Is the threat real?

Mattias Borg

IT Security Specialist, SBAB Tech

Certified Ethical Hacker

@mattiasborg82

Stefan Schörling

Microsoft MVP

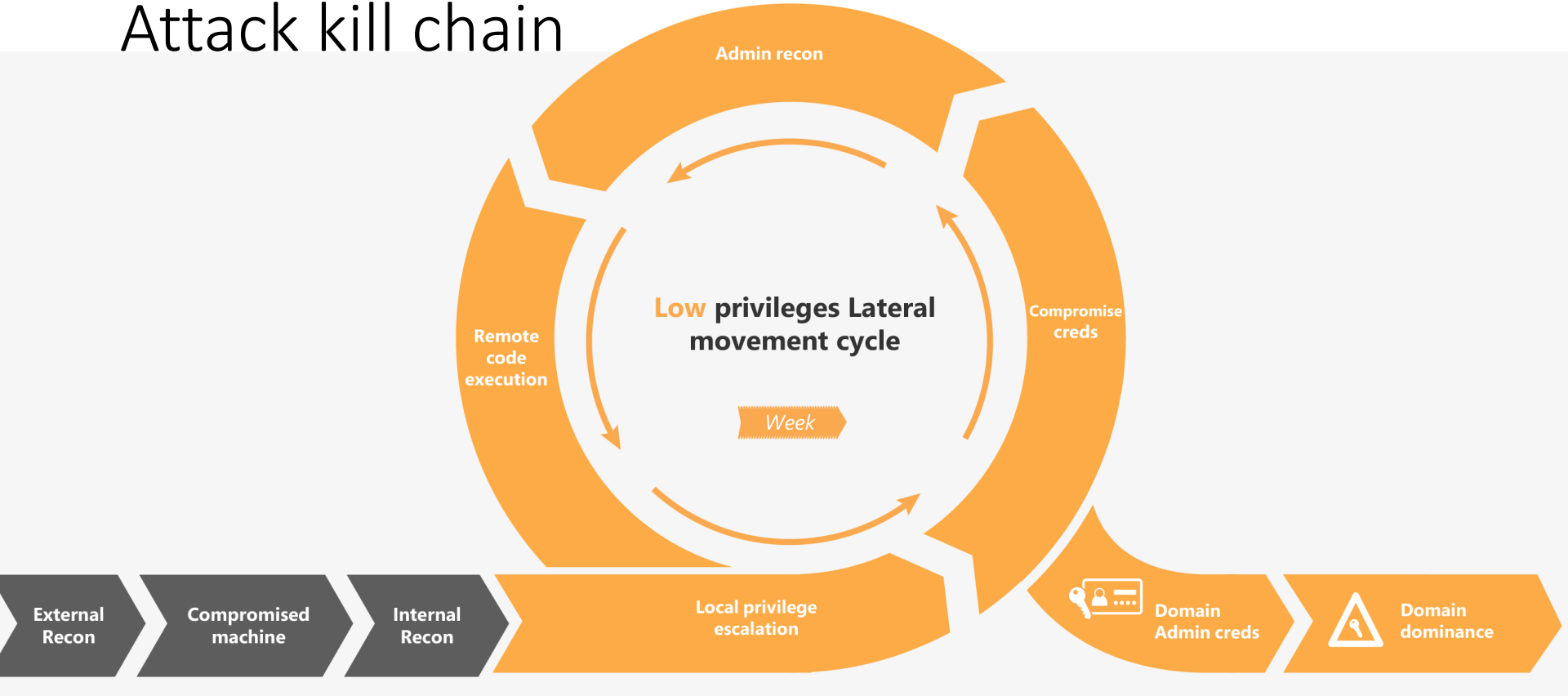
@stefanschorling

Agenda

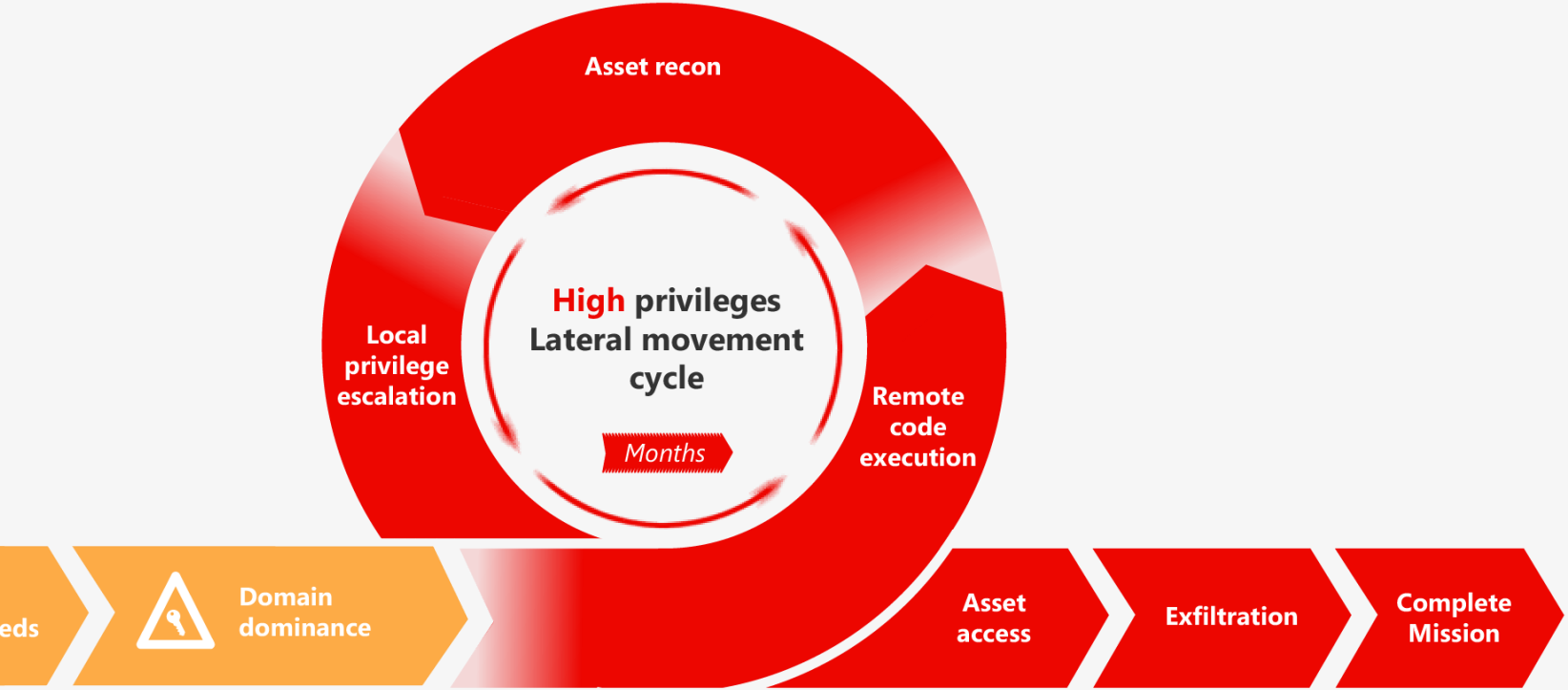
- Anatomy of Attack
- Real Scenario and Demo Hack
  - Focus on Golden Tickets – Not new, but still available

Information is Beautiful

Attack kill chain



Attack kill chain



Tools and methods from the past

When did you last change the PWD of KRBTGT?

- Getting the KRBTGT hash from NTDS.dit
  - ntdsutil “ac i ntds” “ifm” “create full c:\temp” q q
  - Powershell - Invoke-NinjaCopy and many more...

- Use established shell to generate a Golden Ticket - Full Domain controll
  - No elevation required when we have the hash
  - Works until someone changes the krbtgt password ;) which will never happen

Attacking service accounts

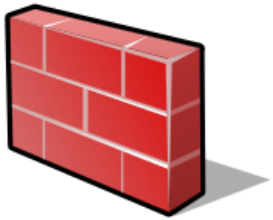
Get a ticket without visit the service
Export the ticket using mimikatz (doesn’t require elevation)
Use kerberoast to crack the password which will be the service account password

You have until the password for the service account is changed

If the system account is used instead the account password is 128 characters and won’t be cracked (more or less)

Scenario and demo

Hacker



User

Microsoft Advanced Threat Analytics

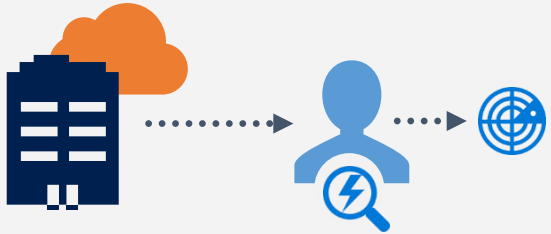
An on-premises platform to identify advanced security attacks and insider threats ***before*** they cause damage

Behavioral Analytics

Detection of advanced attacks and security risks

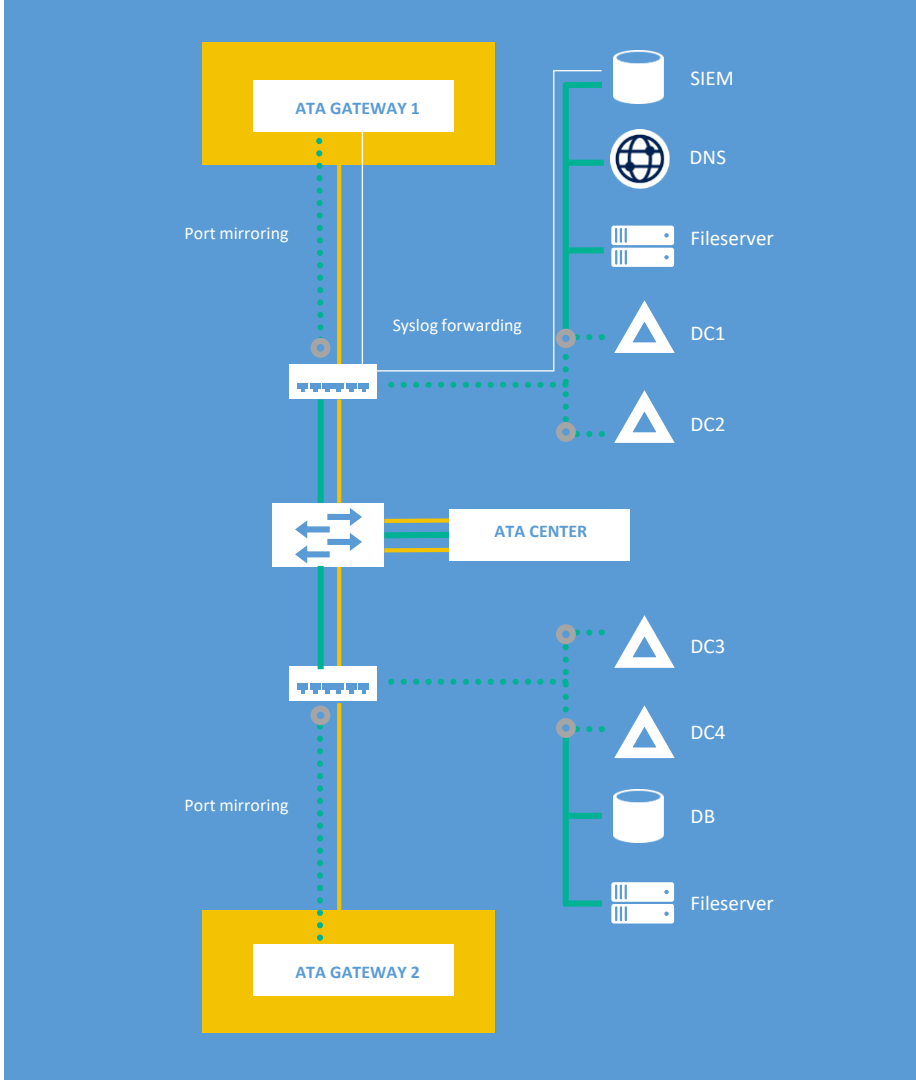
Advanced Threat Detection

Microsoft Advanced Threat Analytics brings the behavioral analytics concept to IT and the organization's users.



Topology - Gateway

- Captures and analyzes DC network traffic via port mirroring
- Listens to multiple DCs from a single Gateway
- Receives events from SIEM
- Retrieves data about entities from the domain
- Performs resolution of network entities
- Transfers relevant data to the ATA Center



What do we do?

- Reset the KRBTGT account Password – twice
  - And all other passwwords
- Rebuild the domain

Contact

Mattias Borg

 @mattiasborg82

Stefan Schörling

 @stefanschorling