Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 02:10:01 UTC

Tool: Sword2033

Names	Sword2033
Category	Malware
Type	Backdoor, Downloader, Exfiltration
Description	(Palo Alto) Pivoting on the C2 domain, we identified one additional sample that also communicated with yrhsywu2009.zapto[.]org. Similar to the PingPull variant above, this sample was designed to connect to port 8443 over HTTPS. However, analysis of the sample revealed that it's a simple backdoor that we track as Sword2033.
Information	<https://unit42.paloaltonetworks.com/alloy-taurus/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/elf.sword2033>

Last change to this tool card: 22 June 2023

Download this tool card in JSON format

All groups using tool Sword2033

Changed	Name	Country	Observed	
APT groups				
	Gallium		2018-Jun 2022	

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