

Secure Cloud Server at a Glance

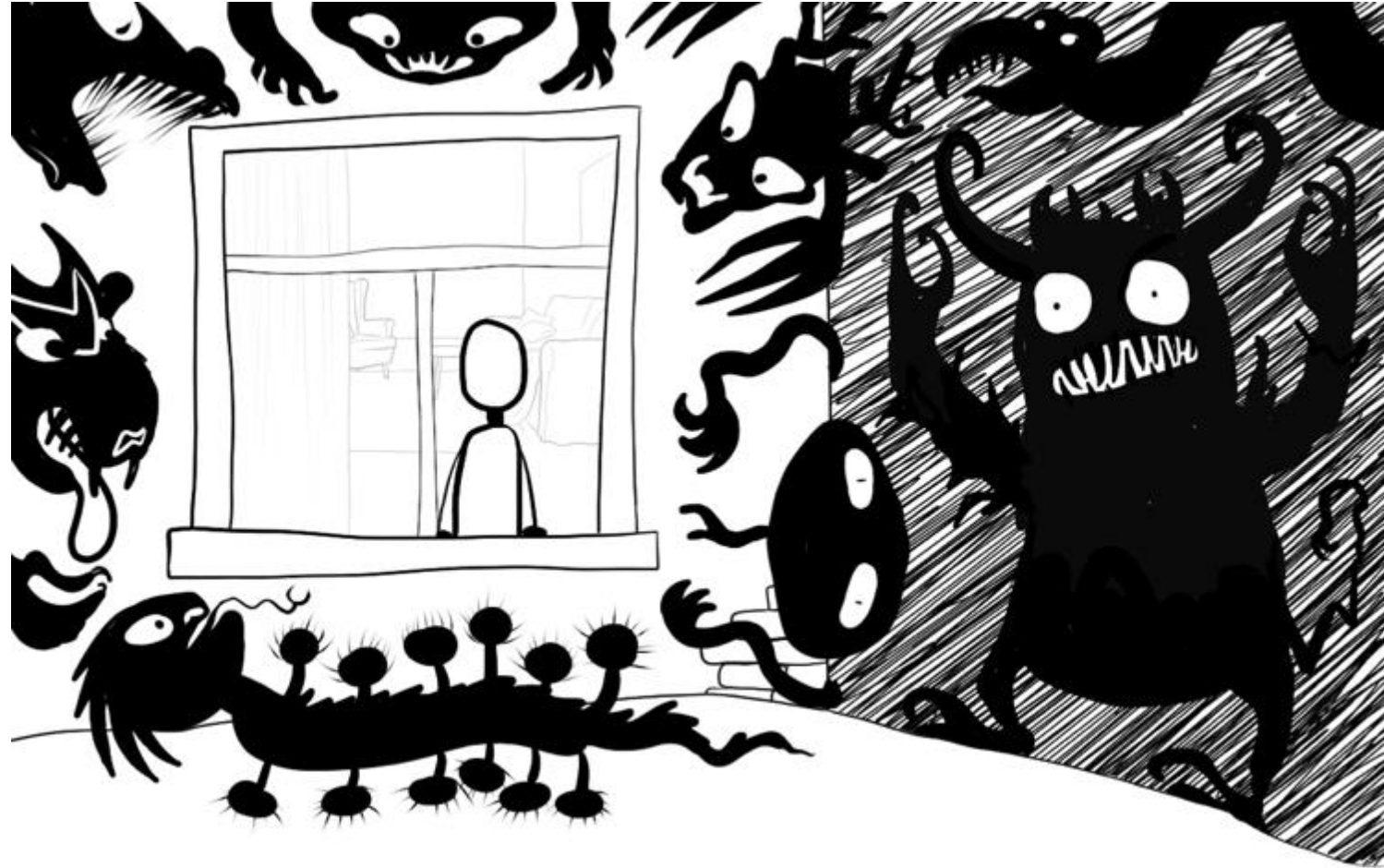
Sergey Lystsev, VP R&D, Plesk

The Plesk logo consists of the word "plesk" in a lowercase, sans-serif font. The letter "p" is black and has a blue horizontal bar extending from its base to the right, underlining the "p" and partially the "l".

plesk

The Night is Dark and Full of Terrors

- 60k sites hacked daily
from internetlivestats.com



The Danger is Real

- 90k attacks each minute

Wordfence.com

- 43%+ attacks target small businesses

reported in Symantec Threat Report

- 52% SMBs see web server as the most vulnerable point

reported in State of Cyber Security in SMB by Ponemon Institute



Are you Up2date?

3.8 mln attacks a month via known vulnerabilities

from WordFence WP attack report

22% of WP hacks done via outdated plugins

from Sucuri's Hacked Websites Report

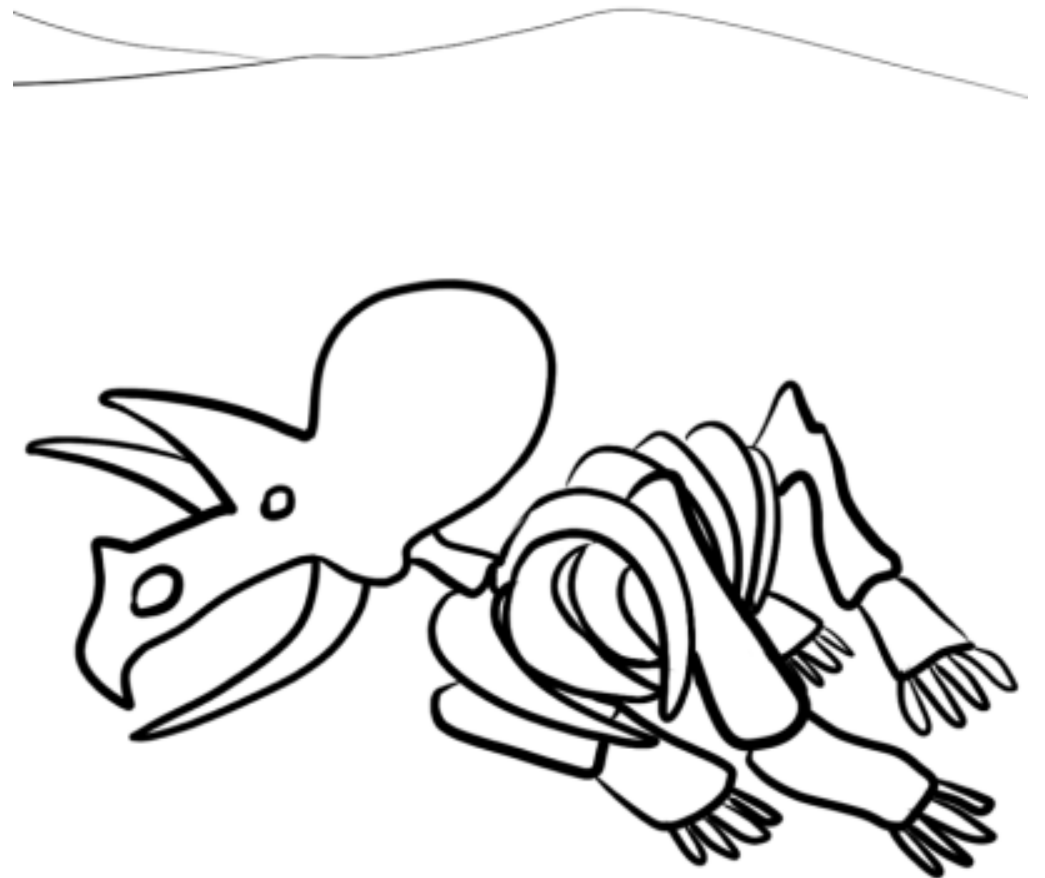
76% websites have known vulnerabilities

9% websites have critical known vulnerabilities

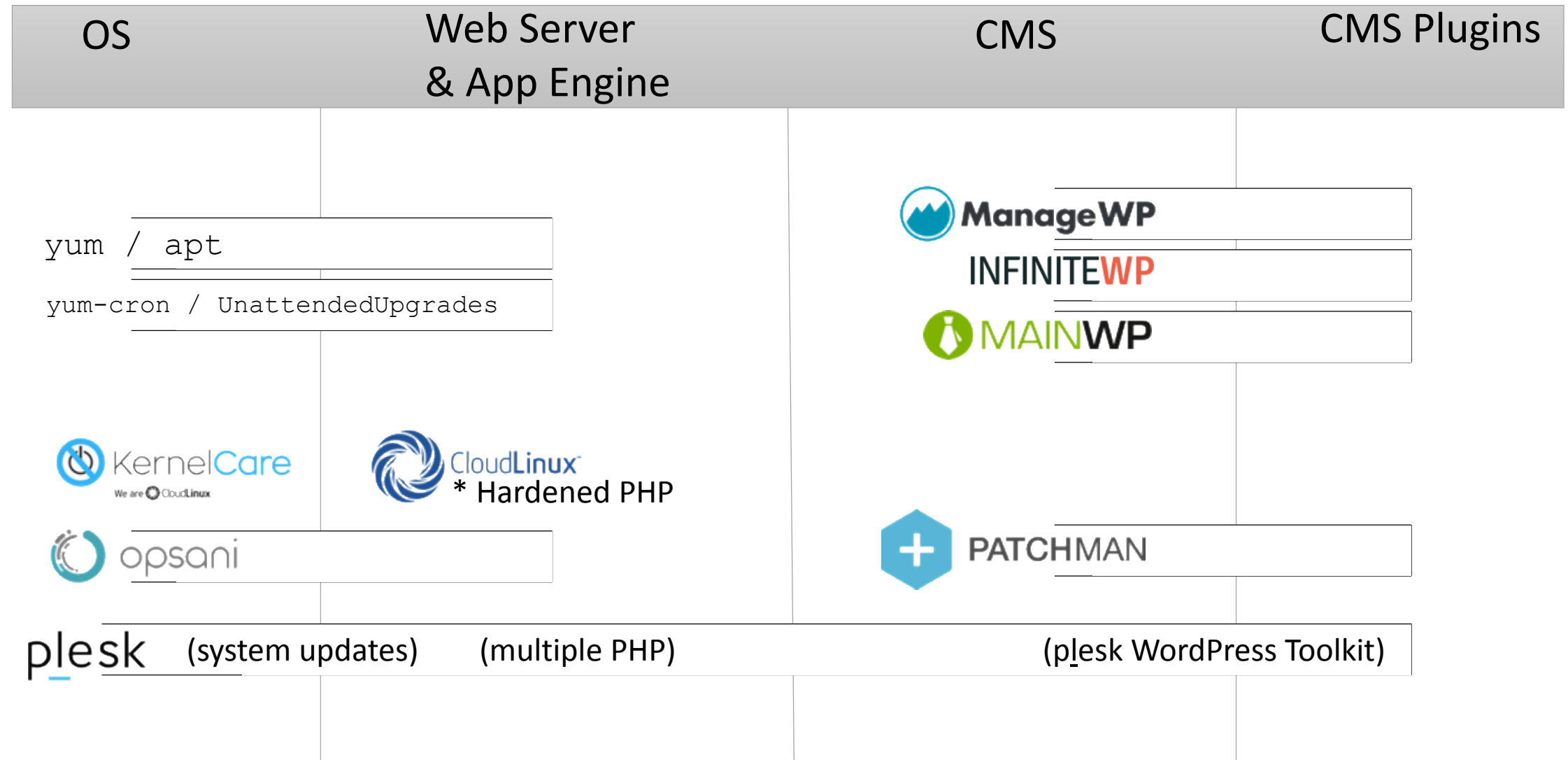
from Symantec Internet Security Threat report

48% websites run on PHP 5.5 and older (no security updates)

from Plesk stats



Be 100% Up2date



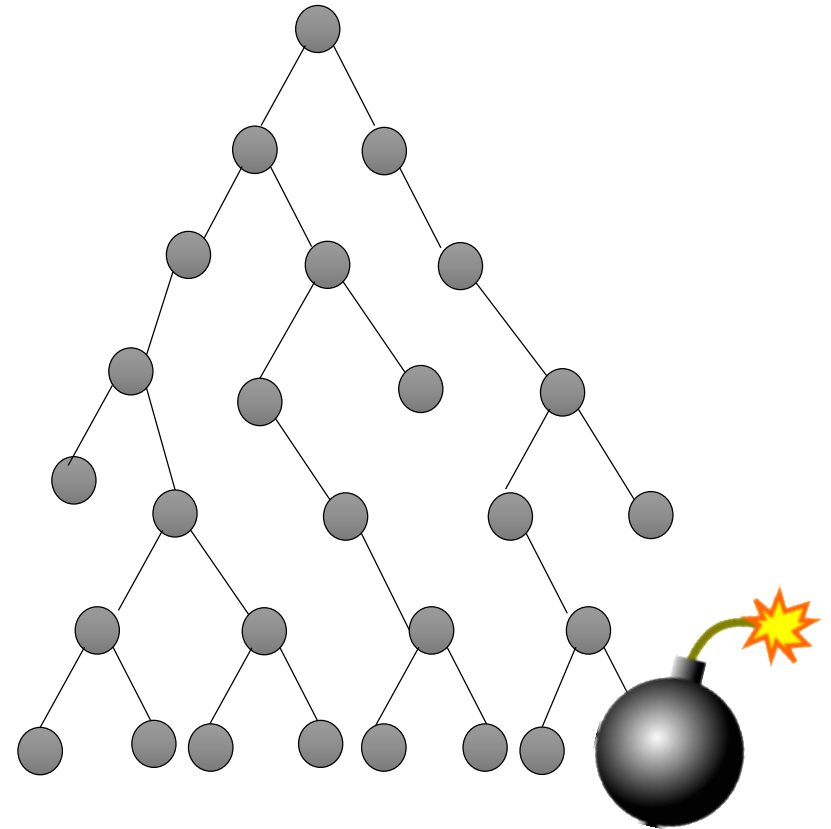
Beware of JS dependencies

- 77% sites use vulnerable JS libs

from State of OpenSource Security by Snyk



Node Security

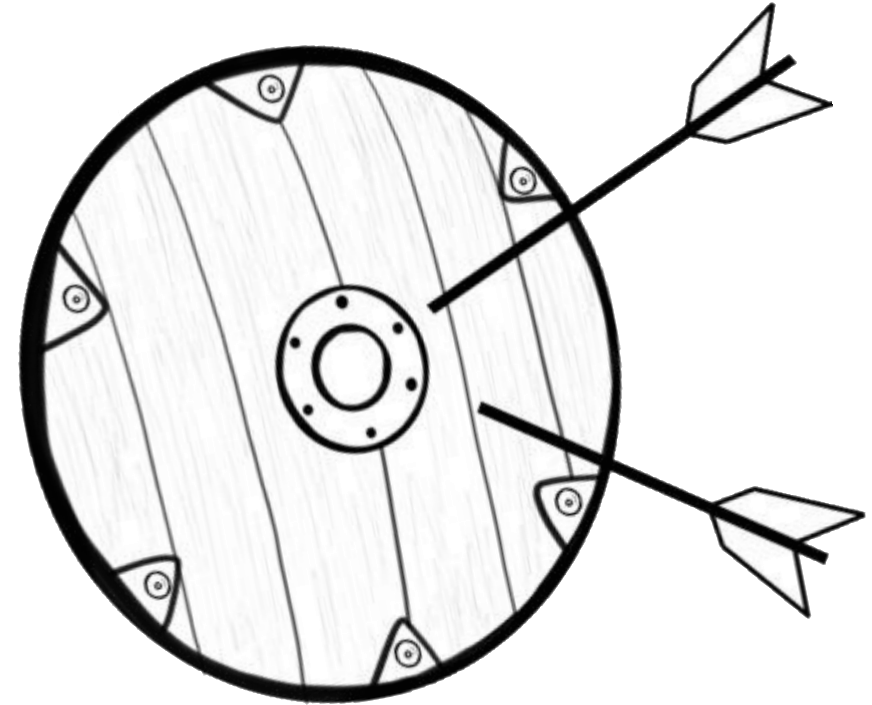


Are you penetrated?

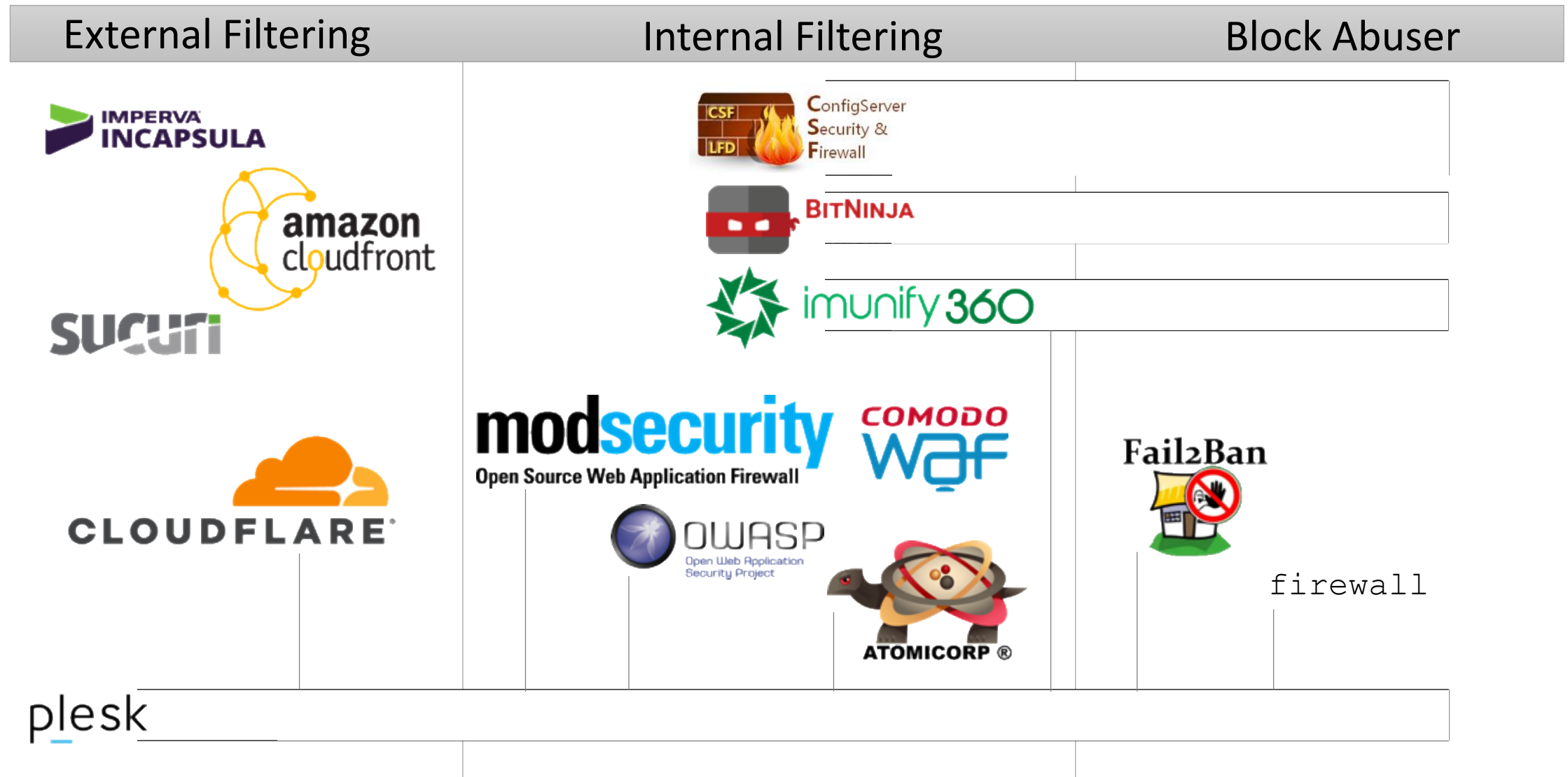
Top Attacks are:

- 19% SQL Injections
- 13% XSS
- 8% DoS

from Web Hacking Incident Database



Protect!



Are you already infected?

Jan'18:

- password logging malware on 2k websites

Feb'18:

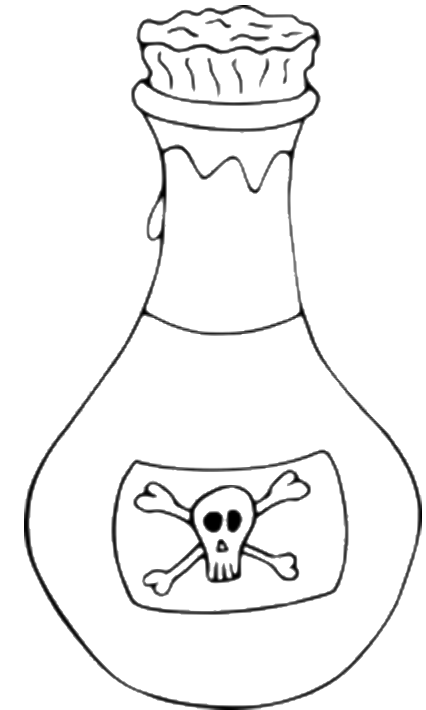
- crypto-mining malware on 4k websites
- ionCube malware at 19k sites in US

reported by WebARX








Overall:

- 20k websites infected every week

from Sucuri's Website Hacked Trend Report



Detect & Cure!

Scan Externally	Scan Internally	Clean or Fix
 OpenVAS		
 Nessus		
 Sucuri		
 SiteLock		
	 Imunify360	
 VirusTotal	 Revisium	
plesk		





Exploited from within?

Multitenant + Local exploit =
Remote Exploit

Multitenant + 1 site exploited =
All sites exploited



Isolate!

Privileges	Resources	Files
<p><i>X mod_php</i></p> <p><i>X mod_perl</i></p> <p><i>X mod_python</i></p> <p>✓ php-fpm</p> <p>✓ fastcgi</p>	<p> CloudLinux</p> <p>✓ cgroups</p> <p></p>	<p> SELinux</p> <p> APPArmor</p> <p>LVE</p> <p>MySQL Governor</p> <p>CageFS</p> <p>✓ chrootsh</p> <p>✓ proper privileges</p> <ul style="list-style-type: none">- WordPress Toolkit- plesk repair fs
<p>plesk</p>		

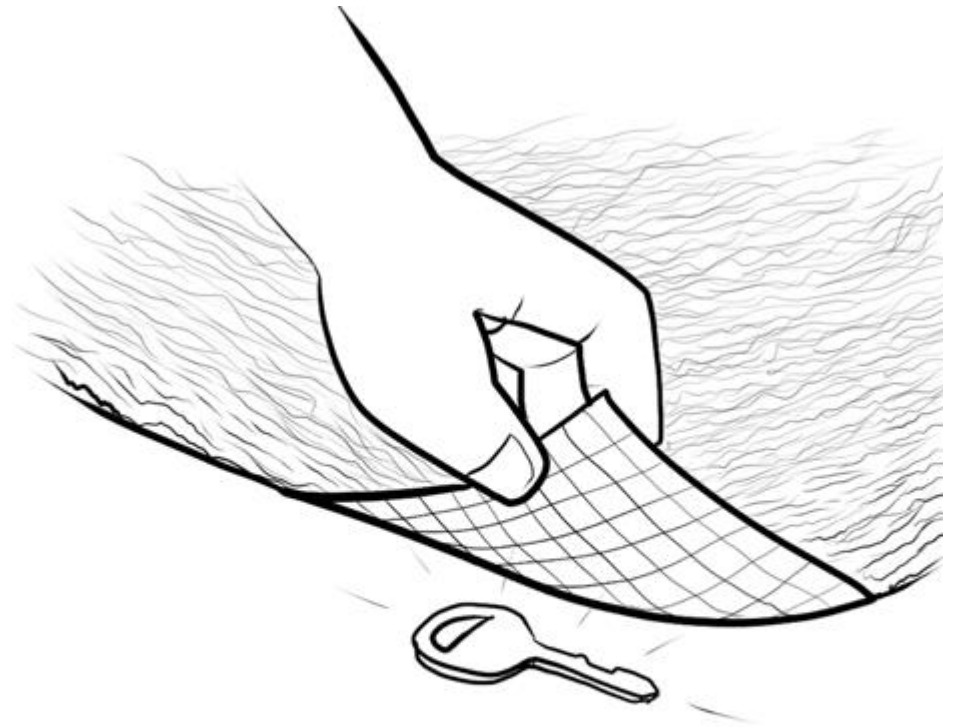
Keys under doormat?

8% breaches via weak password


from wptemplate.com's Safety and Security of WordPress Blog

35 mln brute force attacks each month

from [WordFence.org](https://wordfence.org)'s WordPress Attack Report



Lock!




Network	Authentication	Brute Force Prevention
<ul style="list-style-type: none">✓ IP restrictions✓ VPN	<ul style="list-style-type: none">✓ SSH Key✓ !#Pa\$\$w0rd✓ Two-factor auth✓ Social login <p><i>X shared credentials</i></p>	<p>Fail2Ban</p> 
<p>plesk</p>		

Protect your identity

- 80% devices faced MITM attempts
from Zimperium Global Threat Report
- 76% sites have no valid certificate
from Plesk stats

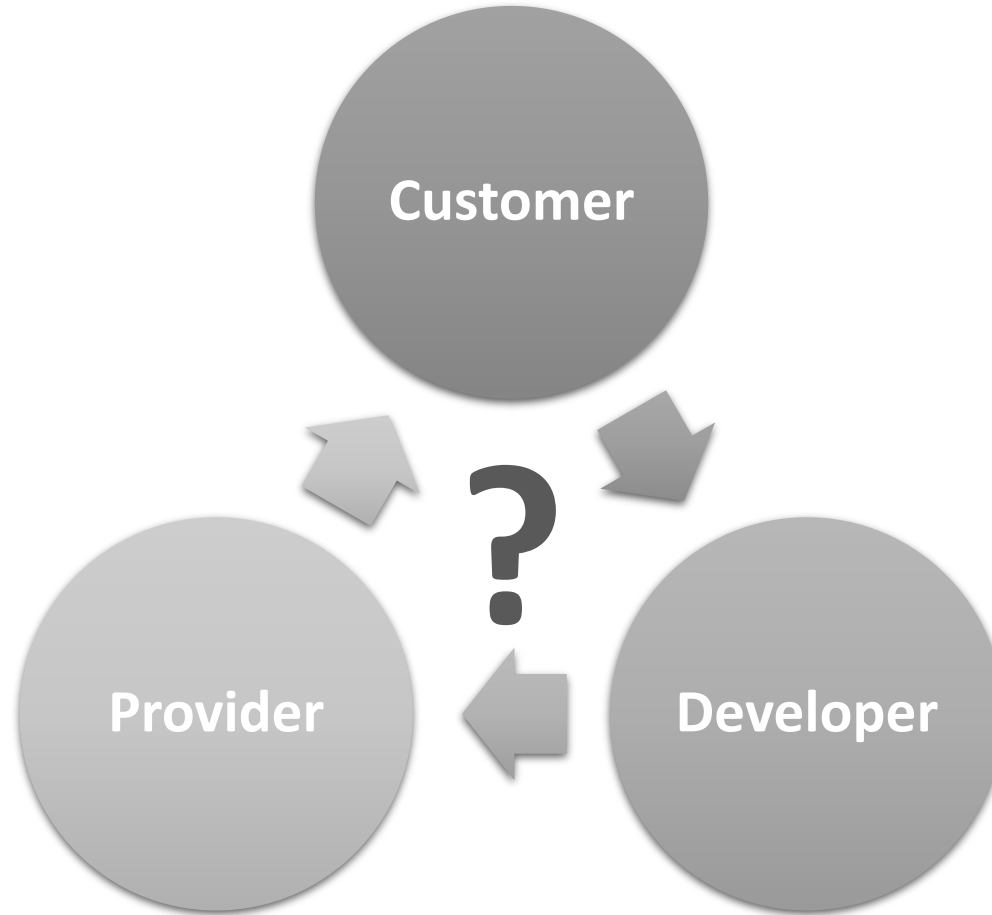


Secure!

Protocol	Certificate	Push
<ul style="list-style-type: none">✓ HTTPS/FTPS✓ up2date ciphers and TLS✓ OCSP Stapling✓ HPKP	<ul style="list-style-type: none">✓ Trusted Cert<ul style="list-style-type: none">X <i>self-signed cert</i>X <i>"multitenant" cert (i.e. in LE)</i>	<ul style="list-style-type: none">✓ HTTP ➤ HTTPS✓ HSTS

✓ SSL Labs A or A+ rank
<https://www.ssllabs.com/ssltest/>

Who takes responsibility?



Who takes responsibility?

The image shows a screenshot of the Plesk web host edition interface. The top navigation bar includes the Plesk logo, the text "web host edition", and user information: "Logged in as Administrator", "Advisor", and "Help". A left sidebar contains a search bar and a menu with categories: "Home", "Hosting Services" (Customers, Resellers, Domains, Subscriptions, Service Plans), "Links to Additional Services" (Google Authenticator), "Server Management" (Tools & Settings, Health Monitoring, Extensions, WordPress, Docker), and "My Profile" (Profile & Preferences, Change Password, Change View).

The main content area is titled "Advisor" and features a "Recommendation" tab. A large grey circle labeled "Customer" is overlaid on the top right of the Advisor section. Below it, a grey circle labeled "Provider" is on the left and a grey circle labeled "Developer" is on the right. A large green checkmark is positioned in the center, with grey arrows pointing from the Provider and Developer circles towards the Customer circle. The Advisor content includes several recommendations:

- Use the KernelCare Extension:** Protect your server against security flaws and vulnerabilities with zero downtime by installing kernel updates on the server without rebooting the server. Status: "is installed".
- Switch to Up-To-Date PHP:** Make your websites more secure by using up-to-date PHP versions. Only current PHP versions contain bugfixes and security vulnerabilities.
- Turn On Automatic Updates:** Keep Plesk stable and secure by turning on the automatic installation of the latest updates containing bugfixes and patches for the latest security vulnerabilities. Status: "Plesk automatic update is turned on".

The interface also shows a "Performance" bar with a green checkmark and a "2070" value, and an "Open" button next to the KernelCare recommendation.

Thank you!



Sergey Lystsev

VP R&D, Plesk

✉ slystsev@plesk.com

📘 [sergey.lystsev](https://www.facebook.com/sergey.lystsev)

plesk

References

- <https://www.symantec.com/content/dam/symantec/docs/infographics/istr-attackers-strike-large-business-en.pdf>
- <https://www.webarxsecurity.com/website-hacking-statistics-2018-february/>
- <https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds>
- <https://sucuri.net/website-security/website-hacked-report>
- http://www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_execsummary_en_xg.pdf
- <https://signup.keepersecurity.com/state-of-smb-cybersecurity-report/>
- <https://arxiv.org/ftp/arxiv/papers/1504/1504.02115.pdf>
- <https://www.mcafee.com/uk/resources/reports/rp-quarterly-threats-dec-2017.pdf>
- <https://www.hackmageddon.com/2018/01/17/2017-cyber-attacks-statistics/>
- <https://edgescan.com/assets/docs/reports/2016-edgescan-stats-report.pdf>