VEDERE LABS

Night Sky Ransomware

A short-lived threat from a long-lived threat actor

April 12, 2022

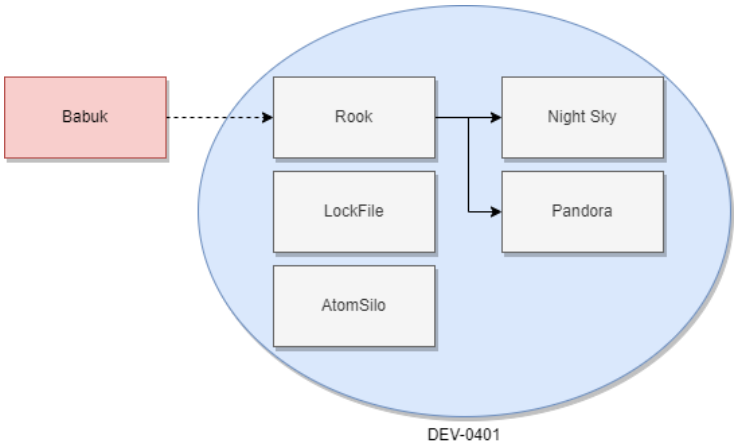
Contents

1. Executive Summary

The Night Sky ransomware was first reported by MalwareHunterTeam on January 1, 2022. Victims were asked to contact the attackers on contact[.]nightsky[.]cyou to pay for the ransom. If the victims refused to pay, attackers threatened to expose their data on a leak site. This is known as a *double extortion ransomware,* which was first used by Maze and is now used by several ransomware groups. Previous reports suggest that Night Sky has been distributed by exploiting the Log4Shell vulnerability and is connected to a threat actor based in China, which is tracked by Microsoft as DEV-0401.

The Night Sky campaign was short and compromised two victims in Bangladesh and Japan. Currently, the Night Sky infrastructure is offline, which suggests the threat actor may have rebranded.

Night Sky provides an interesting view into the relationships among several ransomware families. Night Sky was discovered to be a fork of a ransomware family called Rook, which was itself derived from the leaked source code of Babuk and deployed by the same threat actor that used LockFile and AtomSilo, which are so close they share the same decryption tool. Shortly after the Night Sky and Rook leak sites went offline in January 2022, a new gang named Pandora appeared online, claiming one of the victims of Rook as its own – the Japanese automotive parts manufacturer Denso – and using malware samples that are still detected as Rook. The Pandora leak site (vbfqeh5nugm6r2u2qvghsdxm3fotf5wbxb5ltv6vw77vus5frdpuaiid[.]onion) is still active as of this writing. Currently, they claim a total of seven victims. These relationships are depicted in the figure below.



In this report, we analyze the behavior of the Night Sky malware on two samples obtained from existing reports (Section 2), present a list of IoCs extracted from our analysis (Section 3) and discuss mitigation (Section 4). To the best of our knowledge, there is no tool available to decrypt the targeted files. In addition, their website is no longer available, so there is no way to obtain the decryption keys.

2. Technical Analysis

Night Sky samples first appeared at the beginning of January 2022. They are executables designed to run on Windows x64. The files disguised themselves under different names such as **update.txt**, **unknown** and **wzl6rs0i6.dll** (see VirusTotal). The malware is written in C/C++ using Microsoft Visual C 64 bit Universal and has the size of 5.7 MB, which is relatively large compared to the average size of a malware sample.

Figure 1 shows that the malware has a few abnormal section names and that the entry point of the executable lies outside of standard sections. This suggests the malware is packed. A previous analysis identified that VMProtect was used to pack the malware.

PE file contains sections with non-standard names	Hide sources
Source: 6v9g3tZszP.exe	Static PE information: section name: .2fU0
Source: 6v9g3tZszP.exe	Static PE information: section name: .2fU1
Source: 6v9g3tZszP.exe	Static PE information: section name: .2fU2

Entry point lies outside standard sections	Hide sources
Source: initial sample	Static PE information: section where entry point is pointing to: .2fU2

Figure 1: Abnormal section names of the Night Sky sample

In addition, the presence of the Windows **LoadLibraryA** and **GetProcAddress** APIs in Figure 1 suggests the malware imports other functions at runtime, which hinders static analysis. Figure 2 shows the malware also delays its execution to hinder automated dynamic analysis by triggering the **SleepEx** function to remain idle for a minute.

May sleep (evasive loops) to hinder dynamic analysis		
Source: C:\Users\user\Desktop\Pj7FvnkZ2S.exe TID: 2692	Thread sleep time: -60000s >= -30000s	Jump to behavior

Figure 2: The malware tries to delay the execution to hinder dynamic analysis

Although the Windows API's **IsDebuggerPresent** function is present in the malware, it could be run with the x64dbg debugger.

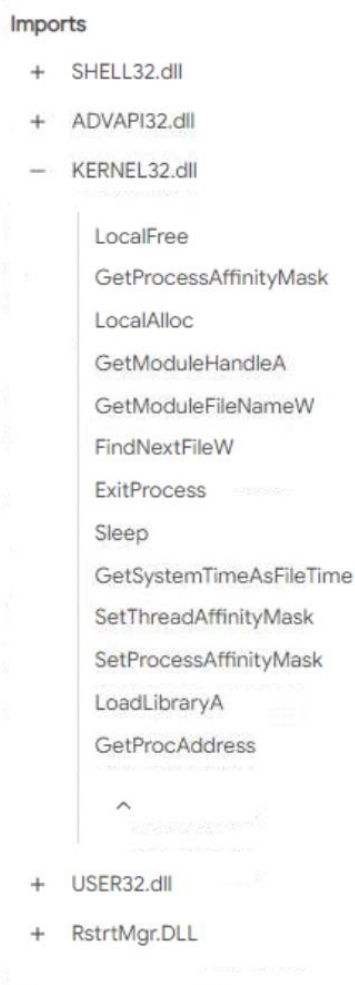


Figure 3: The malware uses LoadLibrary and GetProcAddress for dynamic imports

The malware enumerates the files in the victim's machine using the function **FindNextFileW** (shown in Figure 3) and encrypts them. However, the malware skips 31 folders (e.g., Program Files) and file types (e.g., dll) as shown in Figure 4. This behavior is confirmed by running the ransomware in a physical Windows host.

```
aAppdata:
                text "UTF-16LE", 'AppData',0
aBoot:
                text "UTF-16LE", 'Boot',0
                align 20h
aWindows:
                text "UTF-16LE", 'Windows',0
aWindowsOld:
                text "UTF-16LE", 'Windows.old',0
aTorBrowser:
                text "UTF-16LE", 'Tor Browser',0
aInternetExplor:
                text "UTF-16LE", 'Internet Explorer',0
                align 8
aGoogle:
                text "UTF-16LE", 'Google',0
                align 8
aOpera:
                text "UTF-16LE", 'Opera',0
                align 8
aOperaSoftware:
                text "UTF-16LE", 'Opera Software',0
                align 8
aMozilla:
                text "UTF-16LE", 'Mozilla',0
aMozillaFirefox:
                text "UTF-16LE", 'Mozilla Firefox',0
aRecycleBin:
                text "UTF-16LE", '$Recycle.Bin',0
                align 8
aProgramdata:
                text "UTF-16LE", 'ProgramData',0
aAllUsers:
                text "UTF-16LE", 'All Users',0
```

Figure 4: List of folders and files Night Sky skips the encryption. Source: Netskope

The encrypted files are then appended with an extension **".nightsky"**. Figure 5 shows an example of an encrypted file.

C:\Users\Default\NTUSER.DAT.LOG1.nightsky

Process:	C:\Users\user\Desktop\Pj7FvnkZ2S.exe
File Type:	data
Category:	dropped
Size (bytes):	192016
Entropy (8bit):	7.999077239802471
Encrypted:	true
SSDEEP:	3072:L011X7plZl8Hi1wm/dsqFqcje+cKvMjUoBV2nzPqlFmvLOx0a+1TEuie:L011XNlb8g6qscyiY32nzPqlv0Bouie
MD5:	DF83312939486F6BA43A32DBA9493003
SHA1:	BBD9BC024E3C1A680BB25D097F030BE8621BC0CD
SHA-256:	8DB4A92BA58DEB2D835CBFF88926F3C33F3CCB8548F053A94336546E41CE56C3
SHA-512:	C54A97B53A160DA53A1541B52A7F0D0C3951B6B107703758DADD57EF153EB15FA10A949C7922D197A85D4C68F067E0144D676DCE3422A9B5E49F900B69A0FD80
Malicious:	false
Preview:	hWr.....B4~f.L....z.^..C.....Q.}=..A.A...j.Y..K.i..-........u..v~..>.4>x%..D~.NR.2.mT.; ..-.......^._8,...41T3.......).@..e.{..A..C.K...B....3:1...'...a.6.w^..W....I.f.Co.&S.a+.. 1!|v.@..c.O~.....%.lo{i".R.~+6s.O....Ye..xF.n.`.....8'.,.WF..~.o^...#91J.T.... .e.,..[.:.(....`.~%......*....2......dK....X..2.......a/i....|'f.LwOGG.k....T..P..3w&.=A..4...K.. K.........J..;H..=..{2.`.b...].....V..Int.;.S..+~F......00....N.[.A@.....A...B*...Q P...I,.{a.N.T.........J...{..._.~y.j.......d.t....:<......}._,.<)R....2.B.H. .....VK8.e^.;xf.w..... <..q..|.R..4~.~.........*{a.&<.....{u.l....DJ.R..'..z].*.^4...Q.z8..'(?.Lg..M..u9x...Z...#W.....c...f....g..N...44tb...*.~..a.j.knz.y.c&R..~..^Ih..e|.Q..}..Ju3k...^..4.U..H.... .,....y..F...t.m3..Pf....o.}...@.o8.s`....d.]...}\0.W..l...kI<.d.H>....x,....P..Kc5.v.|P.W.k.........U.w.p&..Q.Bc.WR..........`..Z../.<%"..O./.?yj8..is~/2s.^b.*..!..0.C[.b>&._.v. ..x,.k..>n..u....on....?W.Zs...{. ....Au.>d.T.........L

Figure 5: Example of an encrypted file

The malware drops ransom notes in various folders, including the **Start Menu** folder as shown in Figure 6. The victims would see the ransom note after restarting the system.

Stores files to the Windows start menu directory		Hide sources
Source: C:\Users\user\Desktop\6v9g3tZszP.exe	File created: C:\Documents and Settings\Default\Start Menu\NightSkyReadMe.hta	Jump to behavior
Source: C:\Users\user\Desktop\6v9g3tZszP.exe	File created: C:\Documents and Settings\Default\Start Menu\Programs\NightSkyReadMe.hta	Jump to behavior
Source: C:\Users\user\Desktop\6v9g3tZszP.exe	File created: C:\Documents and Settings\Default\Start Menu\Programs\Accessibility\NightSkyReadMe.hta	Jump to behavior
Source: C:\Users\user\Desktop\6v9g3tZszP.exe	File created: C:\Documents and Settings\Default\Start Menu\Programs\Accessories\NightSkyReadMe.hta	Jump to behavior
Source: C:\Users\user\Desktop\6v9g3tZszP.exe	File created: C:\Documents and Settings\Default\Start Menu\Programs\Maintenance\NightSkyReadMe.hta	Jump to behavior
Source: C:\Users\user\Desktop\6v9g3tZszP.exe	File created: C:\Documents and Settings\Default\Start Menu\Programs\System Tools\NightSkyReadMe.hta	Jump to behavior
Source: C:\Users\user\Desktop\6v9g3tZszP.exe	File created: C:\Documents and Settings\Default\Start Menu\Programs\Windows PowerShell\NightSkyReadMe.hta	Jump to behavior

Figure 6: The ransom note added to Start Menu

In the ransom note shown in Figure 7, Night Sky hackers provide a link to a web chat channel that a victim can join to communicate with them. The channel is currently off. For those victims who refuse to pay the ransom, the hackers threaten to publish their data on a .onion site. The leak site is also offline currently.

Figure 7: A ransom note NightSkyReadMe.hta dropped by Night Sky

The “Steal list” in Figure 7 seemed to be statically set, as our analysis environment did not have the mentioned files. To confirm this hypothesis, we analyzed the malware code. Figure 8 shows that it leverages the Windows’s WriteFile with the ransom note content pointed by the **Buffer** variable.

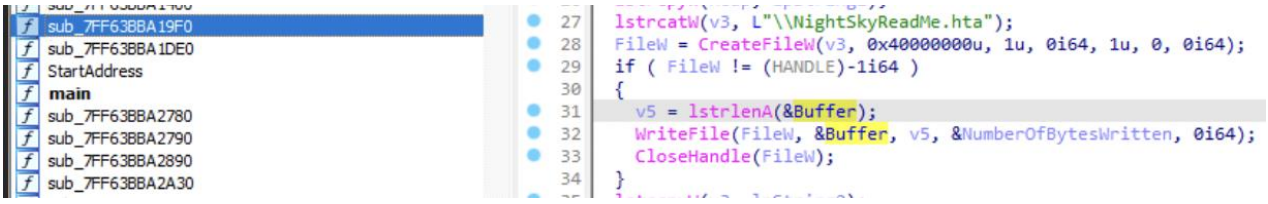


Figure 8: The ransom note is stored in the 'Buffer' variable which points to the data in .rdata

The ransom note is hard coded in the **.rdata** section of the executable. Figure 9 indicates the ransomware does not seem to calculate the actual ransom data in the victim’s machine. This shows that executables are created by dynamically embedding victim information, something that is done by other ransomware such as ALPHV and that makes detection more difficult since file hash IoCs would be different per victim.

```
.rdata:00007FF63BBE2488                 db  32h ; 2
.rdata:00007FF63BBE2489                 db  39h ; 9
.rdata:00007FF63BBE248A                 db  37h ; 7
.rdata:00007FF63BBE248B                 db  47h ; G
.rdata:00007FF63BBE248C                 db  42h ; B
```

Figure 9: A hard-coded string "297GB" in the ransom note

Figure 10 shows that the malware deletes files in the **Recycle Bin** folder before performing other activities.

```
30  SHEmptyRecycleBinA_0(0i64, 0i64, 7u);
31  GetSystemInfo(&SystemInfo);
32  v3 = (4 * SystemInfo.dwNumberOfProcessors) >> 1;
33  v4 = 24 * SystemInfo.dwNumberOfProcessors;
34  dword_7FF63BBF6278 = 24 * SystemInfo.dwNumberOfProcessors;
35  do
36    Heap = RtlAllocateHeap(hHeap, 8u, 8i64 * v4 + 64);
37  while ( !Heap );
38  qword_7FF63BBF6280 = (__int64)Heap;
39  hSemaphore = CreateSemaphoreA(0i64, v4, v4, 0i64);
```

Figure 10: The ransomware deletes all files in the Recycle Bin

The malware creates a mutex **tset123155465463213,** as shown in Figure 11. The mutex is used to avoid re-encrypting files on the infected system. This mutex name can be used to prevent the infection of the ransomware. (See the **Mitgation Recommendations** section at the end).

Creates mutexes	
Source: C:\Users\user\Desktop\Pj7FvnkZ2S.exe	Mutant created: \Sessions\1\BaseNamedObjects\tset123155465463213

Figure 11: The mutex used by Night Sky

Figure 12 shows that the mutex is hard coded and checked in the **main** function using CreateMutexA and OpenMutexA, respectively.

```
if ( !OpenMutexA(0x1F0001u, 0, "tset123155465463213") )
{
  CreateMutexA(0i64, 0, "tset123155465463213");
```

Figure 12: The mutex created by the ransomware

Night Sky uses AES-128-CBC to encrypt files and RSA to encrypt the keys. By looking at the disassembly of the ransomware, we identified the public key stored in the **.data** section shown in Figure 13.

```
.data:00007FF63BBF18F0 aBeginPublicKey db '-----BEGIN PUBLIC KEY-----',0Ah
.data:00007FF63BBF18F0                                         ; DATA XREF: sub_7FF63BBA10F0+100↑o
.data:00007FF63BBF18F0                 db 'MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwetDt+9kp5JJGCb3YrqH',0Ah
.data:00007FF63BBF18F0                 db '48g0rxFIaj5/NjMBvxtpa+7nO/lS0FQXxWJO78dTT6xW/UgVLPK4MvbGeIj17aQF',0Ah
.data:00007FF63BBF18F0                 db 'SqGHbRxTeoPrHufp4sM4J2IQYLc6YLYZMS6XT02rHOjumBJpEKyROQ+df5KU/06o',0Ah
.data:00007FF63BBF18F0                 db 'Rrhljc0Qco+qW8q/xYJQ9VFa87IJM6WM3wsydHVDDeGuWi4/PMUT4/GAa8/WMUYW',0Ah
.data:00007FF63BBF18F0                 db '9Ebw7/hXd/aNX5LykeonN+nkJfbj1fZNTU81tc8Kx4rykLvMVE1H3AaT5ssCBt7p',0Ah
.data:00007FF63BBF18F0                 db 'AFkLLjplOXz3XmhH+J5vm5Ifi7T85j4D6O03qocO2gwezIikCDU2YAOOpJzkb5Ab',0Ah
.data:00007FF63BBF18F0                 db '+wIDAQAB',0Ah
.data:00007FF63BBF18F0                 db '-----END PUBLIC KEY-----',0Ah,0
```

Figure 13: The public key used by the ransomware

To generate a random key or initialization vector, Night Sky might have used the **CryptGenRandom** Windows API as shown in Figure 14.

functions (21)	blacklist (5)	ordinal (0)	library (6)
FindNextFileW	x	-	kernel32.dll
SHEmptyRecycleBinA	x	-	shell32.dll
RmStartSession	x	-	rstrtmgr.dll
CryptGenRandom	x	-	advapi32.dll
RtlExitUserThread	x	-	ntdll.dll

Figure 14: List of suspicious imports by the malware

3. IoCs

IoC	Type	Description
8c1a72991fb04dc3a8cf89605fb85150ef0e742472a0c58b8fa942a1f04877b0	File hash	Night Sky Windows PE executable
a077a55608ced7cea2bd92e2ce7e43bf51076304990ec7bb40c2b384ce2e5283	File hash	Night Sky Windows PE executable
1fca1cd04992e0fcaa714d9dfa97323d81d7e3d43a024ec37d1c7a2767a17577	File hash	Unpacked Night Sky executable
.hta	File extension	File extension of the ransom notes
.nightsky	File extension	File extension of encrypted files
contact[.]nightsky[.]cyou	URL	Web chat used to communicate with attackers
45[.]76.188[.]137	IP	IP address of the contact domain
mail[.]nightsky[.]cyou	URL	The mail domain

87[.]120.36[.]12	IP	IP address of the mail domain
http://gg5ryfgogainisskdvh4y373ap3b2mxafcibeh2lvq5x7fx76ygcosad[.]onion	URL	Website where attackers publish victim's data if ransom is not paid
tset123155465463213	Mutex	The mutex used by Night Sky to avoid double encryption

4. Mitigation Recommendations

- Regularly back up your data and confirm the backup works.
- Scan systems using YARA rules provided here to detect malware samples.
- Run the code provided here to create the same mutex created by Night Sky to prevent the infections.

5. References

- https://www.netskope.com/pt/blog/netskope-threat-coverage-night-sky
- https://blog.malwarebytes.com/ransomware/2022/01/night-sky-the-new-corporate-ransomware-demanding-a-sky-high-ransom/
- https://www.bleepingcomputer.com/news/security/night-sky-ransomware-uses-log4j-bug-to-hack-vmware-horizon-servers/
- https://www.bankinfosecurity.com/night-sky-ransomware-distributed-via-log4j-exploits-a-18294
- https://github.com/Dump-GUY/Malware-analysis-and-Reverse-engineering/blob/main/NightSky_Ransomware%E2%80%93just_a_Rook_RW_fork_in_VMProtect_suit/NightSky_Ransomware%E2%80%93just_a_Rook_RW_fork_in_VMProtect_suit.md