# Clausule verhoor ransomware

Heden bied ik me aan bij jullie diensten teneinde een blokkering van mijn gegevens/informaticasysteem aan te geven.

**Algemene gegevens**

Om welke besmet informaticasysteem gaat het?

- ☐ Stand-alone PC
- ☐ Laptop
- ☐ Tablet
- ☐ Smartphone
- ☐ Server
- ☐ Netwerk
- ☐ Cloud
- ☐ Externe gegevensdrager
- ☐ Huishoudtoestel
- ☐ Wagen
- ☐ Andere:

Wat is het besturingssysteem van het informaticasysteem?

- ☐ Windows 7
- ☐ Windows 8
- ☐ Windows 10
- ☐ Linux
- ☐ Mac OS X
- ☐ IOS
- ☐ Android
- ☐ Andere:

Werd er een antivirus-programma geïnstalleerd?

- ☐ Ja, welk:
- ☐ Neen

Wie is de eigenaar (bedrijf, particulier, …) van het besmette informaticasysteem?

Heeft u de hulp ingeroepen van een ICT-medewerker of een ICT-bedrijf?

☐ Ja ☐ Neen

Contactgegevens:

Bent u de enige die dit informaticasysteem gebruikt? Heeft er nog iemand (collega, gezinslid, ict-medewerker, …) toegang tot uw informaticasysteem?

Wie kan gecontacteerd worden in het kader van het verder onderzoek en hoe (e-mailadres, GSM, …)?

**Wijze van besmetting**

Wanneer werkte het informaticasysteem nog correct?

Door wie en wanneer werd vastgesteld dat het informaticasysteem niet meer correct functioneerde?

Door welke handeling functioneerde het informaticasysteem niet meer correct?

- ☐ Downloaden (hierbij de URL en website vermelden)
- ☐ Websitebezoek (hierbij de URL en website vermelden)
- ☐ Klikken op hyperlink in ontvangen e-mailbericht
- ☐ Openen van bijlage in ontvangen e-mailbericht
- ☐ Andere:

Bent u in het recente verleden slachtoffer geworden van een storing of inbraak in uw computersysteem of inbraak in uw woning/bedrijfsgebouw?

- ☐ Neen
- ☐ Ja, namelijk:

**Uitzicht van het ransomwarescherm**

Op welke wijze heeft het ransomwarescherm zich gemanifesteerd (m.a.w. wat zie je)?

- ☐ Pop-up op scherm
- ☐ txt-bestand op bureaublad
- ☐ txt-bestand in de mapstructuur
- ☐ HTML-bestand op bureaublad
- ☐ HTML-bestand in de mapstructuur
- ☐ Andere:

Bent u in het bezit van een screenshot/foto van de pop-up of een afdruk van het txt-bestand en/of HTML-bestand?

- ☐ Ja en ik overhandig u deze
- ☐ Neen, maar ik zal u deze bezorgen. Ik kan reeds onderstaande informatie meedelen m.b.t. het uitzicht van het ransomwarescherm:
  - ☐ Gebruikte taal:
  - ☐ Eventuele naam van de ransomware op het scherm vermeld:
  - ☐ Logo's:
  - ☐ Kleuren:
  - ☐ De te volgen instructies m.b.t. de betaling:
  - ☐ Andere:
- ☐ Neen en ik kan/zal u er geen bezorgen om volgende reden:
  Ik kan evenwel onderstaande informatie meedelen m.b.t. het uitzicht van het ransomwarescherm:
  - ☐ Gebruikte taal:
  - ☐ Eventuele naam van de ransomware op het scherm vermeld:
  - ☐ Logo's:
  - ☐ Kleuren:
  - ☐ De te volgen instructies m.b.t. de betaling:
  - ☐ Andere:

**Aard van de besmetting**

- ☐ Het informaticasysteem is volledig geblokkeerd
- ☐ Het informaticasysteem is gedeeltelijk geblokkeerd, namelijk:
- ☐ Het informaticasysteem functioneert nog maar bepaalde bestanden/mappen werden versleuteld
  Welke gegevens werden er versleuteld?
  - ☐ Office bestanden (Word, Excel, PowerPoint, ...)
  - ☐ Afbeeldingen

- ☐ PDF-formulieren
- ☐ Videobestanden
- ☐ Boekhouding
- ☐ Master Boot Record
- ☐ Back-ups
- ☐ één of meerdere bestandsmappen
- ☐ Andere:

M.b.t. de versleutelde gegevens, bent u in het bezit van een screenshot/foto van deze mappenstructuur?

- ☐ Ja en ik overhandig u deze
- ☐ Neen, maar ik zal u deze bezorgen
- ☐ Neen en ik kan/zal u er geen bezorgen om volgende reden:

In welke nieuwe extensie werden de gegevens gewijzigd (bijvoorbeeld van .docx naar docx.locked)?

Werden er gegevens vernietigd of wordt ermee gedreigd?

- ☐ Neen
- ☐ Ja, het betreft de volgende gegevens:

Werden er gegevens gestolen?

- ☐ Neen
- ☐ Ja, het betreft de volgende gegevens:
- ☐ Wordt ermee gedreigd deze gestolen gegevens te publiceren?
  ☐ Neen ☐ Ja

**Betaling van het losgeld**

Op welke wijze werden de instructies tot betaling gegeven?

- ☐ Website via aan te klikken link (hier screenshot en URL bijvoegen)
- ☐ Mailverkeer
- ☐ Telefonisch
- ☐ Chat
- ☐ Andere:

Op welke wijze en hoeveel dient er betaald te worden om de bestanden terug vrij te geven?

- ☐ Bitcoins op volgende Bitcoinrekening (tussen de 26 en 35 karakters, beginnend met een 1 of een 3):
- ☐ Andere virtuele valuta op volgende valutarekening:
- ☐ Andere:

Heeft u betaald?

☐ Ik heb het gevraagde bedrag niet betaald. De bestanden zijn nog versleuteld of het informaticasysteem is nog geblokkeerd. Ik ben niet van plan te betalen.
Ik neem er kennis van dat een herinstallatie van het systeem dient overwogen te worden. Verder wordt mij aangeraden mijn wachtwoorden (en veiligheidsvragen) te wijzigen.

☐ Ik heb het gevraagde bedrag niet betaald. De bestanden zijn nog versleuteld of het informaticasysteem is nog geblokkeerd. Ik ben wel van plan te betalen.
Ik neem er kennis van dat na betaling de versleutelde bestanden mogelijks zullen vrijgegeven worden of het informaticasysteem zal gedeblokkeerd worden, maar dat het informaticasysteem nog altijd kan geïnfecteerd zijn en dat een herinstallatie van het systeem dan ook dient overwogen te worden. Verder wordt mij aangeraden mijn wachtwoorden (en veiligheidsvragen) te wijzigen.

☐ M.b.t. de geplande betaling, gelieve ons te bezorgen:
- Transaction ID (kopie bijvoegen):
- Naam van de exchanger waar de Bitcoins werden aangekocht:
- Aankoopbewijs van de virtuele munt:
- Datum en uur van betaling:
- Indien u een decryptiesleutel of een mogelijkheid tot deblokkering zou ontvangen, de wijze waarop en de datum en uur:

☐ Ik heb het gevraagde bedrag reeds betaald, maar de bestanden zijn nog versleuteld of het informaticasysteem is nog geblokkeerd.
Ik neem er kennis van dat een herinstallatie van het systeem dient overwogen te worden. Verder wordt mij aangeraden mijn wachtwoorden (en veiligheidsvragen) te wijzigen.

☐ M.b.t. de uitgevoerde betaling, gelieve ons te bezorgen:
- Transaction ID (kopie bijvoegen):
- Naam van de exchanger waar de Bitcoins werden aangekocht:
- Aankoopbewijs van de virtuele munt:
- Datum en uur van betaling:
- Indien u een decryptiesleutel of een mogelijkheid tot deblokkering ontving, de wijze waarop en de datum en uur:

☐ Ik heb het gevraagde bedrag reeds betaald. De bestanden werden vrijgegeven of het informaticasysteem werd gedeblokkeerd.
Ik neem er kennis van dat, ondanks het feit dat de versleutelde bestanden werden vrijgegeven of het informaticasysteem werd gedeblokkeerd, het informaticasysteem nog altijd kan geïnfecteerd zijn en dat een herinstallatie van het systeem dient overwogen te worden. Verder wordt mij aangeraden mijn wachtwoorden (en veiligheidsvragen) te wijzigen.

☐ M.b.t. de uitgevoerde betaling. Gelieve ons te bezorgen:
- Transaction ID (kopie bijvoegen):
- Naam van de exchanger waar de Bitcoins werden aangekocht:
- Aankoopbewijs van de virtuele munt:
- Datum en uur van betaling:
- Datum en uur en de wijze waarop u de decryptiesleutel of een mogelijkheid tot deblokkering heeft ontvangen:

Is er nog andere schade naast het besmet informaticasysteem?

**Communicatie met de verdachte**

Is er mailverkeer geweest tussen u en de verdachte?

☐ Neen
☐ Ja
Bent u (nog) in het bezit van die berichten?
☐ Ja ☐ Neen
Ik zal u die berichten overmaken om bij het dossier te voegen.
Zijn de e-mailheaders van die berichten (nog) beschikbaar?
☐ Ja ☐ Neen
Ik zal u die e-mailheaders overmaken om bij het dossier te voegen.
Wat was het e-mailadres van verdachte en welke naam gebruikte deze?

Is er telefonisch contact geweest tussen u en de verdachte?

☐ Neen
☐ Ja
Mijn (DEFTEL)nummer betreft:

Datum, tijdstip en duur van de gesprekken:
Oproepnummer verdachte:
Door verdachte gebruikte naam:
Ik geef hierbij de onvoorwaardelijke en vrijwillige toestemming aan het Parket om het onbekend oproepnummer te laten identificeren.
Bent u in het bezit van een opname van het gesprek?
☐ Neen
☐ Ja en ik zal deze bezorgen.

Is er contact via chat (Skype, Bitchat, Torchat, …) geweest tussen u en de verdachte?

☐ Neen
☐ Ja
Gebruikt chatprogramma:
Datum, tijdstip en duur van de chatgesprekken:
Gebruikersnaam verdachte:
Bent u in het bezit van screenshots en/of logfiles?
☐ Ja ☐ Neen
Ik zal u deze overmaken om bij het dossier te voegen.

Zal er in de toekomst nog contact volgen met de verdachte?
☐ Neen
☐ Ja, via ☐ mail
☐ telefoon
☐ chat

**Forensische kopie**

Ik neem er kennis van dat het aangewezen is dat het RCCU een forensische kopie neemt van het informaticasysteem en dit om verder onderzoek mogelijk te maken.
☐ Ik geef hierbij mijn onvoorwaardelijke en vrijwillige toestemming
☐ Ik geef hierbij geen toestemming om volgende reden:

☐ Ik doe vrijwillig afstand van de geïnfecteerde harde schijf.
☐ Ik doe geen afstand van de geïnfecteerde harde schijf.

**Doorverwijzing**

Ik neem er kennis van dat ik voor verdere informatie en advies over ransomware terecht kan op volgende websites:
Particulieren: https://www.nomoreransom.org en htpps://www.safeonweb.be
Bedrijven: https://www.nomoreransom.org en https://cert.be

Ik neem er kennis van dat het gebruik van aangeboden decryptietools gebeurt op eigen verantwoordelijkheid.

**Andere opmerkingen:**