# 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 |

### 

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

|  |
| --- |
| 2020-06-06 22:01:41 10.0.0.12:50134 -> 190.6.193.152:8080 |

### 

### False Positives *(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 21:59:17 172.31.90.209:35997 -> 172.31.0.2:53 |

## Containment:

|  |
| --- |
| 2020-06-06 22:04:00 the network operation center is contacted at (616-555-4662) and asked the on-call staff to disable the system with ip ( 10.0.0.2 ) access to the network from the wall jack (desktop) or network switch (data center).  2020-06-06 22:06:00 the team contacted the Help Desk at (616-555-4357) to start resetting passwords. |

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

|  |
| --- |
| 2020-06-06 22:00:50 an http request from the client 10.0.0.12 was detected on the monitoring system, and system was impacted with a malware (fnpufu.exe)  2020-06-06 22:04:00 the client is disconnected from the network  While analyzing the network flow using Wireshark the following was identifies:  2020-06-06 22:01:41 suspicious outbound requests and communication were identified from the client 10.0.0.12 to 190.6.193.152  When searching for the IP address (190.6.193.152) in VirusTotal, it shows that the IP is malicious.    2020-06-06 22:10:20 no similar alerts have occurred for other systems. |

## Recovery:

|  |
| --- |
| 2020-06-06 22:06:00 the team contacted the Help Desk at (616-555-4357) to start resetting passwords.  2020-06-06 22:10:00 Check the antimalware logs, if available.  2020-06-06 22:30:00 Rebuild the system and restore data from a known good backup before restoring network access. |

## Post-incident recommendations:

|  |
| --- |
| 1. Add a snort rule to detect similar attacks and suspicious activities, from IPs (216.154.220.53 & 190.6.193.152) 2. Restrict the download of executable file for only system administrator. |