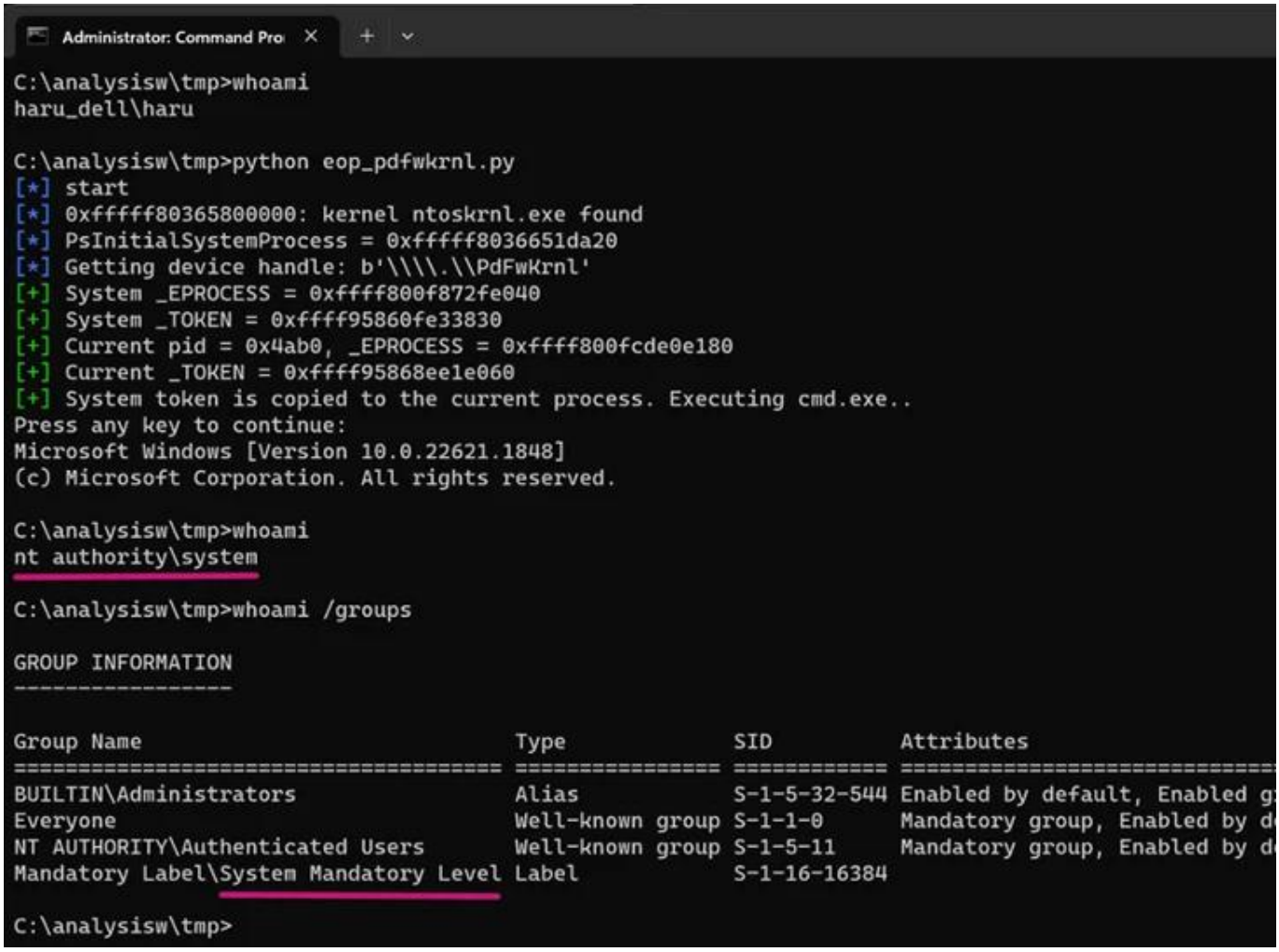
Casi 34 controladores exclusivos del Modelo de Controladores de Windows (WDM) y de los Marcos de Controladores de Windows (WDF) podrían ser aprovechados por actores de amenazas no privilegiados para obtener pleno control de los dispositivos y ejecutar código arbitrario en los sistemas subyacentes.

> *«Mediante la explotación de estos controladores, un atacante sin privilegios podría eliminar/alterar el firmware y/o elevar los privilegios del sistema operativo»*, afirmó Takahiro Haruyama, un investigador sénior de amenazas en VMware Carbon Black.

Esta investigación amplía estudios anteriores, como ScrewedDrivers y POPKORN, que utilizaron la ejecución simbólica para automatizar el descubrimiento de controladores vulnerables. Se enfoca específicamente en controladores que brindan acceso al firmware a través de E/S de puerto y E/S mapeada en memoria.

Algunos de los nombres de los controladores vulnerables incluyen AODDriver.sys, ComputerZ.sys, dellbios.sys, GEDevDrv.sys, GtcKmdfBs.sys, IoAccess.sys, kerneld.amd64, ngiodriver.sys, nvoclock.sys, PDFWKRNL.sys (CVE-2023-20598), RadHwMgr.sys, rtif.sys, rtport.sys, stdcdrv64.sys y TdkLib64.sys (CVE-2023-35841).



De los 34 controladores, seis permiten el acceso a la memoria del núcleo que podría ser abusado para elevar privilegios y superar soluciones de seguridad. Doce de los controladores podrían ser explotados para sortear mecanismos de seguridad como la aleatorización del espacio de direcciones del núcleo (KASLR).

Siete de los controladores, incluido stdcdrv64.sys de Intel, pueden ser utilizados para borrar el firmware en la memoria flash SPI, lo que inutilizaría el sistema. Intel ha lanzado una corrección para este problema.

VMware también identificó controladores WDF como WDTKernel.sys y H2OFFT64.sys que no son vulnerables en términos de control de acceso, pero que pueden ser fácilmente utilizados por actores de amenazas privilegiados para llevar a cabo lo que se conoce como un ataque de *«Trae Tu Propio Controlador Vulnerable»* (BYOVD).

Esta técnica ha sido empleada por varios adversarios, incluido el grupo Lazarus vinculado a Corea del Norte, como una manera de obtener privilegios elevados y desactivar el software de seguridad en los puntos finales comprometidos para evadir la detección.

> *«El alcance actual de las API/instrucciones dirigidas por el script de IDAPython para el análisis estático de código x64 de controladores vulnerables es limitado y se restringe solo al acceso al firmware. Sin embargo, es sencillo ampliar el código para abarcar otros vectores de ataque (por ejemplo, finalizar procesos arbitrarios)»*, afirmó Haruyama.