Research on the use of Russian Trusted CA and self-signed SSL Certificates in the Russian Internet

Permalink to research

Introduction

This report delves into digital security and the usage of the digital certificates on the Russian segment of the Internet. This analysis examines the prevalence of Ministry of Digital Development, Communications and Mass Media root certificates and self-signed SSL certificates associated with Russia. SSL-certificates play a critical role in securing online communication. Our research sheds light on their usage within the Russian cyber landscape.

Note: The information in project's GitHub repository is regularly updated to provide up-to-date statistics on root and self-signed certificates usage.

The role of the Russian Trusted CA

Sanctions and Certification Authorities

One of the key drivers behind the use of Russian Trusted CAs is the sanctions imposed on Russian companies after 24 Feb 2022 (as stated by the Russian government). These sanctions have forced many reputable companies to avoid financial transactions with their Russian counterparts in order to avoid sanctions-related investigations. Even some Certification Authorities, which issue encryption keys for websites, have refrained from working with Russian companies because of these sanctions.

The Russian Ministry of Digital Development, Communications, and Mass Media

As a result, some websites have resorted to using certificates issued by the Russian Ministry of Communications. However, it's important to note that these certificates are marked as insecure in all modern web browsers, with some exceptions like Yandex Browser and certain custom in-house builds of Chromium Browser used by government agencies. Moreover, it should be noted that the analysis of the source code of Yandex.Browser shows that the application of the Russian Trusted CA is currently possible only on sites from a special list source. Attempting to apply the certificate to other domains will result in a standard error and inaccessibility of the site for the user.

Understanding the dataset

Our research is based on an extensive dataset comprising 21,698 websites. This dataset serves as the foundation for our exploration of digital certificate usage patterns across different categories of websites.

Note: What is an SSL Certificate?

Before we go any further, it's important to clarify what an SSL Certificate is. A Secure Sockets Layer (SSL) certificate is a digital certificate that authenticates the identity of a website and encrypts data sent to the server. In simple terms, it ensures that the information exchanged between a user's browser and a website remains private and secure.

Government-related sites

We identified 715 government-related sites websites that require a Russian Trusted CA, and 249 sites that use self-signed SSL certificates issued by Russian-linked companies. These findings reveal the significant presence of such certificates in the government sector.

Socially important sites

We also examined socially important sites. Within this category, we found that 7 sites require a Russian Trusted CA, while none of them use self-signed SSL Certificates issued in Russia. These results provide an insight into the reliance on Russian Trusted CAs for access to socially important platforms.

Note:

- *Government-related sites* include official sites that are either directly or indirectly related to the government. The list of these sites can be found here.
- *Socially important sites* are sites to which telecom operators are required by law to provide free access for every citizen source. These sites are considered critical for access by all citizens and include entities such as Russian social networks, banks, government portals, etc.

It's important to note that these categories, especially *Socially important sites*, include very important and popular platforms such as SberBank (the most popular bank in Russia) and GosUslugi, which provides access to state functions and services. Consequently, the requirement to use Russian Trusted CA in this category has the potential to force a large number of people to install Russian Trusted CA on their primary devices.

Top-100 websites in Russia

This research extended to the top 100 websites in Russia by traffic. Among these, only one site required a Russian Trusted CA, and none of them used self-signed SSL Certificates issued in Russia. But that's SberBank – an extra popular bank in Russia. But in general, this result shows that the most popular websites in Russia tend to use certificates issued by internationally recognised certification centres.

Security risks and concerns

There are inherent risks in using Russian certificates. It remains unclear whether these certificates meet the rigorous standards expected of a trusted Certificate Authority. This uncertainty raises concerns about the reliability and trustworthiness of the certificates issued by Russian CAs.

It's important to note that cryptography in Russia has already been criticised, including issues such as a lack of randomness in the permutation table source and the theoretical possibility of a backdoor in S-Box source in "Streebog" and "Kuznyechik" algorithms.

There is an apparent disparity in the perception of security between Russian browsers and those used internationally. While Russian browsers may accept these certificates, they are met with skepticism by most international browsers. This divergence in trust standards can lead to unforeseen consequences for users and organizations relying on such certificates.

Potential for abuse

There are also concerns that Russian Certificate Authorities may issue additional private keys for government agencies such as the Federal Security Service (FSB) and other intelligence services. See the MITM incident in Kazakhstan. Such practices could potentially compromise the security and privacy of online communications.

Implications and consequences

The results of our research underscore the complex landscape of digital security on the Russian internet. The proliferation of Russian Trusted CAs and self-signed SSL Certificates associated with Russia poses significant challenges and risks to both individuals and organisations.

Conclusion

In conclusion, our research provides valuable insights into the use of Russian Trusted CA and self-signed SSL Certificates on the Russian Internet. These certificates, while prevalent in certain sectors, come with security and trustworthiness concerns. It is essential for users and organizations to make informed choices when navigating the online landscape to ensure their digital security and privacy are protected. The implications of these findings go beyond just the

technical; they touch upon the very fabric of civil society and society at large, where privacy and security are fundamental rights that must be protected. The use of such certificates may have unforeseen consequences, given the uncertainty about their compliance with international standards and some concerns about potential access by the government to private keys.