Cyber Threat Profile MALTEIRO

blog.scilabs.mx/cyber-threat-profile-malteiro/

SCILabs December 23, 2021

Panorama general

El presente post tiene como objetivo mostrar el modus operandi, el *malware* utilizado y los *TTP* de un grupo de ciberdelincuentes nombrado por el equipo de SCILabs como **Malteiro**, el cual opera y distribuye el troyano bancario *URSA/Mispadu.* Por otro lado, se presenta una investigación de las campañas de distribución de los troyanos bancarios más recientes, las cuales representan un riesgo potencial para la información de los titulares de cuentas bancarias mexicanas y latinoamericanas. Si bien las campañas de *URSA/Mispadu* se han lanzado desde finales de 2019, ha sufrido diversas modificaciones a lo largo del tiempo, hasta convertirse en un *malware* sofisticado y difícil de detectar por las soluciones antivirus. Este *malware* reutiliza y mejora algunos *TTP* utilizados en sus primeras versiones, que en su momento fueron analizados en algunos *blogs* de seguridad.

Región de operación

De acuerdo con la evidencia recopilada por SCILabs, la campaña está dirigida principalmente a México y Latinoamérica y otros países de los continentes europeo, africano y asiático. Es importante resaltar que algunos estudios apuntan a que *URSA/Mispadu* es uno de los troyanos bancarios que más está afectando a la región.

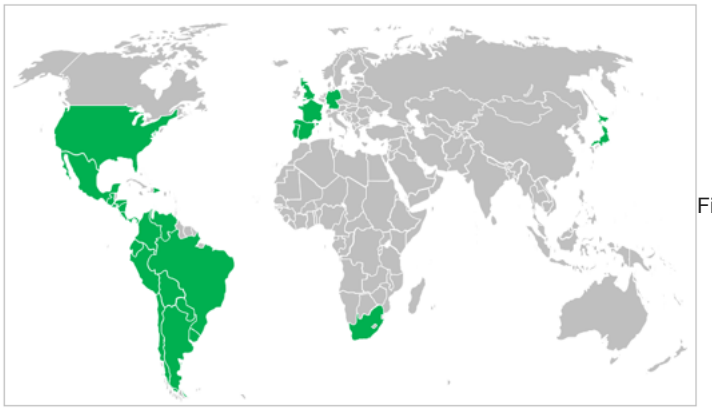


Figura 1 – Países objetivo

Con base en la información analizada por SCILabs de fuentes públicas y nuestro ciberecosistema, a continuación, se presenta el cronograma de las campañas identificadas:

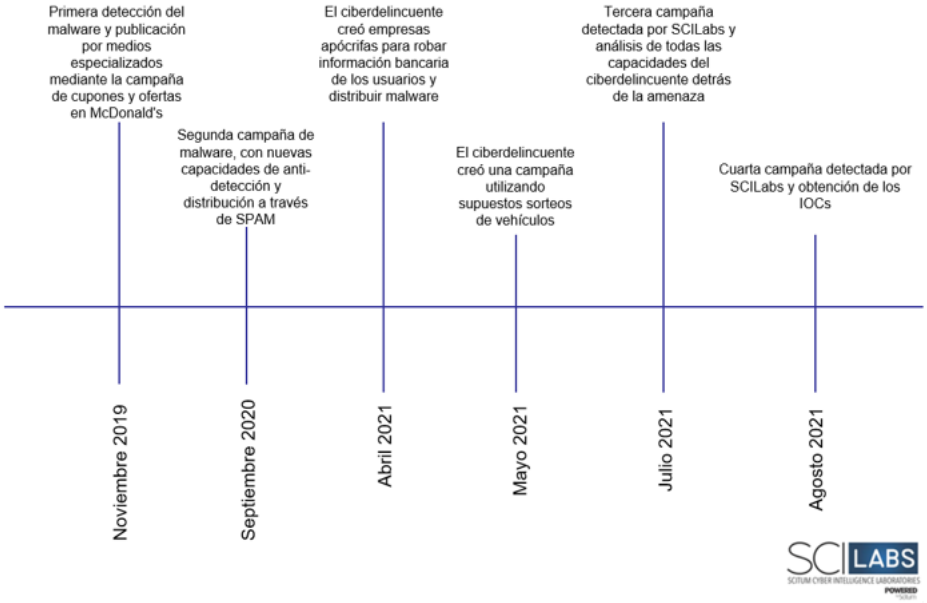


Figura 2 – Línea del tiempo de las campañas

Acerca de las víctimas

Durante la investigación, SCILabs identificó que las campañas de *phishing* están dirigidas principalmente a México. De acuerdo nuestra telemetría, se enumeran los principales sectores a los que podrían dirigirse estas campañas:

- Sector financiero
- Sector alimenticio
- Sector de las comunicaciones
- Sector salud
- Sector minorista
- Industria manufacturera
- Sector Industrial
- Gobierno

Modelo de operación

Contexto de la amenaza Malteiro es un grupo de ciberdelincuentes que opera, administra y vende el troyano bancario *URSA/Mispadu*, así como las herramientas para su instalación y configuración. Con la información obtenida por SCILabs, es posible determinar que los ciberdelincuentes utilizan el modelo de negocio *Malware-as-a-Service (MaaS)*.

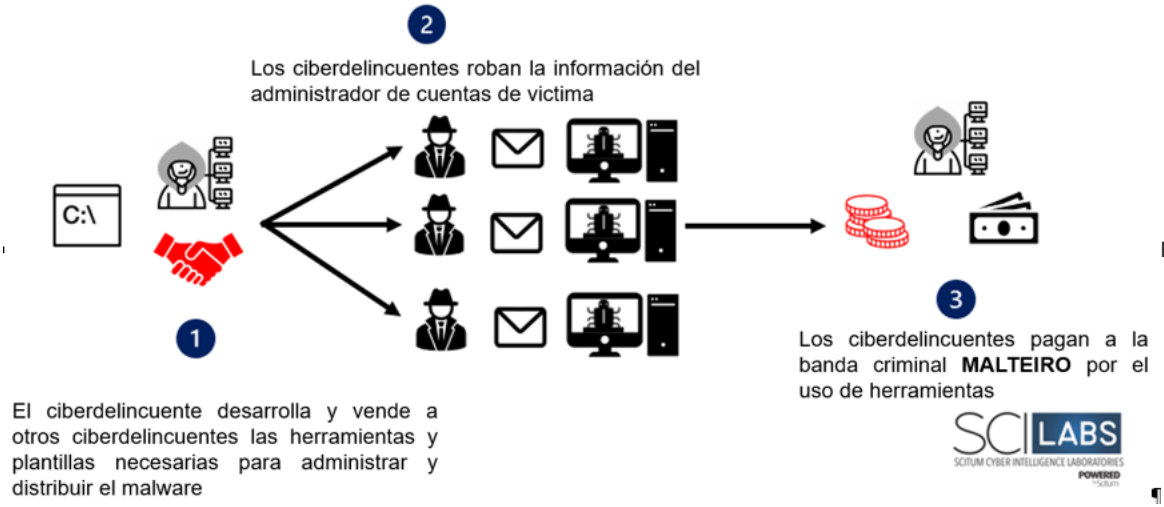


Figura 3 – Modus operandi de los ciberdelincuentes basado, en el modelo de negocio Malware as a Service

Asimismo, supervisan la creación de campañas y otras técnicas para la distribución de *malware*, como se puede ver en la siguiente imagen:

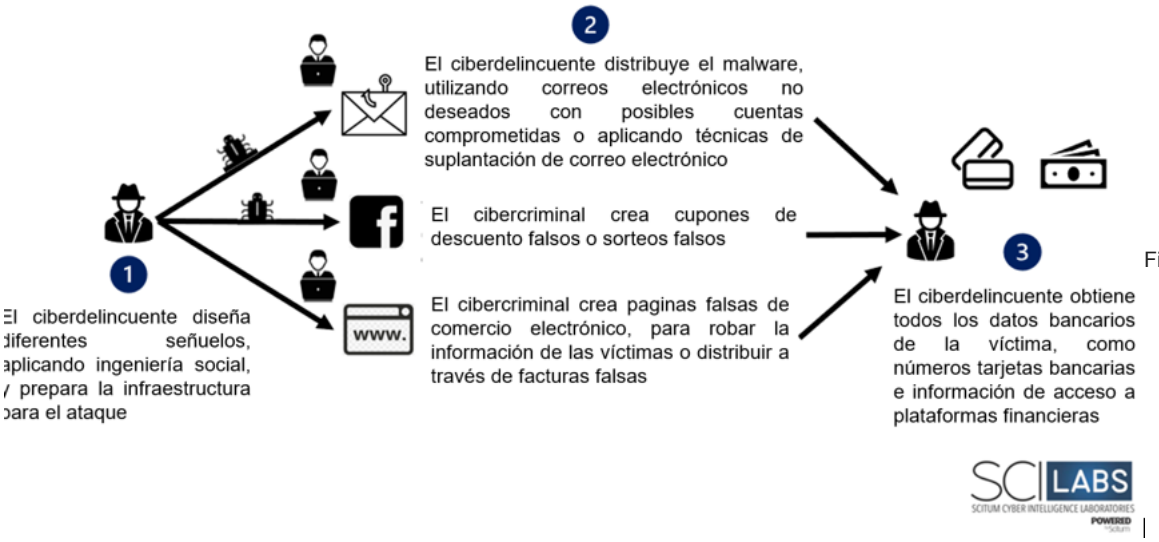


Figura 4 – Modus operandi utilizado para la distribución de URSA/Mispadu

URSA/Mispadu es una familia de troyanos bancarios que se dirige principalmente a México y Latinoamérica, la cual se observó por primera vez en noviembre de 2019. El *malware* está escrito en *Delphi* y puede ejecutar acciones como captura de pantalla, simular acciones de mouse y teclado, registro de pulsaciones de teclas y control remoto del equipo infectado. Además, tiene capacidades de actualización a través de un archivo de *Visual Basic Script* (VBS), que se descarga y ejecuta automáticamente. Durante el proceso de infección, el *malware* recopila los siguientes datos de la computadora de la víctima:

- Versión del sistema operativo
- Nombre de la computadora
- Idioma del dispositivo
- Antivirus instalado

El principal vector de entrada de *URSA/Mispadu* es el *spam* y la publicidad maliciosa, al igual que en otras campañas activas en la región. También se utilizan cupones de descuento falsos, así como correos electrónicos maliciosos con supuestas facturas vencidas, en donde los atacantes crean una situación aparentemente urgente que luego invita a los destinatarios a descargar un archivo .zip desde una *URL* maliciosa.

La ingeniería social como método de propagación

Generación de empresas apócrifas para distribuir *malware* En el proceso de investigación, SCILabs observó que el ciberdelincuente utiliza empresas apócrifas de comercio electrónico para desplegar el troyano *URSA/Mispadu* a través de facturas falsas y robo de información bancaria de los clientes. A continuación, se muestra un sitio, llamado "**Baratomx**", que es una página falsa de comercio electrónico, creada para distribuir *malware*:

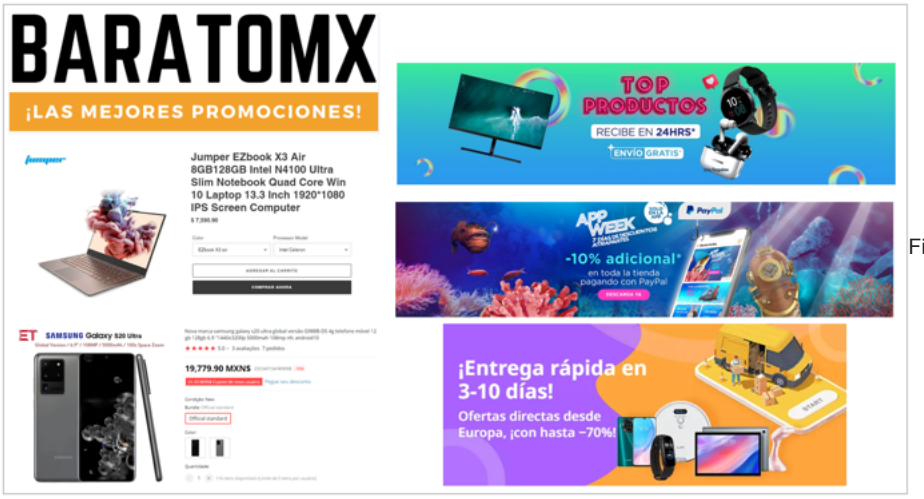


Figura 5 – Página de comercio electrónico falsa, creada por ciberdelincuentes para distribuir malware

Cupones, sorteos y premios falsos basados en la suplantación de instituciones financieras en México El grupo cibercriminal ha compartido en redes sociales como *Facebook*, cupones de descuento falsos de *McDonald's*, así como rifas de vehículos a nombre de bancos en México, las cuales conducen a páginas maliciosas.

Figura 6 – Campaña de malversting en redes sociales

Entre las campañas de publicidad maliciosa identificadas por SCILabs, también hay una relacionada con un supuesto sorteo de 50 *iPhone*, que se distribuyó a través de las redes sociales. A continuación, el análisis de cada una de las campañas de *malware* generadas por los ciberdelincuentes.

Primera campaña distribuida a través de publicidad maliciosa y spam.

Se colocaron anuncios patrocinados en *Facebook* que ofrecían falsos cupones de descuento de *McDonald's*. En caso de hacer clic en uno de los anuncios, la víctima potencial es dirigida a una de las páginas Web apócrifas que, al hacer clic en el botón sugerido por el anuncio, descargará un archivo ZIP con un instalador malicioso de tipo *MSI*. Ocasionalmente, el archivo ZIP también incluirá *software* legítimo como *Mozilla Firefox* o *PuTTY*, usados como señuelos para engañar a la víctima. El grupo cibercriminal compiló dos versiones diferentes del troyano bancario, según el país al que ataca. Además, decidió utilizar diferentes instaladores y etapas posteriores para cada país.

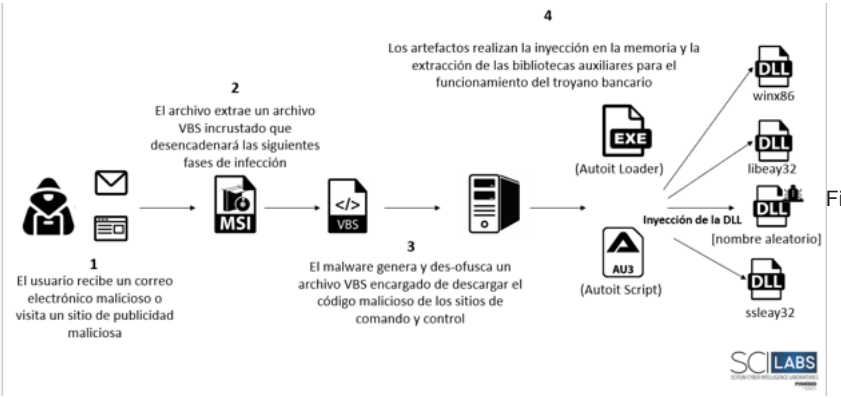


Figura 7 – Flujo de infección de la primera campaña

Segunda campaña distribuida a través de campañas de phishing

Se caracterizó porque los operadores de *URSA/Mispadu* enviaron correos electrónicos de *phishing* con supuestas facturas, siendo México el país más afectado de Latinoamérica. En Portugal y países cercanos, se lanzaron campañas de *phishing* suplantando a entidades como Vodafone o la policía judicial portuguesa. En esta campaña, los ciberdelincuentes invitan a los destinatarios de los correos electrónicos a descargar un archivo .zip desde una *URL* maliciosa. Al igual que en la campaña anterior, el archivo .zip contiene un instalador de tipo *MSI* con un *script* de *Visual Basic*; a esto le sigue la descarga de dos *droppers* y tres capas de ofuscación que, cuando se eliminan, generan el archivo .vbs final que ejecuta un *script* de *AutoIT*. El objetivo final es cargar en memoria un binario de *Delphi* que contiene el código malicioso. Cabe resaltar que el *malware* utiliza nombres y logotipos bancarios legítimos para crear ventanas y superponer el navegador de la víctima, para robar sus datos bancarios. El binario también utiliza dos herramientas legítimas, ***WebBrowserPassView*** y ***Mail PassView de NirSoft***, que se utilizan para robar las credenciales almacenadas en los navegadores y clientes de correo electrónico de la víctima. Entre las funcionalidades de esta versión del troyano está finalizar la ejecución del *script* si detecta un entorno virtual como *Hyper-V*, *VirtualBox* o *VMWare*; también verifica que la computadora de la víctima tenga un código correspondiente a los idiomas español – España, portugués brasileño, español – México, portugués – Portugal o español. Si el sistema usa un ID de idioma diferente a los listados, el proceso de ataque se detiene, cosa que también ocurre si el nombre de la computadora es **"JOHN-PC".**

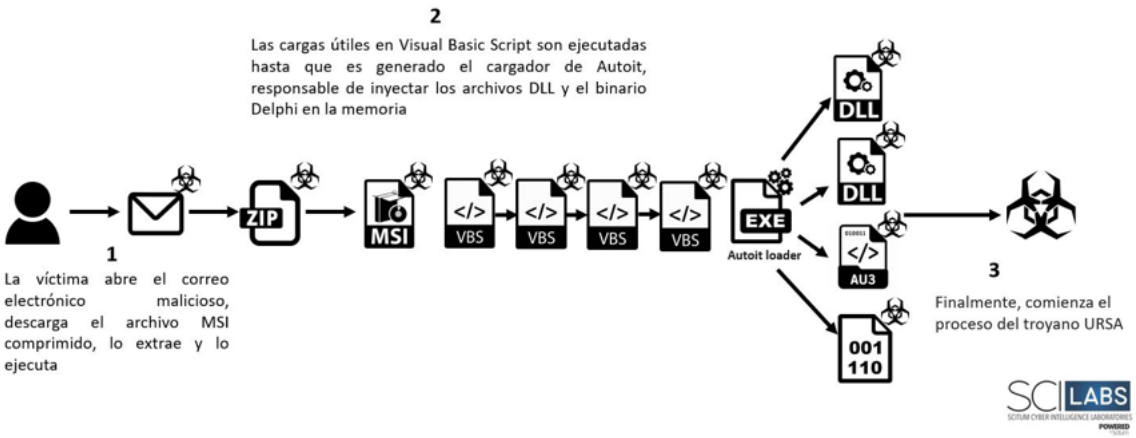


Figura 8 – Flujo de infección de la segunda campaña

Tercera campaña analizada por SCILabs

El análisis de SCILabs identificó que, con respecto a campañas anteriores de *URSA/Mispadu*, los *TTP* utilizados por los ciberdelincuentes han evolucionado. Además, el grupo de cibercriminales tiene una gran infraestructura para la distribución, almacenamiento y administración de computadoras infectadas con el troyano bancario *URSA/Mispadu*. Una vez que la víctima descarga y ejecuta el correo electrónico de phishing, se descarga otro archivo .vbs que realiza una solicitud *GET* a un archivo .xml en línea que contiene otro código .vbs. Este código funciona como un *dropper* para obtener los archivos: *Autoit* script y un cargador del ejecutable. El objetivo es inyectar en memoria una DLL maliciosa correspondiente a *URSA/Mispadu* y descargar los complementos necesarios para concluir su actividad maliciosa. **Flujo técnico** La víctima recibe el correo electrónico de *phishing,* relacionado con una supuesta factura, que contiene un archivo comprimido adjunto. Si la víctima lo extrae y lo ejecuta, el flujo de infección continúa como se muestra en el siguiente diagrama:

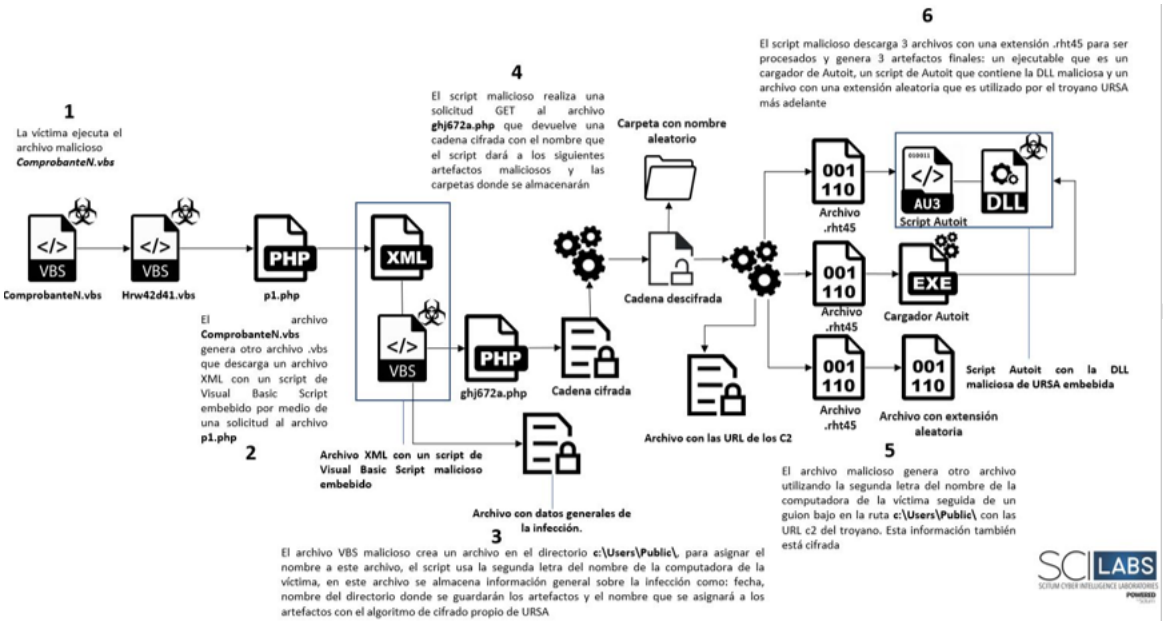


Figura 9 – Flujo de infección de la tercera campaña

Como se observó en la campaña anterior, para crear, descargar y procesar los artefactos de infección, el *dropper* verificará que el código de idioma de la máquina víctima sea español – España, español – México, portugués – Brasil, portugués – Portugal o español; además revisará que el equipo no tenga el nombre **"JOHN-PC"** y **que** no se esté ejecutando en una máquina virtual, tal y como se muestra en el siguiente diagrama:

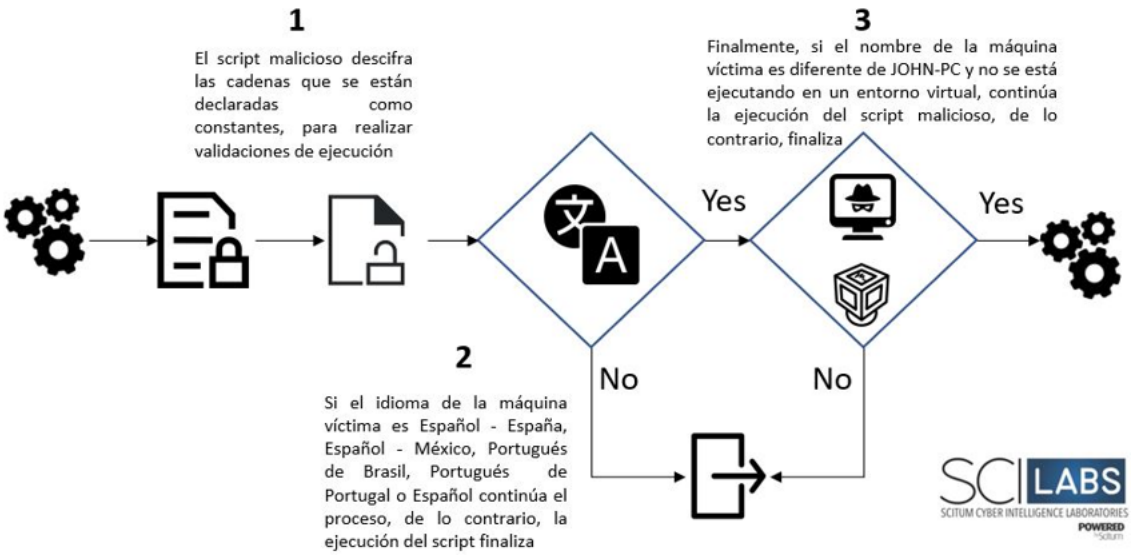
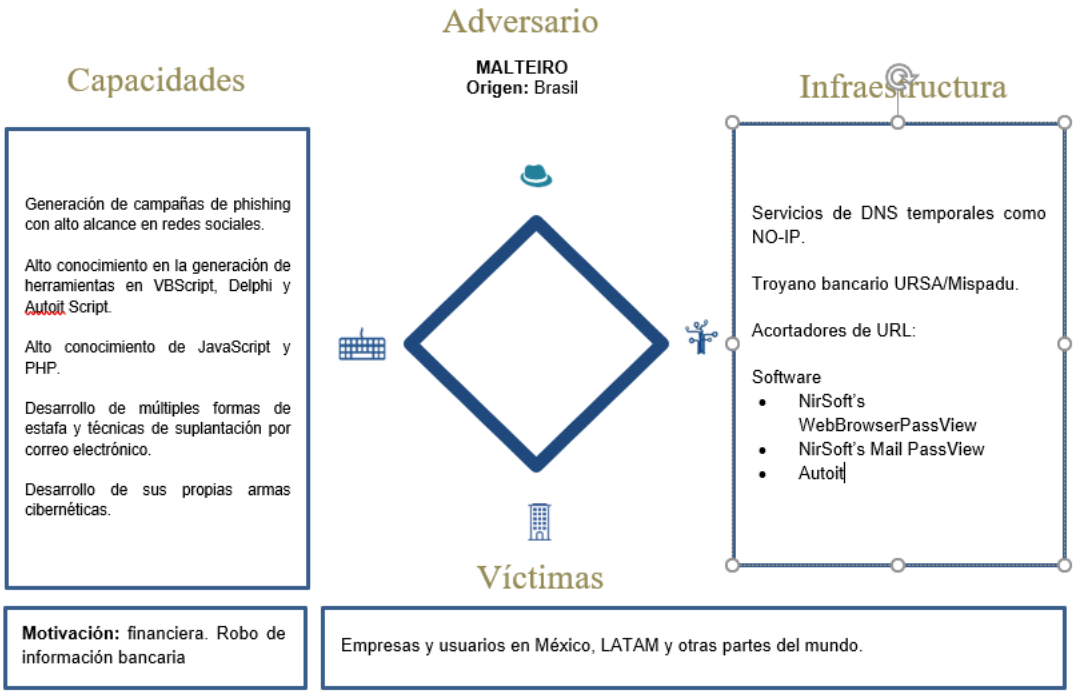


Figura 10 – Flujo de validación del script malicioso

Una vez que se generan los artefactos finales (*Autoit loader*, un *autoit* script con la DLL maliciosa y un archivo de extensión aleatoria), el *script* malicioso llamará al método *ShellExecute* y cargará el *script Autoit*, para continuar la infección. Cuando la *DLL* maliciosa se carga en memoria, se descargan dos carpetas comprimidas que contienen los archivos **ssleay32.dll** y **libeay32.dll,** que están asociados con el *kit* de herramientas *OpenSSL* utilizado por el troyano. En la última etapa, este *malware* puede crear ventanas bancarias apócrifas superpuestas en el navegador cuando las víctimas ingresan a portales bancarios, para robar sus credenciales. Además, el troyano utiliza dos herramientas legítimas (***WebBrowserPassView*** y ***Mail PassView***) para extraer las credenciales almacenadas en los navegadores y correo electrónico. Finalmente, los datos se envían al servidor de comando y control. Cuando el troyano detecta que una víctima ingresa a un portal bancario, establece una conexión con el servidor C2, con lo cual el ciberdelincuente gana el control de la computadora comprometida, permitiéndole utilizar diferentes comandos bajo demanda.

Modelo de diamante



Perfil de amenaza basado en la matriz MITRE (PRE-ATT&CK)

Con base en la investigación realizada por SCILabs, se obtuvo la siguiente matriz:

Reconnaissance	T1592.002-Software	T1592.004-Client Configurations	T1589.001-Credentials	T1589.002-Email Address	T1598.003-SpearPhishingAttachment		
Resource Development	T1583.001-Domains	T1583.003-Virtual Private Server	T1583.004-Server	T1586.001-SocialMediaAccounts	T1586.002-Email Accounts	T1587.001-Malware	T1585.001-Social Media Accounts

Perfilamiento de la amenaza basado en la matriz MITRE (ATT&CK)

Initial Access	**Execution**	**Persistence**	**Defense Evasion**	**Credential Access**	**Discovery**	**Collection**	**C&C**	**Exfiltration**
T1566.002-Phishing: Spearphishing Link	T1059.005-Command and Scripting Interpreter: Visual Basic	T1176-Browser Extensions	T1140-Deobfuscate/Decode Files or Information	T1552.001-Unsecured Credentials: Credentials in Files	T1083-File and Directory Discovery	T1056-Input Capture	T1573-Encrypted Channel	T1041-Exfiltration Over C2 Channel
	T1106-Native API	T1547.001-Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	T1036-Masquerading	T1081-Credentials in Files	T1057-Process Discovery	T1115-Clipboard Data	T1132.002-Non-Standard Encoding	
T1204.002–Malicious File		T1027-Obfuscated Files or Information	T1552.002-Unsecured Credentials: Credentials in Registry	T1518.001-Software Discovery: Security Software Discovery	T1113-Screen Capture	T1001-Data obfuscation		
	T1055.001-Dynamic-link Library Injection	T1555.003-Credentials from Web Browsers	T1010-Application window discovery	T1560-Archive Collected Data				
T1497-Virtualization/Sandbox Evasion		T1082-System Information Discovery	T1005-Data from local system					
	T1614-System Location Discovery	T1074-Data Staged						
T1497.001-System Checks								

Recomendaciones

- Realizar, en todos los niveles de la organización, campañas constantes de sensibilización sobre las diferentes técnicas de ingeniería social y *phishing*.
- Evitar descargar y ejecutar archivos adjuntos de correos electrónicos sospechosos, especialmente si tienen extensiones: “.exe”, “.vbs”, “.jar” y “.msi”.
- Crear políticas de contraseñas seguras y aplicar el principio de privilegio mínimo para los usuarios dentro de la organización.
- Mantener todo el equipo informático de la organización con las últimas versiones del sistema operativo y las actualizaciones de seguridad aplicadas.
- Considerar los indicadores de compromiso que se comparten en este documento.

IOC

Troyano bancario URSA/Mispadu D2099233A72C282E64E85ABCDDB284CDFFC18B24E088947254F9B55670F52F83
87340165EA0FB1E06364AA479ACB2FF104CEDDEAACE0E548F687B2960A28ED36
09886CE8106CD07A3694F221DD19899AA29A72826F2FEE8A8BAA1B044704737A
91A687ED27F469797317D82B8EB2BCEB4DFC84973B4BFB00F15E951DFDAEA9AE
0916767D0EAA4E3E94DAF740B621C62258832F3F811FE4FA1C9536227FCBEA17
C9E22D965771D8A8005D79B771AF602B95C14B0E23187ED4F718FFC0E87B26E2
4BDA083A30A82698F57F672C5A333ADC84F37FE53D8FED6D8AA7AA31ECAC02FC
02F541522898F87AA36552EAC38A70DC8A23B59E2BF6D4F65EE55485B05EDAAB