|  |
| --- |
| **Objective – Questions to be answered** |
|  |

|  |
| --- |
| **Executive summary** |
|  |

**Analyst information**

|  |  |  |
| --- | --- | --- |
| **Name:** | **E-mail Address:** | **Phone Number:** |
|  |  |  |

**Capture file information**Basic information from pcap file/files  
Run capinfo with the following command - capinfos -T -m -Q <Path to capture file>

|  |
| --- |
| **Capinfo information** |
|  |

**Host names with IP-addresses and MAC addresses.**Only for identified known hosts.

|  |  |  |
| --- | --- | --- |
| **Host name / information** | **IP adresse** | **MAC adresse** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**OS information type and MAC vendor**Information about the hosts

|  |  |  |
| --- | --- | --- |
| **OS information** | **TTL Information** | **MAC vendor** |
|  |  |  |

**Protocol hierarchy information from capture file / files**Traffic types listed in the pcap file ore files

|  |
| --- |
| **Protocol hierarchy information** |
|  |

**Triggered IDS events on replay:**Triggered event from IDS replay of the capture file.

|  |  |  |
| --- | --- | --- |
| **IDS rule MSG** | **SID Number** | **Number of alerts** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Extracted Evil files ore related files.**Marked red is missing detection - Marked Green has detection

|  |  |  |  |
| --- | --- | --- | --- |
| **File name** | **MD5** | **AV detection rate** | **Artifact number** |
|  |  |  |  |
|  |  |  |  |

**Identified evil domains with A, AAAA ore MX record IP address.**IP address information from record types

|  |  |  |  |
| --- | --- | --- | --- |
| **Domains** | **Record type** | **Artifact number** | |
|  |  | |  |
|  |  | |  |

**Virustotal Information**Identified information from Virustotal about IP addresses, domains ore Anti-virus.

|  |  |
| --- | --- |
| **Virustotal** | **Artifact number** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**Identified evil IP’s and ports numbers**Type of protocol, IP’s and port numbers.

|  |  |  |  |
| --- | --- | --- | --- |
| **Protocol** | **IP** | **Port numbers** | **Artifact number** |
|  |  |  |  |
|  |  |  |  |

**AV detection names of malware. Only names by used AV vendor for Costumer.**Make sure that the costumer is able to detect the malware.

|  |  |  |
| --- | --- | --- |
| **AV Detection name** | **AV used** | **Artifact number** |
|  |  |  |

**Exploit kit information**  
If possible identify the Exploit / Exploit kit used during the attack like Angler, Magnitude, RIG, or Nuclear

|  |  |
| --- | --- |
| **Exploit /Exploit Kit used in the attack** | **Vulnerability** |
|  |  |

**Time line**Time line for relevant events

|  |  |  |  |
| --- | --- | --- | --- |
| **Time** | **Source** | **Destination** | **What happend** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Description.**Explanation of Events. Add screen shots.

|  |
| --- |
|  |

**Mitigating measures.**Describe recommended mitigation actions.

|  |
| --- |
|  |

**Created new IDS / IPS signatures**This is SNORT IDS signatures to help identify related attacks ore malware, there can be used in the current indecent.

|  |
| --- |
| **IDS / IPS Rule** |
|  |
|  |
|  |