Today's Ransomware–HelloKitty
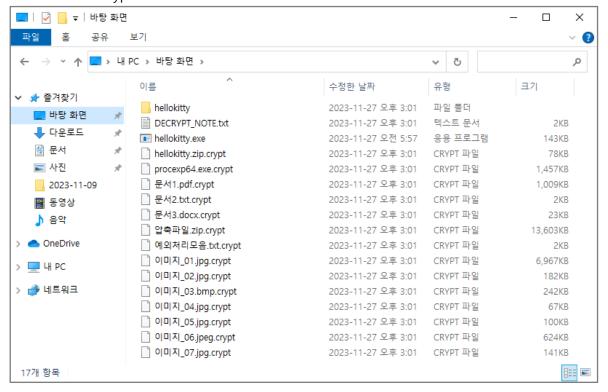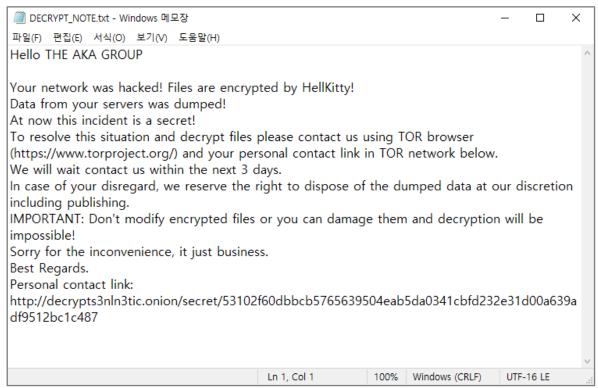
1. Blocking screenshot by trueEP®

2. Victim in case trueEP®wasnot installed - All file name's extensions were changed to <File Name>.crypt.

3. Ransomware Notice.


```
📄 DECRYPT_NOTE.txt - Windows 메모장                              —   □   ×
파일(F)  편집(E)  서식(O)  보기(V)  도움말(H)
Hello THE AKA GROUP

Your network was hacked! Files are encrypted by HellKitty!
Data from your servers was dumped!
At now this incident is a secret!
To resolve this situation and decrypt files please contact us using TOR browser
(https://www.torproject.org/) and your personal contact link in TOR network below.
We will wait contact us within the next 3 days.
In case of your disregard, we reserve the right to dispose of the dumped data at our discretion
including publishing.
IMPORTANT: Don't modify encrypted files or you can damage them and decryption will be
impossible!
Sorry for the inconvenience, it just business.
Best Regards.
Personal contact link:
http://decrypts3nln3tic.onion/secret/53102f60dbbcb5765639504eab5da0341cbfd232e31d00a639a
df9512bc1c487
                                            Ln 1, Col 1      100%   Windows (CRLF)   UTF-16 LE
```

4. Victim screen attacked by 'HelloKitty' ransomware.