Additional Activities of the Tick Group That Attacks with a Modified Q-Dir and Their Ties with Operation Triple Tiang

By AhnLab_en ⋮⋮ 4/17/2023

In March 2023, Eset analyzed malware that was found in an East Asian DLP manufacturer and announced that the Tick group was responsible for it.

The Tick group has been active mainly in Korea and Japan since 2014, targeting various sectors such as aerospace, military, defense industries, heavy industries, electronics, telecommunications, government agencies, and diplomacy.
AhnLab Security Emergency response Center (ASEC) has confirmed additional activities from this group and will be disclosing them here.

*** Modified Q-Dir Variants**

From January 2021 to August 2022, AhnLab Security Emergency response Center (ASEC) discovered 3 additional malware disguised as Q-Dir in Korea.
Two of the confirmed variants drop a ReVBSHell backdoor, but the variant (md5: 00b170970d46c9212b6d75ce7afc0870) discovered in August of 2022 creates an FTP server file.

*** ShadowPY Variant**

Eset also revealed information about the ShadowPY malware used in the attack, and upon verification, it was found to be similar to the malware that was reported to AhnLab in September 2021 by a Korean

client.
The program used as a loader at the time was Avira's avshadow.exe, and the name of the malicious DLL file was also vssapi.dll. Both of these align with the information disclosed by Eset.

The code was also found to be similar.

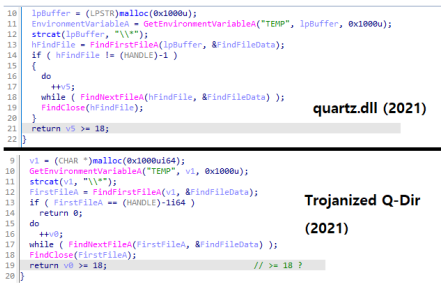
vssapi.dll file comparison

*** Ties with Operation Triple Tiang**

Eset revealed that there is a chance that Operation Triple Tiang, which was reported on by AhnLab, is related to the Tick group.
Operation Triple Tiang is a cyber attack campaign that has been targeting political and diplomatic sectors of Korea. A clear culprit behind this campaign was not identified at the point the report was released in 2022.

AhnLab Security Emergency response Center (ASEC) has confirmed that the ReVBSHell dropper used in Operation Triple Tiang and the ReVBSHell dropper variant used in the attack against the DLP manufacturer utilizes the same technique.

Both droppers check the number of files in the temp folder when the malware is executed, and only create the malware file when the number exceeds a certain amount (10 or 18 depending on the variant).



Operation comparison to check number of files inside Temp

Considering that they both use the same ReVBSHell and their droppers use similar codes, there is a high possibility that the Tick group is behind Operation Triple Tiang.

*** Conclusion**

The Tick group has been targeting government agencies, the military, and various industries in Korea and Japan for over a decade. There is a high possibility that they are still active covertly, and AhnLab plans to continue tracking their activities.

* Special thanks to Facundo Muñoz from Eset for providing the samples and information.

[File Detection]

Backdoor/VBS.Agent (2023.03.29.02)
Dropper/Win.Revbshell (2023.03.28.03)
Dowonloader/Win.Agent (2022.03.15.00)
Trojan/VBS.Obfus (2023.04.06.00)
Trojan/Win.ShadowPY (2023.04.05.03)

[IOC]

00b170970d46c9212b6d75ce7afc0870
19d0edc452b32b0d3da407459a1a9c56
2db7b0e8b0a3b7f142c4246d8c8bf892
31329cce9d0517233053b5363f06f5af
574df15b8bc888750ca28dd4f4f11fae
cb4a15d941a20985d145cd99fcaf3c82
ddbd1fcf0c332ce8dc38f6b48b29c597
ed97cf996bda070de3b7fa1e75b762b1