ICT POWER.IT

Microsoft

#POWERCON2022

Blue Team Experience: Detection and Mitigation

Domenico Caldarelli
Ethical Hacker
domenico.caldarelli@itisistemi.it

Speaker

Domenico Caldarelli
Head of Cyber Security, ITI srl

- Ethical Hacker
- Systems Engineer
- ICTPower

Agenda

- Mimikatz – Prevenzione
- Attacchi verso AD: Come rilevarli

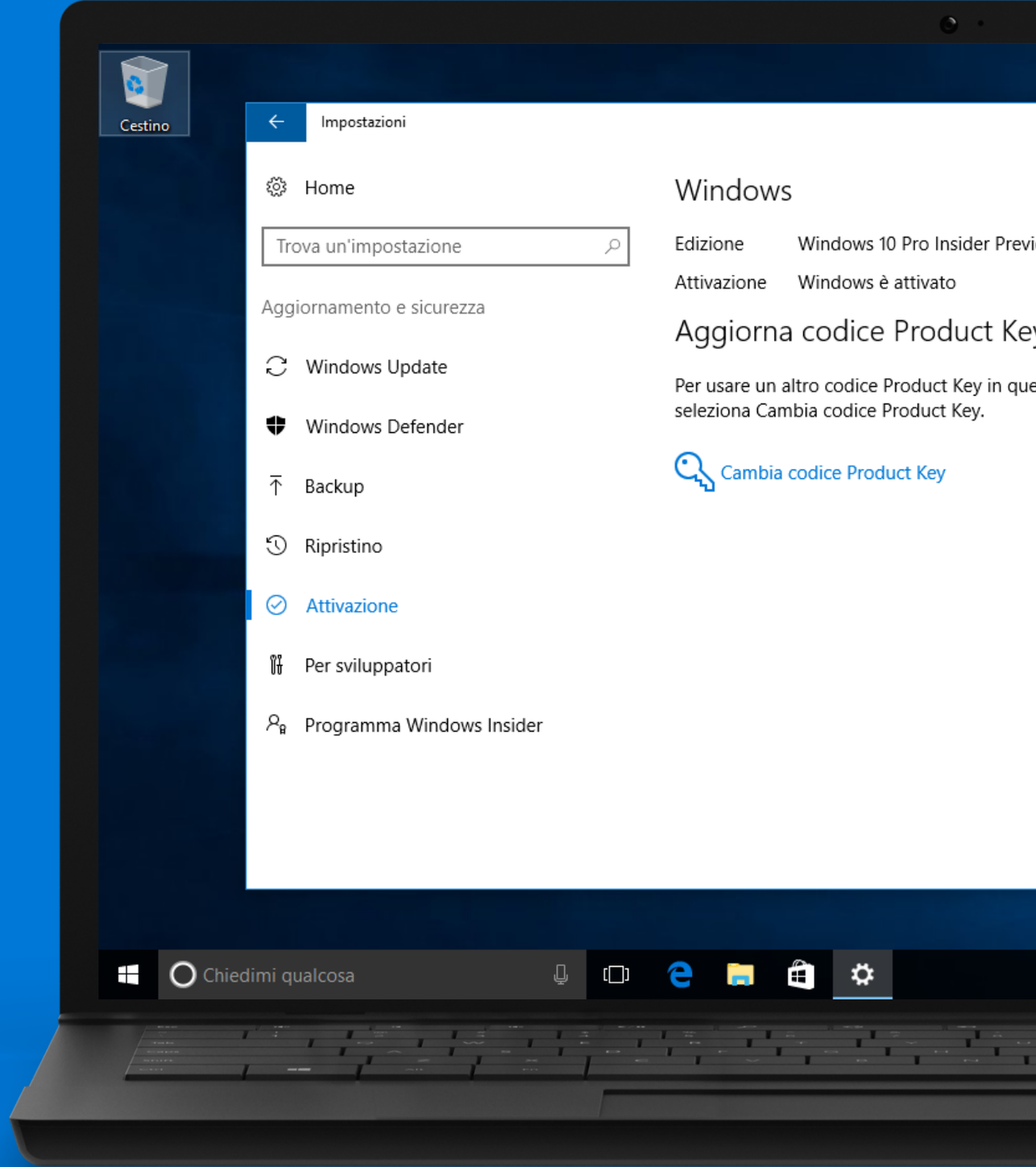
Mimikatz - Prevenzione

- Debug Privilege
- WDigest
- LSA Protection
- Restricted Admin Mode
- Credential Caching
- Protected Users Group

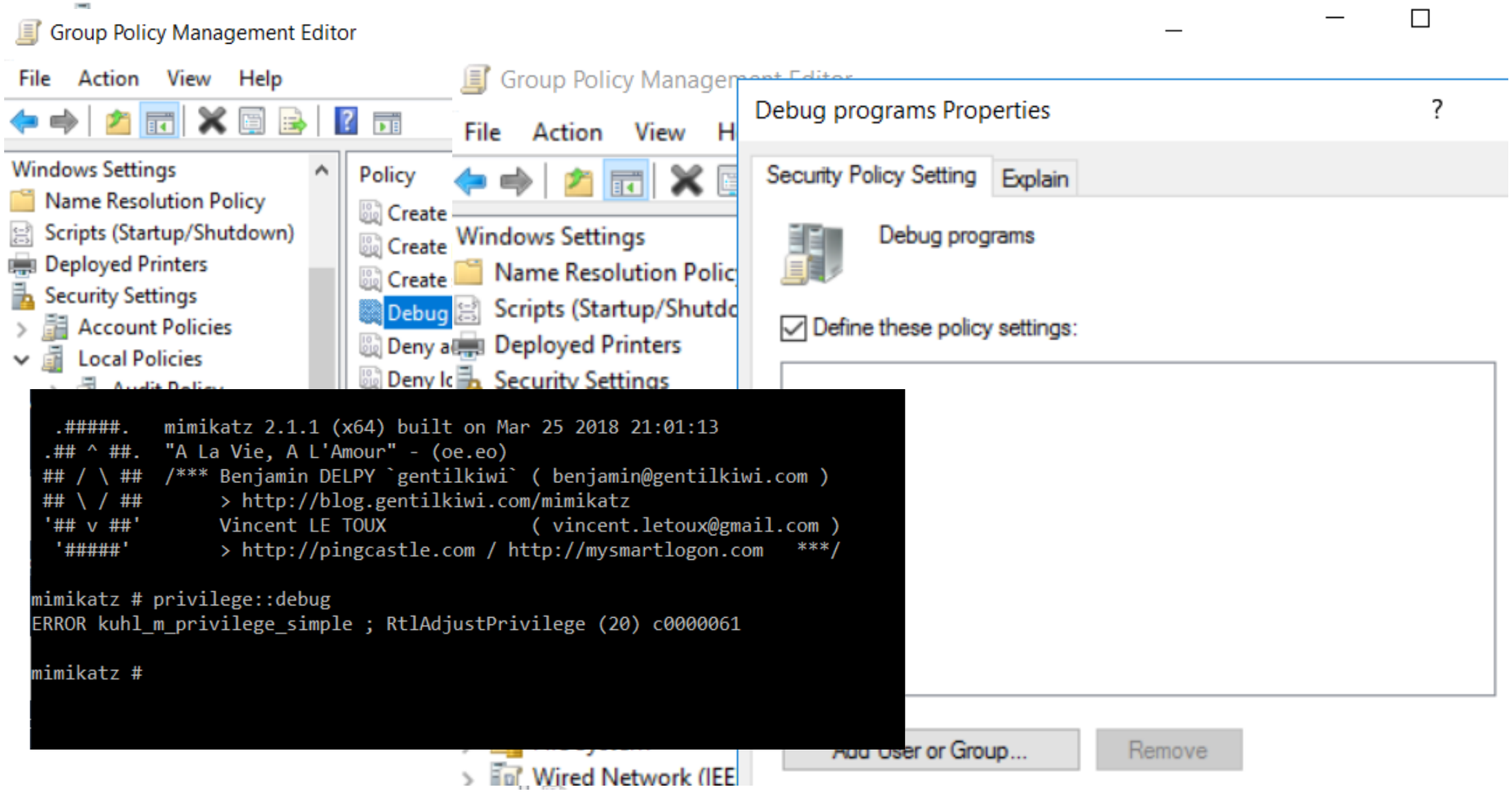
Attacchi ad AD e come rilevarli

- Skeleton Key
- DSRM – Directory Services Restore Mode
- Malicious SSP (Security Support Provider)
- Kerberoast
- Delegation
- DCShadow

Prevenzione



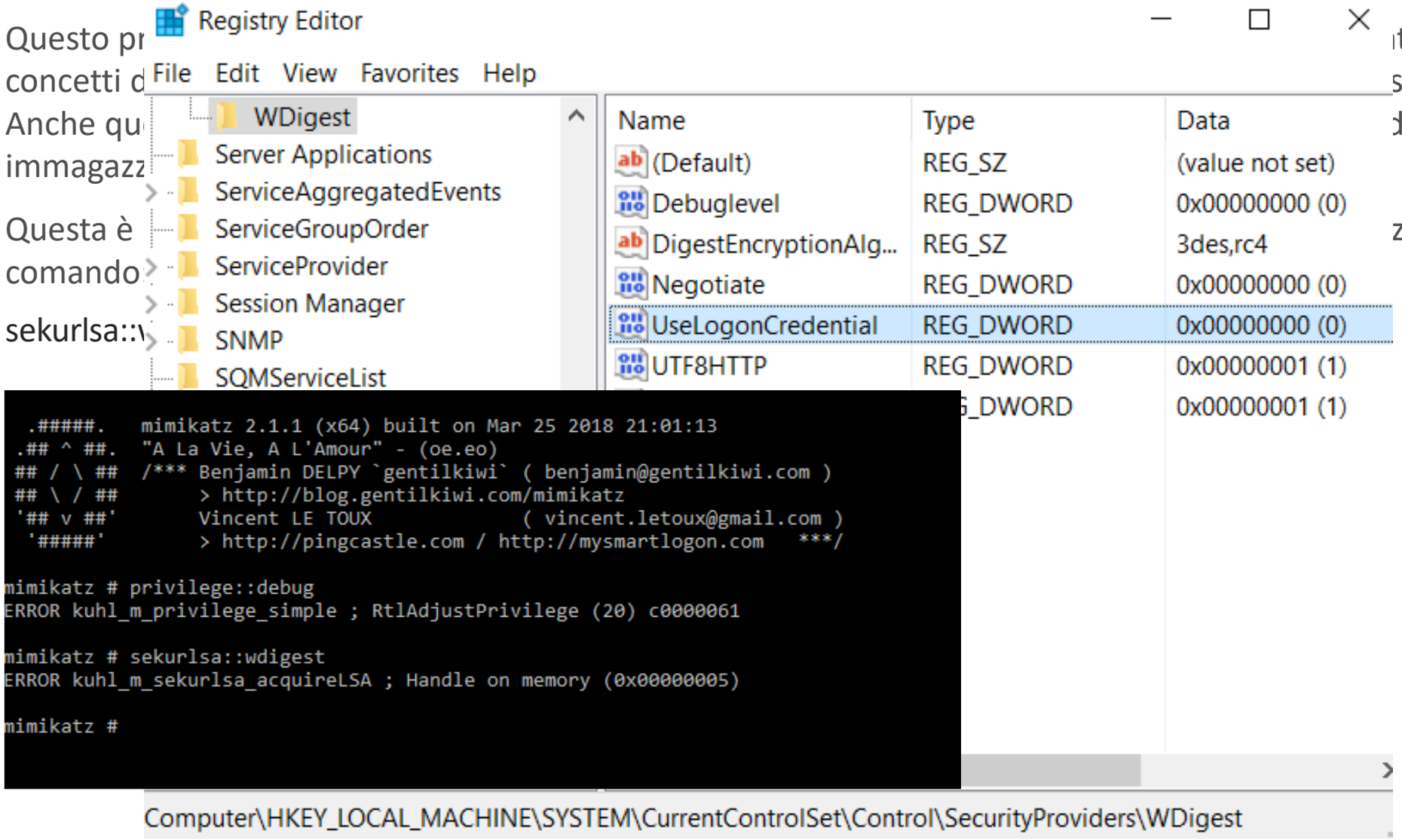
Debug Privilege



WDigest

Questo pr ... ta pensata per unire
concetti d ... sata su scambio di chiavi.
Anche qu ... d relative agli utenti
immagazz

Questa è ... zzando il seguente
comando
sekurlsa::w



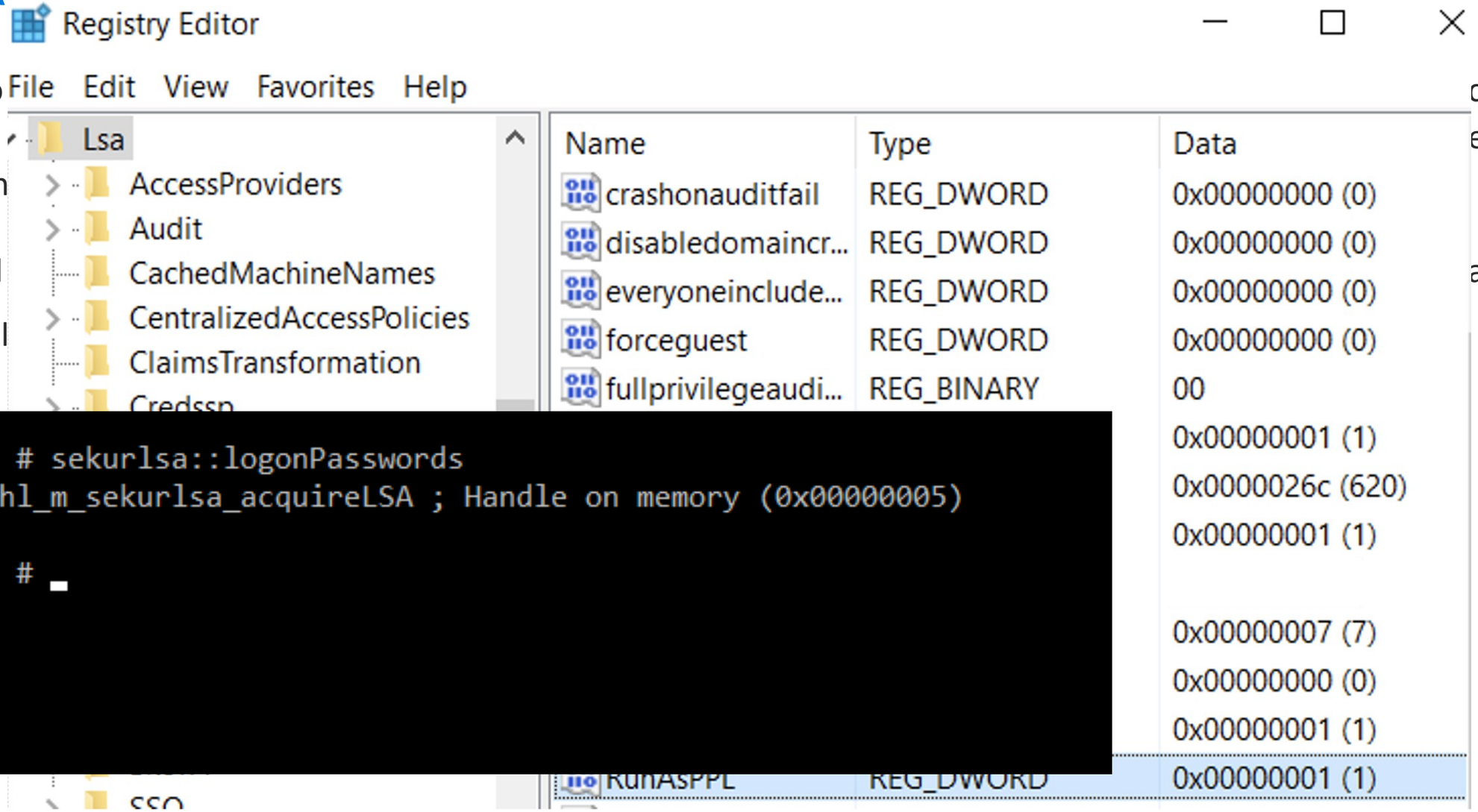
KB2871997

LSA Protection

Il servizio ... ca i criteri di sicurezza ... e ai processi non atten...

Usando il ... a LSA

sekurlsa::l...




```
mimikatz # sekurlsa::logonPasswords
ERROR kuhl_m_sekurlsa_acquireLSA ; Handle on memory (0x00000005)

mimikatz # _
```

Restrict delegation of credentials to remote servers

Restrict delegation of credentials to remote servers

Previous Setting | Next Setting

Registry

randosi

Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: mstsc /restrictedadmin

This task will be created with administrative privileges.

OK | Cancel | Browse...

Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>mstsc /restrictedadmin
```

ting all requests back to the client device.

pating apps:
Remote Desktop Client

If you enable this policy setting, Restricted Administration mode or Remote Credential Guard is enforced and participating apps will not delegate credentials to remote devices.

)000000 (0

)000000 (0

)000000 (0

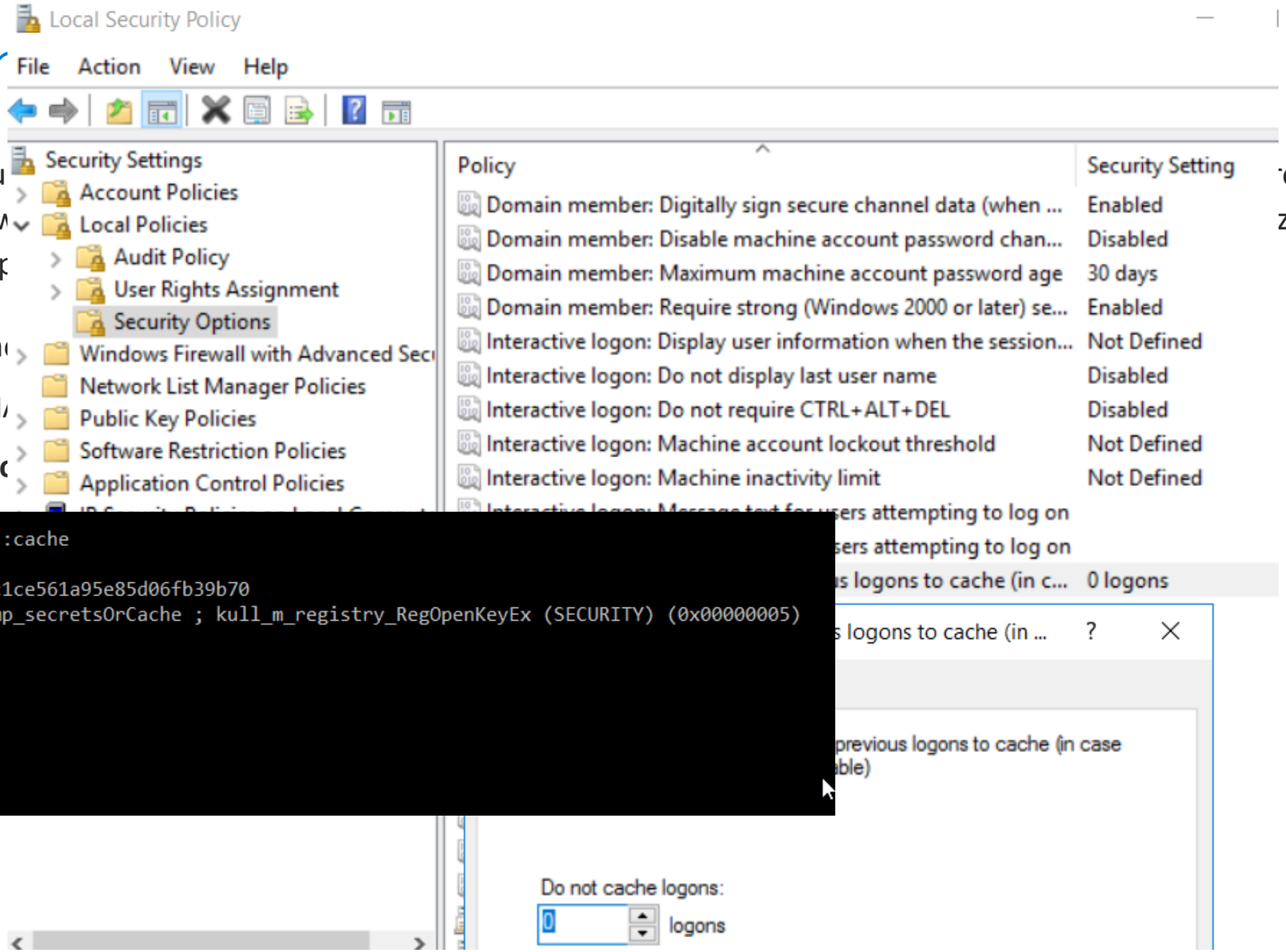
Creder

Nel caso in cui u ollerà gli ultimi hash delle passw zare gli hash delle ultime 10 p

Questi hash son

HKEY_LOCAL_M

Configurare la **Lo**




```
mimikatz # lsadump::cache
Domain : DC
SysKey : 2904f4be8c1ce561a95e85d06fb39b70
ERROR kuhl_m_lsadump_secretsOrCache ; kull_m_registry_RegOpenKeyEx (SECURITY) (0x00000005)

mimikatz #
```

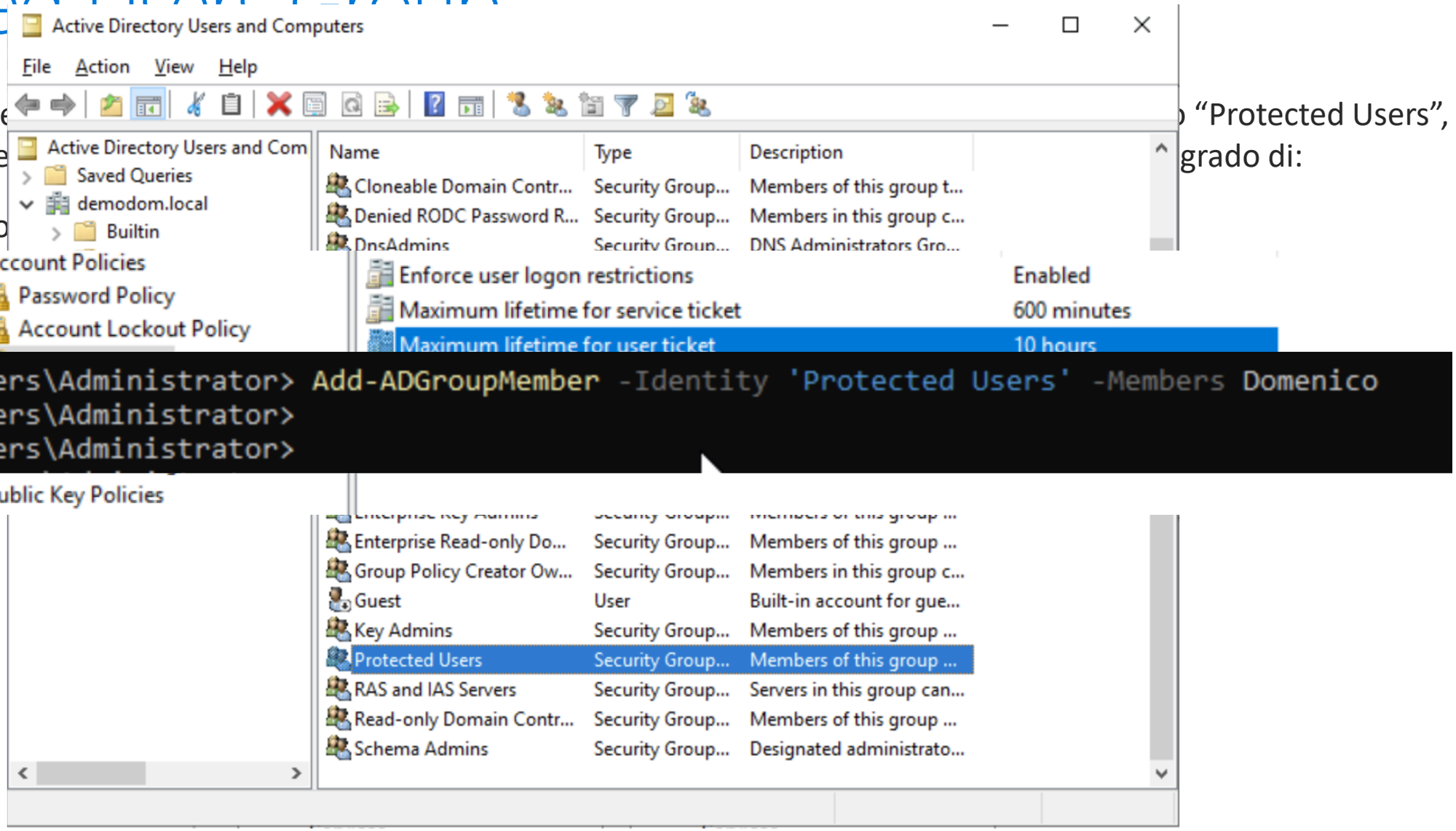
Protected Users Group

Con Windows Serve ... o “Protected Users”, i cui membri che ese ... grado di:

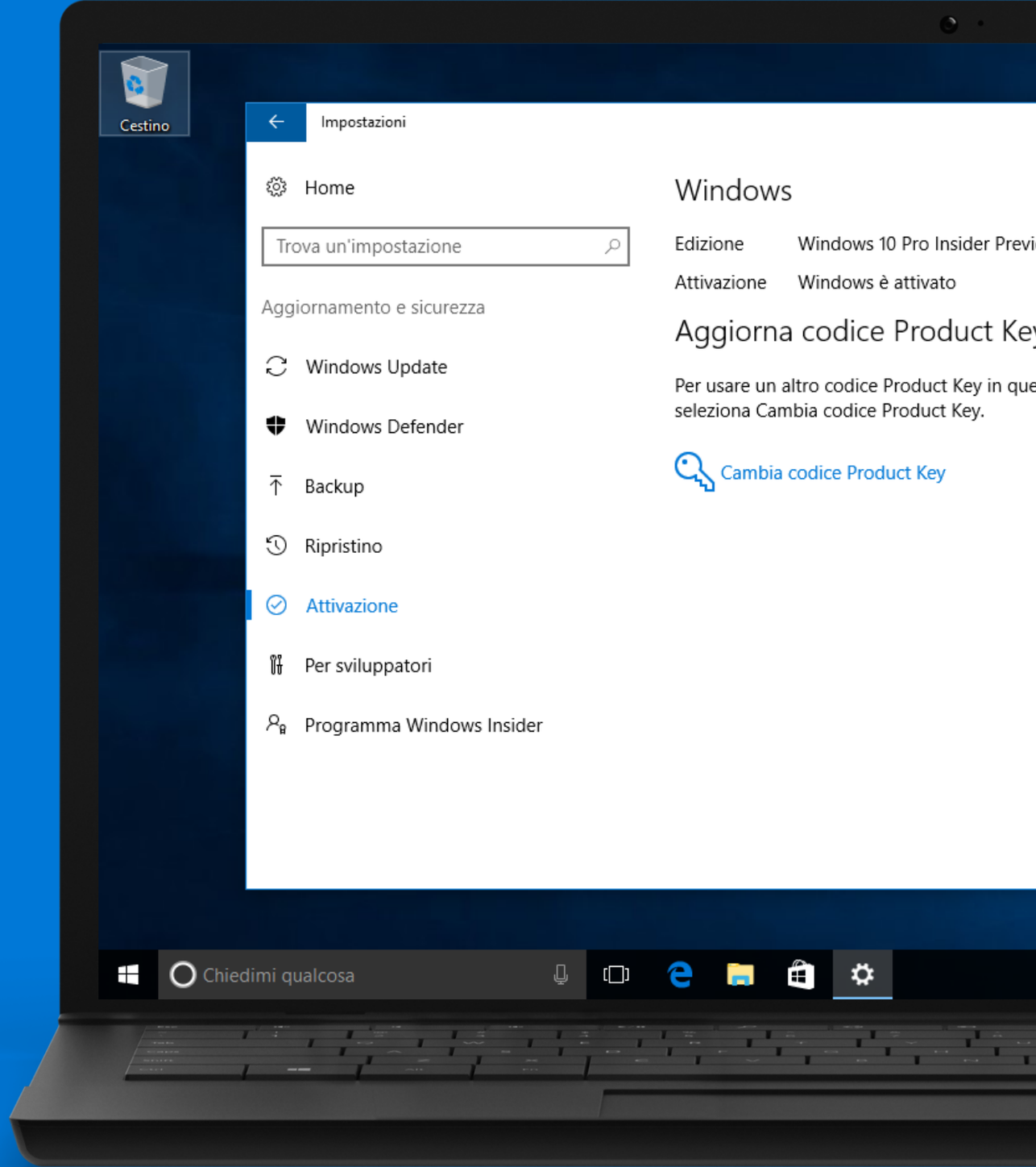
- Autenticarsi co
- Utilizza
- Essere
- Rin

Unconst

Constrained



Monitoraggio

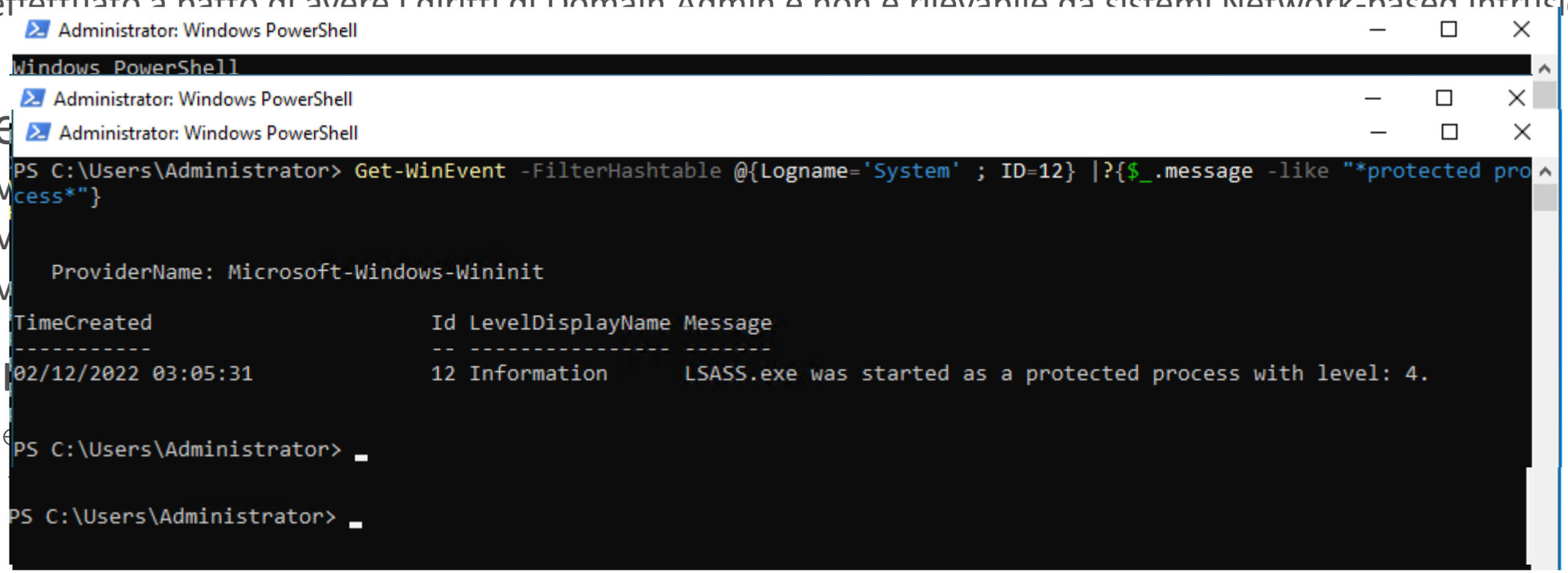


Skeleton Key

Questo attacco è caratterizzato dall'utilizzo di un malware (Mimikatz, PowerShell Empire, ecc…) caricato in memoria che consente ad un attaccante di autenticarsi come un qualsiasi utente di dominio utilizzando una sorta di master password.

Può essere effettuato a patto di avere i diritti di Domain Admin e non è rilevabile da sistemi Network-based Intrusion Detection o IPS/IDS.

- Eve
  - Ev
  - Ev
  - Ev
- Co
  - Ge
    ?



- Mitigazioni
  - Eseguire il processo LSASS come processo protetto
  - `New-ItemProperty HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\ -Name RunAsPPL -Value 1 -Verbose`

```
PS C:\Users\Administrator> Get-WinEvent -FilterHashtable @{Logname='Security' ; ID=4657}


   ProviderName: Microsoft-Windows-Security-Auditing

TimeCreated                      Id LevelDisplayName Message
-----------                      -- --------------- -------
02/12/2022 12:15:28            4657 Information      A registry value was modified....
02/12/2022 12:15:27            4657 Information      A registry value was modified....
02/12/2022 12:15:21            4657 Information      A registry value was modified....
02/12/2022 12:15:21            4657 Information      A registry value was modified....
```

er denominato account

e raramente viene

```
PS C:\Users\Administrator> Set-ItemProperty "HKLM:\SYSTEM\CURRENTCONTROLSET\CONTROL\LSA" -name DsrmAdminLogonBehavior -value 1 -Verbose
VERBOSE: Performing the operation "Set Property" on target "Item:
HKEY_LOCAL_MACHINE\SYSTEM\CURRENTCONTROLSET\CONTROL\LSA Property: DsrmAdminLogonBehavior".
PS C:\Users\Administrator> Get-ItemProperty "HKLM:\SYSTEM\CURRENTCONTROLSET\CONTROL\LSA" -name DsrmAdminLogonBehavior


DsrmAdminLogonBehavior : 1
PSPath                 : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CURRENTCONTROLSET\CONTROL\LSA
PSParentPath           : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CURRENTCONTROLSET\CONTROL
PSChildName            : LSA
PSDrive                : HKLM
PSProvider             : Microsoft.PowerShell.Core\Registry


PS C:\Users\Administrator>
```

- Eve
  pas
- Mitig
  - Le cr
  - *"HKLM\System\CurrentControlSet\Control\Lsa\L*
    esistere o deve avere come valore «1»

Privilege Use
System
Global Object Access Auditing

Process ID: 0x12ec
Process Name: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Change Information:
Old Value Type: REG_DWORD
Old Value: 1
New Value Type: REG_DWORD
New Value: 2

Malicious SSP – Security Support Provider

L'interfaccia SSPI (Security Support Provider Interface) consente di estendere facilmente i metodi di autenticazione di Windows consentendo l'aggiunta di nuovi Security Support Providers.

In questo caso, se un attaccante riesce ad avere i privilegi di Domain Admin può utilizzare questa tecnica per creare una persistenza.

- Eventi
  - Event ID 4657: Creazione o modifica della chiave di Registro: *"HKLM:\System\CurrentControlSet\Control\Lsa\SecurityPackages\"*
  - Controllare l'esistenza del file "mimilsa.log" o "kiwissp.log" (solitamente in System32) sui Domain Controller
- Mitigazioni
  - Controllare le chiavi di registro: "HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Security Packages" e "HKLM\SYSTEM\CurrentControlSet\Control\Lsa\OSConfig\Security Packages" se nei loro valori è presente "mimilib" o valori riconducibili a mimikatz.
  - Monitorare l'esecuzione di comandi su cmd.exe e PowerShell.

Kerberoast

Kerberoasting è una tecnica di attacco usata nella fase di post-exploitation per tentare di decifrare la password di un account di servizio all'in del dominio, non necessariamente da un e pacchetti al servizio target.

- Eventi
  - System Event
  - Siccome l'ever ri:
    - Il service na
    - Il service na
    - L'account n dalle macchine")
    - Il Failure co
    - La tipologia
    - Il Ticket Opt
- Mitigazioni
  - Le password degli account di servizio devono essere complesse (maggiori di 25 caratteri).
  - Utilizzare "Managed Service Accounts" (Cambio password degli SPN periodico automatico).

Additional Information:

Ticket Options:	0x40810000
Ticket Encryption Type:	0x17
Failure Code:	0x0
Transited Services:	-

This event is generated every time access is requested to a resource such as a computer or a Windows service. The service name indicates the resource to which access was requested.

This event can be correlated with Windows logon events by comparing the Logon GUID fields in each event. The logon event occurs on the machine that was accessed, which is often a

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	1/23/2017 10:24:15 PM
Event ID:	4769	Task Category:	Kerberos Service Ticket Operation
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	
OpCode:	Info		
More Information:	Event Log Online Help		

```
Get-WinEvent -FilterHashtable @{Logname=Security;ID=4769} -MaxEvents 1000 |
?{$_.Message.split("`n")[8] -ne 'krbtgt' -and
$_.Message.split("`n")[8] -ne '*$' -and
$_.Message.split("`n")[3] -notlike '*$@*' -and $_.Message.split("`n")[18] -
like '*0x0*' -and $_.Message.split("`n")[17] -like "*0x17*"} | select -
ExpandPropertymessage
```

Delegation

Unconstrained Delegation (delega svincolata): il domain controller inserisce una copia del TGT dell'utente nel service ticket. Quando il service ticket dell'utente (TGS) viene mandato al server per l'utilizzo del servizio, il server apre il TGS e inserisce il TGT dell'utente nel LSASS per un uso successivo consentendo al server di impersonare l'utente.

Constrained delegation (delega vincolata): fornisce agli amministratori di servizio la possibilità di applicare restrizioni limitando l'ambito in cui i servizi possono agire per conto di un utente.

- Comandi
  - `Get-ADComputer -Filter {TrustedForDelegation -eq $true -and primarygroupid -eq 515} -Properties trustedfordelegation,serviceprincipalname,description`
  - `Get-DomainUser -TrustedToAuth`
- Mitigazioni
  - Disabilitare l'unconstrained delegation. Configurare la constrained delegation ove necessario.
  - Abilitare il parametro "Account is sensitive and cannot be delegated" per account amministrativi come Domain Admin.
  - Aggiungere gli account amministrativi/a rischio al gruppo "Protected Users Security Group" così da prevenire la possibilità di deleghe.
  - Limitare la possibilità di accesso dei Domain Admin/Admin a specifici server.

DCShadow

Il DCShadow ... Don ... Directory. Per essere effettu...

[MS-ADTS ... ervice Specificati...

Article • 04/27/2022 • 4 minu...

Specifies the core function ... cation and Lightweight Directory Acc...

This page and associated ... e to the RSS feed to receive update notificat...

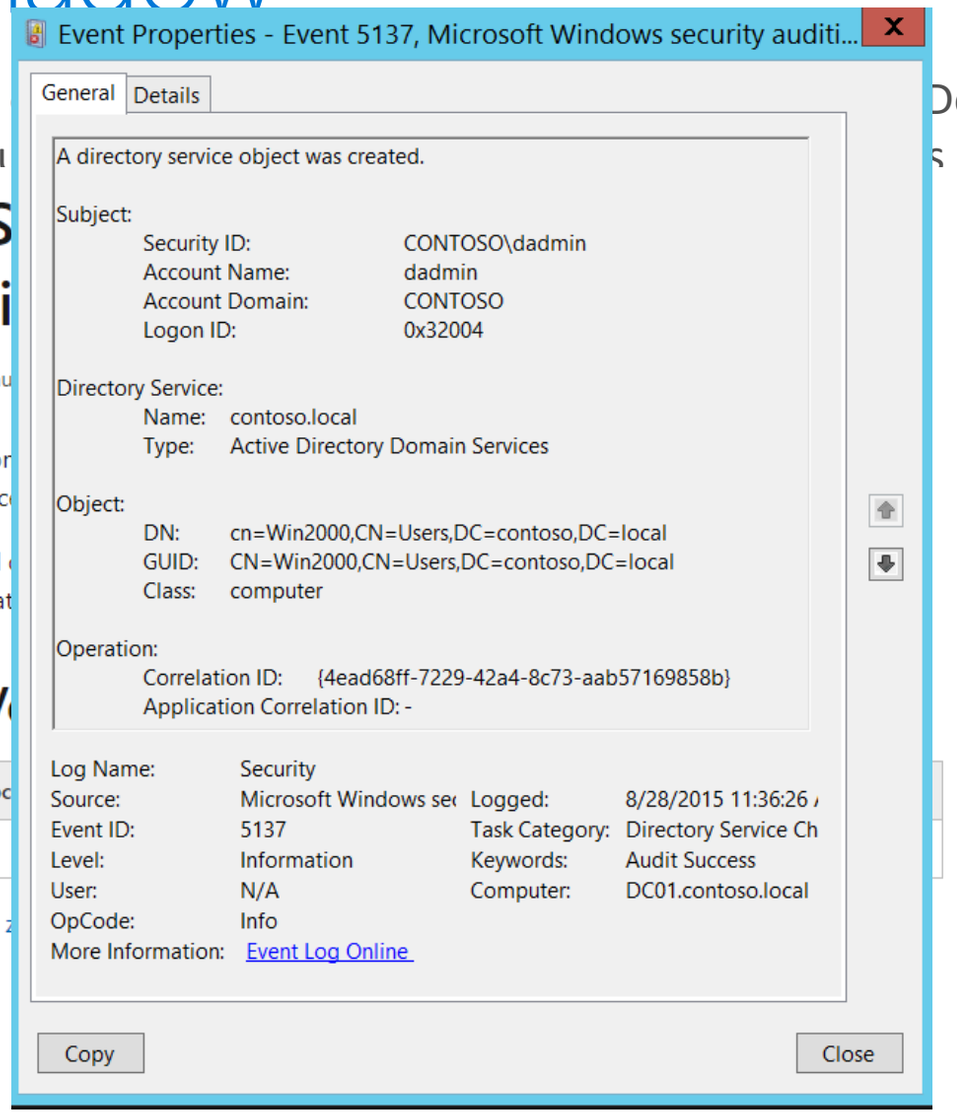
Published V...

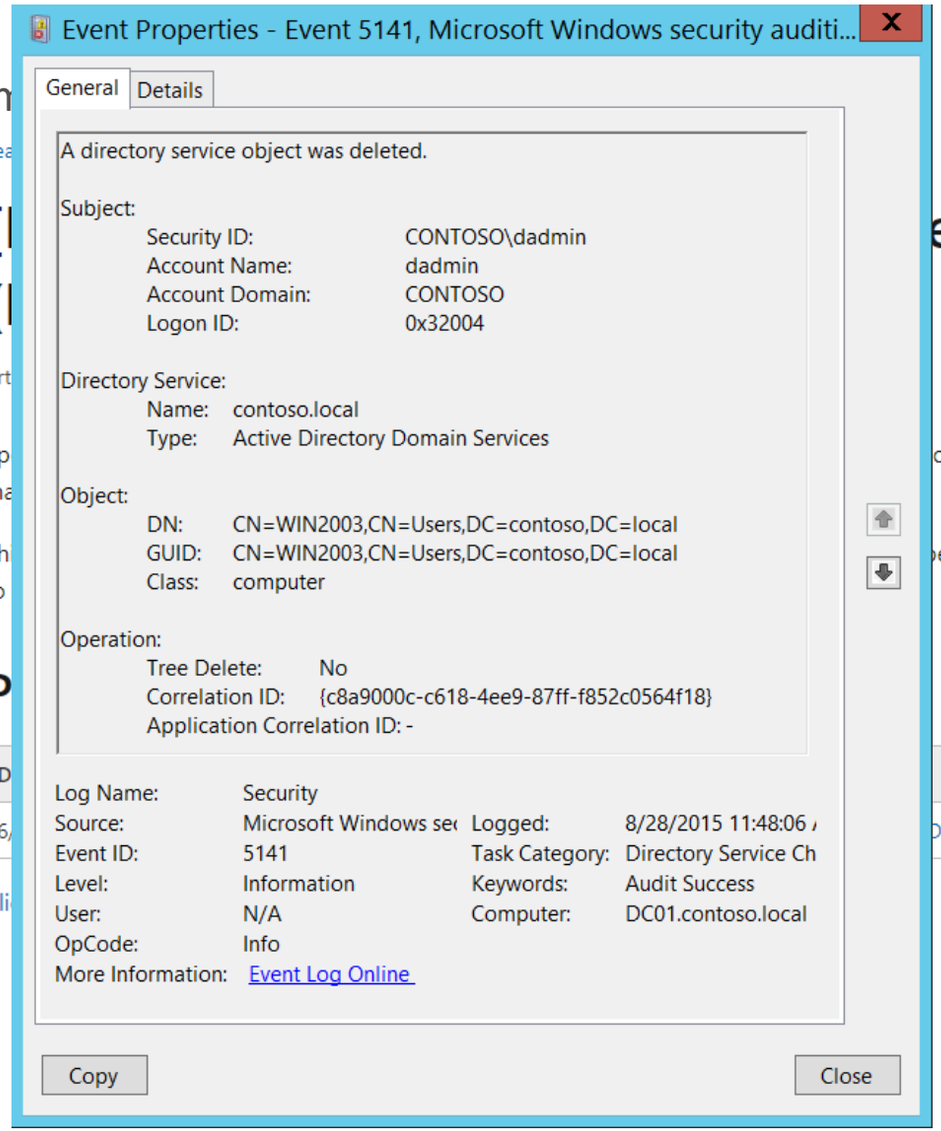
Date	Protoc...
4/29/2022	55.0

Click here to download a z...

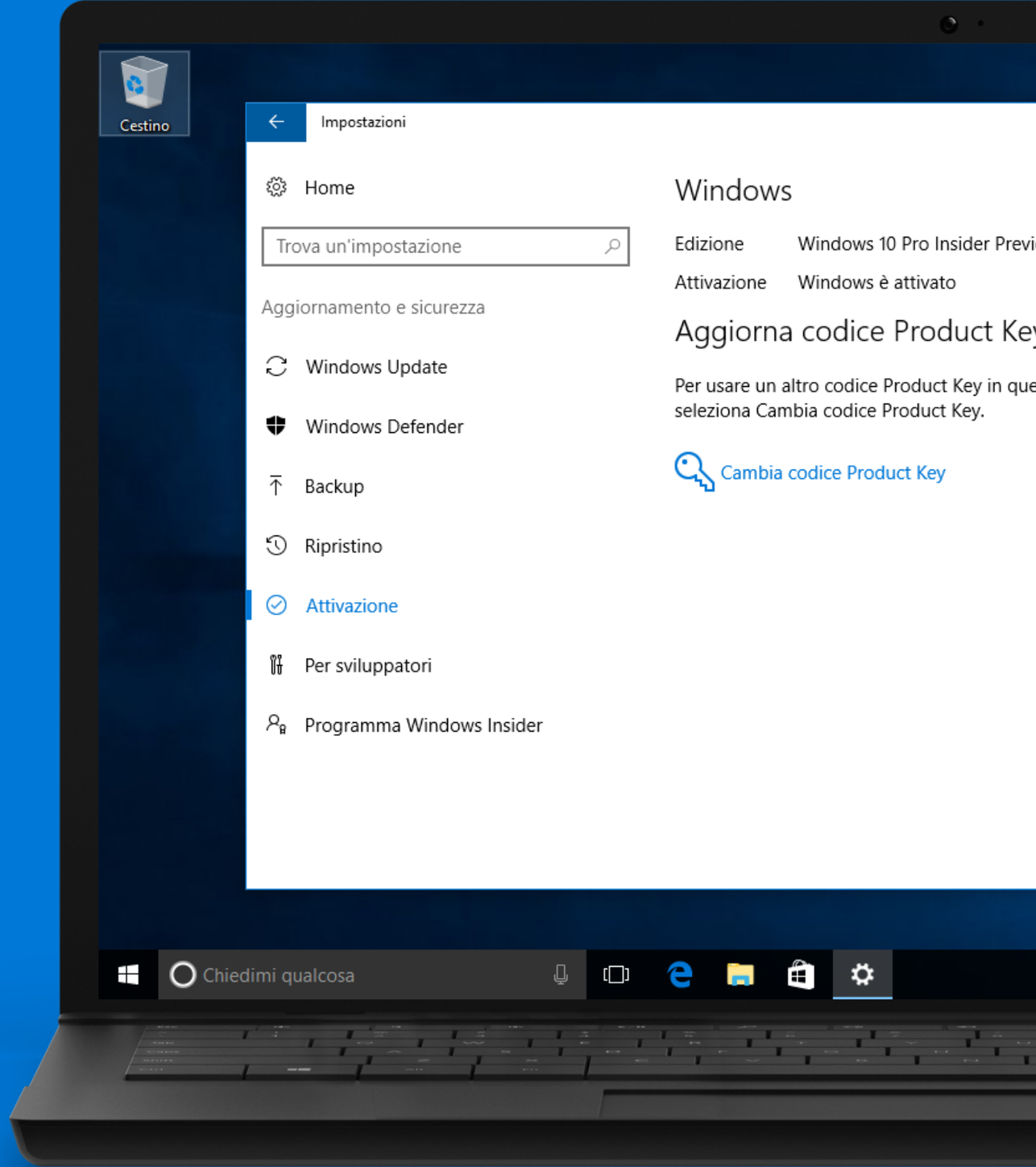
Feedback

Diff



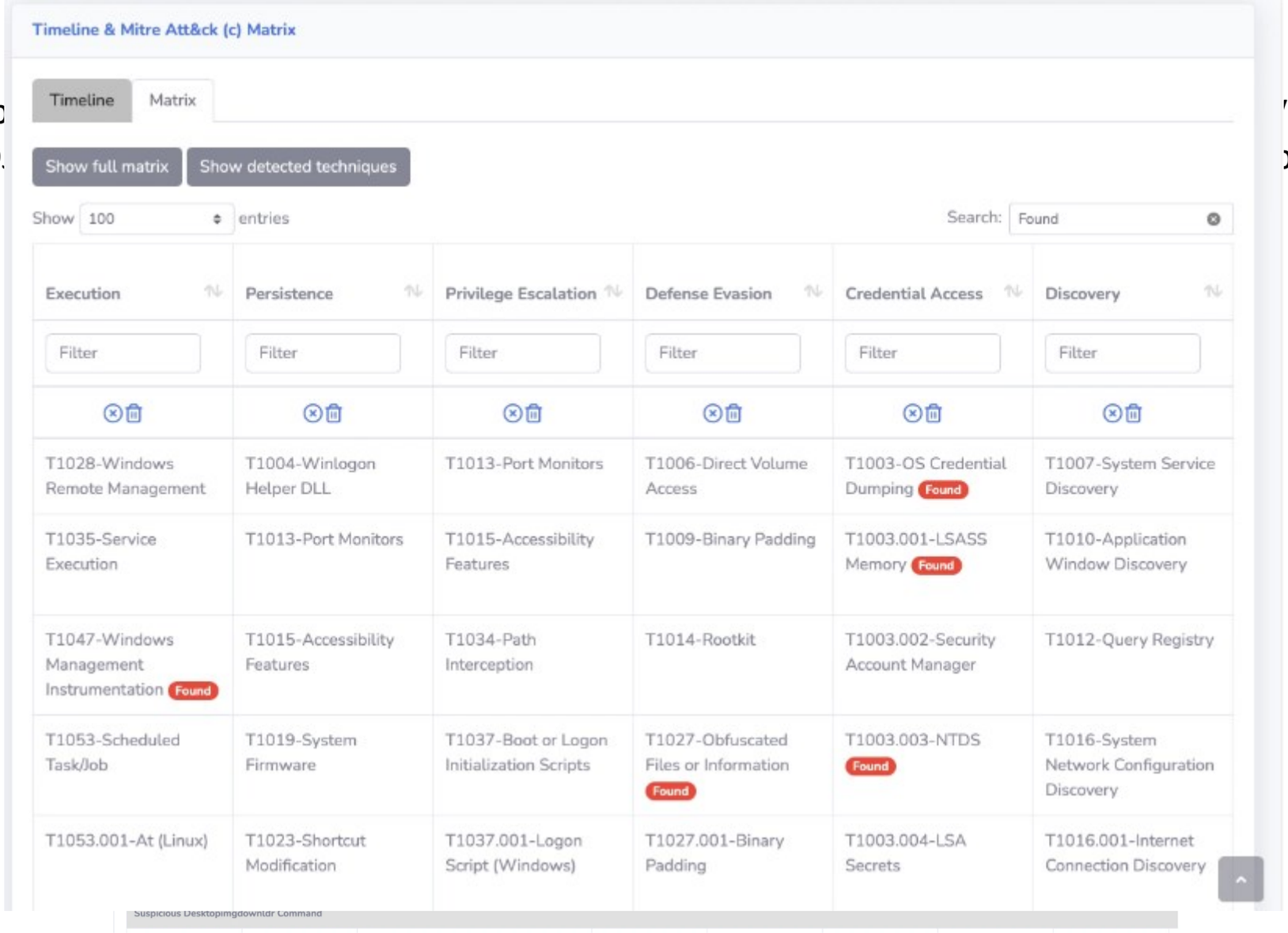


Si, ok...
E ora?


Cestino
Impostazioni
Home
Trova un'impostazione
Aggiornamento e sicurezza
Windows Update
Windows Defender
Backup
Ripristino
Attivazione
Per sviluppatori
Programma Windows Insider
Windows
Edizione
Windows 10 Pro Insider Previ
Attivazione
Windows è attivato
Aggiorna codice Product Key
Per usare un altro codice Product Key in que
seleziona Cambia codice Product Key.
Cambia codice Product Key
Chiedimi qualcosa

Zircolite

Zircolite è un tool op 'TX, Auditd, Sysmon o JSONL/ND. ber threat all'interno dei log.



ICT POWER.IT

Microsoft

Grazie

Domenico Caldarelli
Ethical Hacker
domenico.caldarelli@itisistemi.it