Threat Group Cards: A Threat Actor Encyclopedia

Tool: WARPRISM

Names	WARPRISM
Category	Malware
Type	Dropper
Description	(FireEye) WARPRISM is a PowerShell dropper that has been observed by Mandiant delivering SunCrypt, Cobalt Strike, and Mimikatz. WARPRISM is used to evade endpoint detection and will load its payload directly into memory. WARPRISM may be used by multiple groups.
Information	<https://www.fireeye.com/blog/threat-research/2021/04/unc2447-sombrat-and-fivehands-ransomware-sophisticated-financial-threat.html>

Last change to this tool card: 15 May 2021

Download this tool card in JSON format

All groups using tool WARPRISM

Changed	Name	Country	Observed	
APT groups				
	Carbanak, Anunak		2013-Apr 2023	
	SunCrypt Gang	[Unknown]	2019-Oct 2020	
	UNC2447	[Unknown]	2020	

3 groups listed (3 APT, 0 other, 0 unknown)