**IR Report 9**

**Team #:**

**Report #:**

**Report Type:**Quick

**Report title:**

**Time of incident:**4/1/23 2:44PM EST

**IP Block Request:**N/A

**Executive Summary:**

On 4/1/23 at 2:44PM EST we noticed multiple servers are bricked when trying to login as root. The both servers give the error “I say no” when any command is attempted to be ran. In addition the office server say “Hello starshine, the earth says hello” it appears as if the red team are avid fans of the tellitubbies.

**Detailed Analysis:**

After logging into these servers, no commands are able to be ran. The only output from these commands is “I say no” and “hello starshine, the earth says hello”, no commands are able to be ran at all. It appears as if both server has an infinite broadcast running that is an alias that turns any command into the messages are shown.

* The terminal is inoperable and no commands are able to be ran.

**Remediations and Mitigations:**

Remediations: The service will be taken offline until a fix can be found

Mitigations: The team will do its best to find a solution and block the issue at its source.

The SOC recommends the following remediation actions:

* Taking the service offline while waiting for a fix.

The SOC recommends the following Mitigation actions:

* To research how to take control back of a system
* Potentially reverting the entire system to a known working state.

**References:**

*NA*