Kolejne dokumenty Snowdena

19 lipca 2014

Brytyjska agencja szpiegowska opracowała szereg narzędzi do monitorowania, przeczesywania sieci, i w razie potrzeby umieszczania fałszywych informacji, stwierdził Glenn Greenwald podczas ujawniania nowych partii plików Snowdena.

Zgodnie z opublikowanymi dokumentami narzędzia zostały stworzone przez Joint Threat Research Intelligence Group (JTRIG) w ramach Government Communications Headquarters (GCHQ),

Poprzednie dokumenty szczegółowo wykazały wykorzystywanie przez JTRIG „fałszywych wiadomości na blogach", „operacji pod fałszywą flagą," jak również „honey traps"(uwodzicielskie spotkanie zaaranżowane w celu wydobycia informacji) oraz różne formy psychologicznej manipulacji użytkownikami internetu.

Niedawno wydany dokument GCHQ, zatytułowany „Narzędzia i techniki JTRIG", daje pełniejszy obraz skali operacji, w tym wskazując na to jak bardzo mogą być one inwazyjne i jakie mogą powodować spustoszenie w sieci.

Niektóre z narzędzi korzystają z tych samych metod, za które ścigano w USA i W. Brytanii działaczy online, w tym ataki typu „rozproszona odmowa usługi" i „call bombing".

Narzędzia dają szpiegom Cheltenham zdolność do aktywnego monitorowania wiadomości i połączeń Skype w czasie rzeczywistym, podnosząc te same, stare pytania o wiarygodność szyfrowania w Skype, i czy Microsoft w rzeczywistości współpracuje z agencjami szpiegowskimi.

W swoich notatkach w stylu przewodnika wiki, JTRIG mówi, że większość posiadanych narzędzi internetowych jest w „trybie operacyjnym, są przetestowane i wiarygodne" i wzywa kolegów z GCHQ by myśleli poza ramami, jeśli chodzi o internetowe

oszustwa. „Nie traktuj tego jak katalog. Jeśli nie widzisz tego tutaj, to nie znaczy, że nie można tego zbudować” stwierdza JTRIG.

Wśród narzędzi wymienionych w dokumencie jest „Gestator”, który zapewnia „wzmocnienie [dodanie liczby odwiedzin i promocja] danej wiadomości, zwykle wideo na popularnych stronach internetowych multimedialnych (YouTube).” Tymczasem, „Challenging” daje GCHQ możliwość podszywania się pod dowolny adres e-mail i wysłanie wiadomość pod tą tożsamością. “Angry Pirate” może trwale wyłączyć konto na komputerze zaatakowanej osoby. „Underpass” może zmienić wyniki sondaży internetowych, a „Deer Stalker” daje możliwość uzyskania wsparcia geolokalizacji telefonów satelitarnych i komórkowych GSM przez ich ciche wydzwanianie. Dokument JTRIG pojawił się w archiwum używanym przez GCHQ, omawiając internetowe działania w zakresie dozoru.

Ostatnia bomba informacyjna pojawiła się w tym samym momencie gdy brytyjski parlament debatuje nad przyspieszonym przyjęciem większego uzasadnienia dla olbrzymich uprawnień nadzoru agencji szpiegowskich, wobec czego premier David Cameron powiedział, iż jest to konieczne, aby „nas chronić.” GCHQ nie skomentowało artykułu i wydało zwykłą odpowiedź, a mianowicie, że działa „zgodnie ze ścisłymi ramami prawnymi i politycznymi” i podlega „intensywnemu nadzorowi.” Jednak poprzednie notatki GCHQ jakie wyciekły do Guardiana stwierdzały, że „naszym głównym problemem jest to, że odniesienia do praktyk biura (tj. skala przechwytywania i usuwania) może doprowadzić do niszczącej debaty publicznej, która może prowadzić do problemów prawnych w stosunku do obecnego systemu.”

Istnieje również możliwość, że najwyżsi ministrowie i urzędnicy w rządzie Wielkiej Brytanii nie są w pełni świadomi tego, co robi GCHQ. Chris Huhne, członek Rady Bezpieczeństwa Narodowego do 2012 roku, powiedział, że ministrowie są w „zupełnej ignorancji”, nawet wobec systemu „Tempora,” największego programu cyfrowego dozoru agencji szpiegowskiej.

Tymczasem brytyjska organizacja broniąca praw do prywatności Privacy International rozpoczęła działania prawne przeciwko GCHQ za wykorzystywanie złośliwego oprogramowania do szpiegowania użytkowników internetu i telefonów komórkowych.

Na podstawie: RT
Źródło: PrisonPlanet.pl