Identificador
[Análisis Técnico]

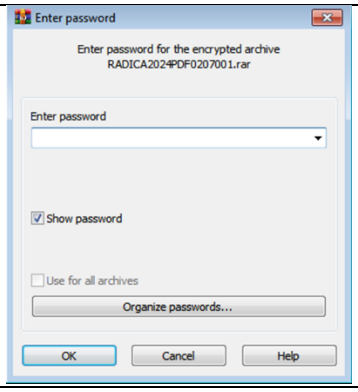
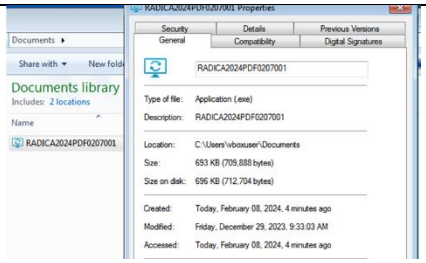
2024-02-22 | **Análisis Técnico Malware**

TLP:CLEAR

Análisis Técnico Malware AsyncRAT

No. INCIDENTE: [COLCERT IN-0221-2879]

Nivel de Riesgo **ALTO**

Nombre del archivo	RADICA2024PDF0207001.rar
Visualización de la descarga	 
MD5	272949643241D3183AEB92135D093FB6
SHA-1	442C2D0C9F765146988B70457FBE55034C9BE759
SHA-256	323B2A134FE2BE90D64F2FDFB1B55AA11170EF3F65F88A0E556E20E6CE1A1E47
Tipo de archivos relacionados	RAR archive data, v4, os: Win32
Extensión del archivo	.exe
Tamaño del archivo	696 KB (712.704 bytes)
Sistema Operativo	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Taxonomía	Contenido dañino – Configuración de malware
Tipo de Malware	Troyano de Acceso Remoto

Nombre conocido	AsyncRAT
Descripción	Malware que monitorea y controla remotamente sistemas infectados. Este malware se introdujo en Github como un software legítimo de administración remota de código abierto, pero los ciberdelincuentes lo utilizan por sus numerosas y potentes funciones maliciosa, se filtra en los dispositivos para entregar cargas útiles maliciosas, infecta los equipos de cómputo de las víctimas, analiza la información de su sistema. Los ciberdelincuentes suelen entregar cargadores a través de correos electrónicos y enlaces de phishing, basándose en la ingeniería social para engañar a los usuarios para que descarguen y ejecuten sus ejecutables. Los cargadores emplean tácticas avanzadas de evasión y persistencia para evitar ser detectados.
Modo de análisis	Sandbox
Comportamiento gráfico	
	Actividades y/o modificaciones registradas por el malware NOTA: El equipo de TI debe verificar en todos los activos de información relacionados con el correo sospechoso, la siguiente información
Actividad interna en Windows al ejecutar el malware	• C:\Users\admin\AppData\Local\Temp\RADICA2024PDF0207001.exe • C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
	<u>Explicación de la actividad de cada uno de los archivos</u>
	C:\Users\admin\AppData\Local\Temp\RADICA2024PDF0207001.exe Comportamiento del malware e intenciones: • Ubicación en el sistema: El archivo se encuentra en la carpeta Temp del usuario "admin". La carpeta Temp es comúnmente utilizada por aplicaciones y procesos de Windows para almacenar archivos temporales. Los malwares, incluyendo los RATs, a menudo se colocan en esta carpeta porque los archivos temporales son menos propensos a ser inspeccionados por los usuarios y pueden ser borrados fácilmente, ayudando al malware a permanecer oculto. • Nombre del archivo: El nombre "RADICA2024PDF0207001.exe" parece estar diseñado para disfrazarse como un archivo PDF legítimo, posiblemente relacionado con un evento o documento específico ("RADICA2024"). Sin embargo, la extensión ".exe" indica que es un archivo ejecutable de Windows. Este tipo de engaño se utiliza para convencer a los usuarios de abrir el archivo, pensando que es un documento inofensivo, cuando en realidad es un programa malicioso. • Función y propagación: Una vez ejecutado, AsyncRAT puede realizar varias acciones maliciosas sin el conocimiento del usuario. Puede robar credenciales,

	datos personales, enviar comandos al sistema infectado, y potencialmente propagarse a otros sistemas conectados a la red. El uso de archivos ejecutables disfrazados de documentos inofensivos es una técnica común de propagación.
	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe El uso de "C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe" en el contexto de AsyncRAT sugiere una táctica avanzada de evasión y persistencia por parte de los atacantes. AsyncRAT, como se mencionó anteriormente, es un troyano de acceso remoto que permite a los atacantes controlar máquinas infectadas, realizar vigilancia, robar datos y distribuir más malware. Veamos cómo este camino específico y el archivo involucrado encajan en las operaciones de un malware: Ubicación y Archivo Utilizado • Ubicación Estándar: El archivo "aspnet_compiler.exe" es una herramienta legítima que forma parte del .NET Framework de Microsoft, ubicada comúnmente en "C:\Windows\Microsoft.NET\Framework\v4.0.30319". Esta herramienta se utiliza para precompilar aplicaciones ASP.NET, lo que mejora el tiempo de inicio de la aplicación al eliminar la necesidad de una compilación en el primer acceso. • Abuso de Herramientas Legítimas: El hecho de que AsyncRAT esté asociado con "aspnet_compiler.exe" sugiere que los atacantes están utilizando técnicas de "Living off the Land" (LotL), que implican el uso de herramientas y procesos legítimos del sistema para llevar a cabo actividades maliciosas. Esto hace que el malware sea más difícil de detectar, ya que se esconde detrás de procesos que parecen legítimos. Comportamiento e Intenciones • Evasión: Al inyectar código malicioso en procesos legítimos o al reemplazar herramientas legítimas con versiones maliciosas, el malware puede evadir soluciones de seguridad que de otra manera lo detectarían como malicioso. La detección basada en el comportamiento y la reputación del archivo puede no ser efectiva si el archivo malicioso se ejecuta desde un directorio de confianza o imita a una herramienta legítima. • Persistencia: Utilizar componentes del sistema operativo o del framework de desarrollo para ejecutar el malware puede facilitar la persistencia del mismo en el sistema infectado. Esto se debe a que las herramientas legítimas, como "aspnet_compiler.exe", a menudo están configuradas para ejecutarse en determinadas circunstancias o pueden ser manipuladas para ejecutar código adicional sin levantar sospechas. • Propagación y Acciones Maliciosas: Una vez establecido en el sistema, AsyncRAT puede realizar una amplia gama de acciones, desde el robo de datos hasta la instalación de ransomware o la creación de botnets. La intención detrás de usar una herramienta como "aspnet_compiler.exe" es mantener estas actividades ocultas el mayor tiempo posible. <u>Protección y Mitigación</u>

<table>
<tr><td></td><td>

Monitoreo y Análisis del Comportamiento: Las soluciones de seguridad modernas incluyen el monitoreo del comportamiento de los archivos y procesos para detectar anomalías, incluso si se utilizan herramientas legítimas.
Actualizaciones y Parches: Mantener el sistema y el software de seguridad actualizados es crucial para protegerse contra las tácticas, técnicas y procedimientos (TTP) conocidos utilizados por los atacantes.
Educación en Seguridad: La concienciación sobre las tácticas de engaño, como el phishing, que a menudo se utiliza para inicialmente comprometer un sistema, es una defensa crítica contra este tipo de ataques.

Si se detecta actividad sospechosa relacionada con "aspnet_compiler.exe" o cualquier otro proceso legítimo, es importante realizar una investigación detallada para determinar si se trata de una actividad legítima o de un abuso por parte de actores maliciosos. Las herramientas de seguridad avanzadas y los equipos de respuesta a incidentes pueden ayudar a identificar y mitigar estas amenazas.
</td></tr>
<tr><td>Dropped files

Archivos descargados por un malware</td><td>En el contexto de un AsyncRAT se refiere a los archivos que el malware crea o descarga en el sistema infectado como parte de su proceso de infección y operación. Estos pueden incluir archivos ejecutables adicionales, scripts, documentos configurados para realizar tareas específicas (como establecer comunicación con el servidor de comando y control, espiar al usuario, robar datos, etc.), o cualquier otro tipo de archivo que el RAT necesite para funcionar correctamente o para llevar a cabo sus objetivos maliciosos. El término "dropped" se utiliza porque el malware "suelta" estos archivos en el sistema, a menudo en carpetas específicas, para asegurar su persistencia, evasión y la ejecución de diversas actividades maliciosas.</td></tr>
<tr><td>Verificar en las siguientes rutas, para detectar archivos descargados por el malware</td><td>
<table>
<tr><th>NO.</th><th>Process</th><th>Filename</th><th>Type</th><th>MD5:</th><th>SHA256:</th></tr>
<tr><td>1</td><td>RADICA2024PDF02070 01.exe</td><td>C:\Users\admin\ AppData\Roaming\Kvcofs.exe</td><td>executable</td><td>272949643241D3183AEB92135D093FB6</td><td>323B2A134FE2BE90D64F2FDFB1B55AA11170EF3F65F88A0E556E20E6CE1A1E47</td></tr>
</table>
</td></tr>
<tr><td>Información del Malware

AsyncRAT</td><td>
<table>
<tr><td>Configuración Malware</td><td></td></tr>
<tr><td>AsyncRat</td><td></td></tr>
<tr><td>(PID) Process (548) aspnet_compiler.exe</td><td></td></tr>
<tr><td>C2 (1) sebastianmindioladomini.con-ip.com</td><td>sebastianmindioladomini.con-ip.com",

Hace referencia a un componente clave de la comunicación y operación de AsyncRAT o de cualquier otro malware que utilice una arquitectura cliente-servidor. Explicación brevemente cada parte:

C2: Se refiere a "Command and Control" (Comando y Control). Es el mecanismo mediante el cual los atacantes pueden comunicarse, enviar instrucciones y recibir datos del malware instalado en una máquina infectada. La infraestructura de C2 es crucial para la operatividad de muchos</td></tr>
</table>
</td></tr>
</table>

		tipos de malware, especialmente aquellos diseñados para permitir control remoto, como los RATs. (1): Este número probablemente indique la cantidad de servidores de comando y control identificados o la secuencia en la que se detectó este servidor en particular durante el análisis. sebastianmindioladomini.con-ip.com: Esta es la dirección del servidor de comando y control utilizado por el AsyncRAT. Es un dominio que ha sido identificado como parte de la infraestructura de comunicación del malware con su operador. Los dominios y direcciones IP asociados con servidores C2 a menudo se registran o se secuestran de manera que dificultan su rastreo y atribución a los atacantes. Utilizar nombres de dominio en lugar de direcciones IP directas permite a los atacantes cambiar rápidamente las direcciones IP subyacentes sin necesidad de modificar el malware distribuido, facilitando la evasión de listas negras y medidas de seguridad.
	Ports (1)	4040
	BotnetDefault	MIERCOLES
	Version|	0.5.7B
	Options	
	AutoRun	false
	Mute	Cookies
	InstallFolder%AppData%	
	BSoD	false
	AntiVM	false
	Certificates	MIIE8jCCAtqgAwIBAgIQAK8zaZwRZ+fUWJcLHGATZzANBgkqhkiG9w0BAQ0FADAaMRgwFgYDVQQDDA9Bc3luY1JBVCBTZXJ2ZXIwIBcNMjAwNTEyMTg0NTIwWhgPOTk5OTEyMzEyMzU5NTlaMBoxGDAWBgNVBAMMD0FzeW5jUkFUIFNlcnZlcjCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAMdIblOtWCpzNPqAOf1S+7vlC2kB/dxtq8f4H/YsqylaofoKNpxtFlRjT/B6NvNf7WO7iRO1Wv63...
		xVD/p4GpSkU4wCYsBAspHrCn4Qo8c15vIOQWDop6oRblmL8hMrj+WusVOA3TYaKehRnUfAUH28iCUfQAmV3K/RlWaifzCSh/IqmnEe2qzus3pe/lCjDdlt8lCxnVUW34xBZsI+Er3vSii1+ao5AnBt/NmsBRKnZNLRXEEQfiGuX5TDHkogqE4BTRU7l4q92z7XDzjPRQcZmJ4oZEmNmsb01rAXdX7KwBM2t5PYOR2TmENcD+2hH84oUWvDOmQ+Cy

<table>
<tr><td></td><td><table>
<tr><td></td><td>uRu9xoLVOFpaYSBs+xk44PuCbN1ilNYkmwVBQgEP/isZ...</td></tr>
<tr><td rowspan="2">Keys</td><td>6af530143bde335771122a0111fa375853589d3b656e8100b98e1551cf315019</td></tr>
<tr><td>bfeb1e56fbcd973bb219022430a57843003d5644d21e62b9d4f180e7e6c33941</td></tr>
</table></td></tr>
<tr><td>Ejecución de función legítima de Windows Media Player</td><td>"C:\Program Files\Windows Media Player\wmpnscfg.exe"

La ruta "C:\Program Files\Windows Media Player\wmpnscfg.exe" refiere al ejecutable de una función legítima de Windows Media Player. El archivo wmpnscfg.exe es un componente de Windows Media Player que se encarga de la configuración del servicio de compartir en red. Su función principal es permitir que Windows Media Player se inicie y se mantenga a la espera de compartir medios en la red.

Sin embargo, en el contexto de un análisis de malware como AsyncRAT, la presencia de esta ruta indica una táctica de evasión o persistencia por parte del malware. Los ciberdelincuentes frecuentemente camuflan sus malwares como archivos legítimos de Windows, o inyectan su código malicioso en procesos legítimos, por varias razones:

<u>Evasión</u>

• Difuminar entre procesos legítimos: Al ubicarse en carpetas de confianza y nombrarse como procesos legítimos, el malware intenta evitar ser detectado por usuarios y soluciones de seguridad. Los softwares de seguridad a menudo dan menos prioridad a los archivos ubicados en directorios de sistema legítimos, lo que puede ser aprovechado por los atacantes.

<u>Persistencia</u>

• Autoinicio: wmpnscfg.exe es un proceso que puede configurarse para ejecutarse automáticamente al iniciar Windows. Si el malware reemplaza este archivo por uno malicioso o modifica el registro para ejecutar su propio código, puede asegurar que se active cada vez que se inicia el sistema.

<u>Ejecución de Malware</u>

• Inyección de código o reemplazo de ejecutable: Si AsyncRAT modifica el archivo wmpnscfg.exe original o inyecta su código en el proceso en ejecución, puede ejecutar sus operaciones maliciosas bajo el disfraz de un proceso legítimo de Windows, lo que le permite operar sin ser detectado fácilmente.</td></tr>
<tr><td>Actividad de red</td><td><table>
<tr><th>Proceso</th><th>IP</th><th>Dominio</th><th>ISP</th></tr>
<tr><td>System</td><td>192.168.100.255:137</td><td></td><td></td></tr>
<tr><td>System</td><td>192.168.100.255:138</td><td></td><td></td></tr>
<tr><td>svchost.exe</td><td>224.0.0.252:5355</td><td></td><td></td></tr>
<tr><td>aspnet_compiler.exe</td><td>181.71.216.30:4040</td><td>sebastianmindioladomini.con-ip.com</td><td>Colombia Móvil</td></tr>
</table></td></tr>
</table>

<table>
<tr>
<td>solicitudes DNS (Sistema de Nombres de Dominio) realizadas por un AsyncRAT</td>
<td>
<table>
<tr><th>Dominio</th><th>IP</th><th>Reputación</th></tr>
<tr><td>sebastianmindioladomini.con-ip.com</td><td>181.71.216.30</td><td>malicious</td></tr>
<tr><td>dns.msftncsi.com</td><td>131.107.255.255</td><td>shared</td></tr>
</table>
Domain: sebastianmindioladomini.con-ip.com

IP: 181.71.216.30
Reputation: Malicious

Este dominio parece ser un servidor de comando y control (C&C o C2) para el AsyncRAT. La reputación "malicious" indica que fuentes de seguridad han identificado actividades maliciosas asociadas con este dominio, lo que significa que es utilizado por el malware para recibir instrucciones o exfiltrar datos. Las direcciones IP y dominios con mala reputación son señales claras de comunicación maliciosa.

Domain: dns.msftncsi.com

IP: 131.107.255.255
Reputation: Shared

dns.msftncsi.com es un dominio legítimo utilizado por Microsoft Windows para comprobar la conectividad a Internet. El servicio Network Connectivity Status Indicator (NCSI) realiza solicitudes a este dominio como parte de sus comprobaciones. La reputación "shared" indica que este dominio es utilizado por una amplia gama de usuarios y sistemas, tanto legítimos como potencialmente maliciosos, pero en este contexto, su uso es típicamente inofensivo.

<u>Análisis</u>

Comunicación con C&C: La solicitud DNS a sebastianmindioladomini.con-ip.com muestra el intento del malware de comunicarse con su servidor de comando y control. Esta es una actividad crítica para el RAT, ya que le permite recibir instrucciones y exfiltrar datos. Bloquear esta comunicación puede impedir que el malware funcione correctamente.

Uso de Infraestructura Legítima: La solicitud a dns.msftncsi.com sugiere que el AsyncRAT puede estar intentando verificar la conectividad a Internet o simular comportamiento legítimo para evitar la detección. El uso de solicitudes a servicios legítimos es una táctica común para mezclarse con el tráfico normal y dificultar la identificación del malware.
</td>
</tr>
<tr>
<td>Reputación IP</td>
<td>
<table>
<tr><th>IP</th><th>IPS</th><th>País - Ciudad</th><th>Lista Negra</th></tr>
<tr><td>181.71.216.30</td><td>tigo.com.co colombia movil s.a.</td><td>Colombia Valledupar</td><td>Spamhaus ZEN</td></tr>
</table>
</td>
</tr>
</table>

<table>
<tr><td>Ubicación IP</td><td> 

Proveedor de servicios de internet: Tigo Colombia
Nombre del servidor: com.co
País: Colombia, Departamento del Cesar, Valledupar
Región/Estado: Departamento del Cesar
Ciudad: Valledupar
Código de zona: 200001</td></tr>
<tr><td>Spamhaus ZEN</td><td>Combinación de todas las listas de bloqueo de IP basadas en la red (DNSBL) ofrecidas por The Spamhaus Project en un solo conjunto de consulta. ZEN significa "Zen Spamhaus", y es una herramienta utilizada por administradores de redes y servidores de correo electrónico para filtrar correos electrónicos no deseados (spam) y proteger contra amenazas relacionadas con direcciones IP maliciosas.</td></tr>
<tr><td>Amenaza</td><td><table>
<tr><th>Proceso</th><th>Etiqueta</th><th>Mensaje</th></tr>
<tr><td>svchost.exe</td><td>Potentially Bad Traffic</td><td>ET INFO DNS Redirection Service Domain in DNS Lookup (con-ip .com)</td></tr>
</table></td></tr>
<tr><td></td><td>Análisis de cada componente:

• Process: svchost.exe es un archivo ejecutable del sistema en Windows que hospeda o contiene servicios que se ejecutan desde bibliotecas de enlace dinámico (DLL). Dado que muchos servicios diferentes pueden ejecutarse bajo svchost.exe, es común ver múltiples instancias de este proceso en el Administrador de tareas. Los malwares, incluidos los RATs como AsyncRAT, a menudo se inyectan en este proceso o imitan su nombre debido a su naturaleza legítima y crítica, para ocultar su actividad maliciosa.

• Class: "Potentially Bad Traffic" indica que la actividad de red generada o asociada con este proceso se considera sospechosa o potencialmente maliciosa. No necesariamente confirma que la actividad es maliciosa, pero sí que merece una inspección más detallada debido a patrones conocidos de comportamiento malicioso.

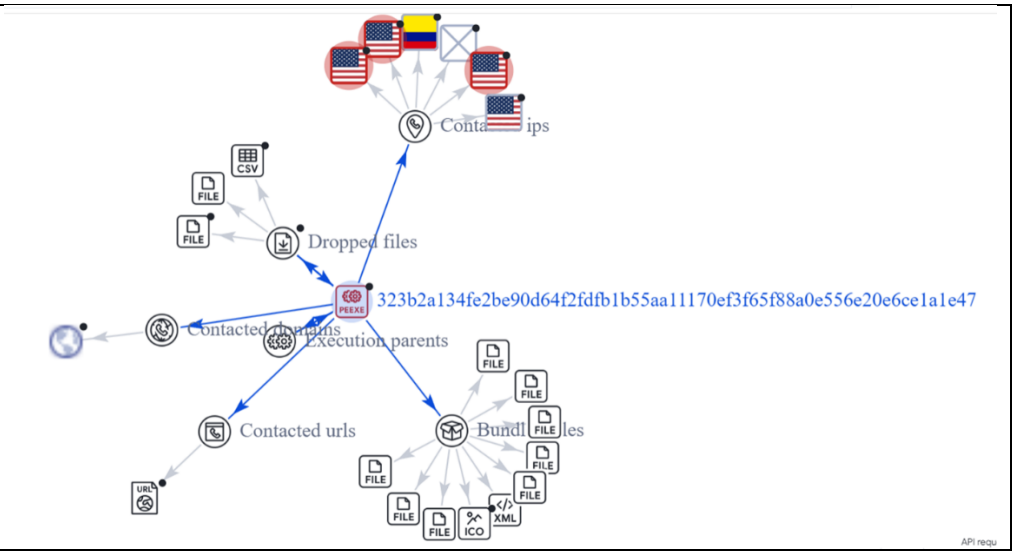
• Message: "ET INFO DNS Redirection Service Domain in DNS Lookup (con-ip .com)" es una alerta específica que señala que se realizó una consulta DNS para un dominio que es conocido por estar asociado con servicios de redirección de DNS o que forma parte de una infraestructura utilizada comúnmente por malwares. Los dominios "con-ip.com" se utilizan a menudo para la resolución dinámica de DNS, lo que puede permitir a los atacantes cambiar rápidamente las direcciones IP de sus servidores de comando y control para evitar ser detectados o bloqueados. Este tipo de alerta se genera basándose en firmas de detección de tráfico de red que reconocen patrones asociados con actividades maliciosas.

<u>Conclusión</u>

La alerta indica que un proceso legítimo de Windows (svchost.exe) está siendo utilizado para generar tráfico de red sospechoso, específicamente consultas DNS a un dominio asociado con actividades maliciosas. Esto sugiere que el malware AsyncRAT podría estar utilizando este proceso para comunicarse con su infraestructura de comando y control o para realizar actividades maliciosas, aprovechando la legitimidad del proceso svchost.exe para ocultar su presencia. Este tipo de comportamiento es característico de los malwares que buscan mantener una</td></tr>
</table>

	persistencia sigilosa en el sistema infectado mientras realizan sus operaciones maliciosas. La detección de este tipo de tráfico es crucial para identificar y mitigar la amenaza representada por el AsyncRAT y otros malwares similares.
Virus Total	 36 security vendors and 1 sandbox flagged this file as malicious 323b2a134fe2be90d64f2fdfb1b55aa11170ef3f65f88a0e556e20e6ce1a1e47 Dhostcsrybu.exe
Reporte de 36 antivirus	**Análisis de proveedores de seguridad**

AlibabaTrojanDownloader:MSIL/Seraph.d4ae90b1	KingsoftMalware.kb.c.780
AvastWin32:CrypterX-gen [Trj]	LionicTrojan.Win32.Seraph.a!c
AVGWin32:CrypterX-gen [Trj]	MaxSecureTrojan.Malware.300983.susgen
Avira (no cloud)TR/Dropper.MSIL.Gen	McAfeeArtemis!272949643241
Bkav ProW32.AIDetectMalware.CS	MicrosoftTrojan:MSIL/Seraph.DIAA!MTB
ClamAVWin.Trojan.EmbeddedDotNetBinary-9940868-0	Sangfor Engine ZeroSuspicious.Win32.Save.a
CrowdStrike FalconWin/malicious_confidence_90% (D)	SecureAgeMalicious
CybereasonMalicious.c9f765	SentinelOne (Static ML)Static AI - Malicious PE
CylanceUnsafe	Skyhigh (SWG)Artemis!Trojan
CynetMalicious (score: 100)	SophosMal/Generic-S
DeepInstinctMALICIOUS	SymantecML.Attribute.HighConfidence
DrWebTrojan.Inject4.30867	TencentWin32.Trojan.FalseSign.Adhl
ElasticMalicious (high Confidence)	TrapmineMalicious.moderate.ml.score
ESET-NOD32A Variant Of MSIL/GenKryptik.GTOJ	Trellix (FireEye)Generic.mg.272949643241d318
FortinetMSIL/Kryptik.AKVA!tr	TrendMicro-HouseCallTROJ_GEN.R06CH07B724
GoogleDetected	VirITTrojan.Win32.MSIL_Heur.A
IkarusTrojan.MSIL.Crypt	WithSecureTrojan.TR/Dropper.MSIL.Gen
KasperskyHEUR:Trojan-Downloader.MSIL.Seraph.gen	ZoneAlarm by Check PointHEUR:Trojan-Downloader.MSIL.Seraph.gen

Grafo Virus total	
Nombres	• Dhostcsrybu.exe • Kvcofs.exe • RADICA2024PDF0207001.exe
IOCs	http://ngcrhighosfrhpe/ http://xgdtkcedgsx/ http://vpktfwswoqqez/ 157[.]52[.]208[.]82/www[.]googleapis[.]com:443 sebastianmindioladomini.con-ip.com
	RADICA2024PDF0207001.exe (272949643241d3183aeb92135d093fb6)
	Dirección IP 181.71.216.30 Dirección IP 184.24.77.202

Mapeo MITRE ATT&CK™	
Técnicas	**Tácticas**
Ejecución - TA0002 El adversario está intentando ejecutar código malicioso. La ejecución consta de técnicas que dan como resultado la ejecución de código controlado por el adversario en un sistema local o remoto.	**Native API T1106** Los adversarios pueden interactuar con la interfaz nativa de programación de aplicaciones OS (API) para ejecutar comportamientos.
Persistencia TA0003 El adversario está tratando de mantener su punto de apoyo. La persistencia consiste en técnicas que los adversarios utilizan para mantener el acceso a los sistemas a través de reinicios, credenciales cambiadas y otras interrupciones que podrían cortar su acceso.	**Ejecución de inicio automático de inicio o inicio de sesión: claves de ejecución del registro/carpeta de inicioT1547.001** Los adversarios pueden lograr persistencia agregando un programa a una carpeta de inicio o haciendo referencia a él con una clave de ejecución del Registro.
Escalada Privilegio TA0004 técnicas que los adversarios utilizan para obtener permisos de nivel superior en un sistema o red. Los adversarios a menudo pueden ingresar y explorar una red con acceso sin privilegios, pero requieren permisos elevados para cumplir con sus objetivos	**Ejecución de inicio automático de inicio o inicio de sesión: claves de ejecución del registro/carpeta de inicioT1547.001** Los adversarios pueden lograr persistencia agregando un programa a una carpeta de inicio o haciendo referencia a él con una clave de ejecución del Registro.

Evasión de defensa - TA0005 La Evasión de Defensa consiste en técnicas que los adversarios utilizan para evitar la detección a lo largo de su compromiso. Las técnicas utilizadas para la evasión de defensa incluyen desinstalar/deshabilitar software de seguridad u ofuscar/cifrar datos y scripts.	**Archivos o Información OfuscadosT1027** Los adversarios pueden intentar hacer que un ejecutable o un archivo sea difícil de descubrir o analizar cifrando, codificando u ofuscando de otro modo su contenido en el sistema o en tránsito.
	Archivos o Información Ofuscados: Embalaje de Software T1027.002 Los adversarios pueden realizar el embalaje de software o la protección de software de máquina virtual para ocultar su código.
	Enmascaramiento: Cambiar el nombre de las utilidades del sistema - T1036 Los adversarios pueden cambiar el nombre de las utilidades legítimas del sistema para tratar de evadir los mecanismos de seguridad relacionados con el uso de esas utilidades.
	Virtualización/Evasión de Sandbox T1497 Los adversarios pueden emplear diversos medios para detectar y evitar entornos de virtualización y análisis. Esto puede incluir comportamientos cambiantes basados en los resultados de las verificaciones de la presencia de artefactos indicativos de un entorno de máquina virtual (VME) o sandbox.
	Defensas de Deterioro: Desactivar o Modificar Herramientas T1562.001 Los adversarios pueden modificar y/o deshabilitar las herramientas de seguridad para evitar la posible detección de su malware/herramientas y actividades.
	Carga de código reflectante T1620 Los adversarios pueden cargar código reflectivamente en un proceso para ocultar la ejecución de cargas útiles maliciosas.
Acceso Credencial – TA0006 El adversario está tratando de robar nombres de cuentas y contraseñas. El acceso a credenciales consiste en técnicas para robar credenciales como nombres de cuentas y contraseñas.	**Captura de Entrada T1056** Los adversarios pueden usar métodos para capturar la entrada del usuario para obtener credenciales o recopilar información.
Descubrimiento - TA0007 El adversario está tratando de descubrir su entorno.	**Descubrimiento Remoto del Sistema T1018** Los adversarios pueden intentar obtener una lista de otros sistemas por dirección IP, nombre de host u otro identificador lógico en una red que pueda usarse para Movimiento lateral del sistema actual.
	Descubrimiento de Información del Sistema T1082 Un adversario puede intentar obtener información detallada sobre el sistema operativo y el hardware, incluida

	la versión, los parches, las revisiones, los paquetes de servicio y la arquitectura.
	Virtualización/Evasión de Sandbox -T1497 Los adversarios pueden emplear diversos medios para detectar y evitar entornos de virtualización y análisis.
	Descubrimiento de software de seguridad - T1518.001 Los adversarios pueden intentar obtener una lista de software de seguridad, configuraciones, herramientas defensivas y sensores que están instalados en un sistema o en un entorno de nube. Esto puede incluir cosas como reglas de firewall y antivirus.
Colección TA0009 El adversario está tratando de recopilar datos de interés para su objetivo. La recopilación consiste en técnicas que los adversarios pueden usar para recopilar información y las fuentes de las que se recopila información que son relevantes para cumplir con los objetivos del adversario.	**Captura de Entrada - T1056** Los adversarios pueden usar métodos para capturar la entrada del usuario para obtener credenciales o recopilar información. Durante el uso normal del sistema, los usuarios a menudo proporcionan credenciales a varias ubicaciones diferentes, como páginas/portales de inicio de sesión o cuadros de diálogo del sistema.
Comando y control - TA0011 El adversario intenta comunicarse con los sistemas comprometidos para controlarlos.	**Puerto No Estándar- T1571** Los adversarios pueden comunicarse usando un protocolo y emparejamiento de puertos que normalmente no están asociados
	Protocolo de Capa de Aplicación - T1071 Los adversarios pueden comunicarse utilizando protocolos de capa de aplicación OSI para evitar la detección/filtrado de red mezclándose con el tráfico existente. Los comandos al sistema remoto, y a menudo los resultados de esos comandos, se incrustarán dentro del tráfico de protocolo entre el cliente y el servidor.
	Protocolo de Capa No Aplicable T1095 Los adversarios pueden usar un protocolo de capa de no aplicación OSI para la comunicación entre el host y el servidor C2 o entre los hosts infectados dentro de una red.
Capacidades	• Control Remoto: Los RATs permiten a los atacantes tomar el control remoto del sistema infectado. Esto incluye la capacidad de ver y manipular el escritorio, ejecutar comandos, y realizar diversas acciones en el sistema. • Captura de Teclas (Keylogging): Pueden registrar y enviar al atacante las teclas que se presionan en el teclado, lo que facilita la obtención de información confidencial, como contraseñas. • Captura de Pantalla: Pueden tomar capturas de pantalla del escritorio del sistema infectado, permitiendo al atacante ver la actividad del usuario.

	• Grabación de Audio y Video: Algunos RATs tienen la capacidad de activar la cámara y el micrófono del sistema para grabar audio y video sin el conocimiento del usuario. • Transferencia de Archivos: Permiten la transferencia de archivos entre el sistema infectado y el servidor controlado por el atacante. • Reinicio y Apagado Remotos: Algunos RATs pueden reiniciar o apagar el sistema de forma remota. • Persistencia: Pueden implementar mecanismos de persistencia para asegurarse de que el malware permanezca en el sistema incluso después de un reinicio. • Camuflaje: Pueden intentar ocultarse de los programas antivirus y de seguridad, utilizando técnicas de evasión.
Recomendaciones de protección de la infraestructura tecnológica	• Configurar herramientas de seguridad para detectar este tipo de amenazas de forma temprana, monitoreo del tráfico de red. • Concienciar a los colaboradores con el objetivo de identificar y alertar de manera inmediata mensajes sospechosos con el fin de evitar un posible ataque informático. • Mantener documentado los programas instalados en los equipos de cómputos identificando su función. • Mantener el antivirus actualizado. • Revisar de manera periódica el Backup (continuidad del negocio) de acuerdo con el procedimiento estandarizado. • No descargar ningún archivo adjunto desde páginas que no sean verificadas como confiables previamente. • Evitar suministrar información sensible como la dirección de correo en sitios web que no hagan parte de los servicios de la organización. • Evitar hacer clic sobre enlaces o hipervínculos adjuntos sobre correos de dudosa procedencia. • Revisar la dirección del remitente de los correos que recibe. • Recuerda verificar si anteriormente has recibido correos de la misma dirección. • Verificar la integridad de los archivos los archivos ejecutables de Java. Cualquier cambio inesperado podría ser indicativo de actividad maliciosa. • Monitoreo del Tráfico de Red, para identificar cualquier comunicación inusual desde o hacia el sistema. Algunos malware intentan comunicarse con servidores remotos para recibir comandos o enviar información. • Utilizar herramientas del sistema operativo o de terceros para examinar los procesos en ejecución y verificar si hay algún proceso relacionado con ese archivo DLL. • Implementar restricciones en la ejecución de archivos desde la carpeta Temporal para prevenir la ejecución de archivos maliciosos. • Validar las modificaciones realizadas por malware como AsyncRAT es crucial para asegurar la integridad y seguridad de un sistema. A continuación, te proporciono una serie de recomendaciones para validar y responder a las modificaciones sospechosas asociadas con archivos ejecutables mencionados, como "RADICA2024PDF0207001.exe" y el uso de "aspnet_compiler.exe" de manera potencialmente maliciosa. • Actividades que deben realizar el equipo de TI

Análisis Inicial

- Revisión de Logs: Revisa los registros de eventos del sistema y del firewall para detectar actividades inusuales, como conexiones de red desconocidas, ejecuciones de programas en momentos inusuales, etc.

- Análisis de Malware: Utiliza herramientas de análisis de malware (como VirusTotal) para escanear los archivos sospechosos y determinar si son conocidos por ser maliciosos.

Validación de Integridad

- Comparación de Hashes: Compara los hashes de los archivos mencionados con las versiones legítimas. Diferencias inesperadas pueden indicar modificaciones maliciosas.

- Verificación de Firmas Digitales: Verifica que los archivos ejecutables tengan firmas digitales válidas y que correspondan al editor esperado.

Análisis Forense

- Análisis de Comportamiento: Utiliza herramientas de análisis forense para monitorear el comportamiento de los archivos sospechosos en un entorno aislado (sandbox). Observa las acciones realizadas, como modificaciones en el registro, creación de archivos, y conexiones de red.

- Revisión del Registro: Verifica las claves de registro asociadas con la ejecución automática para identificar entradas inusuales o maliciosas. Las claves de registro a revisar incluyen, pero no se limitan a, Run, RunOnce, Startup folder entries, etc.

Respuesta y Mitigación

- Aislamiento del Sistema: Si se confirma actividad maliciosa, aísla el sistema afectado para prevenir la propagación del malware.

- Eliminación de Malware: Utiliza herramientas de eliminación de malware confiables para limpiar el sistema. Esto puede incluir la eliminación manual de archivos maliciosos, entradas de registro, y la restauración de configuraciones modificadas.

- Actualización de Seguridad: Asegúrate de que todos los sistemas operativos y aplicaciones estén actualizados para proteger contra vulnerabilidades conocidas.

- Educación y Prevención: Capacita a los usuarios sobre las amenazas de seguridad, incluyendo la ejecución de archivos desconocidos y la importancia de mantener prácticas de seguridad robustas.

Revisión del .NET Framework

- Dado que aspnet_compiler.exe es una herramienta legítima del .NET Framework, su uso indebido puede ser más difícil de detectar. Monitoriza la

	ejecución de esta herramienta para asegurarte de que se utilice de manera legítima y en contextos esperados. • Restauración de Configuraciones: Si se detectan modificaciones maliciosas, restaura las configuraciones del registro a valores de confianza o utiliza puntos de restauración del sistema si están disponibles. • Actualización y Parches: Asegúrate de que el sistema operativo, el navegador y todas las aplicaciones estén actualizadas con los últimos parches de seguridad para prevenir futuras vulnerabilidades.	
Pilar de seguridad de la información afectado	**Alto**	**Confidencialidad:** cuando el troyano de acceso remoto es ejecutado en un equipo, les permite a los actores detrás de la amenaza monitorear el sistema comprometido, de igual manera, capturar información sensible del usuario, sistema informático o entidad objetivo; esta información puede ser utilizada por los ciberdelincuentes para fraudes o ser expuesta en foros de la Deep y Dark web a disposición de otros cibercriminales
Conclusiones	• Se ha identificado y analizado minuciosamente una muestra específica del malware AsyncRAT, un peligroso troyano de acceso remoto. Este análisis incluyó la revisión de características técnicas clave, como firmas digitales, comportamiento operativo y estrategias de evasión y persistencia. Se utilizaron herramientas avanzadas de análisis, como entornos sandbox y plataformas de evaluación de seguridad como VirusTotal, para una comprensión detallada del malware. • AsyncRAT se disemina principalmente mediante técnicas de ingeniería social, engañando a los usuarios para que ejecuten archivos malintencionados que se hacen pasar por documentos legítimos. Una vez activo en un sistema, AsyncRAT es capaz de realizar diversas operaciones dañinas, como captura de teclado, grabación de pantalla, audio y video, así como el robo de datos personales y credenciales. Se resalta el uso estratégico de herramientas legítimas del sistema, como aspnet_compiler.exe, para camuflar su presencia, evidenciando la sofisticación de las tácticas de los atacantes. • El documento proporciona pautas detalladas para fortalecer la seguridad de las infraestructuras tecnológicas, subrayando la importancia de la concienciación de los usuarios, el mantenimiento constante de las actualizaciones de seguridad y la adopción de medidas preventivas y de detección temprana. Se enfatiza la relevancia del monitoreo y la validación de la integridad de los sistemas para detectar y responder a cambios maliciosos, empleando análisis forense y herramientas especializadas de análisis de malware. • El informe recalca la necesidad urgente de un enfoque integral y proactivo hacia la seguridad digital, combinando elementos de tecnología avanzada, educación continua y procesos estructurados de respuesta ante incidentes. Esta estrategia es fundamental para combatir eficazmente amenazas cibernéticas avanzadas como AsyncRAT. Se destaca especialmente la confidencialidad de la información como el aspecto de seguridad más comprometido, señalando las severas consecuencias del acceso no autorizado y la fuga de datos sensibles.	

Si tiene desea reportar un incidente de seguridad digital, puede comunicarse con el COLCERT como privado y al CSIRT Gobierno para entidades, a través de los siguientes canales:

 Bogotá: +57 601 344 22 22

 contacto@colcert.gov.co / csirtgob@mintic.gov.co

 @colCERT