Backdoor Malware

¿Qué tipo de amenaza es?

En informática un **backdoor** es un **tipo** de virus diseñado para dar acceso a usuarios maliciosos al control de un equipo infectado de manera remota.

¿Cómo comienza y cómo se propaga esta amenaza?

Como vectores de infección inicial, el grupo ha estado aprovechando la explotación de dispositivos vulnerables expuestos a Internet, como servidores web e interfaces de gestión para equipos de red. Una vez dentro de un sistema, sus operadores utilizan herramientas de código abierto para escanear el entorno y realizar movimiento lateral. El acceso interactivo se logra de dos maneras: (1) a través de un backdoor personalizado que llamamos Turian que deriva del backdoor Quarian; y (2) en menos casos, cuando se requiere un acceso más directo e interactivo, se implementan ciertas herramientas de acceso remoto de código abierto.

¿Hay más de una amenaza aplicada?

Si, también hacen mención de un Dropper (Este tipo de amenazas usa dos métodos para tratar de evadir los procesos de detección. En principio se valen de técnicas destinadas a embeber código malicioso “a cuentagotas” (de ahí su nombre). Y adicionalmente funcionan como *matryoshkas*, las muñecas rusas que por fuera simulan ser una única pieza, pero esconden representaciones más pequeñas en su interior.

BackdoorDiplomacy apuntó a servidores con puertos expuestos a Internet, probablemente explotando vulnerabilidades sin parchear o la pobre implementación de la seguridad de carga de archivos.

¿Qué solución o medida recomendarían?

Aplicar estrategias de defensa en profundidad: activando el firewall local siempre que sea posible y usando un programa antimalware vigente, con las firmas actualizadas a diario. Implementar esquemas de mínimo privilegio: utilizando cuentas de acceso estándar y dejando las del tipo *root* , *admin* o *superusuario* sólo para tareas específicas o de mantenimiento)