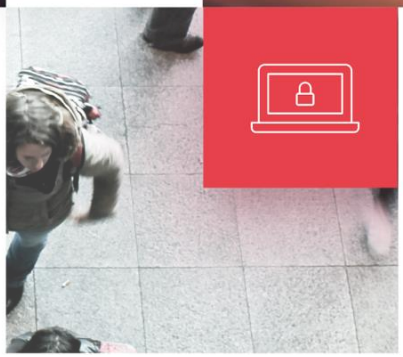
PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

ALERTA INTEGRADA DE SEGURIDAD DIGITAL



asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Lima, 30 de julio de 2021

N° 190-2021-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 y Transformación Digital de la Presidencia del Consejo de Ministros, en el marco de la Seguridad Digital del Estado Peruano.

El objetivo de esta alerta **es informar a los responsables de la seguridad digital de las entidades públicas y las empresas privadas sobre las amenazas en el entorno digital** 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 con 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.

Contenido

Windows Server, vulnerable a ataque de retransmisión NTLM.....3
Vulnerabilidad Oday de RCE en el servicio Print Spooler de Microsoft Windows. 4
Vulnerabilidad de escalamiento de privilegios del dispositivo de seguridad web de Cisco.....5
Propagación del troyano Vultur mediante app Protection Guard 7
Índice alfabético 9

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 190	Fecha: 30-07-2021
		Página: 3 de 9

Componente que reporta	**COMANDO OPERACIONAL DE CIBERDEFENSA DEL COMANDO CONJUNTO DE LAS FUERZAS ARMADAS**		
Nombre de la alerta	Windows Server, vulnerable a ataque de retransmisión NTLM		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	ECV
Medios de propagación	Red, internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. Resumen:

   A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó una vulnerabilidad de severidad crítica denominada PetitPotam, que podría permitir a un atacante remoto acceder a información de autenticación NTLM u otros certificados de autenticación, y tomar el control de los equipos de una red.

   El nuevo ataque utiliza el protocolo remoto del sistema de archivos de cifrado de Microsoft (EFSRPC) para obligar a un dispositivo y controladores de dominio, a autenticarse en una retransmisión NTLM remota controlada por un actor de amenazas. Una vez que un dispositivo se ha autenticado en un servidor NTLM malintencionado, el atacante puede robar hash y certificados que se pueden usar para hacerse cargo de la identidad y los privilegios del dispositivo.

2. Detalles:

   Una vulnerabilidad en el sistema operativo de Windows podría permitir a un atacante remoto desarrollar un ataque de retransmisión NTLM, mediante el abuso del protocolo MS-EFSRPC, para recopilar información de autenticación NTLM u otros certificados de autenticación y así, acceder y tomar el control de los equipos de una red.

3. Productos afectados
   - Windows Server 2012
   - Windows Server 2008
   - Windows Server 2016
   - Windows Server 20H2
   - Windows Server 2004
   - Windows Server 2019

4. Recomendaciones:
   - Desactivar la autenticación NTLM en el controlador de dominio de Windows
   - Desactivar NTLM en cualquier servidor AD CS mediante políticas de grupo
   - Mantener activas y actualizadas las herramientas de protección, como el antivirus, antimalware, etc.
   - Mantener actualizado el sistema operativo

Fuentes de información	https://www.incibe-cert.es/alerta-temprana/avisos-seguridad/windows-server-vulnerable-ataque-retransmision-ntlm

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 190	Fecha: 30-07-2021
		Página: 4 de 9

Componente que reporta	**CIBERDEFENSA Y TELEMÁTICA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	Vulnerabilidad Oday de RCE en el servicio Print Spooler de Microsoft Windows.		
Tipo de ataque	Ransomware	Abreviatura	Ransomware.
Medios de propagación	Correo electrónico, redes sociales, entre otros		
Código de familia	C	Código de subfamilia	C01
Clasificación temática familia	Codigo Malicioso.		

Descripción

1. El 29 de julio de 2021, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se tomo conocimiento através de la información publicada por “bleepingcomputer” y de “Kaspersky”, dando a conocer un tipo de ransomware que cifra los dominios de windows.

   Los ataques con LockBit comenzaron originalmente en septiembre de 2019,cuando fue apodado el virus ".abcd". El moniker era en referencia al nombre de extensión de archivo utilizado al cifrar los archivos de una víctima. Entre los objetivos anteriores notables figuran organizaciones de los Estados Unidos, China, la India, Indonesia y Ucrania. Además, varios países de Toda Europa (Francia, Reino Unido, Alemania) han sido testigos de ataques

   Una nueva versión de la LockBit 2.0 ransomware se ha encontrado que automatiza el cifrado de un dominio de Windows mediante directivas de grupo de Active Directory.

2. Detalles:

   - LockBit ransomware es considerado por muchas autoridades para ser parte de la "LockerGoga & MegaCortex" familia de malware. Esto simplemente significa que comparte comportamientos con estas formas establecidas de ransomware dirigido. Como explicación rápida, entendemos que estos ataques son:
   - **Auto-difusión** dentro de una organización en lugar de requerir dirección manual.
   - **Dirigido** en lugar de propagarse de una manera scattershot como el malware de spam.
   - **Uso de herramientas similares** para propagar, como Windows Powershell y bloque de mensajes de servidor (SMB).
   - LockBit es un nuevo ataque de ransomware en una larga línea de ciberataques de extorsión. Anteriormente conocido como "ABCD" ransomware, desde entonces se ha convertido en una amenaza única dentro del alcance de estas herramientas de extorsión. LockBit es una subclase de ransomware conocido como un 'virus cripto' debido a la formación de sus solicitudes de rescate en torno al pago financiero a cambio de descifrado. Se centra en las empresas y las organizaciones gubernamentales más que en los individuos.

3. Se recomienda:
   - Se deben implementar contraseñas seguras.
   - Activar la autenticación multifactor.
   - Asegúrese de que las configuraciones del sistema siguen todos los procedimientos de seguridad.
   - Vuelva a evaluar y simplifique los permisos de la cuenta de usuario.

Fuentes de información	▪ LockBit ransomware - ¿qué es y cómo mantenerse a salvo | Kaspersky ▪ LockBit ransomware ahora cifra los dominios de Windows utilizando políticas de grupo (bleepingcomputer.com)

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 190**	**Fecha: 30-07-2021**
		Página: 5 de 9

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad de escalamiento de privilegios del dispositivo de seguridad web de Cisco		
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. Resumen:

   Cisco ha reportado una vulnerabilidad de severidad ALTA de tipo falta de validación de entrada XML en la administración de la configuración de Cisco AsyncOS para Cisco Web Security Appliance (WSA). La explotación exitosa de esta vulnerabilidad podría permitir que un atacante remoto autenticado ejecutar comandos arbitrarios en el sistema operativo subyacente y elevar los privilegios a root.

2. Detalles:

   Esta vulnerabilidad registrada como CVE-2021-1359 se debe a una validación insuficiente de la entrada XML proporcionada por el usuario para la interfaz web. Un atacante podría aprovechar esta vulnerabilidad cargando archivos de configuración XML especialmente diseñados que contienen código de secuencia de comandos en un dispositivo vulnerable.

   Un exploit exitoso podría permitir al atacante ejecutar comandos arbitrarios en el sistema operativo subyacente y elevar los privilegios a root. Un atacante necesitaría una cuenta de usuario válida con derechos para cargar archivos de configuración para aprovechar esta vulnerabilidad.

3. Productos afectados:

   Esta vulnerabilidad afecta a Cisco AsyncOS para Cisco WSA, tanto a dispositivos virtuales como de hardware:

   - Cisco AsyncOS para Cisco WSA versiones 11.8 y anteriores;
   - Cisco AsyncOS para Cisco WSA versión 12.0, 12.5 y 14.0.

4. Solución:

   Cisco ha publicado actualizaciones de software que abordan esta vulnerabilidad. Se recomienda a los clientes que actualicen a una versión de software fija adecuada, como se indica en la siguiente tabla:

Cisco AsyncOS para la versión principal del dispositivo de seguridad web	Primera versión fija
11.8 y anteriores	11.8.4-004
12,0	12.0.3-005
12,5	12.5.2
14.0	No afectado.

La versión 12.5.2 será una versión de mantenimiento (MR) unos días después de la fecha de publicación de este aviso de seguridad.

Además, el software se podría actualizar a través de la red mediante las opciones de actualización del sistema en la interfaz web de Cisco WSA. Para actualizar un dispositivo mediante la interfaz web deberá realizar lo siguiente:

- Elegir “Administración del sistema”> “Actualización del sistema”;
- Hacer clic en Opciones de actualización;
- Elegir Descargar e instalar;
- Elegir la versión a la que desea actualizar;
- En el área de preparación de la actualización, elegir las opciones adecuadas;
- Hacer clic en Continuar para comenzar la actualización. Una barra de progreso muestra el estado de la actualización; Una vez completada la actualización, el dispositivo se reinicia.

Fuentes de información	hxxps://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-scr-web-priv-esc-k3HCGJZ

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 190	Fecha: 30-07-2021
		Página: 7 de 9

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Propagación del troyano Vultur mediante app Protection Guard		
Tipo de ataque	Troyanos	Abreviatura	Troyanos
Medios de propagación	USB, disco, red, correo, navegación de internet		
Código de familia	C	Código de subfamilia	C01
Clasificación temática familia	Código malicioso		

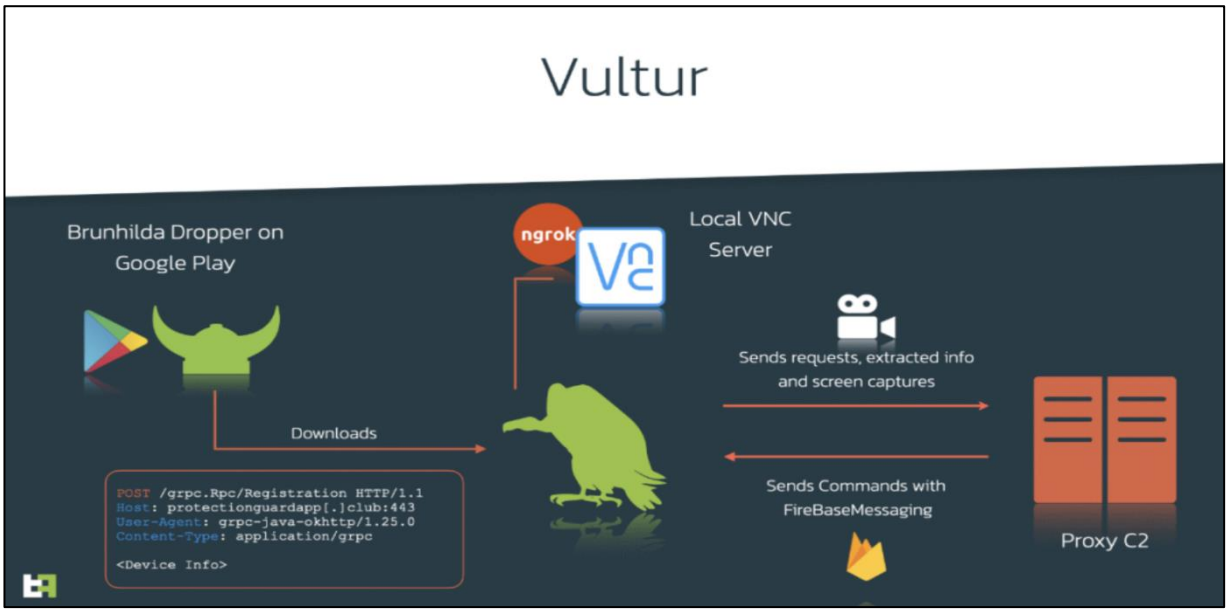
Descripción

1. Mediante del monitoreo y búsqueda de amenazas en el ciberespacio, se tomó conocimiento que a través de la plataforma de distribución digital de aplicaciones móviles para los dispositivos con sistema Android "Google Play Store" actores de amenazas vienen propagando el troyano bancario denominado **"Vultur"** por medio de la app "**Protection Guard**" con la finalidad de obtener información bancaria.

2. Vultur, troyano de acceso remoto (RAT) basado en Android, utiliza funciones de grabación de pantalla para robar información confidencial en el dispositivo, incluyendo credenciales bancarias y así abrir una puerta al fraude en el dispositivo, además el malware de Android cuenta con tecnología VNC (Computación Virtual en Red) para registrar y transmitir la actividad del teléfono inteligente de una víctima.

3. Vultur, como muchos troyanos bancarios de Android, depende en gran medida de los servicios de accesibilidad integrados en el sistema operativo móvil. Cuando se instala por primera vez, Vultur abusa de estos servicios para obtener los permisos necesarios para trabajar. Para hacer esto, el malware usa una superposición tomada de otras familias de malware. A partir de ese momento, Vultur monitorea todas las solicitudes que activan los servicios de accesibilidad, para ello solicita los siguientes permisos:
   - Acceso a la cámara
   - Información de la red
   - Instalación de paquetes requeridos
   - Permite que las aplicaciones deshabiliten el bloqueo del teclado si no es seguro.
   - Permite que las aplicaciones abran enchufes de red.

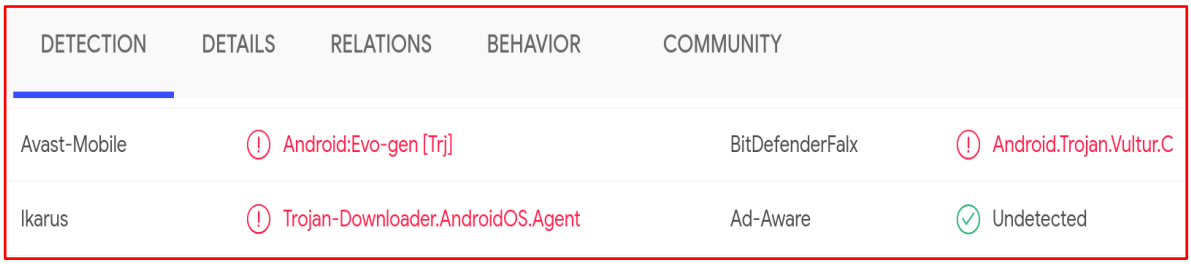
4. Una vez instalado, Vultur, inicia la grabación de la pantalla, utilizando la implementación de VNC (Computación Virtual en Red) de Alpha VNC. Para proporcionar acceso remoto al servidor VNC que se ejecuta en el dispositivo infectado, el malware usa ngrok2, una aplicación que usa un túnel encriptado para exponer los sistemas locales ocultos detrás de los firewalls a la Internet pública.



5. Información de la app Protection Guard

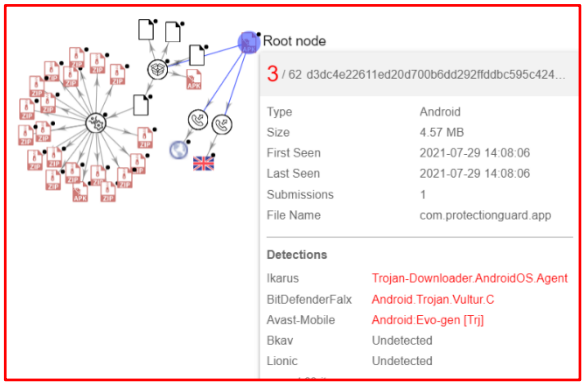
Nombre de paquete	com.protecctionguard.app	
Versión	1.0	
Tamaño	4.45 MB	
Requiere	Android 8.0	
Archivos por tipo	- PNG	304
	- XML	524
	- UNKNOWN	172
Objetivos	Dispositivos Android	

6. Se procedió analizar el aplicativo, Protection Guard, en las diferentes plataformas virtuales de seguridad digital, obteniendo como resultado que 03 compañías de seguridad informática reportan como **TROYANO.**



- **MD5:** b1b5eacc4d1cd7500e930286833f1626
- **SHA1:** bfae871e0c89814e133a6810276ff324d0bd376e
- **SHA256:** d3dc4e22611ed20d700b6dd292ffddbc595c42453f18879f2ae4693a4d4d925a
- **VHASH:** 5e8739af0601af68cea6dc9716293373

7. Topología:



8. Apreciación de la Información:

   Que los actores de amenazas a través de la plataforma de distribución digital de aplicaciones móviles para los dispositivos con sistema Android "Google Play Store", vienen propagando el troyano bancario denominado "Vultur" el cual vienen insertado en la app "Protection Guard", con la finalidad de obtener información bancaria.

9. Algunas Recomendaciones:
   - Desinstalar de los dispositivos de Android la aplicación mencionada en el presente reporte.
   - Desconfiar de programas ofrecidos en forma gratuita.
   - Mantener el antivirus actualizado.
   - Realizar las actualizaciones correspondientes desde fuentes originales.

Fuentes de información	Análisis propio de redes sociales y fuente abierta

Índice alfabético

Código malicioso 7
Correo electrónico 4
Correo electrónico, redes sociales, entre otros 4
Explotación de vulnerabilidades conocidas 3, 5
Intento de intrusión 3, 5
malware 4, 7
ransomware 4
Ransomware 4
Red, internet 3, 5
redes sociales 1, 8
servidor 3, 4, 7
software 5, 6
troyanos 7
Troyanos 7
USB, disco, red, correo, navegación de internet 7
Vulnerabilidad 4, 5