Hive Pro

THREAT ADVISORY

Multiple government entities targeted by China-linked Daxin malware	TA2022044
Threat Level RED	**Published Date –** Mar 2, 2022

A technologically advanced and previously undocumented malware Daxin was used as the advanced persistent threat (APT) weapon by China-linked actor against government critical infrastructures across the globe. This malware can read and write arbitrary files, start and interact with arbitrary processes, and perform advanced lateral movement and stealth.

Daxin malware is a sophisticated rootkit backdoor with complicated, stealthy command and control (C2) features that allowed remote actors to communicate with secured devices that were not directly connected to the internet. This malware communicates with legitimate services through network tunneling and uses daisy-chain communication that provides it the ability to move internally via hops between several linked computers. The malware appears to be designed for the use against hardened targets, allowing actors to dig deeply into targeted networks and exfiltrate data without raising suspicions. Organizations can look for the Indicators of Compromise listed down below.

The Mitre TTPs used by Daxin malware in the current attack are:
TA0007: Discovery
TA0009: Collection
TA0006: Credential Access
T1056: Input Capture
T1049: System Network Connections Discovery

Indicators of Compromise (IoCs)

Type	Value
SHA-256	ea3d773438c04274545d26cc19a33f9f1dbbff2a518e4302addc1279f9950cef, e7af7bcb86bd6bab1835f610671c3921441965a839673ac34444cf0ce7b2164e, e6a7b0bc01a627a7d0ffb07faddb3a4dd96b6f5208ac26107bdaeb3ab1ec8217, cf00e7cc04af3f7c95f2b35a6f3432bef990238e1fa6f312faf64a50d495630a, c791c007c8c97196c657ac8ba25651e7be607565ae0946742a533af697a61878, c0d88db11d0f529754d290ed5f4c34b4dba8c4f2e5c4148866daabeab0d25f9c, b9dad0131c51e2645e761b74a71ebad2bf175645fa9f42a4ab0e6921b83306e3, b0eb4d999e4e0e7c2e33ff081e847c87b49940eb24a9e0794c6aa9516832c427, aa7047a3017190c66568814eb70483bf74c1163fb4ec1c515c1de29df18e26d7, a0ac5f7d41e9801b531f8ca333c31021c5e064f13699dbd72f3dfd429f19bb26, 9c2f3e9811f7d0c7463eaa1ee6f39c23f902f3797b80891590b43bbe0fdf0e51, 96bf3ee7c6673b69c6aa173bb44e21fa636b1c2c73f4356a7599c121284a51cc, 8dafe5f3d0527b66f6857559e3c81872699003e0f2ffda9202a1b5e29db2002e, 8d9a2363b757d3f127b9c6ed8f7b8b018e652369bc070aa3500b3a978feaa6ce, 81c7bb39100d358f8286da5e9aa838606c98dfcc263e9a82ed91cd438cb130d1, 7a7e8df7173387aec593e4fe2b45520ea3156c5f810d2bb1b2784efd1c922376, 7a08d1417ca056da3a656f0b7c9cf6cd863f9b1005996d083a0fc38d292b52e9, 705be833bd1880924c99ec9cf1bd0fcf9714ae0cec7fd184db051d49824cbbf4, 6908ebf52eb19c6719a0b508d1e2128f198d10441551cbfb9f4031d382f5229f

Type	Value
SHA-256	49c827cf48efb122a9d6fd87b426482b7496ccd4a2dbca31ebbf6b2b80c98530, 447c3c5ac9679be0a85b3df46ec5ee924f4fbd8d53093125fd21de0bff1d2aad, 3e7724cb963ad5872af9cfb93d01abf7cd9b07f47773360ad0501592848992f4, 1a5c23a7736b60c14dc50bf9e802db3fcd5b6c93682bc40141d6794ae96138d3, 0f82947b2429063734c46c34fb03b4fa31050e49c27af15283d335ea22fe0555, 08dc602721c17d58a4bc0c74f64a7920086f776965e7866f68d1676eb5e7951f, 06a0ec9a316eb89cb041b1907918e3ad3b03842ec65f004f6fa74d57955573a4, 5c1585b1a1c956c7755429544f3596515dfdf928373620c51b0606a520c6245a, 5bc3994612624da168750455b363f2964e1861dba4f1c305df01b970ac02a7ae, 53d23faf8da5791578c2f5e236e79969289a7bba04eee2db25f9791b33209631, 514d389ce87481fe1fc6549a090acf0da013b897e282ff2ef26f783bd5355a01, 7867ba973234b99875a9f5138a074798b8d5c65290e365e09981cceb06385c54,
MD5	f242cffd9926c0ccf94af3bf16b6e527, bf14555b3a8378ab1276642160b52ffe, 79df0eabbf2895e4e2dae15a4772868c, 6d131a7462e568213b44ef69156f10a5, 4b058945c9f2b8d8ebc485add1101ba5, 47e6ac52431ca47da17248d80bf71389
SHA-1	e5f4ec79c3d4cb85732265ff668f852afff5143f, d417c0be261b0c6f44afdec3d5432100e420c3ed, d02403f85be6f243054395a873b41ef8a17ea279, 53f776d9a183c42b93960b270dddeafba74eb3fb, 37e6450c7cd6999d080da94b867ba23faa8c32fe, 25bf4e30a94df9b8f8ab900d1a43fd056d285c9d

References

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/daxin-backdoor-espionage