BLACKSWAN
CYBERSECURITY

THREAT ANALYSIS

Mar 16, 2023

GlobeImposter Ransomware Being Distributed with MedusaLocker via RDP

SUMMARY

ASEC (AhnLab Security Emergency response Center) identified GlobeImposter ransomware being spread by the same threat actors behind MedusaLocker. Evidence gathered by ASEC from infection logs and other artifacts point to the ransomware being distributed via RDP.

TECHNICAL DETAILS

Typical IOCs include a new "skynet work" subdirectory within the "Music" directory to house the malware. The compromised system is then infected with shared folder scanners, Mimikatz, a network password recovery tool, and port scanners. In some instances, XMRig CoinMiner was installed to mine cryptocurrency. Internal reconnaissance is performed after gaining control of the system through RDP.

The same email and onion addresses reported by the CISA as being utilized by the MedusaLocker group are also among those listed in the ransom note of the GlobeImposter ransomware.

INDICATORS OF COMPROMISE (IOCs)

MD5

- 715ddf490dbaf7d67780e44448e21ca1
- 646698572afbbf24f50ec5681feb2db7
- 70f87b7d3aedcd50c9e1c79054e026bd
- f627c30429d967082cdcf634aa735410
- 597de376b1f80c06d501415dd973dcec
- 4fdabe571b66ceec3448939bfb3ffcd1
- 6a58b52b184715583cda792b56a0a1ed

Port Scanner

- 4edd26323a12e06568ed69e49a8595a5
- a03b57cc0103316e974bbb0f159f78f6

mimispool.dll

- ddfad0d55be70acdfea36acf28d418b3

mimilib.dll

- 21ea77788aa2649614c9ec739f1dd1b8
- 5e1a53a0178c9be598edff8c5170b91c
- bb8bdb3e8c92e97e2f63626bc3b254c4

mimikatz.exe C&C

- hxxp://46.148.235[.]114/cmd.php

REFERENCES

- https://asec.ahnlab.com/en/48940/
- https://www.hhs.gov/sites/default/files/medusalocker-ransomware-analyst-note.pdf