Timeline Overview.

From December 10, 2020 to December 7, 2022, 1 tools, 2 malwares, 1 indicators, 2 identities, 1 intrusion sets, 2 attack patterns and 2 locations had been publicly released.

December, 2020.

In December, 2020, 1 malware had been published.

Explosive.

It has been publicly released on December 10, 2020. The malware's description is:

(Check Point) Explosive is implanted within its targets and then used to harvest information. Tracking down these infections was quite a difficult task due to the multiple concealment measures taken by the attackers. The attackers select only a handful of targets to avoid unnecessary exposure. New and custom versions are developed, compiled and deployed specifically for certain targets, and ”radio silence” periods are configured and embedded specifically into each targeted implant.

The malware's kill chain phase is not provided.

June, 2021.

In June, 2021, 1 tool had been published.

Adminer

It has been publicly released on June 15, 2021. The tool's description is not provided.

October, 2021.

In October, 2021, 2 identities had been publicly released.

[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.

January, 2022.

In January, 2022, 1 malwares and 1 indicators had been publicly released.

Caterpillar WebShell.

Caterpillar WebShell has been published on January 19, 2022. Its description is:

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

Its kill chain phase is not provided.

"IP address: 23.29.115.180".

IP address: 23.29.115.180 has been publicly released on January 28, 2022. Its indicator type is not provided. Its description is not provided.

The indicator's pattern type is not provided. Its pattern is not provided.

The indicator's "valid from" time is not provided. The indicator's "valid until" time is not provided.

Its kill chain phase is not provided.

June, 2022.

In June, 2022, 2 location had been published.

United States

The location has been publicly released on June 10, 2022. Its description is not provided.

Jordan

The location has been publicly released on June 10, 2022. Its description is not provided.

October, 2022.

In October, 2022, 1 intrusion set had been published.

“Volatile Cedar”

It has been publicly released on October 10, 2022. The set's aliases are "Volatile Cedar" and "Lebanese Cedar". Its 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 has been first observed on February 8, 2021. The set has been last observed on April 20, 2022. It is a nation-state actor that is well resourced and persists long term.

December, 2022.

In December, 2022, 2 attack patterns had been published.

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.

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].