# **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-Jun-06 22:00:50 216.154.220.53:80 --> 10.0.0.12:50134 |

### 

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

|  |
| --- |
| 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 Content-Type: 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.  I extracted the detected file, calculated the file’s SHA-256 as: 006d5fda899149df4cc5d6d1b1ae52e9fcc4ade7541c1dd4391e0429d843b4d5. Then I checked the hash value against VirusTotal and determined the malware as aTrojan Emotet AFS. |

### 

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

|  |
| --- |
| 2020-Jun-06 21:57:09 192.168.1.56:36982 --> 34.239.152.87:80  2020-Jun-06 21:57:20 192.168.1.56:36984 --> 34.239.152.87:80  2020-Jun-06 21:57:33 192.168.1.56:36986 --> 34.239.152.87:80  2020-Jun-06 21:57:52 192.168.1.56:36988 --> 34.239.152.87:80  2020-Jun-06 21:58:05 192.168.1.56:36990 --> 34.239.152.87:80  2020-Jun-06 21:58:20 192.168.1.56:36992 --> 34.239.152.87:80  2020-Jun-06 21:59:17 172.31.90.209:35997 --> 172.31.0.2:53 |

## **Containment:**

|  |
| --- |
| We have identified an infected assets(s) and want to physically remove them from the network following the organization’s incident response playbook.   * We have secured copies of the malicious code (malware), affected systems and any identified artefacts for further investigation. * The Network Operations Center (616-555-4662) has been contacted and the on-call staff has been asked to disable network access to the wall jack (desktop) or network switch (data center). * The account passwords for any system users will be reset, including local and administrative accounts. Help Desk (616-555-4357) will assist with this. * Login credentials of suspected compromised accounts are suspended. * To ensure business continuity for users affected by such disconnection include: * Replacing disconnected devices with fresh builds from IT. where stocks permit (ensuring they first have relevant updates applied). * Users may be directed to work remotely (in the case where there is clear remote work policies), or they may be directed to work from other locations within the organization such as another office, a Disaster Recovery facility. |

## 

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

|  |
| --- |
| We are monitoring for any new infections which might suggest that the malware is spreading across the infrastructure.   * The latest malware definitions have been deployed across the antimalware solution. * An estate-wide anti-malware scan is initiated. * We will determine whether the malware appeared to be communicating with outside parties and take steps to block any such communication. * We will Inform business data owner(s) and stakeholders of the progress of containment activities. |

## 

## **Recovery:**

|  |
| --- |
| * Run an up-to-date reputable antimalware tool or antivirus to scan and remove the malware. Complete a deep scan to ensure traces of malware are identified and removed. * Re-set the login credentials for any system users including local and administrative. * Re-build systems. * Restore any corrupted or destroyed data from a trusted backup. * Restore any suspended services. |

## 

## **Post-incident recommendations:**

|  |
| --- |
| * Develop a post-incident report that includes the following details as a minimum: * Details of the entire incident handling process, identifying areas for improvement and remediations. * New security actions that must be implemented to increase the overall security of the IT environment. * Recommendations where any aspects of people, process or technology could be improved across the organization to help prevent a similar cyber incident from reoccurring, as part of a formalized lessons identified process. * Schedule a follow-up review to identify what has been implemented to ensure there’s no future. * Complete the formal lessons identified process to feedback into future preparation activities. * Consider sharing lessons identified with the stakeholders. * Establish a communication channel to inform and educate employees on malware attacks and security awareness. |