WEBSITE SECURITY
trends & predictions
FOR 2019

altinet

Websites are targeted by an average of 58 attacks per day.

MALWARE

Malicious bots represent 87% of all traffic filtered through WAFs.

BACKDOORS

Backdoors are increasingly used to break into sites and launch cryptojacking attacks.

SEO SPAM

SEO spam software can invoke spam penalties from search engines and damage your search engine results.

VULNERABILITIES

Unpatched vulnerabilities leave you open to malware infections

SQL INJECTIONS

At 19%, injection vulnerabilities were the most common of 2018, with SQL specifically leaving you 4x more vulnerable to malware.

SQLi

CROSS SITE SCRIPTING

XSS

At 14%, XSS was the second most common web application vulnerability of 2018, leaving you 5x more vulnerable to malware.

PREDICTED THREATS

Cryptomining saw a 44.5% rise in atacks through 2018

CRYPTOMINING

The number & quality of ready-made cryptomining tools means that criminals don't need to be technically skilled.

ARTIFICIAL INTELIGENCE

Experts fear that hackers will use AI to bypass advanced security implementations & learn defence tools.

PREDICTED DEFENCES

The rise in data breaches has led users to lose trust in password protection.

MULTI-FACTOR AUTHENTICATION

Most websites and online services will abandon password-only access in favour for multi-factor authentication.

HTTP SECURITY HEADERS

SSL only secures your website so much, but HTTP security headers such as CSP & HSTS can be used to stop threats like cryptomining.

For more information on web application security visit:

info.altinet.co.uk/altinet-waf-as-a-service