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 03

Hierarchical Access Limited Corporation

www.halcorp.biz

PART ONE: COMPLETED UPON INITIAL DETECTION

Case Number:	IR-02232019-03
Date & Time Incident Detected:	2/23/19 3:21 PM
Status:	Resolved
1st Responder:	Charlton Trezevant
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:** Charlton Trezevant
Notification Method:	Word of Mouth
Response Time:	10 Minutes

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

The incident was detected when a routine audit of the host's application revealed that a malicious PHP file, cookie_check.php, was present on the host system. The system administrator observed that the purpose of this file was to execute a variety of unauthorized commands and functions such as MySQL queries, local commands, and arbitrary PHP scripts. The system administrator also noted that the developers of the application were credited as "rootshell-team.info".

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. Initially, the system administrator audited the functionality of the page. Upon realizing its purpose, the offending PHP file was immediately removed from the web root in order to prevent access to the file.
2. Following this, an audit of running processes was undertaken in order to determine whether any unauthorized processes had spawned from the malicious PHP file. After none were find, a similar audit was performed of the web application's access log in order to determine who (if anyone) had accessed the file. Outside of the system administrator's own IP address, the apparent IP of the attacker, 10.23.45.5 was recorded in the logs.
3. It was determined that the attacker had accessed the "shell" feature of the application 6 times, and the "command" feature of the application (in the directory of /var/www/html 5 times. Both of these events occurred on March 22, 2018.

PART TWO: COMPLETED UPON INCIDENT RESOLUTION

Time Incident was Resolved: 3:31 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.)

1. As the administrator had implemented a number of hardening measures on the system's PHP configuration, it was determined that the system was now invulnerable to these types of attacks. In the future, malicious PHP web shells should not be able to function on the system.

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

1. The primary defense against malicious command execution was a policy put into place by the system administrator which disabled PHP's ability to execute commands and spawn other processes. It is recommended that a similar policy be put into place on any HAL systems hosting PHP based web applications.
2. An alerting policy should be enacted for the above. This would be easy to implement using a log aggregation solution such as Splunk.
3. In addition, application log audits should happen on a routine basis. The malicious activity was recorded in the server's access logs in March of 2018, and should have been uncovered much earlier than February of 2019.

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

Was System Equipment Recovered?	Y	Returned to service?	Y

Notes:

Normal operation of the system was restored without impact to service availability. However, HAL Corp should continue to aggressively investigate the motivation of the attacker, the scope of their activity, and their origin.

Is the incident completely resolved /case closed?	Y
Is Legal Recourse Required?	Y
Report Submitted By:	Charlton Trezevant

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.