Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 10:57:56 UTC

Tool: Winos

Names	Winos
Category	Malware
Type	Backdoor, Info stealer, Keylogger, Loader, Exfiltration
Description	(Trend Micro) The final payload of this attack is the Winos 4.0 implant, which is written in C++ and targets the Windows platform. Winos has features that include file management, distributed denial of service (DDoS) using TCP/UDP/ ICMP/HTTP, full disk search, webcam control, and screen capturing. Additionally, it supports many functionalities including process injection and microphone recording, system and service management, remote shell access, and keylogging functionalities, further enhancing its ability to control and monitor the infected system.
Information	<https://www.trendmicro.com/en_us/research/24/f/behind-the-great-wall-void-arachne-targets-chinese-speaking-user.html> <https://www.fortinet.com/blog/threat-research/winos-spreads-via-impersonation-of-official-email-to-target-users-in-taiwan>

Last change to this tool card: 02 March 2025

Download this tool card in JSON format

All groups using tool Winos

Changed	Name	Country	Observed	
APT groups				
	Void Arachne		2024-Jun 2025	

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