

**HO  
GENT**



# Cybersecurity

## 3. Bedreigingen, aanvallen en kwetsbaarheden



### **3. Bedreigingen, aanvallen en kwetsbaarheden**

- 3.1 Malware en kwaadaardige code
- 3.2 Misleiding en oplichting
- 3.3 Cyber aanvallen

**HO  
GENT**

## **3.1 Malware en kwaadaardige code**

**HO  
GENT**

## Verschillende soorten malware

- Cyber criminelen vallen de toestellen van de gebruikers aan door het installeren van kwaadaardige code
- **Virussen:** een computervirus is een kwaadaardig stukje code die vasthangt aan een uitvoerbaar bestand. De meeste virussen hebben een zekere vorm van actie van de eindgebruiker nodig. De virussen kunnen dan onmiddellijk of op een bepaald moment worden geactiveerd.

## Verschillende soorten malware

- **Worms:** is een stukje kwaadaardige code die zich kenmerkt doordat het **zichzelf reliceert** door gebruik te maken van een kwetsbaarheid in het netwerk. Worms zullen hierdoor ook vaak het **netwerk vertragen**. Een virus heeft een host programma nodig om te draaien, een worm kan **op zichzelf draaien**. Behalve de initiële infectie, heeft de worm geen interactie van de gebruiker meer nodig. De worm doet zelf al het werk.

**HO  
GENT**

## Worm



**HO  
GENT**

<https://www.youtube.com/watch?v=9BtxDdq5dwc>

## Verschillende soorten malware

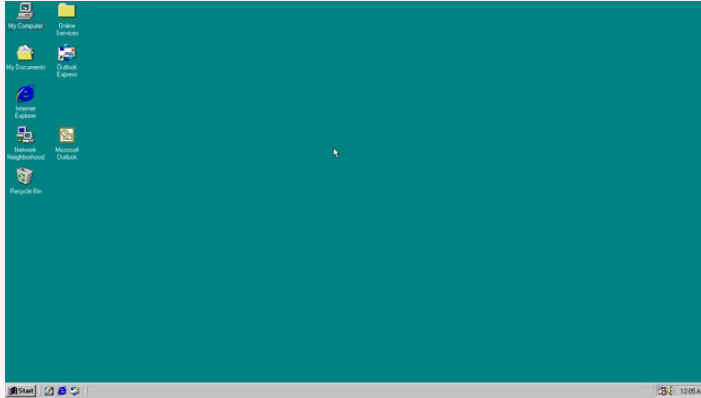
- **Trojaanse paarden:** Trojan horses zijn malware die **verborgen zit in gewenste bestanden** zoals foto's of een game. De gebruiker is hier uiteraard niet van bewust. Een Trojan horse verschilt van een virus omdat een Trojan horse **een niet-uitvoerbaar bestand** (zoals een afbeelding of een pdf) **infecteert**. Een virus heeft een executable bestand nodig. Een Trojaans paard is dus geen programma dat zelfstandig beschadigingen aan de geïnfecteerde computer veroorzaakt, zoals een computervirus. Een Trojaans paard moet bovendien door de gebruiker worden gekopieerd en **kopieert zichzelf niet** naar andere computers, zoals een worm wel doet.

**HO  
GENT**



### 3.1 Malware en kwaadaardige code

# Trojan Horse



**HO  
GENT**

<https://www.youtube.com/watch?v=LSgk7ctw1HY>

## Verschillende soorten malware (cont.)

- **Logic bomb:** een logische bom is een kwaadaardig programma die wordt **geactiveerd op bepaald moment (= trigger)**. Het wacht op de trigger om te activeren en schade toe te brengen. De trigger kan een bepaalde datum zijn, een ander programma dat wordt opgestart, een bepaalde actie die werd gedaan, etc.
- **Ransomware:** een computersysteem of data wordt **geblokkeerd of geëncrypteerd** tot het moment dat het slachtoffer een **geldsom** betaalt. De key om de data opnieuw te decrypteren blijft dan geheim tot er betaald wordt. Hopelijk, want er zijn natuurlijk geen garanties. Het blijven (cyber) criminelen.
- **Backdoors en Rootkits:** Een rootkit zal het **operating system aanpassen** en zo een backdoor creëren. Deze backdoor wordt dan gebruikt om het gecompromitteerde systeem binnen te dringen, zonder enige vorm van authenticatie.

**HO  
GENT**

## Logic Bomb

### Tikkende bom ontslagen collega

Rajendrasinh Makwana was Unix-beheerder bij de Amerikaanse hypotheekverstrekker Federal National Mortgage Association, ook wel Fannie Mae (FNMA). Tijdens zijn werkzaamheden schreef hij een programma die de instellingen van de servers wijzigde zonder fatsoenlijke autorisatie. De hypotheekverstrekker ontsloeg Makwana om die reden aan het eind van een vrijdagochtend in 2008. Zijn beveiligingspas werd ingenomen, maar hij werd wel teruggebracht naar zijn werkplek waar hij zijn werkzaamheden kon afronden.

's Middags liet hij een [afscheidscadeau achter in de vorm van een logic bomb](#) die financiële data van de Fannie Mae gewist zou hebben, midden in de crisis op de Amerikaanse huizenmarkt. Het programma stond op een timer voor eind januari 2009. Volgens de aanklagers zou de malware de hypotheken van miljoenen huiseigenaren hebben laten verdwijnen.

**HO  
GENT**

<https://webwereld.nl/nieuws/business/17-wraakzuchtige-iters-die-brokken-maakten-3772547/>

## Ransomware

**tweakers** Nieuws Reviews Pricewatch Vraag & Aanbod Forum Carrière Meer  

### 'Garmin heeft ransomware-losgeld betaald'

Garmin lijkt betaald te hebben voor de decryptor van de WastedLocker-ransomware waardoor het vorige maand getroffen werd. BleepingComputer heeft deze decryptor in handen weten te krijgen en aangezien er geen bekende kwetsbaarheid in het algoritme zit, is er waarschijnlijk betaald.

[BleepingComputer heeft](#) een softwarepakketje in handen gekregen dat afkomstig zou zijn van de it-afdeling van Garmin. Daarin zit de decryptor en een aantal security-toepassingen. In die eerste zitten verwijzingen naar de bedrijven Emsisoft en Coveware, respectievelijk een cybersecuritybedrijf dat decryptors maakt op basis van decryption-keys en een ransomware-onderhandelaar. Emsisoft zegt nooit betrokken te zijn bij onderhandelingen en Coveware weigert commentaar.

Hoeveel Garmin betaald heeft, weet BleepingComputer niet zeker. Wel heeft het van een werknemer vernomen dat de gijzelnemers tien miljoen dollar aan losgeld eisten.

Hoewel het betalen van losgeld op zich een vanzelfsprekende schaduwzijde heeft, komt er nog meer bij kijken dan dat. BleepingComputer schrijft dat de groep achter deze ransomware, Evil Corp, staat op de Amerikaanse *sanctions list*, waardoor het betalen van het losgeld kan betekenen dat Garmin boetes van de Amerikaanse overheid opgelegd kan krijgen.

Garmin, dat onder andere smartwatches en navigatiesystemen maakt, werd op 23 juli getroffen door de ransomware, waardoor veel van zijn onlinesystemen werden onderbroken. Vier dagen later, op 27 juli, begonnen de diensten weer online te komen.

 Door **Mark Hendrikman**  
Nieuwsposter  
[Feedback](#)

02-08-2020 • 11:44

362   

Advertentie

 Pre-order nu en krijg 50% korting op Fitbit weegschaal.

Fitbit  
Fitbit Sense Grijs + Fitbit Aria Air Zwart  
359,- 399,99

[Bekijk ze allemaal](#)

HO  
GENT

<https://tweakers.net/nieuws/170450/garmin-heeft-ransomware-losgeld-betaald.html>

### 3.1 Malware en kwaadaardige code

# Ransomware

```
apdata.jpg.garminwasted_info - Notepad2
File Edit View Settings ?
1 GARMIN
2
3 YOUR NETWORK IS ENCRYPTED NOW
4
5 USE PROTONMAIL.CH | @AIRMAIL.CC TO GET THE PRICE FOR YOUR DATA
6
7 DO NOT GIVE THIS EMAIL TO 3RD PARTIES
8
9 DO NOT RENAME OR MOVE THE FILE
10
11 THE FILE IS ENCRYPTED WITH THE FOLLOWING KEY:
12 [begin_key]
13
14
15
16
17
18
19
20
21
22 [end_key]
23 KEEP IT
24
```

1:21 PM	File folder
3:33 PM	GARMINWASTED File
8:44 AM	GARMINWASTED_INFO File
10:55 AM	GARMINWASTED File
8:44 AM	GARMINWASTED_INFO File
1:07 PM	GARMINWASTED File *
8:44 AM	GARMINWASTED_INFO File
11:44 AM	GARMINWASTED File
8:44 AM	GARMINWASTED_INFO File
4:13 PM	GARMINWASTED File
8:44 AM	GARMINWASTED_INFO File
2:51 PM	GARMINWASTED File
8:44 AM	GARMINWASTED_INFO File
3:01 PM	GARMINWASTED File
2020 8:44 AM	GARMINWASTED_INFO File
2020 3:13 PM	GARMINWASTED File
3/2020 8:44 AM	GARMINWASTED_INFO File
2/2020 4:17 PM	GARMINWASTED File
23/2020 8:44 AM	GARMINWASTED_INFO File
22/2020 4:17 PM	GARMINWASTED File

## E-mail en browser aanvallen

- E-mail wordt natuurlijk wereldwijd courant gebruikt. Het geschikte doelwit voor cyber criminelen dus!
- **Spam:** spam, junk mail, ongewenste email, allemaal synoniemen voor iets waar we ons dagdagelijks aan ergeren. In de meeste gevallen gaan de ongewenste emails over advertenties, maar deze kunnen ook verwijzen naar kwaadaardige links met mogelijks misleidende informatie.

Van: PostNL (<mailto:noreply@notificatie.postnl.nl>)  
Verzonden: dinsdag 5 juli 2016 10:45  
Aan: [e-mailadres]  
Onderwerp: Uw PostNL Pakket



Pakketten

Beste heer/mevrouw,

Vandaag bezorg ik bij u een pakket van XPO / ZIGGO, met barcode 352GO452694526. Kijk op [postnl](#), om te zien hoe laat ik bij u langskom.

Mocht u niet thuis zijn dan ontvangt u een bericht met een 'Niet-thuis-code'. Met deze code kunt u vandaag voor 22.00 uur een keuze maken voor een tweede bezorgafspraak.

Maakt u geen keuze, dan kom ik morgen nog een keer bij u langs (m.u.v. zon- en feestdagen).

Met vriendelijke groet,

Uw PostNL Pakketbezorger

Dit is een automatisch gegenereerd bericht - u kunt hier niet op reageren

## E-mail en browser aanvallen

- **Spyware:** probeert informatie te vergaren over een de gebruiker en deze doorsturen naar een externe partij. Vaak worden hiervoor de beveiligingsinstellingen aangepast. Het gaat dan soms over keystrokes verzamelen of data capture. Het doel van spyware is meestal om geld te verdienen.



**HO  
GENT**

## E-mail en browser aanvallen (cont.)

- **Adware:** typisch voor adware zijn de lastige **pop-ups**. Deze pop-ups proberen op één of andere manier winst op te leveren voor de auteur. Het is dan ook **advertentie-ondersteunende software**. Het woord spyware verwijst strikt genomen naar programma's die bijvoorbeeld toetsaanslagen, surfgedrag en ander privacygevoelige informatie achterhalen. Intussen wordt de term gebruikt voor veel meer. Zo wordt adware vaak gemakshalve tot de spywarecategorie gerekend.

**HO  
GENT**



### 3.1 Malware en kwaadaardige code

## E-mail en browser aanvallen (cont.)

- Adware (cont.)



**HO  
GENT**

## E-mail en browser aanvallen (cont.)

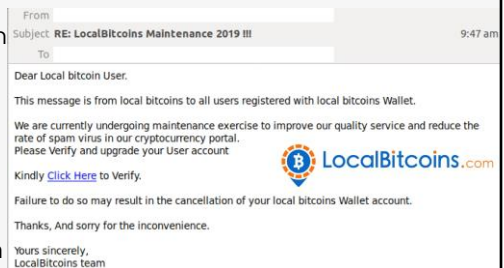
- **Scareware:** probeert de gebruiker te overtuigen door ze bang te maken. Het doet zich bvb. voor als een dialoogvenster van het besturingssysteem.



**HO  
GENT**

## E-mail en browser aanvallen (cont.)

- **Phishing:** is een vorm van fraude. Het woord phishing is ontstaan door het samenvoegen van de woorden 'Password Harvesting Fishing'; in hackerstaal wordt de 'f' wel vaker vervangen door een 'ph'. Hierbij probeert de aanvaller informatie (meestal logingegevens, credit card informatie, etc.) te verkrijgen van het slachtoffer. Vaak krijg je via sociale media of email een link doorgestuurd. De webpagina doet zich dan bvb. voor als een loginscherm van een bank. Gebruikers die denken dat dit loginscherm legitiem is, geven zo hun gegevens bloot aan de aanvaller(s).



**HO  
GENT**

## E-mail en browser aanvallen (cont.)

- **Spear phishing:** is minder algemeen dan phishing. Ze kunnen beide via een email worden verstuurd. Maar bij spear phishing is deze specifiek gericht op een individu, organisatie of bedrijf.
- **Cat phishing:** hierbij wordt vaak een valse identiteit gemaakt en op die manier het vertrouwen van het slachtoffer gewonnen. Soms gaat het hier over een liefdesrelatie op dating sites. Bekende personen worden ook al eens het slachtoffer van cat phishing.

**HO  
GENT**

## Cat phishing

**HILN** + EXCLUSIEF VOOR ABONNEES

### Dit is hoe de mysterieuze 'Eveline' drie BV's kon overtuigen om naaktbeelden van zichzelf te versturen

Onderzoek spitst zich toe op persoon achter Instagramaccount die drie BV's in de val lokte

Erwin Verhoeven | 14 september 2020 | 18u34

**CELEBRITIES** Het gerecht probeert volop te achterhalen wie schuilgaat achter de Instagramaccount 'Eveline', die Stan Van Samang (41), Peter Van de Veire (48) en Sean Dhondt (36) in de val lokte. Volgens onze informatie gebeurde dat volgens een goed geolied scenario dat in alle drie de gevallen bijna identiek verliep. Wie ze is weet voorlopig niemand, en of ze alleen dan wel in opdracht van anderen werkte ook niet. Wel konden we te weten komen hoe ze het deed.

**HO  
GENT**

<https://www.hln.be/showbizz/celebrities/dit-is-hoe-de-mysterieuze-eveline-drie-bv-s-kon-overtuigen-om-naaktbeelden-van-zichzelf-te-versturen~aaf3212c/>

## E-mail en browser aanvallen (cont.)

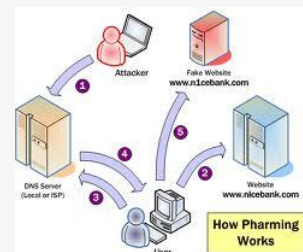
- **Vising:** ofwel **voice phishing** is een vorm van criminele telefoonfraude, waarbij gebruik wordt gemaakt van social engineering via de **telefoon** om toegang te krijgen tot persoonlijke en financiële informatie met het oog op een financiële beloning.



**HO  
GENT**

## E-mail en browser aanvallen (cont.)

- **Pharming:** is een samentrekking van 'phishing' en 'farming'. Bij phishing-aanvallen worden nietsvermoedende slachtoffers met "aas" gelokt. Bij pharming-aanvallen worden **grote aantallen internetgebruikers** gezamenlijk naar de nepwebsite van de hacker geleid. Bij pharming wordt een bestaande webpagina schijnbaar overgenomen door de fraudeur. Hij maakt net als bij phishing een kopie van de betreffende webpagina. De webpagina lijkt op dezelfde plek te staan als het origineel, maar schijn bedriegt. Bij pharming wordt de originele DNS-verwijzing gewijzigd. Door de wijziging wordt de consument doorverwezen naar de nagebootste webpagina, die dan beheerd door de fraudeur.



## E-mail en browser aanvallen (cont.)

- **Whaling:** is een phishing aanval die als doelwit een **hooggeplaatst persoon** heeft. Een CEO of CIO bvb.
- **Plugins:** hackers kunnen ook plugins misbruiken. Plugins zoals Flash en Shockwave (Adobe) worden gebruikt om (browser) content te tonen die met hun software wordt gemaakt.
- **SEO poisoning:** zoekmachines zoals Google werken tonen de resultaten op basis van de query van de gebruiker. Deze **zoekresultaten** worden **geordend** dmv. Search Engine Optimalization. Dit is een verzameling van technieken die er moet voor zorgen dat jouw website **hoog scoort bij de zoekmachines**. Cyber criminelen durven SEO wel eens te misbruiken om hun kwaadaardige software hoog in Google te laten ranken.
- **Browser Hijacker:** dit zorgt dat de browser instellingen worden gewijzigd. Op die manier kunnen criminelen ervoor zorgen dat **jouw browser doorlinkt** naar de website van de “klant” van deze crimineel.

**HO  
GENT**



## **3.2 Misleiding en oplichting**

**HO  
GENT**

## De kunst van het oplichten

- **Social Engineering:** gebruikt geen technologische hoogstandjes, maar is daarom niet minder doeltreffend. Het bestaat erin om het **vertrouwen van jouw slachtoffer te winnen** om dan nadien van het slachtoffer iets te verlangen. Zo kan je bvb. doen alsof je van de beveiligingsfirma bent en vragen om de poort te openen.
- **Pretexting:** het slachtoffer wordt opgebeld en gevraagd om gevoelige informatie vrij te geven om identificatie mogelijk te maken. Er wordt bvb. een credit card nummer gevraagd aan het slachtoffer.
- **Something for something (quid pro quo):** wanneer een attacker persoonlijke informatie over iemand vraagt en **in ruil iets in de plaats geeft**, zoals een cadeau.



# Twitter says hacking of high-profile Twitter accounts was a "coordinated social engineering attack"

BY LI COHEN

JULY 16, 2020 / 11:11 AM / CBS NEWS



Some of the world's richest and most influential politicians, celebrities, tech moguls and companies were the subject of a massive Twitter hack on Wednesday. Elon Musk, Joe Biden, Jeff Bezos, Michael Bloomberg, Kim Kardashian West and Bill Gates were among the accounts pushing out tweets asking millions of followers to send money to a Bitcoin address.



**HO  
GENT**

<https://www.cbsnews.com/news/twitter-hack-verified-accounts-social-engineering-bitcoin-scam/#:~:text=Bob%20Woodward-,Twitter%20says%20hacking%20of%20high%2Dprofile%20Twitter%20accounts,a%20%22coordinated%20social%20engineering%20attack%22&text=Some%20of%20the%20world%27s%20richest,massive%20Twitter%20hack%20on%20Wednesday.>

## Soorten oplichting

- **Shoulder Surfing en Dumpster Diving:** verwijst naar het **aflezen/meelezen** van PIN-codes of wachtwoorden en dergelijke. Hiervoor kan de dader dichtbij staan of hij kan een camera of verrekijker gebruiken.
- **Impersonation en Hoaxes:** letterlijk: verpersonificeren of uitbeelden. Doen alsof je iemand anders bent. Een hoax is een **nepbericht** zoals een valse email van het WWF.
- **Piggybacking en Tailgating:** beiden zijn een term voor het **mee glippen** met personen die wél toegang hebben tot een plaats met beperkte toegang.
- **Online, Email, en Web-based Trickery:** het bewust forwarden van hoax emails, grappige filmpjes en dergelijke. Dit kan ingaan tegen de bedrijfspolicy en kosten bedrijven heel wat geld.



**HO  
GENT**

## **3.3 Cyber aanvallen**

**HO  
GENT**

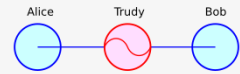
## Soorten cyber aanvallen

- **Denial-of-Service (DoS) Attacks:** is een manier om een netwerk aan te vallen. Zo een aanval resulteert in het **niet beschikbaar** zijn van een bepaalde netwerk service (bvb. web service). Een DoS attack is een groot risico en kan ervoor zorgen dat je veel tijd en geld verliest. Je hoeft niet veel talent te hebben om een DoS attack uit te voeren: deze zijn relatief makkelijk uit te voeren.
- **Sniffing:** is gelijkaardig aan iemand afluisteren. De dader zal alle **netwerkverkeer** die passeert aan de NIC (Network Interface Card) **bekijken**, ook het netwerkverkeer dat niet voor hem bedoeld was. Daders gebruiken speciale software en/of hardware om het netwerk te sniffen.
- **Spoofing:** hierbij ga je de werkelijkheid gaan **vervalsen**. Zo gaat de dader kenmerken gaan aanpassen om te doen alsof hij/zij iemand anders is. Zo zal men bij *email spoofing* de header (bvb. From (Van), Return-Path (Afzender), ...) aanpassen. Zo kan men doen alsof de email door iemand anders werd verstuurd. Je hebt ook nog andere vormen van spoofen zoals *URL spoofing* of *IP spoofing*.

HO  
GENT

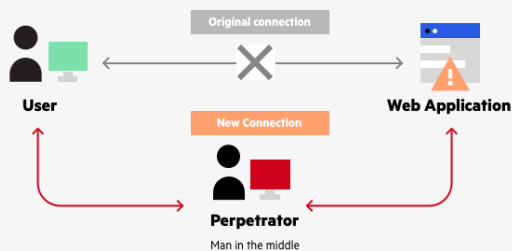
DDoS digital attack maps:

- <https://www.digitalattackmap.com>
- <https://cybermap.kaspersky.com/>
- <https://threatmap.checkpoint.com/>



## Soorten cyber aanvallen (cont.)

- **Man-in-the-middle:** bij een MitM-aanval zal de cyber crimineel trachten informatie te stelen dat wordt verstuurd over een netwerk **tussen twee toestellen**. Hij kan er ook voor kiezen om de boodschap aan te passen en op die manier valse informatie verspreiden tussen de hosts. De hosts zijn zich op dat moment niet bewust van de aanval. Een MitM-aanval laat de dader toe om de controle over te nemen zonder dat de andere partijen dit weten.



**HO  
GENT**

## Soorten cyber aanvallen (cont.)

- **Zero-Day attacks:** bij een zero-day attack wordt geprobeerd om gebruik te maken van een **kwetsbaarheid** in software die **nog niet** is **gekend**. Day zero (of zero hour) verwijst naar het moment waarop de lek wordt ontdekt.



**HO  
GENT**



## Soorten cyber aanvallen (cont.)

- **Keyboard Logging:** is een computerprogramma die de **toetsenbordaanslagen** (keystrokes) gaat **opnemen** of loggen. Dit stukje software wordt dan op het toestel van het slachtoffer geïnstalleerd. De dader programmeert de software om dan na afloop de log file of opname via email door te sturen naar de dader. In de log file kan dan gevoelige informatie staan zoals de emailadressen, wachtwoorden, pincodes, etc.



**HO  
GENT**

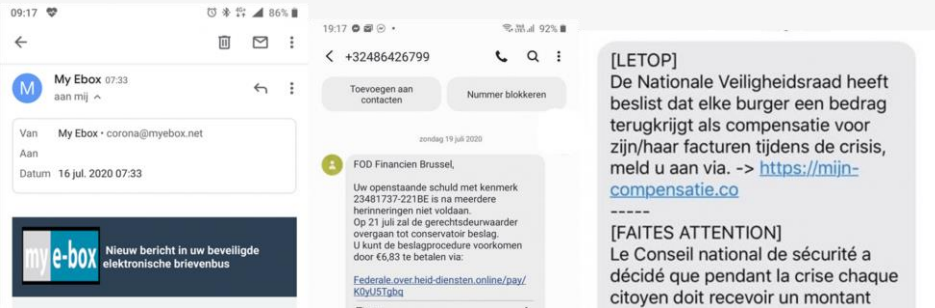
## Draadloze en mobiele aanvallen

- **Grayware:** omvat apps die zich **enerverend** of **ongewenst** gaan gedragen. Met de groei aan populariteit van de smartphone wordt dit alsmaar een groter probleem
- **SMiShing:** ofwel SMS Phishing zal fake SMS (Short Message Service) gebruiken om **valse berichten** te sturen. De dader zal op die manier proberen het slachtoffer te **lokken** naar een website of **verleiden** om te bellen naar een bepaald telefoonnummer. Nietsvermoedende slachtoffers kunnen dan vertrouwelijke informatie doorgeven. Het bezoeken van een schadelijke website kan dan weer zorgen dat je ongewenste malware op jouw toestel downloadt.



### 3.3 Cyber aanvallen

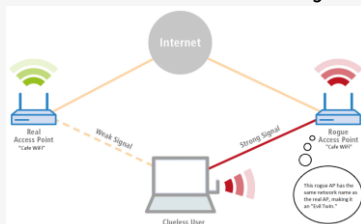
## SMiShing



**HO  
GENT**

## Draadloze en mobiele aanvallen (cont.)

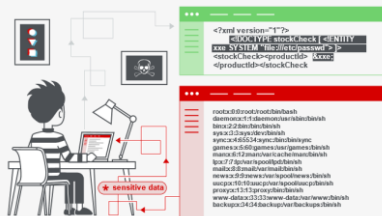
- **Frauduleuze (Rogue) Access Point:** wordt in het netwerk geplaatst en **doet zich voor als** een **vertrouwelijk** apparaat. Dit laat je toe MitM-attacks uit te voeren. Het Access Point wordt geplaatst en zorgt ervoor dat mensen hun verkeer via dit Access Point versturen waardoor het Access Point de data kan zien en analyseren.



**HO  
GENT**

## Applicatie aanvallen

- Cross-site scripting (XSS): is een **kwetsbaarheid** die wordt gevonden **in web applicaties**. Via XSS kan je **scripts injecteren** in een webpagina die beschikbaar is voor de gebruiker. De crimineel valt het **slachtoffer niet rechtstreeks** aan maar wel de website. Uiteraard is het het slachtoffer die de website bezoekt. De dader slaagt er soms in om files te bekijken op de web server die niet voor hem bedoeld zijn.

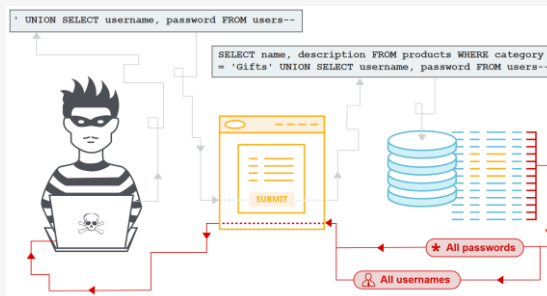


**HO  
GENT**

Meer info op <https://portswigger.net/web-security/xxe>

## Applicatie aanvallen

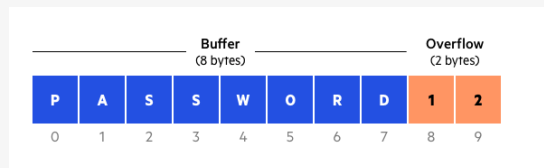
- **Code Injections aanvallen:** één van de meest gebruikte manieren om data op te slaan voor een website is door gebruik te maken van een **databank** (DB). Via een *SQL injection* bvb. zal men proberen om een SQL databank aan te vallen. Men **injecteert** dan een **query** om deze uit te voeren. Developers dienen zich bewust te zijn van de potentiële gevaren. In een labo zullen we zo een login trachten te omzeilen. *XML injections* kunnen evenwel een gevaar vormen.



HO  
GENT

## Applicatie aanvallen (cont.)

- **Buffer Overflow:** wanneer data **over zijn limiet** gaat. Buffers zijn geheugen die door een applicatie worden gebruikt. Door de data aan te passen en te vergroten tot het de **buffers overschrijdt**, gebruikt de applicatie geheugen dat door een ander proces wordt gebruikt en krijg je een error. Deze error kan dan een applicatie crash of het verlies van data zijn.



**HO  
GENT**

## Applicatie aanvallen (cont.)

- **Remote code executions:** hierbij kan de dader gebruik maken van een **kwetsbaarheid** waarbij hij/zij code **vanop** afstand kan uitvoeren. Het is dan bvb. mogelijk om over het **netwerk** of over het internet het toestel van het slachtoffer aan te vallen.
- **ActiveX Controls:** stukjes software die worden geïnstalleerd als **plug-in** in een browser zoals Internet Explorer. Deze software kan dan bvb. de gewoontes van de gebruiker analyseren of het lezen van toetsaanslagen, etc.

**HO  
GENT**



## Applicatie aanvallen (cont.)

- **Java:** wordt uitgevoerd via een interpreter (= vertaler), de Java Virtual Machine (JVM). Normaal gezien draait kwaadaardige code in de **sandbox** omgeving van de JVM. Soms lukt het daders echter om deze sandbox te omzeilen en zo toch code uit te voeren op het besturingssysteem van het slachtoffer. De dader maakt hierbij dan gebruik van een al dan niet gekende kwetsbaarheid in Java.

## Java wordt gepatcht

NEWS

f in t

### Oracle's Latest CPU Includes 20 Security Patches for Java SE

By John K. Waters ■ 10/22/2019

Oracle's latest quarterly [Critical Patch Update](#) (CPU) provides 219 new security patches across Oracle's product line, including 20 new patches for Java SE. But none of the Java patches in this CPU earned a CVSS risk score of greater than 6.8 out of 10.0.

The Java versions affected by this CPU are Java SE, versions 7u231, 8u221, 11.0.4, 13; and Java SE Embedded, version 8u221.

Oracle uses the Common Vulnerability Scoring System (CVSS) to provide an open and standardized rating of the security holes it finds in its products. Each vulnerability is issued a unique CVE number (<http://cve.mitre.org>). The highest CVSS score this time around (6.8) went to CVE-2019-2909, a vulnerability in the Java VM component of Oracle Database Server.



HO  
GENT

<https://adtmag.com/articles/2019/10/22/oracle-cpu.aspx>

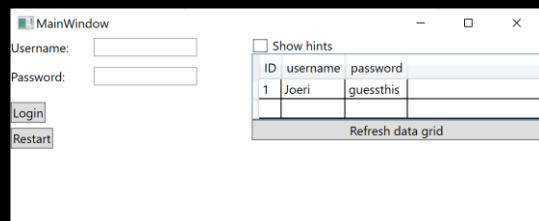
## Applicatie aanvallen (cont.)

- Beschermen tegen deze aanvallen:
  - First-line defense: programmeurs moeten stabiele code schrijven
  - Alle user input van buitenaf beschouwen als vijandige of kwaadaardige code
  - Alle user input valideren en controleren
  - Alle software waaronder plug-ins up-to-date houden door updates regelmatig uit te voeren
  - Niet alle updates worden automatisch uitgevoerd, dus controleer zelf manueel ook altijd eens of er geen updates kunnen worden uitgevoerd
  - Never ending story: in de volgende jaren zal je nog meer leren hoe je je kan beschermen en hoe je aanval uitvoert.

**HO  
GENT**

# Labo – SQL Injection

We gaan volgende login proberen aanvallen



The screenshot shows a web application window titled "MainWindow". On the left, there is a login form with two input fields: "Username:" and "Password:". Below these fields are two buttons: "Login" and "Restart". On the right, there is a checkbox labeled "Show hints" which is currently unchecked. Below the checkbox is a data grid with three columns: "ID", "username", and "password". The first row of the grid contains the values "1", "Joeri", and "guessthis". Below the grid is a button labeled "Refresh data grid".

ID	username	password
1	Joeri	guessthis

Labo

## Labo – SQL Injection

- We gaan volgende login proberen hacken
- Download op Chamilo deze applicatie

MainWindow

Username:

Password:

Login

Restart

☐ Show hints

ID	username	password
1	Joeri	guessthis

Refresh data grid

© 2007 het Hogeschool / Hoger Instituut vzw

**HO  
GENT**

Labo

## Labo – SQL Injection

- Start volgende applicatie en probeer zelf:

The screenshot shows a web application window titled "MainWindow". On the left, there is a login form with two input fields: "Username:" and "Password:". Below these fields are two buttons: "Login" and "Restart". On the right, there is a checkbox labeled "Show hints" which is currently unchecked. Below the checkbox is a data grid with three columns: "ID", "username", and "password". The first row of the grid contains the values "1", "Joeri", and "guessthis". Below the grid is a button labeled "Refresh data grid".

ID	username	password
1	Joeri	guessthis

**HO  
GENT**

Labo

## Labo – SQL Injection

- Ga zelf eens op het internet op zoek naar info over SQL Injections

The screenshot shows a web application window titled "MainWindow". On the left, there is a login form with two input fields labeled "Username:" and "Password:", followed by "Login" and "Restart" buttons. On the right, there is a "Show hints" checkbox and a data grid. The data grid has three columns: "ID", "username", and "password". The first row contains the values "1", "Joeri", and "guessthis". Below the grid is a "Refresh data grid" button. At the bottom left of the window, there is a small copyright notice: "© 2022 Doe Management (For demo purposes only)".

ID	username	password
1	Joeri	guessthis

## **Labo – SQL Injection**

- Probeer eens om:
  - In te loggen zonder dat je het wachtwoord gebruikt (vertrouwelijkheid)
  - Een nieuwe gebruiker toe te voegen (integriteit)
  - De tabel te verwijderen zodat het systeem niet meer beschikbaar is (beschikbaarheid)



# Scenario 0

– Proberen in te loggen met verkeerde login gegevens

The screenshot shows the 'MainWindow' of a login application. The 'Username' field contains 'Joeri' and the 'Password' field contains 'DontKnow'. Below the password field, the text 'Bad login! Not through' is displayed in red. The 'Login' button is highlighted in red, and the 'Restart' button is visible below it. On the right side, a panel titled 'Try this in the password field' contains three scenarios: Scenario 1: 'OR 1=1--', Scenario 2: 'Robert; DROP TABLE Users; --', and Scenario 3: 'Robert; INSERT INTO Users (username, password) VALUES('Lindsay', 'LetMeIn'); --'. Below the scenarios is a table with columns 'ID', 'username', and 'password'. The first row shows '1', 'Joeri', and 'guessthis'. A 'Refresh data grid' button is at the bottom of the table.

ID	username	password
1	Joeri	guessthis

– Proberen in te loggen met de juiste login gegevens

The screenshot shows the 'MainWindow' of the login application after a successful login. The 'Username' field contains 'Joeri' and the 'Password' field contains 'guessthis'. Below the password field, the text 'Welcome, Joeri. You successfully loggedin.' is displayed in green. The 'Login' button is highlighted in green, and the 'Restart' button is visible below it. The right panel is identical to the previous screenshot, showing the same scenarios and table.

ID	username	password
1	Joeri	guessthis

HO  
GENT

# Scenario 1

– Inloggen zonder de login gegevens te kennen

MainWindow

Username:

Password:

Welcome, Joeri. You successfully loggedin.

Try this in the password field:

Scenario 1:  
' OR 1=1--

Scenario 2:  
Robert'; DROP TABLE Users; --)

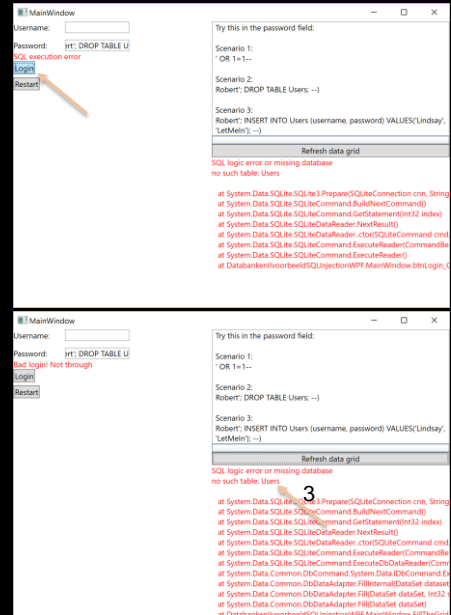
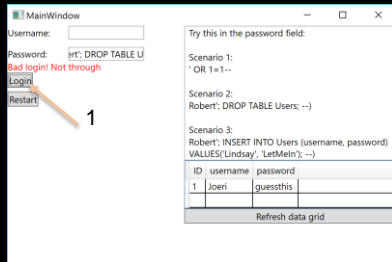
Scenario 3:  
Robert'; INSERT INTO Users (username, password)  
VALUES('Lindsay', 'LetMeIn'); --)

ID	username	password
1	Joeri	guessthis

HO  
GENT

# Scenario 2

– Verwijderen van de tbl Users



# Herbegin

MainWindow

Username:

Password:

You can start again

Login

Restart

Try this in the password field:

Scenario 1:  
' OR 1=1--

Scenario 2:  
Robert'; DROP TABLE Users; --)

Scenario 3:  
Robert'; INSERT INTO Users (username, password) VALUES('Lindsay', 'LetMeIn'); --)

ID	username	password
1	Joeri	guessthis

Refresh data grid

HO  
GENT

# Scenario 3

– Nieuwe gebruiker toevoegen

MainWindow

Username:

Password:  ert; INSERT INTO U

Bad login! Not through

Login

Restart

Try this in the password field:

Scenario 1:  
' OR 1=1--

Scenario 2:  
Robert; DROP TABLE Users; --)

Scenario 3:  
Robert; INSERT INTO Users (username, password) VALUES('Lindsay', 'LetMeIn'); --)

ID	username	password
1	Joeri	guessthis

Refresh data grid

MainWindow

Username:  Lindsay

Password:  LetMeIn

Welcome, Lindsay, You successfully logged in.

Login

Restart

Try this in the password field:

Scenario 1:  
' OR 1=1--

Scenario 2:  
Robert; DROP TABLE Users; --)

Scenario 3:  
Robert; INSERT INTO Users (username, password) VALUES('Lindsay', 'LetMeIn'); --)

ID	username	password
1	Joeri	guessthis

Refresh data grid

HO  
GENT

# Scenario 3

– Gebruiker is effectief toegevoegd (zie data grid)

MainWindow

Username:

Password:

Welcome, Lindsay. You successfully loggedin.

Try this in the password field:

Scenario 1:  
' OR 1=1--

Scenario 2:  
Robert'; DROP TABLE Users; --)

Scenario 3:  
Robert'; INSERT INTO Users (username, password)  
VALUES('Lindsay', 'LetMeIn'); --)

ID	username	password
1	Joeri	guessthis
2	Lindsay	LetMeIn

Refresh data grid

HO  
GENT

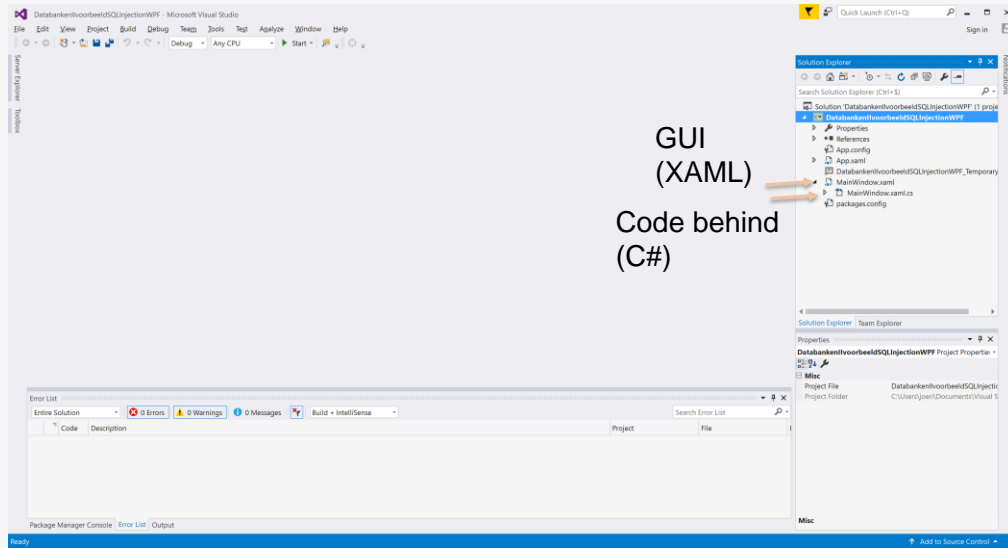
Labo

## **Labo – SQL Injection – kwetsbaarheid**

- Wat is het probleem hier?
- Wat denk jij?

**HO  
GENT**

## Labo





```

Labo
private void btnLogin_Click(object sender, RoutedEventArgs e)
{
    var command = conn.CreateCommand();

    //Lezen uit tabel
    command.CommandText = "SELECT * FROM Users WHERE Username = '" + txtUsername.Text +
        "' AND Password = '" + txtPassword.Text + "'";

    try
    {
        SQLiteDataReader reader = command.ExecuteReader();

        if (reader.Read()) //kwetsbaarheid
        {
            //logged in (volledige toegang)
            lblOutput.Foreground = new SolidColorBrush() { Color = Colors.Green };
            lblOutput.Text = "Welcome, " + reader.GetString(1) + ". You successfully
logged in.";
            lblError.Text = "";
        }
        else
        {
            //not logged in
            lblOutput.Foreground = new SolidColorBrush() { Color = Colors.Red };
            lblOutput.Text = "Bad login!";
        }
    }
}

```

**HO  
GENT**

## **Labo – SQL Injection – Oplossing**

- Wat is hier het probleem?
- Invoer van de gebruiker is mogelijks een kwetsbaarheid (verwerken van data – zie H2)
  - Parameters
  - Stored procedure
  - Valideer invoer van de gebruiker
- Zie meer in Databanken II (2de jaar)

**HO  
GENT**