Los perpetradores responsables de los ataques de phishing BazaCall utilizando llamadas de retorno han sido vistos empleando Google Forms para conferir al esquema una apariencia de autenticidad.

Este método constituye un *«esfuerzo por elevar la percepción de autenticidad de los correos electrónicos maliciosos iniciales»,* según el informe presentado hoy por la firma de ciberseguridad Abnormal Security.

BazaCall (también conocido como BazarCall), inicialmente identificado en 2020, se refiere a una serie de ataques de phishing donde se envían mensajes de correo electrónico que simulan avisos legítimos de suscripción a los objetivos, instándoles a contactar a un servicio de soporte para impugnar o cancelar el plan, o enfrentar cargos que oscilan entre $50 y $500.

Mediante la inducción de una falsa urgencia, el atacante persuade al objetivo, a través de una llamada telefónica, para que le otorgue capacidades de acceso remoto mediante software de escritorio remoto y, finalmente, establecer persistencia en el host bajo el pretexto de ofrecer ayuda para cancelar la presunta suscripción.

Algunos de los servicios populares que se hacen pasar incluyen Netflix, Hulu, Disney+, Masterclass, McAfee, Norton y GeekSquad.

En la más reciente variante de ataque detectada por Abnormal Security, se utiliza un formulario creado con Google Forms como un canal para compartir detalles de la supuesta suscripción.

Es relevante señalar que el formulario tiene habilitada la opción de recibir respuestas, lo que envía una copia de la respuesta al respondiente por correo electrónico, permitiendo al atacante enviar una invitación para completar el formulario y recibir las respuestas.

> *«Ya que el atacante ha activado la opción de recibo de respuestas, el objetivo*

> *recibirá una copia del formulario completado, diseñado para parecer un comprobante de pago del software antivirus Norton»,* indicó el investigador de seguridad Mike Britton.

La elección de utilizar Google Forms también es astuta, ya que las respuestas se envían desde la dirección *«forms-receipts-noreply@google[.]com»*, un dominio confiable que, por ende, tiene una mayor probabilidad de eludir las puertas de enlace de correo electrónico seguro. Esto se evidenció en una reciente campaña de phishing con Google Forms descubierta por Cisco Talos el mes pasado.

> *«Además, los formularios de Google a menudo emplean URL generadas dinámicamente. La naturaleza en constante cambio de estas URL puede evadir las medidas de seguridad tradicionales basadas en análisis estático y detección de patrones, que dependen de identificar amenazas mediante patrones conocidos»,* explicó Britton.

Un Actor de Amenazas Dirige sus Ataques a Profesionales de Recursos Humanos Utilizando la Puerta Trasera More_eggs

La divulgación surge a medida que Proofpoint revela una nueva campaña de phishing que se centra en reclutadores a través de correos electrónicos directos que finalmente conducen a una puerta trasera de JavaScript conocida como More_eggs.

La empresa de seguridad empresarial atribuye esta ola de ataques a un *«actor de amenazas con habilidades avanzadas y motivación financiera»,* identificado como TA4557, que tiene antecedentes de abusar de servicios de mensajería legítimos y de ofrecer empleos ficticios por correo electrónico para, en última instancia, distribuir la puerta trasera More_eggs.

> *«En concreto, en la cadena de ataque que utiliza esta nueva técnica de correo electrónico directo, una vez que el destinatario responde al correo electrónico inicial, se ha observado que el actor responde con una URL que enlaza a un sitio web controlado por el actor, haciéndose pasar por el currículum de un candidato»*, explicó Proofpoint.

> *«Como alternativa, se ha observado que el actor responde con un archivo adjunto en formato PDF o Word que contiene instrucciones para visitar el falso sitio web del currículum.»*

More_eggs se ofrece como un servicio de malware y es utilizado por otros grupos ciberdelincuentes prominentes como el Grupo Cobalt (también conocido como Cobalt Gang), Evilnum y FIN6. A principios de este año, eSentire vinculó el malware a dos operadores ubicados en Montreal y Bucarest.