Cazadores de amenazas han revelado dos campañas de malware distintas que han explotado vulnerabilidades y configuraciones incorrectas en entornos en la nube con el objetivo de desplegar mineros de criptomonedas.

Los grupos de actividad maliciosa han sido identificados bajo los nombres de Soco404 y Koske por las firmas de seguridad en la nube Wiz y Aqua, respectivamente.

Soco404 "tiene como blanco sistemas tanto Linux como Windows, desplegando malware específico para cada plataforma", explicaron los investigadores de Wiz, Maor Dokhanian, Shahar Dorfman y Avigayil Mechtinger. *"Utilizan técnicas de suplantación de procesos para hacer pasar la actividad maliciosa como si fueran procesos legítimos del sistema."*

El nombre de la actividad hace alusión al hecho de que las cargas útiles están incrustadas en falsas páginas HTML con error 404, alojadas en sitios creados mediante Google Sites. Estos sitios fraudulentos ya fueron eliminados por Google.

Wiz señaló que esta campaña, anteriormente detectada atacando servicios Apache Tomcat con credenciales débiles, así como servidores vulnerables de Apache Struts y Atlassian Confluence a través del botnet Sysrv, parece formar parte de una infraestructura más amplia dedicada a fraudes con criptomonedas, incluyendo plataformas falsas de trading.

La campaña más reciente también ha apuntado a instancias PostgreSQL expuestas públicamente, y ha hecho uso de servidores Apache Tomcat comprometidos para alojar cargas útiles diseñadas para sistemas Linux y Windows. Además, los atacantes comprometieron un sitio legítimo de transporte surcoreano para distribuir el malware.

Una vez obtenida la entrada inicial, los atacantes aprovechan el comando SQL `COPY ... FROM PROGRAM` de PostgreSQL para ejecutar comandos shell arbitrarios en el sistema y obtener ejecución remota de código.

"El actor detrás de Soco404 parece llevar a cabo escaneos automatizados en busca de servicios expuestos, con la intención de explotar cualquier punto de entrada accesible",

indicó Wiz. *"El uso de una amplia gama de herramientas de entrada, incluyendo utilidades de Linux como wget y curl, y herramientas nativas de Windows como certutil y PowerShell, demuestra una estrategia oportunista."*

En entornos Linux, se ejecuta directamente en memoria un script shell que actúa como dropper para descargar y lanzar la siguiente fase del ataque. Al mismo tiempo, elimina mineros competidores para maximizar beneficios y reduce la visibilidad forense sobrescribiendo registros relacionados con cron y wtmp.

La carga útil de esta segunda fase consiste en un binario que actúa como cargador del minero, contactando a un dominio externo (*www.fastsoco[.]top*), también basado en Google Sites.

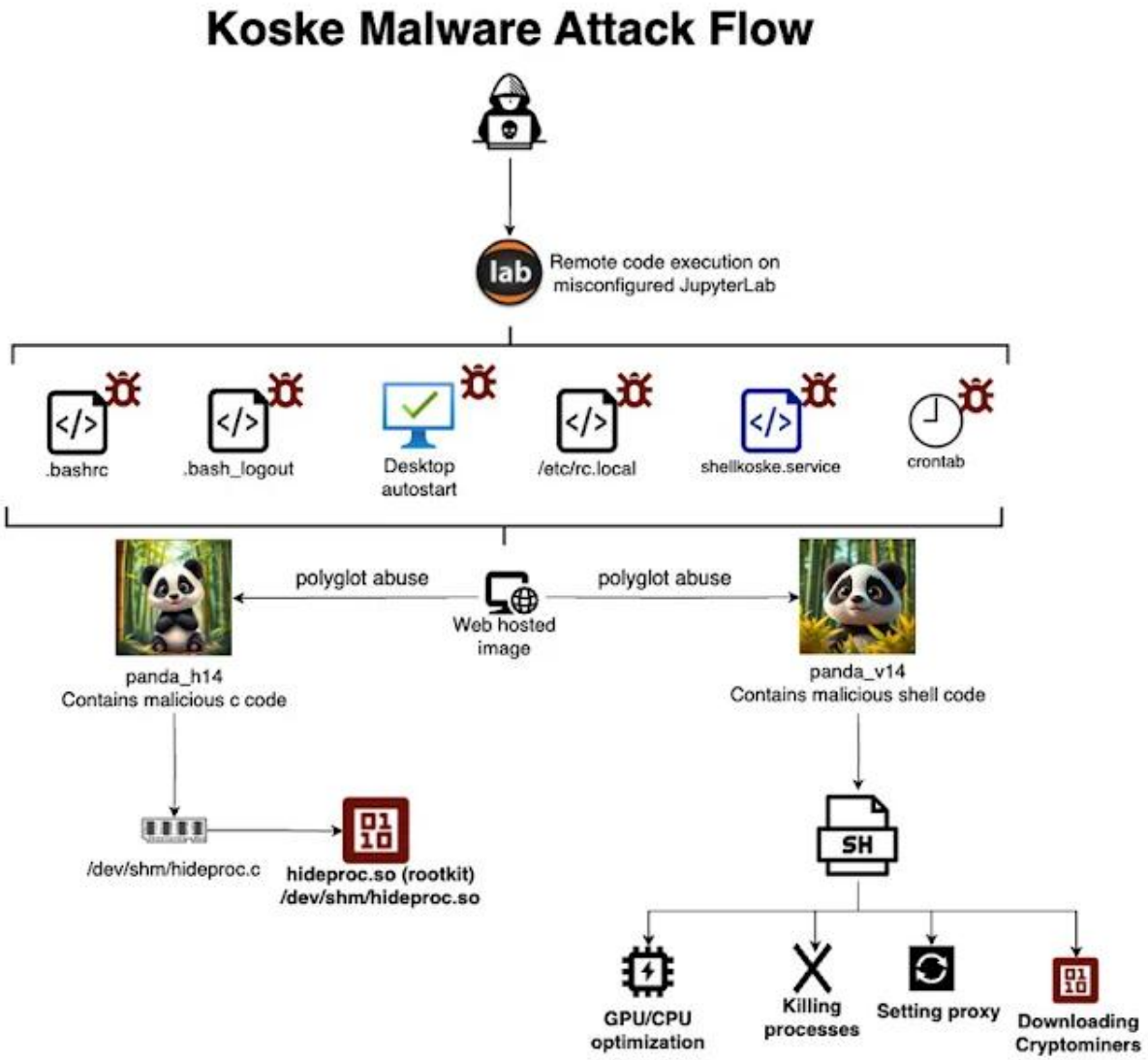
En el caso de Windows, el ataque emplea un comando posterior a la explotación para descargar y ejecutar un binario de Windows, que funciona como su equivalente en Linux: un cargador que incluye tanto el minero como el controlador *WinRing0.sys*, utilizado para escalar privilegios hasta *NT\SYSTEM*.

Además, el malware intenta detener el servicio de registros de eventos de Windows y ejecuta un comando de autoeliminación para evitar ser detectado.

"En lugar de depender de un solo método o sistema operativo, el atacante lanza una red amplia, utilizando cualquier herramienta o técnica disponible en el entorno para desplegar su carga útil", señaló la empresa. *"Este enfoque flexible es característico de una campaña automatizada de criptominería diseñada para lograr el mayor alcance y persistencia posible en múltiples objetivos."*

El descubrimiento de Soco404 coincide con la aparición de una nueva amenaza para sistemas Linux denominada Koske, que se sospecha fue desarrollada con asistencia de un modelo de lenguaje de gran escala (LLM) y se propaga usando imágenes aparentemente inofensivas de pandas.

El ataque inicia con la explotación de un servidor mal configurado, como JupyterLab, para instalar varios scripts extraídos de dos imágenes JPEG. Entre estos se incluye un rootkit en C que oculta archivos relacionados con el malware utilizando *LD_PRELOAD* y un script shell que finalmente descarga los mineros de criptomonedas en el sistema comprometido. Ambas cargas se ejecutan directamente en memoria para evitar dejar rastros en el disco.



El objetivo final de Koske es desplegar mineros optimizados para CPU y GPU que utilicen los recursos del sistema para minar 18 criptomonedas diferentes, incluyendo Monero, Ravencoin, Zano, Nexa y Tari, entre otras.

"Estas imágenes son archivos poliglota, con cargas maliciosas añadidas al final. Una vez descargadas, el malware extrae y ejecuta los segmentos maliciosos en memoria, eludiendo así los antivirus", explicó el investigador de Aqua, Assaf Morag.

"Esta técnica no es esteganografía, sino un abuso de archivos poliglota o una forma de incrustación maliciosa. Se utiliza un archivo JPG válido al que se le añade shellcode malicioso al final. Solo se descargan y ejecutan los últimos bytes, lo que convierte esto en una forma sigilosa de abuso de archivos poliglota."