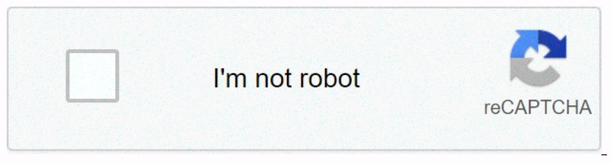

Continue

Anti malware free for pc

Like any threat, malware evolves. To stay ahead of ransomware, credential theft and more, download the Cofense Malware Review. Get information from Cofense Intelligence about how malware is constantly changing. Discover trends and what to prioritize to defend your network. There is a new form of iOS malware doing the rounds that uses previously employed mechanisms to hack apps as a way to infect iPhones and iPads. Nicknamed AceDeceiver, it simulates iTunes to get a trojan app on its device, at which point it tries to engage in other nefarious behavior. What is AceDeceiver? From Palo Alto Networks: AceDeceiver is the first iOS malware we've seen that abuses certain design flaws in Apple's DRM protection mechanism —i.e. FairPlay—to install malicious apps on iOS devices, regardless of whether they're jailbroken. This technique is called FairPlay Man-In-The-Middle (MITM) and has been used since 2013 to spread pirated apps for iOS, but this is the first time we've seen it used to spread malware. (The FairPlay MITM attack technique was also introduced at the USENIX Security Symposium in 2014; however, attacks using this technique are still occurring successfully.) We've seen cracked apps used to infect desktop computers for years, in part because people go to extraordinary lengths, including deliberately circumventing their own security when they think they're getting something for nothing. What's new here is how this attack gets malicious apps on iPhones and iPads. How's this happening? Basically creating a PC app that pretends to be iTunes and then transfers the malicious apps along when you attach your iPhone or iPad over USB to Lightning cable. Once again, Palo Alto Networks: To carry out the attack, the author created a Windows client called the (Aisi Helper) to carry out the FairPlay MITM attack. Aisi Helper is intended to be software that provides services for iOS devices such as system reinstallation, jailbreaking, system backup, device management, and system cleanup. But what it is also doing is subresively installing malicious applications on any iOS device connected to the PC on which Aisi Helper is installed. (Note, only the latest app is installed on iOS devices at the time of infection, not all three at the same time.) These malicious iOS apps provide a connection to an author-controlled third-party app store for the user to download apps or games for iOS. It encourages users to enter their Apple IDs and passwords for more features, and provided these credentials are sent to acedeceiver's C2 server after they are encrypted. We also identified some previous versions of AceDeceiver that had corporate certificates March 2015. So only people in China are at risk? From this specific implementation, yes. Other implementations, however, could reach other regions. Am I at risk? Most people are not at risk, at least not now. Although much depends on individual individual Here's what's important to remember: pirated app stores and customers used to enable them are giant neon targets for exploration. Stay away, far away. This attack starts on the PC. Don't download software you don't trust. Malicious apps spread from PC to iOS over Lightning to USB cable. Don't make that connection and they can't spread. Never - never - give a third-party app your Apple ID. EVER. So what makes this different from the previous iOS malware? Previous cases of malware on iOS depended on distribution through the App Store or abusing corporate profiles. When distributed through the App Store, once Apple removed the offensive app, it could no longer be installed. With corporate profiles, the corporate certificate could be revoked, preventing the application from launching in the future. In the case of AceDeceiver, iOS apps are already signed by Apple (through the App Store approval process) and distribution is being performed through infected PCs. So simply removing them from the App Store —which Apple has already done in this case—also doesn't remove them from already infected PCs and iOS devices. How Apple fights these types of attacks in the future will be interesting to see. Any system with humans involved will be vulnerable to social engineering attacks—including the promise of free applications and resources in exchange for downloading and/or sharing logins. It's up to Apple to fix the vulnerabilities. It's up to us to always be vigilant. Is this where you talk about the FBI versus Apple? Absolutely. This is exactly why mandatory backdoors are a bad bad idea disastrously bad. Criminals are already working overtime to find accidental vulnerabilities they can exploit to harm us. Giving them the deliberate ones is nothing short of recklessly irresponsible. From Jonathan Zdziarski: This particular design flaw would not allow something like FBiOS to run, but it demonstrates that software control systems have weaknesses, and cryptographic collars like this can be broken in extremely difficult ways to fix with a large customer base and an established distribution platform. If a similar collar is found that would affect something like FBiOS, it would be catastrophic for Apple, and potentially leave hundreds of millions of devices exposed. Everyone should work together to harden our systems, not to weaken them and leave them, people, vulnerable. Because it's the attackers who will be the first to come in and the last to leave. With all our data. You know you have to stay on top of these insidious malware threats, but what is the most effective (and affordable) solution? Here are some solid options. It is a constant battle, the protection of a PC against malicious software. So you think you have your machine cleaned, more appears. Even so, you still need to have some protection installed. So I thought I'd list the tools I prefer to keep Windows as free of malware as possible. They don't cost a dime, and they are as reliable as a malware removal tool can be. 1: Malwarebytes This is my access tool when there is a malware problem. It's fast, it's always reliable, and it's free. The only fall is that there is no component in real time. For the free version of Malwarebytes to be actually active and scanned, the user must run the tool. Now, if the end user is too lazy (or forgotten), I suggest buying the non-free version, which contains a real-time component. But the free version is certainly solid. Note that here are the cases where removing a piece of malware by this tool will require a restart of the machine. 2: ComboFix ComboFix is the Mac Daddy of removal tools. It is also not a standard anti-malware tool as far as it is a great troubleshooter. When you have malware that just won't go away (and you suspect something a little uglier - like a rootkit or Trojan - that keeps reinstructing your machine), you want this tool. I recommend ComboFix, but with a warning: It's powerful. Very powerful. Don't leave the executable for this tool just out there. Use it and remove it. And unlike most malware removal tools, you (or the end user) will not be using the PC while this tool is running. 3: Spybot Search and Destroy Spybot Search and Destroy is one of the most popular anti-malware tools. If there is a piece of anti-malware software on a machine, it will probably be this one. Now, I'll say that S&D is not the most powerful of anti-malware tools, but it's by far the worst. I actually sort it just below Malwarebytes with regard to reliability. And since there's no harm in having two anti-malware tools on one machine (unlike antivirus, which is a big no), using Malwarebytes and S&D as a one-two punch will pick up most of every piece of malware. The only thing S&D has about the free version of Malwarebytes is that it has a real-time scanner. 4: Avast Free I like Avast. I like antivirus. I like anti-malware. The best thing about this tool is that you can have both at the same time for free! Not only is the anti-malware part of the tool safe and reliable, but antivirus is one of the tops of free suites. So this is a win-win, that's for sure. Yes, there are paid versions of the same software package, offering anti-phishing, secure purchases, SPAM protection and the like. But if you are looking for solid anti-malware and antivirus, just download the free version of Avast. 5: AVG Free For a long time, I was a great advocate of AVG Free for antivirus protection. Nwo? Not at all. AVG Free's ability to keep viruses at bay is less than stellar. But it does a good job of removing malware. What I like AVG is the one who is discreet. When a scan is being done, you will barely notice. The big downfall of AVG is that if you have to run ComboFix, you can't just turn it off. To run a tool like ComboFix, you have to completely remove AVG. That's a real pain. The safe side Here's my honest opinion: If your machine is a personal machine (home), tap on AVG Free and Malwarebytes and affect it. Or if you want an all-in-one tool, use Avast. But always keep a copy of ComboFix around just in case these tools miss some of the most nastieruglies crawling around. Regardless of which path you go here, just make sure you have (and use) protection. Practice safe computing! Computing!