

# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 11:07:05 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool FlipCreep

## Tool: FlipCreep

Names	FlipCreep
Category	<a href="#">Malware</a>
Type	<a href="#">Backdoor</a> , <a href="#">Downloader</a> , <a href="#">Exfiltration</a>
Description	( <a href="#">ESET</a> ) FlipCreep is another previously undocumented backdoor written in C# that has a very similar flow of execution as the other backdoors that we have described: it reads commands from orders.txt – a text file stored on an FTP server operated by POLONIUM – and can upload or download files from the server.
Information	< <a href="https://www.welivesecurity.com/2022/10/11/polonium-targets-israel-creepy-malware/">https://www.welivesecurity.com/2022/10/11/polonium-targets-israel-creepy-malware/</a> >

Last change to this tool card: 18 November 2022

Download this tool card in [JSON](#) format

### All groups using tool FlipCreep

Changed	Name	Country	Observed
<b>APT groups</b>			
	<a href="#">Polonium</a>		2022-Sep 2022

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

---

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=a36f16f7-1276-4601-b7ba-d4cac896b48b>