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 02

PART ONE: COMPLETED UPON INITIAL DETECTION

Case Number:	IR-02232019-02
Date & Time Incident Detected:	02/23/2019 3:15PM
Status:	Resolved
1st Responder:	Martin Roberts
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:** Martin Roberts
Notification Method:	Word of Mouth
Response Time:	25 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 linux servers for unauthorized content. All authorized_keys were audited.

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 unauthorized public key was archived.
2. Removed any sessions the user had.

PART TWO: COMPLETED UPON INCIDENT RESOLUTION

Time Incident was Resolved: 3:20 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.)

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

1. Perform routine audits for unauthorized public key plants.

2. Audit what permissions user has when logging in with SSH.

Was Data Lost?	N	Financial Impact: $ 0 (attach documentation as needed)

Was System Equipment Recovered?	Y	Returned to service?	Y

Notes:

Checked the other Linux machines to ensure this key 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.