Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:40:46 UTC

Tool: xPack

Names	xPack NERAPACK
Category	Malware
Type	Backdoor, Remote command, Exfiltration
Description	(Symantec) The backdoor allowed the attackers to run WMI commands remotely, while there is also evidence that they leveraged EternalBlue exploits in the backdoor. The attackers appeared to have the ability to interact with SMB shares, and it's possible that they used mounted shares over SMB to transfer files from attacker-controlled infrastructure. There is also evidence that the attackers were able to browse the web through the backdoor, likely using it as a proxy to mask their IP address.
Information	<https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/china-apt-antlion-taiwan-financial-attacks>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.xpack>

Last change to this tool card: 28 December 2022

Download this tool card in JSON format

All groups using tool xPack

Changed	Name	Country	Observed	
APT groups				
	Antlion		2011	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=499c6ccf-8841-4343-92fe-fa4b37a6fc49