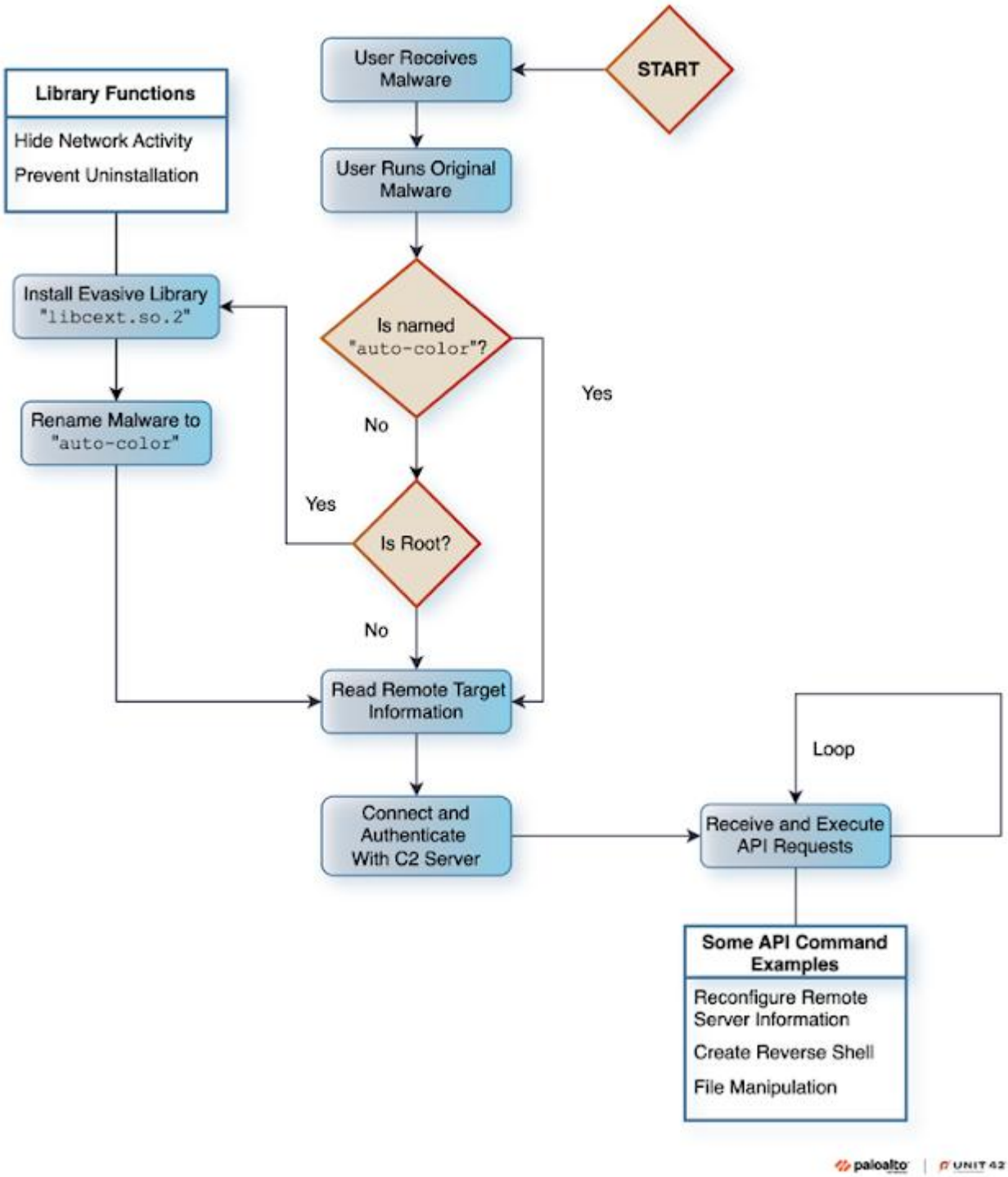
Entre noviembre y diciembre de 2024, universidades y entidades gubernamentales en América del Norte y Asia fueron blanco de un malware para Linux hasta ahora desconocido, denominado Auto-Color, según nuevos hallazgos de Palo Alto Networks Unit 42.

> *«Una vez que Auto-Color se instala, los atacantes obtienen acceso remoto total a los equipos infectados, lo que dificulta su eliminación sin herramientas especializadas»,* explicó el investigador de seguridad Alex Armstrong en un análisis técnico del malware.

El nombre Auto-Color proviene del archivo al que el programa malicioso cambia su nombre tras ser instalado. Aunque aún no se ha identificado su método de propagación, se sabe que requiere que la víctima lo ejecute manualmente en su sistema Linux.

Uno de los rasgos más llamativos de este malware es la variedad de estrategias que emplea para evitar ser detectado. Entre ellas, utiliza nombres de archivos aparentemente inofensivos como «door» o «egg», oculta las conexiones con su servidor de control (C2) y usa algoritmos de cifrado exclusivos para encubrir tanto su comunicación como su configuración.

Si se ejecuta con privilegios de administrador, Auto-Color instala una biblioteca maliciosa llamada «libcext.so.2», se copia a la ruta «/var/log/cross/auto-color» y altera el archivo «/etc/ld.preload» para asegurar su permanencia en el sistema.


START
User Receives Malware
User Runs Original Malware
Is named "auto-color"?
Yes
No
Is Root?
Yes
No
Library Functions
Hide Network Activity
Prevent Uninstallation
Install Evasive Library "libcext.so.2"
Rename Malware to "auto-color"
Read Remote Target Information
Connect and Authenticate With C2 Server
Receive and Execute API Requests
Loop
Some API Command Examples
Reconfigure Remote Server Information
Create Reverse Shell
File Manipulation
paloalto | UNIT 42

> *«Si el usuario no posee permisos de root, el malware no instalará la biblioteca oculta. Aun así, intentará ejecutar la mayor cantidad de acciones posibles en sus etapas posteriores sin este componente»,* señaló Armstrong.

El código malicioso de la biblioteca intercepta ciertas funciones de la libc para modificar la llamada al sistema `open()`, lo que le permite ocultar las comunicaciones con el C2 manipulando el archivo «/proc/net/tcp», que almacena información sobre las conexiones de red activas. Esta táctica ya había sido utilizada por otro malware para Linux, conocido como Symbiote.

Además, impide su eliminación protegiendo el archivo «/etc/ld.preload» contra modificaciones o intentos de borrado.

Después de establecerse en el sistema, Auto-Color se comunica con un servidor C2, lo que permite a los atacantes abrir un shell inverso, recolectar información del sistema, modificar o crear archivos, ejecutar procesos, usar la máquina infectada como un intermediario entre una dirección IP remota y un objetivo específico, e incluso eliminarse a sí mismo mediante un mecanismo de autodestrucción.

> *«Al activarse, el malware busca instrucciones remotas desde un servidor de control, el cual puede establecer puertas traseras de shell inverso en el equipo de la víctima. Los atacantes generan y cifran cada dirección IP del servidor de comando utilizando un algoritmo de encriptación exclusivo»*, explicó Armstrong.