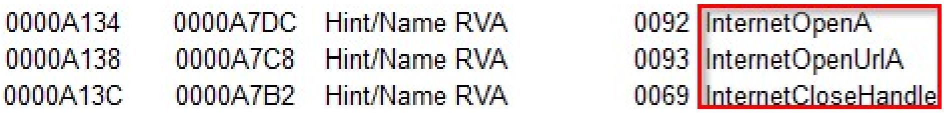
Malware Analysis: wannacry.exe

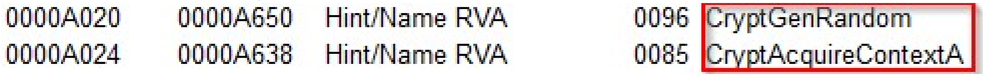
Static Analysis:

- **SHA-256 Hash**: 24D004A104D4D54034DBCFFC2A4B19A11F39008A575AA614EA04703480B1022C
- **VirusTotal Detection**: 69/72 flagged as malicious (Ransomware Trojan)
- **File Type**: Executable
- **Compiler Timestamp**: Sat Nov 20 09:03:08 2010 | UTC
- **File Architecture**: 32-bit
- **Initial File Size**: 3,723,264 bytes
- **Virtual Size**: 8BCA
- **Raw Size**: 9000
- **File Packing**: Not packed
- **Suspicious imports**: API internet related calls:



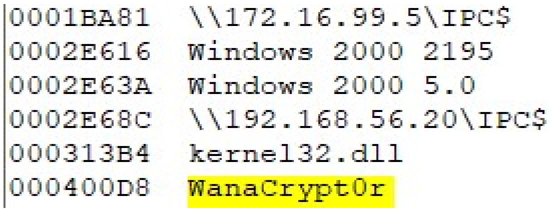
```
0000A134    0000A7DC    Hint/Name RVA         0092 InternetOpenA
0000A138    0000A7C8    Hint/Name RVA         0093 InternetOpenUrlA
0000A13C    0000A7B2    Hint/Name RVA         0069 InternetCloseHandle
```

API functions used by ransomware:



```
0000A020    0000A650    Hint/Name RVA         0096 CryptGenRandom
0000A024    0000A638    Hint/Name RVA         0085 CryptAcquireContextA
```

- **Suspicious strings**: floss didn't find any suspicious strings, but strings found some:

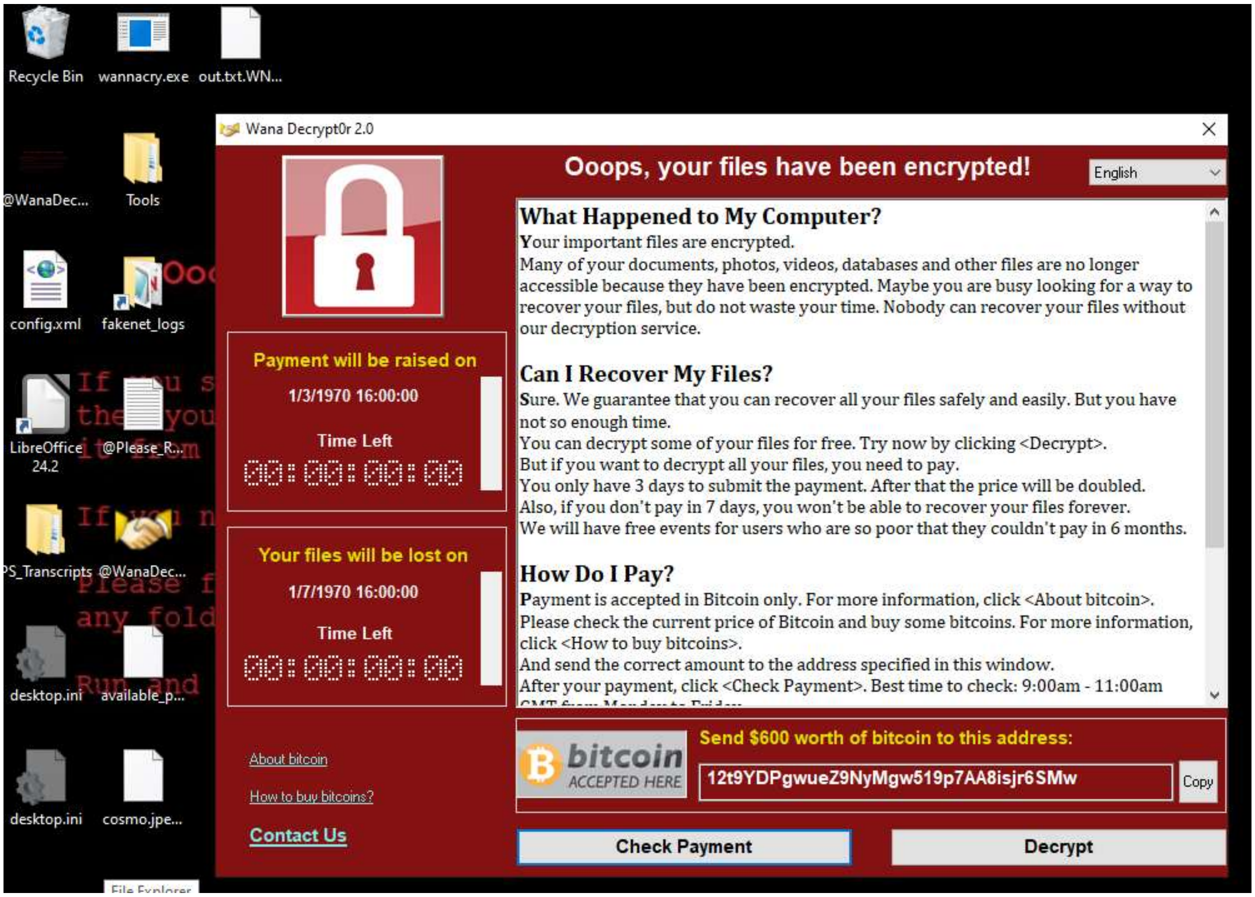


```
0001BA81   \\172.16.99.5\IPC$
0002E616   Windows 2000 2195
0002E63A   Windows 2000 5.0
0002E68C   \\192.168.56.20\IPC$
000313B4   kernel32.dll
000400D8   WanaCrypt0r
```

Dynamic Analysis:

Upon execution, the malware initiates the following actions:

1. The malware encrypts every file on the PC :



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

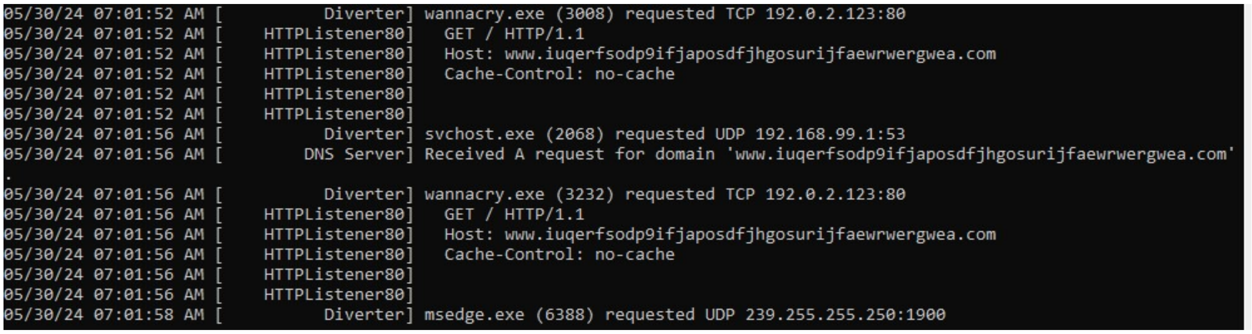
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Payment will be raised on
1/3/1970 16:00:00
Time Left
00:00:00:00

Your files will be lost on
1/7/1970 16:00:00
Time Left
00:00:00:00

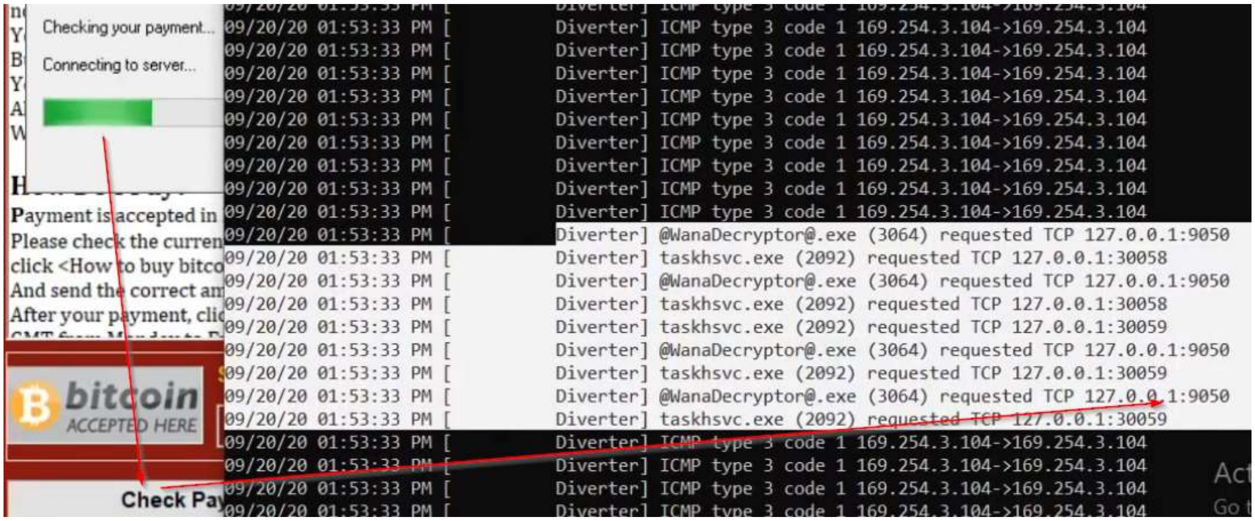
Send $600 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

2. Wannacry request long domain that is set as a kill switch, if the domain doesn’t exist then the malware continues to operate:



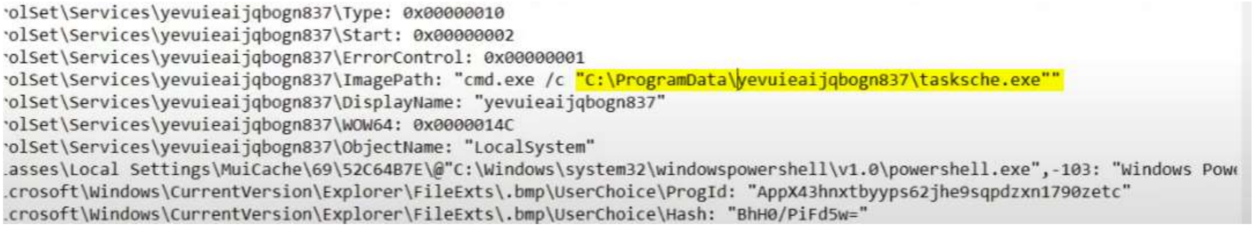
```
05/30/24 07:01:52 AM [          Diverter] wannacry.exe (3008) requested TCP 192.0.2.123:80
05/30/24 07:01:52 AM [    HTTPListener80]   GET / HTTP/1.1
05/30/24 07:01:52 AM [    HTTPListener80]   Host: www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
05/30/24 07:01:52 AM [    HTTPListener80]   Cache-Control: no-cache
05/30/24 07:01:52 AM [    HTTPListener80]
05/30/24 07:01:52 AM [    HTTPListener80]
05/30/24 07:01:56 AM [          Diverter] svchost.exe (2068) requested UDP 192.168.99.1:53
05/30/24 07:01:56 AM [        DNS Server] Received A request for domain 'www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com'
.
05/30/24 07:01:56 AM [          Diverter] wannacry.exe (3232) requested TCP 192.0.2.123:80
05/30/24 07:01:56 AM [    HTTPListener80]   GET / HTTP/1.1
05/30/24 07:01:56 AM [    HTTPListener80]   Host: www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
05/30/24 07:01:56 AM [    HTTPListener80]   Cache-Control: no-cache
05/30/24 07:01:56 AM [    HTTPListener80]
05/30/24 07:01:56 AM [    HTTPListener80]
05/30/24 07:01:58 AM [          Diverter] msedge.exe (6388) requested UDP 239.255.255.250:1900
```

3. When "Check payment" button is clicked the malware tries connecting to local loopback on port 9050. Unfortunately we can't discover the real domain that the malware connected to check the payment or it was never really checked and the victims that had pay didn't retrieve their files back



```
09/20/20 01:53:33 PM [          Diverter] ICMP type 3 code 1 169.254.3.104->169.254.3.104
09/20/20 01:53:33 PM [          Diverter] ICMP type 3 code 1 169.254.3.104->169.254.3.104
09/20/20 01:53:33 PM [          Diverter] ICMP type 3 code 1 169.254.3.104->169.254.3.104
09/20/20 01:53:33 PM [          Diverter] ICMP type 3 code 1 169.254.3.104->169.254.3.104
09/20/20 01:53:33 PM [          Diverter] ICMP type 3 code 1 169.254.3.104->169.254.3.104
09/20/20 01:53:33 PM [          Diverter] ICMP type 3 code 1 169.254.3.104->169.254.3.104
09/20/20 01:53:33 PM [          Diverter] ICMP type 3 code 1 169.254.3.104->169.254.3.104
09/20/20 01:53:33 PM [          Diverter] ICMP type 3 code 1 169.254.3.104->169.254.3.104
09/20/20 01:53:33 PM [          Diverter] ICMP type 3 code 1 169.254.3.104->169.254.3.104
09/20/20 01:53:33 PM [          Diverter] @WanaDecryptor@.exe (3064) requested TCP 127.0.0.1:9050
09/20/20 01:53:33 PM [          Diverter] taskhsvc.exe (2092) requested TCP 127.0.0.1:30058
09/20/20 01:53:33 PM [          Diverter] @WanaDecryptor@.exe (3064) requested TCP 127.0.0.1:9050
09/20/20 01:53:33 PM [          Diverter] taskhsvc.exe (2092) requested TCP 127.0.0.1:30058
09/20/20 01:53:33 PM [          Diverter] taskhsvc.exe (2092) requested TCP 127.0.0.1:30059
09/20/20 01:53:33 PM [          Diverter] @WanaDecryptor@.exe (3064) requested TCP 127.0.0.1:9050
09/20/20 01:53:33 PM [          Diverter] taskhsvc.exe (2092) requested TCP 127.0.0.1:30059
09/20/20 01:53:33 PM [          Diverter] @WanaDecryptor@.exe (3064) requested TCP 127.0.0.1:9050
09/20/20 01:53:33 PM [          Diverter] taskhsvc.exe (2092) requested TCP 127.0.0.1:30059
09/20/20 01:53:33 PM [          Diverter] ICMP type 3 code 1 169.254.3.104->169.254.3.104
09/20/20 01:53:33 PM [          Diverter] ICMP type 3 code 1 169.254.3.104->169.254.3.104
09/20/20 01:53:33 PM [          Diverter] ICMP type 3 code 1 169.254.3.104->169.254.3.104
09/20/20 01:53:33 PM [          Diverter] ICMP type 3 code 1 169.254.3.104->169.254.3.104
```

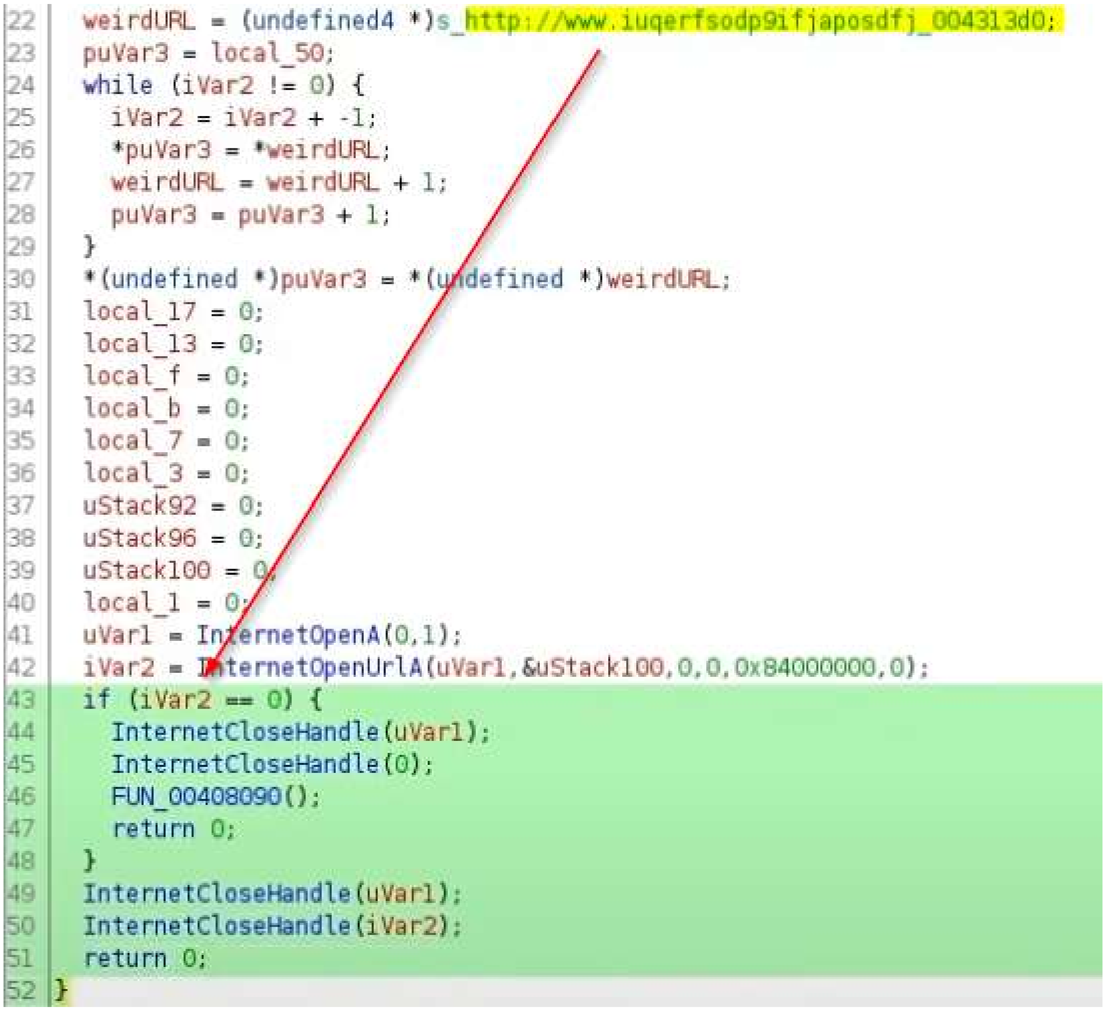
Comparing registry keys using Regshot gives new insights to malware behavior:



```
·olSet\Services\yevuieaijqbogn837\Type: 0x00000010
·olSet\Services\yevuieaijqbogn837\Start: 0x00000002
·olSet\Services\yevuieaijqbogn837\ErrorControl: 0x00000001
·olSet\Services\yevuieaijqbogn837\ImagePath: "cmd.exe /c "C:\ProgramData\yevuieaijqbogn837\tasksche.exe""
·olSet\Services\yevuieaijqbogn837\DisplayName: "yevuieaijqbogn837"
·olSet\Services\yevuieaijqbogn837\WOW64: 0x0000014C
·olSet\Services\yevuieaijqbogn837\ObjectName: "LocalSystem"
.asses\Local Settings\MuiCache\69\52C64B7E\@"C:\Windows\system32\windowspowershell\v1.0\powershell.exe",-103: "Windows Powe
.crosoft\Windows\CurrentVersion\Explorer\FileExts\.bmp\UserChoice\ProgId: "AppX43hnxtbyyps62jhe9sqpdzxn1790zetc"
.crosoft\Windows\CurrentVersion\Explorer\FileExts\.bmp\UserChoice\Hash: "BhH0/PiFd5w="
```

Malware runs command shell to set a new registry key highlighted above, it is hidden directory with purpose to maintain persistence on the end point

Debugger & decompiler analysis of wannacry:



```
  weirdURL = (undefined4 *)s_http://www.iuqerfsodp9ifjaposdfj_004313d0;
  puVar3 = local_50;
  while (iVar2 != 0) {
    iVar2 = iVar2 + -1;
    *puVar3 = *weirdURL;
    weirdURL = weirdURL + 1;
    puVar3 = puVar3 + 1;
  }
  *(undefined *)puVar3 = *(undefined *)weirdURL;
  local_17 = 0;
  local_13 = 0;
  local_f = 0;
  local_b = 0;
  local_7 = 0;
  local_3 = 0;
  uStack92 = 0;
  uStack96 = 0;
  uStack100 = 0;
  local_1 = 0;
  uVar1 = InternetOpenA(0,1);
  iVar2 = InternetOpenUrlA(uVar1,&uStack100,0,0,0x84000000,0);
  if (iVar2 == 0) {
    InternetCloseHandle(uVar1);
    InternetCloseHandle(0);
    FUN_00408090();
    return 0;
  }
  InternetCloseHandle(uVar1);
  InternetCloseHandle(iVar2);
  return 0;
}
```

Wannacry analysis using Ghidra confirms that the malware first checks whether the domain exists and if so then closes the socket and terminates meaning that it is indeed a kill switch. Otherwise main payload functions is called and the encryption process begins along with the timer.