

# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:00:48 UTC

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

## Tool: Voldemort

Names	Voldemort
Category	<a href="#">Malware</a>
Type	<a href="#">Backdoor</a>
Description	<a href="#">(Proofpoint)</a> Voldemort is a custom backdoor written in C. It has capabilities for information gathering and to drop additional payloads. Proofpoint observed Cobalt Strike hosted on the actor's infrastructure, and it is likely that is one of the payloads that would be delivered.
Information	< <a href="https://www.proofpoint.com/us/blog/threat-insight/malware-must-not-be-named-suspected-espionage-campaign-delivers-voldemort">https://www.proofpoint.com/us/blog/threat-insight/malware-must-not-be-named-suspected-espionage-campaign-delivers-voldemort</a> >
Malpedia	< <a href="https://malpedia.caad.fkie.fraunhofer.de/details/win.voldemort">https://malpedia.caad.fkie.fraunhofer.de/details/win.voldemort</a> >

Last change to this tool card: 27 December 2024

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

### All groups using tool Voldemort

Changed	Name	Country	Observed	
<b>APT groups</b>				
	<a href="#">APT 41</a>		2012-Jul 2025	

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

---

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=f5eda429-8c76-4cd5-8a16-749c0dcbd6fb>