Słoweńskie władze, we współpracy z FBI, aresztowały 23-latka znanego pod internetowym pseudonimem „Iserdo", oskarżonego o tworzenie złośliwego oprogramowania i sprzedawanie go cyberprzestępcom. Zestaw Butterfly, który tworzył mężczyzna, to złośliwe oprogramowanie stanowiące podstawę botnetu Mariposa i setek innych botnetów kradnących informacje. W sumie zainfekowały one miliony komputerów na całym świecie: banki, agencje rządowe i firmy w ponad 200 krajach, w tym w Polsce.

Firmy Panda Security i kanadyjska firma Defence Intelligence dostarczyły FBI oraz międzynarodowym władzom kluczowe informacje, które doprowadziły do schwytania 23-letniego „Iserdo", potwierdzonego autora zestawu Butterfly do budowy sieci botnet. Wraz z partnerami z Grupy Roboczej Mariposa obie firmy z branży zabezpieczeń zidentyfikowały Iserdo poprzez analizę oprogramowania botnetu Mariposa, który zainfekował miliony systemów na świecie. Iserdo został aresztowany pod koniec lipca w Mariborze w Słowenii i obecnie przebywa na wolności za kaucją.

Mariposa i inne botnety kradnące informacje są tworzone przy pomocy pakietów złośliwego oprogramowania takich jak zestaw Butterfly. Butterfly sprzedawany w internecie w cenie od 500 do 1500 euro (650-2000 USD) umożliwia osobom o ograniczonych umiejętnościach komputerowych dokonywanie przestępstw na masową skalę. Zestaw posłużył do stworzenia blisko 10 tys. unikalnych złośliwych programów i ponad 700 botnetów. Wśród ofiar znajdują się setki instytucji finansowych, resortów rządowych, a także miliony prywatnych firm i osób na całym świecie. Polska znalazła się na 27 miejscu na liście zainfekowanych krajów z poziomem zarażenia - 0,73%.

„W ciągu ostatnich dwóch lat oprogramowanie użyte do stworzenia botnetu Mariposa zostało sprzedane setkom innych przestępców, co uczyniło je jednym z najpopularniejszych na świecie" - powiedział dyrektor FBI, Robert S. Mueller, III. „Te cyber-włamania, kradzieże i oszustwa podkopują bezpieczeństwo internetu i firm, które są od niego uzależnione; zagrażają również prywatności i portfelom wszystkich użytkowników internetu".

Defence Intelligence i Panda Security monitorowały zestaw Butterly przez prawie dwa lata. Jego ofiarami padły instytucje finansowe, agencje rządowe i firmy w ponad 200 krajach.

„Ekscytujące w tych aresztowaniach jest to, że po raz pierwszy udało się namierzyć twórców. Zwykle ujmowani są operatorzy botnetów, a schwytanie autora zestawu stanowiącego podstawę botnetu jest bardzo rzadkie", powiedział Christopher Davis, prezes Defence Intelligence. Firma ma nadzieję, że te aresztowania staną się precedensem i ostrzeżeniem dla innych. Davis dodaje: „Musimy ścigać ich wszystkich – ludzi, którzy piszą kod, tych którzy go sprzedają, rozpowszechniają, nawet tzw. słupy wykorzystywane do zamiany skradzionych kart kredytowych i danych bankowych na gotówkę".

„Jesteśmy niezwykle dumni z udziału w stale podejmowanych wysiłkach w celu zwalczania cyberprzestępców takich jak Iserdo, ale wiemy, że to tylko jeden z wielu cyberprzestępców i wiele jest jeszcze do zrobienia" - powiedział Juan Santana, prezes Panda Security. „W Panda Security jesteśmy przekonani, że walka z przestępczością internetową wymaga międzynarodowej współpracy między branżą zabezpieczeń komputerowych i instytucjami publicznymi. Musimy wspólnie pracować nad zwiększeniem wiedzy społeczeństwa na temat zagrożeń oraz domagać się wprowadzenia odpowiednich przepisów, które będą stanowić podstawę wymierzania kar zniechęcających do działań przestępczych. Dodatkowo, powinno się zapewnić właściwe przeszkolenie takim zespołom jak Grupa Robocza Mariposa w celu opracowania odpowiednich technologii zapobiegawczych i zaradczych, które umożliwią skuteczne ściganie przestępców".

Jeffrey Troy, zastępca dyrektora działu cyberprzestępczości FBI ujął to tak: „w odróżnieniu od aresztowania faceta, który włamał się do państwa domu, my aresztowaliśmy faceta, który dał mu łom i mapę z najlepszymi domami w okolicy. I to jest ogromny przełom w śledztwie dotyczącym cyberprzestępstw".

W ciągu ostatnich siedmiu miesięcy Grupa Robocza Mariposa przyczyniła się do aresztowania pięciu cyberprzestępców i zlikwidowała jeden z największych botnetów na świecie - Mariposa. Obecnie Defence Intelligence przekierowuje setki botnetów do sieci zbiorczych, które blokują ich rozpowszechnianie i ułatwiają analizę. „Dziesiątki milionów unikalnych adresów IP kontaktują się z nami zamiast z przestępcami” - mówi Matt Thompson, główny naukowiec Defence Intelligence. Przewidywane są kolejne aresztowania w miarę namierzania użytkowników zestawu Butterfly.

Panda Security