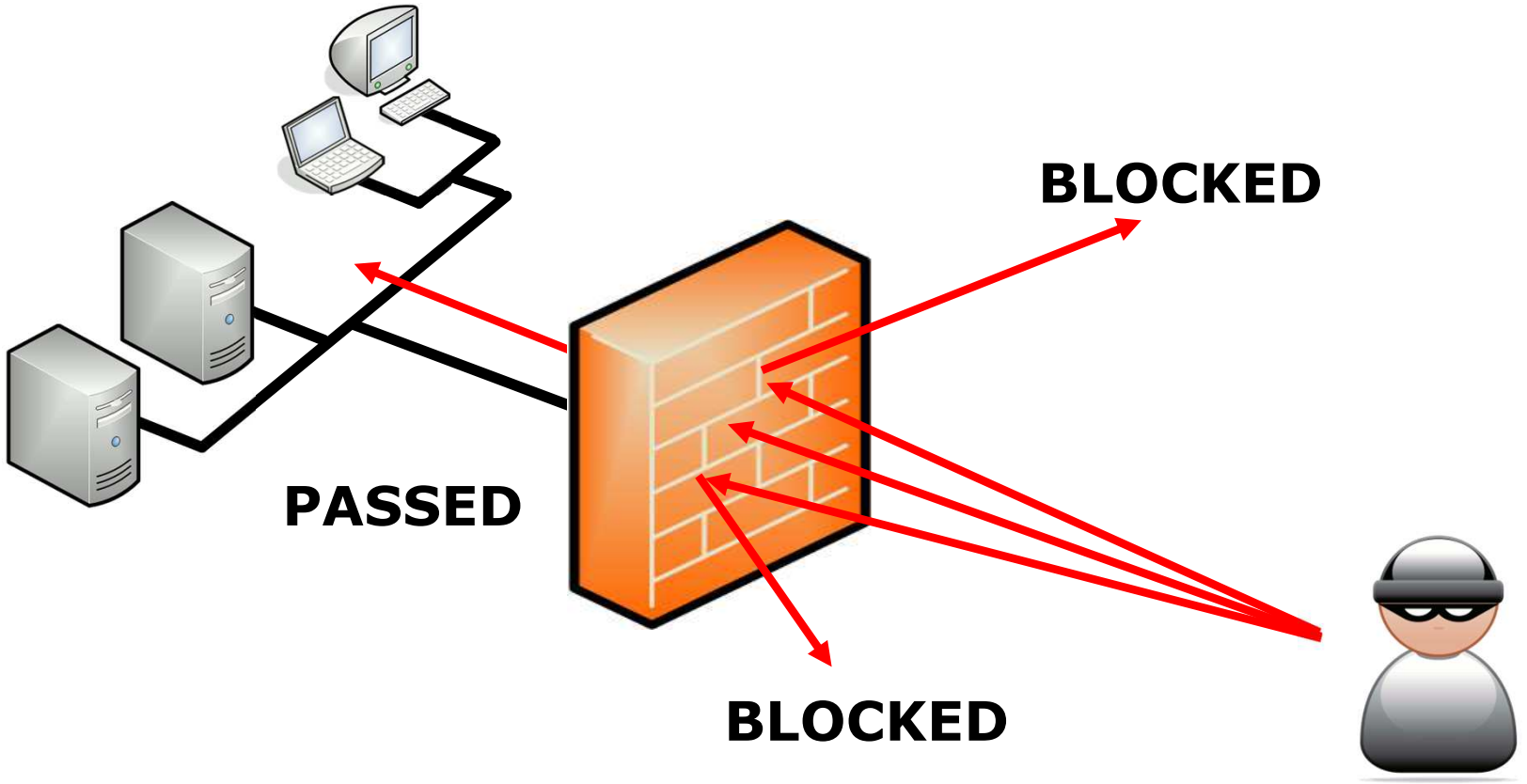
- Einführung “Direkte versus Indirekte Attacken”
- Was ist ein APT Angriff?
- Welche Schutzkonzepte bieten sich an?
- Braucht Deutschland Cyber Security Spezialisten?
- Wie sieht der Penetration Test NG aus?
- Zusammenfassung

Agenda

- **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

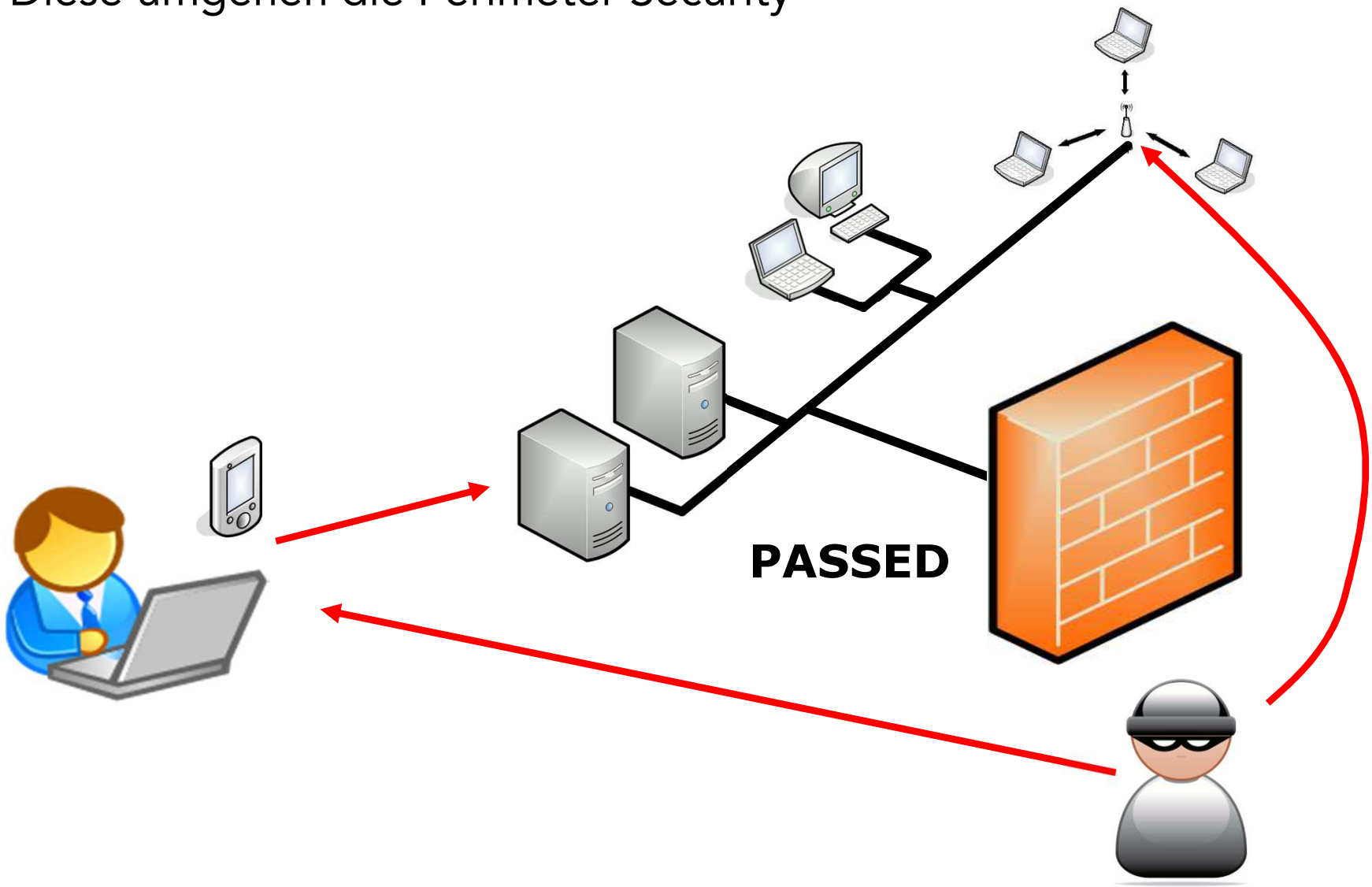
Direkte Angriffe

Hacker Attacken auf Web Anwendungen (Internet Facing)



Indirekte Angriffe

Diese umgehen die Perimeter Security



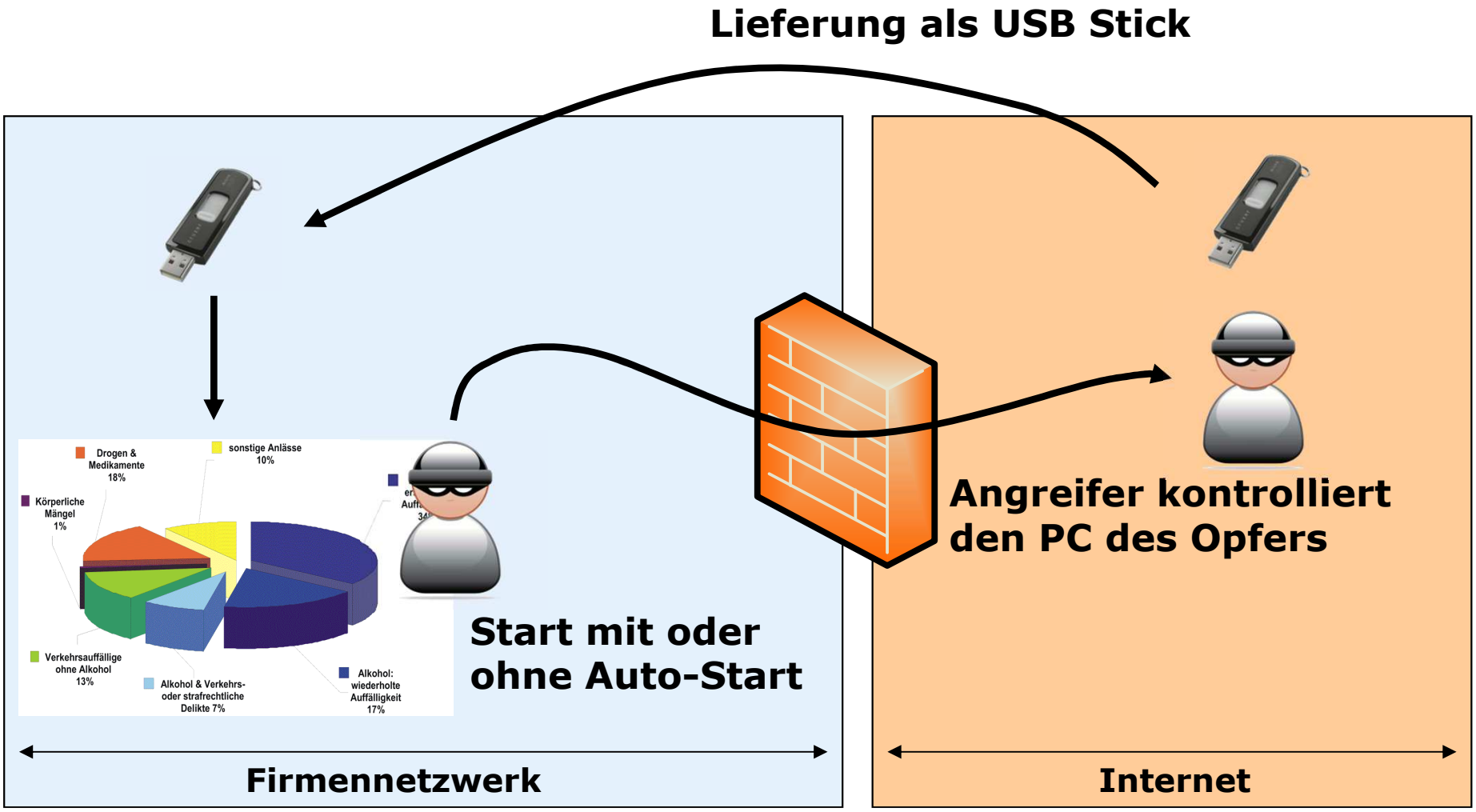
Der USB Stick als Waffe

Stuxnet basierte auf USB Stick

Der Stick enthält ein Trojanisches Pferd

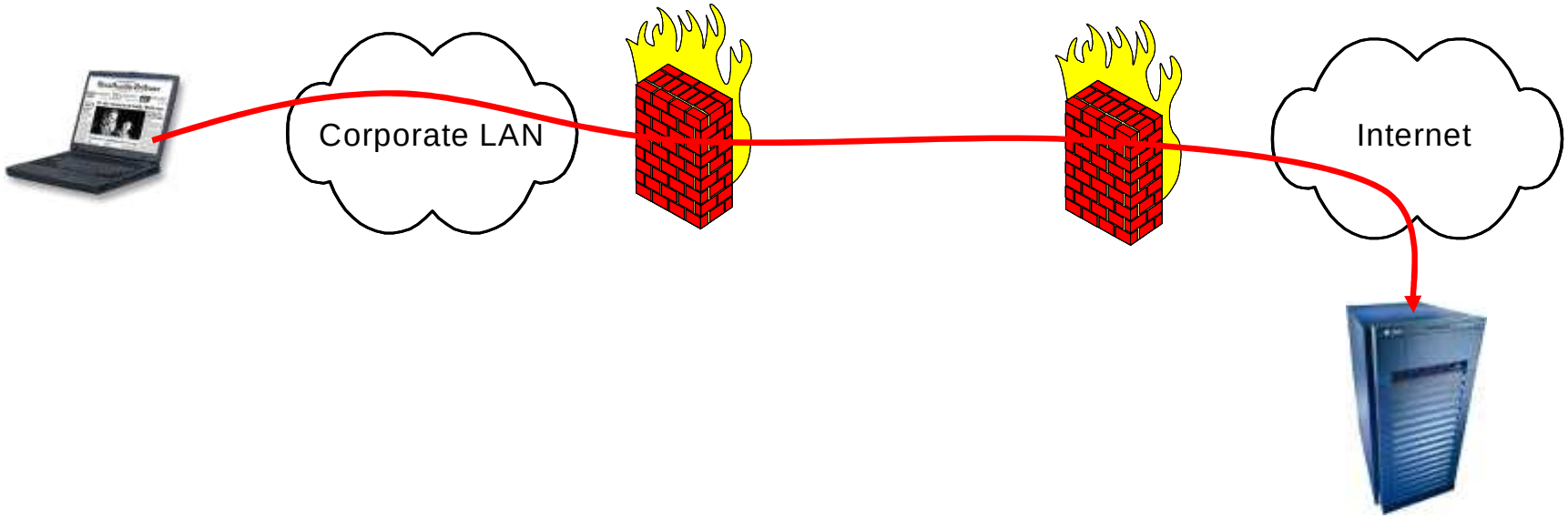
Wie macht es Compass in Pentests?

Covert Channels



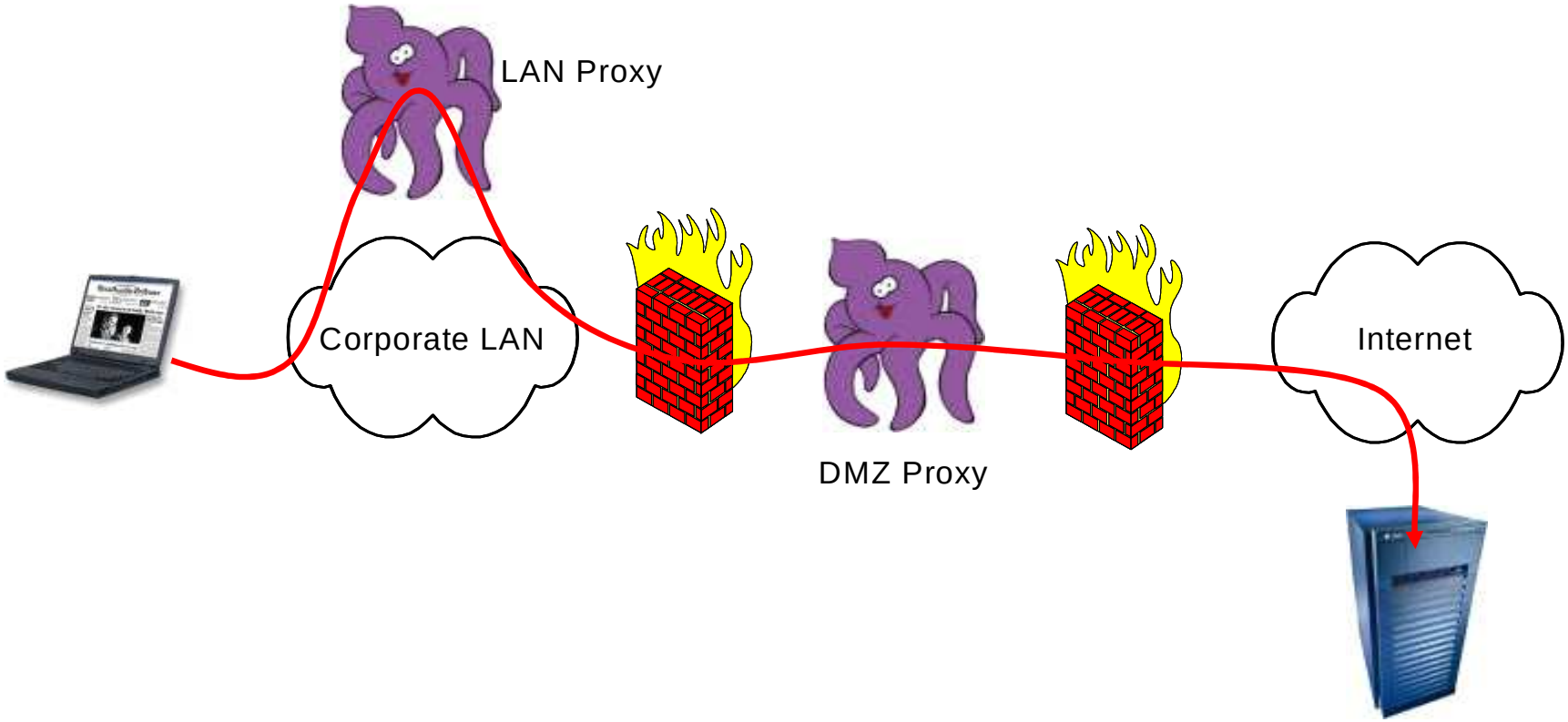
Data Exfiltration & Covert Channel

Einfache Exfiltrierung (Home Systeme)



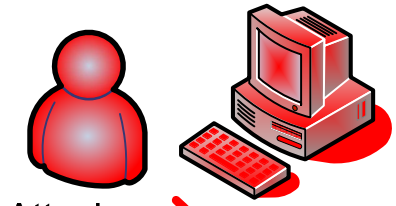
Data Exfiltration & Covert Channel

Exfiltrierung aus Firmen heraus (Proxies)

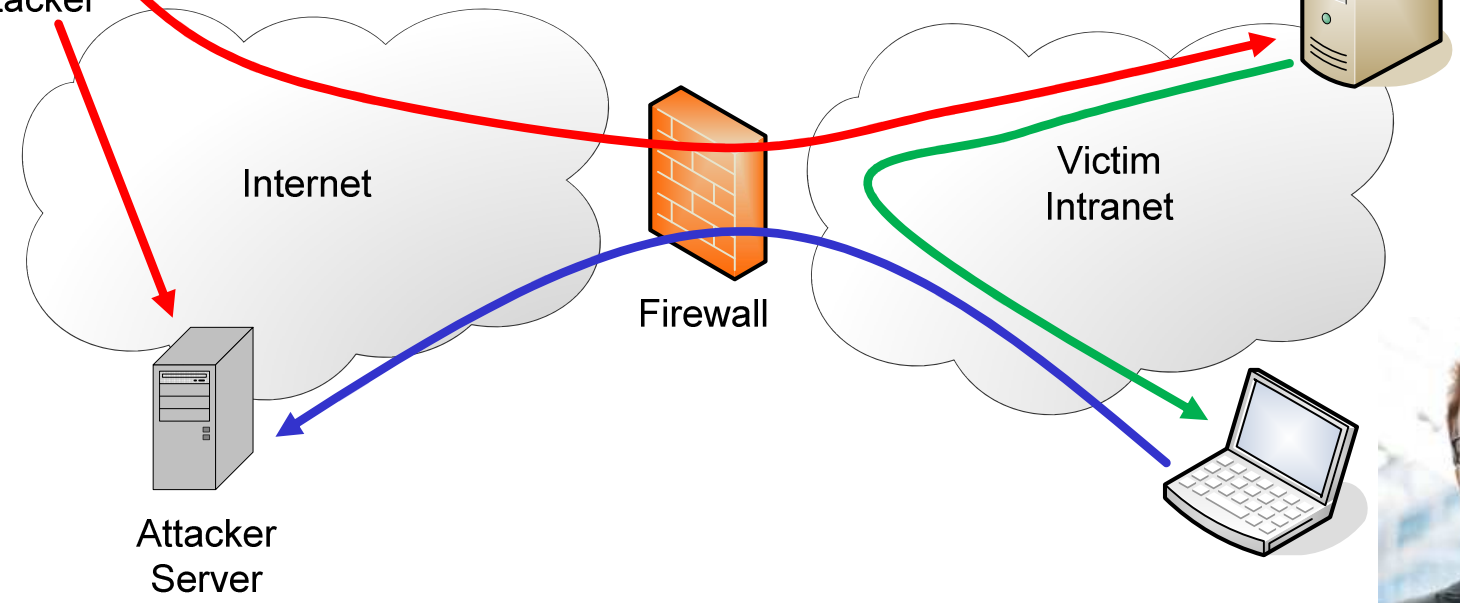


Word Virus

Mail



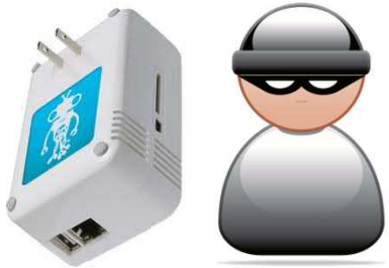
Attacker



Hardware Bot Clients

Hardware Bot Clients

GPRS/UMTS
Covert Channel



Central Command

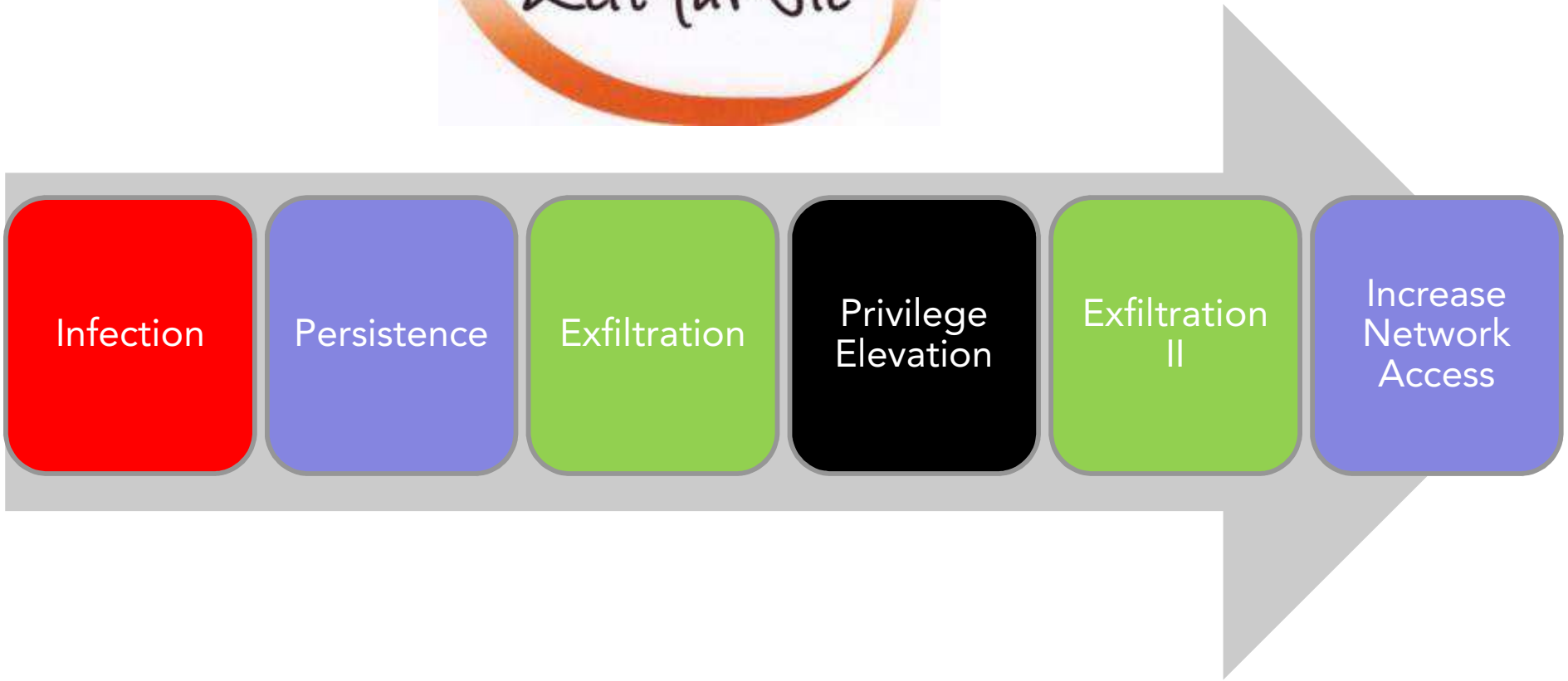
Agenda

- 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

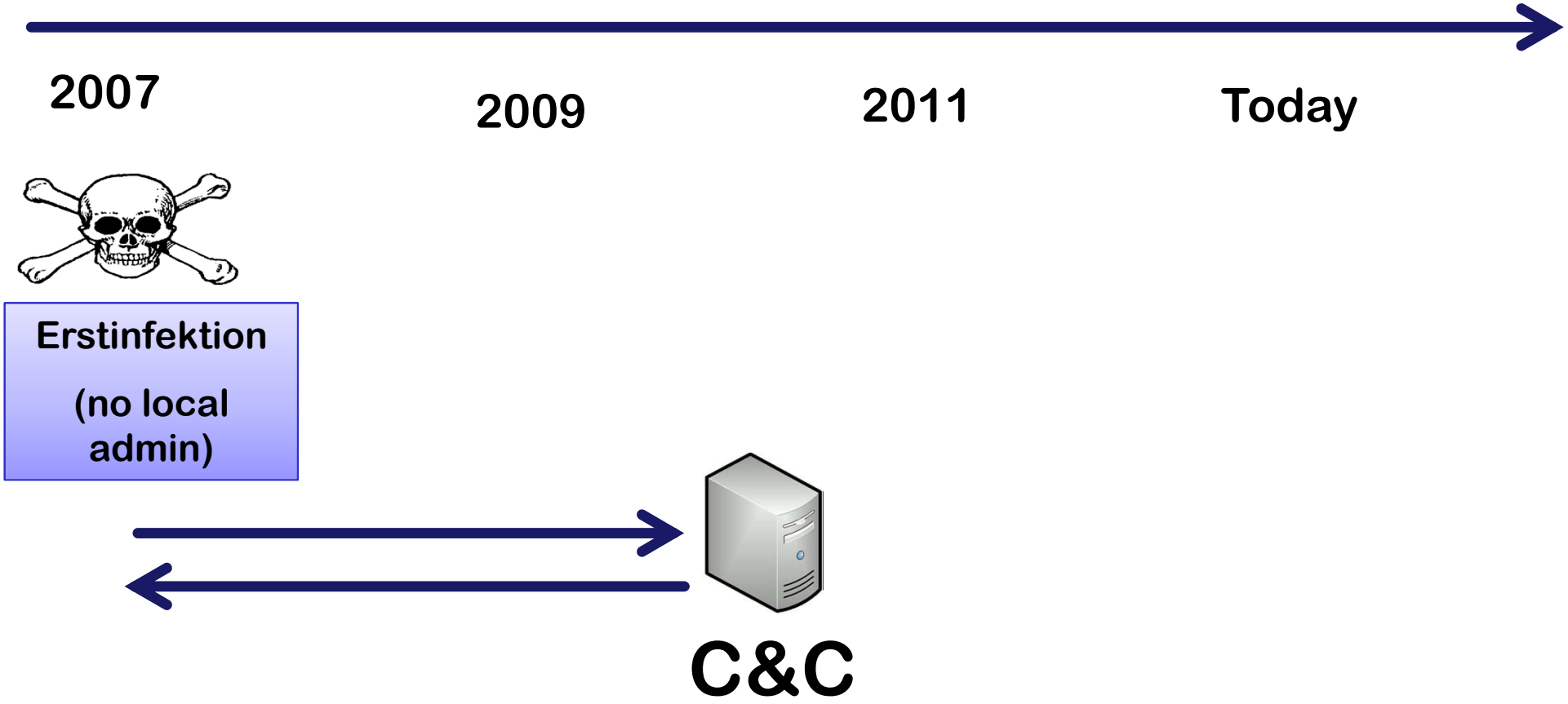
Hackerangriff auf Angela Merkel: "CyberBerkut" bekennt sich

08.01.2015, 10:02 Uhr | dpa

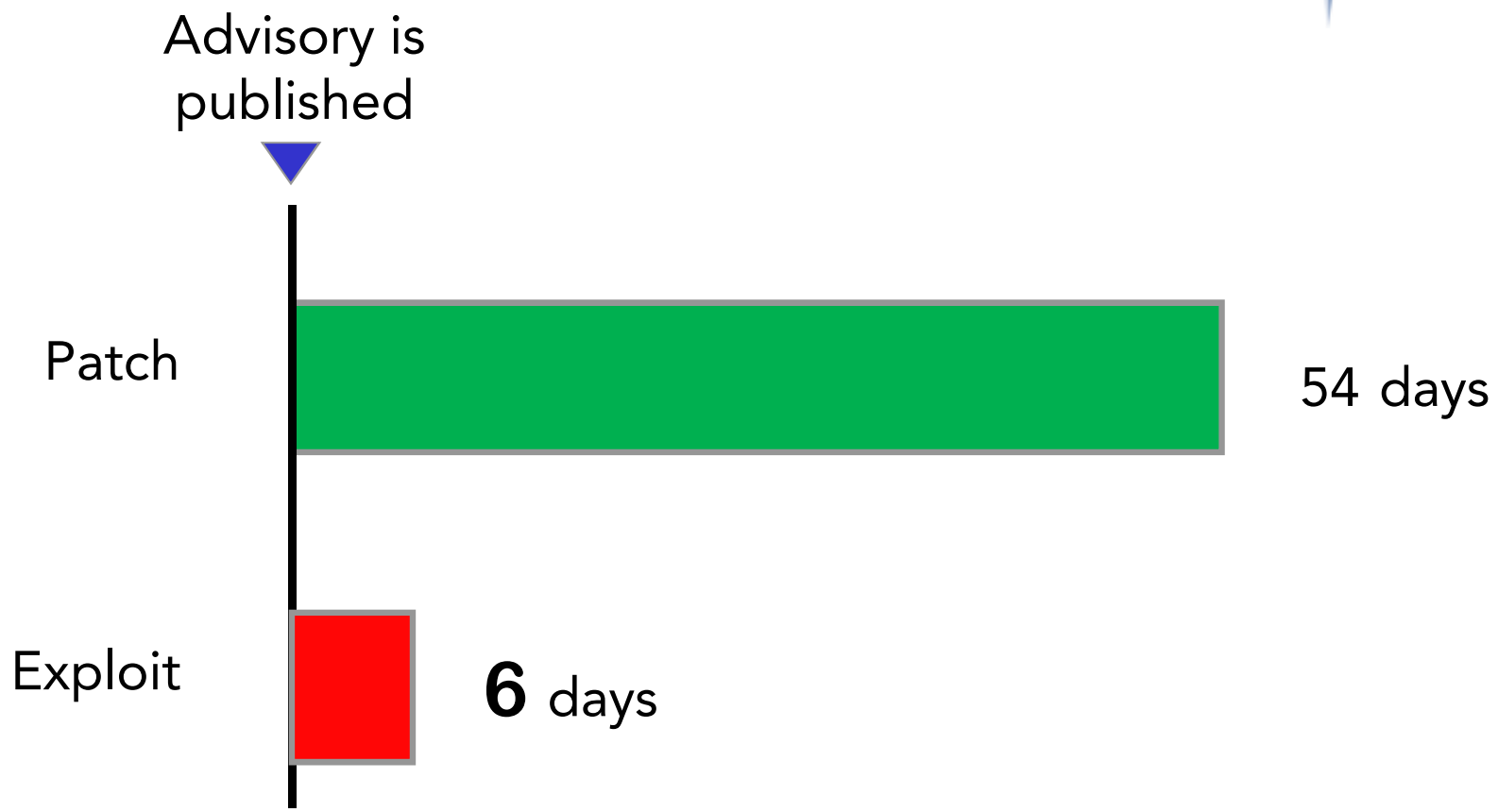
Advanced Persistent Threat



Advanced Persistent Threat



Die Macht der Statistik – 48 Tage



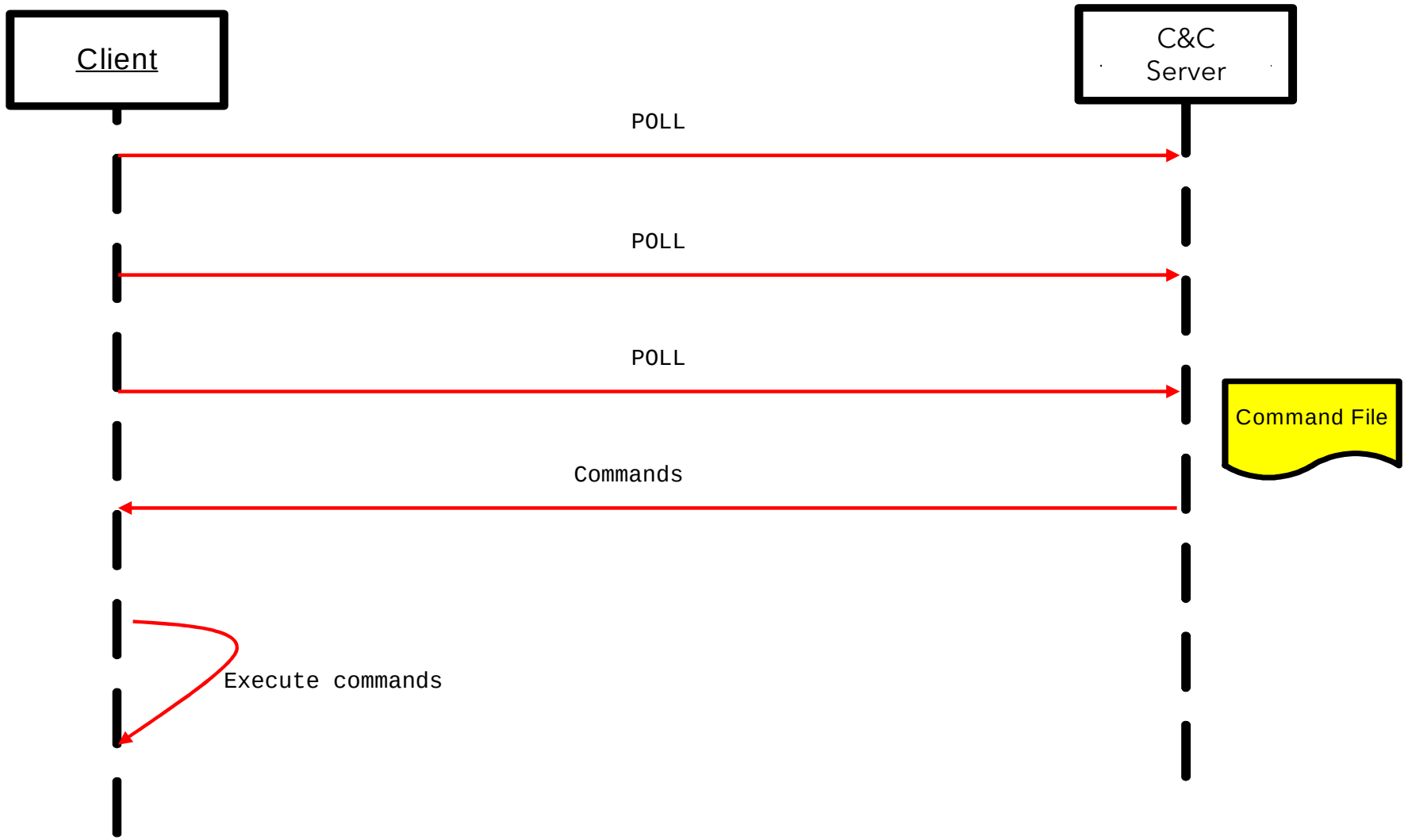
[3] ETHZ Stefan Frei 2009 (Dissertation): We found that exploit availability consistently exceeds patch availability since 2000

Die Macht der 48 Tage

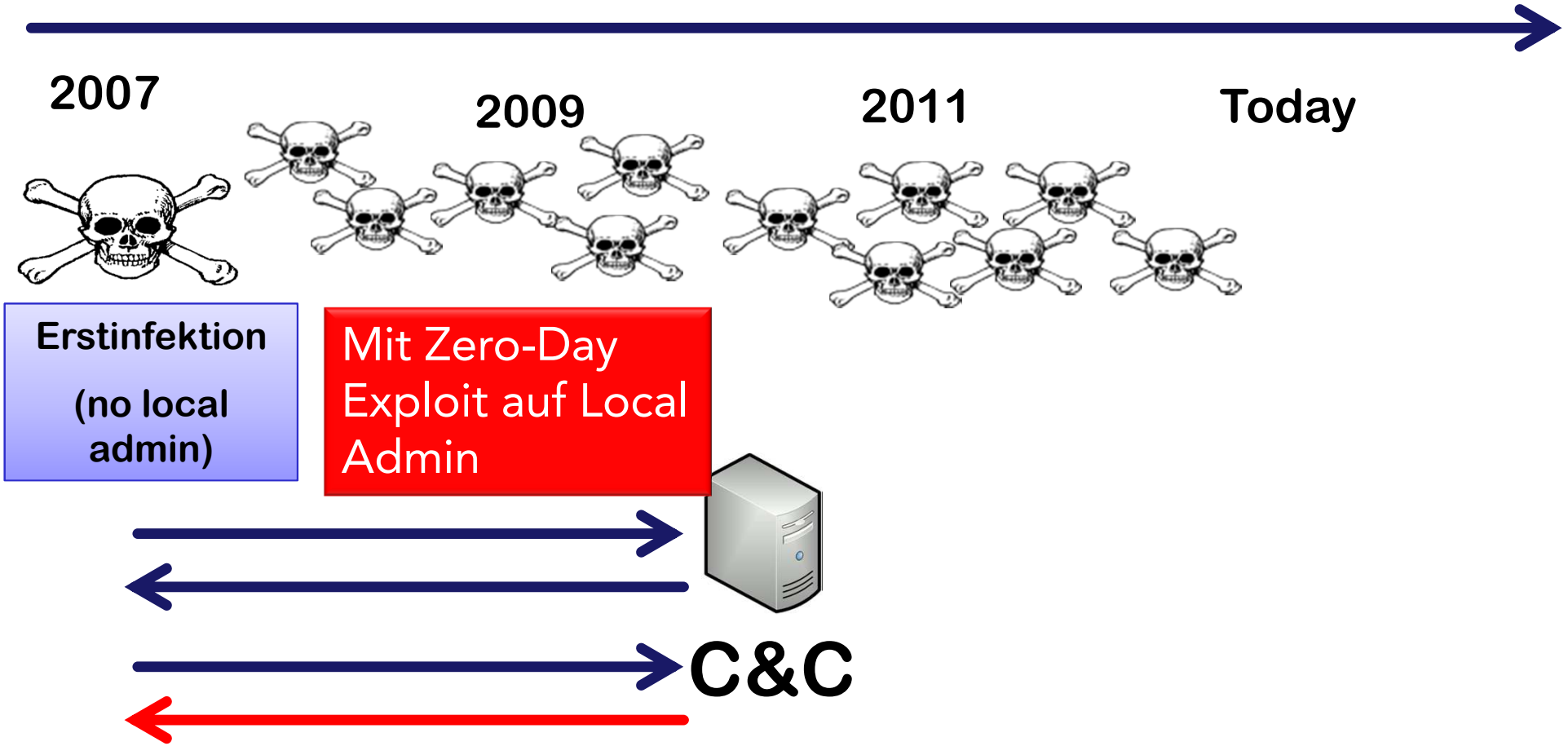
Statistisch gesehen sind alle Firmen regelmässig während 48 Tagen verwundbar und diesen Zustand nützen die APT Angreifer aus!

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

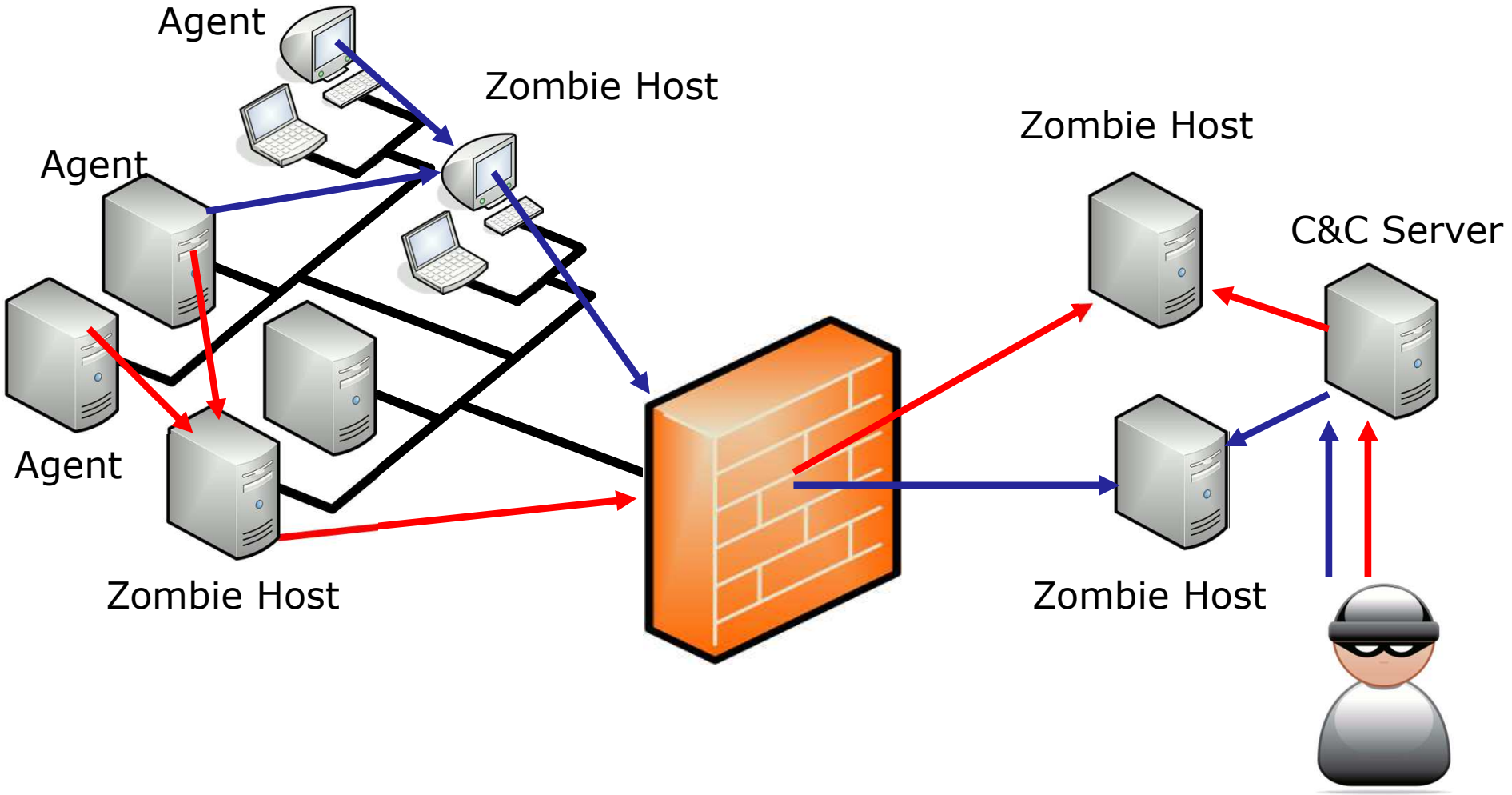
Command & Control Communication



Advanced Persistent Threat



Advanced Persistent Threat

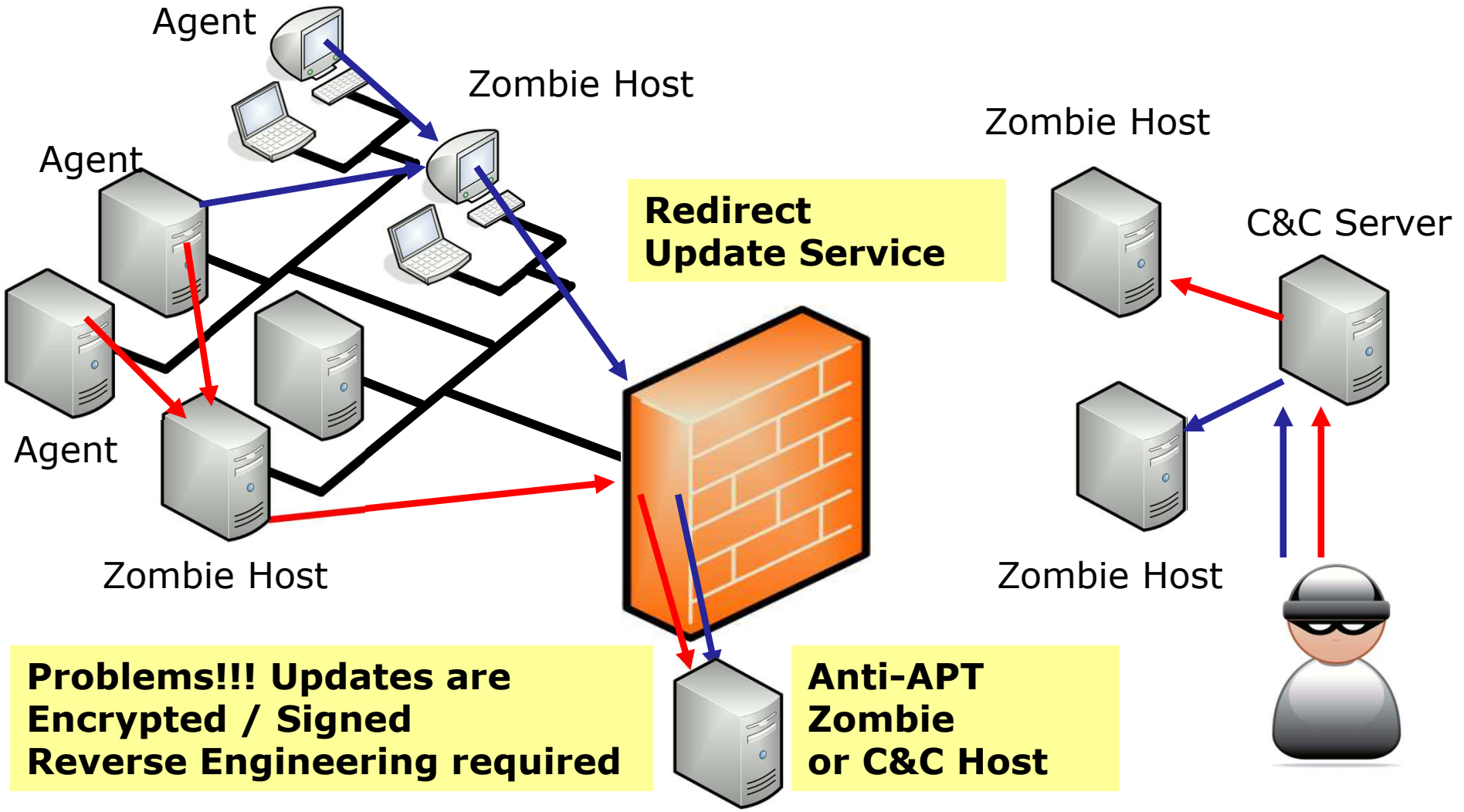


Agenda

- 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

Advanced Persistent Threat

Reaktion auf APT ? – C&C Traffic Redirection



Schutzkonzepte

Beten und nichts machen. Wird schon nichts passieren

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

Schutzkonzepte

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

Monitoring mit IDS/IPS Next Generation

FireEye

DAMBALLA

APT Detection mit Splunk

FireEye basiert auch auf Splunk

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

HACKING-LAB

HOME

E-Mail: Password: Login »

29007 Anonymous User

- 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

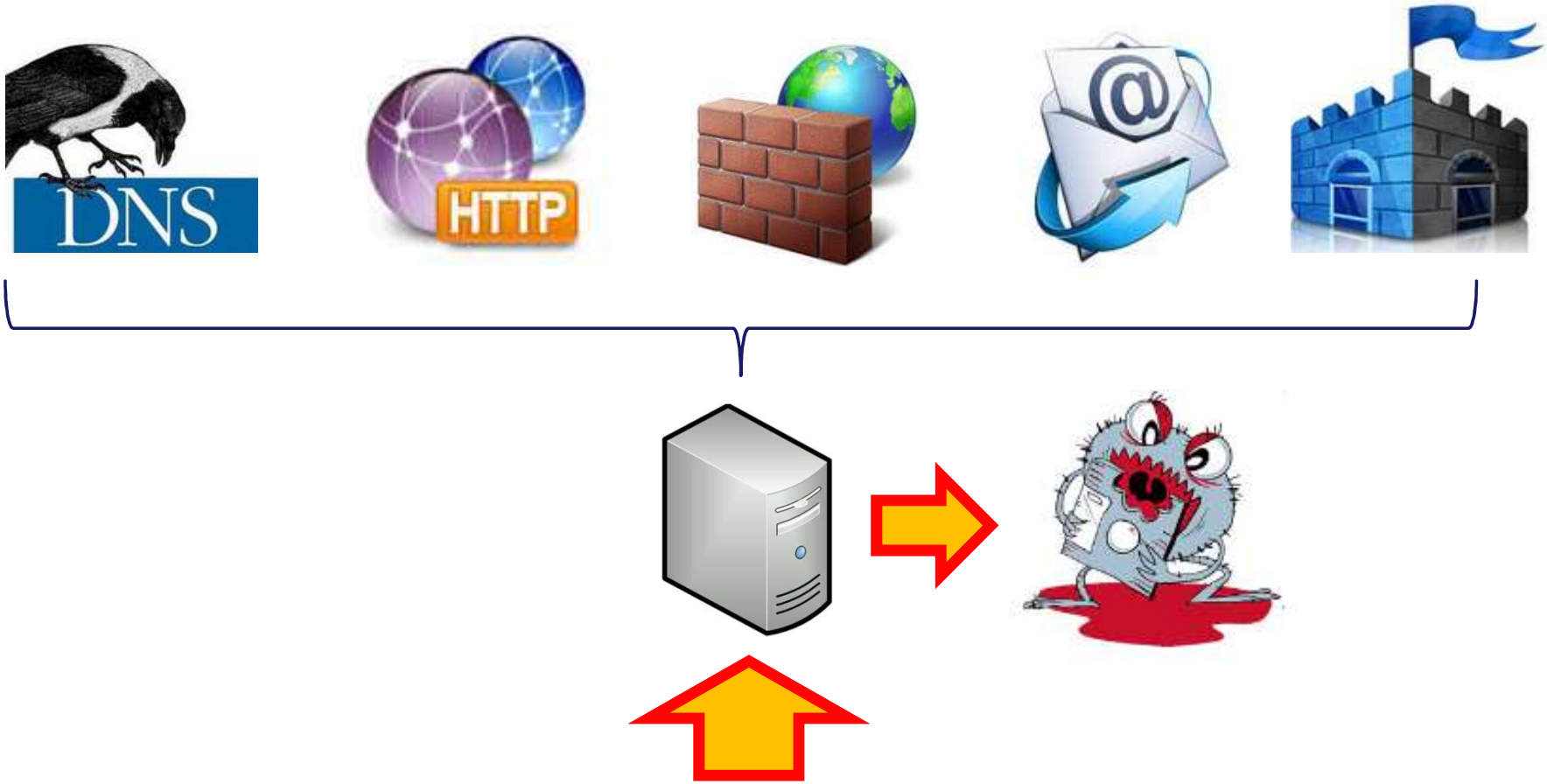

www.tavabaki.gr

Splunk Installation in Hacking-Lab

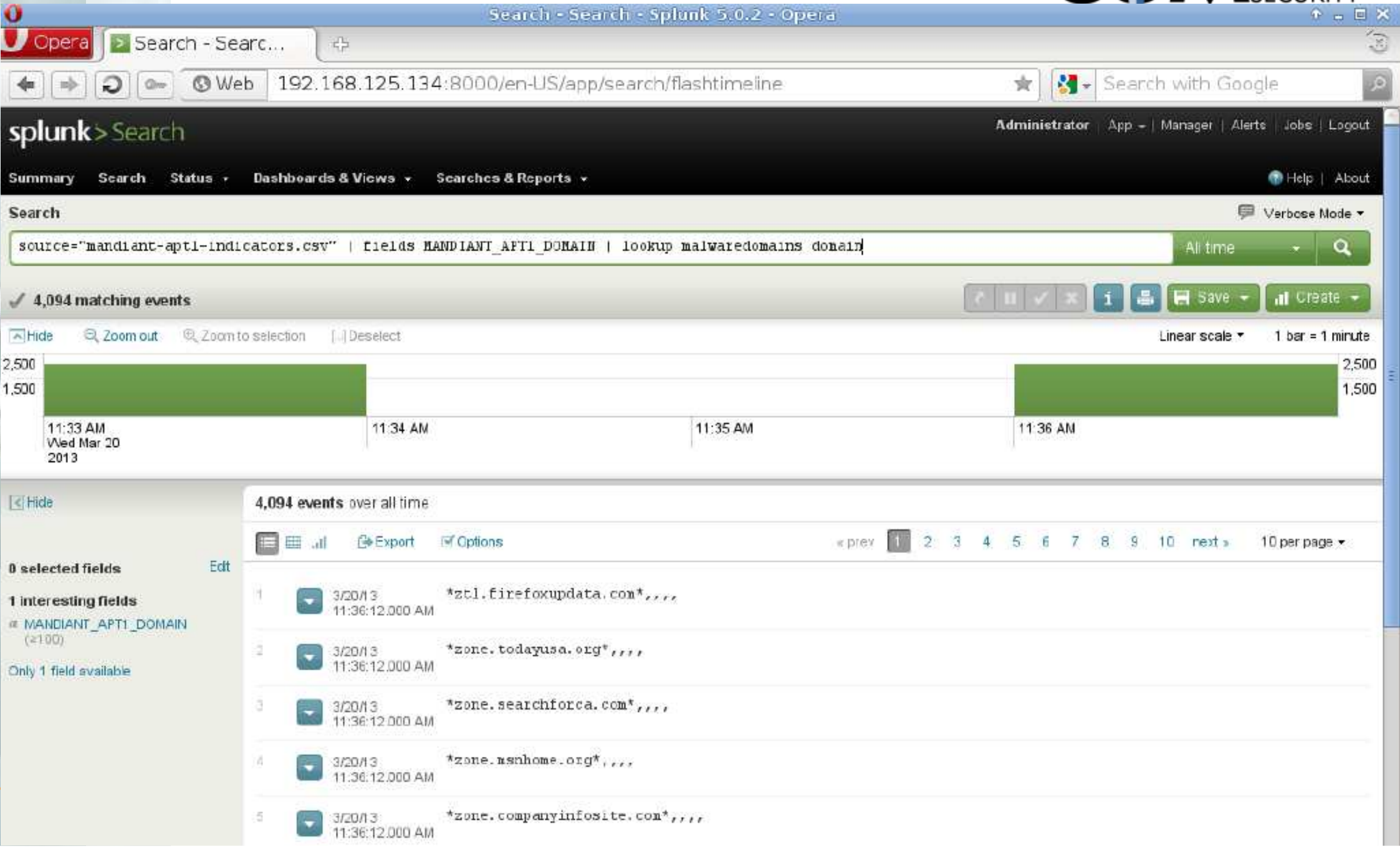
splunk>™

APT Intelligence Engine

Splunk Installation in Hacking-Lab



Splunk Screenshot



Internet Lookups mit getwatchlist

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

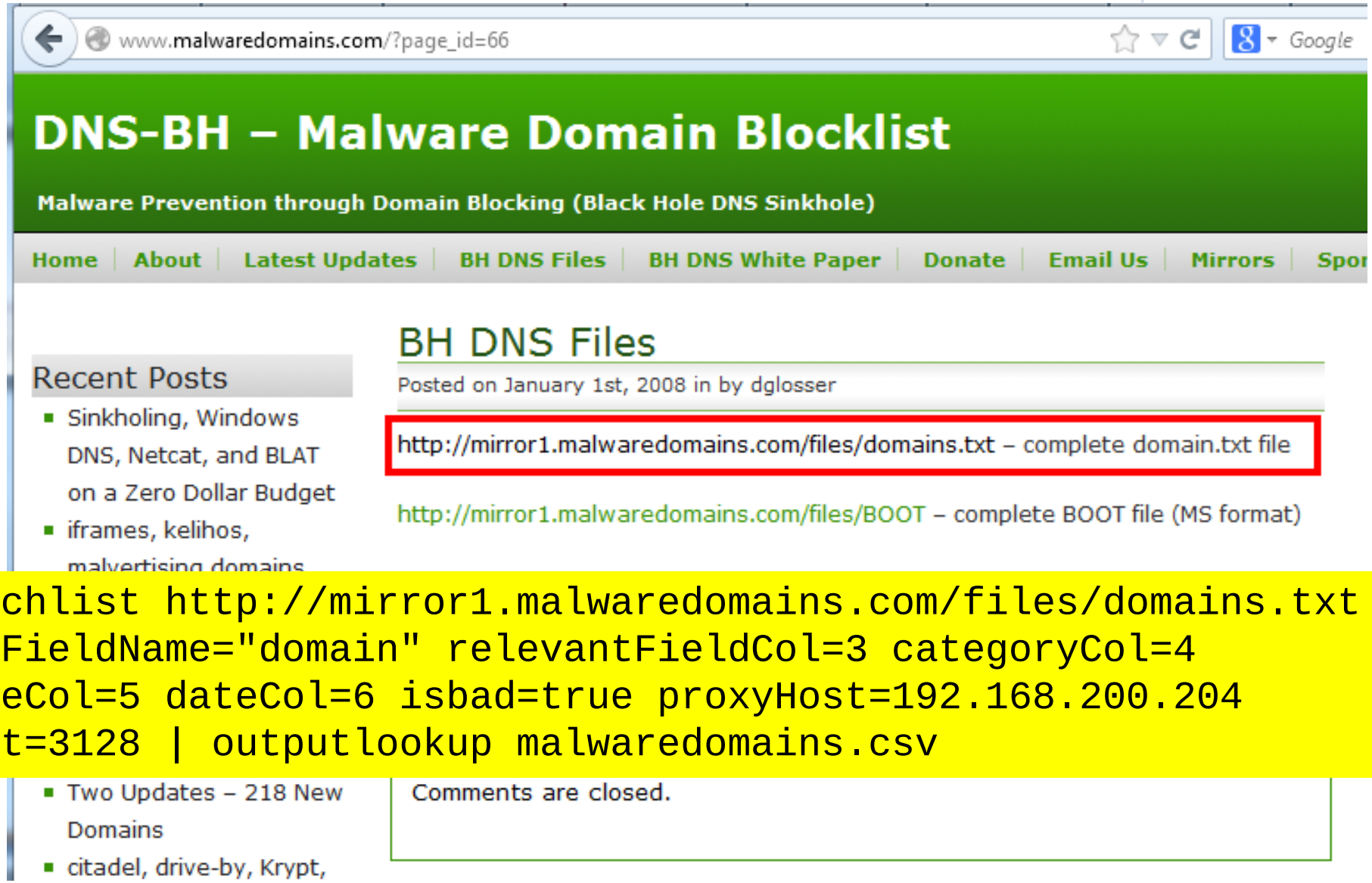
Mandiant Sources

- 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/

Malwaredomains



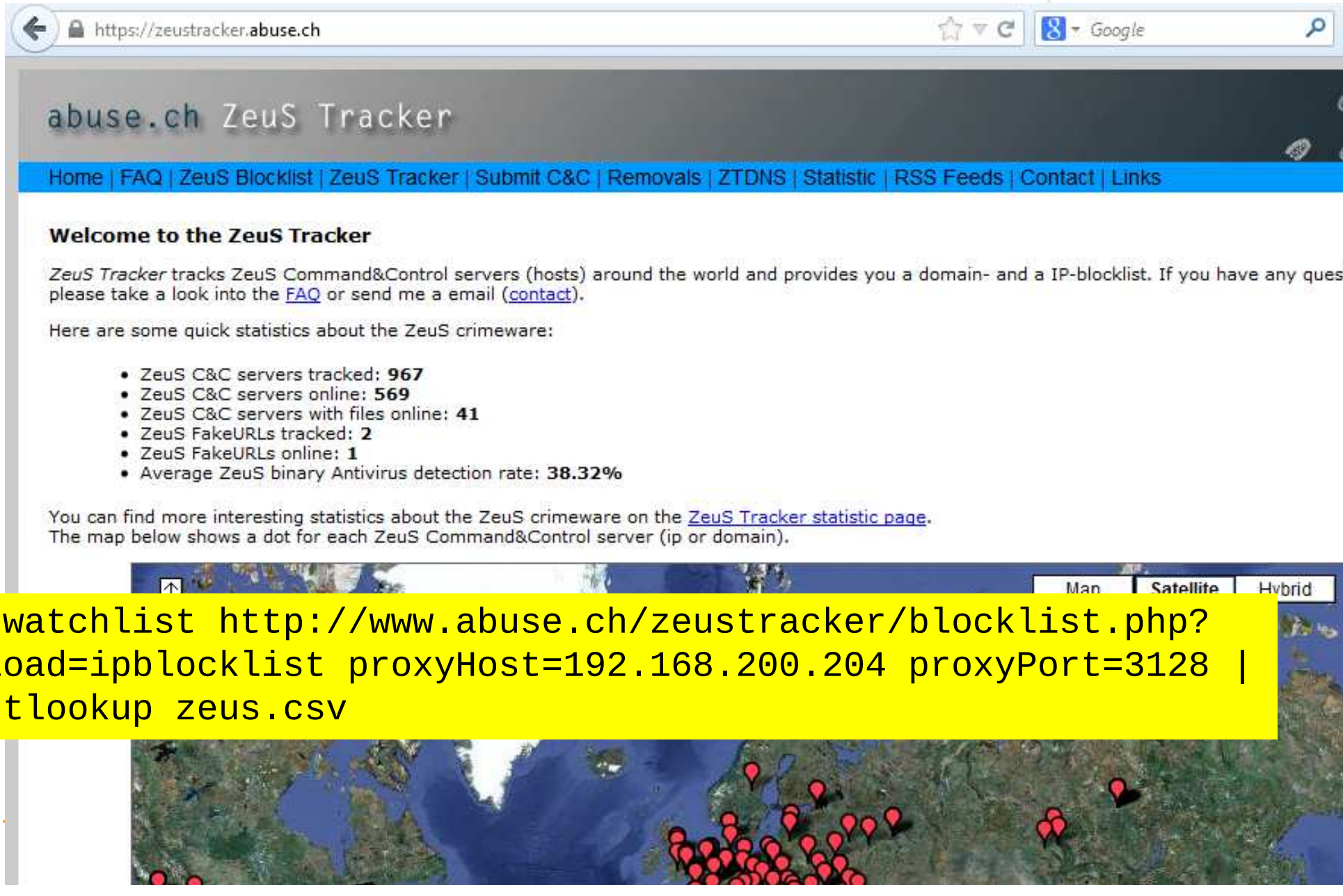

```
| getwatchlist http://mirror1.malwaredomains.com/files/domains.txt
relevantFieldName="domain" relevantFieldCol=3 categoryCol=4
referenceCol=5 dateCol=6 isbad=true proxyHost=192.168.200.204
proxyPort=3128 | outputlookup malwaredomains.csv
```

Mandiant Source

www.joshd.ca/sites/default/files/mandiant-apt1-indicators-list.txt

```
MANDIANT-APT1-DOMAIN,MANDIANT-APT1-MD5SUM,MANDIANT-APT1-FILENAME,MANDIANT-APT1-FILESIZE,MANDIAN
*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*,*c2xlZXA=*
*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\
*busketball.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




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

Malware Samples

Malware Sample Acquisition Cycle

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

Open Indicators of Compromise (OpenIOC)

Improvement trough 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 XML File Format

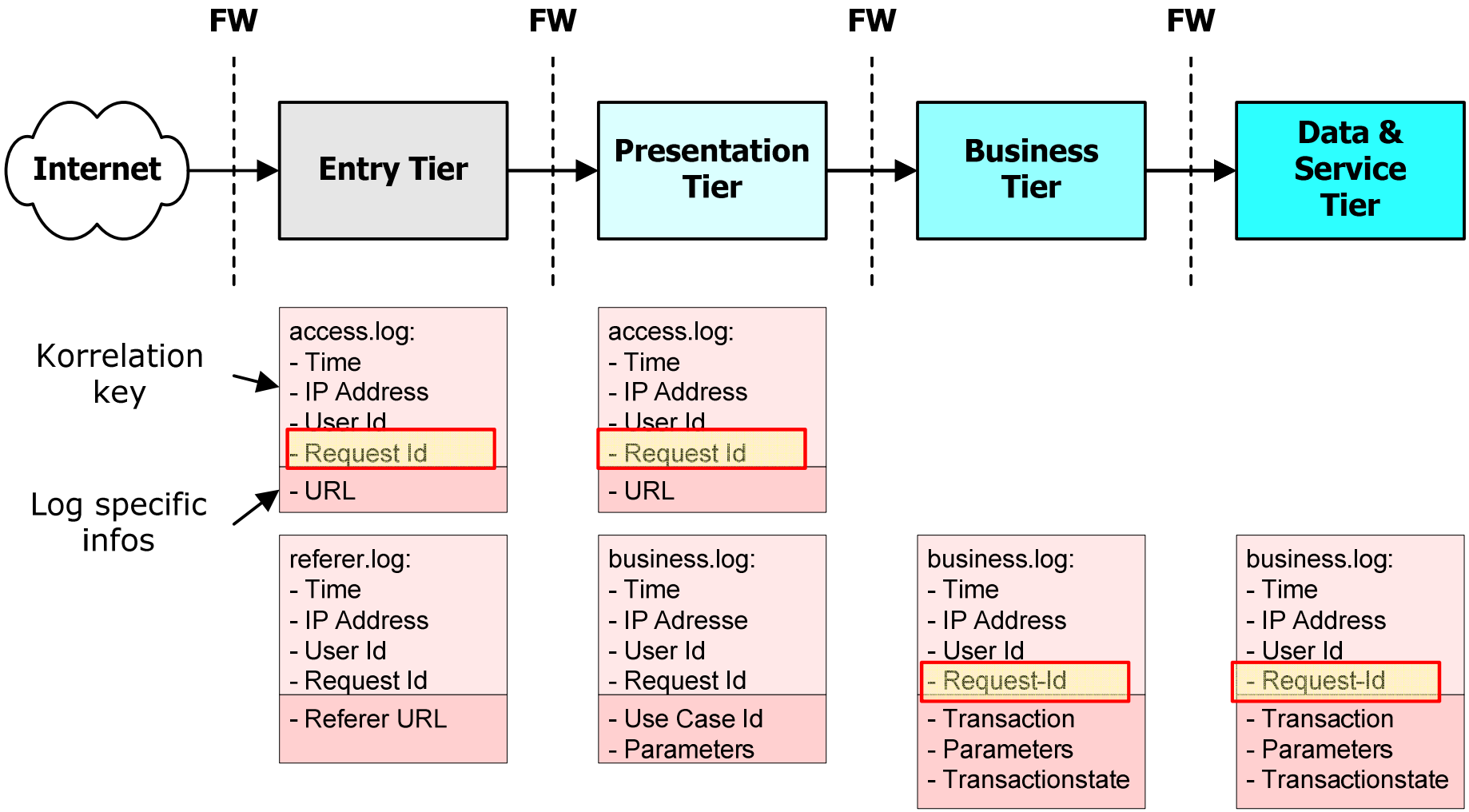
IP Reputation (Honeypot DB)

Description

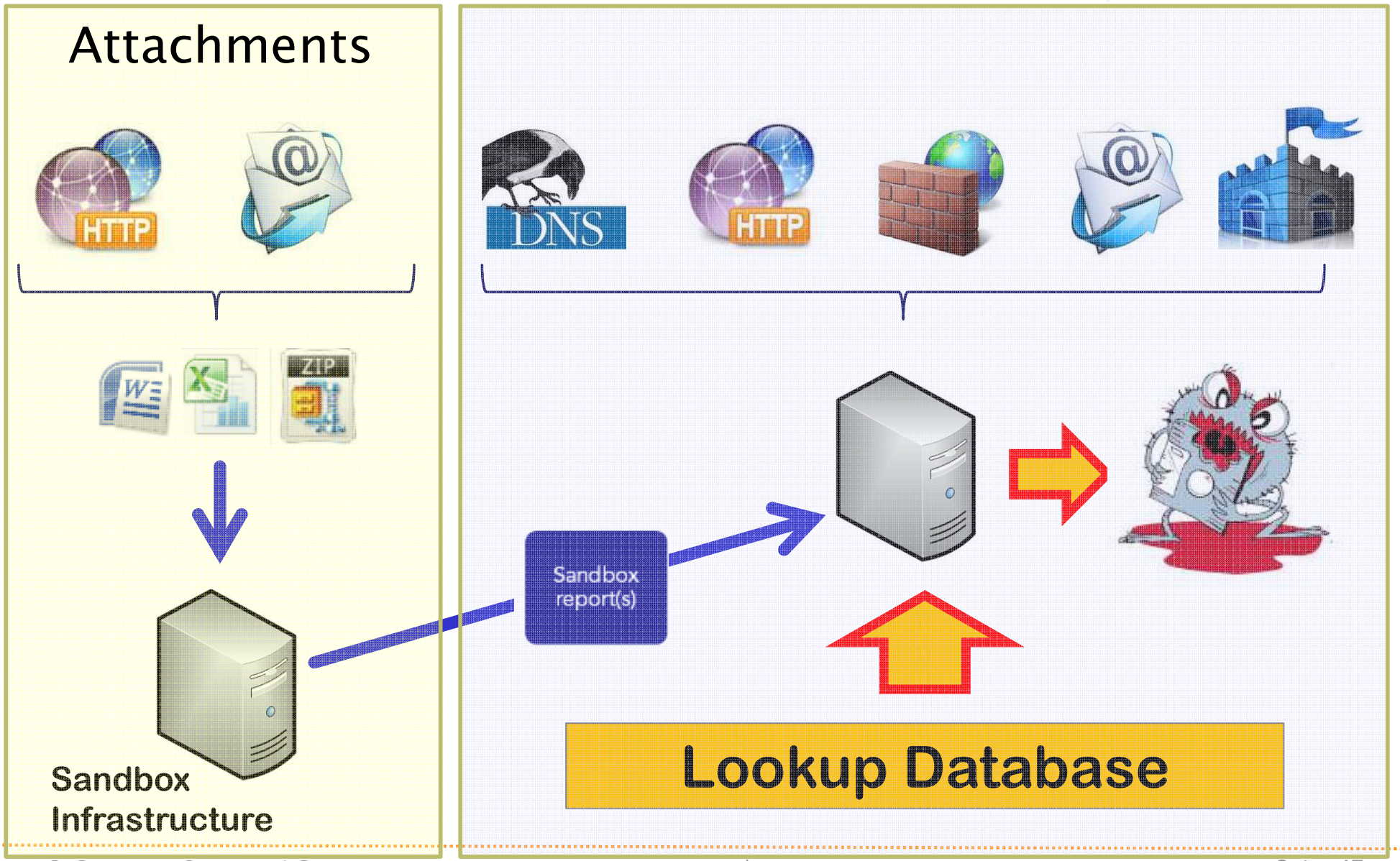
This app allows you to enrich your IP Data with realtime threat information by contacting the Project Honey Pot database via DNS-Blacklist requests.

Voraussetzungen für diese Analysen sind ‘**gute**’ Logfiles

Correlation across tier (Simplified illustration)



Splunk Installation in Hacking-Lab



Cuckoo Sandboxing Analysis

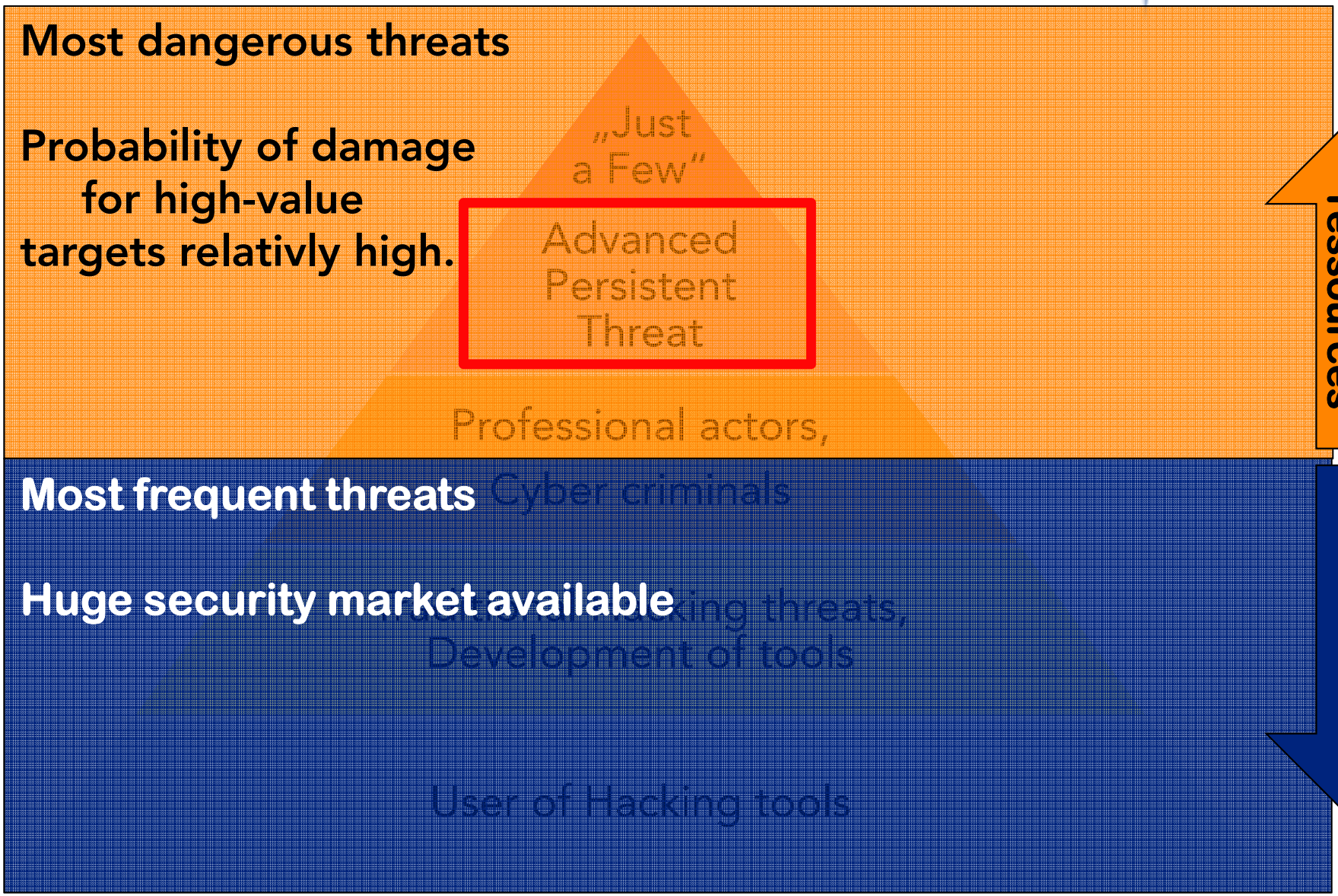
- Do I want to analyze PDF exploits?
- Do I want to analyze Office exploits?
- Do I want to analyze PHP and Perl scripts?
- Do I want to analyze browsers' exploits?
- What else do I want to analyze?
- Do I want it to communicate with the outside?

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

Agenda

- 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

Bedrohungs Pyramide




Cyber Security
Challenge
GERMANY

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

Cyber Security Challenge: Partner

- **Kooperationspartner**

if(is) internet-sicherheit.

TeleTrusT Pioneers in IT security.

COMPASS SECURITY

Heise Zeitschriften Verlag

- **Förderer**

IT-Sicherheit IN DER WIRTSCHAFT

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

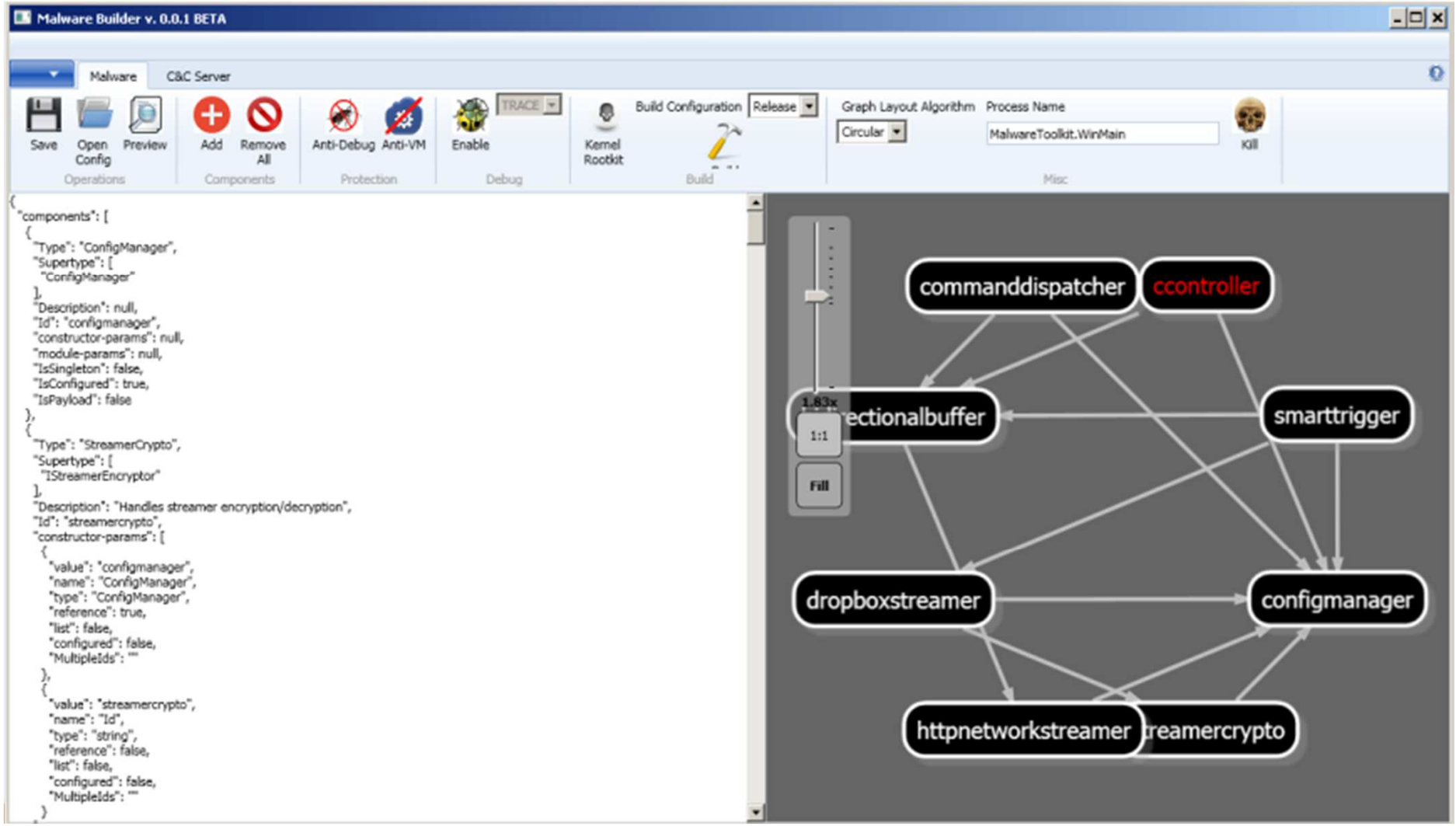
Agenda

- 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

Wie müssen Penetration Tester

- Testing von APT ohne “Schadware”
- Unabhängig von Metasploit und allfälliger Viren Erkennung
- Unterstützung vieler verschieder Covert Channels

Compass APT Testing Framework



Compass APT Testing Framework

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

Agenda

- 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**

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!**