Ransomware On Websites- How WebOrion can help as a countermeasure against attacks

With the recent trend of Ransomware attacks like WannaCrypt and Petya/NotPetya, more people have been concerned with cyber security and how they can protect their personal computer. However, there have been a rising variant of ransomware that targets web servers instead of personal computers. Critroni, better known as CTB-Locker (web server edition), is one such example.

One might argue that a web server infected by ransomware is more damaging than a personal computer. So, here are some ways WebOrion can help you protect your web server from ransomwares and other deadly, destructive attacks.

WebOrion Web Application Firewall (WAF)

The first line of defence should always be a firewall to block out most of the attacks. Besides a normal network firewall, a web application firewall (WAF) is highly recommended to protect important websites and web applications. Our WebOrion WAF helps to protect against the OWASP Top 10 most application web application security risks and does deep inspection of HTTP/HTTPS packets which allows it to prevent many more kinds of web attacks like SQL Injection and Cross-Site Scripting.

Furthermore, our cloud-based WebOrion WAF comes with different packages of global CDN that enhances the performance of websites globally and in some cases provide DDOS capabilities to counter volumetric attacks.

WebOrion Monitor (WM)

The WAF is essential as a security wall that blocks out 80-90% of the attacks and unfortunately there is no WAF in the industry that will block out every single kind of attack. And as such, there is still a remote possibility that the website may still be compromised, eg. by an attacker that comes from within the network. As such, it is still important to have proactive monitoring to complement the WAF.

With WebOrion Monitor, we aim to let you, rather than your visitors, be the first to detect any defacements or ransomware attacks on your website. With an early detection, you essentially have more time to fix and remedy the problem, minimizing the reputational damage done to your organization

WebOrion Restorer (WR)

What happens when your website has already been defaced or attacked by ransomware? A simple backup and restore could fix your website, but it would still have the vulnerabilities that it had before the attack. Attackers could simply make use of the same vulnerabilities to deface or even infect your website again.

WebOrion's Restorer creates a secure replica that is hosted on a security hardened server and strips off all the possible points of intrusion. In the event of a defacement or ransomware attack, we can divert the traffic from your original website to the secure replica. This buys you time to find out the root cause of the attack and allow you to fix the vulnerabilities before reverting the traffic back to your original website.

In this case, you will be able to maintain your web presence and prevent any damage to your reputation as your visitors will not even realise that your website has been compromised, making fixing and restoring much less stressful.

WebOrion Web Scanner (WS)

A web scanner is able to sniff out system vulnerabilities, application vulnerabilities or traces of malware. Being able to detect weakness in your configuration would allow you to enhance and fortify your server. Early detection is important so that you can secure your website before those nasty hackers find any exploits.

Conclusion

WebOrion Business SaaS is an affordable cloud-based security solution with packages for both small businesses to large enterprises. WebOrion is a single unified portal containing essential web security tools that helps you prevent and detect an attack. No hardware and software installation is required and setting up is straightforward and there will be assistance from our friendly customer support if needed.

Find out more at www.weborion.io to start protecting your website!