OST
Ostschweizer
Fachhochschule

APT

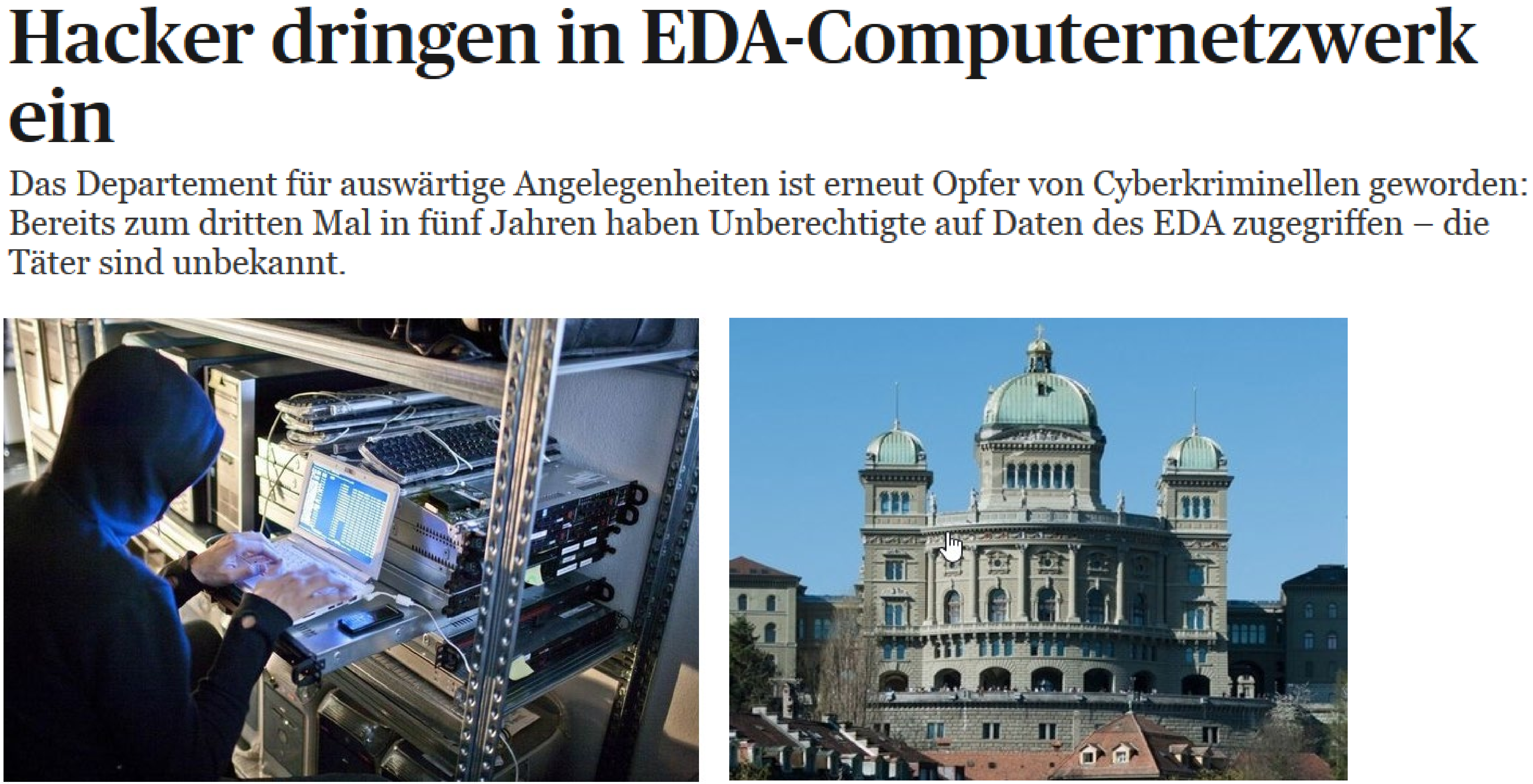
Advanced Persistent Threats

Ivan Bütler

6. Oktober 2024

Abteilung Informatik, Rapperswil

Stuxnet

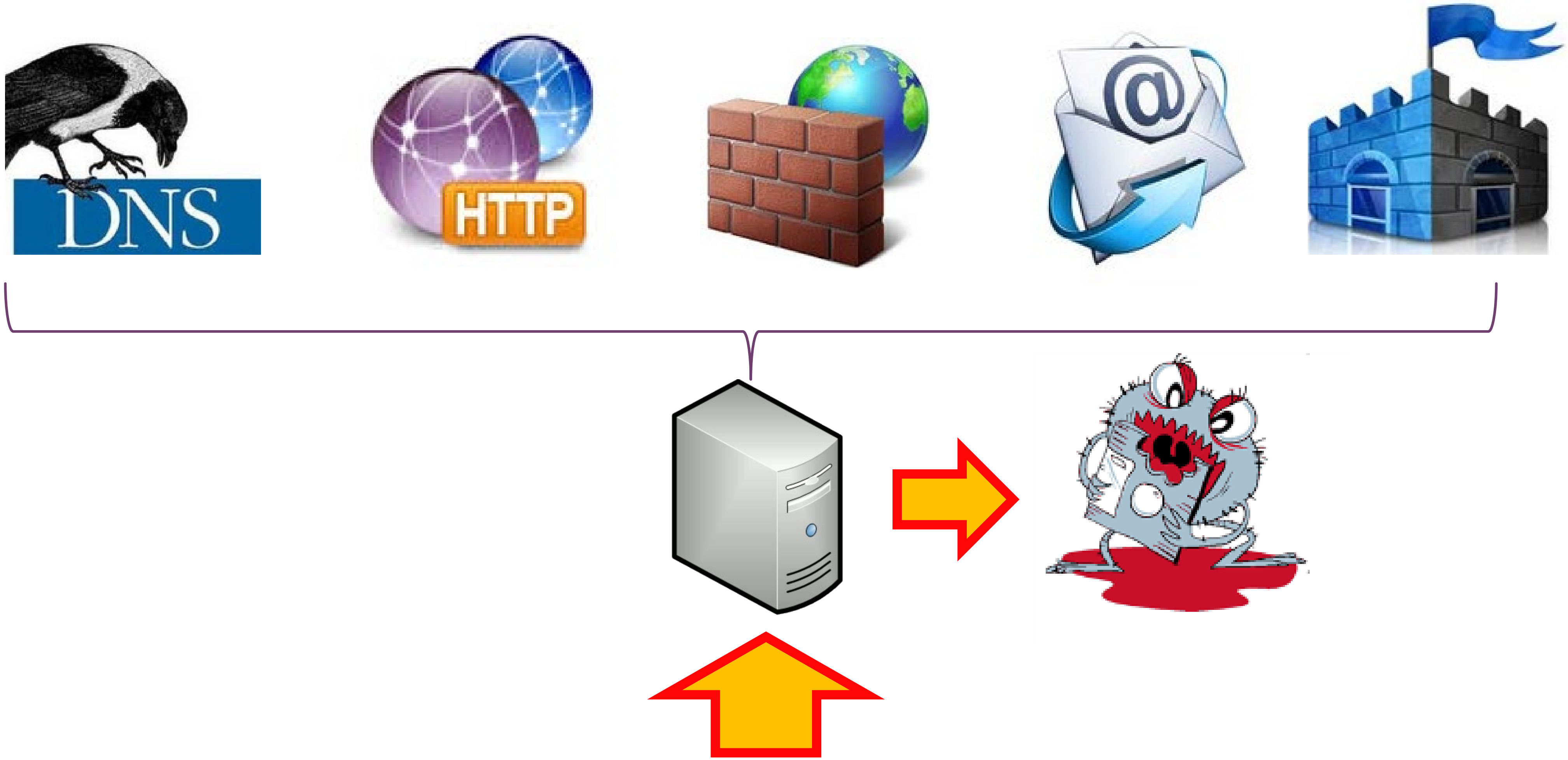


Hacker dringen in EDA-Computernetzwerk ein

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.

Monitoring & Detection

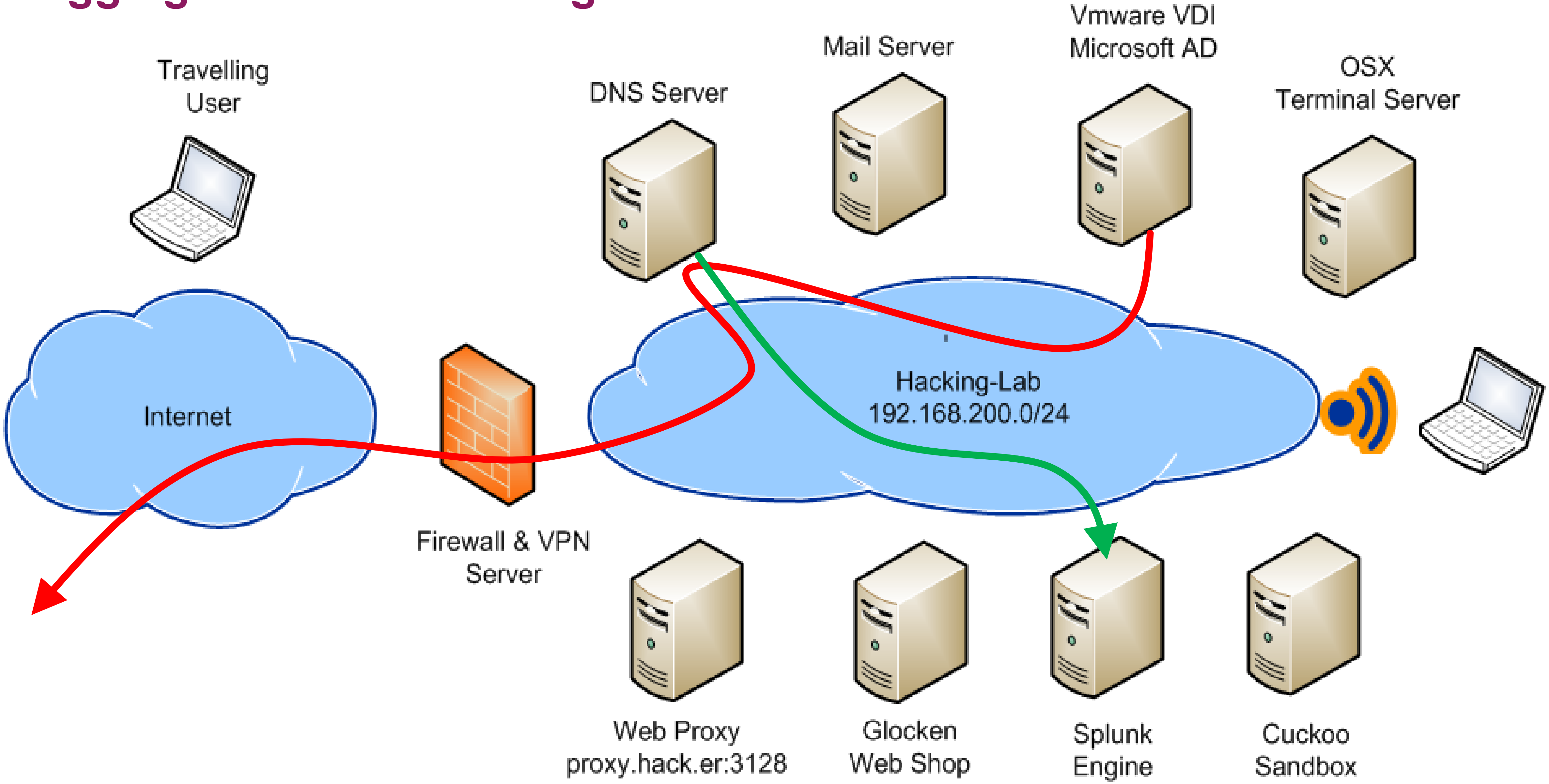
APT Detection / Level 1



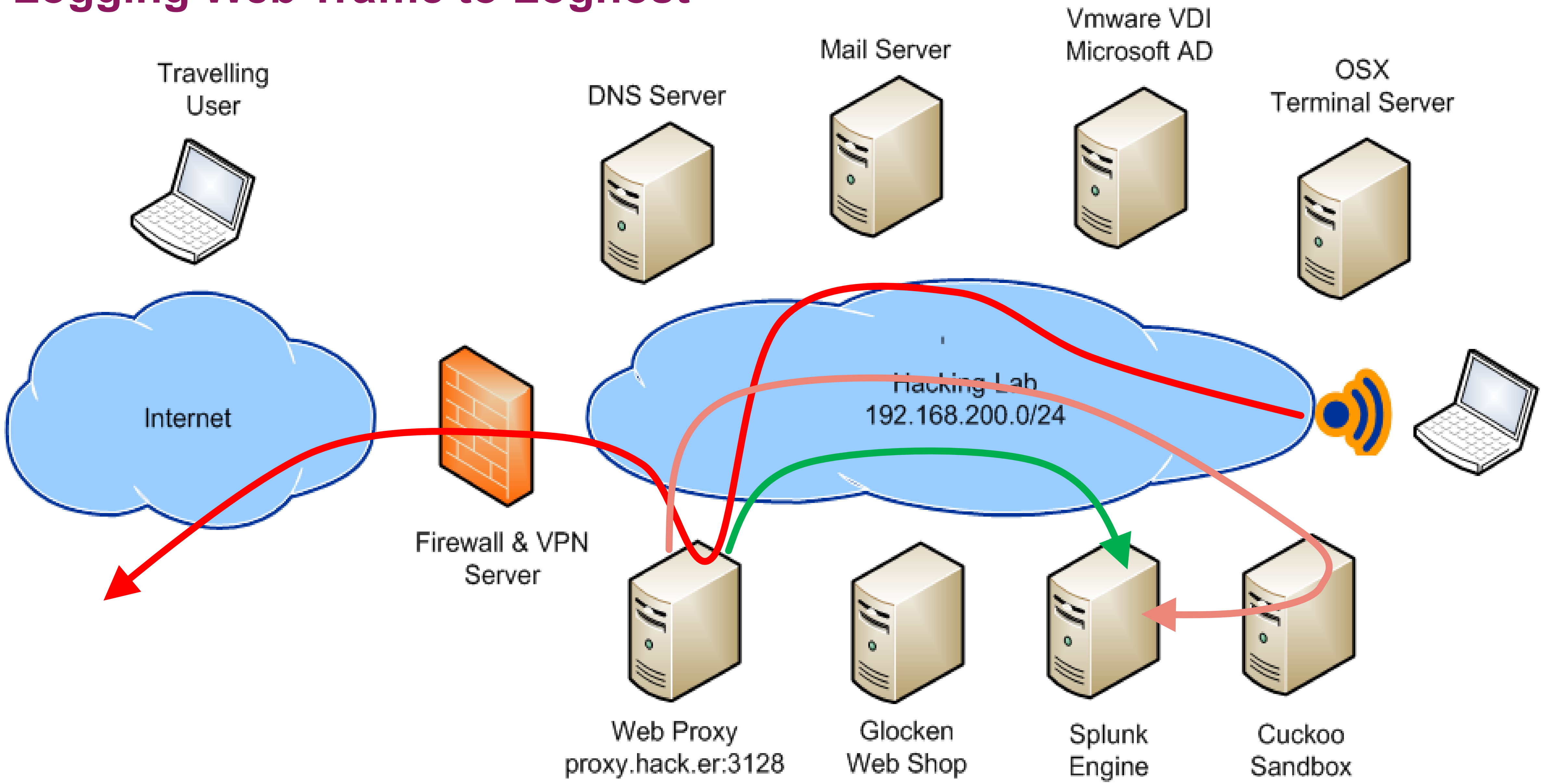
Lookup Services

Logging to Sentinel, Splunk, ElasticSearch

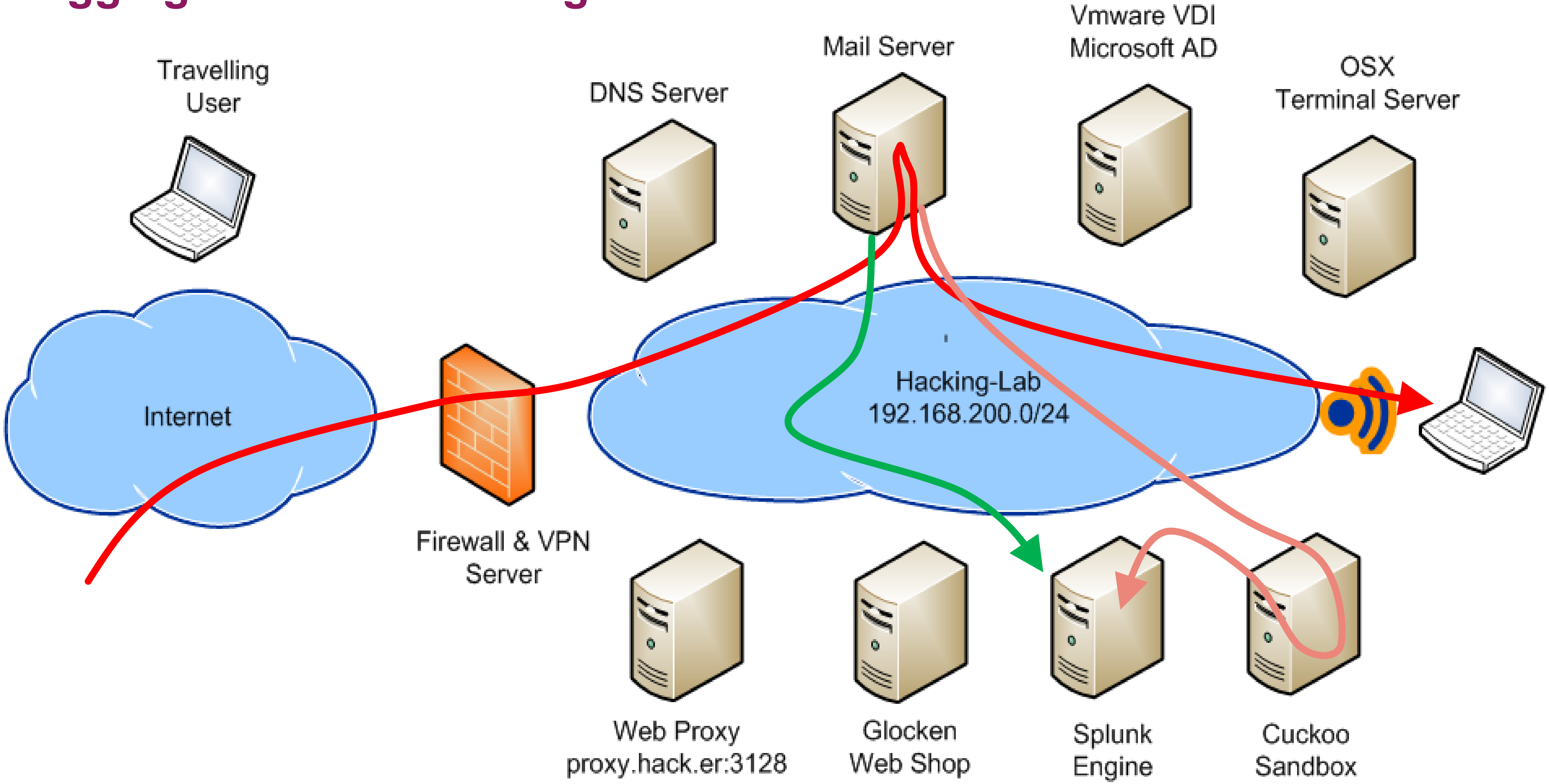
Logging DNS Traffic to Loghost



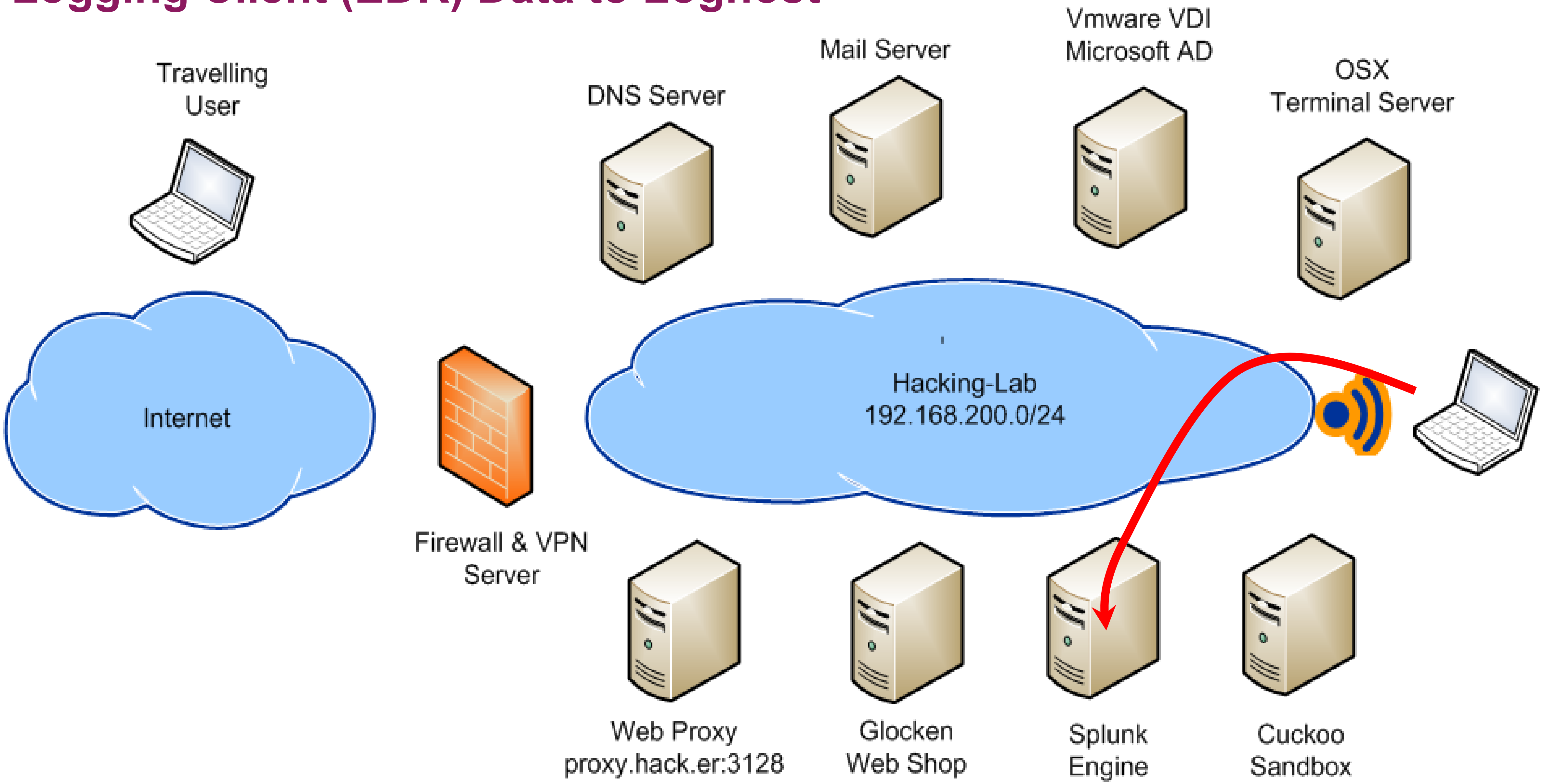
Logging Web Traffic to Loghost



Logging Mail Traffic to Loghost

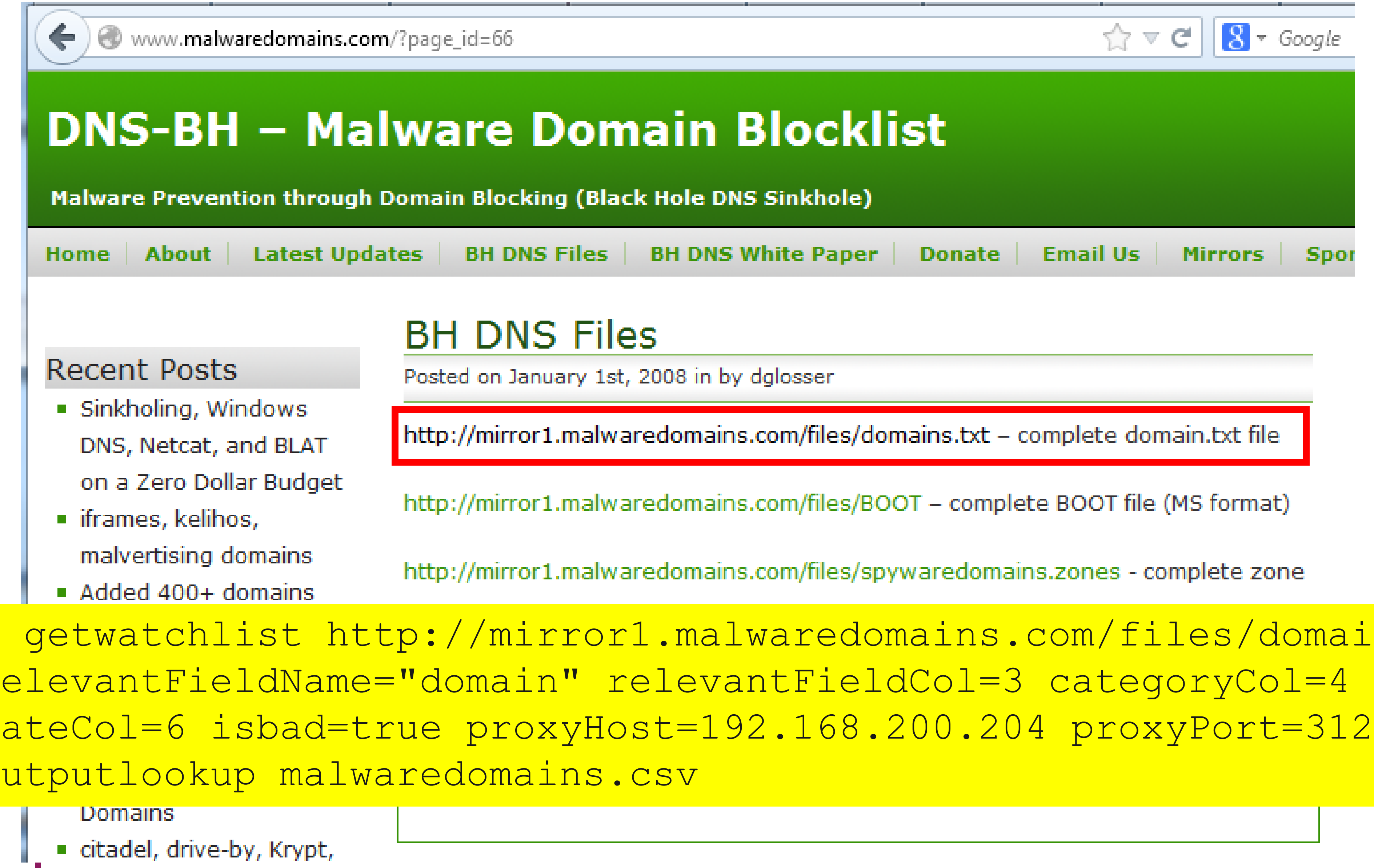


Logging Client (EDR) Data to Loghost



Lookup Services (Intelligence)
for Loghost (Sentinel, Splunk, Elasticsearch)

Lookup Block&Black Lists



www.malwaredomains.com/?page_id=66
Google

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 | Spo

Recent Posts

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

Domains

- citadel, drive-by, Krypt,

BH DNS Files

Posted on January 1st, 2008 in by dglosser

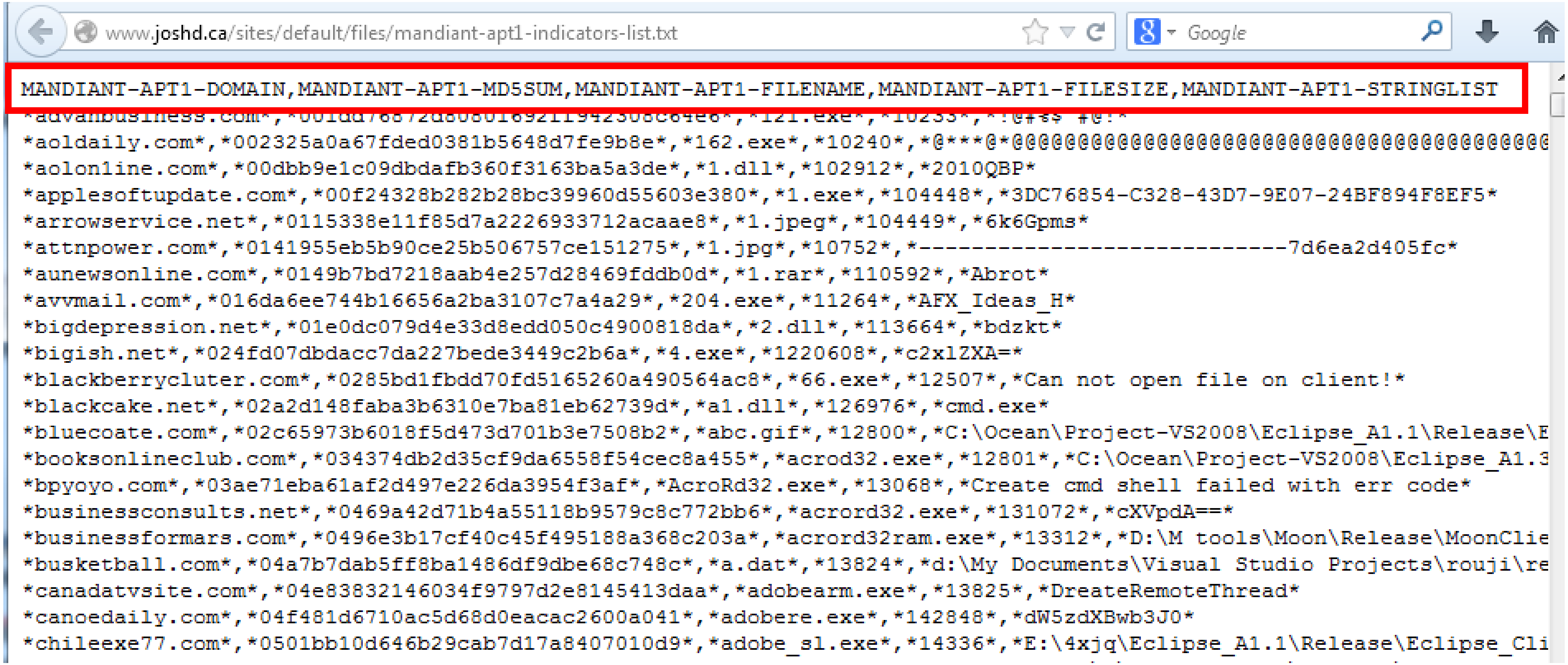
http://mirror1.malwaredomains.com/files/domains.txt – complete domain.txt file

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

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

```
| 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
```

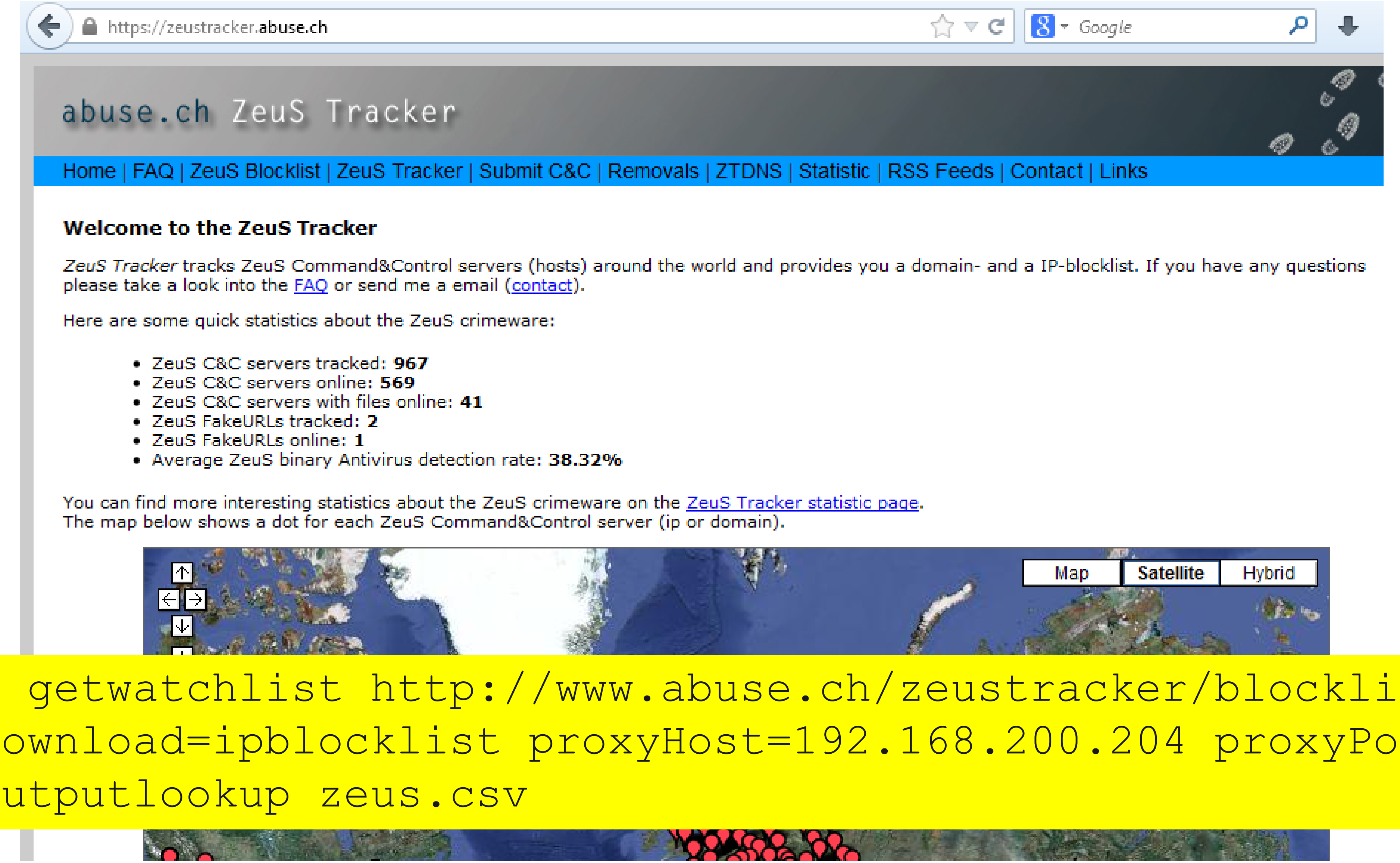
Lookup Mandiant List



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

```
MANDIANT-APT1-DOMAIN,MANDIANT-APT1-MD5SUM,MANDIANT-APT1-FILENAME,MANDIANT-APT1-FILESIZE,MANDIANT-APT1-STRINGLIST
*advanbusiness.com*,*001dd76872d80801692ff942308c64e6*,*121.exe*,*10233*,*!@#$$ #@!*
*aoldaily.com*,*002325a0a67fded0381b5648d7fe9b8e*,*162.exe*,*10240*,*@***@*@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
*aolon1ine.com*,*00dbb9e1c09dbdafb360f3163ba5a3de*,*1.dll*,*102912*,*2010QBP*
*applesoftupdate.com*,*00f24328b282b28bc39960d55603e380*,*1.exe*,*104448*,*3DC76854-C328-43D7-9E07-24BF894F8EF5*
*arrowservice.net*,*0115338e11f85d7a2226933712acaae8*,*1.jpeg*,*104449*,*6k6Gpms*
*attnpower.com*,*0141955eb5b90ce25b506757ce151275*,*1.jpg*,*10752*,*----------------------------7d6ea2d405fc*
*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 on client!*
*blackcake.net*,*02a2d148faba3b6310e7ba81eb62739d*,*a1.dll*,*126976*,*cmd.exe*
*bluecoate.com*,*02c65973b6018f5d473d701b3e7508b2*,*abc.gif*,*12800*,*C:\Ocean\Project-VS2008\Eclipse_A1.1\Release\E
*booksonlineclub.com*,*034374db2d35cf9da6558f54cec8a455*,*acrod32.exe*,*12801*,*C:\Ocean\Project-VS2008\Eclipse_A1.3
*bpyoyo.com*,*03ae71eba61af2d497e226da3954f3af*,*AcroRd32.exe*,*13068*,*Create cmd shell failed with err code*
*businessconsults.net*,*0469a42d71b4a55118b9579c8c772bb6*,*acrord32.exe*,*131072*,*cXVpdA==*
*businessformars.com*,*0496e3b17cf40c45f495188a368c203a*,*acrord32ram.exe*,*13312*,*D:\M tools\Moon\Release\MoonClie
*busketball.com*,*04a7b7dab5ff8ba1486df9dbe68c748c*,*a.dat*,*13824*,*d:\My Documents\Visual Studio Projects\rouji\re
*canadatvsite.com*,*04e83832146034f9797d2e8145413daa*,*adobearm.exe*,*13825*,*DreateRemoteThread*
*canoedaily.com*,*04f481d6710ac5d68d0eacac2600a041*,*adobere.exe*,*142848*,*dW5zdXBwb3J0*
*chileexe77.com*,*0501bb10d646b29cab7d17a8407010d9*,*adobe_sl.exe*,*14336*,*E:\4xjq\Eclipse_A1.1\Release\Eclipse_Cli
```

Lookup ZEUS TRACKER List



https://zeustracker.abuse.ch
Google
abuse.ch ZeuS Tracker
Home | FAQ | ZeuS Blocklist | ZeuS Tracker | Submit C&C | Removals | ZTDNS | Statistic | RSS Feeds | Contact | Links
Map
Satellite
Hybrid

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%**

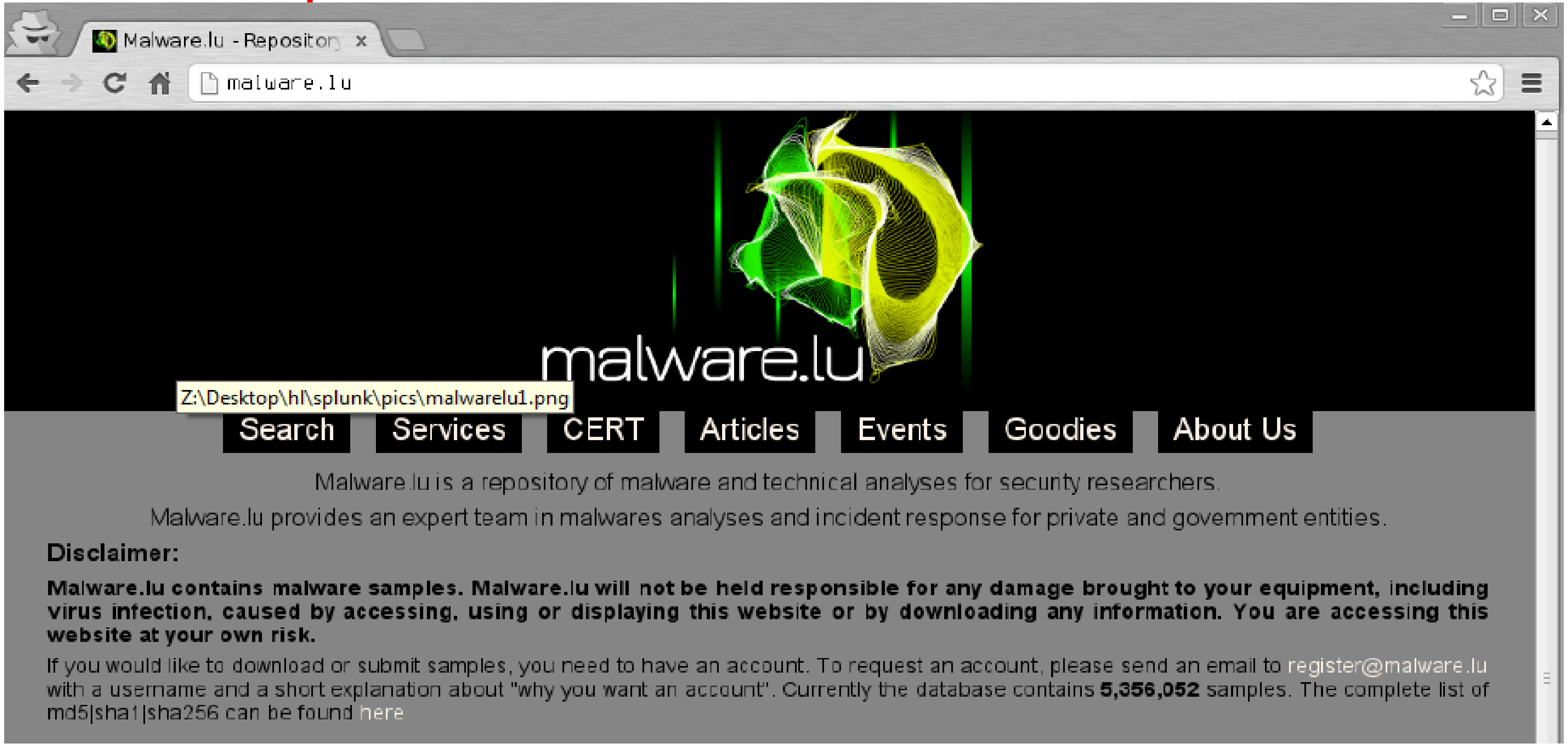
You can find more interesting statistics about the ZeuS crimeware on the ZeuS Tracker statistic page.
The map below shows a dot for each ZeuS Command&Control server (ip or domain).

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

Lookup **Malware Hash** List

Malware Sample Acquisition Cycle

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



Malware.lu is a repository of malware and technical analyses for security researchers.

Malware.lu provides an expert team in malwares analyses and incident response for private and government entities.

Disclaimer:

Malware.lu contains malware samples. Malware.lu will not be held responsible for any damage brought to your equipment, including virus infection, caused by accessing, using or displaying this website or by downloading any information. You are accessing this website at your own risk.

If you would like to download or submit samples, you need to have an account. To request an account, please send an email to register@malware.lu with a username and a short explanation about "why you want an account". Currently the database contains **5,356,052** samples. The complete list of md5|sha1|sha256 can be found here

Lookup OpenIOC List

OpenIOC

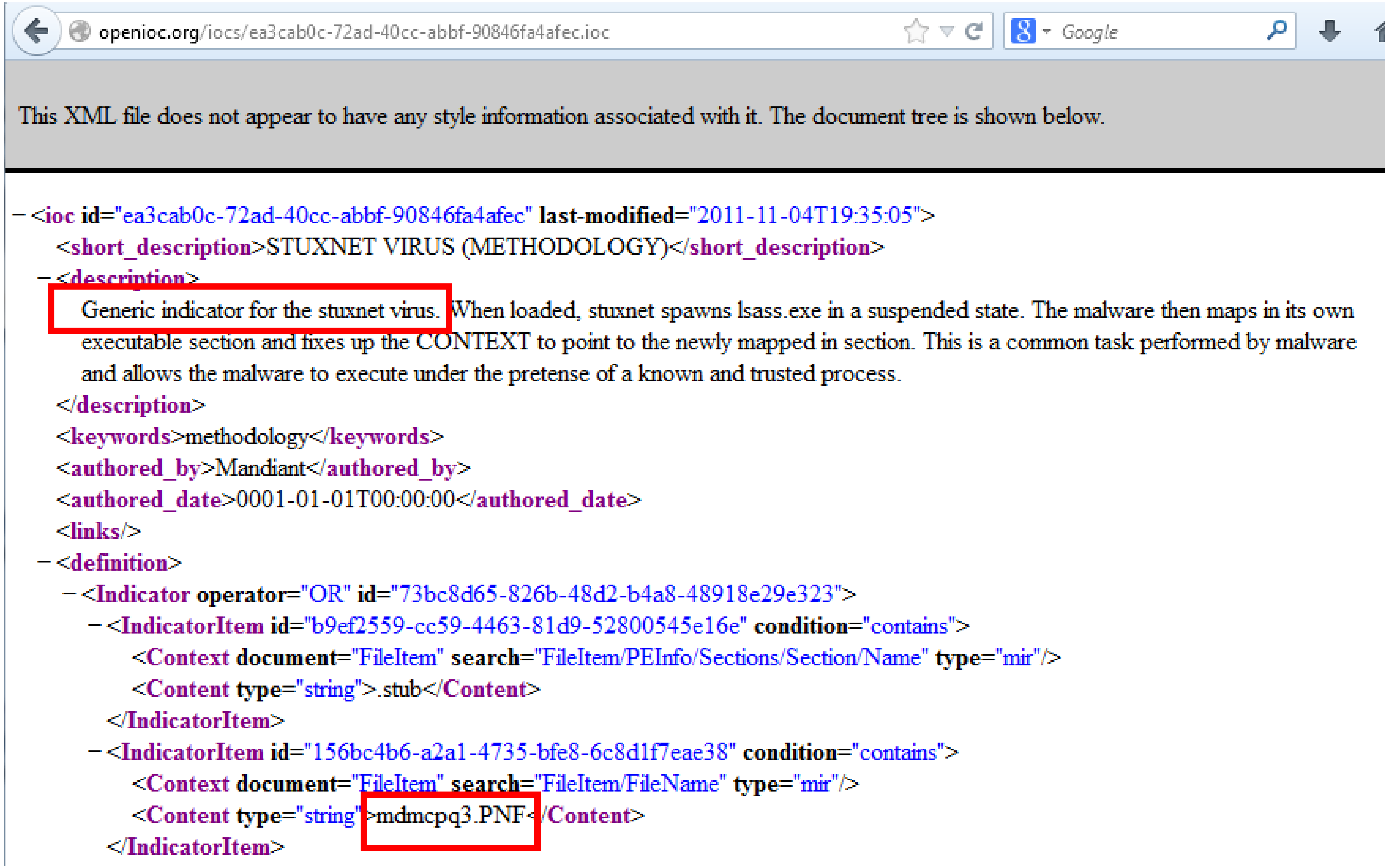
An Open Framework for Sharing Threat Intelligence

Sophisticated Threats Require Sophisticated Indicators

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



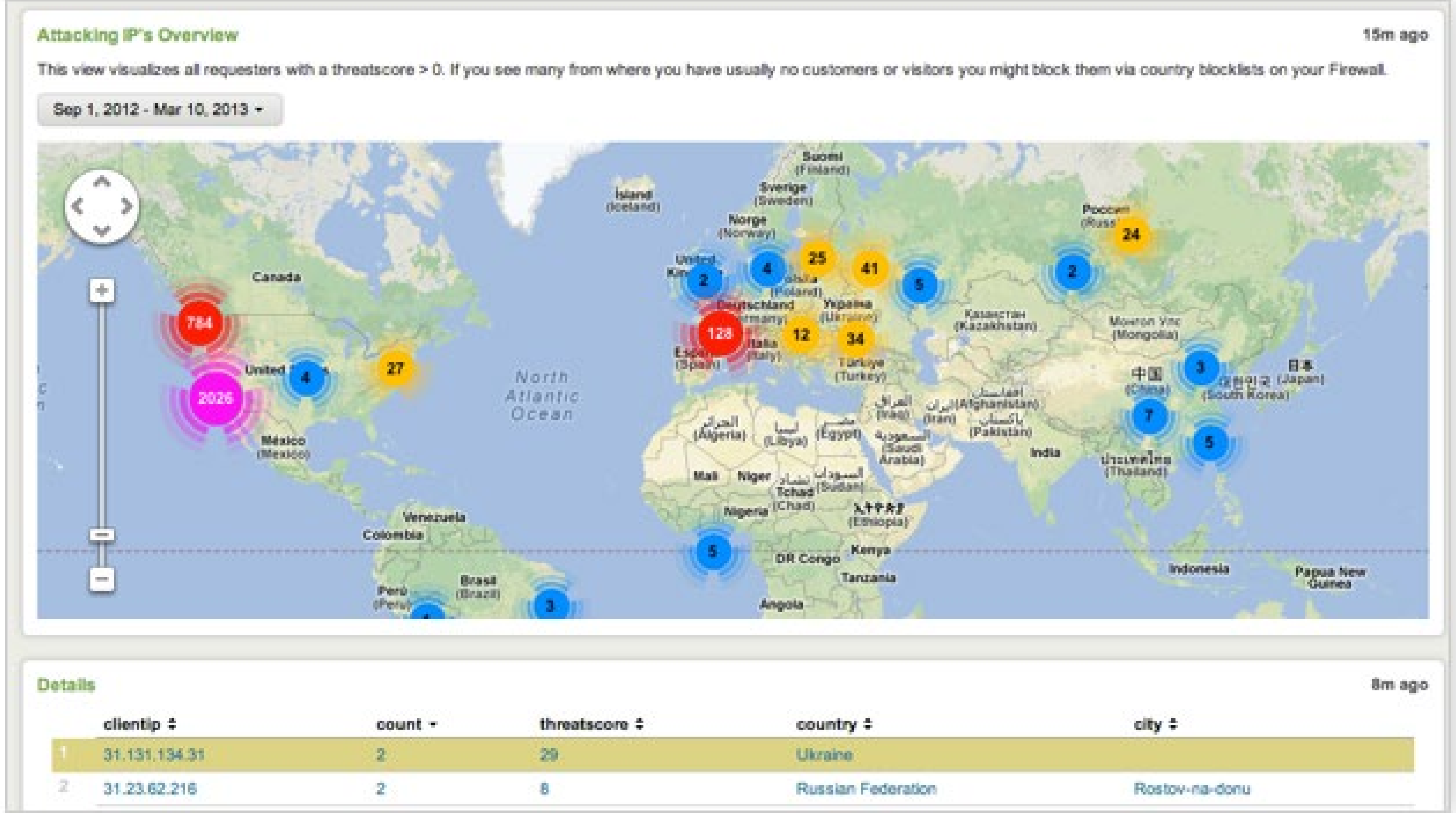
openioc.org/iocs/ea3cab0c-72ad-40cc-abbf-90846fa4afec.ioc

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>
```

Lookup IP Reputation List

IP Reputation (Honeypot DB)



Attacking IP's Overview

15m ago

This view visualizes all requesters with a threatscore > 0. If you see many from where you have usually no customers or visitors you might block them via country blocklists on your Firewall.

Sep 1, 2012 - Mar 10, 2013 ▾

Details

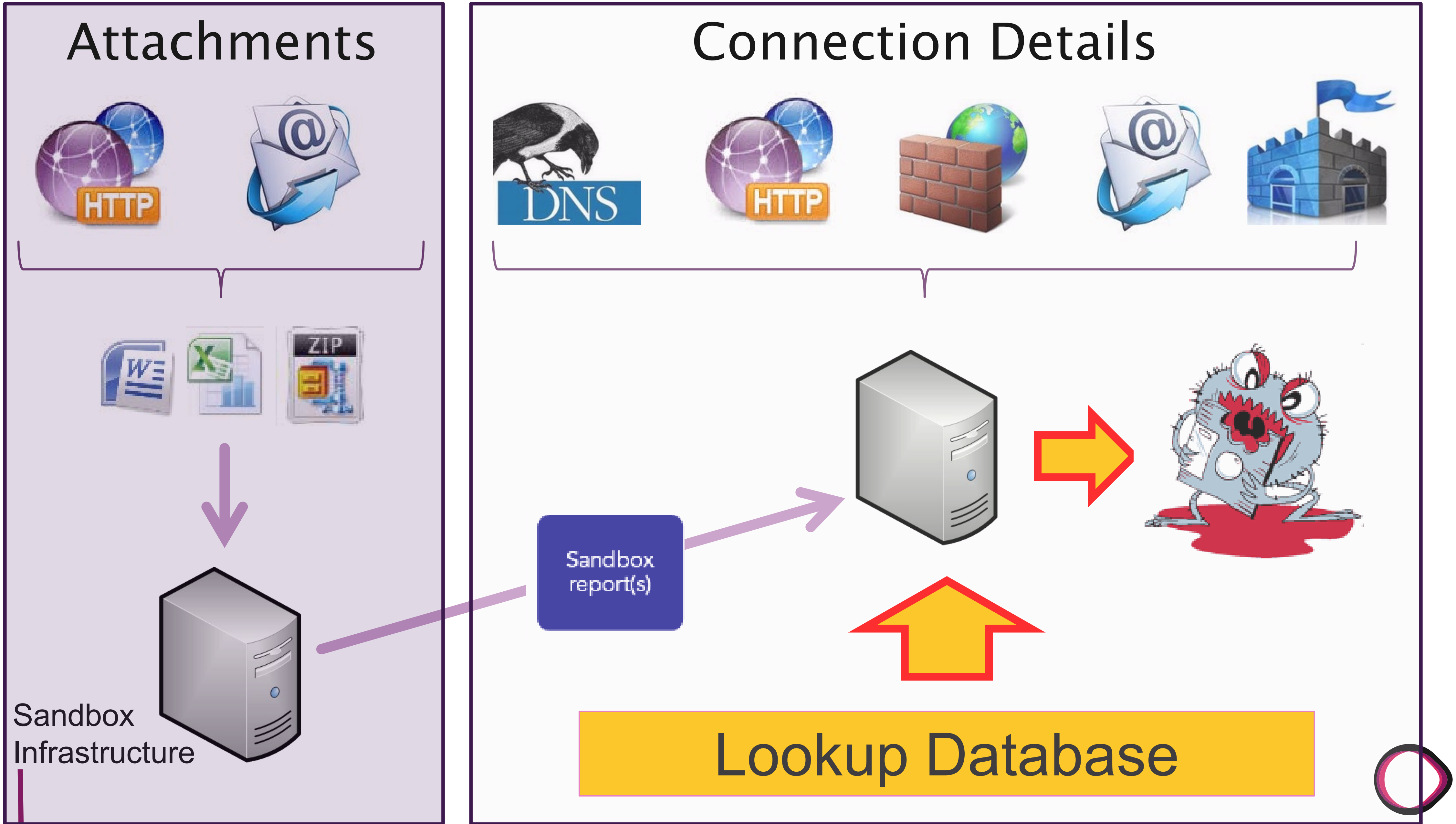
8m ago

	clientip ⇕	count ▾	threatscore ⇕	country ⇕	city ⇕
1	31.131.134.31	2	29	Ukraine	
2	31.23.62.216	2	8	Russian Federation	Rostov-na-donu

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



Attachments

Connection Details

Sandbox report(s)

Sandbox Infrastructure

Lookup Database