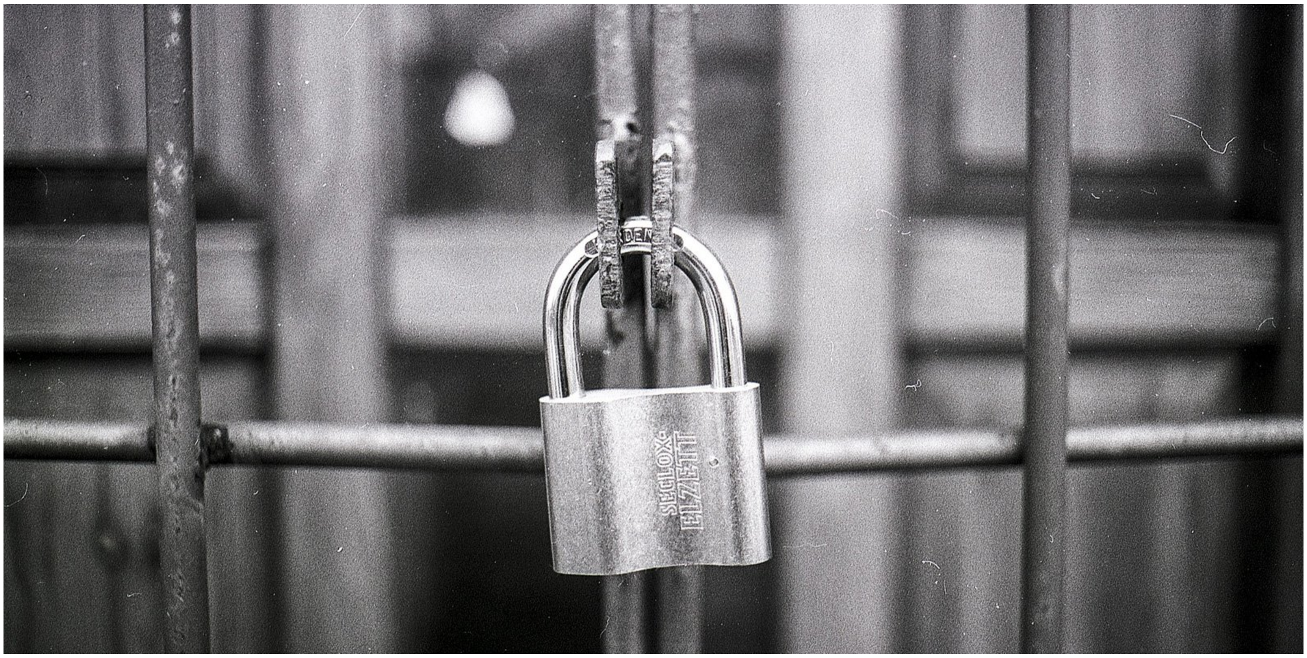
Night Sky is the latest ransomware targeting corporate networks

bleepingcomputer.com/news/security/night-sky-is-the-latest-ransomware-targeting-corporate-networks/

Lawrence Abrams

By
Lawrence Abrams

- January 6, 2022
- 05:09 PM
- 0



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One of the victims has received an initial ransom demand of $800,000 to obtain a decryptor and for stolen data not to be published.

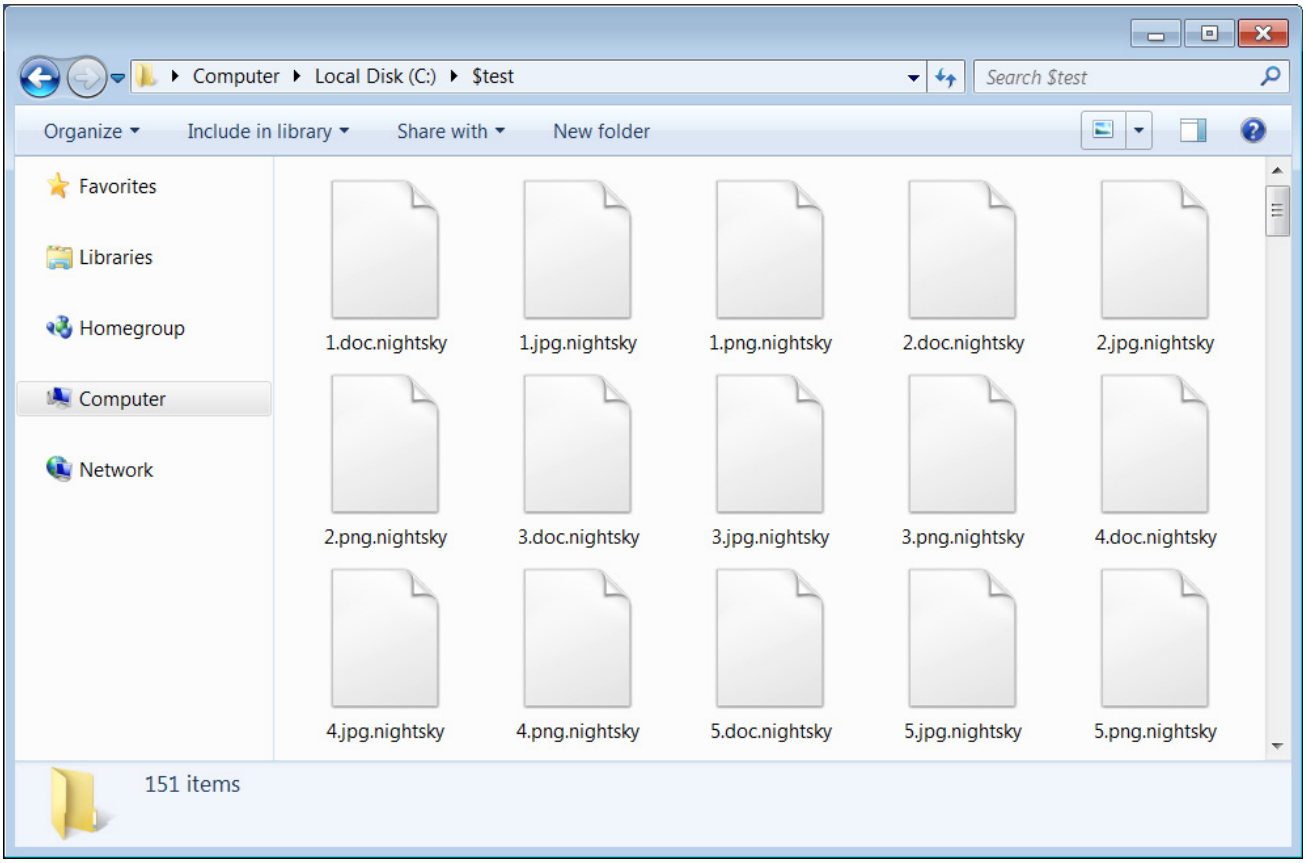
How the Night Sky encrypts devices

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.

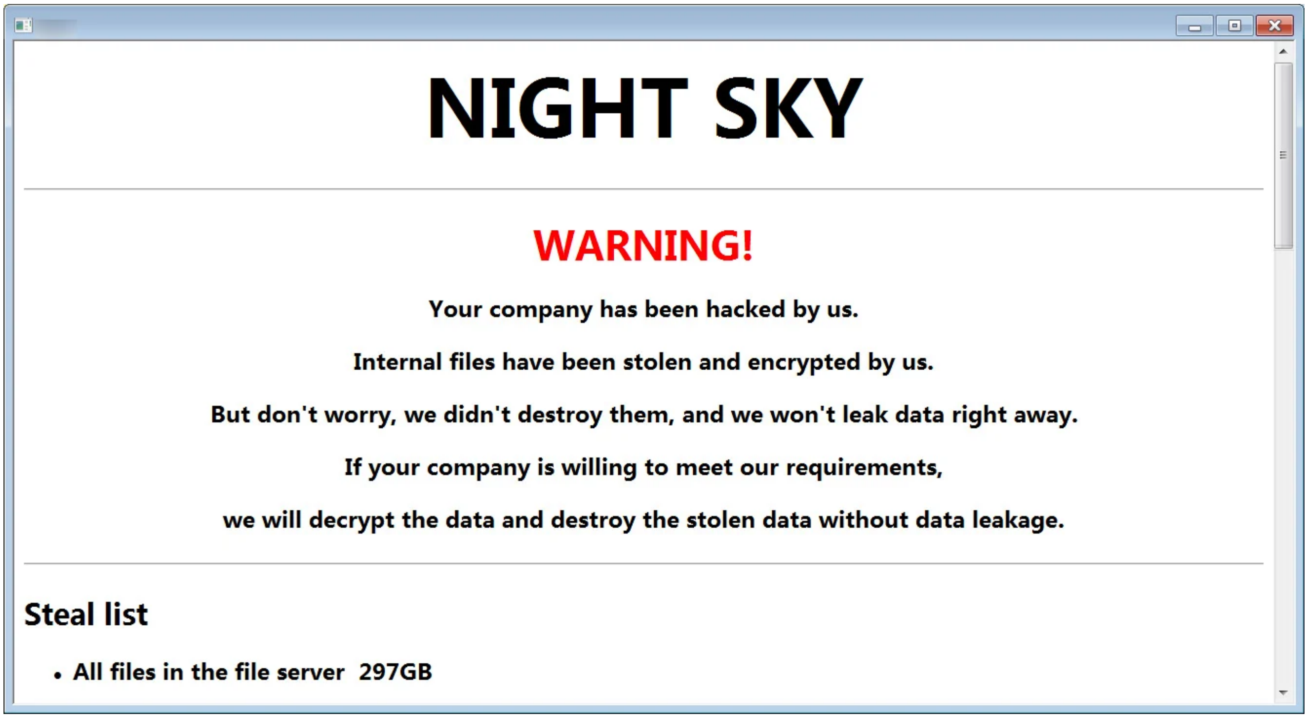


1.doc.nightsky 1.jpg.nightsky 1.png.nightsky 2.doc.nightsky 2.jpg.nightsky
2.png.nightsky 3.doc.nightsky 3.jpg.nightsky 3.png.nightsky 4.doc.nightsky
4.jpg.nightsky 4.png.nightsky 5.doc.nightsky 5.jpg.nightsky 5.png.nightsky

151 items

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

WARNING!

Your company has been hacked by us.

Internal files have been stolen and encrypted by us.

But don't worry, we didn't destroy them, and we won't leak data right away.

If your company is willing to meet our requirements,

we will decrypt the data and destroy the stolen data without data leakage.

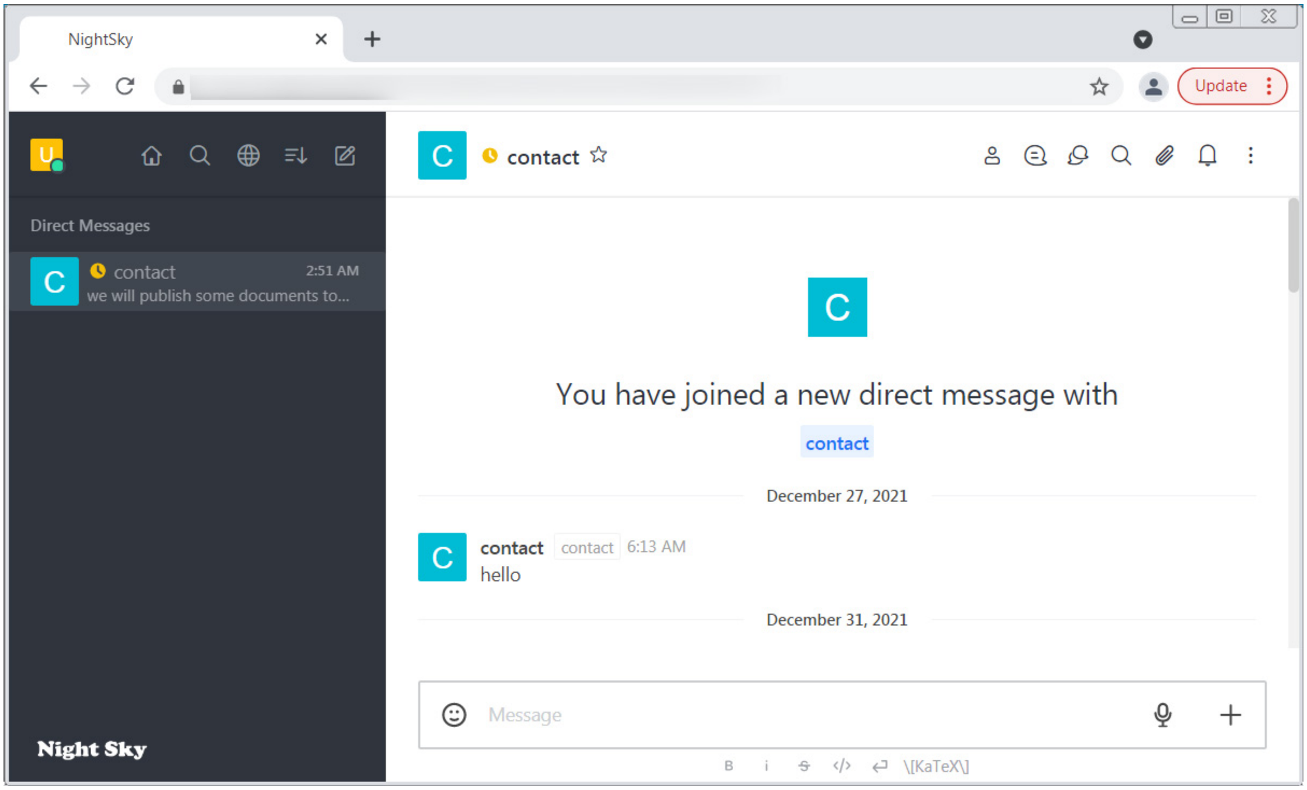
Steal list

- **All files in the file server 297GB**

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.



contact 2:51 AM
we will publish some documents to...

contact

You have joined a new direct message with contact

December 27, 2021

contact contact 6:13 AM
hello

December 31, 2021

Night Sky Rocket.Chat negotiation site

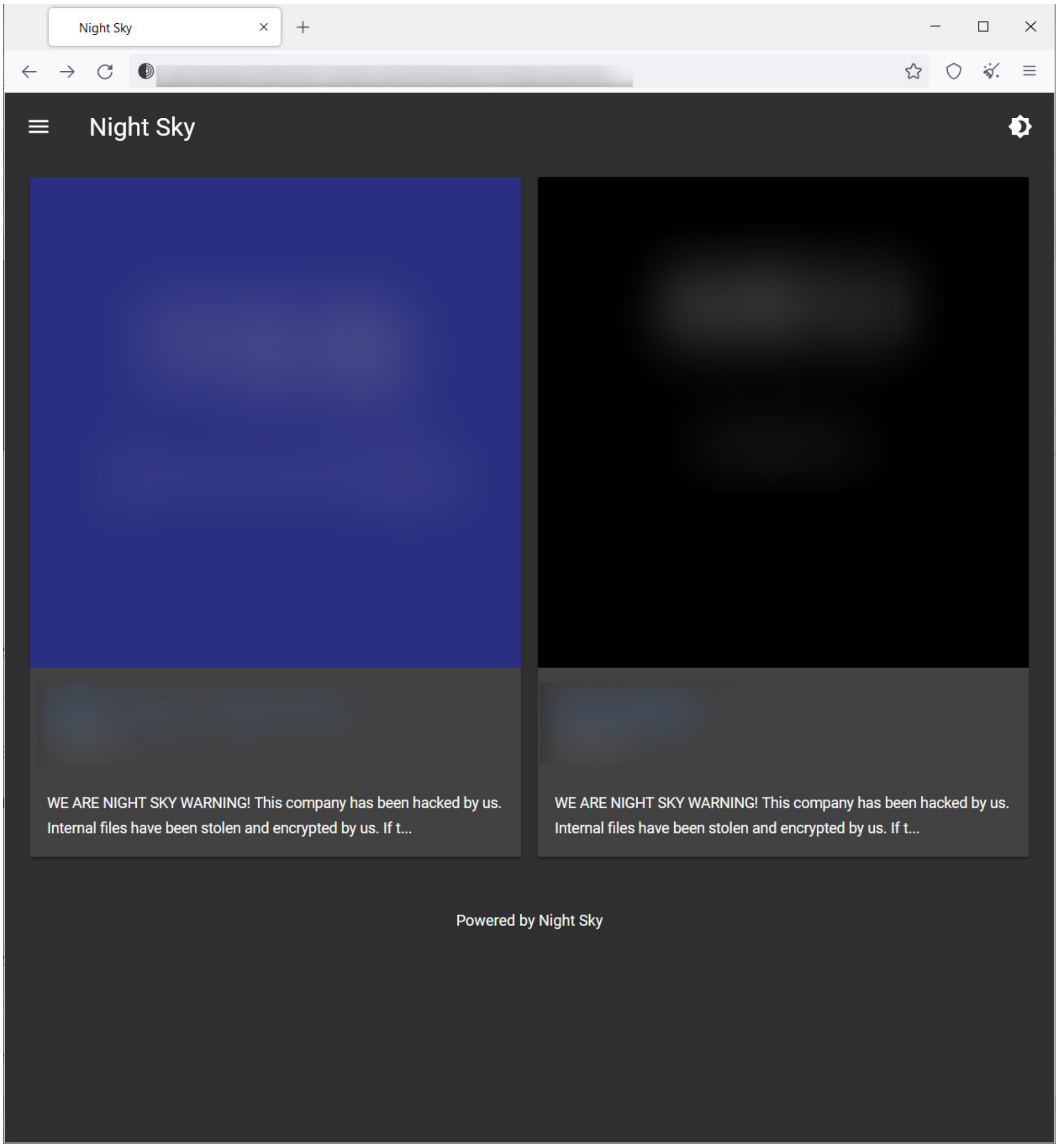
Source: BleepingComputer

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.



WE ARE NIGHT SKY WARNING! This company has been hacked by us. Internal files have been stolen and encrypted by us. If t...

WE ARE NIGHT SKY WARNING! This company has been hacked by us. Internal files have been stolen and encrypted by us. If t...

Powered by Night Sky

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.

Related Articles:

Industrial Spy data extortion market gets into the ransomware game

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

Quantum ransomware seen deployed in rapid network attacks

Snap-on discloses data breach claimed by Conti ransomware gang

Shutterfly discloses data breach after Conti ransomware attack

- Data Exfiltration
- Double-Extortion
- Night Sky
- Ransomware

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: