El Python Package Index, PyPI, fue alertado el miércoles debido a una campaña de phishing en curso que tiene como objetivo robar las credenciales de los desarrolladores e inyectar actualizaciones maliciosas a los paquetes legítimos.

> *«Este es el primer ataque de phishing conocido contra PyPI»,* dijeron los mantenedores del repositorio.

El ataque de ingeniería social implica el envío de mensajes con temas de seguridad que crean una falsa sensación de urgencia al informar a los destinatarios que Google está implementando un proceso de validación obligatorio en todos los paquetes y que deben hacer clic en un enlace para completar la validación antes de septiembre, o corren el riesgo de obtener sus módulos PyPI eliminados.

Si un desarrollador desprevenido cae en la trampa, los usuarios son dirigidos a una página de destino similar que imita la página de inicio de sesión de PyPI y está alojada en Google Sites, desde donde se capturan y se abusa de las credenciales ingresadas para acceder sin autorización a las cuentas y comprometer los paquetes para incluir malware.

Las modificaciones, por su parte, están diseñadas para descargar un archivo desde un servidor remoto.

> *«Este malware tiene un tamaño inusualmente grande, ~63 MB, (posiblemente en un intento de evadir la detección) y tiene una firma válida (firmada el 23 de agosto de 2022)»*, dijo Aviad Gershon, investigador de Checkmarx.

«Estas versiones se eliminaron de PyPI y las cuentas de mantenimiento se congelaron

temporalmente», dijo PyPI. Dos de los paquetes afectados hasta ahora incluyen «exotel» y «spam». Además, se dice que se han eliminado cientos de typosquats.

PyPI también dijo que está monitoreando activamente los informes de nuevos paquetes maliciosos y asegurando su eliminación. Los desarrolladores que crean que pudieron haber sido comprometidos deben restablecer sus contraseñas con efecto inmediato, restablecer los códigos de recuperación 2FA y revisar los registros de la cuenta PyPI para detectar actividad anómala.

El ataque de phishing es otra señal de cómo el ecosistema de código abierto está cada vez más en riesgo por parte de los atacantes, que están capitalizando bibliotecas y proyectos que están entretejidos en la estructura de varias aplicaciones para montar ataques en la cadena de suministro que pueden tener efectos en cascada.

A inicios del mes, los investigadores de Checkmarx revelaron dos paquetes maliciosos de Python (typeping-unions y aiogram-types) que se hacían pasar por paquetes populares de tipeo y aiograma para engañar a los desarrolladores para que los descargaran e infectaran sus máquinas con Cobalt Strike.

Otro ataque a gran escala involucró a un atacante que publicó una docena de paquetes con errores tipográficos bajo los nombres de proyectos ampliamente utilizados con ligeras permutaciones para instalar un malware persistente de varias etapas en sistemas comprometidos.

El desarrollo también llega unos meses después que el registro comenzara a imponer un requisito obligatorio de autenticación de dos factores (2FA) para proyectos considerados *«críticos».*