Internal Memorandum

To: Paula Alexander <hal.cio@seccdc.org>

CC: Room Judge

From: Team 09

Date: 02/23/2019

Re: Incident Response Report – 004

**PART ONE: COMPLETED UPON INITIAL DETECTION**

|  |  |
| --- | --- |
| Case Number: | IR-02232019-00 |
| Date & Time Incident Detected: | 02/23/2019 3:00 PM |
| Status: | Resolved |
| 1st Responder: | Matthew St. Hubin |
| Case Manager: | Michael Roberts |
| Attack Type: | Attrition: Improper Usage |
| Trigger: | Malware Scan |
| Reaction Force and Lead: | LEAD: Michael Roberts  Archivist: Matthew St. Hubin |
| Notification Method: | Malware Anti |
| Response Time: |  |
| Incident Detection  (Describe the events that resulted in the identification of a possible (candidate) incident. | |
|  | |
| 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 | |
|  | |

**PART TWO: COMPLETED UPON INCIDENT RESOLUTION**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Time Incident was Resolved: | | | | | | |
| 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) | | | | | | |
|  | | | | | | |
| Was Data Lost? | Y / N | Financial Impact: $  (attach documentation as needed) | | | | |
| Was System Equipment Recovered? | | | Y / N | Returned to service? | | Y / N |
| Notes: | | | | | | |
| Is the incident completely resolved /case closed? | | | | | Y / N | |
| Is Legal Recourse Required? | | | | | Y / N | |
| Report Submitted By: | | | | |  | |

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