NetWalker Ransomware Report

Archived: 2026-04-05 12:58:21 UTC

Written by: Omer Solomon

EXECUTIVE SUMMARY

With the world dealing with the Coronavirus crisis, cyber-criminals are taking advantage of the situation to spread new variants of ransomware via Coronavirus phishing campaigns.

The newest of these variants is the NetWalker.

Home-users, enterprises, government agencies and health organizations have reported to be attacked by NetWalker.

Two widely reported attacks using NetWalker were on the Toll Group, an Australian transportation and logistics company, and the Illinois Champaign-Urbana Public-Health District (CUPHD) website, which temporarily prevented health district employees from accessing certain files.

The attack forced the FBI and the U.S Department of Homeland Security step in, showing the severity of this crisis and how important it is to be familiar with this variant in order to prevent further attacks.

This is part of an extensive series of guides about Ransomware Protection

Overview of the NetWalker Payload

NetWalker ransomware was discovered in August 2019, it was initially named Mailto based on the extension that was appended to encrypted files, but analysis of one of its decryptors indicates that its name is NetWalker.

NetWalker compromises the network and encrypts all Windows devices connected to it.

When executed, NetWalker uses an embedded configuration that includes a ransom note, ransom note file names, and various configuration options.

So far, we have noticed that NetWalker spreads itself in two ways.

One way is via a VBS script that has been attached to Coronavirus phishing emails that execute the payload of the ransomware once it’s double-clicked or by opening the office documents that contain the VBS script inside.

The second method occurs through an executable file that been spread on the network, and once it has been executed by the user, without the right guards in place, it is game over.

NetWalker Meta-Data

MD5	993b73d6490bc5a7e23e02210b317247
SHA-1	6fd314af34409e945504e166eb8cd88127c1070e
SHA-256	de04d2402154f676f757cf1380671f396f3fc9f7dbb683d9461edd2718c4e09d
Vhash	094056651d15756bz1!z
Authentihash	b2b4de7d9abc19602b5aaf5a233f19a5f79794736f510f8c47a203c0c605f016
Imphash	e82dd51b077167be63c004bed23d0c1e
SSDEEP	1536:NQVICPQRhNs3POdM0ty2XGe0W7Pbk3sPkO5M/Y8fGMNvgaN:NQ3CPAC/YM0tyAGe0WDPx9MNvg8
File type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
File size	94.00 KB (96256 bytes)

Names

WTVConverter.exe

qeSw.exe

Signature Info

Signature Verification

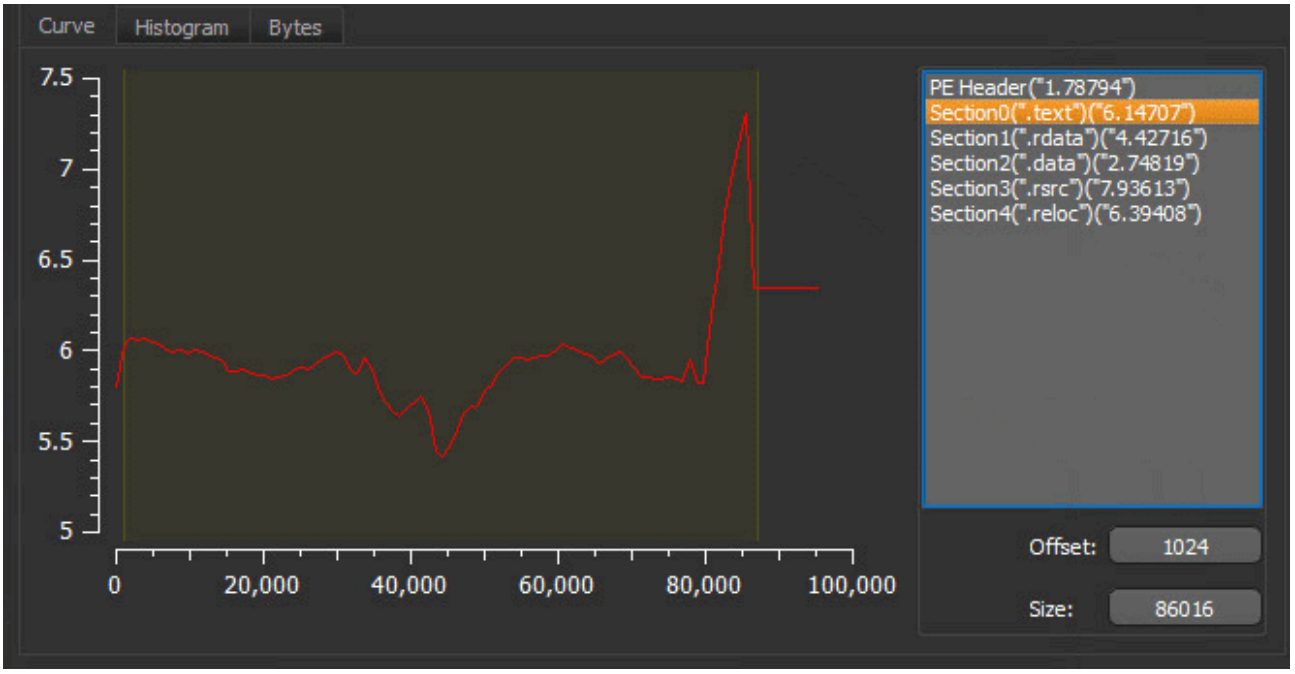
⚠ File is not signed

File Version Information

Copyright	© Microsoft Corporation. All rights reserved.
Product	Microsoft® Windows® Operating System
Description	WTV file converter
Original Name	WTVConverter.exe
Internal Name	WTVConverter.exe
File Version	6.1.7600.16385 (win7_rtm.090713-1255)

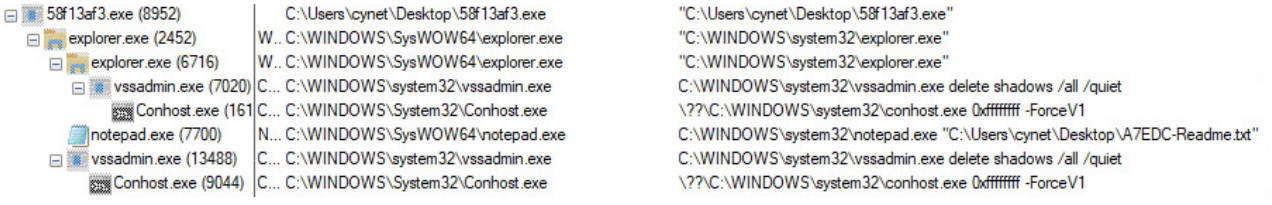
As we see above, the file impostor claims to belong to ‘Microsoft’, pretending to be legitimate and safe.

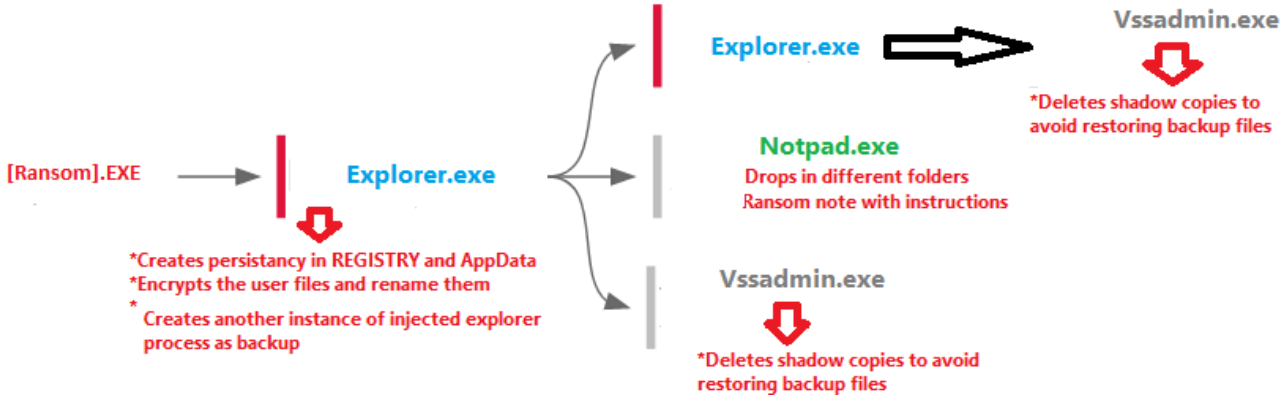
Another indicator, is the high entropy levels this executable has. We can assume that the payload hides under the ‘.rsrc’ and ‘reloc’ sections, which tells us that the attacker tries to evade traditional AV’s mechanism from detecting this file by statically file scanning on the disk which is signature-based, by compressing the file with a unique format.



Attack Flow

Once the file is executed, the following events flow will take place:

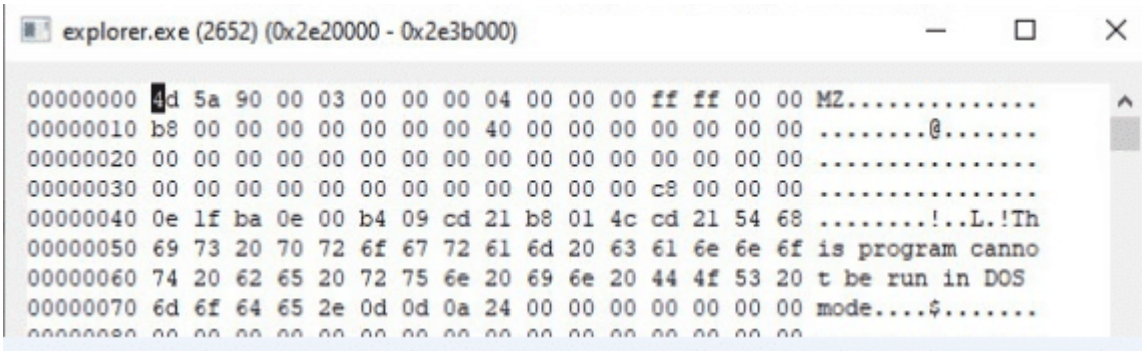




Process Hollowing Technique

The attacker uses a technique called **Process hollowing** to inject the payload into ‘explorer.exe’.
Process hollowing occurs when a process is created in a suspended state then its memory is unmapped and replaced with malicious code.

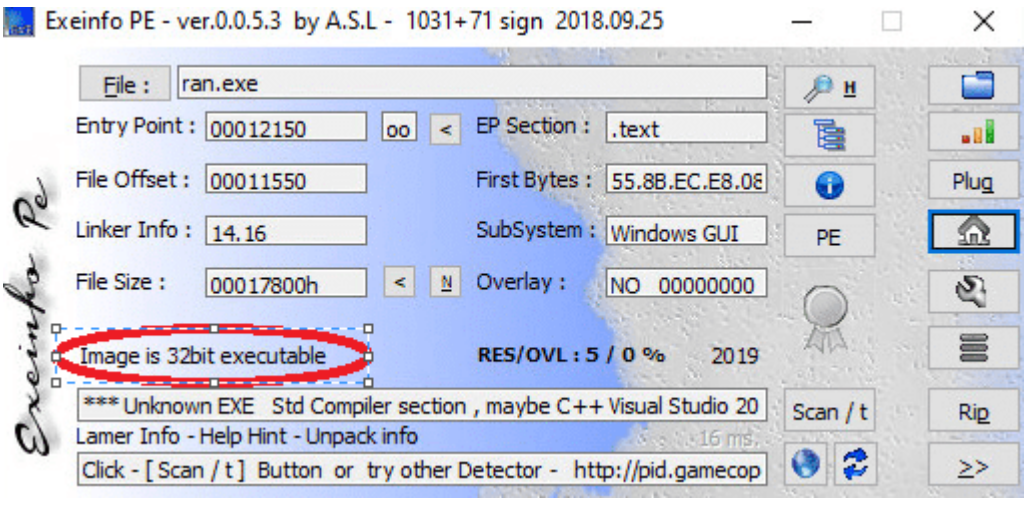
Below we can see how the injection of the payload is located inside the explorer process.



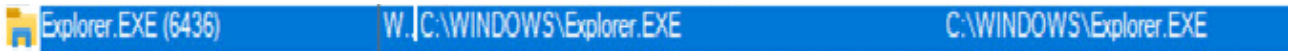
Base address	Type	Size	Protection	Use
0x6c8a1000	Image: Commit	92 kB	RX	C:\Windows\SysWOW64\rmclient.dll
0x6c391000	Image: Commit	456 kB	RX	C:\Windows\SysWOW64\twinapi.dll
0x6c361000	Image: Commit	92 kB	RX	C:\Windows\SysWOW64\dwmapi.dll
0x6c341000	Image: Commit	56 kB	RX	C:\Windows\SysWOW64\srvcli.dll
0x791000	Image: Commit	2,444 kB	RX	C:\Windows\SysWOW64\explorer.exe
0x2e20000	Mapped: Commit	108 kB	RWX	
0x4af0000	Private: Commit	8 kB	RW+G	Stack 32-bit (thread 7524)
0x3385000	Private: Commit	12 kB	RW+G	Stack (thread 7524)
0x3090000	Private: Commit	8 kB	RW+G	Stack 32-bit (thread 2600)

After the injection of the payload to the legitimate ‘explorer.exe’ process occurred it spawned a new instance of ‘explorer.exe’ and the original executable process will be killed (58f13af3.exe). When a regular user looks at their task manager, they won’t see a suspicious behavior since the payload hides under a legitimate process.

Another verification that we have for the payload injection to the explorer is the path, which is in ‘SysWOW64’ while comparing to the real explorer process that is located in WINDOWS path we can relate that to the fact that the malicious file is 32-bit and an instance of a 32bit explorer will run through the ‘SysWOW64’ folder if the operating system is 64-bit.

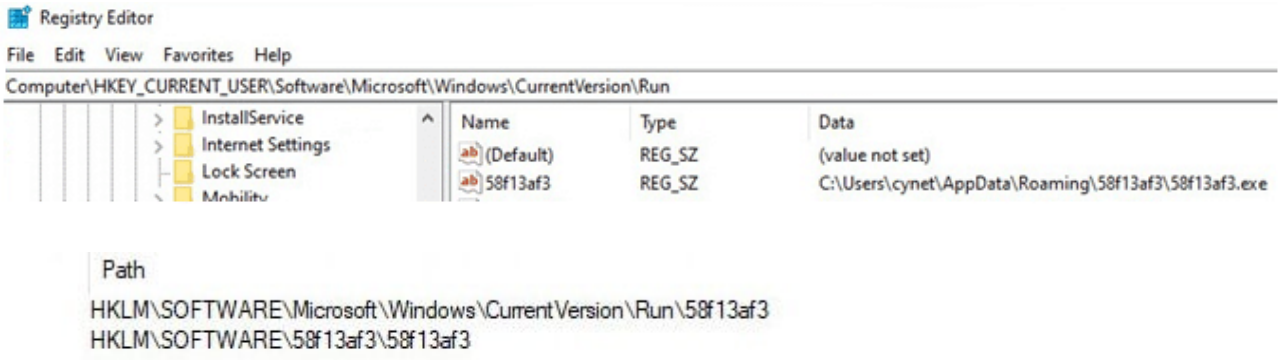


Below we can see the path of the legitimate explorer.exe process, this legitimate explorer runs from WINDOWS because it’s a 64 bit operation system like it should be.



Persistency Technique

In order to maintain the persistency of the malicious file on the user's host, the payload deletes the original executable from its location and drops it in the user 'AppData\Roaming\' folder and creates a registry key that will execute the file every time the host will startup.

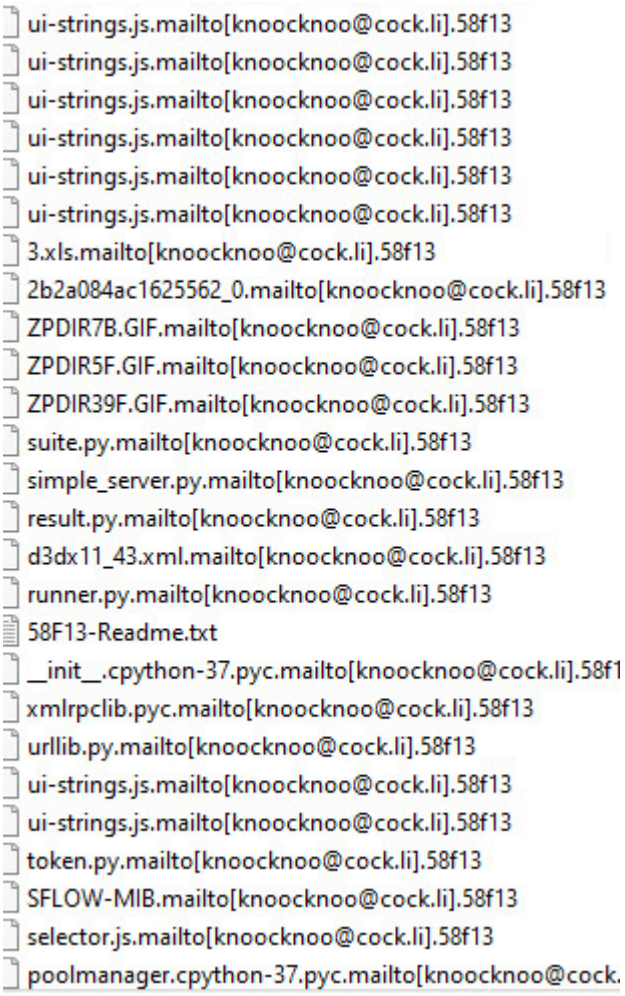


The reason that attackers like to drop the malicious files to the 'AppData' is that it's a hidden path that a regular user won't notice that there is a malicious file in it, and you don't have to have an administrator user to 'write' to this path, regular users also have 'write' permissions.

Encryption Technique

So far, we have seen the injection of the payload to the explorer and the persistency set to maintain the malware in the system.

The next step we see is related to the encryption technique, most of the files on the host are being encrypted and their extensions are being changed to 'mailto[knoocknoo@cock.li].[generated-file-name]' .



After we dig a little dipper to the payload, we found the config of the payload that contains the paths that will be excluded from encryption and a list of processes that were meant to be terminated if they exist.

For example, if a user will have a Word document running while the malware is being executed, it will be terminated immediately to avoid any encryption interruption.

software’s\processes that will be exclude from the encryption, for example:

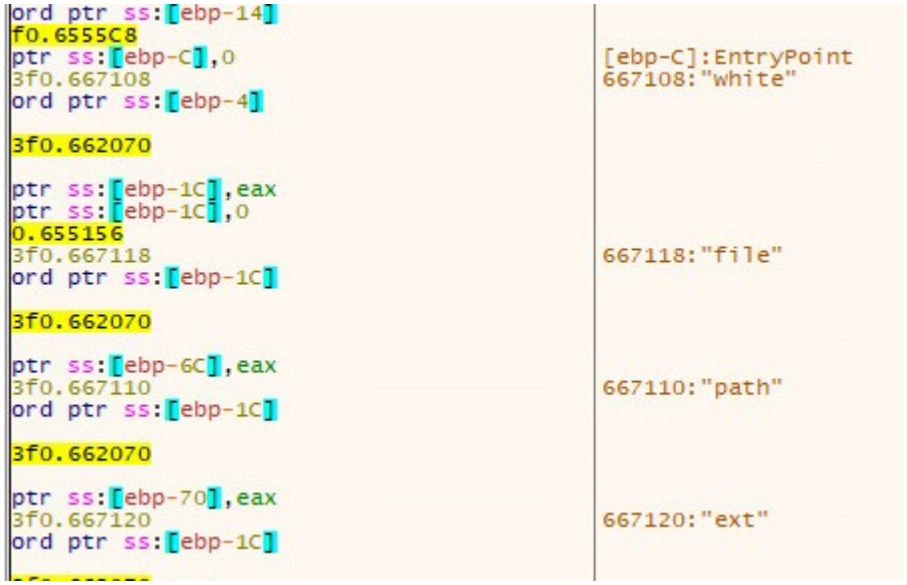
\program files\vmware, **windows defender**,*media player, etc.

Files extensions that will be exclude, for example:

‘exe’, ‘msi’, ‘ps1’, ‘cmd’, etc.

Processes that will be killed to avoid interruption in the encryption:

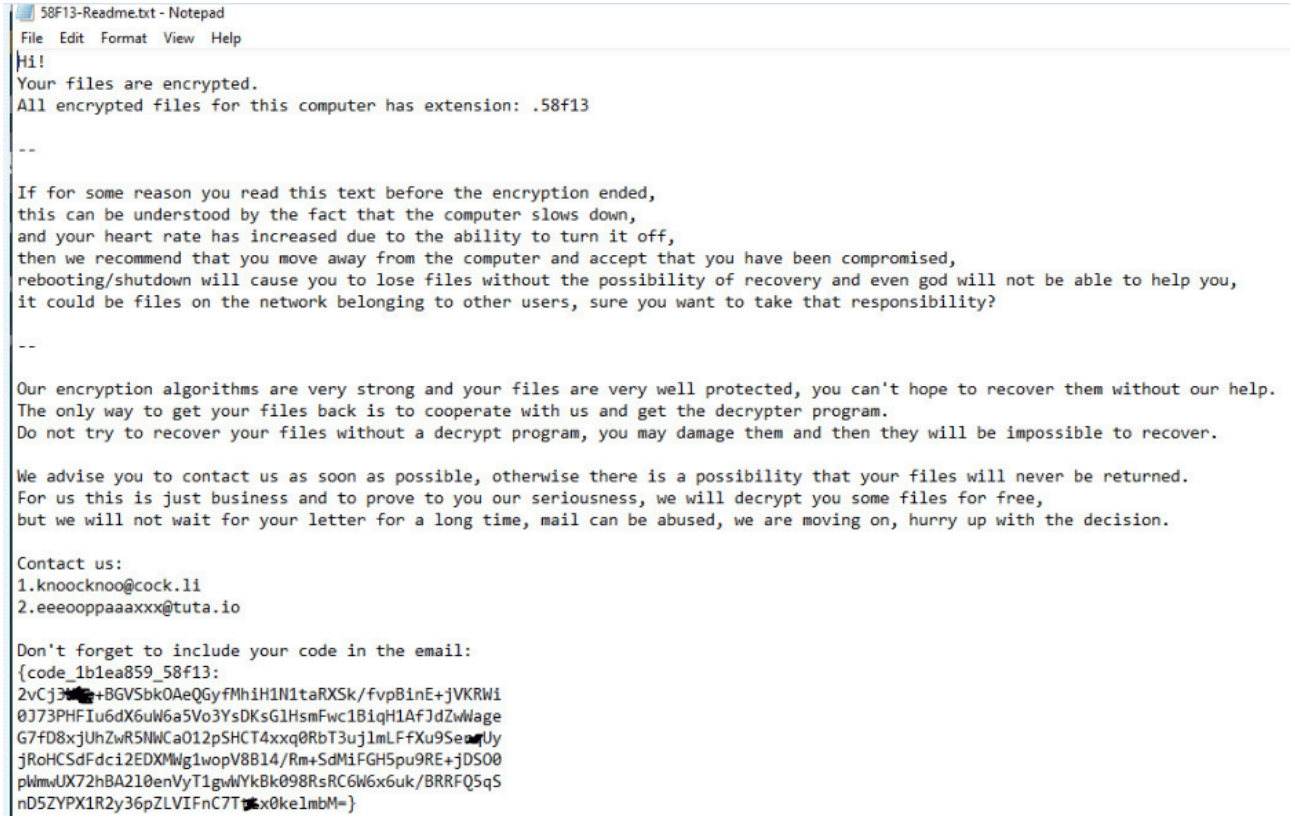
Wordpad.exe, winword.exe outlook.exe, excel.exe, oracle.exe, ntrtscan.exe, *sql*, etc.



The exception of this path combined with the list of tasks to kill was meant to keep the functionality of the host while encrypting the relevant user files smoothly and allow the user to be able to pay the ransom.

Once the files encryption is complete, a ransom note with further instructions is being dropped in each folder that contains encrypted files.

The note will include a unique code and two email addresses that belong to the attackers.



Obfuscation Technique

When we dive into the payload memory strings to locate any signs that related to the ransomware note, we find obfuscated strings.
After a deep lookup, we find the encoding type that our strings are encoded with – BASE64.

```
63 48 51 67 65 57 39 31 49 48 4E 76 62 57 55 67  cHQgeW91IHNvbWUg
5A 6D 6C 73 5A 58 4D 67 5A 6D 39 79 49 47 5A 79  ZmlsZXMgZm9yIGZy
5A 57 55 73 49 41 30 4B 59 6E 56 30 49 48 64 6C  ZWUsIA0KYnV0IHdl
49 48 64 70 62 47 77 67 62 6D 39 30 49 48 64 68  IHdpbGwgbm90IHdh
61 58 51 67 5A 6D 39 79 49 48 6C 76 64 58 49 67  aXQgZm9yIHlvdXIg
62 47 56 30 64 47 56 79 49 47 5A 76 63 69 42 68  bGV0dGVyIGZvciBh
49 47 78 76 62 6D 63 67 64 47 6C 74 5A 53 77 67  IGxvbmcgdGltZSwg
62 57 46 70 62 43 42 6A 59 57 34 67 59 6D 55 67  bWFpbCBjYW4gYmUg
59 57 4A 31 63 32 56 6B 4C 43 42 33 5A 53 42 68  YWJ1c2VkLCB3ZSBh
63 6D 55 67 62 57 39 32 61 57 35 6E 49 47 39 75  cmUgbW92aW5nIG9u
4C 43 42 6F 64 58 4A 79 65 53 42 31 63 43 42 33  LCBodXJyeSB1cCB3
61 58 52 6F 49 48 52 6F 5A 53 42 6B 5A 57 4E 70  aXRoIHRoZSBkZWNp
63 32 6C 76 62 69 34 4E 43 67 30 4B 30 4B 46 76  c2lvbi4NCg0K0KFv
62 6E 52 68 59 33 51 67 64 58 4D 36 44 51 6F 78  bnRhY3QgdXM6DQox
4C 6E 74 74 59 57 6C 73 4D 58 30 4E 43 6A 49 75  LnttYWlsMX0NCjIu
65 32 31 68 61 57 77 79 66 51 30 4B 44 51 70 45  e21haWwyfQ0KDQpE
62 32 34 6E 64 43 42 6D 62 33 4A 6E 5A 58 51 67  b24ndCBmb3JnZXQg
64 47 38 67 61 57 35 6A 62 48 56 6B 5A 53 42 35  dG8gaW5jbHVkZSB5
62 33 56 79 49 47 4E 76 5A 47 55 67 61 57 34 67  b3VyIGNvZGUgaW4g
64 47 68 6C 49 47 56 74 59 57 6C 73 4F 67 30 4B  dGhlIGVtYWlsOg0K
```

0x36eda70	26	Base64 Encode
0x36edaa0	20	MIME Tools
0x36edad0	54	Base64 Encode with Unix EOL
0x36edb20	42	Base64 Encode by line
0x36edb60	26	Base64 Decode
0x36edb90	40	Base64 Decode strict
0x36edbd0	42	Base64 Decode by line
0x36edc10	46	Quoted-printable Encode
0x36edc50	46	Quoted-printable Decode
0x36edc90	20	URL Encode
0x36edcc0	30	Full URL Encode
0x36edcf0	20	URL Decode
0x36edd20	22	SAML Decode

The ransomware note template after de-coding the strings with BASE64,

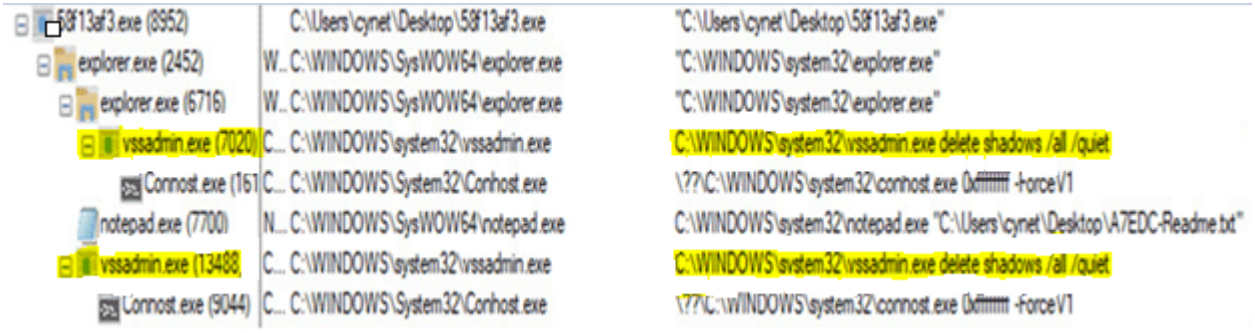
```
The only way to get your files back is to cooperate with us and get the decrypter program.
Do not try to recover your files without a decrypt program, you may damage them and then they will

We advise you to contact us as soon as possible, otherwise there is a possibility that your files will r
For us this is just business and to prove to you our seriousness, we will decrypt you some files for fr
but we will not wait for your letter for a long time, mail can be abused, we are moving on, hurry up w

Contact us:
1.{mail1}
2.{mail2}

Don't forget to include your code in the email:
{code}
```

And the variables that will be attached to the template that includes the attacker email addresses,

```
"mpk.:"LCiJ44QQcMh5P1jJtpV7XaJoMezvQc0D8bxdK97oWHM=.,"mode.:0,"thr.:1500,"spsz.:51200,"namesz.:8,"idsz.:5,
 "crmask.:".mailto[{mail1}].{id}.,"mail.:["knoocknoo@cock.li.,"eeeooppaaaxxx@tuta.io.],"lfile.:"{ID}-Readme.txt.,
```

Erasing Backup Copies

In order to erase all of the backup copies in the host, an instance of ‘vssadmin.exe’ has been spawned both from the first injected explorer and from the second instance that was spawned by the first one, both are running silently with the same command in order to erase the volume shadow copies and preventing backup copies from recovering.



NetWalker Variants in the Field

Another common way this ransomware is being distributed in the field is by phishing emails that are related to COVID-19 updates.

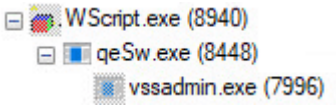
At the office, it’s common to be more aware of the kinds of emails coming through—there’s a certain vigilance about opening suspicious emails or clicking unknown links. At home, though, remote employees may let their guard down.

The attack flow starts with an email that contains an attachment that supposed to include updates and information regarding COVID-19, one of the most common ways is through an Office document such as ‘Word’ or ‘Excel’ that contains macros (series of commands and instructions that you group together as a single command to accomplish a task automatically) that will execute the ‘VBS’ script.

Double-clicking the masquerading file or opening the malicious Office document will start executing the payload by using ‘wscript.exe’ which is a service that provides scripting abilities for Windows operating system.

```
Path:       C:\WINDOWS\System32\WScript.exe
Command:    "C:\WINDOWS\System32\WScript.exe" "C:\Users\cynet\Desktop\CORONAVIRUS_COVID-19.vbs"
```

A new executable file will be dropped by the name ‘qwSw.exe’ in the user temporary directory ‘AppData/local/temp’, and will be executed.



Once the executable file is running, the following steps will occur:

- A registry key will be set to maintain persistency of the payload on the host in the following: ‘HKLM/software/’ and ‘HKCU/software/’
- All of the files will be encrypted and their extensions will be changed except for the files the attacker exclude in order to allow the host to be functional.
- Vssadmin.exe service will be launched to delete shadow copies of the user backups so files won’t be restored.

  ```
  Path:       C:\WINDOWS\system32\vssadmin.exe
  Command:    C:\WINDOWS\system32\vssadmin.exe delete shadows /all /quiet
  ```

- A ransom note will be dropped in several locations on the host with instructions.

Variants Comparison

We see two main techniques that evolve different attack flows which will eventually lead to the same result: demanding money to recover your data.

A process hollowing doesn’t occur when the VBS script is executed as compared to the ‘EXE’ file.

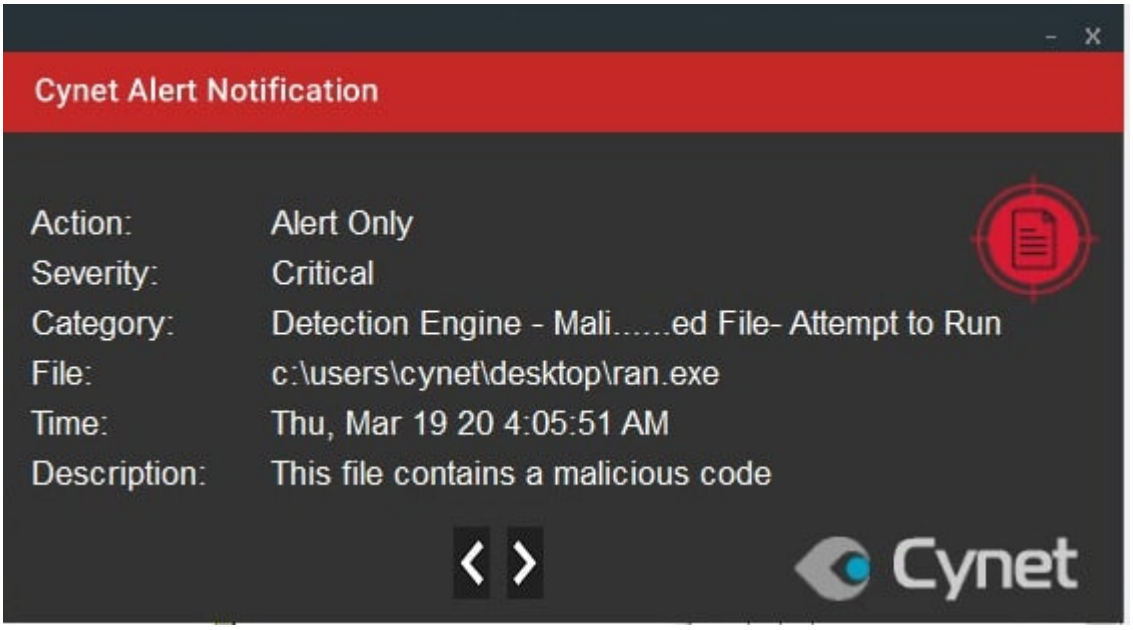
The location of the created registry keys is a bit different, the VBS payload was able to set a registry key in the ‘HKCU’ and ‘HKLM’ which includes the entire machine compared to the executable which was able to reach the ‘HKCU’ – current user only.

The rest of the events are pretty much the same.

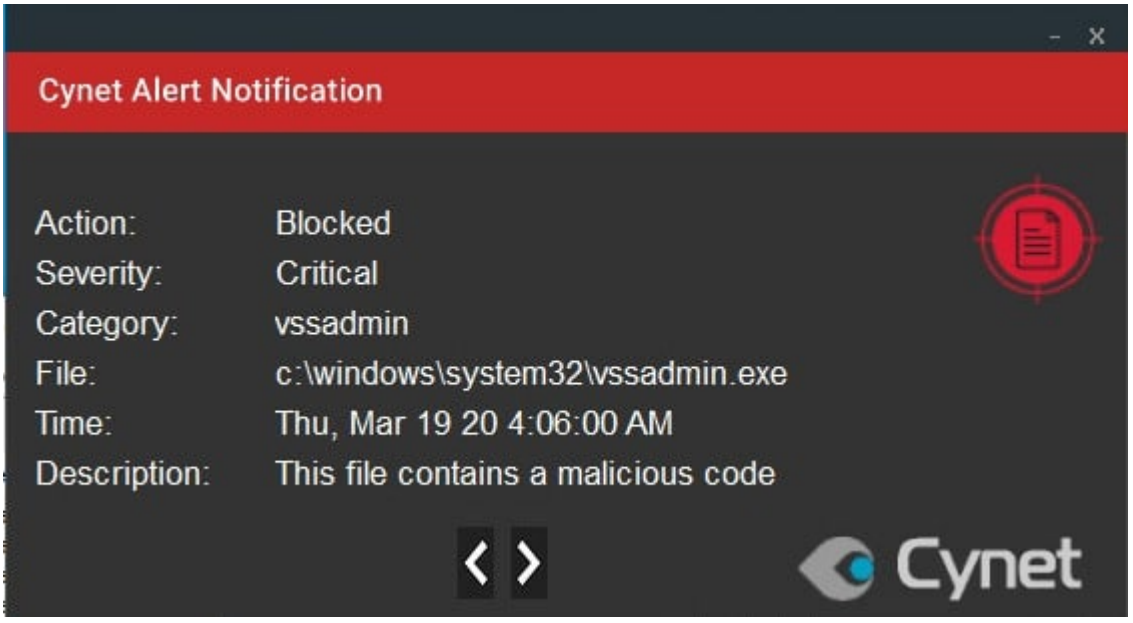
Cynet VS NetWalker

Cynet detects and prevents this attack by using several mechanisms:

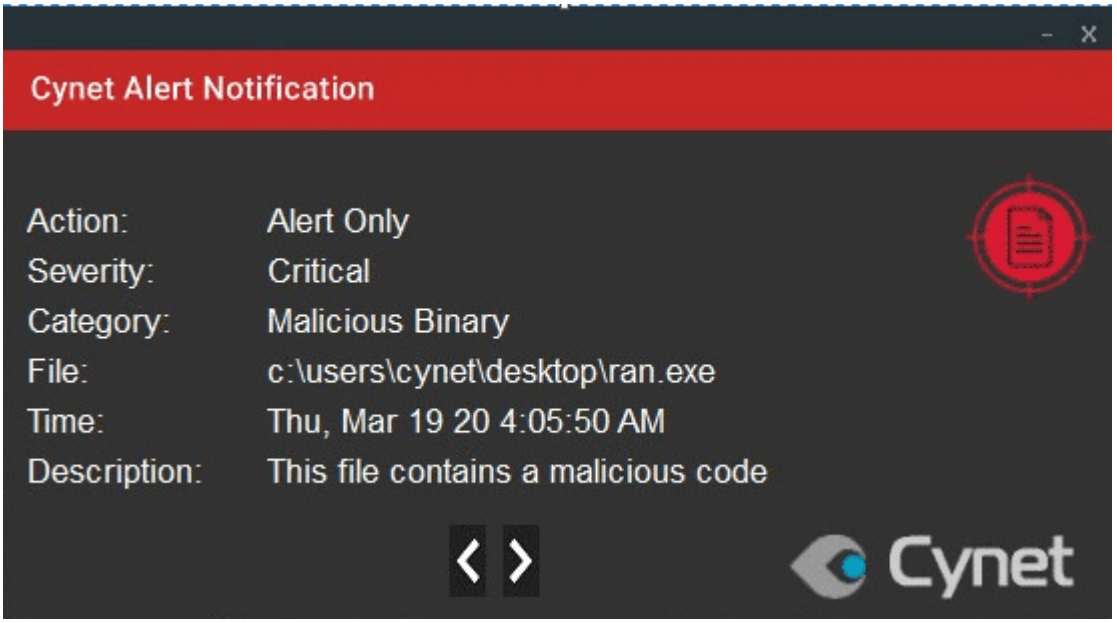
Anti-Virus/AI – This alert triggers when Cynet’s AV/AI engine detects a malicious file that was dumped on the disk.



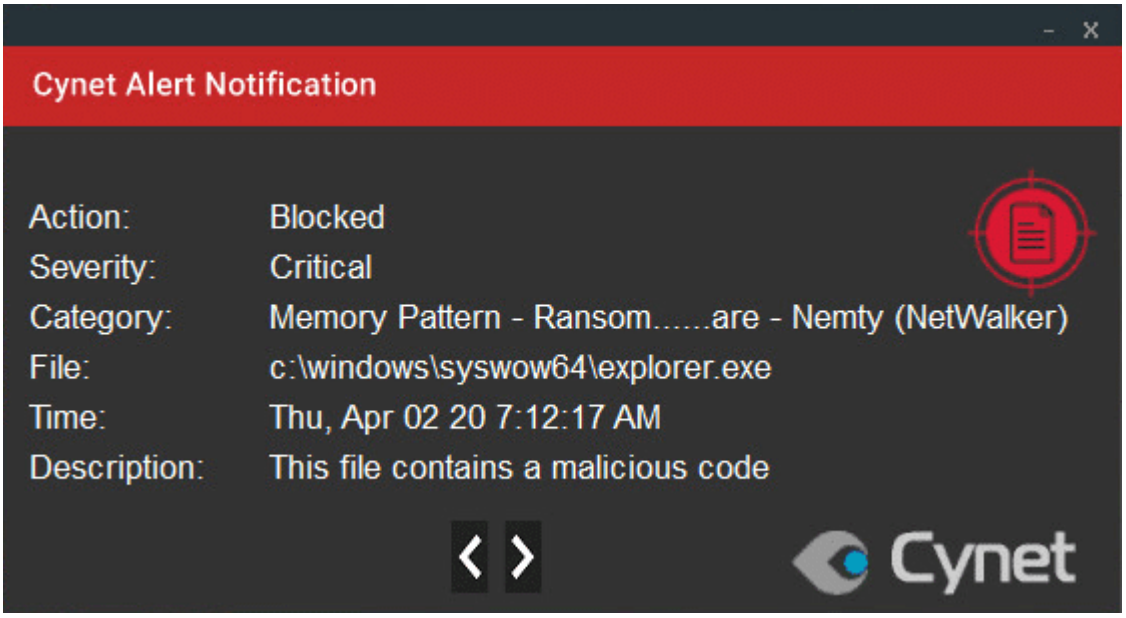
ADT – Ransomware Heuristic – This alert triggers when Cynet detects suspicious behavior which can be associated with Ransomware (such as an attempt to delete shadow copies.)



ADT – Malicious Binary – This alert triggers when Cynet detects a file that is flagged as malicious in Cynet's endpoint scanner built-in threat intelligence database.



Memory Pattern – This alert triggers when Cynet detects memory strings which are associated with Malware or with malicious files.



RECOMMENDATIONS

- In order to clean up an infected host, it crucial to revert each of the steps taken by the payload of the attack.
- Be aware of phishing emails that contain an attachments
- Clean the Registry for any of the manipulated values (once infected).
- Delete the malicious file from the paths mentioned under (once infected).
- Blacklist the SHA256 of the ransomware.
- Enabling the heuristic, AV and driver mechanisms.
- If necessary – format the host and install a clean version of Windows (once infected).

INDICATORS OF COMPROMISE

Type	Indicator
Registry Keys	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run**56f13af3**[1] HKCU\software**56f13af3****56f13af3**[1] HKCU\software\classes\virtualstore\machine\software\ 1. "**56f13af3**" – 8 Randomized characters.
Payload instance locations	C:\User\AppData\Local\Temp****.exe C:\User\AppData\Roaming********.exe
Ransom note names	{ID} – Readme.txt (e.g. 58f13-Readme.txt)
Emails related to the attacker	{Random}@cock.li {Random}@tuta.io
SHA256's for example	ad8d379a4431cabd079a1c34add903451e11f06652fe28d3f3edb6c469c43893 f69fb7049f7a75f75c3a6bba86741b8ccdd28dbf7fe65bc0c7700c3905447512 d950a94534129202aa308f22d6c3d33f71af884d5556671a2b7f6ba8994cc995 1f327163478eff3a64a7af170098c10a482df67fd9454b5f64078be516b200f1 9f9027b5db5c408ee43ef2a7c7dd1aecbdb244ef6b16d9aafb599e8c40368967 8639825230d5504fd8126ed55b2d7aeb72944ffe17e762801aab8d4f8f880160 c414bbb789af8e3fb93b33344b31f1991582ec0f06558b29a3178d2b02465c72 de04d2402154f676f757cf1380671f396f3fc9f7dbb683d9461edd2718c4e09d

Source: https://www.cynet.com/attack-techniques-hands-on/netwalker-ransomware-report/