|  |
| --- |
| OTO Oefening |
|  |
| Technical exercise for CERTs and other interested parties |
|  |
|  |
|  |

# Exercise Goals

This exercise concerns a digital forensic investigation, as frequently carried out by SOCs/CERTs, based on a network forensic capture in PCAP format. It is based on a NetResec training (<http://www.netresec.com/?page=PcapFiles>). The challenge combines the knowledge and skills that are (among other) part of the GIAC Network Forensic Analyst certification.

The ‘win condition’ of this exercise is a comprehensive description of the historical events through analysis of the PCAP.

# Requirements

* A work room
* USB-keys for handing out the PCAP
* Time: 1-2 hours – max. 15 minutes explanation and evaluation
* Attendees:
  + Laptop suitable for digital forensic investigation of network-captures with Wireshark, e.g.: DEFT, SIFT, Kali

## Structure

* One master of ceremonies covering both guiding of content and process
* Attendees fulfil their usual roles

## Rules

* Cooperation should be zero or limited, in order to prevent:
  + Answers from being shared
  + Few people actually working on the exercise

# Description

In a fictitious company, a network administrator has noticed unusual traffic flowing over the network edge routers to the outside world, coming from one of the networked systems. He has captured this traffic and has requested the company’s Security Team, to investigate the case. After the Security Team has acquired the PCAP in a forensically sound way, they have asked you for your technical expertise oin analyzing network traffic and have handed you the PCAP with the following MD5 hash:

**1f8ab1f2b261371f48f708574b8fe5db** **vm-2.pcap**

The Security Team has established through interviews that the user of the system, John Smith, was the only one person to ever use that system. They would like you to investigate and answer the following questions, if possible:

1. **What was the system doing in this PCAP?**
2. **Has the user done anything that would be out of line with company policies?** For the sake of the exercise, assume common and basic guidelines such as using the equipment for work purposes only, due diligence in visiting websites, etc.
3. **Can anything be said of the integrity of the system?**
4. **Do you, as a digital forensics expert, recommend any follow-up investigation(s)?**

## Answers

The PCAP should be loaded into Wireshark.

Traces of suspicious network traffic:

* Searching through Google for software (born to help)
* Redirection to **kritikaa.ilanes.com**
* Malware gets downloaded
* Malware attempts to C2 to **intohave.com / 88.216.164.117**
* Malware uses URLs with cookies (**88.216.164.117/entries & .../videos/forumdisplay.php**)

Extraction of the **google\_born\_help.exe** binary with VirusTotal etc. reveals:

* PE32 executable, packed
* W32/Kryptik.KO!tr / Suspicious.Cloud.5

Unpacked file is recognized as a Trojan by pretty much all AV solutions. In the analysis sandboxes, the **88.216.164.77** addresses/URLs also show up, as does another **77.79.11.29** IP (but with the same URL).

Cleary, the user has:

* Searched for a term (**born to help**). This can be deduced from the Google CH requests, where character by character is visible in the exchange with the server.
* Downloaded a malicious file after being redirected, probably by a malicious search result
* Run that file and compromised the integrity of his system with a trojan

After the compromise, the infected system is shown to communicate over SMB. At the very least, it would be advisable to investigate further if other systems on the network have been accessed by the compromised system.