RANSOMWARE
ARCHITECTURE

Malware

Malicious + Software

How it spreads

- Virus
- Worm
- Trojan

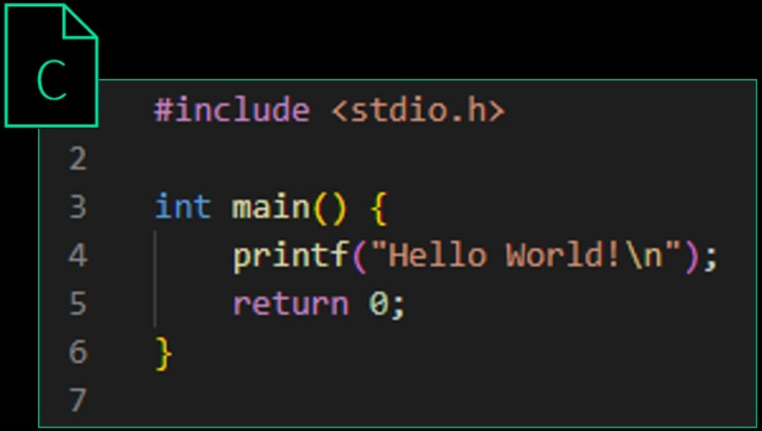
What it does

- Ransomware
- Spyware
- Adware
- Backdoor
- Cryptojacking

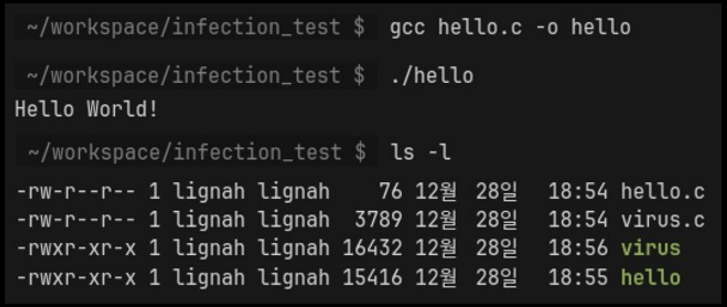
Where it entered

- Trojanized Software
- Phishing Email
- Removable Media
- MitM
- Drive-by Download
- Supply Chain Attack

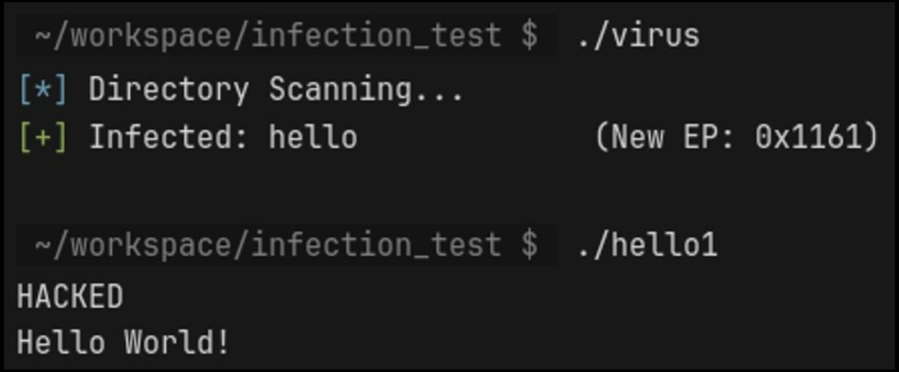
Virus



```c
#include <stdio.h>

int main() {
    printf("Hello World!\n");
    return 0;
}

```



```
~/workspace/infection_test $  gcc hello.c -o hello

~/workspace/infection_test $  ./hello
Hello World!

~/workspace/infection_test $  ls -l
-rw-r--r-- 1 lignah lignah    76 12월  28일   18:54 hello.c
-rw-r--r-- 1 lignah lignah  3789 12월  28일   18:54 virus.c
-rwxr-xr-x 1 lignah lignah 16432 12월  28일   18:56 virus
-rwxr-xr-x 1 lignah lignah 15416 12월  28일   18:55 hello
```



```
 ~/workspace/infection_test $  ./virus
[*] Directory Scanning...
[+] Infected: hello             (New EP: 0x1161)

 ~/workspace/infection_test $  ./hello1
HACKED
Hello World!
```

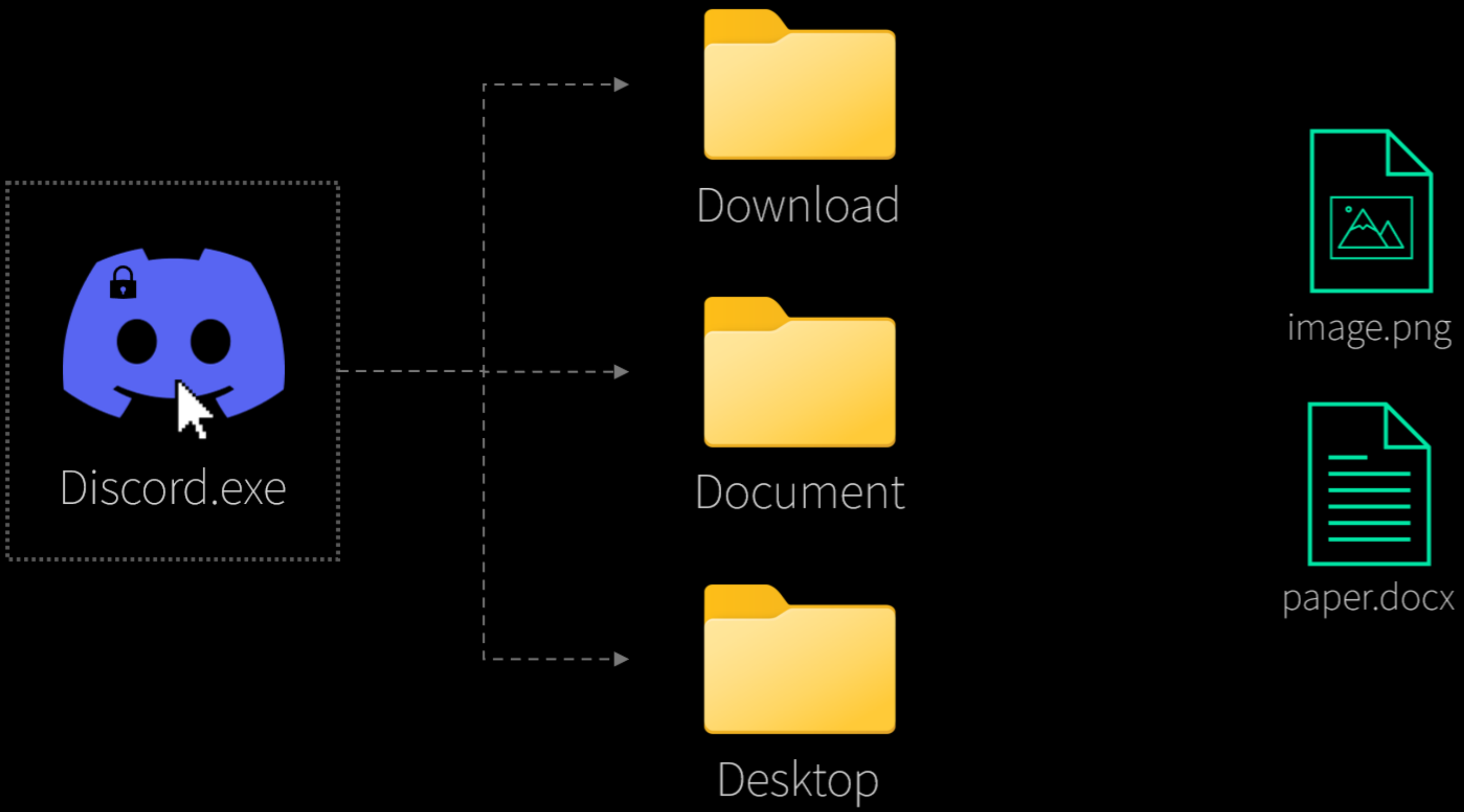
Sys Destruction

Data leakage

Cryptojacking

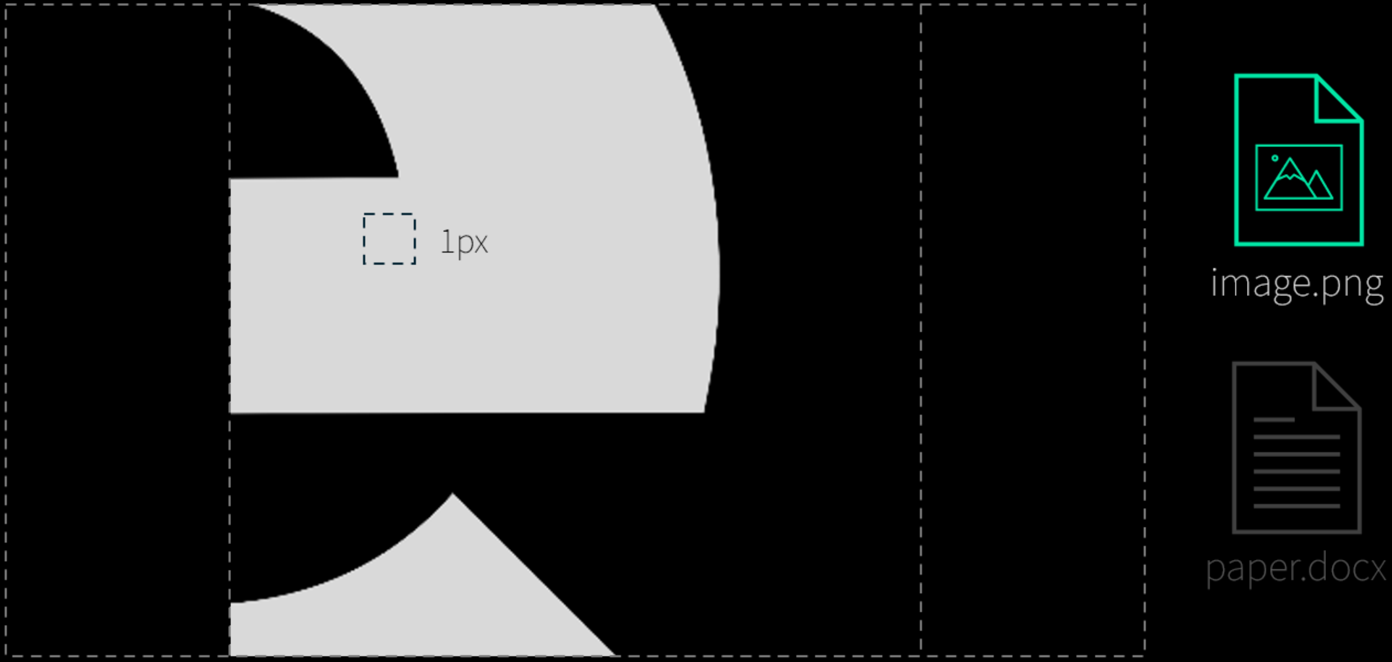
Software

Ransomware


Discord.exe
Download
Document
Desktop
image.png
paper.docx

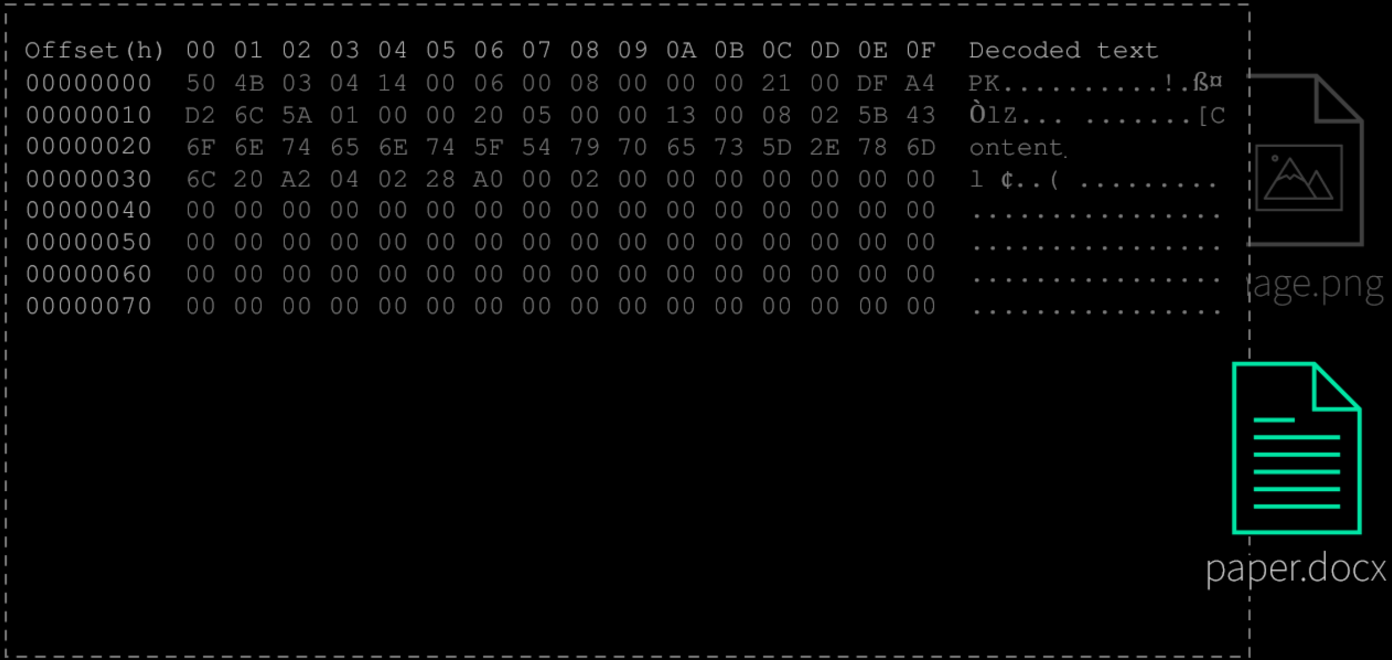
Ransomware

File structure



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000000  89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52  %PNG........IHDR
00000010  00 00 00 01 00 00 00 01 08 02 00 00 00 90 77 53  ..............wS
00000020  DE 00 00 00 01 73 52 47 42 00 AE CE 1C E9 00 00  Þ....sRGB.®Î.é..
00000030  00 04 67 41 4D 41 00 00 B1 8F 0B FC 61 05 00 00  ..gAMA..±..üa...
00000040  00 09 70 48 59 73 00 00 0E C3 00 00 0E C3 01 C7  ..pHYs...Ã...Ã.Ç
00000050  6F A8 64 00 00 00 0C 49 44 41 54 18 57 63 F8 FF  o¨d....IDAT.Wcøÿ
00000060  FF 3F 00 05 FE 02 FE A7 35 81 84 00 00 00 00 49  ÿ?..þ.þ§5.„....I
00000070  45 4E 44 AE 42 60 82                             END®B`‚
```

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000000  89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52  %PNG........IHDR
00000010  00 00 00 01 00 00 00 01 08 02 00 00 00 90 77 53  ..............wS
00000020  DE 00 00 00 01 73 52 47 42 00 AE CE 1C E9 00 00  Þ....sRGB.®Î.é..
00000030  00 04 67 41 4D 41 00 00 B1 8F 0B FC 61 05 00 00  ..gAMA..±..üa...
00000040  00 09 70 48 59 73 00 00 0E C3 00 00 0E C3 01 C7  ..pHYs...Ã...Ã.Ç
00000050  6F A8 64 00 00 00 0C 49 44 41 54 18 57 63 60 60  o¨d....IDAT.Wc``
00000060  60 00 00 00 04 00 01 5C CD FF 69 00 00 00 00 49  `......\Íÿi....I
00000070  45 4E 44 AE 42 60 82                             END®B`‚
```



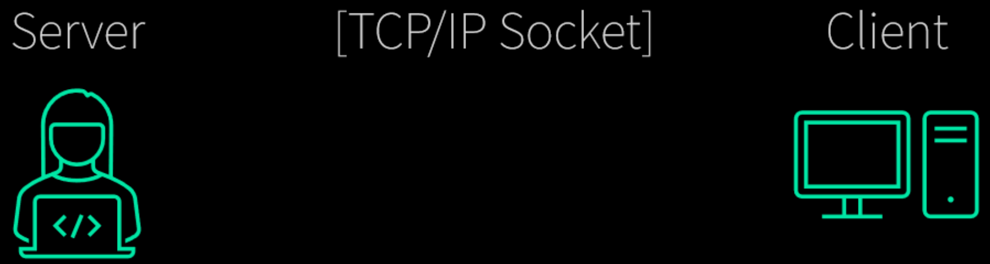
```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000000  50 4B 03 04 14 00 06 00 08 00 00 00 21 00 DF A4  PK..........!.ß¤
00000010  D2 6C 5A 01 00 00 20 05 00 00 13 00 08 02 5B 43  ÒlZ... .......[C
00000020  6F 6E 74 65 6E 74 5F 54 79 70 65 73 5D 2E 78 6D  ontent
00000030  6C 20 A2 04 02 28 A0 00 02 00 00 00 00 00 00 00  l ¢..( .........
00000040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

Biyard_resume.pdf

Mario.exe

Ps_cracked.exe

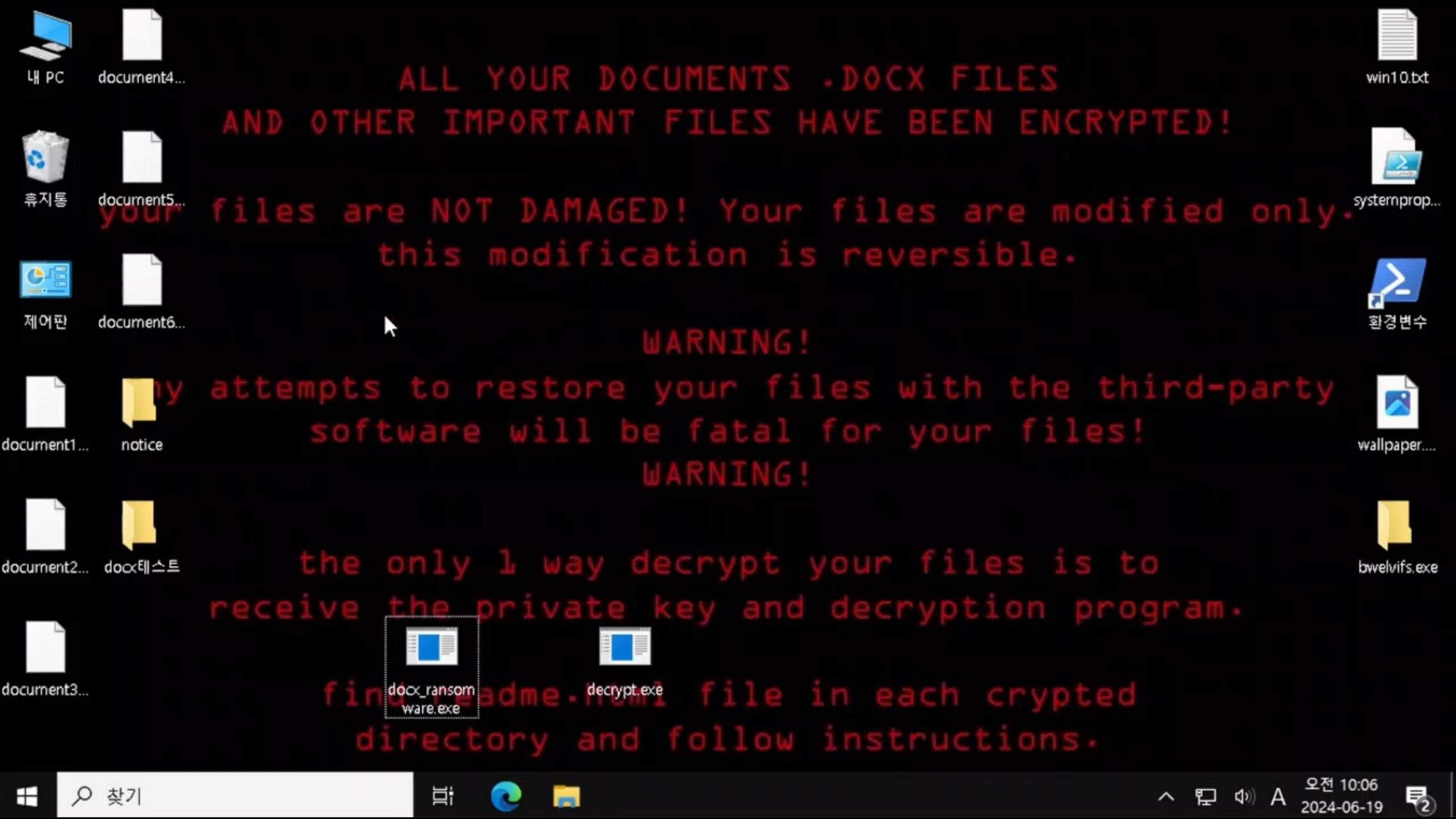
Starcraft.exe



Server

[TCP/IP Socket]

Client



ALL YOUR DOCUMENTS .DOCX FILES
AND OTHER IMPORTANT FILES HAVE BEEN ENCRYPTED!

your files are NOT DAMAGED! Your files are modified only.
this modification is reversible.

WARNING!
Any attempts to restore your files with the third-party
software will be fatal for your files!
WARNING!

the only 1 way decrypt your files is to
receive the private key and decryption program.

find readme.html file in each crypted
directory and follow instructions.