PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno Digital

EL PERÚ PRIMERO

# ALERTA INTEGRADA DE SEGURIDAD DIGITAL



DIRECCIÓN NACIONAL DE INTELIGENCIA DINI

asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ

# ALERTA INTEGRADA DE SEGURIDAD DIGITAL

**Lima, 10 de junio de 2020**

## N° 067-2020-PECERT

La presente **Alerta Integrada de Seguridad Digital** corresponde a un análisis técnico periódico realizado por el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aérea del Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros, en el marco del Centro Nacional de Seguridad Digital.

El objetivo de esta Alerta **es informar a los responsables de la Seguridad de la Información de las entidades públicas y las empresas privadas sobre las amenazas en el ciberespacio** para advertir las situaciones que pudieran afectar la continuidad de sus servicios en favor de la población.

Las marcas y logotipos de empresas privadas y/o entidades públicas se reflejan para ilustrar la información que los ciudadanos reciben por redes sociales u otros medios y que atentan contra la confianza digital de las personas y de las mismas empresas **de acuerdo a lo establecido por el Decreto de Urgencia 007-2020**.

La presente Alerta Integrada de Seguridad Digital es información netamente especializada para informar a las áreas técnicas de entidades y empresas. **Esta información no ha sido preparada ni dirigida a ciudadanos.**

# Contenido

Suplantan página de ingreso a la banca virtual del Banco de Estado de Chile .....3

Suplantan la página web del Ministerio de Sanidad de España para hacer phishing. .....4

Google está indexando los números de teléfono de los usuarios de WhatsApp que plantean problemas de privacidad .....5

Kupidon es el último ransomware dirigido a sus datos.....6

Exploit RCE para SMBGhost que afecta a SMBv3 en Windows 10.....7

Ataque malware se hace pasar por aplicación que da información sobre la pandemia .....8

Ataque tipo phishing suplantan la identidad de Microsoft. .....9

Vulnerabilidad CallStranger afecta a millones de dispositivos.....10

Vulnerabilidad SMBleed afecta a dispositivos con Windows 10.....11

Nueva campaña de SPAM distribuye el ransomware “Avaddon”.....12

SMBleed Vulnerabilidad crítica afecta el protocolo SMB de Windows.....14

Índice alfabético .....16

| | | |
|---|---|---|
| PERÚ \| Presidencia del Consejo de Ministros | **ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 067** | **Fecha: 10-06-2020** |
| | | **Página: 3 de 16** |

| | | | | |
|---|---|---|---|---|
| Componente que reporta | **PECERT \| EQUIPO DE RESPUESTAS ANTE INCIDENTES DE SEGURIDAD DIGITAL NACIONAL** | | | |
| Nombre de la alerta | Suplantan página de ingreso a la banca virtual del Banco de Estado de Chile | | | |
| Tipo de ataque | Phishing | | Abreviatura | Phishing |
| Medios de propagación | Red, internet | | | |
| Código de familia | G | Código de subfamilia | G02 | |
| Clasificación temática familia | Fraude | | | |

Descripción

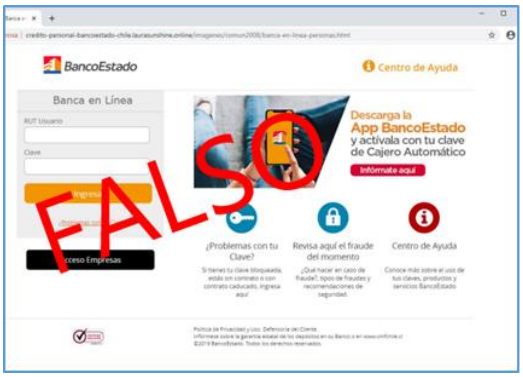
1. Resumen

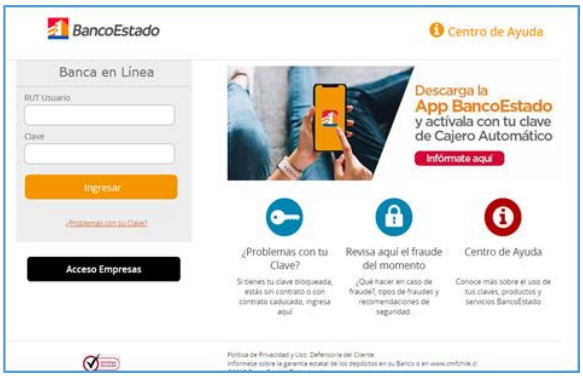
   El Equipo de Respuesta ante Incidentes de Seguridad Digital Nacional, informa que viene circulando un correo electrónico phishing haciéndose pasar por una Entidad Bancaria con el fin de cometer fraude.

2. Detalle de la alerta

   A través del monitoreo y búsqueda de amenazas en el ciberespacio, se tuvo conocimiento que ciberdelincuentes mediante una campaña tipo phishing suplantan la página Banco de Estado de Chile, específicamente a

   la banca virtual, donde los usuarios ingresan su nombre de usuario y contraseña. Cabe resaltar que estos delincuentes informáticos siguen usando de diversos métodos el nombre de la actual pandemia (COVID19) para seguir robando información bancaria después.




**URL sitio falso:**

hxxp://www.credito-personal-bancoestadochile.laurasunshine[.]online/imagenes/comun2008/banca-en-linea-personas.html

**SHA256** e6d8d53cc66ce07cf2e63ebad4cdb3f632350b5a4774d21bc36572515356b259

**Datos del IP**

| | | | | | |
|---|---|---|---|---|---|
| IP Address | 94[.]237[.]77[.]204 | Country | Singapore [SG] | Region | Singapore |
| City | Singapore | ISP | UpCloud Ltd | | |

3. Recomendaciones

   - Si recibe un correo electrónico o un mensaje de texto al celular de instituciones o personas conteniendo enlaces sospechosos solicitando información; no responda ni abra el enlace, podría ser un caso de suplantación de identidad.
   - Evite ingresar a su correo electrónico o a realizar comercio electrónico desde una cabina de internet o conexiones de internet libres.
   - Mantenga actualizado el antivirus de su PC: Instale las actualizaciones de seguridad de su sistema operativo y de todas las aplicaciones que utiliza, especialmente las de su antivirus.
   - Recuerde: No conteste ni abra ningún mensaje que le parezca sospechoso. Tampoco descargue ni abra archivos de fuentes desconocidos. Esos archivos pueden contener virus o software malicioso que podrían permitir a un atacante acceder a su computadora.

| | |
|---|---|
| Fuentes de información | Equipo de Respuestas ante Incidentes de Seguridad Digital Nacional |

| | ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 067 | Fecha: 10-06-2020 |
|---|---|---|
| | | Página: 4 de 16 |

| | | | | |
|---|---|---|---|---|
| Componente que reporta | **COMANDO OPERACIONAL DE CIBERDEFENSA DEL COMANDO CONJUNTO DE LAS FUERZAS ARMADAS** | | | |
| Nombre de la alerta | Suplantan la página web del Ministerio de Sanidad de España para hacer phishing. | | | |
| Tipo de ataque | Phishing | | Abreviatura | Phishing |
| Medios de propagación | Redes sociales, SMS, correo electrónico, videos de internet, entre otros | | | |
| Código de familia | G | Código de subfamilia | G02 | |
| Clasificación temática familia | Fraude | | | |

Descripción

1. El 09 de junio de 2020, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se ha encontrado información publicada sobre el equipo de investigadores de Check Point Software Technologies, proveedor especializado en ciberseguridad a nivel mundial, ha detectado este caso de phishing gracias a sus propios sistemas de protección ante los ciberataques. El caso más reciente de phishing, detectado hace un par de días, afecta a la web del Ministerio de Sanidad de España.
2. En este tipo de mails siempre hay un enlace que lleva a una web falsa, donde nos piden nuestras credenciales. Mediante este método, los piratas consiguen entrar en nuestras cuentas bancarias o nos roban las contraseñas para acceder a otros servicios. En ocasiones, se utiliza esta técnica para acceder a nuestros contactos para también robar sus datos.
3. Las posibles víctimas de esta ciberestafa reciben un correo electrónico engañoso haciéndose pasar por el Ministerio de Sanidad español y les informan de que han sido denunciados por sus vecinos por no llevar mascarilla. En el correo hay un enlace para descargar la presunta notificación de la denuncia. Pero si hacen click en él, lo más probable es que se cuele un troyano que puede robar sus datos bancarios.


4. Se trata del troyano bancario para Android Ginp. Después de instalarse en el equipo de la víctima, pide que se activen los servicios de accesibilidad, para a continuación enviar al servidor del atacante información sobre todas las aplicaciones que se encuentran en funcionamiento.
5. Se recomienda:
   - No abrir correos de usuarios desconocidos o que no se haya solicitado.
   - No abrir, ni descargar archivos adjuntos a correos, SMS, redes sociales de usuarios de dudosa procedencia.
   - No ingresar a páginas sospechosas.
   - No proporcionar datos bancarios.

| | |
|---|---|
| Fuentes de información | https[://]www.lavanguardia.com/tecnologia/20200609/481697889864/suplantan-pagina-web-ministerio-sanidad-phishing.html |

| | ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 067 | Fecha: 10-06-2020 |
|---|---|---|
| | | Página: 5 de 16 |

| | | | |
|---|---|---|---|
| Componente que reporta | **CIBERDEFENSA Y TELEMÁTICA DEL EJÉRCITO DEL PERÚ** | | |
| Nombre de la alerta | Google está indexando los números de teléfono de los usuarios de WhatsApp que plantean problemas de privacidad | | |
| Tipo de ataque | Explotación de vulnerabilidades conocidas | Abreviatura | EVC |
| Medios de propagación | Red, internet | | |
| Código de familia | H | Código de subfamilia | H01 |
| Clasificación temática familia | Intento de intrusión | | |

Descripción

1. El 10 de junio de 2020, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se ha encontrado información publicada el 08 de junio de 2020 por Security Affairs, sobre google está indexando los números de teléfono de los usuarios de WhatsApp que podrían ser abusados por actores de amenazas por actividades maliciosas.

2. Los atacantes mal intencionados podrían ver las imágenes de perfil de los usuarios en WhatsApp y realizar una búsqueda de imagen inversa en la imagen de perfil del usuario para recopilar información adicional sobre el potencial víctima (es decir, minar cuentas de redes sociales donde la víctima usa la misma imagen de perfil).
3. Se descubrió una fuga de datos con el dominio 'wa.me' de WhatsApp que revelaba números de teléfono de contacto en Google.
4. El dominio 'wa.me' se usa para alojar enlaces de ' hacer clic para chatear ' que permiten a los usuarios iniciar un chat con alguien sin tener su número de teléfono guardado en la libreta de direcciones del teléfono.
5. Para crear enlaces de clic para chatear, use https[://]wa.me/ <número> donde <número> es un número de teléfono completo en formato internacional.
6. Los dominios "wa.me" o "api.whatsapp.com" no evitan que los motores de búsqueda rastreen números de teléfono en el sitio web permitiendo que cualquier enlace como "https[://]wa.me/" sea indexado por Google.
7. A medida que se filtran números de teléfono individuales, un atacante puede enviarles mensajes, llamarlos y vender sus números de teléfono a vendedores, spammers, estafadores.
8. Se recomienda:

   Se recomienda utilizar un robot.txt en los dominios anteriores es posible evitar que Google rastree estos resultados.

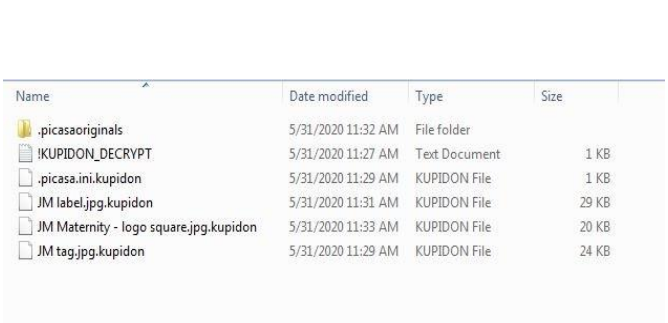
| | |
|---|---|
| Fuentes de información | https[://]www.bleepingcomputer.com/news/security/kupidon-is-the-latest-ransomware-targeting-your-data/ |

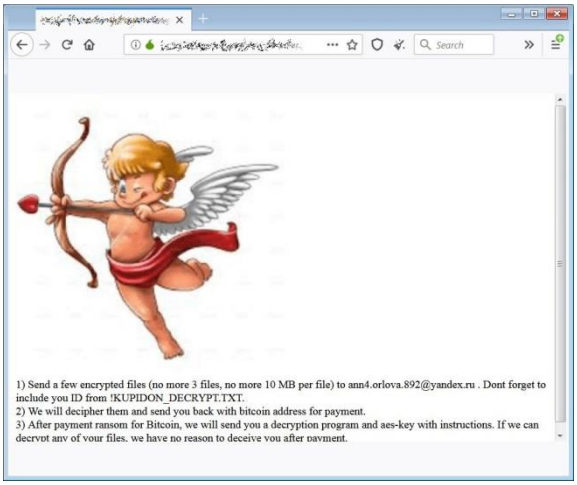
| | ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 067 | Fecha: 10-06-2020 |
|---|---|---|
| | | Página: 6 de 16 |

| | | | |
|---|---|---|---|
| Componente que reporta | **CIBERDEFENSA Y TELEMÁTICA DEL EJÉRCITO DEL PERÚ** | | |
| Nombre de la alerta | Kupidon es el último ransomware dirigido a sus datos. | | |
| Tipo de ataque | Malware | Abreviatura | Malware |
| Medios de propagación | USB, disco, red, correo, navegación de internet | | |
| Código de familia | C | Código de subfamilia | C02 |
| Clasificación temática familia | Código malicioso | | |

Descripción

1. El 10 de junio de 2020, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se ha encontrado información publicada el 05 de junio de 2020 por Bleepingcomputer, sobre el ultimo ransomware que se llama Kupidon, y se dirige no solo a las redes corporativas, sino también a los datos personales de los usuarios domésticos.
2. Este malware está dirigido tanto a usuarios personales como a empresas, probablemente a través de servidores de escritorio remotos expuestos.
3. Una vez que los actores de la amenaza obtienen acceso, cifran manualmente los archivos en las computadoras de la víctima. Al cifrar datos, agregará la extensión .kupidon al nombre del archivo.
4. En cada carpeta en la que se cifra un archivo, el ransomware también creará una nota de rescate llamada '! KUPIDON_DECRYPT.TXT'.
5. Dependiendo de si la víctima es un negocio o un individuo, las notas de rescate eliminadas serán ligeramente diferentes y contendrán diferentes demandas de rescate.
6. La nota de rescate dirigirán a los usuarios a un sitio TOR que contiene información sobre lo que sucedió con los archivos de una víctima y una dirección de correo electrónico para contactar para obtener instrucciones de pago. La dirección de correo electrónico actual que se utiliza en el sitio TOR es ann4.orlova.892@yandex.ru.




7. Se recomienda:

   Se recomienda la actualización del sistema y aplicaciones, mantener el sistema operativo actualizado con los últimos parches de seguridad y todas las aplicaciones que tengamos instaladas es el mejor punto de partida.

| | |
|---|---|
| Fuentes de información | https[://]www.bleepingcomputer.com/news/security/kupidon-is-the-latest-ransomware-targeting-your-data/ |

| | | |
|---|---|---|
| | **ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 067** | **Fecha: 10-06-2020** |
| | | **Página: 7 de 16** |

| | | | | |
|---|---|---|---|---|
| Componente que reporta | **CIBERDEFENSA Y TELEMÁTICA DEL EJÉRCITO DEL PERÚ** | | | |
| Nombre de la alerta | Exploit RCE para SMBGhost que afecta a SMBv3 en Windows 10 | | | |
| Tipo de ataque | Exploits | | Abreviatura | Exploits |
| Medios de propagación | USB, disco, red, correo, navegación de internet | | | |
| Código de familia | C | Código de subfamilia | C03 | |
| Clasificación temática familia | Código malicioso | | | |

Descripción

1. El 10 de junio de 2020, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se ha encontrado información publicada el 08 de junio de 2020 en la red social Twitter por el usuario “cipherstorm”, sobre un exploit RCE (ejecución remota de código) que afecta a SMBv3 (protocolo que permite compartir archivos, impresoras, etc.) en Windows 10 y algunas versiones de Windows Server.

2. El exploit RCE afecta a la vulnerabilidad identificada con el código (CVE-2020-0796) atacando al protocolo Microsoft Server Message Block 3.1.1 (SMBv3).
3. La vulnerabilidad podría explotarse para obtener la capacidad de ejecutar código en el servidor SMB o el cliente SMB de destino. En el primer caso, enviando un paquete especialmente diseñado a un servidor SMBv3 específico. En el último, configurando un servidor SMBv3 malicioso y convenciendo a un usuario para que se conecte a él.
4. Aunque la PoC (prueba de concepto) publicada por el investigador de seguridad que se conoce con el nombre de "chompie" funciona de manera demostrable, no funciona todo el tiempo. Sin embargo, los atacantes persistentes podrían aprovecharlo con suficiente tiempo y esfuerzo repetido. Aquellos más conocedores podrían incluso encontrar una manera de modificarlo y mejorar su efectividad.
5. Se recomienda:
   - Tener siempre actualizado el programa antivirus.
   - Tener siempre actualizado el Sistema Operativo, con los últimos parches de seguridad.

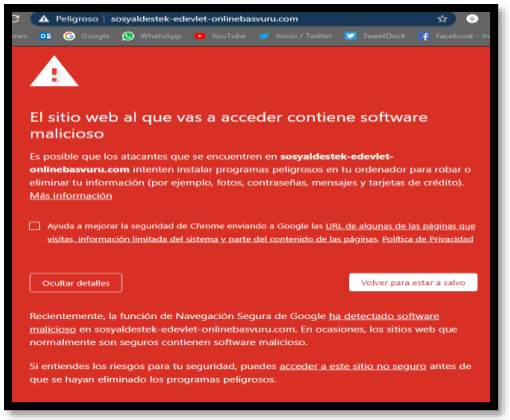
| | |
|---|---|
| Fuentes de información | https[://]twitter.com/cipherstorm/status/1269935844921507841<br>https[://]www.helpnetsecurity.com/2020/06/08/smbghost-poc-rce-exploit/ |

| | ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 067 | Fecha: 10-06-2020 |
|---|---|---|
| | | Página: 8 de 16 |

| | | | | |
|---|---|---|---|---|
| Componente que reporta | **COMANDANCIA DE CIBERDEFENSA DE LA MARINA DE GUERRA DEL PERÚ** | | | |
| Nombre de la alerta | Ataque malware se hace pasar por aplicación que da información sobre la pandemia | | | |
| Tipo de ataque | Malware | | Abreviatura | Malware |
| Medios de propagación | Red, Correo electrónico. | | | |
| Código de familia | C | Código de subfamilia | | C03 |
| Clasificación temática familia | Código malicioso | | | |

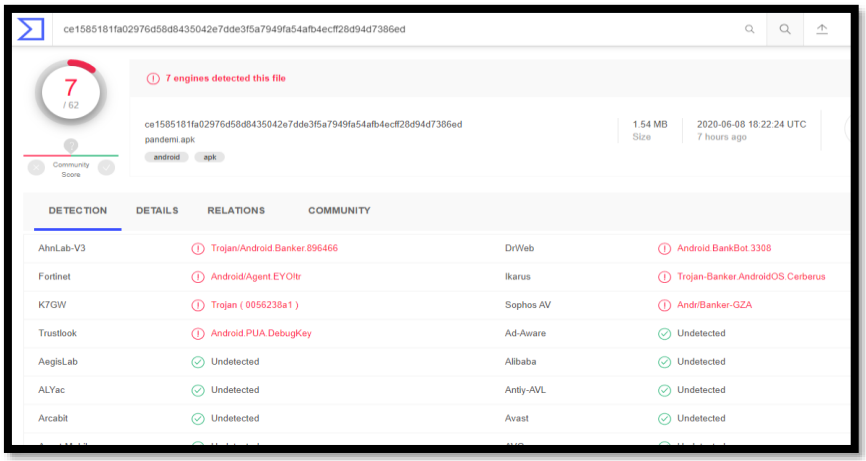
Descripción

1. El 10 de junio de 2020, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se identificó de un aplicativo fraudulento de nombre “pandemi.apk” circula principalmente por redes sociales, invitando a los usuarios a descargar e instalarlo, que en su lugar sería una aplicación maliciosa.





2. Se analizó el citado aplicativo en la página web “Virus Total” donde es catalogado como troyano.




3. Se recomienda:

- Evitar ingresar a enlaces no confiables.
- Evitar descargar y abrir archivos de fuentes no confiables.
- Mantener los equipos protegidos, con el software actualizado.

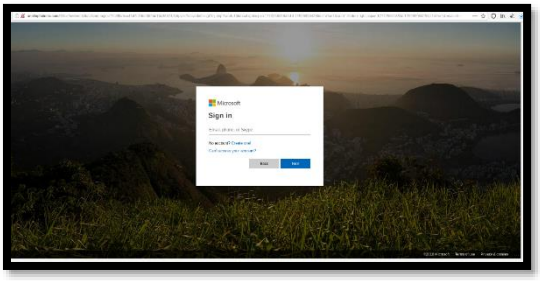
| | |
|---|---|
| Fuentes de información | Comandancia de Ciberdefensa de la Marina, OSINT. |

| | ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 067 | Fecha: 10-06-2020 |
|---|---|---|
| | | Página: 9 de 16 |

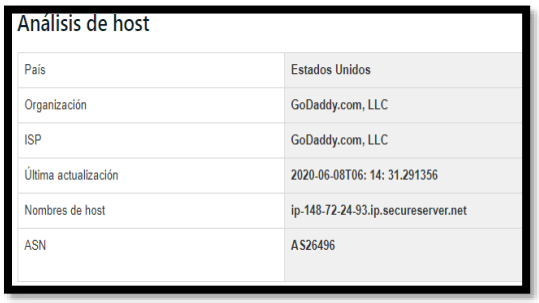
| | | | | |
|---|---|---|---|---|
| Componente que reporta | **COMANDANCIA DE CIBERDEFENSA DE LA MARINA DE GUERRA DEL PERÚ** | | | |
| Nombre de la alerta | Ataque tipo phishing suplantan la identidad de Microsoft. | | | |
| Tipo de ataque | Phishing | | Abreviatura | Phishing |
| Medios de propagación | Redes sociales, SMS, correo electrónico, videos de internet, entre otros | | | |
| Código de familia | G | Código de subfamilia | G02 | |
| Clasificación temática familia | Fraude | | | |

Descripción

1. El 10 de junio de 2020, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que ciberdelincuentes siguen aprovechándose del confinamiento social generado por la pandemia Covid-19 (Coronavirus), vienen suplantando la identidad de la página web de inicio de sesión de Microsoft por medio del enlace fraudulento **anellophotonic.com**, con la finalidad de que el usuario ingrese sus credenciales y logren robar su información.




2. Asimismo, se realizó el análisis del enlace en la página web de Shodan donde se obtuvo los siguientes datos.

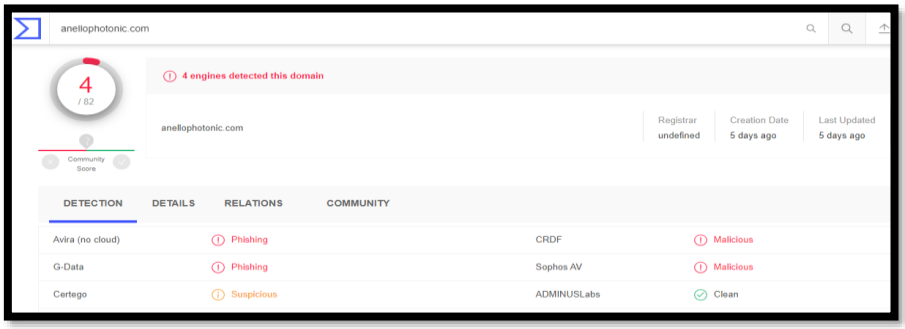


Análisis de host

| | |
|---|---|
| País | Estados Unidos |
| Organización | GoDaddy.com, LLC |
| ISP | GoDaddy.com, LLC |
| Última actualización | 2020-06-08T06: 14: 31.291356 |
| Nombres de host | ip-148-72-24-93.ip.secureserver.net |
| ASN | AS26496 |

Análisis de dominio.


```
{
    "status": 1,
    "domain_name": "anellophotonic.com",
    "query_time": "2020-06-08 13:47:41",
    "whois_server": "whois.godaddy.com",
    "domain_registered": "yes",
    "create_date": "2020-06-04",
    "update_date": "2020-06-04",
    "expiry_date": "2021-06-04",
    "domain_registrar": {
        "iana_id": 146,
        "registrar_name": "GoDaddy.com, LLC",
        "whois_server": "whois.godaddy.com",
        "website_url": "http://www.godaddy.com",
        "email_address": "abuse@godaddy.com",
        "phone_number": "+1.4806242505"
    },
    "registrant_contact": {
        "state_name": "Florida",
        "country_name": "United States",
        "country_code": "US"
    },
    "name_servers": [
        "ns59.domaincontrol.com",
        "ns60.domaincontrol.com"
    ],
    "domain_status": [
        "clientDeleteProhibited",
        "clientRenewProhibited",
        "clientTransferProhibited",
        "clientUpdateProhibited"
    ]
}
```


3. Por otro lado, se verifico el enlace en la página web de Virus Total donde es catalogado como phishing.
4. Se recomienda:
   - Evitar ingresar a enlaces no confiables.
   - Evitar descargar y abrir archivos de fuentes no confiables.
   - Mantener los equipos protegidos, con el software actualizado.

| | |
|---|---|
| Fuentes de información | Comandancia de Ciberdefensa de la Marina. Osint |

| | | |
|---|---|---|
| | **ALERTA INTEGRAL DE SEGURIDAD DIGITAL N° 067** | **Fecha : 10-06-2020** |
| | | **Página: 10 de 16** |

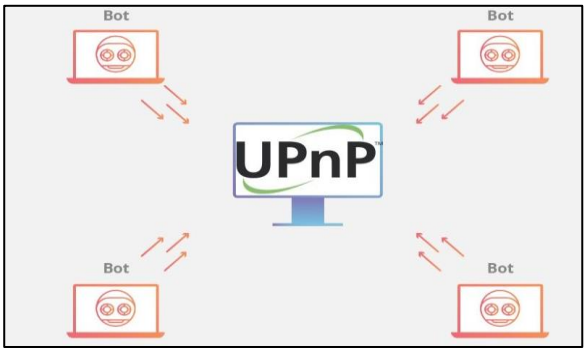
| | | | |
|---|---|---|---|
| Componente que reporta | **DIRECCIÓN DE INTELIGENCIA DE LA FUERZA AÉREA DEL PERÚ** | | |
| Nombre de la alerta | Vulnerabilidad CallStranger afecta a millones de dispositivos | | |
| Tipo de ataque | Escaneo de puertos Scan | Abreviatura | Scanning |
| Medios de propagación | Red, internet | | |
| Código de familia | J | Código de subfamilia | J01 |
| Clasificación temática familia | Reconocimiento de información | | |

Descripción

1. El 10 de junio de 2020, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó un fallo de seguridad denominado **CallStranger**, que afecta al protocolo UPnP (Universal Plug and Play), que está presente en millones de dispositivos, dentro de ellos podemos incluir dispositivos que ejecutan windows 10, routers, puntos de acceso, impresoras, videoconsolas multimedia, cámaras, televisores, etc.

   Cabe mencionar que, el protocolo UPnP es usado para la detección automática de dispositivos de redes y poder interaccionar entre ellos, todo esto dentro de una red local fiable ya que no cuenta con verificación o autenticación.

2. Asimismo, el fallo de seguridad ha sido registrado como CVE-2020-12695, el cual puede ser aprovechado de forma remota sin necesidad de autenticación y se encuentra ubicado en el valor encabezado de devolución de llamada, que podría ser controlado por un atacante, normalmente en la capa de enlace de datos. Si un ciberdelincuente aprovechara este fallo, tendría la capacidad de eludir dispositivos de seguridad de red y las soluciones de prevención de perdida de datos diseñadas para evitar el envío de información crítica o confidencial fuera de la red corporativa.




   Del mismo modo, el mayor riesgo del fallo es la filtración de datos, pero también podría ser útil para realizar ataques de DDoS (denegación de servicio distribuido), desde múltiples dispositivos accesibles desde la web.

3. Se recomienda:

   - Los administradores de las infraestructuras tecnológicas de las diversas áreas, deberán deshabilitar el protocolo UPnP, y si fuese necesario su uso, realizar un diagnóstico para verificar que no se tenga el fallo en nuestros dispositivos.

| | |
|---|---|
| Fuentes de información | https[://]www.redeszone.net/noticias/seguridad/callstranger-vulnerabilidad-escanea-puertos-lan/ |

| | | |
|---|---|---|
| | **ALERTA INTEGRAL DE SEGURIDAD DIGITAL N° 067** | **Fecha : 10-06-2020** |
| | | **Página: 11 de 16** |

| | | | |
|---|---|---|---|
| Componente que reporta | **DIRECCIÓN DE INTELIGENCIA DE LA FUERZA AÉREA DEL PERÚ** | | |
| Nombre de la alerta | Vulnerabilidad SMBleed afecta a dispositivos con Windows 10 | | |
| Tipo de ataque | Escaneo de puertos Scan | Abreviatura | Scanning |
| Medios de propagación | Red, Internet | | |
| Código de familia | J | Código de subfamilia | J01 |
| Clasificación temática familia | Reconocimiento de información | | |

Descripción

1. El 10 de junio de 2020, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó un fallo de seguridad denominado SMBleed (CVE-2020-1206), que afecta al protocolo SMB de Microsoft, ejecutándose sobre el puerto TCP 445, de las versiones 1903 y 1909 de Windows 10. Uno de los casos más sonados que aprovecha este puerto es EternalBlue, quien del mismo modo usa el protocolo SMB para poder vulnerar distintos equipos que tengan Microsoft Windows.

   Cabe mencionar que, para aprovechar la vulnerabilidad contra un cliente, un atacante no autenticado necesitaría configurar un servidor SMBv3 malicioso y convencer a un usuario para que se conecte a él.


2. Se recomienda:

   Los administradores de las infraestructuras tecnológicas de las diversas áreas, deben deshabilitar el protocolo 445 y gestionar soluciones para evitar que ciberdelincuentes aprovechen el fallo.

| | |
|---|---|
| Fuentes de información | https[://]www.redeszone.net/noticias/seguridad/smbleed-error-critico-protocolo-smb/ |

| | | |
|---|---|---|
| DINI | **ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 067** | **Fecha: 10-06-2020**<br>**Página: 12 de 16** |

| | | | | |
|---|---|---|---|---|
| Componente que reporta | **DIRECCIÓN NACIONAL DE INTELIGENCIA** | | | |
| Nombre de la alerta | Nueva campaña de SPAM distribuye el ransomware “Avaddon” | | | |
| Tipo de ataque | Ransomware | | Abreviatura | Ransomware |
| Medios de propagación | Correo electrónico, redes sociales, entre otros | | | |
| Código de familia | C | Código de subfamilia | | C09 |
| Clasificación temática familia | Código malicioso | | | |

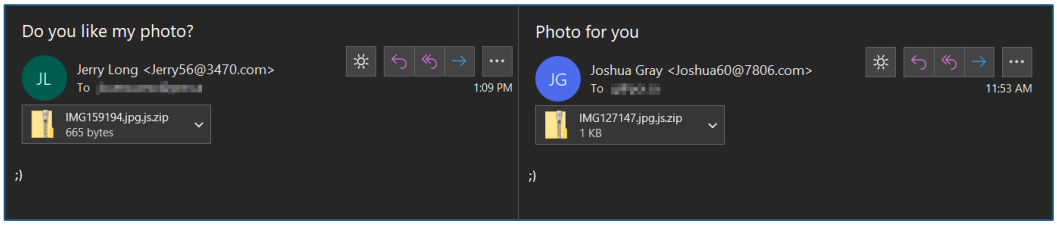
Descripción

8. Resumen:

   Los investigadores de la empresa de ciberseguridad Appriver, han descubierto recientemente un nuevo ransomware denominado “Avaddon” que se distribuye a través de una campaña masiva de spam y que se encuentra activa desde inicios del mes de junio de 2020.

9. Detalles:

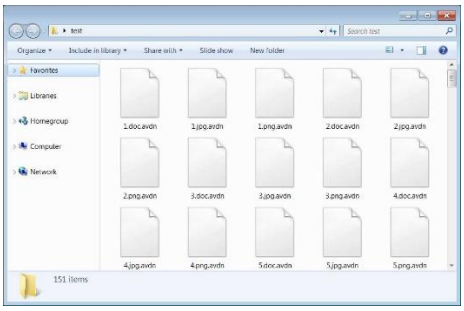
   En esta campaña de correo electrónico no deseado, el ransomware Avaddon se distribuye a través de correos que usan temas como: "¿Tu nueva foto?" o "¿Te gusta mi foto?" que no contiene más que una carita sonriente que distribuye un descargador de JavaScript para el ransomware Avaddon. Los actores de amenaza detrás de esta campaña utilizan la botnet Phorphiex / Trik para distribuir los correos maliciosos.




   Todos los mensajes contienen un archivo adjunto que llega en el formato IMG <número> .jpg.js.zip. Una vez que se extrae el zip, hay un pequeño archivo JavaScript de 1 kilobyte dentro. Este archivo en formato .jpg pretende hacerse pasar por una imagen. Los atacantes utilizan esta técnica para que Windows oculte la extensión del archivo de manera predeterminada, aunque es un riesgo de seguridad conocido.



   Cuando se ejecuta, el archivo inicia el host de secuencias de comandos de Windows para ejecutar un comando que inicia PowerShell con el indicador de omisión de la política de ejecución. Esto indica a Windows que ejecute el script sin firmar sin ser bloqueado o mostrar advertencias. Luego se descarga un archivo llamado sava.exe de la IP de 217 [.] 8 [.] 117 [.] 63 en la carpeta %Temp% y se guarda como 5203508738.exe, antes de ejecutarse. Una vez que se ejecute, el ransomware buscará datos para cifrar y añadirá la extensión .avdn a los archivos cifrados.



En cada carpeta afectada se creará una nota de rescate llamada "[id] -readme.html". Esta nota de rescate contiene un enlace al sitio de pago TOR y una identificación de la víctima única utilizada para iniciar sesión en el sitio. El sitio también proporciona instrucciones sobre múltiples métodos para obtener bitcoins y asistencia de soporte 24/7, a través de una interfaz de chat. También se incluye un código QR y una dirección única de billetera bitcoin para el pago.

Los actores de la amenaza brindan la capacidad de probar el descifrado con 3 archivos de imagen para establecer la confianza y, además, especificar que las imágenes no valen tanto como otros datos cifrados. El sitio ofrece 9 opciones de idiomas diferentes, que proporcionan información sobre la amplia gama de nacionalidades y víctimas a las que se dirige el ataque.

Avaddon opera como un ransomware como servicio (RaaS). Esto quiere decir que el creador de la amenaza es el responsable del desarrollo y del funcionamiento del sitio de pago TOR. El RaaS funciona como un servicio afiliado, donde los afiliados son responsables de la distribución a través de correos electrónicos no deseados, redes comprometidas y kits de explotación.

10. Indicadores de Compromiso (IoC):

Dirección IP

- 217[.]8[.]117[.]63

Hashes

- MD5: 06072312768ba47c162d2aead14bb170
- SHA-256: cc4d665c468bcb850baf9baab764bb58e8b0ddcb8a8274b6335db5af86af72fb
- MD5: c9ec0d9ff44f445ce5614cc87398b38d
- SHA-256: 05af0cf40590aef24b28fa04c6b4998b7ab3b7f26e60c507adb84f3d837778f2

Archivos asociados

- IMG123101.jpg.js.zip
- IMG123101.jpg.js
- IMG126172.jpg.js
- %temp%\97459754.exe
- %temp%\646246465.exe
- [id]-readme.html

11. Recomendaciones:

- Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.
- Contar con herramientas de seguridad. Se debe tener instalado un buen antivirus para prevenir la entrada de malware que pueda poner en riesgo nuestro sistema. Será necesario tener por tanto software de seguridad que nos permita realizar análisis y evitar amenazas.
- Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos. Será vital tener siempre los últimos parches y actualizaciones instalados.
- Descargar solo de fuentes oficiales. De esta forma nos aseguraremos que ese software que estamos agregando no ha sido modificado de forma maliciosa.
- No descargar o abrir archivos adjuntos que recibamos en nuestro e-mail. Tampoco acceder a posibles links fraudulentos que puedan poner en riesgo nuestros sistemas. Estos enlaces fraudulentos pueden llegar también a través de las redes sociales o incluso aplicaciones de mensajería instantánea como puede ser WhatsApp.
- Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización.
- Bloquear los indicadores de compromisos (IoC) mostrados, en los dispositivos de seguridad de su infraestructura.
- Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

| | |
|---|---|
| Fuentes de información | ▪ hxxps://appriver.com/resources/blog/june-2020/phorphiextrik-botnet-delivers-avaddon-ransomware<br>▪ hxxps://www.bleepingcomputer.com/news/security/new-avaddon-ransomware-launches-in-massive-smiley-spam-campaign/ |

| | ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 067 | Fecha: 10-06-2020 |
|---|---|---|
| | | Página: 14 de 16 |

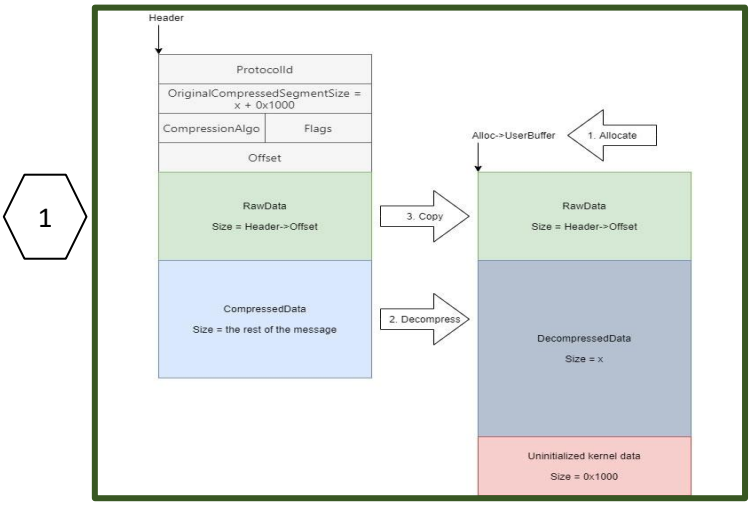
| | | | | |
|---|---|---|---|---|
| Componente que reporta | **DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ** | | | |
| Nombre de la alerta | SMBleed Vulnerabilidad crítica afecta el protocolo SMB de Windows | | | |
| Tipo de ataque | Explotación de vulnerabilidades conocidas | | Abreviatura | EVC |
| Medios de propagación | Red, Internet | | | |
| Código de familia | H | Código de subfamilia | H01 | |
| Clasificación temática familia | Intento de intrusión | | | |

Descripción

1. El 09 de junio de 2020, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, en el sitio web thehackernews.com, se informa sobre una vulnerabilidad que afecta el protocolo del Bloque de mensajes del servidor (SMB) que podría permitir que los atacantes pierdan la memoria del núcleo de forma remota, y cuando se combina con un error "wormable" previamente divulgado, la falla puede ser explotada para lograr ataques de ejecución remota de código.
2. Apodado " SMBleed ", el defecto reside en la función de descompresión de SMB, la misma función que con el error SMBGhost o EternalDarkness (CVE-2020-0796)

- La falla se debe a la forma en que la función de descompresión en cuestión (" Srv2DecompressData ") maneja las solicitudes de mensajes especialmente diseñados (p. Ej., SMB2 WRITE) enviado a un servidor SMBv3 de destino, lo que permite a un atacante leer la memoria del núcleo no inicializada y realizar modificaciones en la función de compresión.

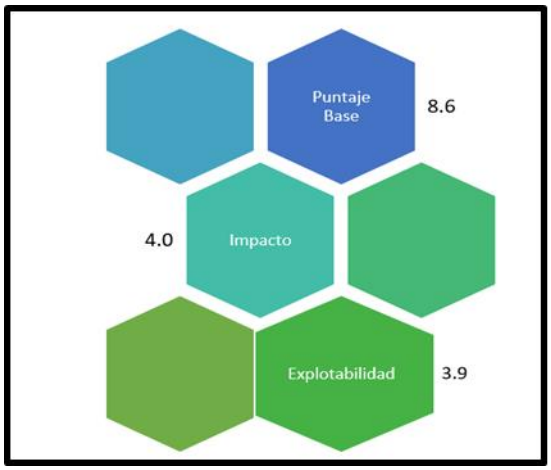

- La vulnerabilidad recién descubierta afecta las versiones de Windows 10 1903 y 1909, para las cuales Microsoft lanzó hoy parches de seguridad como parte de sus actualizaciones mensuales de Patch Tuesday para junio.
- SMB, que se ejecuta sobre el puerto TCP 445, es un protocolo de red que proporciona la base para compartir archivos, navegar por la red, servicios de impresión y comunicación entre procesos a través de una red.
- Aunque Microsoft reveló y proporcionó actualizaciones para esta vulnerabilidad en marzo de 2020, los ciber actores maliciosos están apuntando a sistemas no parcheados con el nuevo PoC, según informes recientes de código abierto, mencionaron los especialistas encargado de analizar la vulnerabilidad:
  - "Para aprovechar la vulnerabilidad contra un cliente, un atacante no autenticado necesitaría configurar un servidor SMBv3 malicioso y convencer a un usuario para que se conecte a él".



- Análisis de la Vulnerabilidad: (CVE-2020-1206)
  - Descripción:
    - Existe una vulnerabilidad de divulgación de información en la forma en que el protocolo Microsoft Server Message Block 3.1.1 (SMBv3) maneja ciertas solicitudes. Un atacante que explotara con éxito la vulnerabilidad podría obtener información para comprometer aún más el sistema del usuario.
    - Para aprovechar la vulnerabilidad contra un servidor, un atacante no autenticado podría enviar un paquete especialmente diseñado a un servidor SMBv3 de destino. Para aprovechar la vulnerabilidad contra un cliente, un atacante no autenticado necesitaría configurar un servidor SMBv3 malicioso y convencer a un usuario para que se conecte a él.
  - Vectores: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N
  - Detalles:

| Vector | Red |
|---|---|
| **Complejidad de Ataque** | Local |
| **Privilegio Requerido** | Ninguno |
| **Interacción de Usuario** | Ninguno |
| **Confidencialidad** | Alto |
| **Integridad** | Ninguno |
| **Disponibilidad** | Ninguno |

  - Gráficos:




Puntaje Base


Riesgo

3. Algunas Recomendaciones

- Para sistemas donde el parche no es aplicable, se recomienda bloquear el puerto 445 para evitar el movimiento lateral y la explotación remota.
- Para mitigar la vulnerabilidad, se recomienda que los usuarios domésticos y empresariales instalen las últimas actualizaciones de Windows lo antes posible.
- Descargar la guía de seguridad de Microsoft sobre SMBleed y SMBGhost en Windows 10 versión 1909 y 1903.

| | |
|---|---|
| Fuentes de información | https[://]thehackernews.com/2020/06/SMBleed-smb-vulnerability.html |

# Índice alfabético

botnet ..... 12, 13
Código malicioso ..... 6, 7, 8, 12
Correo electrónico ..... 8, 12
Correo electrónico, redes sociales, entre otros ..... 12
DDoS ..... 10
Exploits ..... 7
Explotación de vulnerabilidades conocidas ..... 5, 14
Fraude ..... 3, 4, 9
hxxp ..... 3
Intento de intrusión ..... 5, 14
internet ..... 3
malware ..... 2, 6, 8, 13
Malware ..... 6, 8
phishing ..... 2, 3, 4, 9
Phishing ..... 3, 4, 9
puerto ..... 11, 14, 15
ransomware ..... 2, 5, 6, 12, 13
Ransomware ..... 12
Reconocimiento de información ..... 10, 11
Red, internet ..... 3, 5, 10
redes sociales ..... 1, 4, 5, 8, 13
Redes sociales ..... 4, 9
Redes sociales, SMS, correo electrónico, videos de internet, entre otros ..... 4, 9
servidor ..... 4, 7, 11, 14, 15
servidores ..... 6
software ..... 3, 8, 9, 13
URL ..... 3
USB, disco, red, correo, navegación de internet ..... 6, 7
Vulnerabilidad ..... 2, 10, 11, 14, 15