What is Root Certificate? How is it used for online monitoring?

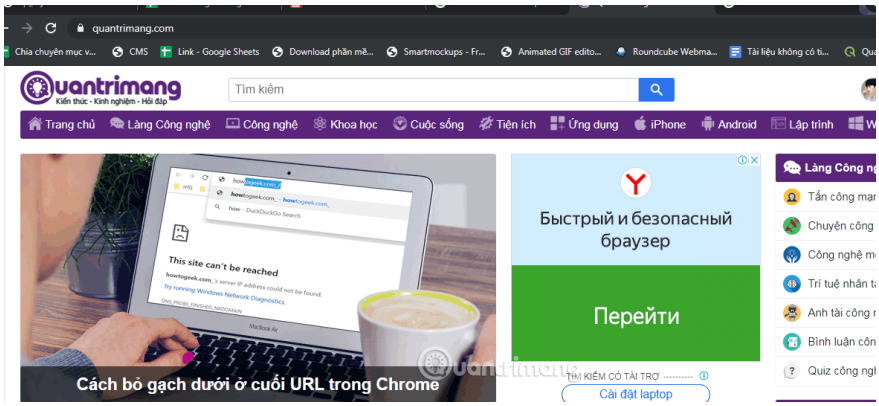
The abuse of root certificates is not just a problem in Kazakhstan. Internet users around the world should know about how this security tool is used to monitor online.

According to the news, in 209, the Kazakh government will take extreme measures to monitor its citizens. In particular, the government uses a tool called a Root certificate to track citizens' online activities.

However, the abuse of root certificates is not just a problem in Kazakhstan. Internet users around the world should know about how this security tool is used to monitor online. These tools can invade your privacy and collect data about the websites you visit and the messages you send online.

1. 7 reasons your website needs an SSL certificate
2. Don't trust these 7 myths about SSL and HTTPS certificates
3. How to view SSL certificate details on Chrome browser?

What is a root certificate?



When browsing a website like Quantrimang, you'll see the URL starts with https instead of http. You will also see an icon that looks like a key next to the URL in the address bar. This is an encryption called Secure Socket Layer / Transport Layer Security (SSL / TLS) securing the website.

With this encryption, data transmitted between you and the site is secure. So you can make sure the site you're actually visiting is the Quantrimang site, not the impersonating site that tries to steal your data.

To get this trust user lock icon, the website owner must pay to an organization called a Certificate Authority (CA) to verify them. When the CA verifies a website is authentic, it will be issued a security certificate. Web

browser developers like Firefox and Chrome keep a list of trusted CAs with certificates they accept.

So when visiting a website like Quantrimang, your browser looks for a certificate, verifies it comes from a trusted CA, and displays a secure website.

Root certificate is the highest level of security certificate. It is important because this certificate verifies all certificates below it. This means that the security of the root certificate determines the security of the entire system. Developers use root certificates for many valid reasons.

However, when organizations abuse the root certificate, they can install spyware on encrypted communications and access private data.

How does the Kazakh government abuse the original certificate?

In July 2019, the Kazakh government issued a notice to Internet service providers in the country, requiring them to install a government-issued root certificate that is mandatory for users to access the Internet. This certificate is called Qaznet and is described as a 'national security certificate'.

After installing the certificate, the government can use it to block large amounts of browsing data. They can view activity on popular sites like Google, Facebook and Twitter. It can even decrypt HTTPS and TLS connections, and access usernames and account passwords. This means that no website is safe if this certificate is installed.

According to security blog The Hacker News, basically, the government launched a man in the middle attack across the country. Because Internet service providers must install mandatory certificates that users cannot avoid if they want to continue accessing the Internet.

In addition, users can only install certificates over non-HTTPS connections. And hackers can block this process to install their insecure certificate.

How technology companies respond to misuse of root certificates

Technology companies including Google, Apple and Mozilla have responded to the situation in Kazakhstan. They have pledged to protect users against government oversight. The Google Chrome browser currently blocks certificates used by the Kazakh government, according to a blog post.

Google has taken this action to protect users from blocking or modifying TLS connections made on websites. Users do not need to take any action to be protected, the browser will automatically block this specific certificate.

Similarly, Mozilla has implemented a solution for Firefox. This solution will also block certificates used by the Kazakh government.

As a user, what can you do to prevent root certificates from being abused?

Using the wrong root certificate is obviously a concern, but what can you, an Internet user, do in this case? First of all, do not install a certificate on your device. If installed, remove it immediately. You should change the passwords for all online accounts to prevent organizations from accessing your browsing data.

Also, beware of suspicious certificates. If asked to install a security certificate, research it to see if it is trustworthy before installing it on your device.

Users should also take other steps to protect data such as using a VPN to avoid surveillance. In addition, you should also consider using the Tor browser to access the Internet anonymously. Be careful with email because it is difficult to protect it from surveillance. You might consider using a secure messaging app like Signal or Telegram.

The situation in Kazakhstan is just one example of how organizations can track users through Internet activities. You should learn about how companies can implement surveillance techniques to avoid them.

You finished reading the article "**What is Root Certificate? How is it used for online monitoring?**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

© 2019 TipsMake.com