Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:47:06 UTC

APT group: Volatile Cedar

Names	Volatile Cedar *(Check Point)* Dancing Salome *(Kaspersky)* DeftTorero *(Kaspersky)* VolcanicTimber *(?)* Amethyst Rain *(Microsoft)* G0123 *(MITRE)*
Country	Lebanon
Sponsor	State-sponsored, Hezbollah
Motivation	Information theft and espionage
First seen	2012
Description	(Check Point) Beginning in late 2012, the carefully orchestrated attack campaign we call Volatile Cedar has been targeting individuals, companies and institutions worldwide. This campaign, led by a persistent attacker group, has successfully penetrated a large number of targets using various attack techniques, and specifically, a custom-made malware implant codenamed Explosive. This report provides an extended technical analysis of Volatile Cedar and the Explosive malware. We have seen clear evidence that Volatile Cedar has been active for almost 3 years. While many of the technical aspects of the threat are not considered “cutting edge”, the campaign has been continually and successfully operational throughout this entire timeline, evading detection by the majority of AV products. This success is due to a well-planned and carefully managed operation that constantly monitors its victims’ actions and rapidly responds to detection incidents.
Observed	Sectors: Education, Government and Hosting. Countries: Canada, Egypt, Israel, Jordan, Lebanon, Russia, Saudi Arabia, UAE, UK, USA and Palestinian Authority.

Tools used	Adminer, ASPXSpy, Caterpillar, DirBuster, Explosive, GoBuster, JuicyPotato, RottenPotato, SharPyShell.	
Operations performed	Jun 2015	After going public with our findings, we were provided with a new configuration belonging to a newly discovered sample we have never seen before. <https://blog.checkpoint.com/2015/06/09/new-data-volatile-cedar/>
	Early 2020	In early 2020, suspicious network activities and hacking tools were found in a range of companies. <https://www.clearskysec.com/cedar/>
Information	<https://www.checkpoint.com/downloads/volatile-cedar-technical-report.pdf> <https://securelist.com/sinkholing-volatile-cedar-dga-infrastructure/69421/> <https://securelist.com/defttorero-tactics-techniques-and-procedures/107610/>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0123/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
