Los actores de amenazas norcoreanos responsables de la campaña Contagious Interview han sido vistos utilizando versiones actualizadas de un malware multiplataforma llamado OtterCookie, diseñado para robar credenciales de navegadores web y otros archivos.

Según NTT Security Holdings, que publicó los nuevos hallazgos, los atacantes han estado *«actualizando el malware de forma activa y continua»,* lanzando las versiones v3 y v4 en febrero y abril de 2025, respectivamente.

Esta empresa japonesa de ciberseguridad monitorea este grupo bajo el nombre WaterPlum, también conocido como CL-STA-0240, DeceptiveDevelopment, DEV#POPPER, Famous Chollima, PurpleBravo y Tenacious Pungsan.

OtterCookie fue identificado por primera vez por NTT el año pasado, tras observar su uso en ataques desde septiembre de 2024. Se distribuye a través de un payload JavaScript incluido en un paquete npm malicioso, un repositorio manipulado en GitHub o Bitbucket, o una aplicación falsa de videollamadas. Su propósito es conectarse a un servidor remoto para ejecutar comandos en los equipos comprometidos.

La versión v3 incluye un nuevo módulo que permite subir archivos con extensiones específicas a dicho servidor. Entre los archivos objetivo se encuentran variables de entorno, imágenes, documentos, hojas de cálculo, archivos de texto y aquellos que contengan frases mnemotécnicas o de recuperación de billeteras de criptomonedas.

Cabe destacar que en la versión anterior, OtterCookie v2, este módulo era ejecutado mediante un comando shell recibido del servidor.

La cuarta versión amplía la funcionalidad de su predecesora con dos nuevos módulos: uno para robar credenciales almacenadas en Google Chrome, y otro para extraer datos de la extensión MetaMask en Chrome, Brave y iCloud Keychain.

Otra novedad de OtterCookie v4 es su capacidad para detectar si se está ejecutando en entornos virtuales como Broadcom VMware, Oracle VirtualBox, Microsoft y QEMU.

Module	Capability	V1			v2			v3			v4		
		Windows	MacOS	Linux	Windows	MacOS	Linux	Windows	MacOS	Linux	Windows	MacOS	Linux
Main	Remote Command Execution	-	-	-	✓	✓	✓	✓	✓	✓	✓	✓	✓
	VM Detection	-	-	-	-	-	-	-	-	-	✓	✓	✓
	Clipboard Data	-	-	-	✓	✓	✓	-	-	-	✓	✓	-
Upload	File Grabber	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Credential Stealer	Chrome Credential	-	-	-	-	-	-	-	-	-	✓	-	-
	MetaMask Extension	-	-	-	-	-	-	-	-	-	✓	✓	✓
	Chrome/Brave Login Data DB	-	-	-	-	-	-	-	-	-	✓	✓	✓
	MacOS Keychain	-	-	-	-	-	-	-	-	-	-	✓	-

Curiosamente, se descubrió que el primer módulo destinado a recolectar credenciales de Chrome lo hace después de descifrarlas, mientras que el segundo módulo obtiene datos de acceso aún cifrados de navegadores como Chrome y Brave.

> *«Esta diferencia en el tratamiento de los datos o en el estilo de codificación sugiere que los módulos fueron desarrollados por distintos programadores»*, afirmaron los investigadores Masaya Motoda y Rintaro Koike.

Esta revelación llega tras el descubrimiento de varios payloads maliciosos asociados con Contagious Interview en los últimos meses, lo cual indica una evolución en las tácticas de los actores.

Entre ellos, destaca un stealer escrito en Go que se presenta como una actualización de un controlador de Realtek («WebCam.zip«). Al abrirse, ejecuta un script que descarga el malware y lanza una aplicación falsa para macOS («DriverMinUpdate.app«) diseñada para robar la contraseña del sistema del usuario.

Se cree que este malware forma parte de una versión actualizada de la campaña denominada «ClickFake Interview«, según Sekoia, ya que utiliza engaños similares a los de ClickFix para simular problemas inexistentes de audio o video durante entrevistas laborales

en línea.

> *«El objetivo principal del stealer es establecer un canal de comunicación persistente con su servidor de control, perfilar el sistema infectado y extraer información sensible»,* explicó el equipo de ciberseguridad Moonlock de MacPaw. *«Esto lo logra combinando reconocimiento del sistema, robo de credenciales y ejecución remota de comandos.»*

Se ha determinado que DriverMinUpdate forma parte de un conjunto más amplio de aplicaciones maliciosas, como ChromeUpdateAlert, ChromeUpdate, CameraAccess y DriverEasy, identificadas por dmpdump, SentinelOne, ENKI y Kandji.

Otra familia de malware relacionada con esta campaña es Tsunami-Framework, entregado como payload secundario tras una puerta trasera en Python llamada InvisibleFerret. Este malware modular basado en .NET está diseñado para robar datos de navegadores y monederos de criptomonedas.

Además, incluye funciones de registro de teclas, recopilación de archivos e incluso un componente de botnet que aún estaría en fase temprana de desarrollo, según un informe reciente de la empresa alemana HiSolutions.

Según ESET, Contagious Interview forma parte de un nuevo conjunto de actividades vinculado al Grupo Lazarus, un colectivo de ciberespionaje norcoreano conocido por sus ataques motivados tanto por razones políticas como financieras, con el fin de apoyar los objetivos estratégicos del régimen y evadir sanciones internacionales.

A principios de este año, se les atribuyó el robo récord de mil millones de dólares a la plataforma de criptomonedas Bybit.

La amenaza de los falsos trabajadores de TI norcoreanos persiste

Este informe coincide con una alerta de la empresa de ciberseguridad Sophos, que reveló que los responsables del esquema de falsos trabajadores de TI de Corea del Norte —también conocidos como Famous Chollima, Nickel Tapestry y Wagemole— han empezado a enfocarse cada vez más en organizaciones de Europa y Asia, y en sectores fuera del tecnológico, con el objetivo de conseguir empleo y canalizar ingresos hacia Pyongyang.

> *«Durante el proceso previo al empleo, estos actores suelen manipular digitalmente fotografías para sus currículums falsificados y perfiles en LinkedIn, además de usarlas como prueba de experiencia laboral o trabajos en grupo»,* indicó el equipo SecureWorks Counter Threat Unit (CTU).
>
> *«Es común que empleen fotos de stock combinadas con imágenes reales de ellos mismos. También ha aumentado el uso de IA generativa, incluyendo herramientas de redacción, edición de imágenes y generadores de currículums.»*

Una vez contratados, estos trabajadores fraudulentos han sido detectados utilizando herramientas como mouse jigglers, VPNs como Astrill VPN y acceso remoto por KVM sobre IP, llegando incluso a permanecer en llamadas de Zoom de hasta ocho horas para compartir pantalla.

La semana pasada, la plataforma de criptomonedas Kraken reveló que una entrevista para un puesto de ingeniería se convirtió en una operación de inteligencia al descubrir que un hacker norcoreano intentaba infiltrarse en la empresa usando el alias «Steven Smith«.

> *«El candidato utilizaba escritorios Mac remotos, pero accedía a otros componentes a través de una VPN, una configuración comúnmente usada para ocultar la ubicación y la actividad en la red»,* explicó la empresa. *«Su currículum estaba*

> *vinculado a un perfil de GitHub con una dirección de correo electrónico comprometida en una filtración anterior.»*
>
> *«La principal forma de identificación del candidato parecía haber sido manipulada, probablemente utilizando datos robados en un caso de suplantación de identidad ocurrido dos años antes.»*

Sin embargo, en lugar de rechazar directamente la solicitud, el equipo de seguridad y reclutamiento de Kraken optó por avanzar con el proceso de selección de manera «estratégica», con el fin de tenderle una trampa. Para ello, le pidieron que confirmara su ubicación, mostrara un documento oficial de identidad y recomendara algunos restaurantes locales de la ciudad en la que afirmaba encontrarse.

> *«Desconcertado y fuera de lugar, tuvo dificultades con las pruebas básicas de verificación, y no pudo responder de forma convincente preguntas en tiempo real sobre su ciudad de residencia o su país de ciudadanía»,* señaló Kraken. *«Al finalizar la entrevista, no quedaban dudas: no era un candidato legítimo, sino un impostor que intentaba infiltrarse en nuestros sistemas.»*

En otro incidente documentado el mes pasado por el Departamento de Justicia de EE. UU. (DoJ), un hombre de 40 años de Maryland, Minh Phuong Ngoc Vong, se declaró culpable de fraude tras obtener un empleo con un contratista del gobierno y luego subcontratar el trabajo a un ciudadano norcoreano que vivía en Shenyang, China, lo que resalta la gravedad de estas actividades ilícitas de financiamiento.

La capacidad de Corea del Norte para introducir discretamente a miles de sus trabajadores en grandes empresas —frecuentemente con la ayuda de intermediarios que operan lo que se conoce como «granjas de laptops»— ha motivado reiteradas advertencias de los gobiernos de Japón, Corea del Sur, Reino Unido y Estados Unidos.

Se ha descubierto que estos trabajadores permanecen infiltrados hasta 14 meses dentro de una organización, y que algunos de ellos también participan en el robo de información o incluso en extorsiones tras ser despedidos.

> *«Las organizaciones [deberían] implementar procedimientos reforzados de verificación de identidad como parte de su proceso de entrevistas»,* recomendó la empresa de ciberseguridad Sophos. *«El personal de recursos humanos y los reclutadores deben recibir actualizaciones frecuentes sobre las tácticas empleadas en estas campañas, para ayudarles a detectar posibles trabajadores fraudulentos de origen norcoreano.»*
>
> *«Además, las organizaciones deberían monitorear actividades internas sospechosas, el uso inusual de herramientas legítimas, y alertas de viajes imposibles, con el fin de identificar comportamientos frecuentemente asociados a empleados falsos»,* agregó Sophos.