Hive Pro

THREAT ADVISORY

New PlugX variant "Talisman" used by famous Chinese APT

TA2022083

Threat Level RED

Publish Date – Mar 30, 2022

PlugX is a well-known malware family with samples dating back to as early as 2008. A Chinese state-backed threat actor, **RedFoxtrot** group, is discovered to use a new variant of the **PlugX** malware, **Talisman**. The threat actor group has staged campaigns on telecommunication and defense sectors in South Asian countries. These victims were attacked to protect the Belt and Road initiative of the Chinese government, a program that aims to establish strong socioeconomically relationships across Europe, Asia, and Africa.

PlugX is a fully featured Remote Access Tool/Trojan (RAT) with capabilities such as file upload, download, and modification, keystroke logging, webcam control, and access to a remote cmd.exe shell. Talisman is a new PlugX variant that uses a signed and safe binary to load a modified DLL and run shellcode. The shellcode is used to decrypt the PlugX RAT, which subsequently acts as a backdoor with plug-in capability. Unlike previous versions, the malware's internal configuration signature has changed, as have other small changes inside the code.

The MITRE ATT&CK TTPs used by **PlugX** are:
TA0002: Execution
TA0003: Persistence
TA0004: Privilege Escalation
TA0005: Defense Evasion
TA0006: Credential Access
TA0007: Discovery
TA0009: Collection
TA0011: Command and Control
T1071: Application Layer Protocol
T1059: Command and Scripting Interpreter
T1543: Create or Modify System Process
T1140: Deobfuscate/Decode Files or Information
T1574: Hijack Execution Flow
T1056: Input Capture
T1036: Masquerading
T1112: Modify Registry
T1106: Native API
T1135: Network Share Discovery
T1095: Non-Application Layer Protocol
T1057: Process Discovery
T1012: Query Registry
T1113: Screen Capture
T1049: System Network Connections Discovery

Actor Details

Name	Origin	Target Locations	Target sectors	Motive
RedFoxtrot (Nomad Panda)	China	Afghanistan, India, Kazakhstan, Kyrgyzstan, Uzbekistan, Tajikistan, Pakistan	Defense, Aerospace, Mining, Research Organizations, Government, Telecommunications	Information theft and espionage

Indicators of Compromise (IoCs)

Type	Value
Domain	freewula.strangled[.]net, szuunet.strangled[.]net, dhsg123.jkub[.]com, final.staticd.dynamic-dns[.]net oprblemoyo.kozow[.]com, asd.powergame.0077.x24hr[.]com, w.asd3.as.amazon-corp.wikaba[.]com, randomanalyze.freetcp[.]com, darkpapa.chickenkiller[.]com, miche.justdied[.]com
IPv4	209[.]97[.]166[.]143, 149[.]28[.]139[.]86, 159[.]65[.]152[.]7, 143[.]110[.]242[.]139, 158[.]247[.]204[.]191, 143[.]110[.]250[.]149, 202[.]182[.]111[.]249, 207[.]148[.]119[.]147, 149[.]28[.]128[.]117, 159[.]65[.]147[.]83, 143[.]110[.]241[.]54, 157[.]245[.]111[.]30, 207[.]148[.]64[.]239, 45[.]76[.]188[.]118, 45[.]77[.]16[.]91
SHA256	c09ff32519f112674bd5f4b1687feadf18844c5423e6f28df8be50eb9503e606 1c0cf69bce6fb6ec59be3044d35d3a130acddbbf9288d7bc58b7bb87c0a4fb97 6dc98a3c771f9f20d099e2d64995564dd083be9ac6ed9586a6e57c20ebd4176c 344fc6c3211e169593ab1345a5cfa9bcb46a4604fe61ab212c9316c0d72b0865 e71d355dec64cbf8f02a754bf0585437ce48f7b68108cb642fb202393cd1ef90 0a00204517283c9a8d1e2d1a8743249c14de0edcec4a8292500083437735663c 45c944889a482ae2e0e0a8e260c3be737cb612c8804164badef61e8a8713b92f f6b939dcc97c1c43f1c616174f936b6ef19c5ccc872a1a0ef14f2989cf11b02b ad48650c6ab73e2f94b706e28a1b17b2ff1af1864380edc79642df3a47e579bb 46cd5079a69d9a68029e37f2680f44b7ba71c2b1eecf4894c2a8b293d5f768f10 0468005682c814e7a5f07f3554e9fadbb2d2ba7527dcaee9a1a456f244c49ddb a072133a68891a37076cd1eaf1abb1b0bf9443488d4c6b9530e490f246008dba fdada5ba799bd9f5270b218cfad543d99fde3eb7898fd9e3ee79603b643b3c48 37b3fb9aa12277f355bbb334c82b41e4155836cf3a1b83e543ce53da9d429e2f fe18adaec076ffce63da6a2a024ce99b8a55bc40a1f06ed556e0997ba6b6d716 3c5d08f20a7bd04b1e6866344af59bec2152ec3542f2eae0c7925555e670676e f44ede464f752ea3aa3595f8137945a4dee7298c8155c39f366aad05b125ac8b
SHA1	dc40970a3c8f03866e0b700460d3b1f7afa6a433, ef3e558ecb313a74eeafca3f99b7d4e038e11516, 2294ecbbb065c517bd0e01f3f01aabd0a0402f5a, 80e5fd86127de526be75ef42ebc390fb0d559791
MD5	8e886df3cb6160188f9748f14f249063, b4f12a7be68d71f9645b789ccdc20561, 60cb70545fbe3c96a0f82eeb54940553, c6c6162cca729c4da879879b126d27c0

References

https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/plugx-a-talisman-to-behold.html