Beware of Root Certs in VPN

labs.k7computing.com/index.php/beware-of-root-certs-in-vpn/

By Harihara Sudhan July 8, 2022

After the recent pandemic, Remote and Hybrid jobs have become the new working model. This has forced organizations to provide VPN access to their employees for their day-to-day work. This is evident from the fact that there has been a steep increase in the number of VPN users across the globe. More than 31% of internet users rely on VPN services. A study found that VPN downloads increased by 184% from 2020 to 2021. From 277 million downloads in 2020 to 785 million in 2021 as shown in Figure 1.

3. 785 million VPN downloads in 2021

A study by AtlasVPN found that VPN downloads exploded to 785 million in 2021. Compare this to 277 million downloads in 2020, and you have an increase of over 184 percent in uptake.

Figure 1 – source: https://www.comparitech.com/vpn/vpn-statistics/

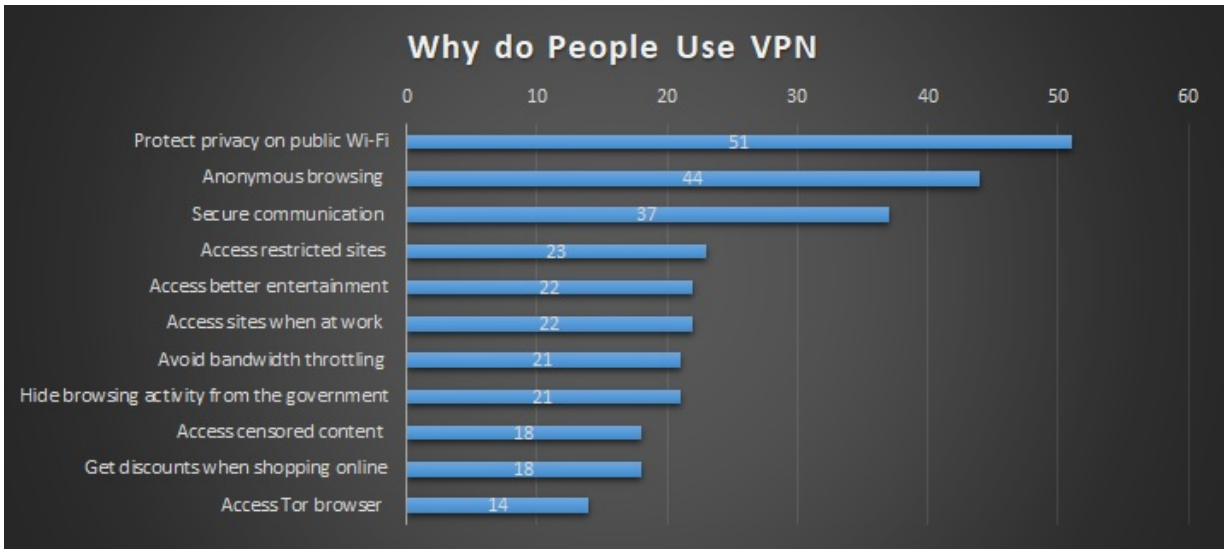

Figure 2 – Why do People use VPN

The recent surge in VPN usage has given rise to a new set of issues that the users were not aware of until new research revealed that many VPN products are installing root certificates in the user's device, without the user's consent. These VPNs have come under the radar after they were all flagged by Appesteem.

Here are some of the Suspicious behaviours that were identified –

- During the installation, the VPN also installed a trusted root certificate without any user action, and neither was there any proper intimation to the users that such a certificate has to be installed on their machine.
- Not disclosing the potential risk of adding an untrusted certificate & the effect it has in reducing the security posture.
- Also doesn't remove the installed root certificate, even after uninstalling the application.
- During installation, a start-up entry is created without user consent and there's no control over this.

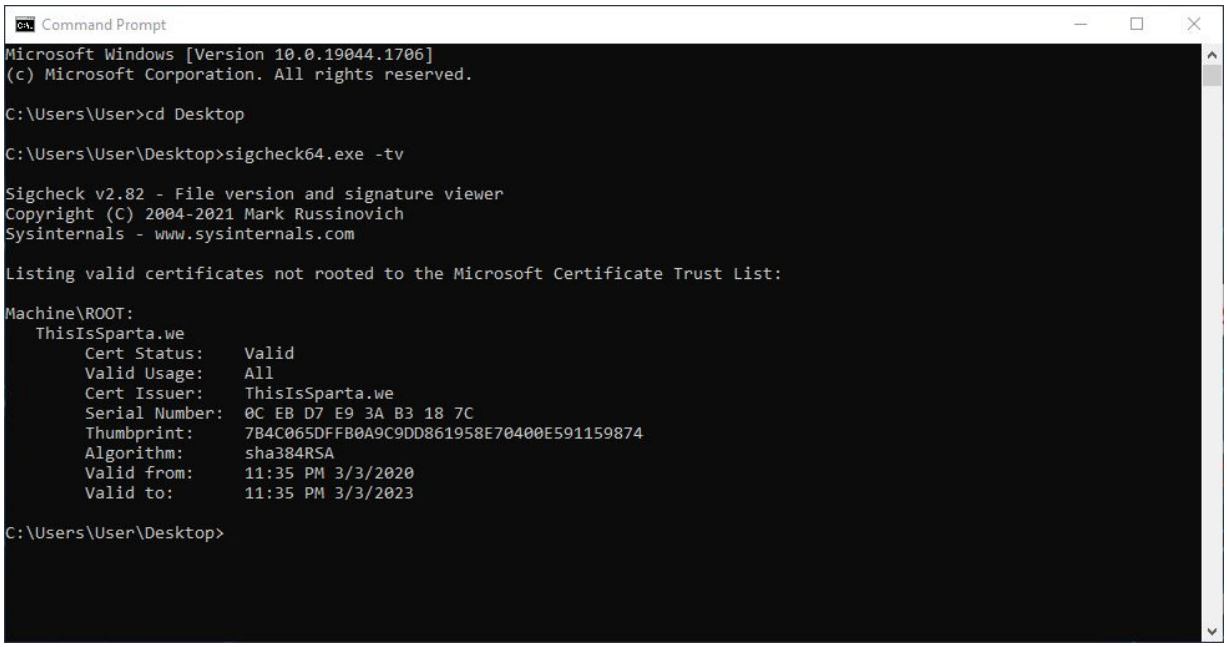

Figure 3 – Checking Valid certificates that are not rooted to MS Certificate Trust list

SigCheck is a command-line utility to check the details of the digital signatures, their timestamp info, etc. As seen above in figure 3, we used the " Sigcheck -tv" command to list certificates that are not rooted to the Microsoft certificate trust list.

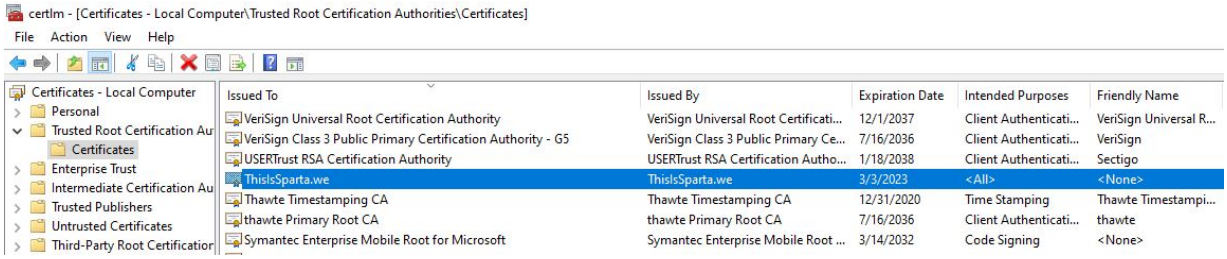

Figure 4 – Non-trusted Root Certificate

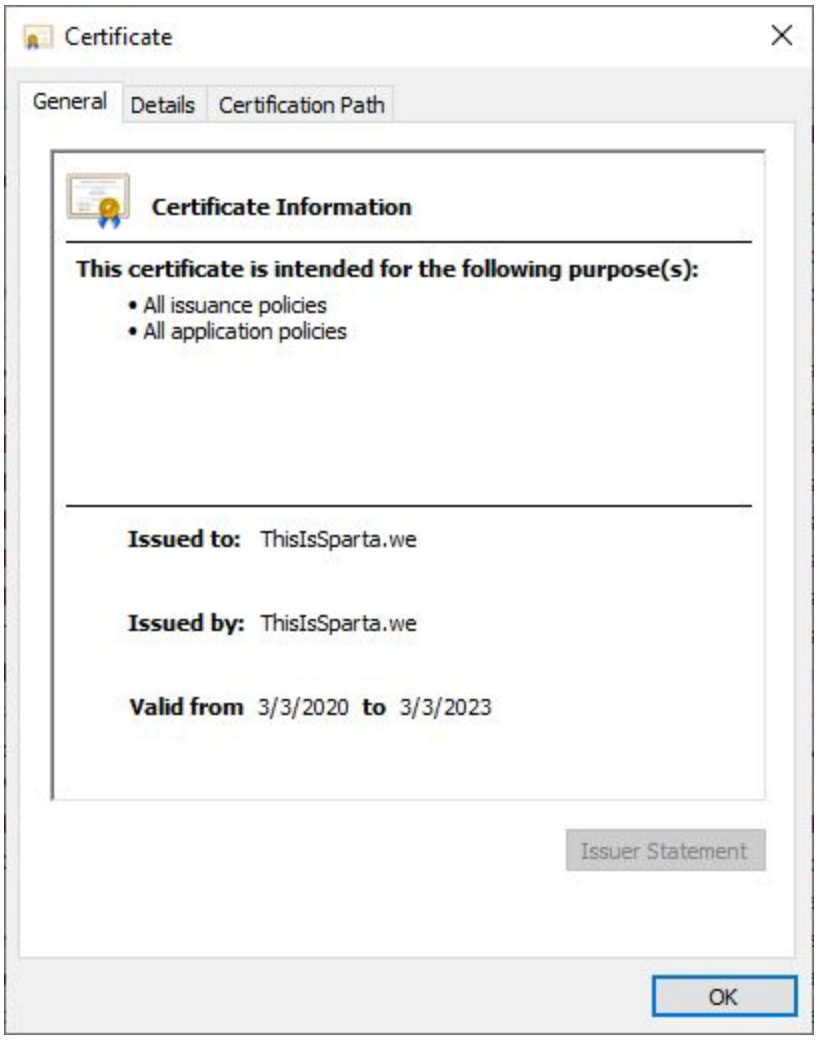

Figure 5 – Detailed view of the Non-rooted Certificate

Right after the installation of a VPN client, the Non-trusted Root Certificate "ThisIsSparta.we" is installed with the Intended purpose "All", without any user consent, as seen in Figures 4 and 5.

Abuse of Root Certificate

A root cert is a self-signed public-key certificate that represents the root certificate authority. It's the tree's topmost certificate and all other certificates on the system derive their trustworthiness from it.

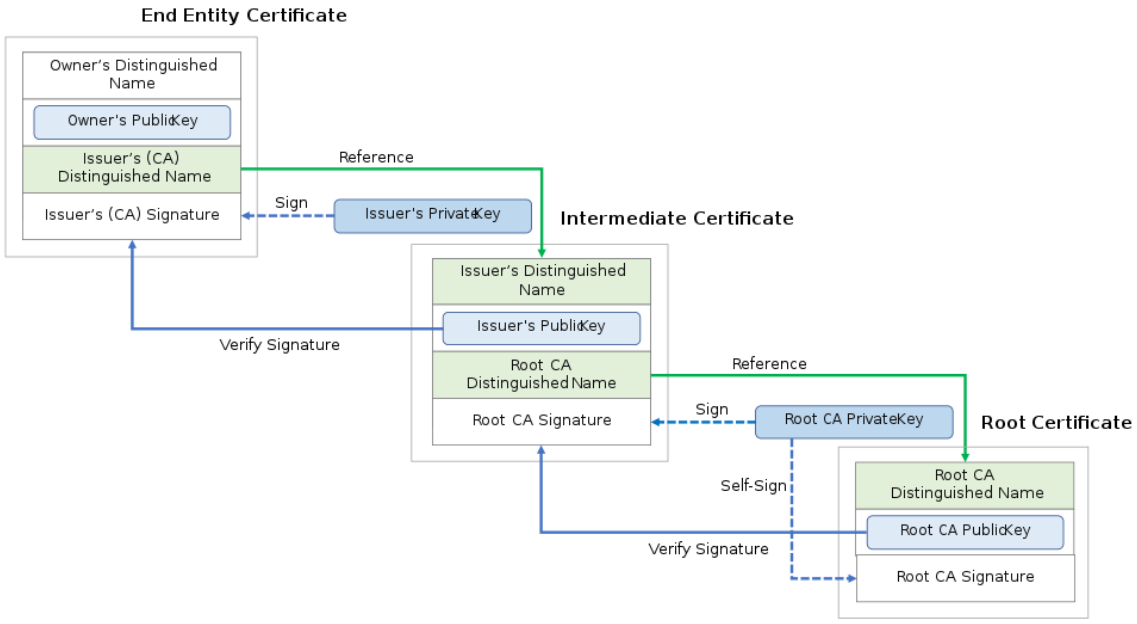

Figure 6 – source: https://en.wikipedia.org/wiki/Root_certificate

Secure communications through browsers and many applications on the local system rely on root certificates to validate claims of authenticity and origin. So when a rogue root certificate is installed on the Certification store, it severely compromises the security stance of the system. It leads to opportunities for phishing, man-in-the-middle attack, and illegitimate applications running amok in the system.

Notable incidents of root certificate issue

Russia's own Certificate Authority to bypass sanctions
Following sanctions from western countries, Russia was unable to renew its certificates, causing issues in webaccess. To resolve the issue, Russia has created its own TLS certificate authority (CA).

Microsoft Windows Insider renewal
Microsoft forgets to renew the certificate of one of its subdomains 'insider.windows.com' causing all browsers to stall loading the related webpage.

CNNIC Issuance of Fake Certificates
CNNIC stands for China Internet Network Information Center. Google discovered in 2015 that CNNIC had issued an intermediate CA certificate to an Egyptian organization impersonating Google domains using CNNIC's keys. Google responded by removing CNNIC's root certificate from Google Chrome's certificate store, as well as all of Google's other products.

DigiNotar hack of 2011
DigiNotar, a Dutch certificate authority, had a security breach in 2011. This resulted in the creation of several fake certificates, which were used to target Iranian Gmail users. The trust in DigiNotar certificates was retracted and the operational management of the company was taken over by the Dutch government.

We at K7 Labs provide detection against such apps & latest threats. Users are advised to use a reliable security product such as **“K7 Total Security”** and keep it updated to stay safe from the latest threats.

Further Readings