Awareness materiaal: Infostealer

Datum: 21 mei 2025
Gemaakt door: Cybersave Yourself & SURFcert

Table of Contents

Introductie **3**

Teksten ***4***

Tekst intranet NL **4**

TekstIntranet EN **6**

Tekst mail NL **8**

Tekst mail EN **9**

Afbeeldingen ***10***

CSY afbeelding **10**

CSY afbeelding NL ..... Error! Bookmark not defined.

CSY afbeelding EN ..... Error! Bookmark not defined.

Stockafbeeldingen **10**

Kant en klare CSY posters en schermafbeeldingen **11**

Colofon **12**

Introductie

Het aantal meldingen over infostealers neemt toe. Ook SURFcert ziet dat infostealers vaker ingezet worden, en daarmee een gevaar vormen voor instellingen. Naast de technische maatregelen die instellingen kunnen nemen (zoals het implementeren van MFA) willen we de instellingen ook ondersteunen om de awareness te verhogen bij medewerkers en studenten. Deze teksten zijn geschreven als hulp middel voor instellingen die de awareness willen verhogen binnen hun instelling.

Vrij te gebruiken
De teksten mogen in hun geheel of gedeeltelijk overgenomen worden en vrij gebruikt zonder vermelding voor interne communicatie.

Gebruik je de (een deel van) het materiaal op een externe website? Vermeld dan ergens op de pagina 'powerd by Cybersave Yourself' met een link naar www.cybersaveyourself.nl

Hierdoor kunnen we zien hoeveel instellingen gebruik maken van het materiaal van CSY. Het helpt voor het onderbouwen van onze huidige en toekomstige dienstverlening vanuit SURF.

Praktische tip
In de teksten vind je op meerdere plekken [contactpunt instelling] en [intranet instelling] terug. Dit kan een servicedesk zijn, het CSIRT/CERT of een speciaal meldpunt.

Vervang [contactpunt instelling] in een keer op alle plekken met de 'zoek en vervang' functie in Word.

1. Ga naar Start > **Vervangen**.
2. Voer in het vak **Zoeken** naar het woord of het zinsdeel in waarnaar u wilt **zoeken**.
3. Voer in het vak **Vervangen** door uw nieuwe tekst in.
4. Kies Alles **vervangen** om alle vermeldingen van het woord of de woordgroep te wijzigen.

Tenslotte
Deze tekst is gemaakt door een werkgroep met medewerkers van Universiteit Twente, Universiteit Utrecht, SURFcert en Cybersave Yourself. Heb je opmerkingen of aanvullingen, laat het weten via info@cybersaveyourself.nl

Dit product komt voort uit de samenwerking communities SCIRT en SCIPR. Op SURF.nl lees je meer over deze communities.

Samen werken we aan een veiligere sector!

Teksten

Tekst intranet NL

Inleiding

Cybercriminelen bedenken continu nieuwe manieren om onze data te pakken te krijgen. Bijvoorbeeld via mail, chat en telefonisch. Maar ook via je laptop of computer; bijvoorbeeld bij het downloaden van software of een applicatie. Aanvallers kunnen kwaadaardige software meesturen, je via een tussenstap iets laten invullen of kopiëren, of je naar een 'valse' omgeving sturen. Dus.....zodra je iets ziet of moet doen dat 'anders is dan anders' of 'niet goed voelt' neem direct contact op met [contactpunt instelling].

Wat zijn infostealers?

Infostealers zijn een vorm van schadelijke software die cybercriminelen gebruiken om persoonlijke informatie van jouw computer of apparaat te stelen. Eenmaal geïnstalleerd op je apparaat, verzamelt de malware onopgemerkt gevoelige informatie en stuurt deze naar de criminelen. Ze kunnen enorme schade veroorzaken als ze niet op tijd ontdekt worden.

Wat voor informatie verzamelen infostealers?

Infostealers richten zich op verschillende soorten gevoelige informatie:

- **Inloggegevens**: Gebruikersnamen en wachtwoorden van e-mailaccounts of sociale media.
- **Financiële gegevens**: Creditcardnummers, bankgegevens en informatie over cryptowallets.
- **Persoonlijke gegevens**: Informatie zoals je naam, adres, telefoonnummer of burgerservicenummer.
- **Systeeminformatie**: Gegevens over de hardware van je apparaat, geïnstalleerde software en beveiligingsprogramma's.

Al deze gegevens zijn voor criminelen waardevol en kunnen worden misbruikt voor identiteitsdiefstal, financiële fraude of verdere cyberaanvallen.

Hoe komen infostealers binnen?

Infostealers kunnen op verschillende manieren op je apparaat terecht komen, vaak zonder dat je het doorhebt:

- **Phishing-e-mails**: E-mails die eruitzien alsof ze van een betrouwbare bron komen, maar die een kwaadaardige link of bijlage bevatten. Als je daarop klikt, wordt de malware geïnstalleerd.
- **Kwaadaardige websites**: Door te klikken op een link naar een geïnfecteerde website of via malvertising (kwaadaardige advertenties) kun je ongemerkt

malware downloaden. Ook een betrouwbare website kan gehackt worden om malware te verspreiden.
- **Illegale software**: Het downloaden van illegale software brengt grote risico's met zich mee. Vaak zijn deze pakketten besmet met malware.
- **Kwetsbaarheden in software**: Sommige infostealers maken gebruik van beveiligingslekken in verouderde software of browsers om je apparaat te infecteren.

Hoe herken je infostealers?

Wordt je op een website gevraagd om iets uit te te voeren omdat je anders niet op de website kan, of vertrouw je een website of email niet? Meld dit zo snel mogelijk bij [contactpunt instelling]

Infostealers zijn ontworpen om ongemerkt te werken wanneer ze actief zijn. Dit zijn signalen waar je op kunt letten:

- Als je bericht krijgt dat je dringend moet inloggen, en het verzoek om dat via de link in de mail/sms te doen.
- Onverwachte e-mails, sociale media berichten of transacties op je bankrekening. Ook berichten van 'bekenden' die vreemd/'anders dan normaal' zijn of die je niet verwacht.
- Als je bericht krijgt om (nogmaals) je 2e factor (MFA) te gebruiken, zonder dat je zelf aan het inloggen bent.

Herken je deze signalen, onderneem dan direct actie en scan je apparaat op malware en/of koppel je apparaat los van internet. Gebeurt dit op een apparaat van je instelling, meld dit dan zo snel mogelijk.

Wat kun je doen tegen infostealers?

- **Gebruik meerdere factoren om in te logen (Multifactorauthenticatie (MFA)**: Dit voegt een extra beveiligingslaag toe, waarbij je bijvoorbeeld een sms-code moet invoeren naast je wachtwoord. Soms moet je dit zelf aanzetten bij je social media accounts.
- **Update je software regelmatig**: Zorg ervoor dat je computer en antivirussoftware up-to-date zijn.
- **Log in door bekende website zelf op te zoeken**: Als je gevraagd wordt om in te loggen, doe dat niet via de link in de mail maar ga naar de officiele pagina.
- **Wees voorzichtig met e-mails**: Open geen verdachte bijlagen of klik niet op onbekende links, vooral als de afzender je onbekend is.
- **Vermijd illegale software:** Gebruik legale software en download software alleen van betrouwbare platforms, bijvoorbeeld SURFspot.

Tekst intranet EN

Introduction

Cybercriminals are constantly devising new ways to get hold of our data. For example, via email, chat, and telephone. But also via your laptop or computer, for example when downloading software or an application. Attackers can send malicious software, ask you to fill in or copy something via an intermediate step, or send you to a 'fake' environment. So... as soon as you see or have to do something that 'is different from usual' or 'doesn't feel right', contact [contactpunt instelling]

What are infostealers?

Infostealers are a type of malicious software that cybercriminals use to steal personal information from your computer or device. Once installed on your device, the malware collects sensitive information without your knowledge and sends it to the criminals. They can cause enormous damage if they are not detected in time.

What kind of information do infostealers collect?

Infostealers target various types of sensitive information:

- **Login details**: Usernames and passwords for email accounts or social media.
- **Financial details**: Credit card numbers, bank details, and information about cryptocurrency wallets.
- **Personal details**: Information such as your name, address, phone number, or social security number.
- **System information**: Data about your device's hardware, installed software, and security programs.

All of this data is valuable to criminals and can be misused for identity theft, financial fraud, or further cyberattacks.

How do infostealers get in?

Infostealers can find their way onto your device in various ways, often without you even noticing:

- **Phishing emails**: Emails that look like they come from a trusted source but contain a malicious link or attachment. If you click on it, the malware is installed.
- **Malicious websites**: By clicking on a link to an infected website or through malvertising (malicious advertisements), you can download malware without noticing. Even a trusted website can be hacked to spread malware.

- Illegal software: Downloading illegal software carries significant risks. These packages are often infected with malware.
- Vulnerabilities in software: Some infostealers exploit security flaws in outdated software or browsers to infect your device.

How can you recognize infostealers?

Are you being asked to do something on a website because you cannot access the website otherwise, or do you not trust a website or email? Report this as soon as possible to [contactpunt instelling]

Infostealers are designed to work unnoticed when they are active. These are signs to look out for:

- If you receive a message saying that you need to log in urgently and are asked to do so via the link in the email/text message.
- Unexpected emails, social media messages, or transactions on your bank account. Messages from “acquaintances” that are strange/different than usual or that you do not expect.
- If you receive a message to use your second factor (MFA) again without you being logged in.

If you recognize these signs, take immediate action and scan your device for malware and/or disconnect your device from the internet. If this happens on a device belonging to your institution, report it as soon as possible.

What can you do against infostealers?

- **Use multiple factors to log in (Multi-factor authentication (MFA)**: This adds an extra layer of security, requiring you to enter an SMS code in addition to your password, for example. Sometimes you have to enable this yourself in your social media accounts.
- **Update your software regularly**: Make sure your computer and antivirus software are up to date.
- **Log in by searching for the website yourself**: If you are asked to log in, do not do so via the link in the email, but go to the official page.
- **Be careful with emails**: Do not open suspicious attachments or click on unknown links, especially if the sender is unknown to you.
- **Avoid illegal software:** Use legal software and only download software from reliable platforms, such as SURFspot.

Tekst mail NL

Je krijgt deze mail omdat cybercriminelen steeds vaker infostealers gebruiken.

Infostealers zijn een vorm van schadelijke software die cybercriminelen gebruiken om persoonlijke informatie van jouw computer of apparaat te stelen. Eenmaal geïnstalleerd op je apparaat, verzamelt de malware onopgemerkt gevoelige informatie en stuurt deze naar de criminelen. Ze kunnen enorme schade veroorzaken als ze niet op tijd ontdekt worden.

Wordt je op een website gevraagd om iets uit te te voeren omdat je anders niet op de website kan, of vertrouw je een website of email niet? Meld dit zo snel mogelijk bij [contactpunt instelling]

Cybercriminelen wekken de indruk dat iets heel erg belangrijk is en je nu meteen moet reageren. Dat kan via e-mail, sms, telefoon of bij bezoek aan een website. Zodra je iets ziet of moet doen dat anders is dan anders of niet goed voelt, meld dit ook bij [contactpunt instelling].

Infostealers zijn ontworpen om ongemerkt te werken wanneer ze actief zijn. Dit zijn signalen waar je op kunt letten:

- Als je bericht krijgt dat je dringend moet inloggen, en het verzoek om dat via de link in de mail/sms te doen.
- Onverwachte e-mails, sociale media berichten of transacties op je bankrekening. Ook berichten van 'bekenden' die vreemd/'anders dan normaal' zijn of die je niet verwacht.
- Als je bericht krijgt om (nogmaals) je 2e factor (MFA) te gebruiken, zonder dat je zelf aan het inloggen bent.

Herken je deze signalen, onderneem dan direct actie en scan je apparaat op malware en/of koppel je apparaat los van internet. Gebeurt dit op een apparaat van je instelling, meld dit dan zo snel mogelijk.

Kijk voor meer informatie op [intranet instelling]

Tekst mail EN

You are receiving this email because cybercriminals are increasingly using infostealers.

Infostealers are a type of malicious software that cybercriminals use to steal personal information from your computer or device. Once installed on your device, the malware collects sensitive information without your knowledge and sends it to the criminals. They can cause enormous damage if they are not detected in time.

If you are asked to do something on a website because you cannot access the website otherwise, or if you do not trust a website or email, report this as soon as possible to [contactpunt instelling].

Cybercriminals give the impression that something is very important and that you must respond immediately. They may do this via email, text message, phone, or when you visit a website. As soon as you see or have to do something that is different from usual or does not feel right, report this to [contactpunt instelling]..

Infostealers are designed to work unnoticed when they are active. These are signs to look out for:

- If you receive a message saying that you need to log in urgently and are asked to do so via the link in the email/text message.
- Unexpected emails, social media messages, or transactions on your bank account. Messages from “acquaintances” that are strange/different than usual or that you do not expect.
- If you receive a message to use your second factor (MFA) again without you being logged in.

If you recognize these signs, take immediate action and scan your device for malware and/or disconnect your device from the internet. If this happens on a device belonging to your institution, report it as soon as possible.

For more information, visit [intranet instelling].

Afbeeldingen

CSY afbeelding

Deze afbeelding in de CSY toolkit is eerder ontwikkeld om het onderwerp ‘nep websites’ onder de aandacht te brengen. Deze afbeelding kan rechtenvrij gebruikt worden intern, en met naamsvermelding op een externe website.

De hoge resolutie versie en de photoshop bestanden zijn te vinden in de CSY toolkit. Log in met instellingsaccount vis SURFconext om in de toolkit te komen.
https://wiki.surfnet.nl/x/1YGACg

Stockafbeeldingen

Maakt je instelling gebruik van Stockphoto’s en afbeeldingen, dan vind je hier wat voorbeelden voor afbeeldingen bij dit onderwerp:

- https://www.istockphoto.com/en/vector/cartoon-thief-car-burglary-and-house-robbery-flat-scenes-criminal-person-wearing-gm1174348916-326567650
- https://www.istockphoto.com/en/vector/vector-graphic-of-cartoon-computer-hacker-gm165807414-19633148
- https://pixabay.com/illustrations/scam-phishing-fraud-email-attack-3933004/
- https://pixabay.com/illustrations/hack-fraud-card-code-computer-3671982/
- https://pixabay.com/illustrations/scam-hacker-phishing-cybersecurity-7070718/
- https://pixabay.com/vectors/phishing-credentials-data-login-6573326/

Kant en klare CSY posters en schermafbeeldingen

In de CSY toolkit vind je materialen opgemaakt in de CSY huisstijl. Dezekun je direct inzetten bij je instelling.Van alle materialen staan de Photoshop en Indesign bestanden in de toolkit. De communicatieafdeling kan de materialen daarmee ook aanpassen.

- Afbeelding voor TV-scherm (Narrowcasting(NL en EN)
- Poster A2 NL/EN

Colofon

Heb je opmerkingen of aanvullingen, laat het weten via info@cybersaveyourself.nl

Communities
Dit product komt voort uit de samenwerking communities SCIRT en SCIPR. SURF kent twee beveiligingscommunity's: SCIPR en SCIRT. Informatiebeveiligers en privacyofficers werken samen in SCIPR (SURF Community voor Informatiebeveiliging en PRivacy). Technisch, operationele securityspecialisten kunnen terecht bij SCIRT, de SURF Community van Incident Response Teams. Beide community's werken nauw met elkaar samen.
https://www.surf.nl/themas/cybersecurity/beveiligingscommunitys-samen-werken-aan-beveiliging-en-privacy

SURFcert
SURFcert biedt 24 uur per dag, 7 dagen per week ondersteuning bij beveiligingsincidenten. Ook biedt SURFcert je diverse security-oplossingen om zelf de beveiliging bij je instelling te optimaliseren.
https://www.surf.nl/diensten/beveiliging/surfcert

Cybersave Yourself
Cybersave Yourself (CSY) is een campagne en een toolkit waarmee je het bewustzijn van je medewerkers en studenten vergroot op het gebied van security en privacy.
https://www.surf.nl/diensten/beveiliging/cybersave-yourself