HIDDENBEE MALWARE

Hidden Bee, a Chinese crypto miner with a complicated structure, is a one of a major threat in cyber space. Because this virus operates invisibly, the only way a victim will notice that their system has been compromised is if they notice a increase in processor consumption. A deeper inspection will reveal that the malware payloads were injected into a number of programmes, with anomalous executable parts in those processes.

Hidden Bee has been seen distributed via Malvertising on adult sites, redirecting visitors to an exploit kit landing page or a malicious loader. In these attacks, the threat actors use randomization of the URL path to avoid detection by security products and antivirus programs. of the While Hidden Bee debuted using the underminer exploit kit, which utilizes Internet Explorer and Flash Player exploits, it has evolved to the use of payloads inside WAV files, as well as hiding them in JPEG and PNG images. After infecting the victim's system, the attackers ensure persistence by installing boot kit that will run the miner every time the system restarts**.**

A very powerful hardware is necessary to efficiently mine cryptocurrency, since electricity bills and other expenses are significant. Therefore, the entire process can be costly. To avoid time and money building mining rigs, cyber criminals develop malicious miners such as Hidden Bee and proliferate them. An average home PC is not a good choice to mine cryptocurrency, since the cost of electricity is higher than any revenue generated, however, infecting thousands of machines and not having to pay is another strategy that can work for criminals. Therefore, proliferating malicious miners is becoming increasingly popular. Hidden Bee employs mainly CPU resources, however, there also are traces of CUDA platform/API usage. Cryptocurrency mining is essentially a process by which computers solve various mathematical equations. The same equation is solved by multiple computers at once (all data is transferred through the Internet) and the more problems solved, the more revenue the owner generates, and the more cryptocurrency is mined. The process can take up to 100% of system resources and the system can become unstable and virtually unusable. Furthermore, fully-loaded hardware components generate excessive heat and, within certain circumstances they might overheat and be permanently damaged. Furthermore, all revenue goes to cyber criminals, whilst victims take all risks with no benefits in return. As mentioned above, Hidden Bee is distributed using an exploit kit. In fact, cryptominers are often distributed using trojans, which cause chain infections. Therefore, if you have noticed a significant increase in resource usage (the components often work at their maximum, even when no software is running), it is strongly advised to scan the system with a reputable anti-virus suite and eliminate all detected threats.

Let us analyse the details for the malware samples provided in 2018-08 Hidden Bee Elements

Sample: 11310b509f8bf86daa5577758e9d1eb5

Basic Details:

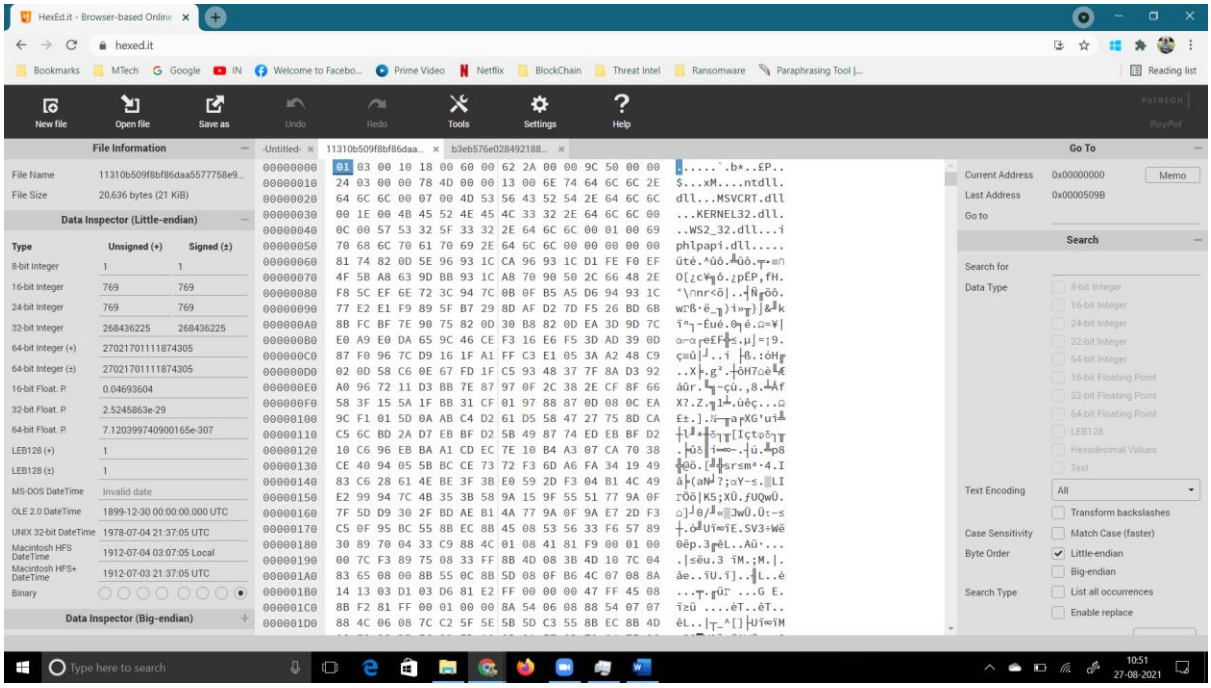
SHA-1: 66b63db1efc14c659e0d13ec21aabcc43df7e79e

SHA-256: c1a6df241239359731c671203925a8265cf82a0c8c20c94d57a6a1ed09dec289

SSDEEP:
384:P29KPvCAs3Ww/ZjVNLFy73pM3rjy2nqRCMm/utdgmayvTNljNtjxjs1M78dYM:P20PaAsHZNLFy73pEnbt/Gdgm5ZtjxDc

TLSH:
T17D925A75A1C20031DAE2C2B6A2753B3D953CF9B821C7676EF7449CA06E107A3E57931E

File Size: 20.15 KB (20636 bytes)



Sample: b3eb576e02849218867caefaa0412ccd

Basic Details

SHA-1: 79d8cf39e0dbf06a63e4ff657affda87aac47eb7

SHA-256: 76b70f1dfd64958fca7ab3e18fffe6d551474c2b25aaa9515181dec6ae112895

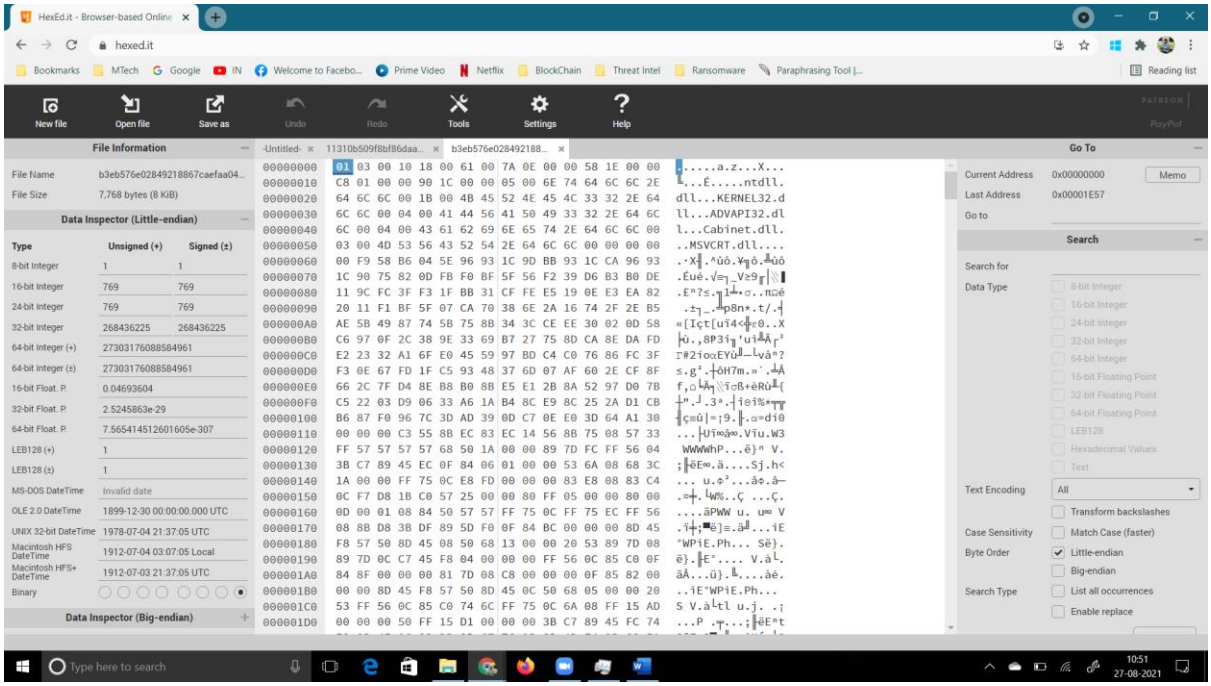
SSDEEP:

96:5ljqp3/drW5OdH9C7Crb5bfn/L9vxPxbf4HGottRORpFmCJybRmu57K3uyXZhRmY:njqrIgFhvxP9KGottRSdu5WhRmzRckM

TLSH:

T165F14C17F4F1386AC65342B5A5C7C319FA9D16462D6AD8EF3B5808C468F18C28A5B70F

File size: 7.59 KB (7768 bytes)



From the two sample files taken, there are some strings which we can take for writing Yara rules. They are ntdll.dll, kernel32.dll, advapi32.dll, cabinet.dll, msvcrt.dll, ws2_32.dll and iphlpape.dll.

A DLL (Dynamic Link Library) file is an executable file that allows applications to share code to perform one or more predetermined functions. One of the biggest advantages is that a DLL isn't loaded into RAM, saving memory and enabling multiple programs to function efficiently. Most DLL files are very useful and aid in the process of running your applications. However, others are malicious, acting as browser hijackers or Trojan horses. These programs can alter your system and allow intruders to gain remote access to your system. Malware and viruses are also transmitted through dll files.

NTDLL.DLL

1. This file is required by Windows, and deleting the file would make Windows inoperable. The ntdll.dll file is located in the c:\windows\system32 or c:\winnt\system32 directory, also found in the c:\i386 directory.
2. Ntdll.dll is mostly concerned with system tasks and it includes a number of kernel-mode functions which enables the "Windows Application Programming Interface (API)". The ntdll.dll is also responsible for messages, timing, threading and synchronization in the operating system.
3. The ntdll.dll file included with Microsoft Windows is not spyware, a trojan, or a virus. However, like any file on your computer, it can become corrupted by a virus or trojan. Antivirus programs can detect and clean this file if it's infected. Because this file is part of Windows, users should never delete or remove this file. If they think it is infected, let the antivirus program handle it.

Source: https://www.freefixer.com/library/file/ntdll.dll-26111/

KERNEL32.DLL

1. The genuine kernel32.dll file is a software component of Microsoft Windows by Microsoft.
2. Microsoft Windows is an operating system. Kernel32.dll is a dynamic link library file that is an essential part of the Windows operating system. This is a critical component of the operating system and should not be removed.
3. Its primary task is to manage system memory, input/output operations and interrupts. This file is loaded into a protective memory space when Windows starts up in an effort to prevent other applications from taking over this space.

Source: https://www.file.net/process/kernel32.dll.html

ADVAPI32.DLL

1. The genuine advapi32.dll file is a software component of Microsoft Windows by Microsoft.
2. Advanced API services library is Microsoft utility that is designed to support several APIs including registry and security calls. Advapi32.dll is a dynamic link library file associated with the API services library that provides access to advanced functionality.

Source: https://www.file.net/process/advapi32.dll.html

CABINET.DLL:

1. The genuine Cabinet.dll file is a software component of Microsoft Windows by Microsoft.
2. Cabinet.dll is a resource library that handles Microsoft Cabinet files (.cab) which hold compressed code. This is a critical Windows component and should not be disabled or removed.

Source: https://www.file.net/process/cabinet.dll.html

MSVCRT.DLL:

1. A module containing standard C library functions such as printf, memcpy, and cos.
2. It is a part of the Microsoft C Runtime Library. Non-system processes like msvcrt.dll originate from software you installed on your system.

Source: https://www.file.net/process/msvcrt.dll.html

WS2_32.DLL:

1. ws2_32.dll is a dynamically linked library that is used to handle network connections. It is a small program that relates to software processes, similarly to EXE files, but instead of giving commands, the .dll file allows applications to communicate. ws2_32.dll file works with programs that have a printing function. When you want to print a document, printer DLL file loads to a program and into memory.
2. Unfortunately, ws2_32.dll can also control an essential component of a particular parasite - trojan horse. Most threats depend on such libraries and wouldn't work without them. It is vital to determine whether or not the file is malicious, as stopping the legitimate Windows file from working might compromise your computer and even prevent it from launching correctly.

3. As ws2_32.dll file can be installed and used by a trojan, it can cause various functionality issues with the PC. If a file is related to malware of any sort, it may create abnormal network activities, Windows registry modifications, slow performance. Often parasites use files with unsuspicious names, but malicious functionality.
4. Although in most cases, ws2_32.dll is not malware and is an essential part of Windows, it is still considered to be a CPU-intensive process and may cause several issues if not properly managed

Source: https://www.2-spyware.com/file-ws2_32-dll.html

IPHLPAPE.DLL:

1. IPHLPAPI.DLL a DLL (Dynamic Link Library) file, developed by Microsoft, which is referred to essential system files of the Windows OS. It usually contains a set of procedures and driver functions, which may be applied by Windows.
2. IPHLPAPI.DLL file, also known as IP Helper API, is commonly associated with Microsoft® Windows® Operating System. It is an essential component, which ensures that Windows programs operate properly. Thus, if the iphlpapi.dll file is missing, it may negatively affect the work of the associated software.

Source: https://wikidll.com/other/iphlpapi-dll

Since it is highly likely that malware can be infected through DLL files and the taken sample files have most common dll files in the starting bytes of both samples. The Yara rule (HiddenBee.yara) has been written using the condition to check presence of atleast four in the sample.

```
rule HiddenBeeElement
{
    meta:
        author = "Vigneswaran"
        creationdate = "26.08.2021"
        description = "Sample rule written for 2018-08-Hidden-Bee-Elements"


    strings:

        $a = "ntdll.dll" nocase ascii wide fullword
        $b = "kernel32.dll" nocase ascii wide fullword
        $c = "advapi32.dll" nocase ascii wide fullword
        $d = "cabinet.dll" nocase ascii wide fullword
        $e = "msvcrt.dll" nocase ascii wide fullword
        $f = "ws2_32.dll" nocase ascii wide fullword
        $g = "iphlpapi.dll" nocase ascii wide fullword

    condition:

        4 of ($*) // any 4 of the provided strings

}
```

REFERENCES:

1. https://www.virustotal.com/gui/file/c1a6df241239359731c671203925a8265cf82a0c8c20c94d57a6a1ed09dec289/detection
2. https://www.virustotal.com/gui/file/76b70f1dfd64958fca7ab3e18fffe6d551474c2b25aaa9515181dec6ae112895/detection
3. https://blog.malwarebytes.com/threat-analysis/2018/07/hidden-bee-miner-delivered-via-improved-drive-by-download-toolkit/
4. https://medium.com/mrx-007/basic-static-analysis-of-malware-and-common-dll-ef9455d49968
5. https://www.fireeye.com/blog/threat-research/2010/07/malware-persistence-windows-registry.html
6. https://www.spamlaws.com/malware-dll-file.html