Incident Response Exercise

June 12, 2013
JPCERT Coordination Center, Japan

Exercise Scenario [Systems environment]

[Company A's system]
OS: Debian Linux (6.0.5) [126.25.10.111]
Application: Web server(Apache)

- To promote services/products
- Install Webapp for info-share (since Aug/2011)
- Can ssh login to server only from internal network

Exercise Scenario [Phase 1]

One day, System admin of Company A got phone call …

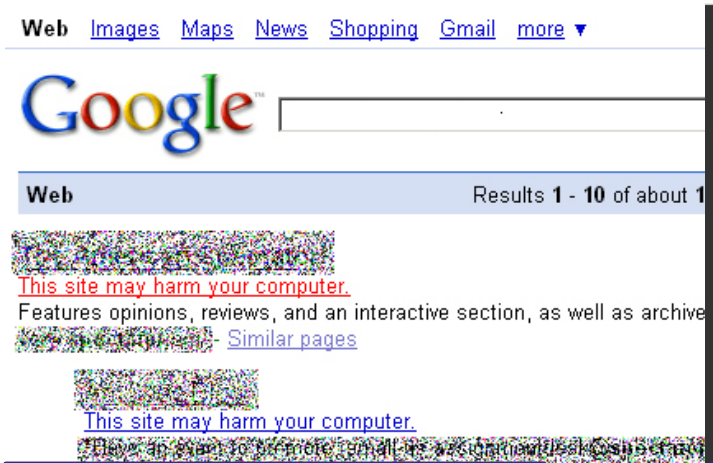
Exercise Scenario[Investigation by system admin]

System admin first accessed company A website.

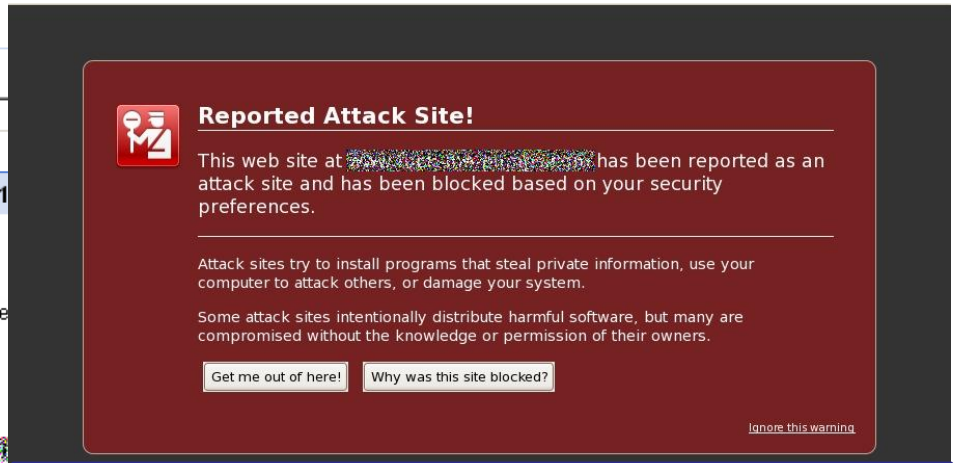
- Web site seems working as usual. No visible error.

Sys admin also asked his colleagues to check the web.

- Some said that they got following errors…



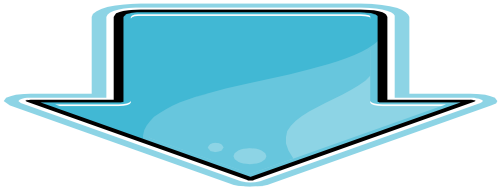
Search result



What they got for company A web when accessed

Two major issues(at this moment)

- Website url is in Google's blacklist
- Web server might be compromised



System admin had less knowledge about incident response.
So they decide to leave this problem to AfricaCERT.

Exercise Scenario [logs]

System admin shared with you only web server logs.

- Access log
- Rewrite log

Check these logs and fill in following answer sheet.

CAUTION!

IP addresses and domain names in this exercise is fake. Please do not access these from your laptop which is internet connected.

- Connect to the IP address:
- User: ais01, ais02, …, ais20
- Password:

Question 1

[Duration of log: When the log begin and end?]

[in this log, how many **unique** IP accessed to web?]

Question 2

JPCERT CC®

[IP address of attacker. Pick up all that apply]

[Date and time of web site compromise]

Question 3

[Describe what happen to users if they access to web site.]

[What is the root cause of this incident?]

Question 4

[What Sys admin should do ?]

[What company A should do?]

Exercise 5

- What We(AfricaCERT/JPCERT) can do for this case???