

Forum:[Hack Forums](#)

Thread: [Could someone confirm these pdfs contain malware?](#)

SIM-4500658 - December 12, 2024, 4:18 am

Hello there ;

I discovered malware/ spyware on my iphone a day after i downloaded and opened these PDFs..

I am not suspicious of any other thing on my phone since it is not jailbroken and all the apps are from the Appstore..

I dont think it matters that the pdfs themselves are in Arabic language..

Its important to confirm because i downloaded these PDFs from a very official source.

I am just an ordinary user and I cannot examine files in such a way..

"Sorry, you cannot post links, videos, or images until you've made more than 50 total posts or have upgraded."

Damn, i got this error, any ideas what to do?

Thank you for your consideration..

Bastille - December 12, 2024, 4:58 am

Hello,

As you mentioned that your iPhone is not jailbroken, and you didn't download weird app, a simple PDF shouldn't be a threat (don't forget to keep it up to date too). Most malicious PDFs files are either :

- scam
- phishing

Advanced PDF files have embedded .exe et Javascript scripts, but they mainly target Windows computers.

If there is no personal information on this PDF, feel free to share in the thread a link where we can download it (use spaces between dots), I allow you to do it.

If you want more info about malicious PDF files take a look at my thread :

<https://hackforums.net/showthread.php?tid=6284659>

If you want to take a look on how to conduct a PDF file analysis, look at this thread :

<https://hackforums.net/showthread.php?tid=6285798>

SIM-4500658 - December 12, 2024, 8:41 am

(Dec 12, 2024 05:58 AM)Bastille Wrote: [\[CITE\]](#) Hello,

As you mentioned that your iPhone is not jailbroken, and you didn't download weird app, a simple PDF shouldn't be a threat (don't forget to keep it up to date too). Most malicious PDFs files are

either :

- scam
- phishing

Advanced PDF files have embedded .exe et Javascript scripts, but they mainly target Windows computers.

If there is no personal information on this PDF, feel free to share in the thread a link where we can download it (use spaces between dots), I allow you to do it.

If you want more info about malicious PDF files take a look at my thread :

If you want to take a look on how to conduct a PDF file analysis, look at this thread :

As I said, I cannot share links unless i upgrade, can you tell me what should i do?

And i cannot upgrade because i dont have a payment method setup..

Should i attempt to bypass it, I dont want to get banned..

I also need to mention that its an old iphone with ios 16, meaning it was probably easy to hack it..

Bastille - December 12, 2024, 9:21 am

(Dec 12, 2024 09:41 AM)SIM-4500658 Wrote: [\[CITE\]](#) As I said, I cannot share links unless i upgrade, can you tell me what should i do?

And i cannot upgrade because i dont have a payment method setup..

Should i attempt to bypass it, I dont want to get banned..

I also need to mention that its an old iphone with ios 16, meaning it was probably easy to hack it..

I allow you to share the link (I'm staff, look at my userbar)

Even if the iOS is not up to date it's not that easy to hack an iPhone

SIM-4500658 - December 12, 2024, 9:49 am

(Dec 12, 2024 10:21 AM)Bastille Wrote: [\[CITE\]](#) I allow you to share the link (I'm staff, look at my userbar)

Even if the iOS is not up to date it's not that easy to hack an iPhone

I also have to add that I scanned with Panda antivirus on Windows, but it did not find anything, but i think it is expected since that antivirus is for Windows not iOS..

gofile.to/O8rX/ezyzip-potential-trojan-virus.zip

PASSWORD: Quote:87654321

As a side note I am sure my phone was hacked because the camera switched on by itself and took 6 or 7 pics

I was also writing a text on whatsapp and suddenly backspace by itself until my text was gone..

Bastille - December 12, 2024, 11:08 pm

(Dec 12, 2024 10:49 AM)SIM-4500658 Wrote: [\[CITE\]](#) I also have to add that I scanned with Panda antivirus on Windows, but it did not find anything,

but i think it is expected since that antivirus is for Windows not iOS..

gofile.to/O8rX/ezyzip-potential-trojan-virus.zip

PASSWORD:

As a side note I am sure my phone was hacked because the camera switched on by itself and took

6 or 7 pics

I was also writing a text on whatsapp and suddenly backspace by itself until my text was gone..
Nothing malicious from the files in the archive, here is how it's composed, in the yellow square there are an archive file (.rar) which contains a folder (blue text), with .docx documents (white) :

1. The PDF file

VirusTotal clean :

<https://www.virustotal.com/gui/file/fc4e942d2a6414212bc211301b00256259200cb4c09a3a86bc5675d002e93aa9>

Here is the PDF file :

Here is the translated version :

AI Quote:

Requirements for applying for a patent or a utility model patent
From Law No. 82 of 2002, Articles 12, 13, and Executive Regulations No. 1366 of 2003 (Articles 3, 4)

Application form:

Three copies of the patent application, including:

A brief description in Arabic

A brief description in English

A detailed description, covering: prior art, the problem and shortcomings in prior art, the innovation, detailed explanation, method of exploitation, protection elements (at least one claim), diagrams and illustrations if available, and the best method known to the inventor for implementation.

The inventor's identity must be proven.

If the applicant is not the inventor, authorization must be provided.

If the applicant is a minor, proof of guardianship is required (e.g., school or university ID).

Submission of a notarized power of attorney, if applicable.

Supporting documents required within a 4-month submission period:

Materials containing biological, botanical, zoological, industrial, agricultural, or cultural heritage origins, along with proof of obtaining them legally.

An extract from the commercial register or a certified contract copy (if the applicant is a legal entity).

An affidavit stating that the applicant is the inventor, or proof otherwise.

A temporary protection certificate, if applicable.

Payment of application fees.

Application for exemption from examination fees, if eligible (for individuals or Egyptian academic/research institutions), or payment within 6 months.

If the application is submitted in a foreign language, a certified translation must be provided

within 6 months.

If prior filing exists in another country, submit supporting documents translated into Arabic within 3 months.

Note: All deadlines start from the application submission date. Applications not submitted within the specified timeline will be dismissed.

1. The Word files

I've scanned all Word files contained in the .rar archive with OLETOOLS and nothing suspicious, same result for all of them, no VBA macro or weird stuff :

Here are few Word documents, weird, but not really interesting :

If you're convinced your iPhone is hacked just reset it and the problem will be fixed, you can also run free AV tools from the AppStore but there are no guarantees

SIM-4500658 - December 13, 2024, 3:54 am

(Dec 13, 2024 12:08 AM) Bastille Wrote: [\[CITE\]](#) Nothing malicious from the files in the archive, here is how it's composed, in the yellow square there are an archive file (.rar) which contains a folder (blue text), with .docx documents (white) :

1. The PDF file

VirusTotal clean :

<https://www.virustotal.com/gui/file/fc4e942d2a6414212bc211301b00256259200cb4c09a3a86bc5675d002e93aa9>

Here is the PDF file :

Here is the translated version :

AI Quote:

Requirements for applying for a patent or a utility model patent

From Law No. 82 of 2002, Articles 12, 13, and Executive Regulations No. 1366 of 2003 (Articles 3, 4)

Application form:

Three copies of the patent application, including:

- A brief description in Arabic

- A brief description in English

- A detailed description, covering: prior art, the problem and shortcomings in prior art, the innovation, detailed explanation, method of exploitation, protection elements (at least one claim),

diagrams and illustrations if available, and the best method known to the inventor for implementation.

The inventor's identity must be proven.

If the applicant is not the inventor, authorization must be provided.

If the applicant is a minor, proof of guardianship is required (e.g., school or university ID).

Submission of a notarized power of attorney, if applicable.

Supporting documents required within a 4-month submission period:

Materials containing biological, botanical, zoological, industrial, agricultural, or cultural heritage origins, along with proof of obtaining them legally.

An extract from the commercial register or a certified contract copy (if the applicant is a legal entity).

An affidavit stating that the applicant is the inventor, or proof otherwise.

A temporary protection certificate, if applicable.

Payment of application fees.

Application for exemption from examination fees, if eligible (for individuals or Egyptian academic/research institutions), or payment within 6 months.

If the application is submitted in a foreign language, a certified translation must be provided within 6 months.

If prior filing exists in another country, submit supporting documents translated into Arabic within 3 months.

Note: All deadlines start from the application submission date. Applications not submitted within the specified timeline will be dismissed.

1. The Word files

I've scanned all Word files contained in the .rar archive with OLETOOLS and nothing suspicious, same result for all of them, no VBA macro or weird stuff :

Here are few Word documents, weird, but not really interesting :

If you're convinced your iPhone is hacked just reset it and the problem will be fixed, you can also run free AV tools from the AppStore but there are no guarantees

Thank you very much.. I am so grateful..

hopefully il be active here more..

I have no idea now how it got hacked.. so must be one of the apps..

I had already backed up and restored, and until now no signs of infection..

but it is concerning atm, since one of my apps right now, must be the culprit..

its a shame I cannot pin point which app is infected..

DramaKing - December 13, 2024, 5:15 am

(Dec 13, 2024 04:54 AM)SIM-4500658 Wrote: [\[CITE\]](#) Thank you very much.. I am so grateful.. hopefully il be active here more..

I have no idea now how it got hacked.. so must be one of the apps..

I had already backed up and restored, and until now no signs of infection..

but it is concerning atm, since one of my apps right now, must be the culprit..

its a shame I cannot pin point which app is infected..

Unless you have an antivirus app that detected the malware (which hardly anyone bothers to develop or use iOS antivirus), I question how you would identify signs of infection. I have yet to come across even a PC user who had an actual virus since the Windows 7 era.

SIM-4500658 - December 13, 2024, 9:52 am

(Dec 13, 2024 06:15 AM)DramaKing Wrote: [\[CITE\]](#) Unless you have an antivirus app that detected the malware (which hardly anyone bothers to develop or use iOS antivirus), I question how you would identify signs of infection. I have yet to come across even a PC user who had an actual virus since the Windows 7 era.

I don't entirely understand this statement..

As I understand, in order for a person to get hacked they need to be infected with malware..

I had stated that my camera would switch on byitself and take pics and my text would get erased..

DramaKing - December 13, 2024, 12:29 pm

(Dec 13, 2024 10:52 AM)SIM-4500658 Wrote: [\[CITE\]](#) I don't entirely understand this statement..

As I understand, in order for a person to get hacked they need to be infected with malware..

I had stated that my camera would switch on byitself and take pics and my text would get erased..

Sorry, I didn't read every post. There's a lot here. Yeah, Apple's screening may miss a weird app that randomly activates the camera. If those pics end up in your Photos, then that is really bad malware. As for the text being erased, it could be a bug. User apps should not be able to manipulate the keyboard.

iOS 16 is insecure, sure. It would still take nation-state malware like Pegasus to exploit your device through an image or document.

ttbr0 - December 13, 2024, 8:23 pm

its unlikely that the pdfs were the access vector and more likely that you may have downloaded a malicious app.

SIM-4500658 - December 16, 2024, 1:47 am

(Dec 13, 2024 09:23 PM)ttbr0 Wrote: [\[CITE\]](#) its unlikely that the pdfs were the access vector and more likely that you may have downloaded a malicious app.

Thank you