TREND MICRO | research

Spam Campaign Targets Colombian Entities with Custom-made 'Proyecto RAT,' Uses Email Service YOPmail for C&C

Appendix

In the spam campaign that we observed targeting the South American region, primarily Colombia, we saw a group use a second stage payload written in Visual Basic 6 that bears many similarities with “Proyecto RAT,” a remote access tool (RAT) that can be customized in a variety of ways. In our blog post, we analyze how this Visual Basic malware takes from a different project called "Proyecto RAT" and the ways it resembles the known Xpert RAT.

Technical analysis of the Visual Basic malware

Decompiling the malware reveals many classes, forms, and modules. Here we discuss its many features, such as the following:

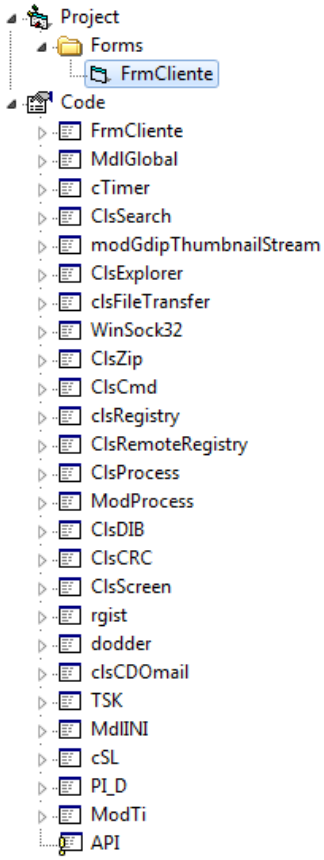

Figure 1. Decompiled RAT module

FrmCliente (as seen in Figure 1) is the main form of the malware written in Visual Basic. It has a few timers: Timer1, with interval 10000 ms, handles initializing Winsock communication to a C&C server and hardcoded port 4444. Timer2, with interval 15000 ms, reads the caption of the current foreground window. If the caption contains one of the following titles, it writes the caption of this window into the configuration file ("LocalOffice\Conf.ini"), section "DN", variable "CAP". CAP likely means “caption.” It also reports the caption back to the C&C server. As you can see below, these captions belong to banking and financial institutions in Latin America, particularly in Colombia.

::: BANCO DAVIVIENDA :::

AV VILLAS

Banca Colpatria Empresarial

Banca Virtual Personas

Banca Virtual Personas - Multibanca Colpatria

BANCO AGRARIO DE COLOMBIA

Banco Agrario de Colombia

Banco AV Villas

Banco Caja Social

Banco Colpatria

Banco de Bogot

Bancolombia Sucursal Virtual Personas

Bancoomeva Banca Empresarial::Coomeva la cooperativa de los profesionales

BBVAnet Colombia

Bienvenido a STransfer

Bitcoin Wallet

Credenciales

DashboardDavivienda

Despegar.com - Checkout de compra

Efecty

Falabella

https://www.bancopopular[.]com[.]co/cgi-bin/cgibbss[.]exe/CORE-Main%20Web/ND000_

Ingreso a transacciones

Inicie sesin en su cuenta PayPal

innerHTML

LocalFileTimeToFileTime

login Banca Empresas

Medios de pago | Avianca

OCCIRED

OFICINA VIRTUAL EMPRESARIAL

OFICINA VIRTUAL PERSONAL

Pagos portal empresarial [Modo de compatibilidad]

Pagos PSE

POR SU SEGURIDAD LE RECOMENDAMOS NO HACER TRANSACCIONES EN SITIOS PUBLICOS

Portal de pagos

Portal Empresarial Davivienda

PSE - Pago con Registro Persona Jur

PSE - Pago con Registro Persona Natural

PSE Colpatria Red Multibanca

Sucursal

Sucursal Virtual Empresas

TiquetesBaratos.com

TRANSUNION

VISITA NUESTROS SERVICIOS

Vuelos VivaColombia

Wallet

Western Union, Giros y Finanzas, Giros Nacionales, Giros Internacionales, Envios de Dinero.

www[.]davivienda[.]com

Timer3, with interval 3000ms, creates directories (LocalOffice, Sys) and files (*SpoolColorLV.exe*) in *%APPDATA%\Roaming* to which it copies malware under a hardcoded filename. The executable file attributes are set to *FILE_ATTRIBUTE_SYSTEM* + *FILE_ATTRIBUTE_HIDDEN*. It checks for present drives by calling *GetDriveType*, and in case of *DRIVE_REMOVABLE*, it writes the variable “USB” to the configuration file. It also establishes persistence via the registry and task scheduler.

FrmCliente also contains nine labels, named “label1” to “label9”, with each of them containing some variables that invoke actions based on the change of label captions. The most interesting ones are described below:

- Label2 writes the current date/time in the config file under section "DN", variable "NO" (variable NO contains C&C address). It sets the title of the hidden form to “On” or “CMD”, depending on the version of RAT involved.
- Label5 writes a value in the config file under section "DN", variable "PAC".
- Label6 writes a value in the config file under section "MI", variable "x8", where MI likely means microprocessor and x8 likely means x86.
- Label7 writes a value in the config file under section "MI", variable "x6", where MI likely means microprocessor and x6 likely means x64.

WebBrowser1 is an object containing an HTML page with a YOPmail disposable email. The C&C configuration is acquired from this email.

Form_Load contains events that happen just after the application starts. It connects to YOPmail, parses C&C configuration, then reads date/time of installation and banking website caption through the configuration file, section “DN”, variables “NA” and “CAP”.

Socket_DataArrival is a function that processes incoming communication. While processing the communication, the malware uses the string "¡@#@!" as a separator between incoming and outgoing streams. This marker is similar to the one used in a commodity RAT called Xpert RAT. It uses the following classes, forming the RAT functions of the malware.

ClsExplorer
ClsCmd
ClsRemoteRegistry
ClsProcess
ClsDesktop

The FrmCliente form is hidden, but by using certain utilities, we can make it visible. The figure below shows such a form with some filled information. GUIPropView (as seen in Figure 2) is the name of the first window, as well as the name of the utility that makes invisible windows visible. As for confe[.]linkpc[.]net, it is the current C&C server, with another label referring to the date and time of installation. At the center of the window is a WebBrowser object with loaded YOPmail email.

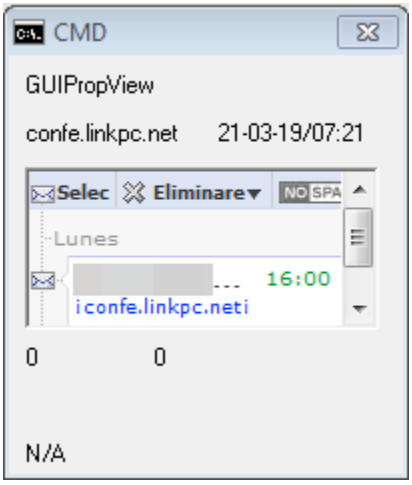

Figure 2. FrmCliente window once visible

Module MdlGlobal references to API functions *IsClipboardFormatAvailable, ClipBoard, GetText, SHFileOperation, GetLocaleInfo, GetUserName, GetComputerName, GetVolumeInformation, GetLogicalDriveStrings, WNetGetConnection,* to name a few, that collect all the required information about the current machine. Class cTimer calls API functions *SetTimer* and *KillTimer*, which create and destroy timers. The decompiled code reveals the string 558BEC50FF7514FF7510FF750CFF75086855555555B866666666FFD0C9C2100000000000, which after x86 decompilation, gives the assembly code below. This string is the second link to the Xpert RAT.

```
00000000 55                PUSH EBP
00000001 8BEC              MOV EBP,ESP
00000003 50                PUSH EAX
00000004 FF7514            PUSH DWORD PTR [EBP+14]
00000007 FF7510            PUSH DWORD PTR [EBP+10]
0000000A FF750C            PUSH DWORD PTR [EBP+0C]
0000000D FF7508            PUSH DWORD PTR [EBP+08]
00000010 6855555555        PUSH 55555555
00000015 B866666666        MOV EAX,66666666
0000001A FFD0              CALL EAX
0000001C C9                LEAVE
0000001D C21000            RET 0010
00000020 0000              ADD BYTE PTR [EAX],AL
00000022 0000              ADD BYTE PTR [EAX],AL
```

Figure 3. Decompiled string's assembly code

This code is an assembly language container. The purpose of the code, as described by the author of the original project from which the code was taken, is "For each instance, a separate TimerProc is called with a different address. An additional instance administration is omitted." If assembly code was not used, then "For each instance, the same WndProc with the same address is called – This requires additional management of the timer instances."

Class ClsSearch is a class with functions *FilterDateTime, MinFileSize, MaxFileSize, SearchInZipFolder, SearchInSubFolder,* and *SearchInSystemFolder*, which are used for searching files used in the ClsExplorer class.

Module modGdipThumbnailStream references API *CreateStreamOnHGlobal*, which is used for screen capture. Reference BB2E617C-0920-11d1-9A0B-00C04FC2D6C1 points to image handler IExtractImage.

Class ClsExplorer is a remote explorer class that implements various file operations. It uses clsFileTransfer and references *ShellExecute, clsZip,* and *clsSearch*. It contains the following error messages in Spanish:

"No se pudo copiar "	- could not copy
"No se pudo cortar "	- could not be cut
"Nueva carpeta"	- new folder
"No se pudo cambiar el nombre a"	- could not change the name to
"Acceso Denegado"	- access denied

Class clsFileTransfer is responsible for uploading files from the local directory *%appdata%\Sys\.*

Module WinSock32 contains socket operations and data transfer operations and references APIs *gethostbyname, Socket_Connect,* and *inet_ntoa.*

Class ClsZip contains zip and unzip functions, and is used by ClsSearch class.

Class ClsCmd implements a reverse shell by calling cmd.exe using "CreateProcessW," while *stdin, stdout,* and *stderr* are redirected to socket.

Class clsRegistry contains registry operations such as search, create, delete, rename, enum, and exist.

Class ClsRemoteRegistry uses clsRegistry class for registry operations.

Class ClsProcess lists windows, processes, CPU usage, and available free memory.

Module ModProcess enumerates and lists currently running processes and their information. It also contains the following error messages in Spanish: "Proceso inactivo del sistema" (inactive system process).

Class ClsDIB (Device-Independent Bitmaps) contains functions for working with bitmaps, calls APIs *GetDeviceCaps* and *CreateDIBSection*.

Class ClsCRC contains functions for calculating CRC checksum.

Class ClsScreen contains functions for working with the screen.

Module rgist could be referring to “remote gestures.” It parses C&C communication, does some remote gestures like mouse clicks, setting cursor position, and screen dimension changes. It references operations related to the screen dimension, clipboard, cursor, and mouse events.

Class clsCDOmail contains (CDO = Collaboration Data Objects) functions for parsing emails.

Module TSK contains functions for adding and removing task scheduler jobs.

Module MdlINI contains functions for writing and reading INI files.

Additional Spam Email Samples

We observed many versions of spam emails sent by this threat campaign. Here we show other document designs we encountered; all of these documents asked its recipients to enable macros that, in turn, will download and execute a RAT.

Figure 4. Delivery document purports to come from SIMIT, an “Integrated system of information on fines and penalties for traffic infractions.”

PARA VISUALIZAR DE FORMA CORRECTA EL CREDITO SOLICITADO Y LOS NUMEROS DE ATENCION AL CLIENTE ES NECESARIO HABILITAR EL CONTENIDO COMO LO MUESTRA LA IMAGEN

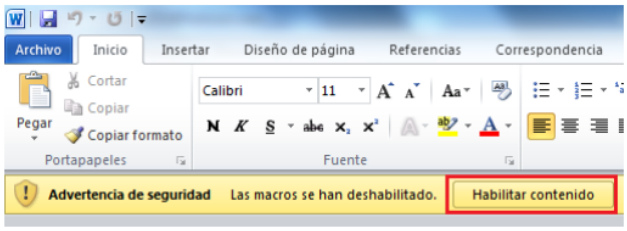

Figure 5. Delivery document purports to come from the bank Serfinansa

PARA VISUALIZAR LOS DETALLES DE LA TRANSFERENCIA QUE HA RECIBIDO ES NECESARIO HABILITAR EL CONTENIDO COMO LO MUESTRA LA IMAGEN A CONTINUACION

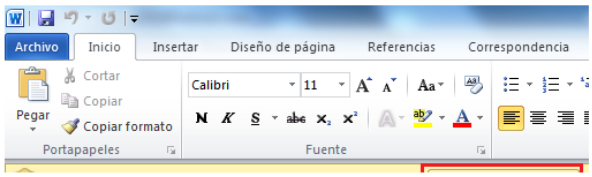

Figure 6. Delivery document purports to come from financial institution ACH Colombia

PARA VISUALIZAR SU REPORTE COMO CODEUDOR ES NECESARIO HABILITAR EL CONTENIDO COMO LO MUESTRA LA IMAGEN A CONTINUACION

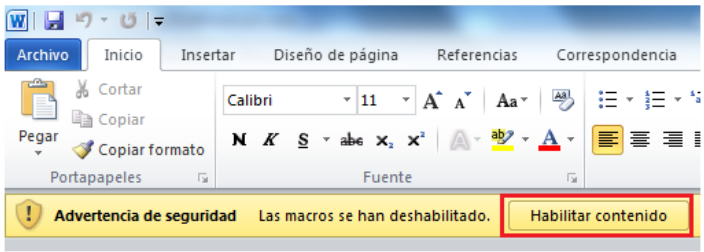

Figure 7. Delivery document purports to come from DataCrédito

Figure 8. Delivery document purports to come from Rama Judicial, a government portal for lawyers

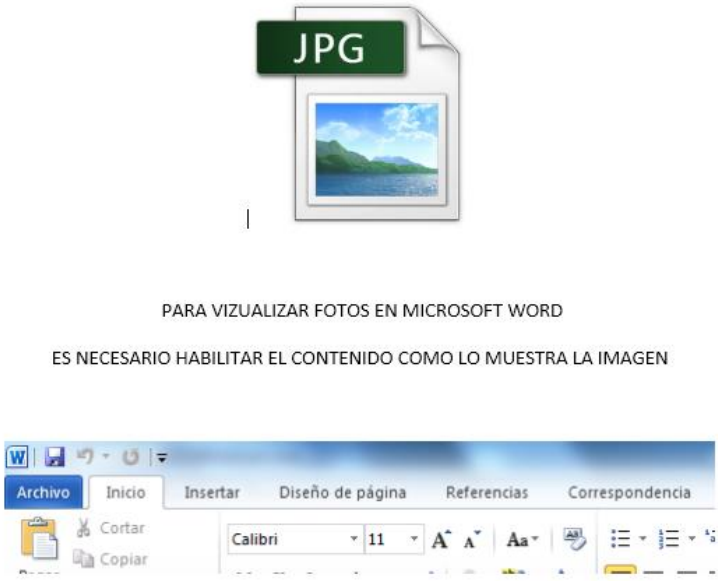

Figure 9. Delivery document with a generic JPG thumbnail

Indicators of Compromise (IoCs)

Note: This section contains only new samples acquired after the publication of the Qihoo360 report in February 2019.

Indicator	Trend Micro Detection	Note
17020564ea92228794d9cd8db51f101b66d56a654f6606c64040589a85f97470	Trojan.W97M.DLOADR.TIOIBEEU	Attachments
9959968a7cdfa1ac21d5ad45f341e9f25c6ec931a786c3231e851abe4d5fa138	Trojan.W97M.DLOADR.TIOIBEEU	Attachments
cb6d613402a5191aad7fc9245a63bca27cae465d7b669f65eadad7bac654c164	Trojan.W97M.MALINK.N	Attachments
66a745b77810b0dc02c9d6bd8a4576b61c86befa8ff6bd76358091edaa965569	Trojan.W97M.PHISH.RFD	Attachments
308a67ed89716a959752514b18dfd2ce3250b56271c23e259c710f1bbee62503	Trojan.W97M.MALINK.N	Attachments
6fde92ec0f74ccec633dc5a8e79775d4be97beb7ff873523236770480f322214	Trojan.W97M.MALINK.N	Attachments
bbc60cf2fac391e87c331cfebf5099693afc84a9bcde3cc34bf96649937ff4d8	Trojan.W97M.MALINK.N	Attachments
010c7e44459efb676037c42e49bcfa5739cf6e79cf124412bf8d036f089d35ed	Trojan.W97M.MALINK.N	Attachments
633ce7e6316542d818c4508f1748f882a2023e16f9c8176718be5decf53849f5	Trojan.W97M.MALINK.AD	Attachments
54f62dc39a0519acf3778a1f983773abfffd217035f74112f636cd3d85006753	Trojan.W97M.MALINK.AE	Attachments
3a43ba1f2e65291dd0093eb30f76280874d2db869e052e3976a585ed93a73b89	Trojan.W97M.MALINK.N	Attachments
4EF15CF9F016466BFDA02E7C624795F126AE7FEA36496AB4C19CC64B3833FA54	Backdoor.MSIL.SHADESRAT.AI	Imminent RAT
455add204b7f78291358bf2f6aae05738ba12913bcfb34f2c4a614bffe7c8787	Backdoor.MSIL.SHADESRAT.AI	Imminent RAT
39b5be95913c9914119f59c19ae255107d12d1a403b7c93edc7373fc4d6e50df	Backdoor.MSIL.SHADESRAT.AI	Imminent RAT
20D737E204B33AED75A8AF762F615694C8C4F72D97EB845194C56001BB0F8CEB	Backdoor.MSIL.SHADESRAT.AI	Imminent RAT
89a26a53852b698dedae8e32df73c58fc52e851cd24833c1dacf9cd68b106f18	Backdoor.MSIL.SHADESRAT.AI	Imminent RAT
2CE1C5D236757211D56196ECFB7BF4957931A33C609F21BD5BFD5658736F2D4F	Backdoor.MSIL.SHADESRAT.AI	Imminent RAT

838B0273DE3757CF28F10053B70621A8AB1DAAF175846F770D30F0287A68F280	Backdoor.MSIL.SHADESRAT.AI	Imminent RAT
d3cb1c338575a376088dd2a9ab89c248ce28ba12d48512e3e855f00714fd9b07	Backdoor.MSIL.SHADESRAT.AI	Imminent RAT
26449a7ca13c0419692dc20641022232680211cf2b181c87e50c1802b005b7b2	Backdoor.MSIL.SHADESRAT.AI	Imminent RAT
2de0cd906b4dcdd17a35ee3a1edae46f115c7adcfa62cd771da18893b788a7da	Backdoor.MSIL.SHADESRAT.AI	Imminent RAT
13747da2dc6d5e123a657f63178aa44bb811c3f03bf49607bb46bd8f412a102f	Backdoor.MSIL.FYNLOSKI.AA	Imminent RAT
436611717cf191ce60d159643e082d83dc6d3dae95965e30aa248385c8e3decb	TrojanSpy.MSIL.IMMONRAT.AA	Imminent RAT
88bd7d3746595c32e927596d1c761908e3ebf1240386bae971f925e9bd50b023	TrojanSpy.MSIL.BOILOD.AA	Imminent RAT
ac7592b651f35ed48262c009e993030c166b824002f71d427340177d11a88092	TrojanSpy.MSIL.BOILOD.AA	Proyecto RAT / Xpert RAT
52501a2c19758d825b9fd6bbfe70d47fda24ffbfe15a5441a44f791af8b8c705	TrojanSpy.Win32.BOILOD.AA	Proyecto RAT / Xpert RAT
8F839A36958BE2C8301DA94D669A1513956CB9511090D3B9113176927A272E3D	Trojan.MSIL.BOILOD.SM4.hp	Proyecto RAT / Xpert RAT
E4B482D1FF18344C380E5B7AF97E88B57E82826B693290FD2BDA12CE4A568D28	TrojanSpy.MSIL.BOILOD.AA	Proyecto RAT / Xpert RAT
d0fc383de8ea4108d24f85059f8aef234ba0f933097240b22c3afe4782083770	TrojanSpy.MSIL.BOILOD.AA	Proyecto RAT / Xpert RAT
a22b27af3f245e8f1641be994b3ac2dbe97de88676334bc109fe901ceec88610	TrojanSpy.MSIL.BOILOD.AA	Proyecto RAT / Xpert RAT
2525156f5a41b3e667141c2575a6b6f5dcaea30b317c7ec07038964cb6810293	TrojanSpy.MSIL.BOILOD.AA	Proyecto RAT / Xpert RAT
1b22eff27b7bb373e8bc529413b389a10a714fe87da31e1f2bb03e43b013375d	BKDR_HPBLADABINDI.SMZ	Proyecto RAT / Xpert RAT
b07cf78fccbe4df92d24a272d89f760e893707204581577df4ed0c942220d9d7	Backdoor.MSIL.XRAT.AA	Proyecto RAT / Xpert RAT
beb04adf9eae6a0b0bec01140a864e9cce4755cebee9c1958270e3a383e129c6	Backdoor.MSIL.XRAT.AA	Proyecto RAT / Xpert RAT
453f2e74f83db5ea9ad5f396468f3f57044c983d28994a36b199f3b13024aed2	Backdoor.MSIL.XRAT.AA	Proyecto RAT / Xpert RAT
c9cecaf200b7099b7adf0eb00ea38c412dfe38836ac62a20066fac1ec70ebdc3	Backdoor.MSIL.XRAT.AA	Proyecto RAT / Xpert RAT
dde4b700ecb15433757619e022542d63957b594675f1b74f3858f101f1fe8468	Backdoor.MSIL.XRAT.AA	Proyecto RAT / Xpert RAT

af4a9c25496392f184ccfc0ae0f24c55f065193bb7246275b30abc89f3d40b69	Backdoor.MSIL.XRAT.AA	Proyecto RAT / Xpert RAT
80d416d3b4365da4e75ba83de050077d46f4111c2af098c21694a30a86d42cfe	TrojanSpy.MSIL.AVEMARIA.C	Warzone RAT
392ce9a1be9b7a5117c467225ffcb82cfa565f75454d3b805ff89df1b5269161		Email samples
4e1612af9299f3d9e788de6b6d1c6bf8e4cd91dd9b0a8adcfc430cf84916f280		Email samples
ceda4f437d7b446e1d9fd0acbc67660a777aefbf11aa9142045ffbcc4a4a06f6		Email samples
22a58844102bf2ac85d07e4af3aaada94c2fd07515b7989785cff0368d4186d4		Email samples
171d0de9e9ec9dcf4912779f3fce2c27ef69a56067bd542a38bf07c58d69443c		Email samples
f55d3e1e34624d2281925abf4a7d97fbf376c942f60c2c9ee5198979d0aae751		Email samples
1b2e649ee6063c39fcfade8fe7b87f7ea4ce66bcb4efe3622e3ba8580d1860b0		Email samples
56c29d66b5509c1192042c4ec1a6f6ee8924502d8503de4f1ef0de2edf1b0df7		Email samples
3ec7caa9fca34652fed6a5ba58c2ff5487261b1d907a7208b4b2ee89eee24c71		Email delivery documents
462983fbf30891c7e746345c84ebb2ec06618e80e3f099ab7634b0410501d2a6		Email delivery documents
b763d7f59864aacc9b4af6c74fee1caafd950b66db667082e84a787c32b983de		Email delivery documents
96cfdfb176b2ccdc4fffda1abaaf158dd9acf55fba6a0437a7087773240f14fe		Email delivery documents
4f835e9766cbef7b243ad5dd97d61530cf00053a5fd247725bfd5f8485185110		Email delivery documents
e73c3f9c1ee5695482dfe45d1b71fe84ca5ba921ee66465f0bfba8725dde47e7		Email delivery documents
c042f1a3cfd1941fb4b3570bfa07b6539dfb4d0243a61e6f8309c6e3ddd5380f		Email delivery documents
4703585c610740dec855aa2c60fa1434bece3a91df79b34ddffab7cbd5f0e7eb		Email delivery documents

ec78c397446c17fd68cadb0933e70a75201e79ecb46fc3a9710b253a90f1fae8		Email delivery documents
22de033ac312613daedfbb0ccf7399e12f72165179dddd03eb7e6a1e3ae0e8c3		Email delivery documents
c4ca6ba35556d0535fefc84c1b92d94b738c5916e19669529717c72de079ff89		Email delivery documents
28ae97b9a92bc7eb9013e84aad7373f104191712f9adf3a2a8b06e0abb3b4fb5		Email delivery documents
c26514bab11d961f230e800553de663fd247a6627242014e290b519b25ef33c5		Email delivery documents
ceosas[.]linkpc[.]net		C&C URLs
confe[.]linkpc[.]net		C&C URLs
medicosco[.]publicvm[.]com		C&C URLs
medicosta[.]linkpc[.]net		C&C URLs
perfect1[.]publicvm[.]com		C&C URLs
hxxp://95[.]179[.]168[.]23/pf[.]exe		Payload delivery URLs
hxxp://144[.]202[.]19[.]31/pf[.]exe		Payload delivery URLs
hxxp://diangovcomuiscia[.]com/media/a[.]jpg		Payload delivery URLs
hxxp://eltiempocomco[.]com/bogota/pf[.]exe		Payload delivery URLs
hxxp://eltiempocomco[.]com/f[.]jpg		Payload delivery URLs
hxxp://eltiempocomco[.]com/pf[.]exe		Payload delivery URLs
hxxp://medicosempresa[.]com/image/l[.]jpg		Payload delivery URLs
hxxp://medicosempresa[.]com/image/win[.]jpg		Payload delivery URLs

TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threats techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com