Overview of Volatile Cedar intrusion set.

The intrusion set has been publicly released on October 10, 2022. It is also known as "Volatile Cedar" and "Lebanese Cedar". The set's description is: [Volatile Cedar] is a Lebanese threat group that has targeted individuals, companies, and institutions worldwide. [Volatile Cedar] has been operating since 2012 and is motivated by political and ideological interests.

The intrusion set's first activity dates back to February 8, 2021. Last activity associated with it dates back to April 20, 2022. The set is a nation-state actor that is well resourced and persists long term.

Motivation.

The intrusion set's primary motivation is information theft and espionage. The set's secondary motivation is not provided. Its goal is not provided.

Associated campaigns.

No entities found.

Associated victims.

[Unknown Government].

[Unknown Government] has been released on October 20, 2021. The identity's identity class is not provided. The identity's sector is government. Its description is not provided.

[Unknown Education].

[Unknown Education] has been published on October 20, 2021. Its identity class is not provided. The identity's sector is education. Its description is not provided.

Associated MITRE ATT&CK TTPs.

T1505.003 - Web Shell

T1505.003 - Web Shell name is "T1505.003 - Web Shell". The attack pattern's description is

Adversaries may backdoor web servers with web shells to establish persistent access to systems. A Web shell is a Web script that is placed on an openly accessible Web server to allow an adversary to use the Web server as a gateway into a network. A Web shell may provide a set of functions to execute or a command-line interface on the system that hosts the Web server. In addition to a server-side script, a Web shell may have a client interface program that is used to talk to the Web server (e.g. [China Chopper].

Overview of Caterpillar WebShell.

Caterpillar WebShell.

It has been released on January 19, 2022. Its description is:

> [Caterpillar WebShell] is a self-developed Web Shell tool created by the group [Volatile Cedar].

The malware's kill chain phase is not provided.

Associated campaigns.

No entities found.

Associated MITRE ATT&CK TTPs.

T1110 - Brute Force

T1110 - Brute Force name is "T1110 - Brute Force". Its description is

Adversaries may use brute force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained. Without knowledge of the password for an account or set of accounts, an adversary may systematically guess the password using a repetitive or iterative mechanism. Brute forcing passwords can take place via interaction with a service that will check the validity of those credentials or offline against previously acquired credential data, such as password hashes. Brute forcing credentials may take place at various points during a breach. For example, adversaries may attempt to brute force access to [Valid Accounts] within a victim environment leveraging knowledge gathered from other post-compromise behaviors such as [OS Credential Dumping], [Account Discovery], or [Password Policy Discovery]. Adversaries may also combine brute forcing activity with behaviors such as [External Remote Services] as part of Initial Access.

Associated indicators.

No entities found.