Hacking like an APT

Alexander Sturz
Atos Information Technology GmbH
05/19/2022

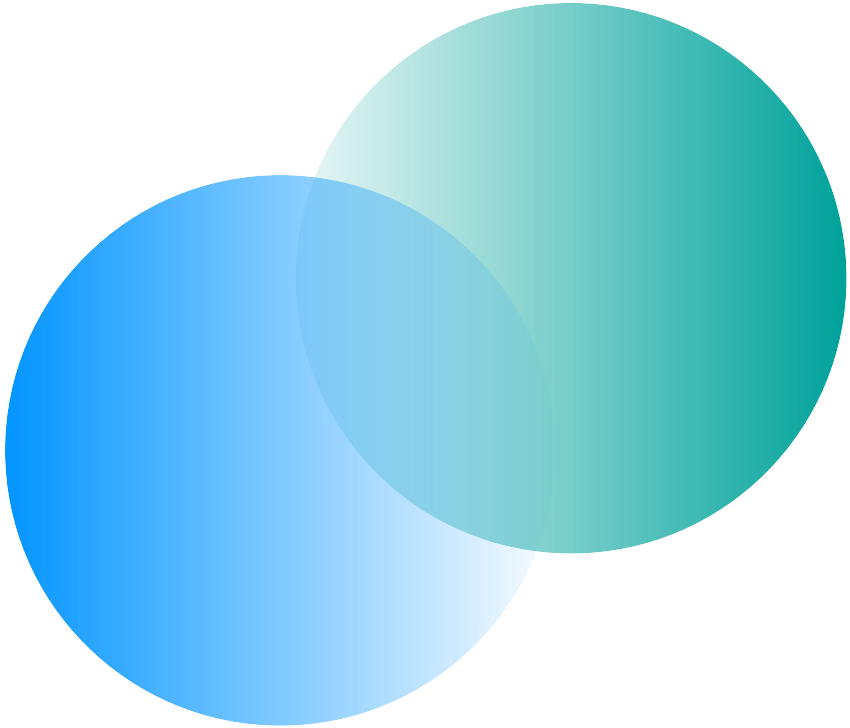
Hacking like an APT

What is an APT???

An **advanced persistent threat** (APT) is a stealthy threat actor, which gains unauthorized access to a computer network and remains undetected for an extended period.

Source: https://en.wikipedia.org/wiki/Advanced_persistent_threat

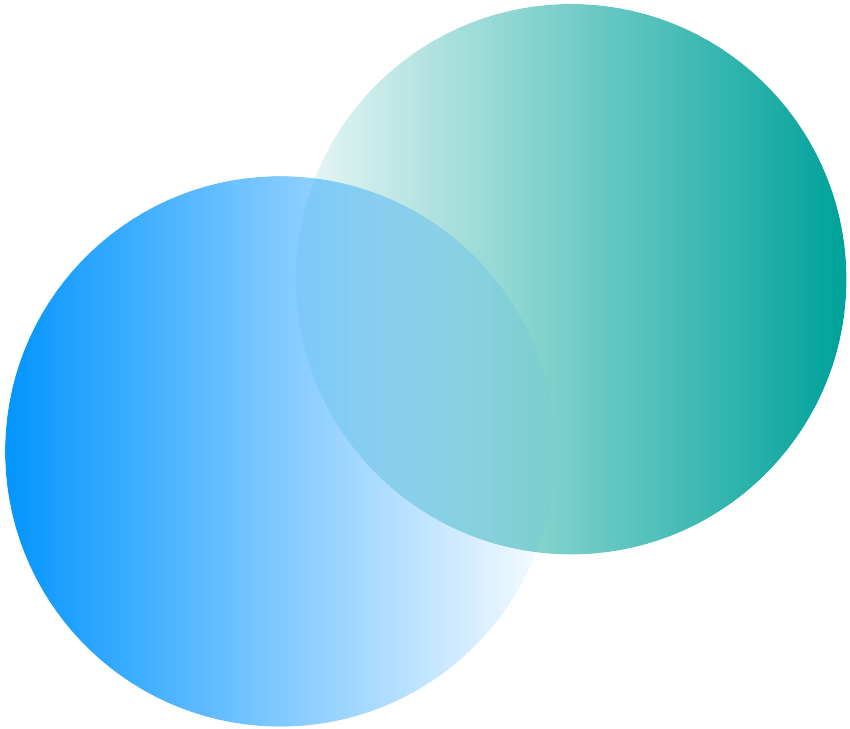
01. Whoami



Whoami

- Alexander Sturz
- Penetration Tester / Red Teamer @ Atos/SEC Consult
- Specialized in Active Directory
  - Github - 61106960

02. Live Hacking Overview

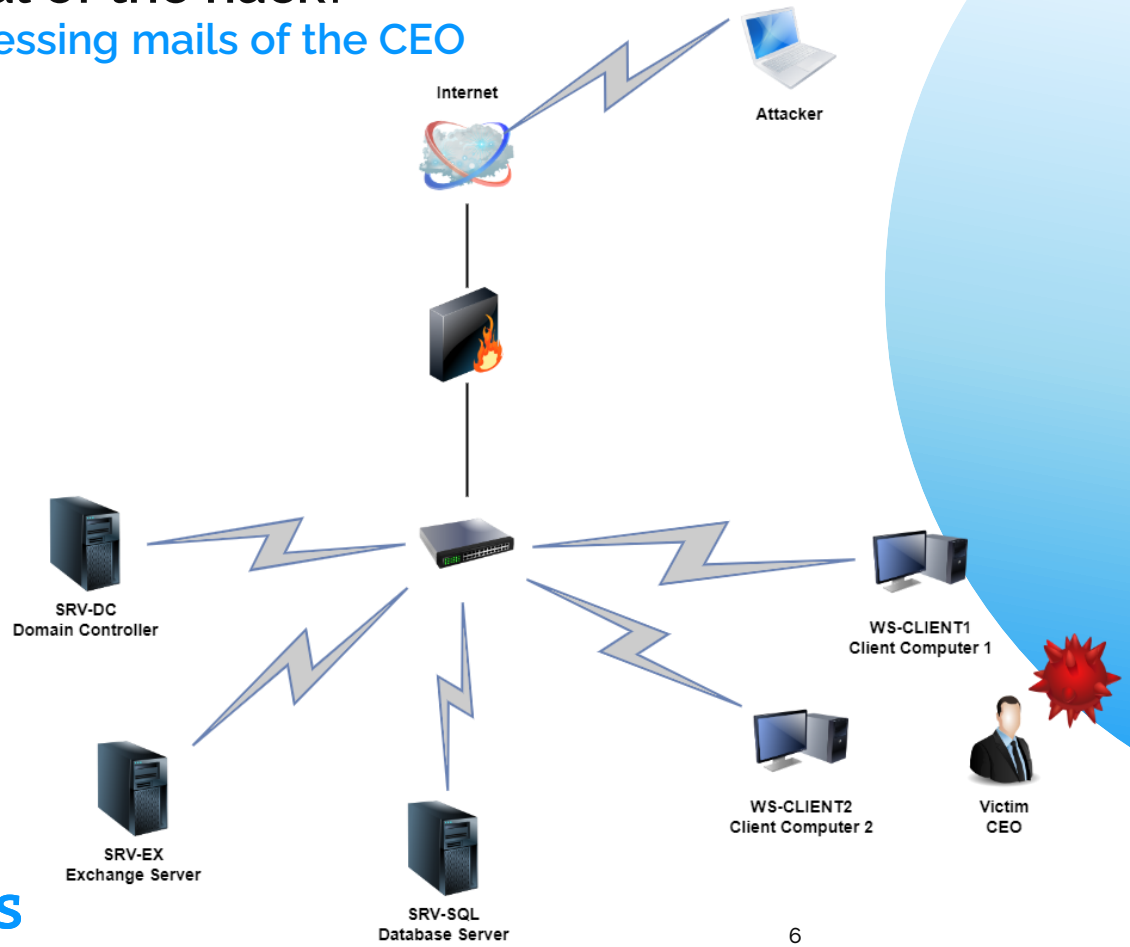


Atos
cryptovision

MINDSHARE 2022

Goal of the hack?

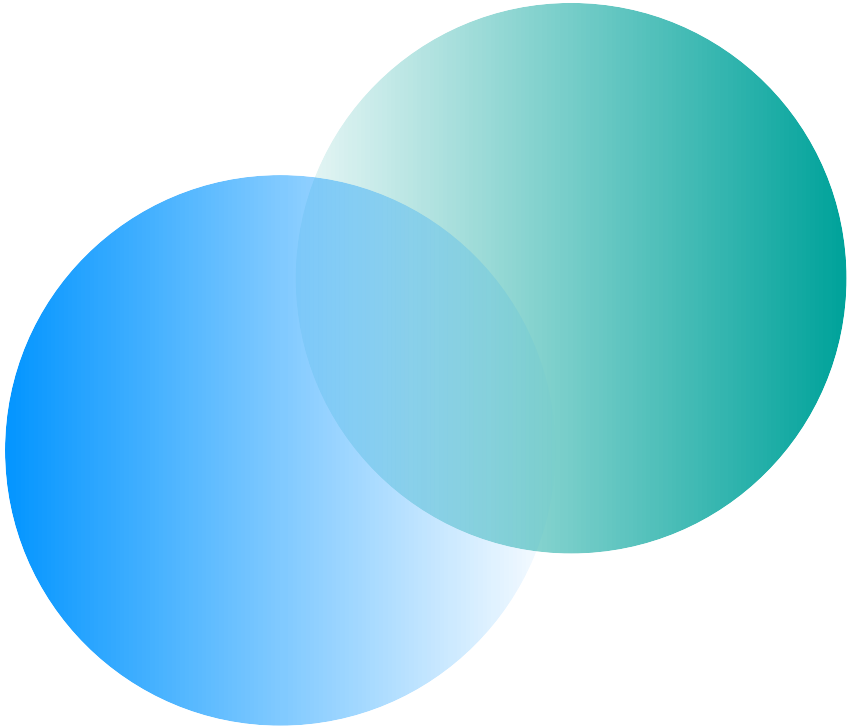
Accessing mails of the CEO



Atos
cryptovision

MINDSHARE 2022

02. Live Hacking Demo



How to do it?
Hacking like an APT

- Stage 1: Infiltration (gain access and establish foothold)
  - Getting foothold on a client computer

- Stage 2: Expansion (deepen access and move laterally)
  - Enumerating Active Directory for jucy information
  - Detecting and attacking SQL Server
  - Doing lateral movement to Exchange Server
  - Elevating privileges in Active Directory

- Stage 3: Extraction (look, learn and exfiltrate data)
  - Placing a backdoor
  - Reading DPAPI protected credentials
  - Accessing mails of the CEO

Questions

DEMO

Thank you!

For more information please contact:
T+ 49 211 399 36014
alexander.sturz@atos.net

Atos
cryptovision

MINDSHARE 2022