Powered by GLESEC

CYBERSECURITY NEWS CUSTOM REPORT

Generated on 03/24/2020 by Luis Araúz

El coronavirus también contagia el ciberespacio

03/15/2020 18:20

Sophos descubre una campaña de spam aprovechando la alarma social

Los laboratorios SophosLabs han descubierto un **nuevo ataque de spam** activo en Italia r**ealizado mediante emails** que incluyen un documento que se ejecuta automáticamente y que contiene el malware Trickbot. Este ciberataque aprovecha el miedo al coronavirus y ofrece un documento en el que los usuarios pueden hacer clic para, supuestamente, conocer una lista de precauciones a tomar para evitar la infección. Desafortunadamente, el documento es un arma de ataque.

Según SophosLabs, el uso del **COVID-19 en mensajes de spam** puede ser nuevo, pero los mecanismos usados para enviar este tipo de mensajes son similares o idénticos a los utilizados en campañas de Trickbot, un troyano que han estado activo durante al menos los últimos 6 meses. Estos mecanismos incluyen "bots" de spam para enviar los mensajes, un documento adjunto cifrado y un software que instala el **malware en el ordenador** – dropper – utilizando el lenguaje de programación JavaScript.

"Los **cibercriminales** que están detrás de Trickbot son, probablemente, atacantes especializados que aprovechan la preocupación de turno para incitar a la gente asustada a hacer clic. Si bien el ataque está presente en Italia por ahora, cabría esperar ataques similares en otros países donde el **temor a los brotes de COVID-19 es alto**. La mejor opción para evitar este tipo de ciberataques es deshabilitar los macros (una serie de comandos para automatizar tareas), ser especialmente cautelosos con dónde se hace clic y borrar los emails sospechosos o que precedan de fuentes inesperadas", explica Chester Wisniewski, principal científico investigador de Sophos. "Siempre que hay un tema de interés público como el coronavirus o los incendios en Australia, vemos como los **ciberdelincuentes** tratan de convertir nuestra preocupación en una oportunidad. Debemos permanecer alerta y desconfiar de todas las comunicaciones recibidas en **periodos de crisis y acudir sólo a las autoridades** de la sanidad pública para obtener información y consejo".

A continuación, incluimos algunos **consejos** en caso de que esta estafa diera el salto del país vecino al nuestro:

· **No te dejes presionar para hacer clic en un enlace**. Lo más importante es que no sigas un consejo que no pediste y que no esperabas. Si realmente buscas consejo e información sobre el coronavirus, haz tu propia investigación y elije qué fuentes utilizar.

· **No te dejes engañar por el nombre del remitente**. Por ejemplo, esta estafa puede ser recibida en nombre de la "Organización Mundial de la Salud", pero en realidad el remitente puede poner el nombre que quiera utilizando el campo "De: …"

· **Pon especial atención en los errores ortográficos y gramaticales**. No todos los ladrones los cometen, pero muchos sí. Tomate un tiempo extra para revisar los mensajes recibido en busca de señales que indiquen que pueden ser fraudulentos. Ya es bastante malo ser estafado como para descubrir que podrías haber descubierto el fraude por adelantado.

· **Comprueba la URL** antes de teclearla o hacer clic en un enlace. Si el sitio web al que estás siendo redirigido no tiene buena pinta, mantente alejado.

· Nunca facilites datos que un sitio web no debería pedir. No hay razón para que una **página web de divulgación sobre salud** te pida tu **dirección de correo electrónico**, y mucho menos tu contraseña. Si te surgen dudas, no des información.

· Si te das cuenta de que acabas de revelar tu contraseña a los impostores, cámbiala en cuanto puedas. Los ladrones que están detrás de **sitios de phishing** suelen probar las contraseñas robadas inmediatamente (de hecho, es un proceso que puede hacerse de forma automática), así que cuanto antes reacciones, más probabilidades tendrás de vencerles.

· Nunca uses la misma contraseña para más de una cuenta. Una vez que **los ciberdelincuentes tienen una contraseña**, suelen usarla para intentar acceder a todos los sitios en los que el usuario puede tener una cuenta para probar suerte.

· Activa la autenticación de dos factores (2FA) si es posible. Esos códigos de seis dígitos que recibes en tu teléfono o que generas a través de una aplicación son un pequeño inconveniente para el usuario, pero suelen ser una gran barrera para los ciberatacantes, así no les es suficiente con saber tu contraseña.

· Aprovecha las formaciones disponibles para tener nociones de ciberseguridad. Productos como Sophos Phish Threat simulan ataques de phishing para empleados pero de una forma segura, mostrando los trucos que utilizan los ciberdelincuentes pero sin que se produzcan daños reales si alguien cae en la trampa. Sophos también ofrece un **kit de herramientas anti-phising** gratuito que incluye posters, ejemplos de **email de phishing**, consejos básicos para detectar un ataque de phishing, etc.

Incremento del riesgo cibernético por el coronavirus

03/23/2020 18:20

Columna de Patricia Villalva, Directora General de Cybnus.

- **El coronavirus nos ha demostrado que situaciones dramáticas con gravísimas repercusiones económicas pueden desencadenarse a velocidad vertiginosa a escala mundial.**

En su afán de reducir al mínimo posible la pérdida de beneficios derivada de la parada de la actividad, resulta sorprendente como la mayor parte de las empresas han sido capaces, de un día para otro, de enviar a sus empleados a trabajar desde casa, pese a que, hasta la fecha, según datos del último informe de Eurostat, solo el 3% de los españoles trabajaba en remoto. Ello se traduce en que las empresas no estaban preparadas para que sus empleados trabajaran a distancia, y por tanto no cuentan con las medidas mínimas de ciberseguridad necesaria, por lo que, en estas circunstancias, se encuentran en alto riesgo de sufrir un ataque cibernético que paralice su actividad.

En la mayoría de los casos, los empleados, que se encuentran fuera del firewall corporativo, se conectan a los servidores de datos de la empresa desde sus ordenadores personales, los cuales probablemente tendrán instalados sistemas operativos obsoletos, no tendrán aplicados los parches de seguridad que recomiendan los fabricantes e incluso no contarán con antivirus ni firewall. Es común, asimismo, que los usuarios domésticos no cambien las contraseñas de los routers que incorporan por defecto, lo cual les convierten en fácilmente vulnerables

Los ciberdelincuentes no se quedan parados en situaciones de crisis. Muy al contrario, las aprovechan para sacar el máximo rédito posible. Es por ello que, durante el período de

confinamiento en que nos encontramos, se espera un notable incremento de los ataques cibernéticos que, sumado a la reducción en la productividad de las empresas, aumentará el caos económico mundial.

Desde CYBNUS, expertos en ciberaseguramiento, realizamos las siguientes recomendaciones básicas para minimizar en la medida de lo posible las consecuencias de los ataques:

- Dotar a los empleados de equipos informáticos gestionados por la empresa.
- Cambiar las contraseñas de acceso de los routers.
- Instalar programas antivirus.
- Instalar programas firewall.
- Aplicar los parches de seguridad de los fabricantes.
- Realizar frecuentes copias de seguridad.
- Para evitar problemas de suplantación de personalidad y secuestro de datos, prestar mucha atención antes de abrir un correo electrónico, comprobar detalladamente la dirección del

emisor y en caso de duda no activar enlaces.

- Externalizar el riesgo a través de la contratación de un seguro que cubra los riesgos cibernéticos.