OnionDuke (Malware Family)

By Fraunhofer FKIE

OnionDuke is a new sophisticated piece of malware distributed by threat actors through a malicious exit node on the Tor anonymity network appears to be related to the notorious MiniDuke, researchers at F-Secure discovered. According to experts, since at least February 2014, the threat actors have also distributed the threat through malicious versions of pirated software hosted on torrent websites.

▶ [TLP:WHITE] win_onionduke_auto (20251219 | Detects win.onionduke.)
