

ADVANCED PERSISTENT THREATS

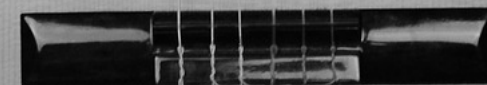
APT



HSR

HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz



Stuxnet



Hacker dringen in EDA-Computernetzwerk ein

Das Departement für auswärtige Angelegenheiten ist erneut Opfer von Cyberkriminellen geworden: Bereits zum dritten Mal in fünf Jahren haben Unberechtigte auf Daten des EDA zugegriffen – die Täter sind unbekannt.



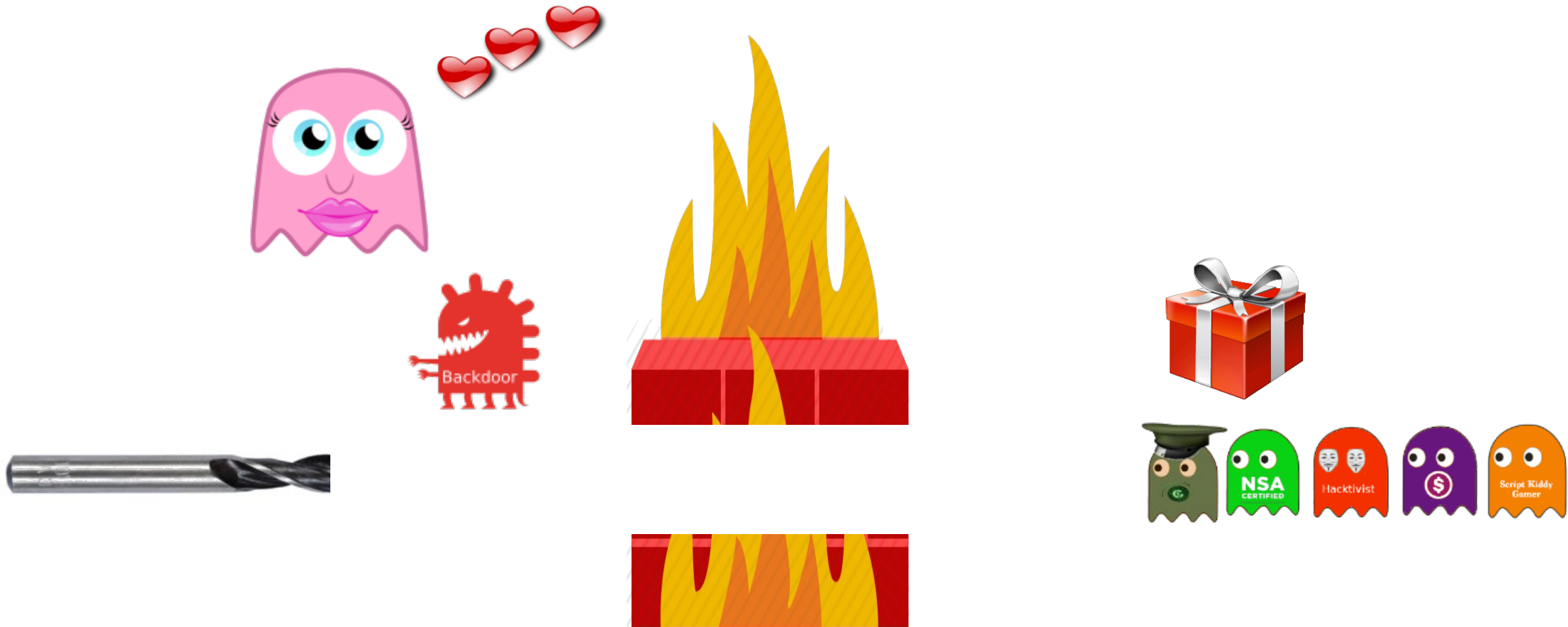


Angriffe über den Mensch

Social Engineering Attacks



Angriff auf den «Mensch»



Infektion «Blackout»

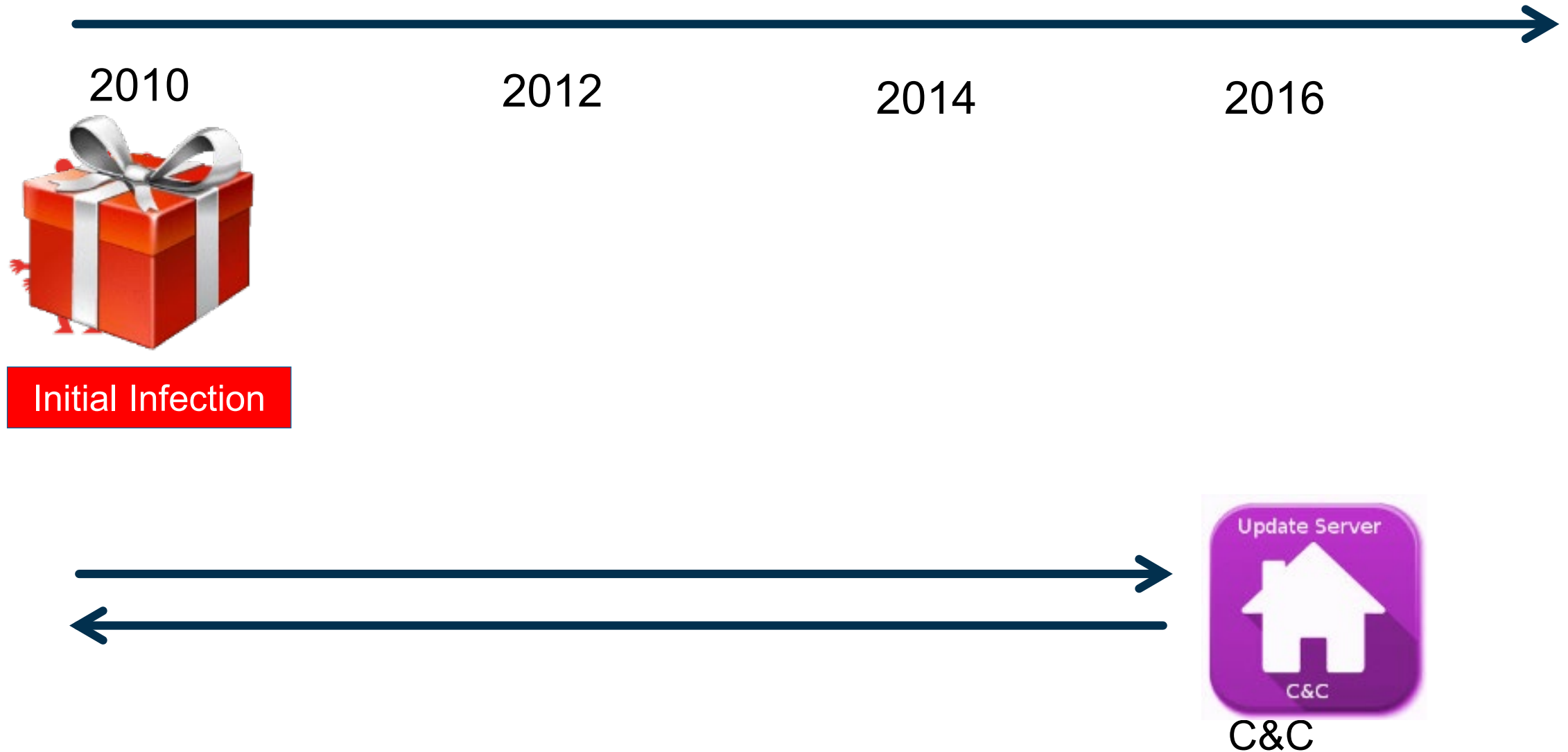


Infektion durch E-Mail



Microsoft Office
Word Document

APT erklärt



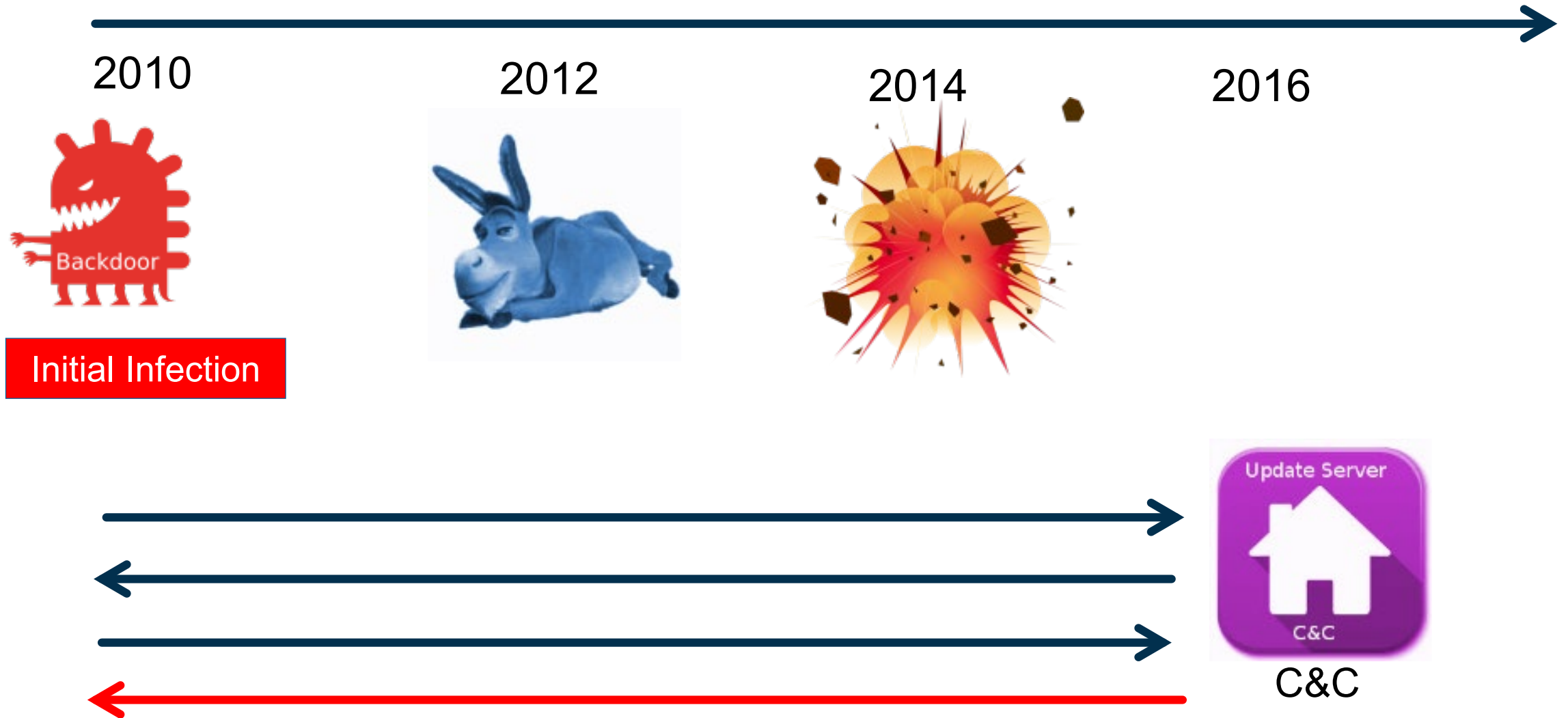
APT erklärt



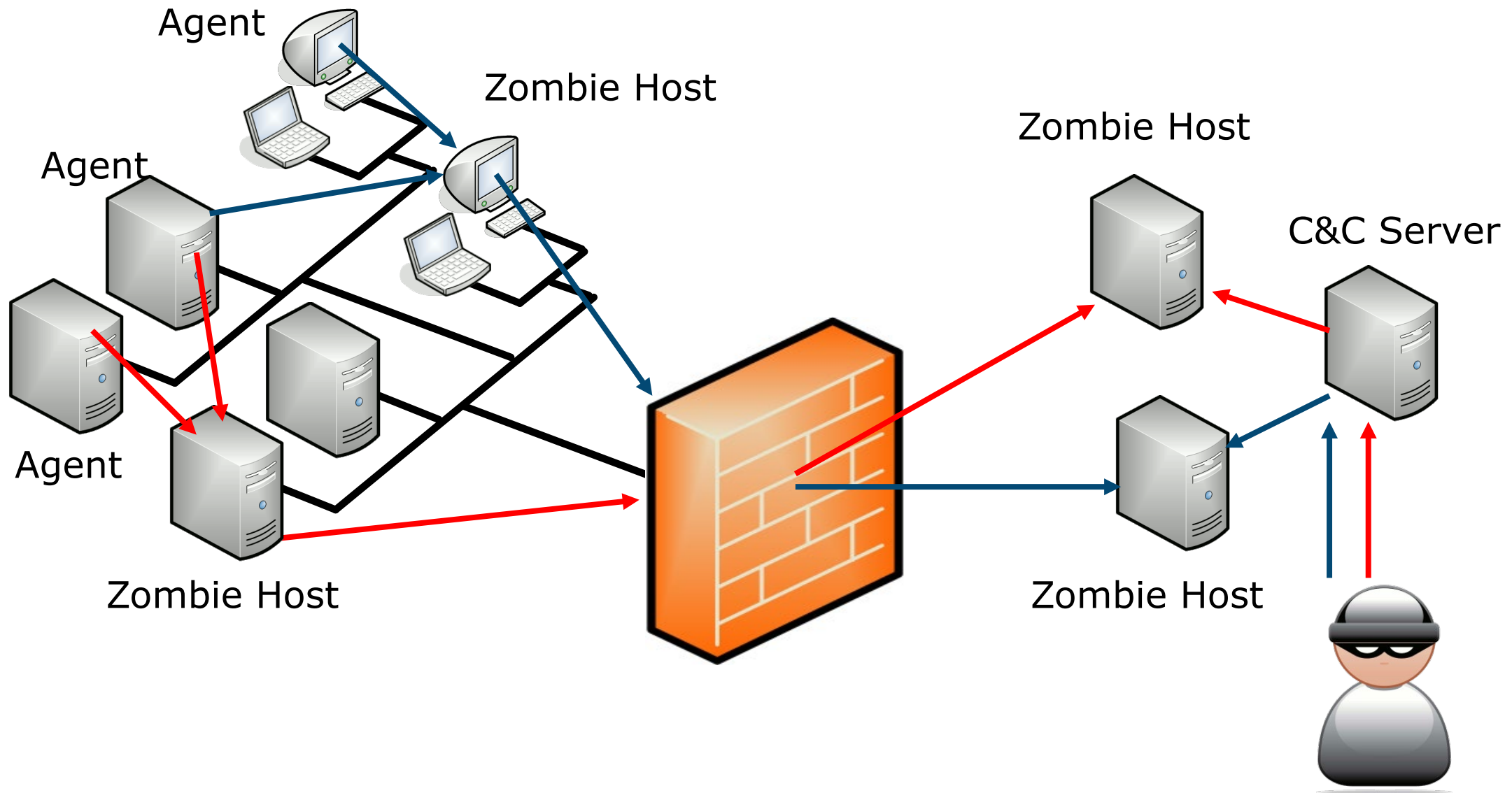
APT erklärt



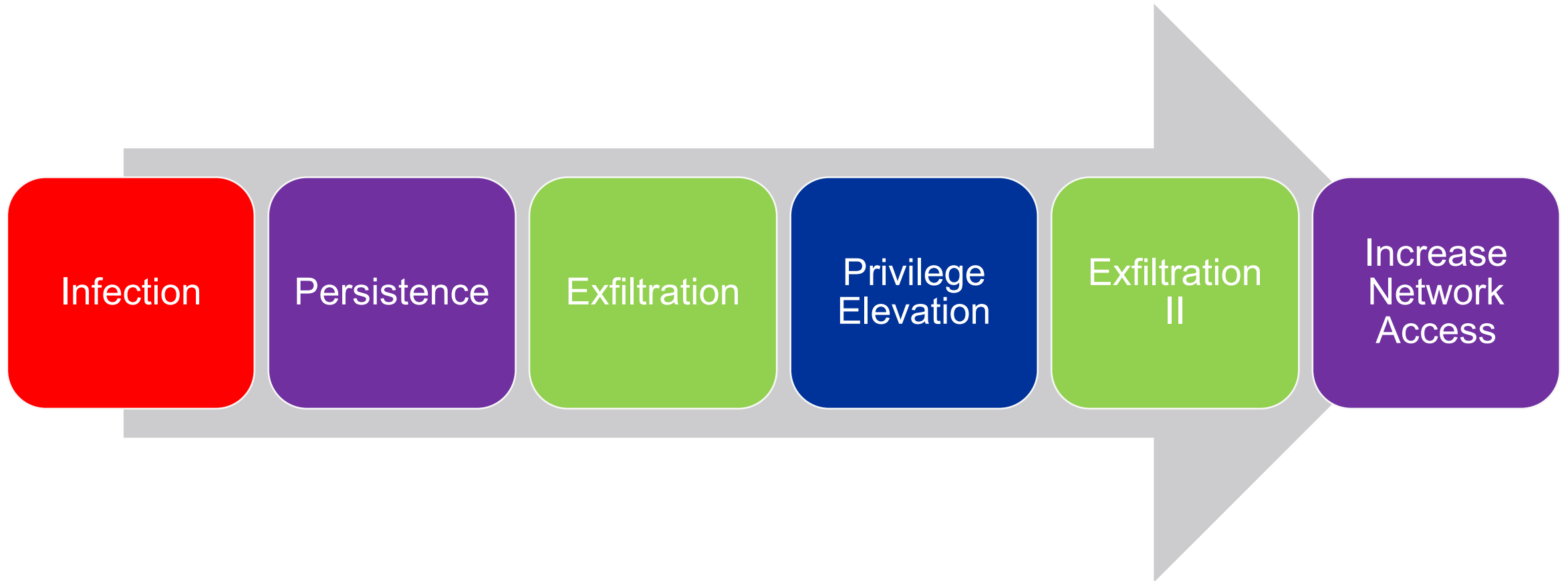
APT erklärt



APT erklärt



APT erklärt



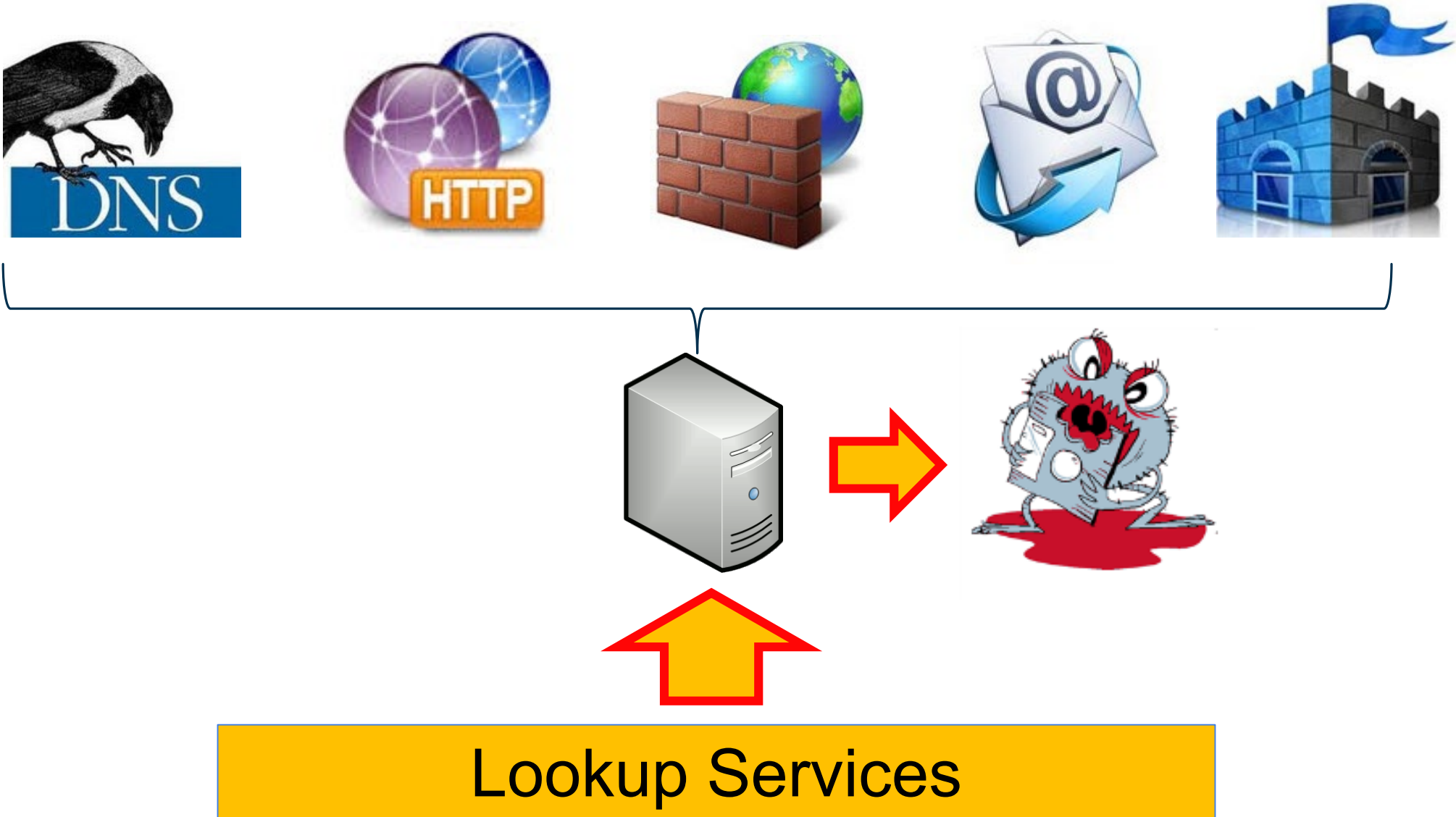
Was macht Locky, WannaCry & Co?



Fachjargon = Ransomware

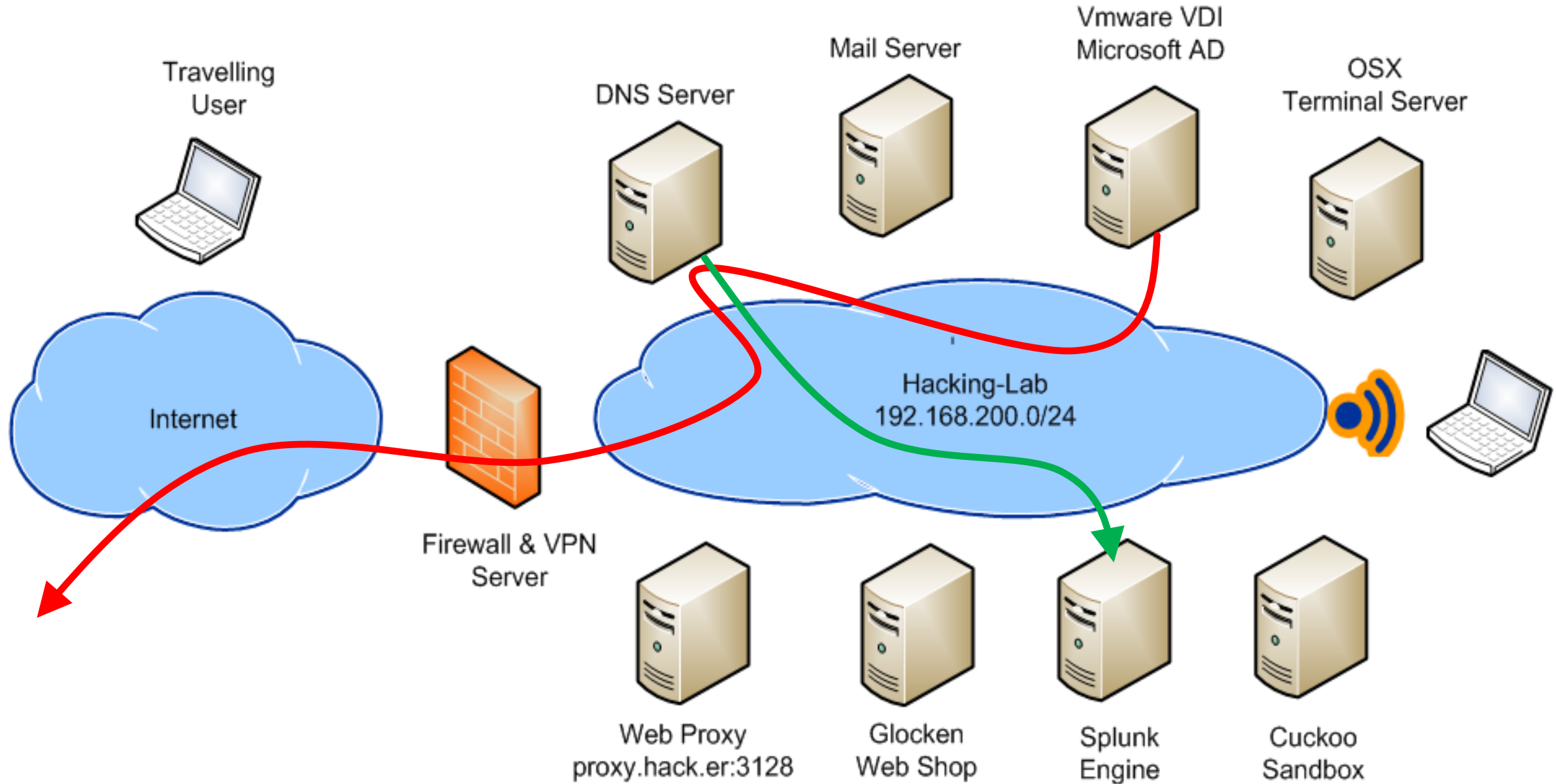
APT Detection using «Intelligence»

APT Detection / Level 1

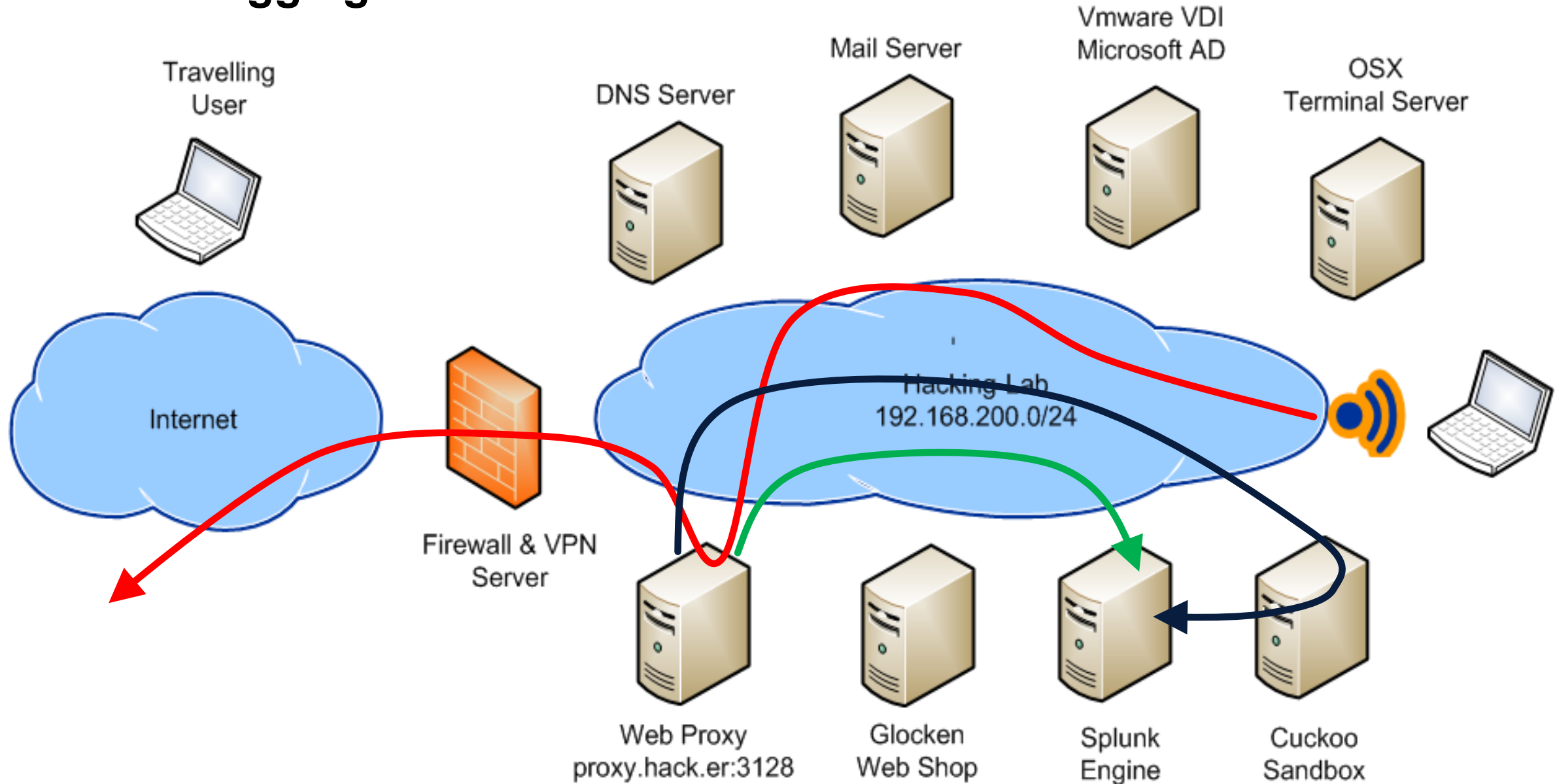


Logging

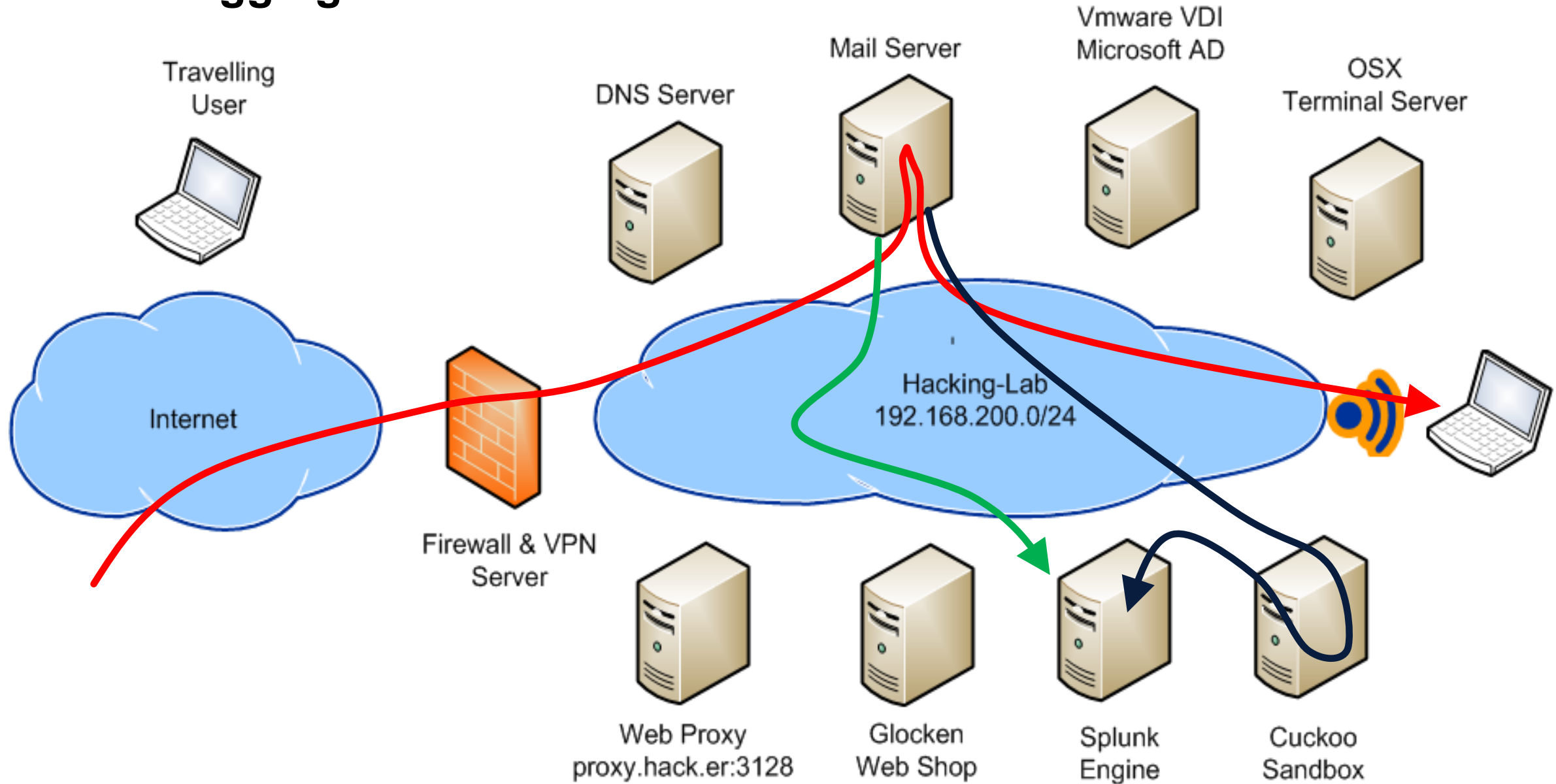
DNS Resolution



HTTP/S Logging



E-Mail Logging



Lookup Services

Lookup **Block&Black** Lists

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 | Sponsor

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)

<http://mirror1.malwaredomains.com/files/spywaredomains.zones> - complete zone

Recent Posts

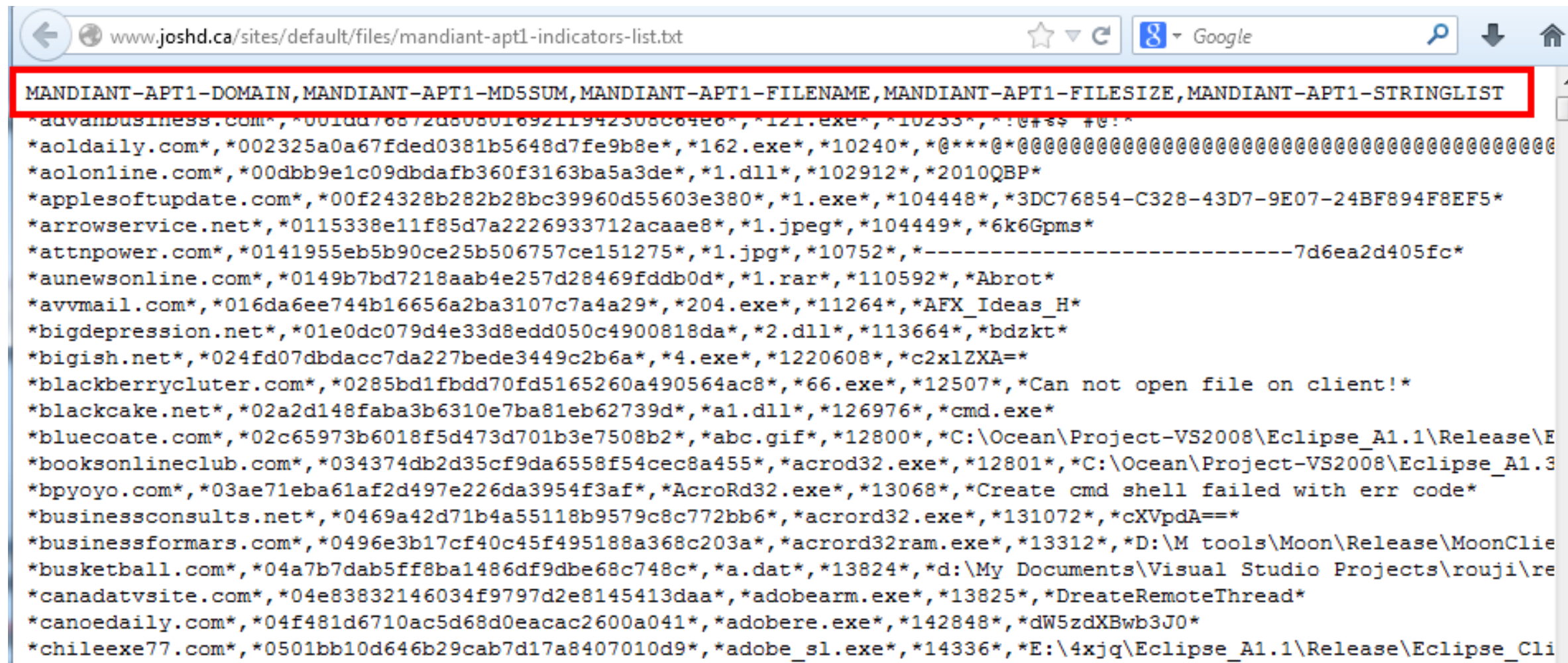
- Sinkholing, Windows DNS, Netcat, and BLAT on a Zero Dollar Budget
- iframes, kelihos, malvertising domains
- Added 400+ domains

```
| 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
```

Domains

- citadel, drive-by, Krypt,

Lookup Mandiant List



Lookup **ZEUS TRACKER** List



The screenshot shows the Zeus Tracker website at <https://zeustracker.abuse.ch>. The page has a navigation bar with links: Home | FAQ | ZeuS Blocklist | ZeuS Tracker | Submit C&C | Removals | ZTDNS | Statistic | RSS Feeds | Contact | Links. The main content area is titled "Welcome to the ZeuS Tracker" and provides a brief description of the service. It includes a list of statistics and a map showing the locations of tracked servers.

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).

Map | Satellite | Hybrid

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

Lookup **Malware Hash** List

Malware Sample Acquisition Cycle

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



Lookup **OpenIOC** List



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/>)

Lookup OpenIOC List

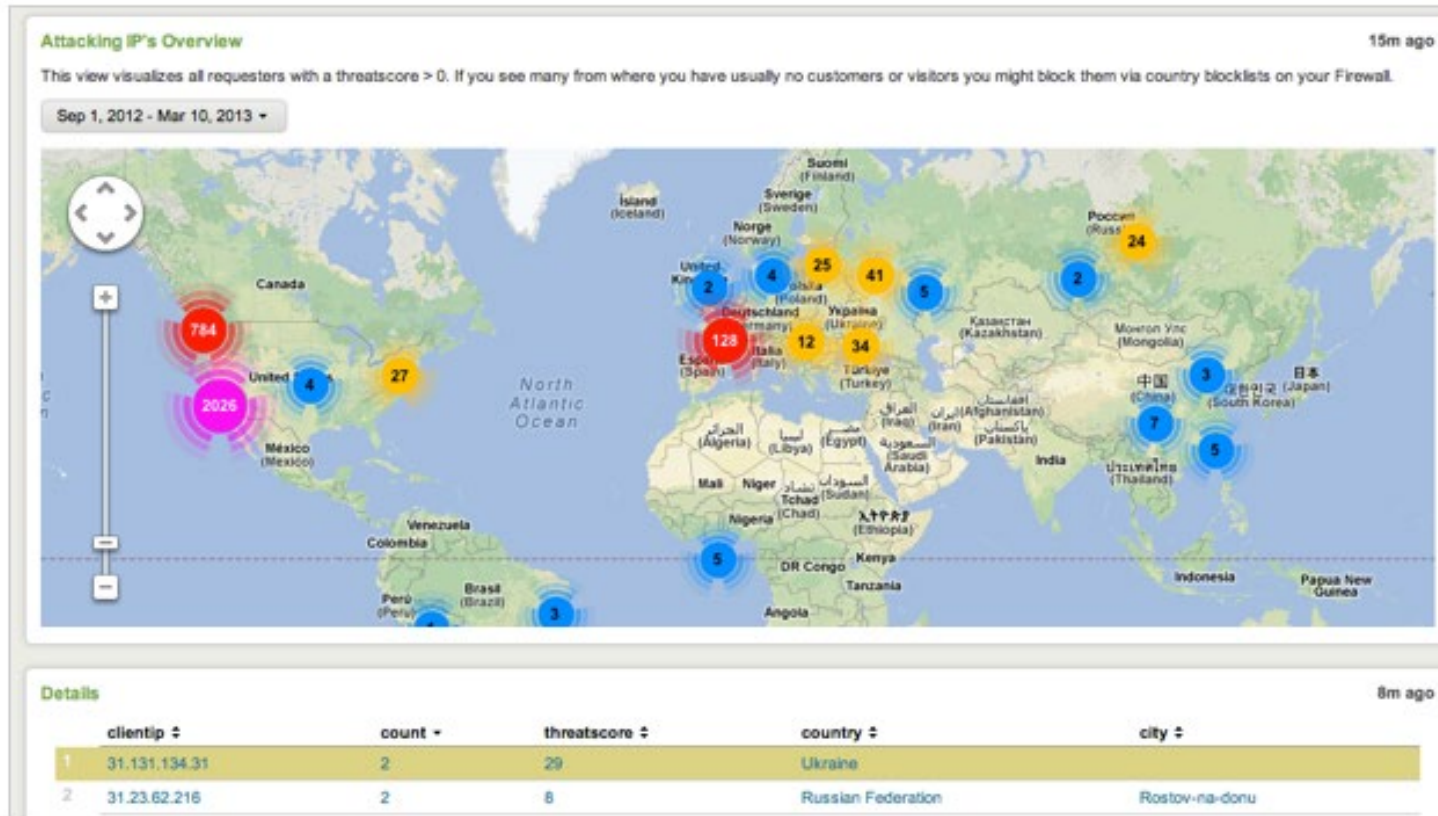


This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
-<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>
    </Indicator>
  </definition>
</ioc>
```

Lookup IP Reputation List

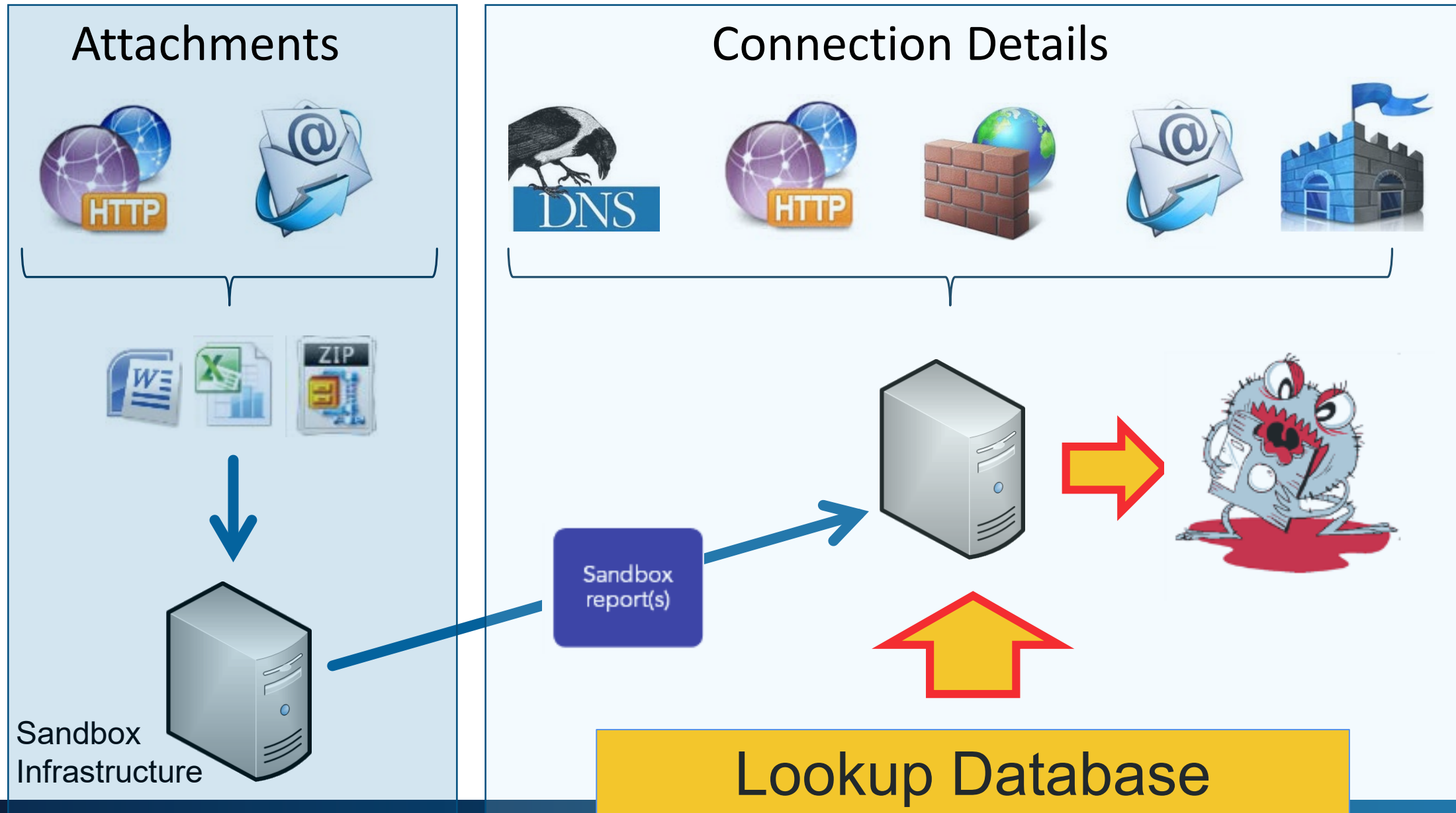
IP Reputation (Honeypot DB)



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.

APT Detection / Level 2





HSR



HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

