# GPW walczyła z włamywaczami od co najmniej 10 dni

Adam dodał 24 października 2014 o 11:09 w kategorii Włamania z tagami: GPW • wyciek • włamanie

Z wiarygodnego źródła otrzymaliśmy informację, że pracownicy GPW wiedzieli o włamaniu do swojej sieci od co najmniej 10 dni. Co prawda podjęli próby usunięcia włamywaczy z systemów, ale początkowo były to próby nieudane.

Opisane przez nas wczoraj włamanie do GPW i powiązany z nim wyciek danych prawdopodobnie zaczęły się wiele dni temu. Wczoraj zostały o nim poinformowane media, co najwyraźniej skłoniło firmę do bardziej zdecydowanego działania.

## *Problemy od wielu dni*

Wiarygodne źródło poinformowało nas, że pierwsze symptomy nieautoryzowanej aktywności w sieci GPW zostały odkryte co najmniej 10 dni temu. Pierwszy na niepokojące zachowanie jednego z serwerów zwrócił uwagę zespół odpowiedzialny za administrację maszyną. Przy pomocy zespołu odpowiedzialnego za funkcjonowanie sieci udało się potwierdzić, że serwer generuje nieautoryzowany ruch i przeprowadza skany sieci wewnętrznych.

Szybko zostały podjęte działania naprawcze, polegające co najmniej na przeinstalowaniu serwera oraz zmianie powiązanych z nim haseł. Niestety okazało się, że to nie wystarczyło, a włamywacze nadal posiadają dostęp do sieci wewnętrznej przedsiębiorstwa.

Wszystko wskazuje na to, że pierwszym przyczółkiem włamywaczy mógł być jeden z dwóch serwisów: gpwtrader.pl lub utp.gpw.pl. W serwisie prawdopodobnie odkryto błąd typu SQLi, za pomocą którego uzyskano dostęp do systemu. W kolejnych krokach włamywacze zdążyli przeskanować większość dostępnych zakresów adresacji wewnętrznej w poszukiwaniu innych podatności i prawdopodobnie zdobyli uprawnienia roota na co najmniej jednej maszynie (wskazuje na to obecność danych z pliku /etc/shadow).

## *Radykalne działania*

Wczoraj około południa do mediów trafiła informacja, wysłana prawdopodobnie przez włamywaczy, z linkiem do serwisu Pastebin, w którym umieszczono wykradzione z GPW materiały. Krótko potem większość serwerów WWW spółki została wyłączona. Główny serwer wrócił po kilku godzinach, jednak spora część stron nie działa do tej pory. Posiadane przez nas informacje wskazują, że włamywacze najprawdopodobniej uzyskali dostęp co najmniej do następujących serwisów:

```
www.gpwcatalyst.pl
www.newconnect.pl
gpwtrader.pl
utp.gpw.pl
```

GPW rozesłała także komunikaty, częściowo potwierdzające zakres włamania.

> *Giełda Papierów Wartościowych informuje, że z przyczyn od niej niezależnych mogło dojść po pozyskania przez podmioty nieuprawnione archiwalnych danych używanych do logowania do Szkolnej Internetowej Gry Giełdowej i symulatora giełdowego GPW Trader.*
>
> *Jednocześnie informujemy, że zaistniała sytuacja pozostaje bez wpływu na*

Najlepsze w tym miesiącu

Poważny błąd Facebooka – loguje użytkowników na losowe profile

Krytyczny błąd w setkach domowych ruterów umożliwia przejęcie kontroli

Ponad 30 tysięcy plików skradzionych Sony Pictures już w sieci

Grupa włamywaczy, którzy masowo okradają banki zamiast ich klientów

Miliarder chciał bombardować Iran, w odpowiedzi ktoś skasował mu serwery

Tor, VPN, OTR, PGP, Truecrypt czyli czego nie potrafi dzisiaj złamać NSA

Projekt stworzenia komputera opartego tylko o wolne i otwarte oprogramowanie

FunSec

:) Obama zhakowany

:) Mocny dowód na udział Korei Północnej we włamaniu

:) Jak absolutnie NIE używać tokenów

Drobiazgi

Największa nagroda za odkryte błędy w usługach Google dla Polaka

Weekendowa Lektura 2014-12-26

Tor Project ostrzega przed próbami wyłączenia sieci Tor

Weekendowa Lektura 2014-12-19

Zdalne wykonanie kodu w NTP

Trzymaj rękę na pulsie

Adres email zapisz

Wyszukiwanie

Szukasz czegoś? szukaj

*prawidłowe funkcjonowanie i bezpieczeństwo systemu transakcyjnego Giełdy.*

> *Szanowni Państwo,*
>
> *Uprzejmie informujemy, że z przyczyn niezależnych od Giełdy Papierów Wartościowych w Warszawie S.A. mogło dojść po pozyskania przez podmioty nieuprawnione Państwa archiwalnych danych używanych w związku z udziałem w projekcie wdrożenia systemu UTP.*
>
> *Bardzo przepraszamy za zaistniałą sytuację i jeśli używali Państwo tych samych haseł w innych serwisach internetowych rekomendujemy ich zmianę.*
>
> *Giełda Papierów Wartościowych SA*

## *Słabe hasła*

Niestety dane, udostępnione przez włamywaczy, wskazują na trwałą bolączkę większości firm na całym świecie, czyli beznadziejnie słabe hasła użytkowników oraz administratorów. O ile tych pierwszych można jeszcze przeboleć, to ci drudzy powinni zmienić swoje nawyki – i to szybko. Nie wiemy, z jakiego systemu pochodzą te dane, ale ich format wskazuje na zrzut z kontrolera domeny.

| username | password | password hash | user_type | Company |
|---|---|---|---|---|
| [redacted] | 1qaz2wsx | 565c98467be7987f95bc2c1e7d4c3 | Administrator | GPW |
| [redacted] | | a576c0b2daee117c99ec3815bb9ca | Administrator | GPW |
| [redacted] | nokia3210 | d6b2647e48887a6213ba0afe4644a | Administrator | GPW |
| [redacted] | qazqaz | e4051778e7f91482e396af2539436 | Administrator | GPW |
| [redacted] | helki123 | f2e0608f19772526395ace9efa88f5 | Administrator | GPW |
| RKU.ADMIN | nokia3210 | 97bc135959f9fbce660e91550f9627 | Super Administrator | |
| admin | qazqaz | ad80e439a1ef6b20e1b0816d0f841 | Super Administrator | GPW |
| RKU.ADMIN.G | nokia3210 | 96b5be1d02e2eabd3e7d141a37be | Super Administrator | GPW |
| [redacted] | | 13022650d5887825d759237ad5d8 | Super Administrator | GPW |

Hasła administratorów

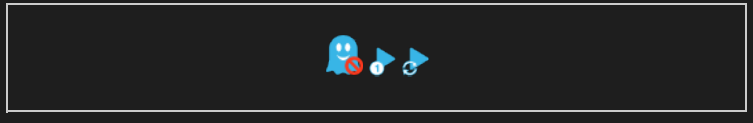
## *Dobra wiadomość?*

Wszystko wskazuje na to, że choć zakres włamania był większy, niż wskazują na to oficjalne komunikaty GPW, to wszystkie zaatakowane serwery znajdowały się w tej samej podsieci, odseparowanej od pozostałych systemów giełdy. Nie natrafiliśmy do tej pory na informacje wskazujące, by włamywacze dotarli do głównych systemów transakcyjnych. To chyba jedyna dobra wiadomość w tej sprawie.



Podobne wpisy

- Szczegółowe projekty koreańskich elektrowni jądrowych wyciekły do sieci
- Miliarder chciał bombardować Iran, w odpowiedzi ktoś skasował mu serwery
- phpBB.com ofiarą włamywaczy



## *Komentarzy: 22*

2014.10.24 11:22 Nocarz

Tematy

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