DosintoS

System do kontrolowania zdalnego i gromadzenia danych jako wektor ataku.
Sterowanie botnetem za pomocą steganografii w aplikacjach mobilnych.

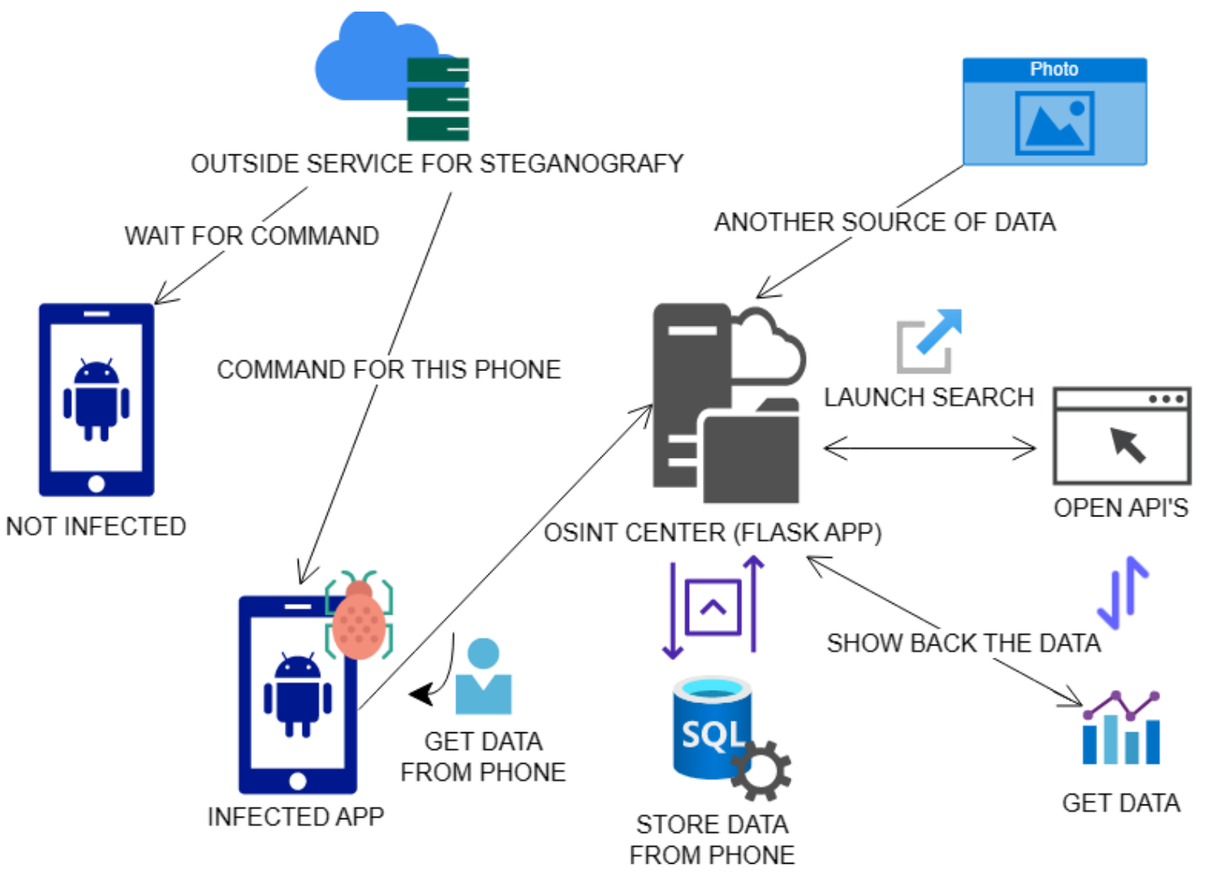
Antonio Rodriguez-Magierowski (antrod@amu.edu.pl)
Kacper Koziełło (kackoz3@st.amu.edu.pl)
24.01.2023, Poznań, Polska

Uniwersytet im. Adama Mickiewicza w Poznaniu

Streszczenie

W ramach przedmiotu realizowanego w związku z projektem "Akademia Innowacyjnych Zastosowań Technologii Cyfrowych" chcemy stworzyć aplikację na system Android 11 oraz starsze, która będzie zbierała dane użytkownika, który ją zainstaluje. Celem jest stworzenie centrum OSINT'owego (open-source intelligence) wykorzystującego steganografię. Będzie to serwis składający się z aplikacji webowej, gdzie można dokonać poszczególnych akcji zdalnie (command&control).
Aplikacja mobilna powinna pytać o jak najmniejszą ilość potrzebnych uprawnień i powinno to być przeprowadzane w sposób uzasadniony, aby użytkownik nie nabrał podejrzeń. W tym celu chcemy stworzyć aplikację, która będzie wykorzystywała dostęp do aparatu i galerii (na przykład czytnik plików PDF).

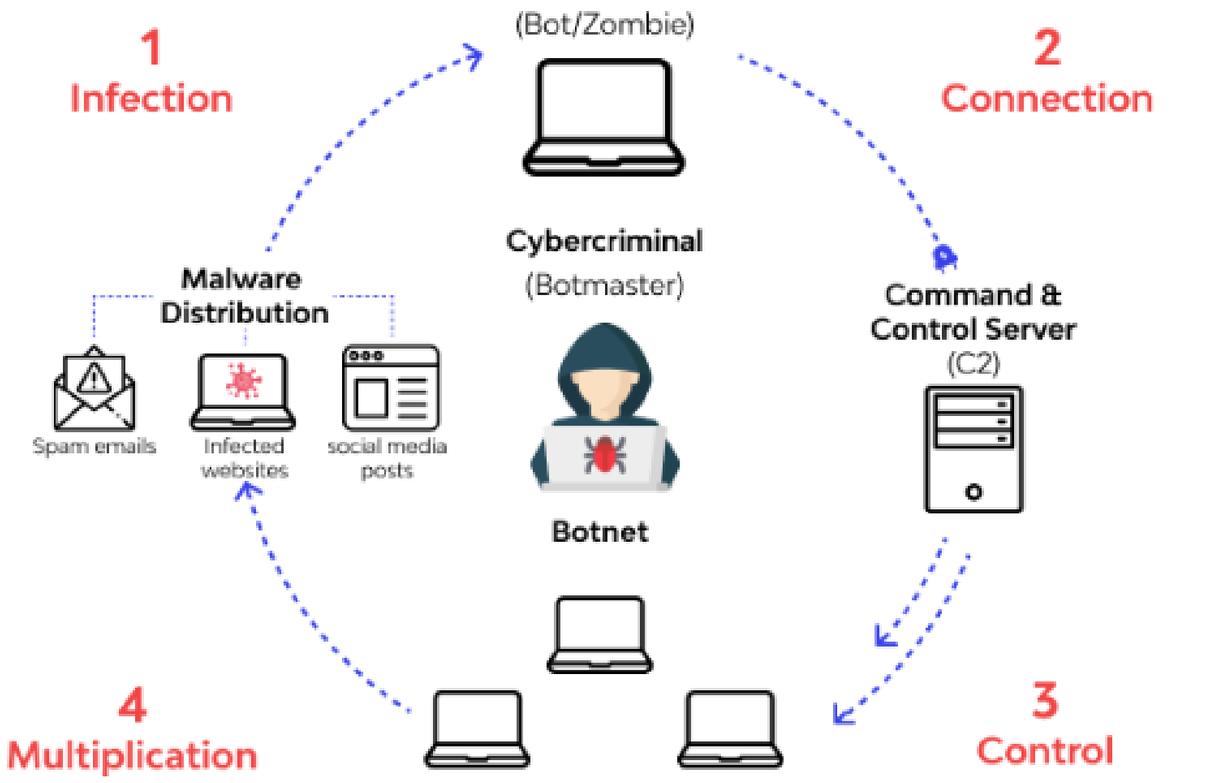
Centrum OSINT'owe



Statystyki

- System Android obsługuje blisko 72.5% wszystkich smartfonów. Dostępne dane z cutoff 2021 pokazują, że ponad 60% użytkowników Androida korzysta z wersji 10 lub niższej.
- W USA w 2021 roku wyciekły dane 212,4 mln użytkowników.
- W pierwszych sześciu miesiącach 2019 roku ponad 3800 ujawnionych publicznie wycieków zawierało ponad 4 miliardy rekordów danych. (Forbes)
- Średni czas identyfikacji naruszenia bezpieczeństwa wynosi 279 dni. (IBM)
- Każdego dnia w wyniku wycieku danych ujawniane jest 780 000 rekordów z danymi użytkowników. (McAfee)
- Naukowcy z Międzynarodowego Instytutu Informatyki odkryli blisko 1325 aplikacji na Androida, które zbierały dane z urządzeń nawet po tym, jak użytkownicy wyraźnie odmówili im pozwolenia.

Jak działa Botnet?



Funkcjonalności systemu

Wyszukiwanie podstawowych informacji o użytkowniku (adres e-mail, numer telefonu, imię, nazwisko, data urodzenia) za pomocą:

- Google Dorks (gotowej bazy zapytań do przeglądarki),
- Linkedin + Outlook,
- Facebook, Instagram.

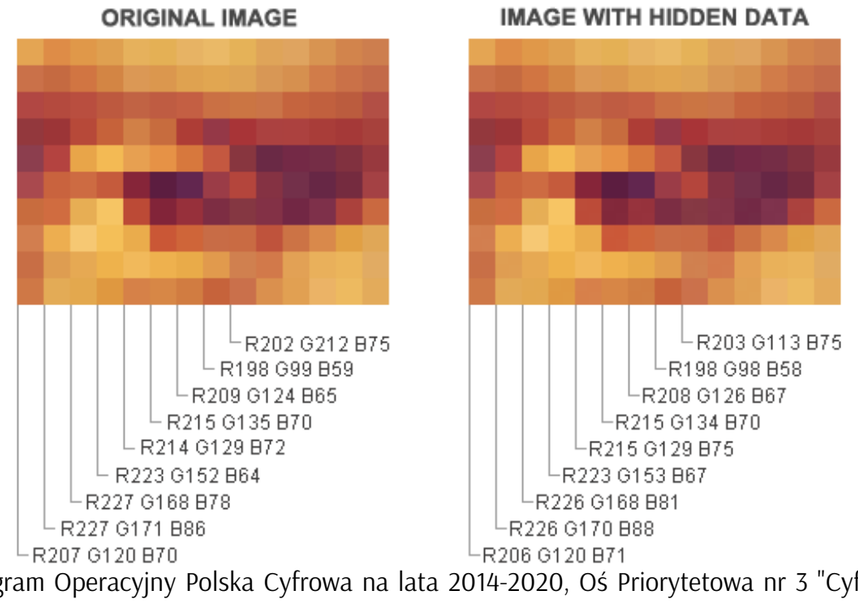
Określenie geolokalizacji urządzenia dzięki:

- wykorzystaniu metadanych zdjęć,
- IpLogger - uzyskanym za pomocą podstawowego żądania.

Co więcej, w przyszłości planowane są rozszerzenia takie jak: przechwytywanie ekranu, keylogger czy overlay do podmiany stron internetowych.

Steganografia

Steganografia jest niewidoczną wymianą informacji między nadawcą i adresatem. Dzięki zastosowaniu steganografii można ukryć informacje we wszelkiego rodzaju plikach. Obecnie najpopularniejszą techniką jest ukrywanie danych w plikach graficznych.
W 2017 roku pod zdjęciami na instagramowym koncie Britney Spears pojawiały się komentarze o podejrzanej treści. Okazało się to sprytną strategią ogłaszania lokalizacji nowego serwera dowodzenia i kontroli przez rosyjskich hackerów. Po zdekodowaniu był to w rzeczywistości adres internetowy serwera.



Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Rozwoju Regionalnego Program Operacyjny Polska Cyfrowa na lata 2014-2020, Oś Priorytetowa nr 3 "Cyfrowe kompetencje społeczeństwa" Działanie nr 3.2 "Innowacyjne rozwiązania na rzecz aktywizacji cyfrowej". Tytuł projektu: „Akademia Innowacyjnych Zastosowań Technologii Cyfrowych (AI Tech)" Porozumienie nr POPC.03.02.00-00-0001/20-00