**ImageGate: Check Point ujawnia nową metodę na dystrybucję malware przez zdjęcia**

**Kilka dni temu świat obiegła informacja o atakach hakerskich dokonywanych za pomocą Facebooka z wykorzystaniem plików graficznych. Firma Check Point Software Technologies już jakiś czas temu zidentyfikowała podobny sposób dystrybucji malware!**

Firma Check Point poinformowała, że jej specjaliści ds. bezpieczeństwa zidentyfikowali nowy wektor ataku nazwany ImageGate, który pozwala osadzić złośliwe oprogramowanie w zdjęciach i plikach graficznych. Co więcej, badacze odkryli metodę hakerów na implementację złośliwego kodu w obrębie social mediów takich jak Facebook czy LinkedIn.

Według badań, napastnicy stworzyli nową metodę osadzenia złośliwego kodu i skutecznego umieszczenia zainfekowanych zdjęć na portale typu social media. Atakujący wykorzystują błąd konfiguracji infrastruktury portali w celu zmuszenia ofiary do pobrania zarażonego pliku graficznego, który infekuje urządzenie użytkownika bezpośrednio po kliknięciu w pobraną grafikę.

**W ostatnich trzech dniach cała branża bezpieczeństwa uważnie śledzi masowe rozprzestrzenianie się ransomware Locky przez media społecznościowe, a zwłaszcza w kampanii opartej o Facebooka. Badacze z firmy Check Point uważają, że technika ImageGate ujawnia w jaki sposób hakerzy mogli przeprowadzić ostatnią kampanię. Jak twierdzi Check Point zarówno Facebook jak i LinkedIn miał zostać poinformowany o nowym sposobie ataków na początku września, przy czym obie platformy miały zostać zaktualizowane.**

W przypadku ransomware Locky, kiedy użytkownik pobierze i otworzy zainfekowany, wszystkie pliki na urządzeniu osobistym są natychmiastowo szyfrowane, a dostęp do nich jest możliwy dopiero po opłaceniu okupu! Wydaje się, że kampania z użyciem Locky wciąż jest aktywna i gromadzi nowe ofiary każdego dnia.

*- Ponieważ coraz więcej ludzi spędza czas na portalach społecznościowych, hakerzy zwrócili się właśnie ku tym platformom* – twierdzi **Oded Vanunu**, szef działu firmy Check Point badającego podatności urządzeń na ataki*. -Cyberprzestępcy zrozumieli, że tego typu strony znajdują się zazwyczaj na „zaufanej liście” i z tego powodu opracowują coraz nowsze techniki użycia mediów społecznościowych jako pola do rozprzestrzeniania szkodliwego oprogramowania. Aby chronić użytkowników przed najbardziej zaawansowanymi zagrożeniami, badacze Check Pointa starają się określić gdzie napastnicy uderzą następnym razem.*

Check Point przedstawił również wizualizację tego typu ataku, która dostępna jest pod linkiem: <https://youtu.be/sGlrLFo43pY>

**Jak pozostać bezpiecznym? Check Point rekomenduje następujące kroki:**

1) Jeśli kliknąłeś w obrazek, a Twoja przeglądarka rozpoczyna ściąganie pliku, nie otwieraj go! Każdy portal społecznościowy powinien umożliwić wyświetlanie zdjęcia bez ściągania go.

2) Nie otwieraj zdjęć z dziwnym rozszerzeniem (np. SVG, JS czy HTA).

**Szczegóły techniczne ataku zostaną opublikowane przez firmę Check Point dopiero w momencie korekcji podatności w większości narażonych stron aby zapobiec wykorzystaniu tych informacji przez atakujących.**