WORKSHOP

Aanvalspad van een hacker

SAMENWERKEN AAN
CYBERVEILIGHEID
IN HET MBO

PROGRAMMA
Cyberveiligheid

NETWERK
Informatiebeveiliging
en Privacy

MBO Raad

mbo digitaal

mbodigitaal.nl/cyberveiligheid

Jeffeny Hoogervorst
LLM, CISM, CISSP, CEH, ECSA, CPTE

Technisch productmanager SURFsoc
Kernel member SURFcert

jeffeny.hoogervorst@surf.nl

Mick Deben
CISSP | CRISC | CGEIT | CCSP

Adviseur Cybersecurity
MBO Digitaal

m.deben@mbodigitaal.nl


The Cyber Kill Chain
SURF

The Cyber Kill Chain

Hoe elke aanval werkt volgens Lockheed Martin (the Cyber Kill Chain®)

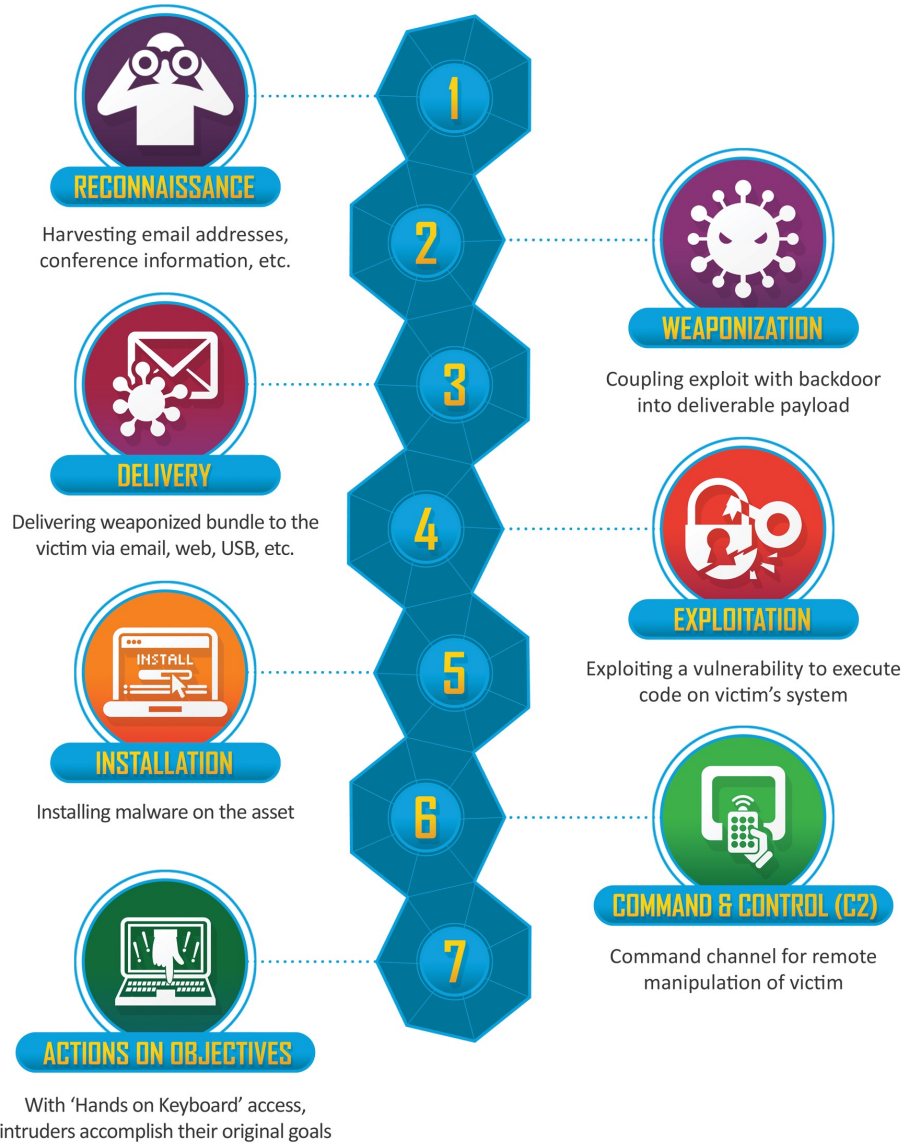


Image source: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Reconnaissance

Verkenning van het “doelwit”

In de eerste fase gaat de aanvaller op onderzoek uit om informatie over Het doelwit te verzamelen. Bijvoorbeeld door de kwetsbaarheden te identificeren die kunnen worden uitgebuit

Informatie verzamelen

- Passief informatie verzamelen
- Actief informatie verzamelen

Reconnaissance

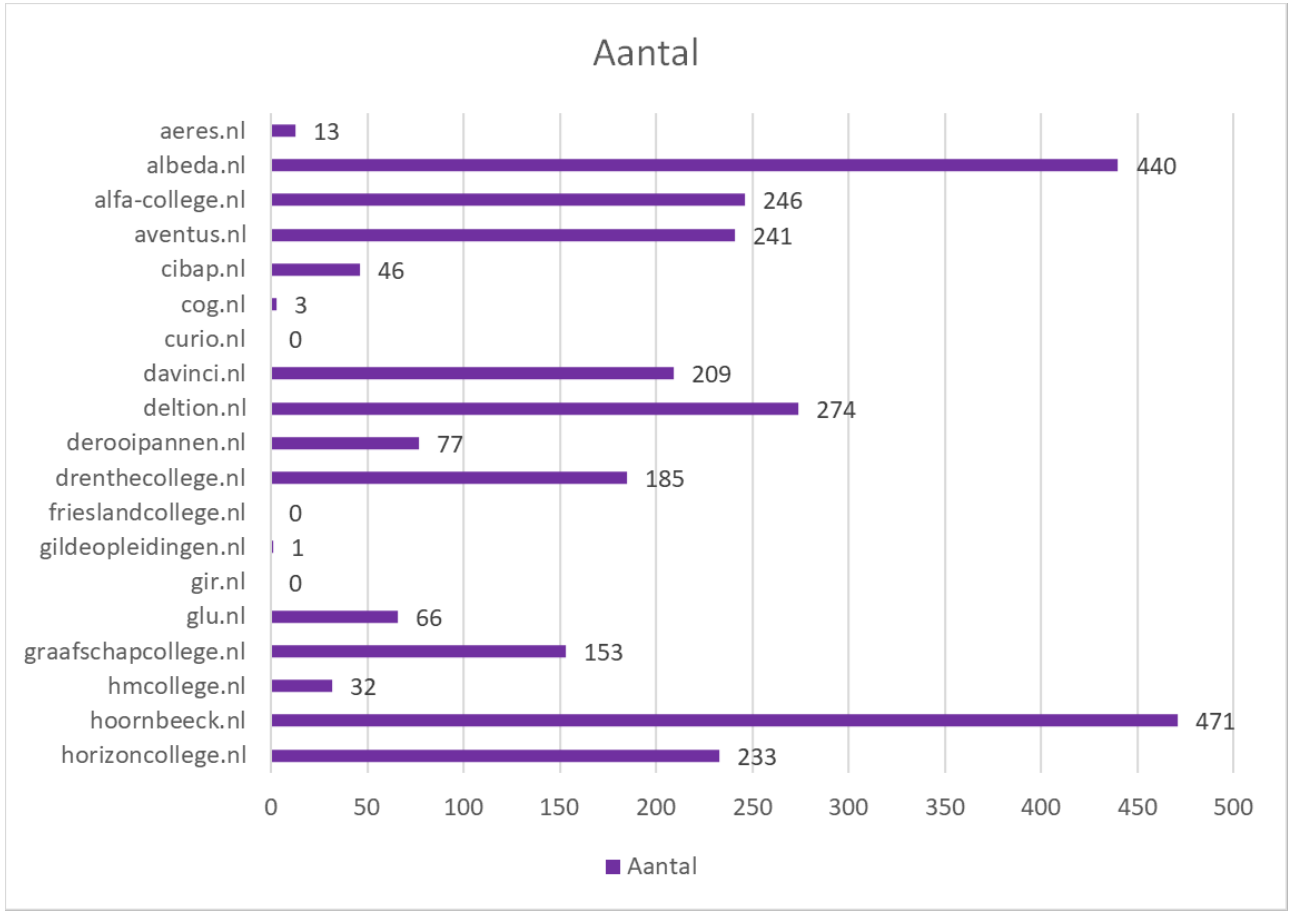
Passief informatie verzamelen

- Informatie uit vacatures
- Metagegevens van documenten
- Marketingcommunicatie
- E-mailadressen
- Externe infrastructuur
- Gebruikte technologieën
- …

- Uitgelekte wachtwoorden
- Toegang op afstand
- Gebruikte defensieve technologieën
- Organisatie structuur
- Kennis over cybersecurity
- Sociale media

Reconnaissance

Uitgelekte wachtwoorden



Reconnaissance

Google Dorks

- Index van zoekopdrachten
- Openbare informatie
- Zoeken naar bepaalde informatie of naar kwetsbare web applicaties
- https://www.exploit-db.com/google-hacking-database

Voorbeelden:

- site:.nl intitle:"index of”
- intitle:"ADSL Router" inurl:"/login.htm”
- site:.lk intitle:"index of" ”backup”
- intitle:"index of" "wp-config.php.bak”

SURF

RECONNAISSANCE

Reconnaissance

Google Dorks

Index of /wordpress

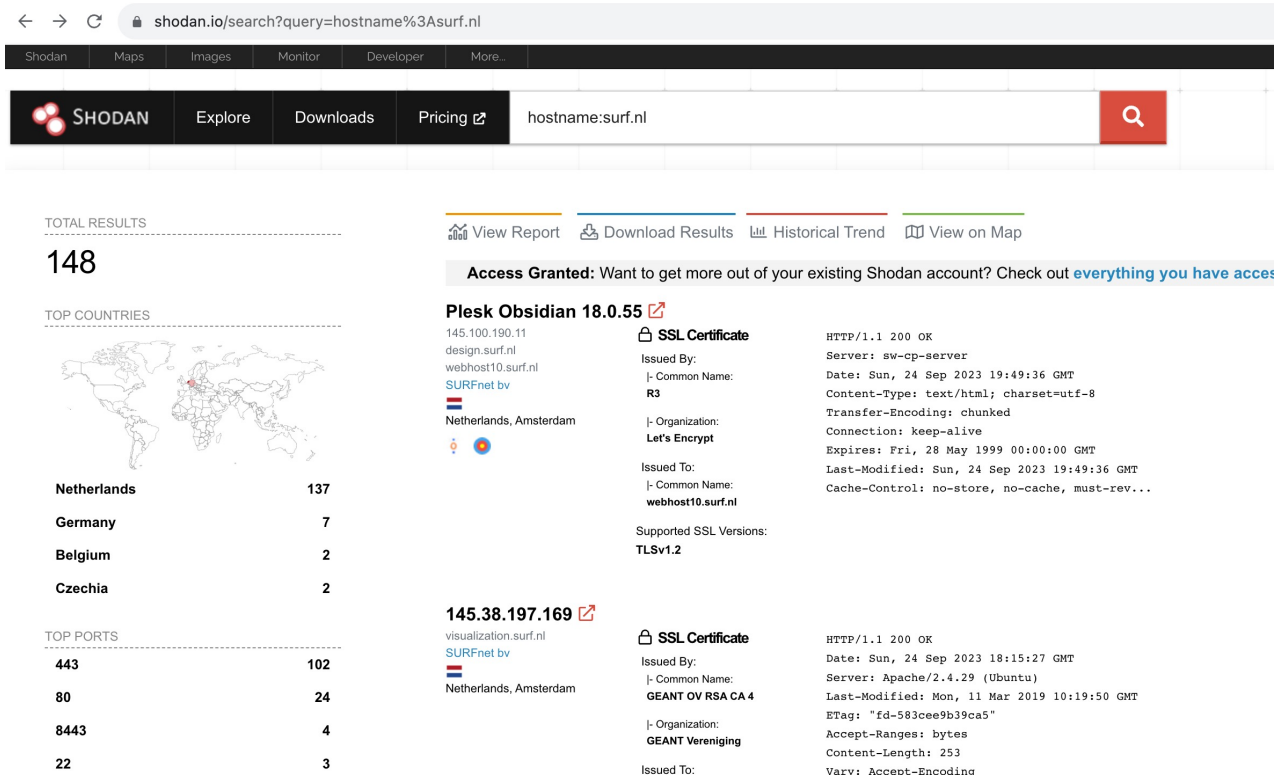
Name	Last modified	Size	Description
Parent Directory		-	
sitemap.xml	2020-04-29 14:29	1.1K	
sitemap.xml.gz	2020-04-29 14:29	512	
wp-config.php.bak	2013-05-03 00:27	3.1K	
wp-content/	2020-05-05 14:38	-	

SURF

RECONNAISSANCE

Reconnaissance

Shodan



SURF

RECONNAISSANCE

Reconnaissance

Censys

censys | Hosts | (location.city=`Utrecht`) and services.service_name=`RDP` | Search

Results | Try CensysGPT Beta | Report

Host Filters

Labels:

487 network-administration
487 remote-access
115 file-sharing
77 login-page
42 network.device
More

Autonomous System:

155 TRANSIP-AS Amsterdam, the Netherlands
89 TNF-AS
82 KPN KPN National
29 LEASEWEB-NL-AMS-01 Netherlands
17 TMOBILE-THUIS
More

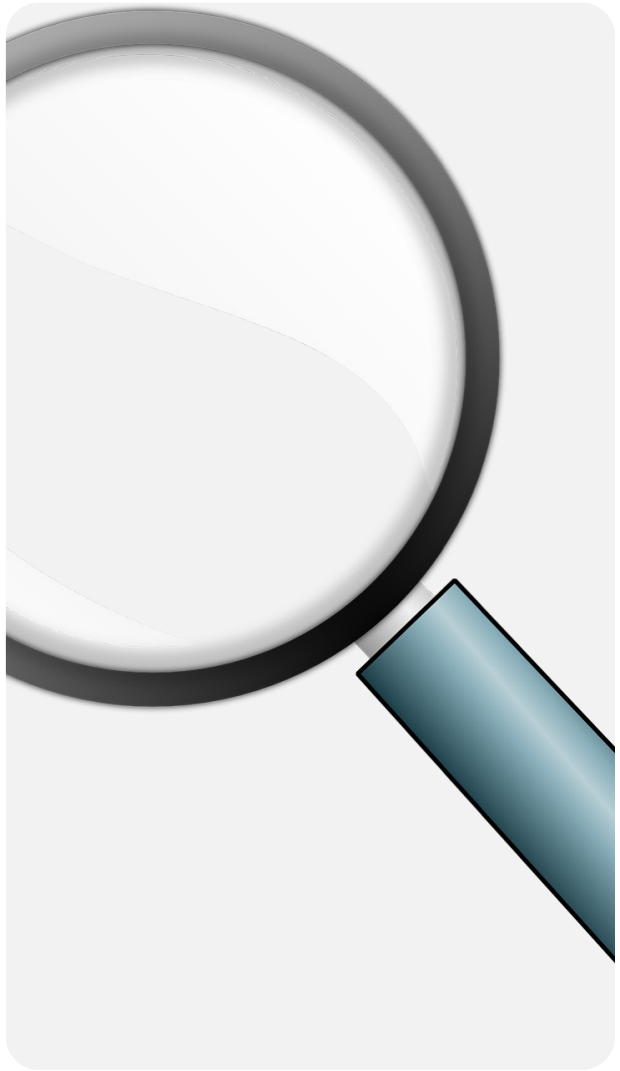
Hosts

Results: 487 Time: 0.11s

213.126.63.60 (D57E3F3C.static.ziggozakelijk.nl)
TNF-AS (33915) Utrecht, Netherlands
remote-access | network-administration
443/UNKNOWN 3500/RDP

149.210.143.61 (149-210-143-61.colo.transip.net)
Microsoft Windows TRANSIP-AS Amsterdam, the Netherlands (20857) Utrecht, Netherlands
network-administration | remote-access
139/NETBIOS 3389/RDP 5000/UNKNOWN 5357/HTTP 5985/HTTP

185.42.73.240 (static.ip-185-042-073-240.signet.nl)
SIGNETBREEDBAND (39700) Utrecht, Netherlands
network-administration | remote-access
150/RDP



SURF

RECONNAISSANCE

Reconnaissance

Actief informatie verzamelen

- Applicaties en services hebben standaard poortnummers

- Enkele bekende poortnummers:
  - FTP tcp/21
  - SSH tcp/22
  - Telnet tcp/23
  - Webserver tcp/80 (insecure) and tcp/443 (secure)
  - MSSQL tcp/1433
  - MySQL tcp/3306
  - Remote Desktop Protocol (RDP) tcp/3389

- https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

SURF

RECONNAISSANCE

Reconnaissance

Actief informatie verzamelen

- Banner grabbing
  - nmap -sV 192.168.1.1 80
  - nc 192.168.1.1 80
  - telnet 192.168.1.1 21
  - wget –q –S 192.168.1.1
  - curl –s –I 192.168.1.1
  - nikto –h http:// 192.168.1.1

SURF

RECONNAISSANCE

Reconnaissance

Nuclei (vulnerability scanner)

```
cat staging-apps.txt
https://staging.example.com
https://staging.admin.example.com
https://staging.crm.example.com
https://api-staging.example.com
https://internal.example.com
https://build-app.example.com
https://demo.example.com
https://preprod.backend-api.example.com

nuclei -t amazon-mww-secret-leak.yaml -l staging-apps.txt

                     __     _
     ____  __  _____/ /__  (_)
    / __ \/ / / / ___/ / _ \/ /
   / / / / /_/ / /__/ /  __/ /
  /_/ /_/\__,_/\___/_/\___/_/   v2.2.0

    projectdiscovery.io

[WRN] Use with caution. You are responsible for your actions
[WRN] Developers assume no liability and are not responsible for any misuse or damage.
[INF] Loading templates...
[INF] [amazon-mww-secret-leak] Amazon MWS Auth Token leak (@puzzlepeaches) [medium]
[INF] Using 1 rules (1 templates, 0 workflows)
[amazon-mww-secret-leak] [http] [medium] https://internal.example.com
[amazon-mww-secret-leak] [http] [medium] https://build-app.example.com
[amazon-mww-secret-leak] [http] [medium] https://staging.admin.example.com
```

Image source: https://github.com/projectdiscovery/nuclei

SURF

RECONNAISSANCE

Reconnaissance

Dumpster diving

Image source: Pixabay

Reconnaissance

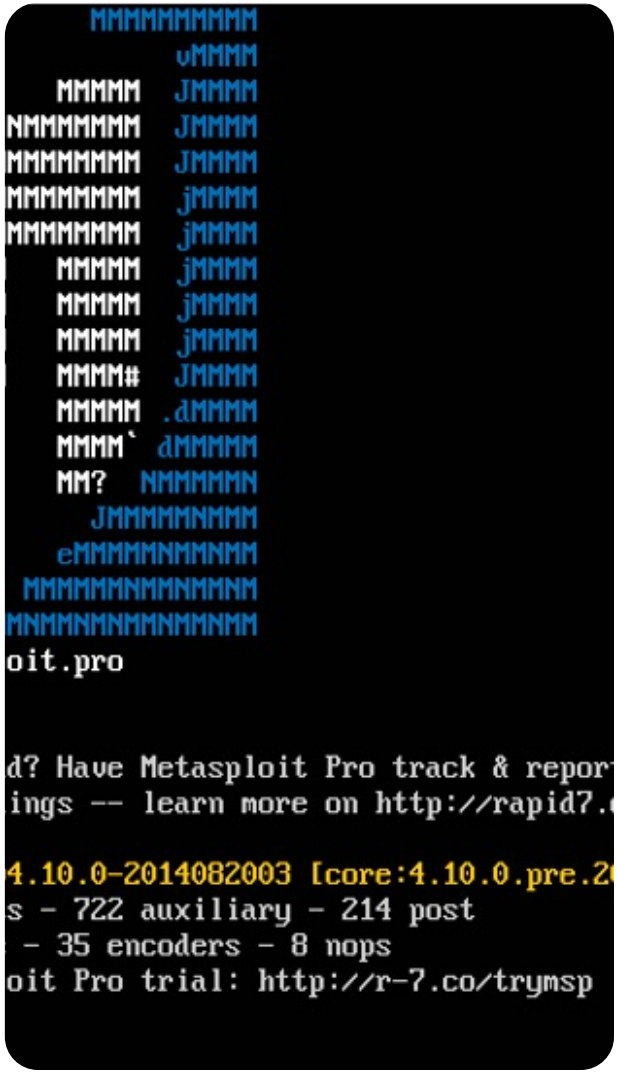
Social engineering

Image source: Pixabay

Weaponization

Bewapening

- Bij bewapening creëert de aanvaller malware om kwetsbaarheden van het doelwit te misbruiken.
- Bijvoorbeeld door het creëren van een PDF document met een reverse TCP sessie.
- Verbergen van aanvalscode (obfuscation)



SURF

WEAPONIZATION

Delivery

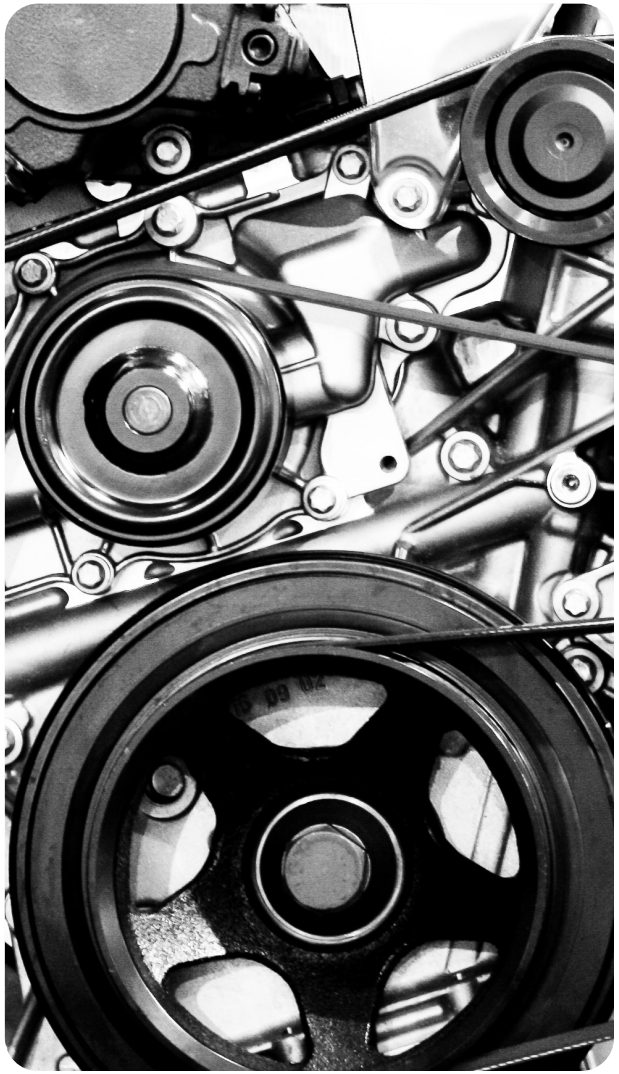
Levering

- Dit is waar het wapen naar het doel wordt gestuurd
- E-mail
- Exploits die via internet/netwerk worden geleverd, kunnen door IDS worden gedetecteerd
- Verstuur van malware per post
- USB-sticks op de parkeerplaats verspreiden
- Maak een afspraak met iemand op kantoor

Exploitation

Uitbuiting

- De malware wordt gelanceerd en maakt misbruik van de kwetsbaarheden van het doelwit.
- Anti-Malware kunnen ze detecteren door kenmerken en afwijkingen
- Het is minder waarschijnlijk dat 0-day, aangepaste en gecodeerde exploits alleen worden ontdekt op basis van handtekeningdetectie.
- Verbindingen van binnen naar buiten zijn vaak (meer) open, daarom wordt vaak gebruik gemaakt van “Reverse TCP sessies”.



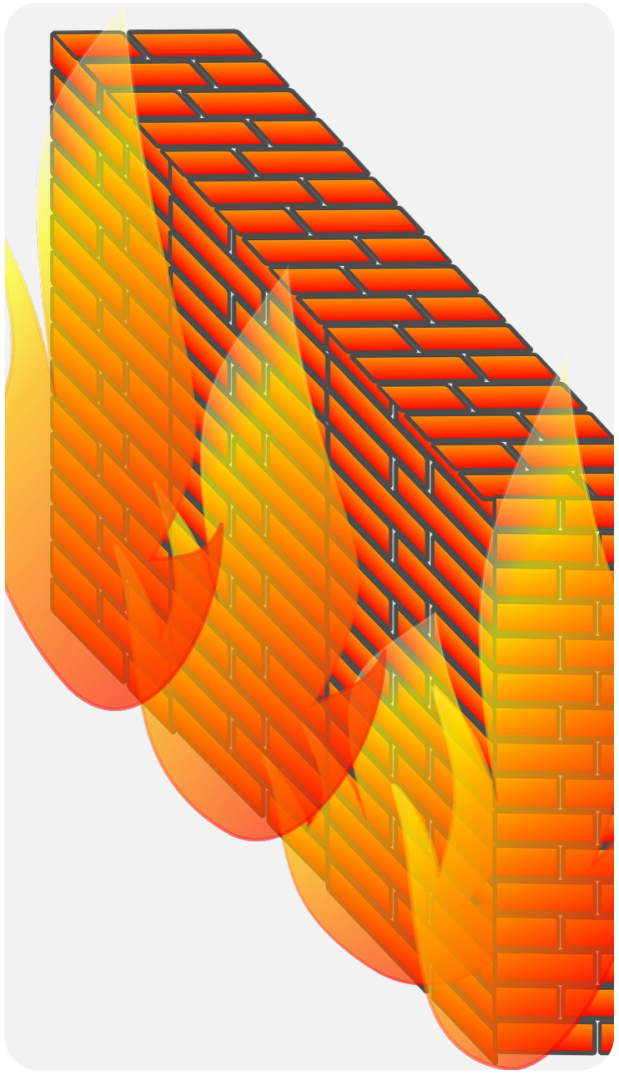
SURF

EXPLOITATION

Installation

Installatie

- Direct na de exploitatiefase wordt de malware op het systeem van het doelwit geïnstalleerd
- Aanvaller creëert een achterdeur of zet een sessie van binnen naar buiten open



Command and Control (C2)

Commando & Controle

De malware geeft de indringer/aanvaller toegang tot het netwerk/systeem

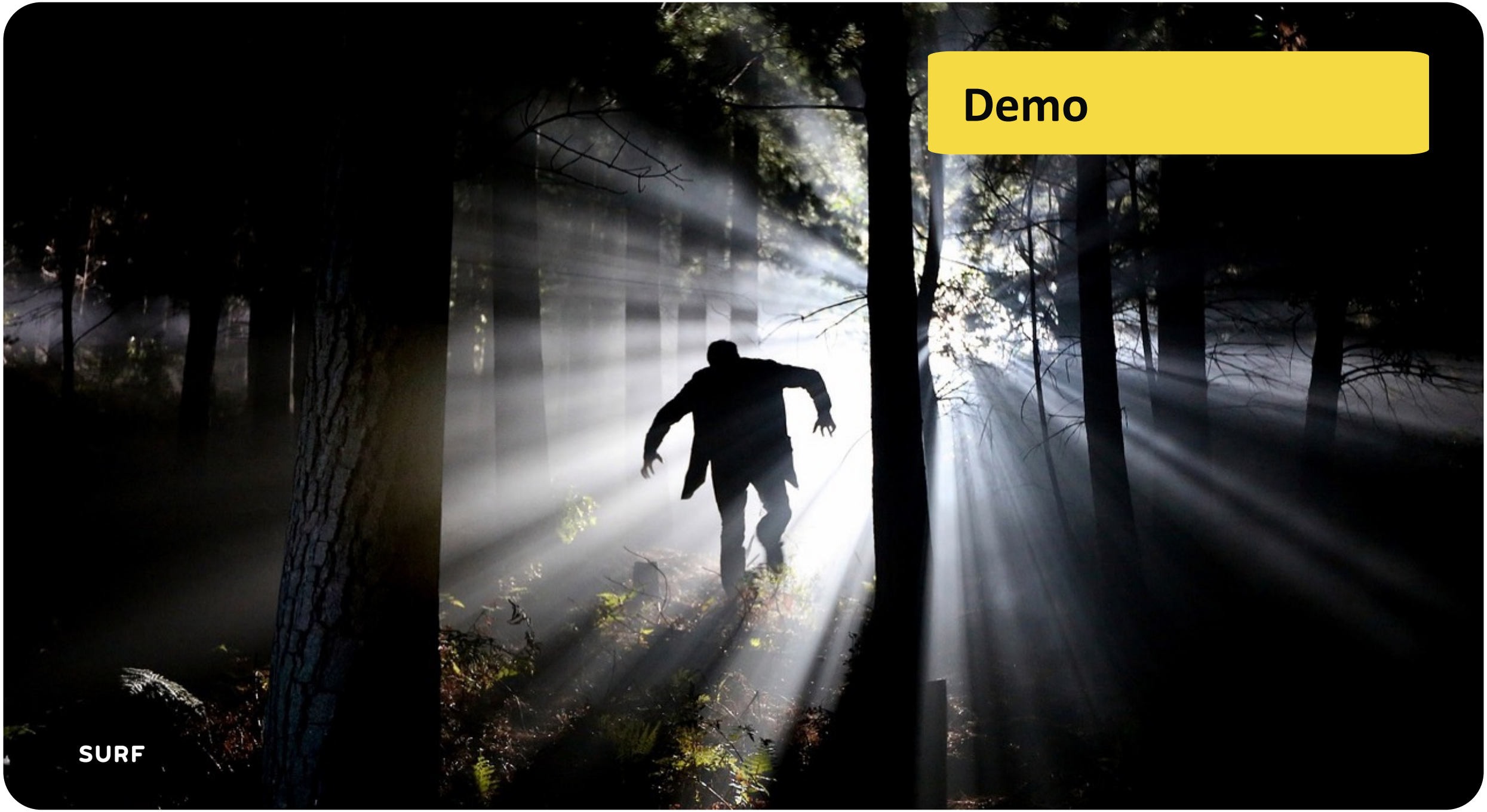
In dit stadium kan de aanvaller ook zijwaarts door het netwerk bewegen (lateral movement) op zoek naar het daadwerkelijke doelwit of de systemen met verhoogde rechten

Actions on Objective

Acties en doelstellingen

Actie ondernemen om de beoogde doelen te bereiken

- Data diefstal (info stealers)
- Destructie (wipers)
- Versleuteling/gijzeling (ransomware)
- …


Demo
SURF


VIVE
Bedankt voor uw aandacht!
SURF