**Containment Strategy**

This document contains counsel as to the scope and severity of infections by malware, as well as steps to fix infected computers and prevent future attacks.

**Scope**

**TODO**: *Summarize the scope of the attack surface vulnerable to this sample. Include information on:*

* Affected operating systems/services and versions
* Types of devices usually targeted

**Severity**

**TODO**: *Explain how severe this malware is. Based on this information, recommend a timeline for patching*. *Look for information on:*

* How much damage the malware does to the infected computer (e.g., is it destroyed vs inaccessible vs just a little bit slower?)
* How hard is it to remove without replacing the computer
* How much data it can get access to—is it just adware, or does it expose a full root shell to an attacker?

Based on the above, we conclude that this sample is of **TODO** severity, and should be patched **TODO**.

**Solution**

**TODO**: *Explain the steps to fix a computer that has been affected; which patches to use, if any; and strategies for preventing future attacks.*

**Awareness Training**

This document explains how end users can

* Identify an infection by malware
* Protect your data and isolate the infected machine
* Determine which organizational stakeholders to notify in the event of a compromise

**Identification**

**TODO**: *Explain the steps to identify an infection with your sample. Refer to your Behavioral Analysis results from before, and list the prominent pieces of suspicious activity.*

* For example, if your malware made a GET request to the server 182.98.28.9, you might tell your users to check their firewall logs for records of communications to that IP address.
* **Be sure to explicitly refer to your behavioral analysis to justify your steps.**

**Quarantine and Response**

**TODO**: *Based on your Behavioral Analysis results from before, explain the steps users should take to minimize damage to their computer and the rest of the network if they find their device to be infected.*

* For example, if your malware made a GET request to the server 182.98.28.9, you might tell your users to disconnect from the network, and recommend setting a firewall rule that blocks all traffic to/from that IP.
* If it downloaded a malicious file, you might recommend disconnecting from the network; backing up personal data to an external hard drive; and restoring the operating system.
* **Be sure to explicitly refer to your behavioral analysis to justify your steps.**

**Escalation**

**TODO**: *Based on your Behavioral Analysis results from before, explain who should be notified in the event a device on an enterprise network is found to be infected with your malware.*

* For example, if your malware is ransomware, you should notify your Security team, as well as your direct manager (who will likely escalate to the executive team).
* If your malware is a trojan, you should simply follow the steps in Quarantine and Response, and notify your security team about the incident.
* **Be sure to explicitly refer to your behavioral analysis to justify your steps.**