Dos semanas después de que surgieran detalles sobre una segunda cepa de borrador de datos lanzada en ataques contra Ucrania, se detectó otro malware destructivo en medio de la continua invasión militar del país por parte de Rusia.

La compañía eslovaca de ciberseguridad ESET, denominó al tercer limpiaparabrisas «CaddyWiper», que se observó por primera vez el 14 de marzo alrededor de las 9:38 am UTC. Los metadatos asociados con el ejecutable («caddy.exe«) muestran que el malware se compiló a las 7:19 am UTC, poco más de dos horas antes de su implementación.

CaddyWiper se destaca por el hecho de que no comparte ninguna similitud con los limpiaparabrisas descubiertos antes en Ucrania, incluidos HermeticWiper (también conocido como FoxBlade o KillDisk) e IsaacWiper (también conocido como Lasainraw), mismos que se han implementado en sistemas pertenecientes a gobiernos y empresas comerciales.

> *«El objetivo final de los atacantes es el mismo que el de IsaacWiper y HermeticWiper: inutilizar los sistemas borrando los datos de los usuarios y la información de las particiones. Todas las organizaciones objetivo de los recientes ataques de limpiaparabrisas estaban en el sector gubernamental o financiero»*, dijo Jean-Ian Boutin, jefe de investigación de amenazas de ESET.

A diferencia de CaddyWiper, se cree que las familias de malware HermeticWiper e IsaacWiper estuvieron en desarrollo por meses antes de su lanzamiento, con las muestras más antiguas compiladas el 28 de diciembre y el 19 de octubre de 2021, respectivamente.

Pero el limpiador recién descubierto comparte una superposición tatica con HermeticWiper en el sentido de que el malware, en un caso, se implementó a través del controlador de dominio de Windows, lo que indica que los atacantes habían tomado el control del servidor de Active Directory.

> *«Curiosamente, CaddyWiper evita la destrucción de datos en los controladores de*

> *dominio. Esta es probablemente una forma de que los atacantes mantengan su acceso dentro de la organización mientras siguen perturbando las operaciones»,* dijo la compañía.

Microsoft, que atribuyó los ataques de HermeticWiper a un grupo de amenazas rastreado como DEV-0665, dijo que *«el objetivo previsto de estos ataques es la interrupción, degradación y destrucción de los recursos específicos en el país».*

El desarrollo llega cuando los ciberdelincuentes aprovechan cada vez más y de forma oportunista el conflicto para diseñar señuelos de phishing, incluidos temas de asistencia humanitaria y varios tipos de recaudación de fondos, para ofrecer una variedad de puertas traseras como Remcos.

> *«El interés global en la guerra en curso en Ucrania lo convierte en un evento de noticias conveniente y efectivo para que los ciberdelincuentes exploten. Si cierto tema de señuelo va a aumentar las posibilidades de que una víctima potencial instale su carga útil, lo usarán»,* dijeron los investigadores de Cisco Talos.

No solo es Ucrania la que ha estado en el extremo receptor de los ataques de limpiaparabrisas. La semana pasada, la compañía de seguridad cibernética Trend Micro, reveló detalles de un limpiador basado en .NET llamado RURansom, que se ha dirigido exclusivamente a entidades en Rusia cifrando archivos con una clave criptográfica generada aleatoriamente.

> *«Las claves son únicas para cada archivo cifrado y no se almacenan en ningún lugar, lo que hace que el cifrado sea irreversible y marca el malware como un limpiador en lugar de una variante de ransomware»*, dijeron los investigadores.