# 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 22:00:50 216.154.220.53:80 -> 10.0.0.12:50134 (ET POLICY PE EXE or DLL Windows file download HTTP)  I found This packet which is using GET method to download file named /malware/fnpufu.exe, and the file name describe itself. After uploading the file to Virustotal.com, it said that file is reported as malicious from 58 Vendors. And this is its SHA-256 hash:  006d5fda899149df4cc5d6d1b1ae52e9fcc4ade7541c1dd4391e0429d843b4d5  It's considered as Trojan.  2020-06-09 02:44:42 190.6.193.152 -> 10.0.0.12 (POST /w00n19tnKeyeyjNO HTTP/1.1)  Also this looks suspicious, and the IP is reported from 12 Vendors as malicious or malware. |

### 

### 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:

|  |
| --- |
| Steps:   1. Contact the Network Operations Center (616-555-4662), and ask them to disable network access to the wall jack (desktop) or network switch (data center). 2. Contact the CISO by calling phone number(616-555-2476). 3. Capture RAM for possible forensic analysis. |

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

|  |
| --- |
| Steps:   1. Document the path to infection, if known. 2. Check for other infected hosts (similar network traffic). 3. Document any signs of lateral movement. 4. Document and signs of data exfiltration. |

## Recovery:

|  |
| --- |
| Steps:   1. Never panic. 2. Run malware scans overall systems. 3. Recover compromised or lost parts. 4. Isolate infected parts. |

## Post-incident recommendations:

|  |
| --- |
| Recommendations:   1. Reset all users password's. 2. Patch all software, make sure it's always patched. 3. Make an incident plan for next time if happens. 4. Make sure plan include every single procedure needed. |