Los actores de amenazas conocidos como Golden Chickens han sido vinculados con dos nuevas familias de malware llamadas TerraStealerV2 y TerraLogger, lo que sugiere un esfuerzo continuo por mejorar y diversificar su conjunto de herramientas.

> *«TerraStealerV2 está diseñado para recolectar credenciales de navegadores, datos de monederos de criptomonedas e información de extensiones de navegador. TerraLogger, en cambio, es un registrador de teclas autónomo. Utiliza un gancho de teclado de bajo nivel común para capturar pulsaciones y guarda los registros en archivos locales«,* indicó el grupo Insikt de Recorded Future.

Golden Chickens, también conocido como Venom Spider, es el nombre de un actor de amenazas con fines económicos vinculado a la familia de malware More_eggs. Se sabe que está activo desde al menos 2018 y ofrece sus herramientas bajo el modelo de malware como servicio (MaaS).

A partir de 2023, se atribuye a Golden Chickens una identidad en línea llamada badbullzvenom, supuestamente operada por individuos de Canadá y Rumania. Otras herramientas maliciosas creadas por este grupo incluyen More_eggs lite (también conocido como lite_more_eggs), VenomLNK, TerraLoader y TerraCrypt.

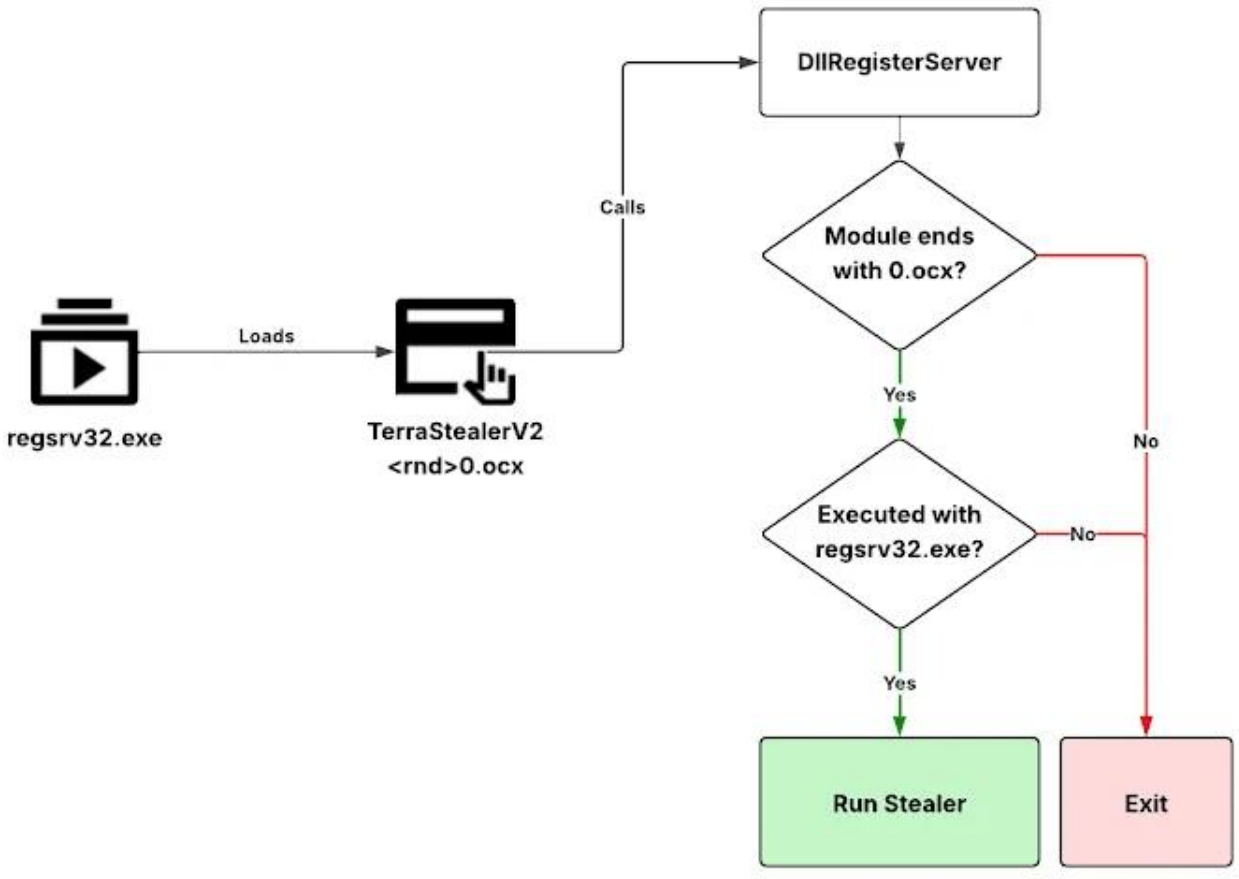
A finales del año pasado, Zscaler ThreatLabz reportó nuevas actividades relacionadas con Golden Chickens, involucrando una puerta trasera llamada RevC2 y un cargador conocido como Venom Loader, ambos entregados mediante VenomLNK.

Los hallazgos más recientes de Recorded Future muestran que el grupo sigue perfeccionando sus herramientas, publicando una versión mejorada de su malware stealer, capaz de robar datos de navegadores, monederos de criptomonedas y extensiones de navegador.

TerraStealerV2 se ha distribuido en múltiples formatos, como archivos ejecutables (EXE), bibliotecas de enlace dinámico (DLL), instaladores de Windows (MSI) y accesos directos (LNK).

En todos estos casos, el código del stealer se entrega en formato OCX (una extensión de control OLE de Microsoft) y se descarga desde un dominio externo («wetransfers[.]io«).

> *«Aunque apunta a la base de datos 'Login Data' de Chrome para obtener credenciales, no evita la protección Application Bound Encryption (ABE) incluida en versiones de Chrome posteriores a julio de 2024, lo que indica que su código está desactualizado o aún en desarrollo,»* explicó la empresa de ciberseguridad.



Los datos recopilados por TerraStealerV2 se envían tanto a Telegram como al dominio

«wetransfers[.]io«. Además, emplea herramientas legítimas de Windows como regsvr32.exe y mshta.exe para eludir la detección.

TerraLogger, también distribuido como un archivo OCX, está diseñado para registrar pulsaciones de teclas. No obstante, carece de funciones de exfiltración de datos o comunicación con servidores de comando y control (C2), lo que sugiere que está en fase inicial o pensado para operar junto a otro malware del ecosistema MaaS de Golden Chickens.

> *«El estado actual de TerraStealerV2 y TerraLogger indica que ambos siguen en desarrollo activo y aún no presentan el nivel de discreción que caracteriza a las herramientas maduras de Golden Chickens,»* señaló Recorded Future.
>
> *«Dada la trayectoria de Golden Chickens en la creación de malware para robo de credenciales y operaciones de acceso, es probable que estas capacidades continúen evolucionando.»*

La revelación coincide con la aparición de nuevas familias de malware tipo stealer como Hannibal Stealer, Gremlin Stealer y Nullpoint Stealer, diseñadas para robar una amplia gama de información sensible de sus víctimas.

También sigue al descubrimiento de una versión mejorada del malware StealC, con soporte para un protocolo de comunicación C2 simplificado y cifrado RC4 añadido.

> *«Las opciones de entrega del payload del malware ahora incluyen paquetes MSI y scripts PowerShell,»* detalló Zscaler ThreatLabz en un informe reciente.
>
> *«Un panel de control rediseñado incluye un generador integrado que permite personalizar las reglas de entrega según la geolocalización, ID de hardware (HWID)*

> *y software instalado. Otras funciones incluyen captura de pantallas en múltiples monitores, recolección unificada de archivos y fuerza bruta desde el servidor para robar credenciales.»*

La nueva versión 2.2.4 (StealC V2), lanzada en marzo de 2025, se ha observado distribuida mediante otro loader llamado Amadey. El panel de control también permite integración con bots de Telegram para enviar notificaciones y personalizar el formato de los mensajes.

> *«StealC V2 introduce mejoras como entrega de payloads optimizada, protocolo de comunicación cifrado y un panel de control renovado que permite una recolección de datos más específica,»* concluyó Zscaler.