About the PIA Client Security and VPN Security in General

There's been much discussion recently about the security of PIA's VPN services in particular and of VPN as a technology in general. This post should help both put our customers' minds at ease and also better educate them about how VPN technologies work and how they interact with the larger ecosystem of applications and network infrastructure.

First things first, no solution is 100% secure by itself. Applications depend on other applications and hardware in order to function properly, and compromise anywhere in the stack can be used to attack your privacy and anonymity.

In order to understand how PrivateInternetAcces works, you need to have a basic understanding of VPNs in general and how networking and routing interact to protect your data.

A VPN is an encrypted tunnel that works by creating a network interface in your computer similar to a simulated Wifi/Network connection. When your computer sends data to that simulated interface, your VPN software encrypts the data and sends it to your gateway through your actual network interface. This gateway then decrypts the data and sends it to whichever original destination you want it to go to.

Your computer knows which connection to send data to by checking your "Routing Table". When you're using the VPN, it usually says something like "in general, always send data to my simulated vpn interface". Aside from that, it often has other more specific rules, depending on your network configuration.

One other rule that you'll always have on your routing table when using a VPN is "when sending data to this VPN gateway, use my WiFi interface". Otherwise, your VPN software won't be able to connect to your VPN server and send your encrypted data to it. Thus, your routing table needs to have connections that allow it to be sent directly to the network.

This means that if your computer is behaving in a way that you don't want it to behave due to a compromise, the setup above can be exploited. By having a malicious actor take control of different parts of your computer or your network, your security can be put at risk.

Web browsers, albeit a fundamental part of our internet experience, are also a critical part of our security profile. Not only are they powerful applications in what they can do on our computers, but they are constantly communicating with servers which might not have our best interest in mind. This is always extremely dangerous: our browser is running attackers' commands on our computers. Also, browsers are really complex applications, and are often capable of running even more powerful plugins like Java and Flash, all of which have had vulnerabilities disclosed in the past.

The fact is that browsers can for instance, on the behalf of the website you're visiting, open arbitrary network connections from your computer to pretty much any other server in the internet. This means there can be amazing power over your computer in the hands of a malicious website operator once you give him free-reign over your browser by accessing his web page.

But the question is: can a malicious website still threaten my security or anonymity by just visiting? The answer is, like in so many complex situations, it depends. Here are some of the scenarios in which the answer might be yes:

- Your flash version is not up to date. The website can take control of your computer and run arbitrary commands on it, and it's likely the malicious website can control your computer in a way that threatens your privacy/anonymity even if you're using a VPN.

- You're using Java. Even though Java is patched every 3 months, given the 30+ vulnerabilities announced every trimester, it's very likely that you're at risk by browsing with Java enabled. It's recommended practice that if you need to use Java for anything (usually corporate intranet applications or banks) that you use a browser just for that, so you reduce the risk of opening a malicious website on it.

- There's an exploit on the browser itself. This is what happened when the FBI injected malware on users of the Tor Bundle firefox browser by hacking into a website and serving users of the website the malware it used to de-anonymize them.

- By forcing you to connect to another website that keeps track of your identity through cookies or by signing in, this other website can now match your VPN IP to your previous original IP on file as the same user assuming you used the website directly in the past, even if you never planned to let this other website know your VPN IP.

- The website opens a connection to a server which is not on your 'default' route. In other words, the data won't be sent through the VPN, and the malicious operator has the capability to either inspect network traffic by compromising your router or being able to read packets on your network, or to receive network packets directed to that server. Mitigating this is one of the biggest reasons why we don't recommend any sort of split tunneling.

Note that while these attacks are technically feasible when visiting a malicious website, they're generally not straightforward, to the point of being impractical and even more so on a Man In The Middle (MitM) scenario, ie., someone manipulating network data between you and a legitimate website. The reason is that the VPN connection already protects you against MitM attacks all the way until the VPN Gateway server, and it's way harder to do an attack far away from the Gateway than it is before it, say by compromising your public/home WiFi router.

In any case this is why we recommend users who really need to be as sure as possible of their anonymity to add layers of protection because you never know where the next vulnerability will be. Unfortunately the most common operating systems (Windows and OSX) do not offer this solution directly. However, by having a firewall that makes sure that only your VPN application sends unencrypted data to your

WiFi/Network interface, for instance, you can prevent any other malicious application from sending data with your original IP. There’s a chance your firewall has a weakness on it, but it does act as another layer of security.

Likewise, if your browser has a proxy setup on it, it’ll from then on always send data directly to that proxy, instead of relying on the routing table. There’s still a chance your proxy could be compromised, but you add another layer of security.

By disabling javascript and only enabling it on known non-malicious websites you trust, you can prevent some types of network connections from being open. There are still ways to open connections without javascript, and the site you trust could be compromised by a third-party (like in the FBI case discussed previously). But it is another layer of security.

Our team at PrivateInternetAccess is working around the clock to keep your anonymity and your data safe. It’s important to be aware that no single solution can protect everything 100% of the time regardless of flaws and vulnerabilities elsewhere. Computers and networks form an inter-dependent ecosystem, and cracks on any of those interactions can be exploited by someone who doesn’t have your best interest in mind. In particular, web browsers are really powerful applications and in the hands of malicious website operations they can, in clever ways, put your privacy at risk.

Albeit we do not believe any of what is exposed above should concern the everyday user, it’s always important to understand that the internet can be a dangerous place, and that we are doing our best to make sure you are protected.