Report on Volatile Cedar

Overview

Volatile Cedar, also known as Lebanese Cedar and operating under these names as an intrusion-set, is primarily focused on information theft and espionage. It was first detected on February 8th, 2021 and last observed on April 20th, 2022. This threat group, which has been in existence since 2012, targets individuals, companies, and institutions globally, motivated by political and ideological interests.

Relationships

The group specifically focuses on targeting unknown educational and governmental institutions located in both the United States and Jordan. To carry out their malicious activities, they employ the use of Caterpillar WebShell and Explosive malware, as well as the Adminer tool. Their preferred attack-pattern is T1505.003 - Web Shell.

Stats

The set is related to these malwares:
- 6 backdoors (RottenPotato, Caterpillar, JuicyPotato, Explosive, ASPXSpy and SharPyShell)
- 2 info stealers (Caterpillar and Explosive)
- 2 downloaders (Caterpillar and SharPyShell)
- 1 reconnaissance (Caterpillar)

It is related to these tools:
- 2 reconnaissances (DirBuster and GoBuster)

The group is related to these attack-patterns:
- 1 command-and-control (T1105 - Ingress Tool Transfer)
- 1 persistence (T1505.003 - Web Shell)
- 1 initial-access (T1190 - Exploit Public-Facing Application)
- 2 reconnaissances (T1595.003 - Wordlist Scanning and T1595.002 - Vulnerability Scanning)

Mitre Matrix

Name	Tactic	ATT&CK Code	Description
T1505.003 - Web Shell	persistence		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.(Citation: volexity_0day_sophos_FW) 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](https://attack.mitre.org/software/S0020) Web shell client).(Citation: Lee 2013)

IOCs

Type	Value
ipv4-addr	23.29.115.180

Useful Resources

Useful material to know better the set can be found at: https://attack.mitre.org/groups/G0123, https://www.clearskysec.com/wp-content/uploads/2021/01/Lebanese-Cedar-APT.pdf and https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2015/03/20082004/volatile-cedar-technical-report.pdf.

Report on Caterpillar WebShell

Overview

Caterpillar WebShell is a type of malware that is also known as Caterpillar WebShell. This particular malware is a self-developed Web Shell tool that was created by the group known as Volatile Cedar.

This malware was first observed on February 10, 2021 and the last known sighting of it occurred on April 27, 2021.

Relationships

The intrusion-set Volatile Cedar uses attack-patterns T1110 - Brute Force, as their primary approach for Caterpillar WebShell distribution.

Stats

Caterpillar webshell is related to these attack-patterns:
- 1 credential-access (T1110 - Brute Force)
- 1 exfiltration (T1041 - Exfiltration Over C2 Channel)
- 1 execution (T1059.003 - Windows Command Shell)
- 1 collection (T1005 - Data from Local System)
- 1 command-and-control (T1105 - Ingress Tool Transfer)
- 2 defense-evasions (T1112 - Modify Registry and T1014 - Rootkit)
- 8 discoveries (T1082 - System Information Discovery, T1007 - System Service Discovery, T1046 - Network Service Discovery, T1033 - System Owner/User Discovery, T1083 - File and Directory Discovery, T1016 - System Network Configuration Discovery, T1069.001 - Local Groups and T1057 - Process Discovery)

Mitre Matrix

Name	Tactic	ATT&CK Code	Description
T1110 - Brute Force	credential-access		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](https://attack.mitre.org/techniques/T1078) within a victim environment leveraging knowledge gathered from other post-compromise behaviors such as [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), [Account Discovery](https://attack.mitre.org/techniques/T1087), or [Password Policy Discovery](https://attack.mitre.org/techniques/T1201). Adversaries may also combine brute forcing activity with behaviors such as [External Remote Services](https://attack.mitre.org/techniques/T1133) as part of Initial Access.

Useful Resources

Useful material to know better Caterpillar WebShell can be found at: https://attack.mitre.org/software/S0572, https://www.clearskysec.com/wp-content/uploads/2021/01/Lebanese-Cedar-APT.pdf and https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2015/03/20082004/volatile-cedar-technical-report.pdf.