# Internal Memorandum

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

**CC:** judge_29@seccdc.org

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

**Date:** 2/23/2019

**Re:** Incident Response Report 06

Hierarchical Access Limited Corporation

www.halcorp.biz

---

**PART ONE: COMPLETED UPON INITIAL DETECTION**

| | |
|---|---|
| Case Number: | IR-02232019-06 |
| Date & Time Incident Detected: | 02/23/2019 6:35PM |
| Status: | Resolved |
| 1st Responder: | Peyton Duncan |
| Case Manager: | Michael Roberts |
| Attack Type: | Other: An undocumented machine on our network. |
| Trigger: | Manual forensic investigation |
| Reaction Force and Lead: | **LEAD:** Michael Roberts<br>**Archivist:** Peyton Duncan |
| Notification Method: | Network log investigation |
| Response Time: | 30 Minutes |

Incident Detection
(Describe the events that resulted in the identification of a possible (candidate) incident.

The incident was detected when the system administrator was performing a routine analysis of the Wireshark logs for suspicious activity. The administrator observed a suspicious file being downloaded from 10.0.0.100, and engaged the forensic specialist on the team.

Incident Containment Procedures
(Describe the incident as it evolved once detected and classified and
the corresponding actions taken by the CSIRT Team members to contain the Incident

1. The malicious system was blocked by each machine on the network segment.

2. Firewall policy was implemented on the Palo Alto to block communication from the malicious host to all other hosts on our network.

3. We informed our system administrators to audit the network regularly.

## PART TWO: COMPLETED UPON INCIDENT RESOLUTION

Time Incident was Resolved: 7:05PM

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. Analyzed intercepted malware and archived following HAL malware containment protocols.

2. Other team members were informed of the issue in order to check their systems and whether it had the malware.

3. Ensured the malware never executed and was not able to interfere with any existing HAL data.

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

1. Perform routine malware scans on all assets.

2. Regularly scan internal networks for signs of unknown hosts

3. Review Incident prevention measures on a regular basis to ensure they are being followed.

| | | | |
|---|---|---|---|
| Was Data Lost? | N | Financial Impact: $ 0<br>(attach documentation as needed) | |
| Was System Equipment Recovered? | Y | Returned to service? | Y |

Notes:

Checked the other windows machines to ensure this malware was not present on them.

| | |
|---|---|
| Is the incident completely resolved /case closed? | Y |
| Is Legal Recourse Required? | N |
| Report Submitted By: | Team 9 |

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.