Torrent z danymi Sony Pictures był wysyłany z serwerów PlayStation

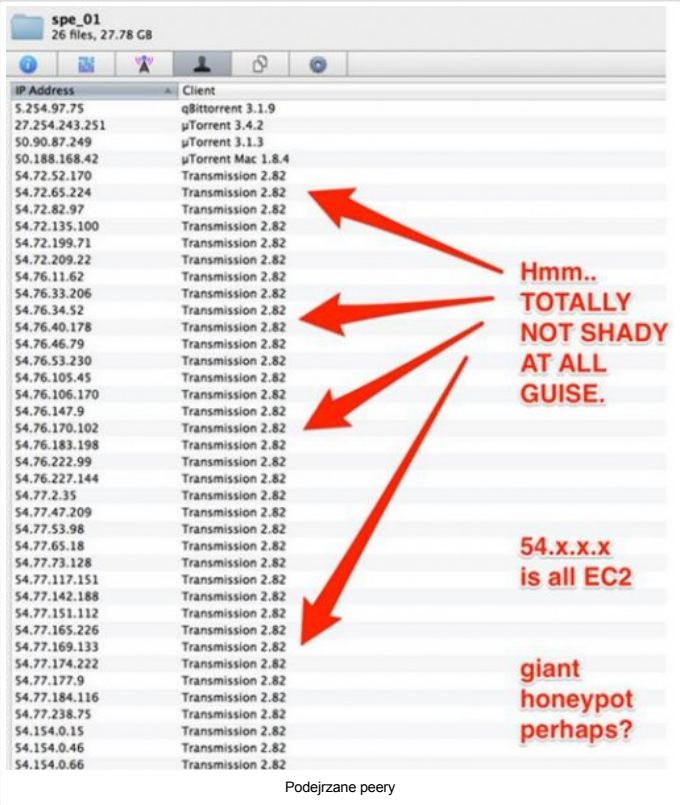
Adam dodał 3 grudnia 2014 o 10:36 w kategorii Włamania z tagami: PlayStation • Sony Pictures • torrent

Informacje dotyczące włamania do Sony Pictures nie przestają nas zadziwiać. Tym razem dowiadujemy się, że kilkadziesiąt komputerów biorących udział w rozpowszechnianiu wykradzionych danych przez protokół torrent należało do infrastruktury Sony.

Wczoraj informowaliśmy o udostępnieniu w sieci ponad 25GB danych należących do Sony Pictures. Jedną z form ich dystrybucji był protokół torrent. Osoby pobierające plik w pierwszych godzinach po jego publikacji zauważyły, że wśród udostępniających go komputerów znajduje się mnóstwo serwerów należących do Amazona. Co najmniej część z nich najwyraźniej należała do Sony.

To w ogóle nie wygląda podejrzanie

Przez pierwsze kilkanaście godzin od momentu udostępnienia torrenta na liście peerów (komputerów udostępniających i pobierających dane, z którymi można się połączyć, by pobrać od nich części pliku) znaleźć można było ponad 60 adresów należących do infrastruktury EC2 Amazona. Uwagę jednego z badaczy, Dana Tentlera, przyciągnął fakt, że wszystkie te serwery korzystały z tej samej wersji klienta torrent.



Podejrzane peery

Pierwsze teorie mówiły o honeypocie, którego zadaniem było zidentyfikowanie wszystkich adresów IP próbujących pobrać udostępnione dane. Kiedy jednak inny badacz, Dave

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 bolało – 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

Adres email zapisz

Wyszukiwanie

Szukasz czegoś? szukaj

Maynor, przeskanował powyższe adresy, znalazł tam sporą niespodziankę.

Sieć Sony PlayStation udostępnia dane Sony Pictures

Niektóre z adresów (na przykład 54.77.62.39) okazały się być serwerami WWW należącymi do PlayStation. Co więcej, nie były to tylko strony, które można skopiować z oryginału, ale serwery posiadały także certyfikaty SSL należące do Sony, które znacznie trudniej ukraść (choć pewnie w tym włamaniu wszystko było możliwe). Wszystko wskazuje jednak na to, że pliki serwowane były przez kilkanaście godzin (potem serwery zniknęły z listy peerów) z własnej infrastruktury Sony.

Czy mogła to być po prostu wyrafinowana pułapka? Jest to raczej mało prawdopodobne, ponieważ dane udostępniane w ten sposób faktycznie należały do Sony Pictures i było wśród nich wiele poufnych informacji. Nie spodziewamy się raczej, by firma była skłonna poświęcić swoje tajemnice dla takiego eksperymentu. Jakie zatem może być wytłumaczenie inne niż to, że włamywacze udowodnili w ten sposób fakt kontrolowania również konta Sony w serwisie Amazon? Ciągle szukamy odpowiedzi.

Podobne wpisy

- Z Sony Pictures wyciekają scenariusze, dane aktorów
- To będzie bolało – ponad 100 plików z tysiącami haseł Sony w sieci
- Ponad 30 tysięcy plików skradzionych Sony Pictures już w sieci

Komentarzy: 14

2014.12.03 11:44 x
Nie wiem, czy można mówić tu o poświęceniu. Dane i tak były publiczne, więc to ciągle może być honeypot. Albo bardzo, bardzo wielka wtopa.

Odpowiedz

2014.12.03 12:15 Jan
A może poprostu chcieli ściągnąć to archiwum i zobaczyć co w nim jest? A podczas ściągania automatycznie je udostępniali. Po ściągnięciu wyłączyli klienta i zniknęli z listy peerów

Odpowiedz

2014.12.03 12:53 Adam
Z 60 serwerów naraz? I to maszyn udostępniających inne usługi? :)

Odpowiedz

2014.12.03 13:47 Duży Pies
To zależy jak skonfigurujesz klienta torrentowego.
Możesz ustawić go tak, że tylko ściągasz, bez wysyłania (ratio 0) i wtedy nie mogą ci zarzucić że udostępniałeś pliki pochodzące z przestępczej działalności.
Poza tym, jak ktoś jest sprytny to będzie ściągał przez VPN, więc namierzenie będzie jeszcze trudniejsze, o ile w ogóle możliwe w przypadku naprawdę dobrego

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