Cybersecurity fundamenten

Cyberboswachters

Tim Dams

Wat is cybersecurity?

> *“Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks.”* — Cisco

Alles draait rond het beschermen van **informatie** — op een server, in een document, of in iemands hoofd.

> **Opmerking**
>
> Er zijn nu meer **verbonden apparaten** dan mensen, en aanvallers worden steeds innovatiever.

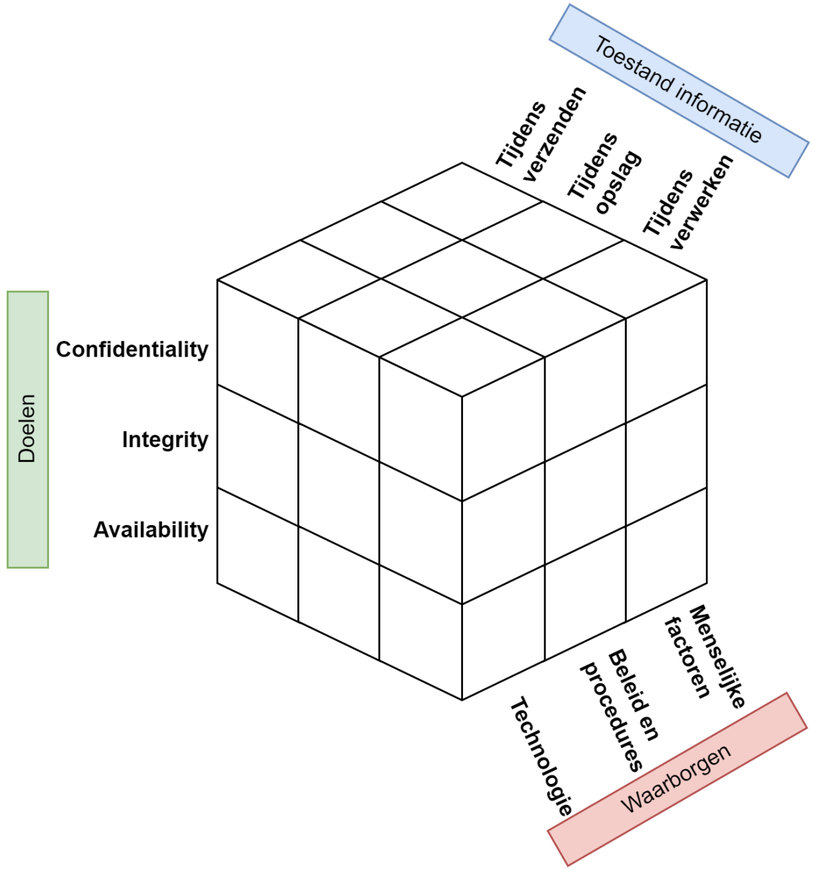
CIA-model

Pijler	Betekenis	Oplossingen
Confidentiality	Enkel bevoegde partijen kunnen data lezen	Encryptie, wachtwoorden
Integrity	Data is ongewijzigd en betrouwbaar	Hashing, digitale handtekeningen
Availability	Data is bereikbaar wanneer nodig	Back-ups, firewalls, redundantie

> **Tip**
>
> **DoS-aanvallen** richten zich specifiek op de *Availability*-pijler.

McCumber kubus

- Ontwikkeld door **John McCumber** (1991)
- Framework om niets over het hoofd te zien:
  - → **Informatiestatus**: opslag, verzenden, verwerken
  - → **Beveiligingsmaatregel**: technologie, beleid, mensen
  - → **Doel**: C.I.A.



De McCumber kubus.

Belangrijk

Technologie alleen is niet genoeg. Een werknemer die z'n wachtwoord op een post-it plakt, vernietigt de beste firewall.

ISO 27001

> ⚠ **Waarschuwing**
>
> De **ISO 27001** norm is dé internationale standaard voor informatiebeveiliging.
>
> - Bedrijven tonen hiermee aan dat ze serieus omgaan met security
> - Een **externe auditor** controleert of aan alle eisen voldaan is
> - Certificaat moet **elke 3 jaar** hernieuwd worden
> - Dekt alle dimensies van de McCumber kubus

Een ongelijke strijd

De cyberboswachter van de 21e eeuw heeft het moeilijker dan ooit:

- **Snelheid**: aanvallers kunnen miljoenen systemen tegelijk aanvallen
- **Attack surface**: netwerken zijn veel groter en complexer dan 20 jaar geleden
- **Lage drempel**: een krachtige aanval = IP invullen + één klik
- **Zero-day snelheid**: nieuwe kwetsbaarheden worden sneller gevonden dan gepatcht
- **Botnets**: gigantische legers aan gecompromitteerde machines
- **Gebruikers**: klikken sneller dan ooit op phishing-links

Zero days en patching

- **Zero day** = kwetsbaarheid die nog onbekend is bij de softwarefabrikant
  - → Gegarandeerd werkzaam — er bestaat nog geen patch

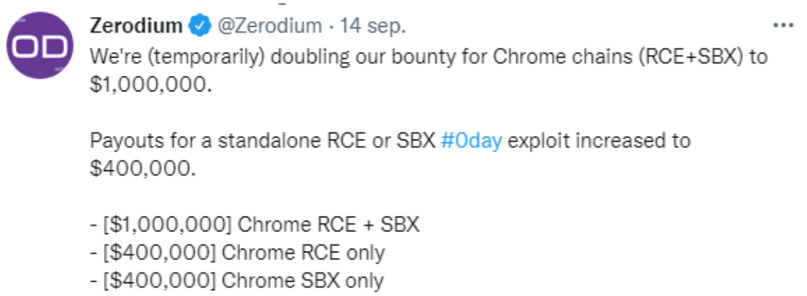
> ⚠ **Waarschuwing**
>
> **Window of vulnerability**: de periode tussen het ontdekken van een zero day en de release van een patch.
>
> In dit *window* heeft de aanvaller vrij spel.

Zelfs **ná de patch**: niet elk systeem wordt meteen bijgewerkt → één niet-gepatcht systeem = het gaatje in de linie.

Zero days: een markt

- Zero days worden verhandeld op een **schimmige markt**
- Prijzen kunnen oplopen tot **meer dan 1 miljoen dollar**
- Fabrikanten zoals Apple en Microsoft brengen patches uit op **vaste dagen**

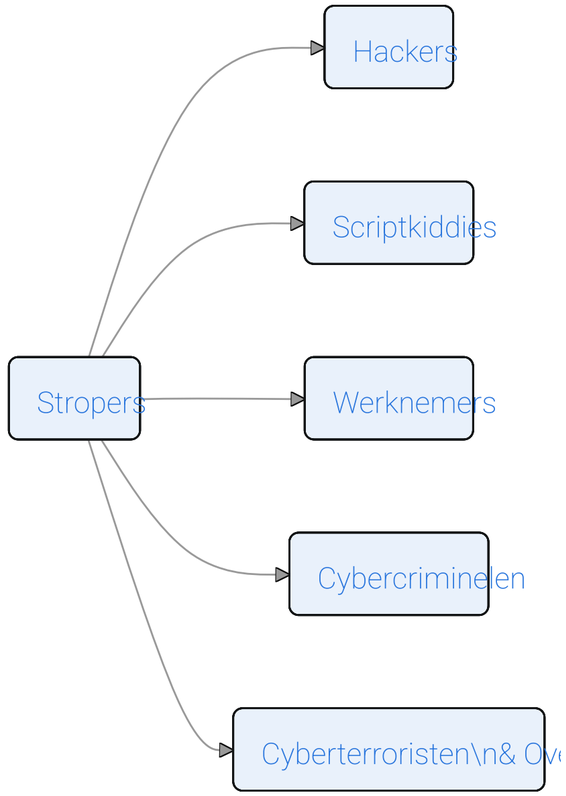
  → Voordelig voor aanvallers: ze kunnen de *windows* voorspellen



Zerodium: een zero-day broker.

> **Tip**
>
> *"How They Tell Me the World Ends"* van Nicole Perlroth (NYT, 2021) geeft een griezelig inzicht in de zero-day markt.

Wie zijn de stropers?



Elke groep heeft **eigen motivaties, middelen en methodes**.

Hackers: de kleurcode

Kleur	Type	Beschrijving
⬜ **Whitehat**	Ethisch hacker	Legaal pentesten, bug bounty
🩶 **Greyhat**	Grijs gebied	Goede intenties, niet altijd legaal
⬛ **Blackhat**	Crimineel (*cracker*)	Illegale toegang, eigenbelang
🟥 **Redhat**	Vigilante	Vecht terug tegen blackhats — middelen niet altijd legaal
🟦 **Bluehat**	Wraaklustig	Eén doel: wraak nemen
🟩 **Greenhat**	Beginner	Scriptkiddie in opleiding

Scriptkiddies

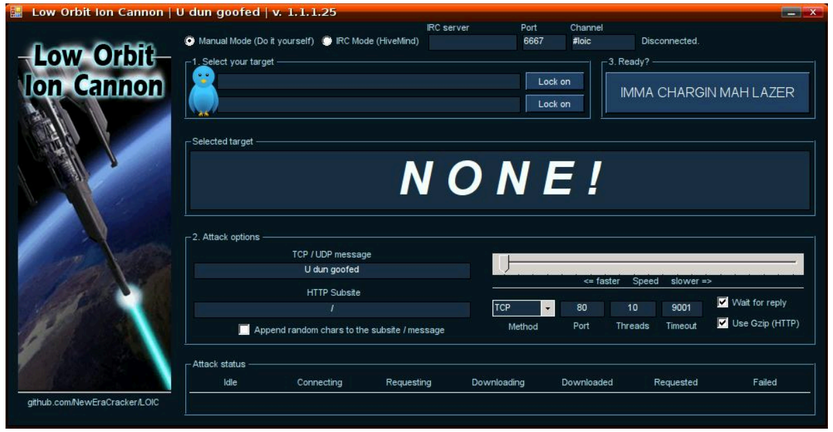
- Weinig tot geen kennis — maar gebruiken **krachtige, gebruiksvriendelijke tools**
- Beseffen vaak **niet** dat hun acties strafbaar zijn
- Gevolgen kunnen even ernstig zijn als bij doorgewinterde aanvallers

> ⚠ **Waarschuwing**
>
> Veiligheidsdiensten kunnen niet zien wie er achter een aanval zit — ze reageren altijd op dezelfde manier.
>
> Een politie-inval + zware boetes als gevolg van “gewoon een knopje indrukken”.

Scriptkiddies: Low Orbit Ion Cannon

- Gratis DDOS-tool, eenvoudig in gebruik
- In **2010** gebruikt om Visa, MasterCard en PayPal urenlang lam te leggen

  → Reden: protest tegen blokkering WikiLeaks-betalingen
- Wanneer voldoende gebruikers tegelijk aanvallen → massale impact



Low Orbit Ion Cannon UI (Bron: Wikipedia).

Werknemers: de vergeten bedreiging

Bewust (insider threats):

- Ontevreden of ontslagen werknemers
- Sabotage, datadiefstal, losgeld eisen
- Zitten *aan de binnenkant* van je beveiliging

Onbewust (menselijke fouten):

- Wachtwoord op post-it
- Onbekenden binnenlaten (*piggybacking*)
- Eigen access point installeren voor betere wifi

BYOD-risico:

Eigen apparaten = potentieel geïnfecteerde apparaten die het bedrijfsnetwerk binnenkomen.

De “veilige burcht” werkt niet meer als je iedereen met hun eigen sleutel naar binnen laat.

Cybercriminelen

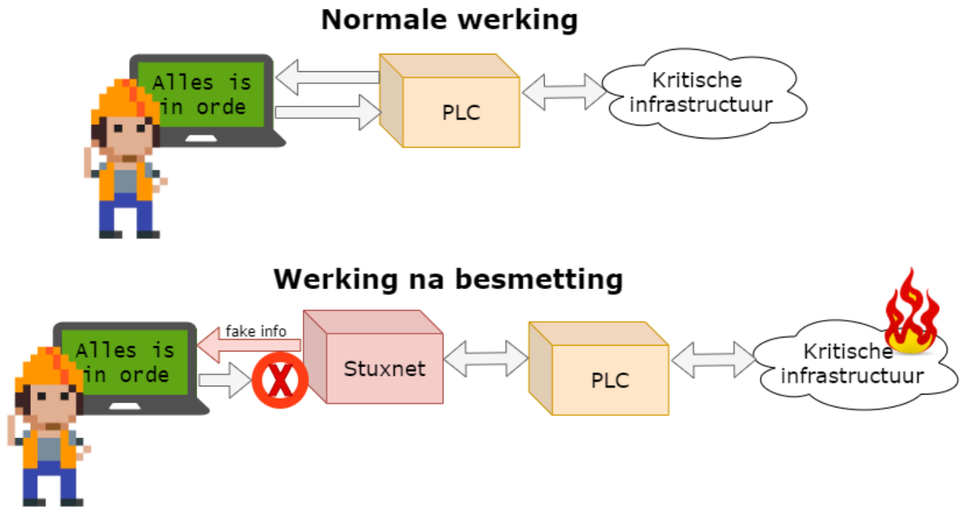
- **Geld** is de enige motivatie
- Meer dan **$700 miljard schade** in 2021 (schatting)
- Werken als moderne bedrijven:
  - → Helpdesks voor ransomware-betalingen
  - → **RaaS**: Ransomware-as-a-Service
  - → Botnets verhuren op het darkweb

> ⚠ **Waarschuwing**
>
> Het “bedrijfsmodel” van cybercriminelen zorgt ervoor dat aanvallers zelf geen technische kennis meer nodig hebben.

Cyberterroristen, spionnen & overheden

- De scheidslijn tussen **terrorist**, **spion** en **staatshacker** is vaag en politiek
- Financiële en technische middelen zijn **immens** groter dan andere groepen

> **Opmerking**
>
> Het **Mossad/Non-Mossad principe**:
>
> Maak een realistische inschatting van je tegenstander. Een staatsactor *zal* binnenkomen ongeacht je budget. Focus op de dreigingen die relevant zijn voor jou.



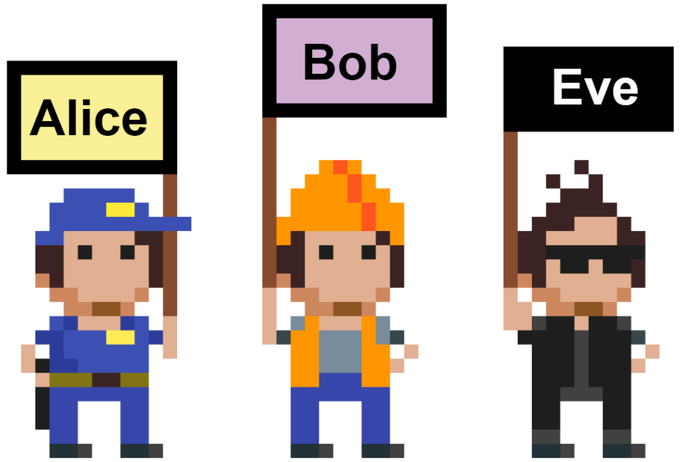
De 5 fasen van een aanval

De 5 fasen: detail

Fase	Activiteit
1. Verkennen	Google, sociale media, dumpster diving — *onzichtbaar voor het slachtoffer*
2. Scannen	Port scanners, vulnerability scanners — *detecteerbaar*
3. Toegang	Kwetsbaarheid uitbuiten, phishing, privilege escalation
4. Bestendigen	Backdoor installeren, laterale beweging in netwerk
5. Sporen wissen	Logs aanpassen of verwijderen, backdoors opruimen

> **Tip**
>
> **Red team / Blue team**: bij legale pentests speelt het *red team* de aanvallers, het *blue team* de verdedigers.

Alice, Bob en Eve

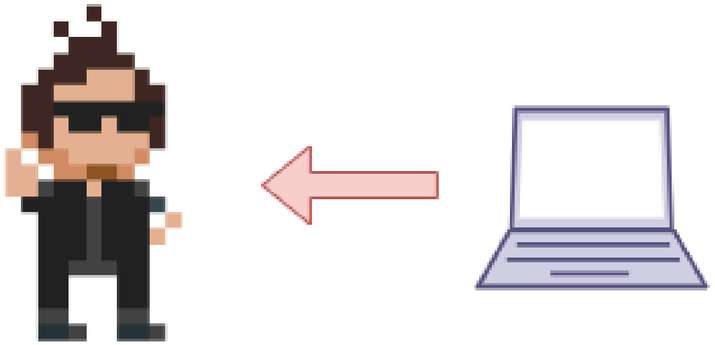


Meet the crew.

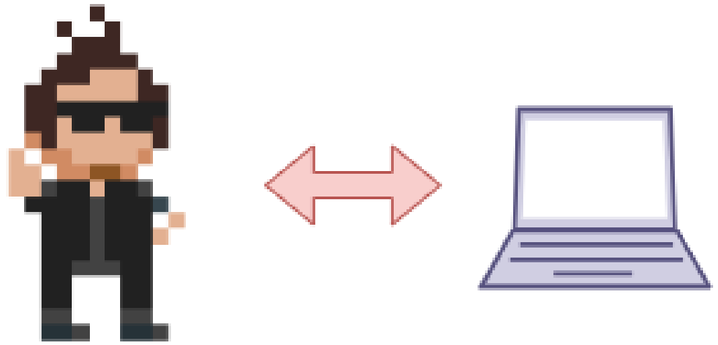
- **Alice en Bob**: willen veilig communiceren
- **Eve**: wil hun communicatie onderscheppen, aanpassen of blokkeren

> ⚠ **Waarschuwing**
>
> Alice en Bob zijn eender welk start- en eindpunt van informatie: ook CPU → RAM, database → schijf, server → gebruiker.

Actieve vs. passieve aanvallen



Passief

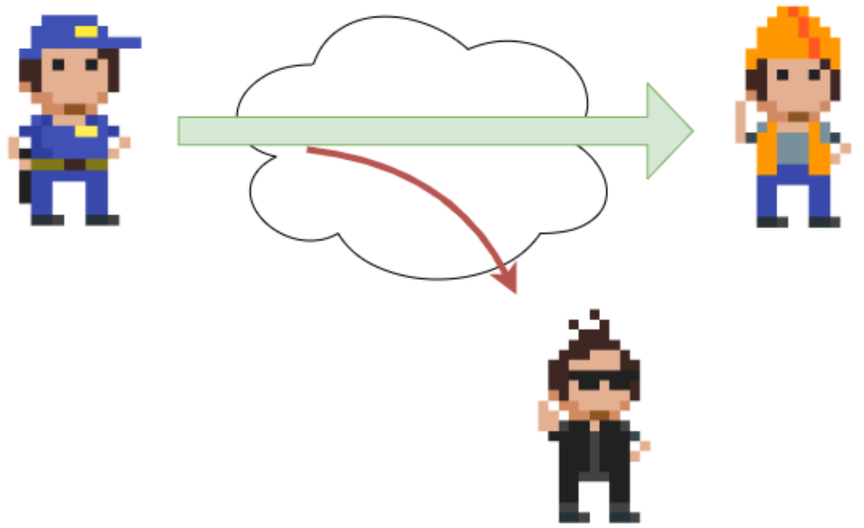


Actief

Passieve vs actieve aanvallen.

	Passief	Actief
Eve's rol	Luisteren en wachten	Ingrijpen in communicatie
Detecteerbaarheid	Zeer moeilijk	Groter risico op detectie
Controle	Afhankelijk van slachtoffer	Meer controle voor Eve

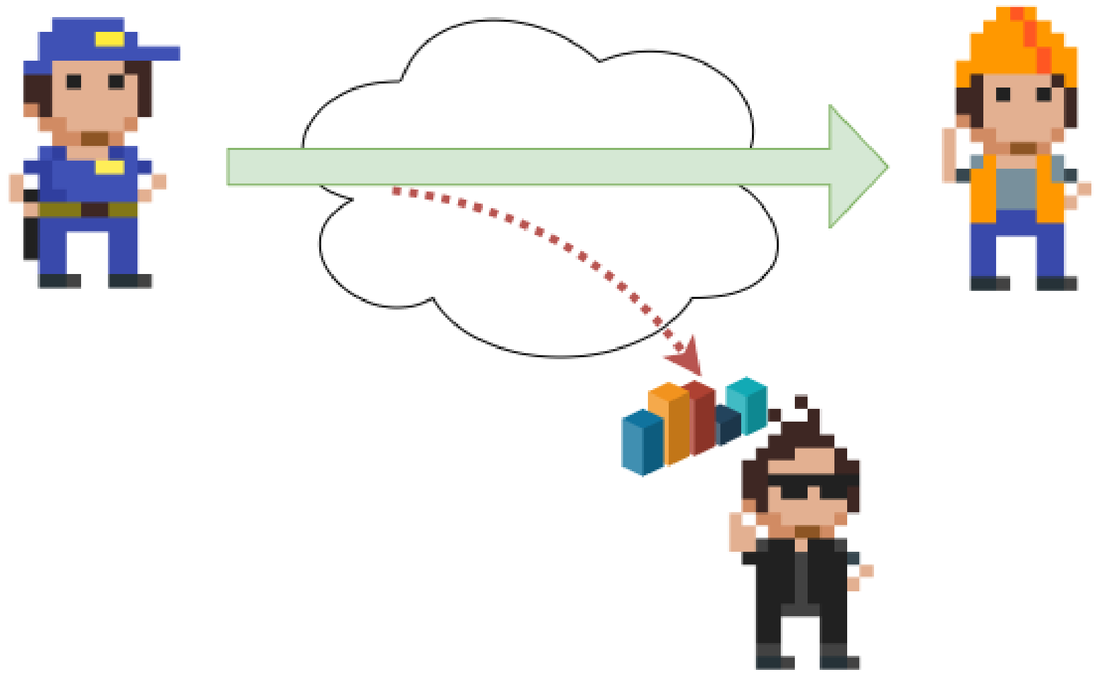
Passieve aanval 1: Sniffing



Passieve aanval, type 1: Sniffing.

- Eve gebruikt een **sniffer** (bv. Wireshark) om netwerktrafiek af te luisteren
- Zelfs geëncrypteerde trafiek lekt **metadata**: MAC-adressen, timing, gebruikersinfo
- Slecht beveiligde third-party apps sturen soms credentials **onversleuteld** → goudmijn voor Eve

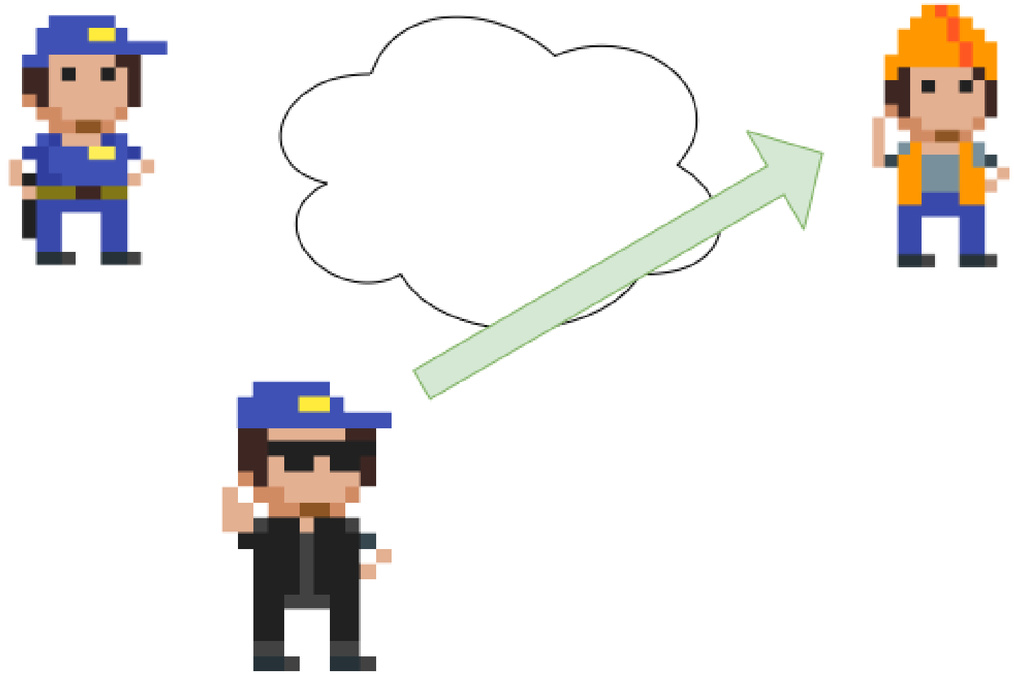
Passieve aanval 2: Trafiekanalyse



Passieve aanval, type 2: Trafiek analyse.

- Eve registreert **wanneer en hoe** het slachtoffer communiceert
- Laat toe actieve periodes te kennen → aanvallen beter plannen
- Onthult type activiteit: e-mail, VoIP, bestandsoverdracht, …

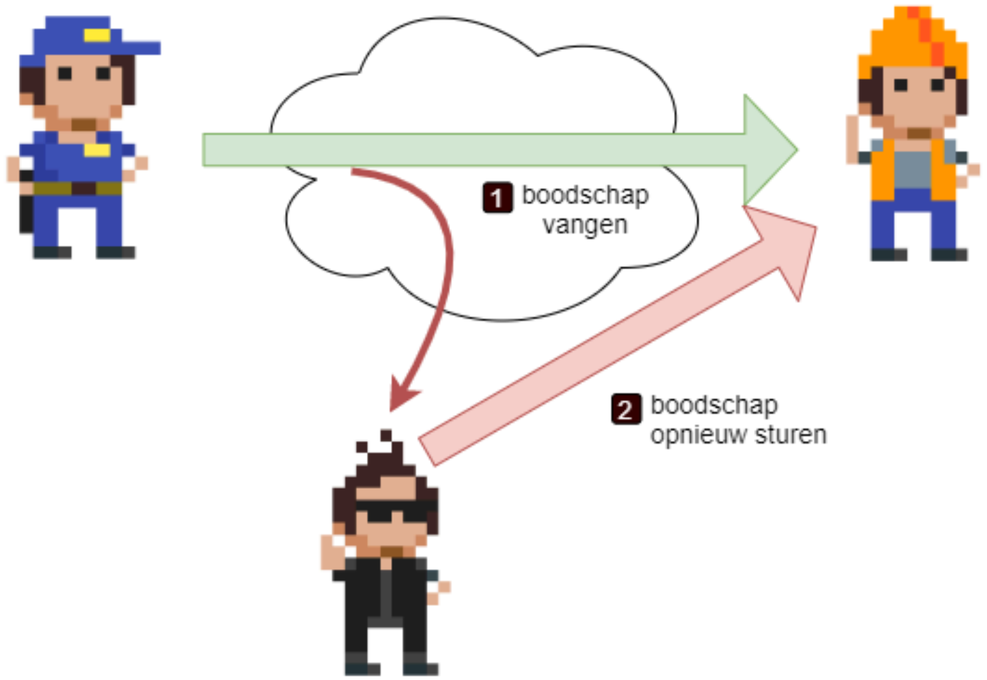
Actieve aanval 1: Masquerading & Spoofing



Actieve aanval, type 1: Masquerading.

- Eve neemt de **digitale identiteit** van een legitieme gebruiker over
- Bv. **MAC-spoofing**: hardware-adres van een netwerkkaart overnemen
- Doel: anonimiteit én toegang tot afgeschermde bronnen

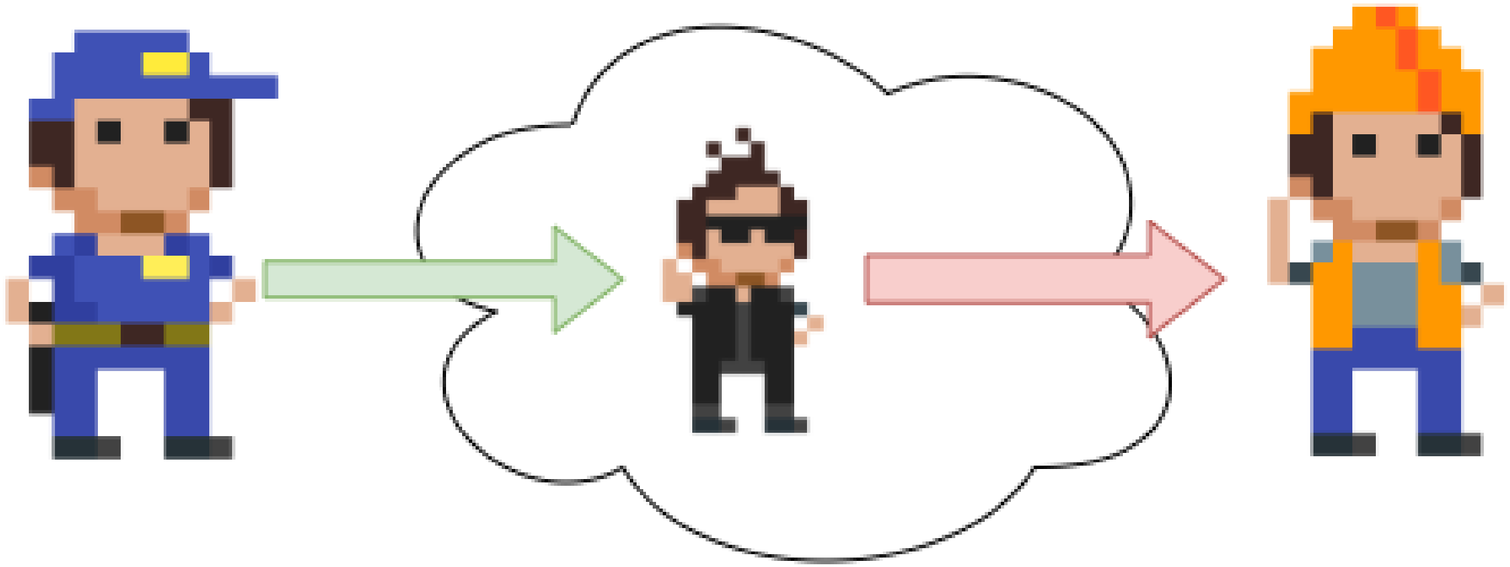
Actieve aanval 2: Replay attack



Actieve aanval, type 2: Replay attack.

- Eve bewaart een legitiem communicatiepakket (bv. een login)
- Later verstuurt ze dit opnieuw → systeem denkt dat het Alice is
- Gevaarlijk bij systemen zonder **session tokens** of **tijdstempels**

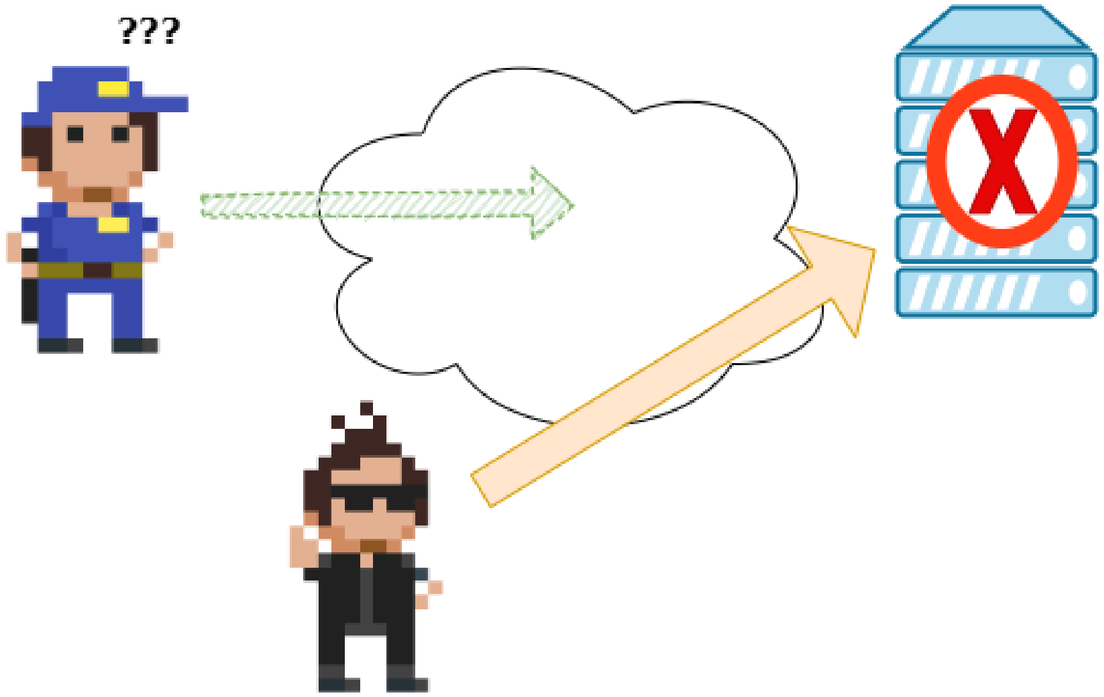
Actieve aanval 3: Man-in-the-Middle (MitM)



Actieve aanval, type 3: Man-in-the-middle aanval.

- Eve nestelt zich **tussen** Alice en Bob
- Kan communicatie **lezen, aanpassen of blokkeren** — volledig onzichtbaar
- Vereist vaak ook masquerading naar beide kanten tegelijk

Actieve aanval 4: Denial-of-Service (DoS)



Actieve aanval, type 4: Denial-of-Service aanval.

- Doel: systeem of gebruiker **onbereikbaar maken**
- Vormen: trafiek overstromen, signaalstoring, fysiek de stekker uittrekken
- **DDOS** = *Distributed* DoS via botnet van duizenden zombies tegelijk

Hoe verdedigen? De 4+1 principes

Principe	Beschrijving
Layering	Meerdere beveiligingslagen rondom je data (als een ui)
Limiting	Enkel de rechten die iemand echt nodig heeft
Diversity	Verscheidenheid aan beveiligingen → één faling ≠ totale neergang
Simplicity	KISS: *Keep It Simple, Stupid* — complexiteit introduceert fouten

> ⚠ **Waarschuwing**
>
> **+1 — Obscurity**: verberg hoe je verdediging is opgebouwd. Maar gebruik dit **nooit** als vervanging voor echte beveiliging. Gebruik standaarden en vertrouwde producten — heruitvind het wiel niet!

Social Engineering: het hacken van mensen

- Mensen zijn de **zwakste schakel** in elk securitymodel
- Social engineering misbruikt menselijke eigenschappen: **vertrouwen, nieuwsgierigheid, angst, hebzucht**

Voorbeelden van fysieke social engineering:

- Verkleden als pizzakoerier → werknemers houden deur open
- Bij rokers naar binnen meelopen (*piggybacking*)
- Bellen als “Telenet-technieker” en wachtwoord opvragen

> **Tip**
>
> Je hoeft niet eens aanwezig te zijn: **phishing via e-mail** is de meest gebruikte techniek.

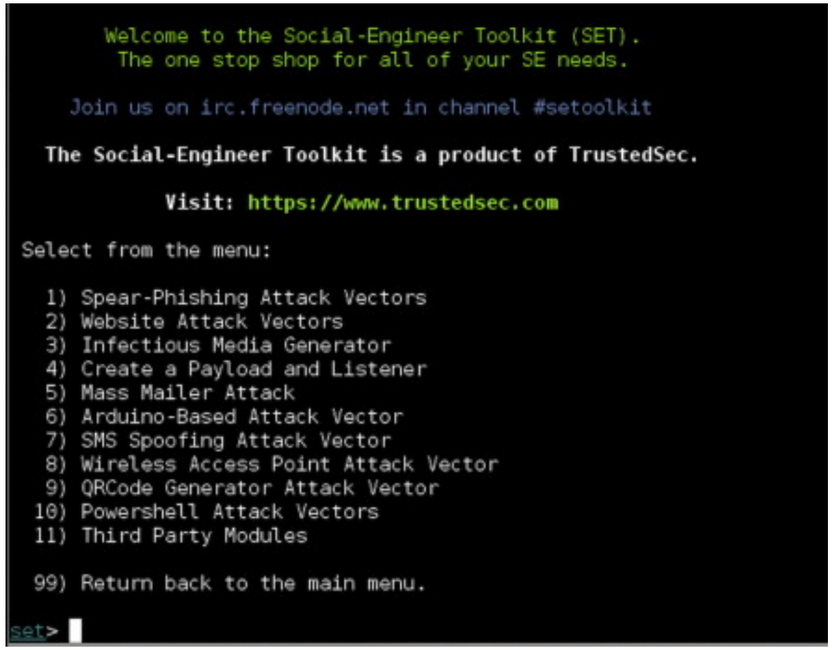
Phishing vs. Spear Phishing

	Phishing	Spear Phishing
Doelgroep	Zoveel mogelijk mensen	Één specifiek persoon of groep
Aanpak	Generieke e-mail	Op maat gemaakt bericht
Slaagkans	Laag per persoon	Veel hoger
Voorbeeld	Nep-ING mail naar iedereen	Gerichte mail naar de CEO van bedrijf X

> **Opmerking**
>
> De naam *phishing* is afgeleid van *fishing* — hengelen naar slachtoffers.

Social Engineering Toolkit (SET)

- Open source toolkit in **Kali Linux**
- Mogelijkheden:
  - → (Spear) phishing campagnes opzetten
  - → Bestaande websites klonen
  - → Malware injecteren in afbeeldingen
- Integreert met **Metasploit** voor complexe aanvallen

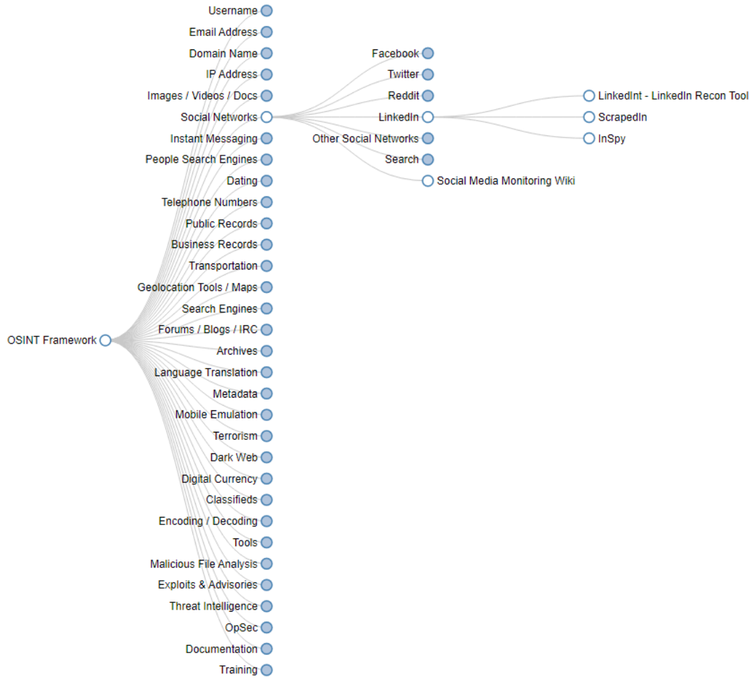


Social Engineering Toolkit.

OSINT: Open Source Intelligence

- Informatie verzamelen via **publiek beschikbare bronnen**
- Cruciale stap bij spear phishing (reconnaissance-fase)

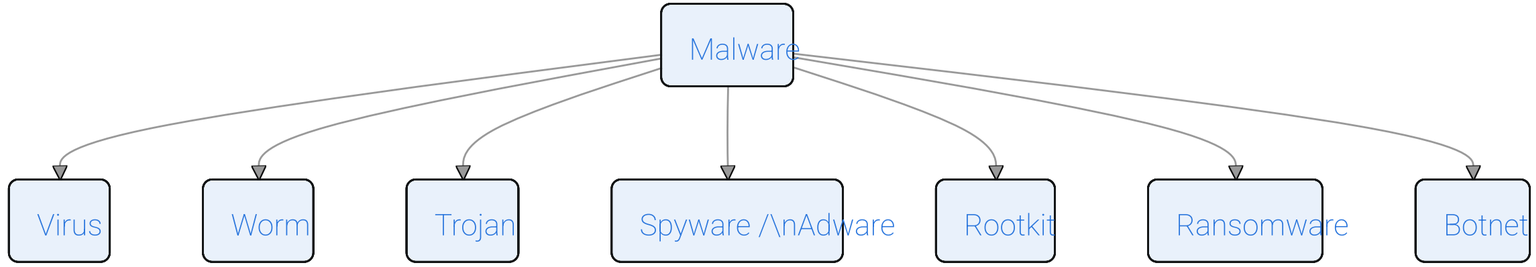
Technieken: * Geavanceerde zoekopdrachten (`site:`, `filetype:`, `+`) * **Reverse image search** (Google Lens) * **EXIF-data** uit foto's (locatie, toestelinfo, tijdstip)



OSINT Framework overzicht.

> **Tip**
>
> osintframework.com toont hoe véél publieke informatie er over iemand beschikbaar is — zonder één illegale stap te zetten.

Malware: overzicht



Opmerking

CVE (*Common Vulnerabilities and Exposures*): publieke database van alle gekende kwetsbaarheden — essentieel hulpmiddel voor elke cyberboswachter.

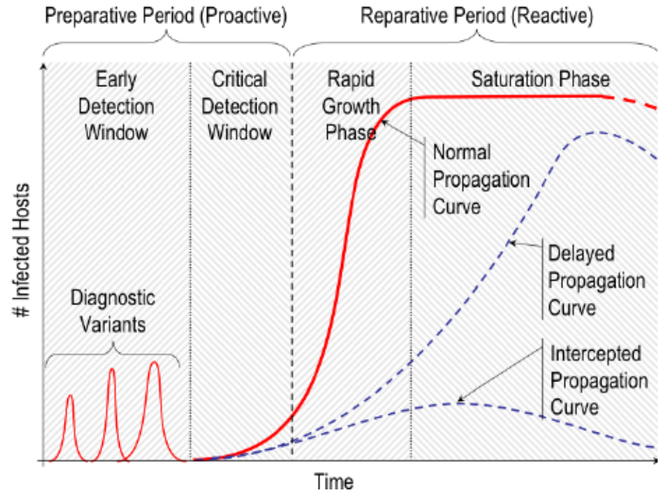
Virus

- Nestelt zich in een **uitvoerbaar bestand** (.exe, .bat, .com) — heeft een hostfile nodig
- Verspreidt zich via gebruikershandeling: bestand openen, download, diskette
- Vroeger: bootsector infecteren, bestanden verwijderen
- Nu: geëvolueerd naar gevaarlijkere varianten (wormen, ransomware)

> **Tip**
>
> *Don't pirate, kids* — gepirateerde software was (en is) een klassieke virusdrager.

Worm

- Zoals een virus, maar **verspreidt zichzelf** via netwerken, e-mail, Bluetooth, …
- **Geen hostfile** nodig — actiever en gevaarlijker dan een virus
- Kan zichzelf **vervormen** (*polymorfisme*) om virusscanners te misleiden
- Groei is **exponentieel** tot quasi alle kwetsbare systemen besmet zijn



Worm propagation model (Bron: ResearchGate).

Trojan

- Verbergt zich binnenin een **legitieme applicatie**
- Gebruiker installeert bewust → trojan wordt mee geactiveerd

Trojan.

Mogelijke payloads:

- Backdoor installeren
- Computer zombie maken (botnet)
- Keylogger activeren
- Spyware droppen

> **Opmerking**
>
> De naam is gebaseerd op de legende van *Het Paard van Troje* uit de Aeneid van Vergilius.

Spyware & Adware

	Spyware	Adware
Doel	Informatie stelen (logins, bankgegevens)	Reclame tonen
Zichtbaarheid	Verborgen	Soms zichtbaar
Installatie	Via trojan	Via gratis software of browser-extensies

> ⚠ **Waarschuwing**
>
> Sommige adware gebruikt **rootkit-technieken** en is bijzonder moeilijk te verwijderen.

Rootkit

- Nestelt zich op **kernel-niveau** — dieper dan een gewoon virus
- Kan bepalen **wat het besturingssysteem aan de gebruiker toont** → volledig onzichtbaar
- Systeembestanden worden aangepast → verwijderen veroorzaakt systeemschade
- Enige zekere oplossing: **harde schijf formatteren**

> **Belangrijk**
>
> Zelfs een OS herinstallatie via aanwezige installatiebestanden biedt geen garantie — de rootkit kan al in die bestanden zitten!

Ransomware

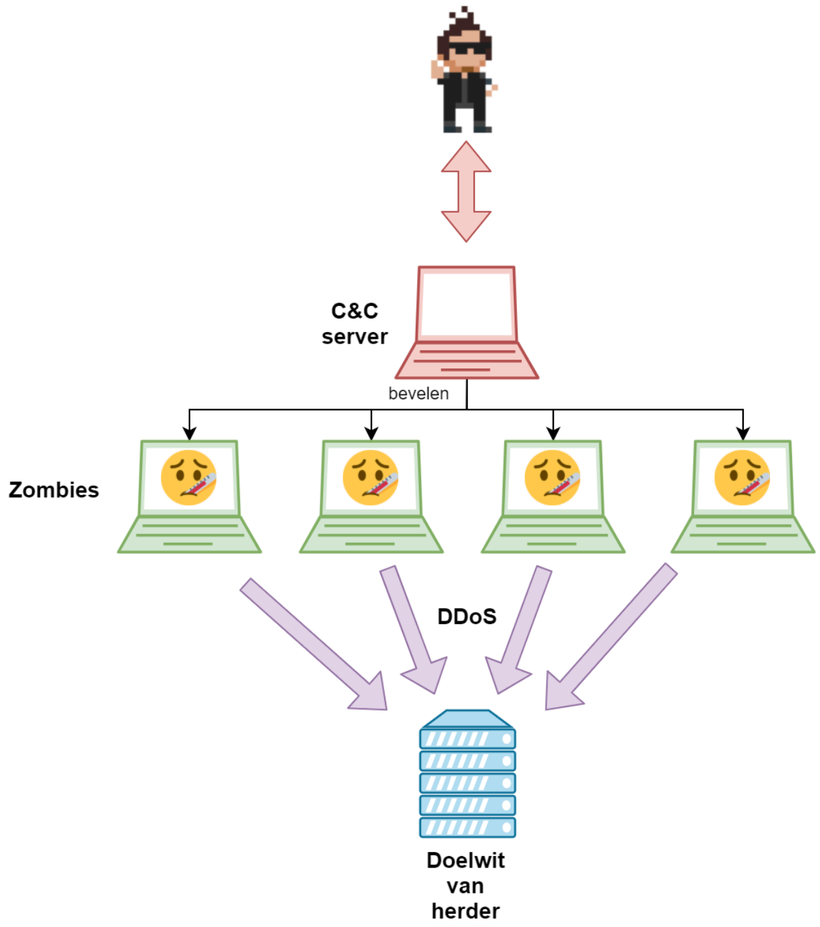
- **Gijzelt data** door ze te versleutelen met een sleutel die enkel de crimineel kent
- Slachtoffer krijgt betaalinstructies (crypto)
- Zelfs ziekenhuizen en havens werden getroffen (WannaCry, Petya — 2017)

Typisch ransomware scherm (Bron: Wikipedia).

> **Tip**
>
> Back-ups helpen — maar enkel als ze **buiten het bereik van de ransomware** staan!

Botnet: zombie-legers

- Aanvaller besmet computers met **zombie-malware**
- Zombies verbinden met de **C&C-server** van de *herder*
- Herder stuurt bevelen: DDOS, cryptomining, spam, app store-ratings, …
- Botnets worden **verhuurd of verkocht** op het darkweb



Een botnet met C&C-server.

Belangrijk

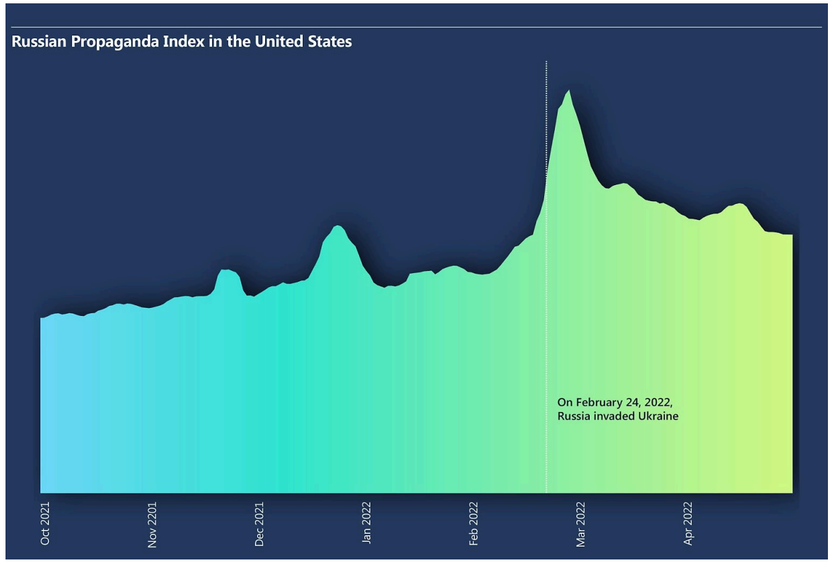
Oplossing: **C&C-server uit de lucht halen** → de zombies worden nutteloos.

Hardware-based aanvallen

Aanval	Beschrijving
USB stick	Gevuld met malware → autorun bij aansluiten
USB of death	Stuurt 220V door computer → directe hardwareschade
BIOS rootkit	Nestelt zich in UEFI-chip (bv. Moonbounce) — overleeft formattering
Warshipping	Raspberry Pi in postpakket → belt terug naar aanvaller
Keylogger	Registreert toetsaanslagen → wachtwoorden stelen
Juice hacking	Valse USB-oplaadpunt steelt data of installeert malware

Hacking hardware

- **USB Ninja**: gewone USB-kabel met ingebouwde RF-zender → stuurt data draadloos door
- **RFID cloners**: kopieer toegangsbadges voor een habbekrats
- **Warshipping**: Raspberry Pi verstopt in postpakket → belt terug naar de aanvaller



Raspberry Pi: groot genoeg om te verbergen, krachtig genoeg om aan te vallen.

Beschikbaar op lab401.com en hak5.org

> **Opmerking**
>
> In 2026 werd een Bluetooth-tracker van **€5** verstopt in een briefkaart en verstuurd naar een Nederlands marineschip van **€585 miljoen**. De tracker zond **24 uur lang** ongemerkt de locatie van het oorlogsschip uit. Bron: Tom's Hardware

Side-channel aanvallen

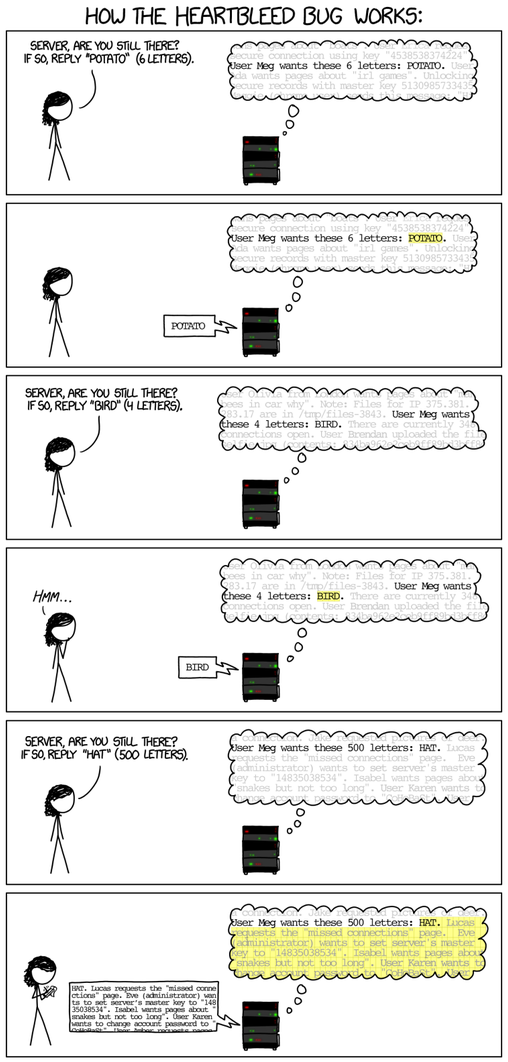
Informatie stelen via een **onverwachte weg** — niet via het protocol zelf.

> **Tip**
>
> Vergelijking: je wil inbreken in een bank, maar enkel als de bewaker slaapt. Je volgt hem op Goodreads. Zodra hij zijn leesvoortgang post → tijd om in te breken. Dat is een side-channel aanval.

Reële voorbeelden:

- **Strava + militairen**: workouts in de woestijn onthulden een geheime basis
- **Power consumption**: data uit een computer lezen via stroomverbruik
- **Rowhammer / Spectre**: geheugendata lezen zonder de juiste rechten
- **Heartbleed**: OpenSSL antwoordsnelheid onthulde geheugeninhoud

Heartbleed: uitgelegd



De briljante xkcd.com strip legt perfect uit hoe Heartbleed werkt.

Side-channel: bonus

Opmerking

Janet Jackson's "Rhythm Nation" heeft een officieel **CVE-nummer** gekregen.

Het liedje bevat frequenties die resoneren met de harde schijf van bepaalde oude laptops, waardoor ze crashen als het nummer wordt afgespeeld.

Dit is een echte, gedocumenteerde side-channel DoS-aanval!

Conclusie

- **CIA-model** is het fundament van alle cybersecurity
- De **McCumber kubus** helpt om niets over het hoofd te zien — inclusief mensen
- Aanvallers zijn divers: van scriptkiddies tot staatshackers
- Aanvallen volgen **5 fasen**: verkennen → scannen → toegang → bestendigen → wissen
- **Social engineering** is de meest effectieve aanvalsvector
- Malware heeft vele vormen: virus, worm, trojan, ransomware, botnet, …
- Hardware- en side-channel aanvallen zijn reëel en vaak onderschat

> **Belangrijk**
>
> De sterkste firewall ter wereld helpt niet als een werknemer z’n wachtwoord op een post-it plakt.