‘Lebanese Cedar’ APT – ClearSky Cyber Security

Published: 2021-01-28 · Archived: 2026-04-05 23:10:29 UTC

In early 2020, suspicious network activities and hacking tools were found in a range of companies. Comprehensive forensic research of the infected systems revealed a strong connection to a threat actor we call ‘Lebanese Cedar’, ‘Lebanese Cedar’ APT has been operating since 2012. These operations were first discovered by Check-Point researchers and Kaspersky labs in 2015. Since 2015 Lebanese Cedar APT – also referred to as “Volatile Cedar” – maintained a low profile and operated under the radar.

Read the full report: “Lebanese Cedar” APT – Global Lebanese Espionage Campaign Leveraging Web Servers

In the comprehensive forensic research, a new version of the “Explosive” V4 RAT (Remote Access Tool) or “Caterpillar” V2 WebShell was found within the victim’s networks.

Lebanese Cedar Timeline

Based on a modified JSP file browser with a unique string that the adversary used to deploy ‘Explosive RAT’ into the victims’ network, we found some 250 servers that were apparently breached by Lebanese Cedar. This file was installed in vulnerable Atlassian (JIRA) and Oracle 10g servers. In order to install the JSP in the vulnerable server, Lebanese Cedar exploit 1-day publicly known vulnerabilities such as CVE-2012-3152.

Our report reveals a partial list of the companies that the group has attacked. The target companies are from many countries including: The United States, the United Kingdom, Egypt, Jordan, Lebanon, Israel, and the Palestinian Authority. We assess that there are many more companies that have been hacked and that valuable information was stolen from these companies over periods of months and years.

Modified JSP File Browser – Scanned world-wide

According to Check-Point's report, the group is motivated by political and Ideological interests, targeting individuals, companies, and institutions worldwide. We endorse Check Point's strong case attributing Lebanese Cedar APT to the Lebanese government or a political group in Lebanon. Moreover, there are several indications that link Lebanese Cedar APT to the Hezbollah Cyber Unit.

"Caterpillar WebShell" was found in most of the victims we investigated, in many of the systems we also found traces of "Explosive" RAT. We identified the specific open-source JSP file browser that was modified for the hackers' purposes. We found that Lebanese Cedar deployed the payload of Explosive RAT into the victims' network. **Lebanese Cedar is the only known threat actor that uses this code**.

Lebanese Cedar Modus Operandi