Se ha detectado una reciente campaña de malvertising que utiliza sitios falsos que simulan ser un portal de noticias legítimo de Windows para difundir un instalador malicioso de una herramienta de perfilado del sistema llamada CPU-Z.

> *«Este evento forma parte de una campaña de malvertising más extensa que apunta a otras utilidades como Notepad++, Citrix y VNC Viewer, como se evidencia en su infraestructura (nombres de dominio) y en las plantillas de camuflaje utilizadas para eludir la detección»*, señaló Jérôme Segura de Malwarebytes.

Aunque las campañas de malvertising suelen establecer sitios replicados que publicitan software ampliamente utilizado, la última actividad representa una variación en el hecho de que el sitio imita a WindowsReport[.]com.

El objetivo es engañar a usuarios desprevenidos que buscan CPU-Z en motores de búsqueda como Google al mostrar anuncios maliciosos que, al hacer clic, los redirigen al portal falso (workspace-app[.]online).

Simultáneamente, a los usuarios que no son el objetivo previsto de la campaña se les presenta un blog inofensivo con diferentes artículos, utilizando una técnica conocida como camuflaje.

El instalador MSI firmado que se encuentra en el sitio web fraudulento contiene un script malicioso de PowerShell, un cargador conocido como FakeBat (también conocido como EugenLoader), que sirve como canal para desplegar RedLine Stealer en el host comprometido.

> *«Es posible que el actor de amenazas haya optado por crear un sitio de señuelo que se asemeje a Windows Report porque muchas utilidades de software suelen descargarse desde tales portales en lugar de su página web oficial»*, observó Segura.

Esto está lejos de ser la primera vez que anuncios engañosos de Google para software popular resultan ser un vector de distribución de malware. La semana pasada, la firma de ciberseguridad eSentire reveló detalles de una campaña de Nitrogen actualizada que allana el camino para un ataque de ransomware BlackCat.

Otras dos campañas documentadas por la firma de ciberseguridad canadiense muestran que el método de descarga silenciosa para dirigir a los usuarios a sitios web dudosos se ha utilizado para propagar varias familias de malware como NetWire RAT, DarkGate y DanaBot en los últimos meses.

Este desarrollo se produce a medida que los actores de amenazas continúan confiando cada vez más en kits de phishing de adversarios en el medio (AiTM) como NakedPages, Strox y DadSec para eludir la autenticación de múltiples factores y apoderarse de cuentas específicas.

Para colmo, eSentire también llamó la atención sobre un nuevo método llamado el ataque Wiki-Slack, un ataque de dirección de usuario que tiene como objetivo llevar a las víctimas a un sitio web controlado por el atacante al desfigurar el final del primer párrafo de un artículo de Wikipedia y compartirlo en Slack.

Específicamente, explota una peculiaridad en Slack que *«maneja incorrectamente el espacio en blanco entre el primer y el segundo párrafo»* para generar automáticamente un enlace cuando la URL de Wikipedia se representa como una vista previa en la plataforma de mensajería empresarial.

Cabe señalar que un requisito previo clave para llevar a cabo este ataque es que la primera palabra del segundo párrafo en el artículo de Wikipedia debe ser un dominio de nivel superior (por ejemplo, en, at, com o net) y que los dos párrafos deben aparecer dentro de las primeras 100 palabras del artículo.

Con estas restricciones, una amenaza podría aprovechar este comportamiento para que la forma en que Slack formatea la vista previa de la página compartida apunte a un enlace

malicioso que, al hacer clic, lleve a la víctima a un sitio trampa.

> *«Si uno no cuenta con límites éticos, pueden ampliar la superficie de ataque del ataque Wiki-Slack editando páginas de Wikipedia de interés para desfigurarlas»,* comentó eSentire.