Los perpetradores de amenazas han estado aprovechando la recién descubierta vulnerabilidad zero-day en el software PAN-OS de Palo Alto Networks desde el 26 de marzo de 2024, casi tres semanas antes de que saliera a la luz ayer.

La división Unit 42 de la empresa de seguridad en red está monitoreando la actividad bajo el nombre Operación EclipseNocturno, atribuyéndola como la obra de un único actor de amenazas de procedencia desconocida.

La vulnerabilidad de seguridad, identificada como CVE-2024-3400 (puntuación CVSS: 10.0), es una falla de inyección de comandos que permite a los atacantes no autenticados ejecutar código arbitrario con privilegios de root en el firewall.

Es relevante destacar que el problema solo afecta a las configuraciones de firewall PAN-OS 10.2, PAN-OS 11.0 y PAN-OS 11.1 que tienen habilitado el gateway GlobalProtect y la telemetría del dispositivo.

La Operación EclipseNocturno implica la explotación de la vulnerabilidad para crear una tarea programada que se ejecuta cada minuto para obtener comandos alojados en un servidor externo («172.233.228[.]93/policy» o «172.233.228[.]93/patch»), los cuales luego se ejecutan utilizando el intérprete de comandos bash.

Se dice que los atacantes gestionaron manualmente una lista de control de acceso (ACL) para el servidor de comando y control (C2) para asegurarse de que solo pueda acceder desde el dispositivo que se comunica con él.

Aunque la naturaleza exacta del comando es desconocida, se sospecha que la URL sirve como vehículo de entrega para un backdoor basado en Python en el firewall que Volexity, que descubrió la explotación en la naturaleza de CVE-2024-3400 el 10 de abril de 2024, está rastreando como UPSTYLE y está alojado en un servidor diferente («144.172.79[.]92» y «nhdata.s3-us-west-2.amazonaws[.]com»).

El archivo Python está diseñado para escribir y ejecutar otro script de Python («system.pth»),

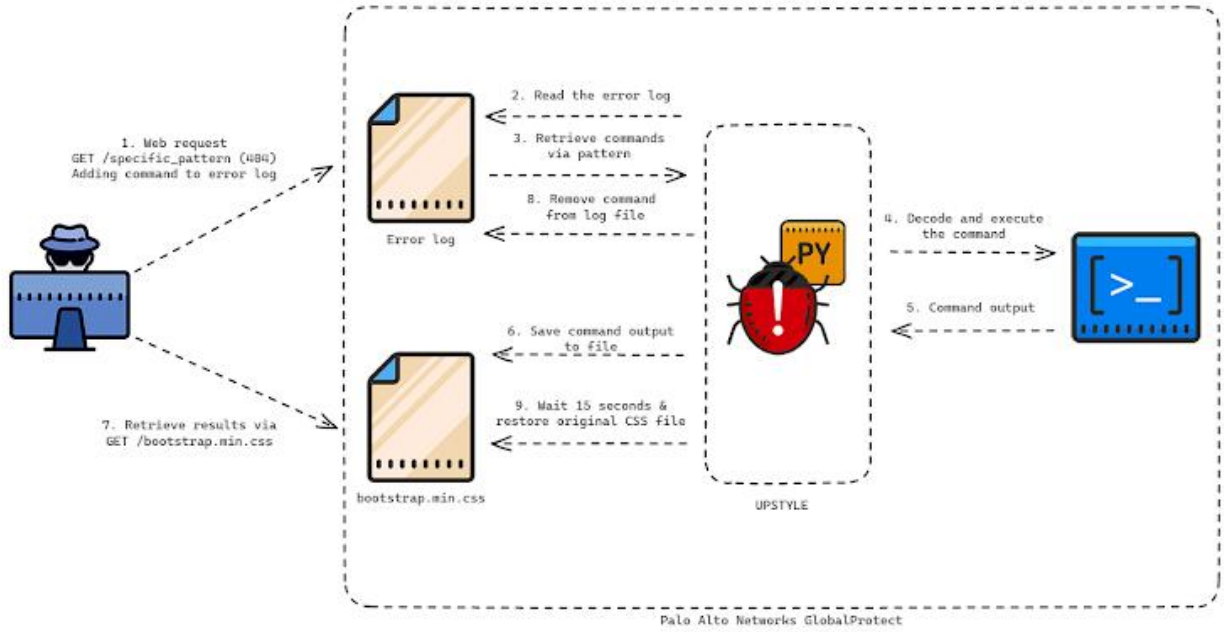
que posteriormente decodifica y ejecuta el componente de backdoor incrustado que es responsable de ejecutar los comandos del actor de amenazas en un archivo llamado «sslvpn_ngx_error.log». Los resultados de la operación se escriben en un archivo separado llamado «bootstrap.min.css».

El aspecto más interesante de la cadena de ataque es que tanto los archivos utilizados para extraer los comandos como para escribir los resultados son archivos legítimos asociados con el firewall:

- /var/log/pan/sslvpn_ngx_error.log
- /var/appweb/sslvpndocs/global-protect/portal/css/bootstrap.min.css

En cuanto a cómo se escriben los comandos en el registro de errores del servidor web, el actor de amenazas falsifica solicitudes de red especialmente diseñadas a una página web inexistente que contiene un patrón específico. El backdoor luego analiza el archivo de registro y busca la línea que coincida con la misma expresión regular («img[([a-zA-Z0-9+/=]+)]») para decodificar y ejecutar el comando dentro de él.

> *«El guion luego creará otro hilo que ejecuta una función llamada restaurar. La función de restauración toma el contenido original del archivo bootstrap.min.css, así como los tiempos de acceso originales y modificados, duerme durante 15 segundos y escribe los contenidos originales de nuevo en el archivo y restablece los tiempos de acceso y modificación a sus valores originales»,* dijo Unit 42.



El objetivo principal parece ser evitar dejar rastros de las salidas de los comandos, lo que requiere que los resultados sean exfiltrados dentro de 15 segundos antes de que se sobrescriba el archivo.

Volexity, en su propio análisis, dijo que observó al actor de amenazas explotando remotamente el firewall para crear un shell inverso, descargar herramientas adicionales, pivotar hacia las redes internas y, en última instancia, exfiltrar datos. La escala exacta de la campaña no está clara en este momento. La empresa ha asignado al adversario el alias de UTA0218.

> *«El modus operandi y la rapidez empleados por el atacante sugieren un actor de amenazas altamente capaz con un claro manual de instrucciones sobre qué acceder para avanzar en sus objetivos,»* dijo la firma de ciberseguridad estadounidense.

> *«Los objetivos iniciales de UTA0218 estaban dirigidos a obtener las claves de copia de seguridad del dominio DPAPI y apuntar a las credenciales de Active Directory*

> *obteniendo el archivo NTDS.DIT. También apuntaron a las estaciones de trabajo de los usuarios para robar cookies guardadas y datos de inicio de sesión, junto con las claves DPAPI de los usuarios.»*

Se recomienda a las organizaciones que busquen signos de movimiento lateral internamente desde su dispositivo Palo Alto Networks GlobalProtect firewall.

El desarrollo también ha llevado a la Agencia de Ciberseguridad e Infraestructura de EE. UU. (CISA) a agregar la falla a su catálogo de Vulnerabilidades Explotadas Conocidas (KEV), requiriendo que las agencias federales apliquen los parches antes del 19 de abril para mitigar posibles amenazas. Se espera que Palo Alto Networks lance correcciones para la falla a más tardar el 14 de abril.

> *«Dirigirse a dispositivos perimetrales sigue siendo un vector de ataque popular para actores de amenazas capaces que tienen el tiempo y los recursos para invertir en investigar nuevas vulnerabilidades,»* dijo Volexity.

> *«Es muy probable que UTA0218 sea un actor de amenazas respaldado por un estado basado en los recursos necesarios para desarrollar y explotar una vulnerabilidad de esta naturaleza, el tipo de víctimas atacadas por este actor y las capacidades mostradas para instalar el backdoor de Python y acceder aún más a las redes de las víctimas.»*