WRITE UP FOR
OPERATION BLACKOUT

Contact :
contact@cybercohesion.com

APAC / JAPAN / INDIA / MIDDLE EAST / AFRICA / SOUTH AMERICA

Questions :

1. What is the programming language used to write the binary?

Python

2. What is the format of the binary? (ELF, PY, SH, EXE)

ELF

3. What is the tool used to package the binary?

Pyinstaller

4. What type of Encryption is used on this binary (Asymmetric, Symmetric,hybrid)

Asymmetric

5. What is the cryptosystem used? (RSA, AES, XOR, ALL)

RSA

6. What are the first four bytes of the key found in the compiled binary?

MIIC

7. What is the Command & Control (domain: port)?

cVcyfY6YR8GmNw45fJdA4ukP2qjgGXJTMSSLfzYUfqwvY2somh.xyz:3339

8. What is the process that is responsible for the power grid system?

gldcore

9. Which transport layer protocol was used to send data to the Command & Control? (TCP, UDP, SCTP, NONE)

TCP

10. What is the malware's original country? (RUSSIA, CHINA, IRAN, UK)

CHINA

11. there was a scheduled date time by the threat actor for a specific operation what is it?

April 15, 2024, 12:00:00 {CORRECT}
April 12, 2024, 15:00:00
April 12, 2024, 24:00:00
April 24, 2024, 12:00:00

12. What is the path to the configuration file that the mawlare compromises?

/etc/Gridlab-d/conf/master.glm

13. what data does the malware send to the C&C?

(hostname, port, timestamp, timezone, signal_timeout, username, server_name) hostname, port, timestamp, timezone, signal_timeout, username, server_name

14. Which of these directories are affected by the malware?

/etc/ CORRECT
/var/log/ CORRECT
/sys/
/usr/
/root/

15. What type of affection applied into those directories?

PURGE
DELETE {CORRECT }
EDIT

16. What is the first thing the malware does after deploy?

Enumeration {CORRECT }
Configration file manipulation
Ransomware infection
Shutdown the power grid

17. What are the malware capabilities?

Enumerating the power grid {CORRECT}
Configuration file manipulation {CORRECT}
Ransomware infection
Shutdown the power grid {CORRECT }
Erase the logs {CORRECT}

AND THAT WAS IT

for Operation Blackout !