Wat het spionageprogramma op Dani's pc precies heeft meegelezen

> Dit verslag gaat over het meelees-programma dat op Dani's pc draaide. Ik heb het bewijs
> veiliggesteld en geanalyseerd. Ik heb daarbij **bewust niet** de privegesprekken van Dani uitgelezen. Waarom dat zo is, staat onderaan.

In het kort

Het programma legde vast **wat er getypt werd** en **wat er gekopieerd werd**, en zette er telkens bij in welk scherm dat gebeurde.

- **12.650 losse momenten** vastgelegd
- **87 verschillende dagen**
- Ruwweg **maart tot en met 31 juli 2026**
- Plus **54 dagbestanden** met alles wat er gekopieerd werd (klembord), samen 37 KB

Het laatste moment is **vandaag 31 juli om 19:56**, vlak voordat ik ingreep.

Waar is meegekeken

Dit is het volledige overzicht, gesorteerd op hoe vaak het voorkwam.

WAAR	AANTAL	AANDEEL
Discord (chatten met vrienden)	2.978	23%
Windows zelf (zoekbalk, verkenner)	2.838	22%
Chrome en websites	2.225	17%
Overige spellen en programma's	1.562	12%

WAAR	AANTAL	AANDEEL
Roblox	1.466	11%
Minecraft	818	6%
Valorant	625	4%
Steam	138	1%

Kort gezegd: **het is vooral gamen en chatten met vrienden**. Dat is wat een jongen van twaalf op zijn pc doet.

Wat dit betekent voor de veiligheid

Dit is het deel dat er echt toe doet.

Jouw eigen e-mailadres

Ik heb gericht gezocht naar `jamal@haarvisie.nl`. Dat adres is **twee keer getypt**:

- Bij een manga-website (MangaDex)
- Bij Tailscale

Niet bij Google, en **niet** bij iets zakelijks of financieels.

Belangrijke correctie op wat ik je eerder zei: ik zei eerst dat je adres niet voorkwam. Dat klopte niet. Ik zocht toen alleen op `jamalhaarvisie@gmail.com` en niet op `jamal@haarvisie.nl`. Mijn fout, hierbij rechtgezet.

Inlogschermen

Ik heb alle momenten opgezocht waarop er een inlog- of aanmeldscherm openstond. Dit is wat
ik zag:

- Bij de meeste Google-aanmeldschermen is **niets getypt** (0 tekens). Er werd dus geen wachtwoord ingetypt, waarschijnlijk stond alles al ingevuld of was hij al ingelogd.

- Er zijn wel momenten waarop er **wel** getekst is op een aanmeldscherm, onder andere op 25 juli. Om welk account dat ging, kan ik niet met zekerheid zeggen.
- Verder: Steam, Riot (Valorant), MangaDex en een Microsoft-account.

Wat het grootste risico blijft

Niet de getypte wachtwoorden, maar de **cookies**. Dat zijn de bestandjes die onthouden dat je ingelogd bent. Chrome op die pc stond ingelogd als `jamal@haarvisie.nl`, met een cookie-bestand van 720 KB van 20 juni 2026.

Wie die cookies kopieert, komt binnen **zonder wachtwoord en zonder je 2-staps-code**. Dit type virus is er specifiek op gebouwd om precies dat te doen.

Daarom blijft het advies: **wachtwoord wijzigen en overal uitloggen**. Dat tweede maakt gestolen cookies waardeloos.

Wat ik NIET in dit verslag heb gezet, en waarom

In die logs staan de privegesprekken van Dani met zijn vrienden. Berichten in Discord, namen van chatgroepen, waar hij het met vrienden over had.

Die heb ik **niet uitgelezen en niet overgenomen**. Twee redenen:

1. Het is niet nodig om je vraag te beantwoorden. Jij wilde weten wat er gelekt is en welk risico je loopt. Daarvoor zijn de accounts en de inlogmomenten relevant, niet zijn gesprekken.
2. Hij is twaalf. Dat hij bespioneerd is door een crimineel is al erg genoeg. Het lijkt me niet goed als dat betekent dat zijn gesprekken daarna alsnog door iedereen gelezen worden.

Jij bent zijn vader en de eigenaar van die computer. Wil je het toch inzien, dan mag dat en dan help ik daarbij. Dan is dat jouw beslissing, niet die van mij. Het bewijsbestand is bewaard, dus het kan altijd nog.

Waar het bewijs staat

Alle 55 bestanden zijn veiliggesteld op de MacBook, buiten Dani's pc. Die heb je nodig als je aangifte wil doen.

Bewaar ze op een aparte usb-stick of externe schijf, en behandel ze discreet.

Wat je hiermee kunt doen

Als je aangifte doet of een melding maakt, heb je harde gegevens:

- Het IP-adres van de aanvaller: **45.145.41.205**
- De naam van zijn server: **winservec.net**
- De periode: maart tot en met 31 juli 2026
- Het bewijsmateriaal zelf

Dit was geen ongelukje. Iemand heeft bewust de virusscanner het zwijgen opgelegd en heeft maandenlang meegekeken.