랜섬웨어 통합 복구도구
사용 매뉴얼
- Hive 버전1 ~ 버전4 -

2022. 06

차세대암호융합팀

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

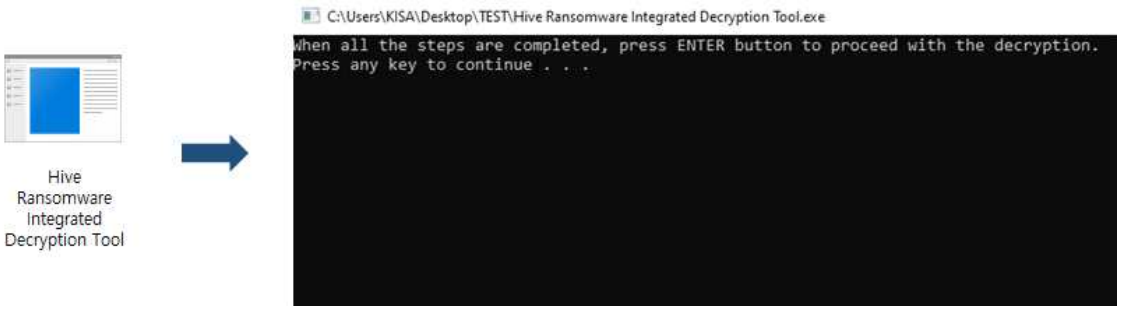
통합 복구도구 사용 방법

주의 : 먼저 시스템에서 악성코드를 삭제하시기 바랍니다. 그렇지 않으면 감염 파일이 복구되더라도 다시 감염될 수 있습니다.
Hive 랜섬웨어의 암호학적 특성상 100% 복구는 어렵습니다.
오사용으로 인한 문제 발생 시 책임지지 않습니다.
통합 복구도구는 연속적으로 동작하기 때문에 중간에 프로그램을 종료하면 파일 복구가 불가능합니다.

통합 복구도구는 Hive 랜섬웨어 버전1부터 버전4까지 복구 가능하다. 다만, 버전2의 경우 감염된 파일의 확장자가 '.w2tnk', '.uj1ps'인 경우에만 복구 가능하다.

1. 통합 복구도구 실행

Hive 랜섬웨어 통합 복구도구(Hive Ransomware Integrated Decryption Tool.exe)를 관리자 권한으로 실행하면 명령 프롬프트(CMD) 창이 나타난다.



그리고, 복구도구가 위치한 경로에 4개의 폴더가 생성된다. 생성된 폴더에 랜섬웨어 공격자가 암호화한 암호키 파일, 감염된 파일, 원본 파일, 복구할 파일을 복사하면 파일 복구 준비가 완료된다.

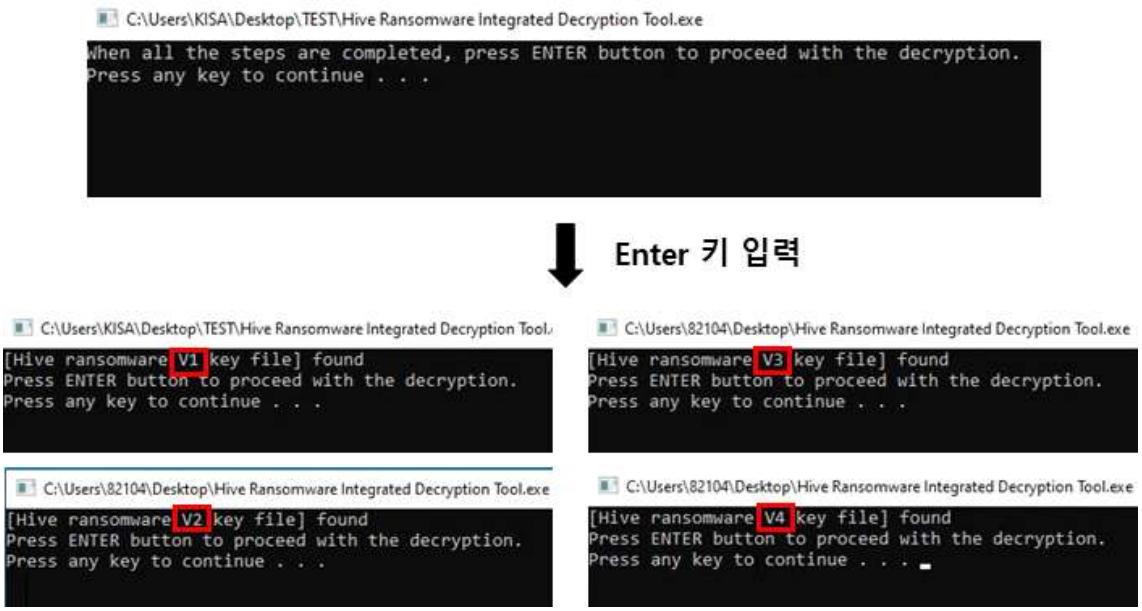
폴더명		복사 대상
0_Encrypted_keyfile	⇨	공격자가 암호화한 암호키 파일
1_infected_files	⇨	감염된 파일
2_original_files	⇨	감염된 파일의 원본 파일
3_recovery_target_files	⇨	복구할 파일

2. 버전 확인

Hive 랜섬웨어 버전은 감염 시 C 드라이브에 생성된 랜섬웨어 공격자가 암호화한 암호키의 파일 확장자와 크기를 보고 확인할 수 있다. 다만, 버전1의 경우 실행 프로그램이 관리자 권한으로 실행되지 않으면 가상화 폴더에 암호화된 암호키가 생성된다. 가상화 폴더에 대한 내용은 '3.1.1. 버전1' 목차에서 자세하게 확인할 수 있다.

버전	파일명	파일 확장자	파일 크기	예시
1	랜덤한 문자열	.hive	약 10MB	Jub3Ee9tNMK1Wy0PRwuVTw.**key.hive**
2		.w2tnk	약 10MB	Ns9SQ_476LclOK71vDYbAwrFKbt.**key.w2tnk**
		.uj1ps		wMeaAeiQD-vkcgjVMdenTtLGAST.**key.uj1ps**
3		랜덤한 문자열	약 3KB, 100KB, 1MB	xDKszTbfp3gyp7ixGWIWuZp5iS0B.**key.fayg2**
4		랜덤한 문자열	약 3MB	VICqe_MNCP-TubaUvhZ4IU5f1rqr.**key.bvddx**

암호화된 암호키를 0_Encrypted_keyfile 폴더에 복사한 후, 이전 창에서 Enter 키를 입력하면 Hive 랜섬웨어 버전을 확인하고 결과를 알려준다.



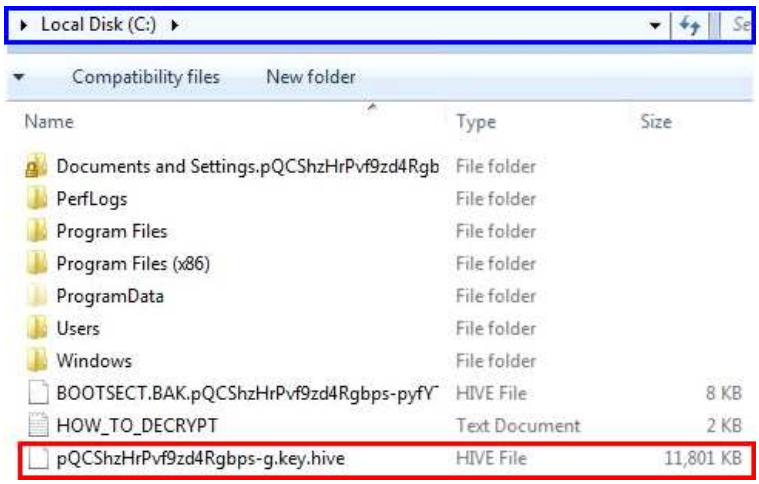
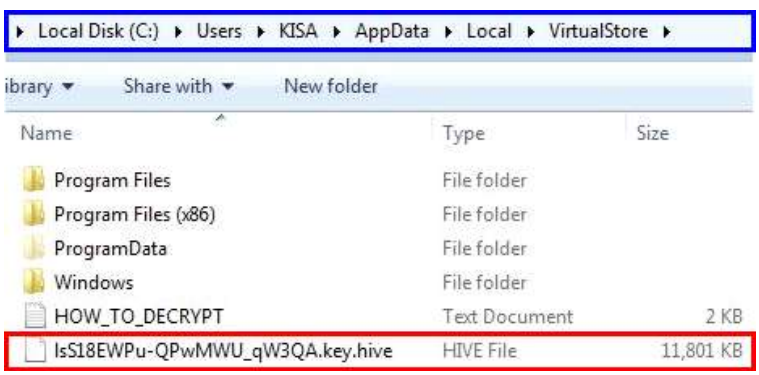
3. 원본 파일 수집

3.1. 버전에 따른 원본 파일 수집 방법

Hive 랜섬웨어 통합 복구도구를 사용하려면 감염된 파일과 감염된 파일의 원본 파일이 필요하다. 버전1부터 버전4까지의 원본 파일 수집 방법은 기본적으로 동일하다. 하지만, 버전1은 랜섬웨어 실행 프로그램이 관리자 권한으로 실행되지 않은 경우에 원본 파일을 다른 방법으로 수집해야 한다.

3.1.1. 버전1

Hive 랜섬웨어 버전1 실행 프로그램의 관리자 권한 실행 여부는 공격자가 암호화한 파일 암호키의 위치를 보고 확인할 수 있다. 관리자 권한으로 실행된 경우 루트 디렉터리(C 드라이브), 그렇지 않은 경우 가상화 폴더(C:\Users\<User_name>\AppData\Local\VirtualStore)에 암호화된 파일 암호키가 존재한다. 파일명은 '랜덤한 문자열.key.hive'이며, 파일 크기는 약 10MB이다.

관리자 권한 실행 여부	암호화된 파일 암호키 위치
관리자 권한으로 실행됨 (C 드라이브)	
관리자 권한으로 실행되지 않음 (가상화 폴더)	

① **관리자 권한으로 실행된 경우**

Hive 랜섬웨어가 관리자 권한으로 실행되면 가상화 폴더(VirtualStore)에 감염된 파일이 생성되지 않지만, C 드라이브의 'Program Files', 'Program Files(x86)', 'ProgramData' 폴더에 감염된 파일이 생성되고 해당 파일의 원본 파일은 삭제된다.

이 경우에 감염된 PC에 설치된 프로그램과 동일한 버전을 재설치하여 원본 파일을 수집할 수 있다. 프로그램을 재설치하면 'Program Files', 'Program Files(x86)' 등의 설치 경로에 '.lib', '.dll' 형태의 라이브러리 파일, '.jpeg', '.png' 형태의 사진 파일 등 다양한 형태의 파일이 생성된다. 해당 파일을 감염된 파일과 비교하는 과정을 반복하면 많은 양의 원본 파일을 수집할 수 있다.

또한, 이메일을 통해 송·수신한 파일, USB 저장 장치에 있는 파일, 클라우드 스토리지에 저장된 파일을 감염된 파일과 비교하여 원본 파일을 수집하는 방법도 있다.

② **관리자 권한으로 실행되지 않은 경우**

Hive 랜섬웨어가 관리자 권한으로 실행되지 않으면 가상화 폴더(Virtual Store)에 감염된 파일이 생성된다. 감염된 파일의 원본 파일은 C 드라이브의 'Program Files', 'Program Files(x86)', 'ProgramData' 폴더에 있다. 해당 원본 파일과 가상화 폴더의 감염된 파일을 이용하여 암호키 복구가 가능하며, 원본 파일이 삭제된 감염된 문서, 사진, 동영상 등의 파일을 복구할 수 있다.

3.1.2. 버전2 ~ 버전4

Hive 랜섬웨어 버전2부터 버전4까지 감염된 파일의 원본 파일을 수집하는 방법은 '3.1.1. 버전1'의 ① 관리자 권한으로 실행된 경우와 같다. 따라서 해당 방법을 사용하여 감염된 파일의 원본 파일을 수집하면 된다.

3.2. 조건

감염된 파일과 원본 파일을 수집할 시 3가지 조건을 만족해야 한다. 조건이 만족되지 않은 상태에서 복구를 수행하면 에러가 발생하거나 복구도구 프로그램이 종료된다. 해당 조건은 아래와 같다.

> 감염된 파일과 원본 파일은
>
> ① **이름**이 같아야 한다.
> ② **총 개수**가 같아야 한다.
> ③ **버전**이 같아야 한다.

Hive 랜섬웨어의 암호학적 특성으로 인해 복구에 필요한 파일의 개수는 가변적이어서 정량화하기 어려우므로, 아래의 설명을 참고하는 것을 권장한다.

버전1의 경우 파일의 총 크기에 따라 복구에 필요한 파일의 개수가 달라진다. 파일의 총 크기를 50KB 이하로 구성할 경우 500 ~ 1,000개의 파일, 1 ~ 5MB 사이로 구성할 경우 100개 이상의 파일, 25MB로 구성할 경우 30 ~ 50개 사이의 파일이 필요하다.

버전	파일의 총 크기	필요한 파일 개수
1	50KB 이하	500 ~ 1,000개
	1 ~ 5MB	100개 이상
	25MB	30 ~ 50개

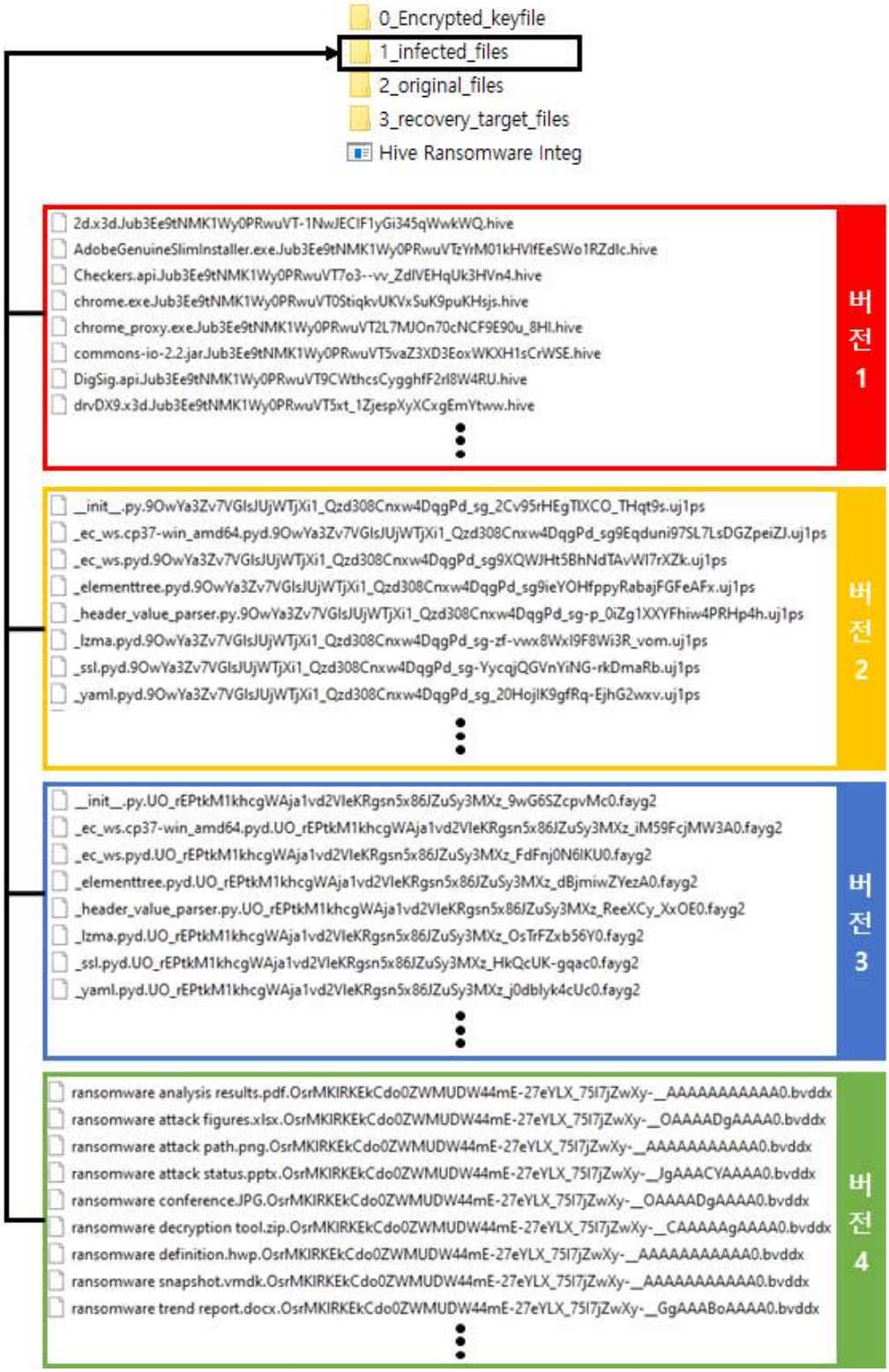
버전2부터 버전4까지의 경우 개별 파일의 크기에 따라 복구에 필요한 파일의 개수가 달라진다. 버전2 중 감염된 파일의 확장자가 '.w2tnk'인 경우 86KB 이상 크기의 파일 500 ~ 1,000개, '.uj1ps'인 경우 128KB 이상 크기의 파일 1,000개 또는 345KB 이상 크기의 파일 500개가 필요하다. 버전3인 경우 128KB 이상 크기의 파일 100개, 버전4인 경우 5KB 이상 크기의 파일 5개 이상 필요하다.

버전		개별 파일의 크기	필요한 파일 개수
2	w2tnk	86KB 이상	500 ~ 1,000개
	uj1ps	128KB 이상	1,000개
		345KB 이상	500개
3		128KB 이상	100개
4		5KB 이상	5개 이상

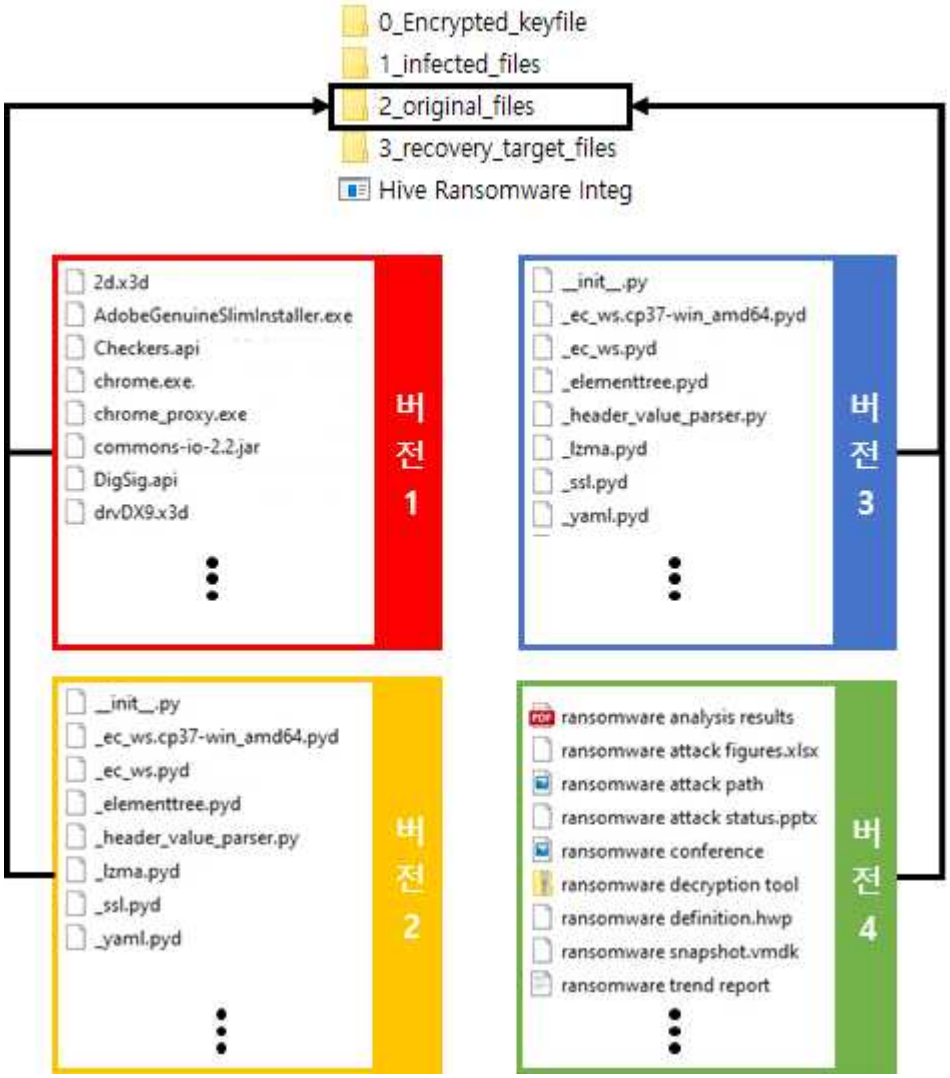
복구에 필요한 파일의 개수는 버전에 따라 파일의 총 크기 또는 개별 파일의 크기와 반비례 관계여서 사용자가 임의로 필요한 파일의 개수를 조정할 수 있으며, 이에 따라 복구율은 달라질 수 있다. 다만, 개수가 너무 적으면 암호키 복구에 필요한 값들을 추출할 수 없으니 이 점을 주의해야 한다(버전4 제외).

4. 복구 수행

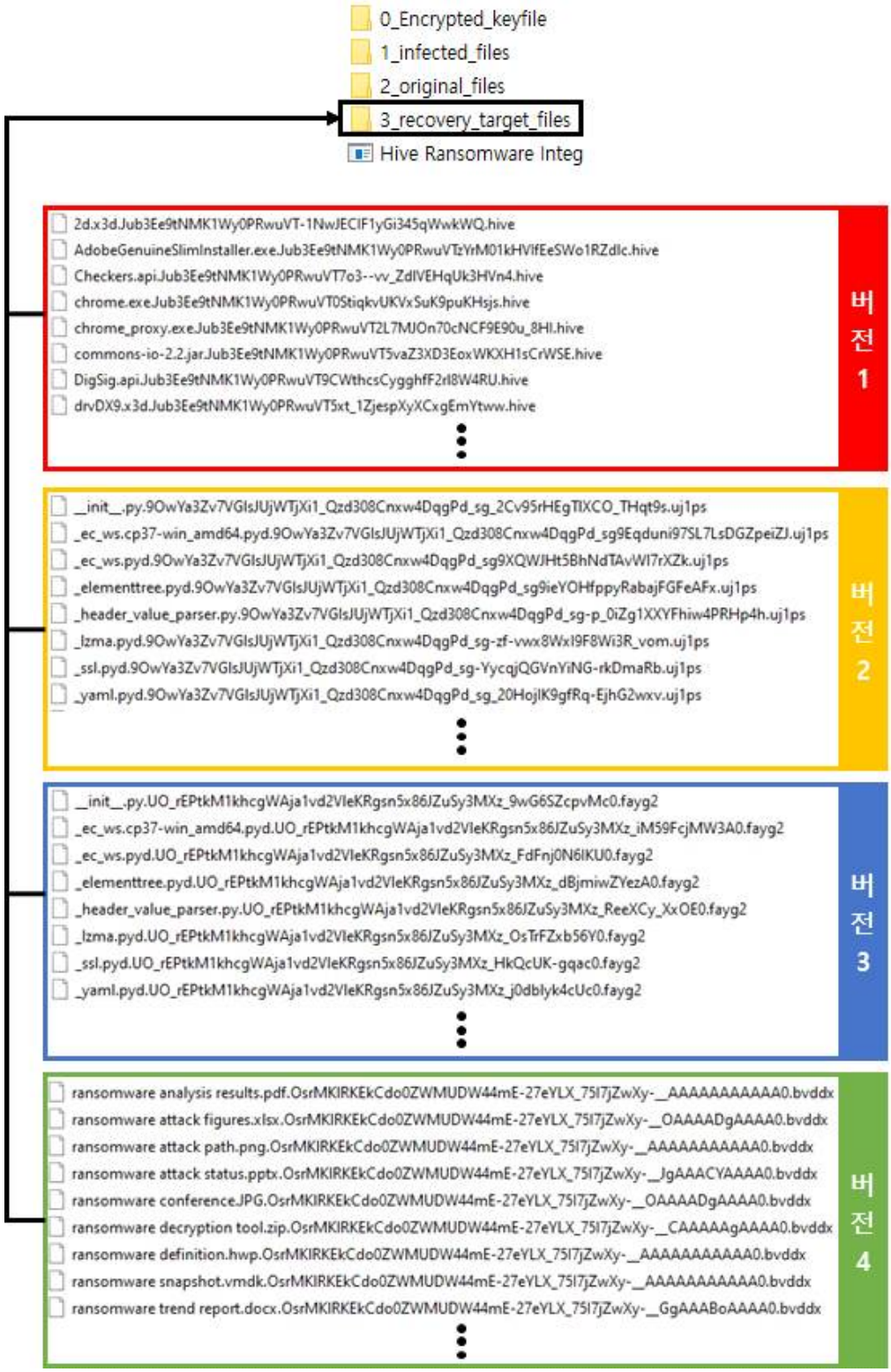
원본 파일 수집이 완료된 후, 감염된 파일을 '1_infected_files' 폴더에 복사한다.



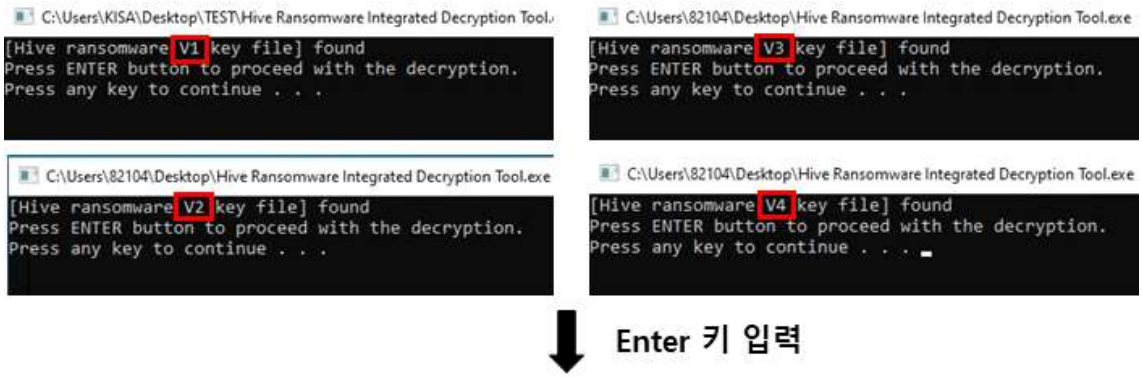
그다음, 원본 파일을 '2_original_files' 폴더에 복사한다.



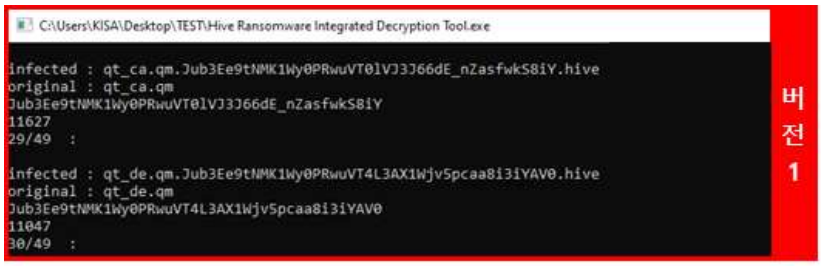
마지막으로, 복구할 파일을 '3_recovery_target_files' 폴더에 복사한다.

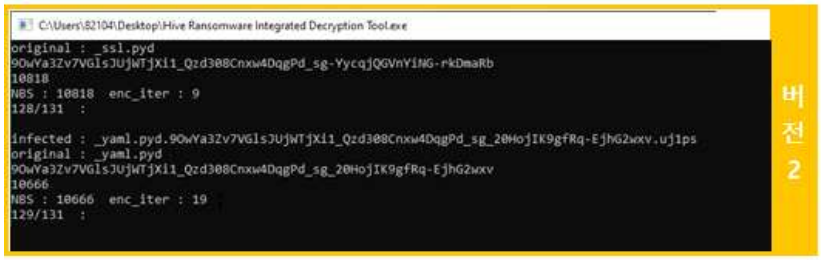


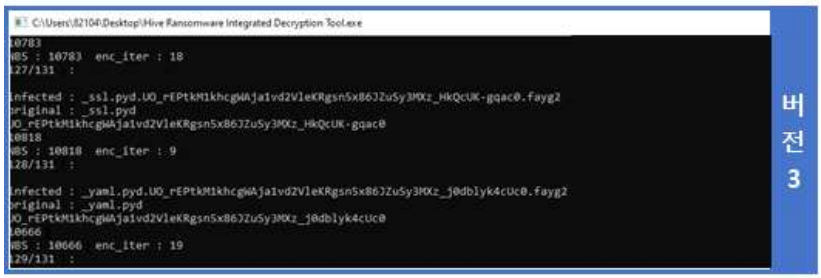
복구에 필요한 파일과 복구할 파일을 각 폴더에 복사한 후 이전 창에서 Enter 키를 입력한다. 복구도구는 감염된 파일과 원본 파일을 이용하여 복구에 필요한 값들을 추출하고 암호키를 복구한다. 감염된 파일과 원본 파일의 개수에 따라 암호키 복구에 소요되는 시간이 다를 수 있다.

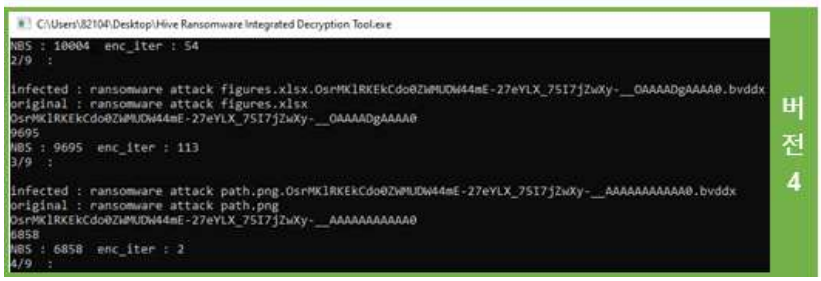


Enter 키 입력

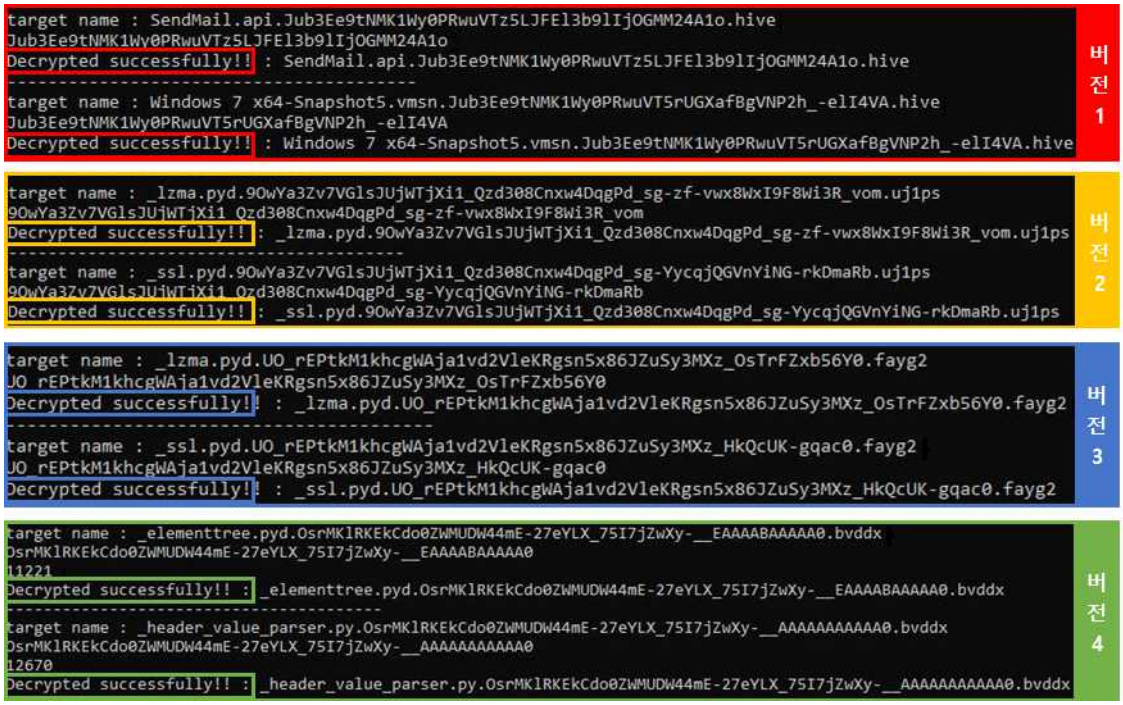




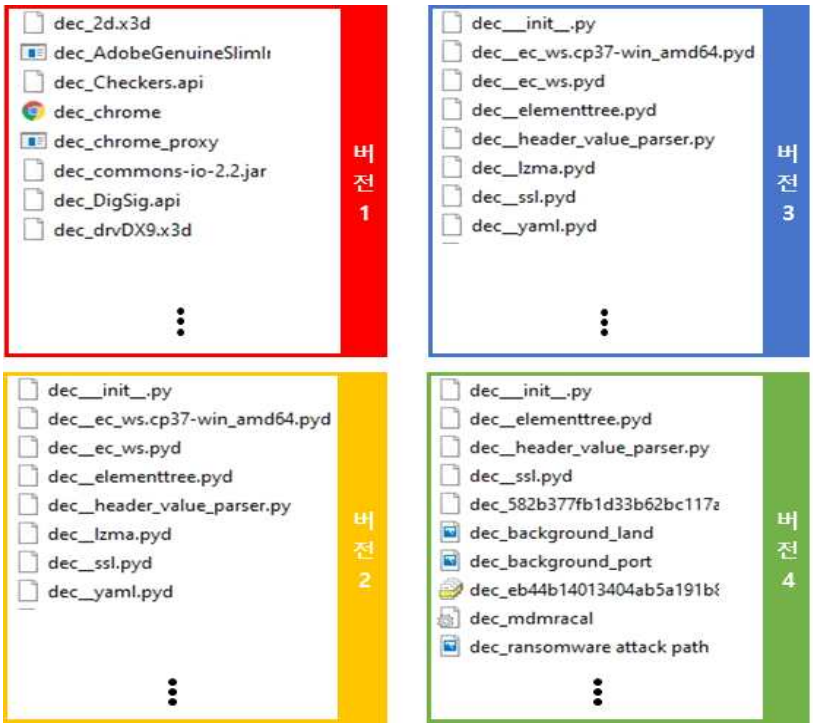




암호키 복구가 완료되면 '3_recovery_target_files' 폴더에 있는 파일을 대상으로 복구를 수행한다. 복구가 성공한 파일에 대해서는 'Decrypted successfully!!'라는 문자열이 창에 출력된다.



복구가 완료되면 '3_recovery_target_files' 폴더에 복구된 파일이 생성된다. 해당 파일 이름 앞에 'dec_'라는 문자열이 추가되어 감염된 파일과 구분된다.



Hive 랜섬웨어란?

Hive 랜섬웨어는 2021년 6월에 발견된 랜섬웨어이며 주로 기업을 대상으로 공격한다. 다양한 방법을 사용해 공격 대상 시스템에 침투하여 랜섬웨어를 배포한다. 현재 다양한 변종이 계속해서 발견되고 있어 감염되지 않도록 각별한 주의가 필요하다.

Hive 랜섬웨어 통합 복구도구 사용 매뉴얼

2022년 6월

발행처 KISA 한국인터넷진흥원 KOREA INTERNET & SECURITY AGENCY