Cazadores de amenazas han descubierto una serie de siete paquetes en el repositorio del Índice de Paquetes de Python (PyPI) que están diseñados para apoderarse de frases mnemotécnicas BIP39 utilizadas para recuperar claves privadas de una billetera de criptomonedas.

La campaña de ataque a la cadena de suministro de software ha sido llamada BIPClip por ReversingLabs. Estos paquetes fueron descargados colectivamente 7,451 veces antes de ser eliminados de PyPI. La lista de paquetes es la siguiente:

- jsBIP39-decrypt (126 descargas)
- bip39-mnemonic-decrypt (689 descargas)
- mnemonic_to_address (771 descargas)
- erc20-scanner (343 descargas)
- public-address-generator (1,005 descargas)
- hashdecrypt (4,292 descargas)
- hashdecrypts (225 descargas)

Se informa que BIPClip, dirigido a desarrolladores que trabajan en proyectos relacionados con la generación y seguridad de billeteras de criptomonedas, ha estado activo desde al menos el 4 de diciembre de 2022, cuando hashdecrypt fue publicado por primera vez en el registro.

> *«Esta es simplemente la más reciente campaña de ataque a la cadena de suministro de software dirigida a activos criptográficos. Esto confirma que las criptomonedas siguen siendo uno de los objetivos más populares para los actores de amenazas que buscan infiltrarse en la cadena de suministro»,* mencionó el investigador de seguridad Karlo Zanki en un informe

Para evitar la detección, uno de los paquetes en cuestión, mnemonic_to_address, carecía de cualquier funcionalidad maliciosa aparte de listar bip39-mnemonic-decrypt como su dependencia, el cual contenía el componente malicioso.

> *«Incluso si los revisores optaban por examinar las dependencias del paquete, el nombre del módulo importado y la función invocada estaban cuidadosamente seleccionados para imitar funciones legítimas y no levantar sospechas, ya que las implementaciones del estándar BIP39 incluyen numerosas operaciones criptográficas»,* explicó Zanki.

El paquete, en sí mismo, está diseñado para robar frases mnemotécnicas y enviar la información a un servidor controlado por los atacantes.

Dos de los otros paquetes identificados por ReversingLabs, public-address-generator y erc20-scanner, operan de manera similar, con el primero actuando como un señuelo para transmitir las frases mnemotécnicas al mismo servidor de comando y control (C2).

Por otro lado, hashdecrypts opera de manera un tanto diferente en el sentido de que no necesita trabajar en conjunto con otros paquetes y contiene dentro de sí código casi idéntico para recopilar los datos.

```
from hashDecrypts import hdec
VAULT = '{"data": "M5YT....9Mk+97", "iv": "6CD2Hm...Cg==", "salt": "TkHQ....xaSC/g="}'
PASSWORD = "Awerawer22"
w = hdec()
obj = w.decrypt(PASSWORD, VAULT)
print(obj)
```

```
from tkinter import *

from hdwallet import HDWallet
- from hashDecrypt import hdec
+ from hashDecrypts import hdec
from urllib3.util import SKIP_HEADER
from requests import get, post
from datetime import datetime

@@ -541,4 +541,4 @@ def hcatBrute():
        totalTime = round(eTime - sTime, 2)
        endTime = normlTime.strftime("%d.%m.%Y %H:%M:%S")
        print(f"{totalTime} sec.\n{endTime}")
-       input("Press ENTER to continue.")
```

Según la firma de seguridad de la cadena de suministro de software, este paquete incluye referencias a un perfil de GitHub llamado «HashSnake», que cuenta con un repositorio llamado hCrypto que se anuncia como una forma de extraer frases mnemotécnicas de billeteras de criptomonedas utilizando el paquete hashdecrypts.

Un análisis más profundo del historial de commits del repositorio revela que la campaña ha estado en marcha durante más de un año, basado en el hecho de que uno de los scripts de

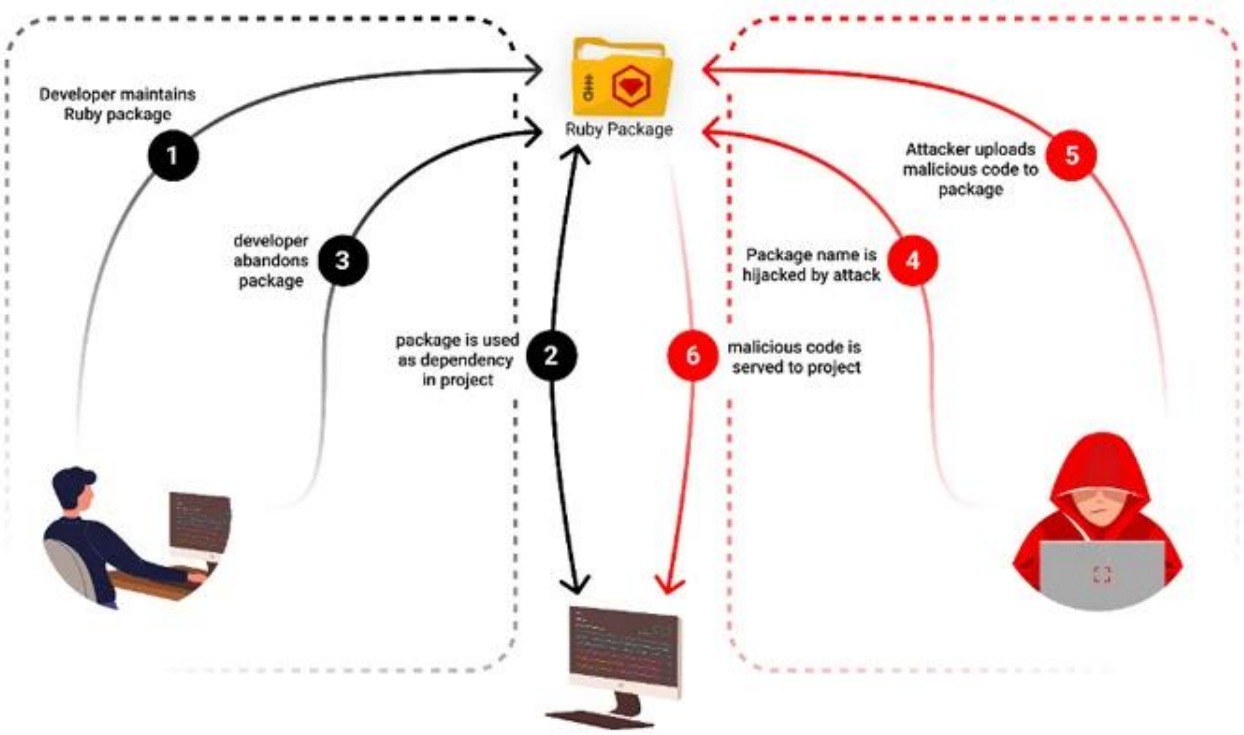
Python anteriormente importaba el paquete hashdecrypt (sin la «s») en lugar de hashdecrypts hasta el 1 de marzo de 2024, la misma fecha en que se cargó hashdecrypts en PyPI.

Es importante señalar que los actores detrás de la cuenta de HashSnake también tienen presencia en Telegram y YouTube para promocionar sus herramientas. Esto incluye la publicación de un video el 7 de septiembre de 2022, que muestra una herramienta de verificación de registros criptográficos llamada xMultiChecker 2.0.

> *«El contenido de cada uno de los paquetes descubiertos fue meticulosamente elaborado para que parecieran menos sospechosos»,* dijo Zanki.
>
> *«Estaban enfocados en comprometer billeteras de criptomonedas y robar las criptomonedas que contienen. La falta de una agenda y ambiciones más amplias hizo que esta campaña fuera menos probable de ser detectada por herramientas de seguridad y monitoreo desplegadas dentro de organizaciones comprometidas».*

Una vez más, los descubrimientos resaltan las amenazas de seguridad que acechan en los repositorios de paquetes de código abierto, situación que se agrava debido a que servicios legítimos como GitHub son utilizados como medios para distribuir software malicioso.

Adicionalmente, los proyectos abandonados están atrayendo la atención como un vector interesante para los actores de amenazas, quienes buscan hacerse con el control de las cuentas de desarrolladores y publicar versiones modificadas que podrían facilitar ataques de gran escala en la cadena de suministro.



> *«Los activos digitales dejados en el olvido no son reliquias del pasado; son peligros latentes y los atacantes están aprovechándolos cada vez más, convirtiéndolos en herramientas de engaño dentro de los ecosistemas de código abierto»*, mencionó Checkmarx el mes pasado.

> *«Los estudios de caso de MavenGate y CocoaPods muestran cómo los dominios y subdominios abandonados pueden ser tomados para confundir a los usuarios y propagar intenciones maliciosas».*