Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:18:30 UTC

Tool: POWERSOURCE

Names	POWERSOURCE
Category	Malware
Type	Backdoor
Description	(FireEye) POWERSOURCE is a heavily obfuscated and modified version of the publicly available tool DNS_TXT_Pwnage. The backdoor uses DNS TXT requests for command and control and is installed in the registry or Alternate Data Streams. Using DNS TXT records to communicate is not an entirely new finding, but it should be noted that this has been a rising trend since 2013 likely because it makes detection and hunting for command and control traffic difficult.
Information	<https://www.fireeye.com/blog/threat-research/2017/03/fin7_spear_phishing.html>
MITRE ATT&CK	<https://attack.mitre.org/software/S0145/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powersource>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool POWERSOURCE

Changed	Name	Country	Observed	
APT groups				
	Carbanak, Anunak		2013-Apr 2023	
	FIN7		2013-Jul 2024	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=bfd159e4-ca5e-493f-a580-a1c803026c5d