DriftingCloud APT Group Exploits Zero-Day In Sophos Firewall

Published: 2022-06-17 · Archived: 2026-04-05 15:44:40 UTC

Cybersecurity researchers have revealed that Sophos Firewall has been actively exploited by DriftingCloud APT group since early March. Apparently, the attacks started long before the CVE-2022-1040 vulnerability was patched, affecting v18.5 and older versions of Sophos Firewall. CVE-2022-1040 is an **authentication bypass vulnerability** in the Web Admin and User Portal that allows threat actors to perform RCE, leading to a breach of web servers.

Sophos Firewall released a security advisory on 25th March. The advisory includes remediation methods concerning CVE-2022-1040, which has a CVSS score of 9.8.

Who Is DriftingCloud?

According to Volexity's research, the attack is associated with a **Chinese APT group named DriftingCloud**. The APT group opened a backdoor on the firewall back in March. The same APT group might be related to an attack last December when Zimbra was exploited using a zero-day vulnerability. It was a spear-phishing campaign, and the attackers targeted the European government and media organizations. The phishing lasted two weeks, and the hotfix came in February, two months later.

DriftingCloud isn't the newest threat. Sophos Firewall was also targeted in April 2020. It was due to yet another **zero-day vulnerability**. The entry vector was SQL injection, and the attackers deployed the "Asnarok" trojan on devices. A write-up was published after the event to elaborate on attack details.

How Did The Attack Happen?

DriftingCloud APT Group's attack flow (Source: Veloxity)

First Stage

In the first stage of the attack, the threat actors breach the firewall and load the web shell. In this step, the attacker sends **malicious web requests** containing "base64 string".

By searching the base64 string values in the device's disk memory in these sent requests, attackers can make changes to the "/usr/share/webconsole/WEB-INF/classes/cyberoam/sessionmanagement/SessionCheckFilter.class" file.

Requests sent by DriftingCloud APT Group

The modified file is a legitimate file included in Sophos Firewalls. When the file runs, it calls the "SessionCheckHelper" file with the correct parameters, thus verifying whether the user has a valid session. The SessionCheckHelper file is called whenever a request is made to any component of the Sophos Firewall interface. The attacker has modified this file to include his own logical expressions.

The threat actor has taken some actions to ensure persistence on the **firewall**. These actions are as follows:

- Creating VPN user accounts and associated certificate pairs in the firewall
- Writing and running /conf/certificate/pre_install.sh on device disk to **breach** firewall
- When the “pre_install.sh” file is run, it downloads a binary file. After running the binary file, it is deleted from the disk.

Second Stage

In the second stage of the attack, the attacker changes the DNS responses using the firewall he violated. Thus, a MITM (man-in-the–middle) attack can be made on target websites. Modified DNS responses are intended to obtain the admin domains of the victim organization. In this way, the attacker obtained the **user credentials** and session cookies from administrative access to the website’s content management system (CMS).

The cookie information obtained allows the WordPress admin panel page to be accessed without sending a username and password. Then the page used to download and add the plugin can be accessed.

The attacker installed the **File Manager** extension on the victim system to load a PHP file. Then he disabled this plugin.

Using the attacker’s web server access, the open-source malware families PupyRAT, Pantegana, and Sliver were installed on the victim system.

DriftingCloud TTPs

TTPs of DriftingCloud APT Group

DriftingCloud IoCs

File indicators

Network Indicators

URLs

Domains

Additional Suspicious Domains

IPs

Filesystem Paths

In addition, Volexity provided a set of YARA rules that may alert users to potentially dangerous conduct resulting from this kind of attack.

With SOCRadar® Free Edition, you'll be able to:

- Prevent Ransomware attacks with Free External Attack Surface Management
- Get Instant alerts for fraudulent domains against phishing and BEC attacks
- Monitor Deep Web and Dark Net for threat trends
- Get vulnerability intelligence when a critical zero-day is disclosed
- Get IOC search & APT tracking & threat hunting in one place
- Get notified with data breach detection

Free for 12 months for one corporate domain and 100 auto-discovered digital assets.
Get Free Access.
