Analýza cíleného útoku, část první

Vložil/a cm3l1k1 [1], 7 Srpen, 2013 - 13:13

- Hacking [2]
- Security [3]
- Top Secret [4]

Jak jistě víte, na náš web byl v noci z 29. na 30. června veden úspěšný cílený útok. Výsledkem útoku byla instalace několika útočných skriptů sloužících k další infiltraci. V tomto dvoudílném článku se dozvíte jak útok probíhal, jakou slabinu vlastně využili, jaké skripty u nás nechali (se zdrojovými kódy), jak se dostali ke kořenovému adresáři webu, proč jsme se stali zajímavým cílem a jak podobným útokům předejít.

To co pravděpodobně nevíte (možná tušíte) je fakt, že SP odolává útokům denně. Denně nás někdo scanuje, někdo zkouší SQLi, XSS, RFI, LFI, RCE, FPD, Directory Traversal a další podobné útoky. A komentářový spam? Denně ho zablokujeme několik stovek. Nyní se však jednalo o cílený útok a to je přeci jen něco ojedinělého. Zřejmě jsme se stali již dostatečně známými, protože útok nebyl veden z České Republiky.

Pokud si dobře pamatuji, za ta léta co SP existuje, se jedná o třetí úspěšný útok. Přesněji řečeno druhý úspěšný útok, umožňující manipulaci se soubory, protože při třetím byly jen změněny autoritativních DNS servery. Vzhledem k tomu, že jsou všechny informace na SP veřejné, neřešíme případný únik dat (až na malé výjimky) příliš paranoidně. Přesto se snažíme analyzovat útok, poučit se z chyb a musím říct, že každý podobný útok nás posouvá o malý krůček kupředu. Nevím, zda je dobrý nápad podělit se zde o tuto informaci, ale máme na webu již tři roky úmyslně nastrčenou skutečně zneužitelnou chybu a čekáme komu se to povede jako prvnímu :]

Slovo úvodem

Redakční systém SP obsahuje hned několik bezpečnostních prvků, z nichž některé fungují naprosto autonomně. Jednoduše řečeno, pokud někdo dělá neplechu, systém sám takového jedince zablokuje, případně i přidá na trvalý blacklist. Útočníci se k nám však nedostali přes hlavní web www.security-portal.cz [5], ale přes jeho subdoménu. Navíc se jednalo o ne úplně běžný způsob útoku a i proto si myslím, že by mohla být tato analýza, na které jsem pracoval jak já, tak RubberDuck, pro čtenáře zajímavá.

Vzhledem ke skutečnosti, že SP je nekomerční portál a náklady na provoz hradí sami administrátoři, tak běží na sdíleném hostingu. Hlavně z tohoto důvodu nemůžeme použít ani zdaleka tolik bezpečnostních prvků, kolik bychom chtěli (jako například mod_security [6]). Jednoduše jsme limitováni možnostmi hostingu. Tento fakt také vedl k úspěšnému napadení.

Z access logů jsme zjistili, že reálný útok začal oťukáváním okolo desáté hodiny večer a byl veden z většího počtu IP adres. Zahrnoval testování všech subdomén, testování existence běžných souborů, zjišťování verzí redakčních systémů a případně i nainstalovaných modulů. Část byla vedena pomocí běžně dostupných, či upravených skriptů. Sběr informací a infiltrace pak téměř výhradně manuálně. Většina útočných skriptů byla enkódována, nebo obfuskována, takže vám je nabídneme již v čitelnější formě.

Prvotní analýza

Záleží na tom co přesně se na vašem webu stalo a podle toho byste měli pokračovat. V našem

případě mě o nedostupnosti webu informoval separátní monitorovací systém, nicméně emaily jsem si přečetl až ráno. Opravdu krásné probuzení. Hlavní web byl nedostupný a fórum SP vracelo chybu se zpracováním scriptu. Co teď? Především zachovat chladnou hlavu. Stalo se... pokud se však necháte strhnout emocemi, můžete to ještě zhoršit. Buď upozorníte útočníky, že o útoku již víte (čímž mohou více infiltrovat váš web) a nebo svým počínáním smažete důkazy o jejich pohybu.

Jako první věc jsem stáhnul logy webového serveru, vylistoval si seznam IP adres a seřadil je podle nejčastějšího výskytu.

```
awk '{ print $2 }' access_log | sort | uniq -c | sort -n
```

Protože bylo ráno, tak jsem předpokládal, že útočníkova IP bude mezi TOP10. Nečekal jsem však, že všech TOP10 budou útočníci (celkem používali asi 30 IP adres, některé dokonce ze sítě Microsoft Network).
Když už znáte alespoň jednu IP adresu, tak je dobré sledovat kam přesně útočník přistupoval a jaký dostal HTTP response (200 OK, 302 Moved, 404 Not Found, ...).

Nejvíce by vás mělo zajímat:

- response kód 200, především pokud ho dostal při přístupu do administrační části webu
- POST, kdy útočník něco odesílal na server (data na web shell, upload souboru, ...)
- jestli nepřistupuje k souboru, který je vám neznámý a může se tak jednat o nově nahraný script
- jestli se o podobný přístup nepokouší více IP adres
- najít specifický podpis útočníka, například verzi prohlížeče a OS

Pokud najdete důkaz o podezřelých aktivitách, tak jste již příliš daleko a musíte zpět. Musíte zjistit kdy poprvé provedl něco, na co by neměl mít oprávnění.

Když už něco podezřelého naleznete, tak projděte logy znovu a všechny nalezené IP adresy si zapisujte. Až budete mít pocit, že většinu máte, tak si vyfiltrujte logy na základě těchto IP adres a rovnou odstraňte z logů soubory, které s útokem nemají nic společného (obrázky, css, javascript, ...). Bude se vám to mnohem lépe číst.

```
grep -f soubor_s_IP_adresama.txt access_log | grep -vE "gif HTTP|png HTTP|js HTTP|css HTTP|jpg HTTP|ico HTTP|js?n HTTP|css?n HTTP" > filter.log
```

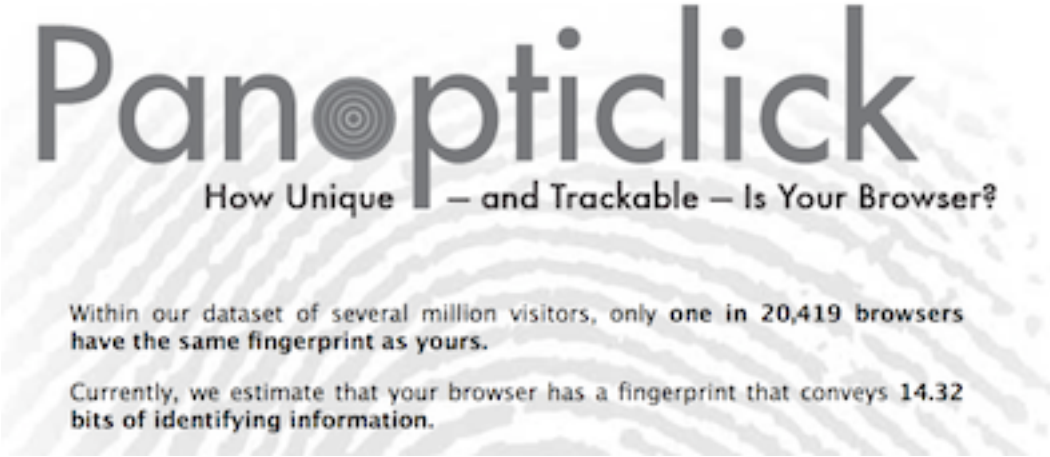
Rozeberme si jeden ukázkový záznam Apache logu, pro jeho lepší pochopení:

```
convertor.security-portal.cz 109.186.96.51 - - [29/Jun/2013:22:41:28 +0200] "GET / HTTP/1.1" 200 1137 "http://www.bing.com/search?q=convertor+security" "Mozilla/5.0 (Windows NT 6.1; rv:2.0.1) Gecko/20100101 Firefox/4.0.1"
```

1. convertor.security-portal.cz - host na který byl dotaz směřován
2. 109.186.96.51 - IP adresa klienta/útočníka
3. [29/Jun/2013:22:41:28 +0200] - datum a čas požadavku
4. "GET /index.html HTTP/1.1" - požadavek na stažení/zobrazení (GET) souboru index.html umístěného v kořenovém adresáři hosta convertor...
5. 200 - HTTP kód 200 znamená vše v pořádku
6. 1137 - počet zaslaných bajtů klientovi
7. "http://www.bing.com/search?q=convertor+security" - referer, stránka ze která na náš web přistoupil (kliknul na odkaz)
8. "Mozilla/5.0 (Windows NT 6.1; rv:2.0.1)..." - webový prohlížeč klienta, OS, případně i moduly

Specifický podpis útočníka může být také nápomocný. Např. jeden z útočníků přistupoval (podle hlaviček) z prohlížeče Chrome 0.2 (Chrome/0.2.149.27), což opravdu není nic obvyklého, takže si

vylistujete IP se stejným podpisem a přidáte je do seznamu “podezřelých”.
Podpis prohlížeče je přitom poměrně slušným identifikačním znakem. Zde si můžete ověřit jak moc všední je ten váš: https://panopticlick.eff.org [7]



Teď nastává ta titěrnější část analýzy, kdy musíte jít téměř řádek po řádku a hledat něco neobvyklého. Zapisujte si podrobnosti, podivnosti a časy kdy se co stalo do textového editoru. Opakující se záznamy odstraňte pomocí grepu, ale snažte se o co nejpřesnější filtr, abyste si nesmazali něco důležitého.

Bylo téměř odpoledne, když jsem si všimnul, že fórum již funguje. Očividně to bylo způsobeno chybou útočníků a tu již sami opravili. Musím postupovat opatrně. Teď právě jsou na webu a nesmím si je vyplašit :)

Komunikace s hostingem

V tento moment teprve oceníte kvalitu supportu vašeho hostingu. Průběžná komunikace s administrátorem je důležitá, ideálně přes komunikátor, protože admin hostingu může ověřit a zjistit mnohem více údajů než vy. Může i zjistit jestli daný útok není veden na více webů, případně pak navrhnout řešení jak podobným útokům předejít.

Hned jak jsem znal IP adresy a přibližný čas útoku, kontaktoval jsem helpdesk hostingu, aby mi zjistili z jakého dne jsou poslední zálohy naší domény. Výslovně jsem uvedl, aby je zatím jen připravili pro přehrání, ale nic nepřepisovali. Soubory totiž nestačí jen přepsat, zůstaly by tam backdoory. Musíte je všechny smazat a nahrát kompletní zálohu. Ale na to je teď ještě brzy...

Jako další věc je poprosté (budou to mít mnohem rychleji než vy), aby vám vypsali všechny soubory, které byli modifikované ode dne útoku po aktuální čas a rovnou vám udělali zálohu těchto souborů. Na ty se pak musíte více zaměřit.

Zajímavosti z logů

Je toho mnohem víc, ale ukáži vám jen to zajímavější, protože kompletní log má desítky tisíc řádků. Jak tedy postupovali?

testování verze modulů WordPressu na subdoméně

```
bflow.security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:20 +0200] "GET
/wp-content/plugins/twitter-facebook-google-plusone-share/tfg_style.css?ver=3.5.2
HTTP/1.1" 200 183 "http://bflow.security-portal.cz/" "Mozilla/5.0 (Windows NT 6.1;
WOW64; rv:21.0) Gecko/20100101 Firefox/21.0"
bflow.security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:20 +0200] "GET
/wp-content/plugins/wp-syntax/css/wp-syntax.css?ver=1.0 HTTP/1.1" 200 815
```

```
"http://bflow.security-portal.cz/" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:21.0)
Gecko/20100101 Firefox/21.0"
bflow.security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:20 +0200] "GET
/wp-content/plugins/wp-stats/stats-css.css?ver=2.50 HTTP/1.1" 200 436
"http://bflow.security-portal.cz/" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:21.0)
Gecko/20100101 Firefox/21.0"
bflow.security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:42 +0200] "GET
/wp-includes/js/jquery/jquery.js?ver=1.8.3 HTTP/1.1" 200 33444
"http://bflow.security-portal.cz/" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:21.0)
Gecko/20100101 Firefox/21.0"
bflow.security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:42 +0200] "GET
/wp-content/plugins/mlanguage/mlanguage.js?ver=3.5.2 HTTP/1.1" 200 1077
"http://bflow.security-portal.cz/" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:21.0)
Gecko/20100101 Firefox/21.0"
bflow.security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:20:09 +0200] "GET
/wp-admin/css/wp-admin.min.css?ver=3.5.2 HTTP/1.1" 200 23842 "http://bflow.security-p
ortal.cz/wp-login.php?redirect_to=http%3A%2F%2Fbflow.security-portal.cz%2Fwp-admin%2F
&reauth=1" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:21.0) Gecko/20100101 Firefox/21.0"
```

testování existence souborů

```
security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:02 +0200] "GET /UserFiles
HTTP/1.1" 404 59060 "-" "-"
security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:03 +0200] "GET /userFiles
HTTP/1.1" 404 59060 "-" "-"
security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:04 +0200] "GET /UserFile
HTTP/1.1" 404 58933 "-" "-"
security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:05 +0200] "GET /userfile
HTTP/1.1" 404 58933 "-" "-"
security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:06 +0200] "GET /CV HTTP/1.1"
404 59105 "-" "-"
security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:08 +0200] "GET /cv HTTP/1.1"
404 59105 "-" "-"
security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:10 +0200] "GET /upload
HTTP/1.1" 404 63017 "-" "-"
security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:12 +0200] "GET /uploads
HTTP/1.1" 404 58853 "-" "-"
security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:13 +0200] "GET /jobs HTTP/1.1"
404 60036 "-" "-"
security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:15 +0200] "GET /jobs/cv
HTTP/1.1" 404 58916 "-" "-"
security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:16 +0200] "GET /jobs/cv/up.php
HTTP/1.1" 404 59165 "-" "-"
security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:18 +0200] "GET /jobs/cv/upload
HTTP/1.1" 404 58956 "-" "-"
security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:24 +0200] "GET
//jops/cv/attachments HTTP/1.1" 404 59099 "-" "-"
security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:25 +0200] "GET /www.zip
HTTP/1.1" 404 60955 "-" "-"
security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:27 +0200] "GET /public_html.zip
HTTP/1.1" 404 59264 "-" "-"
security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:29 +0200] "GET /www(1).zip
HTTP/1.1" 404 60175 "-" "-"
security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:31 +0200] "GET /www_1.zip
HTTP/1.1" 404 60288 "-" "-"
security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:33 +0200] "GET
/public_html(1).zip HTTP/1.1" 404 58996 "-" "-"
```

```
security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:34 +0200] "GET /www.zip
HTTP/1.1" 404 60955 "-" "-"
security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:34 +0200] "GET /public_html.zip
HTTP/1.1" 404 59264 "-" "-"
security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:35 +0200] "GET /www(1).zip
HTTP/1.1" 404 60175 "-" "-"
security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:35 +0200] "GET
/public_html(1).zip HTTP/1.1" 404 58996 "-" "-"
security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:36 +0200] "GET /up.zip
HTTP/1.1" 404 58862 "-" "-"
security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:38 +0200] "GET /upload.zip
HTTP/1.1" 302 - "-" "-"
security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:19:58 +0200] "GET /forum.zip
HTTP/1.1" 404 59137 "-" "-"
security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:20:00 +0200] "GET /forum(1).zip
HTTP/1.1" 404 58866 "-" "-"
security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:20:02 +0200] "GET /forum_1.zip
HTTP/1.1" 404 59045 "-" "-"
security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:20:03 +0200] "GET /iran.zip
HTTP/1.1" 404 59043 "-" "-"
```

testování známých chyb

```
# Full path disclosure =
www.securitate.md/blog/drupal-7-x-search-module-full-path-disclosure/201... [8]
security-portal.cz 41.100.181.234 - - [29/Jun/2013:23:26:09 +0200] "GET
/search?keys[0]=securitate.md HTTP/1.1" 200 13470 "-" "Mozilla/5.0 (Windows NT 6.1;
rv:18.0) Gecko/20100101 Firefox/18.0"
# phpinfo
bflow.security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:22:42 +0200] "GET
//wp-content/plugins/wp-syntax/test/inde
x.php
?test_filter[wp_head][99][0]=pi&test_filter[wp_head][99][1]=cos&test_filter[wp_head][
99][2]=phpinfo HTTP/1.1" 301 20 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:21.0)
Gecko/20100101 Firefox/21.0"
bflow.security-portal.cz 2.91.36.135 - - [29/Jun/2013:22:24:14 +0200] "GET
/wp-includes/js/jquery/jquery.js?ver=1.8.3 HTTP/1.1" 200 33444
"http://bflow.secu
rity-portal.cz/wp-content/plugins/wp
-syntax/test/
?test_filterwp_head990=session_start&test_filterwp_head991=session_id&test_filterwp_h
ead992=system" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:21.0) Gecko/20100101
Firefox/21.0"
```

sběr subdomén pomocí vyhledávání na bing.com

```
ebook.security-portal.cz 109.186.96.51 - - [29/Jun/2013:22:41:28 +0200] "GET /
HTTP/1.1" 200 1137
"http://www.bing.com/search?q=ip%3A195.210.29.4+security
&qs=n&form=QBRE&pq=ip%3A195.210.29.4+security&sc=8-23&sp=-1&sk=" "Mozilla/5.0
(Windows NT 6.1; rv:2.0.1) Gecko/20100101 Firefox/4.0.1"
webirc.security-portal.cz 109.186.96.51 - - [29/Jun/2013:22:41:41 +0200] "GET /
HTTP/1.1" 200 1181 "http://www.bing.com/search?q=ip%3A195.210.29.4+security&qs=n&form
=QBRE&pq=ip%3A195.210.29.4+security&sc=8-23&sp=-1&sk=" "Mozilla/5.0 (Windows NT 6.1;
rv:2.0.1) Gecko/20100101 Firefox/4.0.1"
paste.security-portal.cz 109.186.96.51 - - [29/Jun/2013:22:41:44 +0200] "GET /
```

```
HTTP/1.1" 200 4601 "http://www.bing.com/search?q=ip%3A195.210.29.4+security&qs=n&form
=QBRE&pq=ip%3A195.210.29.4+security&sc=8-23&sp=-1&sk=" "Mozilla/5.0 (Windows NT 6.1;
rv:2.0.1) Gecko/20100101 Firefox/4.0.1"
convertor.security-portal.cz 109.186.96.51 - - [29/Jun/2013:22:41:49 +0200] "GET /
HTTP/1.1" 200 1184 "http://www.bing.com/search?q=ip%3A195.210.29.4+security&qs=n&form
=QBRE&pq=ip%3A195.210.29.4+security&sc=8-23&sp=-1&sk=" "Mozilla/5.0 (Windows NT 6.1;
rv:2.0.1) Gecko/20100101 Firefox/4.0.1"
cm3l1k1.security-portal.cz 109.186.96.51 - - [29/Jun/2013:22:41:52 +0200] "GET /
HTTP/1.1" 200 1672 "http://www.bing.com/search?q=ip%3A195.210.29.4+security&qs=n&form
=QBRE&pq=ip%3A195.210.29.4+security&sc=8-23&sp=-1&sk=" "Mozilla/5.0 (Windows NT 6.1;
rv:2.0.1) Gecko/20100101 Firefox/4.0.1"
network-tools.security-portal.cz 109.186.96.51 - - [29/Jun/2013:22:41:58 +0200] "GET
/ HTTP/1.1" 200 1424 "http://www.bing.com/search?q=ip%3A195.210.29.4+security&qs=n&fo
rm=QBRE&pq=ip%3A195.210.29.4+security&sc=8-23&sp=-1&sk=" "Mozilla/5.0 (Windows NT
6.1; rv:2.0.1) Gecko/20100101 Firefox/4.0.1"
flack.security-portal.cz 109.186.96.51 - - [29/Jun/2013:22:44:58 +0200] "GET /
HTTP/1.1" 200 746 "http://www.bing.com/search?q=ip%3a195.210.29.4+security&qs=n&pq=ip
%3a195.210.29.4+security&sc=8-23&sp=-1&sk=&first=11&FORM=PERE" "Mozilla/5.0 (Windows
NT 6.1; rv:2.0.1) Gecko/20100101 Firefox/4.0.1"
owasp.security-portal.cz 109.186.96.51 - - [29/Jun/2013:23:06:39 +0200] "GET /
HTTP/1.1" 200 3528 "http://www.bing.com/search?q=ip%3a195.210.29.4+security&qs=n&pq=i
p%3a195.210.29.4+security&sc=8-23&sp=-1&sk=&first=21&FORM=PERE1" "Mozilla/5.0
(Windows NT 6.1; rv:2.0.1) Gecko/20100101 Firefox/4.0.1"
tor.security-portal.cz 109.186.96.51 - - [29/Jun/2013:23:06:42 +0200] "GET /
HTTP/1.1" 200 2420 "http://www.bing.com/search?q=ip%3a195.210.29.4+security&qs=n&pq=i
p%3a195.210.29.4+security&sc=8-23&sp=-1&sk=&first=21&FORM=PERE1" "Mozilla/5.0
(Windows NT 6.1; rv:2.0.1) Gecko/20100101 Firefox/4.0.1"
convertor.security-portal.cz 41.102.154.48 - - [29/Jun/2013:23:18:45 +0200] "GET /
HTTP/1.1" 200 1184 "http://www.bing.com/search?q=ip%3A195.210.29.4+security-portal.cz
&go=&qs=n&form=QBRE&filt=all&pq=ip%3A195.210.29.4+security-portal.cz&sc=0-0&sp=-1&sk=
" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/27.0.1453.116 Safari/537.36"
```

hraní na našem sql injection playgroundu

```
flack.security-portal.cz 109.186.96.51 - - [29/Jun/2013:22:48:04 +0200] "POST
/login/level5/ HTTP/1.1" 200 449 "-" "Mozilla/5.0 (Windows NT 6.1; rv:2.0.1)
Gecko/20100101 Firefox/4.0.1"
flack.security-portal.cz 109.186.96.51 - - [29/Jun/2013:22:50:12 +0200] "GET /
HTTP/1.1" 200 746 "-" "Mozilla/5.0 (Windows NT 6.1; rv:2.0.1) Gecko/20100101
Firefox/4.0.1"
flack.security-portal.cz 109.186.96.51 - - [29/Jun/2013:22:50:18 +0200] "GET
/analyze/level1/ HTTP/1.1" 403 225 "http://flack.security-portal.cz/" "Mozilla/5.0
(Windows NT 6.1; rv:2.0.1) Gecko/20100101 Firefox/4.0.1"
flack.security-portal.cz 109.186.96.51 - - [29/Jun/2013:22:50:29 +0200] "GET
/analyze/level1/ HTTP/1.1" 403 225 "http://flack.security-portal.cz/" "Mozilla/5.0
(Windows NT 6.1; rv:2.0.1) Gecko/20100101 Firefox/4.0.1"
flack.security-portal.cz 109.186.96.51 - - [29/Jun/2013:22:50:33 +0200] "GET
/login/level1/ HTTP/1.1" 200 361 "http://flack.security-portal.cz/" "Mozilla/5.0
(Windows NT 6.1; rv:2.0.1) Gecko/20100101 Firefox/4.0.1"
...stovky zaznamu...
flack.security-portal.cz 109.186.96.51 - - [29/Jun/2013:23:17:17 +0200] "POST
/login/level5/ HTTP/1.1" 200 456 "-" "sqlmap/1.0-dev (http://sqlmap.org [9])"
flack.security-portal.cz 109.186.96.51 - - [29/Jun/2013:23:17:18 +0200] "POST
/login/level5/ HTTP/1.1" 200 456 "-" "sqlmap/1.0-dev (http://sqlmap.org [9])"
flack.security-portal.cz 109.186.96.51 - - [29/Jun/2013:23:17:18 +0200] "POST
/login/level5/ HTTP/1.1" 200 456 "-" "sqlmap/1.0-dev (http://sqlmap.org [9])"
```

```
...tisice zaznamu...
```

takto jsme se dozvěděli (mimo jiné) odkud pánové jsou - zdravíme Alžírsko

```
flack.security-portal.cz 41.100.181.234 - - [29/Jun/2013:23:22:12 +0200] "GET /
HTTP/1.1" 200 746
"http://www.google.dz
/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&ved=0CCwQFjAA&url=http%3A%2F%2Fflac
k.security-portal.cz%2F&ei=_k_PUaeDLOTj4QS334HoCw&usg=AFQjCNEQPOZgkzKtfHNY26ITv4TZ7gs
fkQ&sig2=cgpCXtAYpH2_whdOW5IgRQ&bvm=bv.48572450,d.bGE" "Mozilla/5.0 (Windows NT 6.1;
rv:18.0) Gecko/20100101 Firefox/18.0"
paste.security-portal.cz 41.100.181.234 - - [29/Jun/2013:23:22:24 +0200] "GET /
HTTP/1.1" 200 4601 "http://www.google.dz/url?sa=t&rct=j&q=&esrc=s&source=web&cd=12&ca
d=rja&ved=0CDAQFjABOAo&url=http%3A%2F%2Fpaste.security-portal.cz%2F&ei=C1DPUdLVDIGO4A
SBmoC4Cg&usg=AFQjCNF8J3jyNzFOsC0aUBXCUOF9paltwQ&sig2=lHvHkgrDXl9cW7akmTGvYQ&bvm=bv.48
572450,d.bGE" "Mozilla/5.0 (Windows NT 6.1; rv:18.0) Gecko/20100101 Firefox/18.0"
cm3l1k1.security-portal.cz 41.100.181.234 - - [29/Jun/2013:23:22:31 +0200] "GET /
HTTP/1.1" 200 1672 "http://www.google.dz/url?sa=t&rct=j&q=&esrc=s&source=web&cd=20&ca
d=rja&ved=0CHgQFjAJOAo&url=http%3A%2F%2Fcm3l1k1.security-portal.cz%2F&ei=C1DPUdLVDIGO
4ASBmoC4Cg&usg=AFQjCNGKg2fXK0v4rhjao3TBQoXgy-etyw&sig2=6Xe6GlIsV-_upZpm2eauaA&bvm=bv.
48572450,d.bGE" "Mozilla/5.0 (Windows NT 6.1; rv:18.0) Gecko/20100101 Firefox/18.0"
```

Několik minut před půl dvanáctou se v logu objevil velký počet přístupů na přihlašovací stránku jedné ze subdomén. Jednalo se o téměř 3500 přístupů s frekvencí 10 přístupů za sekundu. Nakonec se útočník úspěšně přihlásil:

```
bflow.security-portal.cz 41.100.181.234 - - [29/Jun/2013:23:33:09 +0200] "POST
/wp-login.php HTTP/1.1" 200 1712 "-" "-"
bflow.security-portal.cz 41.100.181.234 - - [29/Jun/2013:23:33:09 +0200] "POST
/wp-login.php HTTP/1.1" 200 1712 "-" "-"
bflow.security-portal.cz 41.100.181.234 - - [29/Jun/2013:23:33:09 +0200] "POST
/wp-login.php HTTP/1.1" 200 1712 "-" "-"
bflow.security-portal.cz 41.100.181.234 - - [29/Jun/2013:23:33:09 +0200] "POST
/wp-login.php HTTP/1.1" 200 1712 "-" "-"
bflow.security-portal.cz 41.100.181.234 - - [29/Jun/2013:23:33:09 +0200] "POST
/wp-login.php HTTP/1.1" 200 1712 "-" "-"
bflow.security-portal.cz 41.100.181.234 - - [29/Jun/2013:23:34:03 +0200] "GET
/wp-admin/ HTTP/1.1" 302 20 "-" "Mozilla/5.0 (Windows NT 6.1; rv:18.0) Gecko/20100101
Firefox/18.0"
bflow.security-portal.cz 41.100.181.234 - - [29/Jun/2013:23:34:03 +0200] "GET /wp-log
in.php?redirect_to=http%3A%2F%2Fbflow.security-portal.cz%2Fwp-admin%2F&reauth=1
HTTP/1.1" 200 1183 "-" "Mozilla/5.0 (Windows NT 6.1; rv:18.0) Gecko/20100101
Firefox/18.0"
bflow.security-portal.cz 41.100.181.234 - - [29/Jun/2013:23:34:04 +0200] "GET
/wp-admin/css/wp-admin.min.css?ver=3.5.2 HTTP/1.1" 200 23842 "http://bflow.security-p
ortal.cz/wp-login.php?redirect_to=http%3A%2F%2Fbflow.security-portal.cz%2Fwp-admin%2F
&reauth=1" "Mozilla/5.0 (Windows NT 6.1; rv:18.0) Gecko/20100101 Firefox/18.0"
bflow.security-portal.cz 41.100.181.234 - - [29/Jun/2013:23:34:04 +0200] "GET
/wp-content/plugins/mlanguage/mlanguage.js?ver=3.5.2 HTTP/1.1" 200 1077 "http://bflow
.security-portal.cz/wp-login.php?redirect_to=http%3A%2F%2Fbflow.security-portal.cz%2F
wp-admin%2F&reauth=1" "Mozilla/5.0 (Windows NT 6.1; rv:18.0) Gecko/20100101
Firefox/18.0"
bflow.security-portal.cz 41.100.181.234 - - [29/Jun/2013:23:34:04 +0200] "GET
/wp-content/plugins/twitter-facebook-google-plusone-share/tfg_style.css?ver=3.5.2
HTTP/1.1" 200 183 "http://bflow.security-portal.cz/wp-login.php?redirect_to=http%3A%2
F%2Fbflow.security-portal.cz%2Fwp-admin%2F&reauth=1" "Mozilla/5.0 (Windows NT 6.1;
```

```
rv:18.0) Gecko/20100101 Firefox/18.0"
bflow.security-portal.cz 41.100.181.234 - - [29/Jun/2013:23:34:05 +0200] "GET
/wp-admin/images/wordpress-logo.png?ver=20120216 HTTP/1.1" 200 2480
"http://bflow.security-portal.cz/wp-admin/css/wp-admin.min.css?ver=3.5.2"
"Mozilla/5.0 (Windows NT 6.1; rv:18.0) Gecko/20100101 Firefox/18.0"
bflow.security-portal.cz 41.100.181.234 - - [29/Jun/2013:23:34:08 +0200] "POST
/wp-login.php HTTP/1.1" 302 20 "http://bflow.security-portal.cz/wp-login.php?redirect
_to=http%3A%2F%2Fbflow.security-portal.cz%2Fwp-admin%2F&reauth=1" "Mozilla/5.0
(Windows NT 6.1; rv:18.0) Gecko/20100101 Firefox/18.0"
# welcome
bflow.security-portal.cz 41.100.181.234 - - [29/Jun/2013:23:34:09 +0200] "GET
/wp-admin/ HTTP/1.1" 200 18274 "http://bflow.security-portal.cz/wp-login.php?redirect
_to=http%3A%2F%2Fbflow.security-portal.cz%2Fwp-admin%2F&reauth=1" "Mozilla/5.0
(Windows NT 6.1; rv:18.0) Gecko/20100101 Firefox/18.0"
```

Ne, nešlo o slabé heslo. Mělo 16 znaků...

Poté uploadoval své moduly/scripty a modifikoval kód některých základních pluginů WordPressu, aby si zajistil zadní vrátka v případě smazání ostatních scriptů (to není špatný nápad):

```
# Module upload
bflow.security-portal.cz 41.100.181.234 - - [29/Jun/2013:23:34:47 +0200] "POST
/wp-admin/update.php?action=upload-plugin HTTP/1.1" 200 4658
"http://bflow.security-portal.cz/wp-admin/plugin-install.php?tab=upload" "Mozilla/5.0
(Windows NT 6.1; rv:18.0) Gecko/20100101 Firefox/18.0"
# Plugin editor
bflow.security-portal.cz 41.100.181.234 - - [29/Jun/2013:23:35:12 +0200] "GET
/wp-admin/plugin-editor.php HTTP/1.1" 200 14477
"http://bflow.security-portal.cz/wp-admin/post.php?post=419&action=edit" "Mozilla/5.0
(Windows NT 6.1; rv:18.0) Gecko/20100101 Firefox/18.0"
# Akismet edit
bflow.security-portal.cz 41.100.181.234 - - [29/Jun/2013:23:35:52 +0200] "GET
/wp-admin/plugin-editor.php?file=akismet/akismet.php&a=te&scrollto=0 HTTP/1.1" 200
14981 "http://bflow.security-portal.cz/wp-admin/plugin-editor.php" "Mozilla/5.0
(Windows NT 6.1; rv:18.0) Gecko/20100101 Firefox/18.0"
```

Mimo jiné útočník nahrál i starou verzi WP modulu pro vedení statistik přístupů, která však obsahuje známou chybu. Další pokus o skrytí jednoho z backdoorů.

Zde již máme první GET na útočný script nahraný útočníkem:

```
bflow.security-portal.cz 41.100.181.234 - - [29/Jun/2013:23:36:40 +0200] "POST
/wp-admin/up.php HTTP/1.1" 200 251 "http://bflow.security-portal.cz/wp-admin/up.php"
"Mozilla/5.0 (Windows NT 6.1; rv:18.0) Gecko/20100101 Firefox/18.0"
```

Zdrojové kódy skriptů

Právě teď přijde vhod seznam modifikovaných souborů od vašeho hostingu. Některé z nich mohou být cache soubory, ale ty byste měli být schopni jednoduše rozlišit. Zbytek podrobte důkladné analýze. Pochopte co dělají a jak dál mohly infiltrovat váš systém.

Většina dnešních skriptů je obfuskovaná, takže vám přijde vhod služba jako PHP Decoder [10], která vám změť nesmyslných znaků převede za vás (příklad [11]).

Script up.php naleznete zde: http://paste.security-portal.cz/view/2c41210c [12]

Jedná se o klasický upload script. Všimněte si na začátku souboru řetězce “GIF89a1”. Obcházení špatného ověřování GIF souboru z hlavičky.

Pomocí up.php nahrál soubor perl.php, který po spuštění vytvořil soubor perl.dam

Script perl.php: http://paste.security-portal.cz/view/ef8c63c9 [13]

```
bflow.security-portal.cz 41.100.181.234 - - [29/Jun/2013:23:36:44 +0200] "GET
/wp-admin/perl.php HTTP/1.1" 200 689 "-" "Mozilla/5.0 (Windows NT 6.1; rv:18.0)
Gecko/20100101 Firefox/18.0"
```

Script vytvoří htaccess soubor, který souborům *.dam přiřadí CGI handler, povolí spuštění CGI skriptů a zapíše soubor perl.dam do stejné cesty.

Tímto obešli nastavení open_basedir které zneumožňuje PHP scriptům na subdoménách vyskočit až na úroveň root adresáře SP.

CGI scripty obecně běží pod jinými právy než běžné PHP scripty. Zpravidla s vyšším oprávněním. Spuštění CGI jsme na doméně z historických důvodů/skriptů nevypnuli globálně pomocí -ExecCGI na VirtualHostu a to byla jedna z našich hlavních chyb.

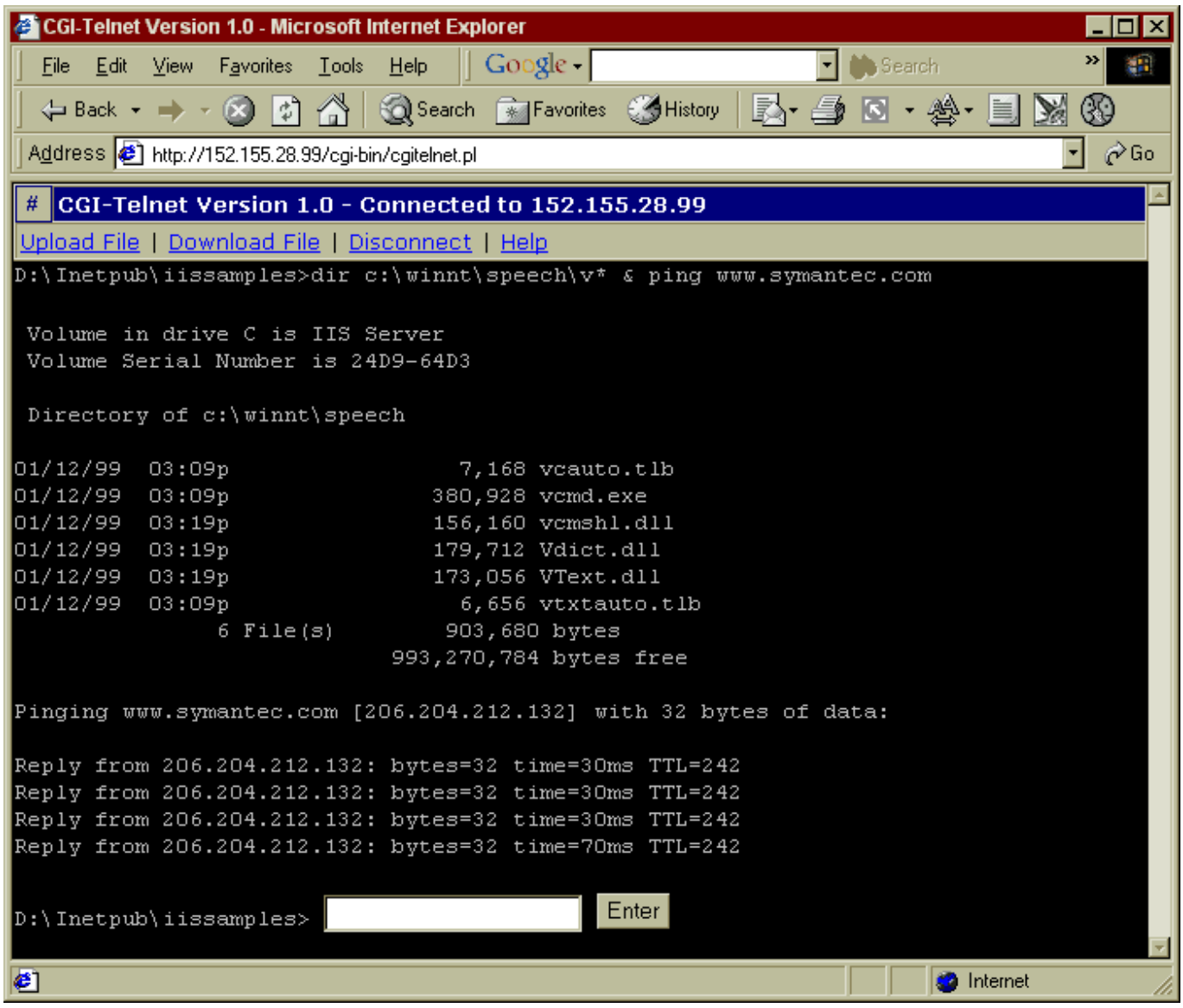
```
Options FollowSymLinks MultiViews Indexes ExecCGI
AddType application/x-httpd-cgi .dam
AddHandler cgi-script .dam
AddHandler cgi-script .dam
```

Script perl.dam: http://paste.security-portal.cz/view/b99d28b5 [14]

```
bflow.security-portal.cz 41.100.181.234 - - [29/Jun/2013:23:36:44 +0200] "GET
/wp-admin/perl/perl.dam HTTP/1.1" 200 1022
"http://bflow.security-portal.cz/wp-admin/perl.php" "Mozilla/5.0 (Windows NT 6.1;
rv:18.0) Gecko/20100101 Firefox/18.0"
bflow.security-portal.cz 41.100.181.234 - - [29/Jun/2013:23:36:48 +0200] "POST
/wp-admin/perl/perl.dam HTTP/1.1" 200 615
"http://bflow.security-portal.cz/wp-admin/perl/perl.dam" "Mozilla/5.0 (Windows NT
6.1; rv:18.0) Gecko/20100101 Firefox/18.0"
```

Tento skript je klasický zástupce CGI skriptů. V tomto případě CGI-telnet skript, který se chová prakticky totožně jako klasický telnet, jen s tím rozdílem, že běží na webovém serveru. Pochází z dílny Rohitab.com a byl vytvořen již v roce 2001.

Ukázka:



Jak můžete vidět skript perl.dam kóduje cestu pro upload nových souborů do URI. Zde nahrál jeden z útočníků soubor na fórum SP

```
# Upload souboru
bflow.security-portal.cz 41.100.181.234 - - [29/Jun/2013:23:37:16 +0200] "GET
/wp-admin/perl/perl.dam?a=upload&d=%2fdata%2fs%2fe%2f
security%2dportal%2ecz%2fsub%2fforum HTTP/1.1" 200 692
"http://bflow.security-portal.cz/wp-admin/perl/perl.dam" "Mozilla/5.0 (Windows NT
6.1; rv:18.0) Gecko/20100101 Firefox/18.0"
```

A zde ověřil jiný útočník existenci nového souboru (200 OK):

```
forum.security-portal.cz 41.200.64.48 - - [29/Jun/2013:23:38:56 +0200] "GET
/team5.txt HTTP/1.1" 200 36 "-" "Mozilla/5.0 (Windows NT 5.1; rv:23.0) Gecko/20100101
Firefox/23.0"
```

Stejným scriptem nahráli script dir.php do rootu SP:

```
bflow.security-portal.cz 41.100.181.234 - - [29/Jun/2013:23:59:38 +0200] "GET
/wp-admin/perl/perl.dam?a=upload
&d=%2fdata%2fs%2fe%2fsecurity%2dportal%2ecz%2fweb%2fimg HTTP/1.1" 200 691
```

```
"http://bflow.security-portal.cz/wp-admin/perl/perl.dam" "Mozilla/5.0 (Windows NT
6.1; rv:18.0) Gecko/20100101 Firefox/18.0"
bflow.security-portal.cz 41.100.181.234 - - [29/Jun/2013:23:59:47 +0200] "POST
/wp-admin/perl/perl.dam HTTP/1.1" 200 662 "http://bflow.security-portal.cz/wp-admin/p
erl/perl.dam?a=upload&d=%2fdata%2fs%2fe%2fsecurity%2dportal%2ecz%2fweb%2fimg"
"Mozilla/5.0 (Windows NT 6.1; rv:18.0) Gecko/20100101 Firefox/18.0"
security-portal.cz 41.100.181.234 - - [30/Jun/2013:00:00:10 +0200] "GET //img/dir.php
HTTP/1.1" 200 1306 "-" "Mozilla/5.0 (Windows NT 6.1; rv:18.0) Gecko/20100101
Firefox/18.0"
```

Script dir.php: http://paste.security-portal.cz/view/d9745074 [15]
Shell (lépe řečeno File Manager) z dílny Tryagteamu [16]. Umí provádět základní operace nad soubory. Smazat, přejmenovat, editovat a změnit mód. Rovněž umožňuje soubory uploadovat.

Výhodou pro nás je, že dir.php pro každou cestu k vylistování adresáře, změnu kódu souboru apod. tento požadavek kóduje v URI pomocí base64.

```
security-portal.cz 41.100.181.234 - - [30/Jun/2013:00:00:32 +0200] "GET
//img/dir.php?path=L2RhdGEvcy9lL3NlY3VyaXR5LXBvcnRhbC5jei9zdWIvZm9ydW0= HTTP/1.1" 200
2065
"http://security-portal.cz//img/dir.php?
path=L2RhdGEvcy9lL3NlY3VyaXR5LXBvcnRhbC5jei9zdWI=" "Mozilla/5.0 (Windows NT 6.1;
rv:18.0) Gecko/20100101 Firefox/18.0"
security-portal.cz 41.100.181.234 - - [30/Jun/2013:00:00:35 +0200] "GET
//img/dir.php?
filesrc=L
2RhdGEvcy9lL3NlY3V
yaXR5LXBvcnRhbC5jei9zdWIvZm9ydW0vY29
uZmlnLnBocA==&path=L2RhdGEvcy9lL3NlY3VyaXR5LXBvcnRhbC5jei9zdWIvZm9ydW0= HTTP/1.1" 200
1058 "http://security-portal.cz//img/dir.php?path=L2RhdGEvcy9lL3NlY3VyaXR5LXBvcnRhbC5
jei9zdWIvZm9ydW0=" "Mozilla/5.0 (Windows NT 6.1; rv:18.0) Gecko/20100101
Firefox/18.0"
```

Takže s pomocí logů, bashe a base64 decode můžeme sledovat kam všude přistupovali.

```
grep 'dir\.php' access_log | cut -d'=' -f2,3,4 | cut -d'&' -f1 | cut -d' ' -f1 | grep
-v security-portal > dir-path
for i in $(cat dir-path); do echo $(echo $i | base64 --decode) >> paths.log; done

cat paths.log | sort | uniq

/nfsmnt/hosting2_1/2/5/
250f3929-f8f7-40e6-a193-f76a88388f0c/security-portal.cz/sub/bflow
/nfsmnt/hosting2_1/2/5/
250f3929-f8f7-40e6-a193-f76a88388f0c/security-portal.cz/sub/bflow/.htaccess
/nfsmnt/hosting2_1/2/5/
250f3929-f8f7-40e6-a193-f76a88388f0c/security-portal.cz/sub/bflow/forum
/nfsmnt/hosting2_1/2/5/
250f3929-f8f7-40e6-a193-f76a88388f0c/security-portal.cz/sub/bflow/forum/config.php
/nfsmnt/hosting2_1/2/5/250f3929-f8f7-40e6-a193-f76a88388f0c/security-portal.cz/logs
/nfsmnt/hosting2_1/2/5/
250f3929-f8f7-40e6-a193-f76a88388f0c/security-portal.cz/logs/error_log-2013-06-29
/data/s/e
/nfsmnt/hosting2_1/2/5/250f3929-f8f7-40e6-a193-f76a88388f0c/security-portal.cz/sub
/nfsmnt/hosting2_1/2/5/
250f3929-f8f7-40e6-a193-f76a88388f0c/security-portal.cz/sub/cm3l1k1
/nfsmnt/hosting2_1/2/5/
```

```
250f3929-f8f7-40e6-a193-f76a88388f0c/security-portal.cz/sub/forum
/nfsmnt/hosting2_1/2/5/
250f3929-f8f7-40e6-a193-f76a88388f0c/security-portal.cz/sub/forum/config.php
/nfsmnt/hosting2_1/2/5/
250f3929-f8f7-40e6-a193-f76a88388f0c/security-portal.cz/sub/kernelhunter
/nfsmnt/hosting2_1/2/5/
250f3929-f8f7-40e6-a193-f76a88388f0c/security-portal.cz/sub/kernelhunter/
wp-config.php
/nfsmnt/hosting2_1/2/5/
250f3929-f8f7-40e6-a193-f76a88388f0c/security-portal.cz/sub/owasp
/nfsmnt/hosting2_1/2/5/
250f3929-f8f7-40e6-a193-f76a88388f0c/security-portal.cz/sub/tor
/nfsmnt/hosting2_1/2/5/250f3929-f8f7-40e6-a193-f76a88388f0c/security-portal.cz/web
...
```

Script instal.php: http://paste.security-portal.cz/view/a9ca7d70 [17]

```
security-portal.cz 213.139.60.75 - - [30/Jun/2013:02:10:31 +0200] "GET /instal.php
HTTP/1.1" 200 4573 "-" "Mozilla/5.0 (Windows NT 5.1; rv:22.0) Gecko/20100101
Firefox/22.0"
```

Upravená verze C99 Shellu. Asi není co dodávat.

Script instoll.php: http://paste.security-portal.cz/view/61a0f534 [18]
Další File Manager. Tentokrát z dílny TeaM HacKer EgypT. Prakticky se jedná o podobný výtvor jako v případě File Managera Tryagteamu jen s tím rozdílem, že umí navíc soubory i přesouvat a vytvářet.

Script cgiPyathon.py: http://paste.security-portal.cz/view/46b9068a [19]
Klasický shell v provedení CGI. Prakticky se neliší od svých PHP bratříčků a ASP sestřiček. Script umožňuje připojení na vzdálený C&C server (o tomto je také dobré informovat hosting).

Závěr dílu

Jste napnutí? Záměrně jsme neřekli jak se mohli dostat do administrace WordPressu a necháme si to pro další díl, ve kterém přineseme i finální rozuzlení důvodu útoku a možnosti jak podobné útoky detekovat a jak jim efektivně zabránit.

Vzhledem k tomu, že útočníci na nás po několik dalších týdnů vedli ještě DDoS (200 IP adres, kdy cílem bylo vytížení databázového serveru) a znásobili počet scanování a útoků, tak, prosím, omluvte případnou nedostupnost Security Portálu, jakožto reakci na vydání tohoto článku. Bereme to sportovně :)

Stay tuned, more to come!

URL článku:
https://security-portal.cz/clanky/anal%C3%BDza-c%C3%ADlen%C3%A9ho-%C3%BAtoku-%C4%8D%C3%A1st-prvn%C3%AD

Odkazy:
[1] https://security-portal.cz/users/cm3l1k1
[2] https://security-portal.cz/category/tagy/hacking
[3] https://security-portal.cz/category/tagy/security
[4] https://security-portal.cz/category/tagy/top-secret
[5] http://www.security-portal.cz
[6] https://modsecurity.org/
[7] https://panopticlick.eff.org/index.php?action=log

[8] http://www.securitate.md/blog/drupal-7-x-search-module-full-path-disclosure/2012/03/14/
[9] http://sqlmap.org
[10] http://ddecode.com/phpdecoder/
[11] http://ddecode.com/phpdecoder/?results=e0719289a4608ed4ef4efa66375337ef
[12] http://paste.security-portal.cz/view/2c41210c
[13] http://paste.security-portal.cz/view/ef8c63c9
[14] http://paste.security-portal.cz/view/b99d28b5
[15] http://paste.security-portal.cz/view/d9745074
[16] https://www.facebook.com/Tryagteam
[17] http://paste.security-portal.cz/view/a9ca7d70
[18] http://paste.security-portal.cz/view/61a0f534
[19] http://paste.security-portal.cz/view/46b9068a