ECP Jaarfestival

VIBE SHIFT

Forum Standaardisatie
Standaard Samenwerken

SIDN fonds

SIDN Zorgeloos online

dutch digital delta
connect and create

TNO innovation for life

Over Informatie Gesproken

NL AI Coalitie

ai technology for people

Ministerie van Justitie en Veiligheid

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Ministerie van Economische Zaken en Klimaat

Agentschap Telecom
Ministerie van Economische Zaken en Klimaat

ONLINE TRUST COALITIE

Veilig internetten.nl

Dutch Blockchain Coalition
connect and create

Leren door ervaren en oefenen

ECP Jaarfestival

We moeten klaar staan voor de ***'grote cybercrisis'****.*

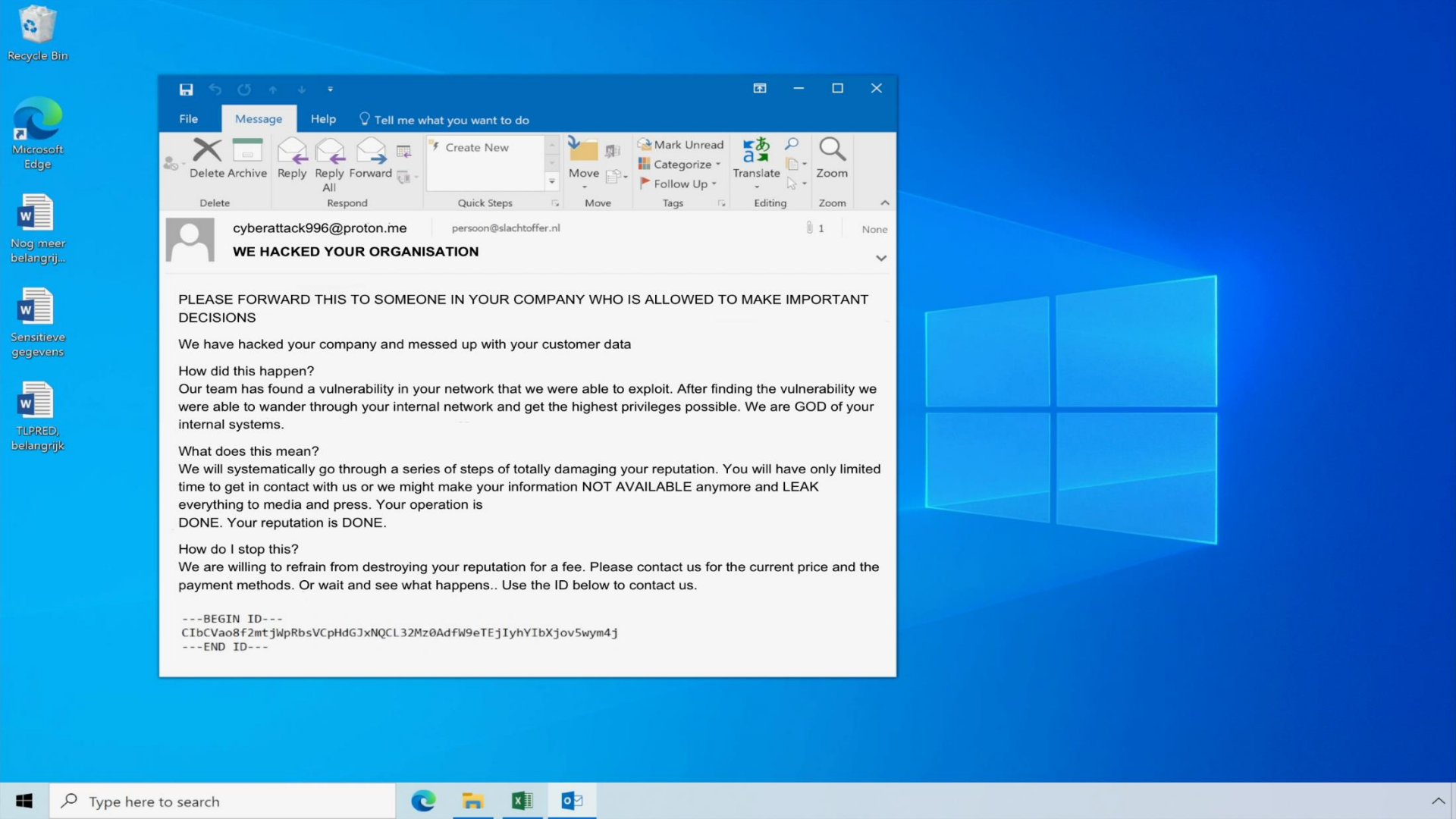
Wie zijn jullie?

- Jullie zelf, onderdeel van het crisisteam bij een crisis ☺
- Verschillende rollen, verschillende antwoorden
- Niks is goed of fout!

Gebruik van Mentimeter

- Ga naar menti.com
- Voer de volgende code in:

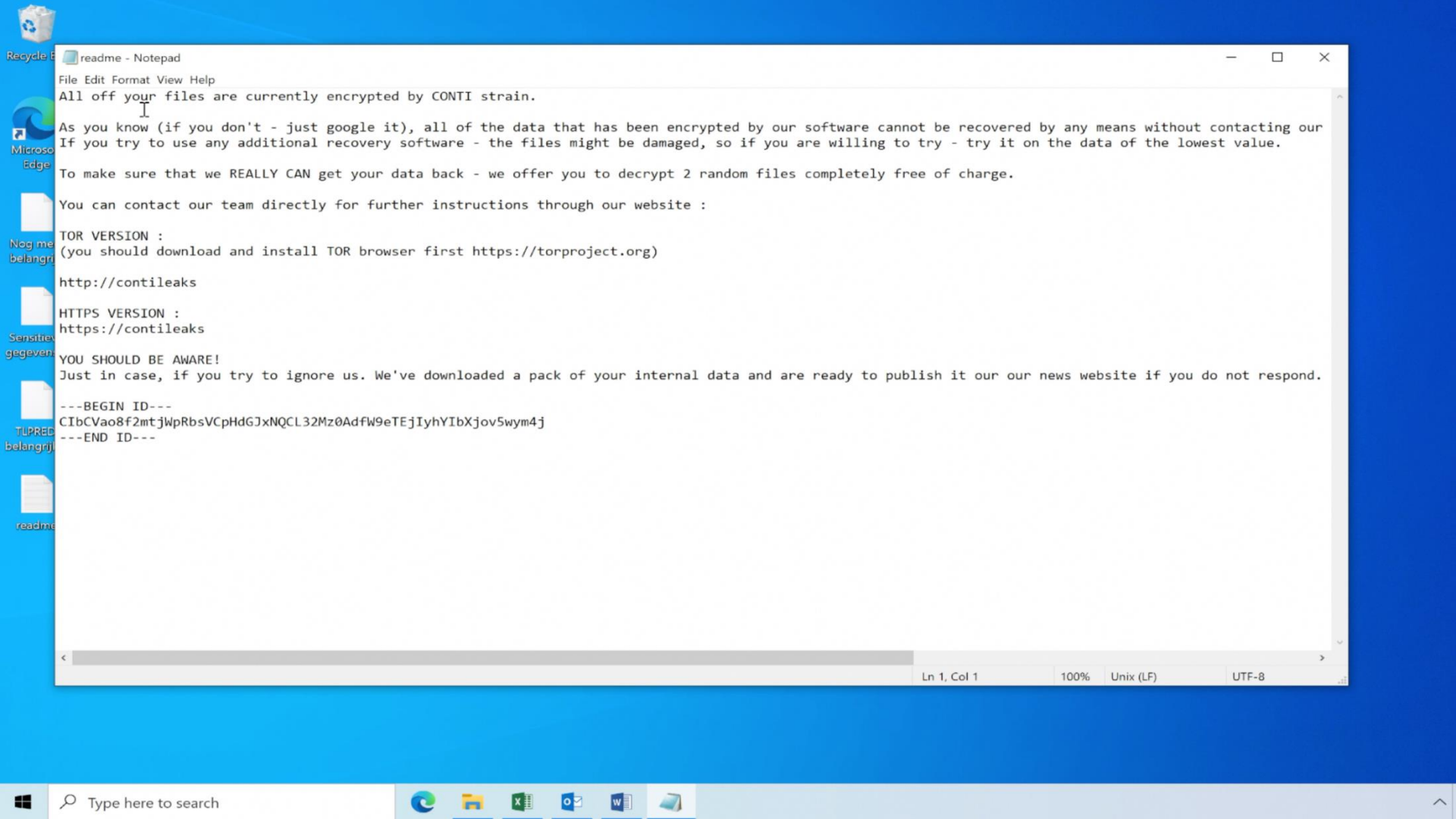
3462 3678


Recycle Bin
Microsoft Edge
Nog meer belangrij...
Sensitieve gegevens
TLPRED, belangrijk
File
Message
Help
Tell me what you want to do
Delete
Archive
Reply
Reply All
Forward
Create New
Move
Mark Unread
Categorize
Follow Up
Translate
Zoom
Delete
Respond
Quick Steps
Move
Tags
Editing
Zoom
cyberattack996@proton.me
persoon@slachtoffer.nl
1
None
WE HACKED YOUR ORGANISATION
PLEASE FORWARD THIS TO SOMEONE IN YOUR COMPANY WHO IS ALLOWED TO MAKE IMPORTANT DECISIONS
We have hacked your company and messed up with your customer data
How did this happen?
Our team has found a vulnerability in your network that we were able to exploit. After finding the vulnerability we were able to wander through your internal network and get the highest privileges possible. We are GOD of your internal systems.
What does this mean?
We will systematically go through a series of steps of totally damaging your reputation. You will have only limited time to get in contact with us or we might make your information NOT AVAILABLE anymore and LEAK everything to media and press. Your operation is
DONE. Your reputation is DONE.
How do I stop this?
We are willing to refrain from destroying your reputation for a fee. Please contact us for the current price and the payment methods. Or wait and see what happens.. Use the ID below to contact us.
---BEGIN ID---
CIbCVao8f2mtjWpRbsVCpHdGJxNQCL32Mz0AdfW9eTEjIyhYIbXjov5wym4j
---END ID---
Type here to search

Wie ga je bellen nu te komen?

- Technisch specialisten
- Communicatie
- Legal
- Directie
- HR
- Crisiscoördinatie

Antwoord op menti.com, code: 3462 3678


readme - Notepad
File Edit Format View Help
All off your files are currently encrypted by CONTI strain.
As you know (if you don't - just google it), all of the data that has been encrypted by our software cannot be recovered by any means without contacting our
If you try to use any additional recovery software - the files might be damaged, so if you are willing to try - try it on the data of the lowest value.
To make sure that we REALLY CAN get your data back - we offer you to decrypt 2 random files completely free of charge.
You can contact our team directly for further instructions through our website :
TOR VERSION :
(you should download and install TOR browser first https://torproject.org)
http://contileaks
HTTPS VERSION :
https://contileaks
YOU SHOULD BE AWARE!
Just in case, if you try to ignore us. We've downloaded a pack of your internal data and are ready to publish it our our news website if you do not respond.
---BEGIN ID---
CIbCVao8f2mtjWpRbsVCpHdGJxNQCL32Mz0AdfW9eTEjIyhYIbXjov5wym4j
---END ID---
Ln 1, Col 1
100%
Unix (LF)
UTF-8
Type here to search

created_at	updated_at
26-12-19 6:09	4-09-22 5:17
20-04-21 19:37	4-09-22 5:17
26-12-19 6:09	4-09-22 5:17
14-01-20 7:16	4-09-22 5:17
8-09-20 21:22	4-09-22 5:17
8-01-22 15:33	4-09-22 5:17
9-01-22 15:33	4-09-22 5:17
7-06-22 5:45	4-09-22 5:17
25-09-20 21:16	4-09-22 5:17
15-04-19 14:36	4-09-22 5:17
29-06-22 8:49	4-09-22 5:17
10-06-22 8:05	4-09-22 5:17
8-02-20 16:56	4-09-22 5:17
9-02-20 16:56	4-09-22 5:17
4-02-22 1:17	4-09-22 5:17
30-12-20 17:13	4-09-22 5:17
31-12-20 17:13	4-09-22 5:17
20-08-22 18:16	4-09-22 5:17
30-04-22 7:29	4-09-22 5:17
1-05-22 7:29	4-09-22 5:17

35.88.232.153	10:05	3389	closed
35.88.232.153	10:10	3389	closed
35.88.232.153	10:15	3389	closed
35.88.232.153	10:20	3389	closed
35.88.232.153	10:25	3389	closed
35.88.232.153	10:30	3389	closed
35.88.232.153	10:35	3389	closed
35.88.232.153	10:40	3389	closed
35.88.232.153	10:45	3389	closed
35.88.232.153	10:50	3389	closed
35.88.232.153	10:55	3389	closed
35.88.232.153	11:00	3389	closed
35.88.232.153	11:05	3389	open
35.88.232.153	11:10	3389	closed
35.88.232.153	11:15	3389	closed
35.88.232.153	11:20	3389	closed
35.88.232.153	11:25	3389	closed
35.88.232.153	11:30	3389	closed
35.88.232.153	11:35	3389	closed
35.88.232.153	11:40	3389	closed
35.88.232.153	11:45	3389	closed
35.88.232.153	11:50	3389	closed
35.88.232.153	11:55	3389	closed
35.88.232.153	12:00	3389	closed

created_at	updated_at
26-12-19 6:09	4-09-22 5:17
20-04-21 19:37	4-09-22 5:17
26-12-19 6:09	4-09-22 5:17
14-01-20 7:16	4-09-22 5:17
8-09-20 21:22	4-09-22 5:17
8-01-22 15:33	4-09-22 5:17
9-01-22 15:33	4-09-22 5:17
7-06-22 5:45	4-09-22 5:17
25-09-20 21:16	4-09-22 5:17
15-04-19 14:36	
29-06-22 8:49	
10-06-22 8:05	
8-02-20 16:56	
9-02-20 16:56	
4-02-22 1:17	
30-12-20 17:13	
31-12-20 17:13	
20-08-22 18:16	
30-04-22 7:29	4-09-22 5:17
1-05-22 7:29	4-09-22 5:17

35.88.232.153	10:05	3389	closed
35.88.232.153	10:10	3389	closed
35.88.232.153	10:15	3389	closed
35.88.232.153	10:20	3389	closed
35.88.232.153	10:25	3389	closed
35.88.232.153	10:30	3389	closed
35.88.232.153	10:35	3389	closed
35.88.232.153	10:40	3389	closed
35.88.232.153	10:45	3389	closed
35.88.232.153	10:50	3389	closed
35.88.232.153	10:55	3389	closed
35.88.232.153	11:00	3389	closed
	11:05	3389	open
	11:10	3389	closed
	11:15	3389	closed
	11:20	3389	closed
	11:25	3389	closed
	11:30	3389	closed
	11:35	3389	closed
	11:40	3389	closed
	11:45	3389	closed
	11:50	3389	closed
35.88.232.153	11:55	3389	closed
35.88.232.153	12:00	3389	closed

Google cyberattack996@proton.me

https://mandiant.com › blog › known ▾ Vertaal deze pagina

Actor report: APT108

7 mrt. 2022 — APT108 is known for trying to disrupt organisations with national impact, using **cyberattack996@proton.me** as their primary email address for communication..

Wat ga je nu als eerste doen?

Forensisch onderzoekers

Back-ups veiligstellen

Contact opnemen actor

Pers te woord staan

Systemen uitschakelen

Business continueren

Antwoord op menti.com, code: 3462 3678

NOS Nieuws • Vandaag, 14:02

Nederlandse organisatie gehackt, klanten de dupe van haperende dienstverlening

Hackers bieden gestolen gegevens van een grote Nederlandse organisatie aan op het dark web. Het gaat volgens de hackersgroep APT108 om e-mails en documenten met klantdata en interne documentatie. Omdat er persoonsgegevens tussen zitten, is de Autoriteit Persoonsgegevens op de hoogte gebracht.

Hoe had je deze crisis kunnen voorkomen?

IR & crisisplan

Leverancier toetsen

Test op kwetsbaarheden

Compliance-testen

Security awareness

Externe expertise inhuren

Antwoord op menti.com, code: 3462 3678


JOURNAAL

Waar ging het nou om?

- Hacker is zonder detectie systemen binnengedrongen via een service die tijdelijk bereikbaar was via het internet door een configuratiefout

- Bespreek of je wel of niet moet betalen
- Maar ook: hoe ga je om met de media en reputatieschade?

- Zorg voor een up to date ‘Crisis & incident response-plan’
- Oefen dit plan met regelmaat en “leer door ervaring”

BEDANKT!


Forum
Standaardisatie
Standaard Samenwerken


SIDNfonds


SIDN
Zorgeloos online


dutch
digital
delta
connect and create


TNO
innovation
for life


Over
Informatie
Gesproken


NL AI Coalitie


ai
technology
for people


Ministerie van Justitie en Veiligheid


Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties


Ministerie van Economische Zaken
en Klimaat


Agentschap Telecom
Ministerie van Economische Zaken
en Klimaat


ONLINE TRUST
COALITIE


Veilig internetten.nl


Dutch
Blockchain
Coalition
connect and create