BLACKSWAN CYBERSECURITY

THREAT ANALYSIS

April 4, 2023

APT43 Group (North Korea) Espionage Operations Funded by Cybercrime

SUMMARY

Mandiant reported that APT43 (North Korea) has been targeting organizations in the U.S., Europe, Japan, and South Korea over the past five years. The Mandiant report points to a state-sponsored threat actor (high confidence) and that the threat actor belongs to the North Korean Reconnaissance General Bureau (medium confidence), North Korea's primary foreign intelligence service.

TECHNICAL DETAILS

Mandiant believes the APT43 group is laundering stolen cryptocurrency through legal cloud mining services while also conducting on-going social engineering campaigns, creating false names and sock puppet relationships with targets.

The malware being used by APT43 is unique and not commonly used by other threat actors; including: Hangman backdoor, Pencildown, Pendown, Laptop, Venombite and tools like QuasarRAT, Amadey, and gh0st RAT.

Mandiant also added that APT43 targets groups involved in politics, business, manufacturing, think tanks, education, and research related to nuclear and geopolitical policies in the US, South Korea, and Japan.

INDICATORS OF COMPROMISE (IOCs)

Hashes:

- 982fc9ded34c85469269eacb1cb4ef26
- e205ed81ccb99641dcc6c2799d32ef0584fa2175
- 557ff6c87c81a2d2348bd8d667ea8412a1a0a055f5e1ae91701c2954ca8a3fdb
- de9a8c26049699dbbd5d334a8566d38d
- 47a32bc992e5d4613b3658b025ab913b0679232c
- 43c2d5122af50363c29879501776d907eaa568fa142d935f6c80e823d18223f5
- 144bd7fd423edc3965cb0161a8b82ab2
- 1087efbd004f65d226bf20a52f1dc0b3e756ff9e
- 2b78d5228737a38fa940e9ab19601747c68ed28e488696694648e3d70e53eb5a
- cd83a51bec0396f4a0fd563ca9c929d7
- f3b047e6eb3964deb047767fad52851c5601483f
- fb7fb6dbaf568b568cd5e60ab537a42d5982949a5e577db53cc707012c7f20e3
- 33df74cbb60920d63fe677c6f90b63f9
- 539acd9145befd7e670fe826c248766f46f0d041
- 94aa827a514d7aa70c404ec326edaaad4b2b738ffaea5a66c0c9f246738df579
- ebaf83302dc78d96d5993830430bd169
- bc6cb78e20cb20285149d55563f6fdcf4aaafa58
- 5cbc07895d099ce39a3142025c557b7fac41d79914535ab7ffc2094809f12a4b
- b846fa8bc3a55fa0490a807186a8ece9
- c0c6b99796d732fa53402ff49fd241612a340229
- 855656bfecc359a1816437223c4a133359e73ecf45acda667610fbe7875ab3c8
- f92a75b98249fa61cf62e8b63cb68fae
- e5b312155289cdc6a80a041821fc82d2cca80bcd
- d0971d098b0f8cf2187feeed3ce049930f19ec3379b141ec6a2f2871b1e90ff7
- 1dcd5afeccfe2040895686eefa0a9629
- 40826e2064b59b8b7b3e514b9ef2c1479ac3b038
- 07aed9fa864556753de0a664d22854167a3d898820bc92be46b1977c68b12b34
- 5fe4da6a1d82561a19711e564adc7589
- e79527f7307c1dda62c42487163616b3e58d5028

- 8d0bafca8a8e8f3e4544f1822bc4bb08ceaa3c7192c9a92006b1eb500771ab53
- e8da7fcdf0ca67b76f9a7967e240d223
- b0c2312852d750c4bceb552def6985b8b800d3f3
- 9dac6553b89645ac8d9e0a3dc877d12641e6d05fb52e8de6ae5533b2bdf0abc9
- 2bf26702c6ecbd46f68138cdcd45c034
- 1b9a4c0a5615a4f96a041d771646c1a407b17577
- 38d1d8c3c4ec5ea17c3719af285247cb1d8879c7cf967e1be1197e60d42c01c5
- 2d330c354c14b39368876392d56fb18c
- a1f72c890d0b920f4f4cb2d59df6fa40734de90d
- f86d05c1d7853c06fc5561f8df19b53506b724a83bb29c69b39f004a0f7f82d8
- 15ec5c7125e6c74f740d6fc3376c130d
- fb09b89803da071b7b7eb23244771c54d979a873
- 4a1c43258fe0e3b75afc4e020b904910c94d9ba08fc1e3f3a99d188b56675211

REFERENCES

- https://mandiant.widen.net/s/zvmfw5fnjs/apt43-report
- https://www.bleepingcomputer.com/news/security/newly-exposed-apt43-hacking-group-targeting-us-orgs-since-2018/
- https://thehackernews.com/2023/03/north-korean-apt43-group-uses.html