Superintendencia FEDERAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

ANÁLISIS Y DETECCIÓN DE VULNERABILIDADES

Departamento CIBERSEGURIDAD

División SEGURIDAD INFORMÁTICA

Centro de Operaciones de Seguridad (SOC)

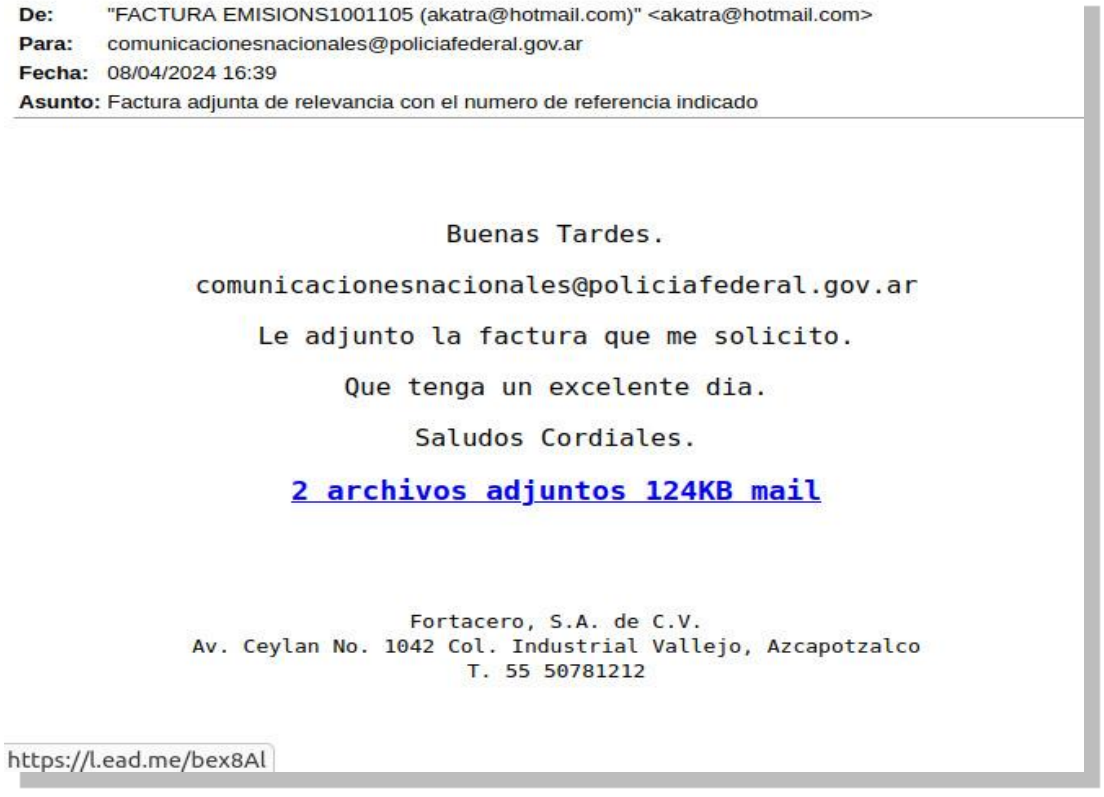
División COMUNICACIONES NACIONALES

Introducción

El día 08 de abril del corriente año, se recibió un correo electrónico proveniente de la cuenta comunicacionesnacionales@policiafederal.gov.ar perteneciente a la División COMUNICACIONES NACIONALES, donde recibe un mail el cual simula ser la descarga de una factura electrónica.

Desarrollo

Una vez identificado el caso, se procedió al análisis del correo proveniente de **"akatra@hotmail.com".** El mismo simula ser la empresa "Fortacero S.A." y dice adjuntar una factura solicitada por dicha Dependencia.



De: "FACTURA EMISIONS1001105 (akatra@hotmail.com)" <akatra@hotmail.com>
Para: comunicacionesnacionales@policiafederal.gov.ar
Fecha: 08/04/2024 16:39
Asunto: Factura adjunta de relevancia con el numero de referencia indicado

Buenas Tardes.

comunicacionesnacionales@policiafederal.gov.ar

Le adjunto la factura que me solicito.

Que tenga un excelente dia.

Saludos Cordiales.

2 archivos adjuntos 124KB mail

Fortacero, S.A. de C.V.
Av. Ceylan No. 1042 Col. Industrial Vallejo, Azcapotzalco
T. 55 50781212

https://l.ead.me/bex8Al

Imagen 1. Cuerpo del mail.

A continuación se procede a analizar el encabezado del mismo, el cual se puede observar que no se encuentra enmascarado siendo el remitente original akatra@hotmail.com

X-FEAS-SPF:	spf-result=pass, ip=40.92.22.109, helo=nam12-dm6-obe.outbound.protection.outlook.com, mailFrom=akatra@hotmail.com
X-FEAS-DKIM:	Valid
X-FEAS-Client-IP:	40.92.22.109
X-FE-Last-Public-Client-IP:	40.92.22.109
X-Spam-Processed:	policiafederal.gov.ar, Mon, 08 Apr 2024 16:39:05 -0300
X-FE-Envelope-From:	akatra@hotmail.com
X-FE-Policy-ID:	4:1:1:policiafederal.gov.ar
X-MDArrival-Date:	Mon, 08 Apr 2024 16:39:05 -0300
X-Rcpt-To:	comunicacionesnacionales@policiafederal.gov.ar
X-MDRcpt-To:	comunicacionesnacionales@policiafederal.gov.ar
X-Return-Path:	akatra@hotmail.com
X-Envelope-From:	akatra@hotmail.com
X-MDaemon-Deliver-To:	comunicacionesnacionales@policiafederal.gov.ar

Imagen 2. Encabezado.

Continuando con el análisis, dentro del cuerpo del mensaje, se puede observar un enlace, donde se redirecciona al sitio **"https://ilaymaxsk.fr-1.paas.massivegrid.net"** el cual contiene otro link, simulando descargar una factura electrónica en un archivo .PDF.

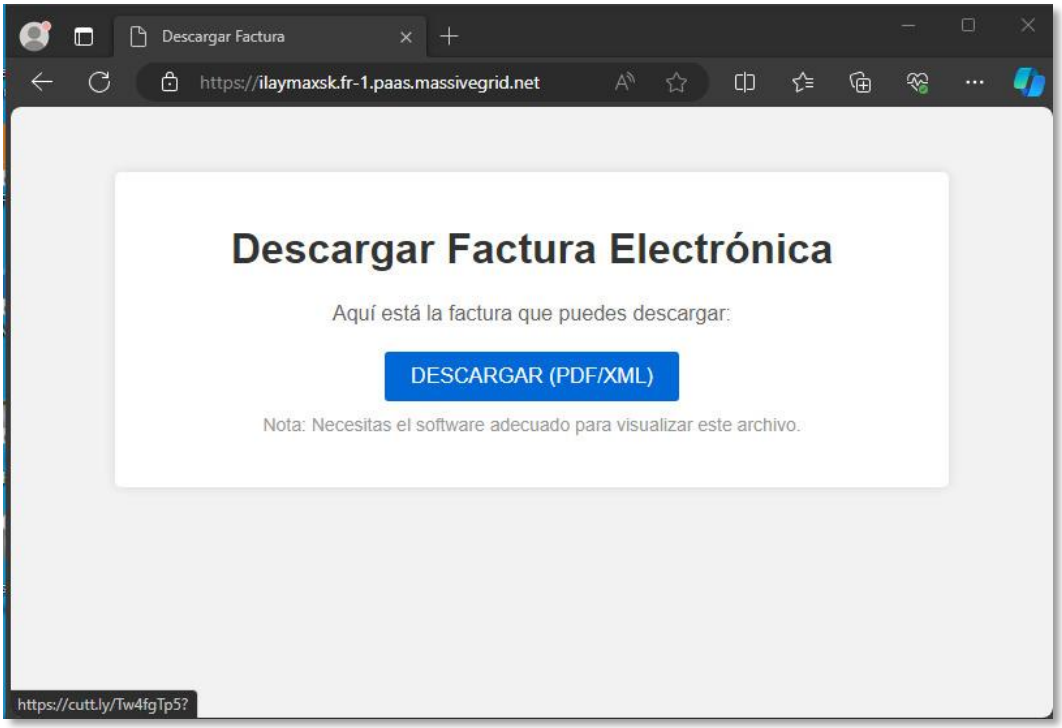


Imagen 3. Sitio de descarga archivo PDF.

Al ingresar sobre el link, nos descarga un archivo .ZIP.

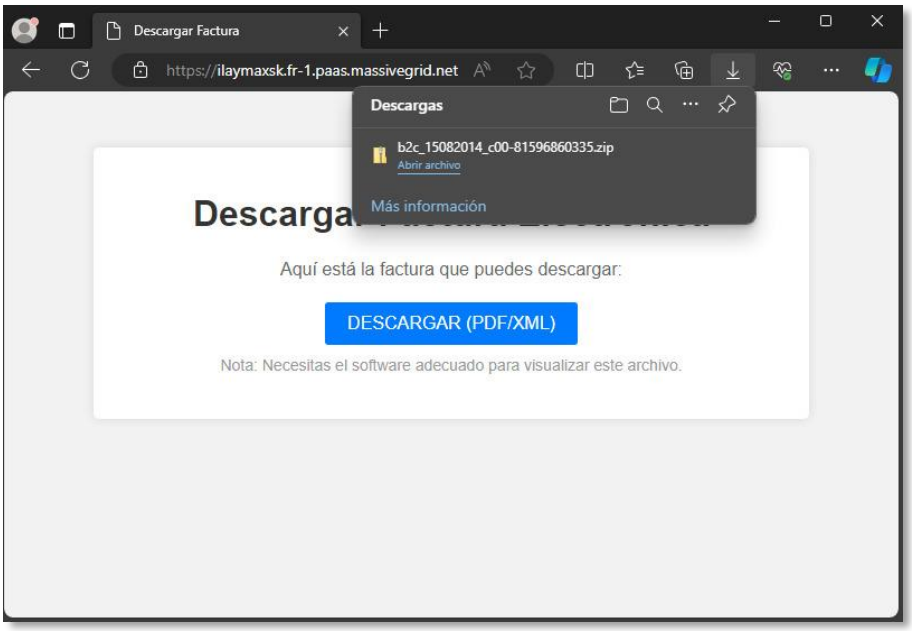


Imagen 4. Descarga de archivo ZIP.

Al descomprimir el archivo .ZIP descargado, se obtiene una Aplicación HTML.

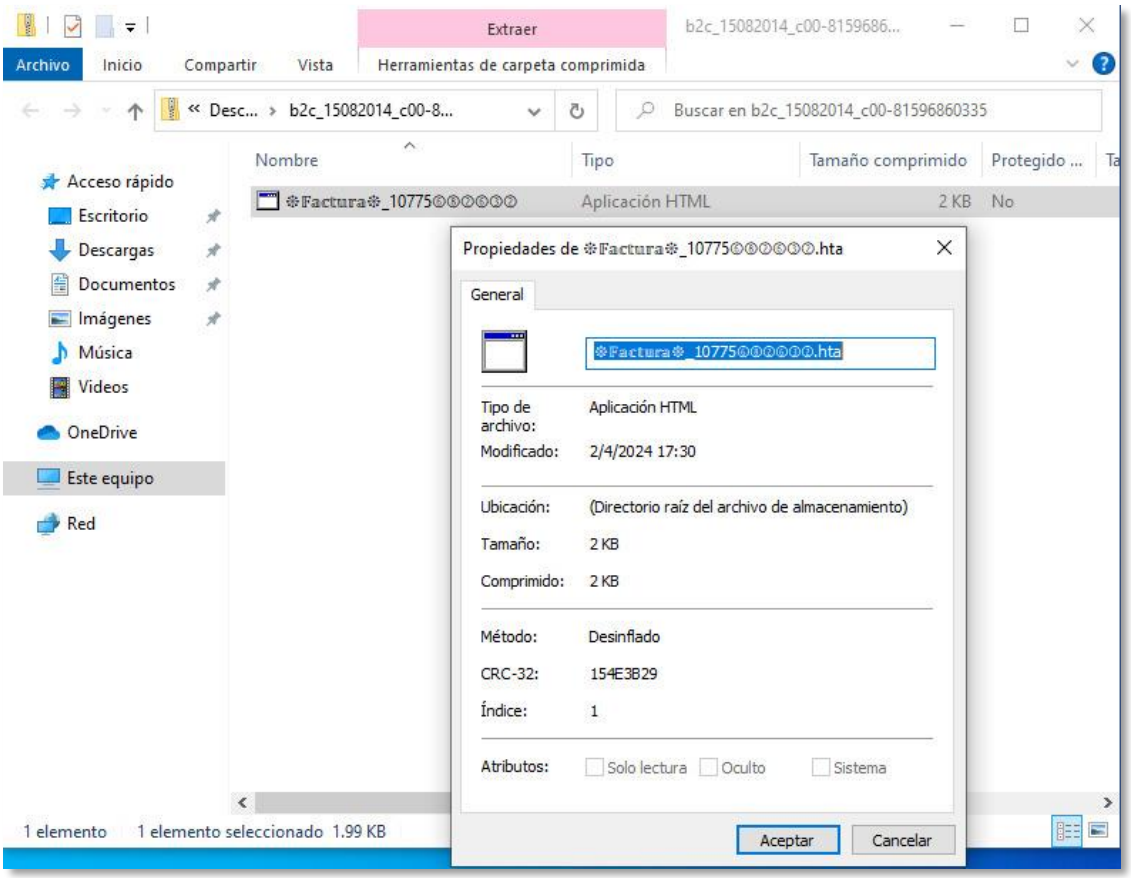


Imagen 5. Aplicación HTML.

Al ejecutar el archivo HTML se abre una ventana la cual tiene un campo para ingresar una contraseña, que sin realizar interacción con la misma procede a cerrarse.

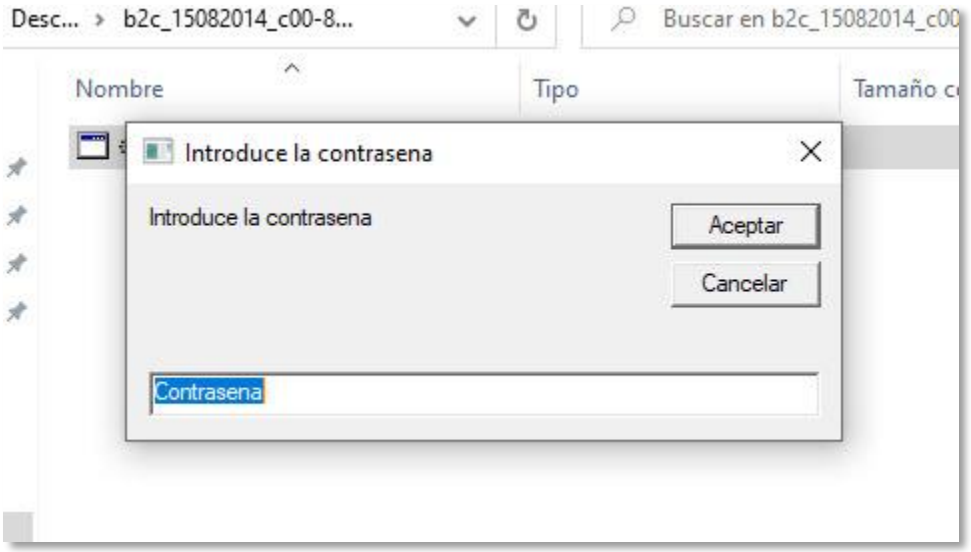


Imagen 6. Ejecución de archivo HTML.

Al realizar análisis del archivo ZIP en el sitio VirusTotal nos encontramos con que este se encuentra reportado por varios VENDORS, catalogado como un TROYANO.

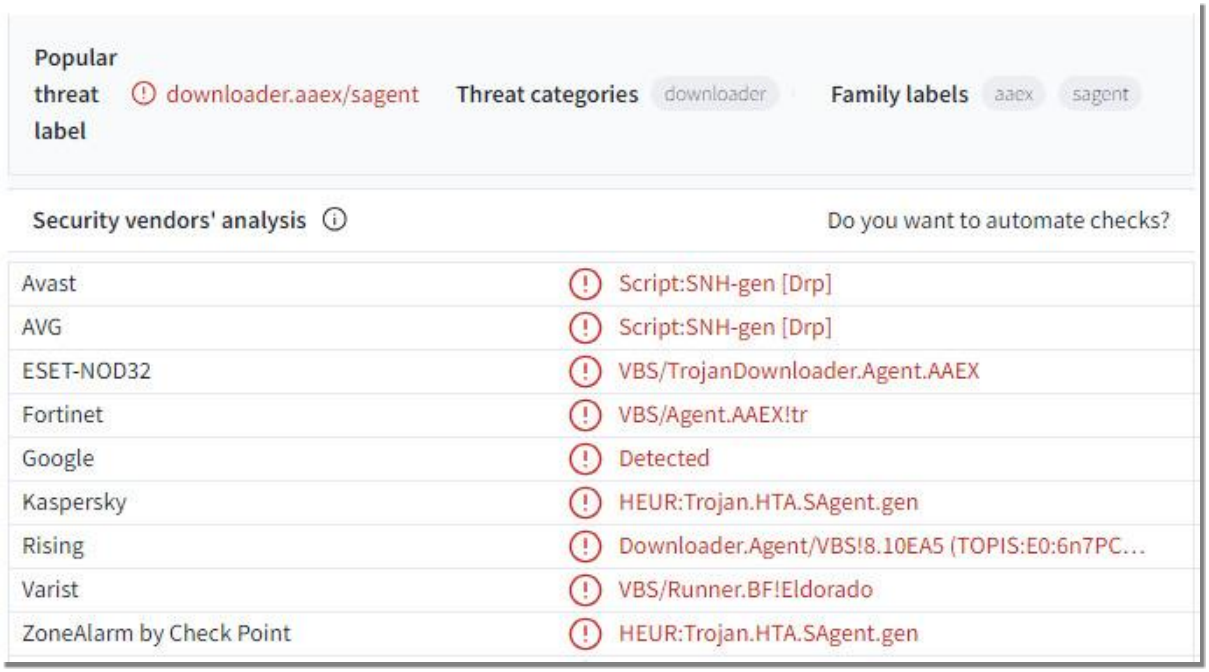


Imagen 7. Análisis de archivo ZIP en Virustotal.

Se realizó comparación de estado del sistema operativo antes y después de la ejecución del archivo descargado con la herramienta Sysinspector. El cual arroja que hay un proceso corriendo, llamado "**microsoftedge_x64_123.0.2420.65.exe**" catalogado por la herramienta como proceso peligroso.

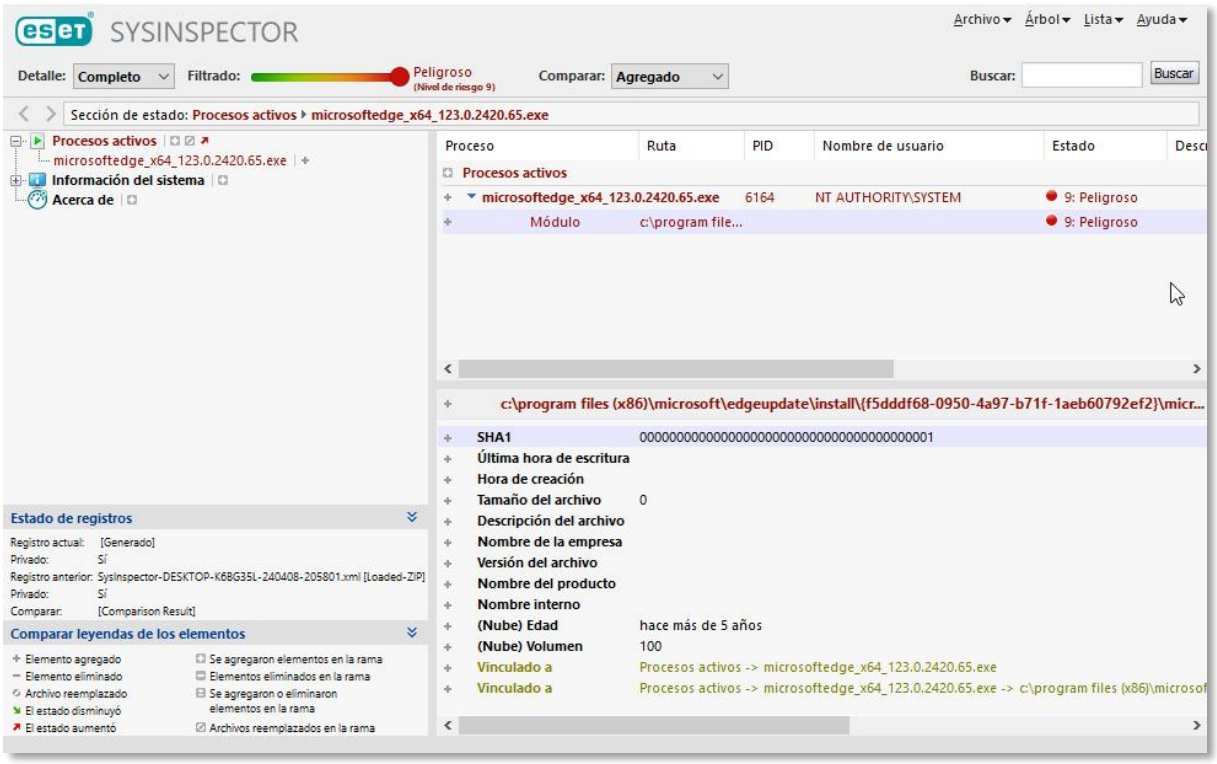
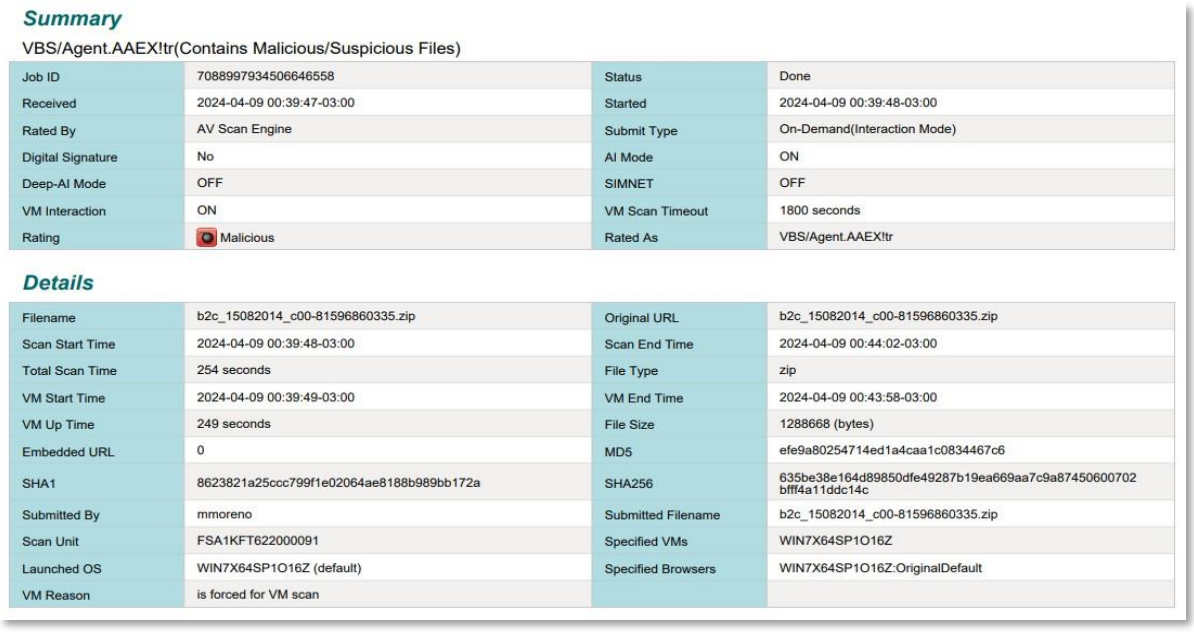


Imagen 8. Análisis con herramienta Sysinspector.

Se procedió al análisis del archivo ZIP en la herramienta FortiSandbox. Donde dio como veredicto que se trata de un archivo malicioso de tipo TROYANO con el nombre "**b2c_15082014_c00-81596860335.zip".**



Summary

VBS/Agent.AAEX!tr(Contains Malicious/Suspicious Files)

Job ID	7088997934506646558	Status	Done
Received	2024-04-09 00:39:47-03:00	Started	2024-04-09 00:39:48-03:00
Rated By	AV Scan Engine	Submit Type	On-Demand(Interaction Mode)
Digital Signature	No	AI Mode	ON
Deep-AI Mode	OFF	SIMNET	OFF
VM Interaction	ON	VM Scan Timeout	1800 seconds
Rating	Malicious	Rated As	VBS/Agent.AAEX!tr

Details

Filename	b2c_15082014_c00-81596860335.zip	Original URL	b2c_15082014_c00-81596860335.zip
Scan Start Time	2024-04-09 00:39:48-03:00	Scan End Time	2024-04-09 00:44:02-03:00
Total Scan Time	254 seconds	File Type	zip
VM Start Time	2024-04-09 00:39:49-03:00	VM End Time	2024-04-09 00:43:58-03:00
VM Up Time	249 seconds	File Size	1288668 (bytes)
Embedded URL	0	MD5	efe9a80254714ed1a4caa1c0834467c6
SHA1	8623821a25ccc799f1e02064ae8188b989bb172a	SHA256	635be38e164d89850dfe49287b19ea669aa7c9a87450600702bfff4a11ddc14c
Submitted By	mmoreno	Submitted Filename	b2c_15082014_c00-81596860335.zip
Scan Unit	FSA1KFT622000091	Specified VMs	WIN7X64SP1O16Z
Launched OS	WIN7X64SP1O16Z (default)	Specified Browsers	WIN7X64SP1O16Z:OriginalDefault
VM Reason	is forced for VM scan		

Imagen 9. Información de herramienta FortiSandbox.

Conclusión

En base a lo expuesto en el presente informe, y en referencia al mail remitido por la División COMUNICACIONES NACIONALES, para su análisis, se determinó que la maniobra empleada consiste en una técnica de Ingeniería Social del tipo **Phishing**, ya que intenta suplantar la identidad de una empresa de facturación. Este simula enviar una factura a descargarse como un archivo PDF, el cual al acceder descarga un archivo comprimido con extensión ZIP, que al descomprimir nos arroja un archivo ejecutable que contiene un malware llamado "**VBS/Agent.AAEX!tr**" de tipo troyano.

Este malware, descarga y ejecuta un script (comandos para realizar instalaciones de forma automática dentro de un sistema) para realizar diferentes tareas, y permite a los atacantes robar información sensible como por ejemplo credenciales de acceso (usuarios y contraseñas), tarjetas de créditos, entre otras. Como también puede realizar actividades sin el conocimiento del usuario. Estas actividades comúnmente incluyen establecer conexiones de acceso remoto, capturar entradas del teclado, recopilar información del sistema, descargar/cargar archivos, colocar otro malware en el sistema infectado, realizar ataques de denegación de servicio (DoS) y ejecutar/terminar procesos.

Se recomienda, al recibir correos de dudosa procedencia**,** no ingresar a los enlaces o archivos adjuntos y en ninguna circunstancia completar los datos solicitados en los mismos, a su vez, reportarlo cuanto antes a nuestra División a través de la casilla de correo electrónico csoc@policiafederal.gov.ar.