SharpStage (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 14:37:47 UTC

SharpStage

aka: LastConn

Actor(s): Molerats

The SharpStage backdoor is a .NET malware with backdoor capabilities. Its name is a derivative of the main activity class called “Stage_One”. SharpStage can take screenshots, run arbitrary commands and downloads additional payloads. It exfiltrates data from the infected machine to a dropbox account by implementing a dropbox client in its code. SharpStage was seen used by the Molerats group in targeted attacks in the middle east.

References

There is no Yara-Signature yet.
