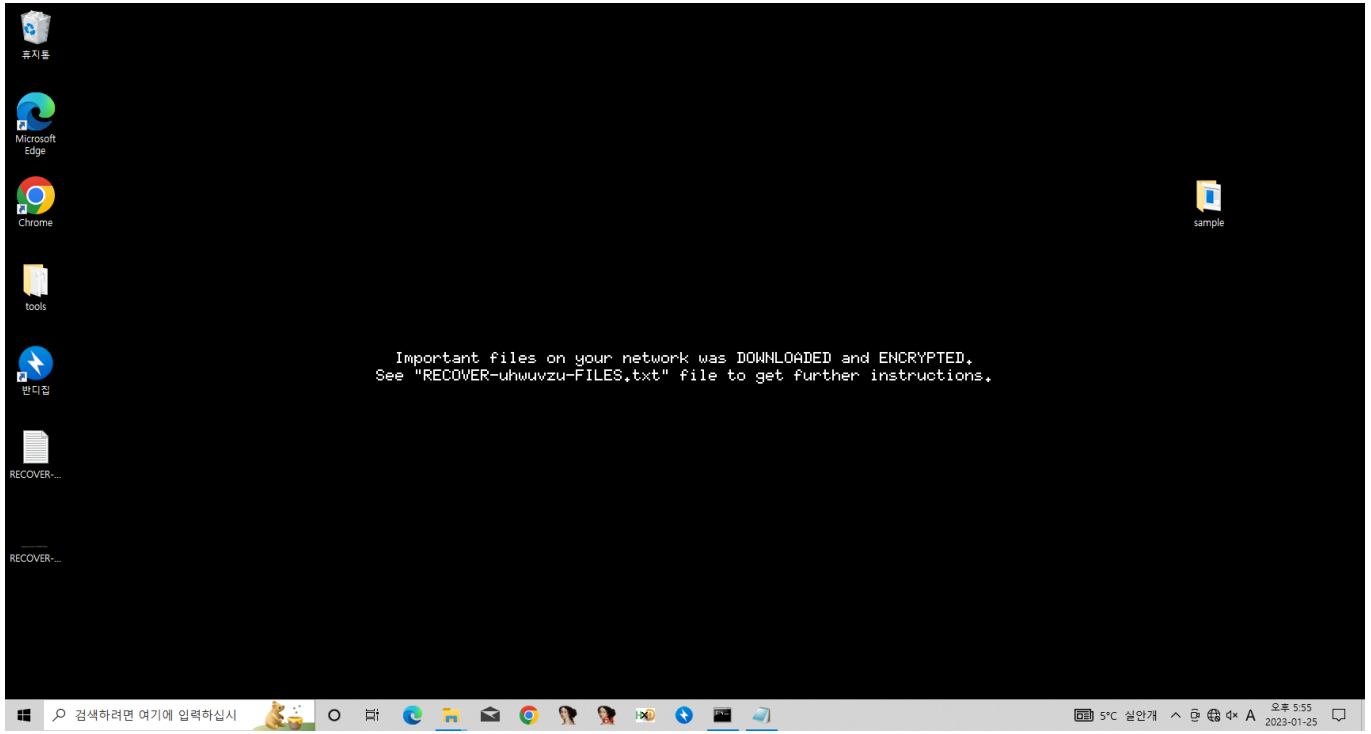
91913622 송태현

발표

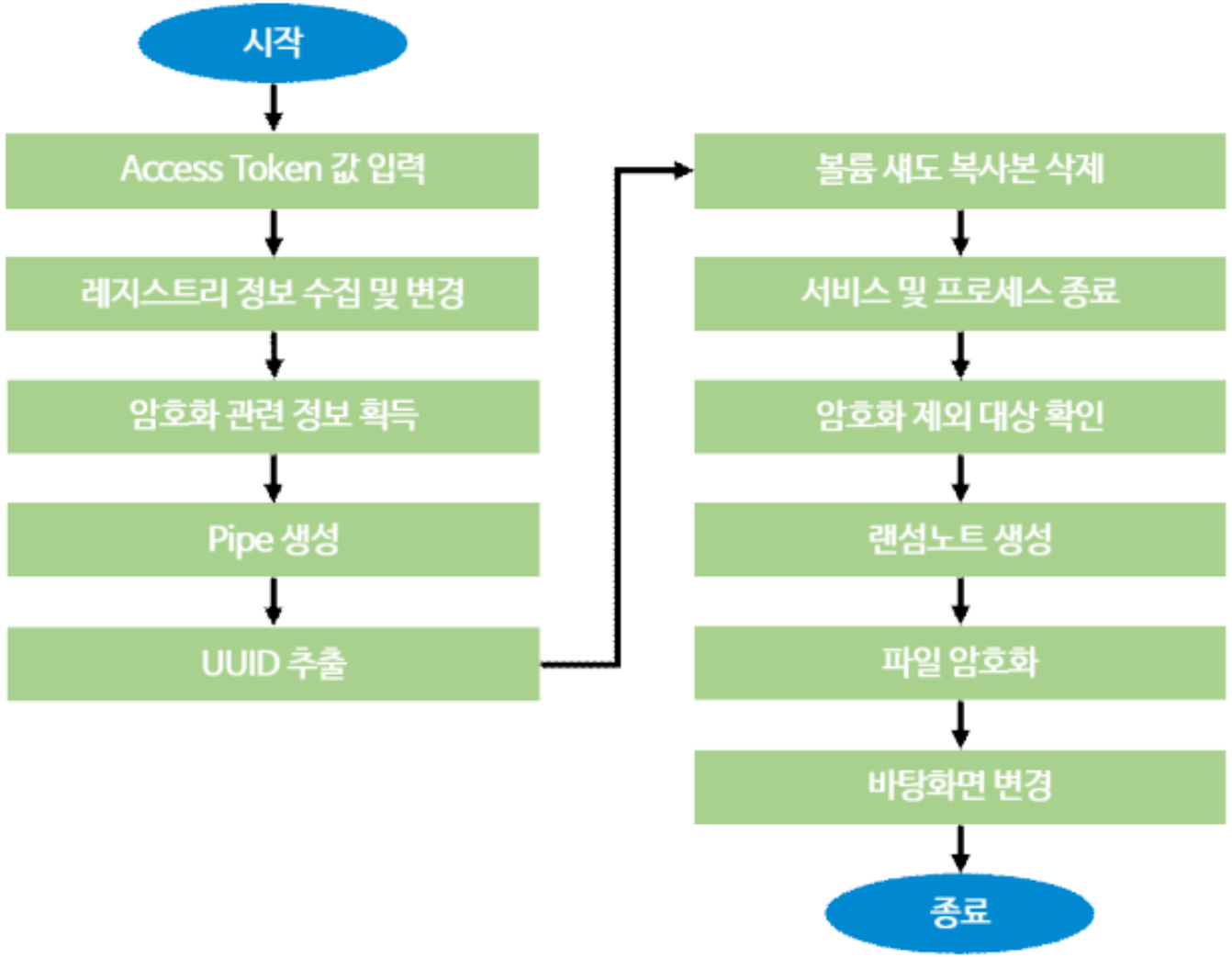
1. What kind of malware is it?



파일명	[임의의 파일명].exe
파일 크기	14,963,200 Bytes
파일 타입	Executable
SHA-256	847FB7609F53ED334D5AFFBB07256C21CB5E6F68B1CC14004F5502D714D2A456
행위	Ransomware

Name : BlackCat(ALPHV)
Language : Rust
Since : 2021 November
Victim : France, Switzerland, Italy.

2. Malware operation process



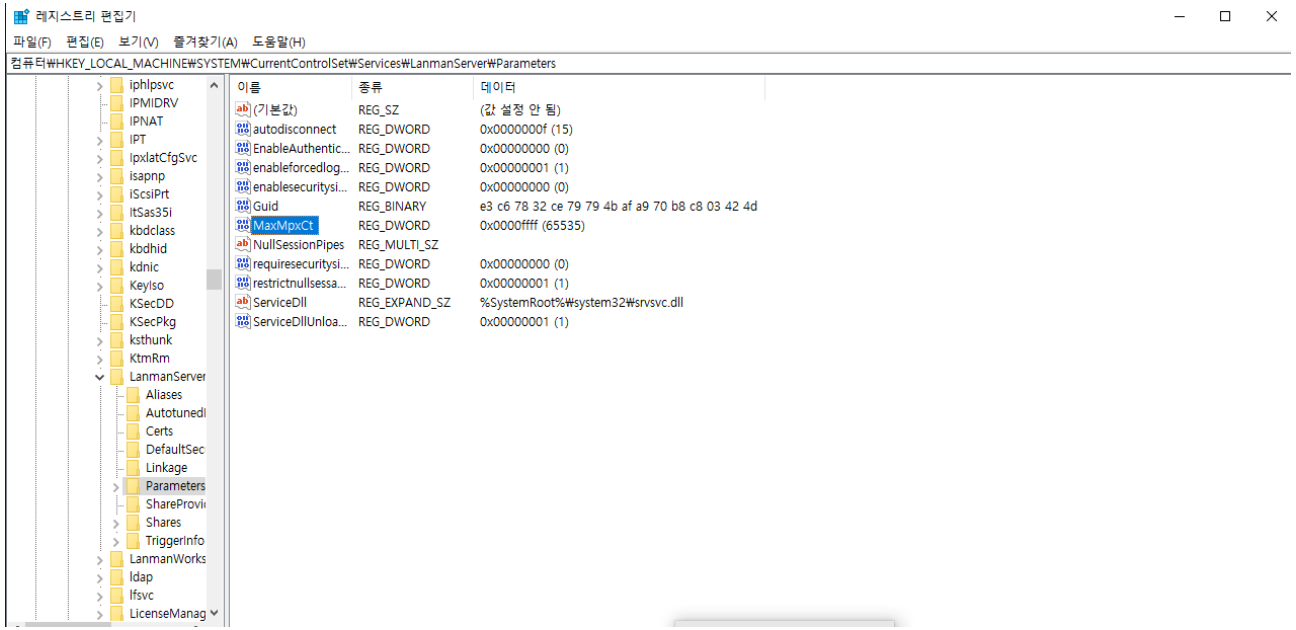
3.Analysis

```
C:₩Users₩truebird₩Desktop₩sample>blackcat.exe --help

USAGE:
    [OPTIONS] [SUBCOMMAND]

OPTIONS:
        --access-token <ACCESS_TOKEN>                Access Token
        --bypass <BYPASS>...
        --child                                      Run as child process
        --drag-and-drop                              Invoked with drag and drop
        --drop-drag-and-drop-target                  Drop drag and drop target batch file
        --extra-verbose                              Log more to console
    -h, --help                                       Print help information
        --log-file <LOG_FILE>                        Enable logging to specified file
        --no-net                                     Do not discover network shares on Windows
        --no-prop                                    Do not self propagate(worm) on Windows
        --no-prop-servers <NO_PROP_SERVERS>...       Do not propagate to defined servers
        --no-vm-kill                                 Do not stop VMs on ESXi
        --no-vm-kill-names <NO_VM_KILL_NAMES>...     Do not stop defined VMs on ESXi
        --no-vm-snapshot-kill                        Do not wipe VMs snapshots on ESXi
        --no-wall                                    Do not update desktop wallpaper on Windows
    -p, --paths <PATHS>...                           Only process files inside defined paths
        --propagated                                 Run as propagated process
        --ui                                         Show user interface
    -v, --verbose                                    Log to console
```

▶ BlackCat은 Access Token 값이 입력 되었을 때 악성 행위를 수행한다.

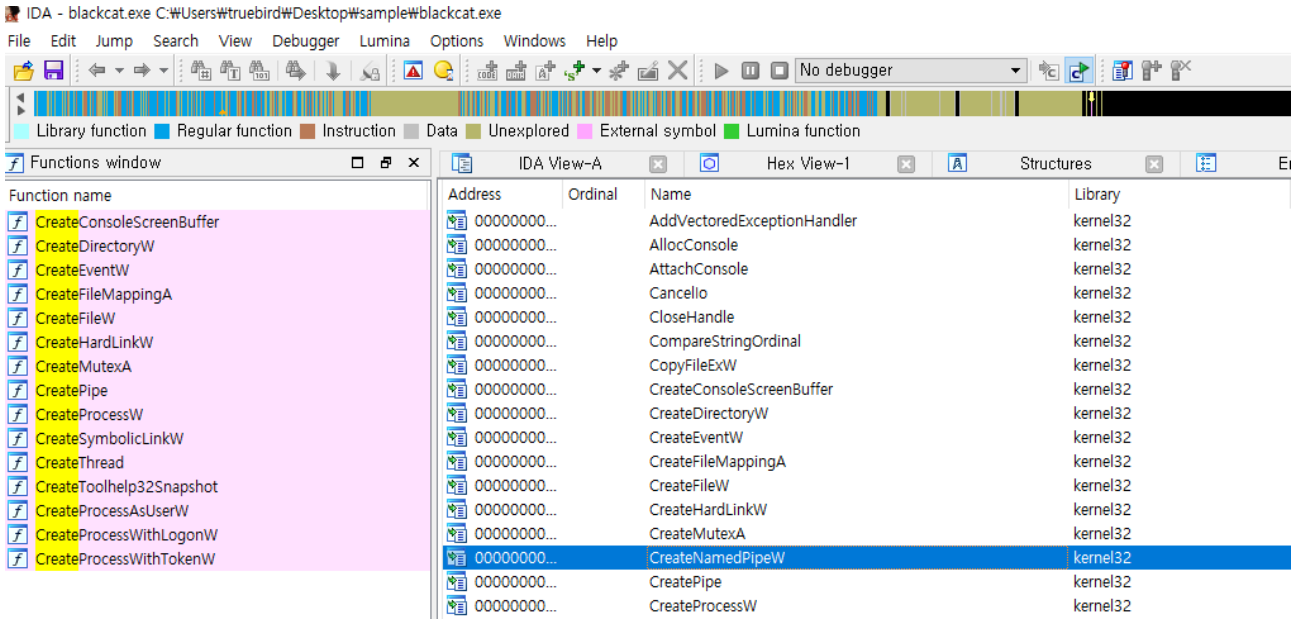
▶ AccessToken의 경우 공개된 것을 사용했고 Access Token을 입력하게 되면 악성 행위가 시작 된다.

3.Analysis



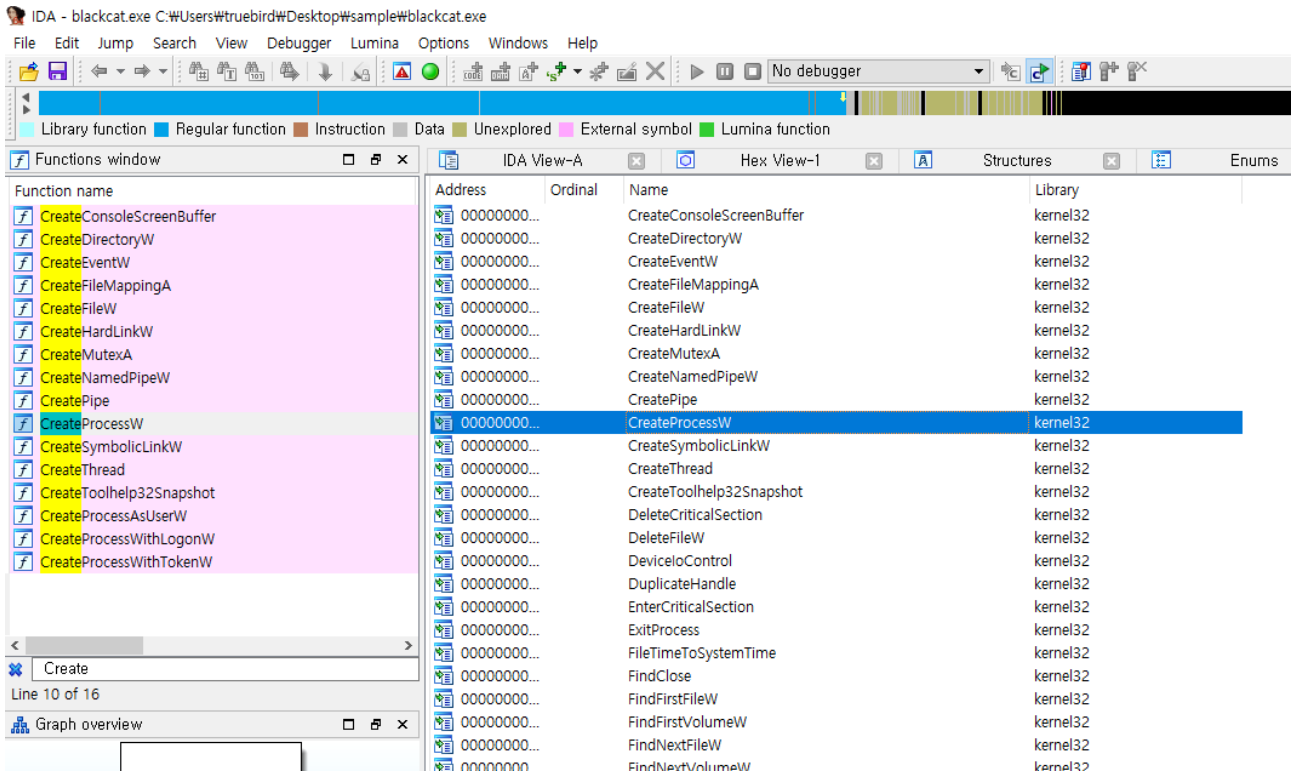
▶레지스트리 경로 '**₩HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services₩LanmanServer₩Parameters**'에서 MaxMpxCt(네트워크 최대 연결수) 값을 65535로 설정한다.

3.Analysis



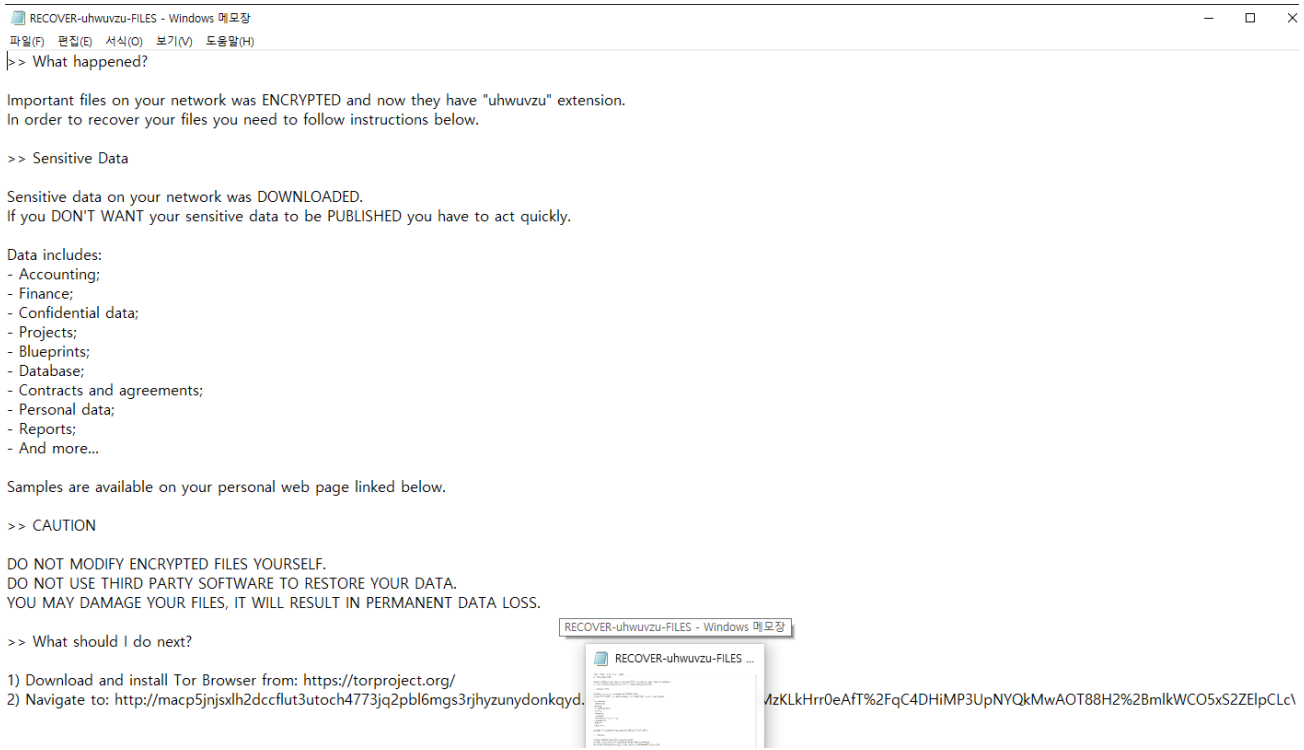
▶사용자의 프로세스 ID를 기반으로 CreateNamedPipeW 함수를 이용하여 Pipe를 생성한다.

3.Analysis



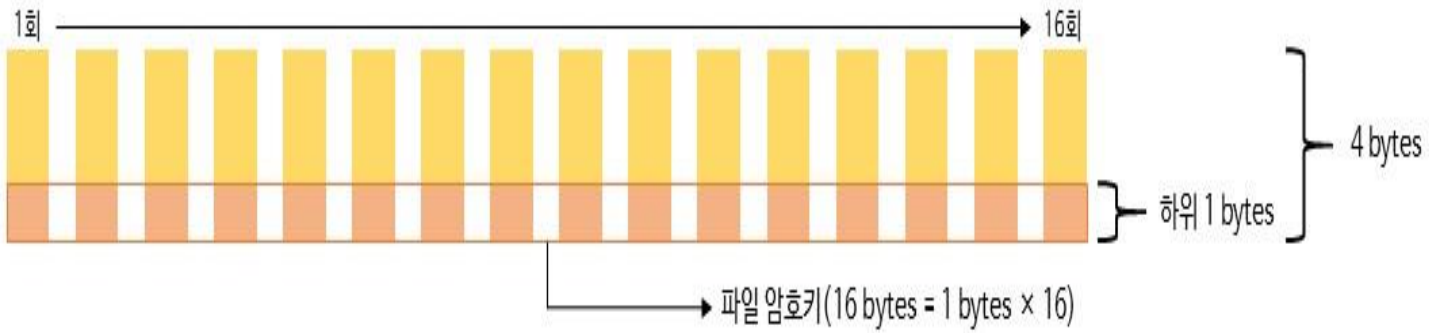
▶ CreateProcessW를 통해서 사용자의 UUID 값을 추출 하는 것을 볼 수 있다.

3. Analysis



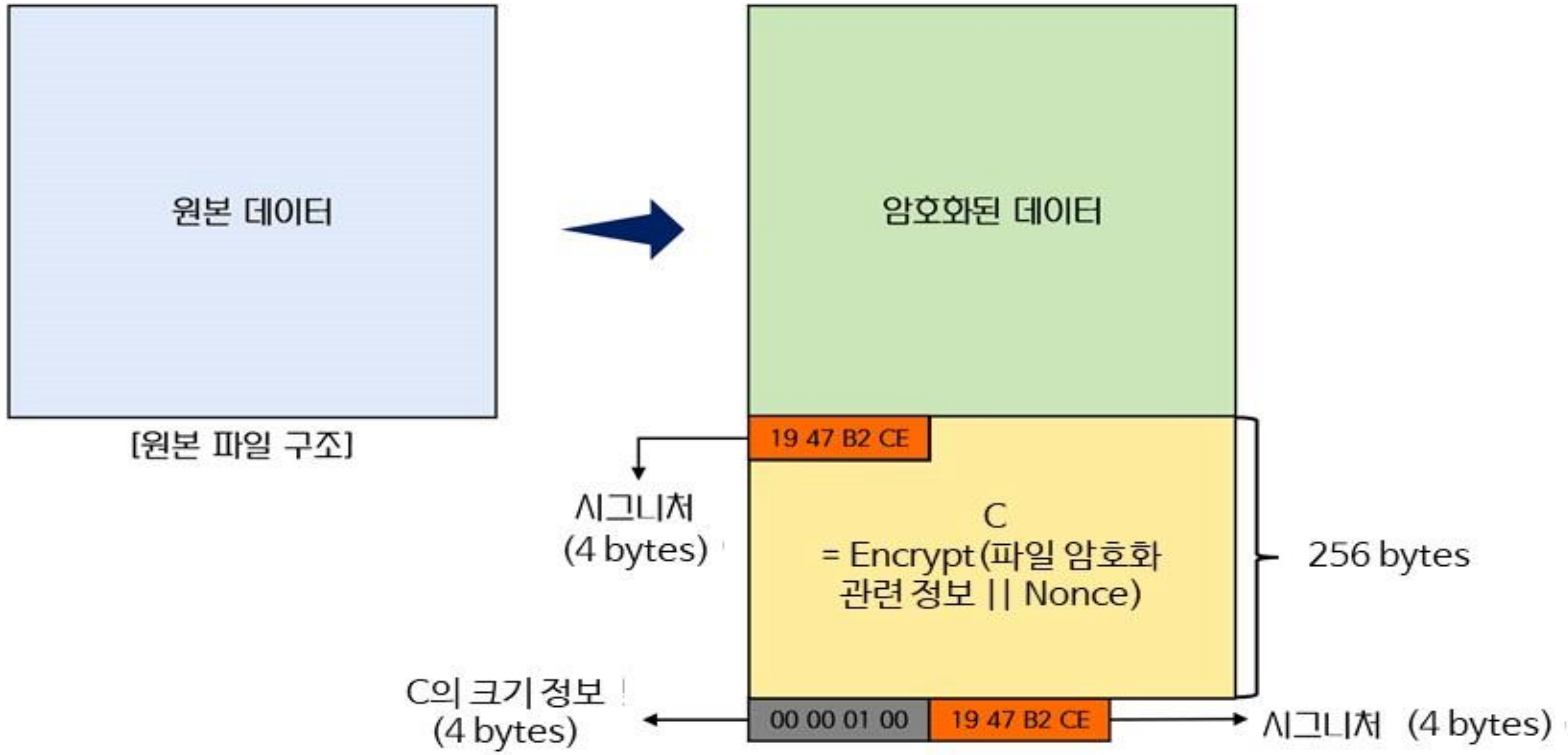
▶ BlackCat 랜섬웨어는 암호화 대상 파일이 존재하는 폴더마다 'RECOVER-uhwuvzu-FILES.txt' 라는 랜섬노트를 생성한다. 해당 파일에는 암호화된 데이터 종류, 공격자의 Tor 사이트 주소 등의 정보가 포함되어 있다.

3. Analysis



▶4 bytes 크기의 난수를 16개를 생성하고, 각 난수의 하위 1 bytes만 파일 암호키로 사용한다

3. Analysis


원본 데이터
[원본 파일 구조]
암호화된 데이터
19 47 B2 CE
시그니처
(4 bytes)
C
= Encrypt(파일 암호화
관련 정보 || Nonce)
256 bytes
C의 크기 정보
(4 bytes)
00 00 01 00
19 47 B2 CE
시그니처 (4 bytes)

4.The End

Blackcat분석.p