



Zaufana Trzecia Strona

Sony Pictures zhakowane, wszystkie komputery pod kontrolą włamywaczy

Adam dodał 24 listopada 2014 o 23:40 w kategorii [Włamania](#) z tagami: [GOP](#) • [hacked](#) • [Sony](#) • [Sony Pictures](#)

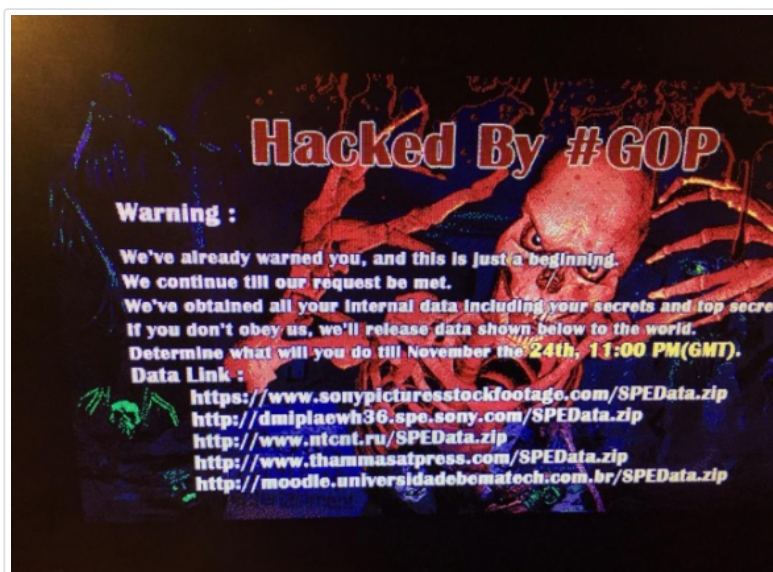


Jeśli mieliście dzisiaj zły dzień w pracy, to pomyślcie o administratorach w Sony Pictures a od razu zrobi się Wam lepiej. Na wszystkich komputerach firmy na całym świecie pojawił się komunikat od włamywaczy wraz z ogromną listą plików.

Pracownicy Sony Pictures zostali dzisiaj wypuszczeni do domów gdy okazało się, że cała sieć firmowa jest pod kontrolą bliżej niezidentyfikowanych hakerów. Grożą oni ujawnieniem tajemnic firmy jeśli ich żądania nie zostaną spełnione w ciągu najbliższych godzin.

Komunikat od #GOP

Na ekranach wszystkich komputerów w Sony Pictures pojawił się dzisiaj następujący komunikat:



Komunikat na komputerach Sony Pictures

Hacked By #GOP

Warning:

*We've already warned you, and this is just a beginning.
We continue till our request be met.
We've obtained all your internal data, Including your secrets and top secrets.
If you don't obey us, we'll release data shown below to the world.
Determine what will you do till November the 24th, 11:00 PM (GMT).*

W komunikacie haker/rzy opisujący się jako #GOP (Guardians of Peace) informują, że są w posiadaniu wielu tajemnic firmy i są gotowi je ujawnić jeśli ich bliżej niesprecyzowane

Najlepsze w tym miesiącu

[Sony Pictures zhakowane, wszystkie komputery pod kontrolą włamywaczy](#)

[Wersja testowa systemu PKW dostępna publicznie w trybie DEBUG](#)

[Ponad 30 tysięcy plików skradzionych Sony Pictures już w sieci](#)

[Kontrowersyjne nowe narzędzie do wykrywania rządowych trojanów](#)

[To będzie bolalo – ponad 100 plików z tysiącami haseł Sony w sieci](#)

[Wybrali z bankomatów małą fortunę, podając odpowiedni kod serwisowy](#)

[I Ty możesz zhakować swój ruter – przykład od Czytelnika](#)

FunSec

[:\) Uniwersalna odpowiedź na problemy z bezpieczeństwem](#)

[:\) Niektórych zasobów nie da się zabezpieczyć](#)

[:\) Ironiczny XSS](#)

Drobiazgi

[Z Sony Pictures wyciekają scenariusze, dane aktorów](#)

[Bezpieczeństwo Google App Engine Java rozbite przez Polaka](#)

[The Pirate Bay wyłączony po nalocie policji](#)

[Jak pisać raporty z pentestów](#)

[Weekendowa Lektura
2014-11-28/2014-12-06](#)

Trzymaj rękę na pulsie



Wyszukiwanie

żądania nie zostaną spełnione. Pod komunikatem znajdują się linki do kopii pliku o rozmiarze ponad 200MB, zawierającego dwie ogromne listy plików znajdujących się rzekomo w rękach hakerów. Same listy po rozpakowaniu mają ponad 1GB, co oznacza, że włamywacze co najmniej zindeksowali albo wielkie zasoby sieciowe, albo osobiste komputery wszystkich pracowników firmy. Analiza zawartości archiwów [przeprowadzona na Reddicie](#) wskazuje, że faktycznie nazwy plików wskazują na ich pochodzenie z komputerów pracowników Sony Pictures. Przykładowy fragment listy:

```
list1.txt:Logins -passwords.xlsx
list1.txt:Publication usernames and passwords.xls
list1.txt:IDs and passwords.doc
list2.txt:Password History - past 11 passwords.txt
list2.txt:passwords.zip
list2.txt:passwords.zip
list2.txt:passwords .txt
list2.txt:Extranet Oracle & SQL passwords 4.3.06.txt
```

Wśród plików wymienionych z nazwy znajdują się także informacje finansowe, klucze prywatne, kopie skrzynek pocztowych, kopie dowodów tożsamości, bazy menedżerów haseł, umowy, diagramy sieci czy wyciągi bankowe. Jeśli wierzyć nazwom plików znajdują się tam także paszporty gwiazd

```
list1.txt:Diaz, Cameron - Passport.pdf
list1.txt:Angelina Jolie passport.pdf
```

a także trochę ironicznie wyglądająca w tym kontekście polisa

```
list1.txt:INSURANCE for security breaches.doc
list2.txt:Security Breach Course Of Action.v1.txt
```

Prawdziwość danych potwierdza także fakt [włamania na liczne konta Twittera](#) związane z filmami wytwórni. Najwyraźniej pracownicy Sony Pictures odzyskali już dostęp do kont, ponieważ wpisy poznikwały, jednak zachowały się ich kopie.



Soul Surfer @SoulSurferMovie · 2h

Hacked By #GOP

You, the criminals including Michael Lynton will surely go to hell.
Nobody can help you.



← ↻ ★ 1 ⋮

Reakcja firmy

Jak donoszą magazyny [Deadline](#) oraz [Variety](#) wszystkie komputery w biurach zostały wyłączone. Pracownicy dostali zakaz uruchamiania swoich komputerów lub zdalnego łączenia się z biurami i zostali wypuszczeni do domów. Zostali także podobno poproszeni o wyłączenie WiFi w swoich telefonach.

Wygląda na to, że mamy do czynienia z jednym z najbardziej spektakularnych ataków komputerowych w historii. Spodziewajcie się aktualizacji tego wpisu.

Tematy

[Oday](#) [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](#) [podśluch](#) [Polska](#)
[prywatność](#) [ruter](#) [Silk Road](#) [SSL](#)
[szyfrowanie](#) [TOR](#) [Twitter](#) [tylna](#) [furtka](#)
[USA](#) [Weekendowa](#)
[Lektura](#) [wirus](#) [wpadka](#)
[wpadka](#) [tygodnia](#) [wyciek](#)
[włamanie](#)