Mass Attack buhtiRansom

blog.threatzero.io/buhtiransom-934b4ed3c3fd

Raphael Mendonça February 16, 2023

```
---------- [ Welcome to buhtiRansom ] ------------>

What happend?
-------------------------------------------
Your files are encrypted. We use strong encryption algorithms, so you cannot decrypt your data.
But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your files.
Follow our instructions below and you will recover all your data.

What guarantees?
-------------------------------------------
We value our reputation. If we do not do our work and liabilities, nobody will pay us. This is not in our interests.
All our decryption software is perfectly tested and will decrypt your data.

How to get access?
-------------------------------------------
Using a browser:
1) Open website: https://satoshidisk.com/pay/
2) Enter valid email to receive download link after payment.
3) Pay amount to Bitcoin address.
4) Receive email link to the download page.
5) Decrypt instruction included.

!!! DANGER !!!
DO NOT MODIFY or try to RECOVER any files yourself. It WILL NOT be able to RESTORE.
!!! DANGER !!!
```

Restore-My-Files.txt
An unknown threat actor launched this week a wave of ransomware attacks against vulnerable servers with CVE-2022–47986.

The vulnerability that affects IBM Aspera Faspex applications in versions prior to 4.4.2, is present in approximately 300 hosts indexed in the Shodan platform.

Aspera Faspex is an application designed for file transfer and therefore it is common for affected servers to have large volumes of connected storage.

We identified different encrypted servers, with the files renamed to the *.buhti* extension and with the ransom note created on the same date, where the threat actor provides a link to the SatoshiDisk platform as a payment method.

Considering the simple characteristics of the attacks, its expected to be just another threat actor taking advantage of the opportunity.

We will continue to follow!

More information:

- https://blog.assetnote.io/2023/02/02/pre-auth-rce-aspera-faspex/
- https://github.com/ohnonoyesyes/CVE-2022-47986/

- https://www.ibm.com/docs/en/aspera-faspex/4.4?topic=notes-release-aspera-faspex-442