



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)

Departamento TÉCNICO OPERATIVO

Introducción

El día 13 de abril del corriente año, se recibió un correo electrónico proveniente de la cuenta deptotecnicoperativo@policiafederal.gov.ar perteneciente al Departamento TÉCNICO OPERATIVO, donde se simula el envío e indicación de descarga de una factura electrónica.

Desarrollo

Una vez identificado el caso, se procedió al análisis del correo proveniente desde secretaria@smtplw-09.com. En el mismo se indica que una factura ya se encuentra disponible para descargar.



Imagen 1. Cuerpo del mail.

A continuación se procede a analizar el encabezado del mismo, el cual se puede observar que se encuentra enmascarado siendo el remitente original el siguiente dominio: "bounce-804b01e5f78b960151b9a37fbfe0ad5b@smtplw-09.com"

X-FEAS-SPF:	spf-result=pass, ip=179.188.7.196, helo=smtp1797196.saaspmta0004.correio.biz, mailFrom=bounce-804b01e5f78b960151b9a37fbfe0ad5b@smtplw-09.com
X-FEAS-DKIM:	Valid
X-FEAS-Deferred:	Spam outbreak
X-MDAV-Processed:	policiafederal.gov.ar, Sat, 13 Apr 2024 02:36:12 -0300
X-FEAS-Client-IP:	179.188.7.196
X-FE-Last-Public-Client-IP:	179.188.7.196
X-FE-Envelope-From:	bounce-804b01e5f78b960151b9a37fbfe0ad5b@smtplw-09.com
X-FE-Policy-ID:	4:1:1:policiafederal.gov.ar
X-Spam-Processed:	policiafederal.gov.ar, Sat, 13 Apr 2024 02:36:12 -0300
X-MDArrival-Date:	Sat, 13 Apr 2024 02:36:12 -0300
X-Rcpt-To:	deptotecnicoperativo@policiafederal.gov.ar
X-MDRcpt-To:	deptotecnicoperativo@policiafederal.gov.ar
X-Return-Path:	bounce-804b01e5f78b960151b9a37fbfe0ad5b@smtplw-09.com
X-Envelope-From:	bounce-804b01e5f78b960151b9a37fbfe0ad5b@smtplw-09.com
X-MDaemon-Deliver-To:	deptotecnicoperativo@policiafederal.gov.ar

Imagen 2. Encabezado

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

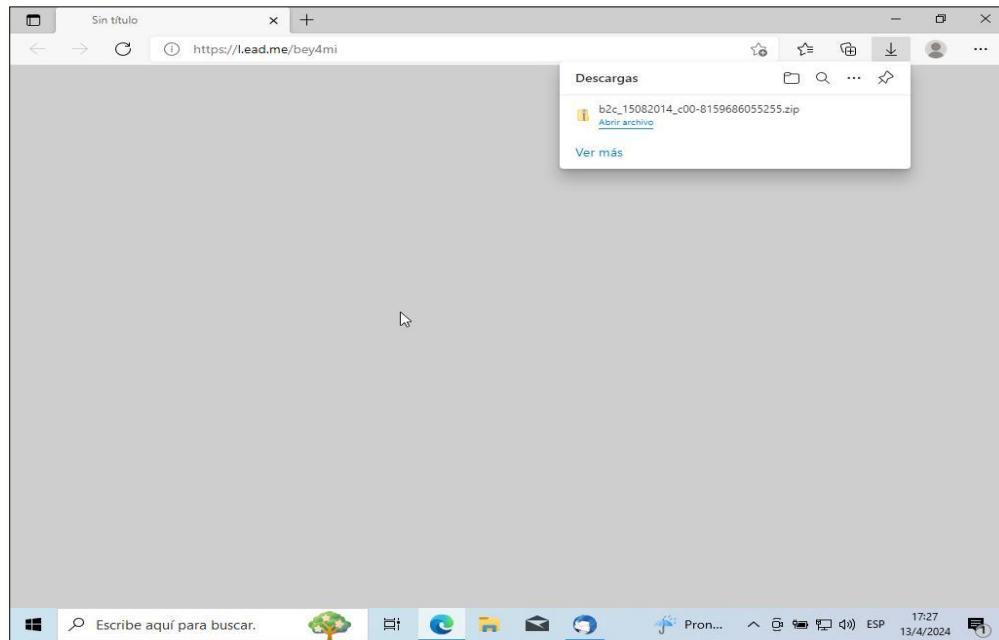


Imagen 3. Descarga de archivo ZIP.

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

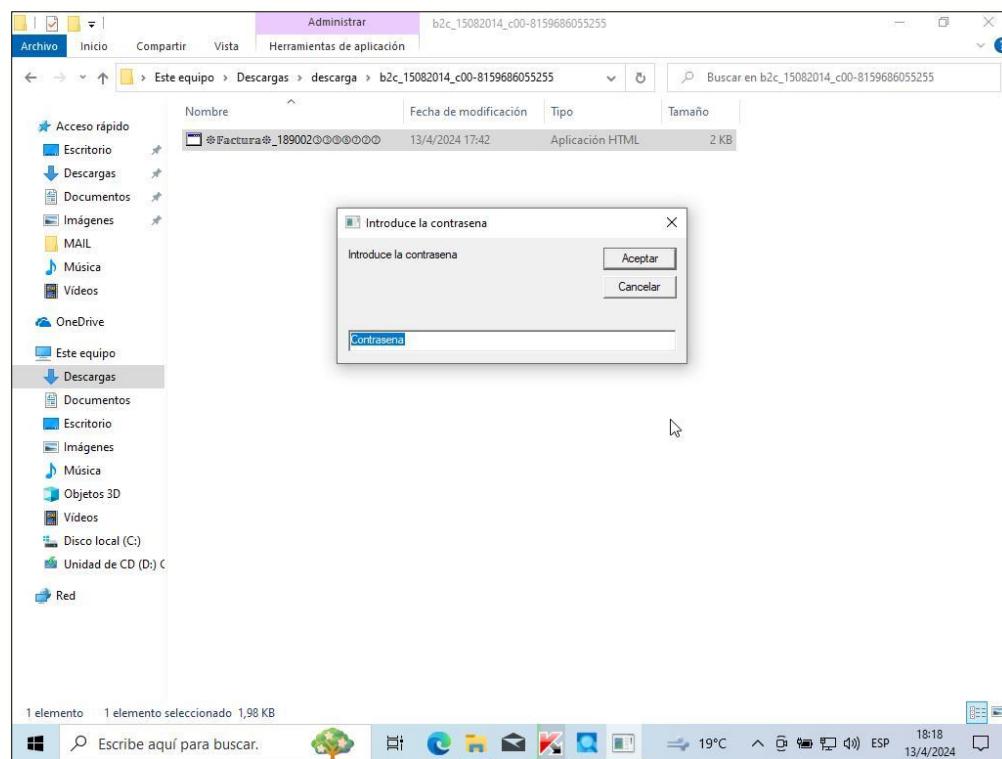


Imagen 4. Aplicación HTML.

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.

The screenshot shows the VirusTotal interface. At the top, there are filters for 'Popular threat label' (downloader.aaex/sagent) and 'Family labels' (aaex, sagent). Below this, a section titled 'Security vendors' analysis' lists nine vendors and their findings:

Vendor	Findings
Avast	Script:SNH-gen [Drp]
AVG	Script:SNH-gen [Drp]
ESET-NOD32	VBS/TrojanDownloader.Agent.AAEX
Fortinet	VBS/Agent.AAEX!tr
Google	Detected
Kaspersky	HEUR:Trojan.HTA.SAgent.gen
Rising	Downloader.Agent/VBS!8.10EA5 (TOPIS:E0:6n7PC...)
Varist	VBS/Runner.BF!Eldorado
ZoneAlarm by Check Point	HEUR:Trojan.HTA.SAgent.gen

Imagen 5. 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.

The screenshot shows the ESET SysInspector interface. The main pane displays a table of active processes, with one entry highlighted:

Proceso	Ruta	PID	Nombre de usuario	Estado	Desc
microsoftedge_x64_123.0.2420.65.exe	6164	NT AUTHORITY\SYSTEM	● 9: Peligroso		
Módulo	c:\program file...			● 9: Peligroso	

Below the table, a detailed view of the process shows its file path: c:\program files (x86)\microsoft\edgeupdate\install\f5dddf68-0950-4a97-b71f-1aeb60792ef2\micr... and its SHA1 hash: 00.

Imagen 6. Análisis con herramienta Sysinspector.

Se procedió al análisis de la aplicación HTML en la herramienta FortiSandbox. Donde dio como veredicto que se trata de un archivo malicioso de tipo TROYANO.

Summary			
VBS/Agent.AAEX!tr (low risk WEBSITE Payload)			
Job ID	7096419327738623521	Status	Done
Received	2024-04-14 00:39:19-03:00	Started	2024-04-14 00:39:29-03:00
Rated By	AV Scan Engine	Submit Type	On-Demand
AI Mode	ON	Deep-AI Mode	OFF
SIMNET	OFF	Video Record	ON
VM Scan Timeout	60 seconds	Rating	Malicious
Rated As	VBS/Agent.AAEX!tr		

Details			
Filename		Original URL	http://i.lead.me/bey4mi/_189002@0@0@0@0@0.htm
Scan Start Time	2024-04-14 00:39:29-03:00	Scan End Time	2024-04-14 00:40:37-03:00
Total Scan Time	68 seconds	File Type	htm
VM Start Time	2024-04-14 00:39:30-03:00	VM End Time	2024-04-14 00:40:34-03:00
VM Up Time	64 seconds	Redirect URL	http://mstercontenerirk.eastus.cloudapp.azure.com/apanetmaster.php
Embedded URL	0	MD5	a841f6cc031d1ff085dd807ff07403ba
SHA1	e7f56478b9f7c4ac98a1c10b56adaba4c539e2db	SHA256	0ffcad3ae186334f3d94ec88a4f103e1627d5e319ed9e6753e2891e31cb72494
Submitted By	mrobin	Submitted Filename	scan_of_lead.me
Scan Unit	FSA1KFT622000091	Launched OS	WIN10X64VM (optional)
Specified Browsers	WIN10X64VM-OriginalDefault	Launched Browsers	WIN10X64VM:Internet Explorer
VM Reason	is forced for VM scan		

Imagen 7. Información de herramienta FortiSandbox.

Conclusión

En base a lo expuesto en el presente informe, y en referencia al mail remitido por el Departamento TÉCNICO OPERATIVO para su análisis, se determinó que la maniobra empleada consiste en una técnica de Ingeniería Social del tipo **Phishing**, ya que intenta engañar al destinatario con una supuesta facturación falsa. Este simula enviar una factura, la 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.