Checklista_
Jak postępować gdy mamy włam na sklepie PrestaShop

Wstęp

Hej! Jesteśmy Convertis! - Software House oferujący wsparcie programistycznie dla sklepów opartych o technologię PrestaShop.

W okresie lipiec/sierpień 2022 spotkaliśmy się z procederem włamów na tej platformie u Klientów.

W naszej firmie jedną z najważniejszych rzeczy (zaraz po Ludziach) są procesy i instrukcje. Pozwalają nam one efektywnie, sprawnie, ale przede wszystkim skutecznie działać.

Tym razem stworzyliśmy narzędzie, z którego sami korzystamy pomagając sklepom przy kolejnych potencjalnych lub wykrytych przypadkach włamów.

I teraz chcemy się nim z Wami podzielić, abyście mogli z niego skorzystać, kiedy przydarzy Wam się atak hakerski.

Ten dokument cały czas będziemy aktualizować według naszej najnowszej wiedzy, kolejnych przypadków (miejmy nadzieję, że się nie zdarzą), a także doniesień z branży.

To roboczy skrypt, oparty na naszym doświadczeniu, także, jeśli uważasz, że trzeba coś w nim zmienić, poprawić lub uzupełnić o jakieś info czy działania daj znać na: Hello@convertis.pl

Będziemy wdzięczni!

Mamy nadzieję, że będzie to z korzyścią dla całej branży!

v1.0 z dnia 220816

Checklista

Zapewne podejścia do tematu będą różne w zależności od tego jaki miał wymiar i jak wyglądał atak. Poniżej prezentujemy listę rzeczy, które warto zrobić gdy już takie zdarzenie nastąpi.

W zależności od skutków ataku, podejmij środki, by przede wszystkim jak najmniej ucierpiał potencjalny użytkownik/ Klient Twojego sklepu:

1. Zablokuj serwer przed dostępem z zewnątrz - wyłącz serwer http i ftp. Skonfiguruj sobie bezpieczny dostęp do zasobów serwera przez ssh.

2. Zmień hasła do FTP serwera, poczty itp.
   Pamiętaj o wszystkich hasłach i kluczach dostępowych do zewnętrznych api, systemów płatności, mailingowych itd. które były w konfiguracji sklepu - należy je zmienić.
   Jeśli miałeś skonfigurowane wysyłanie poczty przez smtp - te hasła także są do zmiany.

3. Stwórz kopię sklepu i bazę danych obecnego stanu (przyda Ci się - np. z niej dograsz brakujące zamówienia).

4. Przywróć sklep z kopii zapasowej np. sprzed tygodnia lub takiej, która wydaje Ci się najbardziej bezpieczna (tu nie ma reguły. Jeśli sklep został zaatakowany dziś, to np. wczorajsza kopia może być również zainfekowana).
   W każdym razie jeśli chcesz jak najszybciej przywrócić sklep do działania - zrób to, bo znalezienie luki, w której doszło do włamania może zająć sporo czasu lub może być niemożliwe. Tym możesz zająć się po opanowaniu pożaru, porównując np. pliki źródłowe backupu i zainfekowaną kopią sklepu.

5. Nanieś wszystkie możliwe, znane poprawki np. skorzystaj z naszej checklisty => ***Checklista _ Jak zabezpieczyć sklep Prestashop przed atakami hakerskimi i co zrobić, gdy nie zdążyłeś tego zrobić***

6. Zmień hasło do bazy danych.

7. Skonfiguruj dostęp do serwera serwera http poprzez bezpieczny kanał ssh lub vpn - uruchom serwer http i sklep z dostępem tylko przez ten kanał.

8. Zmień hasła wszystkim użytkownikom panelu administracyjnego sklepu.

Kontakt: hello@convertis.pl

9. Zmień klucze webapi jeśli udostępniasz je komuś.

10. Możesz zmodyfikować core PrestaShop tak, by blokował wgrywanie modułów z poziomu panelu administracyjnego.

11. Przeskanuj kopię skanerem antywirusowym.

12. Przenieś z zainfekowanej bazy danych dane zamówień wraz z powiązaniami (dane zamówień powinny być stosunkowo odporne na infekcję, ale też należy je przejrzeć pod kątem zainfekowania.

13. Uruchom sklep publicznie.