asec.ahnlab.com /ko/90628/

RenPy로 제작된 게임으로 위장한 Rhadamanthys 악성코드 유포

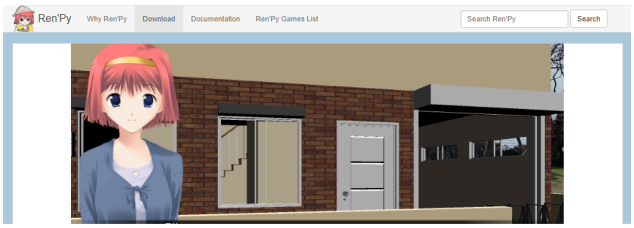
⋮ 10/19/2025

악성코드

- 2025년 10월 20일

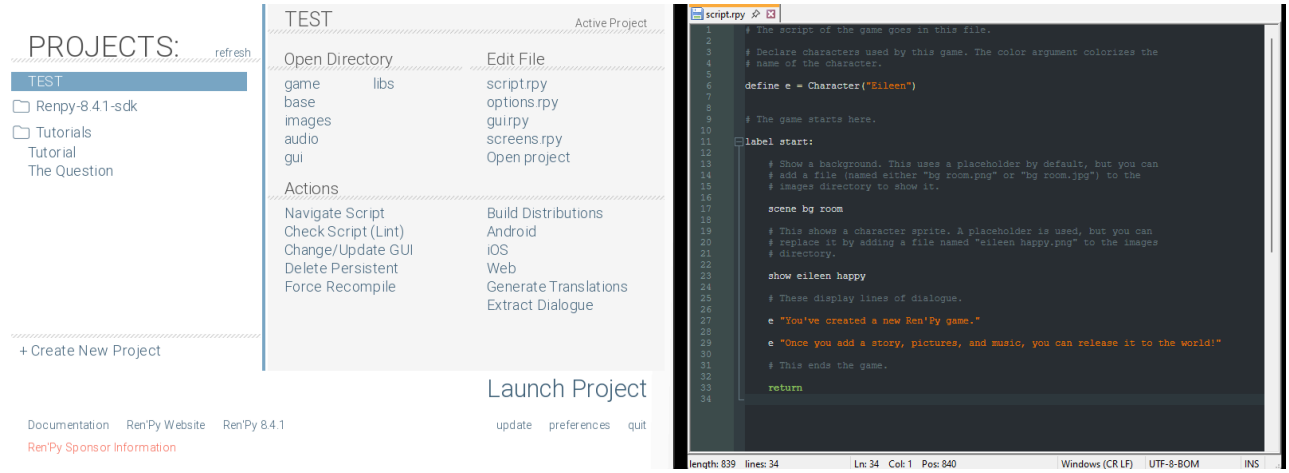
AhnLab SEcurity intelligence Center(ASEC)은 인포스틸러인 Rhadamanthys 악성코드가 RenPy로 만들어진 게임으로 위장하여 유포되고 있는 것을 확인하였다. RenPy는 Python 기반의 게임 제작 도구로, 사용자가 간단한 스크립트만으로 스토리, 대사, 이미지 및 사운드 등을 손쉽게 구성할 수 있도록 지원한다. 오픈소스 형태로 배포되며 다양한 운영체제에서 실행이 가능해 인디 개발자들 사이에서 폭넓게 활용되고 있으며, Steam과 같은 주요 게임 플랫폼에서도 사용될 정도로 인기가 많다.

해당 공격은 정상적인 게임 파일로 위장하여 실행 시 내부에 포함된 악성 로더를 통해 최종적으로 Rhadamanthys 인포스틸러가 실행된다. 본 보고서에서는 해당 악성코드의 유포 방식, 내부 동작 구조, 그리고 탐지 회피 기법에 대해 상세히 기술하고자 한다.



[그림 1] RenPy 공식홈페이지

RenPy로 게임을 개발할 때 필수적으로 사용되는 스크립트 파일은 “script.rpy”, “options.rpy”, “gui.rpy”, “screens.rpy”로 총 4개이며, 모두 RenPy 전용 확장자인 “.rpy”를 사용하는 Python 기반 스크립트 파일이다.



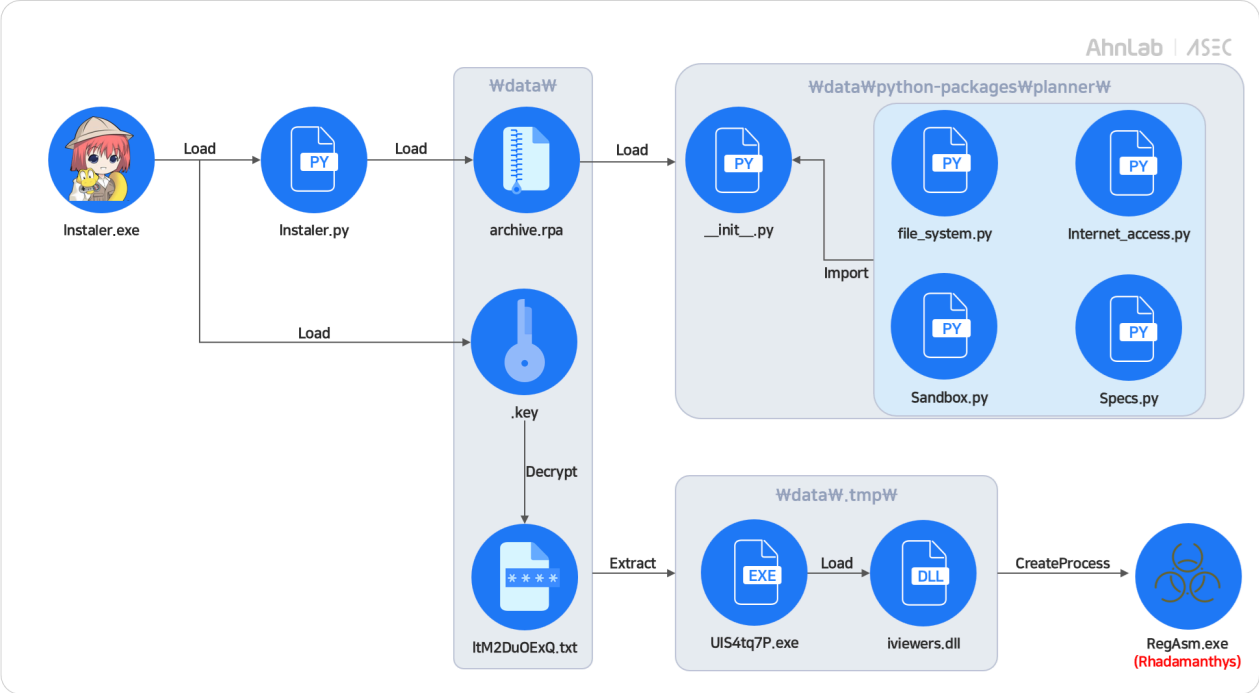
[그림 2] 정상 “script.rpy” 템플릿 코드

게임을 최종 빌드 시 위 4개의 파일을 그대로 게임 경로에 생성하는 것이 일반적인 기능이고, 이를 하나의 파일로 압축 및 컴파일하여 생성할 수 있는데, 이때 생성되는 파일의 이름은 “archive.rpa”이다. 4개의 파일을 1개로 압축 및 컴파일하기 때문에 파일 용량을 줄일 수 있으며, 게임 소스 코드도 보호할 수 있어 대부분의 개발자들이 컴파일하여 배포한다. 게임 빌드 완료 이후 게임 런처 프로그램이 실행될 때 “archive.rpa” 파일을 압축 및 디컴파일 해제를 통해 스크립트 파일들을 추출하고 읽어와 실행하게 된다.

이 가운데 핵심은 “script.rpy” 파일로, 게임 실행 흐름의 진입점이자 시나리오와 레이블 등 본문 로직이 정의된다. 공격자는 이 파일에 악성 스크립트를 삽입하여 악성 코드를 실행하도록 조작할 수 있다. 본문의 사례에서도 공격자는 이러한 실행 메커니즘을 이용하여 “script.rpy” 파일에 악성 스크립트를 작성하고, 이를 통해 같은 경로에 존재하는 추가 악성코드를 실행한다.

공격 흐름도

위에서 언급했듯이, 공격자는 실제로 게임 실행에 필요한 스크립트 파일인 'script.rpy' 파일에 악성 스크립트를 삽입했다. 런처 파일인 'Instaler.exe'를 실행하게 되면 악성 코드가 함께 실행되며, 전체적인 공격 흐름도와 파일별 기능은 아래 [그림 2]와 [표 1]과 같다.



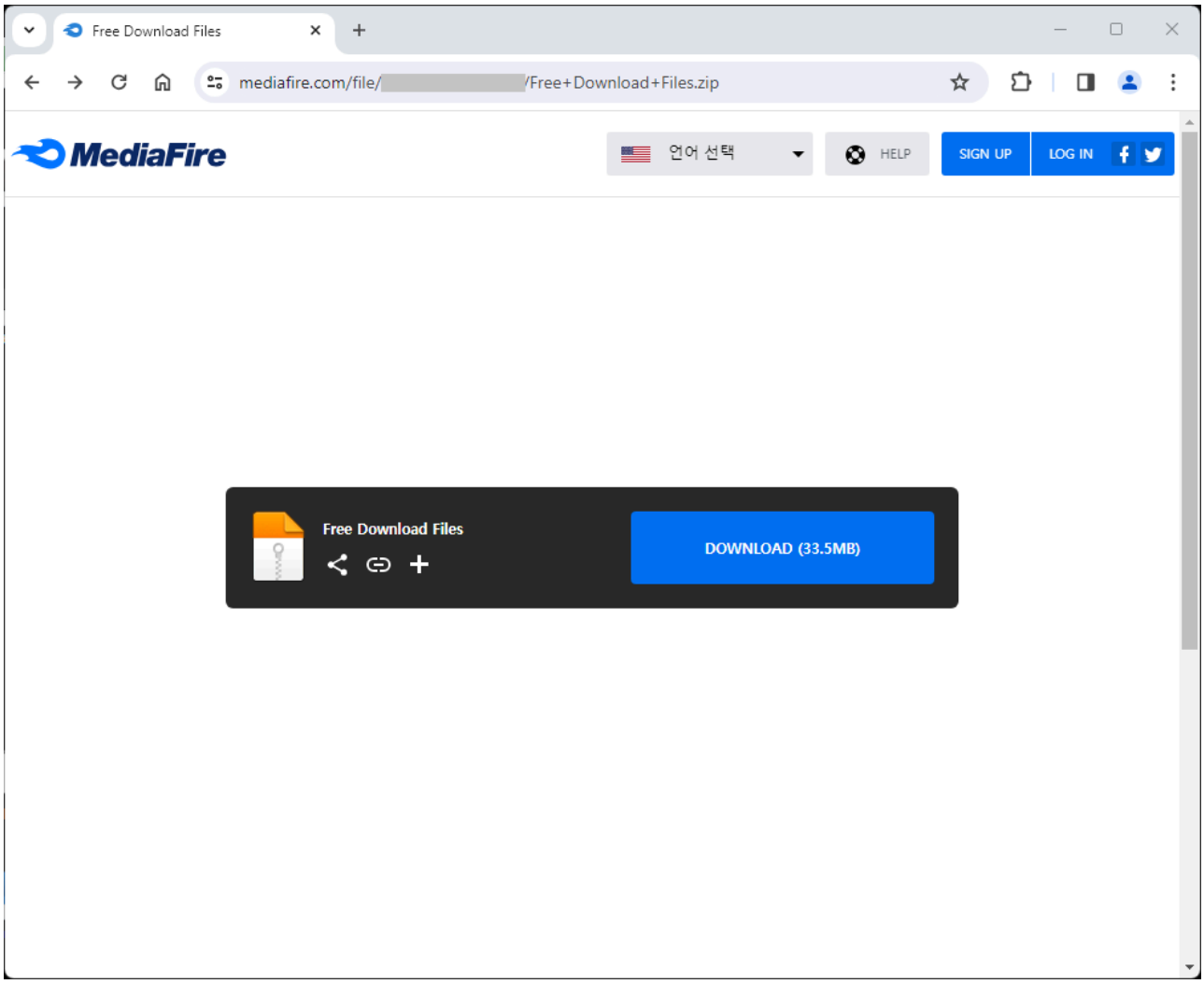
[그림 3] 공격 흐름도

번호	파일 이름	기능
1	Instaler.exe	실행 런처
2	Instaler.py	Instaler.exe가 게임 폴더를 찾기 위해 참고하는 파일
3	.key	BASE64인코딩되어 있는 JSON형태의 설정 파일
4	archive.rpa	컴파일 및 압축된 게임 실행에 필요한 스크립트
5	__init__.py	file_system.py, internet_access.py, sandbox.py, specs.py를 import한 스크립트
6	file_system.py	VM관련 프로세스 및 레지스트리 정보 확인 스크립트 (sandbox.py와 연계됨)
7	internet_access.py	외부 인터넷 연결 확인 스크립트
8	sandbox.py	가상 환경 여부 판정 스크립트
9	specs.py	시스템 정보(CPU 정보, Drive 용량, RAM 용량 등) 확인 스크립트

[표 1] 주요 파일 정보

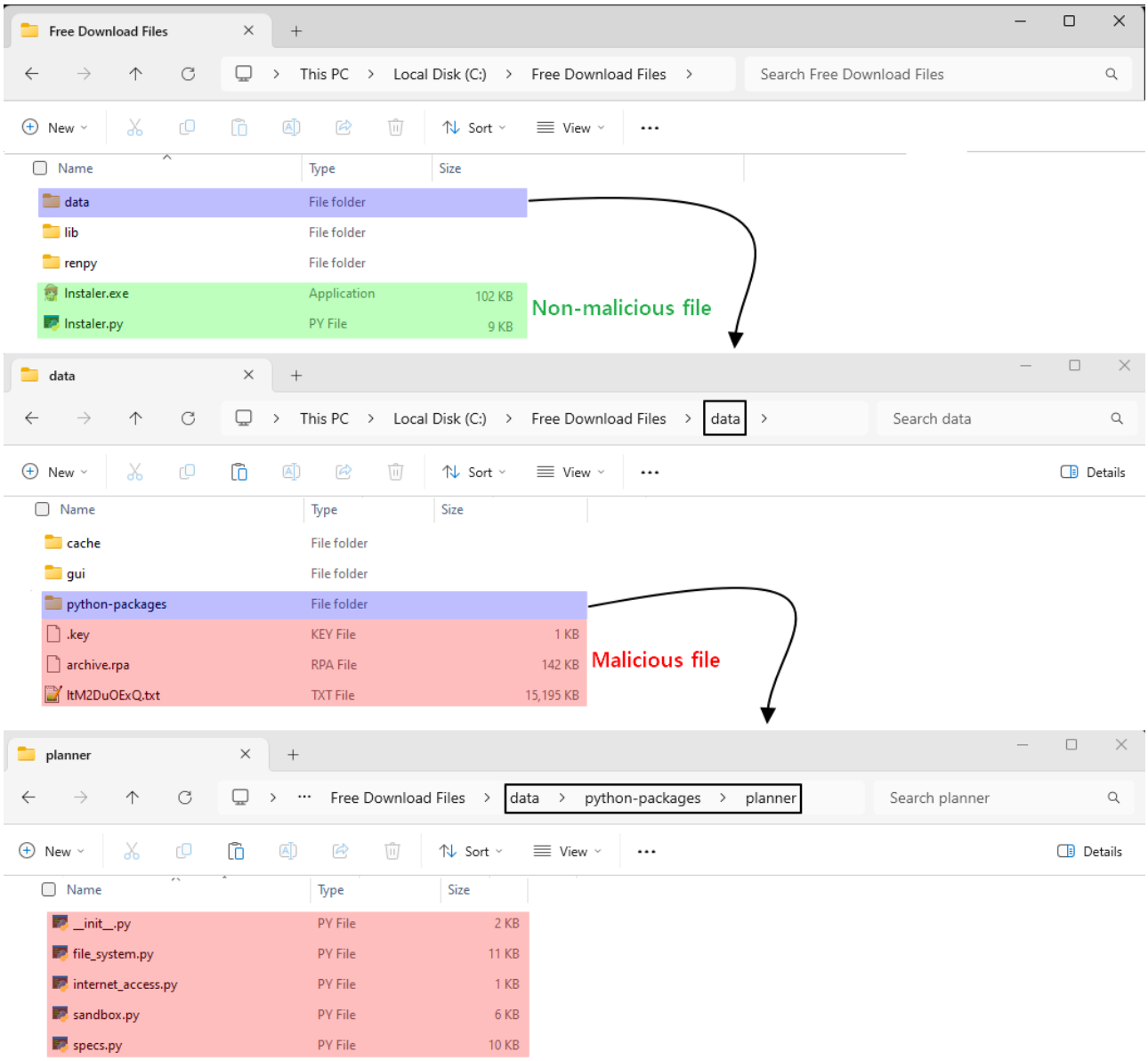
분석 내용

해당 공격은 MediaFire를 통해 ZIP 파일을 배포하는 방식으로 시작된 것으로 확인되었다. 지금까지 수집된 ZIP 파일은 모두 “Free Download Files.zip”이라는 동일한 이름을 사용하고 있다. 이러한 점을 미루어 볼 때, 공격자는 유료 게임을 무료로 다운로드할 수 있는 것처럼 위장된 링크를 게시하여 악성 파일을 유포하고 있는 것으로 추정된다.



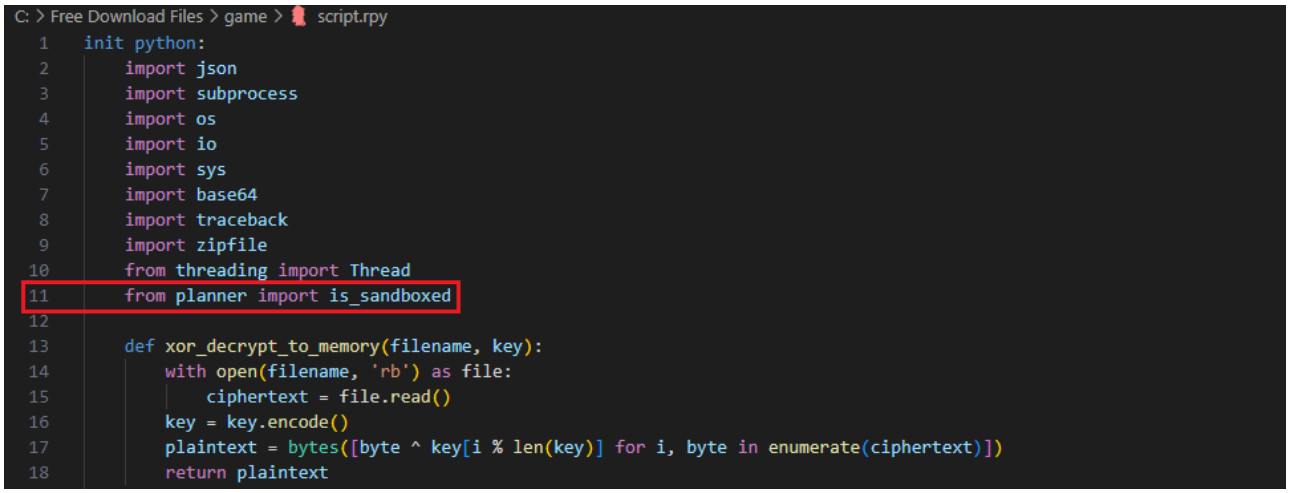
[그림 4] MediaFire를 통해 유포중인 악성 ZIP파일

ZIP 파일의 구성은 [그림 5]와 같으며, 주요 파일별 기능은 아래 [표 1]에 정리되어 있다. 사용자가 정상 실행 파일인 “Instaler.exe”를 실행하면, 해당 파일은 내부적으로 정상 스크립트인 “Instaler.py”를 로드하여 게임 폴더(data)를 탐색하고 경로를 설정한다. 이후 공격자는 악성 스크립트(script.rpy)가 컴파일된 “archive.rpa” 파일을 디컴파일하여 “script.rpy”를 추출하고 실행한다. 이 과정에서 “\data\python-packages\planner” 경로에 위치한 악성 “__init.py__” 파일이 자동으로 import된다.



[그림 5] ZIP파일 구성

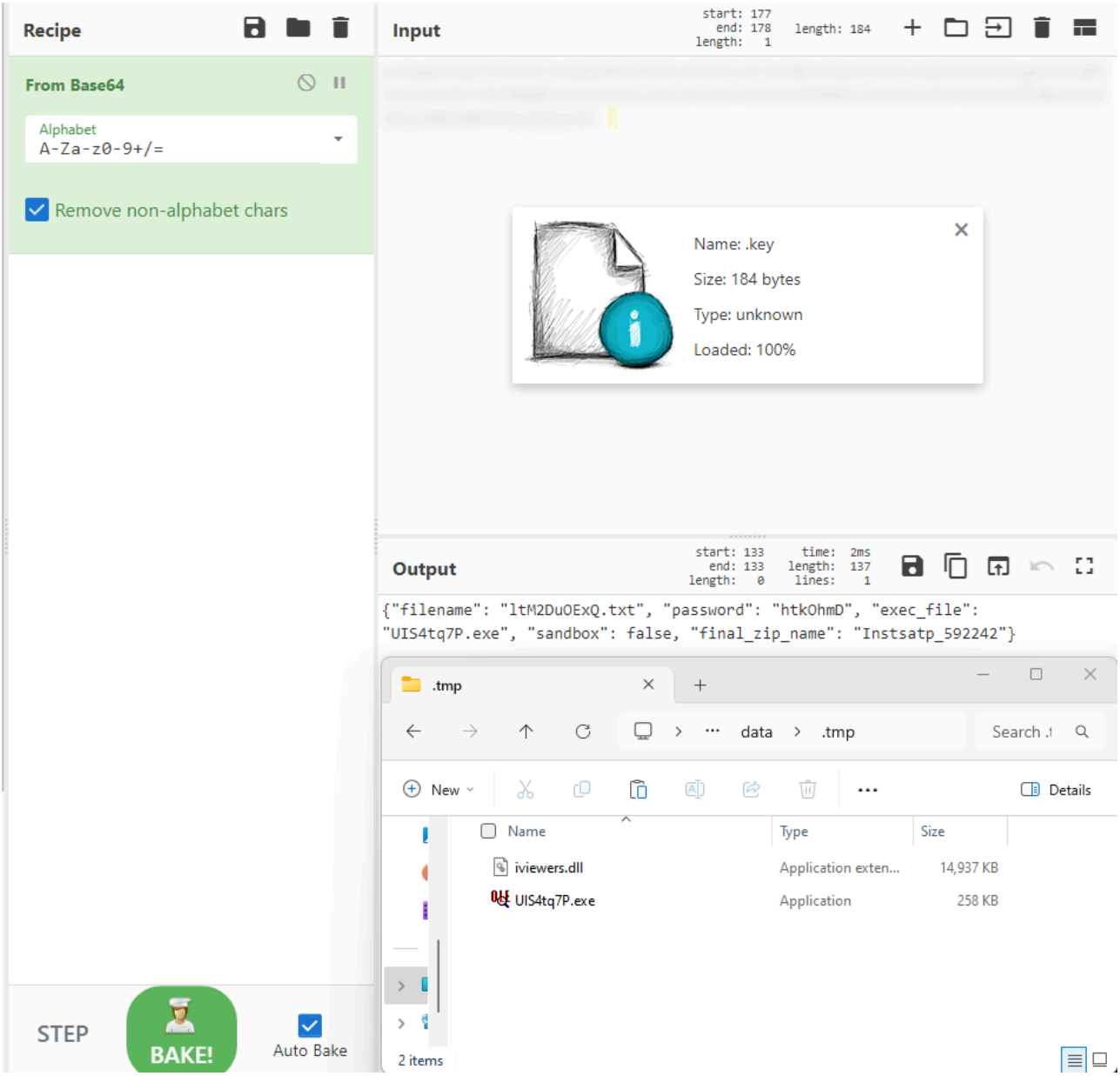
“__init__.py” 파일이 자동으로 import되는 이유는 RenPy에서 사용자가 직접 작성한 모듈이나 패키지를 “python-packages” 폴더를 생성하여 사용할 수 있도록 지원하기 때문이다.[1] 또한, “script.rpy” 파일이 해당 폴더 내의 모듈을 import하도록 작성되어 있어, 결과적으로 “\data\python-packages\planner” 경로의 “__init__.py” 파일이 자동으로 import되며, 이 폴더 내의 스크립트를 사용할 수 있게 된다.



[그림 6] planner 폴더의 파일을 improt중인 “script.rpy”

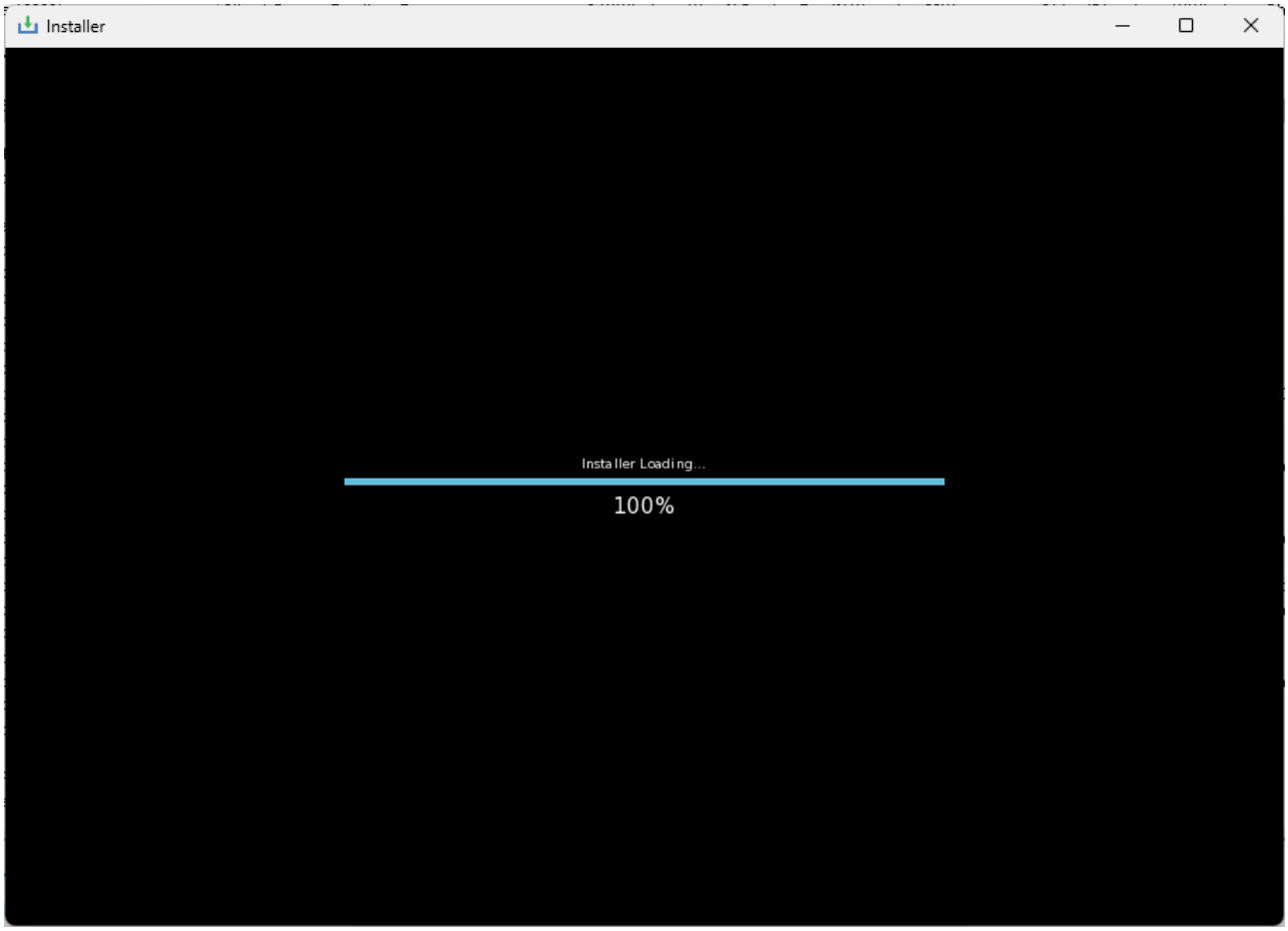
이어서 “script.rpy”가 실행되면 “__init__.py”의 코드가 먼저 실행되어 “가상 환경 여부, 외부 인터넷 연결 여부, 시스템 드라이브 정보” 등 여러 정보를 수집하여 외부로 전송한다. 이후 “.key” 파일을 찾아 BASE64로 디코딩한 뒤, JSON 형식으로 저장된 복호화 대상 파일명, 비밀번호, 실행할 파일명을 추출한다. 그런 다음 “.tmp”라는 이름의 폴더를 생성하여 압축을 풀고, 압축 해제된 정상 “OLEViewer” 프로그램인 “UIS4tq7P.exe” 파일을 실행한다.

※ 파일 이름은 샘플마다 다르며 본문에서는 “UIS4tq7P.exe” 와 “iviewers.dll”을 사용한다.



[그림 7] “.key”파일 구성과 압축 해제된 파일들

“UIS4tq7P.exe” 파일이 실행되면, 동일한 경로에 존재하는 “iviewers.dll” 파일을 로드한 후 “.NET” 프로세스를 자식 프로세스로 생성한다. 이후 최종적으로 Rhadamanthys 악성코드를 해당 프로세스에 인젝션한다. 이와 동시에 게임 로딩창이 표시되는데, 이는 사용자를 속이기 위한 가짜 화면이며, 999,999초 동안 대기한 뒤 종료된다.



[그림 8] 가짜 로딩 화면

공격자는 RenPy의 실행 메커니즘을 정확히 이해하고 이를 악용하여 Rhadamanthys를 유포하였다. Rhadamanthys는 다양한 방식으로 꾸준히 유포되고 있으며, 이번 사례에서는 Rhadamanthys 악성코드가 유포되는 것을 확인하였다. 한편, 합법 및 불법 성인 게임을 공유하는 포럼에서는 게임 개발자의 계정이 탈취되어 정상적인 게임 파일 대신 LummaC2 인포스틸러가 유포된 사례도 확인된 바 있다. 즉, Rhadamanthys뿐만 아니라 다양한 다른 악성코드도 유포될 가능성이 존재한다. 이러한 사례는 해당 포럼의 파일 공유 환경이 악성코드 유포에 악용될 수 있음을 보여주며, 사용자들은 이와 같은 경로를 통해 파일을 다운로드할 때 각별한 주의가 필요하다.

파일 진단

- Trojan/Win.Generic.R729425 (2025.10.08.01)
- Trojan/Win.Injector.R729869 (2025.10.13.01)
- Trojan/Win.Injector.R729189 (2025.10.05.00)
- Trojan/Win.Injector.R731064 (2025.10.19.01)
- Trojan/Win.Injector.R730188 (2025.10.14.00)
- Trojan/Win.Injector.R730185 (2025.10.13.03)

MD5

0026aee93b911e3e8588724e30f0816c

01ff1b158afbe84c8f7fd4fce19d748b

0401aba66ff3ae558f290e8c7da15ba3

0758c5416e1b8a3972a9e220b53d9f78

0a2e925e1aacdd8f67979205dd41cf2c

추가 IoC는 ATIP에서 제공됩니다.
URL

https[:]//146[.]103[.]114[.]25/gateway/bi24namg[.]diqdh

https[:]//api[.]blagomezbart[.]top/gateway/j2ucqiol[.]ccile

https[:]//api[.]ganjasmokeha[.]top/gateway/dv55j64q[.]qamne

https[:]//api[.]goblaosdrt[.]top/gateway/7rjhfv2i[.]vq0fk

https[:]//api[.]khljokas[.]top/gateway/j85bu13i[.]bib6n

추가 IoC는 ATIP에서 제공됩니다.