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, 04 de agosto de 2022

N° 210-2022-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° 210	Fecha: 04-08-2022
		Página 04 de 10

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Woody RAT, utiliza archivos ZIP y Follina		
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

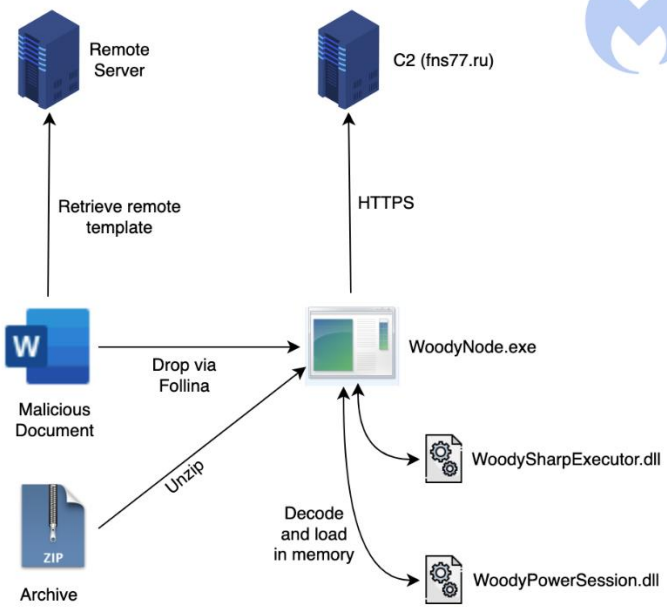
En una publicación realizada en agosto por "The Hacker News", se menciona que se ha identificado un nuevo troyano de acceso remoto (RAT), al que llamaron Woody RAT.

ANTECEDENTES:

- Este RAT personalizado avanzado es principalmente el trabajo de un actor de amenazas que apunta a entidades rusas mediante el uso de señuelos en formato de archivo y, más recientemente, documentos de Office que aprovechan la vulnerabilidad de Follina.

DETALLES:

- El equipo de Malwarebytes Threat Intelligence ha identificado un nuevo troyano de acceso remoto (RAT), al que pusieron de nombre Woody RAT, el cual ha estado en estado salvaje durante al menos un año.
- Woody RAT se ha distribuido utilizando dos formatos diferentes:
  - Archivos de archivo (las primeras versiones normalmente se distribuían en un archivo ZIP que pretendía ser un documento específico de un grupo ruso).
  - Documentos de Office utilizando la vulnerabilidad Follina (cuando la vulnerabilidad de Follina se dio a conocer en todo el mundo, el actor de amenazas cambió a ella para distribuir la carga útil).
- Según un dominio falso registrado por los actores de amenazas, intentaron apuntar a una entidad aeroespacial y de defensa rusa conocida como OAK.
- El siguiente diagrama muestra el flujo de ataque general utilizado por el actor de amenazas para propagar a Woody RAT:



Archivos comprimidos

- En este método, Woody RAT se empaqueta en un archivo y se envía a las víctimas. Estos archivos se han distribuido mediante correos electrónicos de phishing dirigido y estos son algunos ejemplos:
  - anketa_brozhik[.]doc[.]zip: contiene el ejecutable de Woody RAT con el mismo nombre.
  - zayavka[.]zip: Contiene Woody RAT haciéndose pasar por una aplicación válida.

Vulnerabilidades de Follina

- El actor de amenazas está utilizando un documento de Microsoft Office (*[.]docx) que se ha armado con la vulnerabilidad Follina (CVE-2022-30190) para descargar a Woody RAT. El señuelo utilizado en ruso se llama "Memo de seguridad de la información", que proporciona prácticas de seguridad para contraseñas, información confidencial, etc.

Indicadores de Compromiso (IoC)

- **Woody RAT**

982ec24b5599373b65d7fec3b7b66e6afff4872847791cf3c5688f47bfcb8bf0
66378c18e9da070629a2dbbf39e5277e539e043b2b912cc3fed0209c48215d0b
b65bc098b475996eaabbb02bb5fee19a18c6ff2eee0062353aff696356e73b7a
43b15071268f757027cf27dd94675fdd8e771cdcd77df6d2530cb8e218acc2ce
408f314b0a76a0d41c99db0cb957d10ea8367700c757b0160ea925d6d7b5dd8e
0588c52582aad248cf0c43aa44a33980e3485f0621dba30445d8da45bba4f834
5c5020ee0f7a5b78a6da74a3f58710cba62f727959f8ece795b0f47828e33e80
3ba32825177d7c2aac957ff1fc5e78b64279aeb748790bc90634e792541de8d3
9bc071fb6a1d9e72c50aec88b4317c3eb7c0f5ff5906b00aa00d9e720cbc828d

- **C2s**

kurmakata.duckdns[.]org
microsoft-ru-data[.]ru
194[.]36[.]189[.]179
microsoft-telemetry[.]ru
oakrussia[.]ru

- **Follina Doc:**

Памятка[.]docx
ffa22c40ac69750b229654c54919a480b33bc41f68c128f5e3b5967d442728fb

- **Archivo html de Follina:**

garmandesar[.]duckdns[.]org:444/uoqiuwef[.]html

- **Woody RAT url:**

Fcloud[.]nciinform[.]ru/main[.]css (edited)

RECOMENDACIONES:

- Los usuarios deben utilizar configuraciones robustas de seguridad.
- Tener políticas de seguridad ante malware actualizadas.
- Reforzar medidas de seguridad ante ataques de malware (herramientas de seguridad robustas)
- Realizar backups de información de carácter sensible y confidencial de manera periódica.
- No confiar ni abrir los archivos adjuntos y enlaces sospechosos.

Fuentes de información	▪ hxxps://blog.segu-info.com.ar/2022/08/woody-rat-utiliza-archivos-zip-y[.]html ▪ hxxps://thehackernews.com/2022/08/new-woody-rat-malware-being-used-to[.]html ▪ hxxps://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30190 ▪ hxxps://blog.malwarebytes.com/threat-intelligence/2022/08/woody-rat-a-new-feature-rich-malware-spotted-in-the-wild/ ▪ Análisis propio de fuentes abiertas.

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 210	**Fecha: 04-08-2022**
		Página 07 de 10

Componente que reporta	**CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	VirusTotal revela el software más suplantado en los ataques de malware		
Tipo de ataque	Malware	Tipo de ataque	Malware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de familia	C02
Clasificación temática familia	Código Malicioso		
Descripción			

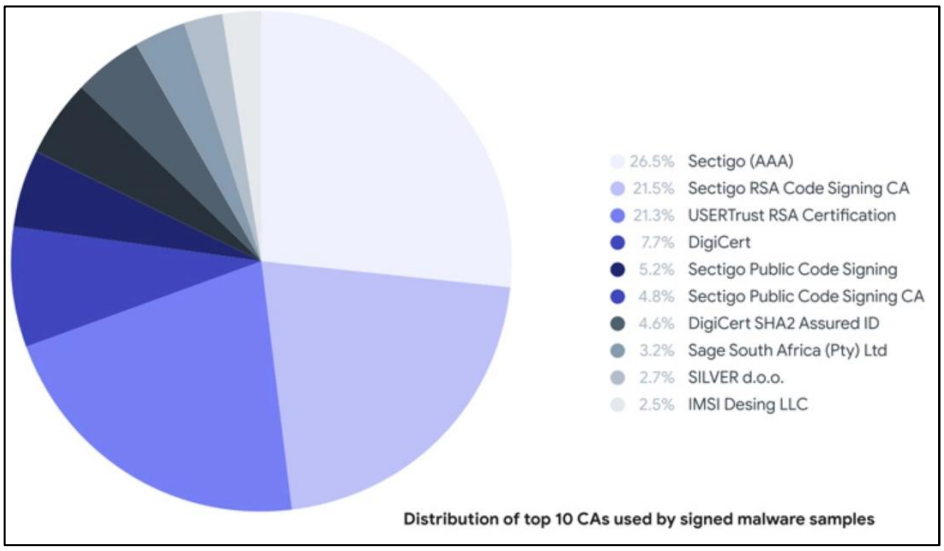
ANTECEDENTES

1. El 03 de agosto del 2022, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se tuvo conocimiento que, según reveló un análisis de VirusTotal, los actores de amenazas imitan cada vez más las aplicaciones legítimas como Skype, Adobe Reader y VLC Player como un medio para abusar de las relaciones de confianza y aumentar la probabilidad de un ataque de ingeniería social exitoso.
2. Otras aplicaciones legítimas más suplantadas por ícono incluyen 7-Zip, TeamViewer, CCleaner, Microsoft Edge, Steam, Zoom y WhatsApp.

MODO DE ATAQUE

3. Uno de los trucos de ingeniería social más simples que hemos visto consiste en hacer que una muestra de malware parezca un programa legítimo, El ícono de estos programas es una característica fundamental que se utiliza para convencer a las víctimas de que estos programas son legítimos
4. No sorprende que los actores de amenazas recurran a una variedad de enfoques para comprometer los puntos finales al engañar a los usuarios involuntarios para que descarguen y ejecuten ejecutables aparentemente inocuos.

   Esto, a su vez, se logra principalmente aprovechando los dominios genuinos en un intento por sortear las defensas de firewall basadas en IP. Algunos de los principales dominios abusados son discordapp[.]com, squarespace[.]com, amazonaws[.]com, mediafire[.]com y qq[.]com. En total, se han detectado no menos de 2,5 millones de archivos sospechosos descargados de 101 dominios pertenecientes a los 1000 principales sitios web de Alexa.
5. El mal uso de Discord ha sido bien documentado, ya que la red de entrega de contenido (CDN) de la plataforma se convirtió en un terreno fértil para alojar malware junto con Telegram, al tiempo que ofrece un "centro de comunicaciones perfecto para los atacantes".



6. Otra técnica utilizada con frecuencia es la práctica de firmar malware con certificados válidos robados a otros fabricantes de software. El servicio de escaneo de malware dijo que encontró más de un millón de muestras maliciosas desde enero de 2021, de las cuales el 87% tenía una firma legítima cuando se cargaron por primera vez en su base de datos.
7. VirusTotal dijo que también descubrió 1.816 muestras desde enero de 2020 que se hicieron pasar por software legítimo al empaquetar el malware en instaladores para otro software popular como Google Chrome, Malwarebytes, Zoom, Brave, Mozilla Firefox y Proton VPN. Dicho método de distribución también puede resultar en un ataque a la cadena de suministro cuando los adversarios logran ingresar al servidor de actualización de un software legítimo u obtener acceso no autorizado al código fuente, lo que hace posible infiltrar el malware en forma de archivos binarios troyanos.
8. Alternativamente, los instaladores legítimos se empaquetan en archivos comprimidos junto con archivos con malware, en un caso que incluye el instalador legítimo de Proton VPN y el malware que instala el ransomware Jigsaw.
9. Eso no es todo. Un tercer método, aunque más sofisticado, implica incorporar el instalador legítimo como un recurso ejecutable portátil en la muestra maliciosa para que el instalador también se ejecute cuando se ejecuta el malware para dar la ilusión de que el software funciona según lo previsto.

RECOMENDACIÓN

En la industria de apps en el 2021, RPP noticias informó que Perú es de los países que más descarga en el mundo; por ello los usuarios están propensos a caer en estas técnicas de ciberataques; por ellos, se recomienda tomar medidas para evitar que el actor de la amenaza obtenga nuestra información:

- ✓ poner atención a los permisos de las aplicaciones
- ✓ desconfía de las aplicaciones que te piden una actualización dentro de la aplicación
- ✓ examina las aplicaciones con ojo crítico
- ✓ busca recomendaciones de fuentes confiables
- ✓ evita las tiendas de aplicaciones de terceros
- ✓ protege tu smartphone con software de seguridad
- ✓ actualiza el sistema operativo de tu teléfono

Fuentes de información	▪ https://thehackernews.com/2022/08/virustotal-reveals-most-impersonated.html

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 210**	**Fecha: 04-08-2022**
		Página 09 de 10

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad crítica en múltiples enrutadores DrayTek		
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 equipo de Trellix Threat Labs Vulnerability Research, ha reportado una vulnerabilidad de severidad CRÍTICA de tipo desbordamiento de búfer que afecta a múltiples enrutadores DrayTek. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto llevar a un compromiso total del dispositivo y provocar una violación de la red y el acceso no autorizado a los recursos internos.

2. **Detalles:**
   - La vulnerabilidad de severidad **crítica** identificada como CVE-2022-32548 en la interfaz de gestión web de los dispositivos vulnerables de DrayTek está afectada por un desbordamiento de búfer en la página de inicio de sesión en /cgi-bin/wlogin.cgi. Un atacante puede suministrar un nombre de usuario y/o una contraseña especialmente diseñados como cadenas codificadas en base64, dentro de los campos 'aa' y 'ab' de la página de inicio de sesión, provocando un error lógico en la verificación del tamaño de estas cadenas codificadas, lo que podría suponer el compromiso total del dispositivo o al acceso, no autorizado, a los recursos internos.
   - Los investigadores indicaron que el ataque se puede realizar sin la interacción del usuario si la interfaz de administración del dispositivo se ha configurado para estar orientada a Internet. También se puede realizar un ataque con un solo clic desde dentro de la LAN en la configuración predeterminada del dispositivo. El ataque puede llevar a un compromiso total del dispositivo y provocar una violación de la red y el acceso no autorizado a los recursos internos.

3. **Productos afectados:**
   - Vigor3910, versiones anteriores a la 4.3.1.1;
   - Vigor1000B, versiones anteriores a la 4.3.1.1;
   - Vigor2962 Series, versiones anteriores a la 4.3.1.1;
   - Vigor2927 LTE Series, versiones anteriores a la 4.4.0;
   - Vigor2915 Series, versiones anteriores a la 4.3.3.2;
   - Vigor2952 / 2952P, versiones anteriores a la 3.9.7.2;
   - Vigor3220 Series, versiones anteriores a la 3.9.7.2;
   - Vigor2926 LTE Series, versiones anteriores a la 3.9.8.1;
   - Vigor2862 LTE Series, versiones anteriores a la 3.9.8.1;
   - Vigor2620 LTE Series, versiones anteriores a la 3.9.8.1;
   - VigorLTE 200n, versiones anteriores a la 3.9.8.1;
   - Vigor2133 / 2762 Series, versiones anteriores a la 3.9.6.4;
   - Vigor167, versiones anteriores a la 5.1.1;
   - Vigor130, versiones anteriores a la 3.8.5;
   - VigorNIC 132, versiones anteriores a la 3.8.5;
   - Vigor165 / 166, versiones anteriores a la 4.2.4;
   - Vigor2135 / 2765 / 2766 Series, versiones anteriores a la 4.4.2;
   - Vigor2832, versiones anteriores a la 3.9.6;
   - Vigor2865 / LTE Series, versiones anteriores a la 4.4.0;
   - Vigor2866 / LTE Series, versiones anteriores a la 4.4.0;

4. **Solución:**
   DrayTek recomienda actualizar los productos afectados con la última versión de firmware disponible que corrige esta vulnerabilidad.

Fuentes de información	▪ hxxps://www.trellix.com/en-us/about/newsroom/stories/threat-labs/rce-in-dratyek-routers.html

Índice alfabético