Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:35:56 UTC

Tool: FALLCHILL

Names	FALLCHILL FallChill RAT
Category	Malware
Type	Backdoor
Description	(US-CERT) According to trusted third-party reporting, HIDDEN COBRA actors have likely been using FALLCHILL malware since 2016 to target the aerospace, telecommunications, and finance industries. The malware is a fully functional RAT with multiple commands that the actors can issue from a command and control (C2) server to a victim's system via dual proxies. FALLCHILL typically infects a system as a file dropped by other HIDDEN COBRA malware or as a file downloaded unknowingly by users when visiting sites compromised by HIDDEN COBRA actors. HIDDEN COBRA actors use an external tool or dropper to install the FALLCHILL malware-as-a-service to establish persistence. Because of this, additional HIDDEN COBRA malware may be present on systems compromised with FALLCHILL.
Information	<https://www.us-cert.gov/ncas/alerts/TA17-318A>
MITRE ATT&CK	<https://attack.mitre.org/software/S0181/>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:FALLCHILL>

Last change to this tool card: 22 April 2020

Download this tool card in JSON format

All groups using tool FALLCHILL

Changed	Name	Country	Observed
APT groups			

	Lazarus Group, Hidden Cobra, Labyrinth Chollima		2007-May 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=f8f77e1b-9ae1-46a5-9c4f-60894a677b2b