Malware Analysis Spotlight: Hancitor's Multi-Step Delivery Process

vmray.com/cyber-security-blog/hancitor-multi-step-delivery-process-malware-analysis-spotlight/

Hancitor can be grouped into the category of downloaders that are often responsible for delivering further malware families into a compromised network. Recently, it has been observed delivering the Ficker Stealer, Cobalt Strike, and the Cuba ransomware among

others. It is usually distributed to the victim via malicious spam campaigns that are intermittent in nature. In this Malware Analysis Spotlight, we will look at Hancitor's behavior and ability to deliver an information stealer.

View the VMRay Analyzer Report for the Hancitor Infostealer

Analysis of Hancitor's Configurations

If we extract the buildID from Hancitor's configuration, we are able to notice the fact that Hancitor seems to be distributed in waves. The malspam with a particular build is sent for a period of time, after which there is a pause in the distribution before a new wave of malspam distributes another build (Figure 1). Some of the spam waves produce more unique samples than others but the overall trend is pointing upwards. Usually, each batch has a unique configuration containing a new buildID and new C&C URLs (see Extracted Configurations for a non-exhaustive list of configurations).

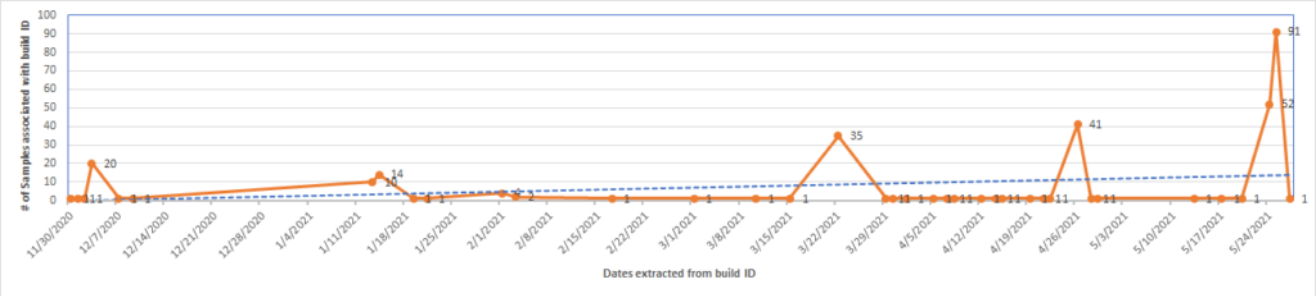


Figure 1: Line graph where the points on the x-axis indicate the date extracted from the config and the y-axis indicates the number of samples associated with a buildID.

Hancitor Analysis

The usual execution chain starts with malicious emails containing an embedded Google Docs URL. Those URLs point the user to a domain controlled by the threat actor. There, the victim is prompted to download a document. This dropped document is responsible for extracting and loading a DLL. The method that the malicious document uses to achieve execution is usually a VBA macro that is executed when the document is opened (Figure 2). The initial DLL is an intermediate stage responsible for extracting and running Hancitor.

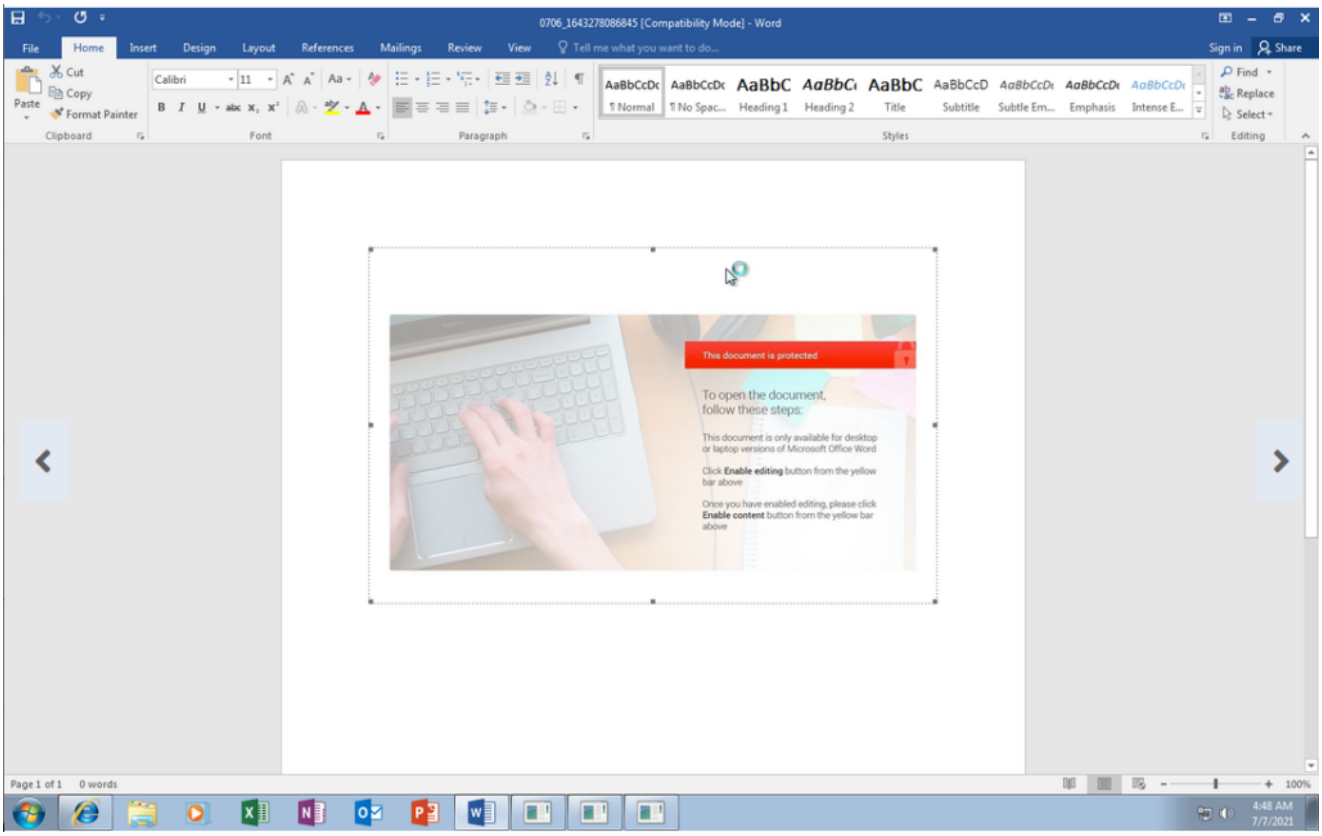


Figure 2: Malicious document telling the user to enable editing.

The VBA macro's main responsibility is to execute the embedded DLL. The DLL doesn't require a specific entry point to run, but it's still invoked with one. The passed entry point isn't used by this initial DLL, but by the actual Hancitor payload at a later stage of the execution process. For Hancitor to run, it's necessary to start it by calling one of its exported functions. The name of the function is hard-coded inside the macro code (Figure 3).

```
Dim cx
cx = wdUserTemplatesPath
bbbb = "r"
vcbc = Options.DefaultFilePath(cx)
bbbb = bbbb & "u" & "n"
Call xz
If Dir(vcbc & "\niberius.dll") = "" Then
Call yyy

If Len(hdv) > 2 Then

Call nam(hdv)




 Dim cvzz As String
cvzz = "13" & "2"


  gc 0, vbNullString, _
    bbbb & cvzz, vcbc & "\niberius.d" & "ll,UBISYAYMQSE", _
     vbNullString, 1
End If
End If
End Sub
```

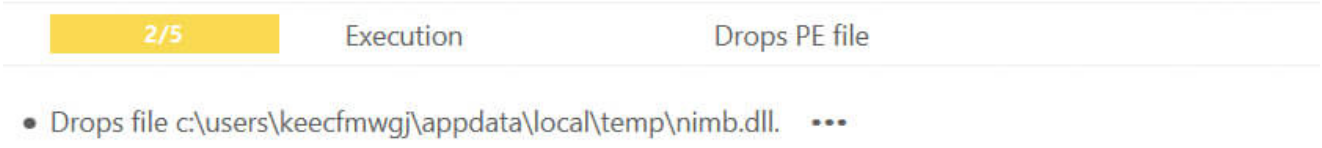


Figure 3: VMRay Analyzer – Excerpt of the macro responsible for starting the embedded DLL (top) and a VTI tracking the dropped file (bottom)

The document's macro is loading the DLL by using the rundll32 utility. By observing the process creation in the VMRay Analyzer we can also see the passed command line arguments. The called entry point corresponds exactly with one of Hancitor's exported functions (Figure 4).

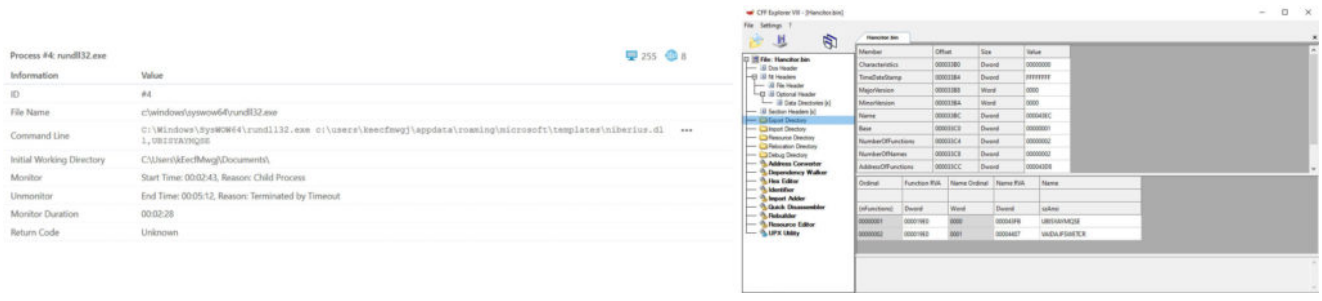
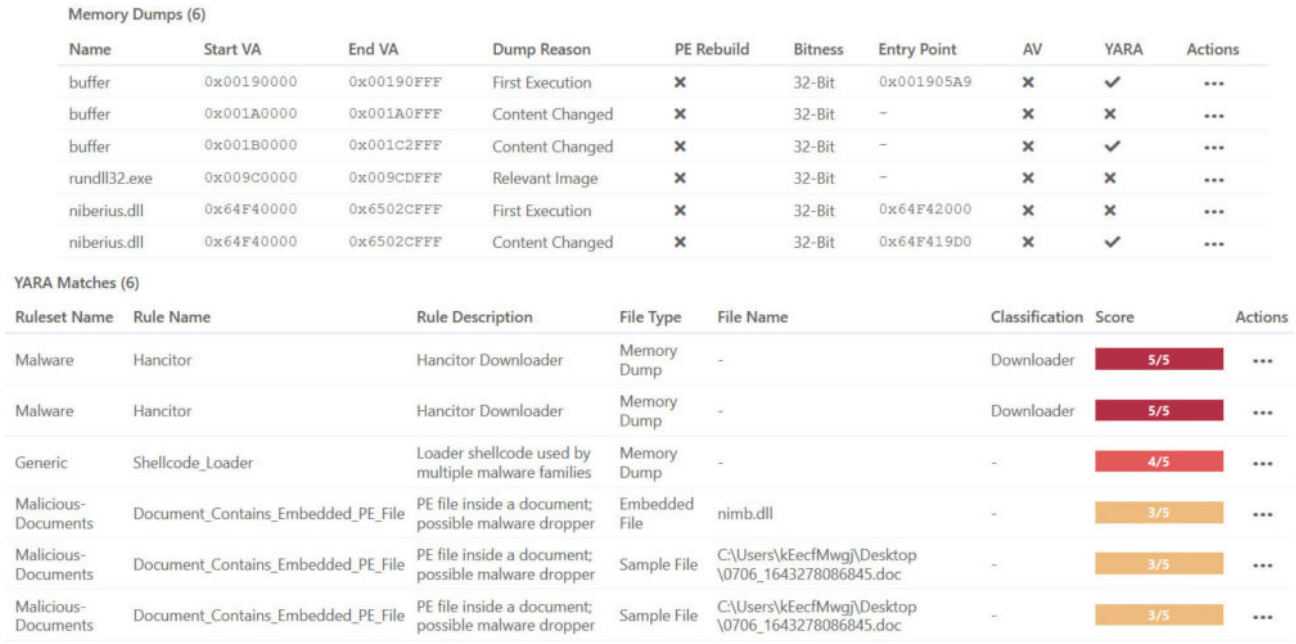


Figure 4: Monitoring of the rundll32 processes in VMRay Analyzer (left) and the export directory of Hancitor (right).

The initial DLL is a packer that is responsible for decrypting, decompressing, and loading the Hancitor payload. The compression library used by the packer is aPLib. aPLib became quite popular with malware authors due to its small footprint and relatively good compression and decompression speed. Nonetheless, the smart memory dumping of the VMRay Analyzer includes the memory dumps of each stage which also contain the final uncompressed Hancitor payload (Figure 5).



Memory Dumps (6)

Name	Start VA	End VA	Dump Reason	PE Rebuild	Bitness	Entry Point	AV	YARA	Actions
buffer	0x00190000	0x00190FFF	First Execution	✗	32-Bit	0x001905A9	✗	✓	•••
buffer	0x001A0000	0x001A0FFF	Content Changed	✗	32-Bit	-	✗	✗	•••
buffer	0x001B0000	0x001C2FFF	Content Changed	✗	32-Bit	-	✗	✓	•••
rundll32.exe	0x009C0000	0x009CDFFF	Relevant Image	✗	32-Bit	-	✗	✗	•••
niberius.dll	0x64F40000	0x6502CFFF	First Execution	✗	32-Bit	0x64F42000	✗	✗	•••
niberius.dll	0x64F40000	0x6502CFFF	Content Changed	✗	32-Bit	0x64F419D0	✗	✓	•••

YARA Matches (6)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Score	Actions
Malware	Hancitor	Hancitor Downloader	Memory Dump	-	Downloader	5/5	•••
Malware	Hancitor	Hancitor Downloader	Memory Dump	-	Downloader	5/5	•••
Generic	Shellcode_Loader	Loader shellcode used by multiple malware families	Memory Dump	-	-	4/5	•••
Malicious-Documents	Document_Contains_Embedded_PE_File	PE file inside a document; possible malware dropper	Embedded File	nimb.dll	-	3/5	•••
Malicious-Documents	Document_Contains_Embedded_PE_File	PE file inside a document; possible malware dropper	Sample File	C:\Users\kEecfMwgj\Desktop\0706_1643278086845.doc	-	3/5	•••
Malicious-Documents	Document_Contains_Embedded_PE_File	PE file inside a document; possible malware dropper	Sample File	C:\Users\kEecfMwgj\Desktop\0706_1643278086845.doc	-	3/5	•••

Figure 5: VMRay Analyzer – The final Hancitor payload extracted from one of the buffers (top) and the corresponding matching YARA rule (bottom).

The DLL itself and the techniques it uses are very similar to the ones previously used by, e.g., Dridex. When it's finally Hancitor's turn to take over the execution flow, it first tries to initiate a connection to its C&C server. Usually, each Hancitor binary knows about three C&C URLs which are embedded in its configuration file. It gathers information about the infected host system (adapter addresses and the volume serial number) and uses that to generate a unique ID. It also checks the external IP address and the AD domain, if the host is part of any. It then bundles it all into the initial request to the server (Figure 6). Some of that information is used by the C&C server to deliver a specific payload. For example, in recent Hancitor campaigns it has been seen delivering Cobalt Strike if the host was part of an AD domain.

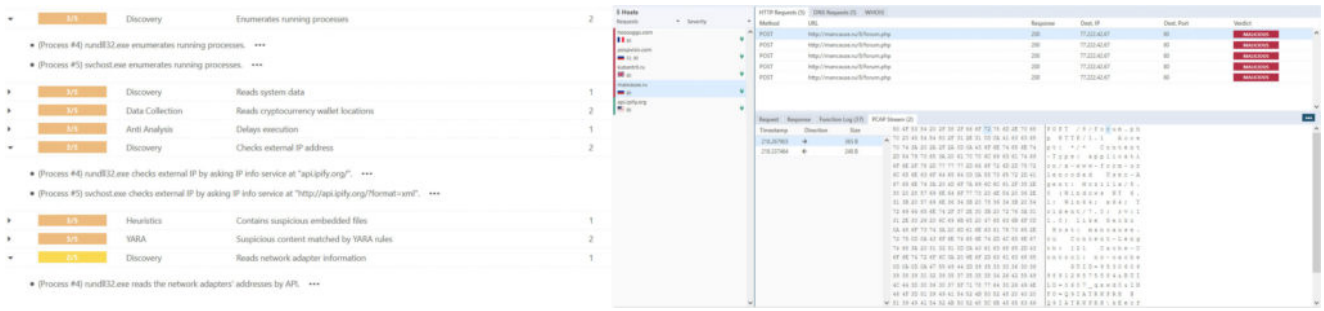


Figure 6: VMRay Analyzer – VTI rules matching the host discovery (left) and the C&C network connection containing the beacon string (right).

The response sent by the server is XORed and base64 encoded. The 1-byte XOR key required to decrypt the data is hard-coded inside the routine responsible for decoding. When the data is decoded, the command is extracted and validated. Then it's processed and the corresponding action is taken. In this analysis, Hancitor downloads a secondary payload from a server which it receives from its C&C (as part of the response). It then starts svchost.exe and injects it with the downloaded payload (Figure 7). In this particular case, the delivered payload is a stealer.

Figure 7: Hancitor contacts its C&C and downloads the payload from another server (left) it then injects it into svchost.exe (right).

Conclusion

Although the capabilities of Hancitor itself didn't really change over the past years, the combination of a multi-step delivery process and different packers, still allows it to avoid detection and deliver further malware families successfully. VMRay Analyzer's dynamic analysis plays an important role in the detection process and can provide defenders with timely information necessary to protect their networks.

IOCs

Initial document

SHA256:

`e431a1bb2efcf6000f5bac4e19673d6deb9de7997dba5f65bae7779cd19e5caf`

Hancitor DLL

SHA256:

```
82E13456113A950EE0FE06975CEC093B2D78F91E75D482428ECFA274EC7D2555
```

Extracted Configurations

Hancitor configuration in the MWCP schema:

{'key': [b'b27242d151accab3'], 'missionid': ['3011_hjdfsfg'], 'c2_url':
['hxxp://propywast[.]com/8/forum.php', 'hxxp://aribliffored[.]ru/8/forum.php', 'hxxp:/

{'key': [b'0e5c84ed4a00f0b8'], 'missionid': ['0112_hjdfsjhf'], 'c2_url':
['hxxp://neectuded[.]com/8/forum.php', 'hxxp://exieverhiltur[.]ru/8/forum.php', 'hxxp:

{'key': [b'c0b9e88c8c15013d'], 'missionid': ['0212_78434'], 'c2_url':
['hxxp://eaussill[.]com/8/forum.php', 'hxxp://hossangerts[.]ru/8/forum.php', 'hxxp://b

{'key': [b'd4cf01508b268707'], 'missionid': ['0312_89324'], 'c2_url':
['hxxp://bandieve[.]com/8/forum.php', 'hxxp://decturnearrips[.]ru/8/forum.php', 'hxxp:

{'key': [b'75a02962251f70df'], 'missionid': ['0712_843923'], 'c2_url':
['hxxp://maduabin[.]com/8/forum.php', 'hxxp://thenexames[.]ru/8/forum.php', 'hxxp://pr

{'key': [b'ddd2e881a29b02ee'], 'missionid': ['0912_3oooiu9'], 'c2_url':
['hxxp://spardethe[.]com/8/forum.php', 'hxxp://tworkityre[.]ru/8/forum.php', 'hxxp://s

{'key': [b'60cd28d0bb2fb7d8'], 'missionid': ['1301_dsf7823'], 'c2_url':
['hxxp://requirend[.]com/8/forum.php', 'hxxp://spabyasiande[.]ru/8/forum.php', 'hxxp:/

{'key': [b'299cdab6ea0db92f'], 'missionid': ['1401_90210'], 'c2_url':
['hxxp://ocifirtaterity[.]com/8/forum.php', 'hxxp://mailartmen[.]ru/8/forum.php', 'hxx

{'key': [b'f3725ea38a05c622'], 'missionid': ['1901_48re93'], 'c2_url':
['hxxp://opulteme[.]com/8/forum.php', 'hxxp://tharepirms[.]ru/8/forum.php', 'hxxp://wo

{'key': [b'155ed9c95666b69e'], 'missionid': ['0102_jerpo3'], 'c2_url':
['hxxp://antialkinno[.]com/8/forum.php', 'hxxp://knorshand[.]ru/8/forum.php', 'hxxp://

{'key': [b'cb5c4a0385406924'], 'missionid': ['0302_095463'], 'c2_url':
['hxxp://efelsdvismade[.]com/8/forum.php', 'hxxp://curishisral[.]ru/8/forum.php', 'hxx

{'key': [b'ea4276b76f53dbde'], 'missionid': ['1702_pro23'], 'c2_url':
['hxxp://hatuderefer[.]com/8/forum.php', 'hxxp://thavelede[.]ru/8/forum.php']}
{'key': [b'85a43da114bd20b4'], 'missionid': ['0103_jepskew'], 'c2_url':
['hxxp://ementincied[.]com/8/forum.php', 'hxxp://watoredprocaus[.]ru/8/forum.php', 'hx

{'key': [b'6727a6d2d2680b3a'], 'missionid': ['0203_lisr93'], 'c2_url':
['hxxp://witakilateg[.]com/8/forum.php', 'hxxp://sonalsovele[.]ru/8/forum.php', 'hxxp:

{'key': [b'c6935de3e9a3daf8'], 'missionid': ['0804_cifp'], 'c2_url':
['hxxp://lerevahel[.]com/8/forum.php', 'hxxp://lerevahel[.]ru/8/forum.php', 'hxxp://me

{'key': [b'430c378c39a69089'], 'missionid': ['1204_spk'], 'c2_url':
['hxxp://varembacen[.]com/8/forum.php', 'hxxp://twomplon[.]ru/8/forum.php', 'hxxp://la

{'key': [b'2347b01e5ff72081'], 'missionid': ['1404_cms3'], 'c2_url':
['hxxp://dingulbolies[.]com/8/forum.php', 'hxxp://culadinces[.]ru/8/forum.php', 'hxxp:

{'key': [b'c836388e91c7977c'], 'missionid': ['1504_wtp'], 'c2_url':
['hxxp://regatimmish[.]com/8/forum.php', 'hxxp://wilewgracted[.]ru/8/forum.php', 'hxxp

{'key': [b'7600d5b6a7526763'], 'missionid': ['1904_hvm'], 'c2_url':
['hxxp://erisastand[.]com/8/forum.php', 'hxxp://trimpledtim[.]ru/8/forum.php', 'hxxp:/

```
{'key': [b'58988055df80892d'], 'missionid': ['2104_mmvm'], 'c2_url':
['hxxp://lectionalt[.]com/8/forum.php', 'hxxp://palimenciont[.]ru/8/forum.php', 'hxxp:

{'key': [b'45c57c2205119f33'], 'missionid': ['2204_fesw09'], 'c2_url':
['hxxp://adrouterigh[.]com/8/forum.php', 'hxxp://fronversimai[.]ru/8/forum.php', 'hxxp

{'key': [b'2bfb5eabc096751b'], 'missionid': ['2604_gthewq'], 'c2_url':
['hxxp://caperesto[.]com/8/forum.php', 'hxxp://watiounds[.]ru/8/forum.php', 'hxxp://th

{'key': [b'e34fc8d1add6defb'], 'missionid': ['2804_jk02pol'], 'c2_url':
['hxxp://sumbahas[.]com/8/forum.php', 'hxxp://staciterst[.]ru/8/forum.php', 'hxxp://se

{'key': [b'b9d0eb646a90825c'], 'missionid': ['2904_x2'], 'c2_url':
['hxxp://nencivelf[.]com/8/forum.php', 'hxxp://chasslace[.]ru/8/forum.php', 'hxxp://sc

{'key': [b'54bef01dcee6813b'], 'missionid': ['1305_vers89'], 'c2_url':
['hxxp://chnicallimigue[.]com/8/forum.php', 'hxxp://amaozedractue[.]ru/8/forum.php', '
```