Tajemnice Pegasusa

Minęły już czasy, gdy do znacznej części komputerów na świecie można było się włamać po przejrzeniu paru forów. Obecnie komputery i komórki mają wiele warstw zabezpieczeń, oprogramowanie jest zwykle aktualizowane na bieżąco, a aktualizacje zamykają znane producentom luki bezpieczeństwa. Wiedza o luce bezpieczeństwa w najnowszej wersji oprogramowania (tzw. exploit „zero-day") ma swoją wartość. Można (często za nagrodą) poinformować producenta i po poprawieniu opublikować ją dla sławy, ale można też wykorzystać po cichu, aby producent się nie dowiedział. Włamanie na telefon, wydobycie informacji, ukrycie śladów jest coraz trudniejsze technicznie, więc jest miejsce dla usługi, która wykona wszystko za użytkownika. Czymś takim zapewne jest Pegasus.

Oczywiście nie ma publicznych, wyczerpujących informacji, czym jest Pegasus. Są jednak pewne szczątkowe informacje ([1], [2], [3]), z których, choć nie jestem specjalistą w tym temacie, mogę spróbować zrekonstruować pewien obraz.

Podstawą działania jest rozpoznanie przez producentów Pegasusa wielu luk w zabezpieczeniach telefonów. W [1] są opisane trzy błędy, które zdzierają, jedna po drugiej, warstwy bezpieczeństwa iPhone'a i zastosowane razem powodują, że kliknięcie na link w SMS-ie skutkuje włamaniem do telefonu i w rezultacie przy każdym włączeniu telefonu uruchamia się oprogramowanie szpiegowskie, które ma dostęp do całego telefonu, łącznie z tzw. jądrem systemu.

Z opisu wynika, że po otrzymaniu informacji o lukach, Apple w 10 dni przygotował aktualizację systemu, która je wszystkie zamyka. Jednak nie słychać, aby producent Pegasusa zawiesił z tego powodu działalność. Zapewne ma długą listę rezerwową luk i zaczął korzystać z innych. Co więcej, w 2019 roku Pegasus poprawił technikę na iPhone'ach z „1-click" na „0-click" – już nie trzeba klikać w link w SMS-ie, tylko włamanie następuje poprzez komunikat iMessage bez wiedzy użytkownika.

Wszystkie materiały opisują włamania do iPhone'ów, ale należy oczekiwać, że Pegasus podobnie potrafi rozbrajać kolejne warstwy zabezpieczeń w telefonach z Androidem *

Kolejnym elementem Pegasusa jest starannie napisane oprogramowanie do wykorzystywania tych luk i gotowa infrastruktura. Materiały sugerują, że linki we wspomnianych SMS-ach prowadzą do serwerów utrzymywanych przez producenta Pegasusa, więc klient Pegasusa nie musi mieć wiedzy, jak je konfigurować – zapewne tylko wpisuje numer telefonu do zaatakowania w jakieś aplikacji.

Autorów raportu zaskoczyło, że:

- Pegasus wykrywa, czy ktoś inny nie próbuje się włamać do telefonu. – w takiej sytuacji sam się kasuje, aby pozostał niezauważony.
- Pegasus włamuje się do telefonu po każdym włączeniu, więc jakiś błąd w tej procedurze może spowodować, że telefon się nie będzie włączać. Pegasus próbuje jednak wykryć takie sytuacje i wtedy też woli się skasować, niż spowodować, że właściciel zaniesie telefon do serwisu.
- Gdyby ktoś wyłączył serwery, na których Pegasus szuka poleceń, jakie dane zbierać, istnieje opcja wysłania SMS-a, wyglądającego jak SMS od Google'a czy Facebooka, który zabłądził, ale w rzeczywistości jest rozkazem dla Pegasusa, aby zaczął używać innych serwerów.

Dochodzimy tu do kolejnej cechy Pegasusa – jest on opisywany przez producenta jako system nie do wykrycia. Traktowałbym to jednak podobnie jak zapewnienia Apple'a, że iPhone jest najbezpieczniejszym telefonem i nie da się do niego włamać – na pewno włożono wiele wysiłku, aby tak było, zapewne amator niczego nie zauważy, ale ktoś, kto włoży odpowiednio dużo pracy, zapewne coś znajdzie. I tak z [2] dowiadujemy się, że:

- Pegasus usuwa z historii przeglądarki WWW strony użyte do włamania, ale pozostawia sygnał, który umożliwia wykrycie, że przeglądarka odwiedziła tę stronę (informację o ikonce tej strony).
- W statystykach zużycia Internetu przez poszczególne procesy (zbieranych przez telefon, aby wyświetlić podsumowanie, która aplikacja spowodowała zużycie pakietu) pozostają ślady procesów Pegasusa.

Oczywiście, skoro stało się to publiczne, należy sądzić, że nowe wersje Pegasusa nie zostawiają tych śladów. Można nawet wyobrazić sobie kampanię włamań do telefonów ze starym Pegasusem, aby zatrzeć te ślady. Jednak pewnie da się znaleźć inne ślady (tak jak Pegasus znajduje inne luki bezpieczeństwa, gdy te stare są usuwane przez producentów telefonów).

Następnym elementem Pegasusa jest zbieranie danych z telefonu i wysyłanie ich na serwery. Wydaje się, że podobnie do serwerów, z których Pegasus przychodzi, są to również serwery zarządzane przez producenta Pegasusa, więc użytkownik nie musi mieć umiejętności w tym zakresie (taki układ dawałby też twórcom Pegasusa możliwość techniczną wykonania kopii).

Telefony zawierają bariery, aby jedna aplikacja nie mogła zaglądać do danych innych aplikacji. Jednak, jeżeli program zdołał wejść tak głęboko w system jak Pegasus (dostęp do jądra systemu), to te ograniczenia nie obowiązują. Pegasus jest ograniczony jedynie tym, jakie aplikacje jego producent rozpracował.

W raporcie [1] jest opisane ściąganie wszystkich danych z kalendarza, kontaktów, historii połączeń, SMS-ów i wiadomości wielu popularnych komunikatorów (np. iMessage, Facebook Messenger, również tych dobrze szyfrowanych, jak Telegram), lokalizacji GPS, wszystkich haseł do sieci WiFi oraz haseł do zmiany konfiguracji routerów. Jest również opisana zapewne najsłynniejsza funkcja programu, czyli zdalne włączenie mikrofonu lub kamery. Aby utrudnić wykrycie swego działania, program zapewne wysyła te dane tylko wtedy, gdy jest odpowiednio szybkie łącze internetowe i dodatkowy strumień danych nie zrobi zauważalnej różnicy.

Są to dane z 2016 roku, więc nie wiadomo, co Pegasus potrafi teraz. Teoretycznie program, który wszedł tak głęboko w system, może podejrzeć lub zmienić wszystko, co dzieje się na telefonie. Na przykład:

- Podejrzeć hasła wpisane w przeglądarkę internetową czy w aplikacje, nawet jeżeli prosiliśmy, aby nie były zapisywane.
- Jeżeli ktoś jest zalogowany z telefonu do banku, pogram może udawać, że został naciśnięty przycisk, aby przejrzeć historię transakcji, ale nie wyświetlić wyniku, tylko przesłać go na serwer Pegasusa.
- Jeżeli ktoś wyłączy telefon, to można tylko wyświetlić animację wyłączającego się telefonu, ale w rzeczywistości nie wyłączyć go, tylko kontynuować nagrywanie.

Są to wszystko funkcje hipotetyczne i wymagające wysiłku. W przypadku profesjonalnego programu są to jednak przykłady działań, których nie możemy wykluczyć.

Być może dobrą wiadomością jest to, że telefon chyba nie jest w stanie nagrywać przez 24 godziny na dobę bez rozładowywania baterii w tempie zauważalnym przez użytkownika (choć nie jestem tego pewien wobec dużych baterii w nowych telefonach). Jest jednak technicznie możliwe automatyczne włączanie nagrywania w wielu sytuacjach. Hipotetyczne przykłady to wykorzystanie energooszczędnych procesorów obecnych w niektórych telefonach, które cały czas nasłuchują mikrofonu aby wychwytywać frazy w rodzaju „OK, Google", lub „Hey, Siri". Zapewne można je (sporym wysiłkiem) przeprogramować, aby wychwytywały inne słowa kluczowe lub określoną barwę głosu i włączały wtedy nagrywanie. Inną energooszczędną możliwością jest monitorowanie pozycji GPS i włączanie nagrywania, gdy telefon znalazł się w jakimś ciekawym obszarze.

Ostatnim elementem systemu jest zapewne zestaw serwerów, które zbierają informacje. Tu z analiz programów znalezionych na telefonach zapewne nigdy się nie dowiemy, czy system tylko przesyła wszystkie zebrane informacje do zleceniodawcy, czy też zawiera jakieś zaawansowane narzędzia wyszukiwania w ogromie danych, które zebrał, a może też ich automatycznej analizy.

Czy Pegasus jest wyjątkowy? To już jest obszar czystych spekulacji, ale sądziłbym, że jeżeli ktoś zaszedł za skórę CIA lub wywiadowi chińskiemu, to powinien się liczyć z co najmniej równie zaawansowanymi programami. Na przykład w 2017 roku wyciekło ponad 500 luk wykorzystywanych przez CIA, w tym 91 aktualnych ([4]). Jednak nowość Pegasusa może polegać na tym, że zostało stworzone narzędzie z myślą o używaniu przez niezbyt zaawansowane technicznie służby, które daje możliwości dostępne wcześniej tylko nielicznym. Z czasem, dzięki stałemu napływowi gotówki od wielu rządów, może też stać się najlepiej dopracowanym programem tego typu.

MIKOŁAJ ZALEWSKI

* Ostatnio, ale już po napisaniu tego artykułu, pojawiły się doniesienia o technikach włamywania na telefony z Androidem.

[1] https://info.lookout.com/rs/051-ESQ-475/images/lookout-pegasus-technical-analysis.pdf
[2] https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/
[3] https://googleprojectzero.blogspot.com/2021/12/a-deep-dive-into-nso-zero-click.html
[4] https://en.wikipedia.org/wiki/Vault_7