Barracuda

PARTNER LOGO

How to Secure Your Web Applications from Ransomware attacks?

While phishing and social engineering are common ways to deliver ransomware, cybercriminals also hack into vulnerable web applications and move laterally to wreak havoc on your system weakness and cause reputational damage to your brand. See the following real-life cases.

CASE 1: Vulnerabilities in a public-facing Internet managed service provider application were exploited to spread ransomware, putting all customers at risk.

CASE 2: The hacker harvested credentials against an unprotected remote desktop application and successfully infected the entire corporate network with ransomware.

CASE 2: The attacker created a website that mimicked a legitimate site using domain impersonation and automated web scraping and successfully stole all users' credentials.

Application security is as critical as email security in fighting against ransomware and other malware. One of the best ways is to deploy a highly configurable and customizable **WEB APPLICATION FIREWALL** that offers full protection against zero-day attacks, credential stuffing, data-leakage, and malicious bots with continuous threat intelligence. It should also be easy to update and scalable enough to support your business growth.

Barracuda Networks is your answer! Learn more about how to safeguard your application security and bolster the organization's security posture with our web application firewall solutions.

- **Barracuda Web Application Firewall**
- **Barracuda WAF-as-a-Service**

To do a free vulnerability scan of your web facing application, try our Applications Vulnerability Scanner or contact us today for a free consultation.

Contact Us

Forward this to a colleague