# Incident Ticket

## 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):

|  |
| --- |
| **Suspicious network traffic:**  POST /wOOnl9tnKeyeyjNO HTTP/1.1  Referer: http://190.6.193.152/wOOnl9tnKeyeyjNO  Content-Type: application/x-www-form-urlencoded  DNT: 1  User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E)  Host: 190.6.193.152:8080  2020-06-06 22:01:41 10.0.0.12:50143 - > 190.6.193.152:8080 (HTTP POST request to suspicious IP address) |

### 

### 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  2020-12-28 18:37:46 10.0.2.15:40165 - > 8.8.8.8:53 |

## Containment:

|  |
| --- |
| 9:56 PM contacted Network Operation Center at 616-555-4662 and spoke to one of the on-call staff, John Smith, about disabling the network for 10.0.0.12 to prevent the spread of infection. |

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

|  |
| --- |
| 1. A client within the Marketing department (i.e., IP address 10.0.0.12) has been compromised with malware (fnpufu.exe with MD5 hash value of 189a128895906bd0f98b509247311e41) on 10:00 PM, June 06, 2020.      1. A minute after, unusual outbound traffic has been observed from the same infected client to suspicious IP address 190.6.193.152 located in Honduras, a country in Central America.     The above events are somehow connected since the client in question was associated with two different suspicious events, indicating that once the client was hit with malware, the attacker was able to establish access to 10.0.0.12 and exfiltrate data with the HTTP POST Request.  10:08 PM contacted the Help Desk at 616-555-4357 and requested to capture RAM for possible forensic analysis and asked for a list of active processes on the infected client.  10:13 PM called in Adam Johnson to handle communication and follow-ups with NOC and the Help Desk and perform an additional investigation to determine the criticality/sensitivity of data stored on the infected client.  As of 10:21 PM, no similar alerts have been observed for other clients. |

## Recovery:

|  |
| --- |
| 10:26 PM contacted the Help Desk at 616-555-4357 with requests to reset passwords for all local and administrative accounts on the infected client.  10:48 PM checked antimalware logs and found that malware has not been detected and as of now there is no assurance that the malware has not downloaded any additional malicious files.  10:51 called the Help Desk at 616-555-4357 to rebuild the infected system and restore data from a known good backup before restoring network access. |

## Post-incident recommendations:

|  |
| --- |
| 1. Blacklist external IP addresses associated with current security incidents (i.e., 216.154.220.53 and 190.6.193.152). 2. Update the antimalware signature database to include the malware in question. 3. Perform a full scan on all network segments to check whether the infection has spread to other clients or not. 4. Analyze network activity and look for suspicious inbound/outbound traffic in case any were missed during the initial detection. 5. Restrict admin privilege to a small group of individuals to prevent the installation of malicious application in the future. 6. Conduct a lesson-learned meeting with CISO to discuss what went well and went wrong to avoid mishandling similar incidents in the future. |