

# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:55:49 UTC

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


## Tool: PapaCreep

Names	PapaCreep
Category	<a href="#">Malware</a>
Type	<a href="#">Backdoor</a>
Description	( <a href="#">ESET</a> ) PapaCreep is a previously undocumented custom backdoor written in C++ that can receive and execute commands from a remote server via TCP sockets. First seen in September 2022, this is the first backdoor used by POLONIUM that was not written in C# or PowerShell.
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 PapaCreep

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=6a59a550-12bb-4bd8-9894-d5b8adc5ad9d>