HELLOKITTY MALWARE ANALYSIS

Hellokitty is a ransomware that caused chaos in CD Projekt Red, the company behind the video game Cyberpunk2077, and to point out it drops unique ransom notes for different executables check out this blog https://www.cadosecurity.com/post/punk-kitty-ransom-analysing-hellokitty-ransomware-attacks that show cases recent attacks. This write-up shows how hellokitty ransomware works and to get a hold on to the sample check https://app.any.run/tasks/8162e38a-9475-4d6f-b4a3-b21012835164/

Static analysis

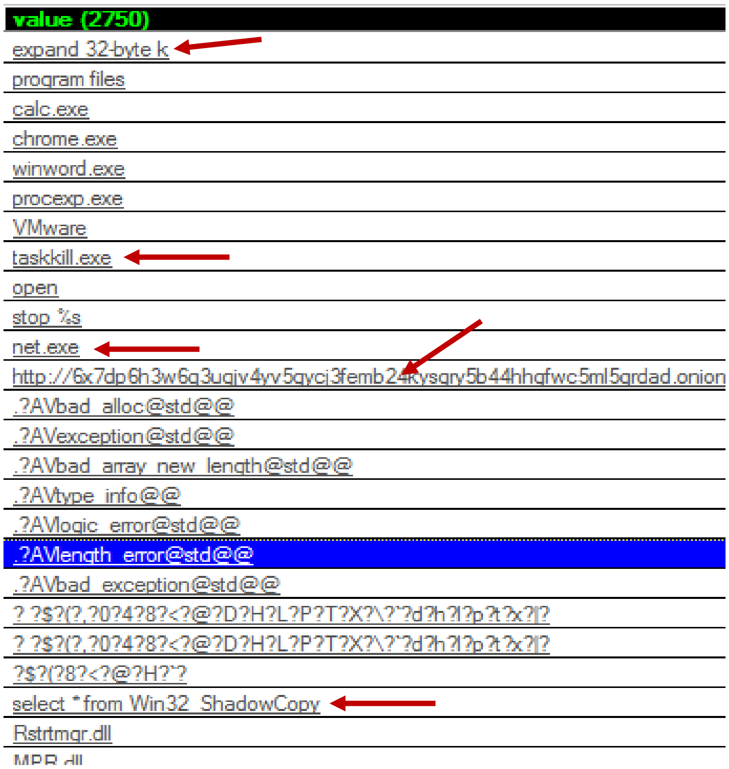
Sha256: fa722d0667418d68c4935e1461010a8f730f02fa1f595ee68bd0768fd5d1f8bb

Signature: Microsoft Visual C++ 8

Compiler-stamp: 0x5F966266 (Sun Oct 25 22:45:10 2020)

Entropy: 5.985

Taking a look at strings there are some juicy stuffs as show in figure 1



```
value (2750)
expand 32-byte k
program files
calc.exe
chrome.exe
winword.exe
procexp.exe
VMware
taskkill.exe
open
stop %s
net.exe
http://6x7dp6h3w6q3ugjv4yv5gycj3femb24kysgry5b44hhgfwc5ml5qrdad.onion
.?AVbad_alloc@std@@
.?AVexception@std@@
.?AVbad_array_new_length@std@@
.?AVtype_info@@
.?AVlogic_error@std@@
.?AVlength_error@std@@
.?AVbad_exception@std@@
? ?$?(?,?0?4?8?<?@?D?H?L?P?T?X?\?`?d?h?l?p?t?x?|?
? ?$?(?,?0?4?8?<?@?D?H?L?P?T?X?\?`?d?h?l?p?t?x?|?
?$?(?8?<?@?H?`?
select * from Win32_ShadowCopy
Rstrtmgr.dll
MPR.dll
```

Figure 1 few strings that gives an overview

The strings here gives an overview of the malware `expand 32-byte k` is a magic byte for salsa20 or chacha cryptographic algorithm we assume it is used to encrypt the files

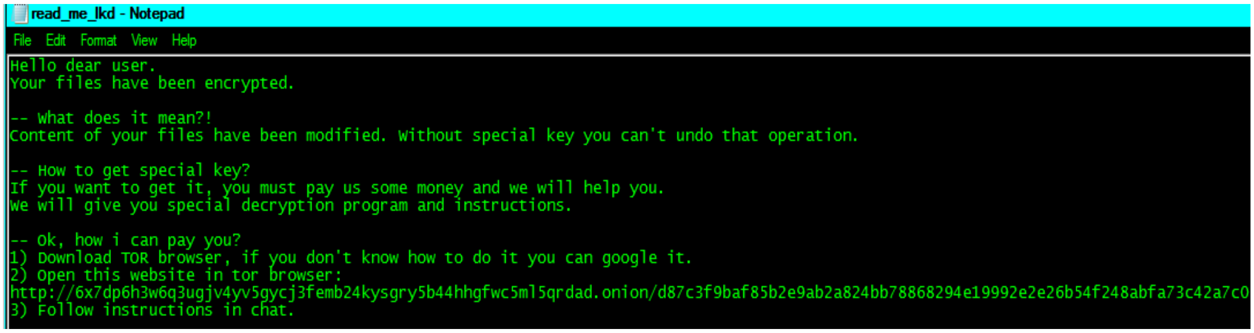
There is a huge blacklist of exe and services that the malware likes to kill, usage of `taskkill.exe` and `net.exe` proves it

There is an onion link that possibly will be used in the ransom note

`Select * from Win32 ShadowCopy` shows it might try to inhibit system recovery

Ransom note

The malware drops its ransom note in each folder it enumerates, the ransom note came with this sample has a name `read_me_lkd.txt` following figure shows the ransom note.



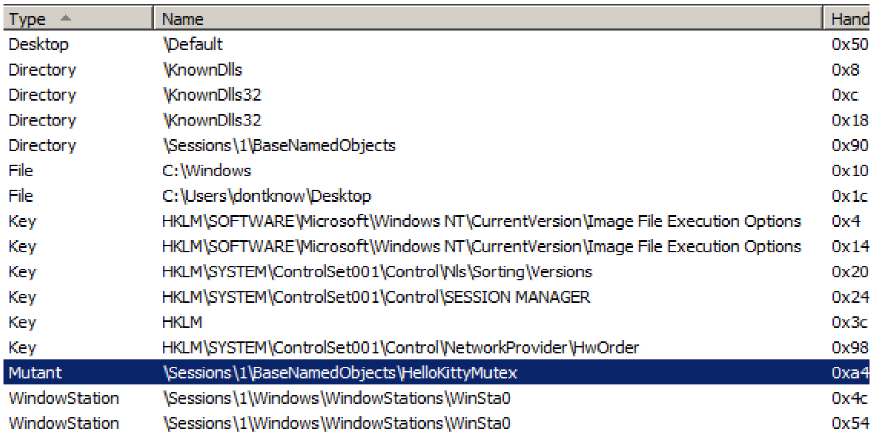
```
Hello dear user.
Your files have been encrypted.

-- What does it mean?!
Content of your files have been modified. Without special key you can't undo that operation.

-- How to get special key?
If you want to get it, you must pay us some money and we will help you.
We will give you special decryption program and instructions.

-- Ok, how i can pay you?
1) Download TOR browser, if you don't know how to do it you can google it.
2) Open this website in tor browser:
http://6x7dp6h3w6q3ugjv4yv5gycj3femb24kysgry5b44hhgfwc5ml5qrdad.onion/d87c3f9baf85b2e9ab2a824bb78868294e19992e2e26b54f248abfa73c42a7c0
3) Follow instructions in chat.
```

Figure 2 ransom note

The malware use APIs like `FindFirstFileW` and `FindNextFileW` to enumerate through folders and `writefile` to save the ransom note to each folder.

Mutant

The malware creates a mutex with the name HelloKittyMutex as show in figure below

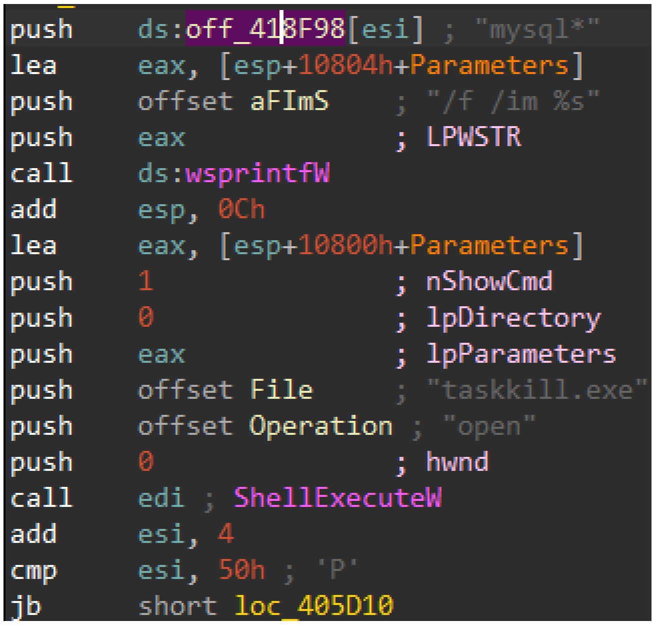


Type	Name	Hand
Desktop	\Default	0x50
Directory	\KnownDlls	0x8
Directory	\KnownDlls32	0xc
Directory	\KnownDlls32	0x18
Directory	\Sessions\1\BaseNamedObjects	0x90
File	C:\Windows	0x10
File	C:\Users\dontknow\Desktop	0x1c
Key	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options	0x4
Key	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options	0x14
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions	0x20
Key	HKLM\SYSTEM\ControlSet001\Control\SESSION MANAGER	0x24
Key	HKLM	0x3c
Key	HKLM\SYSTEM\ControlSet001\Control\NetworkProvider\HwOrder	0x98
Mutant	\Sessions\1\BaseNamedObjects\HelloKittyMutex	0xa4
WindowStation	\Sessions\1\Windows\WindowStations\WinSta0	0x4c
WindowStation	\Sessions\1\Windows\WindowStations\WinSta0	0x54

Figure 3 mutex

It is done to prevent malware from running more than one process of itself.

Now the malware tries to run `taskkill.exe` in a loop and kills security software, database servers and backup software it's a huge list, below figure shows the loop.

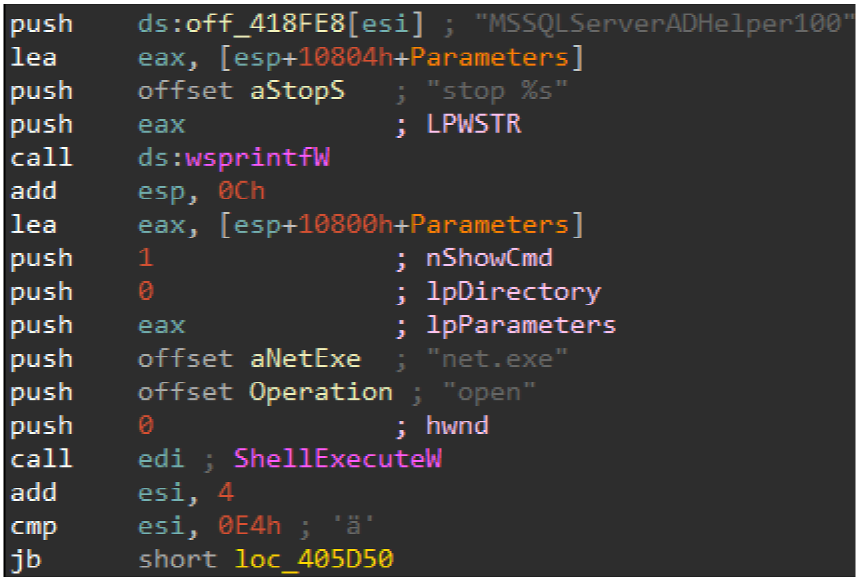


```
push    ds:off_418F98[esi] ; "mysql*"
lea     eax, [esp+10804h+Parameters]
push    offset aFImS     ; "/f /im %s"
push    eax              ; LPWSTR
call    ds:wsprintfW
add     esp, 0Ch
lea     eax, [esp+10800h+Parameters]
push    1                ; nShowCmd
push    0                ; lpDirectory
push    eax              ; lpParameters
push    offset File      ; "taskkill.exe"
push    offset Operation ; "open"
push    0                ; hwnd
call    edi ; ShellExecuteW
add     esi, 4
cmp     esi, 50h ; 'P'
jb      short loc_405D10
```

Figure 4 loop of taskkill.exe

This will end up in command equal to `C:\Windows\System32\taskkill.exe" /f /im mysql`

It also tries to stop windows services using `net.exe` in same way below figure shows the loop.



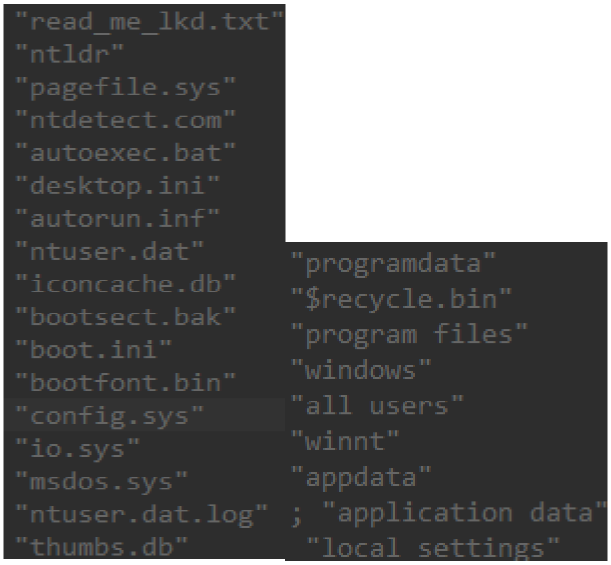
```
push    ds:off_418FE8[esi] ; "MSSQLServerADHelper100"
lea     eax, [esp+10804h+Parameters]
push    offset aStopS    ; "stop %s"
push    eax              ; LPWSTR
call    ds:wsprintfW
add     esp, 0Ch
lea     eax, [esp+10800h+Parameters]
push    1                ; nShowCmd
push    0                ; lpDirectory
push    eax              ; lpParameters
push    offset aNetExe   ; "net.exe"
push    offset Operation ; "open"
push    0                ; hwnd
call    edi ; ShellExecuteW
add     esi, 4
cmp     esi, 0E4h ; 'ä'
jb      short loc_405D50
```

Figure 5 net.exe loop

Command equivalent to it is `"C:\Windows\System32\net.exe" stop MSSQLServerADHelper100.`

Whitelist

Once it drops ransom note in each folder it starts encryption routine. But the malware whitelist the ransom note and few files and folders as show in the figures 6.

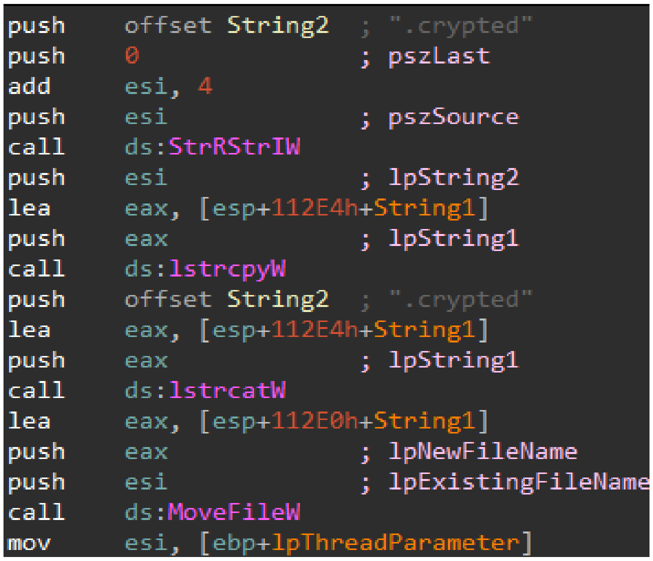


```
"read_me_lkd.txt"
"ntldr"
"pagefile.sys"
"ntdetect.com"
"autoexec.bat"
"desktop.ini"
"autorun.inf"
"ntuser.dat"
"iconcache.db"
"bootsect.bak"
"boot.ini"
"bootfont.bin"
"config.sys"
"io.sys"
"msdos.sys"
"ntuser.dat.log"
"thumbs.db"
```

```
"programdata"
"$recycle.bin"
"program files"
"windows"
"all users"
"winnt"
"appdata"
; "application data"
 "local settings"
```

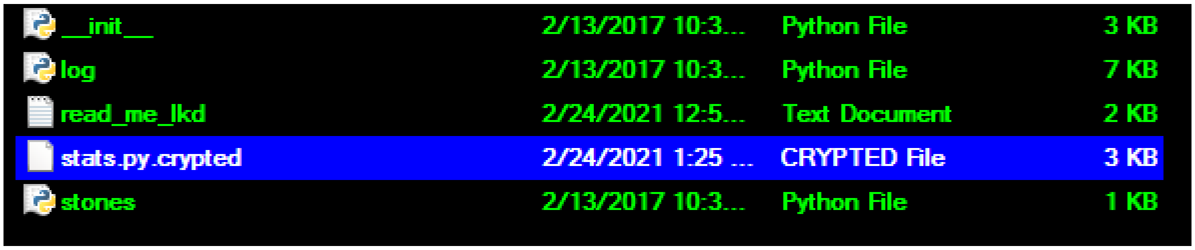
Figure 6 whitelist files and folders

Malware reads the contents of the file and writes encrypted contents to the file, using `MoveFileW` API it changes the extension of the file to `.crypted.`



```
push    offset String2  ; ".crypted"
push    0               ; pszLast
add     esi, 4
push    esi             ; pszSource
call    ds:StrRStrIW
push    esi             ; lpString2
lea     eax, [esp+112E4h+String1]
push    eax             ; lpString1
call    ds:lstrcpyW
push    offset String2  ; ".crypted"
lea     eax, [esp+112E4h+String1]
push    eax             ; lpString1
call    ds:lstrcatW
lea     eax, [esp+112E0h+String1]
push    eax             ; lpNewFileName
push    esi             ; lpExistingFileName
call    ds:MoveFileW
mov     esi, [ebp+lpThreadParameter]
```

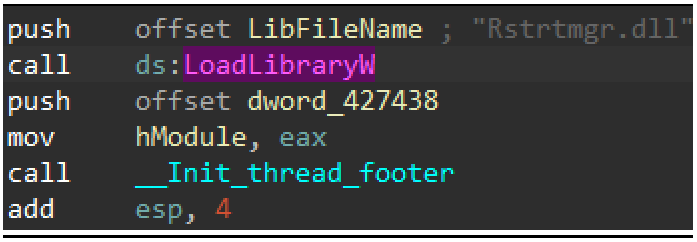
Figure 7loop for changing extension



```
__init__             2/13/2017 10:3...   Python File        3 KB
log                  2/13/2017 10:3...   Python File        7 KB
read_me_lkd          2/24/2021 12:5...   Text Document      2 KB
stats.py.crypted     2/24/2021 1:25 ...  CRYPTED File       3 KB
stones               2/13/2017 10:3...   Python File        1 KB
```

Figure 8 encrypted file with changed extension

If hellokitty comes across a locked file it uses Windows Restart Manager API's to terminate process or services keeping the file open so it can encrypt it. Below figure shows the dll being loaded using `LoadLibraryW`



```
push    offset LibFileName ; "Rstrtmgr.dll"
call    ds:LoadLibraryW
push    offset dword_427438
mov     hModule, eax
call    __Init_thread_footer
add     esp, 4
```

Figure 9 loading Rstrtmgr.dll

IOC's

T1035 - Service Execution

T1082- System Information Discovery

T1012- Query Registry

T1007- System Service Discovery

T1486- Data Encrypted for Impact

Hashes

fa722d0667418d68c4935e1461010a8f730f02fa1f595ee68bd0768fd5d1f8bb

9a7daafc56300bd94ceef23eac56a0735b63ec6b9a7a409fb5a9b63efe1aa0b0

78afe88dbfa9f7794037432db3975fa057eae3e4dc0f39bf19f2f04fa6e5c07c

References

https://www.bleepingcomputer.com/news/security/hellokitty-ransomware-behind-cd-projekt-red-cyberattack-data-theft/