Infekcje wirusowe w WordPress

Krzysztof Łuczak

LH.pl

Agenda

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

Dlaczego mam uważać ?

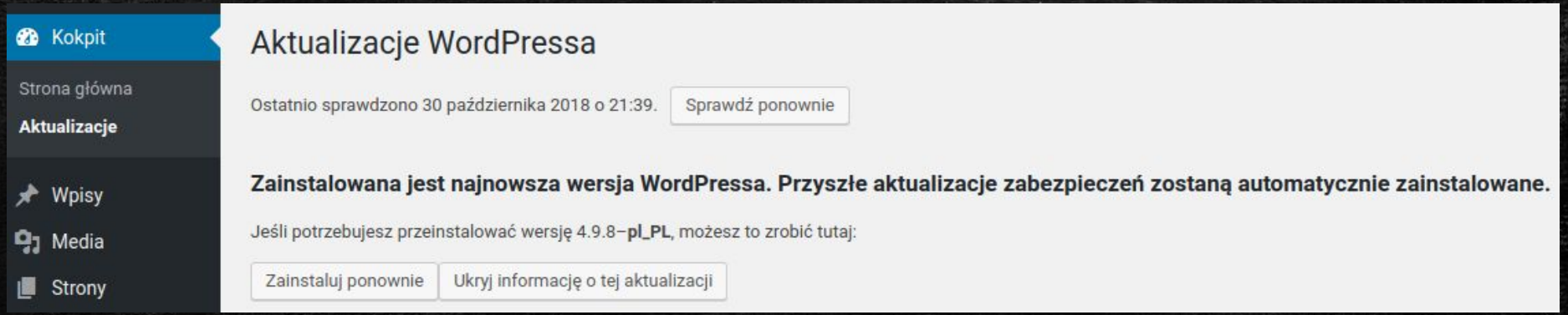
- ✓ uszkodzenie plików
- ✓ wyciek danych
- ✓ SEO
- ✓ spam
- ✓ blokada od firmy hostingowej
- ✓ stajemy się częścią botnetu

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



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