SECURESOFT CORPORATION

e-Secure Consulting Group

REPORTE SEMANAL DE CIBERINTELIGENCIA

SECURESOFT

Fecha:

06 Abril de 2020

Protegemos tu información

El presente documento contiene información para la comunidad de ciberseguridad.

Equipo de Ciberinteligencia

Indice

1. Objetivo

El presente documento de inteligencia tiene como objetivo informar sobre las principales vulnerabilidades y amenazas que se han detectado en el ciberespacio.

2. Alcance

Este documento muestra el resumen, la fecha de publicación, CVE asociado y servicios afectados a cada vulnerabilidad y amenaza que se ha hecho pública en el transcurso del 30 de Marzo hasta el 06 de Abril del 2020.

3. Amenazas

Boletín	Boletín 2020-126
Asunto	Vulnerabilidades de día cero de Draytek son explotadas
Emisión	30/03/2020
CVE	CVE-2020-8515
Categoría	Vulnerabilidad
Severidad	Crítica

Servicios Afectados

Dispositivos Vigor 2960, 3900 y 300B

Descripción

Al menos dos grupos de atacantes explotaron dos vulnerabilidades críticas de inyección remota de código (CVE-2020-8515) que afectan a los dispositivos empresariales de DrayTek Vigor como: Balanceadores de carga, routers y dispositivos de puerta de enlace VPN. En estos dispositivos instalaron backdoors y obtuvieron persistencia.

Las vulnerabilidades de día cero, pueden ser explotadas por cualquier atacante remoto. La explotación exitosa de estas permite inyectar y ejecutar código de manera arbitraria. Para realizar la explotación se tiene que inyectar comandos en los parámetros enviados al servidor durante la petición de login. Los parámetros que se usan para lograr esto son rtick y keyPath.

Los atacantes explotaron la vulnerabilidad para crear:

- Un backdoor como sesión web que no expira.
- Backdoors en los puertos TCP 22335 y 32459.
- Cuentas de sistema con usuario "wuwuhanhan" y contraseña "caonimuqin".

Se recomienda aplicar la actualización del firmware de acuerdo con el productor afectado, ver apartado de actualización o mitigación.

Actualización o mitigación

Vigor3900 / Vigor2960 / Vigor300B Router Web Management Page Vulnerability (CVE-2020-8515)

Imagen 1. Dispositivo Vigor 2960

Boletín	Boletín 2020-127
Asunto	Zoom es aprovechado por los atacantes para distribuir malwares
Emisión	30/03/2020
CVE	No tiene
Categoría	Phishing
Severidad	Alta

Servicios Afectados

Sistema operativo Windows

Descripción

Se han registrado más de 1,700 nuevos dominios que incluyen la palabra Zoom en su nombre desde inicio de la pandemia. Esto ha generado que los atacantes vean esto como una oportunidad para distribuir malwares a través de enlaces de sitios similares a Zoom o documentos enviados.

Zoom es una plataforma de comunicación empresarial basada en la nube, cuenta con opciones para organizar seminarios web y reuniones virtuales en línea. Debido a lo anterior mencionado, Zoom ha conseguido gran popularidad en estos tiempos, haciendo que estudiantes, empresarios e incluso empleados de los gobiernos lo utilicen para trabajar durante esta época.

Por ello, los atacantes han empezado a distribuir los archivos maliciosos zoom-us-zoom _ ##########[.]exe y microsoft-teams_V#mu#D_##########[.]exe, los cuales instalan InstallCore, este es usado para instalar otros malwares.

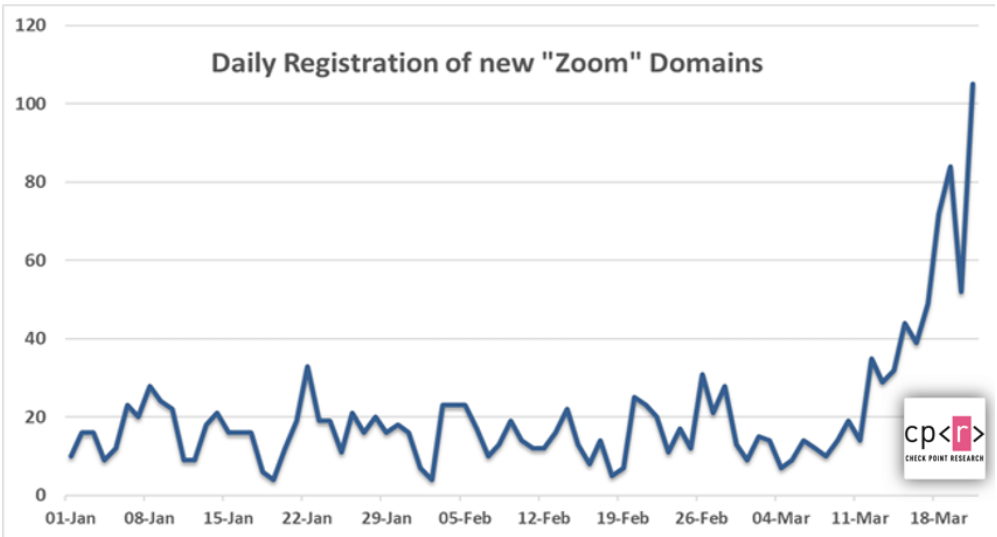

Imagen 2. Incremento de dominios registrados similares a Zoom.

Boletín	Boletín 2020-128
Asunto	Incremento de superficie de exposición por uso de RDP y VPN por el coronavirus
Emisión	31/03/2020
CVE	CVE-2018-13379, CVE-2019-0708, CVE-2019-1453, CVE-2019-1573, CVE-2019-11510
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

Redes que ejecutan servicios RDP y VPN vulnerables.

Descripción

El uso de tecnologías de acceso remoto como RDP y VPN se han incrementado en un 41% y 33% respectivamente desde el inicio de la pandemia. Esto se debe a que una gran cantidad de empresas han pedido a su personal que trabaje desde su casa.

Vulnerabilidades de RDP:
• CVE-2019-0708: Vulnerabilidad de ejecución remota de código. Para más información ver Boletín 2019-156.
• CVE-2019-1453: Vulnerabilidad de denegación de servicio en el protocolo RDP. Para más información ver Boletín 2019-406.

Vulnerabilidades del protocolo VPN:
• CVE-2018-13379: Permite descargar archivos de sistema a través de solicitudes HTTP.
• CVE-2019-1573: Almacenamiento de cookies de autenticación y sesión de forma insegura en memoria.
• CVE-2019-11510: Lectura de archivos arbitraria.

Para más información de las vulnerabilidades ver CVE-2018-13379 y CVE-2019-11510 ver Boletín 2020-087.

Se recomienda:
• Tener activados servicios de monitorización con alertas definidas.
• Revisar los registros y auditorías de las conexiones remotas.
• Tener listados telefónicos de fácil acceso para comunicarse con las diferentes personas.
• Mantener actualizada la relación de personas que pueden acceder remotamente a los equipos de la organización con la dirección IP de acceso y medio de conexión.
• Utilizar sistemas de validación de postura de seguridad para los equipos que estarán por remoto.
• Asegurar si los antivirus escanean los dispositivos USB conectados a los equipos remotos o si se bloquea el acceso de USB en dichos equipos.

Boletín	Boletín 2020-129
Asunto	Zeus Sphinix se aprovecha de la temática del coronavirus para distribuirse
Emisión	31/03/2020
CVE	No tiene
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

Sistema operativo Windows

Descripción

Una campaña de Zeus Sphinx utilizó correos electrónicos de phishing, en los cuales se adjuntan documentos maliciosos que pretenden ser información sobre pagos por parte del gobierno para ayudar a combatir la pandemia.

Los atacantes solicitan a la víctima que completen un formulario protegido por contraseña, estos formularios son documentos con las extensiones .DOC o .DOCX, para convencer a la víctima de llenar estos formularios se les hace creer que después de llenar estos recibirán ayuda económica.

Cuando los archivos son ejecutados, solicitan que se habiliten las macros, lo cual infecta a la computadora con Zeus Sphinx, después de descargar el malware desde un Servidor de Comando y Control (C2, abreviado en inglés).

Una vez que la computadora termina de ser infectada por completo, el malware utiliza inyecciones web para alterar los sitios web de los bancos que visita la víctima, de esta manera se obtienen las credenciales de las víctimas las cuales son enviados al C2 de los atacantes.

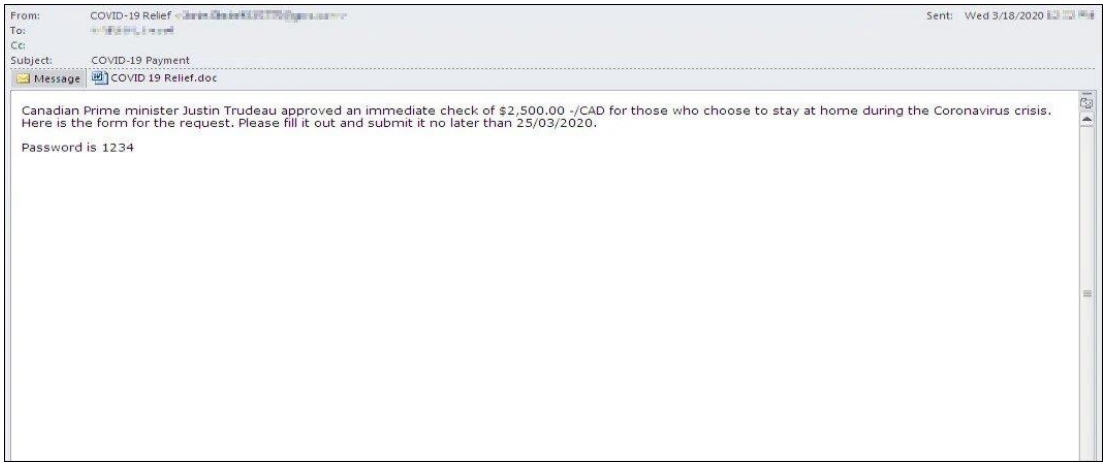

Imagen 3. Captura del correo de phishing usado en la campaña.

Boletín	Boletín 2020-130
Asunto	Atacantes instalan backdoors en servidores MS-SQL
Emisión	01/04/2020
CVE	No tiene
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

Sistema operativo Windows

Descripción

Los atacantes detrás de esta campaña han logrado infectar con éxito entre 2000 y 3000 servidores de bases de datos diariamente, sus principales víctimas pertenecen al sector salud, aviación, informática, telecomunicaciones y educación superior. Para lograr esto los atacantes usaron un tipo de ataque denominado Vollgar.

El ataque Vollgar comienza con intentos de inicio de sesión por fuerza bruta en servidores MS-SQL, cuando se tiene éxito con este ataque, se puede realizar cambios de configuración para ejecutar comandos maliciosos. En paralelo también se validan que ciertas clases COM estén disponibles. Las cuales son aprovechadas para descargar binarios de malwares.

Cuando se completa la configuración inicial, se crean scripts de descarga, dos VBScripts y un script FTP. Una de las cargas, elimina varios procesos esto lo hace con el fin de asegurar los recursos del sistema, así como para eliminar otras amenazas almacenadas en la computadora y eliminar su presencia de la maquina infectada.

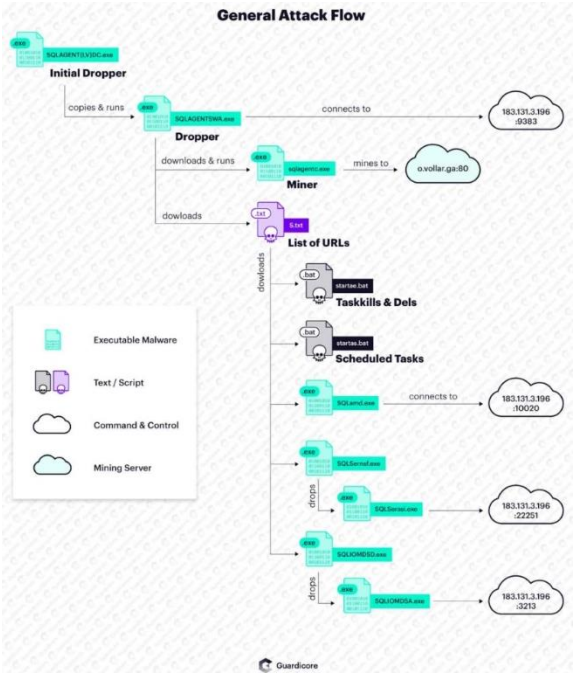

Imagen 4. Flujo general del ataque.

Boletín	Boletín 2020-131
Asunto	Actualización: Zoom es aprovechado por los atacantes para distribuir malwares
Emisión	01/04/2020
CVE	No tiene
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

Aplicación Zoom y sistema operativo Windows

Descripción

La vulnerabilidad radica en la manera que el cliente Zoom convierte las rutas UNC de red de Windows en un enlace en el que se puede hacer clic en los mensajes de chat.

Al hacer esto, de manera predeterminada, Windows enviará el nombre de inicio de sesión del usuario y su hash de contraseña NTLM, que se puede descifrar utilizando herramientas gratuitas como Hashcat para mostrar o revelar la contraseña del usuario.

Además del robo de credenciales de Windows, las inyecciones UNC se pueden utilizar para iniciar programas en una computadora local cuando se hace clic en un enlace.

Se recomienda:
• Aplicar una política de grupo para evitar que sus credenciales NTML se envíen automáticamente a un servidor remoto al hacer clic en un enlace UNC.
• Restringir la comunicación SMB (tcp/445) tanto entrante y saliente del perímetro. Además, asegúrese de habilitar la firma SMB.

Imagen 5. Logo del producto afectado.

Boletín	Boletín 2020-132
Asunto	Vulnerabilidades en el complemento Rank Math de WordPress
Emisión	02/04/2020
CVE	No tiene
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

Complemento Rank Math versiones anteriores a 1.0.41.2

Descripción

Rank Math es un complemento de Posicionamiento en Buscadores (SEO, por sus siglas en inglés) para WordPress.

La primera vulnerabilidad permite a un atacante no autenticado actualizar los metadatos de manera arbitraria, lo que incluye la capacidad de otorgar o revocar privilegios administrativos para cualquier usuario registrado en el sitio. Esta vulnerabilidad se debe a un end-point del REST-API que se encuentra desprotegido.

La segunda vulnerabilidad permite a un atacante no autenticado redirigir a las víctimas a cualquier sitio web y a cualquier ubicación del sitio seleccionado. Esta se debe a un módulo vulnerable que permite a los usuarios crear redirecciones en un sitio web de WordPress.

Se recomienda aplicar las actualizaciones del complemento Rank Math disponible en el apartado de actualización o mitigación.

Actualización o Mitigación

Download WordPress SEO Plugin – Rank Math

Imagen 6. Logo del producto afectado.

Boletín	Boletín 2020-133
Asunto	Campañas de phishing con temática del Coronavirus en Sudamérica
Emisión	02/04/2020
CVE	No tiene
Categoría	Phishing
Severidad	Alta

Servicios Afectados

Sistema operativo Windows

Descripción

Los atacantes alrededor del mundo se están aprovechándose del contexto mundial para realizar ataques de phishing. En estos pretenden que las webs y correos enviados ganen autenticidad, haciéndose pasar por entidades gubernamentales o instituciones de salubridad reconocida a nivel local o mundial. Según Barracuda, en el mes de marzo del 2020 se han detectado más 9000 correos de phishing relacionados al Covid-19.

Sudamérica no es ajena a estas campañas, en el caso del Perú los atacantes han envido correos, creado páginas web falsas, mensaje de texto (sms) y mensajes de WhatsApp, en los que se persuade a la víctima a dejar sus datos, esto aprovechándose de las medidas económicas que ha tomado el Gobierno Peruano para proteger a su población.

En otros países de la región también se han detectado campañas de phishing y web falsas con las mismas intenciones como es el caso de Chile, Ecuador y Colombia.

• Ecuador: Los atacantes realizan campañas de phishing en las cuales se ofrece un falso bono de 150 dólares americanos en Almacenes TIA u acceso a servicios de streaming como Netflix.

• Chile: Los atacantes han creado varías páginas falsas las cuales pretenden brindar información del Coronavirus, se sospecha que están siendo distribuidas a través de correos o mensajes de WhatsApp.

• Colombia: Los atacantes realizaron una campaña en la cual pretendían hacerse pasar por el Ministerio de Salud de ese país, esto con el fin de que las víctimas abran el archivo PDF que se les enviaba. Este en verdad es un malware el cual tiene como objetivo robar información personal de la víctima.

Boletín	Boletín 2020-134
Asunto	Malwares de reescritura de MBRy Wipe se aprovechan del Coronavirus
Emisión	03/04/2020
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

Sistema operativo Windows

Descripción

Se han identificado cuatro malwares que usan la temática del Coronavirus para distribuirse, lo que diferencia a estos cuatro del resto es que estos no están orientados a obtener algún beneficio económico si no a dejar inoperativa la computadora de la víctima.

Dos de los cuatro malwares anteriormente mencionados, atacan sectores del MBR del disco duro reescribiéndolos, esto puede provocar que las computadoras afectadas no puedan iniciar.

• El primero de estos malwares descubiertos, cuando infecta la computadora de la víctima muestra una imagen de un virus acompañado de un mensaje y deshabilita el Administrador de tareas de Windows. Mientras esto ocurre el malware reescribe el MBR y fuerza el reinicio de la computadora. Las modificaciones en el MBR bloquean el arranque de la computadora.

• El segundo de estos malwares descubiertos se hizo pasar por el Coronavirus ransomware, esto lo hacía para despistar a sus víctimas. La función principal de este malware es robar contraseñas, luego de realizar su tarea principal reescribe el MBR.

Por otro lado, se encontraron dos Limpiadores de Datos (Data Wipers, en inglés). Uno de estos estuvo dirigido a víctimas de China, mientras que el segundo se identificó por alguien en Italia. Ambos malwares son considerados ineficientes debido al tiempo que demoran en eliminar los archivos en las computadoras infectadas. Sin embargo, funcionan por lo que son considerados potencialmente peligrosos.

Asunto	Campaña de phishing dirigida a usuarios de bancos peruanos
Emisión	06/04/2020
CVE	No tiene
Categoría	Phishing
Severidad	Alta

Servicios Afectados

Sistema operativo Windows

Descripción

Se han identificado múltiples campañas de phishing dirigida a usuarios de bancos peruanos, a través de aplicaciones de escritorio y móvil. Estas campañas utilizan distintas temáticas.

En una de estas, se le pretende hacer creer a la víctima que ha sido ganador de un premio de 2,000 soles peruanos, esto debido a que es un cliente activo, se le sugiere al cliente ingresar a un link. Este direcciona a la víctima a web falsa, la cual está bajo el control de los atacantes. El de vector de infección es por medio de mensajes LinkedIn, los atacantes utilizan esta plataforma para distribuir su falsa web y aprovecharse de las víctimas.

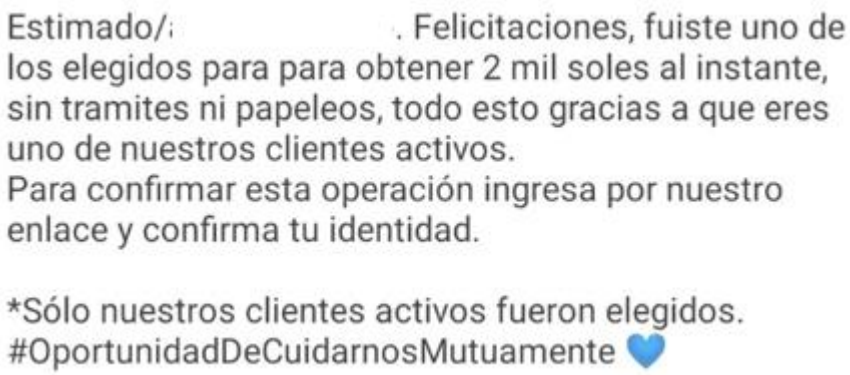

Imagen 7. Captura del mensaje enviado a una de las víctimas.

En otra campaña enfocada en víctimas de dispositivos móviles se le pretende engañar a la víctima haciéndole creer que ha realizado una transferencia de 1,000 soles peruanos o que por falta de actualización en su cuenta esta ha sido bloqueada. En ambas campañas junto al mensaje viene un link, este redirige a las víctimas a páginas falsas controladas por los atacantes, los cuales las usan para obtener beneficios de sus víctimas.

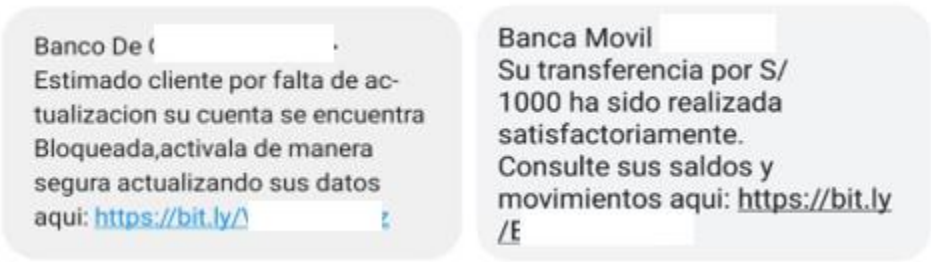

Imagen 8. Mensaje SMS de phishing enviado a víctimas de dispositivos móviles.

Indicadores de Compromiso (IoC's)

IP

198[.]54[.]117[.]244

URL

hxxps://bit[.]ly/BCP-Alertas
hxxps://bit[.]ly/Via-BCPL3nz
hxxp://viabcp[.]com[.]uni-cc[.]ch/
hxxp://www[.]sorteosbbva[.]com/
hxxp://www-bcpzonasegurabeta[.]viabcp[.]com[.]indianbuyer[.]in/
hxxps://bcpzonasegurabeta[.]viabcp[.]com[.]kanku[.]co[.]ke/m/iniciar-sesion
hxxp://viabcp[.]com[.]uni-cc[.]ch/ww[.]bcpzonasegurabeta[.]viabcp[.]com[.]prodigitalnepal[.]com

Asunto	Peruvian hackers amenaza a las AFP
Emisión	03/04/2020
CVE	No tiene
Categoría	Hacktivismo
Severidad	Baja

Servicios Afectados

Sistema operativo Windows

Descripción

Se detectó, el 2 de abril del 2020, a través de nuestras fuentes de información abierta que la página de hacktivismo “Peruvian Hackers” amenazó a las AFP que operan en el Perú. Esto debido a que varios usuarios comunicaron que tenían problemas al momento de acceder a las páginas de sus AFP para realizar el trámite correspondiente al retiro de su dinero, debido a la crisis provocada por el Coronavirus.

Ante esta situación la cuenta hacktivista a través de su página de Facebook emitió un comunicado en el que exigían a los administradores de sistemas de estas AFP hacer todo los posible para que sus portales Web funcionen correctamente. En caso esta demanda no fuese cumplida tomarían medidas en contra de estas empresas.

El 3 de abril del 2020, estos mismos hacktivista utilizaron su página de Facebook para comunicar que ya no tomarían acciones en contra de estas organizaciones debido a que los usuarios ya contaban con un canal para ser atendidos.

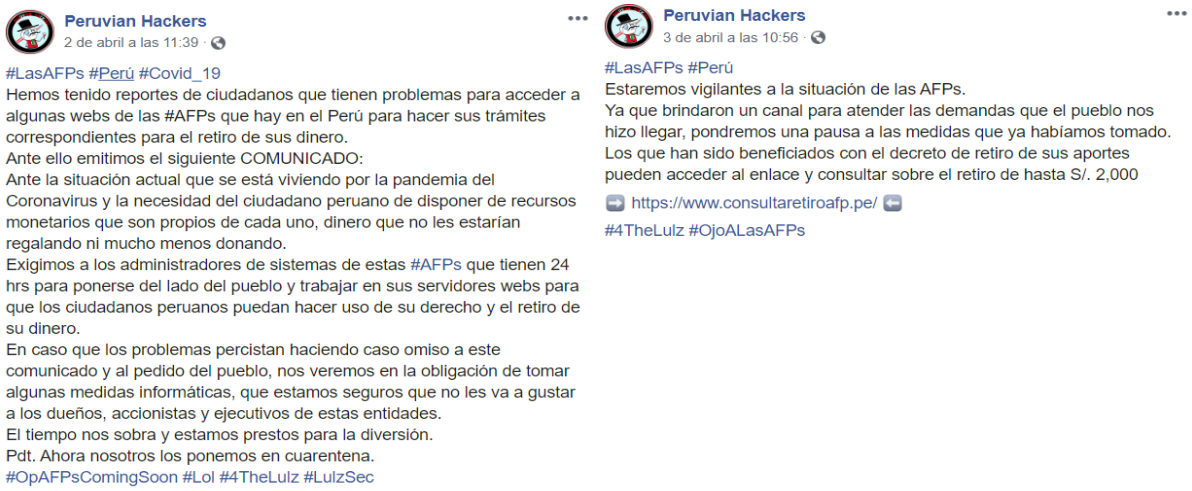

Imagen 9. Captura de los mensajes publicados en Facebook.

4. Recomendaciones

- Leer los boletines citados en las amenazas que tengan uno asociado, esto con la finalidad de encontrar más información de la amenaza como: Una mayor descripción, Indicadores de compromiso,recomendaciones personalizada y fuentes por amenaza.
- Considerar deshabilitar PowerShell y Macros de Microsoft, evitando que pueda ser aprovechado por softwares maliciosos.
- Utilizar una política de uso de contraseñas seguras considerando la complejidad, el cambio de credenciales por defecto y la no reutilización de las mismas.
- Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.
- Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.
- Bloquear los indicadores de compromisos (IOC) compartidos, en los dispositivos de seguridad de su infraestructura.
- Verificar la información de la cuenta que envía el correo, el nombre y la dirección del destinatario para identificar si son sospechosas.
- No abrir correos electrónicos de dudosa procedencia (remitente desconocido), ni dar clic en enlaces, ni descargar archivos adjuntos desconocidos.
- Escanear todo el software descargado de Internet antes de la ejecución.
- De detectar un correo spam, phishing o cualquier actividad anómala reportarlo. inmediatamente a los encargados de seguridad de la información de su institución.

* Antes de realizar el bloqueo de IOCs es importante que previamente en ambiente de desarrollo se valide y confirme a nivel de sus servicios internos y externos, con el propósito de aplicar los cambios de manera controlada.

** Es importante que previamente en ambiente de desarrollo se valide y confirme a nivel de los servicios, con el propósito de aplicar los cambios de manera controlada.