Se detectó a un grupo de hackers en desarrollo que usa Google Ads en una de sus campañas para distribuir varias cargas útiles posteriores al compromiso, incluyendo el ransomware Royal recientemente descubierto.

Microsoft, que detectó el método de entrega de malware actualizado a fines de octubre de 2022, está rastreando al grupo con el nombre DEV-0569.

> *«Los ataques DEV-0569 observados muestran un patrón de innovación continua, con la incorporación regular de nuevas técnicas de descubrimiento, evasión de defensa y varias cargas útiles posteriores al compromiso, junto con una mayor facilitación de ransomware»,* dijo el equipo de Microsoft Security Threat Intelligence.

Se sabe que el atacante confía en la publicidad maliciosa para dirigir a las víctimas desprevenidas a enlaces de descarga de malware que se hacen pasar por instaladores de software para aplicaciones legítimas como Adobe Flash Player, AnyDesk, LogMeIn, Microsoft Teams y Zoom.

El descargador de malware, una variedad conocida como BATLOADER, es un cuentagotas que funciona como un conducto para distribuir las cargas útiles de siguiente etapa. Se ha observado que comparte superposiciones con otro malware llamado ZLoader.

Un análisis reciente de BATLOADER realizado por eSentire y VMware destacó el sigilo y la persistencia del malware, además de su uso de envenenamiento por optimización de motores de búsqueda (SEO) para atraer a los usuarios a descargar el malware de sitios web comprometidos o dominios creados por atacantes.

Alternativamente, los enlaces de phishing se comparten por medio de correos electrónicos no deseados, páginas de foros falsas, comentarios de blogs e incluso formularios de contacto presentes en los sitios web de las organizaciones objetivo.

> *«DEV-0569 ha utilizado divsas cadenas de infección usando PowerShell y sceuencias de comandos por lotes que finalmente condujeron a la descarga de cargas de malware como ladrones de información o una herramienta legítima de administración remota utilizada para la persistencia en la red»*, dijo la compañía.

> *«La herramienta de administración también puede ser un punto de acceso para la puesta en escena y la propagación de ransomware».*

También se utiliza una herramienta conocida como NSudo para iniciar programas con privilegios elevados y debilitar las defensas agregando valores de registro que están diseñadas para deshabilitar las soluciones antivirus.

El uso de Google Ads para entregar BATLOADER selectivamente marca una diversificación de los vectores de distribución de DEV-0569, lo que le permite llegar a más objetivos y entregar cargas útiles de malware, dijo la compañía.

Posiciona aún más al grupo para servir como intermediario de acceso inicial para otras operaciones de ransomware, uniéndose a malware como Emotet, IceID y Qakbot.

> *«Debido a que el esquema de phishing de DEV-0569 abusa de los servicios legítimos, las organizaciones también pueden aprovechar las reglas de flujo de correo para capturar palabras clave sospechosas o revisar amplias excepciones, como las relacionadas con rangos de IP y listas permitidas a nivel de dominio»,* dijo Microsoft.