RAPORT SKANOWANIA ANTY-EXPLOITOWEGO
kont hostingowych
Smarthost.pl za rok 2016

1. Wprowadzenie

Na serwerach hostingowych Smarthost.pl wdrożono system wyszukujący podejrzane fragmenty w kodzie wtyczek i dodatków. Działa on w oparciu o bazę kilku tysięcy exploitów na popularne systemy CMS, w tym Joomla, WordPress, Drupal oraz innych aplikacji internetowych napisanych w języku PHP. Podczas skanowania wykrywa próby nieuprawnionych zmian na stronie (w plikach użytkownika).

Monitoring zabezpiecza przed próbami włamań m.in. poprzez dziurawe biblioteki, które umożliwiają dodanie szkodliwego kodu oraz przez niezabezpieczone formularze na stronach www. Skrypt wykrywa również wgranie przez FTP zawirusowanego pliku na serwer, uniemożliwiając atak w sytuacji, gdy zostało wykradzione hasło dostępowe do menedżera plików.

2. Sposób działania systemu anty-exploitowego

W momencie wykrycia zainfekowanego kawałka kodu, następuje blokada wgrania pliku i automatyczne przesunięcie do oddzielnego katalogu kwarantanny, niedostępnego dla użytkownika.

Informacja o zdarzeniu dociera do administratorów Smarthost.pl oraz właściciela strony internetowej. Pozwala to powstrzymać dalsze działania exploitów, które mogą okazać się bardzo kłopotliwe.

Abonent konta otrzymuje natychmiast wiadomość e-mail z informacją, że na serwerze wystąpiła próba wgrania pliku z zainfekowaną zawartością, wraz z dokładną informacją o zaatakowanym pliku. Sam plik, którego zawartość uległa zmianom, lub nowy plik z podejrzaną zawartością zostaje zablokowany.

System wykrywa każdy typ próby wgrania plików, w tym wgranie przez ftp, upload przez formularz, pobranie pliku przez skrypt.

3. Wykrywanie nieaktualnych wersji skryptów

Oprócz wykrywania szkodliwych skryptów, skrypty na hostingu wykrywają również nieaktualne wersje popularnych CMS-ów oraz ich modułów oraz dodatków. O wykryciu nieaktualnej wersji skryptu informowany jest właściciel konta. Nie jest podejmowana żadna inna akcja, oprócz informacji dla właściciela konta hostingowego.

4. Skrócone podsumowanie roczne liczby wykrytych zagrożeń

Liczba przeskanowanych plików na serwerach hostingowych: **39 810 757**

W powyższej liczbie zawierają się pliki dostępne publicznie w katalogach będących serwowanymi przez Apache (w przypadku serwerów opartych na cPanel jest to public_html.

Liczba plików oznaczonych jako **znany exploit**: ***11 674***

Pliki zarażone zostały zablokowane przed zapisem, a użytkownicy kont zostali poinformowani o próbie wgrania zainfekowanego pliku.

Liczba plików oznaczonych jako **nieaktualna wersja skryptu**: ***3 903***

O nieaktualnej wersji skryptu abonencie kont zostali poinformowani i nie została podjęta żadna inna akcja, oprócz informacji.

5. Podsumowanie wykrywania exploitów wg typu

Typ wykrytego exploita	Liczba wystąpień
PHP Wordpress Exploit	6348
PHP Injection Exploit	1053
PHP Obfuscated Exploit	1000
PHP Exploit	904
PHP Shell Exploit	708
PHP GLOBALS Exploit	570
PHP COOKIE Exploit	393
PHP Upload Exploit	223
PHP DarkLeech Exploit	130
PHP POST Exploit	116
PHP REQUEST Exploit	100
PHP EXIF Exploit	41
PHP Spammer Exploit	21
Hacker Sign Exploit	12
PHP Defacer Exploit	9
PHP PB Exploit	8
Exploited .htaccess	7
Shell Exploit	4
PHP Phishing Exploit	4
PHP CryptoPHP Exploit	4
PHP cPanel Exploit	3
Hacker Signature Exploit	3
Shell LD_PRELOAD Exploit	2
PHP GET Exploit	2
Perl Spammer Exploit	2
Perl Exploit	2
PHP Site Defacer	1
PHP Proxy Exploit	1
PHP Joomla Exploit	1
PHP Hacker Signature	1
PHP Backdoor Exploit	1

6. Nieaktualne wersje skryptów

Uwaga 1: podane wersje dotyczą wykrytych wersji w ciągu całego roku 2016, zatem część z wersji została zaktualizowana, część skryptów została po raz kolejny uznana za pewien czas jako nieaktualna. Wersje skryptów są przybliżone. Ze względów na ew. podatności skryptów, które mogły nie zostać zaktualizowane przez użytkowników nie podajemy w niniejszym raporcie dokładnej wersji nieaktualnych skryptów.

Uwaga 2: Wersje skryptów uznawanych za aktualne zmieniały się w ciągu roku. Zatem zestawienie w ramach jednej z wersji zawiera skrypty które mogły być aktualne, a następnie stały się nieaktualne za pewien czas, ze względu na zmianę wersji aktualnej.

Dokładne wytyczne dla Klientów mają zatem znaczenie w przypadku wystąpienia braku aktualności skryptu w konkretnej dacie, ze wskazaniem używanej wersji skryptu i wersji aktualnej, np.
System wykryje wersję nieaktualną i porówna go z aktualnie najnowszą, stabilną wersją:
Joomla v2.5.24 < v3.4.8
ale za jakiś czas może wykryć inny skrypt i porówna go z aktualnie najnowszą, stabilną wersją obowiązującą w dacie wykrycia:
Joomla v2.5.22 < v3.6.4

Uwaga 3: Nasz system nie informuje Klientów wielokrotnie o nieaktualności skryptu w przypadku, gdy zmieniła się aktualna wersja stabilna. Jeżeli Klient został raz poinformowany, dopóki nie zmieni wersji swojego oprogramowania, nie zostanie poinformowany ponownie. Dzięki takiemu rozwiązaniu, z jednej strony Klient nie jest zalewany informacjami a z drugiej strony nasze zestawienie nie zawiera wielokrotnego sprawdzania tych samych starszych wersji oprogramowania.

Uwaga 4: Zestawienie zawiera jedynie skrypty występujące co najmniej 3 razy w ciągu roku.

Uwaga 5: W przypadku wersji oznaczeniem x zaznaczono wiele wersji, np. Wordpress 4.x może oznaczać wersje np. *v.4.4.4, v.4.4.5, v.4.5.2, v.4.5.3* itp.

Uwaga: 6: Oczywiście nie wszystkie wersje skryptów (a może nawet większość) uznane za nieaktualne mają podatności na ataki.

Nazwa i wersja oprogramowania	Liczba wystąpień
CodeIgniter	22
Drupal v.7.x	4
Joomla Advanced Module Manager Ext v5.3.x	27
Joomla Akeeba Ext v3.x	230
Joomla AllVideos Ext v4.5.x	89
Joomla Asynchronous Google Analytics Ext v2.x	16
Joomla Community Builder Ext v1.x	4
Joomla Google Maps Ext v3.x	37
Joomla JEvents Ext v3.x	17
Joomla JomSocial Ext v4.x	3
Joomla K2 Ext v2.6.x	100
Joomla Kunena Forum Ext v3.x	29
Joomla Modules Anywhere Ext v2.x	107
Joomla Phoca Gallery Ext v3.x	128
Joomla Sourcerer Ext v3.x	82
Joomla Tabs Ext v4.x	25
Joomla v0.6	9
Joomla v1.5.x	131
Joomla v2.5.x	346
Joomla v3.x	369
Joomla XCloner Ext v3.x	4
Moodle v1.2.x	5
Moodle v2.x	51
Moodle v3.x	61
phpBB v3.x	39
phpMyAdmin v4.x	11
Piwik v2.x	6
PrestaShop v1.x	44
Roundcube v0.9.x	13
VirtueMart v1.x	28
VirtueMart v2.x	56
VirtueMart v3.x	28

Wordpress v2.x	3
Wordpress v3.x	62
Wordpress v4.x	680
WP All In One SEO Ext	82
WP Contact Form 7 Ext v3.x	112
WP Google XML Sitemaps Ext v3.x	9
WP Jetpack Ext v3.x	25
WP SEO Ext v1.x	7
WP UpdraftPlus Ext v1.x	3
WP WooCommerce Ext v2.x	6

7. Podsumowanie

Celem niniejszego raportu jest przedstawienie zagrożeń związanych ze stronami internetowymi oraz sposobów ich przezwyciężania. W kwestiach bezpieczeństwa nic nie zastąpi stałej i regularnej aktualizacji oprogramowania na serwerach. Istnieją jednak technologie, w tym stosowane na hostingu Smarthost.pl, które mogą pomagać Klientom w dbaniu o bezpieczeństwo ich systemów.

Niniejszy raport ma charakter badania całkowicie zanonimizowanego, bez wskazywania zarówno Klientów jak i konkretnych wersji oprogramowania.