**Phishing: No se Requiere Licencia**

En el mundo del delito cibernético, el phishing sigue siendo una de las herramientas más consistentes y exitosas para obtener acceso a una computadora o red. Su rango de uso es amplio. Lo emplean los grupos de delitos cibernéticos más sofisticados y organizados (incluidos los grupos de delitos cibernéticos patrocinados por el Estado) hasta los piratas informáticos más poco sofisticados y desconectados, los solitarios que viven en los sótanos de sus padres. El phishing ha sido un paso clave en algunos de los mayores atracos en la historia del cibercrimen, en particular el robo de 81 millones de dólares estadounidenses del Banco Central de Bangladesh. Es una herramienta estándar para obtener acceso a información de tarjetas de crédito y débito, así como a una gran cantidad de información personal que puede venderse fácilmente en los mercados negros de la web oscura.

**Qué es Phishing**

Phishing, en su definición más simple, es el uso de un correo electrónico para atraer o convencer al destinatario de que haga clic en un archivo adjunto o siga un conjunto de instrucciones en una página web a la que se accede a través de una URL de destino. En cualquier caso, el archivo adjunto o la página web, el destinatario es susceptible de intrusión en su computadora o sistema de red, ya sea que ese sistema sea la computadora de su hogar, que podría contener más contraseñas y más acceso para los piratas informáticos, o su red de trabajo, que abre su red profesional a los piratas informáticos. El phishing es una de las herramientas más antiguas y exitosas utilizadas por los piratas informáticos.

Un ejemplo básico y común de phishing es el correo electrónico falso de PayPal™. Su información de pago no está actualizada. ¿Podría ir a la siguiente URL y actualizar su información de pago para continuar usando PayPal? O podría ser una alerta de amenaza. Su cuenta PayPal podría estar comprometida. hubo una sospecha, intento de inicio de sesión desde Indonesia. ¿Eras tú? Este imperativo emocional se utiliza con frecuencia. Quieren asustarte haciéndote pensar que ya has sido pirateado y que podrías perder dinero. Por supuesto, el sitio web al que te diriges no es el sitio web oficial de PayPal y te engañaron para que le dieras a los estafadores la información para iniciar sesión en tu cuenta PayPal. Puede suceder rápidamente (bum, bum, bum) como si estallaran petardos. ¿Qué tan difícil hubiera sido frustrarlo? Pónte en contacto con PayPal o dirígite a su sitio web real e inicia sesión para verificar que tus datos de pago sean incorrectos. Para ser justos con las víctimas, los correos electrónicos pueden tener un aspecto bastante oficial: logotipo correcto, información personal correcta y otros indicadores de que puedes confiar en el mensaje y, por lo tanto, en el archivo adjunto o URL.

**La Variedad del Phishing**

Hay estafas de phishing para todo tipo de grupos demográficos diferentes: personas mayores, jóvenes, jubilados y empresas exitosas. Los datos agregados año tras año sugieren que nadie es inmune y las estafas de phishing aumentan cada año. El cibercrimen está tan extendido que incluso el Departamento de Seguridad Nacional está involucrado en Estados Unidos. No es el mismo truco de siempre una y otra vez. El phishing se encuentra en un constante estado de evolución, adaptación y crecimiento en sofismas. Los practicantes más diligentes del phishing se toman su tiempo para investigar al sujeto al que quieren dirigirse. Esto podría incluir numerosas horas de seguimiento y vigilancia de sus plataformas de redes sociales para obtener una visión más profunda del objetivo. Esta información se puede utilizar para personalizar el correo electrónico de alguna manera, para lograr una familiaridad íntima, lo que elimina las defensas del destinatario y lo hace sentir seguro al hacer clic en el enlace o archivo adjunto. Son delincuentes, pero hacen la debida diligencia.

Los expertos en seguridad cibernética ahora capacitan y asesoran a las personas sobre lo que publican en las redes sociales. El uso de las redes sociales fue una parte integral del ataque al Banco Central de Bangladesh. Sus perfiles de redes sociales: Facebook, LinkedIn, Twitter (X), e Instagram: permita que los ciberdelincuentes lo comprendan y se presenten como familiares. La regla número uno: no publique ningún dato relacionado con el trabajo en sus plataformas de redes sociales.

**Évolution Criminal**

A medida que la tecnología evoluciona, también lo hace el ciberdelito. La industria de la publicidad está comenzando a definir significativamente la publicidad digital delimitada por tiempo y geografía en dispositivos móviles. Esto se hace mediante la recopilación de ID de dispositivos y la ubicación geográfica del usuario, todos los cuales son productos de datos comerciales recopilados y vendidos ahora en el mundo empresarial legítimo. Por ejemplo, estás caminando hacia el andén del metro después del trabajo. Es un miércoles por la tarde, talvez las 5:15 p.m., y recibes un anuncio en tu teléfono sobre un café en tu cafetería favorita, la cual, no es casualidad, pasas por delante de camino a la parada del metro y el anuncio es para un café que te encanta, lo cual ellos saben porque lo has comprado numerosas veces en el pasado usando (sí, lo tienes) tu teléfono como instrumento de pago electrónico, y toda esta sinergia fabricada se reunió y estratégicamente implementado para producir un anuncio efectivo en su teléfono, efectivo porque compró el café. Ahora, imaginemos esta misma técnica publicitaria de vanguardia empleada en el phishing. ¿Ves a dónde va esto?

**Phishing Comercial**

Si el operador solitario en el sótano de su madre, o los pequeños grupos de ciberdelincuentes competentes no fueran suficientes, ahora estamos en la era del phishing comercial, una coincidencia casi uno a uno con el comercio real de la pesca oceánica. El operador del préstamo sería como el viejo cubano de El viejo y el mar de Ernest Hemingway, y las operaciones comerciales de phishing son como barcos de pesca de altura chinos o portugueses con enormes redes. Actualmente hay proveedores que venden servicios de phishing como servicio (PaaS).

En el segundo trimestre de 2023, los expertos en ciberseguridad se dieron cuenta de un producto llamado Greatness. Cisco™ informó lo siguiente en un blog de seguridad publicado el 10 de mayo de 2023.

“Una oferta de phishing como servicio (PaaS) no denunciada anteriormente llamada Greatness se ha utilizado en varias campañas de phishing desde al menos mediados de 2022. Greatness incorpora características que se ven en algunas de las ofertas de PaaS más avanzadas, como la omisión de autenticación multifactor (MFA), el filtrado de IP y la integración con bots de Telegram. Greatness, por ahora, solo se centra en las páginas de phishing de Microsoft 365, proporcionando a sus afiliados un creador de archivos adjuntos y enlaces que crea páginas señuelo y de inicio de sesión altamente convincentes. Contiene características como tener la dirección de correo electrónico de la víctima precompletada y mostrar el logotipo de la empresa y la imagen de fondo correspondientes, extraídos de la página de inicio de sesión real de Microsoft 365 de la organización objetivo. Esto hace que Greatness sea especialmente adecuado para usuarios empresariales de phishing”.

Esta, sin duda, es la primera de muchas ofertas que se harán en el área de la pesca comercial.

Será casi imposible detener la venta de este tipo de software en la web oscura. Ha sido casi imposible detener la venta de casi todo lo demás en la web oscura.

**Procede con precaución**

Su defensa es su responsabilidad, ya sea un usuario individual de una computadora o un empleado de una entidad corporativa más grande. La principal defensa es el entrenamiento. La mayoría de las organizaciones ahora tendrán un departamento de seguridad que monitorea y se mantiene al tanto periódicamente de cuáles son las últimas estafas en línea y, como parte de su función dentro de la organización más grande, capacita al resto de los empleados. Esta formación debe estar actualizada. Constantemente se desarrollan nuevos métodos de ataque de phishing. Asegúrese de que todos sus empleados comprendan los conceptos básicos de la World Wide Web. Entrénelos para que nunca den su información a un sitio no seguro. La URL debe comenzar con https y debería poder ver un ícono de candado cerrado al lado de la URL. Esto puede parecer un poco excesivo porque no todos los sitios sin un certificado de seguridad son una estafa, pero más vale prevenir que lamentar, especialmente cuando se opera desde una computadora del trabajo y se pone en riesgo toda la red. Es muy importante que su organización establezca un programa de rotación de contraseñas y recuerde a los empleados los correos electrónicos. Los empleados deben realizar cursos de capacitación en línea regulares, que el equipo de documentación y capacitación debe desarrollar internamente o subcontratar a proveedores acreditados con un historial sólido. Nada protegerá mejor su red que una fuerza laboral capacitada y educada. Esta ha sido una práctica estándar en el sector financiero durante más de dos décadas, pero debe adoptarse en todas las industrias.

La otra cosa que puedes hacer para protegerte es invertir en tecnología y herramientas, especialmente si interactúas con el público en línea, y esto podría ser tan inocuo como absorber información. Asegúrate siempre de que sean humanos. El acceso de bot a su sistema es otro tipo de phishing pero al revés. En lugar de acceder a la estafa a través de un archivo adjunto o una URL, la estafa llega a usted en forma de bot, pero una vez que ese bot obtiene acceso a su sistema, puede causar el mismo daño que el phishing. Es un hecho conocido en el mundo de la seguridad cibernética que la autenticación multifactor (MFA) es un componente crítico para impedir el phishing y otros tipos de delitos en línea, pero no todos los productos MFA son iguales. Así como ahora sabe que plataformas como Greatness pueden eludir las herramientas MFA débiles, también debe saber que no todas las herramientas MFA son iguales. Algunas son huecas y unidimensionales. Otros, como hCaptcha™, son vanguardistas en el uso del aprendizaje automático (ML) y la inteligencia artificial (IA). Tienes que protegerte de forma inteligente y ¿qué mejor manera que la IA y el ML?