

Infekcje wirusowe w WordPress

Krzysztof Łuczak



Agenda

1. Dlaczego mam uważać ?
2. Jak rozpoznać infekcję ?
3. Jak usunąć infekcję ?
4. Dobre praktyki bezpiecznego WordPressa.

Dlaczego mam uważać ?

- ✓ uszkodzenie plików
- ✓ wyciek danych
- ✓ SEO
- ✓ spam
- ✓ blokada od firmy hostingowej
- ✓ stajemy się częścią botnetu

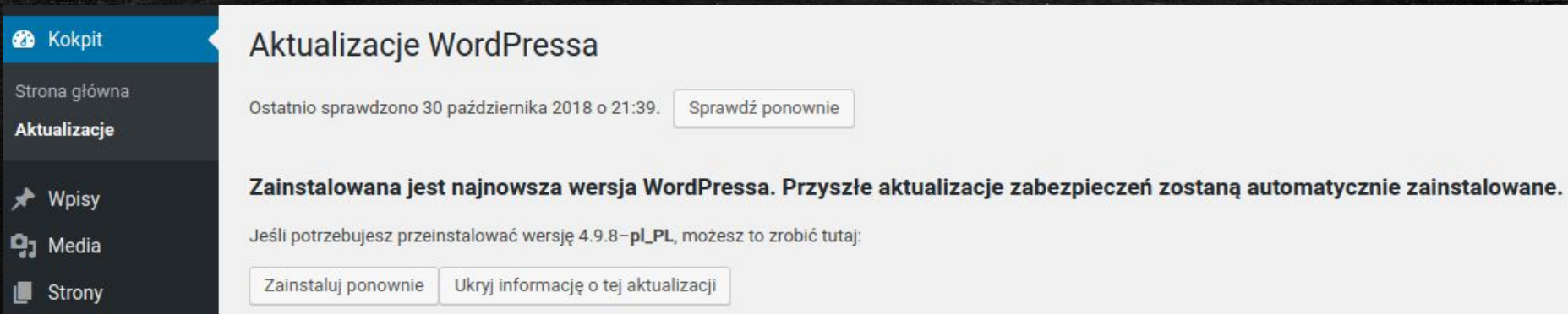
Jak rozpoznać infekcję ?

- ✓ spowolnienie ładowania strony (gtmetrix.com)
- ✓ dostajemy zwrotki mailowe
- ✓ hosting przysyła wiadomość o blokadzie
- ✓ pliki z uprawnieniem do wykonywania w katalogu /tmp
- ✓ połączenia wychodzące do adresów IP z czarnych list
- ✓ skanowanie
 - www.sitecheck.sucuri.net
 - pliki PHP, JS, .htaccess
 - `grep -R "hacked" *`
 - `findbot` (abuseat.org/findbot.pl)



Jak usunąć infekcję ?

- ✓ przywrócenie kopii zapasowej
- ✓ ręczne usuwanie i edycja plików
- ✓ reinstalacja niezmiennych plików WordPressa



The screenshot shows the WordPress dashboard interface. On the left is a dark sidebar with navigation links: 'Kokpit' (Dashboard), 'Strona główna' (Home), 'Aktualizacje' (Updates), 'Wpisy' (Posts), 'Media', and 'Strony' (Pages). The main content area is titled 'Aktualizacje WordPressa' (WordPress Updates). It displays the last check time: 'Ostatnio sprawdzono 30 października 2018 o 21:39.' with a 'Sprawdź ponownie' (Check again) button. Below this, a message states: 'Zainstalowana jest najnowsza wersja WordPressa. Przyszłe aktualizacje zabezpieczeń zostaną automatycznie zainstalowane.' (The latest version of WordPress is installed. Future security updates will be installed automatically.) A note follows: 'Jeśli potrzebujesz przeinstalować wersję 4.9.8–pl_PL, możesz to zrobić tutaj:' (If you need to reinstall version 4.9.8–pl_PL, you can do so here:). At the bottom, there are two buttons: 'Zainstaluj ponownie' (Reinstall) and 'Ukryj informację o tej aktualizacji' (Hide this update information).

Kokpit

Strona główna

Aktualizacje

Wpisy

Media

Strony

Aktualizacje WordPressa

Ostatnio sprawdzono 30 października 2018 o 21:39. [Sprawdź ponownie](#)

Zainstalowana jest najnowsza wersja WordPressa. Przyszłe aktualizacje zabezpieczeń zostaną automatycznie zainstalowane.

Jeśli potrzebujesz przeinstalować wersję 4.9.8–pl_PL, możesz to zrobić tutaj:

[Zainstaluj ponownie](#) [Ukryj informację o tej aktualizacji](#)

Jak usunąć infekcję ? (cd.)

- ✓ w wp-content/uploads/ nie powinno być plików PHP

```
# find wp-content/uploads -type f -name '*.php' -exec rm {} \;
```

- ✓ usunięcie zawartości wp-admin/ oraz wp-includes/ i wgranie czystych plików

```
# wp-cli core download --skip-content --force
```

- ✓ reinstalacja wtyczek

```
# wp-cli plugin install $(wp-cli plugin list --field=name) --force
```

- ✓ reinstalacja motywów

```
# wp-cli wp theme install $(wp-cli theme list --field=name) --force
```

Dobre praktyki bezpiecznego WordPressa

- ✓ regularna aktualizacja
- ✓ cykliczne skanowanie - sitecheck.sucuri.net
- ✓ usunąć nieużywane motywy i wtyczki
- ✓ `.htaccess` (perishablepress.com/6g/)
- ✓ Simply Static, WP Static Site Generator
- ✓ Integrity Checker
- ✓ Blackhole for Bad Bots
- ✓ captcha

Koniec 😊

Dziękuję za uwagę