# Case 2. Intrusion analysis

Files obtained from Malware Traffic Analysis (brad@malware\_traffic) have been legitimately exploited in this task. The files have been changed to the appropriate format for the task.

The task has been prepared in such a way that it can be done in alternative ways, depending on the software/possibilities/enthusiasm/basic information in use:

* If you are able to use [SecurityOnion](https://securityonion.net/) or another IDS system, you can and should take advantage of them (note January 2019).
* If you only use the Wireshark program, then do the task by viewing the images related to SecurityOnion and doing the rest of the analysis with Wireshark itself.
* Or do something of your own accord, but be sure to let it know when you return.

# Task

**The task is to analyse the network penetration that led to a data breach.**

1. *About 70% of data breaches originate from user actions - Jan Mickos CGI*

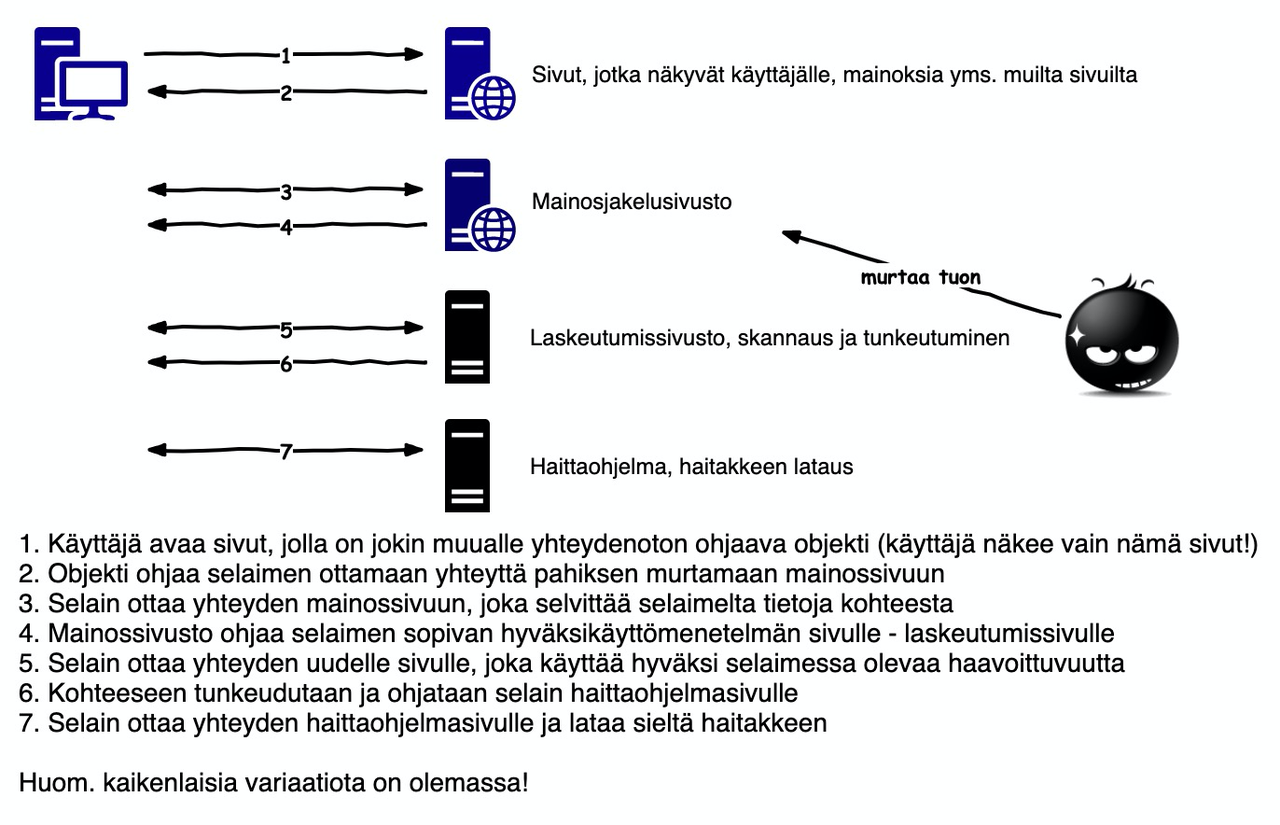
Go through the scenario and materials below. **Answer the questions in** the task and restore your answer by saving it to the recovery folder and mark the task as Case2 suart. Answers come from supporting by taking screenshots eg. From wireshark's suitable found data. The assignment can be done in small groups, but everyone must submit the submission and markup themselves.

## Basic information (google)

1. Briefly explain what theExploit Kit is?T
2. What programmatic weaknesses (which programs) do Exploit Kits usually hit their nails on? Can you find a few?
3. What have been the most famous Exploit Kins in recent years? Find a couple of examples and links to them in response.
4. What could be a good translation for Exploit Kit?

## Analysis

Below is a picture with a diagram of how one of the Exploit Kit works. Take a look at the image and then analyze the data provided for the scenario. Answer the rest of the questions.



You can download the required pcap file below. **The file contains malware** (that is, there inside the pcap file). It is not dangerous to download them in pcap file format, but if you save them from there as Export Objects, then **do notrun them on the machine in any name**!

It may also be that some antivirus program is blocking the download of the file - congratulations, you have really accurate antivirus software at your disposal!

<https://www.dropbox.com/s/rd5yzyt59pwqxa6/case2.pcap?dl=0>

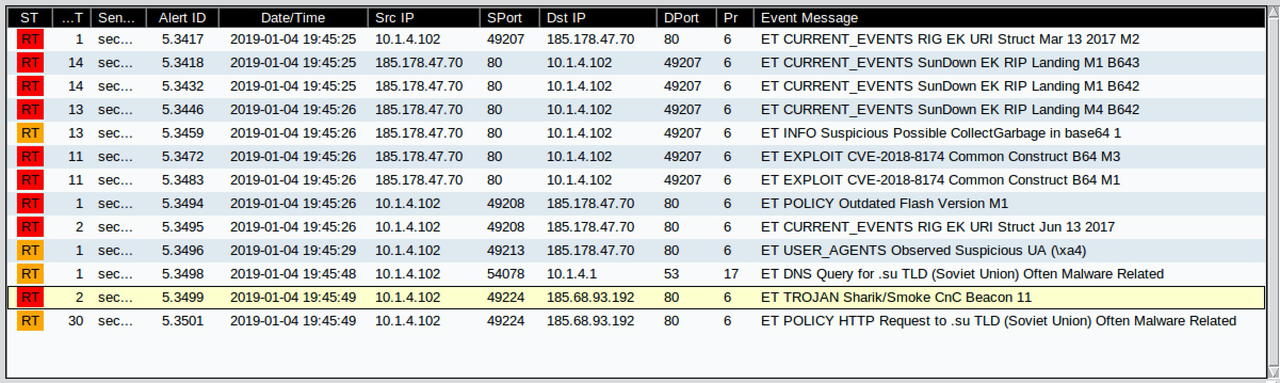
After installation and deployment, SecurityOnion allows you to run the pcap filewith the command so-import-pcap. In the link below, more information:

https://securityonion.readthedocs.io/en/latest/so-import-pcap.html

With Wireshark, you can open the downloaded pcap file normally. In order to find out the country codes related to the task, Wiresharkii's mustinstall location information, e.g. MaxMind Geolite2 (free but requires registration). Installation is carried out according to the following instruction: <https://wiki.wireshark.org/HowToUseGeoIP>

## Scenario

One day, HaiTek Ltd's intrusion detection system looks like this (note the image of the Squirt alarm program):



## Questions

Find answers to questions by doing an analysis using Wireshark (or another method of your choice ):

1. Should you be worried about HaiTek? Why/why not?
2. When did the attack take place and how long did it last in total?
3. What is the Exploit Kit in the scenario (hint: it's not a sunset even though it might seem like it)?
4. Taking into account the details of the scenario, find out the previous picture of how the Exploit Kit works:
   1. What is the ip address of the target?
   2. What is the IP address of the page that appears in the user's browser? What about the URL?
   3. Mage is the ip address and domain name of the ad delivery site?
   4. What is the IP address of my landing page?
   5. What is the IP address of a malware page?
5. Which country (most likely) has the legal and illegal servers in the scenario? (need local data for this)
6. What does the CnC (= C2) detected by the IDS system (pictured above) mean?
7. What traffic between devices has been encrypted? Could there be a reason for this?
8. Are there any other IP addresses associated with the scenario? What and what devices are they?
9. What was the object that redirected the browser to a hacked advertising site?
10. Which component was vulnerable on the target device (browser)?
11. What malware was downloaded? What does it possibly do (google)?

Next, find out if the files downloaded to the target have been identifiedand malware. Three larger files were uploaded to the destination (they can be separated by Wireshark from the pcap file if desired). **Don't run those files on your machine**! However, it is not necessary to separate them into files, but the corresponding information is givenbelow.

Virustotal is a service where you can check if a file is malicious (whether it is recognized as malicious). It can be done by uploading a file to the service, or even more conveniently - by creating a sha256 hash from the file and retrieving information based on it.

https://www.virustotal.com/gui/home/search

You can test the process with any of your own files. First, create a SHA256 hash from the file, and then try retrieving data from the Virustotal service.

https://emn178.github.io/online-tools/sha256\_checksum.html

One of the files filu2 and filu3 is malicious. If you don't want to download files to your computer (disconnect them from the pcap file), then below are their SHA256 hashes.

Filu2 sealant

d7bb1f853e55fa7f80f04bf1cd4b20129843a6821881dff0bf860dbcfbf33bac

Filu3 sealant

134c94abf9760683c74d4ebd54a06ae0db85320d77f97490986e4fdfea8c04cA

1. Use thehashes given above sha256 hash values and test the virustotal service for whether the files are known to be malicious or not? Does a large Finnish antivirus software recognize it as harmful?
2. What vulnerability (CVE identifier) was the malware related to? What is a CVE ID?
3. Describe in your own words what happened so that it would be understood by your own father/mother/grandma/papa/spouse/boss etc. (= someone who is not very familiar with security issues and is not really interested in computer terminology)
4. Which of the followingwould most likely have prevented the intrusion (you can justify if you want:
   1. better user awareness
   2. antivirus (hint: the other filu was malware)
   3. firewall
   4. Up-to-date updates

END