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 01

PART ONE: COMPLETED UPON INITIAL DETECTION

Case Number:	IR-02232019-01
Date & Time Incident Detected:	02/23/2019 3:05PM
Status:	Resolved
1st Responder:	Matthew St. Hubin
Case Manager:	Michael Roberts
Attack Type:	Attrition Improper Usage: Any incident resulting from violation of an organization’s acceptable usage policies by an authorized user, excluding the above categories; for example, a user installs file sharing software, leading to the loss of sensitive data; or a user performs illegal activities on a system.
Trigger:	Manual forensic investigation
Reaction Force and Lead:	**LEAD:** Michael Roberts **Archivist:** Matthew St. Hubin
Notification Method:	Word of Mouth
Response Time:	35 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 domain controller for suspicious activity. The administrator observed a suspicious file in a startup location, 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 startup run key was disabled.

2. The malicious sample was archived and removed.

3. Software restriction policies were enforced to keep the binary from running should it return.

PART TWO: COMPLETED UPON INCIDENT RESOLUTION

Time Incident was Resolved: 3:15PM

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. Malware was archived following HAL malware containment procedure.

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 check system files for any malicious content.

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

Was Data Lost?	N	Financial Impact: $ 0 (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 / N
Is Legal Recourse Required?	Y / 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.