# Internal Memorandum

Hierarchical
Access
Limited
Corporation
www.halcorp.biz

**To:** hal.cio@seccdc.org

**CC:** judge_29@seccdc.org

**From:** Team 9 <hal29@seccdc.org>

**Date:** 2/23/2019

**Re:** Incident Response Report 05

## PART ONE: COMPLETED UPON INITIAL DETECTION

| | |
|---|---|
| Case Number: | IR-02232019-05 |
| Date & Time Incident Detected: | 02/23/2019 5:00PM |
| Status: | Resolved |
| 1st Responder: | Aiden Durand |
| Case Manager: | Michael Roberts |
| Attack Type: | Impersonation |
| Trigger: | Malware Scan returned positive |
| Reaction Force and Lead: | **LEAD:** Michael Roberts<br>**Archivist:** Aiden Durand |
| Notification Method: | Malware Scanner |
| Response Time: | 25 Minutes |
| Incident Detection<br>(Describe the events that resulted in the identification of a possible (candidate) incident. | |
| The incident was detected when a Malwarebytes malware scanner deployed on the Windows 8.1 host detected a virus called “Isass.exe”, an impersonation of the benign lsass.exe. | |
| Incident Containment Procedures<br>(Describe the incident as it evolved once detected and classified and<br>the corresponding actions taken by the CSIRT Team members to contain the Incident | |
| 1. The detected virus was quarantined.<br>2. The effected host was disconnected from the network as to prevent contamination.<br>3. The running processes on the host were scanned for any malicious activity. | |

## PART TWO: COMPLETED UPON INCIDENT RESOLUTION

Time Incident was Resolved: 5:25 PM

Incident Recovery Procedures
(describe the actions taken by the CSIRT Team after the incident was contained
to recover lost, damaged or destroyed data, and to prevent re-occurrence.)

1. The system was deep-scanned to discover any possible traces of the virus
2. The user accounts on the machine were audited to look for any new malicious users
3. All other hosts on the network were scanned for the malicious binary.

Recommended Changes to Incident Prevention Measures
(to prevent exposure, eliminate vulnerability, and mitigate damage in the future)

1. Configure active malware scanning on the hosts on the network, to discover threats before they can activate.

2. Enable Windows Smartscreen to filter downloaded executables to prevent users from running malicious binaries.

3. Schedule routine malware definition updates to keep our scanners up-to-date with emerging threats.

| | | |
|---|---|---|
| Was Data Lost? | N | Financial Impact: $ 0<br>(attach documentation as needed) |

| | | | |
|---|---|---|---|
| Was System Equipment Recovered? | Y | Returned to service? | Y |

Notes:

All other Windows hosts were checked for this binary and they came up clean. Service has been successfully restored and the machine is back on the network.

| | |
|---|---|
| Is the incident completely resolved /case closed? | Y |
| Is Legal Recourse Required? | N |
| Report Submitted By: | Aiden Durand |

Submit this form by email to hal.ciso@seccdc.org or ciso@halcorp.biz, as appropriate, once the incident has been contained and within three (3) hours of initial detection.