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

Siempre con el pueblo

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Centro Nacional de Seguridad Digital

asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ

Lima, 23 de noviembre de 2022

318-2022-CNSD

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 el Centro Nacional de Seguridad Digital de 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

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 318	Fecha: 23-11-2022
		Página 4 de 11

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Ataques contra VMs de Azure		
Tipo de ataque	Explotación de Vulnerabilidades	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de Intrusión		

Descripción

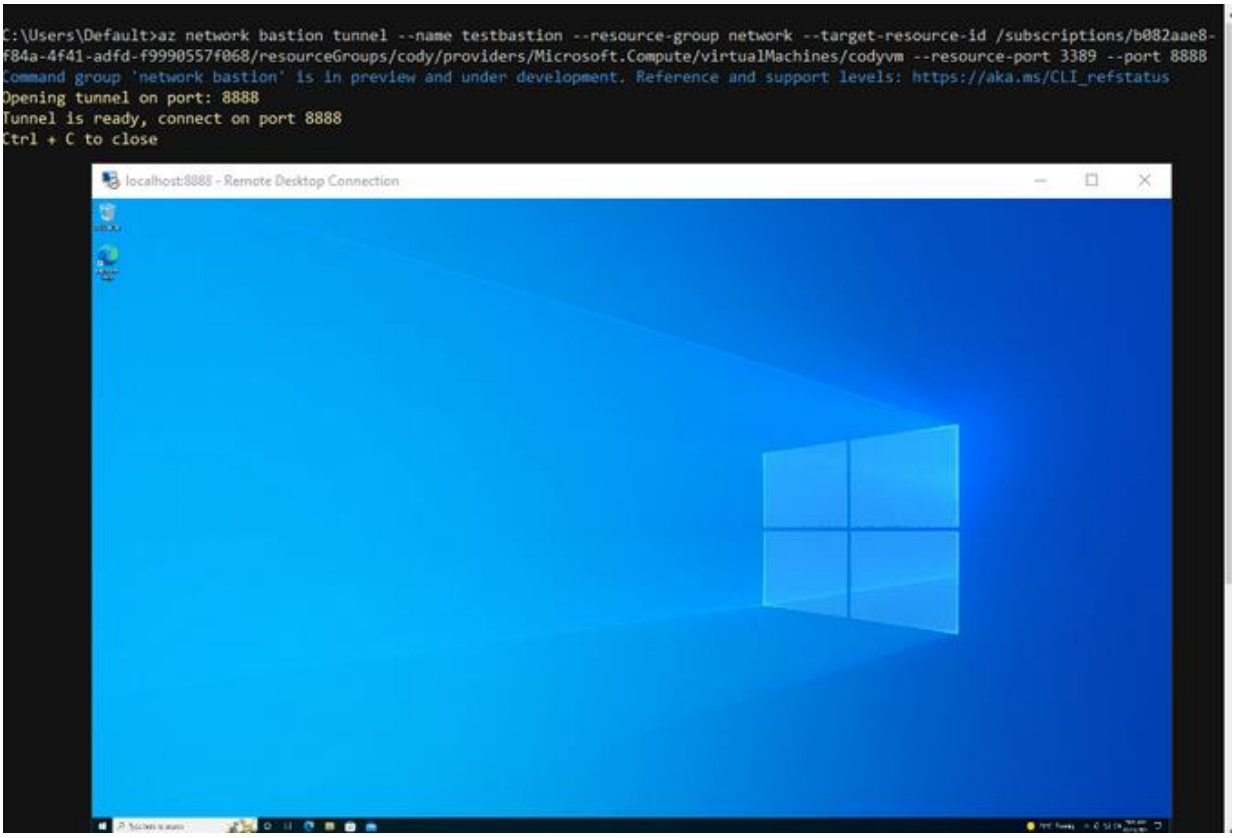
Actualmente los usuarios de Azure tienen la posibilidad de conectarse a sus servidores de bastionado mediante conexiones SSH y RDP con un cliente nativo o usando la interfaz web. Sin embargo, existe la posibilidad de realizar ataques contra VMs de Azure a través de Azure Bastion y su cliente nativo.

ANTECEDENTES:

- Según Microsoft, existen dos opciones mediante las que un usuario puede establecer una conexión con el cliente nativo hacia un servidor de bastionado. La que puede ser utilizada por un atacante es aquella en la que se pueden indicar un mayor número de opciones referentes a la conexión:

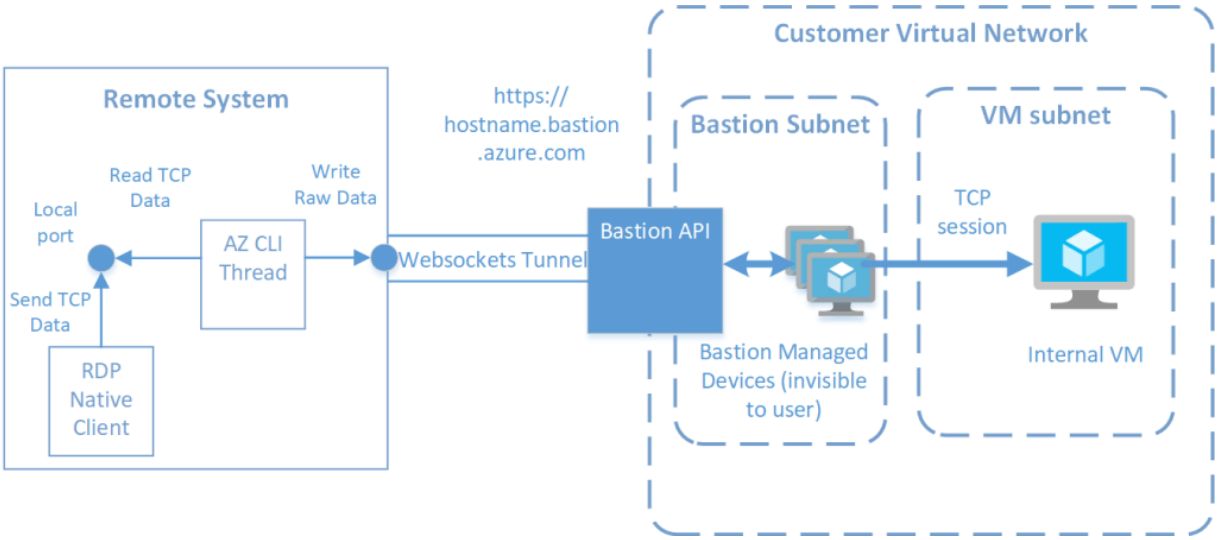
  az network bastion tunnel --name "" --resource-group "" --target-resource-id "" --resource-port "" --port ""

- Al ejecutar el comando anterior, Azure CLI crea un túnel y se pone a la escucha en un puerto local. Es al conectarse a este puerto local con el cliente nativo cuando el usuario gana acceso a la VM interna a través del protocolo utilizado (por ejemplo, RDP).



DETALLES:

- Para entender el proceso de ataque, primero es necesario ver cómo tiene lugar el flujo de trabajo del cliente nativo:



Fuente: Codyburked.com

- Tras recibir un comando vía API para iniciar una nueva sesión, Azure Bastion lleva a cabo tres acciones:
  - Crea una conexión TCP desde el servidor de bastionado hacia la VM del cliente, en el puerto especificado en la petición API.
  - Crea una nueva clave de sesión asociada a dicho puerto.
  - Acepta una nueva conexión websocket usando la clave de sesión, y transfiere toda la información de la conexión websocket a la conexión TCP de la VM interna.
- Del lado del cliente, Azure CLI hace lo siguiente:
  - Escucha en un puerto local.
  - Acepta nuevas conexiones en dicho puerto, y por cada conexión hace llamadas a la API del servicio de bastionado para iniciar una nueva sesión, tal y como se describió anteriormente.
  - Crea un nuevo hilo que transfiere toda la información recibida en la nueva conexión hacia el túnel websocket el servidor de bastionado.
- Así pues, al habilitar esta configuración los usuarios finales se pueden comunicar directamente con la VM interna a través de una conexión websocket, un proceso completamente diferente al de un servidor de bastionado tradicional, el cual se comunica tan solo a través del protocolo del servicio utilizado para el acceso remoto (RDP o SSH, en este caso).
- Además, el hecho de poder especificar un puerto implica que los servicios de la VM interna pueden ser escaneados usando Azure Bastion, y que los puertos que estén exponiendo servicios vulnerables pueden ser accedidos y explotados por cualquier persona que solicite una sesión de bastionado para una VM concreta.
- No obstante, para poder llevar a cabo ataques contra VMs de Azure a través de Azure Bastion el usuario en cuestión debe contar con una serie de permisos y requisitos previos:
  - Debe existir un rol Azure RBAC de lectura asignado a la VM.
  - Debe existir un rol Azure RBAC de lectura asignado a la NIC asociada con la dirección IP privada.
  - Debe existir un rol Azure RBAC de lectura asignado al servicio Azure Bastion.
  - La red debe incluir rutas que permitan que la subred de Azure Bastion se comunique con la VM, ya sea en la misma VNet o mediante VNet peering.

RECOMENDACIONES:

- Asegurarse de que la subred en la que Azure Bastion está desplegado tiene un grupo de seguridad de red (NSG) asociado, de manera que se limite la conectividad a los puertos 3389 y 22.
- Limitar el número de usuarios que tienen acceso RBAC de lectura a un recurso privilegiado.
- Incluir una regla de NSG en la subred de bastionado que limite la conectividad a una dirección IP específica o pequeños rangos de subredes.

Fuentes de información	▪ hxxps://thehackernews.com/2022/11/this-malware-installs-malicious-browser.html

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 318**	**Fecha: 23-11-2022**
		Página 7 de 11

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades críticas en productos “AVEVA Edge”		
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:**

El investigador Sam Hanson de Dragos, ha reportado múltiples vulnerabilidades de severidad CRÍTICA de tipo elemento de ruta de búsqueda no controlada, exposición de información confidencial a un actor no autorizado, consumo de recursos no controlados, control de acceso inadecuado y recorrido de ruta (Windows UNC Share) en el software HMI/SCADA AVEVA Edge. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto insertar archivos DLL maliciosos y engañar a la aplicación para que ejecute código arbitrario.

2. **Detalles:**

- La vulnerabilidad de severidad **alta** registrada como CVE-2016-2542 en las versiones R2020 y anteriores de AVEVA Edge, podría permitir a una entidad maliciosa con acceso al sistema de archivos lograr la ejecución de código arbitrario y la escalada de privilegios al engañar al paquete InstallShield de AVEVA Edge para que cargue una DLL no segura. Este ataque solo es posible durante la instalación o al realizar una operación de instalación o reparación.

- La vulnerabilidad de severidad **media** registrada como CVE-2021-42794 en las versiones R2020 y anteriores de AVEVA Edge podrían permitir el escaneo de la red interna y exponer información confidencial del dispositivo.

- La vulnerabilidad de severidad **crítica** registrada como CVE-2021-42796 en las versiones R2020 y anteriores de AVEVA Edge podrían permitir la ejecución de comandos arbitrarios no autenticados con el contexto de seguridad del proceso StADOSvr.exe. En la mayoría de los casos, será una cuenta de usuario con privilegios estándar con la que se inició el tiempo de ejecución de AVEVA Edge. Es posible que se haya configurado y asignado una cuenta de servicio con muchos privilegios para ejecutar el tiempo de ejecución de AVEVA Edge.

- La vulnerabilidad de severidad **alta** registrada como CVE-2021-42797 en las versiones R2020 y anteriores de AVEVA Edge podrían permitir que un actor no autenticado engañe al tiempo de ejecución de AVEVA Edge para que revele un token de acceso de Windows de la cuenta de usuario configurada para acceder a recursos de base de datos externos.

3. **Productos afectados:**

Las siguientes versiones del software HMI/SCADA AVEVA Edge afectadas son:

- 2020 R2 SP1;
- 2020 R2 SP1 con HF 2020.2.00.40;
- AVEVA Edge 2020 R2 y todas las versiones anteriores (anteriormente conocido como InduSoft Web Studio).

4. Solución:

- AVEVA recomienda actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad;
- Asimismo, recomienda que las organizaciones evalúen el impacto de estas vulnerabilidades en función del entorno operativo, la arquitectura y las implementaciones de productos;
- Los usuarios de AVEV Edge (anteriormente conocido como InduSoft Web Studio) hasta 2020 R2 SP1 con HF 2020.2.00.40 deben aplicar AVEVA Edge 2020 R2 SP2 lo antes posible;
- Restringir el acceso al puerto TCP/3.

Fuentes de información	▪ hxxps://www.cisa.gov/uscert/ics/advisories/icsa-22-326-01 ▪ hxxps://www.aveva.com/content/dam/aveva/documents/support/cyber-security-updates/SecurityBulletin_AVEVA-2022-006.pdf

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 318	Fecha: 23-11-2022
		Página 9 de 11

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Nueva campaña de phishing que tiene como objetivo acceder a la cuenta WhatsApp de la víctima.		
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		

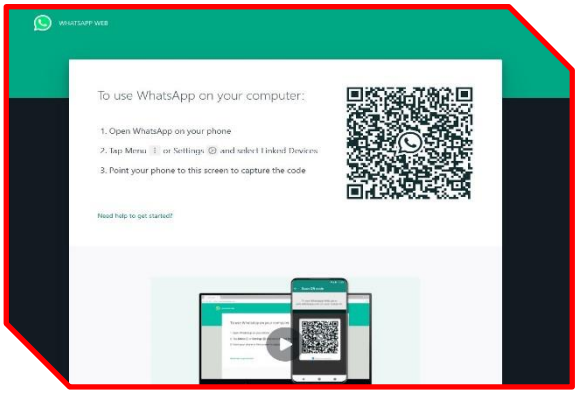
Descripción

1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes vienen llevando a cabo ataques de envió masivos de emails, dirigidas a usuarios de la aplicación de mensajería instantánea "WhatsApp", que, utilizando técnicas de ingeniería social, instan abrir un enlace malicioso adjunto en el mensaje, desde el navegador web de un computador, que mostrará un supuesto código QR de "WhatsApp Web", diseñado por los atacantes, para obtener acceso a la cuenta WhatsApp de la víctima, método que permite espiar y robar datos sensibles.

- Detalles del proceso de phishing.

Imagen 1: Engaño, supuesto "WhatsApp Web" a través del navegador de un computador u ordenador.

Imagen 2: Estafa, aparece un código QR de acceso falso que solicita escanear con el dispositivo móvil de WhatsApp.



- Comparación del sitio oficial de WhatsApp y sitio Falso:

SITIO OFICIAL
URL: https://www.whatsapp.com/

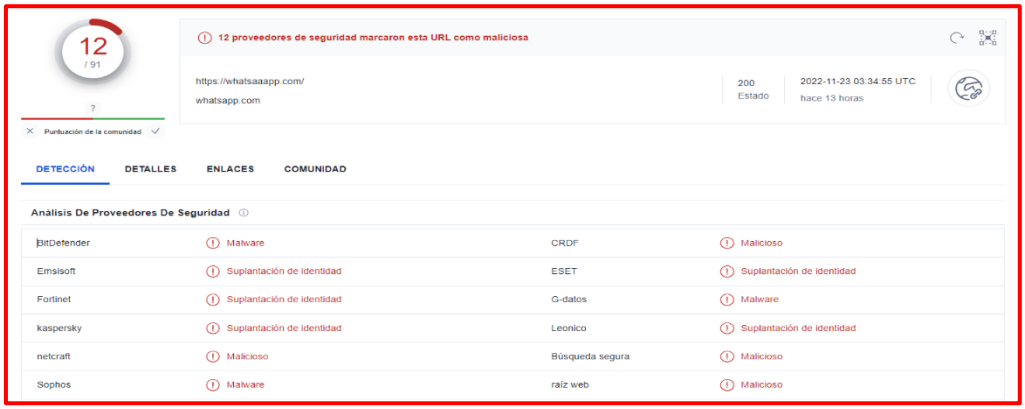
SITIO FRAUDULENTO
URL: hXXps[:]//whatsaaapp[.]com/

- Existe similitud en imagen de fondo, color y escritura.
- Tiene certificado de seguridad de protocolo HTTPS.
- El dominio se hace pasar por el sitio oficial, pero no coincide.

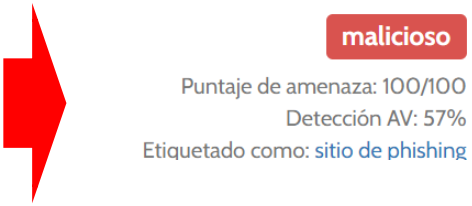
2. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD:**

- Indicadores de compromisos:

  - **URL:** hXXps[:]//whatsaaapp[.]com/
  - **Dominio:** whatsaaapp[.]com
  - **Dirección IP:** 8[.]218[.]129[.]22
  - **Código:** 200
  - **Longitud:** 202.85 KB
  - **SHA-256**: 99701020011be18dae5e99daa0b78d5af436ec0576613b548378aec74f3d946e



- Otras detenciones de análisis:



3. Phishing:

- Es un tipo de ataque de ingeniería social, que consiste en la utilización de envió masivo de email, los cuales se disfrazan para que parezcan proceder de una fuente de confianza. Estos emails están diseñados para engañar a las víctimas y conseguir que proporcionen información personal o financiera.

4. Recomendaciones:

- No ingresar a los enlaces de correos o mensajes de texto de dudosa procedencia.
- Evitar responder mensajes de remitentes desconocidos o que parezcan sospechosos.
- Verificar detenidamente en la redacción y ortografía del enlace, que coincidan con el sitio oficial.
- No compartir la información con terceras personas, amigos o familiares.
- Recordar hacer clic en el botón “Cerrar sesión”, cuando dejas de usar el servicio de WhatsApp.
- Utilizar un antivirus actualizado ya que es la primera barrera ante un ataque cibernético.

Fuentes de información	▪ Análisis propio de redes sociales y fuente abierta

Índice alfabético