

Undoing a Ransomware infection

Matthias Held

University of Konstanz



Ooops, your files have been encrypted!

English

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

CMT from Monday to Friday

Payment will be raised on

1/4/1970 01:00:00

Time Left

00:00:00:00

Your files will be lost on

1/8/1970 01:00:00

Time Left

00:00:00:00

[About bitcoin](#)

[How to buy bitcoins?](#)

[Contact Us](#)



Send \$600 worth of bitcoin to this address:

13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

Copy

Check Payment

Decrypt

Finding the right solution

Real-time solutions

- File system
- Bump-in-the-wire
- File server

Finding the right solution

Real-time solutions

- File system
- Bump-in-the-wire
- File server

Finding the right solution

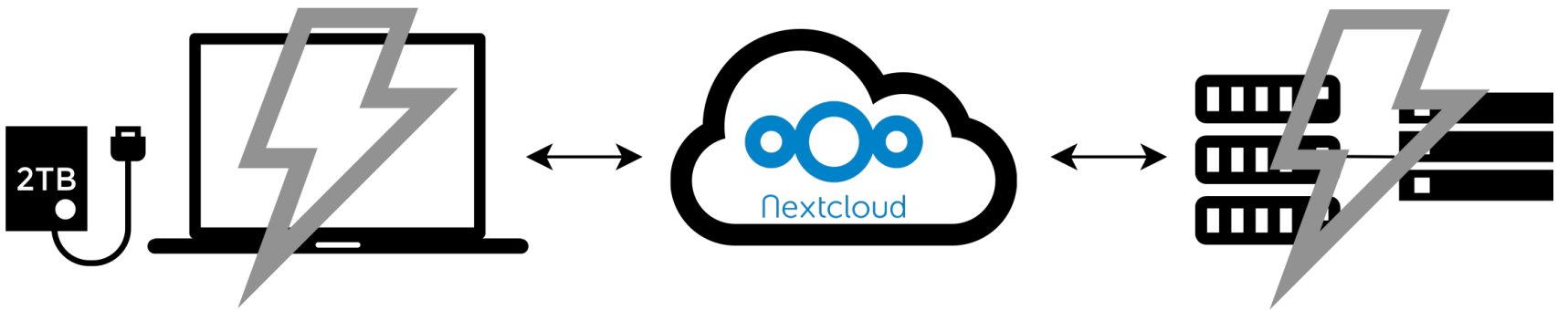
Real-time solutions

- File system
- Bump-in-the-wire
- File server

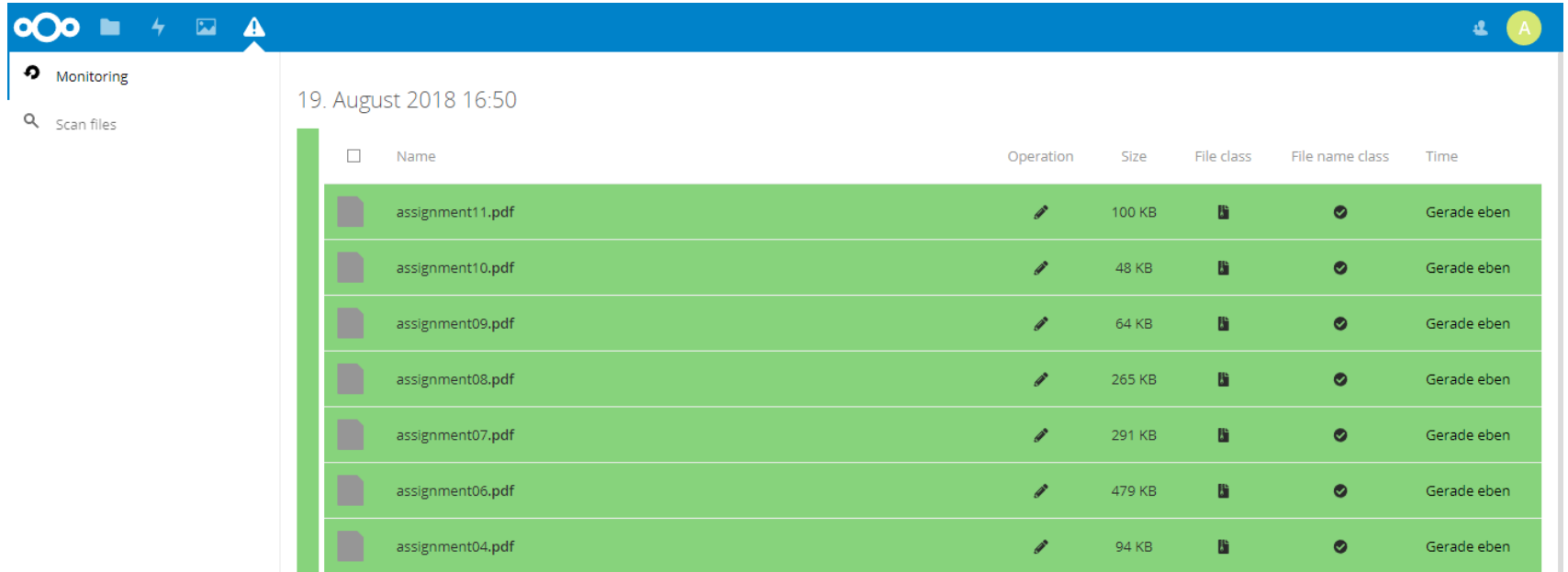
Finding the right solution

Real-time solutions

- ~~File system~~
- ~~Bump-in-the-wire~~
- ~~File server~~



Synchronization monitoring



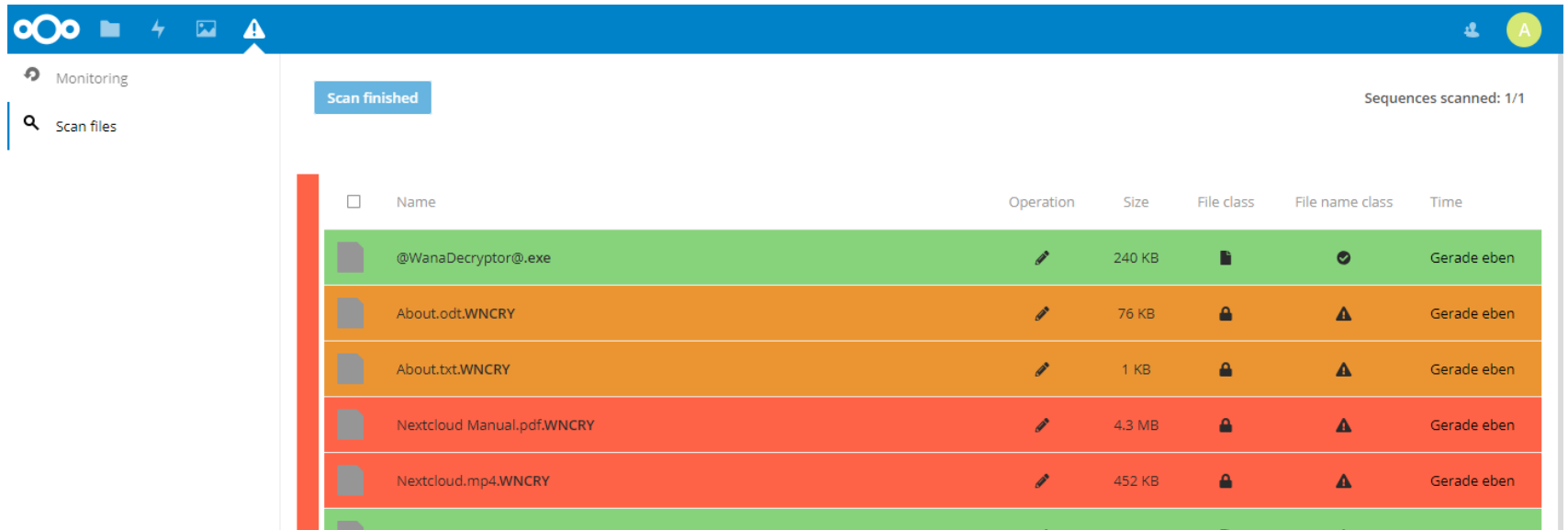
Monitoring

Scan files

19. August 2018 16:50

<input type="checkbox"/>	Name	Operation	Size	File class	File name class	Time
<input type="checkbox"/>	assignment11.pdf		100 KB			Gerade eben
<input type="checkbox"/>	assignment10.pdf		48 KB			Gerade eben
<input type="checkbox"/>	assignment09.pdf		64 KB			Gerade eben
<input type="checkbox"/>	assignment08.pdf		265 KB			Gerade eben
<input type="checkbox"/>	assignment07.pdf		291 KB			Gerade eben
<input type="checkbox"/>	assignment06.pdf		479 KB			Gerade eben
<input type="checkbox"/>	assignment04.pdf		94 KB			Gerade eben

Files scan



Monitoring

Scan files

Scan finished

Sequences scanned: 1/1

<input type="checkbox"/>	Name	Operation	Size	File class	File name class	Time
<input type="checkbox"/>	@WanaDecryptor@.exe		240 KB			Gerade eben
<input type="checkbox"/>	About.odt.WNCRY		76 KB			Gerade eben
<input type="checkbox"/>	About.txt.WNCRY		1 KB			Gerade eben
<input type="checkbox"/>	Nextcloud Manual.pdf.WNCRY		4.3 MB			Gerade eben
<input type="checkbox"/>	Nextcloud.mp4.WNCRY		452 KB			Gerade eben



https://github.com/ilovemilk/ransomware_detection



matthias.held@uni-konstanz.de