Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:04:11 UTC

Tool: KEYPLUG

Names	KEYPLUG ELFSHELF
Category	Malware
Type	Backdoor
Description	(Mandiant) KEYPLUG is a modular backdoor written in C++ that supports multiple network protocols for command and control (C2) traffic including HTTP, TCP, KCP over UDP, and WSS.
Information	<https://www.mandiant.com/resources/blog/apt41-us-state-governments> <https://yoroi.company/en/research/uncovering-an-undetected-keyplug-implant-attacking-industries-in-italy/> <https://hunt.io/blog/keyplug-server-exposes-fortinet-exploits-webshells>
MITRE ATT&CK	<https://attack.mitre.org/software/S1051>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/elf.keyplug>

Last change to this tool card: 27 June 2025

Download this tool card in JSON format

All groups using tool KEYPLUG

Changed	Name	Country	Observed	
APT groups				
	APT 41		2012-Jul 2025	
	RedGolf		2014	

2 groups listed (2 APT, 0 other, 0 unknown)