Observatorio de Derechos Digitales

Nueva ola de ataques de phishing en Ecuador

Alerta No. 2
Noviembre 2023

¿Qué es lo nuevo? Ecuador atraviesa una ola de ataques de phishing de los cuales no se tiene registros. Los atacantes están recurriendo a técnicas nunca antes vistas en el país para evitar ser detectados, dejando expuestas a una gran cantidad de personas a ataque de los cuales no habrían sido víctimas de no ser por esta nueva modalidad.

¿Por qué es importante? Además de víctimas en el sector privado, se ha confirmado que esta ola de ataques afectó a importantes instituciones públicas del país, quedando clara la vulnerabilidad de sistemas y dispositivos que podrían albergar información sensible e incluso, en algunos casos, reservada.

¿Qué debe hacerse? Es necesario profundizar en las motivaciones detrás de los ataques de phishing, lo que permitirá a las autoridades y las organizaciones desarrollar estrategias de prevención y respuesta más precisas. Al comprender mejor el contexto detrás de estos ataques, se pueden tomar medidas más efectivas para proteger a las víctimas y evitar la expansión de posibles ataques.

I. ¿Qué es el phishing?

El phishing es un tipo de ataque digital en el que un adversario envía un correo electrónico intentando engañar al destinatario para que abra un archivo adjunto o haga clic en un enlace. A veces, el objetivo es engañar a las personas para que introduzcan sus contraseñas en sitios web falsos que se ven exactamente como los reales. En otros casos, el objetivo es infectar al destinatario con algún tipo de malware.

El riesgo más evidente es la pérdida de datos personales. Los ataques resultan en la exposición de información personal, financiera y comercial muy delicada. Esto puede dar lugar a robo de identidad, fraude financiero y daño a la reputación de las personas y organizaciones. El costo financiero y, en el caso de las empresas, el impacto en la continuidad del negocio, podría ser devastador.

La información "pescada" se utiliza a menudo por los atacantes para asumir la identidad de la víctima y cometer fraudes financieros y otros delitos. Utilizan la información personal robada para abrir cuentas bancarias, solicitar tarjetas de crédito, obtener préstamos y realizar actividades fraudulentas en nombre de la víctima. El proceso de recuperación del robo de identidad puede ser costoso, agotador y llevar años.

Durante algún tiempo, este tipo de correos electrónicos ha sido bastante fácil de reconocer, excepto cuando se crean específicamente para un persona. Pero ahora, Ecuador está viviendo una ola de correos electrónicos en los que el atacante está utilizando nuevas técnicas para evitar ser detectado. Debido a esto, personas que normalmente no estarían en riesgo están siendo infectadas, de una manera que puede llevar a una gran difusión de estos correos electrónicos, y también al robo o la filtración de cualquier información a la que las víctimas tengan acceso. Del mismo modo, organizaciones pueden quedar expuestas a la infección por ransomware, donde su contenido digital está cifrado y es retenido como un rehén, a la espera del pago de un rescate.

El phishing es un tipo de ataque digital en el que un adversario envía un correo electrónico intentando engañar al destinatario para que abra un archivo adjunto o haga clic en un enlace

El resultado de ataques de phishing en Ecuador no es un riesgo abstracto; es una amenaza tangible que puede tener consecuencias graves para las personas y organizaciones. La información financiera expuesta a través de ataques de phishing es usada para llevar a cabo fraudes financieros. Esto puede incluir la realización de compras no autorizadas, la transferencia de fondos a cuentas controladas por los atacantes y la manipulación de registros financieros. Consecuentemente, las víctimas de fraude financiero a menudo enfrentan pérdidas económicas y reputacionales significativas

La amenaza de ataques de phishing ha evolucionado a un nivel alarmante, superando las barreras de seguridad que una vez consideramos sólidas. El phishing ha experimentado una mutación en Ecuador que merece nuestra atención, desafiando la

detección de los responsables y aumentando su sofisticación respecto de los métodos de ejecución de phishing. Esto debería ser motivo de preocupación para todos los ciudadanos y ciudadanas, así como empresas y organizaciones.

En esta alerta, detallaremos esta amenaza y describiremos algunas acciones que las personas y las organizaciones pueden tomar para protegerse contra esta nueva variante de ataque.

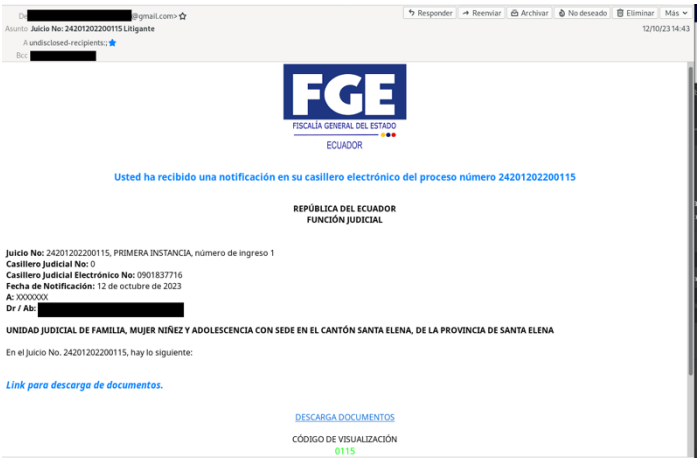
II. La nueva ola de phishing

Tradicionalmente, las personas que envían correos electrónicos de phishing utilizan servidores de correo que no tienen buena reputación. A menudo, las firmas y otros mecanismos de seguridad en los correos electrónicos están ausentes y el remitente suele ser falso, lo que significa que el verdadero remitente es una dirección de correo electrónico completamente diferente a la que dicen los encabezados del correo electrónico.

Por todas estas razones, es relativamente fácil reconocer este tipo de correos electrónicos. A menudo, el cuerpo del correo electrónico contiene errores ortográficos, formatos extraños y otras características que también destacan. Y, finalmente, los enlaces o archivos adjuntos son obviamente maliciosos, lo que significa que software antivirus o de protección de terminales puede reconocer y poner en cuarentena automáticamente estos correos electrónicos.

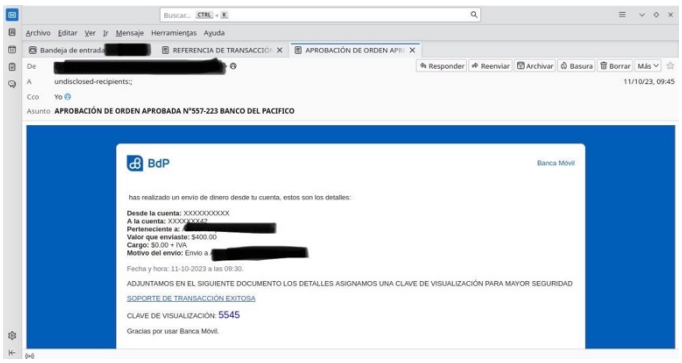
La nueva campaña de phishing cambia todo eso. Nos dimos cuenta de ello por primera vez la semana del 9 de octubre de 2023, cuando varios de los integrantes de una organización recibieron diferentes correos electrónicos que, en la superficie, parecían independientes, pero después de investigar más, compartían rasgos comunes.

Uno decía ser del «Banco del Pacífico», dando apariencia de la confirmación de un



pago. Dos dijeron ser de «Alem», empresa de provisión de equipamiento e insumos médicos, actuando como procesadores de pagos de «Produbanco», y afirmando que habían aprobado un pago a nombre del destinatario. El último afirmó ser de la «Fiscalía General del Estado», informando que se habían agregado nuevos documentos a un proceso.

Cada uno de estos correos electrónicos parecía utilizar un formato y estilo copiados exactamente de correos electrónicos reales del mismo tiempo. La única diferencia fue un enlace agregado al final del correo



electrónico y un código de cuatro dígitos, que precedía al enlace.

Dos de los correos electrónicos provinieron de direcciones del dominio de «Gmail», mientras que el resto se enviaron desde direcciones de correo electrónico que utilizaban una cuenta corporativa de «Gmail», con un dominio personalizado. Era un enlace de descarga de un archivo almacenado en «Google Docs». El archivo descargado compartía el asunto del correo electrónico, con la terminación «tar». Sin embargo, el formato de archivo dentro los archivos en realidad no fueron producidos por el programa *«tar»*; en su lugar, utilizó *«rar»*, en su forma cifrada. Probablemente, la razón para esto es evitar la detección mediante el análisis de virus que Google Docs realiza automáticamente en todo el contenido subido.

Al verificar los encabezados de los correos electrónicos, queda claro que estos correos electrónicos en realidad fueron enviados por la infraestructura de Gmail. No se ha falsificado, ni manipulado de ninguna forma, los encabezados de los correos electrónicos. Lo que delató a estos correos electrónicos fue el hecho de que el receptor estaba en el campo "CCO", no en el campo "Para". Esto da muestras de un correo electrónico que ha sido enviado a muchos receptores, pero de una manera que hace imposible que el receptor vea a los demás destinatarios.

Después de descomprimir las cuatro muestras de malware y proporcionar el código de cuatro dígitos como contraseña de descifrado, cuatro diferentes programas maliciosos de Windows pudieron ser identificados.

Para obtener más información sobre ellos, el lector puede consultar *VirusTotal*. Se pueden encontrar muestras específicas en:
https://www.virustotal.com/gui/file/4e16ac5633744eec5dd1b9fc3a54fdd570bd89fe8070d2063110e468e744a1bd

https://www.virustotal.com/gui/file/aed88bac878b5ce29f79b2e566d3f6be0c0a7c4f7cacdc4a15b342d21ed4848f,

https://www.virustotal.com/gui/file/f3f89a6fa4ff02f3a195915a782087a19c5da969b14d82715aec0f0f0dd659aa/detection y
https://www.virustotal.com/gui/file/e051717e9b2d068631b4c1eb34c28564681a05d981ad442fed3381accd775869/detection

Lo que delató a estos correos electrónicos fue el hecho de que el receptor estaba en el campo "CCO", no en el campo "Para". Esto da muestras de un correo electrónico que ha sido enviado a muchos receptores, pero de una manera que hace imposible que el receptor vea a los demás destinatarios.

Tres de estas muestras parecen ser parte de la familia *Remcos*, que es una herramienta comercial de acceso remoto: una puerta trasera que puede dar acceso completo al sistema de la víctima. La muestra final es una variante de un tipo de malware que se clasifica como *Trojan Downloader*, es decir, que sirve para descargar otro malware. Dado que las otras muestras se basan en *Remcos*, es razonable suponer que

este programa descargaría malware de la misma familia.

Después de la notificación responsable a las organizaciones víctimas y a los propietarios de las cuentas en cuestión, queda claro que la infección inicial se produjo utilizando los mismos mecanismos descritos en este artículo. Lo que eso significa es que el malware en cuestión intentará determinar si la víctima tiene Gmail abierto y luego lo usará para enviar una nueva ola de correos electrónicos de phishing. Esto también significa que la afectación incluye, no sólo las cuentas de Gmail en cuestión, sino también el dispositivo de la víctima.

Los motivos detrás de estos ataques son aún más oscuros. ¿Qué buscan estos atacantes? ¿Se trata simplemente de la obtención de información confidencial, exposición de información delicada y la posible extorsión a través de ransomware, o estamos frente a algo más perverso? La respuesta no es clara, y eso es precisamente lo que hace que esta situación sea tan inquietante.

No queda claro cuáles son los objetivos de estas infecciones, más allá de enviar más oleadas de correos electrónicos de phishing. Varios de los correos electrónicos de los destinatarios no eran públicamente conocidos y normalmente no reciben spam. Se puede especular que estos correos electrónicos se encontraron en bases de datos relacionadas con los dispositivos de las víctimas. En el caso del correo electrónico que pretende provenir de la Fiscalía, el destinatario ha participado en un proceso judicial con esa dirección de correo electrónico registrada.

Después de una investigación de inteligencia de fuentes abiertas (OSINT), los datos muestran que la dirección de correo electrónico que envió la comunicación que afirma ser de la Fiscalía pertenece a una persona que trabaja como desarrollador en la FGE (Fiscalía General del Estado) y consta en la lista de responsables de las bases de datos en esa institución. Si esto es correcto, significa que los atacantes potencialmente podrían tener acceso a contenidos reservados de la Fiscalía. Es urgente que se investigue este incumplimiento y que el hecho sea aclarado. Este tipo de ataques es una grave violación contra el Estado de Derecho y, en general, contra los derechos fundamentales de la población.

La gran pregunta que queda abierta es si el objetivo de esta ola de ataques es extraer información y venderla, o si es un preludio para más ataques, como ransomware o la eliminación de sistemas.

III. Medidas básicas de protección

Para protegerse, todas las recomendaciones de seguridad habituales son útiles. Sin embargo, en este caso específico, lo más importante para las personas que reciben este tipo de correo electrónico es no hacer clic en enlaces o adjuntos, jamás.

Para verificar su autenticidad, puede pasar el cursor sobre el enlace y ver si conduce a "docs.google.com". Si además tiene un código de verificación de 4 dígitos, el correo es fraudulento.

En un sentido más general, lea el correo electrónico cuidadosamente antes de actuar. Si la información que contiene no coincide con sus expectativas, es una clara señal de que debería dudar. En caso de duda, opte siempre por la vía más segura.

Finalmente, la autenticación de doble factor o multifactor es una protección importante contra muchos tipos de phishing.

Si un atacante logra robar su contraseña de «Gmail» usando el ataque descrito en este documento, el multifactor de autenticación aún lo protegería contra la afectación.

Para las empresas que protegen las redes, y especialmente los servidores de correo electrónico, es importante mantener todas las máquinas actualizadas. Si utilizan filtrado perimetral, busquen la cadena de caracteres "PIN DE VISUALIZACIÓN" o "CLAVE DE VISUALIZACIÓN" combinada con un enlace a algo que comience con "https://docs.google.com".

Fuera de estas sugerencias, las referencias anteriores demuestran que no todas las herramientas antivirus reconocen el malware en cuestión. Podrían considerar cambiar a una alternativa que tenga mejores firmas para reconocer malware.

Por último, sigan las recomendaciones estándar sobre segmentación, privilegios mínimos, confianza cero y, si es posible, consideren trasladar su empresa a alternativas de software libre. Si eso no es posible, consideren habilitar Microsoft Defender y el Firewall integrado de Microsoft Windows en todas las máquinas de su empresa.

El análisis del perfil de las víctimas de los ataques de phishing en Ecuador es esencial para comprender las posibles motivaciones detrás de estos ataques. Al examinar a las víctimas y sus relaciones con el contexto político, económico y social de Ecuador, se pueden obtener conocimientos valiosos.

Por ejemplo: (a) Identificar el sector y la actividad de las organizaciones o individuos afectados puede revelar posibles objetivos estratégicos. Si las víctimas están relacionadas con sectores críticos como la energía, la infraestructura o la defensa, esto podría indicar motivaciones geopolíticas; (b) analizar si los ataques de phishing se centran en áreas geográficas o sectores específicos en Ecuador.

Además, si el objetivo es la extorsión a través de ransomware u otros medios, se deben investigar los patrones y demandas de los atacantes para desarrollar estrategias de respuesta y prevención.

Es valioso que para este análisis se ejecuten algunas acciones, por ejemplo: a) Examinar detenidamente los métodos de extorsión utilizados por los atacantes. Esto incluye el análisis de las demandas específicas, como el monto del rescate y la moneda requerida para el pago; y, b) Examinar si los ataques de extorsión están relacionados entre sí o si múltiples grupos de atacantes están operando en Ecuador.

Ecuador enfrenta una grave ola de ataques sofisticados. La mayoría de los sistemas de protección normales no funcionan bien contra este ataque y la colaboración y el compromiso de los usuarios finales son más importantes que nunca para proteger tanto a individuos como a empresas

En resumen, Ecuador enfrenta una grave ola de ataques sofisticados. La mayoría de los sistemas de protección normales no funcionan bien contra este ataque y la colaboración y el compromiso de los usuarios finales son más importantes que nunca para proteger tanto a individuos como a empresas.

El posible ataque contra la FGE parece extremadamente grave y debe ser investigado con urgencia.

Los ataques de phishing no sólo son amenazas en lo digital, sino que también traen consigo asuntos legales y regulatorios.

Las organizaciones afectadas deben cumplir con las leyes de privacidad y notificar a las autoridades y a las partes afectadas. La carga financiera y reputacional de estas violaciones puede ser devastadora.

Este es un llamado a la acción. La seguridad digital es responsabilidad de todos, desde el ciudadano común hasta las empresas y el gobierno. La colaboración entre las autoridades, los expertos en seguridad digital y las organizaciones afectadas es esencial.

Tomen sus propias medidas para protegerse.

Con el apoyo de:

Centro de Autonomía Digital

Orden Conflicto Violencia
Programa de Investigación