

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:58:39 UTC

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



Tool: ShadowPad Winnti

Names	ShadowPad Winnti POISONPLUG.SHADOW XShellGhost
Category	Malware
Type	Backdoor
Description	(Kaspersky) ShadowPad: How Attackers hide Backdoor in Software used by Hundreds of Large Companies around the World.
Information	<p><https://www.kaspersky.com/about/press-releases/2017_shadowpad-how-attackers-hide-backdoor-in-software-used-by-hundreds-of-large-companies-around-the-world></p> <p><https://securelist.com/shadowpad-in-corporate-networks/81432/></p> <p><https://cdn.securelist.com/files/2017/08/ShadowPad_technical_description_PDF.pdf></p> <p><https://st.drweb.com/static/new-www/news/2020/october/Study_of_the_ShadowPad_APT_backdoor_and_its_relation_to_PlugX_en.pdf></p> <p><https://labs.sentinelone.com/shadowpad-a-masterpiece-of-privately-sold-malware-in-chinese-espionage/></p> <p><https://www.secureworks.com/research/shadowpad-malware-analysis></p> <p><https://www.trendmicro.com/en_us/research/25/b/updated-shadowpad-malware-leads-to-ransomware-deployment.html></p>
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.shadowpad >

Last change to this tool card: 22 February 2025

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

All groups using tool ShadowPad Winnti

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

	Bronze Butler , Tick , RedBaldNight , Stalker Panda		2006-Apr 2021	
	Earth Krahang		2022	
	Earth Lusca		2019-Sep 2024	
	Icefog , Dagger Panda		2011-2018/2019	
	Mustang Panda , Bronze President		2012-Jun 2025	
	RedEcho		2020	
	RedFoxtrot		2014-Aug 2021	
	RedHotel , TAG-22		2021-2022	
	Space Pirates		2017-Nov 2024	
	TAG-38		2021	
	Tonto Team , HartBeat , Karma Panda		2009-Apr 2023	
	Tropic Trooper , Pirate Panda , APT 23 , KeyBoy		2011-Jun 2023	
	Velvet Ant		2023-Jul 2024	

14 groups listed (14 APT, 0 other, 0 unknown)

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=0eedd5c2-57d7-447c-954d-e0e2ade187dc>