Hive Pro

Threat Level

Red

THREAT ADVISORY

ATTACK REPORT

BlueSky ransomware incorporates Multithreading to expedite encryption.

Date of Publication	Admiralty Code	TA Number
August 12, 2022	A1	TA2022172

Summary

BlueSky ransomware is actively targeting businesses and demanding a ransom. It appears that they have ties with the Conti ransomware group. The malware is now primarily targeting Windows hosts and uses multithreading to encrypt data on the host for faster encryption.

CVE Table

CVE	NAME	PATCH
CVE-2020-0796	Windows SMBv3 Client/Server Remote Code Execution Vulnerability	✓
CVE-2021-1732	Windows Win32k Elevation of Privilege Vulnerability	✓

Potential MITRE ATT&CK TTPs

TA0040 Impact	**T1486** Data Encrypted for Impact	**TA0005** Defense Evasion	**T1140** Deobfuscate/Decode Files or Information
T1027 Obfuscated Files or Information	**TA0007** Discovery	**T1083** File and Directory Discovery	**T1135** Network Share Discovery
TA0002 Execution	**T1106** Native API		

Technical Details

#1

BlueSky ransomware is initially dropped via PowerShell script start.ps1 onto the intended system. Following the extraction, another PowerShell script named stage.ps1 downloads a bunch of payloads based on the victim's system privileges.

#2

A modified version of JuicyPotato for versions before Windows 10 is downloaded and executed if the victim's machine is the least privileged.

#3

If the host is running Windows 10 or later, the script will download and run ghost.exe and spooler.exe to exploit local privilege escalation vulnerabilities CVE-2020-0796 and CVE-2021-1732, respectively.

#4

After gaining enhanced privileges, stage.ps1 downloads the BlueSky ransomware payload and stores it locally to the filesystem as javaw.exe, attempting to impersonate a legitimate Windows application.

#5

The ransom note is dropped as a text file titled DECRYPT FILES BLUESKY [.]txt and an HTML file named DECRYPT FILES BLUESKY [.]html in a local directory where it has successfully encrypted files and appended them with the file extension .bluesky.

Vulnerability Details

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2020-0796	Windows 10: 1903 - 1909 and Windows Server 2019: 1903 - 1909	cpe:2.3:o:microsoft:windows_10:-:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server_2016:-:*:*:*:*:*:*:*	CWE-119
CVE-2021-1732	Windows: 10 - 2004 and Windows Server: 2019 - 2004	cpe:2.3:o:microsoft:windows_10:-:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server_2019:-:*:*:*:*:*:*:*	CWE-269

Indicator of Compromise (IOC)

TYPE	VALUE
Registry Paths	HKCU\Software\<32-byte hex string>\completed HKCU\Software\<32-byte hex string>\recoveryblob HKCU\Software\<32-byte hex string>\x25519_public
SHA-256	2280898cb29faf1785e782596d8029cb471537ec38352e5c17cc263f1f52b8ef 3e035f2d7d30869ce53171ef5a0f761bfb9c14d94d9fe6da385e20b8d96dc2fb 840af927adbfdeb7070e1cf73ed195cf48c8d5f35b6de12f58b73898d7056d3d b5b105751a2bf965a6b78eeff100fe4c75282ad6f37f98b9adcd15d8c64283ec

TYPE	VALUE
SHA-256	c75748dc544629a8a5d08c0d8ba7fda3508a3efdaed905ad800ffddbc8d3b8df e75717be1633b5e3602827dc3b5788ff691dd325b0eddd2d0d9ddcee29de364f 08f491d46a9d05f1aebc83d724ca32c8063a2613250d50ce5b7e8ba469680605 969a4a55bb5cabc96ff003467bd8468b3079f5c95c5823985416c019eb8abe2f c4e47cba1c5fedf9ba522bc2d2de54a482e0ac29c98358390af6dadc0a7d65ce Cf64c08d97e6dfa5588c5fa016c25c4131ccc61b8deada7f9c8b2a41d8f5a32c 6c94a1bc67af21cedb0bffac03019dbf870649a182e58cc5960969adf4fbdd48
URLs	hxxps://kmsauto[.]us/someone/l[.]exe hxxps://kmsauto[.]us/app1[.]bin hxxps://kmsauto[.]us/server[.]txt hxxps://kmsauto[.]us/encoding[.]txt hxxps://kmsauto[.]us/all[.]txt hxxps://kmsauto[.]us/someone/spooler[.]exe hxxps://kmsauto[.]us/sti/sti[.]bin hxxps://kmsauto[.]us/someone/potato[.]exe hxxps://kmsauto[.]us/someone/ghost[.]exe hxxps://kmsauto[.]us/someone/start[.]ps1 http://ccpyeuptrlatb2piua4ukhnhi7lrxgerrcrj4p2b5uhbzqm2xgdjaqid[.]onion

Patch Links

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-0796

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-1732

References

https://unit42.paloaltonetworks.com/bluesky-ransomware/

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

August 12, 2022 • 6:27 AM

More at www.hivepro.com