Iniciativas y Mecanismos Regulatorios Técnicos y Operativos para Combatir Estafas

Respuesta a la Consulta Pública

Presentada por el Sr. Sharad Agarwal y la Dra. Marie Vasek del Grupo de Investigación en Seguridad de la Información en *University College London (UCL)*, Reino Unido, y el Dr. Guillermo Suárez-Tangil de *IMDEA Networks*

May 4, 2024

Somos un colectivo de científicos, en el área de ciencias de la computación y las telecomunicaciones, especializados en el campo del cibercrimen. El Sr. Agarwal es un estudiante de doctorado en University College London (UCL), en el Reino Unido, bajo la supervisión de la Dra. Marie Vasek. Su investigación se centra en estudiar fraudes financieros en las redes, como estafas mediante SMS. La Dra. Vasek es Profesora Titular en el Departamento de Ciencias de la Computación en UCL. Su trabajo analiza el cibercrimen con un enfoque particular en estafas utilizando herramientas del área de ciencias económicas. El Dr. Suárez-Tangil es Profesor Titular en el Instituto IMDEA Networks en España. Tiene experiencia en seguridad de sistemas, análisis y detección de malware, y su investigación se centra en modelar amenazas emergentes en redes sociales y diseñar estrategias de mitigación efectivas. Esta evidencia que presentamos se basa en nuestra experiencia académica y los resultados derivados de nuestra investigación estudiando estafas telefónicas y mediante SMS. La investigación se lleva a cabo dentro del Grupo de Investigación en Seguridad de la Información en UCL y en IMDEA Networks.

Resumen

1. El fraude en el ecosistema móvil está aumentando continuamente, y la aparición de nuevas tecnologías ha facilitado que los estafadores atraigan a las víctimas mucho más fácilmente que antes.

2. Estimamos que las víctimas pierden al menos £2.3 millones (€2.7 millones) anualmente solo por las estafas de SMS "hola mamá y papá" en el Reino Unido, foco de nuestra investigación reciente.

3. El 23.8% de los nuevos dominios maliciosos registrados utilizados en el phishing/smishing tienen certificados TLS/SSL.

4. Establecer un umbral en el número de mensajes enviados por un CLI es una forma eficiente de detener las estafas de SMS.

5. Los criminales utilizan cajas SIM (*SIM boxes*) para enviar mensajes de SMS fraudulentos simultáneamente. Por lo tanto, la compra, venta o uso de cajas SIM debería ser regulada.

6. Solo el 5.1% de los números móviles utilizados para iniciar 306,757 llamadas fraudulentas eran válidos.

Suplantación de CLI para realizar llamadas fraudulentas (Responde Pregunta 1)

Nuestra investigación estudia llamadas fraudulenta por medio de sistemas comprometidos tanto en el territorio de España como en otros países [1]. Entre las 306,757 llamadas fraudulentas que analizamos, observamos 211,432 números de teléfono distintos. Sorprendentemente, solo 10,872 (5.14%) de estos números resultaron ser válidos, **aportando evidencia científica que socava la eficacia de bloquear números de teléfono no asignados**. Es destacable que una mera fracción de estas campañas, que comprenden aproximadamente 200 llamadas, intentaron alterar el identificador de llamadas (CLI) a números diferentes, una táctica conocida como *spoofing* indicativa de tácticas de fraude Wangiri.

Recomendaciones. Dado que solo el 5.1% de los números de teléfono resultaron ser válidos, es evidente que los ciberdelincuentes han estado utilizando números de teléfono no asignados. Por lo tanto, respaldamos la sugerencia de crear una base de datos de todos los números de teléfono no asignados para que los operadores móviles puedan monitorizar y bloquear todas las llamadas que provengan de ellos. Solo unas pocas campañas intentaron cambiar el identificador de llamadas a otro número de teléfono. *Por lo tanto, las medidas propuestas para la lista de bloqueo podrían tener algún impacto.*

Además, hemos observado casos en los que los estafadores alquilan números de teléfono virtuales para realizar llamadas salientes usando CLIs locales. *Por ello, a las medidas para bloquear las llamadas con origen internacional identificadas por un CLI del plan nacional de numeración, se les ha de acompañar de otras medidas regulatorias contra* **call centers** *en territorio nacional desde donde se operan frecuentemente llamadas fraudulentas.*

[1] Carrillo-Mondéjar, J., Jose Luis Martinez, and Guillermo Suarez-Tangil. "On how VoIP attacks foster the malicious call ecosystem." Computers & Security 119 (2022): 102758.

Nuevos dominios maliciosos registrados en mensajes de SMS o correos electrónicos (Responde a la Pregunta 5)

Nuestro trabajo se concentra específicamente en dominios maliciosos recién creados, especialmente aquellos que alojan URL utilizadas para phishing/SMiShing (phishing a través de mensajes de texto). Nuestra investigación ha identificado varias categorías de marcas suplantadas aquí, como bancos y empresas de mensajería.

Colaboramos con una empresa internacional de inteligencia de amenazas que nos proporcionó un suministro diario de datos de dominios maliciosos recién registrados como sospechosos de estar siendo utilizados en phishing por SMS y correo electrónico. Recolectamos datos entre el 5 de julio de 2023 y el 29 de febrero de 2024. Descubrimos que el 23.8% de estos dominios maliciosos recién registrados (N=11581) tienen certificados SSL/TLS, un protocolo criptográfico que cifra y autentica la comunicación web.[1]

Investigaciones previas han demostrado que los usuarios aún caen en ataques de phishing [2]. Los criminales utilizan diferentes estrategias para cambiar el nombre de dominio, como reemplazar caracteres, para dificultar la diferenciación entre el phishing y una URL legítima. Por ejemplo, correos.es, c0rreos.es, o corre0s.es, que son dificilmente distinguibles a simple vista en un mensaje de texto.

Existe una carrera armamentista entre los criminales y las operadoras o los sistemas de bloqueo. Los criminales continúan creando nuevos dominios para llevar a cabo estafas, y las empresas de eliminación trabajan para detectar y eliminar estos dominios. Servicios como los proveedores de alojamiento "a prueba de balas" (*bulletproof hosting*), amparados por países con legislaciones precarias, que no cumplen con los requerimientos internacionales, están disponibles para los criminales para alojar dominios maliciosos, lo que dificulta la eliminación.

Alternativamente, la página de advertencia de navegación segura de Google para dominios maliciosos es una forma efectiva de advertir a los usuarios, dado que la lista de bloqueo de Google marca un dominio. Sin embargo, estas listas de bloqueo sufren de falsos positivos, es decir, dominios no maliciosos que se agregan a las listas de bloqueo y generan desconfianza en las medidas, así como el dual, los falsos negativos, que generan sensación de falsa seguridad cuando ocurren. También hay un problema de oportunidad: después de que se elimina una página de phishing de un sitio web, es difícil saber cuándo es seguro que un usuario vuelva a visitar el sitio web. Google utiliza su motor de búsqueda para ayudar a realizar este trabajo, pero puede ser poco práctico para empresas diferentes. Otro problema es que Google lo hace en el lado del cliente: cada navegador que utiliza la navegación segura de Google para filtrar necesita descargar una copia reciente de la lista de filtros para bloquear las listas adecuadas. Esto puede ser costoso para los usuarios en dispositivos móviles.

Recomendaciones. El bloqueo de URL ha sido actualmente una contramedida efectiva para advertir o detener a los usuarios de acceder a dominios sospechosos.

[1] https://www.cloudflare.com/en-gb/learning/ssl/transport-layer-security-tls/

Recomendamos que los operadores móviles identifiquen las URL maliciosas de los SMS y bloqueen estos dominios en sus redes. Estas listas de bloqueo deberían ser compartidas con otros proveedores de servicios de internet (ISP) que operen en el país para hundir estos dominios, ya que los servicios como el alojamiento a prueba de balas retrasan las eliminaciones.

[2] Sijie Zhuo, Robert Biddle, Yun Sing Koh, Danielle Lottridge, and Giovanni Russello. 2023. SoK: Human-centered Phishing Susceptibility. ACM Trans. Priv. Secur. 26, 3, Article 24 (August 2023), 27 pages.

La interacción de las estafas de SMS no utiliza URL (Responde a la Pregunta 6).

Colaboramos con un operador móvil en el Reino Unido para investigar las estafas de interacción de SMS "hola mamá y papá" entre el 20 de junio de 2023 y el 15 de septiembre de 2023. En estas estafas, los estafadores envían un SMS a la víctima dirigiéndose a mamá o papá, haciéndose pasar por su hijo, y pidiendo ayuda financiera. La estafa de SMS "hola mamá y papá" comenzó en países de habla inglesa como el Reino Unido y Australia, y se ha extendido a países como Alemania, España e Italia. Recientemente, la policía en España realizó 65 arrestos, lo que demuestra la prevalencia de esta estafa en España.[2]

Aunque iniciada como una estafa de SMS, esta se sitúa en la intersección de los sectores de telecomunicaciones, tecnología y finanzas. Nuestro estudio ha concluido que que el 83.7% (2,850 de 3,402) de los mensajes de estafa originales pedían a las víctimas que respondieran en una plataforma de mensajería en línea. Interaccionamos proactivamente con estafadores sospechosos que se hacían pasar por posibles víctimas e interactuamos con ellos. Los estafadores intentaron appropiarse de £577,000 durante tres meses, estudio que nos permitió recopilar 582 cuentas únicas de mulas. En el contexto de una estafa online, una "mula" se refiere a una persona que actúa como intermediario sin saberlo, facilitando el traslado de dinero o bienes obtenidos de manera fraudulenta. Estas personas pueden ser utilizadas por estafadores para realizar transacciones ilegales sin dejar rastro directo hacia ellos. **La estafa de SMS "hola mamá y papá" es actualmente una de las campañas de estafa de SMS más extensas que no utiliza URL.**

Esta estafa es el ejemplo perfecto de cómo las estafas de SMS involucran a otros sectores: empresas de tecnología e instituciones financieras. La estafa de SMS "hola mamá y papá" utiliza dos números de teléfono móvil: uno para transmitir el mensaje inicial de estafa y el otro donde los estafadores piden a las víctimas que inicien la comunicación. Los estafadores abusan de las cajas SIM para transmitir el mensaje inicial de estafa a miles de posibles víctimas. El segundo número de teléfono móvil permite a los estafadores interactuar con las víctimas en un número de teléfono móvil que no sería detectado fácilmente por los operadores móviles para el abuso.

[2] https://www.theolivepress.es/spain-news/2024/02/07/spains-police-make-65-arrests-in-bust-of-cybercrime-gang-using-the-hi-mum-scam/

Recomendaciones. Recomendamos incentivar a los operadores móviles a colaborar con actores del sector tecnológico y financiero para combatir este tipo de estafas. Investigar las estafas de SMS es más complicado que los correos electrónicos debido a la falta de disponibilidad de metadatos. Los operadores móviles deberían colaborar con otros actores para incluir metadatos en el protocolo de SMS. Las cajas SIM requieren soporte GSM, el cual debería estar deshabilitado por defecto, y se deberían aplicar controles por parte de los operadores de telefonía para habilitarlo en alguno de los terminales operados por sus clientes. **Este elemento fácilmente imponible desde el punto de vista regulador puede tener un gran impacto a la hora de mitigar fraude en sistemas de mensajería.** El uso de cajas SIM debería estar regulado, y las fuerzas del orden deberían trabajar con los operadores móviles para detectarlas y confiscarlas de manera proactiva. Inspeccionar a fondo los SMS podría ayudar a identificar y bloquear los números móviles de los estafadores. Sin embargo, esto plantearía preocupaciones sobre la privacidad, y los estafadores podrían abusar de esto con ataques adversarios.

[3] Sharad Agarwal, Emma Harvey, Enrico Mariconti, Guillermo Suarez-Tangil, and Marie Vasek. "Hey mum, I dropped my phone down the toilet": Investigating Hi Mum and Dad SMS Scams in the United Kingdom. (Under Submission).

Conclusión

Apreciamos la oportunidad de contribuir a la consulta pública sobre iniciativas y mecanismos regulatorios, técnicas y operativas para combatir estafas comerciales y robo de identidad a través de llamadas telefónicas fraudulentas y mensajes de texto fraudulentos. Abordamos las amenazas planteadas por la suplantación del CLI para iniciar llamadas fraudulentas, los dominios maliciosos recién registrados para realizar phishing y un tipo relativamente nuevo de estafa de interacción de SMS sin URL. Nuestra respuesta está respaldada por nuestra investigación académica realizada en UCL y el Instituto IMDEA Networks. Es imperativo que tanto los interesados públicos como privados tomen nota de estas recomendaciones para proteger a individuos y organizaciones de caer víctimas de estafas de SMS y mejorar la postura de ciberseguridad en el ecosistema de SMS.