README

Dumpert, an LSASS memory dumper using direct system calls and API unhooking

Recent malware research shows that there is an increase in malware that is using direct system calls to evade user-mode API hooks used by security products. This tool demonstrates the use of direct System Calls and API unhooking and combine these techniques in a proof of concept code which can be used to create a LSASS memory dump using Cobalt Strike, while not touching disk and evading AV/EDR monitored user-mode API calls.

More info about the used techniques can be found on the following Blog: https://outflank.nl/blog/2019/06/19/red-team-

tactics-combining-direct-system-calls-and-srdi-to-bypass-av-edr/

Two versions of the code are included:

An executable and a DLL version of the code. The DLL version can be run as follows:

```
rundll32.exe C:\Dumpert\Outflank-Dumpert.dll,Du
```

Also, an sRDI version of the code is provided, including a Cobalt Strike agressor script. This script uses shinject to inject the sRDI shellcode version of the dumpert DLL into the current process. Then it waits a few seconds for the lsass minidump to finish and finally downloads the minidump file from the victim host.

Compile instructions:

```
This project is written in C and assembly.
You can use Visual Studio to compile it from so
```

The sRDI code can be found here:
https://github.com/monoxgas/sRDI

Languages

C 84.7% Assembly 15.3%