RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **TECH-M02**

Securing Entry Points and Active Directory to Prevent Ransomware Attacks

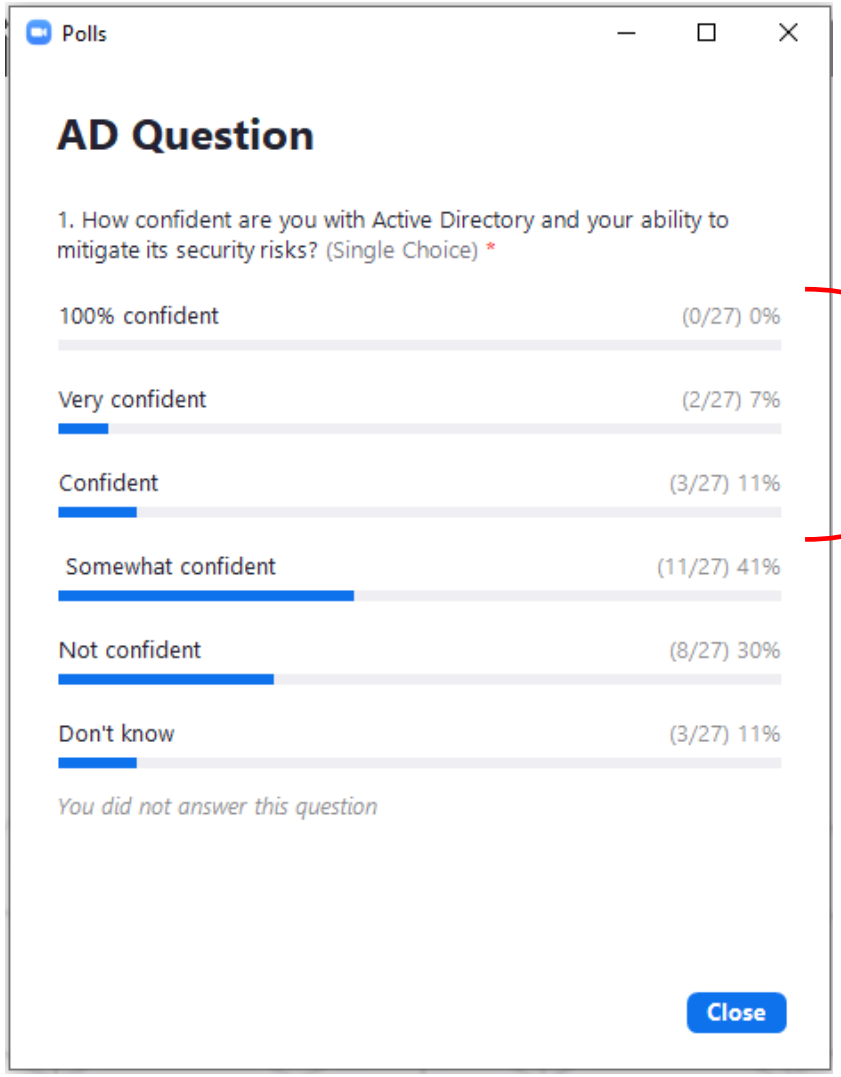
Derek Melber

Chief Technology and Security Strategist
Tenable
@derekmelber

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.


Polls
AD Question
1. How confident are you with Active Directory and your ability to mitigate its security risks? (Single Choice) *
100% confident (0/27) 0%
Very confident (2/27) 7%
Confident (3/27) 11%
Somewhat confident (11/27) 41%
Not confident (8/27) 30%
Don't know (3/27) 11%
You did not answer this question
Close

18%

Attackers Know AD is not Secure

FireEye Analysis of SolarWinds Attack Code

"The backdoor also determines if the system is joined to an Active Directory (AD) domain and, if so, retrieves the domain name. Execution ceases if the system is not joined to an AD domain."

Attackers Know AD is not Secure

FireEye Analysis of SolarWinds Attack Code

"The backdoor also determines if the system is joined to an Active Directory (AD) domain and, if so, retrieves the domain name. **Execution ceases** if the system is not joined to an AD domain."

Attackers Know AD is not Secure

FireEye Analysis of SolarWinds Attack Code

"The backdoor also determines if the system is joined to an Active Directory (AD) domain and, if so, retrieves the domain name. **Execution ceases** if the system is not joined to an AD domain."

MountLocker new variant:

XingLocker

"In essence, the new ransomware will query the compromised computer to see if it is joined to an Active Directory domain. If the computer is not joined to AD, the ransomware will fail and move to another device to perform the same query."

Attackers Know AD is not Secure

FireEye Analysis of SolarWinds Attack Code

"The backdoor also determines if the system is joined to an Active Directory (AD) domain and, if so, retrieves the domain name. **Execution ceases** if the system is not joined to an AD domain."

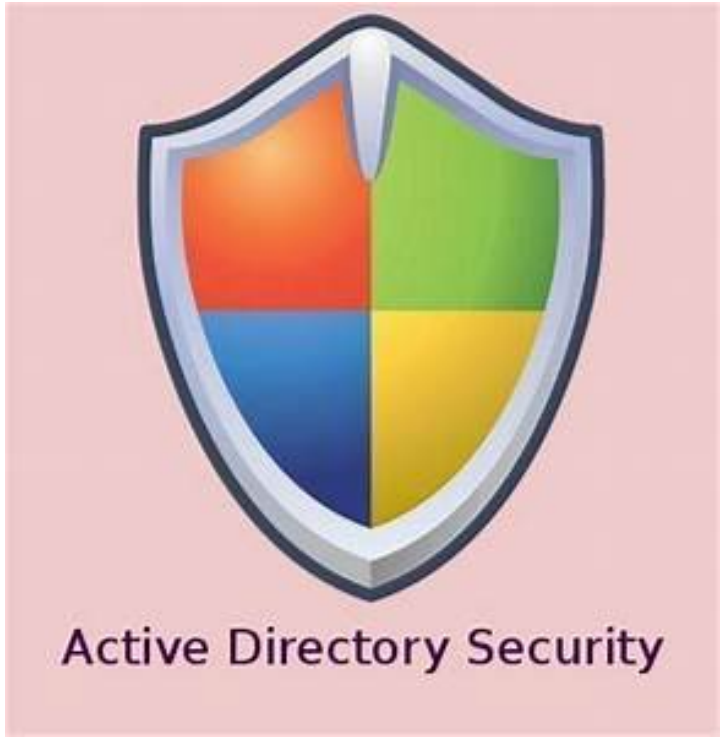
MountLocker new variant:

XingLocker

"In essence, the new ransomware will query the compromised computer to see if it is joined to an Active Directory domain. If the computer is not joined to AD, the **ransomware will fail** and move to another device to perform the same query."

Goals for Today

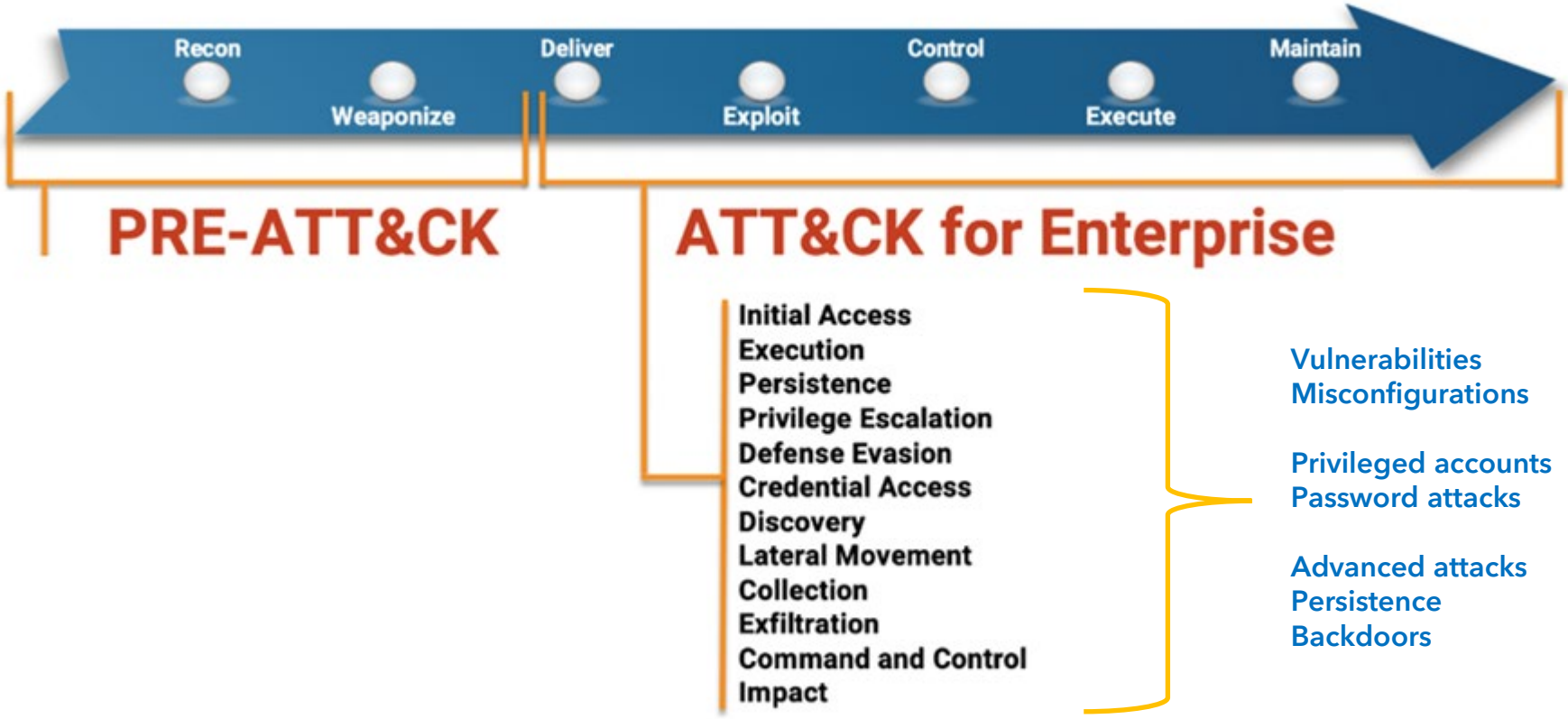
- Attacker Tactics
- Makeup of an Attack
- Steps to Secure Active Directory



RSAConference2022

Attacker Tactics

Attacker Tactics



RSAConference2022

Makeup of an Attack

1 – Entry Points

Phishing

Vulnerability

Misconfiguration

2 – Post Entry Point Tactics

Lateral Movement

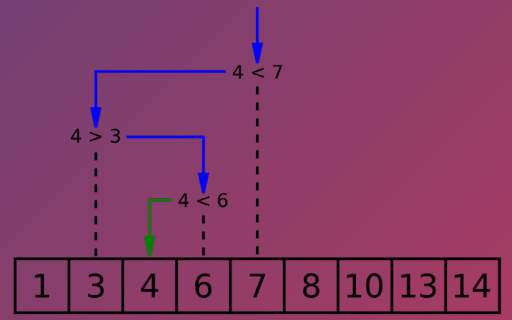
Obtain Local Privileges

Privilege Escalation

3 - Active Directory Attack Tactics

Enumeration of AD and all settings

Analysis of AD to find easiest target



Evading log analysis

RSAConference2022

Steps to Secure Active Directory

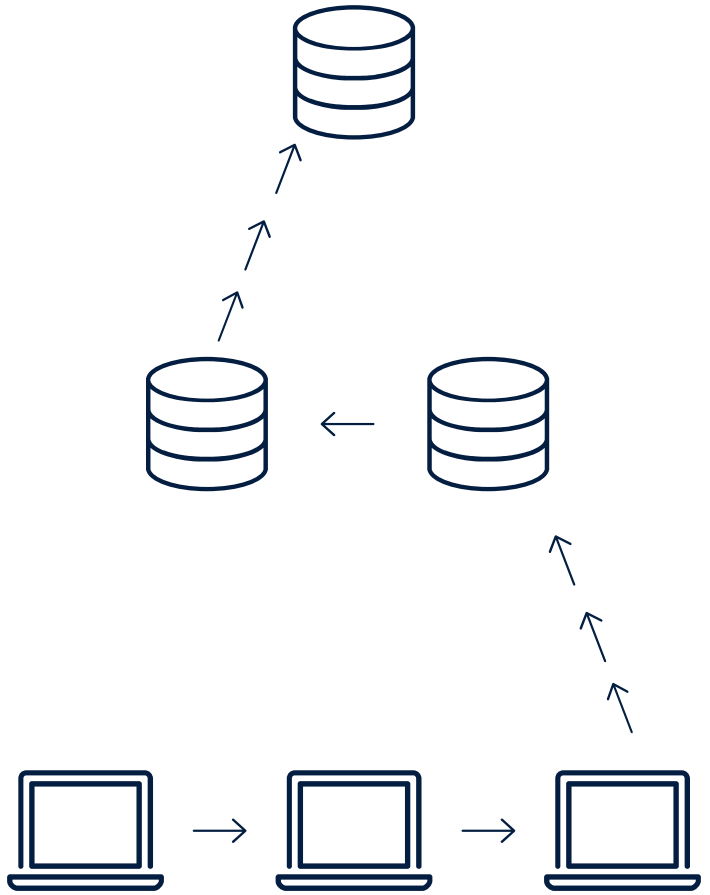
SECURE YOUR ACTIVE DIRECTORY AND DISRUPT ATTACK PATHS

MITIGATE EXISTING THREATS

MAINTAIN HARDENED SECURITY

DETECT ADVANCED ATTACKS IN REAL TIME

Lateral Movement



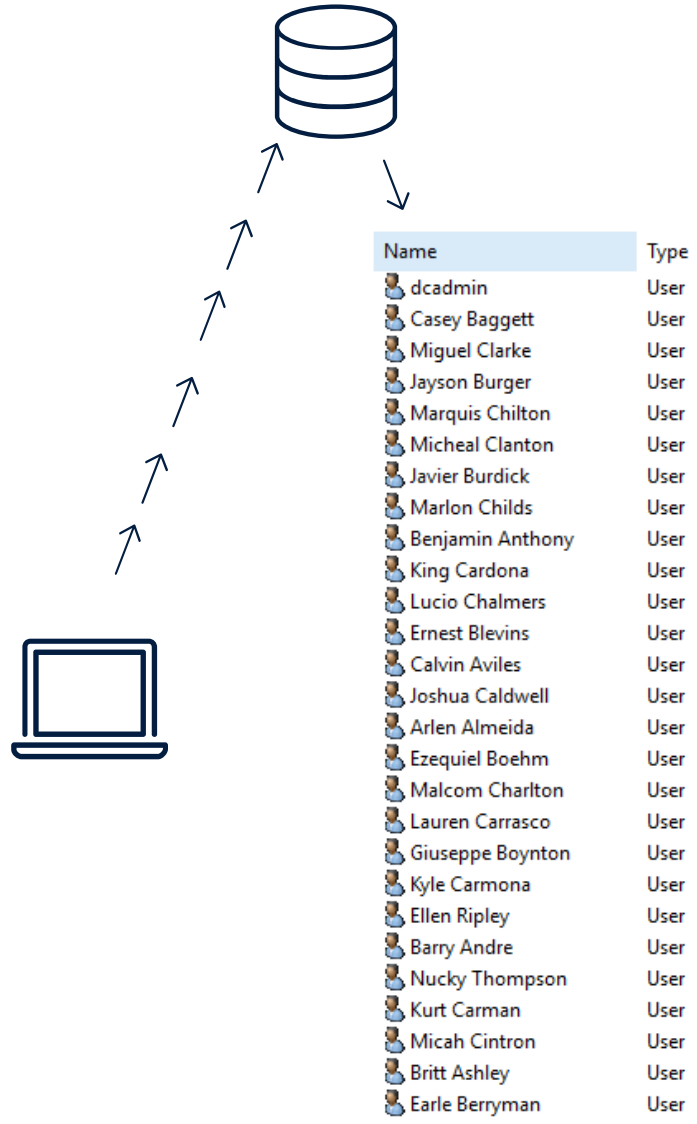
What Attackers Do

- Mine cached credentials
- Attack passwords
- Determine if mined credentials have privileges

How to Protect and Deny

- Use LAPS
- Don't reuse passwords
- Don't use common passwords
- Strong password policy
- Implement MFA

Enumeration – Obtain Privileged Accounts



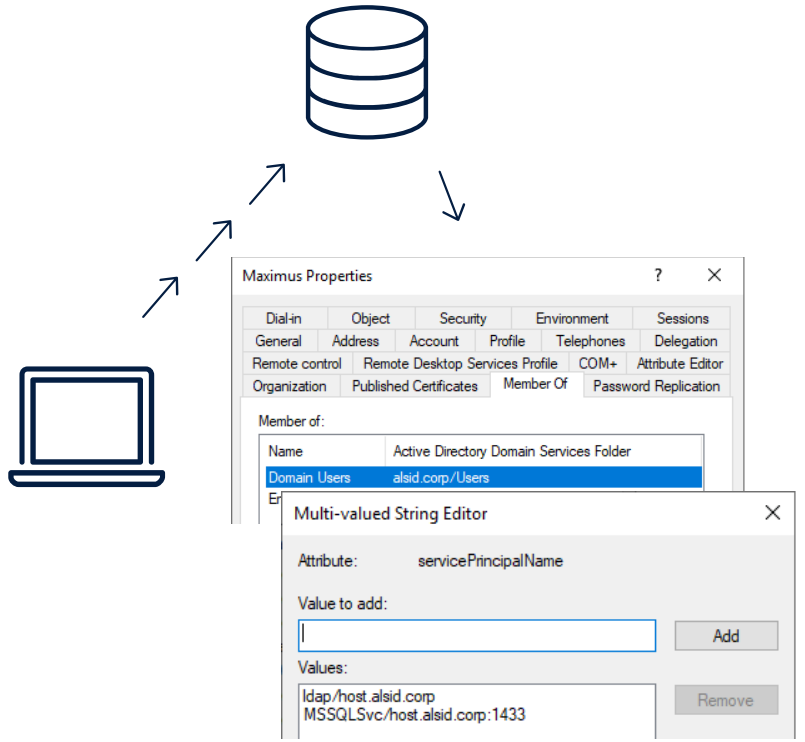
What Attackers Do

- Enumerate AD (read-only)
- Analyze ACLs, group members, user rights, etc.
- Compare mined credentials

How to Protect and Deny

- Secure privileged users
- Secure service accounts
- Secure computers
- Clean up old settings

Enumeration – Attack Accounts



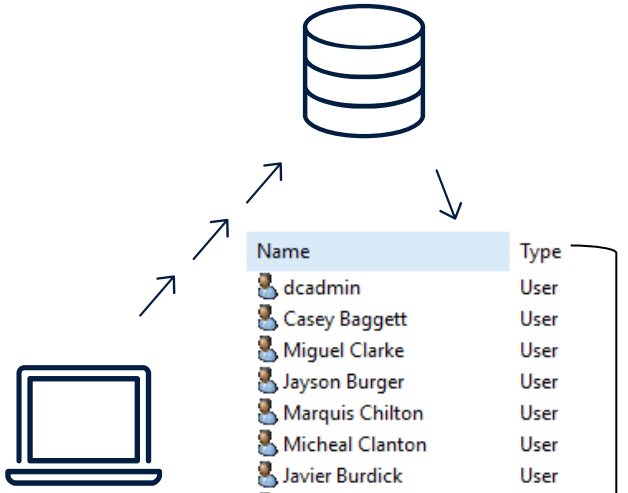
What Attackers Do

- Enumerate AD (read-only)
- Discover users and computers with misconfigurations
- Exploit users and computers

How to Protect and Deny

- No users with SPN have privileges
- No users with delegations have privileges
- No computers with weak Kerberos delegations

Attack AD Users and Their Passwords



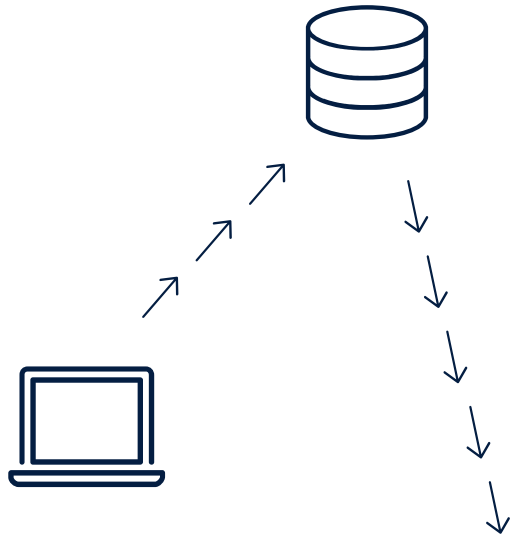
What Attackers Do

- Password spraying
- Password brute force

How to Protect and Deny

- Strong password policy
- Detect password spraying
- Detect brute force

Advanced Attacks – Persistence and Backdoors



What Attackers Do

- DCSync
- DCShadow
- Golden Ticket
- Process Injection

```
C:\Users\victim1\Desktop\mimikatz\x64>mimikatz.exe

  .#####.   mimikatz 2.1.1 (x64) built on May 27 2018 02:37:50 - lil!
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # lsadump::dcsync /domain:hackable.com /user:victim1
[DC] 'hackable.com' will be the domain
[DC] 'WIN-BCO3IIB083E.hackable.com' will be the DC server
[DC] 'victim1' will be the user account

Object RDN           : victim1

** SAM ACCOUNT **
```

How to Protect and Deny

- DCSync detect
- DCShadow detect
- Golden Ticket detect
- LSASS detect
- SIDHistory modification
- Primary Group ID modification

Apply What You Have Learned Today

- When you get back to work you should:
  - Verify exploitable configurations are secured
- Ensure that you get alerts to any new exploitable configurations:
  - Real time automatic analysis is required
  - Alert both SOC and IT
- Attack detection is essential:
  - Basic attacks: password related
  - Advanced attacks: DCSync and DCShadow
  - Vulnerability attacks: ZeroLogon and SAMAccountName

RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

Thank you!

SESSION ID: **TECH-M02**

Securing Entry Points and Active Directory to Prevent Ransomware Attacks

Derek Melber

dmelber@tenable.com
@derekmelber