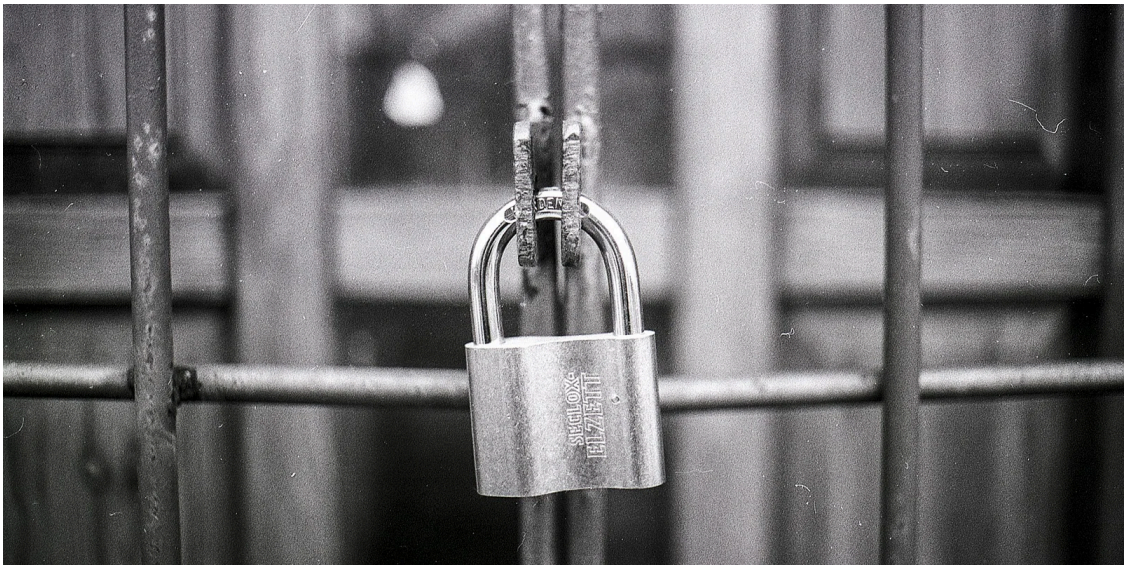
Night Sky is the latest ransomware targeting corporate networks

By Lawrence Abrams

Published: 2022-01-06 · Archived: 2026-04-05 14:01:52 UTC

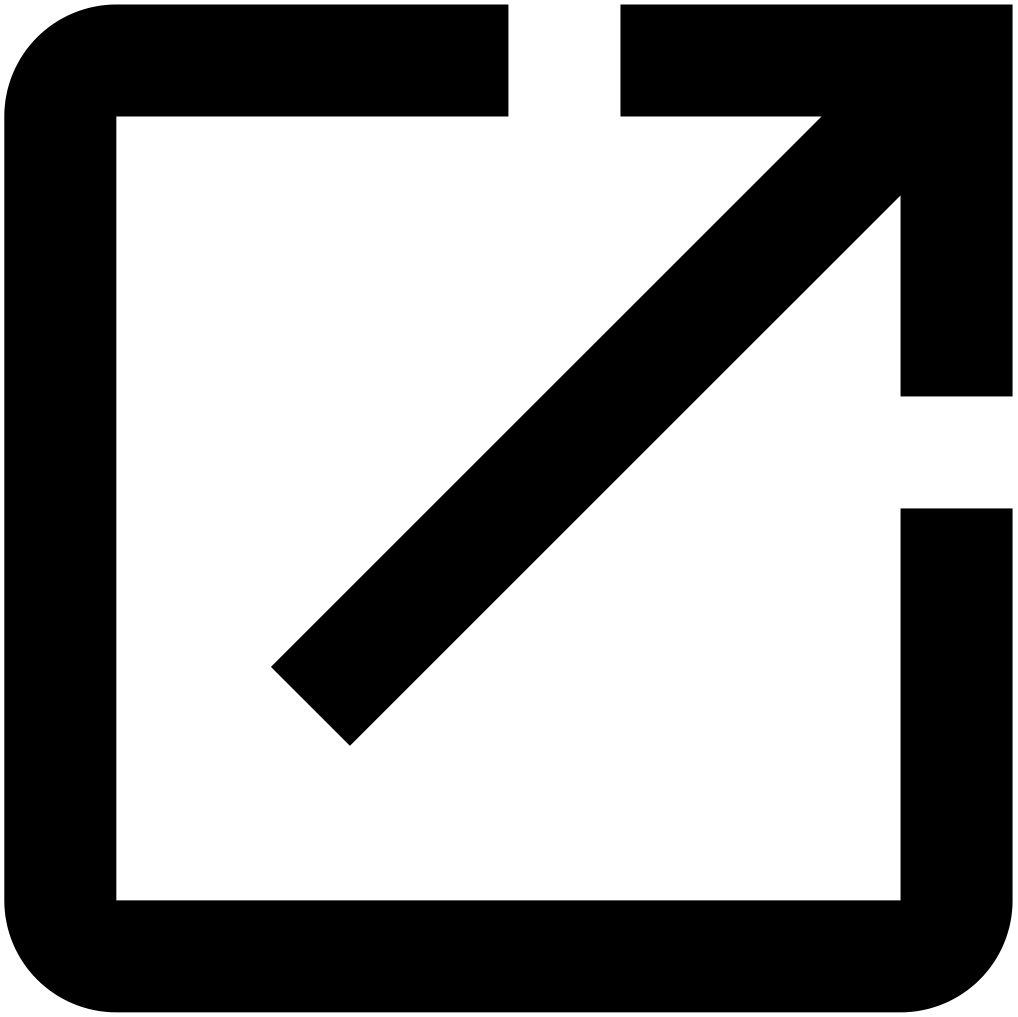


It's a new year, and with it comes a new ransomware to keep an eye on called 'Night Sky' that targets corporate networks and steals data in double-extortion attacks.

According to MalwareHunterTeam, who first spotted the new ransomware, the Night Sky operation started on December 27th and has since published the data of two victims.

One of the victims has received an initial ransom demand of $800,000 to obtain a decryptor and for stolen data not to be published.


DIE LINKE.
0:00



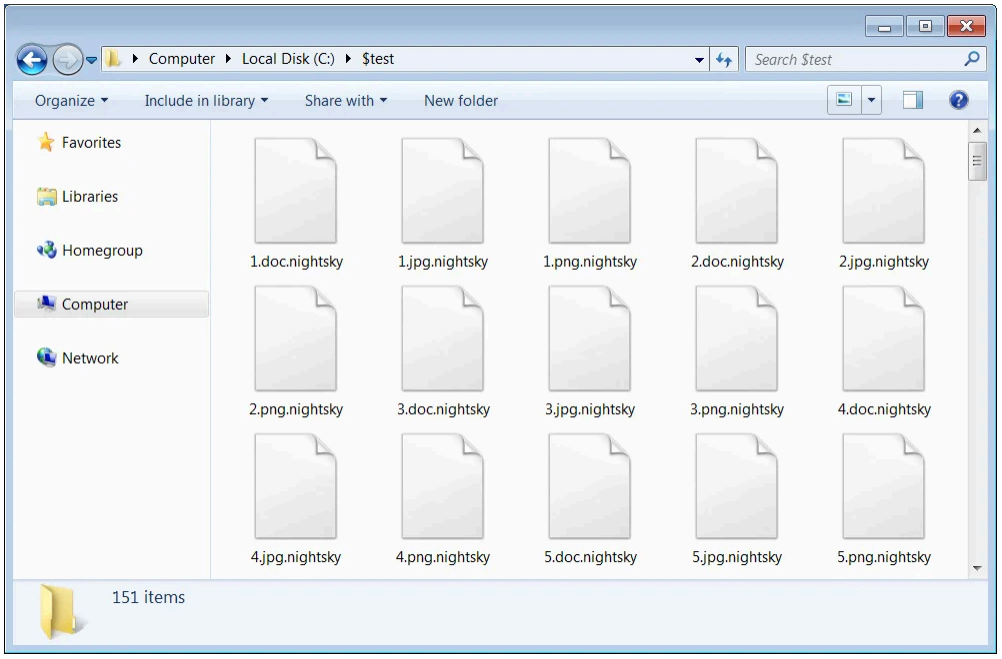
How the Night Sky encrypts devices

A sample of the Night Sky ransomware seen by BleepingComputer is customized to contain a personalized ransom note and hardcoded login credentials to access the victim's negotiation page.

When launched, the ransomware will encrypt all files except those ending with the .dll or .exe file extensions. The ransomware will also not encrypt files or folders in the list below:

```
 AppData
Boot
Windows
Windows.old
Tor Browser
Internet Explorer
Google
Opera
Opera Software
Mozilla
Mozilla Firefox
$Recycle.Bin
ProgramData
All Users
autorun.inf
boot.ini
bootfont.bin
bootsect.bak
bootmgr
bootmgr.efi
bootmgfw.efi
desktop.ini
iconcache.db
ntldr
ntuser.dat
ntuser.dat.log
ntuser.ini
thumbs.db
Program Files
Program Files (x86)
#recycle
```

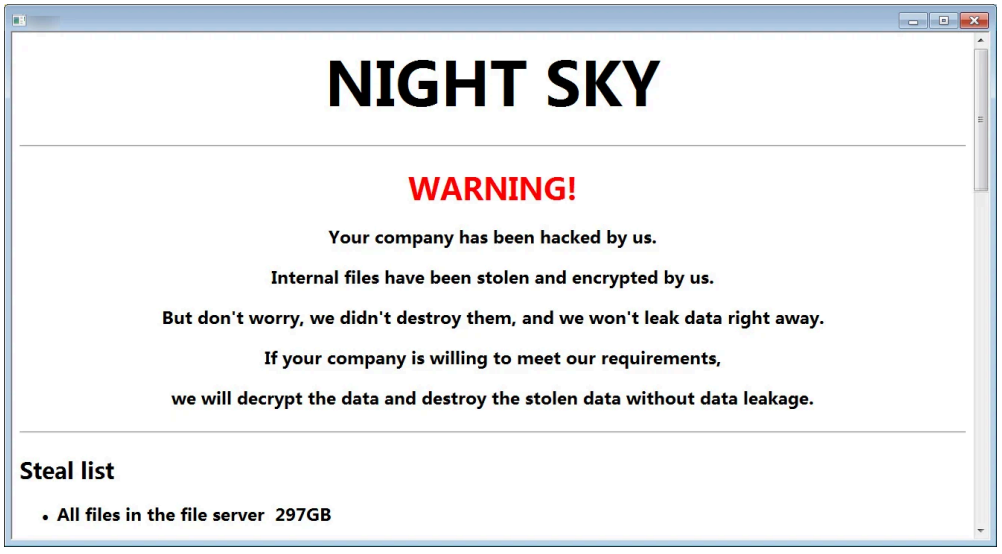
When encrypting files, Night Sky will append the **.nightsky** extension to encrypted file names, as shown in the image below.



Night Sky encrypted files

Source: BleepingComputer

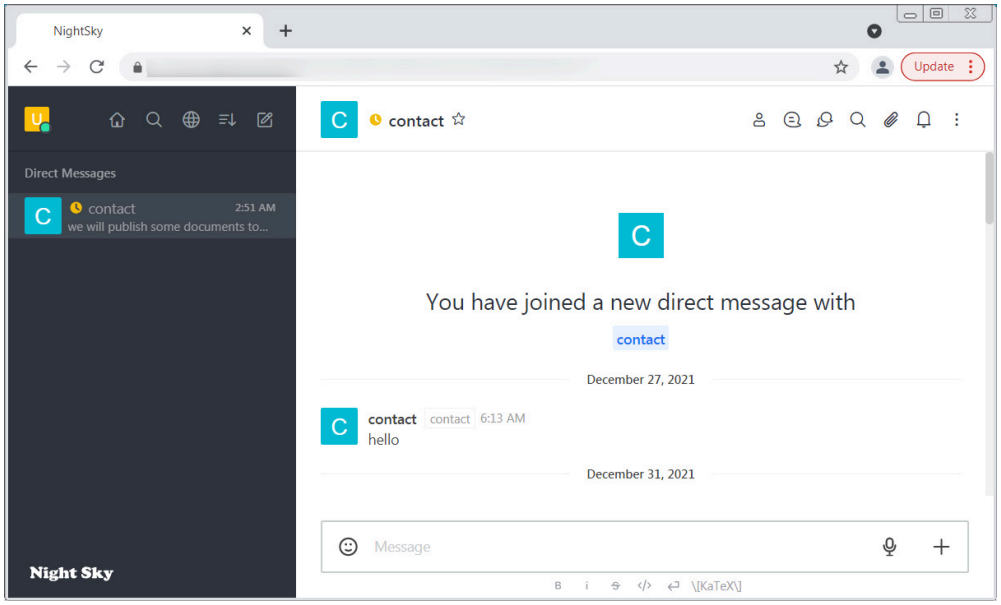
In each folder a ransom note named **NightSkyReadMe.hta** contains information related to what was stolen, contact emails, and hard coded credentials to the victim's negotiation page.



Night Sky ransom note

Source: BleepingComputer

Instead of using a Tor site to communicate with victims, Night Sky uses email addresses and a clear web website running Rocket.Chat. The credentials are used to log in to the Rocket.Chat URL provided in the ransom note.



Night Sky Rocket.Chat negotiation site

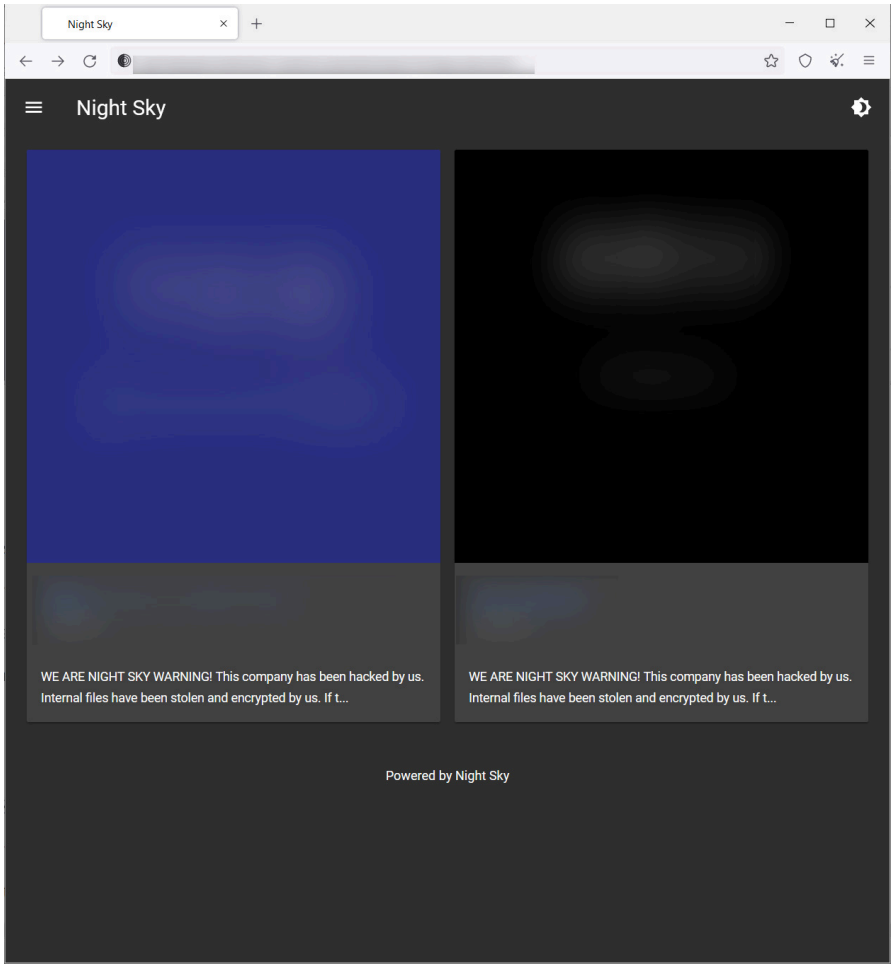
Source: BleepingComputer

Double-extortion tactic

A common tactic used by ransomware operations is to steal unencrypted data from victims before encrypting devices on the network.

The threat actors then use this stolen data in a "double-extortion" strategy, where they threaten to leak the data if a ransom is not paid.

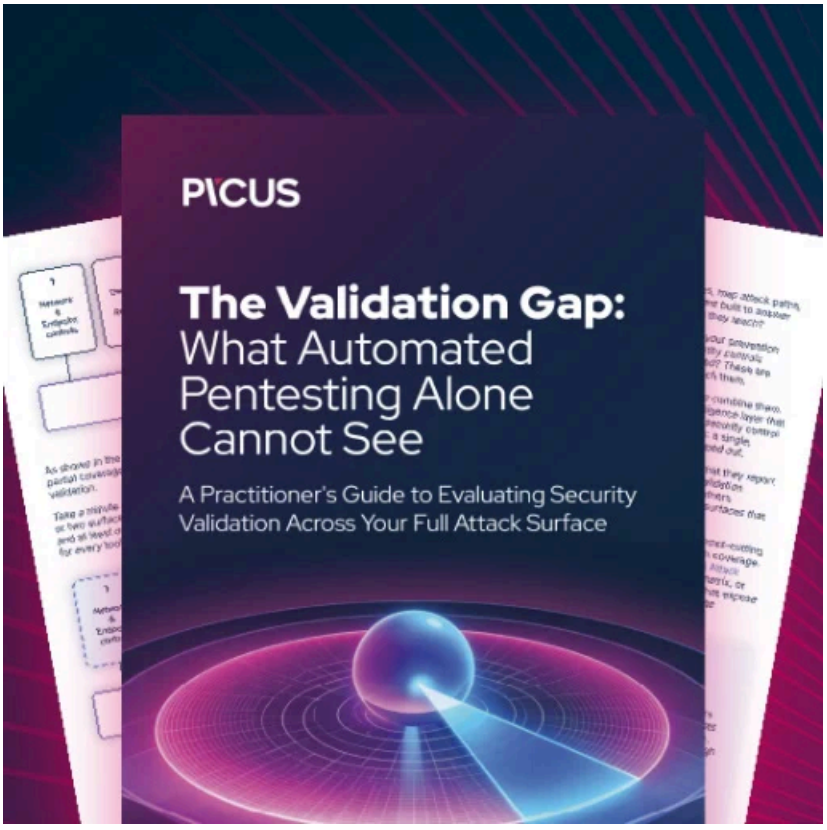
To leak victim's data, Night Sky has created a Tor data leak site that currently includes two victims, one from Bangladesh and another from Japan.



Night Sky data leak site

Source: BleepingComputer

While there has not been a lot of activity with the new Night Sky ransomware operation, it is one that we need to keep an eye on as we head into the new year.



[Automated Pentesting Covers Only 1 of 6 Surfaces.]

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.
