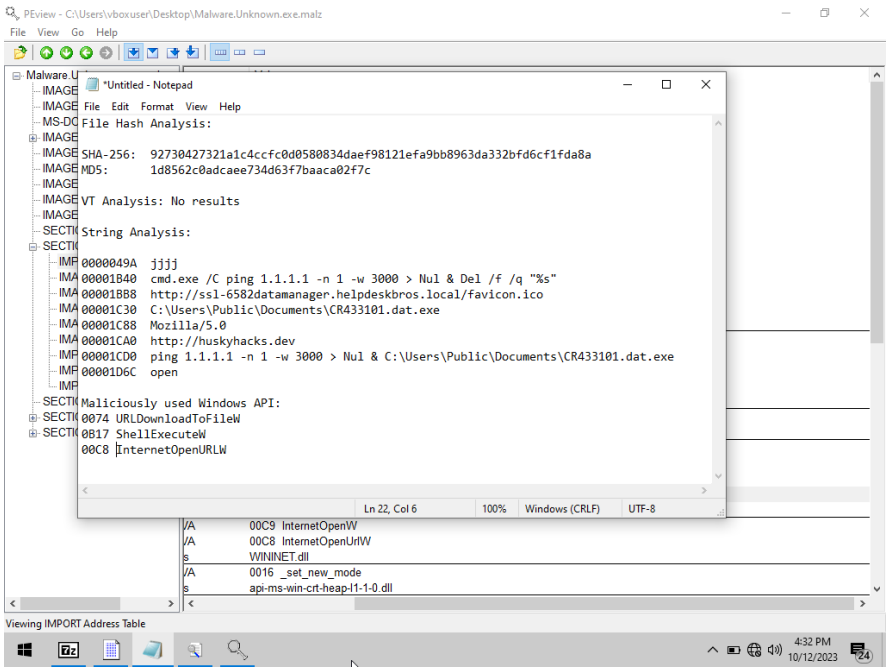
Dynamic analysis

1. Analysis on WannaCry ransomware

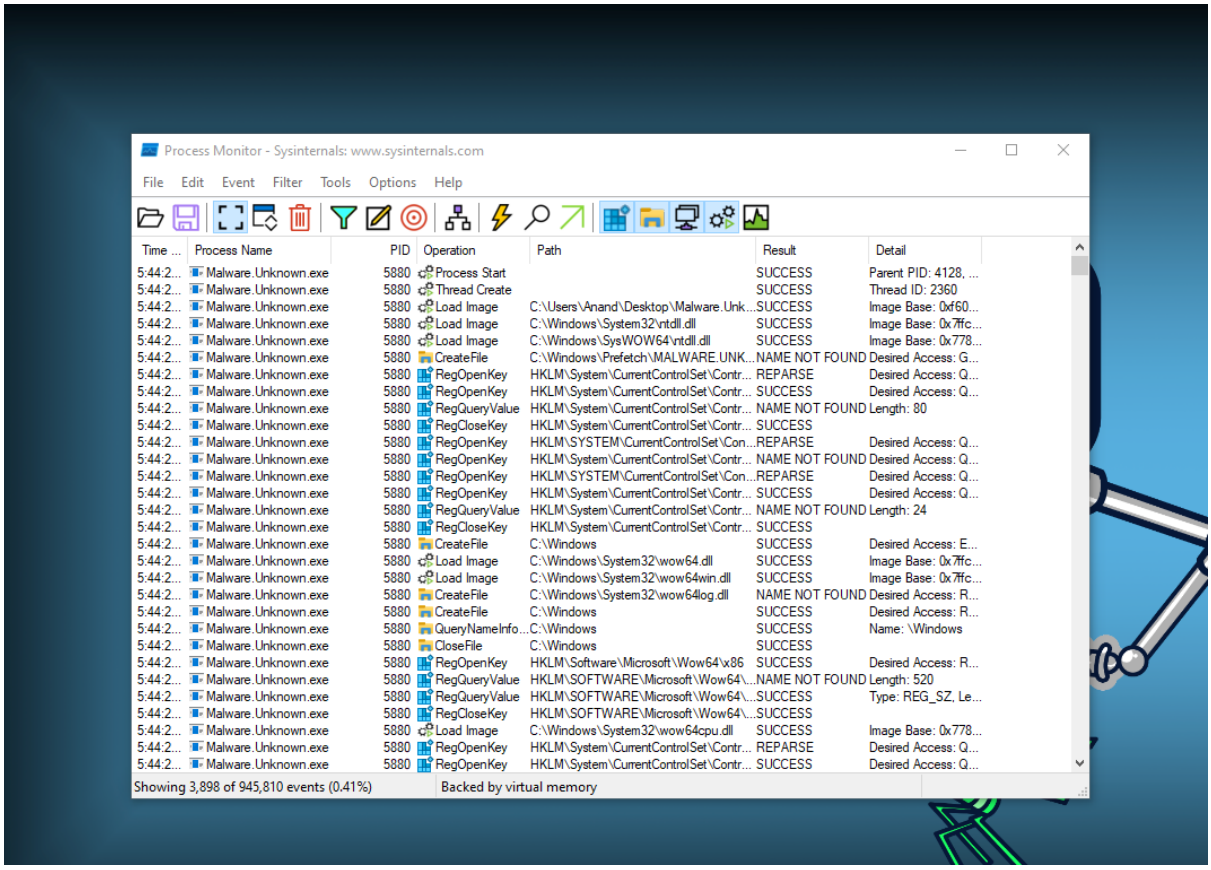


URL request found in static analysis.

Wireshark results in URL request on running the malware

```
Host: www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com\r\n
Cache-Control: no-cache\r\n
\r\n
[Full request URI: http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com/]
[HTTP request 1/1]
[Response in frame: 1328]
```

Filtered http request on wireshark .



Procmon filtered by Process name for Ransomware.wannacry.ex

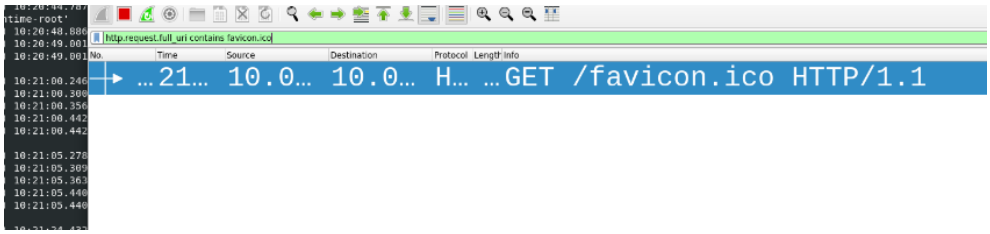
2. Analysis on an unknown malware sample.

On running malware without internet simulation activated,

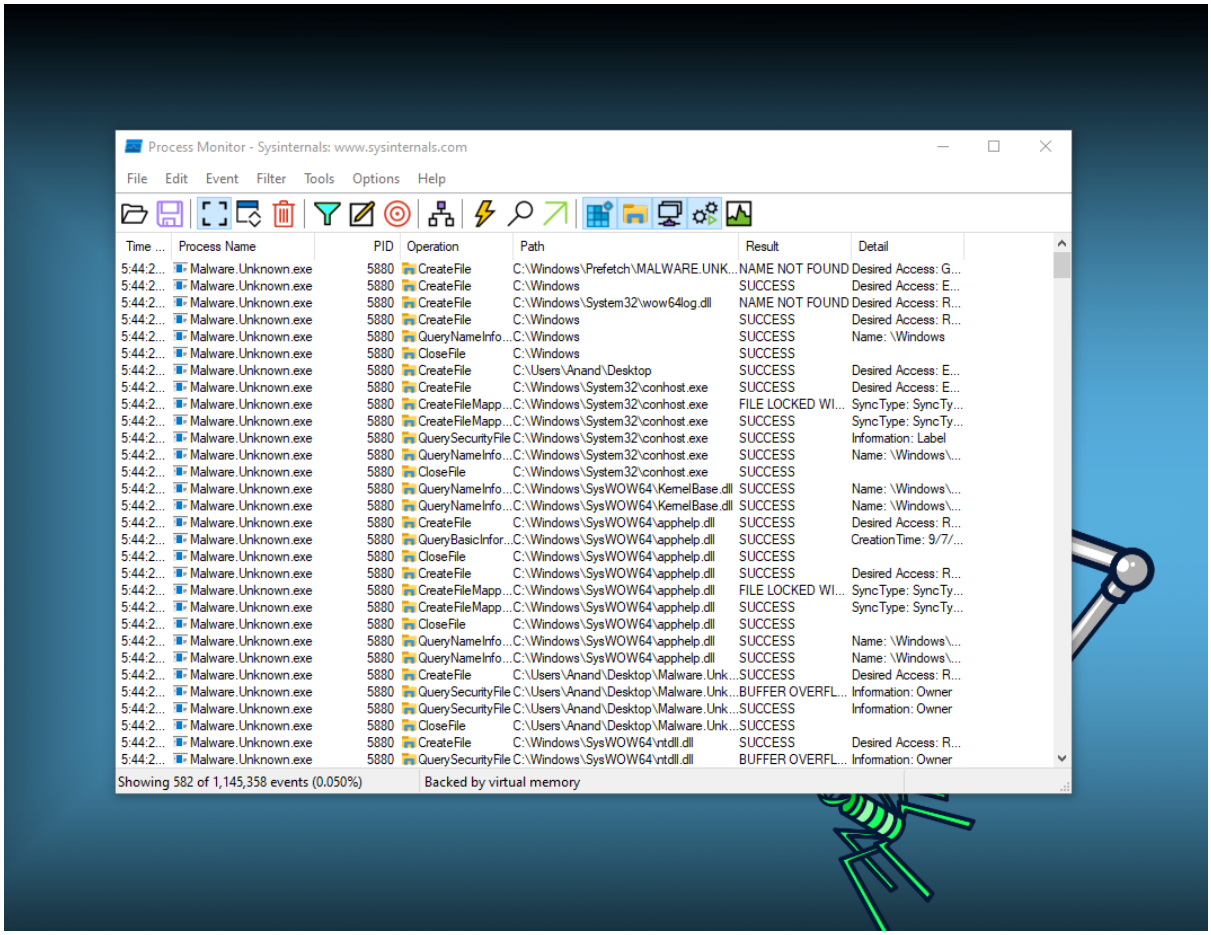
Malware pings for a count of 1 and deletes itself,

On running malware with internet simulation activated,

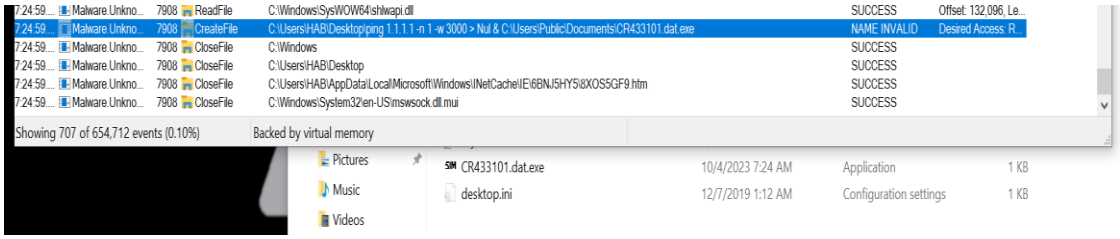
Request to URL found in the strings output goes through when malware is run,



Request to URL found in the strings output goes through when malware is run



Running the malware adds a file to public documents,



Running the malware adds a file to public documents

Process flow of current malware sample

- If URL exists:
  - Download file (favicon.ico)
  - Writes to disk (CR433101.dat.exe)
  - Run favicon.ico (CR433101.dat.exe)
- If URL does not exist:
  - Delete from disk

Do not run