Deep analysis of REvil Ransomware | Written in Korean

medium.com/s2wlab/deep-analysis-of-revil-ransomware-written-in-korean-d1899c0e9317

S2W June 25, 2021

S2W

Jun 23, 2021

.

32 min read

Author: Sojun Ryu (hypen) @ S2WLAB Talon

> We are working on the English version. Coming soon!

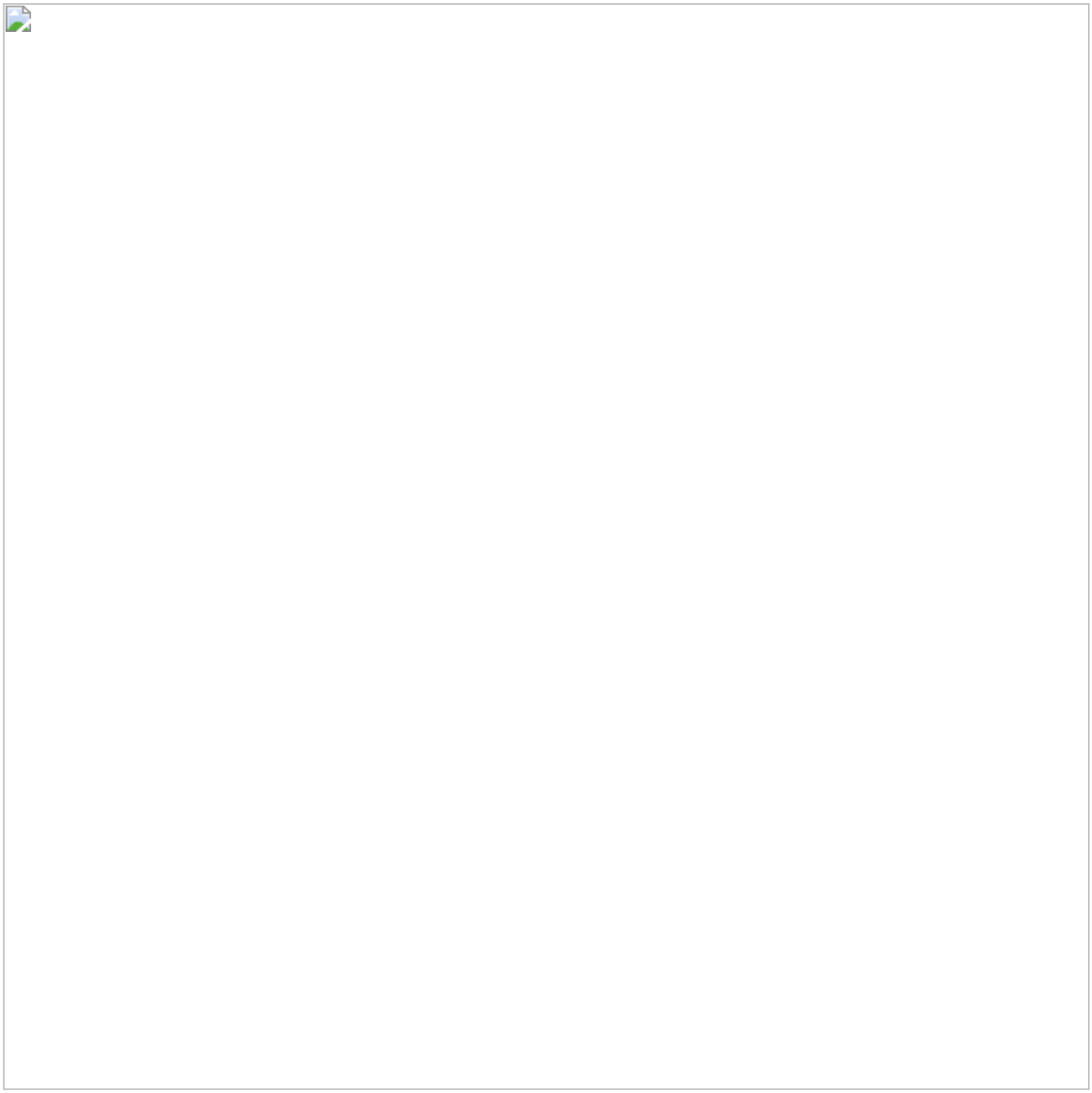


Photo by on

Executive Summary

침투과정

- 2019년 4월에 처음 등장한 REvil 랜섬웨어는 초기 오라클 웹로직 취약점 (CVE-2019–2725)을 이용하여 다양한 환경에 최초 침투를 시도
- 이후 Pulse Secure VPN 취약점 (CVE-2019–11510), FortiOS VPN 취약점 (CVE-2018–13379) 및 RDP 취약점 등 제로데이 취약점이 아닌, 패치가 적용되기 전의 N-day 취약점을 통해 기업 환경에 침투를 시도하여 매우 많은 기업을 감염시킴

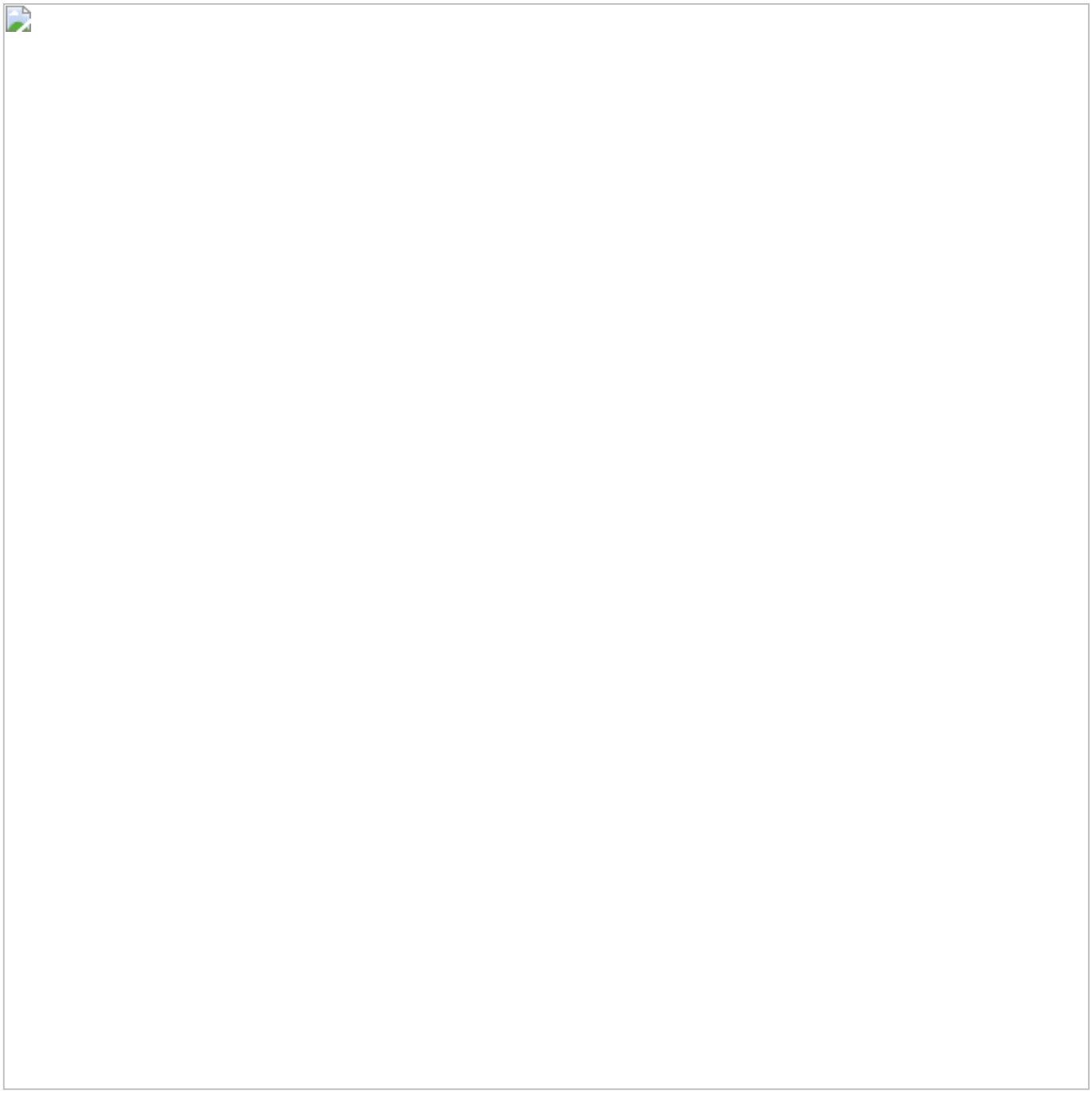
- 최근에는 다크웹에서 이미 유명한 악성코드인 Gootkit, QBot, IcedId와 같은 다운로드 및 로드에 특화된 악성코드에 의해 실행됨

주요 특징

- 암호화 키 교환 시, 랜섬웨어 악성코드들이 주로 사용하는 RSA를 사용하지 않고 타원 곡선 기반 암호(Elliptic Curve Cryptography)를 사용하며, 파일 암호화에는 Salsa20 알고리즘을 이용하여 파일을 암호화
- 로컬 드라이브 내 파일 뿐만 아니라 원격 드라이브 및 공유 드라이브 내 파일도 암호화하며, IOCP기법을 사용한 비동기 I/O방식으로 암호화 속도를 높임
- 2019년 12월부터 자체 Leak 사이트를 운영하여 피해 기업으로부터 탈취한 데이터를 게시하며, 협상에 응하지 않을 시 데이터를 공개하는 이중 갈취 전략을 사용.
- 비트코인을 통해 몸값을 지불받다가 2020년 4월부터 모네로로 변경함. 하지만 최근에는 피해자가 비트코인으로 지불을 원할 시, 10% 추가 금액을 낼 경우 비트코인으로도 지불받음
- 2021년 2월부터는 기존 Leak 사이트를 통한 이중 갈취 전략에서 홈페이지 DDoS 공격 및 피해 기업의 비즈니스 파트너에게 VoIP로 연락하는 협박 방식을 추가하겠다고 언급

최근 이슈

- 최근 Darkside의 Colonial Pipeline 공격, REvil 랜섬웨어의 JBS 공격 이후로 미국이 랜섬웨어 공격에 강력하게 대처하겠다는 발표 후, REvil은 오히려 미국에 대한 공격을 멈추지 않고, 더욱 더 강화하겠다고 언급함
- 현재까지 REvil 랜섬웨어 조직은 Darkside 랜섬웨어 조직, LV 랜섬웨어 조직과 Prometheus 조직까지 최소 3개의 랜섬웨어 조직과 연관되어있음



Overall flow of REvil Ransomware

Malware Information

```
 : 2075566e7855679d66705741dabe82b4 : 136443e2746558b403ae6fc9d9b40bfa92b23420 :
12d8bfa1aeb557c146b98f069f3456cc8392863a2f4ad938722cd7ca1a773b39: 2021-03-21 21:46:43 :
Win32 EXE file
```

Detailed Analysis

1. RC4 알고리즘을 이용하여 데이터 복호화

REvil 랜섬웨어는 RC4알고리즘을 이용하여 악성코드 내부에 포함된 Win32 API함수 주소, 설정 정보 및 문자열을 복호화하고 악성 행위에 사용한다. 악성코드마다 사용되는 key는 상이하다.
`RC4 key : 9UAo1qQ8ce4w13Jv36xcPgMz6NCykVjs`

2. 상세 옵션을 통해 세부 기능 설정

복호화된 정보 중 악성 행위에 필요한 19개의 상세 옵션이 JSON 형태로 표현되어 있다. 분석한 샘플인 2.05 버전의 각 옵션별 기능은 아래와 같다.

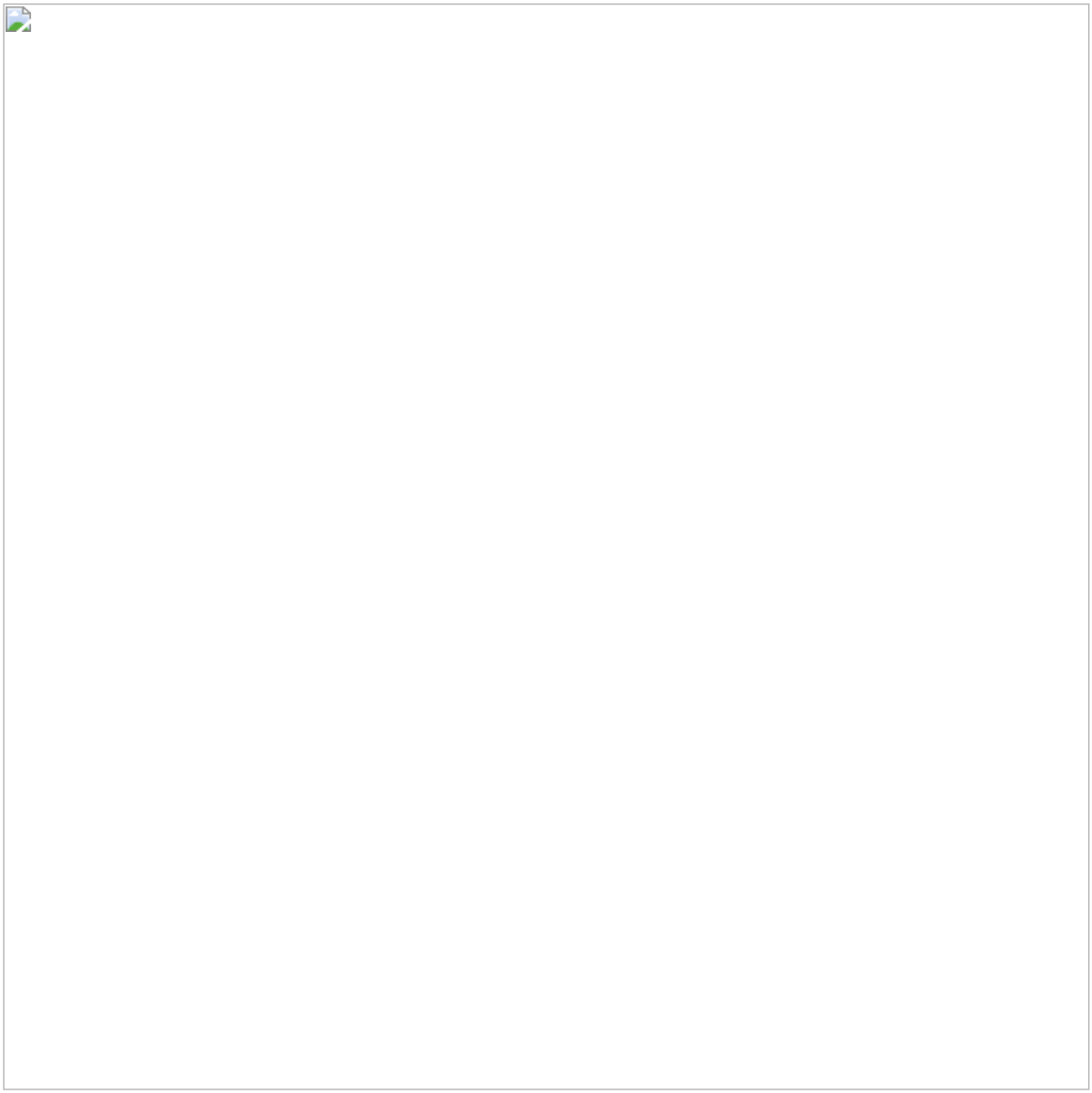
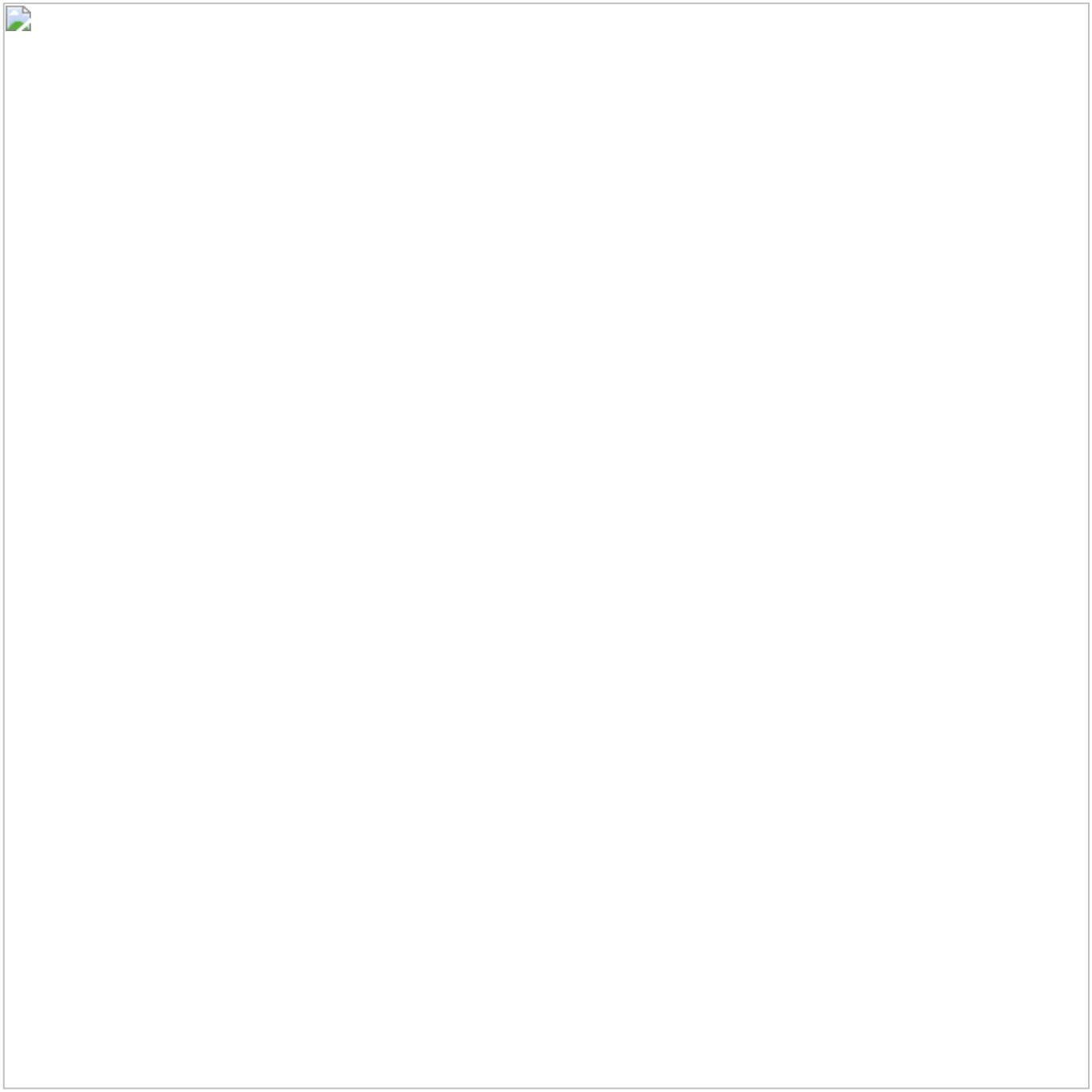


Table 1. 상세 옵션표

3. 암호화 사전 작업

REvil 랜섬웨어는 기존 랜섬웨어 그룹들이 주로 사용하는 RSA와 AES 알고리즘 조합을 사용하지 않고, ECC Diffie hellman 키 교환과 AES-256이 결합된 ECIES 공개키 알고리즘과 Salsa20 비밀키 알고리즘으로 파일 및 데이터를 암호화한다. 이를 위해 악성코드 내에 하드코딩 된 key를 이용하여 암호화에 필요한 구조체 데이터를 사전에 생성하며, 이를 레지스트리에 저장하여 재실행되어도 기존에 생성된 key를 사용함으로써 해당 값이 바뀌지 않도록 한다. 사용되는 레지스트리는 REvil 랜섬웨어 버전별로 상이하다.



Ecryption Flow

1) 레지스트리 path : HKLM\SOFTWARE\BlackLivesMatter

```
key : 54k => value : 공격자 공개키 (pk)key : aOwO => value : 파일 암호화 key생성에 사용된 공개키 (pk_key)key : Krdfp => value : 공격자 공개키로 암호화된 비밀키 구조체 (sk_key struct)key : hq0G6x => value : 제작자 마스터키로 암호화된 비밀키 구조체 (0_key struct)
```

2) HKLM 경로에 등록 실패 시 HKCU로 변경하여 등록 시도

4. 감염기기 정보 수집

이후 감염된 기기의 정보를 수집한다. 수집 목록은 아래와 같다.

1) 감염기기 식별 값 (UID)

- 현재 디스크의 VolumeSerial과 프로세서 이름을 수집
- 각각의 CRC32 체크섬 값을 조합한 16글자 문자열
- 예시 : 3EE1CF8D0ECB68EF

2) 암호화 확장자 (Extension)

- 5~10개의 랜덤 문자 조합 문자열 (기존 화이트리스트에 포함되지 않은)
- 예시 : 670o6j8nm
- 이후 레지스트리에 생성한 랜덤 확장자 저장
- Path : HKLM\ SOFTWARE\\BlackLivesMatter
- Key : x4WHjRs → value : [랜덤 확장자]
- HKLM 경로에 등록 실패 시 HKCU로 경로 변경

3) 유저명
4) 컴퓨터명
5) 현재 기기의 도메인명 `도메인이 없을 경우 WORKGROUP으로 지정`
6) 현재 지역 및 사용 언어
7) 현재 유저의 사용 언어, 시스템의 기본 언어, 키보드 layout을 수집 후 CIS 국가 여부 확인

8) 운영체제 버전
9) 디스크 별 전체 용량 및 사용 가능한 용량
10) 컴퓨터 x86, x64 여부

5. CIS국가 여부 확인

상세 옵션 중 dbg옵션이 False일 경우, 아래와 같이 유저 및 시스템 언어, 키보드 layout을 확인하여 CIS(독립국가연합) 지역의 기기일 경우 악성 행위를 수행하지 않는다. 반면 dbg 옵션이 True일 경우 공격자들의 디버깅용으로 실행되며 언어 및 layout을 확인하지 않는다.

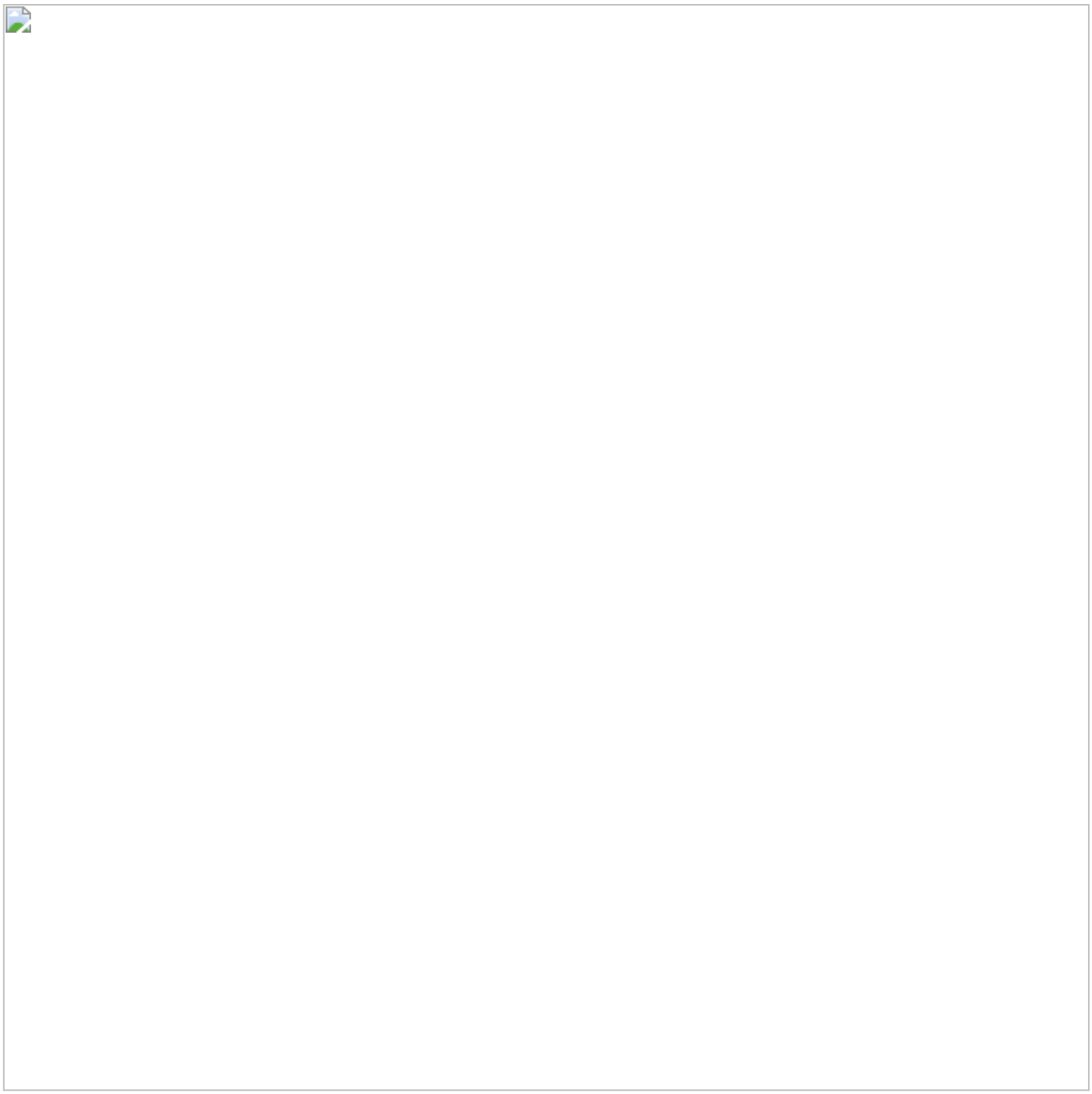


Table 2. 유저/시스템 언어와 키보드 레이아웃

6. 파라미터를 통한 실행 모드 지정

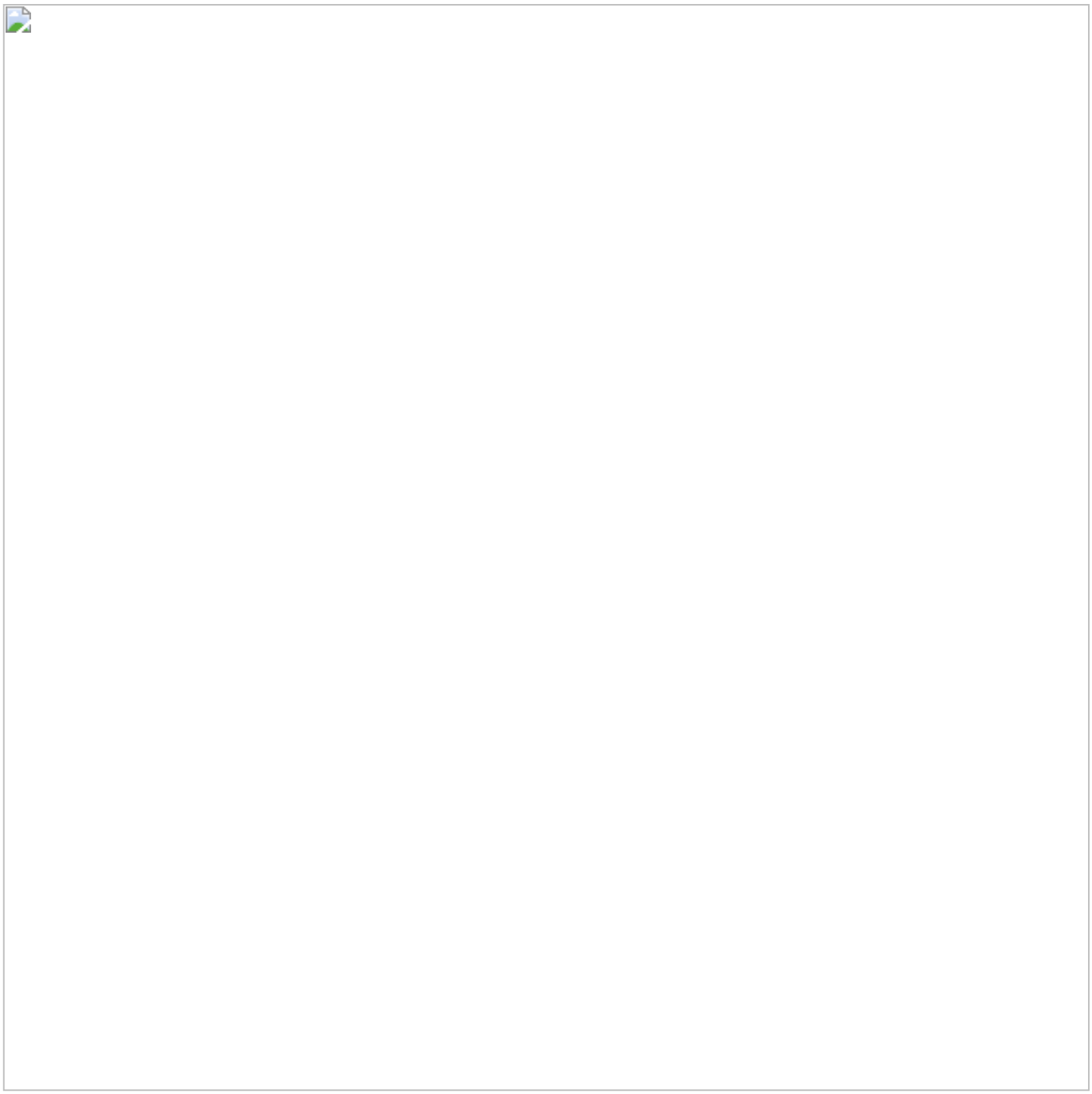


Table 3. 파라미터 목록

`-nolan:` **네트워크 공유드라이브는 감염 대상에서 제외**

1) 파라미터로 주어지지 않은 경우, 네트워크 드라이브 암호화 시도

2) 원격 드라이브 암호화: A~Z드라이브 중 원격 드라이브 내 파일 암호화

3) 공유 드라이브

- 현재 연결된 모든 공유 리소스 내 파일 암호화
- 네트워크 컨텍스트 내 모든 공유 리소스 내 파일 암호화
- 네트워크의 모든 공유 리소스 내 파일 암호화
- 영구적으로 연결된 모든 공유 리소스 내 파일 암호화

- 최근 연결된 모든 공유 리 소스 내 파일 암호화

`-nolocal:` 로컬 드라이브는 감염 대상에서 제외

1) 파라미터로 주어지지 않은 경우, 로컬 드라이브 암호화 시도

2) 로컬 드라이브 암호화: A~Z드라이브 중, 이동식 및 일반 드라이브 내 파일 암호화

`-smode:` 윈도우 계정 비밀번호 변경 및 안전모드로 재부팅

1) 안전모드 부팅이 아닌, 정상 모드로 부팅되었을 경우에만 동작

2) 안전모드에서 암호화를 할 경우, 백신 탐지를 우회하고 파일 암호화의 성공률이 높아질 수 있음

3) 현재 계정의 비밀번호를 “DTrump4ever”로 변경

4) 레지스트리를 변경하여 변경된 비밀번호로 자동 로그인되도록 설정

- Path : HKLM\ SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
- Key : AutoAdminLogon → value : 1
- Key : DefaultUserName → value : 현재 유저 명
- Key : DefaultPassword → value : DTrump4ver

5) 레지스트리 변경 후 재부팅 완료시 악성코드 재실행 및 부팅 모드 정상 모드로 복구

- Path : HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
- Key : *AstraZeneca → value : 악성코드 파일 명
- (Vista 이전) Key : *MarineLePen → value : bootcfg /raw /fastdetect /id 1
- (Vista 이후) Key : *MarineLePen → value : bcdedit /deletevalue {current} safeboot

6) 설정 후, 부팅 모드를 네트워크 가능한 안전모드로 변경하는 명령어 실행

- (Vista 이전) 명령어 : bootcfg /raw /a /safeboot:network /id 1
- (Vista 이후) 명령어 : bcdedit /set {current} safeboot network

7) 설정 완료 후 감염기기 재부팅

- 명령어 : SHUTDOWN -r -f -t 02
- 2초 후 시스템을 강제로 재부팅

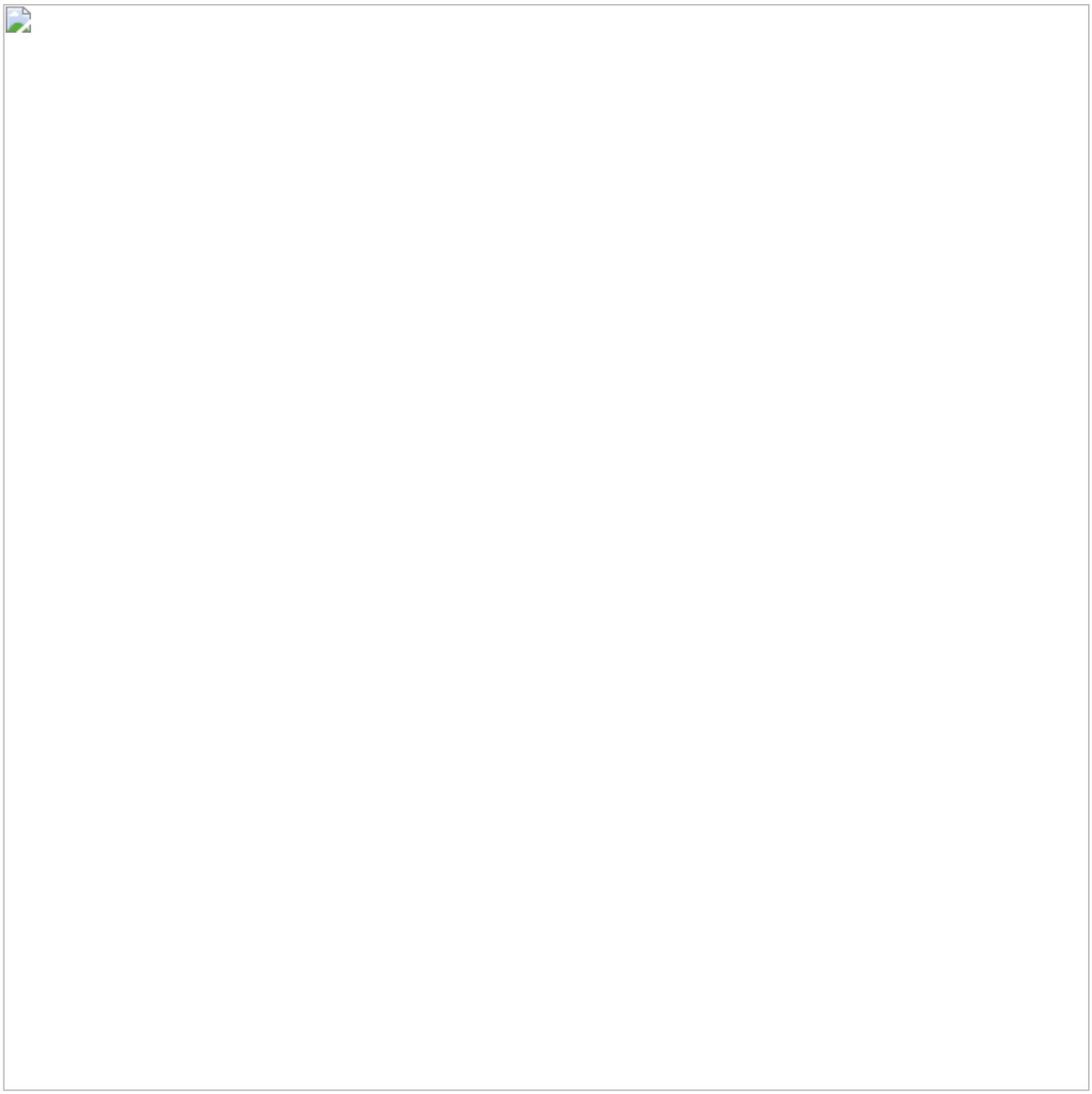
`-silent:` 특정 서비스, 프로세스 종료 및 볼륨 섀도우 카피 삭제 수행하지 않음

1) 파라미터로 주어지지 않은 경우, 특정 서비스와 프로세스 종료 및 볼륨 섀도우 카피 삭제

2) Win32 API를 이용하여 현재 실행 중인 특정 프로세스 종료

3) WMI로 신규 프로세스 생성 Event를 모니터링하여 특정 프로세스 생성 시 종료

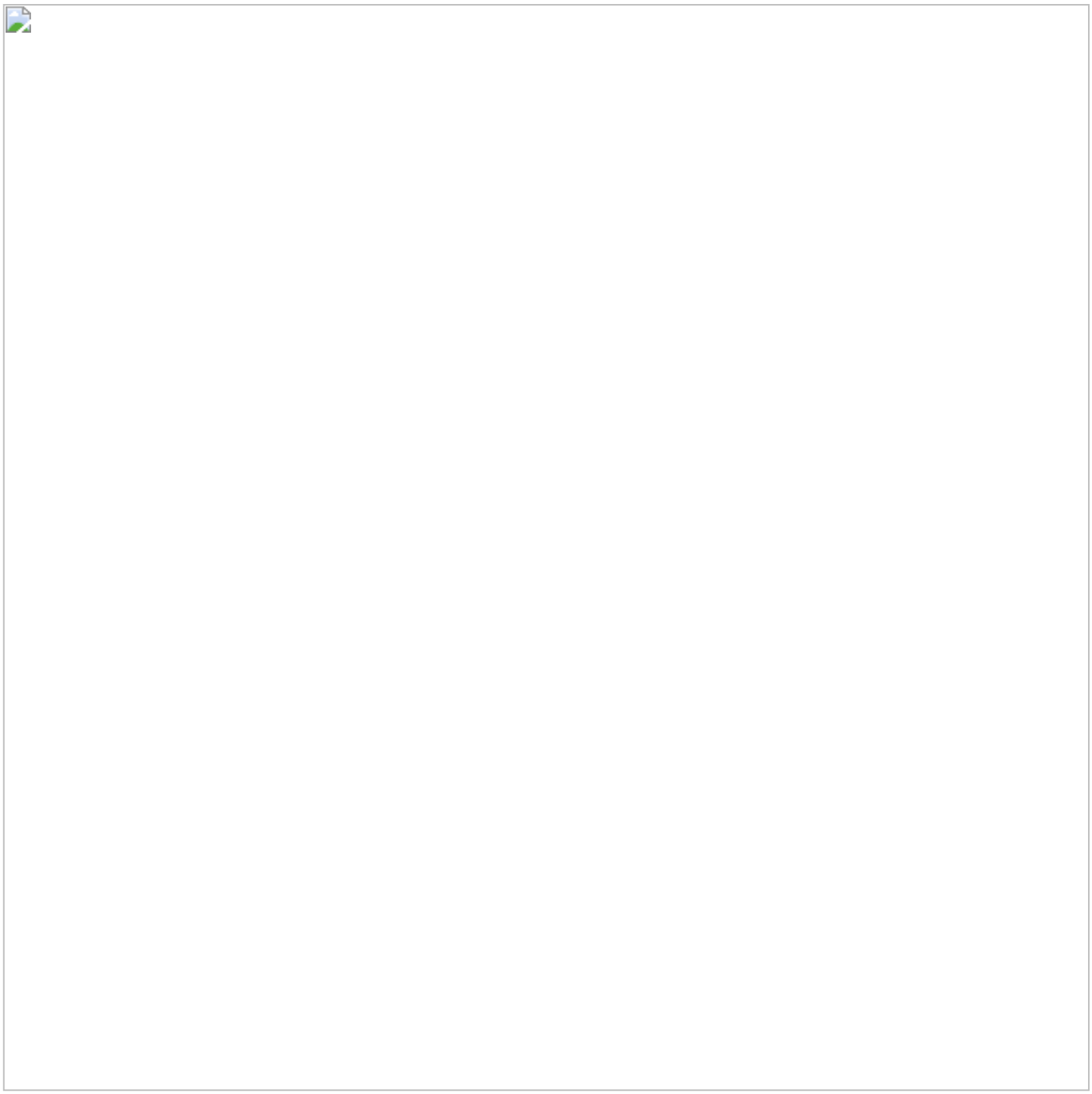
4) 특정 프로세스 목록



5) Win32 API를 이용하여 현재 실행 중인 특정 서비스 종료

6) WMI로 서비스 변동사항 Event를 모니터링하여 특정 서비스 실행 시 중지

7) 특정 서비스 목록



8) WQL(SQL for WMI) 쿼리를 이용하여 감염된 기기의 Volume Shadow Copy를 모두 삭제

- WQL Query : SELECT * FROM Win32_ShadowCopy
- 이후 Win32_ShadowCopy.ID=[조회한 ID]에 대하여 DeleteInstance 작업 수행

`-path:` 특정 경로에 대해서만 암호화 진행

1) 주어진 경로에 대해서만 파일 암호화 진행

2) 네트워크 및 로컬 경로 여부 확인하여 진행

3) 전체 파일 암호화 전에 공격자가 테스트 용도로 사용하는 기능

-path로 실행될 경우 권한 상승, 정보유출, 바탕화면 변경 등을 수행하지 않음

`-fast:` 빠른 암호화 모드

1) -path와 함께 사용되며, 파일 암호화 시 상위 0x100000만 암호화를 수행

2) 상세 옵션 중 et가 1일 때와 동일

`-full:` 전체 암호화 모드

1) -path와 함께 사용되며, 파일 암호화 시 파일 전체에 대해서 암호화를 수행

2) 상세 옵션 중 et가 0일 때와 동일

7. 동작 과정

1) 뮤텍스 생성

악성코드의 중복 실행 방지를 위해 특정 문자열을 이용하여 뮤텍스 생성

- 뮤텍스 명 : Global\\F69C27FF-AB15-CCAA-A2D6–7F7ADA90E7E3
- 문자열은 악성코드마다 다른 값을 사용
- 중복 실행 시 현재 프로세스를 종료

2) 상세 옵션 `exp` (Table 1. 상세 옵션표 참고)에 따른 행위 수행

- 유저가 관리자 권한을 갖고 있지만, 프로세스가 관리자 권한을 갖지 않은 경우 프로세스 재실행
- 유저가 승낙할 때까지 관리자 권한으로 실행을 요구하는 UAC 수락 요청 창을 화면 상에 계속 표출

3) 암호화 작업 전 기타 행위

- 강제로 휴지통 비우기
- 프로세스의 CPU 스케줄링 우선순위를 일반 프로세스보다 한 단계 상승시켜 리소스 사용
- 프로세스가 실행되는 도중 절전 모드 전환 및 디스플레이 꺼짐 방지
- SeDebugPrivilege 권한을 할당하여 타 프로세스에 접근 가능하도록 권한 설정

4) 상세 옵션 `arn` (Table 1. 상세 옵션표 참고) 에 따른 행위 수행

레지스트리를 변경하여 기기를 재부팅하더라도 악성코드가 실행되도록 설정

- Path : HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Key : 3"qZhotTgfr3 → value : 악성코드 파일 명
- HKLM 경로에 등록 실패 시 HKCU로 변경

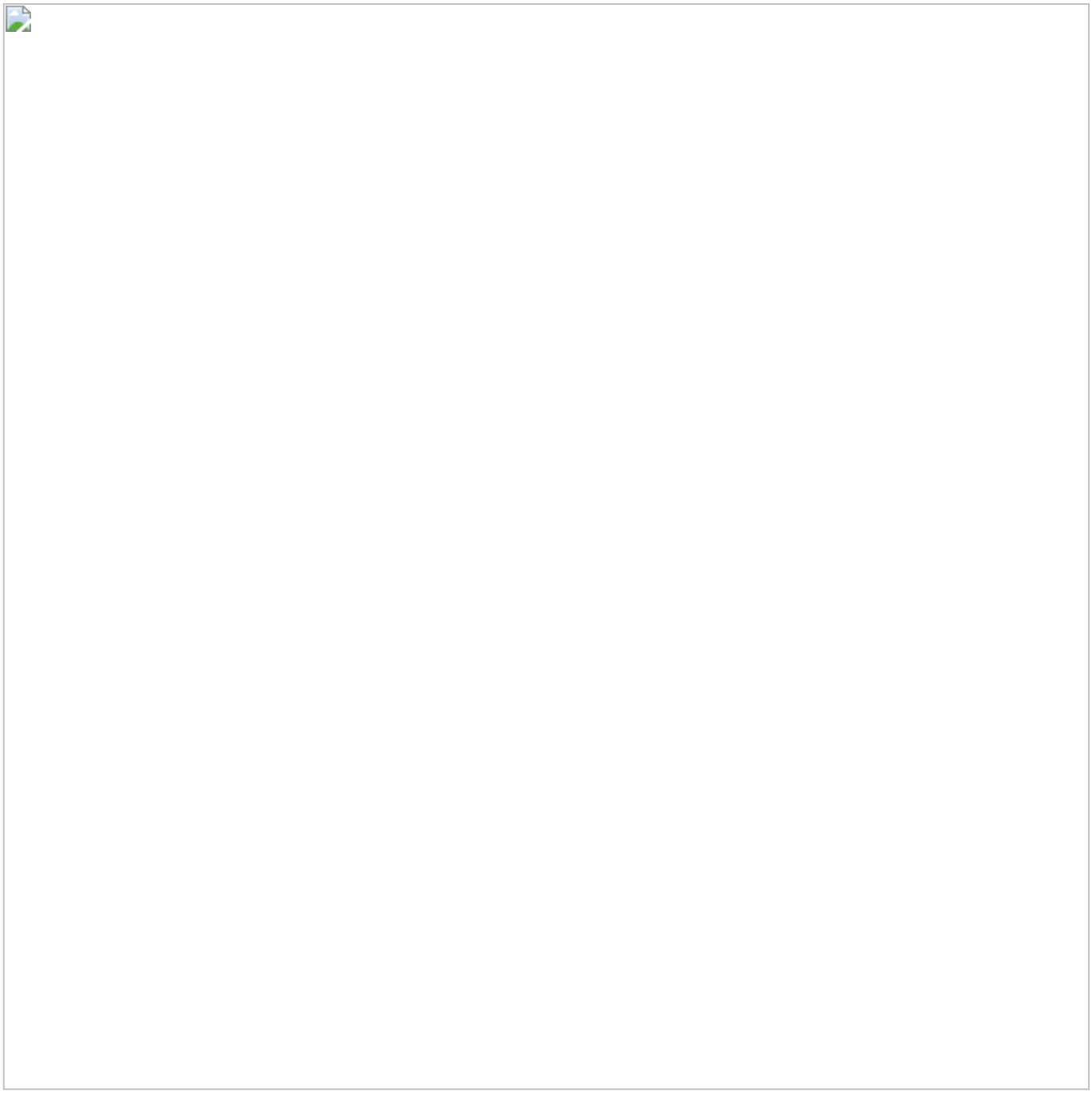
5) 바탕화면 변경

1. 바탕화면을 파란색 배경에 자신들의 메시지가 담긴 이미지로 변경

- 원본 이미지 파일 경로 : %temp%\[랜덤 3~13개의 문자열].bmp
- 아래는 상세 옵션 img에 명시된 협박 메시지이며, 협박 메시지 상에 instuctions 은 instruction의 오타임

```
All of Your fiels are encrypted!Find [Random Extension]-readme.txt and follow
instuctions
```

실제 변경된 바탕화면



Compromised Background

6) 상세 옵션 `net` 에 따른 행위 수행

1. JSON 형태로 감염기기 정보 및 암호화에 사용된 정보 수집

```
{    "ver": [REvil 랜섬웨어 버전],    "pid": [악성코드 식별자], (상세옵션에 명시됨)    "sub": [악성코드 식별자], (상세옵션에 명시됨)    "pk": [암호화에 사용된 공개키 정보], (상세옵션에 명시됨)    "uid": [Victim ID],    "sk": [sk_key struct(비밀키 구조체)],    "unm": [유저 명],    "net": [컴퓨터 명],    "grp": [도메인 명],    "lng": [지역 및 사용언어],    "bro": [CIS 국가 여부],    "os": [운영체제 버전],    "bit": [32bit 또는 64bit 여부],    "dsk": [디스크 별 전체 용량 및 사용 가능한 용량 정보],    "ext": [암호화 확장자]"}
```

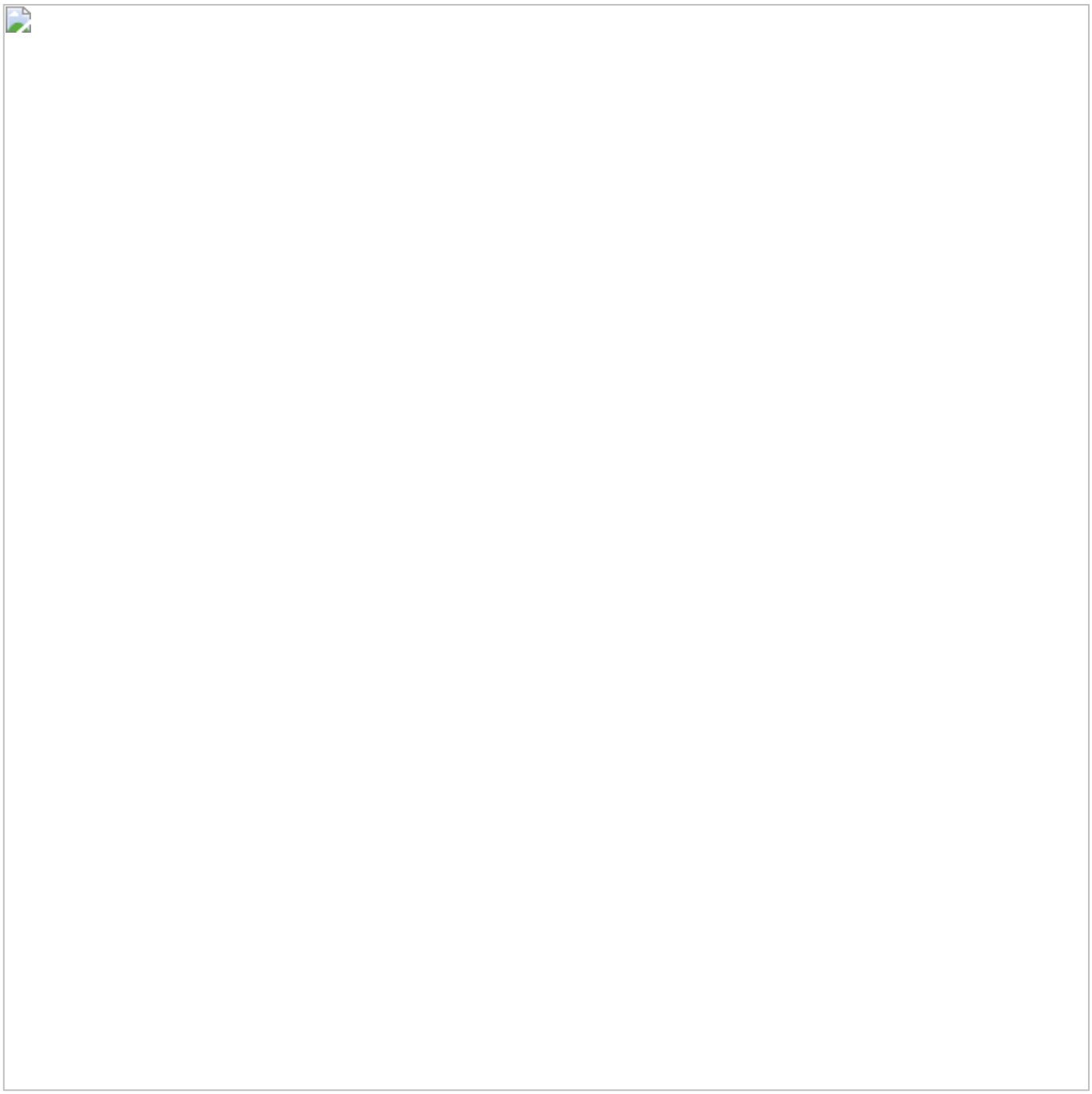
2. 모든 정보를 취합한 뒤, 파일과 동일한 방식으로 데이터를 암호화

    데이터 암호화에는 악성코드 내에 별도로 하드코딩된 공개 key 사용

3. 암호화한 데이터를 레지스트리에 저장

- Path : HKLM\SOFTWARE\BlackLivesMatter
- Key : XFx41h1r → value : [암호화 된 감염기기 정보 및 암호화에 사용된 정보]
- HKLM 경로에 등록 실패 시 HKCU로 변경

4. 상세 옵션 중 `dmn` 에 저장되어 있는 도메인 별로 아래 그림과 같이 특정 문자열을 조합하여 랜덤 URL 주소 생성하여 접속 시도



URL 주소 생성 방식

5. 도메인별로 생성된 URL주소로 수집한 감염기기 정보 목록 전송

- User-agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.125 Safari/537.36
- Method : POST
- Header : Content-Type: application/octet-stream
- Header : Connection: close

7) 메모리 정리

1. 감염정보 전송과 모든 파일 암호화를 마친 뒤 관련 데이터를 모두 정리

2. 상세 옵션 및 암호화에 사용된 키 정보, 감염기기 정보가 할당된 메모리를 모두 해제함

8) 파일 삭제

1. 재부팅될 경우 악성코드가 삭제되도록 설정

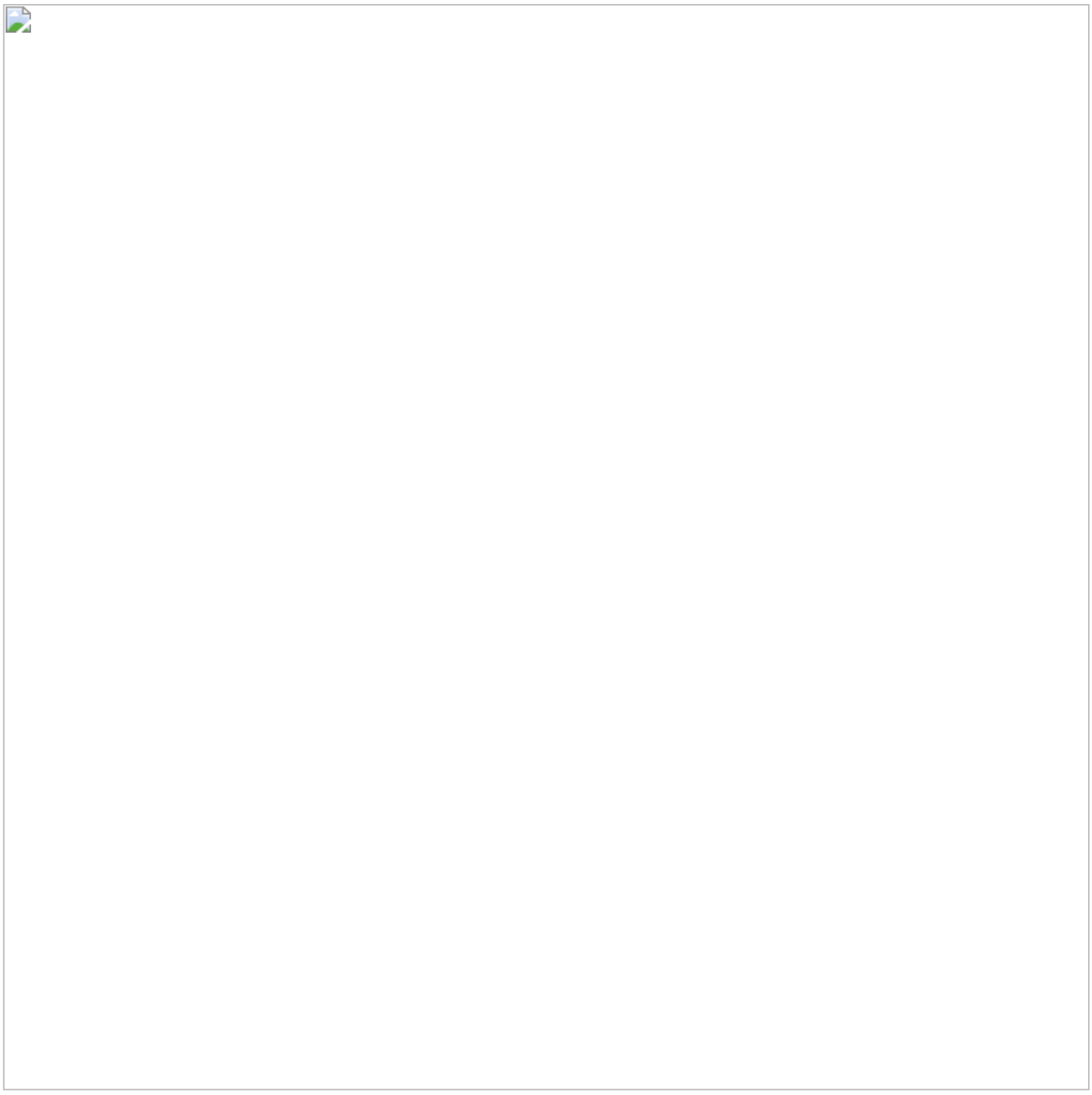
8. 파일 암호화 Thread

1) Input/output completion port (IOCP)를 이용한 암호화 작업 수행

- REvil 랜섬웨어는 IOCP를 이용한 비동기 입출력 방식으로 빠른 암호화를 수행함
- 감염 기기의 프로세서 갯수 * 2개의 암호화 전담 Thread 생성

2) ECIES()를 이용한 파일 암호화

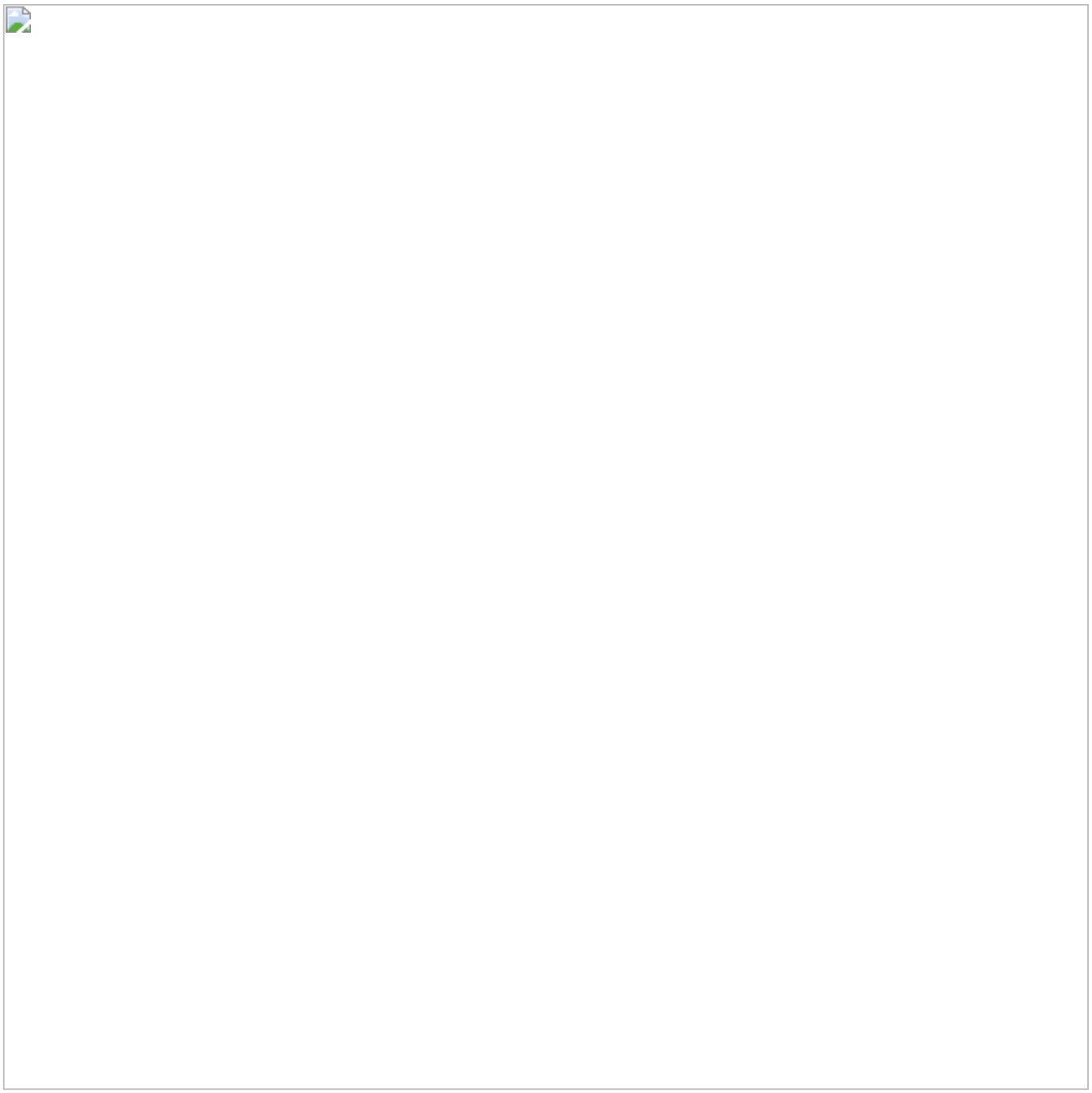
- REvil 랜섬웨어는 ECC Diffie Hellman 키 교환 방식을 사용하여 키 교환을 시도함
- 키 생성에는 Curve25519를 사용하는데, 이는 가장 빠른 곡선 중 하나로 알려짐
- 랜섬웨어 바이너리 내에 미리 포함되어 있는 pk (Attacker Key)를 이용하여 실제 파일 암호화에 사용되는 dk_key에 대한 암호화 진행
- pk 외에 Master Key가 존재하는데, 이는 REvil 랜섬웨어의 메이저 버전마다 동일한 값을 가지며, REvil 랜섬웨어 제작자가 언제든지 파일을 복호화할 수 있는 용도로 사용됨



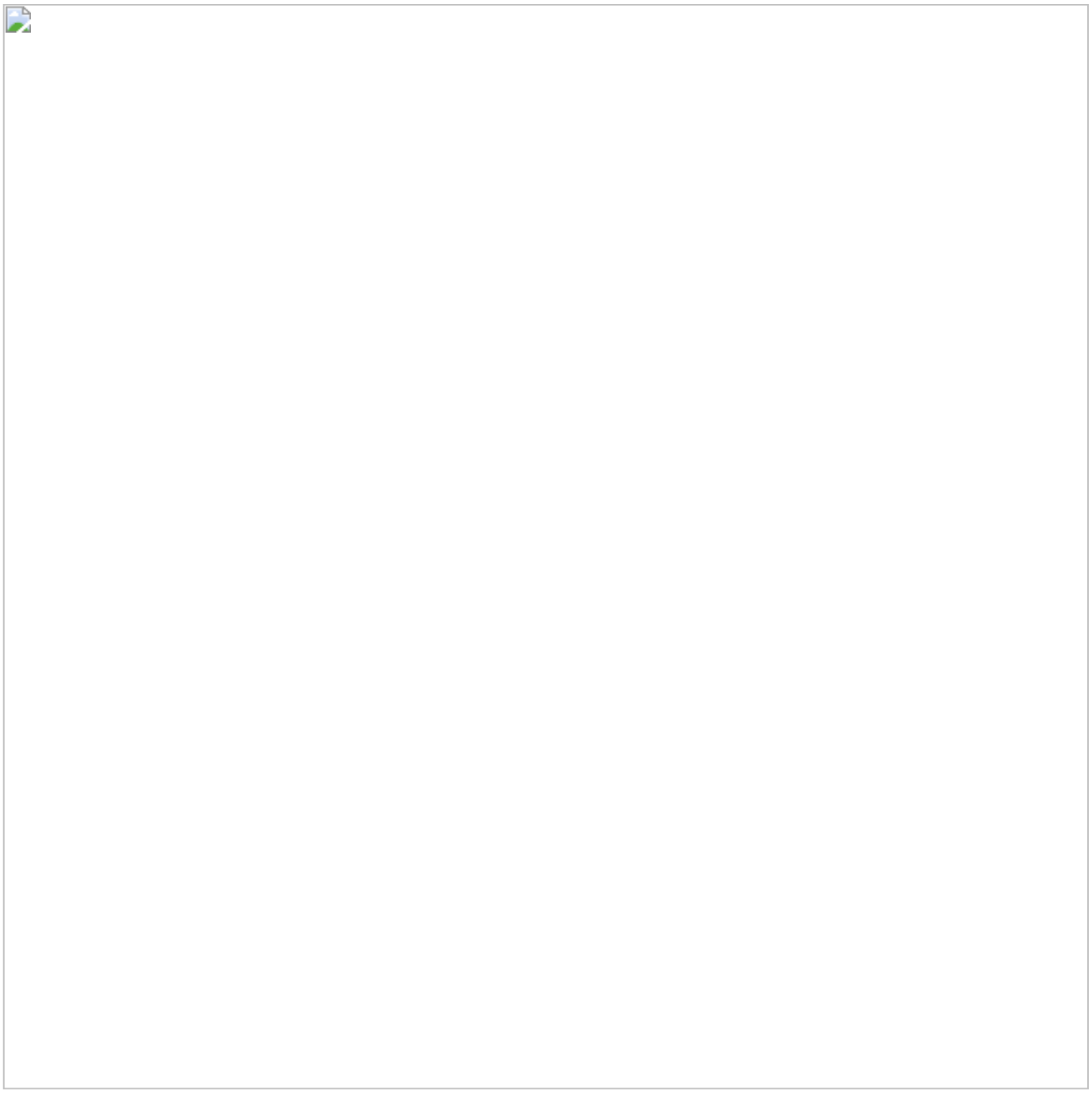
Master key와 Attacke key를 이용한 dk_key 개별 암호화

3) 암호화 대상에서 특정 파일, 폴더 및 확장자 제외

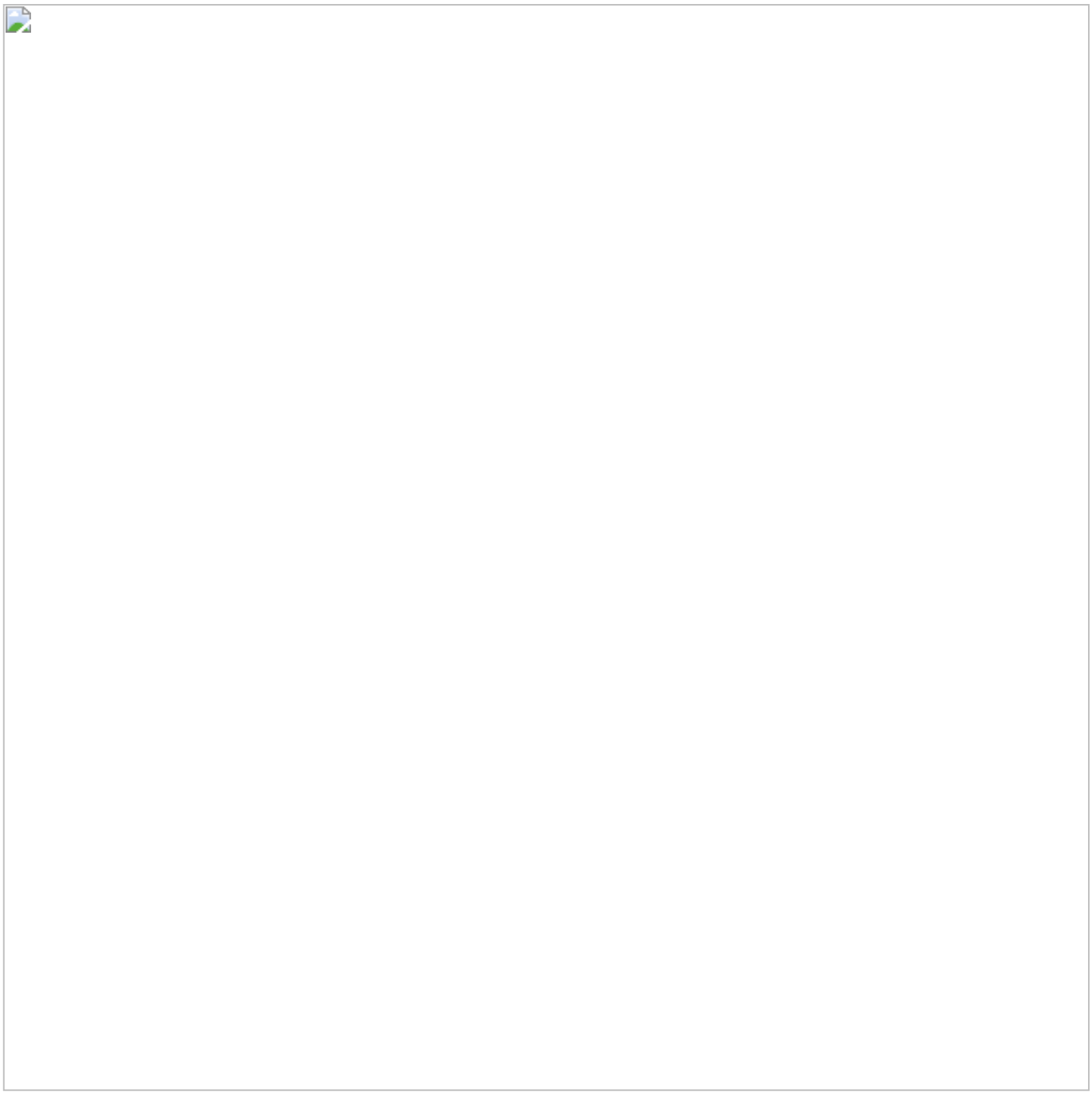
운영체제와 관련되거나 중요도가 낮은 폴더를 암호화 대상에서 제외



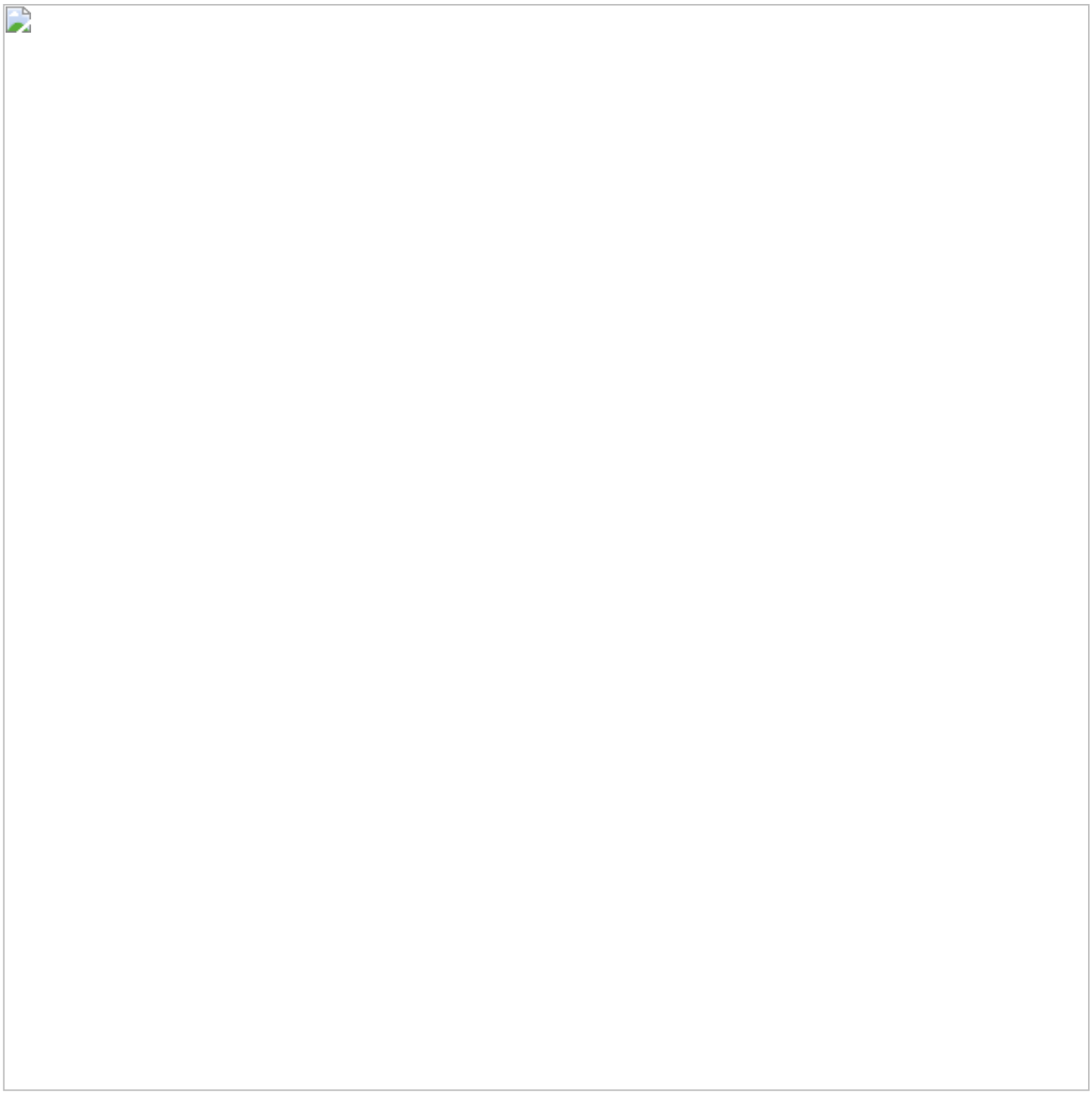
부팅 또는 운영체제 관련 파일을 암호화 대상에서 제외



실행 프로그램 또는 스크립트등과 같은 불필요한 확장자를 감염 대상에서 제외



타겟 파일에 접근 중인 서비스 및 프로세스 중 아래 프로세스를 제외한 서비스와 프로세스를 모두 종료

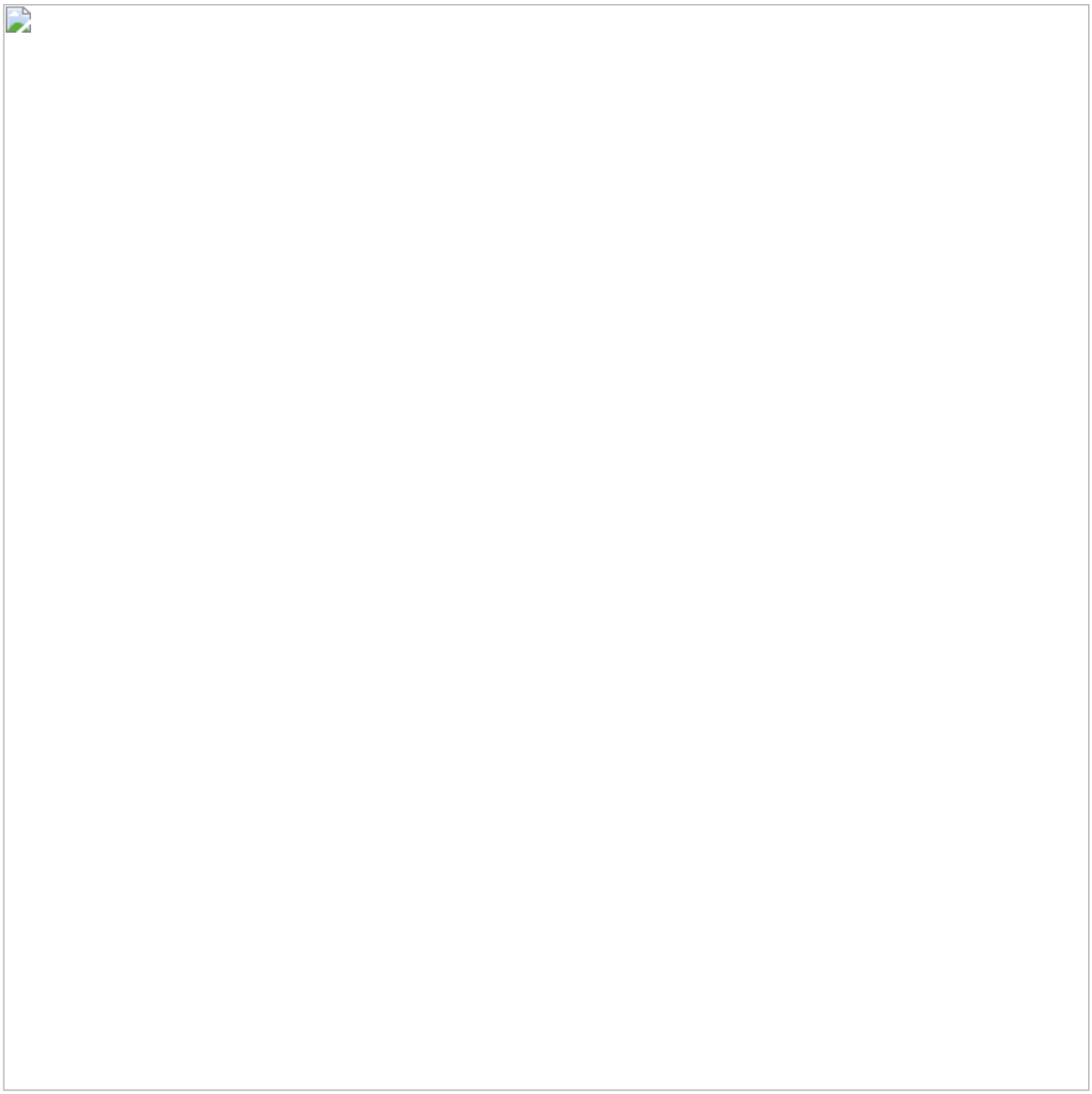


파일의 마지막 176byte위치의 32byte를 읽은 뒤 CRC32 checksum이 마지막 216byte위치의 4byte값과 동일한 경우, 이미 암호화가 된 파일로 판단하여 암호화 대상에서 제외

4) 파일 암호화

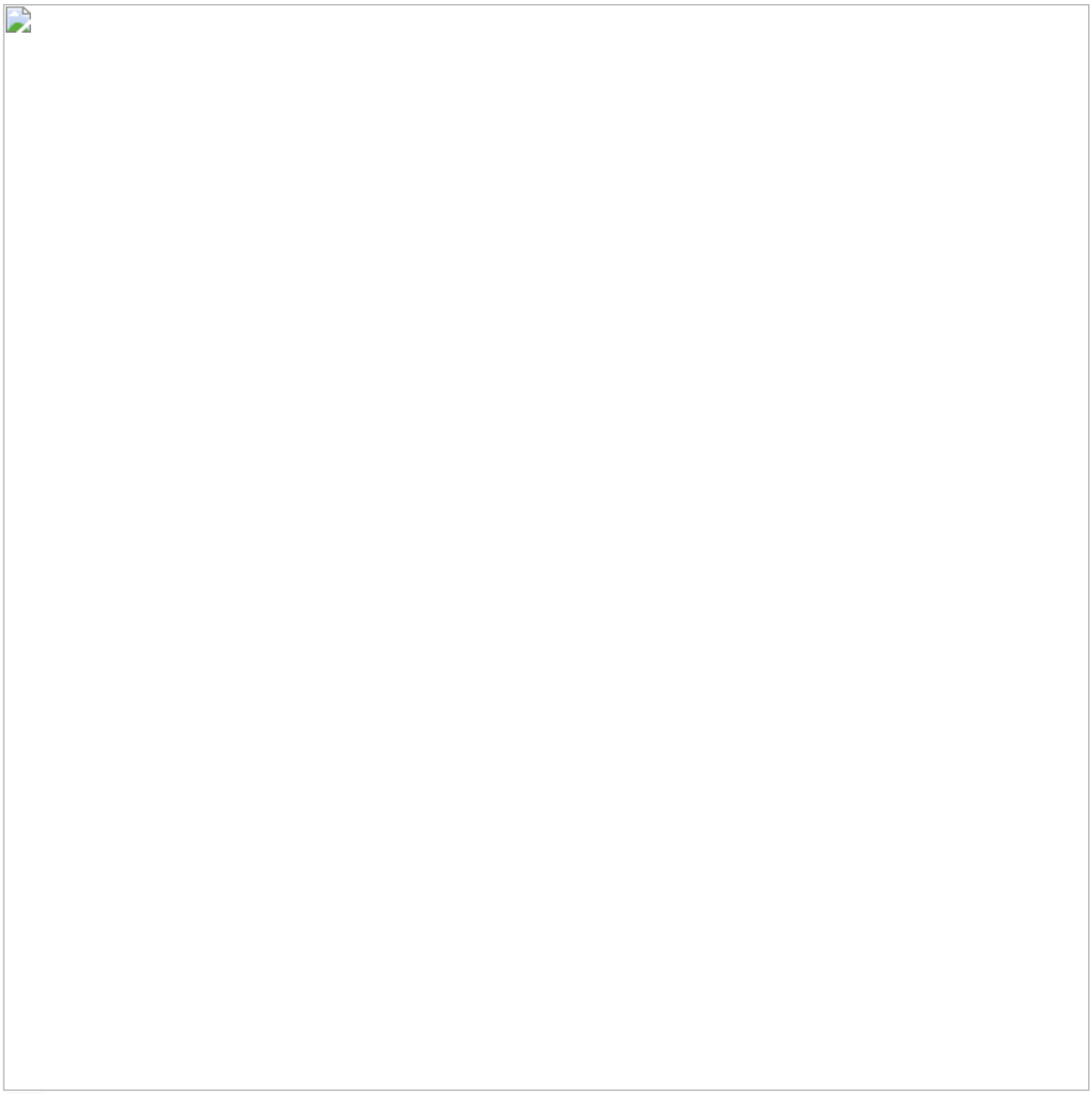
상세 옵션 중 `et` 에 따라 암호화 모드가 구분되며, 기본적으로 0x100000(1MB) 크기 단위로 파일 암호화가 이루어지고 아래와 같은 옵션에 따라 추가 암호화 크기가 정해짐

- , 파일 전체 암호화
- , 파일의 상위 0x100000만 암호화
- , 파일의 상위 0x100000암호화. 이후, spize 옵션에 명시된 크기만큼 간격을 두어 0x100000씩 추가로 파일 암호화 (spsize에 주어진 크기는 MB단위)



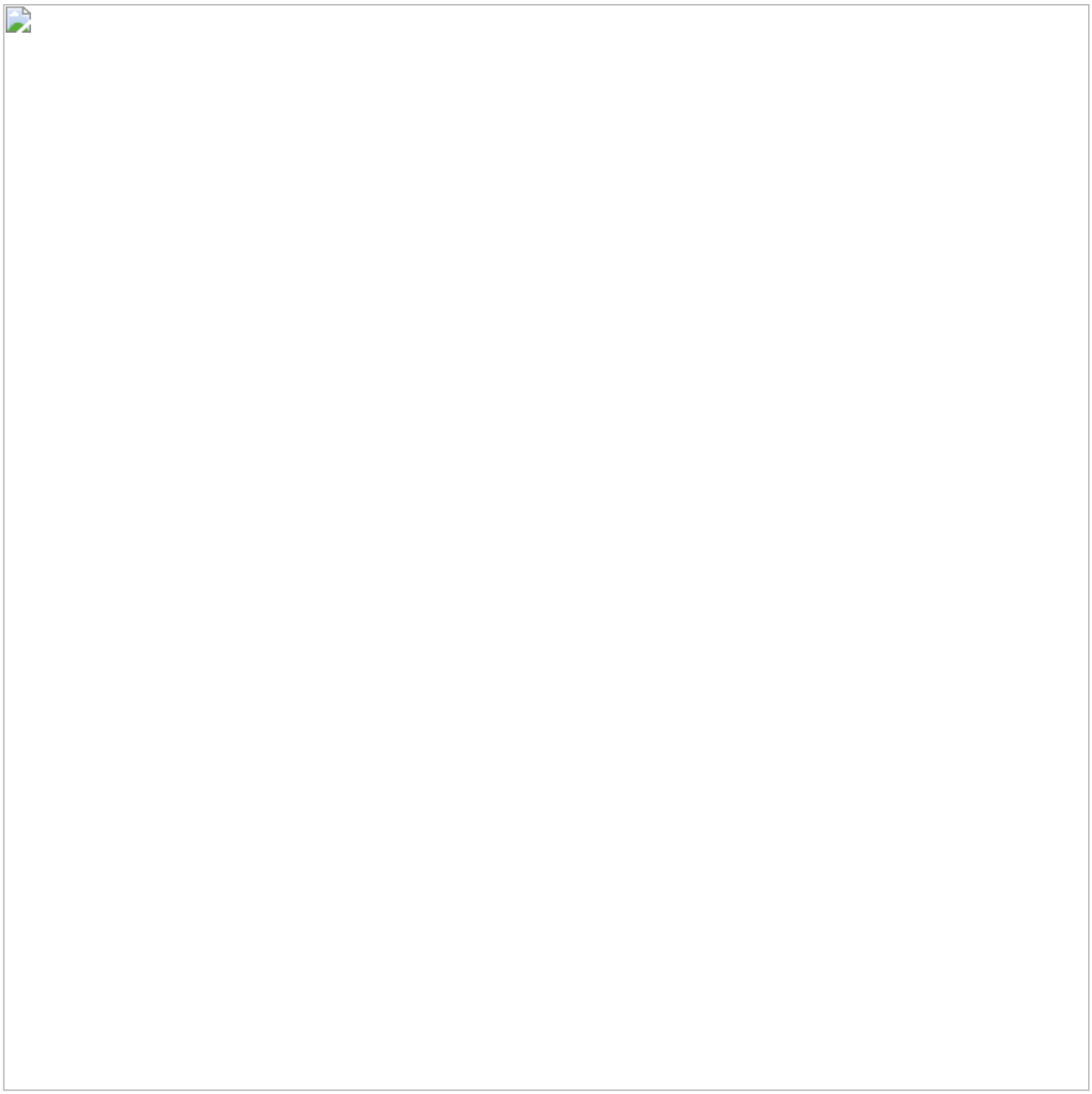
File Encryption Modes

파일 별로 4x4 key matrix를 생성하여 Salsa20 알고리즘으로 파일을 암호화하며, Salsa20에서 사용되는 key matrix 구조는 아래와 같음. REvil 랜섬웨어는 아래 Key영역에는 생성한 Shared Key의 SHA-3 해시 값을 사용하고, Nonce는 랜덤으로 생성한 8byte, Pos는 0으로 설정



`et` 에 따라 파일 암호화를 마친 뒤, 암호화에 사용된 232byte의 메타데이터를 파일에 추가

- sk_key struct : 공격자 공개키로 암호화된 비밀키 구조체
- 0_key struct : 제작자 마스터키로 암호화된 비밀키 구조체
- Meta data struct : 공개키, 암호화 모드 등이 포함된 암호화에 사용된 정보 구조체



Key struct and Meta data struct

4) 암호화 후 파일 확장자 변경

파일의 암호화가 완료되면 원본 파일의 확장자를 기존에 생성한 랜덤 문자열로 변경

5) 랜섬노트 생성

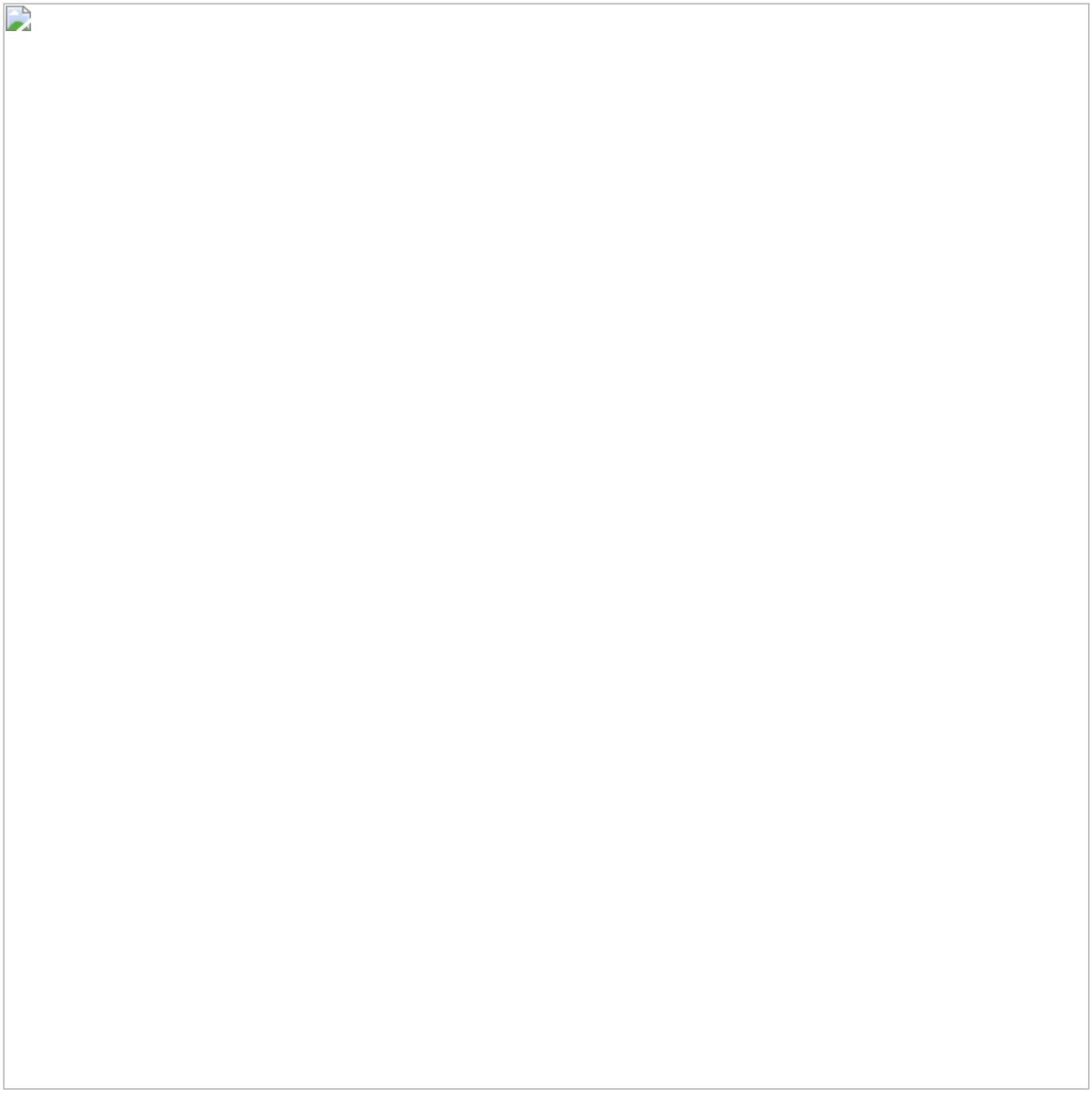
1. 상세 옵션 및 기존에 생성한 랜덤 확장자를 이용하여 폴더마다 랜섬노트 생성

2. `nbody` 옵션 : 랜섬노트 파일명 포맷 → [랜덤 확장자]-readme.txt

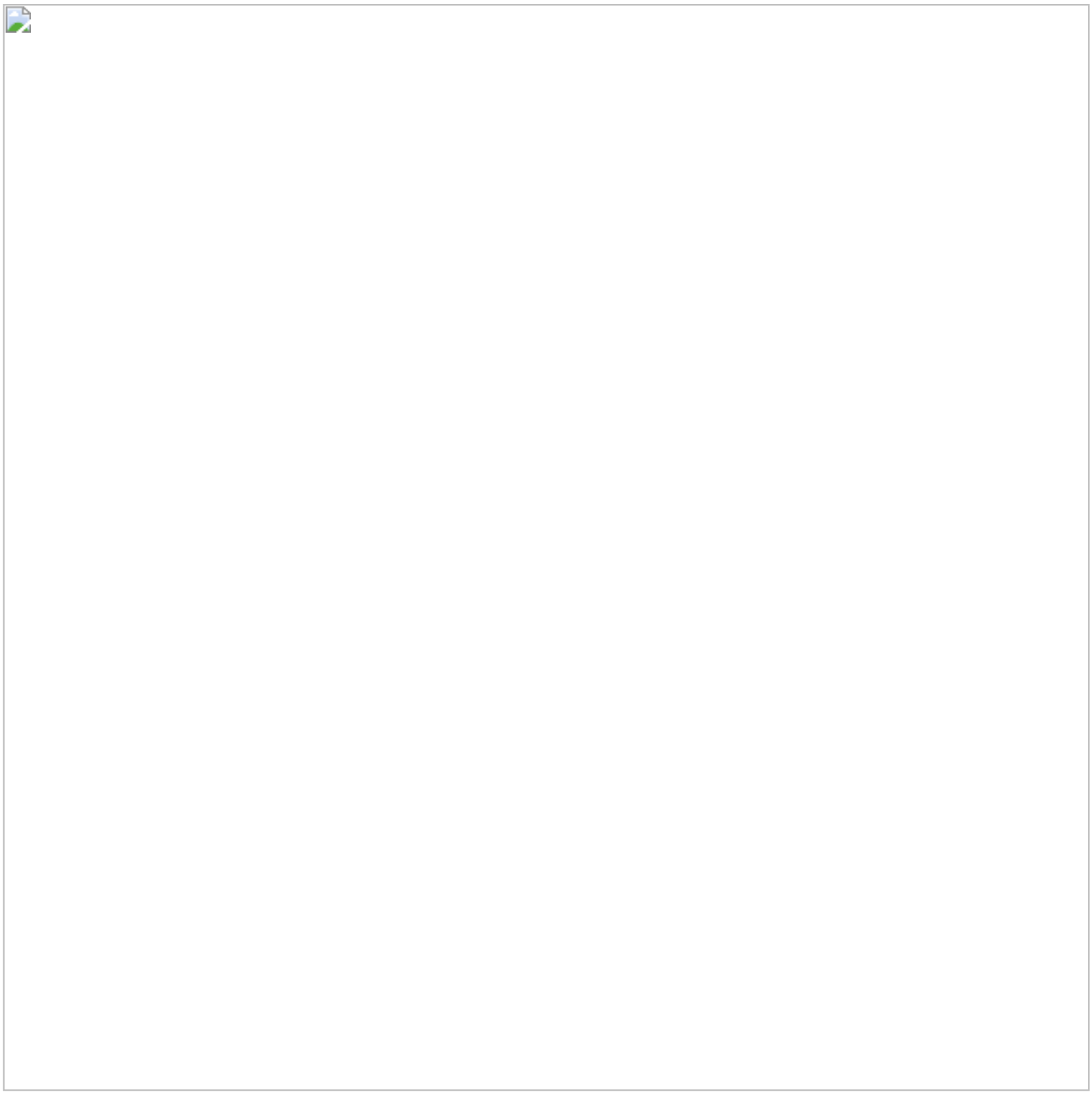
3. `nname` 옵션 : 랜섬노트 내용 포맷

- : 감염 기기 식별 값
- : 정보유출지로 전송한 수집된 정보의 base64 encoding 형태
- : 랜덤 확장자

4. 랜섬노트 예시



5. 암호화 전체 과정

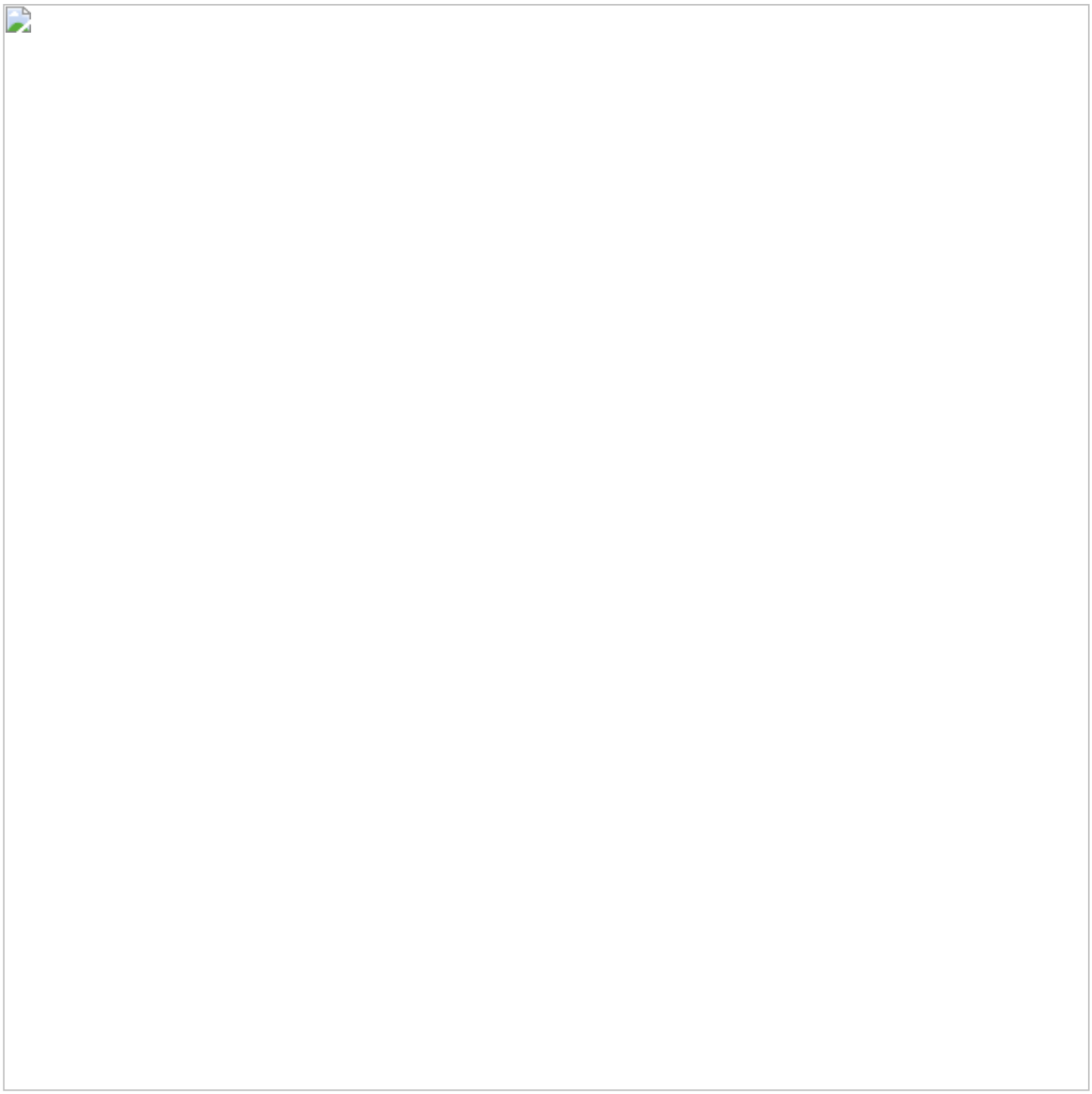


6) 복호화 예시

1. 공격자는 암호화된 파일로부터 sk_key struct에 있는 pk_new 추출

2. 공격자가 가지고 있는 dk와 pk_new를 이용하여 shared key 생성

- 이는 악성코드가 pk와 dk_new를 이용하여 생성한 shared key와 동일함
- ECDH (Elliiptic Curve Diffie-Hellman)상 아래 수식이 성립하기 때문

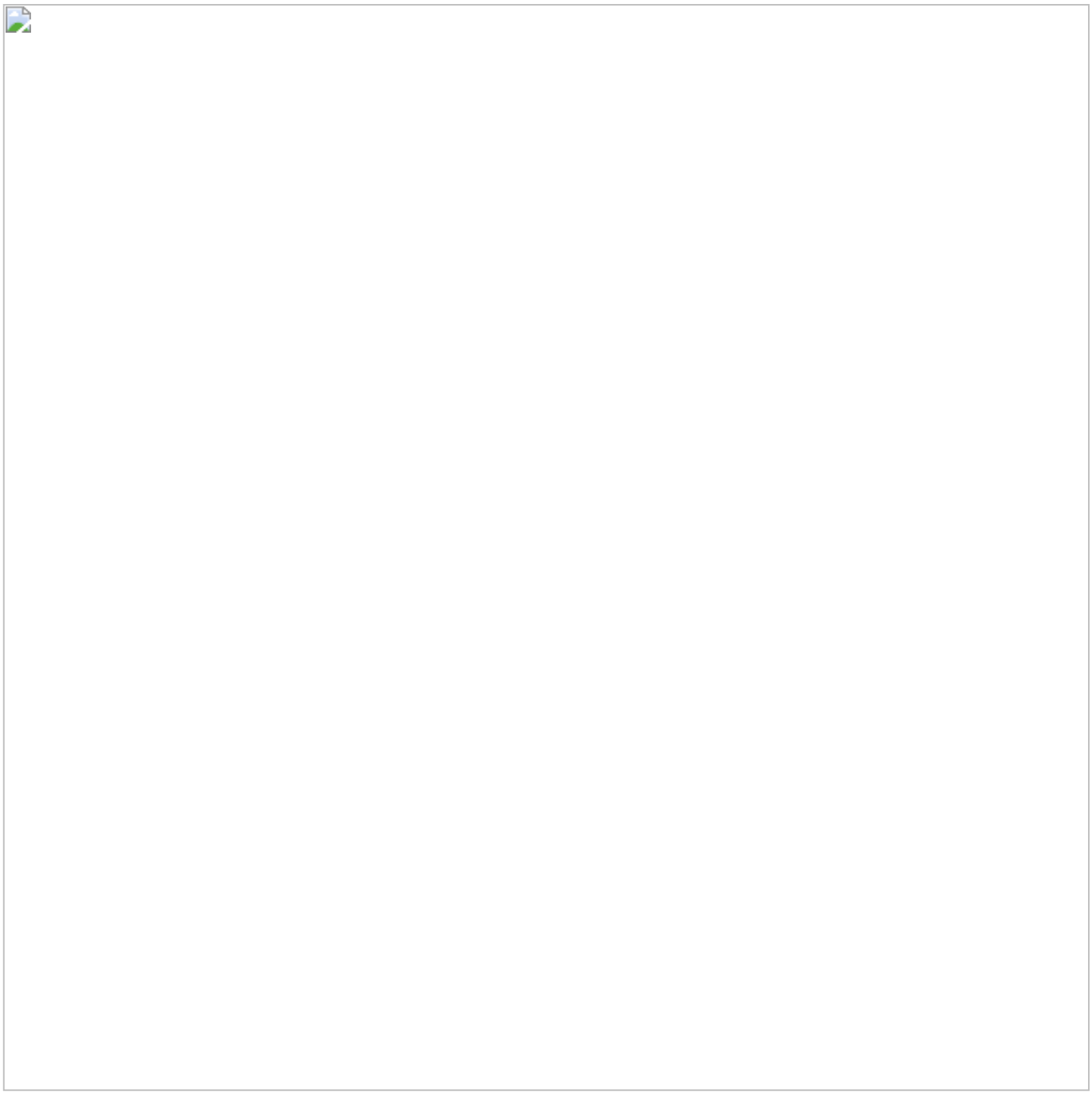


- dA: 공격자의 private key (dk)
- QA: 공격자의 public key (pk)
- dB: 악성코드의 private key (dk_key)
- QB: 악성코드의 public key (pk_key)

3. 생성한 shared key와 sk_key struct에 있는 AES IV로 복호화하여 dk_key 추출

4. 2와 동일한 방식으로 dk_key와 Meta data struct에 있는 pk_new_file로 shared key 생성

5. 생성한 shared key와 Meta data struct에 있는 Salsa nonce를 이용하여 Matrix 생성 후, Salsa IV와 함께 암호화된 파일 데이터 복호화



공격 ATT&CK

> 출처 : Reference에 명시된 분석 블로그 내 IoC 취합

Initial Access

1. 취약점을 통해 원격 명령어 실행 및 접속 시도

- 오라클 WebLogic 취약점 (CVE-2019–2725)
- Microsoft Exchange 서버 취약점 (정확한 CVE는 밝혀지지 않음)
- Sharepoint 취약점 (정확한 CVE는 밝혀지지 않음)

2. VPN 취약점을 통한 내부 파일 탈취 시도

- Pulse Secure SSL VPN (CVE-2019–11510)
- FortiOS SSL VPN (CVE-2018–13379)

3. RDP를 통한 침투

- 취약한 RDP 패스워드를 타겟하는 bruteforce 공격 시도
- 원격 코드 실행이 가능한 RDP Bluegate 취약점 (CVE-2020–0609, CVE-2020–0610)

4. 취약한 Citrix 계정을 통한 침투

5. 스팸 메일을 통해 다운로드 기능의 악성 매크로가 포함된 XLSM 파일 유포

- 숙소 예약 사이트 (booking.com)를 위장한 피싱 메일
- 해외 배소 업체 (DHL)로 위장한 피싱 메일
- DocuSign 전자 서명 메일로 위장한 피싱 메일

6. Supply chain

    이탈리아의 WinRAR 설치 프로그램 공식 사이트(winrar.it)를 통해 배포

7. RIG Exploit kit을 통해 배포

    RIG Exploit kit을 활용한 Malvertising 공격으로 감염 시도

8. MSSP 또는 MSP 업체를 장악 후, 경유하여 침투 시도

9. SEO-Poisoning 로 인해 검색엔진 상단에 노출되는 웹 사이트로부터 악성 파일 다운로드

Execution

1. Powershell (.ps1) 스크립트를 이용하여 명령어 실행

    DownloadFile 명령어를 통해 악성코드 다운로드 및 실행

2. 악성 코드를 드랍 및 실행하는 Javascript (.js) 스크립트

    난독화 된 javascript 스크립트를 실행시켜 추가 악성코드 다운로드

3. WMI (Windows Management Instrumentation) 쿼리를 이용하여 명령어 실행

4. 배치 스크립트를 이용하여 다수의 명령어를 동시에 실행

Persistence

1. 클라우드 원격 데스크톱 소프트웨어 계정을 통한 지속성 유지

    ConnectWise Control (구 ScreenConnect)을 설치 후 지속성 유지

2. Cobalt Strike 비콘을 통한 지속성 유지

3. VPN 취약점으로 지속성 유지

4. On-premise virtual desktop appliances를 통한 지속성 유지

5. Scheduled Task를 이용하여 주기적으로 악성코드 실행

6. 최초 침투 후 웹쉘을 삽입하여 지속성 유지

7. REvil 랜섬웨어는 옵션에 따라 부팅 시 자동실행 되도록 레지스트리에 등록

Privilege Escalation

1. CVE-2018–8453 취약점을 이용하여 로컬 권한 상승 시도

2. GPO(Group Policy Preferences)내에 포함된 패스워드로 로그인하여 권한 상승

3. 내부 망에서 수집한 계정정보를 통해 권한 상승 시도

4. Metasploit의 UAC-TokenMagic 파워쉘 스크립트로 UAC 우회

5. Invoke-SluiBypass 파워쉘 스크립트로 UAC 우회

6. REvil 랜섬웨어는 SeDebugPrivilege 권한을 할당하여 타 프로세스에 접근 시도

Defense Evasion

1. rundll32.exe 라는 정상 프로세스를 이용하여 악성 DLL 파일 실행

2. BITSAdmin 이라는 정상 도구를 이용하여 내부에 랜섬웨어 배포

3. REvil 랜섬웨어는 옵션에 따라 안전모드로 재부팅하여 파일 암호화

4. GPO(Group Policy Preferences)를 통해 Windows Defender 및 백신 비활성화

    배치 스크립트 사용

Credential Access

1. Mimikatz를 이용하여 크리덴셜 수집

2. ProcDump를 이용하여 lsass 프로세스 dump를 통해 크리덴셜 수집

Discovery

1. 윈도우 기본 제공 명령어를 통해 정보 탐색

- net : 네트워크 공유 및 워크스테이션 정보 수집

- nltest : 도메인 컨트롤러 및 신뢰할 수 있는 도메인 목록 수집
- ipconfig : 감염기기 전체 IP 정보 수집
- systeminfo : 감염기기 전체 시스템 정보 수집
- ping : icmp 를 통한 포트스캔 수행

2. Advanced Port Scanner 도구로 포트 스캐닝 수행

3. ADRecon을 이용하여 Active Directory 정보 수집

4. Everything을 이용하여 시스템 내 주요 파일 정보 수집

5. PoS Software 설치 여부 확인

6. SoftPerfect Network Scanner 도구로 내부 네트워크 스캔

7. Bloodhound도구로 LDAP 쿼리를 이용하여 Active Directory정보 수집

8. ADfind 도구로 Active Directory 정보 수집

Lateral Movement

1. Scheduled Task: 예약된 작업을 통해 측면 이동 수행

2. PsExec: 내부 대역에 악성코드 복사 후 원격으로 실행

3. Admin share: 네트워크 공유 기능으로 파일 복사 후 실행

5. WMIExec: WMI 명령어를 통해 내부 대역에 악성코드 복사 후 실행

6. CrackMapExec 도구로 측면 이동 수행

7. RDP 계정을 수집하여 측면 이동 수행

8. Cobalt Strike 기능으로 SMB를 통한 원격 서비스를 생성하여 측면 이동 수행

Command and Control

1. Cobalt Strike 비콘을 통한 감염기기 원격제어 수행

2. Gootkit, Qbot, IcedId 와 같은 유명한 악성코드를 통해 원격제어 명령 및 랜섬웨어 다운로드

3. Wget을 통해 추가 악성코드 다운로드

4. 파워쉘 스크립트로 pastebin의 특정 파일을 읽어와 디코딩 후 실행

Exfiltration

1. Rclone도구를 이용하여 공격자의 원격 서버로 파일 복사

2. Mega 클라우드를 이용하여 탈취한 데이터 저장

Impacts

1. 주요 파일 암호화

2. 주요 백업 및 안티 바이러스 서비스 중지

3. Volume Shadow Copy 삭제

4. VM Snapshot 삭제

5. File backup 삭제

6. 중요한 문서 삭제

Conclusion

REvil 랜섬웨어는 2019년 4월에 최초 등장한 이후, 약 2년이 넘는 시간 동안 다크웹 내 RaaS(Ransomware as a Service) 시장에서 최정상의 자리를 지키고 있다. 지속적인 버전 업데이트, 다양한 기능 및 상세 옵션을 통한 쉬운 커스터마이징이 가능하기 때문이다. 다수의 구매자들(또는 Operator)에 의해 개인부터 JBS와 같은 대형 기업 공격에까지 REvil 랜섬웨어를 이용한 광범위한 공격이 이루어지고 있다.

REvil로부터 파생된 조직들이 계속 생겨나고, 인터뷰를 통해 앞으로 더욱 더 적극적으로 공격할 것임을 밝히기도 했다. REvil은 몸값을 받아내기 위해 기업 정보 유출, DDoS, 파트너사 협박 등과 같은 전략을 취하고 있기 때문에 실제로 감염될 경우, 기업 내 큰 타격을 입을 수 있다.

랜섬웨어의 코드는 2년 동안 크게 바뀌지 않았지만, 이를 사용하는 공격자들이 많은 만큼 매우 다양한 최초 침투 경로, 공격 도구로 배포되고 있다. 그렇기 때문에 랜섬웨어 자체에 대해서만 대응하는 것이 아닌, 전체적인 공격 시나리오를 이해하고 자신 또는 기업의 취약한 부분을 확인하여 점검 및 보완할 수 있어야 한다.

Reference

1. https://blog.talosintelligence.com/2019/04/sodinokibi-ransomware-exploits-weblogic.html

2. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/sodinokibi-ransomware-cobalt-strike-pos

3. https://blog.amossys.fr/sodinokibi-malware-analysis.html

4. https://www.tgsoft.it/immagini/news/20190705Sodinokibi/Sodinokibi_eng.pdf

5. https://i.blackhat.com/eu-20/Wednesday/eu-20-Clarke-Its-Not-FINished-The-Evolving-Maturity-In-Ransomware-Operations.pdf

6. https://blog.malwarebytes.com/threat-analysis/2020/11/german-users-targeted-with-gootkit-banker-or-revil-ransomware/

7. https://asec.ahnlab.com/ko/19640/

8. https://thedfirreport.com/2021/03/29/sodinokibi-aka-revil-ransomware/

Appendix

Appendix #1 : REvil 랜섬웨어 탐지 야라 룰

```
rule REvil_Ransomware_V2_5{    meta:        description = "REvil ransomware v2.05
detection rule"        author = "S2WLAB TALON"        date = "2021-06-23"        version
= "1.0"    strings:        $pattern1 = "ERR0R D0UBLE RUN!" ascii wide nocase
$pattern2 = "vmcompute.exe" ascii wide nocase        $pattern3 = "vmms.exe" ascii wide
nocase        $pattern4 = "vmwp.exe" ascii wide nocase        $pattern5 = "svchost.exe"
ascii wide nocase        $pattern6 = "DTrump4ever" ascii wide nocase        $pattern7 =
"expand 32-byte k" ascii wide nocase        $pattern8 = "expand 16-byte k" ascii wide
nocase        $pattern9 = "__ProviderArchitecture" ascii wide nocase        $code1 = {83
EC 10 B9 5B 04 00 00 53 56 8B 75 08 [0-8] C1 E6 10 33 75 08 81 F6 ?? ?? ?? ?? 8B C6 C1
E8 15 57}        $code2 = {8B 55 08 40 0F B6 C8 8B 45 08 89 4D 10 8B 5D 10 8A 0C 01 0F
B6 C1 03 C6 0F B6 F0 8B 45 08 8A 04 06 88 04 13 8B C2 8B D3 8B 5D 14 88 0C 06 0F B6 04
02 8B 55 0C 0F B6 C9 03 C8 0F B6 C1 8B 4D 08 8A 04 08 32 04 1A 88 03 43 8B 45 10 89 5D
14 83 EF 01 75} // rc4    condition:        ( 8 of ($pattern*) and $code1 ) or        (
8 of ($pattern*) and $code2 )}rule REvil_Ransomware_V1_6{    meta:        description =
"REvil ransomware v1.06 detection rule"        author = "S2WLAB TALON hypen"        date
= "2021-06-23"        version = "1.0"    strings:        $pattern1 = "ServicesActive"
ascii wide nocase        $pattern2 = "expand 32-byte k" ascii wide nocase
$pattern3 = "expand 16-byte k" ascii wide nocase        $code1 = {11 f8 90 45 3a 1d d0
11 89 1f 00 aa 00 4b 2e 24 28 20 bd 49 23 15 d1 11 ad 79 00 c0 4f d8 fd ff 87 a6 12 dc
7f 73 cf 11 88 4d 00 aa 00     4b 2e     24} // rscid        $code2 = {8B 55 08 40 0F B6
C8 8B 45 08 89 4D 10 8B 5D 10 8A 0C 01 0F B6 C1 03 C6 0F B6 F0 8B 45 08 8A 04 06 88 04
13 8B C2 8B D3 8B 5D 14 88 0C 06 0F     B6 04 02 8B 55 0C 0F B6 C9 03 C8 0F B6 C1 8B 4D
08 8A 04 08 32 04 1A 88 03 43 8B 45 10 89 5D 14 83 EF 01 75} // rc4    condition:
all of them}
```

Appendix #2 : Sigma rule

> 출처 : https://thedfirreport.com/2021/03/29/sodinokibi-aka-revil-ransomware/

https://github.com/Neo23x0/sigma/blob/master/rules/windows/process_creation/win_susp_powershell_enc_cmd.yml

https://github.com/Neo23x0/sigma/blob/084cd39505861188d9d8f2d5c0f2835e4f750a3f/rules/windows/process_creation/win_malware_trickbot_recon_activity.yml

https://github.com/Neo23x0/sigma/blob/master/rules/windows/process_creation/win_susp_commands_recon_activity.yml

https://github.com/SigmaHQ/sigma/blob/master/rules/windows/network_connection/sysmon_rundll32_net_connections.yml

https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_process_creation_bitsadmin_download.yml

https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_adfind.yml

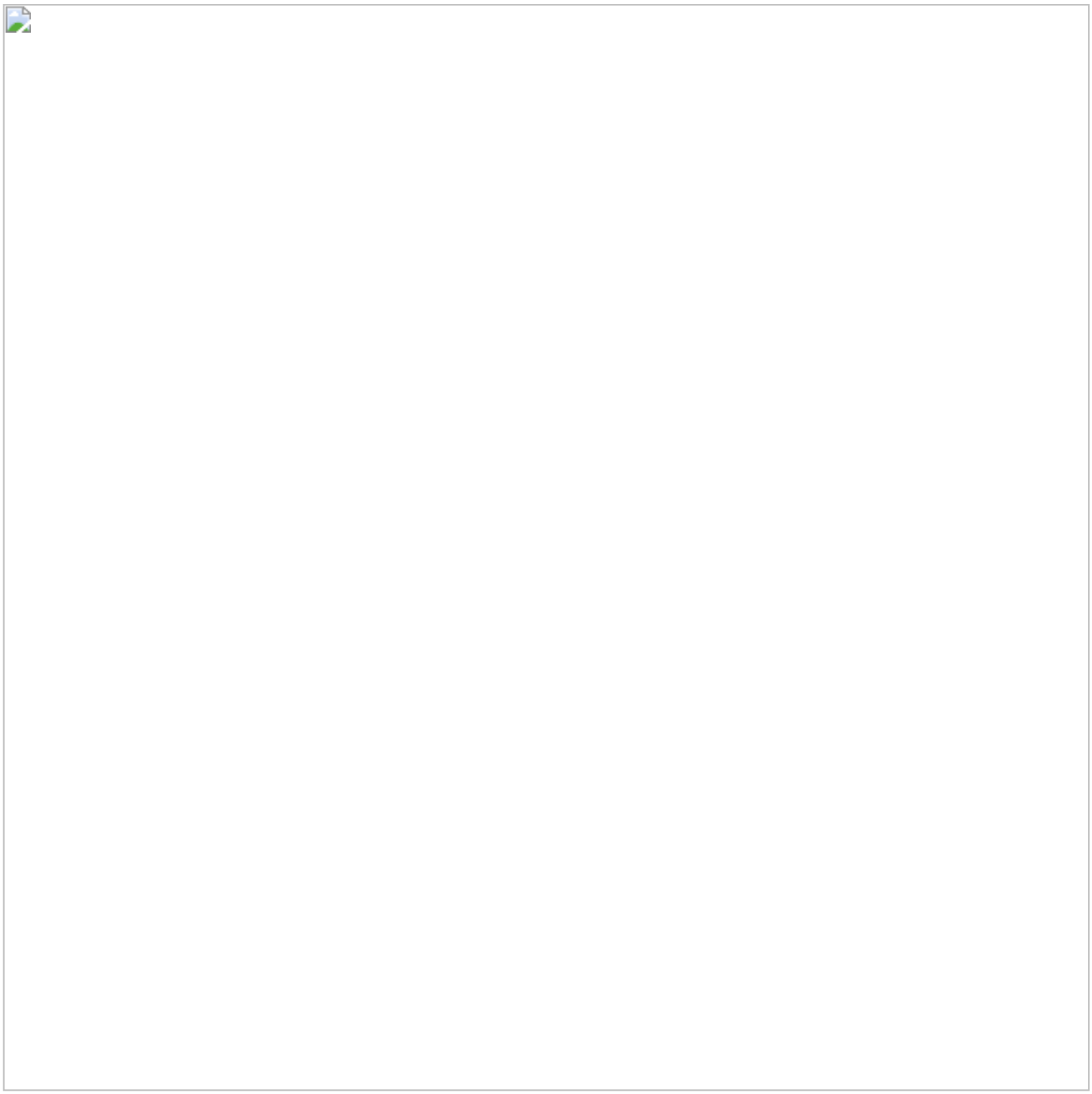
https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_wmi_execution.yml

https://github.com/SigmaHQ/sigma/blob/a08571be9107d1c0e216400ffbb89c394fcd2570/rules/windows/process_creation/win_office_shell.yml

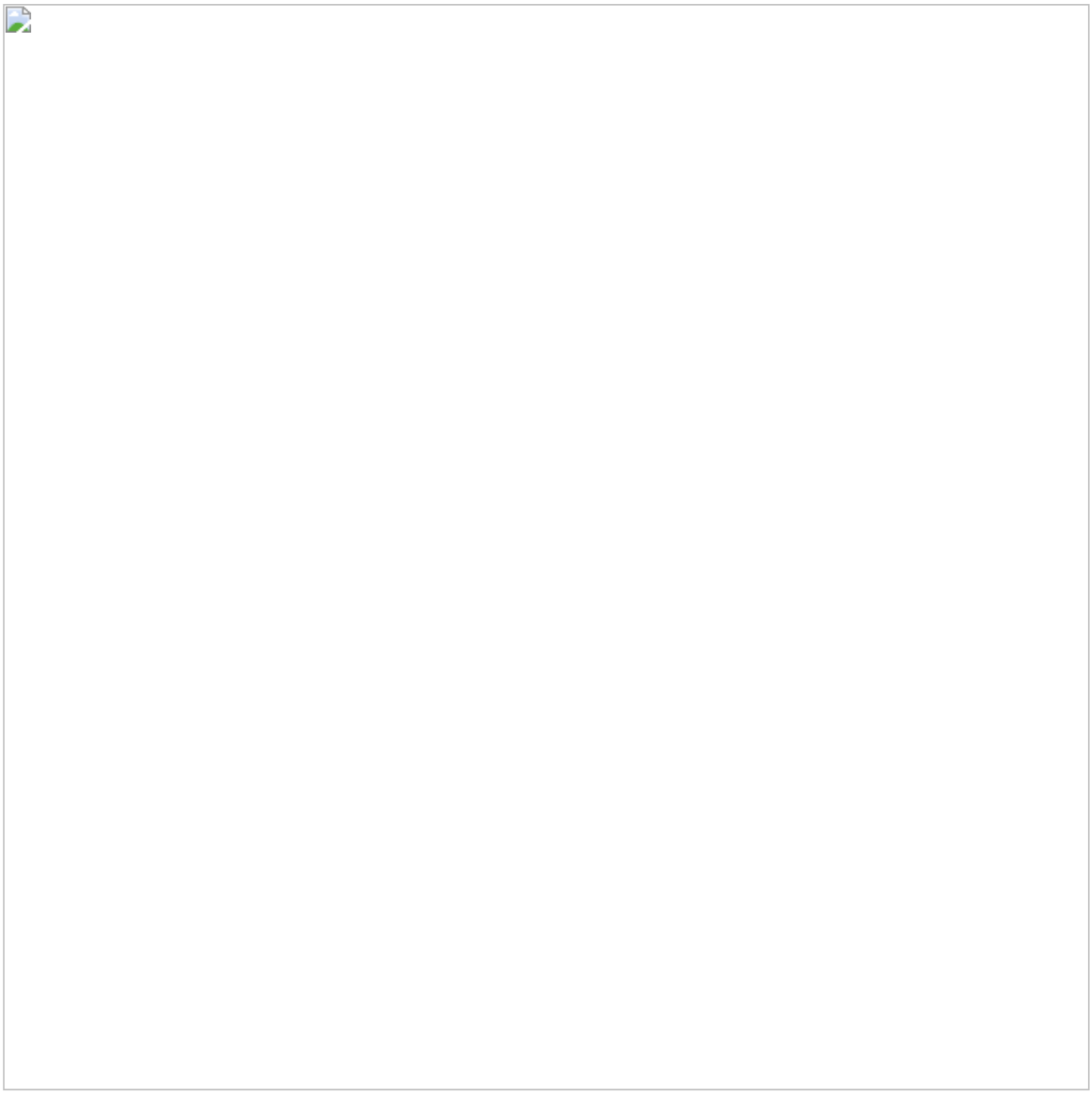
Appendix #3 : IoC

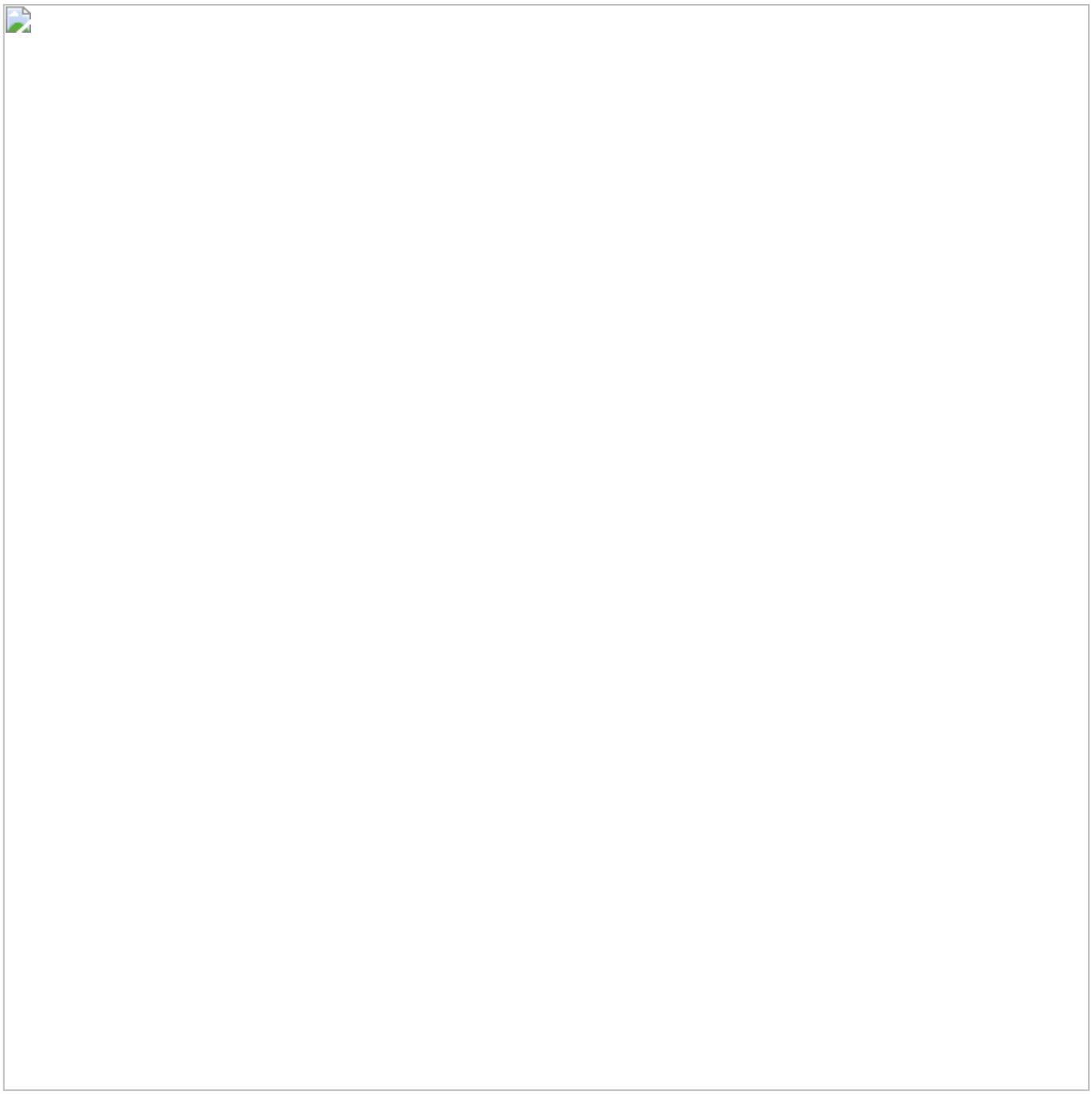
Click the below image then redirect to google spreadsheet

> 출처 : Reference에 명시된 분석 블로그 내 IoC 취합



Appendix #4 : REvil 협상 사이트 페이지 (최초 Key 입력 및 캡차 유도)





Appendix #5 : v2.05와 v2.07 비교

> 현재까지 발견된 REvil 랜섬웨어의 가장 최신 버전은 2.07로 확인됨

1. 로컬 드라이브 암호화

- 2.07 버전에서는 로컬 드라이브 암호화 시, 드라이브 타입이 DRIVE_FIXED(일반 디스크)일 경우, NetShareAdd 함수로 로컬 공유 시작
- NetShareAdd 함수를 이용한 감염 단말 리소스 공유시 사용되는 comment (SHARE_INFO_2 구조체 내 shi2_remark 멤버 변수) 문자열 : “Share added by R”

2. 네트워크 드라이브 암호화

- 2.07 버전에서는 네트워크 드라이브 암호화 함수를 Thread로 생성하지 않음
- 기존에는 explorer.exe의 토큰을 impersonate하여 네트워크 공유 탐색 권한을 획득하였는데, 2.07 버전에서는 이에 더해 현재 Thread를 제외한 현재 프로세스 내 모든 Thread에 동일한 토큰 적용
- 이후 복제된 토큰으로 네트워크 드라이브 암호화를 시도하고, RevertToSelf로 impersonate 종료 후에 한번 더 네트워크 드라이브 암호화를 시도함