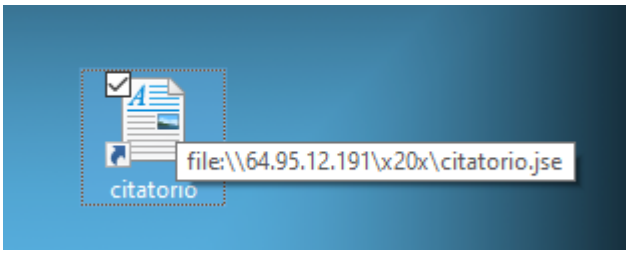
Reporte: Campaña de phishing asociada a **Botnet Fénix** sobre robo de información bancaria a usuarios de LATAM**.**

Resumen Ejecutivo

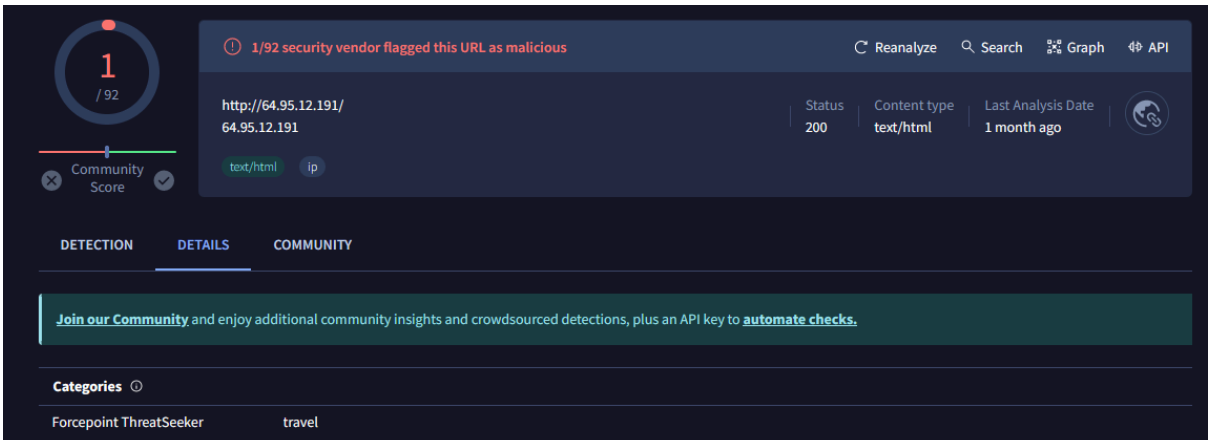
Se detectan correos electrónicos que contienen un URL en formato engañoso, y se comienza una investigación sobre sus intenciones, de esta manera se identifica una cadena completa de infección con distintas etapas donde se comienza a acceder a información del usuario y se culmina con la instalación de un Troyano de Acceso Remoto.
Toda esta cadena deja las suficientes pistas para poder concluir que el atacante es la Botnet Fenix, misma que tiene presencia de afectaciones similares a contribuyentes principalmente de México y Chile, además se detecta que todo el proceso de infección utiliza código principalmente Ruso, por lo cual se intuye que usan la modalidad de Malware como Servicio (MaaS) para la obtención de sus herramientas de ataque.
Esta afectación busca además de tener control sobre la máquina del usuario, realizar acciones concretas al ser detectada información relacionada a una lista de bancos específicos. Y está dirigida principalmente a usuarios que usen alguno o algunos de estos bancos

Detalle Tecnico

El adversario utiliza la técnica de phishing que consiste en enviar un correo electrónico que contiene archivos maliciosos esperando ser abiertos por el usuario. En el caso de esta campaña el archivo es de tipo short cut o .url, que se podría confundir con un acceso directo y simula ser un citatorio del Servicio de Administración Tributaria de México



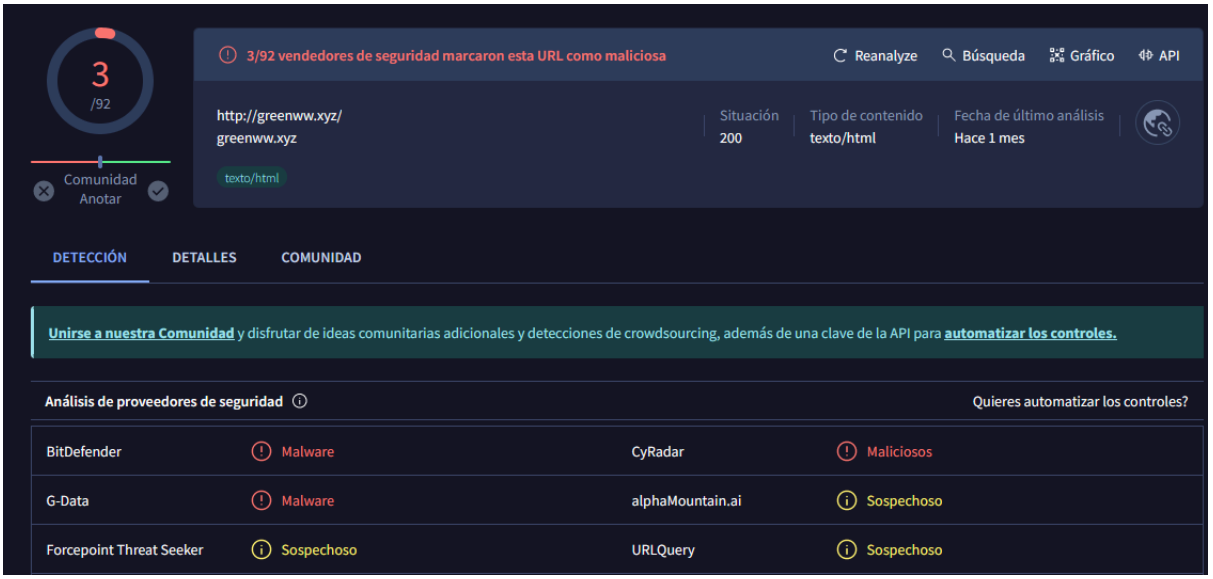
La IP de la cual es descargado este archivo es 64.95.12[.]191 al ser verificada en virus total y podemos ver como ya tiene un reporte como maliciosa.



Después de dar click se descargara un archivo JavaScript que tiene la función de llamar a una IP, sin embargo el código se encuentra ofuscado. Por medio del escaneo de redes se detecta que se recibe una contestación del dominio greenww[.]xyz

```
06/05/24 04:48:03 PM [          Diverter] svchost.exe (1356) requested UDP 192.168.13.128:53
06/05/24 04:48:03 PM [        DNS Server] Received A request for domain 'greenww.xyz'.
06/05/24 04:48:03 PM [          Diverter] wscript.exe (2948) requested TCP 192.0.2.123:443
```

Con esto ahora sabemos el dominio del cual se contesta a la llamada que hace el archivo, al ingresar este dominio en VirusTotal podemos detectar que nuevamente ya se encuentra reportado.



El cometido de esta comunicación es proporcionar un documento de tipo DLL y usando CFF Explorer podemos ya saber además de sus identificadores hash, su nombre original y versión.

Property	Value
LegalTrademarks	
OriginalFilename	ClassLibrary2.dll
ProductName	ClassLibrary2
ProductVersion	1.0.0.0

File Type	Portable Executable 32 .NET Assembly
File Info	Microsoft Visual Studio .NET
File Size	64.00 KB (65536 bytes)
PE Size	64.00 KB (65536 bytes)

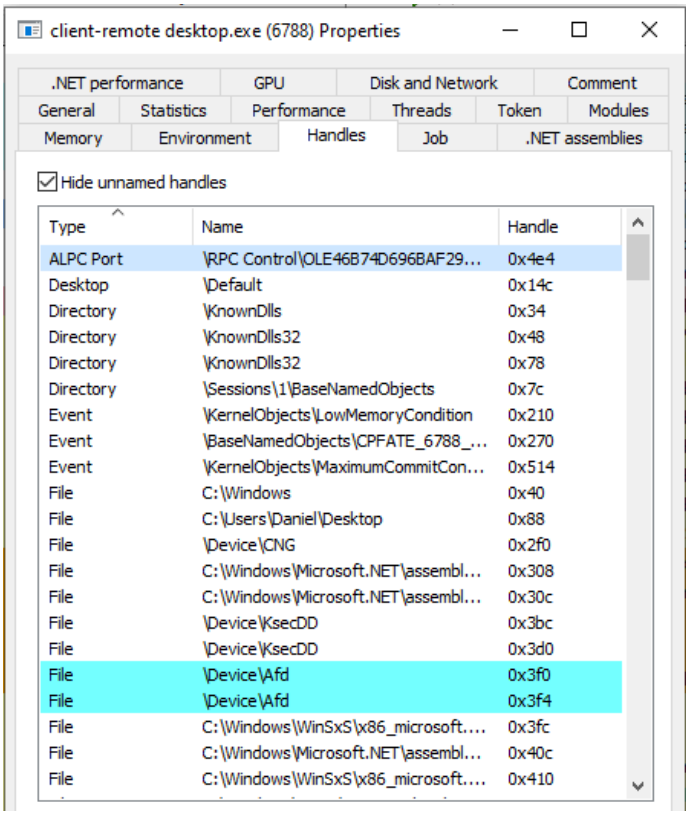
Debugando el DLL encontramos que sus principales funciones serán extraer múltiple información del equipo víctima. De igual manera realizará la instalación de todos los

complementos y realizará modificaciones de configuración que necesita para poder instalar el código que por fin le dará persistencia en el ataque y cumplir con su cometido.

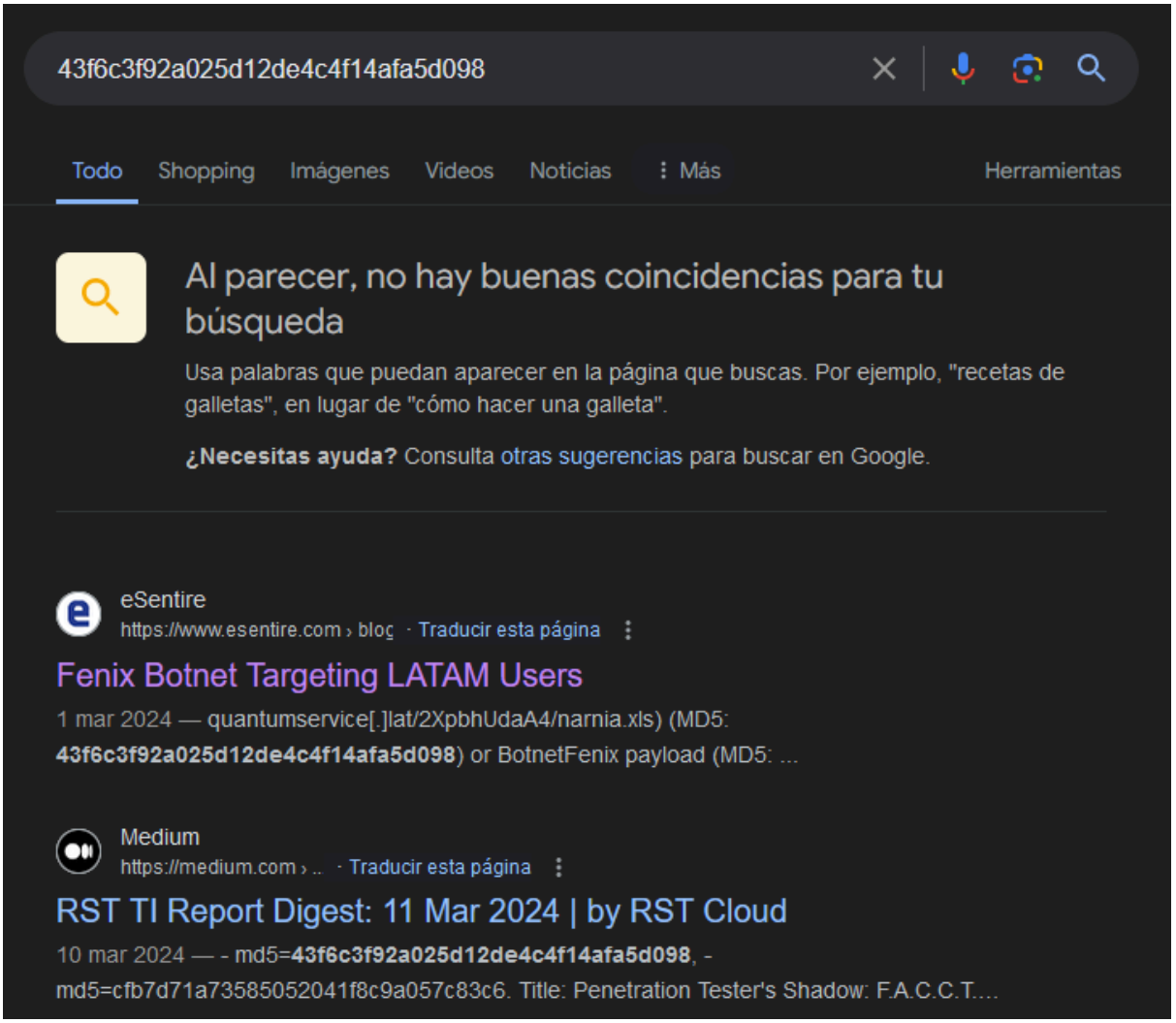
Líneas de debugueo

```
init("installer","Advanced Installer");
    if(PE.compareOverlay("2f30ee1f5e4ee51e"))
    else if(PE.compareOverlay("d0cf11e0a1b11ae1"))
    else if(PE.findSignature(PE.getSize()-0x50, 0x50, "'ADVINSTSFX'")!=-1)
    return result(bShowType,bShowVersion,bShowOptions);
init("protector","CodeSafe");
    if(PE.compareEP("83EC10535657E8C40100",23))
init("protector","CodeVeil");
    if(PE.compareEP("e9$$$$$$$$e9$$$$$$$$8bff60e8$$$$$$$$5ee8"))
```

Una vez el DLL esté instalado la infección ha sido efectuada, se ha instalado un exe que es una puerta trasera dentro del equipo.
Este archivo ejecutable da acceso al control de RPC, además de generar otras configuraciones dentro del equipo para tomar control del mismo. Con todos estos pasos el ataque está concluido y se ha cumplido con la infección.



Para poder determinar la atribución y determinar claramente los fines de la campaña se realiza una investigación por medio del identificador hash de los archivos y encontramos lo siguiente:



Con esto podemos determinar que el objetivo del ataque son usuarios de América Latina, que aplica principalmente métodos de simular trámites gubernamentales de México, y su objetivo es sustraer información bancaria los clientes por medio de un Troyano de Acceso Remoto (RAT). Además de atribuir este ataque a la Botnet Fenix.

Análisis con ATT&CK Framework

Desarrollo de recursos	Acceso inicial	Ejecución	Persistencia	Escalada de privilegios	Evasión de defensa	Movimiento lateral
Adquisición de infraestructura	Phishing	Ejecución de Usuario	Extensiones de navegador	Inyección de proceso	Modificación de permisos de archivo y directorio	Servicios remotos
Obtención de malware Ruso	Correo con url a JavaScript con formato engañoso	El usuario es sometido a ingeniería social para ejecutar el JavaScript	Con la información recabada en la información se sabe que el ataque persiste en una extensión del navegador	El Java Script trae e inyecta el DLL que se encargará de extraer la información existente y dar el acceso a la última etapa del malware	En el debuggeo del DLL se identifica que se comienzan a modificar privilegios posiblemente para no ser detectado	Por medio del DLL se instala el exe que da acceso a RPC que permite la ejecución remota de comandos

Colección	Comando y control	Impacto
Adversary-in-the-Middle Browser Session Hijacking	Inyección de contenido Ofuscación de datos Resolución dinámica	Robo financiero
La finalidad del exe es además de tener acceso remoto activar la extensión del navegador para esperar interacción con los bancos.	El malware en su conjunto de toda la cadena de infección se encuentra ofuscado, y cada archivo que modifica e instala tiene detecciones dinámicas del entorno en el que se encuentran y las respuestas que esperan que complica su análisis.	El impacto que busca tener el malware es el robo de credenciales e información de usuarios de bancos para cometer robo financiero.

Evaluación

La afectación tiene el cometido de explotar debilidades en la educación en cuanto a seguridad informática de usuario de ciertos bancos mexicanos. Además cuida de usar un método de engaño efectivo, pues suele ser sencillo confiar en plataformas que parecen ser gubernamentales.
El daño es principalmente la pérdida del control de la información por parte del usuario del banco, esto puede generar inconvenientes tanto para él como para el propio Banco. Esta afectación también usa la suplantación de identidad de instituciones del Gobierno Méxicano y afecta su propia credibilidad.

Indicadores de Compromiso

Descripción	**Valor**
Nombre del archivo	citatorio.jse
MD5	0a6370f2c04035ef6e154aa47e03645d
SHA1	29ee9cdcc8fcda23df0fc3682fa66b41c13e66fb
SHA256	338507416b13659b57f51e48fcd7236f8035219b26715d612f0ee14505879552
Descripción	Archivo JavaScript que se encarga de descargar el DLL, se obtiene de url que simula ser un acceso directo

Descripción	**Valor**
Nombre del archivo	ClassLibrary2.dll
MD5	59e36b3aa8956021ec3f4bc84abbabba
SHA1	c65593625802627a5e21b5be85812f62b9b8d42b
SHA256	b371d8f75447f9f47a10a2a4d29c0a4f96d49ce42a734fa179ef9e26c8ef042a

Descripción	Archivo .NET con código ejecutable para modificar privilegios, sustraer información y asegurar su persistencia con instalar narnia

Descripción	**Valor**
Nombre del archivo	narnia.exe
MD5	43f6c3f92a025d12de4c4f14afa5d098
SHA1	d5947e68750676d99a59272b8daa11a464a1da59
SHA256	8f887de850a32ae8de88b5e37ba9bbf18de80f0d55d6a575d72c695055afa71b
Descripción	Archivo final de la infeccion en el cual se detecta al menos la oportunidad de ejecutar comandos de forma remota bajo el protocolo RPC

Descripción	**Valor**
Dirección	file:\\64.95.12.191\x20x\citatorio[.]jse
Descripcion	Documento que contiene el script de inicio de la cadena de infección

Descripción	**Valor**
Dominio	greenww[.]xyz
Descripcion	Dominio del cual se descarga el DLL