Techniczna strona internetu ogranicza anonimowość użytkowników

Specjaliści od bezpieczeństwa komputerowego są zgodni, nasza anonimowość w sieci jest mocno ograniczona, przede wszystkim ze względu na architekturę techniczną internetu, czyli na zasady, według jakich przebiega łączenie się i korzystanie z sieci.

Jak wyjaśnia PAP Piotr Konieczny z Niebezpiecznik.pl, firmy testującej sieci komputerowe pod kątem włamań i ataków komputerowych, wiele informacji o użytkowniku wywnioskować można już na etapie łączenia się z internetem.

Kartę sieciową (urządzenie, które jest konieczne do połączenie się z internetem) każdego komputera odczytuje unikatowy adres MAC (ciąg cyfr), a w trakcie łączenia się z siecią komputer przypisuje karcie jeszcze jeden identyfikator, tzw. adres IP (ciąg cyfr, który jest przypisywany każdemu urządzeniu w internecie). Adres IP pobierany jest z serwerów dostawcy internetu i zazwyczaj jest zmienny, co oznacza, że ten sam adres może w różnym okresie identyfikować różne urządzenia. Administrator danej sieci posiada jednak dostęp do informacji, pozwalającej ustalić, który z komputerów w danej chwili korzystał z danego adresu IP.

Piotr Konieczny podkreśla, że w przeciwieństwie do adresu IP adres MAC, co do zasady jest niepowtarzalny i nie ma dwóch takich samych adresów MAC na świecie. W adresie MAC zakodowana jest nazwa producenta, a także unikatowy numer seryjny karty sieciowej. Może on służyć, jako identyfikator urządzenia, ale także pomóc w namierzeniu danej osoby.

"Jeśli ktoś połączył się z siecią Wi-Fi w restauracji i dokonał jakiegoś przestępstwa w internecie, to, jeśli później ponownie połączy się z siecią używając takiego samego sprzętu do innej sieci np. na lotnisku (a restauracja i lotnisko wymieniają informację o adresach MAC swoich klientów) będzie można ustalić, że w obu miejscach skorzystano z tego samego laptopa. Dokładając do tego obraz z monitoringu kamer przemysłowych, być może uda się zdobyć zdjęcie "podejrzanego". Niestety, bardziej zaawansowani technicznie przestępcy potrafią przed "akcją" podmienić swój adres MAC na losowy, co utrudnia identyfikację urządzenia" - zaznaczył Konieczny.

Kolejne informacje, które możemy uzyskać o użytkownikach sieci, wynikają ze sposobu, w jaki komunikujemy się w internecie. Najczęściej użytkownicy komunikują się między sobą bez szyfrowania treści. Informacje przesyłane w ten sposób łatwo można podsłuchać w punktach, będących skrzyżowaniami internetowych łącz (tzw. routery).

Jeśli skorzystamy z szyfrowanego połączenia, to nikt nie podsłucha treści komunikatu, ale dla ludzi, którzy śledzą zachowania użytkowników w sieci istotną informacją będzie już sam fakt, że ktoś łączy się z siecią za pośrednictwem szyfrowanego łącza.

Dodatkowo uzyskamy powiązane z zaszyfrowanym komunikatem, ale niezaszyfrowane informacje, takie jak - adresy IP odbiorcy i nadawcy wiadomości, na podstawie, których zbudować można tzw. siatkę połączeń, (kto z kim rozmawiał, czyli kto hipotetycznie się zna). Analizując takie połączenie można również ocenić częstotliwość komunikacji i określić jakiego typu dane szyfrują użytkownicy, np. filmy wideo, zdjęcia czy e-maile.

"Warto zauważyć przy okazji sprawy PRISM, że służby specjalne prosiły o informacje, kto, z kim i gdzie się komunikował, czyli prosiły o metadane, a nie o same nagrania treści rozmów.

Przedmiotem ich analizy jest to, kto, z kim się zna i kiedy się z kimś komunikował i czy przypadkiem nie łączy się to z innym wydarzeniami, o których służby wiedzą z innych źródeł. Samo, bowiem przetwarzanie i analizowanie treści rozmów wymagałoby komputerów o ogromnych mocach obliczeniowych, a często do znaczących wniosków dojść można jedynie na podstawie łączenia metadanych" - powiedział Konieczny.

Kolejny sposobem, który można wykorzystać do identyfikowania użytkowników sieci, jest tzw. technika fingerprintingu, będąca swoistego rodzaju pobieraniem "odcisku palca każdego urządzenia". Jak wyjaśnia Konieczny, tego typu metody profilowania są niezależne od adresu IP czy adresu MAC.

"Odcisk" urządzenia powstaje w wyniku działania skryptu umieszczonego np. na odwiedzanej przez nas stronie WWW - skrypt ten odczyta informacje, jakie ujawnia nasze oprogramowanie (nazwę przeglądarki, rozdzielczość monitora, głębię kolorów, rodzaj systemu operacyjnego, który jest zainstalowany w urządzeniu, a nawet używane w komputerze rodzaje czcionek, czy też z pozoru niedostępny z internetu adres MAC). Każdy z nas może zobaczyć, jak bardzo jego konfiguracja jest unikatowa, korzystając z eksperymentu dostępnego pod adresem https://panopticlick.eff.org/

Jak łatwo wykorzystać technikę fingerprintingu do analizowania i profilowania użytkowników tłumaczy Konieczny prostym przykładem. *"Jeśli przeglądam strony poświęcone kolarstwu jakiegoś portalu informacyjnego w sieci i strona ta korzysta z techniki fingerprintingu, a jednocześnie współpracuje z innymi serwisami internetowymi, które przeglądam, to można być pewnym, że na kolejnej przeglądanej stronie wyświetlą mi się reklamy powiązane tematycznie z moją aktywnością na poprzednio oglądanych serwisach, np. najnowsza kolekcja kasków rowerowych"* - powiedział Konieczny.

Dodaje, że metoda usuwania po każdym przeglądaniu internetu plików Cookies nie likwiduje problemu, bo cały fingerprinting nie musi przechowywać żadnych danych na komputerze użytkownika. "Jeśli strona internetowe korzysta z techniki fingerprintingu, to przeciętny użytkownik ma niewielkie szanse, aby się o tym dowiedzieć - pozostaje żmudna analiza kodu HTML (język programowania, który jest wykorzystywany do tworzenia stron internetowych) w poszukiwaniu skryptów" - podkreślił Konieczny.

Jak wyjaśnia Konieczny wiedza dotycząca używanego sprzętu i rodzaju oprogramowania może mieć ogromne znaczenie dla cyberprzestępców, bo może ułatwić im przeprowadzenie ataku.

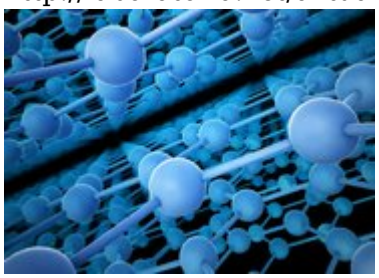
Oprócz informacji wydobytych ze sposobu komunikacji w sieci, kolejnym źródłem informacji mogą być dane, które sami użytkownicy tworzą na swoich komputerach. Chodzi o tzw. metadane. Najciekawsze metadane można wyciągnąć ze zdjęć i dokumentów Microsoft Office Word. Znaleźć w nich można takie informacje jak data powstania pliku, dane jego autora, poprzednie kopie zawartości pliku, a wypadku zdjęć data wykonania zdjęcia, ustawienia przesłony, lokalizacja uchwycona za pośrednictwem GPS.

Jak tłumaczy Piotr Konieczny, wielu użytkowników smartfonów lub tabletów wykonuje zdjęcia, a potem zamieszcza na swoich profilach w serwisach społecznościowych nie mając świadomości jak wiele informacji zawartych jest w metadanych takiego zdjęcia. "Analizując metadane z umieszczanych przez daną osobę zdjęć można odczytać gdzie zostało wykonane zdjęcie, o której godzinie, a także - jeśli zostało przez użytkownika wykadrowane przed wrzuceniem do sieci, poznać jego oryginalny kadr, np. ujawniający kompromitujące detale" - podkreśla Konieczny.

Konieczny podkreślił, że niewiedza dotycząca zapisywanych w metadanych informacji o zdjęciu

przytrafia się nie tylko przeciętnym użytkownikom, ale także specjalistom. *"Przeprowadzając tzw. testy penetracyjne jednej z polskich firm (testy penetracyjne służą sprawdzaniu poziomu bezpieczeństwa na atak ze strony hakerów) przeanalizowaliśmy metadane zdjęć pracowników w formacie paszportowym umieszczonych na stronie internetowej. Okazało się, że zdjęcia były kadrowane z grupowego zdjęcia pracowników, które zostało zrobione w biurze firmy na tle tablicy, na której wisiała informacja z loginem i hasłem do firmowej sieci"* - powiedział Konieczn

Źródło: www.naukawoplsce.pap.pl
http://laboratoria.net/aktualnosci/18411.html



28-05-2024

Drżące nanorurki

Właściwości zależą m.in. od tego, w jaki sposób struktury te wibrują.

28-05-2024

Naukowcy znaleźli sposób na recykling betonu

Informuje “Nature”.

28-05-2024

ADHD zdiagnozowano u co dziewiątego dziecka w USA

W roku 2022 dzieci z diagnozą ADHD było o milion więcej niż w roku 2016.

28-05-2024

Testy na obecność HPV

Co osiem lat równie skuteczne, co regularna cytologia.

28-05-2024

Do środowiska trafiło ponad 1 mld komarów GMO

Przeznaczonych do walki z malarią.

28-05-2024

Może to owady uratują nas przed zwałami plastiku

Niektóre gatunki owadów są w stanie zjadać plastik.

28-05-2024

Terapia daremna przedłuża cierpienie, przedłuża agonię

Terapia daremna nie jest w stanie pomóc pacjentowi.

28-05-2024

Widzimy eskalację zaburzeń związanych ze stresem

Szeroko rozumianych lękowo-depresyjnych.

Informacje dnia: Drżące nanorurki Naukowcy znaleźli sposób na recykling betonu ADHD zdiagnozowano u co dziewiątego dziecka w USA Testy na obecność HPV Do środowiska trafiło ponad 1 mld komarów GMO Może to owady uratują nas przed zwałami plastiku Drżące nanorurki Naukowcy znaleźli sposób na recykling betonu ADHD zdiagnozowano u co dziewiątego dziecka w USA Testy na obecność HPV Do środowiska trafiło ponad 1 mld komarów GMO Może to owady uratują nas przed zwałami plastiku Drżące nanorurki Naukowcy znaleźli sposób na recykling betonu ADHD zdiagnozowano u co dziewiątego dziecka w USA Testy na obecność HPV Do środowiska trafiło ponad 1 mld komarów GMO Może to owady uratują nas przed zwałami plastiku

Partnerzy