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
According to Check Point, the malware is designed to implant itself within targeted systems, harvest sensitive information, and evade detection through a series of concealment measures. The attackers carefully select a limited number of targets and tailor specific versions of the malware for each one. They also implement "radio silence" periods to avoid detection. The malware's ultimate goal is to carry out actions on objectives, leading to a highly effective kill chain.

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 is identified as [Caterpillar WebShell], which originates from the group called [Volatile Cedar] and is a self-developed Web Shell tool.

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
Also known as Volatile Cedar and Lebanese Cedar, this group is primarily focused on information theft and espionage. They were first observed in action on February 8th, 2021 and were last seen on April 20th, 2022. Known for targeting individuals, companies, and institutions globally, the group, also referred to as [Volatile Cedar], has been active since 2012 and is driven by both political and ideological interests.

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

attack-pattern: T1505.003 - Web Shell
Adversaries have been known to implant web shells in web servers as a way of gaining permanent access to a system. Essentially, a web shell is a script that is placed on a public web server and allows the adversary to use it as a gateway into a network. With this kind of access, an adversary may be able to execute commands or access a command-line interface on the system hosting the Web server. Some web shells even come equipped with a client interface, such as the China Chopper web shell client, which enables adversaries to communicate directly with the Web server.

attack-pattern: T1110 - Brute Force
The attack pattern in question involves adversaries utilizing brute force techniques to gain access to accounts that have unknown passwords or have password hashes that have been obtained. These techniques involve an iterative or repetitive mechanism to systematically guess passwords for a particular account or set of accounts. Brute force attacks can happen in two ways - either through service interaction, which checks the validity of the credentials, or offline against previously acquired credential data like password hashes. Brute force credential attacks can occur at various points during a security breach. For example, adversaries may attempt to brute force access to valid accounts within a target environment by leveraging data obtained from other post-compromise behaviors like OS credential dumping, account discovery, or password policy discovery. Additionally, adversaries may combine brute forcing with other techniques like external remote services as a means of initial access to the target environment.

On 16 December 2022, 1 location had been published.

location: Russian Fed

The location's description is: Russia.