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

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Asociación de Bancos del Perú

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

132-2025-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 Aéreadel 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 lasempresas 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°132	Fecha: 07-06-2025 Página: 4 de 7

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Campaña maliciosa distribuye malware a través de un sitio web falsificado de Bitdefender		
Tipo de Ataque	Troyanos	Abreviatura	Troyanos
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Código Malicioso		

Descripción

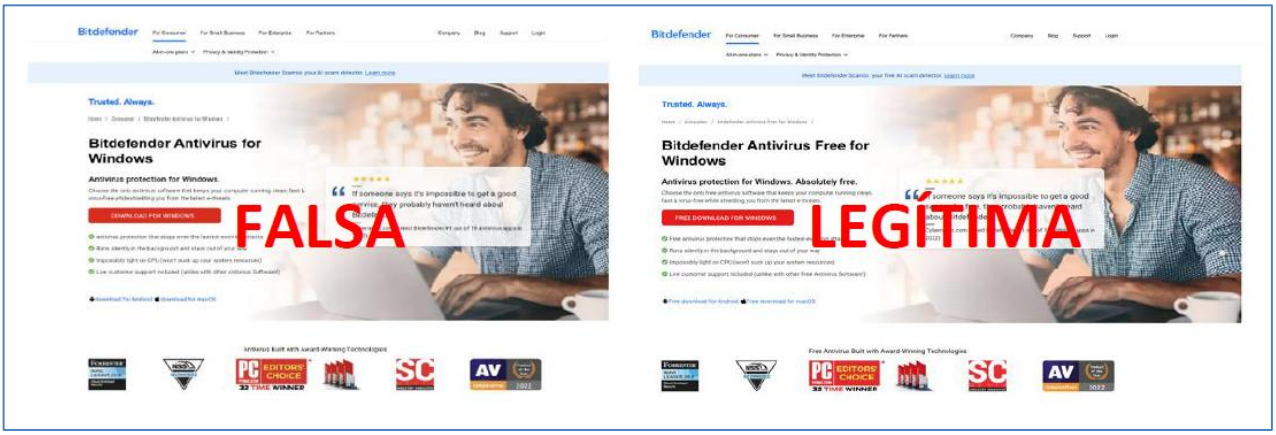
1. **ANTECEDENTES:**

Investigadores de ciberseguridad han revelado una nueva campaña maliciosa que utiliza un sitio web falso que anuncia software antivirus de Bitdefender para engañar a las víctimas para que descarguen un troyano de acceso remoto llamado Venom RAT.

2. **DETALLES:**

Esta campaña implica la propagación de tres programas de malware clave: VenomRAT, StormKitty y SilentTrinity, lo que representa una amenaza significativa para los usuarios al comprometer sus sistemas y robar información confidencial.

El sitio web en cuestión, "bitdefender-download[.]com", invita a los visitantes a descargar una versión para Windows del antivirus. Al hacer clic en el botón "Descargar para Windows", se inicia la descarga de un archivo desde un repositorio de Bitbucket que redirige a un bucket de Amazon S3.



La URL de Bitbucket es

“https[:]//bitbucket[.]org/sadsafsadfsadf/dsfgdsgssdfgdsg/downloads/BitDefender.zip”

la cual redirecciona a su fuente de contenido en Amazon S3.

“https[:]//bbuseruploads.s3.amazonaws[.]com/9e2daa63-bae3-4cbb-9f88-8154ba43261f/downloads/aa7b9593-2ccd-4cd0-9e04-9b4a7da9276b/BitDefender.zip”

La cuenta de Bitbucket ya no está activa.

El archivo ZIP ("BitDefender.zip") contiene un ejecutable llamado "StoreInstaller.exe", que incluye configuraciones de malware asociadas con Venom RAT, así como código relacionado con el marco de post-explotación de código abierto SilentTrinity y el ladrón StormKitty.

A alto nivel, las tres familias de malware funcionan de la siguiente manera:

- **VenomRAT** es un troyano de acceso remoto derivado del proyecto Quasar RAT, el cual proporciona acceso inicial y continuo a las máquinas de las víctimas. Permite a los cibercriminales obtener el control de sistemas Windows comprometidos, facilitando el robo de archivos, el keylogging, el acceso a cámaras web y la ejecución remota de comandos. Este malware se centra particularmente en robar información confidencial como credenciales de inicio de sesión, monederos de criptomonedas y datos bancarios, incluyendo información de tarjetas de crédito.
- **StormKitty** funciona como un recolector de credenciales, recopilando rápidamente datos confidenciales de los sistemas infectados.
- **SilentTrinity** es un framework de postexplotación de código abierto, facilita el acceso sigiloso a largo plazo y la exfiltración de datos, lo que permite posibles ataques repetidos.

La integración de estas herramientas de malware indica una estrategia dual: obtener ganancias financieras inmediatas y controlar persistentemente los sistemas de las víctimas, lo que permite a los atacantes operar con rapidez y pasar desapercibidos.

Indicadores de compromiso (IoC)

SHA256

- eb2b61a5f15b19bf7dd0ff3914d3019c26499dd693647b00c1b073037db72e35.
- 2d3dc51e6752c4fe95b2b7928ed11b5e06c6a68d19b7d884ab2c8eaab97d4e07.
- b1810daed3653b8c2047ff05a01a67d840ce045b17b39c60f335d798612e96aa.
- ab81ceeb26e22a7c6981a8479cccaa184675ad194b83e447185a1ce42abfbcb0.
- aa136a75b8fd954cf753c2c17fcde993b37b79af2f6b5a49556183e9f420fd56.
- f0e479cf0dadc7f7d1f999e091b013d236f2c7959591a6b1268ba31b89442ec6.
- 72b7856f3c6851a36642e952b4fb772b9ea0a6a4075c2ed4b59e60cb922f82e3.
- 7c3a49906e67a1928113554ff75f684ee54ab74abcf26ac1211d0cd8726cb086.
- 68f6ff2543066ec8028d9bc101a17a60c47b693bdc0ee4d6167f17d5d4921ab9.
- 4541fd01a19f1e484f24eff86f42ac36ea9b30686fd405ca0a50f3e517657a61.
- 505ab745198ddb59201abd0292af2b2bb0b6360d5807a2969c1518ae60a396c8.
- ab5e758b27ca23fb06cccb7a5d0e337757b30f5eb0093c03071792516e64ed76.
- 6c8d7f5c3d035f134b7d24594c0c409f1fce4bd460d0b2c634fe49c758c44b13.
- 47e1270376345760986d86218c23c66c74afec864fbf6f1d300a6f39ab13f341.
- 5129e8833504d66bb7332a60e1677697bf3a4ecb2f763acee926e4a6add24160.
- e07f8aa872a5bc6da07e6ddad3a3e9b7e1a57cec33b5bf16d6b56a150318fd81.
- 1b6ed428a5e8255860a44ed6ed3c06079625b6a35762f363029ccb1b322392d4.

IPs C2 de VenomRAT:

- 67.217.228[.]160:4449.
- 172.93.222[.]102:4449.
- 15.228.248[.]225:5552.
- 94.141.123[.]234:4449.
- 157.20.182[.]72:4449.
- 185.208.159[.]121:6000.
- 109.248.144[.]175:4449.
- 95.216.115[.]242:9090.

Direcciones IP adicionales con las mismas configuraciones:

- 157.20.182[.]35.
- 185.23.253[.]204.
- 157.20.182[.]68.

- 185.23.253[.]138.
- 157.20.182[.]167.
- 212.232.22[.]77.
- 157.20.182[.]72.

Sitios de entrega:

- bitdefender-download[.]com.
- hxxp[:]//185.156.72[.]2/files/5297474040/aNXlZBn.exe.
- hxxps[:]//github[.]com/legendary99999/fbvsfdbafdbdqba/releases/download/fdbagbagdbad/adsqwe.exe/.
- hxxps[:]//bitbucket[.]org/sadsafsadfsadf/dsfgdsgssdfgdsg/downloads/BitDefender.zip.
- hxxps[:]//bbuseruploads.s3.amazonaws[.]com/9e2daa63-bae3-4cbb-9f88-8154ba43261f/descargas/aa7b9593-2ccd-4cd0-9e04-9b4a7da9276b/BitDefender.zip.

3. RECOMENDACIONES:

- Bloquear los indicadores de compromisos (IOC) mostrados, en los dispositivos de seguridad de su
- infraestructura.
- Mantener actualizado el sistema operativo, software de seguridad y aplicaciones para protegerse contra vulnerabilidades explotadas por este malware.
- Utilizar software antimalware confiable y actualizado para detectar y eliminar amenazas como "VenomRAT".
- Evitar abrir archivos adjuntos o enlaces sospechosos en correos electrónicos no verificados, especialmente aquellos que aparentan ser pruebas de concepto o exploits.
- Implementar herramientas de monitoreo de red y sistemas para detectar actividades sospechosas o anómalas.
- Implementar un filtrado de correo electrónico sólido para bloquear los intentos de phishing.
- Concientizar al personal sobre temas relacionados a campañas de phishing e ingeniería social.

Fuente de Información:	• hxxps://thehackernews.com/2025/05/cybercriminals-clone-antivirus-site-to_4.html • hxxps://dti.domaintools.com/venomrat/ • hxxps://nquiringminds.com/cybernews/malicious-campaign-distributes-malware-via-spoofed-bitdefender-website/ • hxxps://securityaffairs.com/178366/malware/fake-antivirus-spreads-venom-rat.html • hxxps://www.infosecurity-magazine.com/news/fake-bitdefender-site-spreads/ • hxxps://therecord.media/fake-bitdefender-website-venomrat-infostealer

Índice alfabético