Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 12:52:06 UTC

Tool: Crutch

Names	Crutch
Category	Malware
Type	Reconnaissance, Backdoor, Exfiltration
Description	(ESET) We were able to capture some of the commands sent by the operators to several Crutch v3 instances, which is helpful to understand the goal of the operation. The operators were mainly doing reconnaissance, lateral movement and espionage. The main malicious activity is the staging, compression and exfiltration of documents and various files, as shown in Figure 1. These are commands manually executed by the operators, thus not showing the automated collection of documents by the drive monitor component described in a later section.
Information	<https://www.welivesecurity.com/2020/12/02/turla-crutch-keeping-back-door-open/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0538/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.crutch>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool Crutch

Changed	Name	Country	Observed	
APT groups				
	Turla, Waterbug, Venomous Bear		1996-2024	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=f1fccfe7-45d8-4a18-ac92-ef5aca3809a7