Investigadores de seguridad cibernética descubrieron un nuevo malware destructivo de borrado de datos previamente no descubierto que está siendo utilizado por hackers patrocinados por el estado en la naturaleza, para apuntar a organizaciones energéticas e industriales en el Medio Oriente.

Apodado como ZeroCleare, el malware del limpiador de datos se ha vinculado a los grupos de piratería patrocinados por el estado iraní, APT34, también conocido como ITG13 y Oilrig, además de Hive0081, también conocido como xHunt.

Un equipo de investigadores de IBM que descubrió el malware ZeroCleare, afirma que el nuevo malware limpiador comparte algunas similitudes de alto nivel con Shamoon, una de las familias de malware más destructivas conocidas por dañar 30,000 computadoras en el mayor productor de petróleo de Arabia Saudita en 2012.

Al igual que el malware Shamoon, ZeroCleare también utiliza un controlador de disco duro legítimo llamado *«RawDisk by ElDos»,* para sobrescribir el registro de arranque maestro (MBR) y las particiones de disco de las computadoras específicas que ejecutan el sistema operativo Windows.

Aunque el controlador ElDos no está firmado, el malware logra ejecutarlo cargando un controlador VirtualBox de Oracle vulnerable pero no firmado, explotándolo para omitir el mecanismo de verificación de firma y cargar el controlador ElDos sin firmar.

> *«Para obtener acceso al núcleo del dispositivo, ZeroCleare utilizó un controlador intencionalmente vulnerable y scripts maliciosos PowerShell/Batch para evitar los controles de Windows»,* dijeron los investigadores.

Para implementar el malware ZeroCleare en la mayor cantidad de computadoras posible en una organización, los atacantes intentan por primera vez forzar contraseñas de cuentas de red y luego instalar shells web ASPX, como China Chopper y Tunna, explotando una vulnerabilidad de SharePoint.

> *«Al agregar estas tácticas de living-of-the-land al esquema, ZeroCleare se extendió a numerosos dispositivos en la red afectada, sembrando las semillas de un ataque destructivo que podría afectar a miles de dispositivos y causar interrupciones que podrían tomar meses para recuperarse completamente»,* agregaron los investigadores.

Los mismos actores de amenazas también intentaron instalar un software de acceso remoto legítimo llamado TeamViewer, y utilizaron una versión ofuscada de la herramienta de robo de credenciales Mimikatz para robar más credenciales de red de los servidores comprometidos.

Aunque los investigadores no revelaron los nombres de ninguna organización objetivo, confirmaron que existen dos versiones de ZeroCleare que se han visto en la naturaleza, una para cada arquitectura de Windows, pero solo las de 64 bits funcionan.

Según los investigadores, los ataques ZeroCleare no son oportunistas, y parecen ser operaciones dirigidas contra sectores y organizaciones específicos.

> *«X-Force IRIS ha estado siguiendo un marcado aumento en los ataques destructivos en el último año, después de haber registrado un increíble aumento del 200 por ciento en la cantidad de ataques destructivos en los últimos seis meses. En cuanto a la región geográfica afectada por el malware ZeroCleare, no es la primera vez que Oriente Medio ha visto ataques destructivos dirigidos a su sector energético»,* dijeron los investigadores.