Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 03:00:03 UTC

APT group: WIRTE Group

Names	WIRTE Group *(LAB52)* White Dev 21 *(PWC)* G0090 *(MITRE)*
Country	[Middle East]
Sponsor	Hamas
Motivation	Information theft and espionage, Sabotage and destruction
First seen	2018
Description	(LAB52) The DFIR (Digital Forensics and Incident Response) team of S2 Grupo first identified this actor in August 2018 and since then the follow-up has been carried out during the last few months. This group attacks the Middle East and does not use very sophisticated mechanisms, at least in the campaign started in August 2018 which was monitored. It is considered unsophisticated by the fact that the scripts are unobtrusive, communications go unencrypted by HTTP, they use Powershell (increasingly monitored), and so on. Despite this apparently unsophisticated modus operandi compared to other actors, they manage to infect their victims and carry out their objectives. In addition, as will be seen during the report, the detection rate of some of the scripts in December 2018 by the main antivirus manufacturers is low, an aspect that must be highlighted. We must be aware that once these scripts are executed, it is when the behavior analysis of many solutions will detect them, but this fact has not been studied by LAB52. This actor in all the artifacts analyzed shows his victims a decoy document in Arabic with different themes.
Observed	Sectors: Defense, Government and diplomats. Countries: Egypt, Iraq, Israel, Jordan, Lebanon, Saudi Arabia and Palestinian Authority.
Tools used	EmpireProject, H-Worm, SameCoin, Living off the Land and several VBScript, PowerShell and VBA scripts.

Operations performed	Feb 2024	Hamas-affiliated Threat Actor WIRTE Continues its Middle East Operations and Moves to Disruptive Activity <https://research.checkpoint.com/2024/hamas-affiliated-threat-actor-expands-to-disruptive-activity/>
Information	<https://lab52.io/blog/wirte-group-attacking-the-middle-east/> <https://blog.talosintelligence.com/2018/02/targeted-attacks-in-middle-east.html> <https://securelist.com/wirtes-campaign-in-the-middle-east-living-off-the-land-since-at-least-2019/105044/>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0090/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
