Adversarios no identificados han urdido una sofisticada campaña de ataque que ha afectado a varios desarrolladores individuales, así como a la cuenta de organización en GitHub vinculada a Top.gg, un sitio de descubrimiento de bots de Discord.

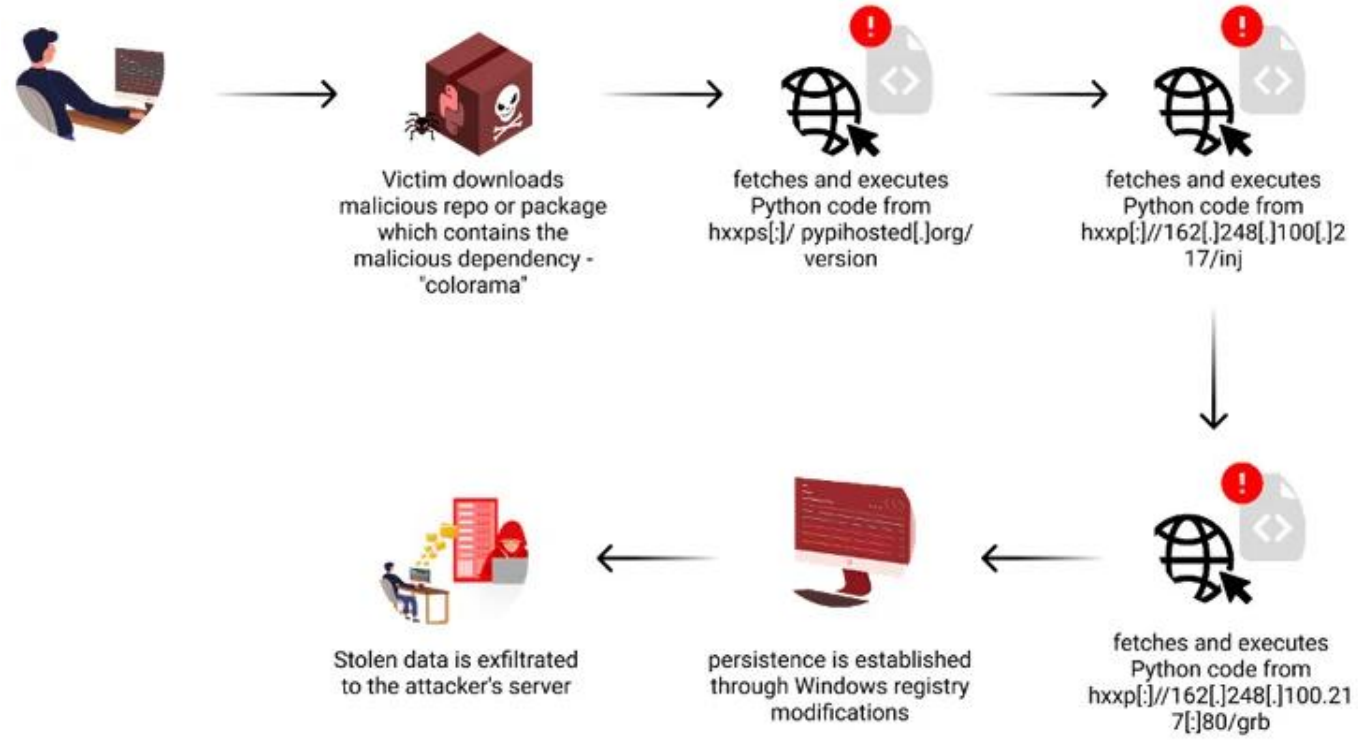
> Según un informe técnico compartido por parte de Checkmarx, *«los perpetradores emplearon múltiples TTPs en este ataque, incluyendo la usurpación de cuentas mediante cookies de navegador robadas, la inserción de código malicioso a través de confirmaciones verificadas, la configuración de un espejo personalizado de Python y la publicación de paquetes maliciosos en el registro de PyPI».*

Se informa que este ataque a la cadena de suministro de software ha resultado en el robo de información sensible, como contraseñas, credenciales y otros datos valiosos. Algunos aspectos de esta campaña fueron revelados previamente a principios de mes por un desarrollador con sede en Egipto llamado Mohammed Dief.

La estrategia principal involucró la creación de un astuto typosquat del dominio oficial de PyPI, conocido como «files.pythonhosted[.]org», al que se le dio el nombre de «files.pypihosted[.]org» y se utilizó para alojar versiones troyanizadas de paquetes bien conocidos, como colorama. Desde entonces, Cloudflare ha eliminado el dominio.

Según los investigadores de Checkmarx, los perpetradores tomaron Colorama (una herramienta muy popular con más de 150 millones de descargas mensuales), la duplicaron e insertaron código malicioso en ella. Luego, ocultaron la carga dañina dentro de Colorama utilizando espacios de relleno y alojaron esta versión modificada en su espejo falso de dominio con errores tipográficos.

Estos paquetes ilegítimos fueron posteriormente difundidos a través de repositorios en GitHub como github[.]com/maleduque/Valorant-Checker y github[.]com/Fronse/League-of-Legends-Checker que incluían un archivo requirements.txt, el cual actúa como la lista de paquetes de Python que deben ser instalados mediante el gestor de paquetes pip.



Uno de los repositorios que permanece activo hasta el momento de esta redacción es github[.]com/whiteblackgang12/Discord-Token-Generator, el cual hace referencia a la versión maliciosa de colorama alojada en «files.pypihosted[.]org.»

También fue modificado como parte de la operación el archivo requirements.txt asociado con el sdk de python de Top.gg por una cuenta llamada editor-syntax el 20 de febrero de 2024. Los administradores del repositorio han solucionado el problema.

Es importante destacar que la cuenta «editor-syntax» es un colaborador legítimo de la organización de GitHub de Top.gg y cuenta con permisos de edición en los repositorios de Top.gg, lo que sugiere que el actor malicioso logró apoderarse de la cuenta verificada para realizar una contribución maliciosa.

> *«Es probable que la cuenta de GitHub 'editor-syntax' haya sido tomada por medio de cookies robadas»*, observó Checkmarx.
>
> *«El atacante obtuvo acceso a las cookies de sesión de la cuenta, lo que les permitió evadir la autenticación y llevar a cabo actividades maliciosas utilizando la interfaz de usuario de GitHub. Este método de toma de control de cuentas es particularmente preocupante, ya que no requiere que el atacante conozca la contraseña de la cuenta.»*

Además, se informa que los responsables de la operación detrás de esta campaña realizaron múltiples modificaciones en los repositorios ilegítimos en una única contribución, alterando hasta 52 archivos en una sola instancia en un intento por ocultar los cambios en el archivo requirements.txt.

El software malicioso integrado en el paquete falsificado de colorama activa una secuencia de infección en múltiples etapas que resulta en la ejecución de código Python desde un servidor remoto. Este código, a su vez, puede establecer una presencia continua en el sistema a través de modificaciones en el Registro de Windows y puede robar información de navegadores web, carteras de criptomonedas, tokens de Discord y tokens de sesión asociados con Instagram y Telegram.

> *«El software malicioso incluye un componente de robo de archivos que busca archivos con palabras clave específicas en sus nombres o extensiones. Se enfoca en directorios como el Escritorio, Descargas, Documentos y Archivos Recientes»*, explicaron los investigadores.

Los datos capturados se transfieren finalmente a los atacantes a través de servicios de intercambio de archivos anónimos como GoFile y Anonfiles. De manera alternativa, los datos también se envían a la infraestructura del actor malintencionado utilizando solicitudes HTTP,

junto con el identificador de hardware o la dirección IP para rastrear la máquina de la víctima.

> *«Este caso es un ejemplo destacado de las tácticas sofisticadas empleadas por actores maliciosos para difundir software malicioso a través de plataformas de confianza como PyPI y GitHub»,* concluyeron los investigadores.
>
> *«Este incidente subraya la importancia de mantener la vigilancia al instalar paquetes y repositorios, incluso cuando provienen de fuentes confiables. Es esencial examinar cuidadosamente las dependencias, supervisar cualquier actividad de red sospechosa y mantener prácticas de seguridad sólidas para reducir el riesgo de ser víctima de tales ataques».*