Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:07:58 UTC

Tool: SLOWDRIFT

Names	SLOWDRIFT
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Downloader
Description	(FireEye) SLOWDRIFT is a launcher that communicates via cloud based infrastructure. It sends system information to the attacker command and control and then downloads and executes additional payloads. Lure documents distributing SLOWDRIFT were not tailored for specific victims, suggesting that TEMP.Reaper is attempting to widen its target base across multiple industries and in the private sector. SLOWDRIFT was seen being deployed against academic and strategic targets in South Korea using lure emails with documents leveraging the HWP exploit. Recent SLOWDRIFT samples were uncovered in June 2017 with lure documents pertaining to cyber crime prevention and news stories. These documents were last updated by the same actor who developed KARAE, POORAIM and ZUMKONG.
Information	<https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0218/>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool SLOWDRIFT

Changed	Name	Country	Observed
APT groups			

	Reaper, APT 37, Ricochet Chollima, ScarCruft		2012-Mar 2025	

1 group listed (1 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=1ef291f7-d98a-4335-9f5a-bef15b828929