



Cyberadvies

Risico op malwarebesmetting tijdens reizen naar China

1 oktober 2025



Cyberadvies

TLP:CLEAR

Risico op malwarebesmetting tijdens reizen naar China

1 oktober 2025

Essentie

- De AIVD heeft bij personen die recent beroepsmatig naar China reisden FlowCloud-malware[1] aangetroffen op hun apparatuur.
- Slachtoffers zijn werkzaam binnen publieke en private organisaties op onderwerpen en dossiers die gevoelig zijn voor China.
- De FlowCloud-malware wordt door middel van fysieke toegang via bijvoorbeeld USB-sticks op laptops geïnstalleerd.
- Ook is bij een aantal personen een kopie gemaakt van hun harddisk, waarna dezelfde malware is geïnstalleerd.
- De AIVD adviseert reizigers naar China om extra alert te zijn op mogelijke spionagepogingen en zich bewust te zijn van de spionagerisico's gericht tegen informatie en apparatuur die op reis wordt meegenomen.
- Om de risico's hiervan zoveel mogelijk te mitigeren adviseert de AIVD om altijd tijdelijke apparatuur te gebruiken tijdens de reis naar China.
- Bovendien adviseren wij om alleen documenten en andere data mee te nemen die nodig zijn tijdens de reis.
- Daarnaast adviseert de AIVD om tijdens de reis deze apparatuur niet uit het oog te verliezen.

[1] FlowCloud is een geavanceerde, in C++ geschreven implant, die drie cruciale componenten omvat:

- Een programma met ingebouwde rootkit-functionaliteit, ontworpen om ongeoorloofde toegang en permanente aanwezigheid te bewerkstelligen op het doelapparaat.
- Een persistentiemodule die ervoor zorgt dat de malware actief blijft na herstarts of andere systeemonderbrekingen, waardoor de hackers een constante controle kunnen behouden over het geïnfecteerde apparaat.
- Een aangepaste backdoor die een verborgen communicatiekanaal naar de command-and-control-server (C2-server) biedt, waardoor aanvallers op afstand toegang hebben tot het systeem voor verdere exploitatie.

TLP:CLEAR

Cyberadvies

TLP:CLEAR

Risico op malwarebesmetting tijdens reizen naar China

1 oktober 2025

Context

De AIVD heeft bij personen die recent beroepsmatig naar China reisden FlowCloud-malware aangetroffen op hun apparatuur. Het installeren van deze malware heeft zeer waarschijnlijk een spionagemotief. Deze personen zijn werkzaam bij zowel publieke- als private organisaties en betrokken bij onderwerpen en dossiers die gevoelig zijn voor China. De FlowCloud-malware wordt door middel van fysieke toegang via bijvoorbeeld USB-sticks op laptops geïnstalleerd.

Naast het installeren van malware is ook vastgesteld dat kopieën gemaakt worden van de harddisk, waarna de malware wordt geïnstalleerd. Indien de harddisk versleuteld is met bijvoorbeeld Bitlocker, dan is het als de actor deze wil ontsleutelen noodzakelijk dat de laptop wordt opengemaakt. Hierbij is het mogelijk dat zichtbare sporen achterblijven op de laptop.

De toegang tot de apparatuur vindt plaats op het moment dat deze gescheiden is van de eigenaar. Dit gebeurt tijdens de deelname aan een diner, vergadering of andere bijeenkomst. Dit kunnen ook georganiseerde verrassingsuitstapjes zijn tijdens het bezoek.



De AIVD adviseert reizigers naar China om extra alert te zijn op mogelijke spionagepogingen en zich bewust te zijn van de spionagerisico's gericht tegen informatie en apparatuur die op reis worden meegenomen.



Cyberadvies

TLP:CLEAR

Risico op malwarebesmetting tijdens reizen naar China

1 oktober 2025

Advies

Beperk zoveel mogelijk het risico om tijdens uw reis naar China slachtoffer te worden van malwarebesmetting. Hiervoor kunt u onderstaande maatregelen treffen.

Maak gebruik van tijdelijke mobiele apparatuur die u alleen op deze bestemming gebruikt. Veel organisaties beschikken al over de mogelijkheid om hiervoor tijdelijke apparatuur te gebruiken. Als dit nog niet het geval is bespreek dan met uw security officer de mogelijkheden hiertoe.

Houd uw apparatuur altijd bij u en laat deze bijvoorbeeld niet achter in een kluis in uw hotelkamer. Het is bekend dat een hotelkluis toegankelijk is voor hotelpersoneel en daarmee ook voor kwaadwillenden die de onbeheerd achtergelaten apparatuur kunnen compromitteren.

Gebruik aparte apparatuur voor applicaties die beschikbaar worden gesteld door, of gelinkt of eventueel verbonden zijn aan de Chinese overheid.

Voorkom dat de apparatuur die u tijdelijk gebruikt verbinding kan maken met uw mail, instant messaging en sociale media.

Sluit gedurende het verblijf en bij terugkomst op kantoor meegebrachte apparatuur niet aan op het netwerk van uw organisatie.

Maak gebruik van harddiskversleuteling van bijvoorbeeld Bitlocker of door de AIVD geëvalueerde producten zoals Hiddn Safedisk en PRIM'X Cryhod. Zorg ervoor dat het apparaat alleen op kan starten met multifactorauthenticatie (pre-bootbeveiliging). Zonder pre-bootbeveiliging met multifactorauthenticatie is het voor statelijke actoren relatief eenvoudig om de versleuteling te doorbreken.

Neem alleen documenten en andere data mee die nodig zijn tijdens de reis.

Maak gebruik van een software restriction policy.

- Voorkom het uitvoeren van onbekende of ongewenste scripts, programma's of executables.
- Zorg dat bestanden niet kunnen worden uitgevoerd vanaf USB-sticks, desktop of downloadfolders.

Wees alert op beschadigingen aan of vreemde gedragingen van meegebrachte apparatuur.



TLP:CLEAR



Cyberadvies

TLP:CLEAR

Risico op malwarebesmetting tijdens reizen naar China

1 oktober 2025

Verder lezen

Raadpleeg onderstaande bronnen voor verdere verdieping:

- [AIVD, Op reis naar het buitenland, d.d. 30 mei 2024](#)
- [AIVD, Geëvalueerde producten](#)
- [ESET Research, A lookback under the TA410 umbrella: Its cyberespionage TTPs and activity, d.d. 27 april 2022](#)
- [Microsoft, BitLocker countermeasures, d.d. 18 juni 2024](#)



Over dit cyberadvies

Het doel van een cyberadvies (CA) is om afnemers door middel van beveiligingsmaatregelen concreet handelingsperspectief te bieden zodat de weerbaarheid tegen statelijke actoren wordt verhoogd. De AIVD biedt dit handelingsperspectief op basis van getoetste inlichtingen, kennis en expertise. Het accent ligt hierbij op de nationale veiligheid.

Verspreiding cyberadvies

Dit document heeft de merking TLP:CLEAR. Onder voorbehoud van de regels op het gebied van auteursrechten kan TLP:CLEAR-informatie onbeperkt worden verspreid (met inachtneming van de toepasselijke voorschriften en procedures voor openbaarmaking van informatie).