Timeline of the graph

From 10 December 2020 to 16 December 2022: 2 malwares, 1 indicator, 2 attack-patterns, 2 identities, 1 tool, 3 locations and 1 intrusion-set had been published.

On 10 December 2020, 1 malware had been published.

malware: Explosive
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.. Its kill chain phase is actions on objectives.

On 15 June 2021, 1 tool had been published.

tool: Adminer

On 20 October 2021, 2 identities had been published.

identity: [Unknown Government]

identity: [Unknown Education]

On 19 January 2022, 1 malware had been published.

malware: Caterpillar WebShell
The malware's description is: [Caterpillar WebShell] is a self-developed Web Shell tool created by the group [Volatile Cedar]. .

On 28 January 2022, 1 indicator had been published.

ipv4-addr: 23.29.115.180

On 10 June 2022, 2 locations had been published.

location: United States
The location's associated country is US.

location: Jordan
The location's associated country is JO.

On 10 October 2022, 1 intrusion-set had been published.

intrusion-set: Volatile Cedar
The set's aliases are Volatile Cedar and Lebanese Cedar. The primary motivation of the group is information theft and espionage. The group was observed for the first time on 8 February 2021 and for the last time on 20 April 2022. The intrusion-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..

On 7 December 2022, 2 attack-patterns had been published.

attack-pattern: 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] Web shell client)..

attack-pattern: T1110 - Brute Force
The attack-pattern's 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..

On 16 December 2022, 1 location had been published.

location: Russian Fed
The location's description is: Russia.