# 1. Experts Detail Multi-Million Dollar Licensing Model of Predator Spyware

Nowa analiza wyrafinowanego komercyjnego oprogramowania szpiegującego o nazwie Predator ujawniła, że jego zdolność do utrzymywania się między ponownym uruchomieniem jest oferowana jako „funkcja dodatkowa” i że zależy od opcji licencjonowania wybranych przez klienta.

„W 2021 r. Predator Spyware nie mogli przetrwać ponownego uruchomienia w zainfekowanym systemie Androida (miał go na iOS)”, powiedzieli badacze Cisco Talos Mike Gentile, Asheer Malhotra i Vitor Ventura w raporcie udostępnionym z Hacker News.„Jednak do kwietnia 2022 r. Ta zdolność była oferowana swoim klientom”.

Predator jest produktem konsorcjum o nazwie Intellexa Alliance, które obejmuje Cytrox (następnie nabyty przez Wispear), NEXA Technologies i SenPai Technologies.Zarówno CYTROX, jak i Intellexa zostały dodane do listy jednostek przez USA w lipcu 2023 r. W celu „Handlu w cyberprzestrzeni używanych do uzyskania dostępu do systemów informatycznych”.

Najnowsze ustalenia pojawiają się ponad sześć miesięcy po tym, jak dostawca bezpieczeństwa cybernetycznego szczegółowo opisał wewnętrzne działanie drapieżników i jego harmonijne równanie z innym komponentem ładowarowym o nazwie Alien.

„Obcy ma kluczowe znaczenie dla udanego funkcjonowania Predatora, w tym dodatkowych komponentów załadowanych przez Predatora na żądanie”, powiedział Malhotra w tym czasie Hacker News.„Związek między kosmitą a drapieżnikiem jest niezwykle symbiotyczny, wymagając od nich ciągłej pracy w tandemie szpiegowania ofiar”.

Tradycyjne środki bezpieczeństwa nie zmniejszą tego w dzisiejszym świecie.Czas na zerowe bezpieczeństwo zaufania.Zabezpiecz swoje dane, jak nigdy dotąd.

Predator, który może celować zarówno na Android, jak i iOS, został opisany jako „zdalny system ekstrakcji mobilnej”, który jest sprzedawany w modelu licencyjnym, który zawiera miliony dolarów na podstawie exploita używanego do początkowego dostępu i liczby jednoczesnych infekcji, umieszczając jepoza zasięgiem skryptowych dzieciaków i początkujących przestępców.

Oprogramowanie szpiegujące, takie jak Predator i Pegasus, które są opracowywane przez NSO Group, często polegają na łańcuchach zero-day exploit w Android, iOS i przeglądarkach internetowych jako tajne wektory włamań.Ale ponieważ Apple i Google nadal zatrzymują luki w bezpieczeństwie, te łańcuchy exploit mogą być nieskuteczne, zmuszając je do powrotu do deski kreślarskiej.



Warto jednak zauważyć, że firmy stojące za narzędziami do nadzoru najemników mogą również pozyskiwać pełne lub częściowe łańcuchy exploit od brokerów exploit i wprowadzić je do operacyjnego exploit, który można wykorzystać do skutecznego naruszenia urządzeń docelowych.

Kolejnym kluczowym aspektem modelu biznesowego Intellexa jest to, że rozładowuje pracę polegającą na konfigurowaniu infrastruktury ataku samym klientom, pozostawiając ją z miejsca na prawdopodobną zaprzeczenie, jeśli kampanie wyjdą na jaw (jak nieuchronnie).

„Dostarczanie sprzętu wspierającego Intellexa odbywa się na terminalu lub lotnisku” - powiedzieli naukowcy.

„Ta metoda dostawy jest znana jako ubezpieczenie kosztów i frachtu (CIF), które jest częścią żargonu przemysłu żeglugowego („ incoterms ”). Ten mechanizm pozwala Intellexa twierdzić, że nie mają one widoczności, gdzie systemy są wdrażane i ostatecznie zlokalizowane."



Ponadto Intellexa posiada „wiedzę z pierwszej ręki” o tym, czy ich klienci wykonują operacje nadzoru poza własnymi granicami ze względu na fakt, że operacje są wewnętrznie podłączone do licencji, która domyślnie ogranicza się do jednego telefonuPrefiks kodu kraju.

To ograniczenie geograficzne można jednak poluzować za dodatkową opłatą.

Cisco Talos zauważył, że chociaż publiczne narażenie ofensywnych aktorów i ich kampanii odniosło sukces w zakresie przypisywania, miało to niewielki wpływ na ich zdolność do prowadzenia i rozwijania działalności na całym świecie, nawet jeśli może to wpłynąć na ich klientów, takiego, takiego, takiego, takiego.jako rządy.

„Może to zwiększyć koszty, powodując, że kupują lub tworzą nowe łańcuchy exploit, ale dostawcy ci wydają się bezproblemowo nabywać nowe łańcuchy exploit, umożliwiając im pozostanie w biznesie, przeskakując z jednego zestawu exploitów na inny jako sposób początkowego dostępu”, ”Naukowcy powiedzieli.

Link: <https://thehackernews.com/2023/12/multi-million-dollar-predator-spyware.html>