

 **BlackBerry**® Intelligent Security. Everywhere.

# ***VISIÓN TÁCTICA DE LAS AMENAZAS EN AMÉRICA LATINA***

2023-03-03



Jose Luis Sánchez Martínez  
**Senior Threat Researcher**

# SOBRE MI



- Senior Threat Researcher en BlackBerry Cylance – España
- Miembro de Ad-hoc Working Group on Cyber Threat Landscapes ENISA (Unión Europea)

 @Joseliyo\_Jstnk

 [linkedin.com/in/joseluisssm/](https://www.linkedin.com/in/joseluisssm/)

# Agenda

- ▶ Introducción
- ▶ Enfoque
- ▶ Análisis de campañas en países de LATAM
- ▶ Conclusiones

# Visión estratégica de amenazas en Iberoamérica



¿Dónde está Carmen Sandiego? Exponiendo a los Enemigos Ocultos en Iberoamérica

Presentación realizada en las IV Jornadas Ciberdefensa ESPDEF-CERT & XVI Jornadas STIC CCN-CERT por @aboutsecurity & @Joseliyo\_Jstnk

[https://www.youtube.com/watch?v=1MUmX1kx\\_wE](https://www.youtube.com/watch?v=1MUmX1kx_wE)

<https://github.com/blackberry/threat-research-and-intelligence/tree/main/Talks/2022-11-25%20-%20XVI%20Jornadas%20STIC%20CCN-CERT>

# Introducción

América Latina al igual que España están muchas veces en “la sombra” debido a que no se publica mucha información sobre intrusiones, sin embargo, existen diferentes campañas activas en algunos de estos países o ataques arbitrarios que son interesantes de conocer para mejorar nuestras capacidades defensivas.

- No es tan interesante como lo que sucede en Estados Unidos, Irán, Rusia y otros países
- Muchos security vendors no tienen negocio en América Latina, por lo que no se esfuerzan en investigar que sucede

# Audiencia

- Comportamientos a bajo nivel
- Posibles oportunidades de detección
- Técnicas utilizadas



- Analistas de SOC
- Analistas de DFIR
- Threat hunters
- Ingenieros de detección



# Enfoque

## CIBERCRIMEN

- Ataques más genéricos, pero con impacto en muchas organizaciones
- Menos sofisticados y preparación
- Menos recursos para llevarlos a cabo

## AMENAZAS AVANZADAS

- Ataques más precisos y con motivaciones muy específicas
- Más sofisticados y larga preparación para que todo salga bien
- Más recursos para llevarlos a cabo

# Datos utilizados

Toda la información incluida en esta presentación, es información real de malware utilizado contra países de América Latina en los tres primeros meses de 2023 (enero, febrero, marzo).



# APT-C-36 > Colombia y Ecuador

APT-C-36 (también conocido como Blind Eagle) es un grupo que se sospecha que tenga como origen América Latina.

Su principal objetivo es Colombia, aunque otros países como Ecuador y España también han tenido impacto durante sus operaciones



<https://blogs.blackberry.com/en/2023/02/blind-eagle-apt-c-36-targets-colombia>

# APT-C-36 > Colombia y Ecuador

Hasta la fecha, se han visto tres formas diferentes con las que APT-C-36 han iniciado sus intrusiones.

1. Email -> Archivo adjunto .uue
2. Email -> Archivo adjunto .pdf -> PDF con link a un servicio URL shortener -> Redirección del servicio URL shortener a Discord para realizar la descarga de un archivo .uue
3. Email -> Archivo adjunto .pdf -> PDF con link a un servicio web temporal creado por APT-C-36 -> El servicio web tiene un botón para la descarga de un archivo .uue desde Discord

# APT-C-36 > Adjunto y link (colombiano)

Subject: Sírvase comparecer dentro de los cinco (5) días siguientes al envío de la presente comunicación  
From: Fiscalía General de la Nación Sede 05<trach-test@sofona.info>

<<https://www.fiscalia.gov.co/colombia/wp-content/uploads/LOGO-WEB-2.png>>

Citación - Notificación Personal

Bogotá- Cundinamarca

Sírvase comparecer dentro de los cinco (5) días siguientes al envío de la presente comunicación, a diligencia de notificación personal, en las oficinas del Grupo de Contratación de Bienes y Servicios

para más información en el link de descarga...

A continuación, podrá descargar su citación

[https://www.fiscalia.gov.co/colombia//cd2451a691901c6a5420/Citaci\\_n\\_73295.R22](https://www.fiscalia.gov.co/colombia//cd2451a691901c6a5420/Citaci_n_73295.R22) <<https://gtly.to/2hDU8C7-X>>

clave para abrir su citacion : 2023

De igual manera hemos adjuntado su citación

Atentamente,

Fiscalía General de la Nación Sede 05

Diagonal. 22B # 52- 01 (Ciudad Salitre)

+57 57(1)570 20 00 -57(1)414 90 00

Abierto · Atendemos hasta 5: PM



BOGOTÁ D.C 28 DE FEBRERO DEL 2023

REFERENCIA: ORDEN DE CITACION UNICO AVISO.

Nº DE PROCESO: 01-0001-005-00-02-2023

Cordial Saludo

Con el fin garantizar el Derecho a la Defensa y darle Tramite a la Diligencia establecida en su contra por el presunto **DELITO DE ABUSO DE CONFIANZA AGRAVADO** y conforme a lo establecido en la ley 1220 art 10 del CPP, este despacho le solicita atender el Requerimiento enviado, para rendir **DECLARACIÓN JURAMENTADA** dentro del proceso llevado en su contra que se dará inicio **EL 01 DE MARZO DEL AÑO 2023**.

Para mayor veracidad nos permitimos anexas información sustancial de los motivos que dieron lugar a la presente diligencia.

Procesos jurídicos Consulte detalles de su Proceso AQUÍ:

<https://www.ramajudicial.gov.co/portal-fiscalia/comunicadojudicial.gov.co>

Por motivos de seguridad y para la visualización de los documentos judiciales por favor ingresar la contraseña: **2023**

Atentamente;

CINDY PALACIOS DELGADO  
Asistente Fiscal

Ciudad Bogotá - Colombia  
Comandante: 56 (1) 570 10 00 - 571 414 90 00  
Atención Dirección Protección y Asistencia: 01 80005 2280 5711 41490754  
Bogotá - Colombia



[https://cdn.discordapp.com/attachments/1079976570845921396/1079976664748007424/CITACION\\_FISCALIA\\_DETALLES-PDF.uue](https://cdn.discordapp.com/attachments/1079976570845921396/1079976664748007424/CITACION_FISCALIA_DETALLES-PDF.uue)



<https://cutt.ly/w8g5VWT>

# APT-C-36 > Contenido web creado

[Dian\\_impuestos\\_2023.pdf](#)



## Estimado/a contribuyente

En la DIAN mantenemos nuestro compromiso de brindarle la asistencia y los servicios necesarios, para que pueda cumplir de manera oportuna y correcta, con sus obligaciones tributarias. Por ello le recordamos que se encuentra en mora con sus obligaciones por un valor adeudado de TRES MILLONES DOSCIENTOS CINCUENTA Y DOS MIL CON CIENTO CUARENTA PESOS \$ 3'252.140 M/CTE con 35 días en mora debido a la falta de compromiso en sus obligaciones financieras regulado en la ley 0248 del año 2005 numeral 12. A continuación, ponemos a su disposición el PDF Virtual con todos los detalles de sus obligaciones generadas a la fecha. Evite un proceso de embargo y pague oportunamente. En el siguiente enlace encontrará la factura de cobro en formato PDF

[https://dian\\_notificaciones\\_contribuyentes-radicado.website.org/](https://dian_notificaciones_contribuyentes-radicado.website.org/)

Para visualizar el documento digitar la contraseña: 2023

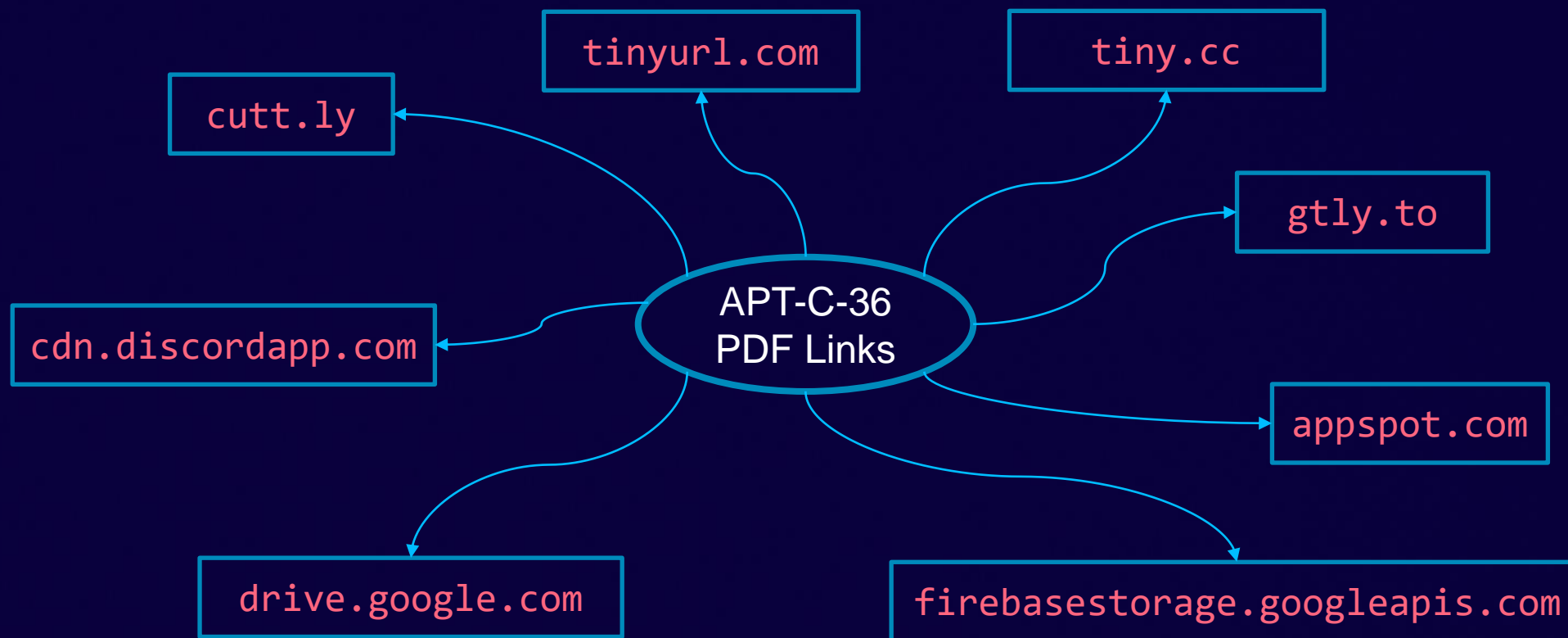
ROBERTO MENDOZA ORTIZ  
Jefe : Dept,embargo financiero

[https://dian\\_notificaciones\\_contribuyentes-radicado.website\[.\]org/](https://dian_notificaciones_contribuyentes-radicado.website[.]org/)



[https://cdn.discordapp\[.\]com/attachments/1075957625696555011/1077934591685431327/DIAN\\_impuesto\\_A\\_pagar\\_2023\\_00000008546978124\\_212\\_2023\\_02\\_22.pdf.uue](https://cdn.discordapp[.]com/attachments/1075957625696555011/1077934591685431327/DIAN_impuesto_A_pagar_2023_00000008546978124_212_2023_02_22.pdf.uue)

# APT-C-36 > URL shorteners utilizados




# APT-C-36 > Colombia y Ecuador

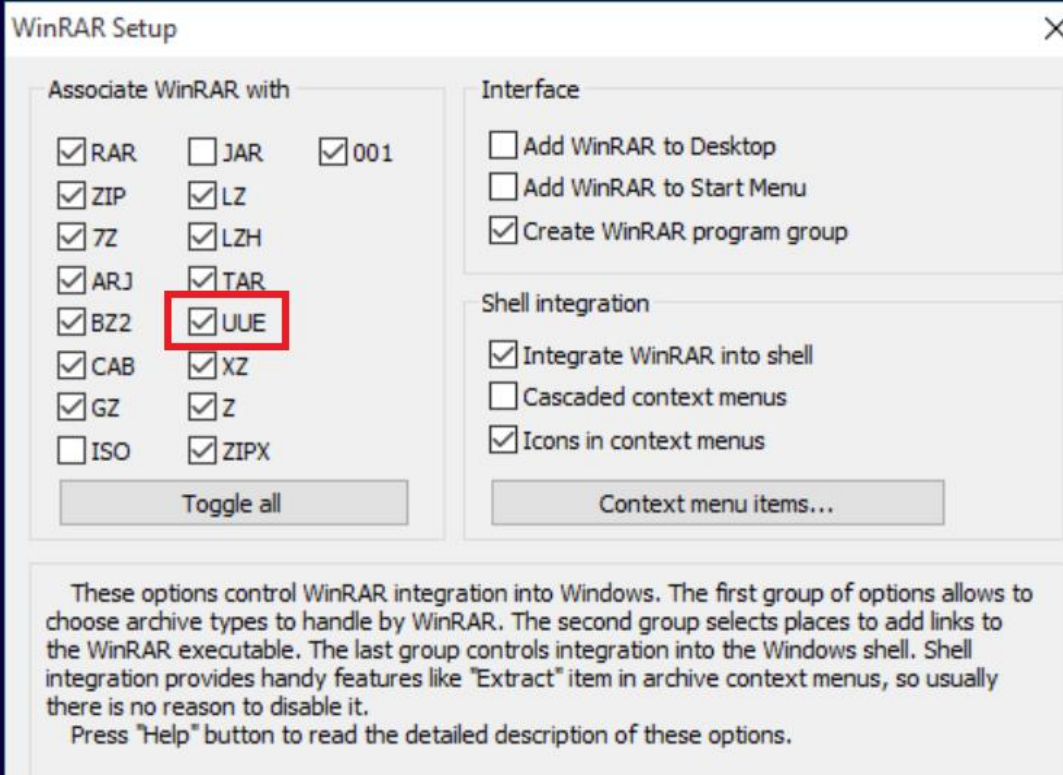
```
alert dns $HOME_NET any -> any any (msg:"ET DNS Query for .to TLD"; dns.query;  
content:".to"; endswith; fast_pattern; classtype:bad-unknown; sid:2027757; rev:5;  
metadata:affected_product Any, attack_target Client_Endpoint, created_at 2019_07_26,  
deployment Perimeter, former_category DNS, signature_severity Minor, updated_at  
2020_09_17;)
```

```
alert tls $HOME_NET any -> $EXTERNAL_NET any (msg:"ET INFO Observed Discord Domain  
(discordapp .com in TLS SNI)"; flow:established,to_server; tls.sni; dotprefix;  
content:".discordapp.com"; endswith; classtype:misc-activity; sid:2035464; rev:3;  
metadata:created_at 2022_03_15, former_category INFO, signature_severity Informational,  
updated_at 2022_09_21;)
```



# APT-C-36 > Colombia y Ecuador

Name	Size	Packed Si...	Modified
 Asuntos_DIAN_N°6440005403992837L2088970004-01-02-2023-pdf.vbs	227 378	1 811	2023-01-31 23:01



El siguiente archivo después del PDF recibido por email que el usuario descarga en sus sistema es un archivo comprimido .uue.

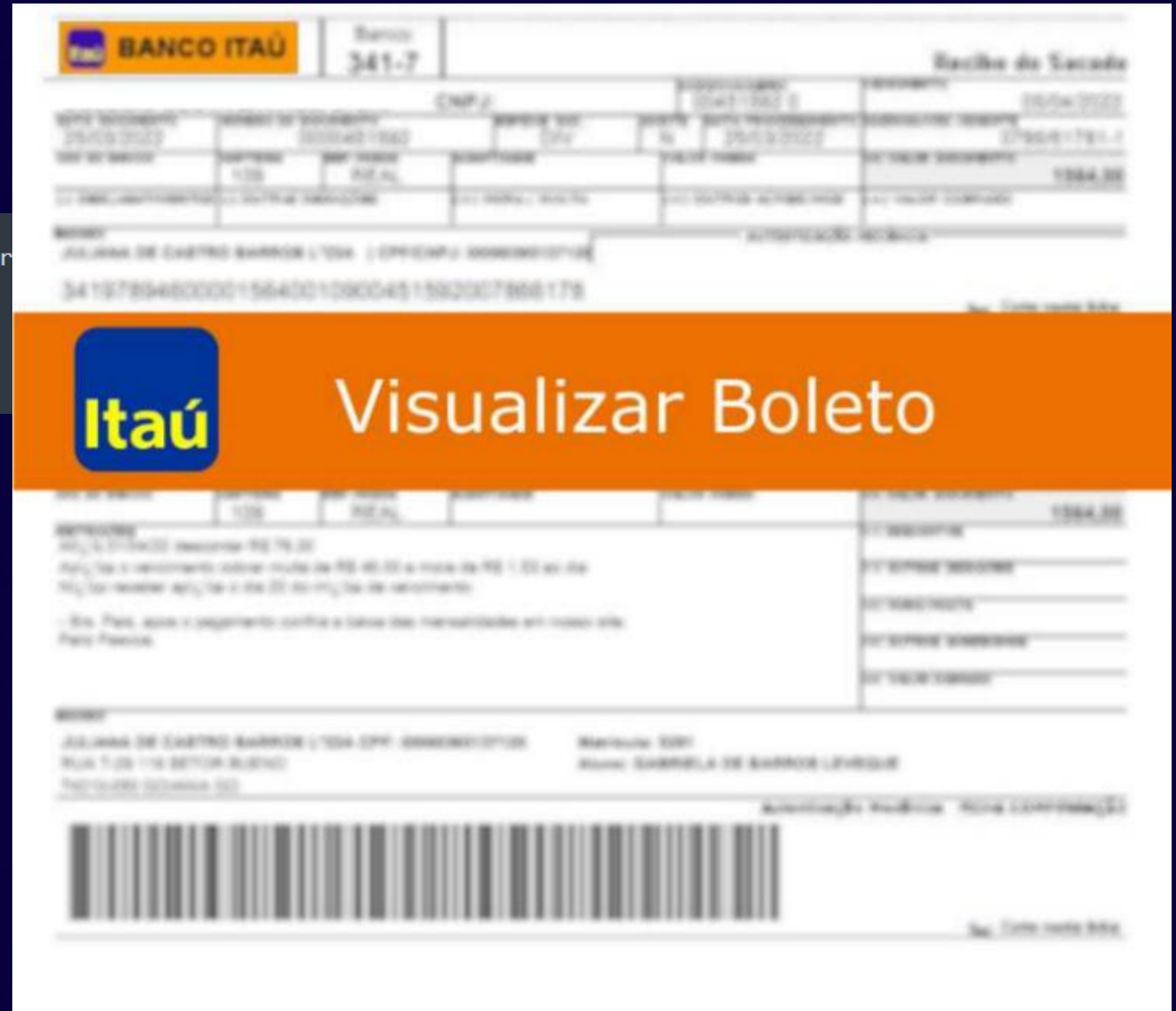
Este archivo contiene un visual basic script (vbs) el cual tiene el mismo nombre que el archivo .uue, y a partir de su ejecución comienza la infección.

Finalmente, la intrusión termina desplegando un RAT (AsyncRAT, NjRAT, QuasarRAT, etc...) realizando una conexión a un servidor DuckDNS

# Brasil, tierra de troyanos

Subject: Lembrete de vencimento! - Pedido: 92722  
 From: contato.fernandajoiias@vd220220230942963258741brc.broservicios.stor  
 To:

SEGUIE ANEXO O BOLETO NO VALOR DE 3.285,43 REFERENTE AO MES DE FEVEREIRO





# Dime de donde vienes

```
Request URL: http://fernandajoias.flmservicios.store/FevereiroDe2023/?Recalculado
Request Method: GET
Status Code: 302 Found
Remote Address: 81.200.156.9:80
Referrer Policy: strict-origin-when-cross-origin
Response Headers
Connection: Keep-Alive
Content-Length: 3
Content-Type: text/html; charset=UTF-8
Date: Wed, 01 Mar 2023 19:41:15 GMT
Keep-Alive: timeout=5, max=100
Location: https://www.google.com
```

View source

El archivo PDF realiza una conexión a un dominio, el cual, si es visitado desde una IP fuera de Brasil no realiza la descarga del payload. En este caso, se puede observar como se hace una redirección a Google

# Dime de donde vienes

```
Request URL: http://fernandajoias.flmservicios.store/FevereiroDe2023/?Recalculado
Request Method: GET
Status Code: 302 Found
Remote Address: 81.200.156.9:80
Referrer Policy: strict-origin-when-cross-origin
▼ Response Headers
Connection: Keep-Alive
Content-Length: 3
Content-Type: text/html; charset=UTF-8
Date: Wed, 01 Mar 2023 19:36:04 GMT
Keep-Alive: timeout=5, max=100
Location: https://www.dropbox.com/s/ea0uk9tccvbvs4i/SLEEP.zip?dl=1
```

[View source](#)

[https://www.dropbox\[.\]com/s/e a0uk9tccvbvs4i/SLEEP.zip?dl=1](https://www.dropbox[.]com/s/e a0uk9tccvbvs4i/SLEEP.zip?dl=1)

Sin embargo, si la petición proviene de una dirección IP brasileña, en este caso se realiza la descarga del siguiente payload a través de Dropbox.


# Los secretos de los MSI brasileños

Action	T...	Source	Target
AI_DOWNGRADE	19		4010
AI_SET_ADMIN	51	AI_ADMIN	1
AI_CORRECT_INSTALL	51	AI_INSTALL	{}
AI_SET_INSTALL	51	AI_INSTALL	1
AI_SET_MAINT	51	AI_MAINT	1
AI_SET_PATCH	51	AI_PATCH	1
AI_SET_RESUME	51	AI_RESUME	1
AI_RESTORE_AI_SETUPEXEPATH	51	AI_SETUPEXEPATH	[AI_SETUPEXEPATH_ORIGINAL]
AI_BACKUP_AI_SETUPEXEPATH	51	AI_SETUPEXEPATH_ORIGINAL	[AI_SETUPEXEPATH]
SET_APPDIR	307	APPDIR	[AppDataFolder][Manufacturer]\[ProductName]

Nombre	Tamaño	Tamaño co...	Creado
Binary.Project1.dll	5 629 440	5 629 440	
Binary.aicustact.dll	382 624	382 976	
!_StringData	82 346	82 432	


Action	Error	Message
Project1.dll	0	{{Erro fatal: }}
SET_SHORTCUTDIR	1	{{Erro [1]. }}
SET_TARGETDIR_TO_APPDIR	2	Aviso [1].
AI_InstallModeCheck	3	
AI_SHOW_LOG	4	Informação [1].
AI_DpiContentScale	5	O instalador encontrou um erro inesperado ao instalar este pacote. Isto pode indicar um problema com este pacote. O código do erro é [1]. {{Os argumentos são: [2], [3], [4]}}
AI_EnableDebugLog	6	
AI_PREPARE_UPGRADE	7	{{Disco cheio: }}
AI_RESTORE_LOCATION	8	Ação [Time]: [1]. [2]
AI_ResolveKnownFolders	9	[ProductName]
AI_DETECT_MODERNWIN	10	{{[2]}}, [3]}, [4]}
	11	Tipo de mensagem: [1], argumento: [2]
	12	=== Registro log iniciado: [Date] [Time] ===
	13	=== Registro log parado: [Date] [Time] ===
	14	Início da ação às [Time]: [1].
	15	Fim da ação às [Time]: [1]. Valor de retorno: [2].
	16	Tempo restante: {[1] minutos }{[2] segundos}
	17	Memória insuficiente. Feche outras aplicações antes de tentar de novo.
	18	O instalador não está respondendo

# Banload trojan



Community Score

! 22 security vendors and no sandboxes flagged this file as malicious



de6dcb5b92e41d3c5087c204da58a303851a749a52b0aa0598e035ea6675aa60

C:\Users\user\AppData\Local\Temp\hg1xk4ev.avr\DanfDigitaEletronic 010320239631 WLFELRTBMECASECMLTBR.msi

TBR.msi


msi

5.93 MB

Size

2023-03-01 15:29:05 UTC

19 hours ago




DETECTION
DETAILS
RELATIONS
BEHAVIOR
CONTENT
TELEMETRY
COMMUNITY 1


**Submissions**  ⓘ

Date	Name	Source	Country
2023-02-27 17:22:47 UTC	BOLET0 VENC 28022023 WLVRECFVBNZAWSVFMLTMS.msi	d5d9c0df - web	BR
2023-03-01 15:28:57 UTC	DanfDigitaEletronic 010320239631 WLFELRTBMECASECMLTBR.msi	5f8b3391 - community	BR

**Submissions per country**



**Submissions per Date**



**Prevalence summary**

First Submission	2023-02-27 17:22:47 UTC
Last Submission	2023-03-01 15:28:57 UTC
Last Rescanned	2023-03-01 15:29:05 UTC
Total Submissions	2
Source submissions	2

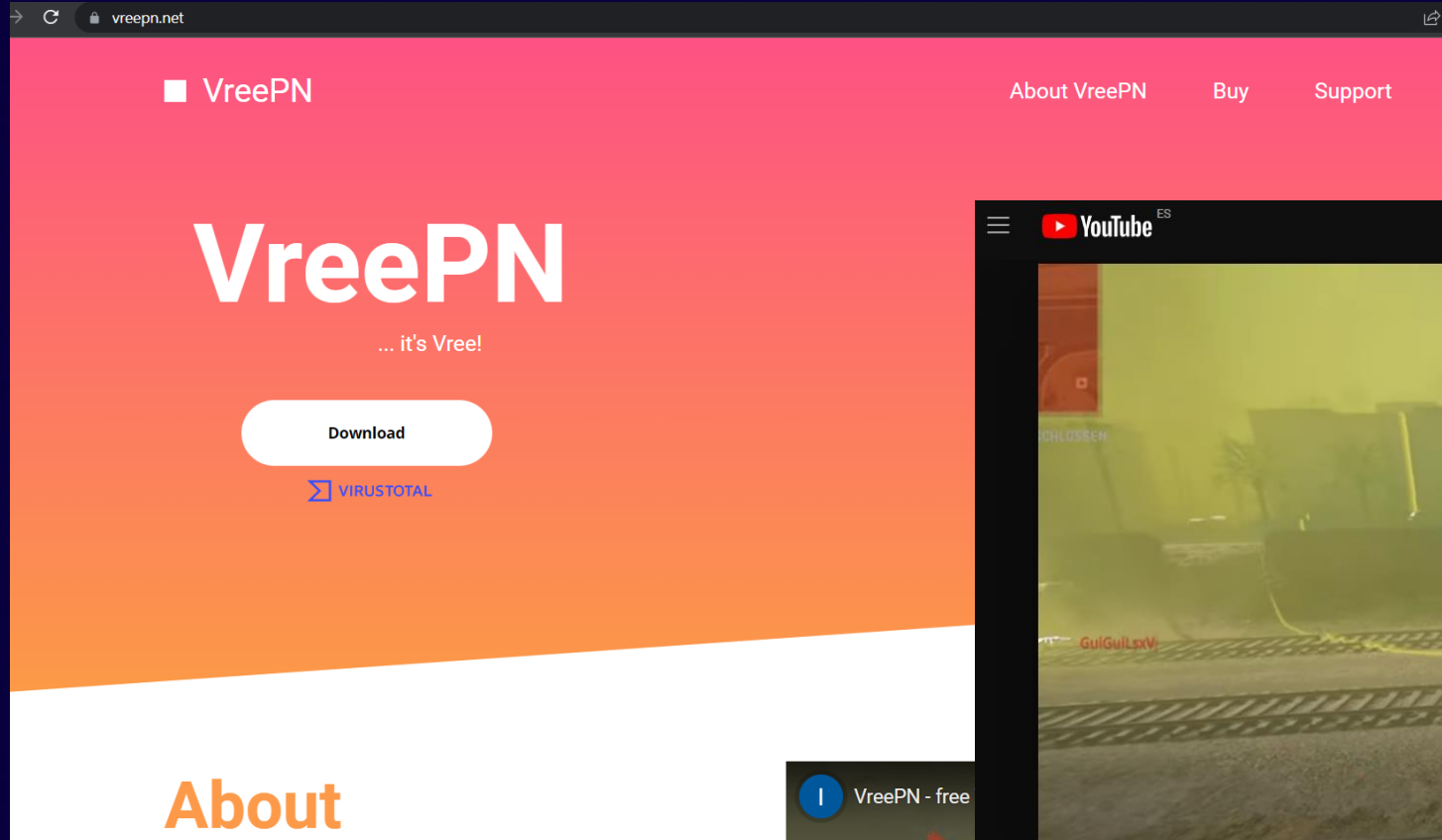
# Patrones de comportamientos Banload Trojan

En las últimas muestras subidas durante 2023 de Banload Trojan, podemos detectar ciertos patrones en todas ellas, los cuales pueden ser utilizados para generar detecciones.

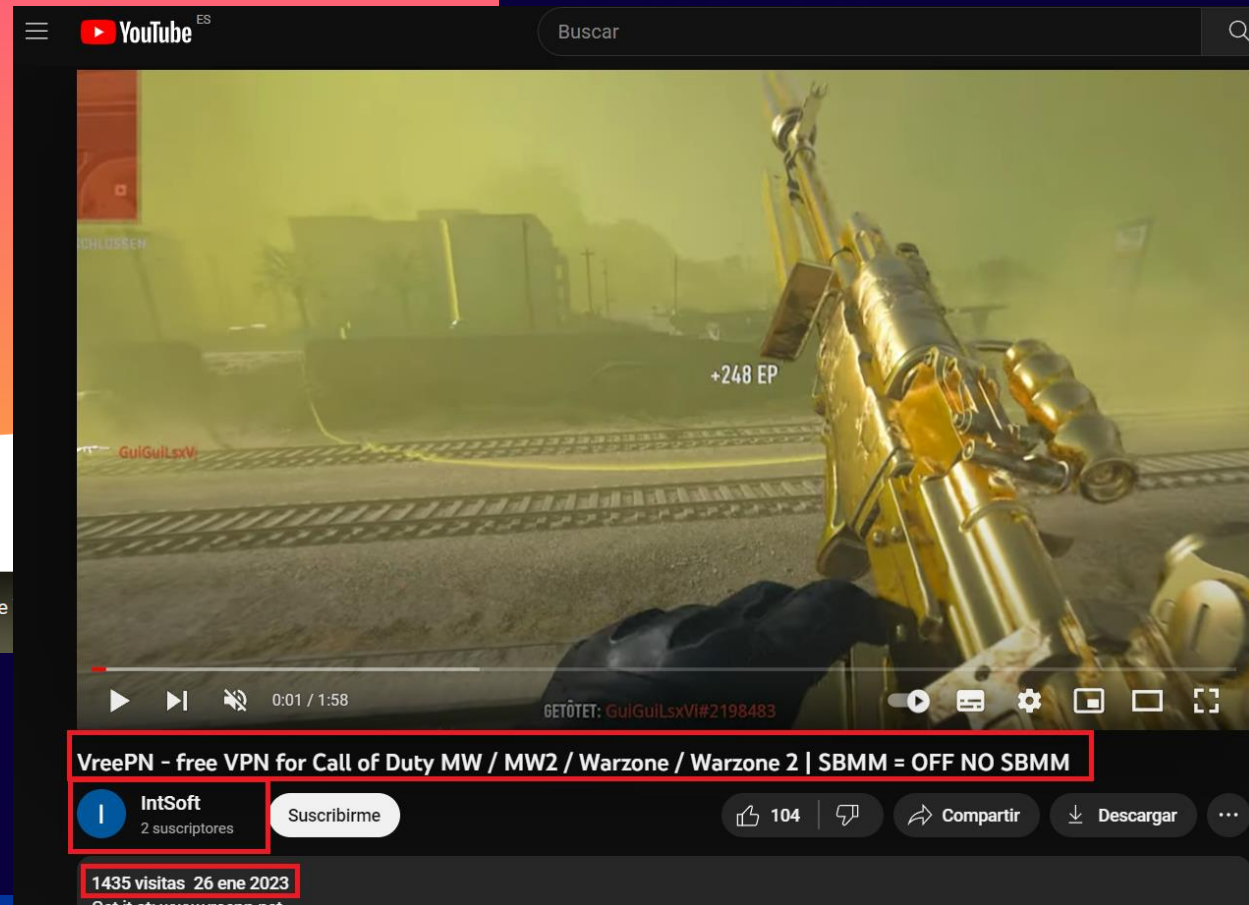
# Banload Trojan añadiendo una exclusion para una "VPN"

```
{
  "values": {
    "TerminalSessionId": "1",
    "ProcessGuid": "{C784477D-B189-63DA-710A-000000004A00}",
    "ProcessId": "3648",
    "Product": "Microsoft\\xae Windows\\xae Operating System",
    "Description": "Windows PowerShell",
    "Company": "Microsoft Corporation",
    "ParentProcessGuid": "{C784477D-B17A-63DA-6D0A-000000004A00}",
    "User": "DESKTOP-B0T93D6\\george",
    "OriginalFileName": "PowerShell.EXE",
    "ParentImage": "C:\\Program Files (x86)\\IntSoft\\VreePN\\updater.exe",
    "FileVersion": "10.0.17134.1 (WinBuild.160101.0800)",
    "ParentProcessId": "6180",
    "CurrentDirectory": "C:\\Program Files (x86)\\IntSoft\\VreePN\\",
    "CommandLine": "\"powershell\" -Command Add-MpPreference -ExclusionPath 'C:\\Program Files (x86)\\IntSoft\\VreePN'",
    "EventID": "1",
    "LogonGuid": "C784477D-9EED-63A4-230A-040000000000",
    "LogonId": "264739",
    "Image": "C:\\Windows\\SysWOW64\\WindowsPowerShell\\v1.0\\powershell.exe",
    "IntegrityLevel": "High",
    "ParentCommandLine": "\"C:\\Program Files (x86)\\IntSoft\\VreePN\\updater.exe\" nb",
    "UtcTime": "1675276681",
    "RuleName": "-"
  }
}
```

# Banload Trojan añadiendo una exclusion para una "VPN"



The screenshot shows the homepage of the VreePN website. The browser address bar displays 'vreepn.net'. The website has a pink and orange gradient background. At the top left, there is a 'VreePN' logo. To the right, there are navigation links for 'About VreePN', 'Buy', and 'Support'. The main heading is 'VreePN' in large white letters, with the tagline '... it's Vree!' below it. A prominent white 'Download' button is centered on the page. Below the button is a 'VIRUSTOTAL' logo. At the bottom left, the word 'About' is written in orange. A small video player in the bottom right corner shows a video titled 'VreePN - free'.



The screenshot shows a YouTube video player. The video title is 'VreePN - free VPN for Call of Duty MW / MW2 / Warzone / Warzone 2 | SBMM = OFF NO SBMM'. The channel name is 'IntSoft' with 2 subscribers. The video has 1435 views and was uploaded on 26 ene 2023. The video content shows a first-person view of a golden sniper rifle in a game environment. The video player interface includes a search bar, play/pause controls, a progress bar at 0:01 / 1:58, and various sharing and download options. The video title and channel information are highlighted with a red box.

# Banload Trojan añadiendo una exclusion para una “VPN”

```
title: Powershell Defender Exclusion
id: 17769c90-230e-488b-a463-e05c08e9d48f
related:
  - id: c1344fa2-323b-4d2e-9176-84b4d4821c88
    type: similar
status: experimental
description: Detects requests to exclude files, folders or processes from Antivirus scanning using PowerShell cmdlets
references:
  - https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-process-opened-file-exclusions-microsoft-defender-antivirus
  - https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdFcd3742bfcf365fee2a9/atomics/T1562.001/T1562.001.md
  - https://twitter.com/AdamTheAnalyst/status/1483497517119590403
author: Florian Roth (Nextron Systems)
date: 2021/04/29
modified: 2022/05/12
tags:
  - attack.defense_evasion
  - attack.t1562.001
logsource:
  category: process_creation
  product: windows
detection:
  selection1:
    CommandLine|contains:
      - 'Add-MpPreference '
      - 'Set-MpPreference '
  selection2:
    CommandLine|contains:
      - '-ExclusionPath '
      - '-ExclusionExtension '
      - '-ExclusionProcess '
      - '-ExclusionIpAddress '
  condition: all of selection*
falsepositives:
  - Possible Admin Activity
  - Other Cmdlets that may use the same parameters
level: medium
```

[https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process\\_creation/proc\\_creation\\_win\\_powershell\\_defender\\_exclusion.yml](https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/proc_creation_win_powershell_defender_exclusion.yml)



# Banload Trojan – Autorun key modificada

```
{  
  "values": {  
    "EventID": "13",  
    "ProcessId": "6324",  
    "EventType": "SetValue",  
    "Image": "C:\\Windows\\system32\\msiexec.exe",  
    "RuleName": "T1060,RunKey",  
    "UtcTime": "1676138035",  
    "Details": "C:\\Users\\george\\AppData\\Roaming\\@MicrosoftCorporation\\Conect\\conect.exe",  
    "ProcessGuid": "{C784477D-D62E-63E7-6C0A-000000004A00}",  
    "TargetObject": "HKU\\S-1-5-21-1015118539-3749460369-599379286-  
1001\\Software\\Microsoft\\Windows\\CurrentVersion\\Run\\System"  
  },  
}
```

# Banload Trojan – Autorun key modificada

```
tags:
  - attack.persistence
  - attack.t1547.001
logsource:
  category: registry_set
  product: windows
detection:
  current_version_base:
    EventType: SetValue
    TargetObject|contains: '\SOFTWARE\Microsoft\Windows\CurrentVersion'
  current_version_keys:
    TargetObject|contains:
      - '\ShellServiceObjectDelayLoad'
      - '\Run\'
      - '\RunOnce\'
      - '\RunOnceEx\'
      - '\RunServices\'
      - '\RunServicesOnce\'
      - '\Policies\System\Shell'
      - '\Policies\Explorer\Run'
      - '\Group Policy\Scripts\Startup'
      - '\Group Policy\Scripts\Shutdown'
      - '\Group Policy\Scripts\Logon'
```

[https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry/registry\\_set/registry\\_set\\_a\\_sep\\_reg\\_keys\\_modification\\_wow6432node.yml](https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry/registry_set/registry_set_a_sep_reg_keys_modification_wow6432node.yml)

# Banload Trojan - Compression Utility Passed Uncommon Directory

```
{
  "values": {
    "TerminalSessionId": "1",
    "ProcessGuid": "{C784477D-E14D-63E8-FC05-000000004400}",
    "ProcessId": "6600",
    "Product": "7-Zip",
    "Description": "7-Zip Console",
    "Company": "Igor Pavlov",
    "ParentProcessGuid": "{C784477D-E14B-63E8-FB05-000000004400}",
    "User": "DESKTOP-B0T93D6\\george",
    "OriginalFileName": "7z.exe",
    "ParentImage": "C:\\Windows\\SysWOW64\\rundll32.exe",
    "FileVersion": "19.00",
    "ParentProcessId": "4624",
    "CurrentDirectory": "C:\\Windows\\Installer\\MSIEAF6.tmp-\\",
    "CommandLine": "\\\"C:\\Windows\\Installer\\MSIEAF6.tmp-\\7z.exe\" x C:\\metasploit-framework.zip -aoa -o\"C:\\metasploit-framework\\\"",
    "EventID": "1",
    "LogonGuid": "C784477D-6FC2-63A4-D2AB-030000000000",
    "LogonId": "240594",
    "Image": "C:\\Windows\\Installer\\MSIEAF6.tmp-\\7z.exe",
    "IntegrityLevel": "High",
    "ParentCommandLine": "\"rundll32.exe \\\"C:\\Windows\\Installer\\MSIEAF6.tmp\\\",zzzzInvokeManagedCustomActionOutOfProc SfxCA_6417375 2 CustomActionFastMsi!CustomActionFastMsi.CustomActions.FastUnzip\"",
    "UtcTime": "1676206413",
    "RuleName": "-"
  }
}
```

# Banload Trojan – svchost ejecutado desde public path

```
{
  "values": {
    "TerminalSessionId": "1",
    "ProcessGuid": "{C784477D-AF1D-63E1-A40A-000000004A00}",
    "ProcessId": "7964",
    "Product": "Microsoft\\xae Windows\\xae Operating System",
    "Description": "Host Process for Windows Services",
    "Company": "Microsoft Corporation",
    "ParentProcessGuid": "{C784477D-AF1C-63E1-A10A-000000004A00}",
    "User": "DESKTOP-B0T93D6\\george",
    "OriginalFileName": "svchost.exe",
    "ParentImage": "C:\\Windows\\SysWOW64\\WindowsPowerShell\\v1.0\\powershell.exe",
    "FileVersion": "6.3.9600.17415",
    "ParentProcessId": "3360",
    "CurrentDirectory": "C:\\Users\\Public\\",
    "CommandLine": "\"C:\\Users\\Public\\svchost.exe\"",
    "EventID": "1",
    "LogonGuid": "C784477D-B1AA-63A4-5428-040000000000",
    "LogonId": "272468",
    "Image": "C:\\Users\\Public\\svchost.exe",
    "IntegrityLevel": "High",
    "ParentCommandLine": "powershell \"C:\\Users\\Public\\svchost.exe\"",
    "UtcTime": "1675734813",
    "RuleName": "-"
  }
},
```

# Banload Trojan – Anydesk creando archivos sospechosos

```
{
  "values": {
    "EventID": "11",
    "ProcessId": "6572",
    "Image": "C:\\Users\\george\\AppData\\Local\\Temp\\MW-7ea13f37-cda1-4e63-bf35-425b8bf83b3a\\files\\AnyDesk.exe",
    "RuleName": "EXE",
    "CreationUtcTime": "1675734787",
    "UtcTime": "1675734787",
    "ProcessGuid": "{C784477D-AEF8-63E1-740A-000000004A00}",
    "TargetFilename": "C:\\Users\\Public\\readme.exe"
  }
}
```

# Banload Trojan – Anydesk creando archivos sospechosos

```
title: Suspicious Binary Writes Via AnyDesk
id: 2d367498-5112-4ae5-a06a-96e7bc33a211
status: experimental
description: |
  Detects AnyDesk writing binary files to disk other than "gcapi.dll".
  According to RedCanary research it is highly abnormal for AnyDesk to write executable files to disk besides gcapi.dll
  which is a legitimate DLL that is part of the Google Chrome web browser used to interact with the Google Cloud API.
  (for more details)
references:
  - https://redcanary.com/blog/misbehaving-rats/
author: Nasreddine Bencherchali (Nextron Systems)
date: 2022/09/28
tags:
  - attack.command_and_control
  - attack.t1219
logsource:
  product: windows
  category: file_event
detection:
  selection:
    Image|endswith: '\anydesk.exe'
    TargetFilename|endswith:
      - '.dll'
      - '.exe'
  filter_dlls:
    TargetFilename|endswith: '\gcapi.dll'
  condition: selection and not 1 of filter_*
falsepositives:
  - Unknown
level: high
```

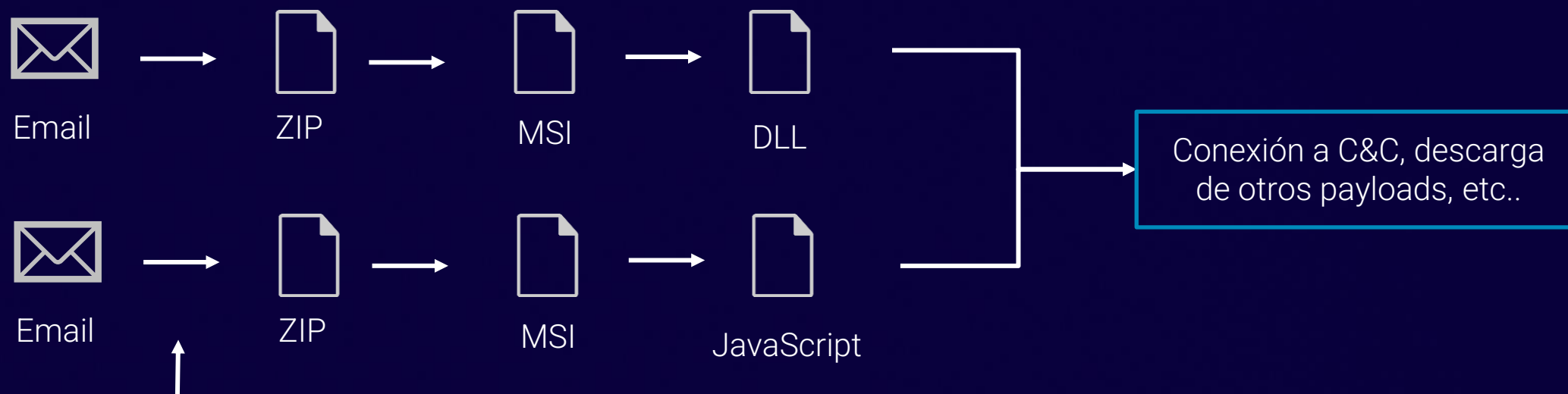
[https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file/file\\_event/file\\_event\\_win\\_anydesk\\_writing\\_susp\\_binaries.yml](https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file/file_event/file_event_win_anydesk_writing_susp_binaries.yml)

# Banload Trojan – Similitud con Glupteba?

```
{
  "rule_title": "Glupteba malware detection",
  "rule_source": "SOC Prime Threat Detection Marketplace",
  "match_context": [
    {
      "values": {
        "EventID": "13",
        "ProcessId": "1360",
        "EventType": "SetValue",
        "Image": "C:\\Windows\\SysWOW64\\reg.exe",
        "RuleName": "T1060,RunKey",
        "UtcTime": "1674043873",
        "Details": "C:\\Users\\george\\AppData\\Roaming\\Microsoft\\Credentials\\georgeL4zy73\\xb0\\xb1\\qikf5da\\xc6\\xee.exe
C:\\Users\\george\\AppData\\Roaming\\Microsoft\\Credentials\\georgeL4zy73\\xb0\\xb1\\imgengine
C:\\Users\\george\\AppData\\Roaming\\Microsoft\\Credentials\\georgeL4zy73\\xb0\\xb1\\sptdintf.dll",
        "ProcessGuid": "{C784477D-E1E1-63C7-850A-000000004A00}",
        "TargetObject": "HKU\\S-1-5-21-1015118539-3749460369-599379286-
1001\\Software\\Microsoft\\Windows\\CurrentVersion\\Run\\george"
      }
    }
  ]
}
```

# Terminando con Brasil

Brasil es conocido por los troyanos bancarios brasileños y otro tipo de malware desarrollado de manera local, en muchas ocasiones, utilizando archivos MSI que tienen embebidos DLL y scripts que son cargados durante la ejecución del MSI.



También puede haber archivos PDF entre el email y el archivo ZIP



# Uruguay

De: Banco de la República Oriental del Uruguay (BROU) <info@brou.com.uy>  
Enviado el: miércoles, 1 de marzo de 2023 13:09  
Asunto: Nueva Notificación de Pago Bancario! (BROU)  
Importancia: Alta

Para tu información;

Este aviso de pago se emite a petición de nuestro cliente.  
Su cuenta bancaria corporativa que termina en \*\*\*\*\* ha sido acreditada con un pago entrante  
Consulte el documento de pago adjunto para obtener más detalles.

Saludos,

Departamento de Remesas  
Banco de la República Oriental del Uruguay  
Address. Cerrito 351 Montevideo, Uruguay, 11000.  
Código SWIFT: BROUYMMXXX  
www.brou.com.uy <<http://www.brou.com.uy>>  
Customer Care Toll Line: 600 200 700

Este correo electrónico es solo para fines informativos y no está listo para aceptar respuestas. Por lo tanto, le agradecemos que no responda a esta dirección.  
Declaración de confidencialidad  
Este mensaje y los documentos que lo acompañan son confidenciales y son para uso exclusivo de la persona o entidad a la que va dirigido, por lo que Barclays no se hace responsable del conocimiento de su contenido por parte de terceros.  
Si usted no es el destinatario de este mensaje, se le informará que ha recibido el mensaje por error y cualquier uso, distribución, reenvío u otra divulgación, impresión o reproducción de este mensaje está expresamente prohibido y debe eliminarlo inmediatamente de su y Destruýalo con todos los archivos adjuntos y notifique a Chase la situación: los clientes, si están en el extranjero, llamen al 21 780 73 64 o al +44 21 780 73 64. Disponible las 24 horas, los 7 días de la semana. Para clientes llamar al 217 807 130. Atención personalizada, de lunes a viernes de 08:00 am a 08:00 pm.



# Uruguay – Los archivos IMG no pasan de moda

Nombre	tamaño	tamaño co...	Modificado	Acceso
BROU_Copia de Pago_PDF.exe	75 776	75 776	2022-12-25...	2022-12-25...



Archivo IMG adjunto  
en el correo



Archivo EXE que se  
encuentra dentro del  
IMG

# Uruguay – Interesante tráfico SMTP saliente

```
{
  "values": {
    "EventID": "3",
    "ProcessId": "5136",
    "DestinationPortName": "-",
    "Protocol": "tcp",
    "DestinationIp": "112.213.93.85",
    "Initiated": "true",
    "SourcePortName": "-",
    "Image": "C:\\Users\\george\\AppData\\Roaming\\Rfudhxxqq\\Nwdbdr.exe",
    "ProcessGuid": "{C784477D-B197-63FF-1606-000000003400}",
    "DestinationHostname": "mail9385.maychuemail.com",
    "UtcTime": "1677488068",
    "User": "DESKTOP-B0T93D6\\george",
    "DestinationPort": "587",
    "RuleName": "Usermode",
    "SourcePort": "49753",
    "SourceIsIpv6": "false",
    "SourceHostname": "DESKTOP-B0T93D6.local",
    "SourceIp": "192.168.2.14",
    "DestinationIsIpv6": "false"
  }
},
```

# Uruguay – Interesante tráfico SMTP saliente

```
author: frack113
date: 2022/01/07
modified: 2022/09/21
tags:
  - attack.exfiltration
  - attack.t1048.003
logsource:
  category: network_connection
  product: windows
detection:
  selection:
    DestinationPort:
      - 25
      - 587
      - 465
      - 2525
    Initiated: 'true'
  filter_clients:
    Image|endswith:
      - \thunderbird.exe
      - \outlook.exe
  filter_mailserver:
    Image|startswith: 'C:\Program Files\Microsoft\Exchange Server\'
  filter_outlook:
    Image|startswith: 'C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_'
    Image|endswith: '\HxTsr.exe'
  condition: selection and not 1 of filter_*
falsepositives:
  - Other SMTP tools
level: medium
```

[https://github.com/SigmaHQ/sigma/blob/master/rules/windows/network\\_connection/net\\_connection\\_win\\_susp\\_outbound\\_smtp\\_connections.yml](https://github.com/SigmaHQ/sigma/blob/master/rules/windows/network_connection/net_connection_win_susp_outbound_smtp_connections.yml)

# Uruguay – Interesante tráfico SMTP saliente

```
alert ( gid:124; sid:5; rev:2; msg:"(smtp) unknown command"; metadata: policy max-detect-ips drop, rule-type preproc; service:smtp; classtype:protocol-command-decode;)
```

# Uruguay – PowerShell base64 encode

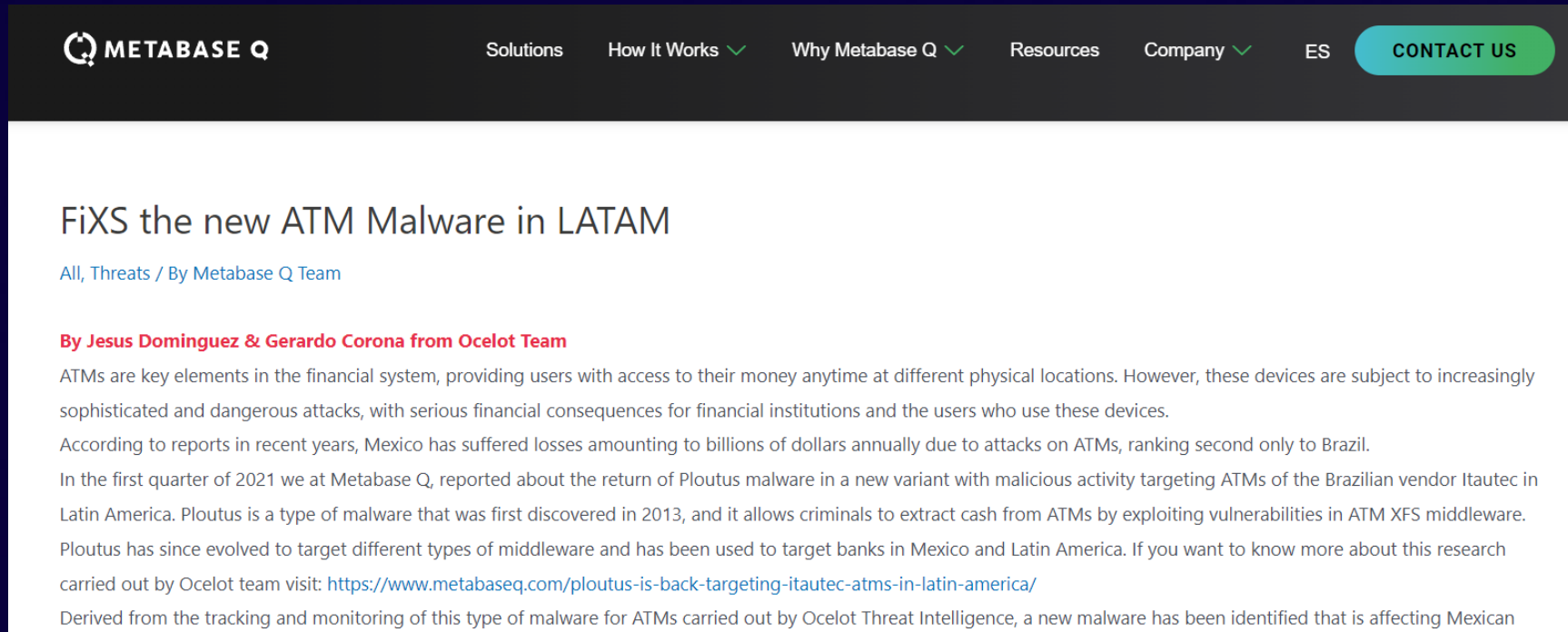
```
{
  "values": {
    "TerminalSessionId": "1",
    "ProcessGuid": "{C784477D-B154-63FF-0D06-000000003400}",
    "ProcessId": "420",
    "Product": "Microsoft\\xae Windows\\xae Operating System",
    "Description": "Windows PowerShell",
    "Company": "Microsoft Corporation",
    "ParentProcessGuid": "{C784477D-B14A-63FF-0B06-000000003400}",
    "User": "DESKTOP-B0T93D6\\george",
    "OriginalFileName": "PowerShell.EXE",
    "ParentImage": "C:\\Users\\george\\Desktop\\BROU_Copia de Pago_PDF.exe",
    "FileVersion": "10.0.17134.1 (WinBuild.160101.0800)",
    "ParentProcessId": "1944",
    "CurrentDirectory": "C:\\Users\\george\\Desktop\\",
    "CommandLine": "\"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe\" -ENC
cwB0AGEAcgB0AC0AcwBsAGUAZQBwACAALQBzAGUAYwBvAG4AZABzACAAMgAwAA==",
    "EventID": "1",
    "LogonGuid": "C784477D-6E01-63FC-46AF-030000000000",
    "LogonId": "241478",
    "Image": "C:\\Windows\\SysWOW64\\WindowsPowerShell\\v1.0\\powershell.exe",
    "IntegrityLevel": "High",
    "ParentCommandLine": "\"C:\\Users\\george\\Desktop\\BROU_Copia de Pago_PDF.exe\"",
    "UtcTime": "1677701460",
    "RuleName": "-"
  }
},
```

# Uruguay – PowerShell base64 encode

```
date: 2022/01/02
modified: 2023/01/05
tags:
  - attack.execution
  - attack.t1059.001
logsource:
  category: process_creation
  product: windows
detection:
  selection:
    Image|endswith:
      - \powershell.exe
      - \pwsh.exe
    CommandLine|contains:
      - '-e'
      - '-en'
      - '-enc'
      - '-enco'
      - '-ec'
  filter_encoding:
    CommandLine|contains: '-Encoding'
  filter_azure:
    ParentImage|contains:
      - 'C:\Packages\Plugins\Microsoft.GuestConfiguration.ConfigurationforWindows\'
      - '\gc_worker.exe'
  condition: selection and not 1 of filter_*
```

[https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process\\_creation/proc\\_creation\\_win\\_powershell\\_encode.yml](https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/proc_creation_win_powershell_encode.yml)

# México – FiXS ATM



The screenshot shows the top navigation bar of the Metabase Q website. The navigation menu includes 'Solutions', 'How It Works', 'Why Metabase Q', 'Resources', 'Company', 'ES', and a prominent 'CONTACT US' button. Below the navigation, the article title 'FiXS the new ATM Malware in LATAM' is displayed, followed by the author information 'All, Threats / By Metabase Q Team'. The article content begins with a paragraph about ATMs being key elements in the financial system and subject to sophisticated attacks. It then discusses reports from Mexico and a specific report from the first quarter of 2021 about Ploutus malware targeting ATMs in Latin America. The text concludes with a mention of Ocelot Threat Intelligence's role in identifying the new malware.



Solutions

How It Works

Why Metabase Q

Resources

Company

ES

CONTACT US

## FiXS the new ATM Malware in LATAM

All, Threats / By Metabase Q Team

By Jesus Dominguez & Gerardo Corona from Ocelot Team

ATMs are key elements in the financial system, providing users with access to their money anytime at different physical locations. However, these devices are subject to increasingly sophisticated and dangerous attacks, with serious financial consequences for financial institutions and the users who use these devices.

According to reports in recent years, Mexico has suffered losses amounting to billions of dollars annually due to attacks on ATMs, ranking second only to Brazil.

In the first quarter of 2021 we at Metabase Q, reported about the return of Ploutus malware in a new variant with malicious activity targeting ATMs of the Brazilian vendor Itaotec in Latin America. Ploutus is a type of malware that was first discovered in 2013, and it allows criminals to extract cash from ATMs by exploiting vulnerabilities in ATM XFS middleware.

Ploutus has since evolved to target different types of middleware and has been used to target banks in Mexico and Latin America. If you want to know more about this research carried out by Ocelot team visit: <https://www.metabaseq.com/ploutus-is-back-targeting-itaotec-atms-in-latin-america/>

Derived from the tracking and monitoring of this type of malware for ATMs carried out by Ocelot Threat Intelligence, a new malware has been identified that is affecting Mexican

Fuente: <https://www.metabaseq.com/fixs-atms-malware/>  
Jesus Dominguez & Gerardo Corona



# México – Archivos dropeados por FiXS

65 / 71

65 security vendors and 1 sandbox flagged this file as malicious

d3c40be552819f57dc51c5a18b8a5b0595e47dd73b09d5bf4c0a2083bd1243c3  
conhost.exe

145.00 KB Size | 2023-02-12 14:36:59 UTC | 18 days ago

peexe detect-debug-environment runtime-modules direct-cpu-clock-access overlay

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR CONTENT TELEMETRY COMMUNITY

Contacted IP addresses (1)

IP	Detections	Autonomous System	Country
20.99.184.37	3 / 88	8075	US

Dropped Files (53)

Scanned	Detections	File type	Name
2023-02-28	2 / 70	Win32 EXE	C:\Users\user\AppData\Local\Temp\3582-490\conhost.exe
2023-02-26	67 / 70	Win32 EXE	C:\ProgramData\Microsoft\Windows Defender\Platform4.18.2102.3-0\ConfigSecurity
2023-01-14	66 / 71	Win32 EXE	C:\Users\user\AppData\Local\Programs\Python\Python39\Lib\distutils\commandwin
2023-02-16	64 / 71	Win32 EXE	C:\Users\user\AppData\Local\Programs\Python\Python39\Scripts\pip.exe
2022-12-27	64 / 72	Win32 EXE	C:\ProgramData\Microsoft\Windows Defender\Platform4.18.2102.4-0\mpextms.exe
2022-12-27	65 / 72	Win32 EXE	C:\ProgramData\Package Cache\53f1dc9d-ed94-4650-a079-129785ce7905\VC_re
2023-02-24	64 / 69	Win32 EXE	C:\ProgramData\Microsoft\Windows Defender\Platform4.18.2102.3-0\X86\MpCmdR
2023-01-14	65 / 71	Win32 EXE	C:\Users\user\AppData\Local\Programs\Python\Python39\Lib\site-packages\pip_ver
2022-12-27	66 / 72	Win32 EXE	C:\Users\user\AppData\Local\Programs\Python\Python39\Scripts\python
2022-12-27	67 / 72	Win32 EXE	C:\Users\user\AppData\Local\Programs\Python\Python39\Scripts\easy_install-3.9.ex
2022-12-27	65 / 72	Win32 EXE	C:\ProgramData\chocolatey\tools\7z.exe
2022-12-27	63 / 72	Win32 EXE	C:\ProgramData\chocolatey\bin\cup.exe
2023-01-14	66 / 71	Win32 EXE	C:\Users\user\AppData\Local\Programs\Python\Python39\Lib\site-packages\pip_ver
2023-01-14	62 / 70	Win32 EXE	C:\Users\user\AppData\Local\Programs\Python\Python39\Lib\site-packages\setupto
2022-12-27	66 / 72	Win32 EXE	C:\ProgramData\Microsoft\Windows Defender\Platform4.18.2102.4-0\MpDlpCmd.ex
2022-12-27	67 / 72	Win32 EXE	C:\Users\user\AppData\Local\Programs\Python\Python39\Scripts\python
2022-12-27	66 / 72	Win32 EXE	C:\ProgramData\Microsoft\Windows Defender\Platform4.18.2102.3-0\MsMpEng.exe
2022-12-27	65 / 72	Win32 EXE	C:\ProgramData\Microsoft\Windows Defender\Platform4.18.2102.3-0\mpextms.exe
2023-01-14	66 / 71	Win32 EXE	C:\Users\user\AppData\Local\Programs\Python\Python39\Lib\site-packages\setupto
2022-12-27	64 / 72	Win32 EXE	C:\ProgramData\chocolatey\bin\cinst.exe

53 droppers diferentes

# México – Ese no es el padre de conhost!

```
{
  "values": {
    "TerminalSessionId": "1",
    "ProcessGuid": "{C784477D-1980-63E7-E005-000000004700}",
    "ProcessId": "7072",
    "Product": "-",
    "Description": "-",
    "Company": "-",
    "ParentProcessGuid": "{C784477D-3D7B-63A5-5F00-000000004700}",
    "User": "DESKTOP-B0T93D6\\george",
    "OriginalFileName": "-",
    "ParentImage": "C:\\Windows\\explorer.exe",
    "FileVersion": "-",
    "ParentProcessId": "4456",
    "CurrentDirectory": "C:\\Users\\george\\Desktop\\",
    "CommandLine": "\"C:\\Users\\george\\Desktop\\conhost.exe\"",
    "EventID": "1",
    "LogonGuid": "C784477D-3D7A-63A5-8D58-030000000000",
    "LogonId": "219277",
    "Image": "C:\\Users\\george\\Desktop\\conhost.exe",
    "IntegrityLevel": "High",
    "ParentCommandLine": "C:\\Windows\\Explorer.EXE",
    "UtcTime": "1676089728",
    "RuleName": "-"
  }
}
```

# México – Ese no es el padre de conhost!

```
logsource:
  category: process_creation
  product: windows
detection:
  selection:
    Image|endswith: '\conhost.exe'
    ParentImage|endswith:
      - '\svchost.exe'
      - '\lsass.exe'
      - '\services.exe'
      - '\smss.exe'
      - '\winlogon.exe'
      - '\explorer.exe'
      # - '\dllhost.exe' # FP on clean system from grandparent 'svchost.exe -k DcomLaunch -p'
      - '\rundll32.exe'
      - '\regsvr32.exe'
      - '\userinit.exe'
      - '\wininit.exe'
      - '\spoolsv.exe'
      # - '\wermgr.exe' # Legitimate parent as seen in EchoTrail https://www.echotrail.io/insights/search/wermgr.exe
      # - '\csrss.exe' # Legitimate parent as seen in EchoTrail https://www.echotrail.io/insights/search/csrs.exe
      # - '\ctfmon.exe' # Seen several times in a testing environment
  filter:
    ParentCommandLine|contains:
      - '-k apphost -s AppHostSvc'
      - '-k imgsvc'
      - '-k localService -p -s RemoteRegistry'
      - '-k LocalSystemNetworkRestricted -p -s NgcSvc'
      - '-k NetSvcs -p -s NcaSvc'
      - '-k netsvcs -p -s NetSetupSvc'
      - '-k netsvcs -p -s wlidsvc'
      - '-k NetworkService -p -s DoSvc'
      - '-k wsappx -p -s AppXSvc'
      - '-k wsappx -p -s ClipSVC'
      - 'C:\Program Files (x86)\Dropbox\Client\'
      - 'C:\Program Files\Dropbox\Client\'
condition: selection and not filter
```

[https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process\\_creation/proc\\_creation\\_winusp\\_parent\\_of\\_conhost.yml](https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/proc_creation_winusp_parent_of_conhost.yml)

# México – No es cosa solo de malware ATM...

sigma\_rule:6f60707627a0617e86bd3005d8ce73a34fa6e674c0169d593509953d67bfaa2e fs:2023-01-01+ p:1+

sigma\_rule:6f60707627a0617e86bd3005d8ce73a34fa6e674c0169d593509953d67bfaa2e fs:2023-01-01+ p:1+

FILES - 20 / 180

		Detections	Size	Filter by
				First seen
<input type="checkbox"/>	553F642ABE8FAB1E8FEE85A43DA2686D6395A76AEF97D1066227054F7ED02836 conhost.exe peexe spreader checks-usb-bus detect-debug-environment long-sleeps checks-user-input persistence	47 / 68	328.00 KB	2023-03-01 16:53:54
<input type="checkbox"/>	B57B846048BA1FED453057EC7E8A9A45F5309F0982BFC6F219000801C2735E2 conhost.exe peexe checks-user-input idle	3 / 69	224.00 KB	2023-03-01 11:55:35
<input type="checkbox"/>	AA5B896FD29A3E8CA462A716E367624A0A517855208A9ADA9083F28791824994 conhost.exe peexe detect-debug-environment long-sleeps checks-usb-bus spreader persistence	50 / 66	328.00 KB	2023-02-27 17:15:55
<input type="checkbox"/>	92FED35F668070A40E052EEF38719EACBCF033825A7C39ED98A668E021B7DA CONHOST.exe peexe 64bits runtime-modules direct-cpu-clock-access detect-debug-environment	29 / 70	323.00 KB	2023-02-23 23:51:28
<input type="checkbox"/>	C20DEF6823301D051F674BFAE8CAE527F0FA450A8358C2F3E3D91197F7E538250 Orcus.exe peexe obfuscated assembly service-scan runtime-modules detect-debug-environment checks-network-adapters ...	60 / 67	908.00 KB	2023-02-20 17:18:26
<input type="checkbox"/>	CBF2A668B3B1FF5380879F9224A1E197C6C3103E35C32881ED87C35387188022 svchost.exe peexe overlay runtime-modules checks-network-adapters spreader direct-cpu-clock-access	64 / 70	202.32 KB	2023-02-17 09:15:56
<input type="checkbox"/>	7E42828600BCA0F0098703EED0712ED619E2575E9608084C5133A0FD08366565 CONHOST.exe peexe 64bits runtime-modules direct-cpu-clock-access detect-debug-environment	21 / 69	99.50 KB	2023-02-13 21:16:42
<input type="checkbox"/>	02C5A6E66593C2ED1539BF3882860231AC40A8F345535565B577086B09E4D95 conhost.exe peexe detect-debug-environment long-sleeps direct-cpu-clock-access checks-user-input checks-usb-bus spreader ...	54 / 69	328.00 KB	2023-02-19 16:31:22

# México – Qué hay de los droppers de FiXS? Un resumen...

```
"statistics": {  
  "Python Initiated Connection": 15,  
  "Failed Code Integrity Checks": 34,  
  "Process Start From Suspicious Folder": 6,  
  "Creation of an Executable by an Executable": 34,  
  "Use Remove-Item to Delete File": 33,  
  "Disable Microsoft Defender Firewall via Registry": 27,  
  "CLOP Ransomware detection (Sysmon)": 1,  
  "Process Creation Using Sysnative Folder": 1,  
  "Wow6432Node CurrentVersion Autorun Keys Modification": 1,  
  "File deletion via CMD (via cmdline)": 2  
}
```

# México – Ese firewall no me gusta

```
{
  "values": {
    "EventID": "13",
    "ProcessId": "1188",
    "EventType": "SetValue",
    "Image": "C:\\Windows\\system32\\svchost.exe",
    "RuleName": "T1089",
    "UtcTime": "2022-06-07 07:25:39.966",
    "Details": "DWORD (0x00000000)",
    "ProcessGuid": "C784477D-FC28-629E-1A00-000000003000",
    "TargetObject":
      "HKLM\\System\\CurrentControlSet\\Services\\SharedAccess\\Parameters\\FirewallPolicy\\DomainProfile\\EnableFirewall"
  }
}
```

# México – Ese no es el padre de conhost!

```
tags:
- attack.defense_evasion
- attack.t1562.004
logsource:
category: registry_set
product: windows
detection:
selection:
  EventType: SetValue
  #HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile\EnableFirewall
  #HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\PublicProfile\EnableFirewall
  #HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\EnableFirewall
  TargetObject|startswith: 'HKLM\System\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\'
  TargetObject|endswith: '\EnableFirewall'
  Details: 'DWORD (0x00000000)'
condition: selection
falsepositives:
- Unknown
level: medium
```

[https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry/registry\\_set/registry\\_set\\_disable\\_defender\\_firewall.yml](https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry/registry_set/registry_set_disable_defender_firewall.yml)

# Conclusiones

América Latina sufre de manera continua intrusiones y operaciones que no son conocidas por la comunidad, pero las cuales son importantes de entender para adoptar una buena estrategia de seguridad.

La información presentada en esta charla puede ser utilizada para:

- Realizar actividades de threat hunting en la red corporativa y servicios externos como pudiese ser VirusTotal
- Crear lógica de detección y usarla en la infraestructura de la organización
- Aprender sobre comportamientos utilizados en América Latina por múltiples familias de malware
- En caso de incidente buscar acciones específicas que hayan sido mostradas durante la presentación



# Comportamientos

FiXS: <https://gist.github.com/jstnk9/11a82b582d451455c4e7636bd4722ae3>

FiXS Droppers: <https://gist.github.com/jstnk9/a09a0ab811117eb87a79faa7fe7006c3>

Banload Trojan: <https://gist.github.com/jstnk9/986cc6b404fa33a6c6e7f7fa23e790a1>

IMG Uruguay: <https://gist.github.com/jstnk9/7a4794e5605bc402b91732e79aff03d1>

(\*) Algunos comportamientos podrían presentar falsos positivos realizados por las sandboxes de VirusTotal

 @Joseliyo\_Jstnk

 [linkedin.com/in/joseluissm/](https://www.linkedin.com/in/joseluissm/)

# Thank you

 **BlackBerry**® Intelligent Security. Everywhere.

© 2022 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY and EMBLEM Design are the trademarks or registered trademarks of BlackBerry Limited and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners.