Onderzoek naar de virussen op Dani's pc, hoe ze binnenkwamen en wat er nu moet gebeuren

---

1. Het antwoord in drie zinnen

Het is vrijwel **zeker** dat de eerste infectie binnenkwam via een gekraakt spel dat op 5 november 2025 om 17:53 werd gestart, want ruim tien minuten na de eerstvolgende keer inloggen stond de achterdeur op de pc, en er is in dat hele tijdvak niets anders verdachts uitgevoerd.

Bij de tweede infectie van 6 maart 2026 weten we **wel precies wanneer** het gebeurde, maar **niet waardoor**, en dat is een vermoeden dat we niet hard kunnen maken: het spel Geometry Dash stond op dat moment op de voorgrond, dus een mod of een custom level daarvan is de meest logische route, maar bewijs daarvoor ontbreekt.

De rode draad is wel duidelijk en die is **zeker**: de pc staat vol gekraakte spellen en nep-installers, en er zijn in totaal **drie losse infecties** gevonden, waarvan er een toetsaanslagen heeft meegelezen **tot en met vandaag**.

Wat we expliciet **niet zeker weten**:

- Welk bestand of programma exact de achterdeur heeft neergezet op 6 november 2025.
- Welk bestand of programma de stealer heeft neergezet op 6 maart 2026.
- Of de aanvaller op 12 mei 2026 zelf op de pc zat, of dat zijn programma dat automatisch deed.

---

2. Tijdlijn infectie 1: de achterdeur, 5 en 6 november 2025

Wat een achterdeur doet: iemand van buiten kan de pc overnemen en meekijken, zonder dat er iets op het scherm te zien is.

Woensdag 5 november 2025

- **17:40:30** Dani logt in op de pc.

- **17:51:11** in de map Downloads verschijnt de map `Guilty-as-Sock-SteamRIP.com`. Dat is een gekraakt spel van de site SteamRIP. Deze download staat in **geen enkele** browsergeschiedenis, dus hij is buiten de browser om binnengekomen.
- **17:53:34 en 17:53:38** het bestand `StandaloneWindows64.exe` uit die map wordt **echt gestart**. Dit staat letterlijk in een Windows-logboek. Windows tekende erbij aan dat het programma iets deed wat op een stuurprogramma diep in Windows lijkt. Dat is geen normaal spelgedrag.
- **20:29:58** Dani logt uit.

Donderdag 6 november 2025

- **12:14:54** Dani logt weer in.
- **12:25:10 tot 12:25:18** de map `CrosshairX` wordt uitgepakt in Downloads. Dat is een hulpprogramma voor gamers.
- **12:25:33** de map `C:\Program Files (x86)\Windows MVC` wordt aangemaakt. Dat is de achterdeur. Dat is **23 seconden** na CrosshairX.

Wat de achterdeur precies is:

- Het is het programma **ScreenConnect**, een legaal hulpprogramma voor computerhulp op afstand, hier misbruikt.
- Het is vermomd als een Windows-onderdeel met de naam **Microsoft Visual C++**, zodat het in de lijst met diensten niet opvalt.
- Alle zichtbaarheid was **uitgezet**: geen icoontje, geen balk, geen melding. Je kunt dus niet zien dat er iemand meekijkt.
- Hij belt naar de server `winservec.net` op poort 8041. Achter die naam zit het IP-adres **45.145.41.205**.
- De pc heeft bij de aanvaller een eigen kenmerk: `140337ae-769f-4dc1-8fd6-b62bb2cc9c3c`.
- Deze dienst is inmiddels **gestopt en uitgeschakeld**.

Eerlijk over de onzekerheid: die 23 seconden tussen CrosshairX en de achterdeur is het strakste tijdsverband dat gevonden is, maar er is **geen bewijs** dat CrosshairX zelf kwaadaardig is. Het gekraakte spel van de dag ervoor is de waarschijnlijkste bron, want dat is aantoonbaar uitgevoerd.

3. Tijdlijn infectie 2: de meelezer, 6 maart 2026

Wat dit doet: het leest alles mee wat er getypt wordt, plus alles wat er gekopieerd wordt, en houdt bij in welk programma dat gebeurt.

Vrijdag 6 maart 2026, de gewone avond eerst

- **15:45** Valorant en de vr-brille starten op.
- **17:24** de Rockstar-launcher wordt bijgewerkt, dus gta.
- **19:03 tot 19:48** weer Valorant en vr, en browsen in Edge.
- **20:16 tot 20:45** een vr-sessie in SteamVR en een Steam-download.
- **21:44:15** het spel **Geometry Dash** schrijft een muziekbestand weg van 4,8 megabyte. Dat is dus 42 seconden voor de infectie.

Dan de infectie zelf, binnen 17 seconden

- **21:44:57** in de map `C:\Users\Public` verschijnen in één keer **vijf bestanden**: `script.vbs`, `cap.ps1`, `1.vb`, `secret_bytes.txt` en `msgbox.txt`. Dat is de complete set.
- **21:45:06** er wordt een geplande taak aangemaakt met de naam **MasterPackager.Updater**. Die zorgt dat het virus na elke herstart weer start.
- **21:45:10** de map `Keyboard` wordt aangemaakt in Dani's profiel.
- **21:45:14** het meelees-bestand `Log.tmp` wordt aangemaakt. De **eerste regel** die erin staat is de naam van het venster dat op dat moment openstond, en dat is **Geometry Dash**.
- **21:54:46** Dani logt uit.
- **22:44:46** Dani logt weer in en gaat verder gamen, terwijl het virus al draait.
- **23:12:25** alle vijf bestanden in `C:\Users\Public` worden nog een keer bijgewerkt.
- **7 maart 00:45:13** uitgelogd.

Hoe het virus technisch werkt (kort, voor het dossier)

- `script.vbs` start `cap.ps1`.
- `cap.ps1` maakt uit `secret_bytes.txt` en `msgbox.txt` een versleuteld programma weer leesbaar en laadt dat **rechtstreeks in het geheugen**, dus zonder een bestand op de schijf.

- Dat programma verstopt zich in een echt Windows-onderdeel met de naam `RegAsm.exe`. Daarom zie je in de takenlijst niets vreemds.
- Het script had ook een lus die andere PowerShell-vensters **doodde** en zichzelf daarna opnieuw startte. Zo bleef het draaien.

Belangrijke vondst: 12 mei 2026, het moment dat de virusscanner de mond werd gesnoerd

- Van **19 april tot 12 mei 2026** heeft Windows Defender dit virus **elke twee minuten** betrapt en in quarantaine gezet. Honderden meldingen.
- De laatste betrapping was **12 mei om 23:55:13**.
- Om **23:56:40**, dus **87 seconden later**, werden er uitzonderingen in Defender gezet voor onder andere `powershell.exe`, `cmd.exe`, `wscript.exe` en hele schijven.
- Daarna was het **80 dagen stil**, tot vandaag.

Dat betekent dat er op 12 mei iemand of iets doelbewust heeft ingegrepen om de scanner uit te schakelen voor dit virus. Die datum stond nog nergens in het dossier.

Nog erger: er kwam een nieuwere versie

- Op **13 mei 2026 om 16:37:56** verscheen er een **nieuw** bestand `script.vbs` in `C:\Users\Public\Downloads`, van 11.801 bytes. De versie van maart was maar 489 bytes. Dit is dus een uitgebreidere variant, één dag nadat de scanner monddood was gemaakt.

Dit meeleesprogramma draaide tot vandaag

- `Log.tmp` is 4,8 megabyte groot en is **vandaag 31 juli om 19:56:28** nog beschreven.
- In dezelfde map staan **55 losse bestanden met alles wat er gekopieerd is**, netjes per dag, van **8 maart 2026 tot en met 30 juli 2026**. Er is dus bijna vijf maanden lang onafgebroken meegelezen.
- In de logs staan de namen van vensters zoals Valorant, Discord, Snapchat en de tabbladen van Chrome, plus de getypte tekst. Er staan ook privéberichten van Dani in. Die zijn met opzet niet overgenomen in dit verslag.
- Wat we **niet** hebben kunnen vaststellen: welk programma dat bestand vandaag om 19:56 nog beschreef. Dat kan de opruimactie van vanavond zijn geweest, of het virus dat nog liep. Dit blijft een open punt.

Wat er vanavond gebeurde

- Om **20:10** zijn tien Defender-uitzonderingen verwijderd.
- Om **20:11** is de nep-dienst Microsoft Visual C++ gestopt en uitgeschakeld.
- Om **20:31 tot 20:34** heeft Defender de bestanden `script.vbs` en `cap.ps1` en de taak MasterPackager.Updater eindelijk zelf herkend en in quarantaine gezet. De taak was 30 seconden later al weg.

---

4. Wat er nog meer gevonden is

Infectie 3: een nep-spel van 6 januari 2026, en die staat er nog

- Map: `C:\Users\Dani-Jay\Downloads\Free Download Files`, aangemaakt **6 januari 2026 om 19:22:09**.
- Het installatiebestand heet `lnstaIer.py`. Kijk goed: dat is geen "Installer", maar een naam met een verwisselde letter. Dat is een klassieke truc.
- Om **19:31:39** werd het spel gestart. In het eigen logboek van dat spel staat direct daarna de regel `<Response [200]>`. Dat betekent: het spel haalde bij het opstarten iets van internet op. Een normaal spel doet dat niet.
- Om **19:31:44** verschenen er in een **verborgen** map bestanden met wartaal-namen, zoals `Seengqueelprond.uy` en `Dob.lqk`, plus een bestand van 15 megabyte met een willekeurige naam. Precies dezelfde werkwijze als bij infectie 2.
- Om **19:32:47** werd een **opstart-snelkoppeling** gezet met de misleidende naam `agenthost_v4_0_release.lnk`, die verwijst naar `faM37hkV.exe` in die verborgen map.
- Die `.exe` is er nu niet meer, maar **de snelkoppeling staat er nog** en probeert bij elke keer inloggen te starten. Die moet weg.

Nog gevonden

- **Outbyte Driver Updater**, bangmaak-software die zegt dat je stuurprogramma's moet kopen. Tientallen meldingen tussen 30 januari en 1 maart 2026. Vervelend, maar niet de kern.
- **Web Companion** en de **AVG-browser**, ook ongewenste meelifters.
- **AnyDesk** staat erop sinds **8 juli 2026**, met **toegang zonder toestemmingsvraag** aangezet. Dat is precies dezelfde dag als jullie eigen meekijk-scripts, dus dit is vermoedelijk gewoon

van jullie zelf. Maar dit moet je **bevestigen**. Zo niet, dan is dit een tweede achterdeur. AnyDesk-nummer: 1694614503.

- De geplande taak **CapScr** verwijst naar een `cap.ps1` in de map Downloads. Let op: dat is een **onschuldig** schermafbeelding-scriptje van jullie zelf, met per ongeluk dezelfde naam als het virusbestand. Niet verwarren.
- Verder staat de map Downloads vol met gekraakte spellen van SteamRIP, een Nintendo-emulator, gekopieerde spellen en gekraakte videosoftware.

Goed nieuws ook

- Er is **geen** kwaadaardig opstart-item in het register.
- Er is **geen** verstopte persistentie via de diepere Windows-onderdelen.
- Er is op dit moment **geen** actieve verbinding meer naar de server van de aanvaller.
- Behalve de nep-dienst was er geen tweede kwaadaardige dienst.

---

5. Wat dit betekent, en wat er nu moet gebeuren

Wat het betekent, zonder omhaal

Iemand kon van buitenaf op deze pc, en er is bijna vijf maanden lang meegelezen met alles wat er getypt en gekopieerd werd. Dus:

- Elk wachtwoord dat sinds **6 maart 2026** op deze pc is getypt, moet je als **gelekt** beschouwen.
- Elke ingelogde sessie op die pc moet je als **overgenomen** beschouwen.
- Ook de privéberichten van Dani in Snapchat en Discord zijn meegelezen.

Dit is geen ramp die je met een virusscan oplost. Dit vraagt om opruimen én wachtwoorden.

Stap voor stap, in deze volgorde

1. **Gebruik de pc van Dani nu niet meer** om iets in te loggen of te typen. Ook niet "even snel".
2. **Wachtwoorden wijzigen vanaf een ander apparaat**, dus jouw telefoon of jouw eigen computer. Begin bij: Microsoft-account, Google, Snapchat, Discord, Roblox, Steam, Riot voor Valorant, en de e-mail van Dani.

3. Zet bij al die accounts **tweestapsverificatie** aan en klik daarna op **overal uitloggen**. Dat gooit de aanvaller er ook uit.

4. **Denk na of jij zelf ooit iets op die pc hebt gedaan.** Salon-mail, bank, boekhouding, WhatsApp Web, een wachtwoord voorgetypt voor Dani. Wat je daar getypt hebt sinds 6 maart, is meegelezen. Wijzig dat ook.

5. **Windows helemaal opnieuw installeren.** Dat is het advies. Er zijn drie losse infecties, er zat een achterdeur op, en de aanvaller heeft de virusscanner bewust gedempt. Losse bestanden weghalen geeft geen zekerheid.

6. **Voordat je wist: bewaar het bewijs.** Zet de map `Keyboard` met `Log.tmp` en de kopieer-bestanden, plus de bestanden uit `C:\Users\Public`, op een aparte usb-stick of externe schijf. Dat heb je nodig als je aangifte wil doen, en om te zien wat er precies gelekt is. Let op: in die logs staan privéberichten van Dani, dus behandel dat discreet.

7. **Als opnieuw installeren nu niet kan**, doe dan minimaal dit nu al:
   - Verwijder de opstart-snelkoppeling `agenthost_v4_0_release.lnk`.
   - Verwijder de hele map `Free Download Files`.
   - Verwijder de resten in `C:\Users\Public`, inclusief de nieuwere `script.vbs` van 13 mei.
   - Verwijder de map `C:\Program Files (x86)\Windows MVC`.
   - Verwijder de map `Keyboard`, maar pas nadat je een kopie hebt.
   - Controleer of de Defender-uitzonderingen leeg blijven.

8. **Bevestig of AnyDesk van jullie is.** Zo niet: verwijderen, want toegang zonder toestemmingsvraag is een achterdeur.

9. **Controleer de andere apparaten in huis.** Niet omdat het virus zich verspreidt, dat doet het niet, maar omdat Dani's accounts ook op zijn telefoon of tablet staan.

0. **Praat met Dani, zonder verwijt.** Dit is belangrijk. Gekraakte spellen downloaden is voor een jongen van twaalf **volstrekt normaal gedrag**. Hij wilde spellen spelen die geld kosten, en het internet staat vol sites die zeggen dat het gratis kan. Hij kon niet weten dat dit erin zat, want er is niets te zien: het spel werkt gewoon, en het virus doet zijn werk onzichtbaar. Wat hij wel moet weten:

   - Gratis versies van betaalde spellen zijn bijna altijd omgebouwd, en wat er verder in zit kun je niet zien.
   - Dat gaat niet alleen over de pc, maar over zijn eigen accounts en zijn eigen chats.

    - Spreek samen af wat wel mag: een budget voor echte spellen, een gezinsaccount op Steam, of een lijstje met sites die veilig zijn.
    - Maak duidelijk dat hij niet in de problemen zit. Anders vertelt hij het de volgende keer niet als iets vreemd doet.

1. **Overweeg een melding of aangifte.** Je hebt harde gegevens: het IP-adres **45.145.41.205**, de naam **winservec.net** en het kenmerk van de pc bij de aanvaller. Dit was een gerichte achterdeur met alle meldingen uitgezet, geen ongelukje.

---

6. Wat we niet hebben kunnen achterhalen, en waarom

Dit is belangrijk om eerlijk te benoemen. Op de volgende punten is het antwoord "we konden het niet lezen", en dat is niet hetzelfde als "er was niets".

- **De browsergeschiedenis heeft een gat** van augustus 2025 tot juli 2026, precies over beide infecties. In Chrome, Edge, Opera, Opera GX en de AVG-browser. Op de infectiedagen staat er geen enkele download geregistreerd. Vermoeden: de downloads liepen niet via de browser maar via het losse programma **Free Download Manager**, dat op de pc staat. Zeker is dat niet.
- **De map met recent gestarte programma's is leeg** voor beide periodes. Windows ruimt die zelf op.
- **De grote logboeken van Windows zijn te kort.** Het systeem-logboek gaat terug tot 10 mei 2026, het beveiligings-logboek pas tot 30 juli 2026. Ze zijn vol en overschrijven zichzelf. Er zijn geen back-ups. Beide infectiedagen vallen buiten bereik.
- **Het logboek van de taakplanner staat uit.** Dat heeft dus nooit iets vastgelegd. Daarom kunnen we niet zien wie de taak MasterPackager.Updater aanmaakte.
- **De geschiedenis van de virusscanner** gaat terug tot 19 april 2026 en bevat niets uit november 2025 en niets van 6 maart 2026. De scanner heeft die dagen dus **niets gemerkt**.
- **De gebruiks-administratie van Windows is te kort** en bevat geen record van 5 en 6 november 2025 of 6 maart 2026.
- **De Discord-cache van begin maart is weg**, die wordt automatisch geschoond. We kunnen Discord dus niet aanwijzen, maar ook niet vrijpleiten.

- **We weten niet welk programma vandaag om 19:56 nog in het meelees-bestand schreef.** Dat kan de opruiming van vanavond zijn geweest, of nog een stukje virus.
- **De achterdeur houdt zijn eigen logboek niet op de pc**, maar bij de aanvaller. We kunnen dus niet zien wanneer er is meegekeken, of hoe vaak, of wat er gedaan is.
- **Één scan is niet afgemaakt.** Een diepe zoekactie door alle systeemmappen liep na tien minuten nog en is afgebroken. Die is dus niet gemeten. Er kan daar nog iets staan.

Wat er tijdens dit onderzoek wél is gedaan: alleen lezen. Er is niets gewist en niets aangepast, behalve het stoppen van de nep-dienst en het verwijderen van de Defender-uitzonderingen vanavond. De rest heeft de virusscanner zelf gedaan.