It is Urgent to Popularize Cloud WAF Protection

The author fully realized the importance of cloud WAF protection from my company's official website to enable cloud WAF service, so it is very simple to think that all websites need cloud WAF protection. Therefore, the author checked the "China Internet Network Security Report (2020)" released by CNCERT/CC (the 2021 report has not yet been released) and the issue of the seventy weekly report on April 26, 2022. From these two reports show that China website security situation is still very serious, and some data are shocking. This article will interpret and analyze the data in these two reports and put forward countermeasures and suggestions for improving China website security situation.

The CNCERT report on website security is divided into 3 parts: phishing, website backdoor, and web page tampering. This article only covers the latter two parts, and phishing will be discussed in another blog post. Let's take a look at the statistics of 2020. In 2020, CNCERT has monitored a total of 53,171 websites in China that have been implanted with backdoors, of which 256 are government websites. This data is very surprising, because government websites contain a large number of personal and business confidential data. A website backdoor is a backdoor program left after a hacker successfully invades a web server. By uploading a remote-control page in a specific directory of the website, hackers can remotely control the website server secretly, upload, view, modify, delete files on the web server, read and modify the data of the website database, and even directly run system commands on the web server and use the web server as a "broiler" for launching DDOS attacks. Why the website can be implanted with backdoor, of course, it is because the website has no security protection.

Looking at the data on web page tampering in 2020, the number of tampered websites in China is 100,484, of which 494 are government websites. Web page tampering refers to maliciously destroying

or changing the content of a web page, making the website unable to work normally or appearing abnormal web page content inserted by hackers. From the perspective of the means of tampering attacks, more than 50% of the tampered websites in China were attacked by implanting dark links. Why web pages can be tampered with, of course, it is because the website has no security protection.

Looking at the website trojan data in 2020, in the incidents of using trojans or bots to control servers to control hosts, the total number of IP addresses of the controlled servers was 65,865. Not only server data was stolen, but also these servers can be exploited to launch various attacks. Why the server can be trojan-ed, of course, it is because the website has no security protection.

The above data is for 2020. Let's look at the data for one week in April this year. CNCERT monitoring found that the number of tampered websites in China was 3611; the number of websites with backdoors implanted was 738. Among them, 17 government websites were tampered with, and 12 government websites were implanted with backdoors. It can be seen that the number of backdoors on websites has declined, but the average amount of web pages tampering has almost doubled than the week average in 2020. Today, two years later, the situation has not improved, but is even more severe, and there are still some government websites implanted with backdoors and web pages tampered with.

You should see from these data that the security situation of websites in China is not optimistic, it can be said to be very serious. There is only one fundamental solution to these security problems: enable cloud WAF protection for all websites, because 99% of website owners are like my company that do not have the ability to protect the website. For government websites, enabling cloud WAF protection can not only ensure the security of government websites, but also meet the compliance requirements of Cyber Security Law.

Therefore, in order to ensure the security of my company's official website after it goes online, we have simultaneously launched Alibaba Cloud WAF protection, which has achieved satisfactory results. This made us decide to implement our website security cloud service based on Alibaba Cloud WAF, because we believe that all websites need cloud WAF protection. One-click setting of CNAME resolution, turning the original website into the source website of cloud WAF, can immediately activate the website security protection, and no backdoors will be implanted, the webpage will no longer be

tampered with, the server will no longer be trojan-ed, and the server will no longer be attacked by SQL injection, no cross-site attacks, no CC attacks, no malicious scans, no worries about vulnerability attacks, etc. all kinds of website security problems have been completely solved. These protections are provided by Alibaba Cloud WAF that rewarded by Gartner, Forrester, IDC, Frost & Sullivan, it effectively guarantees 365-day website security and worry-free, and customers can concentrate on doing their own business with confidence.

The cloud WAF protection effect is so good, of course, the price is not cheap. ZoTrus Technology uses the exclusive version of Alibaba Cloud WAF, which costs hundreds of thousands of RMB Yuan a year. Based on the Alibaba Cloud WAF system with excellent protection performance, we have realized the automatic configuration of SSL certificates, and shared this high-quality cloud resources, which can provide one-stop https encryption, cloud WAF protection and trusted identity validation service three-in-one website security services for all websites, and provides these three website security and trusted services at a fixed annual fee that customers can afford, so that high-end WAF protection and HTTPS encryption makes all websites no longer have security problems at a popular price, no longer worry that the transmission of cleartext will reveal confidential information, no longer worry that all browsers display the website as "Not secure", no longer worry that the website will be attacked, website is safe for 365 days and worry-free, and customers can concentrate on their business with confidence.

ZoTrus Website Security Cloud Service, a global top brand SSL certificate plus top brand cloud WAF protection annual subscription service, integrated automatic https encryption (no need to apply for an SSL certificate), automatic cloud WAF protection (no need to do any configuration) with free website trusted identity validation service, it is definitely a value-for-money service for websites! ZoTrus Website Security Cloud Service makes all websites secure! Clear the website security incident data in CNCERT's next year's security report!

Richard Wang

June 1, 2022
n Shenzhen, China