Hive Pro

Threat Level

Red

THREAT ADVISORY

ATTACK REPORT

DriftingCloud exploits zero-day in Sophos firewall

Date of Publication

June 21, 2022

Admiralty code

A2

TA Number

TA2022130

Summary

The Chinese APT actor DriftingCloud exploits the RCE vulnerability in Sophos firewall to take over the entire network

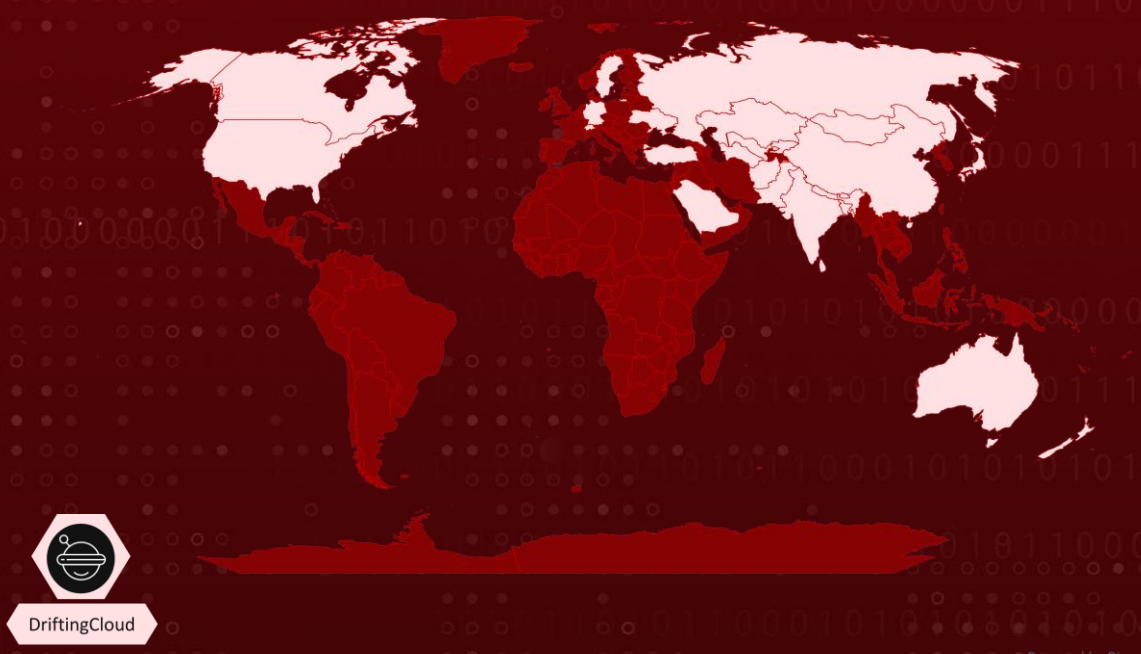
CVE

CVE	NAME	PATCH
CVE-2022-1040	Authentication Bypass Vulnerability	✓

Potential MITRE ATT&CK TTPs

TA0003 Persistence	**T1505** Server Software Component	**TA0004** Privilege Escalation	**T1574** Hijack Execution Flow
TA0002 Execution	**T1059** Command and Scripting Interpreter	**TA0005** Defense Evasion	**T1140** Deobfuscate/Decode Files or Information
TA0006 Credential Access	**T1040** Network Sniffing	**T1027** Obfuscated Files or Information	**TA0011** Command and Control
T1105 Ingress Tool Transfer	**TA0009** Collection	**T1557** Adversary-in-the-Middle	

Actor Map


DriftingCloud
Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Technical Details

#1 DriftingCloud is using a well-known zero-day vulnerability in Sophos firewall, tracked as CVE-2022-1040 to gain access to the firewall network. After exploiting this flaw, they create a web backdoor for persistence.

#2 The APT then modifies the DNS response to perform Man-In-The-Middle (MITM) attack. This allows them to steal cookies and credentials and access the CMS admin page and other network devices using those credentials

#3 DriftingCloud deploys three malwares named PupyRAT, Pentagana, Silver in device for further remote access.

Vulnerability Details

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-1040	Sophos Firewall v18.5 MR3 (18.5.3) and older	cpe:2.3:h:sophos:xg_firewall:-:*:*:*:*:*:*:*	CWE-287

Actor Detail

NAME	ORIGIN	MOTIVE	TARGET LOCATIONS	TARGET INDUSTRIES
DriftingCloud	China	Information theft and Espionage	China, Kazakhstan, Turkey, Kyrgyzstan, Uzbekistan, Pakistan, Saudi Arabia, Australia, Russia, Turkmenistan, Afghanistan, Sweden, Canada, United States, Japan, Germany, Mongolia, Ukraine, Bhutan, India, Nepal, Switzerland, New Zealand, and South Asia	Government

Indicator of Compromise (IOC)

TYPE	VALUE
MD5	ba8f0224307156e670621dd151dffdf1, 284c8ed417d45a15c89ffe65575cf8ac
SHA1	7d110a02f52934dfa15769b9f163cdeb091d352c, 02c6bc4f770baa5fbc21aa0fa57cf9678aa730fe,
SHA256	ce2e935b885c3de97df6e65e29b24f2b07a794ffd9c20eb205307a5e780207bc, df41c20dbbee0d1a28cb151c29fff1e2e22bd7ba89ee8e3d47e7d15f56d89e4e
IP Address	180.149.38[.]136 95.85.71[.]23 95.85.71[.]20 5.188.228[.]40 209.250.231[.]67 158.247.200[.]24 192.248.152[.]58 185.82.218[.]66
Hostname	Akamprod[.]com u2d.servusers[.]com Servusers[.]com Googleanalytics[.]proxydns.com

Patch Details

Update to versions v19.0 GA and v18.5 MR4 (18.5.4)

References

https://www.volexity.com/blog/2022/06/15/driftingcloud-zero-day-sophos-firewall-exploitation-and-an-insidious-breach/

https://thehackernews.com/2022/06/chinese-hackers-exploited-sophos.html

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.

At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

June 21, 2022. 6:45 AM

More at www.hivepro.com