Los hackers se encuentran buscando activamente repositorios de código abierto, como RubyGems, para distribuir paquetes maliciosos con la intención de comprometer computadoras o proyectos de software con backdoors.

En una investigación de la compañía de seguridad cibernética ReversingLabs, se revelaron más de 700 gemas maliciosas, paquetes escritos en lenguaje de programación Ruby, que los atacantes de la cadena de suministro fueron atrapados distribuyendo por medio del repositorio RubyGems.

La campaña maliciosa aprovechó la técnica de typosquatting, en la que los atacantes cargaron paquetes legítimos mal escritos intencionalmente con la esperanza de que los desarrolladores involuntarios escriban mal el nombre e instalen de forma involuntaria la biblioteca maliciosa.

ReversingLabs dijo que los paquetes de typosqatted en cuestión, fueron subidos a RubyGems entre el 16 y el 25 de febrero, y que la mayoría de ellos fueron diseñados para robar fondos en secreto redirigiendo las transacciones de criptomonedas a una dirección de billetera bajo el control del hacker.

Dicho de otro modo, este ataque particular de la supplychain apuntó a los desarrolladores de Ruby con sistemas Windows que también utilizaron las máquinas para realizar transacciones de Bitcoin.

Luego de que los hallazgos fueron revelados en privado a los mantenedores de RubyGems, se eliminaron las gemas maliciosas y las cuentas de los hackers asociados, casi dos días después del 27 de febrero.

> *«Al estar estrechamente integrados con los lenguajes de programación, los repositorios facilitan el consumo y la administración de componentes de terceros»,* dijo la compañía de seguridad.

> *«Consecuentemente, incluir otra dependencia del proyecto se ha vuelto tan fácil como hacer clic en un botón o ejecutar un comando simple en el entorno del desarrollador. Pero solo hacer clic en un botón o ejecutar un comando simple a veces puede ser algo peligroso, ya que los actores de amenazas también comparten un interés en esta conveniencia al comprometer las cuentas de los desarrolladores o sus entornos de compilación, y al tipear los nombres de paquetes»,* agregó.

Typosquatting es una forma de ataque de brandjacking, que generalmente depende de que los usuarios se pongan en peligro al escribir mal una dirección web o un nombre de biblioteca que se hace pasar por paquetes populares en los registros de software.

RubyGems es un administrador de paquetes popular que facilita a los desarrolladores la distribución, adminsitración e instalación de programas y bibliotecas de Ruby.

Utilizando una lista de gemas populares como línea de base para su investigación, los investigadores monitorearon nuevas gemas que se publicaron en el repositorio y marcaron cualquier biblioteca que tuviera un nombre similar de la lista de línea base.

Lo que encontraron fueron algunos paquetes como «atlas-client», que se hacía pasar por la gema «atlas_client», que contenía ejecutables portátiles (PE) que se hacían pasar por un archivo de imagen aparentemente inofensivo (aaa.png).

Durante la instalación, el archivo de imagen se renombra de aaa.png a a.exe y se ejecuta, contiene un VBScript codificado en Base64 que ayuda al malware a ganar persistencia en el sistema infectado y se ejecuta cada vez que se inicia o reinicia.

Además, el VBScript no solo captura los datos del portapapeles de la víctima de forma continua, sino que si encuentra que el contenido del portapapeles coincide con el forma de una dirección de billetera de criptomonedas, reemplaza la dirección con una alternativa

controlada por el atacante (» 1JkU5XdNLji4Ugbb8agEWL1ko5US42nNmc «).

> *«Con esto, el actor de la amenaza está tratando de redirigir todas las posibles transacciones de criptomonedas a su dirección de billetera»,* dijeron los investigadores de ReversingLabs.

Aunque no se realizaron transacciones en esta billetera, todas las gemas maliciosas se remontaron a dos titulares de cuentas, *«JimCarrey»* y *«PeterGibbons»*, con «atlas-client» registrando 2100 descargas, aproximadamente el 30% del total de descargas acumuladas por el legítimo «atlas_client».