

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:52:59 UTC

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

Tool: Volgmer

Names	Volgmer Manuscript
Category	Malware
Type	Reconnaissance , Backdoor , Info stealer , Exfiltration , Botnet
Description	<p>(US-CERT) Volgmer is a backdoor Trojan designed to provide covert access to a compromised system. Since at least 2013, HIDDEN COBRA actors have been observed using Volgmer malware in the wild to target the government, financial, automotive, and media industries.</p> <p>It is suspected that spear phishing is the primary delivery mechanism for Volgmer infections; however, HIDDEN COBRA actors use a suite of custom tools, some of which could also be used to initially compromise a system. Therefore, it is possible that additional HIDDEN COBRA malware may be present on network infrastructure compromised with Volgmer.</p> <p>As a backdoor Trojan, Volgmer has several capabilities including: gathering system information, updating service registry keys, downloading and uploading files, executing commands, terminating processes, and listing directories. In one of the samples received for analysis, the US-CERT Code Analysis Team observed botnet controller functionality.</p>
Information	<p><https://www.us-cert.gov/ncas/alerts/TA17-318B></p> <p><https://securelist.com/operation-applejeus/87553/></p> <p><https://asec.ahnlab.com/en/57685/></p>
MITRE ATT&CK	< https://attack.mitre.org/software/S0180/ >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.volgmer >
AlienVault OTX	< https://otx.alienvault.com/browse/pulses?q=tag:volgmer >

Last change to this tool card: 29 November 2023

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

All groups using tool Volgmer

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=4bfc72e1-fc12-4f92-93da-19b30ff82786>