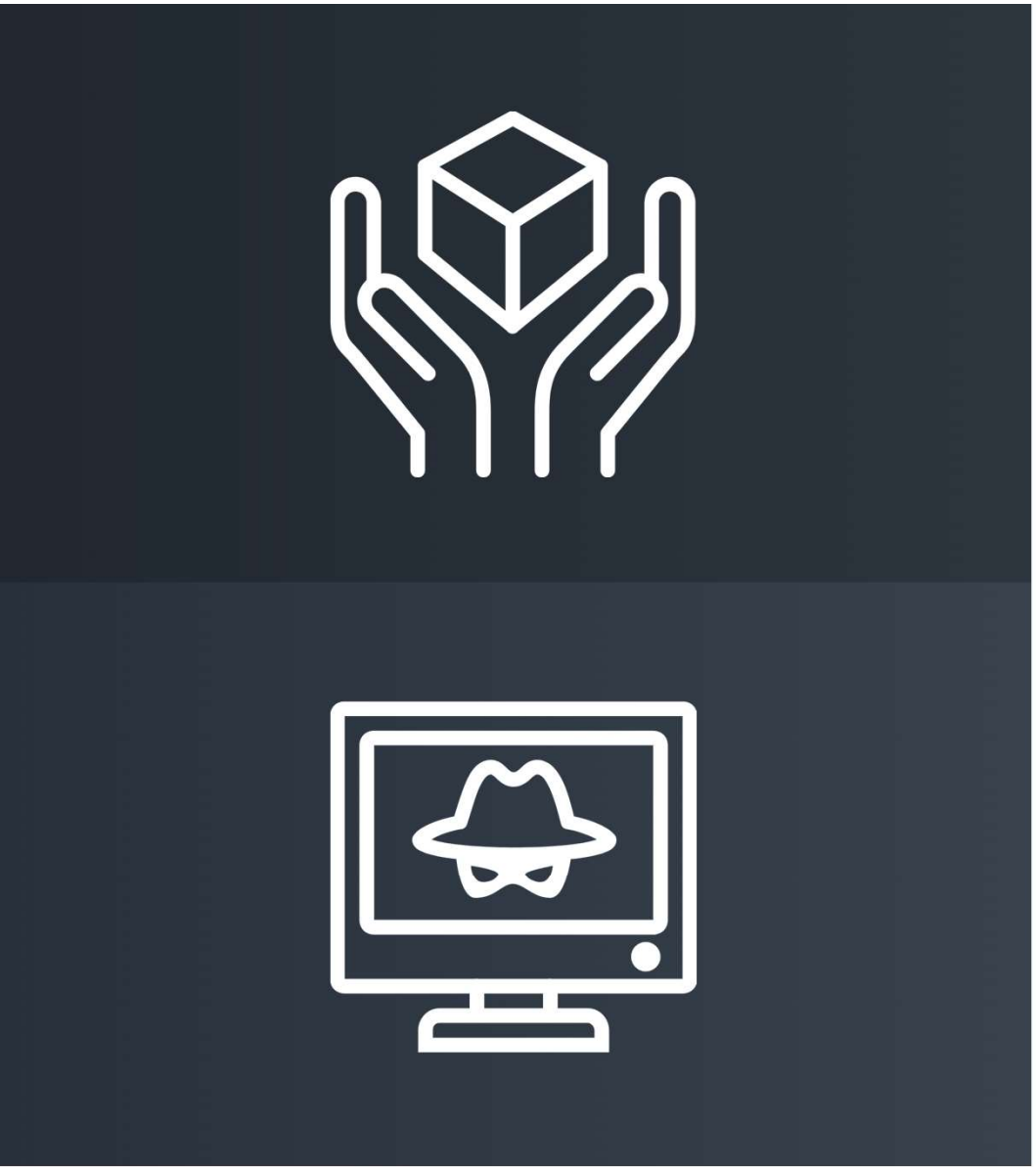
2019-10-06, 15.16.02: SOMEBODY HAS LOGGED IN

Presented by Bård Standal,

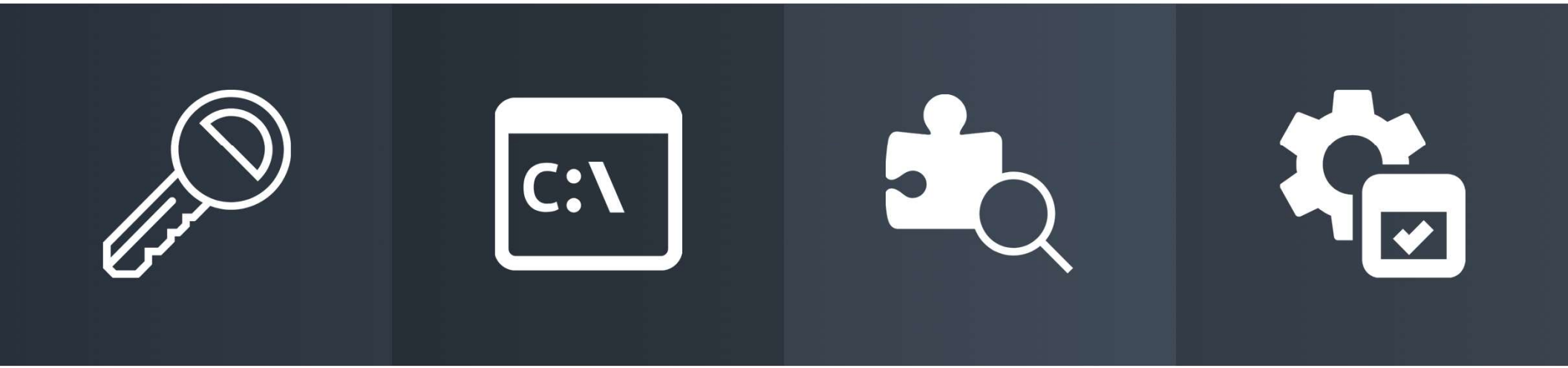


2019-10-06, 15.16.02

At precisely this date and time in 2019, we got hacked. This is the story of how they did it and how we responded.

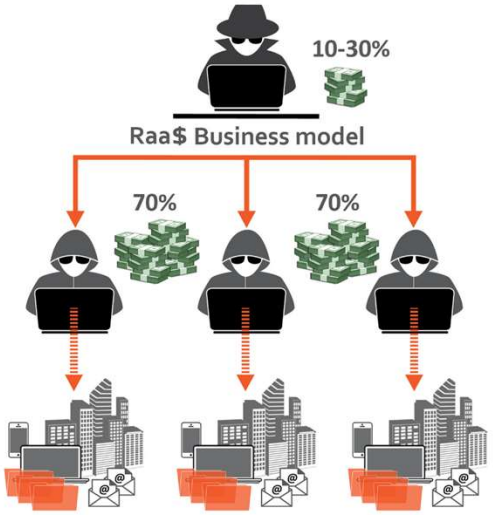
What happened - 15:16:02 - 15:49:00

- Stolen credentials: Keylogger present on non-managed computer
- Full RDP access using stolen credentials
- Poking around: Attacker tests to find weak points
- Landing established: Attacker has global admin access to AD.



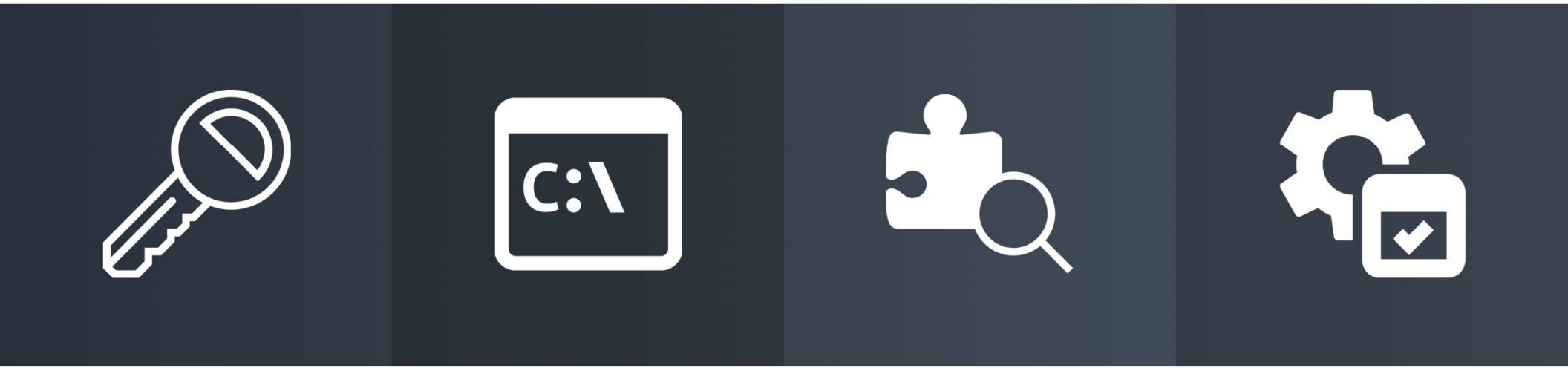
What happened - 15:49:00 - 16:35:00

- What is ransomware as a service (RAA$)?
- What next?



What happened - 16:35:00

- Access sold to multiple attackers
- Multiple simultanious attacks using multiple tools
- Successfull attacker encrypts using PhoneNumber ransomware
- More than 30 servers encrypted



Vulnerabilities

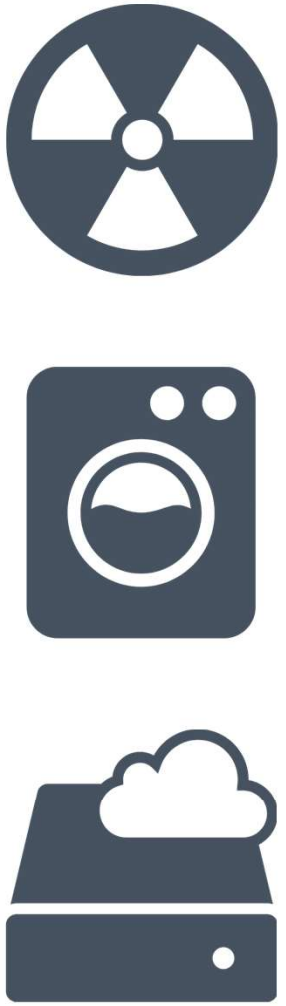
- Remote desktop avalible from the internet
- Out of date software
- Poor operational control
- Insecure centralised logging

Our immidiate actions

- Shut everything down
- Forensics
- Establish small clean platform (Azure AD)
- OODA

Rebuild

- New clean cloud platform
- Factory deployment of windows 10 using all employees
- Recover dirty, clean and redeploy



Reflections

- Too small for proper security
- General crisis management
- Don't underestimate the cleaning process & don't lose focus
- Get the right kind of help

Do you want to know more?

+47 415 21 490

bard.standal@gmail.com

bstandal

Bård Standal
Skibladnir AS