Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:34:53 UTC

Tool: Boostwrite

Names	Boostwrite
Category	Malware
Type	Dropper
Description	(FireEye) An in-memory-only dropper that decrypts embedded payloads using an encryption key retrieved from a remote server at runtime. FIN7 has been observed making small changes to this malware family using multiple methods to avoid traditional antivirus detection, including a BOOSTWRITE sample where the dropper was signed by a valid Certificate Authority. One of the analyzed BOOSTWRITE variants contained two payloads: Carbanak and RDFSNIFFER.
Information	<https://www.fireeye.com/blog/threat-research/2019/10/mahalo-fin7-responding-to-new-tools-and-techniques.html>
MITRE ATT&CK	<https://attack.mitre.org/software/S0415/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.boostwrite>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:BOOSTWRITE>

Last change to this tool card: 22 April 2020

Download this tool card in JSON format

All groups using tool Boostwrite

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

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