Voldemort (Malware Family)

By Fraunhofer FKIE

Voldemort is a backdoor discovered by Proofpoint in August 2024. It is being distributed via phishing E-Mails and makes use of creative techniques such as using saved search files during the infection chain for obfuscation and Google Sheets for C2. While its broad targeting looks like it is related to ecrime, Proofpoint notes that the capabilities of the malware point towards espionage/APT activity.

▶ [TLP:WHITE] win_voldemort_auto (20251219 | Detects win.voldemort.)
