Caja de herramientas de ciberseguridad de la GCA: documento guía para las herramientas de «Protéjase contra el phishing y el malware»

GCA Cybersecurity Toolkit™ For Small Business

Más del 90 % de los ciberataques comienzan con un correo electrónico de phishing. Su propósito es engañar a los usuarios para que crean que se están comunicando con una entidad de confianza con intención de conseguir información confidencial o dinero.

Phishing es un término que suele asociarse a las comunicaciones fraudulentas por correo electrónico, SMS o teléfono. Existen muchos tipos de phishing. Estos son algunos de ellos:

- **Phishing**: no suele tener un objetivo definido. Consiste en enviar de forma masiva correos electrónicos que parecen proceder de organizaciones reputadas. Pueden estar relacionados con noticias recientes y asuntos fiscales o parecer que provienen de organizaciones conocidas, con la esperanza de que alguien responda.
- **Spear phishing**: este ataque tiene un objetivo más definido. El correo electrónico está diseñado de forma que parece que proviene de una persona u organización que la víctima conoce, lo que hace necesaria una investigación previa, normalmente, con un objetivo específico en mente.
- **Whaling o pesca de *peces gordos***: este ataque tiene un objetivo muy concreto, que suelen ser los altos directivos de una organización. Es muy posible que, antes de ejecutar el ataque, los criminales hayan dedicado meses a rastrear los movimientos y recopilar información. Tienen un objetivo muy específico en mente.

Una vez que el mensaje llega a la bandeja de entrada, el atacante espera que el destinatario haga clic en un enlace o abra el archivo adjunto, lo que facilitará sus acciones:

- **Malware**: término genérico que se utiliza para diferentes tipos de software maligno:
    - **Virus**: se propaga automáticamente a través de un huésped. Puede adjuntarse a un programa o archivo legítimo y activarse durante una ejecución posterior.
    - **Gusano**: se propaga automáticamente por sí mismo a través de las conexiones de red. Por ejemplo, podría estar oculto en un archivo adjunto y enviar mensajes a todos los contactos de la agenda de direcciones.
    - **Troyano**: no se propaga. Se hace pasar por un programa legítimo (por ejemplo, un protector de pantalla) mientras se dedica a ocasionar daños en segundo plano.

Los atacantes podrían crear una **puerta trasera** en el dispositivo (una ruta secreta para utilizarla más adelante), dañar los datos e instalar **spyware** (para espiar lo que hace y acceder a sus datos personales) o **ransomware** (para secuestrar sus datos y pedir rescate).

Los correos electrónicos de phishing NO son fáciles de detectar:

- Puede parecer que proceden de alguien a quien conoce.
- Pueden tener exactamente la misma dirección de alguien a quien conoce.
- Pueden imitar los logotipos y el formato de los correos electrónicos de organizaciones conocidas.
- Pueden hacer referencia a noticias recientes o a un trabajo que acaba de realizar.
- Es posible que el atacante haya contactado anteriormente con su organización o le haya investigado a través de Internet para personalizar el correo electrónico y que parezca legítimo.

Los atacantes harán todo lo posible para que el correo electrónico parezca genuino y atractivo. Son muy buenos en esto.

Las consecuencias son graves tanto para los particulares como para las empresas. Numerosos estudios demuestran que las pequeñas empresas corren un riesgo elevado ante este tipo de ataques. Más del 60 % de las pequeñas empresas pueden haber sufrido un ciberataque durante el pasado año iniciado a través del correo electrónico.

Software antivirus

Ayuda a protegerse de las infecciones buscando características asociadas a virus conocidos (lo que se conoce como *firmas*) y, si se identifican, bloquea el virus y limpia el archivo. Los atacantes desarrollan continuamente nuevas cepas para tratar de burlar los antivirus. Cuando aparecen nuevos virus, se tarda algún tiempo en identificar sus características y bloquearlos. Los ataques que utilizan nuevos virus para los que aún no se ha desarrollado ninguna cura se conocen como ataques de *día cero*.

El software antivirus también puede detectar comportamientos inusuales del operador (lo que se conoce como *heurística*). El antivirus aprende los patrones de comportamiento habituales y comienza a sospechar si se produce algún comportamiento fuera de lo normal (por ejemplo, se inicia sesión en un sistema en un momento del día que no es el habitual).

Es importante tener actualizado el antivirus. Continuamente se desarrollan nuevos virus.

- *Asegúrese de todos los equipos y dispositivos móviles cuenten con protección antivirus en tiempo real.*
- *Realice análisis periódicos en todos los sistemas.*

Filtrado de nombres de dominio (filtrado DNS)
Cuando se crean nuevos sitios web, se aplican unos términos y condiciones que garantizan que se utilizan con fines legítimos. Sin embargo, los delincuentes hacen caso omiso de dichos términos y condiciones. Resulta muy difícil identificar la verdadera intención de un sitio web hasta que está operativo.

- Se estima que, de los más de 200 000 dominios nuevos que se registran diariamente en todo el mundo, hasta un 70 % podría tener fines maliciosos.
    - https://unit42.paloaltonetworks.com/newly-registered-domains-malicious-abuse-by-bad-actors/

Muchas empresas especializadas en ciberseguridad monitorizan el uso que se hace de los sitios web junto con otra información para identificar aquellos que tienen un comportamiento sospechoso. Estas empresas recopilan información sobre las amenazas (TI) y, tras analizarla, la utilizan para confirmar este comportamiento delictivo. El filtrado de nombres de dominio utilizará esta información sobre amenazas (procedente de múltiples fuentes) para bloquear el acceso a sitios web malignos, lo que evitará los efectos que estos ataques pretenden.

- **Quad9** es un servicio de filtrado de DNS desarrollado por Global Cyber Alliance en colaboración con IBM y Packet Clearing House. Cuenta con 19 fuentes de información sobre amenazas diferentes y bloquea el acceso a los sitios web malignos conocidos prácticamente en tiempo real. Para ello, se niega a convertir y enrutar el tráfico a la dirección IP vinculada al nombre de dominio del sitio web que se introduce en el explorador. También puede bloquear direcciones IP que podrían configurarse para que los dispositivos o equipos de IoT se conecten de forma automática (sin su conocimiento).

El filtrado de nombres de dominio solo puede bloquear los sitios web tras sobrepasar un umbral de actividad maligna.

DNS: sistema de nombres de dominio

- El sistema de nombres de dominio (DNS, por sus siglas en inglés) es el equivalente en Internet a una guía telefónica.
- Cada sitio web tiene un nombre o un dominio que puede especificarse en un formato legible (por ejemplo, globalcyberalliance.org) y que los servidores de nombres de dominio transforman en una serie única de números (la *dirección IP*; por ejemplo, 192.124.249.5) que los equipos son capaces de interpretar.
- Los registradores de nombres de dominio registran los nuevos dominios y sitios web que se crean, lo que permite asignarles una dirección IP y registrarla (GoDaddy sería un ejemplo de un registrador de nombres de dominio).

Los registradores tienen que asegurarse de que el nombre de dominio y la dirección IP de cada sitio web son únicos. Muchos estafadores tratan de utilizar nombres de dominio de sitios web similares para engañar a sus víctimas y hacerles pensar que se están conectando a un sitio legítimo. Estos sitios pueden tener un nombre parecido al nombre real del sitio web, pero una inspección más detallada revelaría algunas diferencias (por ejemplo, el uso de *rn* en lugar de *m* en la dirección).

Bloqueadores de anuncios

Algunos anuncios o mensajes que aparecen durante la navegación son útiles, pero hay muchos que no lo son o contienen código maligno. Para evitar que aparezcan anuncios en las páginas web mientras navegamos, se puede utilizar un bloqueador de anuncios. Constituyen una línea de defensa adicional contra los ataques.

Utilice las herramientas de «Protéjase contra el phishing y el malware» para mejorar sus defensas contra estos tipos de ataques.

https://gcatoolkit.org/es/pequenas-empresas/protejase-contra-el-phishing-y-el-malware/