What is the first principle of zero trust?

Speaking of zero trust, everyone knows the importance of identity validation, and it is necessary to always verify the identity, but they have ignored an important principle and ignored the constant verification of an important element. What is it? Website Identity! The Web is the largest traffic on the Internet, and the zero trust security solutions of all providers only focus on people's identities, realizing the constant verification of people's access to website resources. But all solutions cookie-cutter ignoring the constant verification of a website's identity is a huge technical misdirection.

According to data released by PandaLabs, more than 57,000 new counterfeit websites are created every week around the world, and about 375 different well-known brands and company brands are used to attract users. 65% of counterfeit websites imitate bank pages, followed by e-commerce sites and auction sites, accounting for 27%. These fake websites are skilled in SEO and searching skills, so that unwary Internet users will be fooled by clicking on these fake websites by mistake. Well-known brands that have been counterfeited include eBay, Western Union, Visa, Amazon, Bank of America, PayPal, and USA Tax Services etc. The most frightening thing is that these fake websites have security padlock since free SSL certificates are readily available. This had to get the FBI to warn consumers - Stop trusting your browser's https security padlock. T. This is zero trust to websites and zero trust to https encryption.

According to the data on web page phishing in the 2020 "China Internet Network Security Report" released by the China Computer Emergency Response Technical Center (CNCERT), in 2020, CNCERT/CC sampled and monitored 220,648 phishing pages counterfeiting Chinese websites. Among them, the number of counterfeit pages with the title of "ETC Online Certification" has grown exponentially and reached a peak of more than 56,000 in August 2020, accounting for 91% of the total number of counterfeit pages. These fake ETO websites trick users into submitting names, bank Accounts, ID numbers, mobile phone numbers, passwords and other personal privacy information have caused many users to suffer economic losses. Affected by the COVID-19 epidemic, many governments

administrative process has turned to online. At the end of 2020, many counterfeit pages with the title of "Unified Business License Information Management System" appeared, and more than 53,000 such counterfeit pages were found in monitoring from November to December 2020 alone. Criminals use such pages to trick users into submitting real name, bank card number, balance in the card, ID number, mobile phone number reserved by the bank and other information on the counterfeit page. In addition, the monitoring also found many counterfeit pages with titles such as "Nucleic Acid Testing" and "Vaccine Appointment", the purpose of which is to illegally obtain personal privacy information such as usernames, addresses, ID numbers, and mobile phone numbers. These fake websites basically do not deploy SSL certificates, if users use a browser to access, they will definitely prompt "Not secure". But unfortunately, if user use WeChat to view the link, there is no "unsafe" prompt.

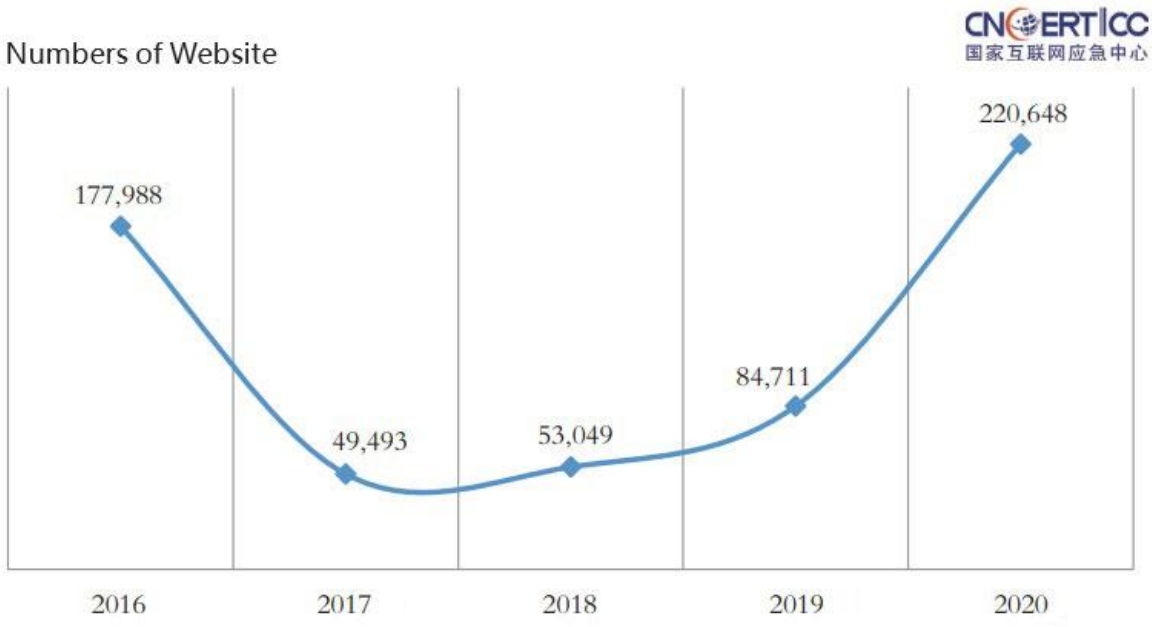


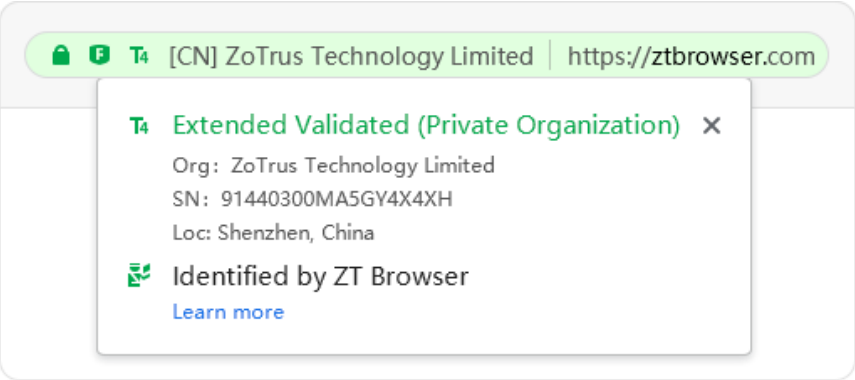
Figure 5-11 Statistics on the number of phishing pages counterfeiting China websites from 2016 to 2020 (Source: CNCERT/CC)

Even if the website deploys an SSL certificate and implements https encryption, we still must have zero trust for each website we visit, and we must verify the real identity of the website. The author believes that the constant verification of website identity should be the first principle of zero trust, followed by zero trust in the identity of website visitors, verifying the source of the data must be the first taking. If the user is visiting a fake website, what is the use of zero trust always verifying the user? Possibly even more harmful because a real user identity falls into the hands of a fake website!

So, how to achieve the always-verification of website identity? This task should be undertaken by the browser, because the browser is the entrance to the Internet, and it is a must for a good browser to display the real identity of the website being visited for the browser user. And how does the browser know the real identity of the website and show it to the user? There are two ways to achieve this. One is to obtain the website identity information contained in the SSL certificate deployed by the website from the https communication of the website. The subject of all SSL certificates will contain the website's identity information that CA operator validated. The browser can directly display this identity information for viewing by the browser user, which is the most convenient and reliable technical means. Because when the CA operator issues the SSL certificate to the website, it will issue the SSL certificate according to the principle of writing the corresponding identity information into the SSL certificate according to the identity verified.

The second way is for the browser producer to validate the identity of the website and display the identity of the website. This is very suitable for websites that have deployed a DV SSL certificate that does not validate the identity of the website. When the CA issues the DV SSL certificate, it only validates the control of the domain name and then issues the DV SSL certificate. The certificate subject information only has the domain and no website identity information. Therefore, the browser cannot obtain the identity information of the website through the SSL certificate, so it can only validate the identity of the website by itself. This is the main reason why ZoTrus Technology launched the Website Trusted Identity Validation Service, which effectively makes up for the defect that there is no website identity information in the DV SSL certificate.

The author believes that it is a very wrong decision for major browsers to remove the green address bar of websites that have deployed EV SSL certificates and directly display the organization name in the address bar. Browsers that don't display the real identity of the website indirectly become an accomplice to the fraudulent fake website! Fortunately, ZT Browser has enhanced the display of the identity information of EV SSL, OV SSL and IV SSL certificates that validated the identity of the website, which can effectively ensure that website visitors can easily understand the real identity of the website they are visiting, so that it is very easy to make the right security decisions.



Therefore, the first principle of zero trust should be not to trust websites that have not passed third-party identity validation, the second is not to trust websites without https encryption, and the third is not to trust the identity of website visitors and always verify the identity of the visitor. This order cannot be wrong, otherwise it will go to the wrong direction. Moreover, the zero trust of these three elements is interrelated. Only when the website has passed the identity validation by a third party (such as a CA operator), deployed an SSL certificate to achieve https encryption, and verified the identity of the website visitor each time is a complete zero trust security chain, this solution can truly ensure that the "right person" visits the "right website" and obtains the "right data".

Richard Wang

June 1, 2022
In Shenzhen, China