# **Incident Ticket Template**

**Use the following as a template for generating a ticket to track activity related to a security incident.**

## **Detection (network events, host events, external report):**

### 

### **Initial detection/IoC:**

|  |
| --- |
| **2020-06-06 22:00:50 216.154.220.53:80 -> 10.0.0.12:50134**  **(ET POLICY PE EXE or DLL Windows file download HTTP)** |

### 

### **Additional indicators (incl. network traffic, host logs):**

|  |
| --- |
| **2020-06-06 22:23:03 88.214.26.53:42069 -> 172.31.83.122:5432**  **(ET SCAN Suspicious inbound to PostgreSQL)**  **The upcoming entries were discovered:**  **﻿4 0.034845 10.0.0.12 216.154.220.53 HTTP 433 GET /malware/fnpufu.exe HTTP/1.1**  **10.0.0.12 -> 190.6.193.152 POST /w00n19tnKeyeyjNO HTTP/1.1**  **Content-Type: application/x-www-form-urelencoded**  **190.6.193.152 -> 10.0.0.12 HTTP/1.1 (text/html)**  **10.0.0.12 -> 216.154.220:53 HTTP 433 GET /malware/fnpufu.exe HTTP/1.1**  **216.154.220:53 is identified as a server in the USA.**  **The detected file fnpufu.exe was extracted and the SHA-256 hash: 006d5fda899149df4cc5d6d1b1ae52e9fcc4ade7541c1dd4391e0429d843b4d5, VirusTotal's website was searched, and Trojan Emotet AFS is the name of the virus found there.** |

### 

### **False Positives (Note: in the real world, false positives are not logged in an incident ticket. This section is unique to our project)**

### **It was determined to be a false positive after deeper inspection and a viral total check utilizing the hash of each file produced a clean result.**

|  |
| --- |
| **(Note: in the real world, false positives are not logged in an incident ticket. This section is unique to our project)**  **2020-06-06 21:57:09 192.168.1.56:36982 -> 34.239.152.87:80**  **2020-06-06 17:02:09 10.0.0.12:51026 -> 168.63.129.16:53** |

## **Containment:**

|  |
| --- |
| **Contacted Network Operations Center (616-555-4662) and asked the on-call staff to disable the network access to desktop, data center.**  **Rest the passwords and called the help desk (616-555-4357) to assist with the task.** |

## 

## **Analysis (other compromised hosts, lateral movement, data exfiltration, etc.):**

|  |
| --- |
| **If there is a malware infection that occurred, the steps to prevent it are:**   1. **Document the path to infection.** 2. **Check for other infected hosts** 3. **Document any lateral movement** 4. **Document signs of infiltration** |

## **Recovery:**

|  |
| --- |
| **I believe that to recover it is best to have an incident response plan, so that the plan will help**  **Determine what is the threat. How to prevent the threat, and what you can do to improve .**  **To recover, I believe that you should :**   1. **Don’t Panic and Remain calm** 2. **Follow established processes** 3. **Confirm the initial analysis.** 4. **Collect additional data** 5. **Document all your steps** 6. **Call in additional resources if needed.** |

## **Post-incident recommendations:**

|  |
| --- |
| **For Post-Incident recommendations,**  **I would say Documenting Evidence, develop a plan on what should be improved**  **Or what you can do to mitigate the threat .** |