**Popularność Gry o Tron wykorzystywana przez hakerów!**

**Mrok wreszcie się skończył. Fani Gry o Tron wreszcie mogą wyjść ze snu zimowego i podobnie jak głodny smok, zacząć pożerać finalny sezon popularnego serialu telewizyjnego. Jednak w przeciwieństwie do serii fantasy, o wiele bardziej realne są oszustwa phishingowe, z którymi spotykają się entuzjaści Gry o Tron.**

Choć podobnych oszustw było wiele - od złośliwego oprogramowania na pirackich stronach torrentowych, po oszustwa phishingowe - Check Point Research niedawno natknął się na najnowszą linię złośliwych działań zmierzających do wykorzystania niczego nie podejrzewających fanów. Przykładem może być witryna zachęcająca fanów GoT do udziału w konkursie, w którym nagrodą ma być paczka akcesoriów Gry o Tron. Nagrody jednak w rzeczywistości nie ma, a strona gromadzi dane e-mail i telefonów komórkowych, które mogą zostać wykorzystane w przyszłej kampanii spamującej.

przykład witryny phishingowej – gameofthronesratings[.]com

Inny przykładek, w którym nieuczciwe zbierane są danych o kartach kredytowych użytkowników, to strona podszywająca się pod oficjalny sklep Gry o Tron.

przykład witryny podszywającej się pod oficjalny sklep GoT – gameofthronesofficalshop[.]com

Wykorzystywanie dobrze rozpoznanych i zaufanych marek, takich jak m.in. Gra o Tron, jest coraz powszechniejszą metodą wykorzystywania użytkowników. Fałszywe strony internetowe wykorzystują popularność marki do wyświetlania reklam, pozyskiwania danych osobowych lub przekonywania użytkownika do zainstalowania niechcianego oprogramowania.

Ich cechą charakterystyczną są m.in. formularze pozyskujące dane czy transmisje strumieniowe, żądające od użytkownika pobrania dodatku do przeglądarki i podania danych osobowych, podczas gdy żadna treść nie jest wyświetlana na końcu procesu.

**Jak uniknąć bycia ofiarą phishingu?**

**Aby zminimalizować ryzyko ataku phishingowego Check Point rekomenduje kilka prostych zasad:**

1. Zastanów się przed kliknięciem. Kliknięcie na linki zaufanych stron powinno być całkowicie bezpieczne. Linki, które pojawiają się w przypadkowych wiadomościach e-mail i wiadomościach błyskawicznych, zwykle nie skończą się dobrze. Skierowanie kursora przed kliknięciem na link, którego nie jesteś pewien podpowie Ci, czy prowadzi do miejsca, którego się spodziewasz (adres odnośnika podawany jest zwykle na dole przeglądarki).

1. Upewnij się, że adres URL strony zaczyna się od "https", a w pobliżu paska adresu znajduje się ikona zamkniętego kłódki.

1. Sprawdzaj nazwę domeny witryny, którą spodziewasz się odwiedzić i zaufać. W przeciwnym wypadku możesz stać się następną ofiarą oszustwa phishingowego.