El grupo de cibercriminales conocido como CosmicBeetle ha lanzado una nueva variante de ransomware personalizada llamada ScRansom, la cual ha sido utilizada en ataques contra pequeñas y medianas empresas (PYMES) en Europa, Asia, África y América del Sur. Además, se sospecha que están operando como afiliados de RansomHub.

> *«CosmicBeetle ha reemplazado su anterior ransomware, Scarab, por ScRansom, que está en constante evolución. Aunque no es de primer nivel, este grupo es capaz de comprometer objetivos relevantes»*, explicó Jakub Souček, investigador de ESET, en un análisis publicado hoy.

Las víctimas de los ataques con ScRansom pertenecen a sectores como manufactura, farmacéutica, legal, educación, salud, tecnología, hospitalidad, ocio, servicios financieros y gobiernos regionales.

CosmicBeetle es particularmente conocido por su conjunto de herramientas maliciosas llamado Spacecolon, que previamente fue identificado como responsable de distribuir el ransomware Scarab a nivel global en diversas organizaciones.

También conocido como NONAME, este actor malicioso ha experimentado con el generador filtrado de LockBit, intentando hacerse pasar por este grupo de ransomware en sus notas de rescate y sitios de filtración desde noviembre de 2023.

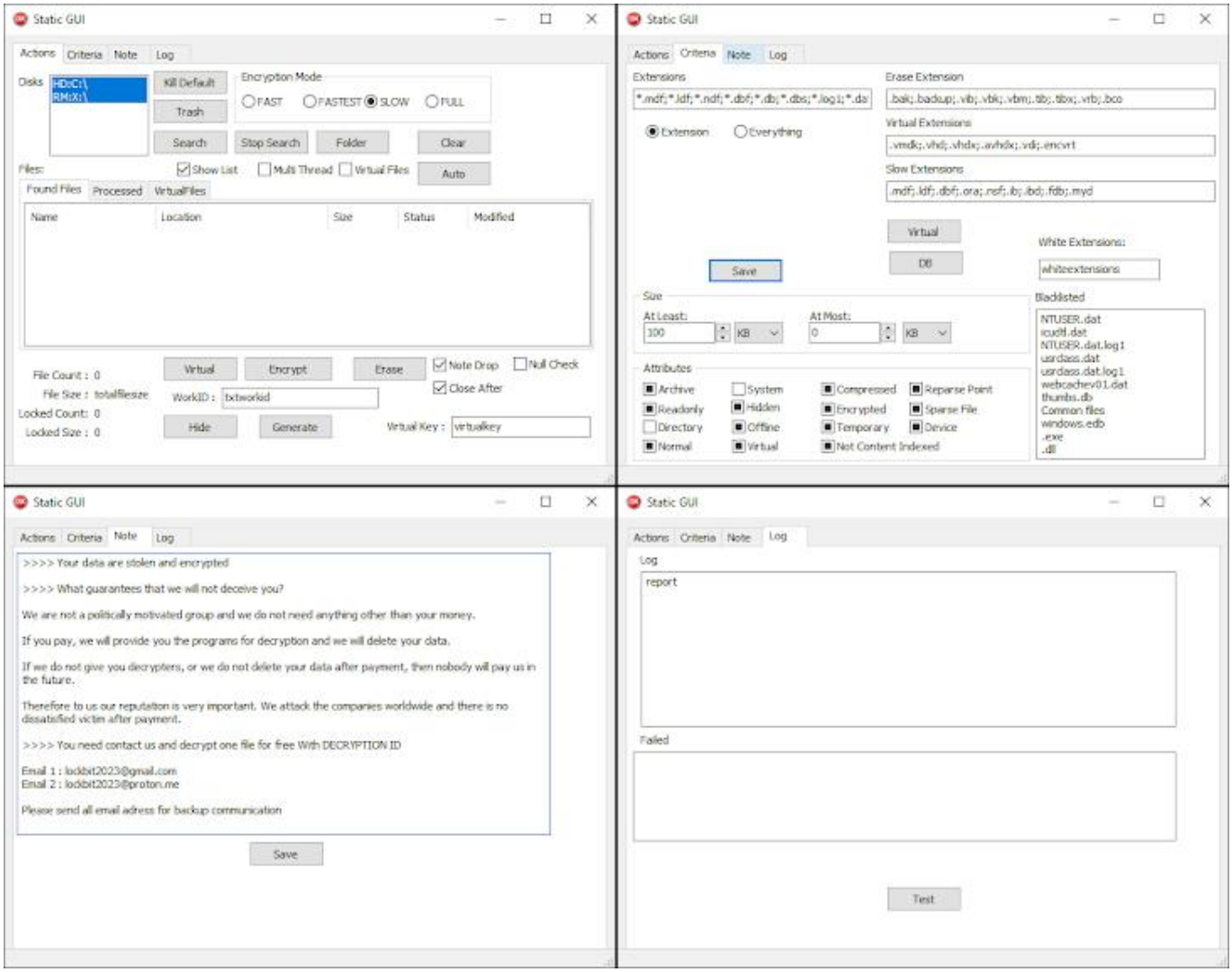
Aún no se ha identificado a los responsables ni su ubicación, aunque anteriormente se especulaba que podrían ser de origen turco debido al uso de un esquema de cifrado personalizado en otra herramienta llamada ScHackTool. Sin embargo, ESET ahora duda de esta hipótesis.

> *«El esquema de cifrado de ScHackTool se utiliza en la herramienta legítima Disk Monitor Gadget. Es probable que este algoritmo haya sido adaptado [de un hilo en Stack Overflow] por VOVSOFT [la empresa de software turca detrás de la*

> *herramienta], y años después, CosmicBeetle lo encontró y lo usó en ScHackTool»*, indicó Souček.

Las cadenas de ataque han sido vistas aprovechando ataques de fuerza bruta y vulnerabilidades conocidas (CVE-2017-0144, CVE-2020-1472, CVE-2021-42278, CVE-2021-42287, CVE-2022-42475 y CVE-2023-27532) para infiltrarse en los sistemas de sus víctimas.

Los ataques también incluyen el uso de varias herramientas, como Reaper, Darkside y RealBlindingEDR, para desactivar procesos de seguridad y evitar la detección antes de desplegar el ransomware ScRansom, que está escrito en Delphi. Este malware admite el cifrado parcial para acelerar el ataque y un modo «ERASE» que sobrescribe los archivos con un valor constante, haciéndolos irrecuperables.



La relación con RansomHub se debe a que la empresa de ciberseguridad eslovaca observó la instalación tanto de cargas útiles de ScRansom como de RansomHub en el mismo equipo dentro de una semana.

> *«Probablemente, debido a las dificultades de crear ransomware desde cero, CosmicBeetle trató de aprovechar la reputación de LockBit, posiblemente para ocultar problemas con su ransomware y aumentar las posibilidades de que las*

> *víctimas paguen»*, afirmó Souček.

Cicada3301 lanza una versión renovada

Esta revelación coincide con la observación de que los actores detrás del ransomware Cicada3301 (también llamado Repellent Scorpius) están utilizando una versión actualizada de su cifrador desde julio de 2024.

> *«Los desarrolladores de la amenaza añadieron un nuevo argumento de línea de comandos, –no-note. Cuando se utiliza este argumento, el cifrador no deja la nota de rescate en el sistema»,* explicó Palo Alto Networks Unit 42 en un informe.

Otra modificación significativa es la eliminación de nombres de usuario o contraseñas codificados en el archivo binario, aunque aún tiene la capacidad de ejecutar PsExec usando esas credenciales si están disponibles, una técnica recientemente destacada por Morphisec.

De manera interesante, el proveedor de ciberseguridad indicó que ha encontrado señales de que este grupo posee datos de compromisos previos a la aparición del grupo bajo el nombre Cicada3301.

Esto sugiere la posibilidad de que este grupo haya operado bajo otra identidad de ransomware en el pasado o que haya adquirido los datos de otros grupos de ransomware. Sin embargo, Unit 42 también detectó algunas similitudes con otro ataque llevado a cabo por un afiliado que usó el ransomware BlackCat en marzo de 2022.

BURNTCIGAR se transforma en un eliminador de EDR

Los descubrimientos también destacan la evolución de un controlador firmado en modo kernel para Windows, utilizado por diversos grupos de ransomware para desactivar el

software de Respuesta y Detección de Endpoint (EDR). Esto le permite funcionar como un eliminador, borrando componentes clave de dichas soluciones en lugar de simplemente cerrarlos.

El malware en cuestión es POORTRY, que se distribuye mediante un cargador conocido como STONESTOP para llevar a cabo un ataque Bring Your Own Vulnerable Driver (BYOVD), eludiendo los mecanismos de Verificación de Firmas de Controladores. La capacidad de este malware para *«eliminar forzosamente»* archivos del disco fue reportada por primera vez por Trend Micro en mayo de 2023.

Detectado desde 2021, POORTRY, también llamado BURNTCIGAR, ha sido empleado por varios grupos de ransomware, incluidos CUBA, BlackCat, Medusa, LockBit y RansomHub a lo largo del tiempo.

> *«Tanto el ejecutable Stonestop como el controlador Poortry están altamente empaquetados y ofuscados. Este cargador fue ofuscado por un empaquetador de código cerrado llamado ASMGuard, que está disponible en GitHub»*, señaló Sophos en un informe reciente.

POORTRY está diseñado para desactivar productos EDR utilizando diferentes métodos, como la eliminación o modificación de rutinas de notificación del kernel. El eliminador de EDR busca terminar procesos de seguridad y dejar inservible al agente EDR, eliminando archivos críticos del disco.

El uso de una versión más avanzada de POORTRY por parte de RansomHub es notable, especialmente porque este grupo de ransomware ha sido visto utilizando otra herramienta de eliminación de EDR llamada EDRKillShifter este año.

> *«Es importante tener en cuenta que los actores maliciosos han estado probando continuamente diferentes técnicas para desactivar productos EDR, una tendencia*

> *que hemos estado observando desde al menos 2022. Estos experimentos pueden involucrar tácticas variadas, como explotar controladores vulnerables o usar certificados que se han filtrado accidentalmente o conseguido por medios ilegales»,* comentó Sophos.
>
> *«Si bien parece que hay un aumento considerable en estas actividades, es más correcto decir que es parte de un proceso en curso y no un incremento repentino».*
>
> *«El empleo de distintas herramientas para desactivar EDR, como EDRKillShifter por parte de grupos como RansomHub, probablemente refleja esta continua experimentación. También es posible que diferentes afiliados estén involucrados, lo que explicaría la variedad de métodos, aunque sin información concreta, preferimos no especular demasiado sobre este aspecto».*