New Memory Scraping Technique in Cherry Picker PoS Malware

trustwave.com/Resources/SpiderLabs-Blog/New-Memory-Scraping-Technique-in-Cherry-Picker-PoS-Malware/

Introduction

Working primarily with point of sale malware, we regularly see the telltale signs of scraping memory for Card Holder Data (CHD). Open up the process, walk through the memory using VirtualQuery, check for numbers between 3 and 6… You know the drill, it's pretty much "the way it's done". Yesterday we posted a blog about Cherry Picker malware. In my first pass through the malware, I found the credit card searching algorithm and glazed over the details while I finished the write up for the forensic team. At that point I realized that I did not see how memory had been accessed. Following the function calls led me to a new technique for scraping memory using the Windows API QueryWorkingSet. Raising awareness of this method can help Antivirus companies and security researchers detect future threats that use this new technique.

The API

The calling function for the credit card scraping algorithm contained a couple of calls to an API call that I have not run across before in malware:

```
BOOL WINAPI QueryWorkingSet(
```

_In_ HANDLE hProcess,

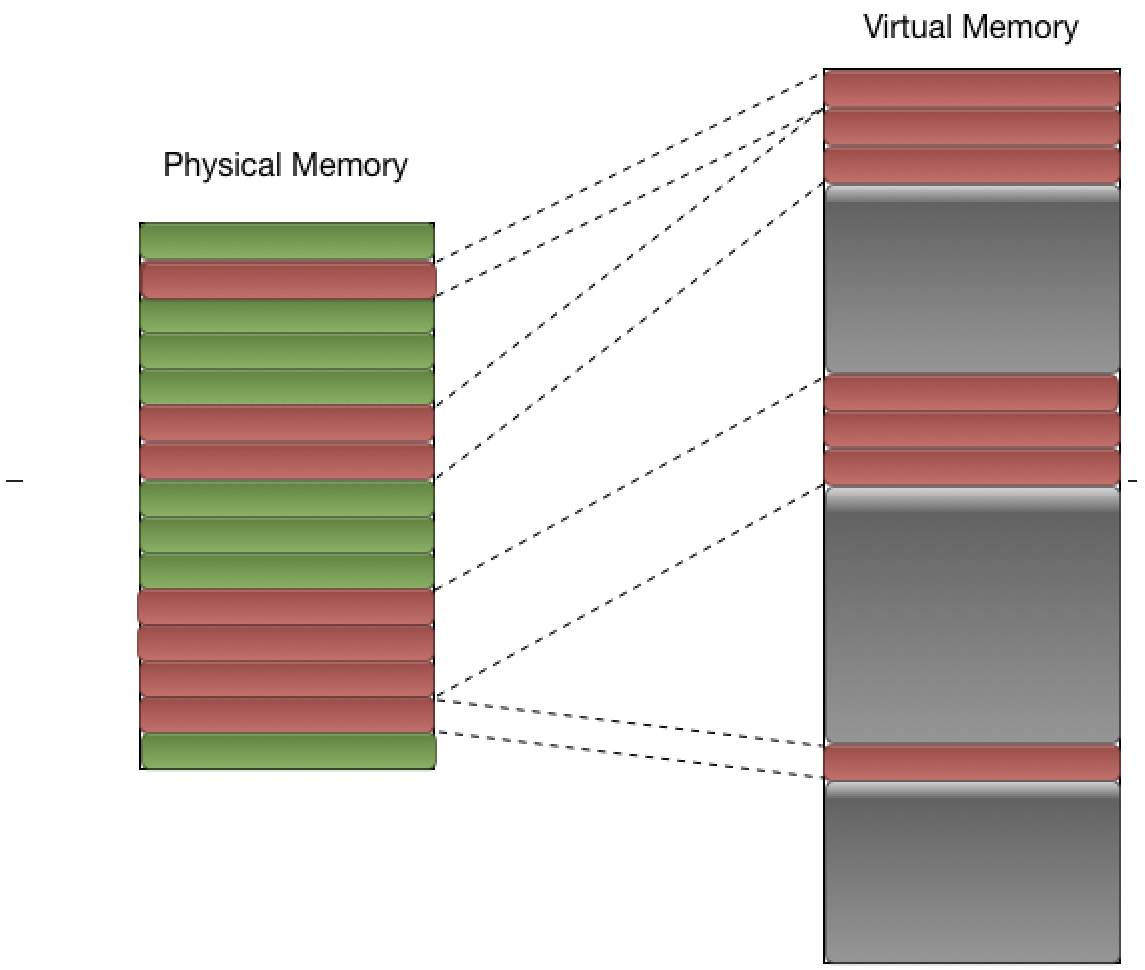
Out PVOID pv,

_In_ DWORD cb);

After investigating this API, it became apparent that this was how the author was accessing memory in the process. Here is a overview of the algorithm.

Cherry Picker Usage

Since Cherry Picker is a DLL that is loaded or injected into the target process, calling GetCurrentProcess retrieves a handle to the current process. This also works on other processes, but both the calling process and the foreign process need to be opened with the correct privileges. With the process handle, a call to QueryWorkingSet is made. This call will actually fail because we don't know how much space we need for the buffer, but even though it fails it will still return the number of virtual pages that the process currently has. This is the information we are after. Knowing the number of pages we have allows us to declare a buffer with the correct amount of space. With a large enough buffer, we can call QueryWorkingSet again to retrieve the information about the pages resident in memory. After translating the linear address into a virtual address, we can check the permissions on the page, read them into a buffer, and scan them for CHD. When scanning for CHD, only read/write pages are relevant.



The image above shows a very simplified visualization of linear pages being mapped into the process's virtual address space. The black boxes in the virtual memory represents unallocated space in the process. The QueryWorkingSet API will return the addresses in virtual space for each physical page that is mapped into the process's virtual memory.

QueryWorkingSet vs. VirtualQuery

You might ask yourself, what is the difference between using QueryWorkingSet and VirtualQuery to analyze memory. Both techniques will give you access to the same virtual memory but in a different way. Microsoft's API documentation describes the working set as:

"The *working set* of a program is a collection of those pages in its virtual address space that have been recently referenced. It includes both shared and private data"

Essentially, QueryWorkingSet is accessing virtual memory a page at a time, while VirtualQuery accesses memory across a variable range.

Wrap-up

It is interesting to see a new technique being used by malware authors for this type of work. I was unable to find any other examples of this being used to scrape CHD from memory, although this technique associated with obtaining the information on some of the lesser-known panels in your average task manager program.

I wrote a proof of concept program to aid understanding of the technique and demonstrate what the code looks like. Interestingly, I found a more recently compiled version of Cherry Picker and discovered that the author had reverted to using VirtualQuery to process memory. Not sure as to the reason, but I felt it was important to expose a technique that has been seen in the wild that I was unable to find anyone else discussing.