Internal Memorandum

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

**CC:** roomjudge@seccdc.org

**From:** Team 02

**Date:** 2/24/2017

**Re:** Incident Response Report

**PART ONE: COMPLETED UPON INITIAL DETECTION**

|  |  |
| --- | --- |
| Case Number: | IR-002 |
| Date & Time Incident Detected: | February 25, 2017 2:30 EST |
| Status: | Resolved |
| 1st Responder: | Charlton Trezevant |
| Case Manager: | Matthew St.Hubin |
| Attack Type: | Other – Website Defacement |
| Trigger: | Indicators: Upon visiting the company website, we discovered that the home page had been defaced, and that inappropriate content was being served. |
| Reaction Force and Lead: | Charlton Trezevant |
| Notification Method: | A message from the CIO |
| Response Time: | 1 Hour |
| Incident Detection  (Describe the events that resulted in the identification of a possible (candidate) incident. | |
| Following the receipt of a message from the CIO, the system administrator found that the company website had been defaced by attackers, indicating that the server in question had been compromised. Further inspection additionally revealed that the entire contents of the webserver’s root directory, which contained the original website’s source code, had been destroyed. After conferring with HAL Corp engineers to confirm that this change was not approved, the system administrator began the remediation process. | |
| 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. To ensure service uptime, an emergency failover was performed to one of our hot spare webservers, which hosts a mirror of the corporate website. This enabled us to temporarily resurrect the service as containment procedures began on the original server. 2. On the original web server and following the migration, the administrator immediately disabled the webserver process and killed all active console sessions. 3. Additional firewall rules were installed on the host machine in order to prevent any unauthorized outbound connections as containment procedures took place. | |

**PART TWO: COMPLETED UPON INCIDENT RESOLUTION**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Time Incident was Resolved: February 25, 2017 3:00 EST | | | | | | |
| 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. Following the containment of the incident, the team began scouring system logs to determine the source of the attack. 2. In order to restore system integrity, the team leveraged system event logs, command history files, authentication, and access logs to determine the scope and extent of the damages caused. Using these, administrators were able to trace back and undo unauthorized changes, as well as determine exactly how the attacker gained access to the system. 3. Following the reversal of unauthorized changes to the system, the web service functionality was restored from a backup, and system passwords were rotated. Additionally, firewall access policies were updated on the system in order to prevent future unauthorized access. | | | | | | |
| Recommended Changes to Incident Prevention Measures  (to prevent exposure, eliminate vulnerability, and mitigate damage in the future) | | | | | | |
| 1. Stricter policies should be in effect to limit the ability of machines outside of the HAL Corp network from accessing system management services. In terms of the compromised system, only the web server should be accessible from outside of the network. 2. Console access policies should be modified to use more secure authentication schemes. Additionally, software such as fail2ban should be deployed in order to prevent the brute-forcing of SSH credentials, to keep attackers out. 3. To improve response time, an intrusion detection system (IDS) such as Tripwire should be deployed in order to provide administrators with a means of immediate notification following system compromise. | | | | | | |
| Was Data Lost? | **N** | Financial Impact: $0  (attach documentation as needed) | | | | |
| Was System Equipment Recovered? | | | **Y** | Returned to service? | | **Y** |
| Notes:  All services on the effected systems have been restored to optimal functionality. | | | | | | |
| Is the incident completely resolved /case closed? | | | | | **Y** | |
| Is Legal Recourse Required? | | | | | **Y** | |
| Report Submitted By: | | | | | Charlton Trezevant | |

Submit this form through the HAL Service Desk once the incident has been contained and within three (3) hours of initial detection.