

# Incident Response – Typische Fehler



CONOVA S-DAY 2021  
Juni 2021



Ooops, your files ha

## What Happened to My Con

Your important files are encrypted.  
Many of your documents, photos, vi  
accessible because they have been en  
recover your files, but do not waste  
our decryption service.

## Can I Recover My Files?

Sure. We guarantee that you can rec  
not so enough time.  
You can decrypt some of your files f  
But if you want to decrypt all your fi  
You only have 3 days to submit the p  
Also, if you don't pay in 7 days, you  
We will have free events for users w

## How Do I Pay?

Payment is accepted in Bitcoin only.  
Please check the current price of Bit  
click <How to buy bitcoins>.  
And send the correct amount to the  
After your payment, click <Check Pa  
GMT from Monday to Friday



Send \$300 v

12t9YDPgv

“  
PANIK

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

[About bitcoin](#)

[How to buy bitcoins?](#)



“

Handlungen im Affekt

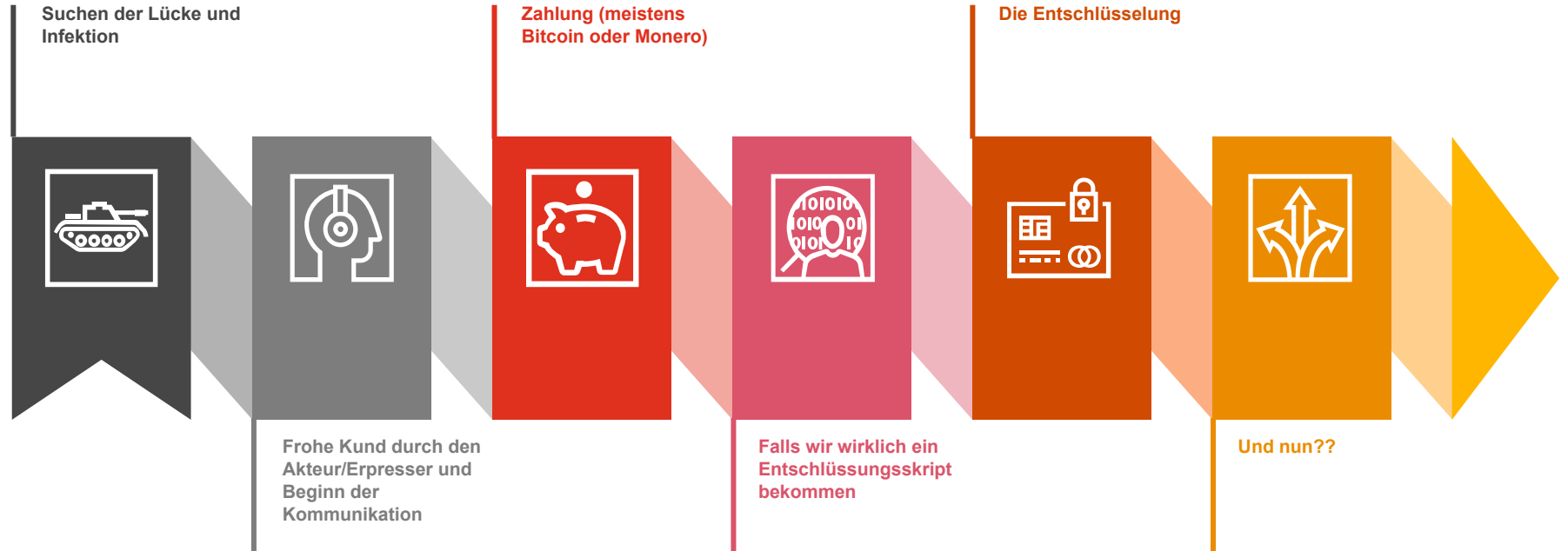




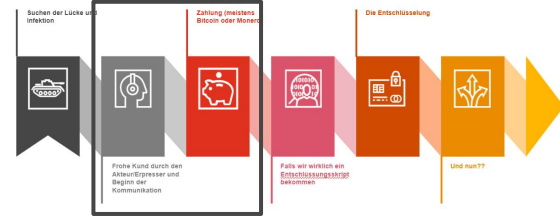
“

Wir haben alles im Blick

# Was wäre wenn wir der Erpressung bei Ransomware folgen ...



# Die Frohe Kund ... Kommunikation und Zahlung anonym ...



```
##IMPORTANT_NOTICE## - Notepad
File Edit Format View Help
Greetings,
There was a serious security breach in your systems and this was detected during our scans.
We encrypt your data that you see important in your system by processing twice. As encryption is done as SHA256 and AES256, we would like to remind you that you can not restore your data with known da
process and / or make copies of them. Corruption of the original files may cause irretrievable damage to your data.
It is useful to know that random deletion techniques are used 3 times when you delete, you can not bring back deleted data by known methods.
These methods will only cause you to lose time.
```

If you wish, you can contact us via the following communication to resolve this issue.  
Do not forget to add the specially generated code below when you want to reach it.

SITE\_CODE:BF0EC0BB

datamoon@mail.com  
data\_lockerer@protonmail.com

```
[: Greetings ::

Little FAQ:
.1.
Q: Whats Happen?
A: Your files have been encrypted. The file structure was not damaged, we did
everything possible so that this could not happen.

.2.
Q: How to recover files?
A: If you wish to decrypt your files you will need to pay in Monero(XMR) - this is one
of the types of cryptocurrency, you can get acquainted with it in more detail here:
https://www.getmonero.org/

.3.
Q: What about guarantees?
A: Its just a business. We absolutely do not care about you and your deals, except
getting benefits. If we do not do our work and liabilities - nobody will cooperate with
us. Its not in our interests.
To check the ability of returning files, you can send to us any 2 files with SIMPLE
extensions(jpg,xls,doc, etc... not databases!) and low sizes(max 1 mb), we will decrypt
them and send back to you. That is our guarantee.

.4.
Q: How to contact with you?
A: Please, write us to our qTOX account:
78DD546F7524089A930B12F793F4C1D1B4470A15A4CBA85AA0DA6D030AFE2E48B8799204F004
You can learn about this way of communication and download it here:
https://qtox.github.io/
Or use Bitmessage and write to our address: BM-2cUbGd124Dcs1Jdc5VfSa2GDMC1iaNtesC
You can learn about this way of communication and download it here:
https://wiki.bitmessage.org/ and here:
https://github.com/Bitmessage/PyBitmessage/releases/
```

```
readme-warning - Notepad
File Edit Format View Help
[: Greetings ::

Little FAQ:
.1.
Q: Whats Happen?
A: Your files have been encrypted and now have the "makop" extension. The file structure was not damaged, we did everything possib
this could not happen.

.2.
Q: How to recover files?
A: If you wish to decrypt your files you will need to pay in bitcoins.

.3.
Q: What about guarantees?
A: Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and
nobody will cooperate with us. Its not in our interests.
To check the ability of returning files, you can send to us any 2 files with SIMPLE extensions(jpg,xls,doc, etc... not databases!)
sizes(max 1 mb), we will decrypt them and send back to you. That is our guarantee.

.4.
Q: How to contact with you?
A: You can write us to our mailbox: datamoon@mail.com or data_lockerer@protonmail.com

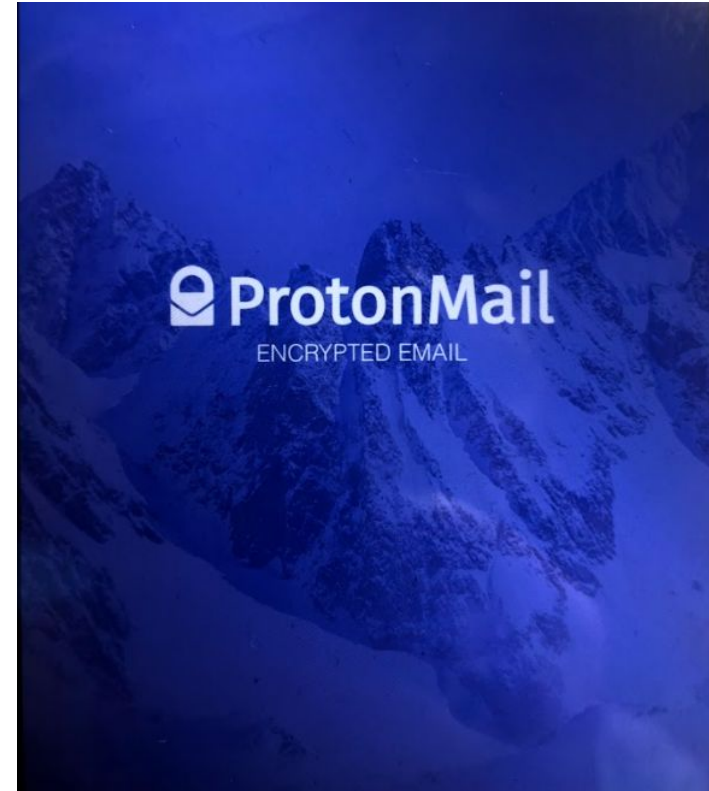
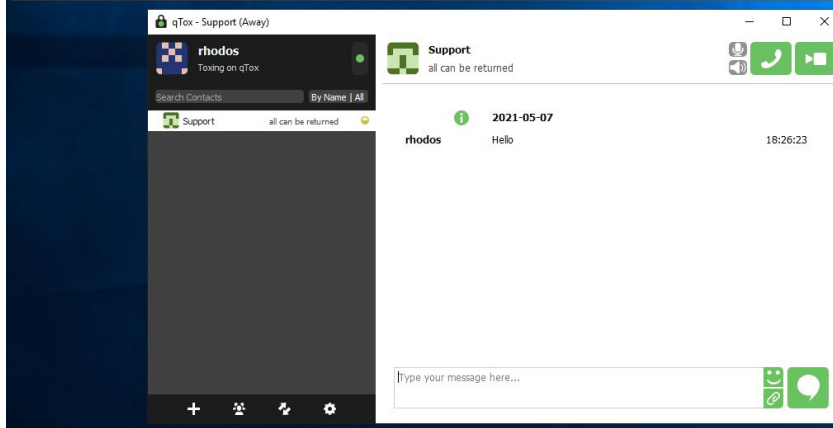
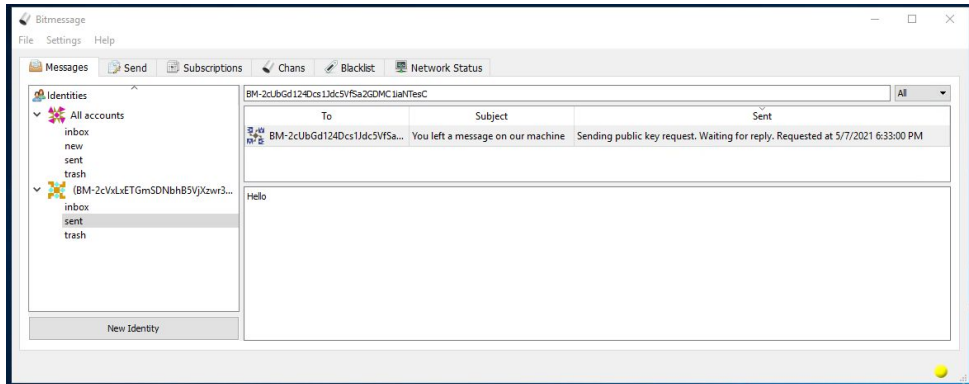
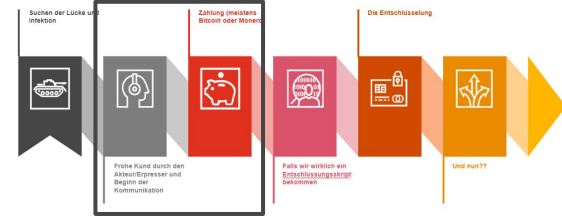
.5.
Q: How will the decryption process proceed after payment?
A: After payment we will send to you our scanner-decoder program and detailed instructions for use. With this program you will be
decrypt all your encrypted files.

.6.
Q: If I don't want to pay bad people like you?
A: If you will not cooperate with our service - for us, it does not matter. But you will lose your time and data, cause only we h
private key. In practice - time is much more valuable than money.

[:BWARE::
DON'T try to change encrypted files by yourself!
If you will try to use any third party software for restoring your data or antivirus solutions - please make a backup for all encry
Any changes in encrypted files may entail damage of the private key and, as result, the loss all data.
```

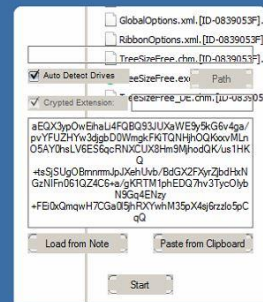
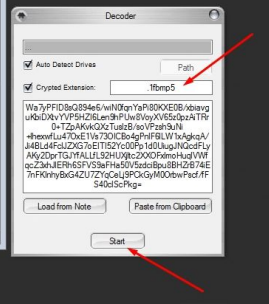
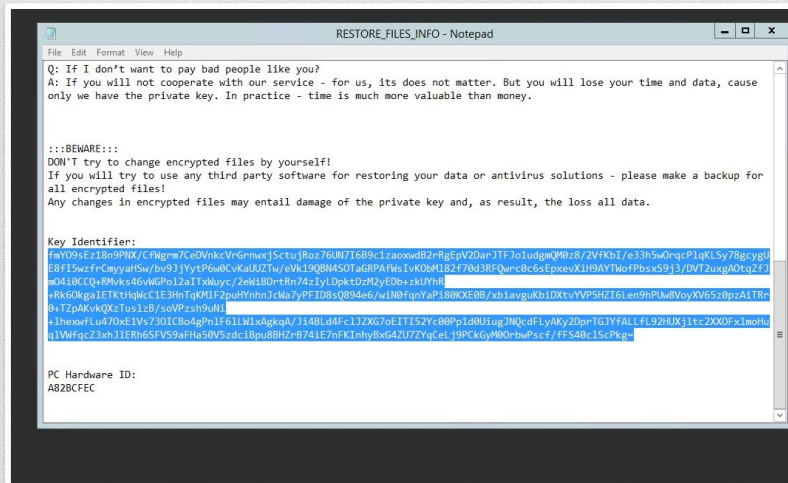
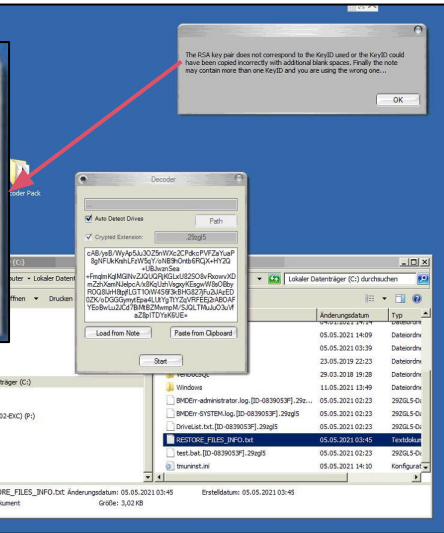
# Die Frohe Kund ...

## Kommunikation und Zahlung anonym ...





# Falls wir wirklich ein Entschlüsselungs-skript bekommen







“

Übungen? Sind nicht  
mehr im Budget.



“

## Schrödinger's Cyber Defense

# Thank you



***Erik Rusek***

Senior Manager  
Cybersecurity & Privacy

Tel.: +43 676 833775456

erik.rusek@pwc.com



***Thomas Kastner***

Manager  
Cybersecurity & Privacy

Tel.: +43 676 833773231

thomas.k.kastner@pwc.com

[pwc.at/cyber](https://pwc.at/cyber)

© 2021 PwC. All rights reserved. Not for further distribution without the permission of PwC. "PwC" refers to the network of member firms of PricewaterhouseCoopers International Limited (PwCIL), or, as the context requires, individual member firms of the PwC network. Each member firm is a separate legal entity and does not act as agent of PwCIL or any other member firm. PwCIL does not provide any services to clients. PwCIL is not responsible or liable for the acts or omissions of any of its member firms nor can it control the exercise of their professional judgment or bind them in any way. No member firm is responsible or liable for the acts or omissions of any other member firm nor can it control the exercise of another member firm's professional judgment or bind another member firm or PwCIL in any way.