Data: 17 Grudnia, 2021
Sprawozdanie: Wykorzystanie systemu szpiegującego w stosunku do Romana Giertycha
Przygotowane przez: The Citizen Lab
Przygotowane dla: Romana Giertycha

Niniejsze sprawozdanie zostało przygotowane na prośbę i za zgodą Romana Giertycha. Potwierdza ono, że przeprowadzona przez nas analiza kryminalistyczna cyfrowych śladów z urządzenia Apple Romana Giertycha ("urządzenie Romana Giertycha") wskazuje, że telefon będący w jego posiadaniu został zainfekowany oprogramowaniem szpiegującym Pegasus, wyprodukowanym przez NSO Group.

Kontekst

Citizen Lab to interdyscyplinarne laboratorium działające w Munk School of Global Affairs & Public Policy na Uniwersytecie w Toronto, koncentrujące się na badaniach, rozwoju i strategicznym zaangażowaniu polityczno-prawnym w zakresie technologii informacyjno-komunikacyjnej, prawach człowieka i bezpieczeństwu światowym.

Badania Citizen Lab dotyczą przede wszystkim identyfikacji przestępstw cyfrowych, a także monitorowania zagrożeń związanych z funkcjonowaniem oprogramowań szpiegowskich. W ramach badań nad oprogramowaniami szpiegowskimi, Citizen Lab opracowało metodę identyfikacji śladów cyfrowych, będących pozostałością po zhakowaniu danego urządzenia oprogramowaniem szpiegowskim Pegasus.

Potwierdzenie zainfekowania urządzenia należącego do Romana Giertycha - oprogramowaniem szpiegującym Pegasus należącym do firmy NSO Group's

Badacze Citizen Lab przeanalizowali ślady kryminalistyczne z urządzenia Romana Giertycha i uzyskali pozytywny wynik dla oprogramowania szpiegującego Pegasus. Dokładna inspekcja wykazała, że urządzenie Romana Giertycha zostało przywrócone z poprzedniego iPhone'a. W procesie przywracania urządzenia wykorzystano wskaźniki wysokiego poziomu ufności, wskazujące na to, że poprzedni iPhone był wielokrotnie zainfekowany oprogramowaniem szpiegowskim firmy NSO Group tj Pegasus.

Pan Roman Giertych poinformował nas, że powodem zmiany telefonu było to, że poprzednie urządzenie przestało normalnie funkcjonować i obecnie jest niefunkcjonalne.

Materiał dowodowy wykazał, że stary telefon, który posiadał, był zainfekowany oprogramowaniem szpiegującym Pegasus w następujących okresach czasu:

1. W dniu lub około 2019-09-05
2. W dniu lub około 2019-09-11
3. W dniu lub około 2019-09-12 r.
4. W dniu lub około 2019-09-13 r.
5. W dniu lub około 2019-09-16 r.
6. W dniu lub około 2019-09-22
7. W dniu lub około 2019-09-23
8. W dniu lub około 2019-09-24
9. W dniu lub około 2019-09-25 r.
10. W dniu lub około 2019-09-29 r.
11. W dniu lub około 2019-09-30 r.
12. W dniu lub około 2019-10-01
13. W dniu lub około 2019-10-04
14. W dniu lub około 2019-10-21 r.
15. W dniu lub około 2019-10-22
16. W dniu lub około 2019-11-18
17. W dniu lub około 2019-11-22
18. W dniu lub około 2019-12-04

Co nie wyklucza prawdopodobieństwa zainfekowania telefonu także w innych okresach.

Z czym wiąże się udana infekcja oprogramowaniem szpiegowskim Pegasus ?

Pegasus to narzędzie do inwigilacji, które zapewnia swojemu operatorowi pełny dostęp do inwigilowanego urządzenia mobilnego. Pegasus pozwala operatorowi na wydobycie haseł, plików, zdjęć, historii sieci, kontaktów, a także danych dotyczących tożsamości (takich jak informacje o urządzeniu mobilnym).

Pegasus może wykonywać zrzuty ekranu i monitorować polecenia użytkownika, a także aktywować mikrofon i kamerę telefonu. Dzięki temu atakujący mogą monitorować całą aktywność na urządzeniu i w jego pobliżu, np. rozmowy prowadzone w pomieszczeniu.

Pegasus pozwala również operatorowi na nagrywanie wysyłanych i odbieranych wiadomości czatu (w tym wiadomości wysyłanych za pośrednictwem aplikacji do wysyłania wiadomości tekstowych z funkcją "szyfrowania"/znikających wiadomości, takich jak WhatsApp czy Telegram), a także rozmów telefonicznych i VoIP (w tym rozmów za pośrednictwem "szyfrowanych" aplikacji do wykonywania połączeń).

Grafika pokazująca niektóre z elementów, które Pegasus może monitorować na urządzeniu celu. ***Źródło:*** *Materiały firmy NSO*

W przypadku niektórych programów czatowych, Pegasus umożliwia również ekstrakcję dzienników wiadomości z przeszłości. Pegasus pozwala również operatorowi na śledzenie lokalizacji celu. Tak jak w przypadku każdej infekcji, oprogramowanie szpiegujące może również umożliwiać modyfikację lub manipulację danymi na urządzeniu.

Więcej informacji na temat NSO Group i jej oprogramowaniu szpiegującym Pegasus

Oprogramowanie szpiegujące Pegasus jest sprzedawane i wprowadzane na rynek przez NSO Group (która występuje pod nazwą Q Cyber Technologies, jak również pod innymi nazwami). NSO Group jest firmą z siedzibą w Izraelu, która opracowuje i sprzedaje technologie szpiegowskie w tym Pegasus. NSO Group jest w większości własnością Novalpina Capital, europejskiej firmy private equity z siedzibą w Londynie.

NSO Group twierdzi, że sprzedaje swoje oprogramowanie szpiegowskie wyłącznie klientom rządowym oraz że cały eksport odbywa się zgodnie z przepisami eksportowymi rządu izraelskiego i mechanizmami nadzoru. NSO Group twierdzi również, że przestrzega polityki w zakresie praw człowieka. Jednak liczba udokumentowanych przypadków, w których ich technologia jest wykorzystywana do nadużyć wymierzonych w społeczeństwo obywatelskie stale rośnie.

Z badaniami Citizen Lab dotyczącymi NSO Group można zapoznać się na tej stronie: *https://citizenlab.ca/tag/nso-group/*