Badacze na tropach cyfrowego atramentu sympatycznego

Aby poufnej informacji nie wykryły niepowołane osoby, można ją spróbować ukryć w innej wiadomości. Dawniej w takiej ukrytej komunikacji stosowano np. atrament sympatyczny, a dziś stosuje się bardziej zaawansowane metody cyfrowe. Badają je steganografowie z Zakładu Cyberbezpieczeństwa w Instytucie Telekomunikacji na Politechnice Warszawskiej.

Niewinnie wyglądająca wiadomość nie zawsze jest taka niewinna. Czasami są w niej ukryte dodatkowe informacje, o których istnieniu wie tylko nadawca i odbiorca. Dawniej wiadomości ukrywano np. we wnętrznościach podarowanego adresatowi zwierzęcia. Znanym ze starożytności pomysłem było też tatuowanie wiadomości na ogolonej głowie posłańca (po odrośnięciu włosów informacja przestawała być widoczna). Nauka, która zajmuje się takimi ukrytymi informacjami to steganografia.

Przez wieki popularną metodą steganograficzną było też stosowanie atramentu sympatycznego (np. pisanie w zwykłym liście poufnych informacji mlekiem czy sokiem z cytryny; schowane wiadomości ukazywały się oczom odbiorcy dopiero po podgrzaniu papieru). Czasem z kolei informację można było odnaleźć, czytając tylko co którąś literę listu.

Dziś ze steganografii korzysta się np. w komunikacji militarnej, w szczególności - w komunikacji między szpiegami. Korzystają z niej również dziennikarze czy grupy aktywistów w miejscach, gdzie jest cenzura i nie wszystkie informacje można przekazywać otwartymi kanałami. Przestępcy z kolei ze steganografii korzystają np. do wykradania poufnych informacji z firm czy do sterowania botnetami (czyli zainfekowanymi komputerami). "Wiele nowoczesnych ataków bazuje na takich technikach" - przyznał w rozmowie z PAP szef projektu stegano.net, dr hab. inż. Krzysztof Szczypiorski, profesor nadzwyczajny w Zakładzie Cyberbezpieczeństwa w Instytucie Telekomunikacji na Politechnice Warszawskiej. Dodał, że prawdopodobnie ze steganografii korzystali np. terroryści przygotowujący zamach na World Trade Center. "Z tą technologią jest trochę jak z nożem - to, do czego zostanie użyta zależy od tego, w czyich jest rękach" - dodał badacz.

W czasach Internetu steganografia oczywiście zyskała zupełnie nowy, cyfrowy wymiar. Informacje ukrywa się np. zastępując w plikach lub pakietach danych nieistotne bity - bitami z ukrytą informacją. Główną gałęzią steganografii stały się np. metody związane z obrazami. Krzysztof Szczypiorski opowiedział, że zajmował się np. wykrywaniem informacji w zdjęciach umieszczonych na Facebooku. "Tekst można schować w zdjęciu np. kosztem kolorów, które są najrzadziej używane. W takim standardowym zdjęciu na Facebooku można - nie budząc większych podejrzeń - umieścić np. 100 bajtów informacji" - zaznaczył Szczypiorski. Przyznał, że to wystarczy, by schować tam np. krótki list miłosny na Walentynki albo - co gorsza - instrukcję wysadzenia jakiejś linii kolejowej.

Naukowcy w ramach projektu stegano.net udowodnili też, jak ukrywać można informacje w telefonii internetowej - np. za pomocą najpopularniejszego komunikatora Skype'a. "Wymyśliliśmy, że ukryte informacje można umieszczać w... ciszy pomiędzy słowami. Program, który skonstruowaliśmy może na bieżąco, w czasie rozmowy wynajdować pakiety z informacjami o ciszy i podmieniać je na pakiety, w których ukryte są informacje" - opowiedział badacz.

Przyznał, że jego zespół opracował ponad 40 różnych metod ukrywania informacji - np. w sygnale WiFi czy Bluetooth - z czego najlepszy kanał ma ogromną przepustowość ponad 1 Mb/sek. Szczypiorski zaznacza, że pomysły te mają pokazać, jak szerokie jest spektrum możliwości działania np. przestępców, którzy chcą ukrywać informacje.

"Najbardziej zainteresował nas jednak aspekt wykrywania tego typu informacji - tak, żeby nie być wobec nich bezbronnymi" - zaznaczył naukowiec. Przyznał, że przydaje się przy tym wykrywanie anomalii. "Bo anomalia wskazuje na coś niestandardowego" - zwrócił uwagę steganograf. W projekcie powstaje system, który anomalie wykrywa w sieciach i systemach telekomunikacyjnych.

Mówiąc o takich odkrytych już przez jego zespół anomaliach, prof. Szczypiorski stwierdził, że część pakietów w sieci działa na zasadzie: pytanie-odpowiedź. Podał przykład programu ping, za pomocą którego sprawdza się, czy jakiś komputer jest aktywny w sieci. "Powinno być tak, że jest więcej takich zapytań do komputerów niż odpowiedzi. Tymczasem zdarza się, że jest więcej odpowiedzi niż pytań. A to znaczy prawdopodobnie, że te odpowiedzi są wykorzystywane do ukrytej komunikacji. To jest właśnie anomalia" - zaznaczył badacz. Zwrócił uwagę, że za pomocą informacji ukrytych w "niewinnych" zapytaniach sieciowych daje się np. z sieci wewnętrznej jakiejś firmy wyprowadzić jakieś strzeżone dane na zewnątrz.

Badacz wyjaśnił, że jego zespół nie zajmuje się odszyfrowywaniem schowanych steganograficznie informacji - to już zadanie dla kryptografów. "Jednak przeciętna osoba nie potrzebuje steganografii do codziennej komunikacji. Więc samo wykrycie, że w komunikacie schowano informację, jest już dla nas wygraną. Użycie tego tajnego kanału świadczy o tym, że to może jakiś wyciek informacji albo jakaś nietypowa sytuacja" - skomentował badacz.

Rozmówca PAP przyznał, że pomysłami, nad którymi pracował, zainteresowały się siły zbrojne Stanów Zjednoczonych. Szczypiorski - wspólnie ze swoim zespołem - opracował steganograficzny router, "cyfrowego szpiega", który łącząc bardzo różne techniki steganograficzne przerabiał poufne dane i przesyłał je dalej, omijając zabezpieczenia, np. firewalle. Dopiero skonstruowanie takiego urządzenia pokazało, że warto skonstruować system zabezpieczeń, który chroniłby przed takimi "cyfrowymi szpiegami".

"Nasza praca badawcza ma służyć aspektom obronnym. Dzięki tej wiedzy możemy sprawdzać, jak obejść

istniejące zabezpieczenia i konstruować systemy, urządzenia i protokoły odporne na różne ataki" - przyznał rozmówca PAP. Wyjaśnił, że dzięki temu można zapobiegać niebezpiecznym aktom. "Jestem przekonany, że wczesna detekcja podejrzanych zachowań jest potrzebna" - skomentował.

PAP - Nauka w Polsce, Ludwika Tomala