

Cybercrime

The background of the slide features a person wearing a dark hoodie. Their face is obscured by a complex, glowing blue digital network of lines and nodes, resembling a circuit board or a data map. The person's right hand is raised, palm facing forward, and a bright, glowing blue dollar sign (\$) is superimposed on it. The entire scene is set against a dark blue background with a dense, intricate pattern of glowing blue lines and nodes, creating a high-tech, cybernetic atmosphere.

Hanko van Giessen
Account manager Publieke Private Samenwerking
Team Cybercrime Oost-Nederland



Wij werken op baanbrekende en vernieuwende wijze aan het voorkomen, verstoren en opsporen van cybercrime met als doel een weerbare maatschappij en organisatie.



Vershil?

CYBERCRIME

Cybercrime waarbij ICT zowel het doel als het middel is. Delict bestond voorheen niet.

Bijvoorbeeld computervredebreuk, DDoS aanval, ransomware.

GEDIGITALISEERDE CRIMINALITEIT

Cybercrime waarbij ICT het middel is. Delict bestond voorheen al.

Bijvoorbeeld online aan- en verkoopfraude, identiteitsfraude of bedreigingen online.



“New crime, new tools”

*“Old school criminaliteit”,
gepleegd met
nieuwe digitale
middelen*



De brede bestrijding



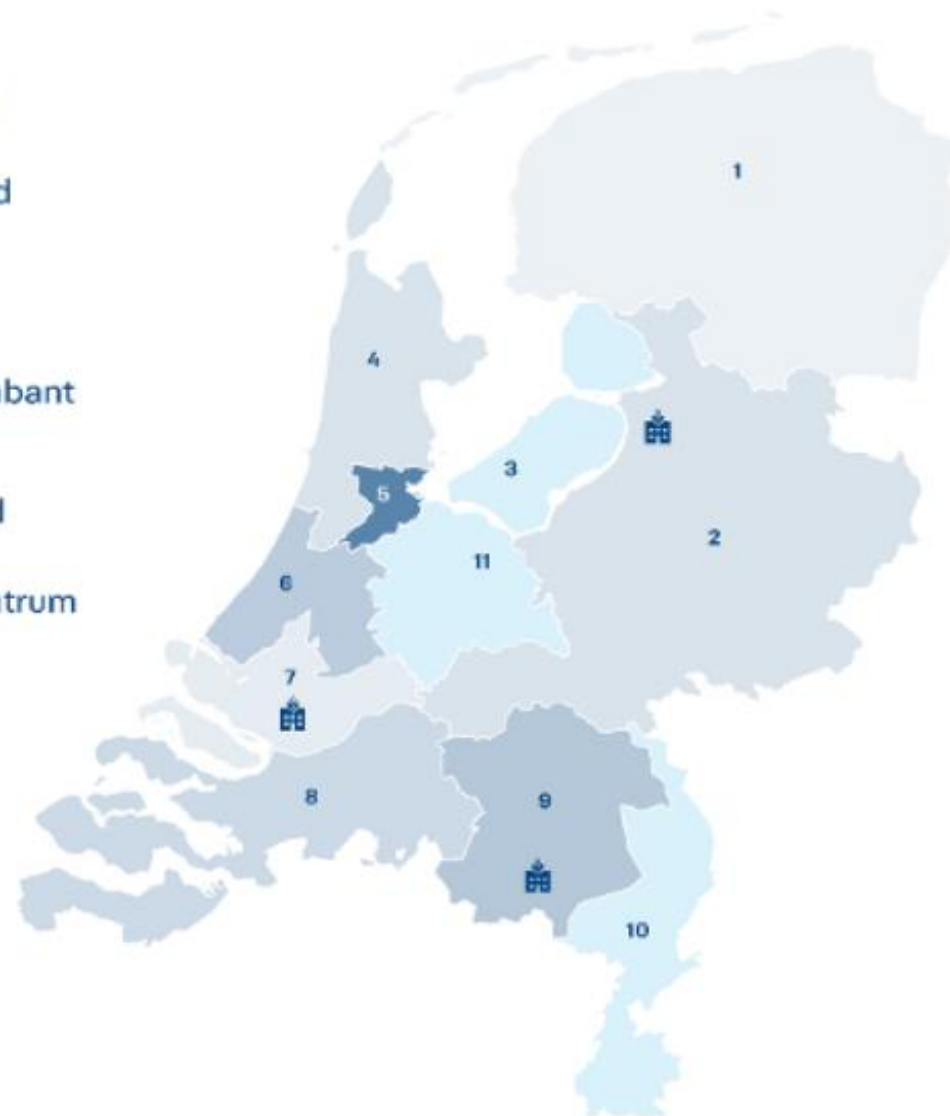
Cybercrime teams

- 11 eenheden
- 10 Cybercrimeteams
- 1 THTC – Landelijke Eenheid

1. Noord-Nederland
2. Oost-Nederland
3. Midden-Nederland
4. Noord-Holland
5. Amsterdam
6. Den Haag
7. Rotterdam
8. Zeeland-West-Brabant
9. Oost-Brabant
10. Limburg
11. Landelijke Eenheid



Politiedienstencentrum



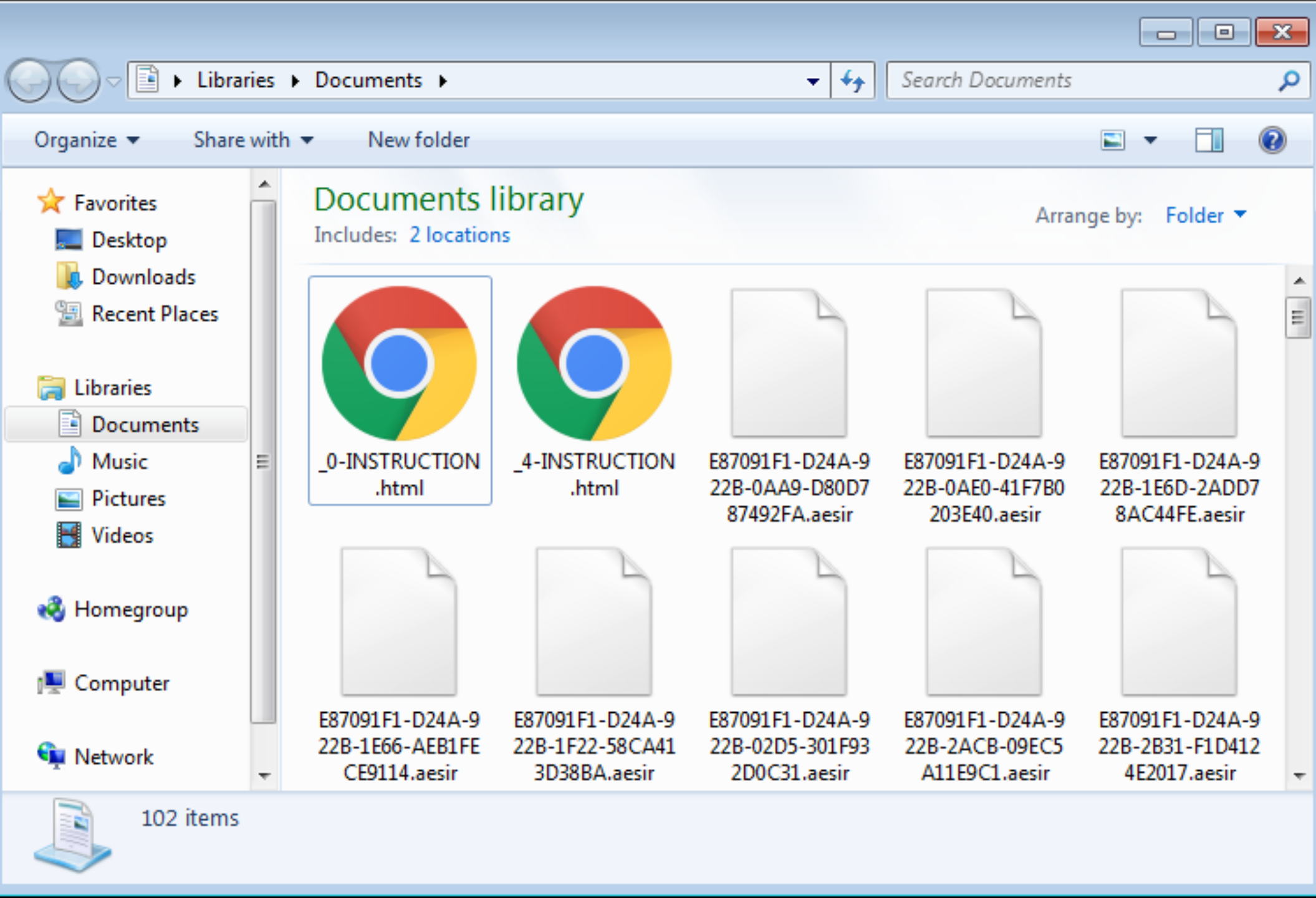
Agenda

- Operatie Yuri
- Operatie Spider
- Operatie Winnie



Casus 1: Operatie Yuri





All your important files are encrypted!
Any attempts to restore your files with the thrid-party software will be fatal for your files!
RESTORE YOU DATA POSSIBLE ONLY BUYING private key from us.
There is only one way to get your files back:

- | 1. Download Tor browser – <https://www.torproject.org/> and install it.
- | 2. Open link in TOR browser – <http://lockbitks2tvnmwk.onion/?E3D94FA5>
This link only works in Tor Browser!
- | 3. Follow the instructions on this page

Attention!

Do not rename encrypted files.

Do not try to decrypt using third party software, it may cause permanent data loss.

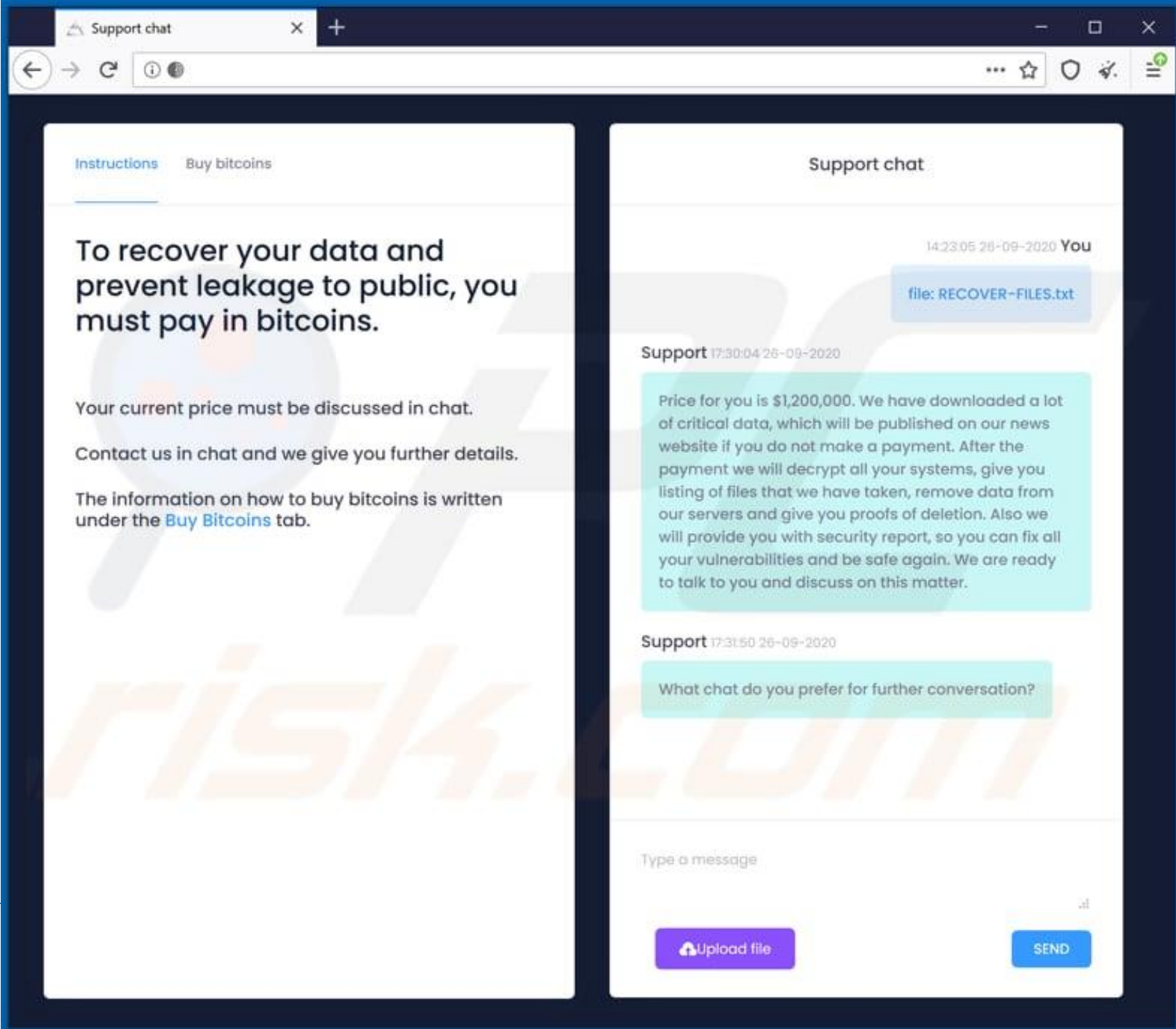
Decryption of your files with the help of third parties may cause increased price(they add their fee to our).

Tor Browser may be blocked in your country or corporate network. Use <https://bridges.torproject.org> or use Tor Browser over VPN.

Tor Browser user manual <https://tb-manual.torproject.org/about>

!!! We also download huge amount of your private data, including finance information, clients personal info, network diagrams, passwords and so on.
Don't forget about GDPR.





Stelling: Wel of niet onderhandelen?



Stelling: Wel of niet betalen?



Operatie Yuri

[Home](#) / [Media & Press](#)



NEWS

Ragnar Locker ransomware gang taken down by international police swoop

Part of the EU Policy Cycle - Empact 



Casus 2: Operatie Spider



Casus Flubot



Your device is infected with the
FluBot[®] malware

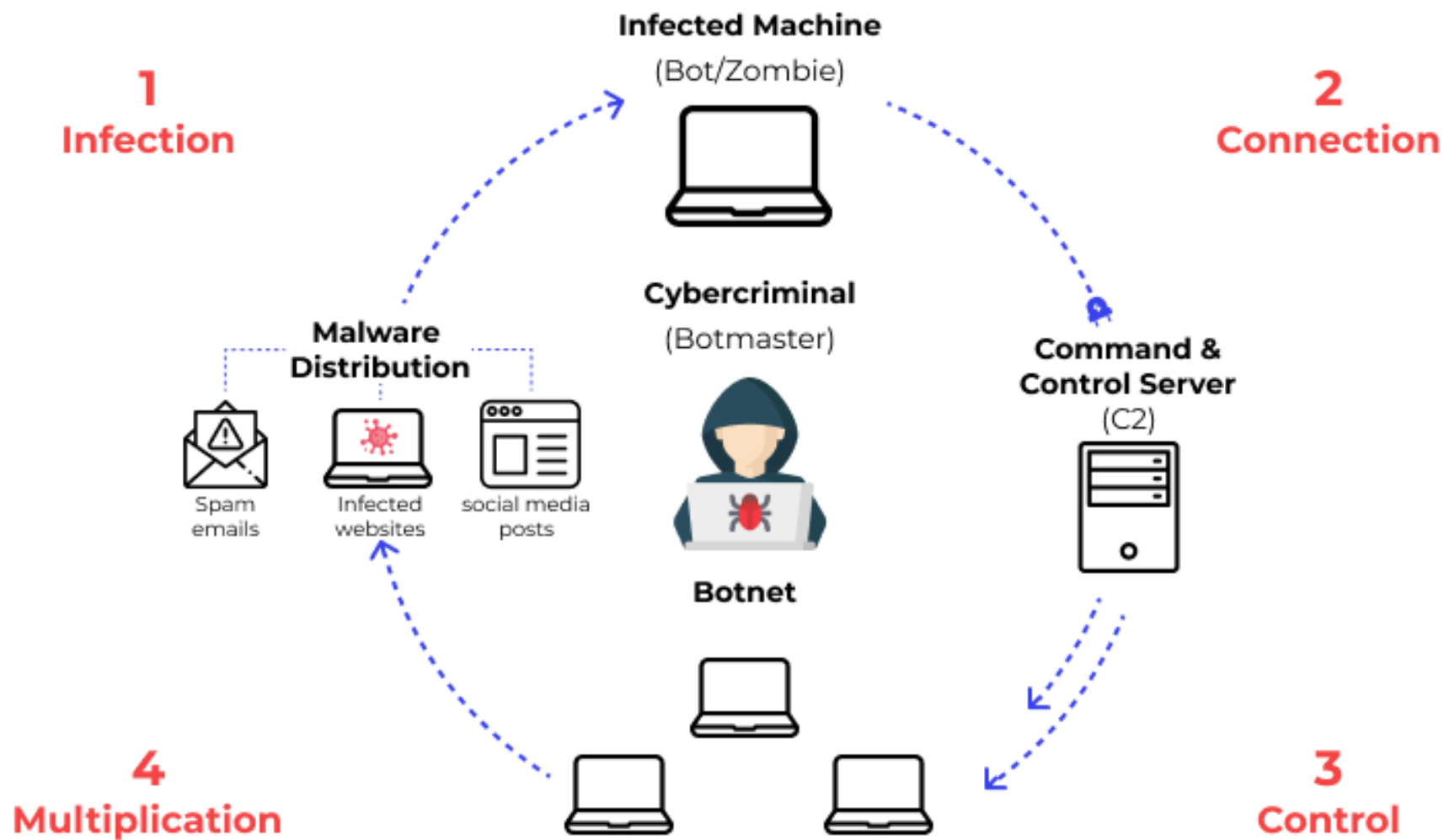
Android has detected that your device has been infected.

FluBot is an Android spyware that aims to steal financial login and password data from your device.

You must install an Android security update to remove FluBot.

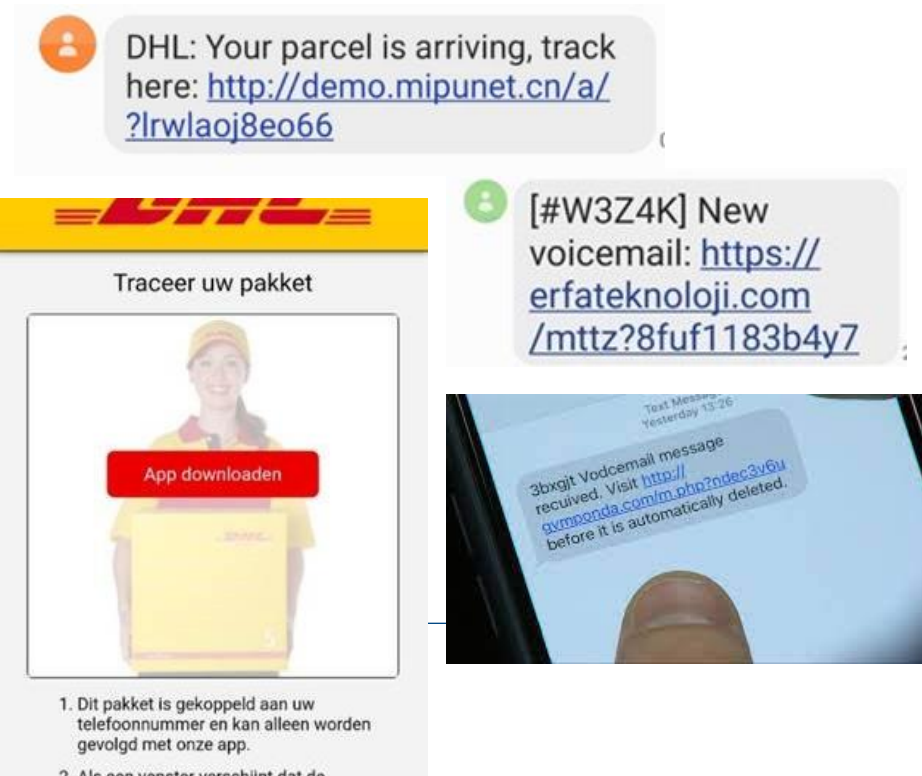
Install security update

How a Botnet works

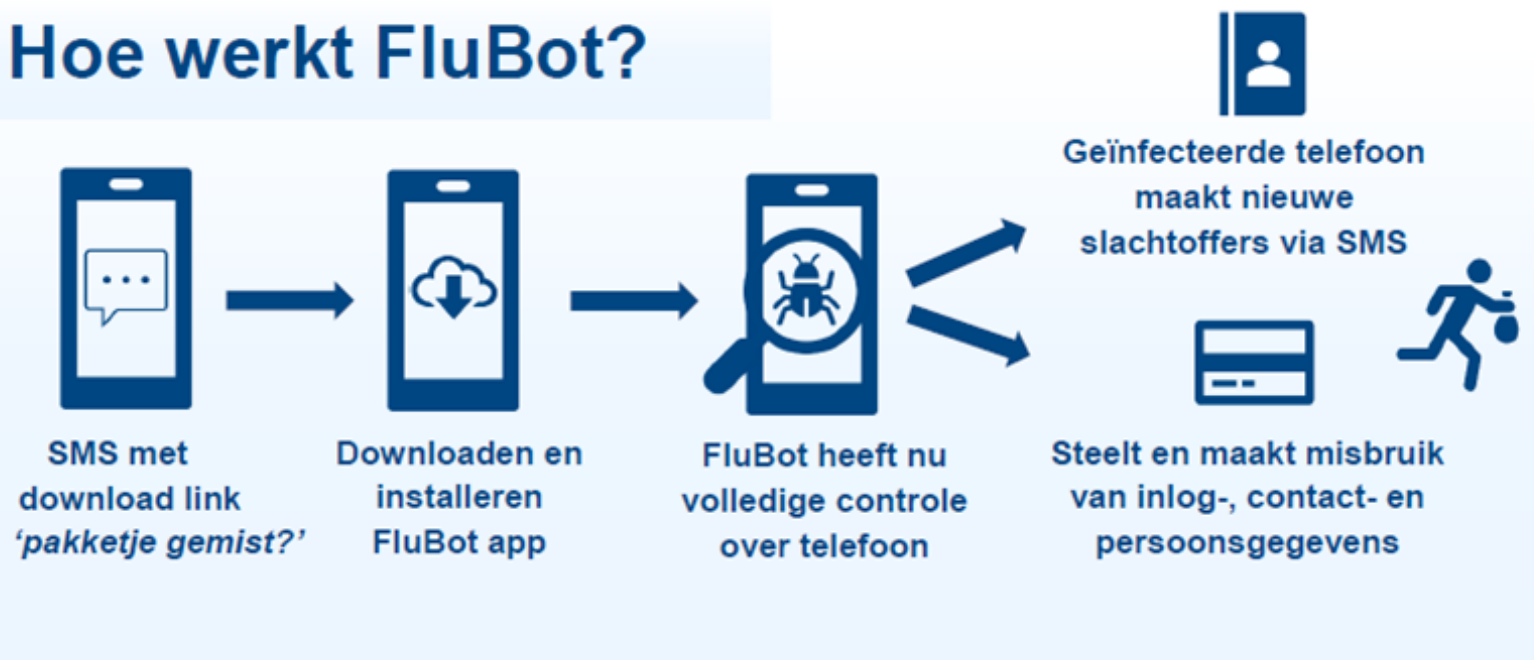


FluBot

- Internationaal
- Besmetting via het downloaden van een fake tracking app
- Verspreiding via SMS



Hoe werkt FluBot?



Stelling: Wel of niet op een externe link klikken?



Schade

1. Hoge telefoonrekeningen
2. Netwerk overbelast
3. Diefstal crypto en geld via internetbankieren
4. Gigantische database aan contact/persoongegevens





Takedown of SMS-based FluBot spyware infecting Android phones

01 JUN 2022

An international law enforcement operation involving 11 countries has resulted in the takedown of one of the fastest-spreading mobile malware to date. Known as FluBot, this Android malware has been spreading aggressively through SMS, stealing passwords, online banking details and other sensitive information from infected smartphones across the world. Its infrastructure was successfully disrupted earlier in May [by the Dutch Police \(Politie\)](#), rendering this strain of malware inactive.



De Nederlandse politie heeft de wereldwijd beruchte Android-malware FluBot weten uit te schakelen. De malware werkt daardoor sinds een maand niet meer. Dat maakt Europol bekend op [zijn website](#).

De Nederlandse politie werkte bij de operatie samen met een aantal internationale partijen waaronder Europol, de United States Secret Service en onder meer de Belgische, Australische en Finse politie. De Joint Cybercrime Action Taskforce (J-CAT) leverde ook ondersteuning bij het onderzoek. Op de dag dat de malware werd uitgeschakeld zette Europol een virtuele commandopost op voor de coördinatie tussen alle betrokken autoriteiten. Op dit moment proberen de organisaties de personen achter de malware nog te identificeren. Verdere details zijn niet bekendgemaakt.

Emotet

De Nederlandse politie is de laatste tijd vaker betrokken bij internationale operaties. Europol noemde in januari het uit de lucht halen van het Emotet-botnet in Nederland, dat zo'n miljoen systemen had besmet met malware, [één van de belangrijkste vangsten](#) in het afgelopen decennium. De politie maakte gebruik van haar hackbevoegdheid om bij het botnet binnen te dringen.

GERELATEERDE ARTIKELEN



Interpol: Politie moet meer wereldwijd samenwerken tegen cybercriminaliteit



Politie: weer meer cybercrime gepleegd



Politie haalt VPNLab offline wegens criminele activiteiten



tweakers

Nieuws

Reviews

Pricewatch

Vraag & Aanbod

Forum

Carrière

Meer

Zoek naar nieuws

Nederlandse politie verstoort infrastructuur van FluBot-Android-malware

De Nederlandse politie heeft in mei de infrastructuur van FluBot verstoord, waardoor deze nu niet meer actief is. FluBot werkte met een sms die zogenaamd van een pakketbezorger kwam en kon wachtwoorden en bankinformatie stelen. De malware bestond sinds eind 2020.

[Europol meldt](#) dat de infrastructuur in mei offline werd gehaald door [het cybercrimeteam van de Oost-Nederlandse politie](#), na een onderzoek waar elf landen aan meewerkten. Ook de Belgische politie werkte aan het onderzoek mee. Europol coördineert het onderzoek en zegt dat verdachten nog worden geïdentificeerd.

Hoe de Nederlandse politie de infrastructuur van FluBot kon verstoren, is niet bekend. De infrastructuur is nu 'onder de controle' van politiediensten, schrijft Europol. De Nederlandse politie zegt op het moment van schrijven 10.000 slachtoffers te hebben losgekoppeld van het FluBot-netwerk en daarbij de verspreiding van 6,5 miljoen sms'jes te hebben voorkomen.

FluBot werd voor het eerst in december 2020 ontdekt en wist in het jaar daarop veel apparaten te infecteren. De malware verspreidde zich via een sms-bericht en vroeg ontvangers een app te installeren om een pakket te volgen, of om naar voicemailberichten te kunnen luisteren. Met de link downloaden gebruikers in werkelijkheid FluBot.



Casus 3: Operatie Winnie



Corrie 75 Slachtoffer Bankhelpdeskfraude



- 200.000 euro

Casus Winnie

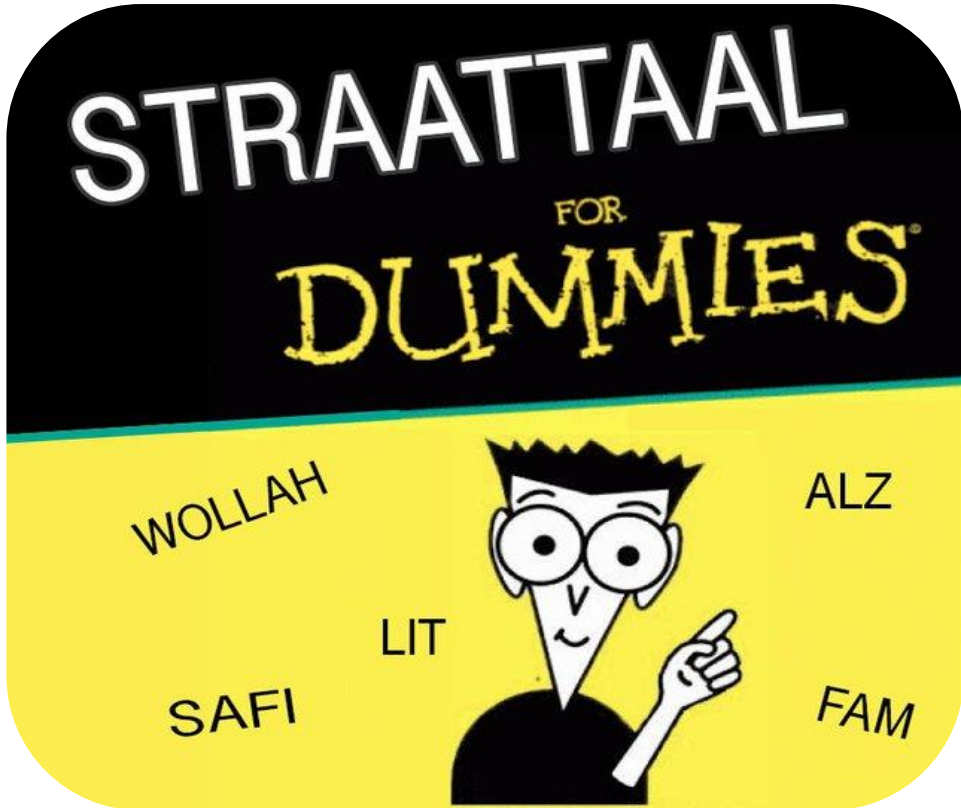
14 november 2020 melding vanuit vakantiepark Ede

- Mogelijke oplichtingspraktijken
- Heterdaad aanhouding 3 personen
- Beslag op diverse gegevensdragers





Casus Winnie – Straattaal



- Djoen = klus/job
- Vis = slachtoffer phishing
- Spitta sturen = pinner of geldophaler sturen
- Klemmen = geld pinnen
- Baro = Rabobank
- Lappie = laptop
- Muur = pinautomaat
- Pap = contant geld
- Dood maken = bankpas is geblokkeerd



Casus Winnie - Vonnis

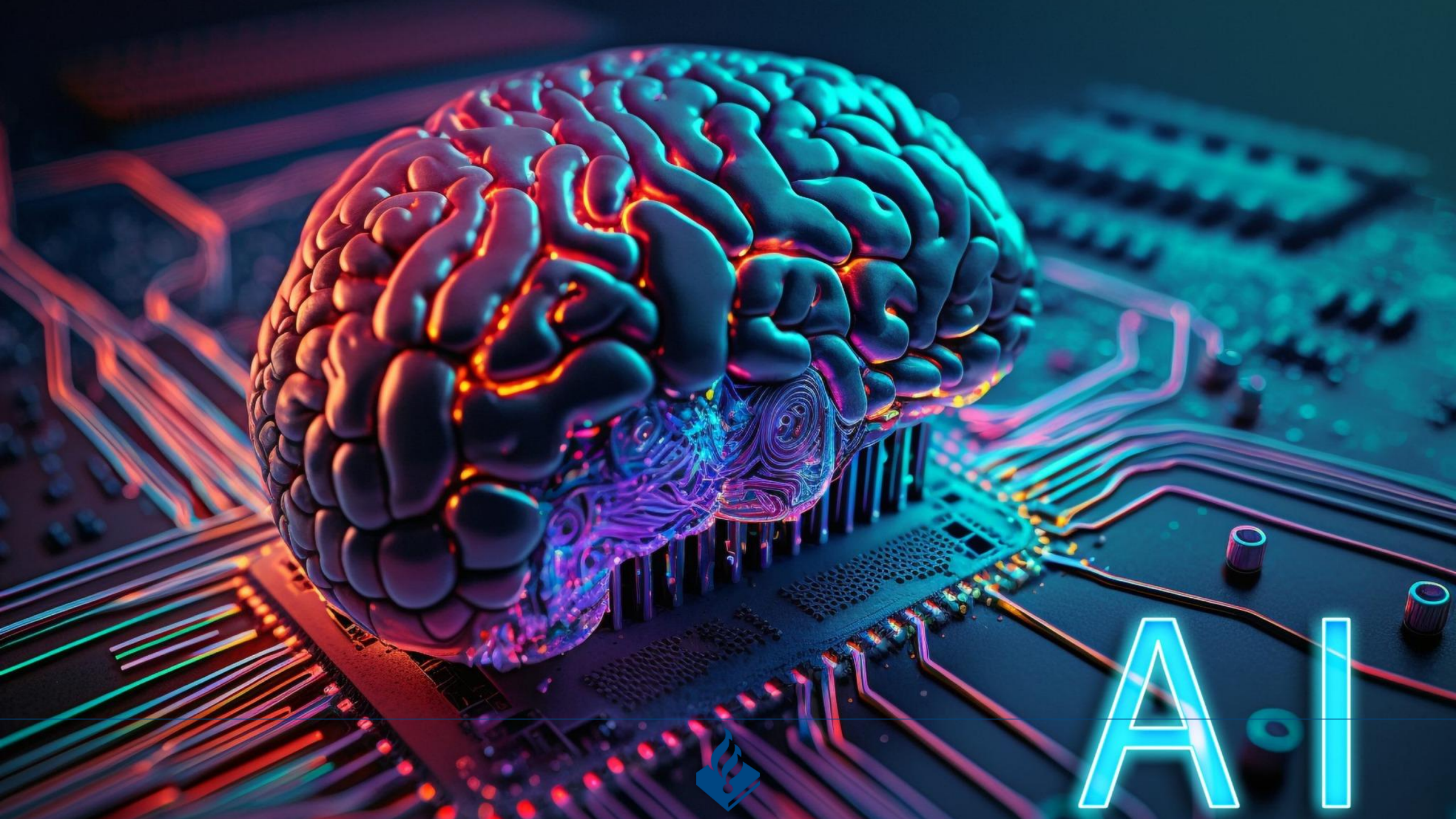
2 Hoofdverdachten

1. **12 maanden gevangenisstraf, waarvan 3 voorwaardelijk**
Schuldig aan samen plegen van 3 oplichtingen en computervredebreuk
2. **Onvoorwaardelijke gevangenisstraf van 2 jaar**
Schuldig aan samen plegen van 8 oplichtingen en computervredebreuk, ook witwassen



Stelling: Wel of niet aangifte doen bij de politie?





AI



7 tips: Voorkom dat je slachtoffer wordt

Internet is niet meer weg te denken uit ons dagelijkse leven. We doen steeds meer online. Ook criminelen zijn online te vinden. Hoe voorkom je dat je slachtoffer wordt van cybercriminelen. Wij zetten een aantal tips voor je op een rij!

Tip 1

Stel tweestapsverificatie in op je WhatsApp. Hoe? Open WhatsApp en ga naar instellingen - Account - Verificatie in twee stappen.

Tip 2

Controleer het als je bent gebeld door jouw eigen bank. Neem zelf contact op met je bank om te kijken of het klopt.

Tip 3

Maak gebruik van sterke en verschillende wachtwoorden of wachtwoordzinnen. Bewaar deze wachtwoorden in een 'wachtwoordkluis'.

Tip 4

Voer beschikbare updates direct uit op je mobiele telefoon, laptop en andere apparaten.

Tip 5

Klik nooit zomaar op een linkje dat je krijgt. Controleren kan op checkjelinkje.nl

Tip 6

Krijg je bericht van een familielid of vriend(in)? Check dit altijd door zelf contact met hem of haar op te nemen. Een belletje is zo gepleegd!

Tip 7

De bank en andere instanties vragen nooit om je pincode of bankpas!

#Echtnietvandaag



« waakzaam en dienstbaar »