# ALERTA TÉCNICA

**MICITT-DGD-DRII-AT-079-2020**

## Malware ¨Drovorub¨ diseñado para Sistemas Operativos Linux para robo de información y ciberataques

Se les comunica a los Directores (as) /Jefes (as) de Tecnologías de Información y a los enlaces de Ciberseguridad, para que tomen las medidas necesarias sobre este Malware llamado ¨¨Drovorub.

La Agencia de Seguridad Nacional (NSA) y la Oficina Federal de Investigaciones (FBI) publicaron un nuevo aviso de seguridad cibernética sobre este malware denominado Drovorub, el cual han relacionado con el grupo APT28 (Fancy Bear) utilizado para acciones contra oficinas gubernamentales, partidos políticos, y departamentos de defensa del mundo.

Drovorub es un conjunto de herramientas de malware de Linux que consta de un implante junto con un rootkit del módulo del kernel, una herramienta de transferencia de archivos y reenvío de puertos y un servidor de comando y control (C2). Cuando se implementa en una máquina víctima, Drovorub proporciona la capacidad de comunicaciones directas con la infraestructura C2 controlada por el actor; capacidades de carga y descarga de archivos; ejecución de comandos arbitrarios; reenvío de puertos del tráfico de la red a otros hosts de la red; e implementa técnicas de ocultación para evadir la detección. El malware ataca sistemas basados en Linux que no están actualizados con el fin de vulnerarlos y robar información.

El documento publicado por la NSA y el FBI (adjunto) incluye un desglose técnico del funcionamiento del malware y las medidas de mitigación. Para evitar una posible infección, el administrador de sistemas tiene que actualizar el kernel de Linux a la

versión 3.7. También es necesario configurar el sistema para la carga exclusiva de módulos que cuenten con una firma digital válida, que se complementa con el Arranque Seguro por UEFI.

Las autoridades de Estados Unidos informan también que los ataques con Drovorub estarían relacionados a un intento de vulnerar y ¨hackear¨ dispositivos IoT con el fin de obtener acceso a redes más amplias.

## Recomendaciones

- Se solicita actualizar todos sus servidores y equipos.
- Se solicita que todas las estaciones de trabajo se encuentren actualizadas.
- Se solicita actualizar el kernel de Linux a la versión 3.7. o superior
- Revisar la documentación adjunta en los siguientes enlaces para tomar las medidas técnicas pertinentes:
  - https://media.defense.gov/2020/Aug/13/2002476465/-1/-1/0/CSA_DROVORUB_RUSSIAN_GRU_MALWARE_AUG_2020.PDF
  - https://www.nsa.gov/Portals/70/documents/resources/cybersecurity-professionals/DROVORUB-Fact%20sheet%20and%20FAQs.pdf?ver=2020-08-13-114246-203

## Referencias


https://www.nsa.gov/news-features/press-room/Article/2311407/nsa-and-fbi-expose-russian-previously-undisclosed-malware-drovorub-in-cybersecu/

https://media.defense.gov/2020/Aug/13/2002476465/-1/-1/0/CSA_DROVORUB_RUSSIAN_GRU_MALWARE_AUG_2020.PDF

https://www.nsa.gov/Portals/70/documents/resources/cybersecurity-professionals/DROVORUB-Fact%20sheet%20and%20FAQs.pdf?ver=2020-08-13-114246-203

**En caso de alguna duda o consulta, se pueden comunicar al CSIRT-CR por medio del correo electrónico csirt@micitt.go.cr**

Firmado digitalmente por JORGE EMILIO MORA FLORES (FIRMA)
Fecha: 2020.08.18 16:15:31 -06'00'

Firmado digitalmente por ROBERTO PAULO LEMAITRE PICADO (FIRMA)
Ubicación: CSIRT-CR
Fecha: 2020.08.18 16:24:50 -06'00'

**Jorge Mora Flores**
**Director de Gobernanza Digital**

**Roberto Lemaitre Picado**
**Coordinador CSIRT-CR**