Zaufana Trzecia Strona

Szczegóły anatomiczne klientów, czyli co jeszcze wyciekło z Hyperiona

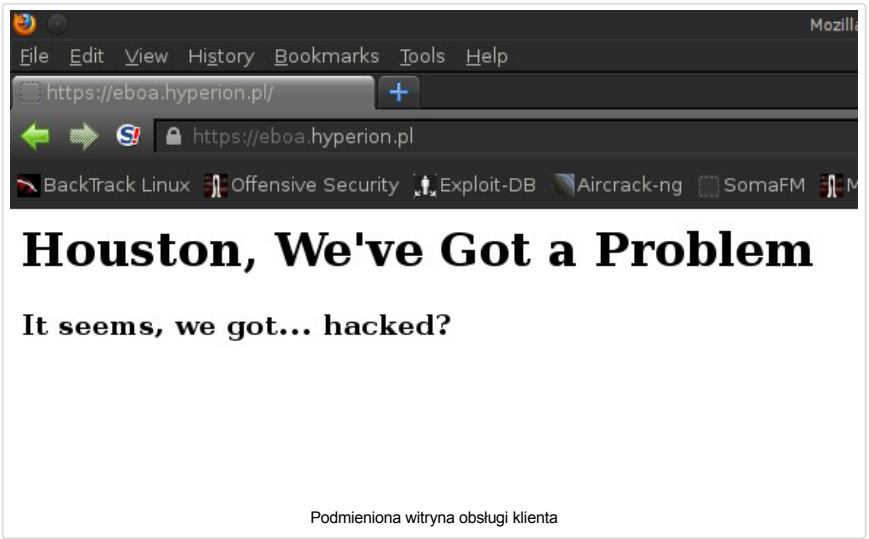
Dodano: 13 listopada 2013 o 19:00 w kategorii Wpadki, Włamania
Tagi wpisu: Hyperion • pensje • wyciek • włamanie

Otrzymane przez nas nowe informacje wskazują, że z firmy Hyperion wyciekło dużo więcej niż tylko baza abonentów. Dane wskazują też na niepokojący fakt całkowitego ignorowania przez firmę wcześniejszych poważnych incydentów bezpieczeństwa.

Jeśli ktoś podmienia stronę Waszej firmy lub Wasi klienci dowiadują się, że mają małego penisa, to wiedzcie, że coś się dzieje i nie wystarczy zmienić hasła roota.

Podmieniona strona? Zmieńmy hasło.

Kilka dni temu poinformowaliśmy o wycieku danych ponad 400 tysięcy klientów firmy Hyperion. Wczoraj otrzymaliśmy kolejne informacje związane z tym incydentem. Według anonimowego informatora, w firmie doszło co najmniej do jednego wcześniejszego włamania, wiążącego się z podmianą witryny obsługi klienta eBoa. Według jego informacji 29 lipca tego roku strona eBoa wyglądała tak:



Podmieniona witryna obsługi klienta

Co ciekawe, podobno w tym stanie trwała co najmniej do południa dnia następnego, a kiedy już wróciła do stanu sprzed włamania, administratorzy serwisu „podnieśli poziom zabezpieczeń", zmieniając hasło roota oraz przenosząc usługę SSH na niestandardowy port. Jak możecie się spodziewać, zabiegi te niewiele dały i krótko potem doszło do kolejnego naruszenia bezpieczeństwa platformy.

Małe penisy abonentów firmy

Trzymaj rękę na pulsie

Najlepsze w tym miesiącu

Jak hakerzy na prośbę dziennikarza jego życie cyfrowe spenetrowali
mBank sam usuwa groźnego konia trojańskiego z telefonów klientów
Instalowaliście cracki tej grupy? Szpiegowały użytkowników.
Urządzenia podsłuchowe NSA na dachu ambasady USA w Warszawie
Czy pliki binarne TrueCrypta były skompilowane z dostępnych źródeł?

Drobiazgi

Włamanie na stronę Wojewódzkiej Inspekcji Transportu Drogowego
infopraca.pl infekowała odwiedzających
Nieautoryzowane użycie komputera NBP
Podmieniona witryna Ruchu Narodowego
Zdalny błąd w OpenSSH – ale wcale nie taki straszny

Adres email zapisz

Tematy

0day Adobe Android Anonymous antywirus Apple atak backdoor bitcoin botnet błąd Chiny dane ddos DNS exploit Facebook FBI Google hacked hash hasła hasło iPhone Java konferencja Microsoft narkotyki NSA podsłuch Polska prywatność Silk Road SSL Symantec TOR Twitter tylna furtka USA Weekendowa Lektura wirus wpadka wpadka tygodnia wyciek włamanie

Według informacji, które podał nam anonimowy czytelnik, w dniu 14 października 2013 nastąpiła drobna, choć znacząca zmiana w strukturze bazy danych abonentów firmy Hyperion. Zmiana ta wyglądała następująco:

```
SQL> update hyperion.klient set imie=imie+' ma malego penisa';
```

Jej skutkiem było zmodyfikowanie danych klienta, wyświetlanych w panelu obsługi i zamiast „Kowalski Jan" klient mógł zobaczyć „Kowalki Jan ma małego penisa". Serwis eBoa zniknął z sieci, a po kilku godzinach zmiana została wycofana, a serwis ponownie udostępniony. Według naszego informatora zamiast tego złośliwego psikusa włamywacz mógł wpędzić firmę w poważniejsze problemy, ponieważ mógł skasować całą bazę abonentów, której kopie bezpieczeństwa pochodziły sprzed dwóch miesięcy.

Pensje, paski i raporty

Kolejne informacje również wydają się interesujące. Cytujemy poniżej fragment otrzymanej wiadomości:

> *Wyciek danych nie jest więc żadnym zaskoczeniem dla Hyperiona, jest to niecierpliwie przez nich oczekiwany argument na podstawie którego mogli pozbyć się tego kukułczego jaja na rzecz ludzi z budżetówki, którzy się na tym znają.*
>
> *A ich kadra naprawdę nie wygląda na zaawansowaną technicznie bo też i nie zarabia [place1.pdf], chociaz niektórym się w życiu poszczęściło [place2.pdf]. Ale jak żyć panie Premierze jak ludzie umowy rozwiązują i płacić za usługi nie chcą [*.xls]?*

Wraz z wiadomością otrzymaliśmy wgląd do kilku dokumentów, wskazujących na dostęp włamywacza do ważnych plików związanych z funkcjonowaniem spółki. Wśród nich znalazł się pasek z wypłaty ze stycznia 2013 osoby zarabiającej w okolicach połowy średniej krajowej, formularz ZUS RMUA jednego z byłych członków zarządu spółki z roku 2005 z wielokrotnie wyższym wynagrodzeniem, plik zawierający wiekowanie należności abonentów na łączną kwotę kilkudziesięciu milionów PLN oraz wyniki sprzedaży i odejść klientów, wskazujące na spadek liczby abonentów.

Podsumowanie

Niestety nie jesteśmy w stanie potwierdzić wiarygodności otrzymanych dokumentów – do tej pory nie otrzymaliśmy odpowiedzi spółki nawet na nasze pytania sprzed tygodnia. Nie da się jednak ukryć, że informacje oraz dokumenty sprawiają wrażenie wiarygodnych i stawiają pod poważnym znakiem zapytania poziom ochrony danych w spółce. Niepokojący jest także brak jakiejkolwiek komunikacji ze strony spółki z abonentami, których dane zostały ujawnione. Część z nich prawdopodobnie do tej pory nie zdaje sobie sprawy z tego, że ich dane znalazły się w niepowołanych rękach.

To już drugi artykuł na temat firmy Hyperion, lecz możliwe, że nie ostatni – nasz informator zakończył swoją wiadomość zwrotem „c.d.n."

Podobne wpisy

- Podmieniona witryna Ruchu Narodowego
- Wyciek danych ponad 400 tysięcy abonentów firmy Hyperion
- Możliwość sprawdzenia, czy dane konto było w wycieku Adobe

Komentarzy: 15

Ciekawy

Czy GIODO nie może zająć się tą sprawą? Skoro jest takie, chyba dość poważne, podejrzenie o wyciek danych ludzi to chyba powinni się tym zająć z automatu, czyż nie?

Odpowiedz

translation

@ciekawy: giodo ma w deupie takie rzeczy stary ;]
nie wierzysz, zadzwon i zapytaj o obsluge takiego czy innego encydentu sieciowego a szybko przekonasz sie ze smiechem na ustach, ze to kolejny twor, pomocny niczym zus. buziaki ;]

Odpowiedz

Robert

Mały penis – dobre :D

Odpowiedz

Czytelnik

Wkradła się literówka.
„Jeśli ktoś podmienia stronę Waszej firmy lub Was klienci…”

Odpowiedz

densi

Przynajmniej nie działali destrukcyjnie, to się chwali. A w czym był problem, skrypt, czy serwer ?

Odpowiedz

Hya

Ułańska fantazja :D

Odpowiedz

bmpte

Jak znam życie, serwer, skrypt i tożsamość pomiędzy monitorem i fotelem.
Chociaż akurat tej tożsamości bym nie winił.

Odpowiedz

str4sznyp1r4t

Co to jest „wiekowanie należności”?

Odpowiedz

Jan

@str4sznyp1r4t z tego co Gugle mówi to rozbicie wszystkich należności na poszczególne okresy. W tym przypadku chodzi pewnie o to, że mają od groma niezapłaconych rachunków z datą w przeszłości.

Odpowiedz

Zen_Xen_ni

Jan Kowalki? To ta zmiana jeszcze wprowadzała też literówki? :D

Odpowiedz

hehe

Czepiliście się hyperiona i jemu zadajecie pytania, ale może kierujecie je do złego podmiotu? Może nie trzeba szukać na czubku góry lodowej, tylko spojrzeć głębiej? Hyperion od jakiegoś czasu należy (chyba w całości) do MNI – może więc to nie jest problem hyperiona, tylko być może nastąpiła „optymalizacja kosztów zatrudnienia" i teraz całym systemem hyperiona zajmują się administratorzy z MNI? Może to do nich trzeba zadać pytanie o prawdziwość tych doniesień?
A może też zostały powołane „firemki i spółeczki" które mają za zadanie wyciągać kasę z „firmy matki" i zajmować się obsługą?
Dysproporcja zarobków o której wspominacie występuje w każdej firmie – to oczywiste że ludzie w zarządzie zarabiają co najmniej o jedno zero więcej. Ignorancja bezpieczeństwa może nie wynikać z tego, że nie chce się zapobiegać włamaniom – może wynikać zwyczajnie z braku wiedzy i doświadczenia lub też ignorancji ze strony „osób decyzyjnych". Teraz „zaprzyjaźniona duża firma z doświadczeniem" za duże pieniądze wykona audyt, modernizację systemu, ci którzy do tej pory go utrzymywali dostaną „po dupie" i wszystko wróci do normy… Być może to nie jest wcale włamanie tylko „wyniesienie danych wrażliwych z firmy".

Odpowiedz

Jerema Wiśniowiecki

jednak ktos tu mysli z czytelnikow… ;)

Odpowiedz

Adam

Piszemy „Hyperion", ponieważ pod taką nazwą spółka świadczy usługi klientom i tak oficjalnie nazywa się główna spółka (podmiot dominujący) grupy kapitałowej. MNI jest największym udziałowcem, ale nie jest udziałowcem większościowym – ma 38% akcji. Co do pozostałej części komentarza – bardzo możliwe, ale nie mamy takiej wiedzy więc opieramy się na tym, co wiemy.

Odpowiedz

Magda

Na infolinii Hyperionu/MNI powiedzieli, że na razie nie potwierdzono wycieku – trwa audyt. Po jego zakończeniu użytkownicy dostaną pisemną informację – prawdopodobnie razem z najbliższą fakturą. Teoretycznie mają obowiązek poinformować abonentów w ciągu 3 dni od WYKRYCIA wycieku, ale skoro jeszcze go nie potwierdzili, więc nie poczuwają się do tego obowiązku.

Odpowiedz

Adam

No tak, porównanie bazy 400 tysięcy rekordów z własną bazą 400 tysięcy rekordów to bardzo pracochłonne zajęcie…

Odpowiedz

Zostaw odpowiedź

Jeśli chcesz zwrócić uwagę na literówkę lub inny błąd techniczny, zapraszamy do formularza kontaktowego. Reagujemy równie szybko.

Imię *

E-mail *

Strona www

Wyślij komentarz

Jesteś tu: Zaufana Trzecia Strona » Wpadki » Szczegóły anatomiczne klientów, czyli co jeszcze wyciekło z Hyperiona