

Forum:[Hack Forums](#)

Thread: [How to get remote access to PC with emailed PDF](#)

MafiK - November 2, 2023, 10:34 am

Hey guys,

I'm new here and I'm super excited to learn. Just want to preface that I have zero black hat intentions, or any intentions to do anything illegal - simply am just curious as to how others do it, how it works, etc.

How can you take remote control of someone's PC using an emailed PDF that they click on to open?

SnowFalling - November 2, 2023, 11:32 am

For genuine curiosity (I know its not) you can infect a PDF file with trojans so that you can control/have control over someone else's device. But it does take time to make and maintenance, though.

MafiK - November 2, 2023, 5:04 pm

(Nov 2, 2023 11:32 AM)SnowFalling Wrote: [\[CITE\]](#) For genuine curiosity (I know its not) you can infect a PDF file with trojans so that you can control/have control over someone else's device. But it does take time to make and maintenance, though.

I know it's hard to believe it's not genuine curiosity. I get it. I'm a first year software engineering major at my college and am fascinated by computers/networks/how they communicate with each other, and the hacking/cybersecurity community is a great niche of that.

Whereabouts would I go to learn about how to infect a PDF file w/ trojans or with a custom python file that I make?

SnowFalling - November 2, 2023, 6:13 pm

(Nov 2, 2023 05:04 PM)MafiK Wrote: [\[CITE\]](#) I know it's hard to believe it's not genuine curiosity. I get it. I'm a first year software engineering major at my college and am fascinated by computers/networks/how they communicate with each other, and the hacking/cybersecurity community is a great niche of that.

Whereabouts would I go to learn about how to infect a PDF file w/ trojans or with a custom python file that I make?

Well, I can't give you info on how to do that, that's Black Hat Hacking. But the internet exists if you'd like to cure your research desires.

??CU?I?? TM - November 3, 2023, 2:33 am

(Nov 2, 2023 10:34 AM)MafiK Wrote: [\[CITE\]](#) Hey guys,

I'm new here and I'm super excited to learn. Just want to preface that I have zero black hat intentions, or any intentions to do anything illegal - simply am just curious as to how others do it, how it works, etc.

How can you take remote control of someone's PC using an emailed PDF that they click on to

open?

What you are talking are exploits which are either bought , or researched and made. You can do either of them to have its access and do your task.

resetti - November 3, 2023, 3:30 am

(Nov 2, 2023 05:04 PM)MafiK Wrote: [\[CITE\]](#) I know it's hard to believe it's not genuine curiosity. I get it. I'm a first year software engineering major at my college and am fascinated by computers/networks/how they communicate with each other, and the hacking/cybersecurity community is a great niche of that.

Whereabouts would I go to learn about how to infect a PDF file w/ trojans or with a custom python file that I make?

"Silent PDF exploits" which are defined as a legitimate, real PDF file which executes malware upon opening, do not exist without a zero day vulnerability.

You cannot "embed" executable PE code into a PDF file and expect it to execute and run when opened. That's not how it works.

To get a payload embedded into a PDF file and have it work, you would need to find a memory corruption/buffer overflow/use-after-free vulnerability in the reader application that is being used to open the PDF file, bare in mind this could be Adobe Reader, Microsoft Edge (the default PDF reader if you dont have one installed), FireFox, Foxit PDF Reader, and lots more.

These vulnerabilities and exploits are NOT easy to find and they cost tens of thousands of dollars, if you're interested in learning how they work, here is a real writeup on a Adobe Reader RCE that was found a few months ago: <https://hacksys.io/blogs/adobe-reader-resetform-cagg-rce-cve-2023-21608>

As you can see, finding an exploit like that is complex.

DramaKing - November 3, 2023, 7:01 am

(Nov 2, 2023 10:34 AM)MafiK Wrote: [\[CITE\]](#) Hey guys,

I'm new here and I'm super excited to learn. Just want to preface that I have zero black hat intentions, or any intentions to do anything illegal - simply am just curious as to how others do it, how it works, etc.

How can you take remote control of someone's PC using an emailed PDF that they click on to open?

I'm surprised that no one has said this yet, but PDF malware did exist. If you are doing this for security research and interested in the historical aspect, go back to about 2012. Metasploit has some old Adobe PDF exploits from when there was more Javascript allowed and no sandboxing.

Ph4n70M Phr34K - November 3, 2023, 7:14 am

(Nov 2, 2023 10:34 AM)MafiK Wrote: [\[CITE\]](#) Hey guys,

I'm new here and I'm super excited to learn. Just want to preface that I have zero black hat intentions, or any intentions to do anything illegal - simply am just curious as to how others do it, how it works, etc.

How can you take remote control of someone's PC using an emailed PDF that they click on to open?

In simple words, you cant.

Just dont be a fool. We live in 2023, not 2003, not 1993.

Almost 2024 actually.

You need to find other way to deliver the payload.

Many people are using PDF documents which contains social engineering template.

Sardukarr - *November 3, 2023, 12:50 pm*

Not to hijack the thread, but how one would deliver a payload these days? I'm doing a security research, of course.