BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-55
Fecha de publicación: 18/10/2024
Tema: Botnet Fénix activa en México
Traffic Light Protocol (TLP): White

Descripción

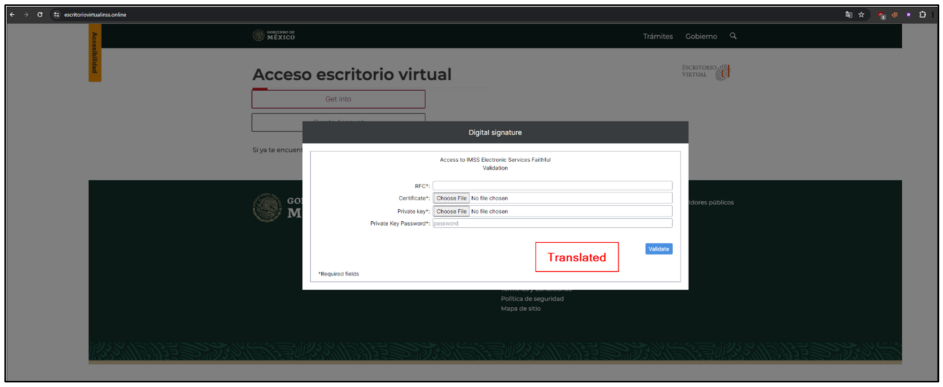
El grupo de criminales que gestiona la botnet Fénix ha intensificado sus actividades desde 2022. Este botnet ha dirigido múltiples ataques, principalmente al SAT (Servicio de Administración Tributaria), utilizando como vectores de ataque el phishing y sitios web fraudulentos que imitan portales oficiales, demostrando así un objetivo centrado fuertemente en ciudadanos mexicanos.

Estos sitios falsos invitan a los usuarios a descargar archivos supuestamente destinados a mejorar la seguridad en la navegación del portal. Sin embargo, la descarga instala la etapa inicial del malware, lo que permite al atacante acceder a información confidencial, como credenciales de acceso.

A continuación, se presentan las campañas más recientes de la botnet Fénix, que ha permanecido activa desde 2022.

Fecha de campaña	Página de aterrizaje	Entidad y país de destino
02-02-2023	citas-sregob-mexico[.]com	Secretaría de Relaciones Exteriores – México
02-02-2023	sre-curpmexico[.]com	Secretaría de Relaciones Exteriores – México
02-02-2023	citas-sat2023[.]com.mx	Servicio de Administración Tributaria (SAT) – México
08-02-2023	mexico-curp[.]com	Secretaría de Relaciones Exteriores – México
04-03-2023	whatsapp.sitio web	Público en general
17-03-2023	sitio web annydesk	Público en general
17-03-2023	tramites-sat[.]com.mx	Secretaría de Relaciones Exteriores – México
14 de marzo de 2023	citasatmx2023[.]lat	Servicio de Administración Tributaria (SAT) – México
14 de marzo de 2023	2repuvegobmx[.]com.mx	Registro Público Vehicular (REPUVE) – México
16 de marzo de 2023	citas-satmx[.]com	Servicio de Administración Tributaria (SAT) – México
29-03-2023	lbci-seguro[.]com	Banco BCI – Chile
13 de abril de 2023	siii-chile[.]com	Servicio de Impuestos Internos (SII) – Chile
15 de abril de 2023	consultacurp-gobmx[.]com.mx	Secretaría de Relaciones Exteriores – México

A inicios de 2024, el grupo de criminales detrás de la botnet Fénix lanzó una nueva campaña de ingeniería social dirigida a usuarios en México y América Latina que utilizan la plataforma del SAT y otros servicios financieros en la región.

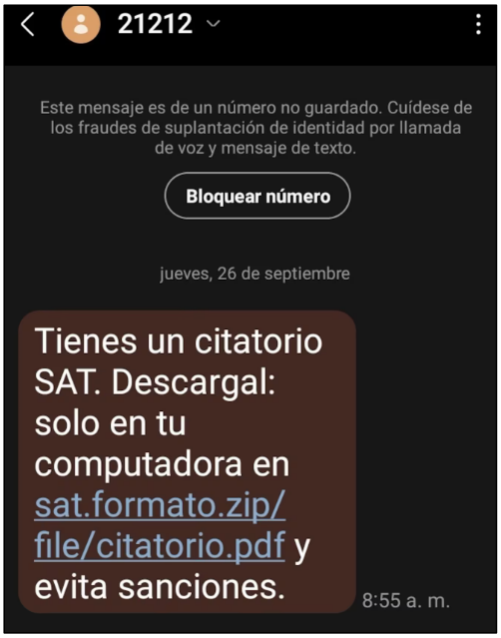


La botnet conocida como "Fénix" ha lanzado recientemente una campaña de estafas enfocada en usuarios bancarios en México. Esta campaña utiliza mensajes de texto fraudulentos que simulan provenir del SAT, con el objetivo de engañar a las víctimas para que descarguen un archivo. Al hacerlo, los usuarios sin saberlo instalan malware en sus dispositivos, lo que permite a los atacantes robar la información necesaria para acceder a sus cuentas bancarias y datos confidenciales.

Procedimiento detallado del funcionamiento de la Botnet Fenix

1. Llegada del mensaje de texto fraudulento:

La víctima recibe un SMS que simula provenir del SAT, notificando sobre un archivo PDF importante pendiente de descarga. Este mensaje sirve como cebo para atraer a la víctima a hacer clic en un enlace malicioso.



2. Visualización del archivo falso:

Al acceder al enlace, la víctima no ve un archivo PDF real, sino una página HTML que simula dicho formato y muestra un mensaje de error, indicando que el archivo no se puede visualizar.

3. Paso para “solucionar” el error:

Aparece un botón de “Solucionar” que, al hacer clic, copia en el portapapeles un código malicioso sin que la víctima lo perciba.

4. Ejecución de comandos maliciosos:

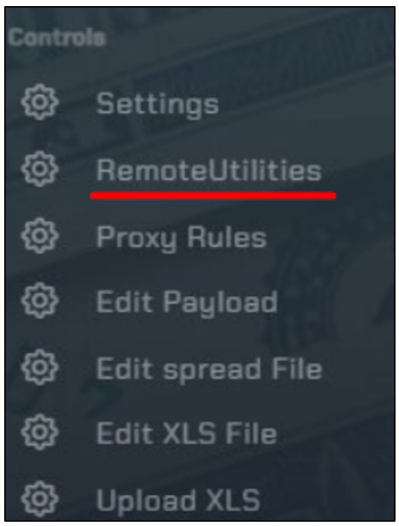
La página web instruye a la víctima a presionar las teclas Windows + R para abrir el cuadro de ejecución de comandos de Windows. Luego, se le pide que pegue el contenido copiado (un código malicioso) en este cuadro y presione Enter.

5. Instalación del malware:

Al ejecutar el código, la víctima permite la instalación del malware, identificado como Narnia RAT, que proporciona acceso remoto a los atacantes. Esto facilita el robo de información bancaria y otros datos personales del usuario.

6. Mecanismo de persistencia del ataque:

Para evitar ser detectado y mantenerse en el sistema, el malware instala un programa adicional llamado Remote Utilities, que garantiza a los atacantes acceso continuo al dispositivo, incluso si el malware original es eliminado por un antivirus.



7. Exfiltración de credenciales bancarias:

Una vez en el sistema, el malware comienza a registrar la actividad del usuario, capturando credenciales de acceso y datos confidenciales de aplicaciones bancarias, incluidas Banamex, BBVA, Santander, entre otras. Esta información se envía a los atacantes, quienes pueden utilizarla para realizar transacciones sin autorización.

Este procedimiento expone cómo la Botnet Fénix recurre a técnicas de ingeniería social, explotando la confianza de los usuarios en instituciones como el SAT para llevar a cabo su ataque.

Recomendaciones

A continuación, damos algunas recomendaciones para evitar verse comprometidos y/o afectados por estas bandas.

- Evitar ejecutar o abrir archivos de acceso directo desconocidos o no solicitados.
- Capacite a los usuarios para que identifiquen y denuncien contenido potencialmente malicioso mediante programas de capacitación sobre concientización sobre seguridad y phishing (PSAT).
- Mantener las firmas de antivirus actualizadas al igual que los servicios más criticos y sobre todos, los expuestos a Internet.
- En redes corporativas, se recomienda la utilización de Endpoint Detection and Response (EDR) o Extended Detection and Response (XDR) centralizador para monitorear los dipositivos digitales de la organización, y tener visibilidad y control sobre los mismos.

Si tiene alguna consulta especificas sobre implementaciones de soluciones de ciberseguridad puede contactar con nuestro equipo a info@cybolt.com con mucho gusto le estarán asesorando.

Información adicional:

- https://www.metabaseq.com/threat/fenix-botnet/
- https://www.esentire.com/blog/fenix-botnet-targeting-latam-users
- https://www.linkedin.com/in/gfdez/
- https://www.publimetro.com.mx/noticias/2024/10/16/modus-operandi-asi-es-como-botnet-fenix-suplanta-al-sat-y-roba-tu-cuenta-bancaria/
- https://www.esentire.com/blog/fenix-botnet-targeting-latam-users

Comentado [GR1]: Agregar siempre igual una seccion de recomendaciones

BEACON LAB
C S I R T

CYBOLT
Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com