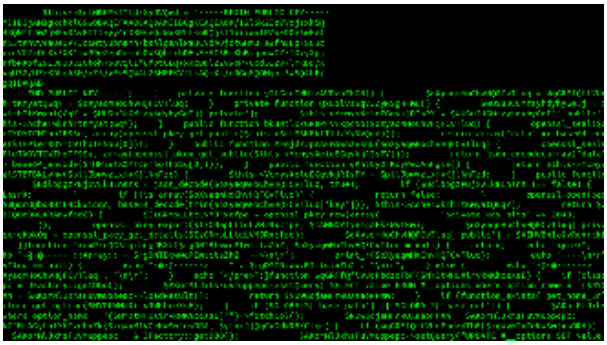


CRYPTOPHP CZYLI "ŻYCIE UKRYTE" NA STRONIE...

Posted on 16 grudnia 2014 by Maciej Cybulski

Categories: aktualności, bezpieczeństwo, porady

Symptomy

W ostatnim czasie zgłosiła się do mnie pewna agencja interaktywna, z prośbą o tuning strony i sprawdzenie co jest ze stroną nie tak "bo jakoś dziwnie ostatnio działa". Strona nie wykazywała na pierwszy rzut oka żadnych nieprawidłowości, poza jedną - w pewnym okresie czasu znacząco spadła wydajność strony mimo iż parametry serwera się nie zmieniły. Próbowano uzasadnić to aktualizacją wtyczek, czy motywu, ale sytuacja była dość uciążliwa więc poproszono o sprawdzeni strony pod kątem obecności „życia ukrytego” ...
Z uwagi na to, że na stronie wykorzystywano motyw którego elementy były chronione za pomocą oprogramowania IonCube, oprogramowanie wyszukujące zaszyfrowany kod dawało sporo alarmów false-positive. Najwidoczniej nikt nie miał wystarczająco cierpliwości by przyjrzeć się raportom wystarczająco dokładnie,a było ich sporo.

W jednej z wtyczek i motywie natrafiłem na kod:

```
define(,WP_OPTION_KEY',true); function dzglksvsporkdJkjfghKLHejs()
      {
       define(,WP_OPTION_KEY','wp_data_new'); new dfdglkhafkljSTlkjATRBsgS();
      }
  private $GDHDHSghSghsgh, $FRGAghgfdsdfHERjkAaSETd5DH,
$drdhTertDTUoIOGQwsaS;
```

Co zwróciło moją uwagę? „dziwne" nazwy funkcji... zatem trop okazał się ciekawy. By dalej nie brnąć w być może ślepy zaułek dopytałem o źródła komercyjnych motywów i wtyczek, bo elementy znalezione w kodzie świadczyły o uwierzytelnianiu za pomocą klucza RSA, co bynajmniej było dziwne.

W kolejnym z plików znalazłem kod:

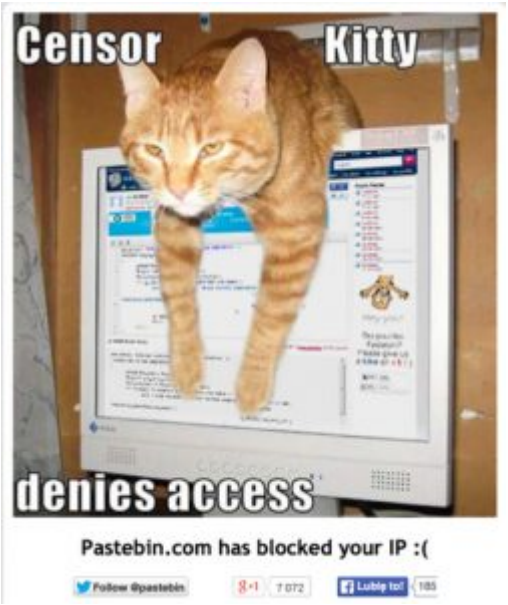
```
 $this->drgFDdShsSHstHSdh =„ - - - - - BEGIN PUBLIC KEY - - - - -
rnMREGRGDjzRGreaanrjnargARgnarkgjnareARG ….
```

Uzyskana odpowiedź odnośnie źródeł pozyskania elementów strony nie była jednoznaczna. Efektem dogłębnej kontroli kodu strony było wykrycie ciekawego w działaniu backdoora o nazwie *CryptoPHP*.

Jaka jest specyfika jego działania?

Najczęściej na stronę trafia poprzez niezaufane źródła programów. Często bywa tak, że zamiast zapłacić za wtyczkę, czy motyw instalujemy go z „darmowego" źródła. Na pierwszy rzut oka jest ok... ale często zwiera w sobie troszkę kodu i innych dodatków. Np. często niewinnie wyglądający i

nazywający się plik *social.png* wchodzący w skład niektórych wtyczek integrujących z social mediami może zawierać zaszyty kod PHP. Innym sposobem infekcji jest atak typu „egg dropp". Obserwując korelację pomiędzy wydaniem aktualizacji do WordPressa (np z 4.0 na 4.0.1) a raportowaniem o próbach włamania na strony którymi się opiekuję, zauważyłem pewną zbieżność.Krótko po opublikowaniu informacji o aktualizacji bezpieczeństwa WP, gwałtownie wzrasta ilość prób włamań wykorzystujących opisane podatności na włamania. Trwa to kilka dni i potem cisza… Za jakiś czas na niektórych stronach pojawiają się chwilowe problemy z wydajnością ale szybko wraca wszystko do normy. Niby nic szczególnego. Nie mniej oprogramowanie monitorujące jest w stanie wychwycić takie zjawiska, co później może pomóc w ustaleniu scenariusza…
Co faktycznie zaszło?



Czas wypuszczenia nowej aktualizacji WP jest najlepszym też czasem na włamania, bo wiadomo gdzie szukać podatności, w raportach zmian WP można często doczytać się gdzie ich szukać. A potem działa już czynnik ludzki i statystyka.
By atak był skuteczniejszy długofalowo ma on dwa etapy. Pierwszy etap, podrzucenie kodu ale w formie „nieaktywnej", czyli kod pojawia się na stronie ale w sposób niewidoczny dla użytkownika, często jako zakomentowane linie kodu, czy dodatkowe pliki .Mija miesiąc lub dwa, kiedy to maleją prawie do zera szanse na to że archiwa strony nie będą zainfekowane i wtedy nawiązywane jest połączenie z zainfekowaną stroną. W międzyczasie informacja o zmianach w plikach zginie w gąszczu raportów dostarczanych przez wtyczki typu WP Firewall czy WordFence. Czujność została uśpiona, kod podrzucony 50% "sukcesu". A potem już tylko zostaje nam obserwować co dzieje się ze stroną.

Po co to wszystko?

Kod typu CryptoPHP może być wykorzystany przez włamywacza do kilku ciekawych działań:

- uwierzytelnianie kluczem RSA może być wykorzystane do przesyłania danych pomiędzy serwerami (tak często przesyłane są programy typu RootShell o których pisałem już kiedyś.) Umożliwiają one przejęcie pełnej kontroli nad stroną i plikami na serwerze.
- do przechowywania danych w bazie danych strony www.

- do wykonania na serwerze dowolnego kodu.

Stąd sam CryptoPHP nie jest może wirusem, ale właśnie backdoorem - tylną furtką - programem umożliwiającym dyskretne wejście do systemu i praktycznie dowolne nim manipulowanie. Najczęściej jest on stosowany też w blackhat seo. Stąd mimo iż na stronie wspomnianej agencji nie pojawiało się nic niepokojącego to spadła wydajność strony, co świadczyło o tym że dzieje się coś „w tle”.

Jak uniknąć infekcji?

- stosować standardowe zasady bezpieczeństwa
  - konto administratora do zarządzania stroną a konto redaktora do publikacji treści
  - silne hasła
  - zawsze aktualne oprogramowanie na stronie (wp, motyw, wtyczki)
- pozyskiwanie wtyczek czy motywów z legalnych, sprawdzonych źródeł

Jak wykryć?

- ręcznie analizując kod strony zwracając też uwagę szczególną na pliki graficzne w których może być zaszyty złośliwy kod
- użycie programu antywirusowego - często pomaga zlokalizować zagrożenie choć nie zawsze skutecznie
- stosowanie wtyczek generujących tzw. hash plików na serwerze, pozwoli to na monitorowanie zmian w plikach i wykrycie najdrobniejszej w nich zmiany.
- stosowanie oprogramowania monitorującego błędne logowania na stronę. Często dopiero po instalacji takiego oprogramowania dowiadujemy się jaką „popularnością” cieszy się nasza strona ;)

Jak usunąć CryptoPHP?

Niestety nie ma metod automatycznych. Zostaje jedynie ręczne usunięcie złośliwego kody z zainfekowanych plików.

Opisane elementy kodu i scenariusz oczywiście mogą się różnić na różnych stronach, nie mniej

schemat infekcji i jej symptomów może być bardzo zbliżony.
Jeśli masz problem z takim zjawiskiem i nie wiesz jak sobie z nim poradzić, napisz zaradzę temu :)

No i oczywiście zapraszam do dyskusji w temacie, bo jak wiadomo każdy przypadek jest inny i nie mniej ciekawy.

Comments

Krystian – 2017-09-01 01:16:18
Strach pomyśleć jakby do serwerów dodawali wydajne karty graficzne. Rosnące koparki btc :D