Una nueva versión de la botnet Mirai, está explotando una vulnerabilidad crítica recientemente descubierta en dispositivos de almacenamiento conectados a red (NAS), como un intento por infectar y controlar de forma remota las máquinas vulnerables.

Denominada como Mukashi, la variante del malware emplea ataques de fuerza bruta utilizando distintas combinaciones de credenciales predeterminadas para iniciar sesión en los productos de firewall Zyxel NAS, UTM, ATP y VPN para tomar el control de los dispositivos y agregarlos a una red de bots infectados que pueden usarse para realizar ataques de denegación de servicio distribuidos (DDoS).

Muchos productos NAS de Zyxel que ejecutan versiones de firmware hasta 5.21 son vulnerables, según el equipo global de inteligencia de amenazas de la Unidad 42 de Palo Alto Networks, afirmando que descubrieron la primera explotación de este tipo en la naturaleza el 12 de marzo.

Mukashi depende de una vulnerabilidad de inyección de comando previa a la autenticación, registrada como CVE-2020-9054, para la cual una prueba de concepto se hizo pública el mes pasado. El error reside en un programa *«weblogin.cgi»* utilizado por los dispositivos Zyxel, lo que potencialmente permite a los atacantes ejecutar código remoto mediante inyección de comandos.

> *«El ejecutable weblogin.cgi no desinfecta de forma correcta el parámetro del nombre de usuario durante la autenticación. El atacante puede usar una comilla simple (') para cerrar la cadena y un punto y coma (;) para concatenar comandos arbitrarios para lograr la inyección de comandos. Debido a que weblogin.cgi acepta solicitudes HTTP GET y POST, el atacante puede incorporar la carga maliciosa en una de estas solicitudes HTTP y obtener la ejecución del código»*, según Unit 42.

Zyxel emitió un parche para la vulnerabilidad el mes pasado luego de que surgió que se vendían instrucciones precisas para la explotación de la vulnerabilidad en foros clandestinos de hacking por 20 mil dólares para utilizar contra objetivos. Sin embargo, la actualización no

soluciona la falla en muchos dispositivos antiguos no compatibles.

Como solución alternativa, el fabricante de equipos de red con sede en Taiwán ha instado a los usuarios de esos modelos afectados, a que no dejen los productos expuestos directamente a Internet y los conecten a un enrutador de seguridad o firewall para una protección adicional.

Al igual que otras variantes de Mirai, Mukashi opera escaneando Internet en busca de dispositivos de IoT vulnerables como enrutadores, dispositivos NAS, cámaras de seguridad y grabadoras de video digital (DVR), en busca de hosts potenciales que estén protegidos solo por credenciales predeterminadas de fábrica o de uso común.

Si un inicio de sesión de fuerza bruta resulta exitoso, Mukashi no solo informa el intento de inicio de sesión a un servidor de comando y control (C2) controlado por un atacante remoto, sino que también espera nuevos comandos para lanzar ataques DDoS.

> *«Cuando se ejecuta, Mukashi imprime el mensaje «Protegiendo su dispositivo de futuras infecciones» en la consola. El malware luego cambia su nombre de proceso a dvrhelper, lo que sugiere que Mukashi puede heredar algunos rasgos de su predecesor»,* dijeron los investigadores.

La botnet Mirai fue desubierta en 2016, y desde entonces, se ha vinculado a una serie de ataques DDoS a gran escala, incluido uno contra el proveedor de servicios DNS Dyn en octubre de 2016, lo que hace que las principales plataformas y servicios de Internet permanezcan inaccesibles para los usuarios en Europa y América del Norte.

Desde entonces, surgieron muchas variantes de Mirai, en parte debido a la disponibilidad de su código fuente en Internet desde 2016.

Se recomienda a los usuarios de Zyxel que descarguen la actualización del firmware para proteger los dispositivos de los secuestros de Mukashi. La actualización de las credenciales predeterminadas con contraseñas de inicio de sesión complejas también pueden contribuir en gran parte a prevenir los ataques de fuerza bruta.

Puedes revisar la lista de productos Zyxel afectados y probar si un dispositivo NAS Zyxel es vulnerable.