CYB490A

At about 1745 (MT), the SOC team started logging into their machines and watching for any unusual activity.

First alert was for port scanning

Then, Brute Force failed log-in events was noticed in Qradar.

Members of the SOC tried to collect more information about failed log-in attacks.

The first alert came in at 0033

0039 Admin log in Failure

0044 successful login

At about 0000 GMT the CSO reported seeing a character appear on his monitor.

The IP address of the hacker was 172.l6.100.22.

The apache2 server was the initial entry of the hack.

Once in the the apache2 firewall hacker ran “whoami” command.

Then, a “.tmp” file was created.

Wget: net tools, archive file

The attacker extracted “.png” to replace image on url.

A member of the SOC discovered that the target server of the attack was Ogami.com.

The hacker left a script kitty on the ogani webpage.

The hack was considered lateral movement through the network.

The following discussion focused on how to prevent future log in hacks.

The loginID/password combination was weak.

Incorporating a new password policy with requirements for increased character length, complexity and lock out policy was determined necessary.

Ssh network access should only be available onsite.

It was discussed that the hacker may have tried Port Scanning and Fuzzing prior to, or in addition to Brute Force password attacks to do recon on the website before attacking.

The hacker then likely created or used a Temp folder to operate out of, storing images and programs that would be installed on the website.

The easiest way to restore the network may have been to re-image the affected servers.

A generalized program that hackers follow is:

* Do recon on the targeted network. Find out information about the target
* Scan the network to find out more about the network
* Prioritize what to attack
* Exploit any advantage to gain access
* Once access is gained, gain higher permissions through privilege escalation, making lateral movement to target
* Exfiltrate any data of interest
* Cover evidence of entry, if possible

That being covered, there are two general types of hacking:

1. Attacks that are loud or aggressive and take place quickly to obtain objective.
2. Attacks that are quiet or subtle and occur over very long periods of time (years) to gain objective.