Graphican (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 15:26:35 UTC

According to Symantec, Graphican is an evolution of the known APT15 backdoor Ketrican, which itself was based on a previous malware - BS2005 - also used by APT15. Graphican has the same basic functionality as Ketrican, with the difference between them being Graphican’s use of the Microsoft Graph API and OneDrive to obtain its command-and-control (C&C) infrastructure.

▶ [TLP:WHITE] win_graphican_auto (20251219 | Detects win.graphican.)
