

# Wykrywanie proxy i prawdziwego adresu użytkownika sieci Tor

<http://ipsec.pl/wykrywanie-proxy-i-prawdziwego-adresu-u%C5%BCytkownika-sieci-tor.html>

Grupa [ja href="http://ha.ckers.org/"](http://ha.ckers.org/) [i ha.ckers.org](http://ha.ckers.org/) przedstawiła oparta o JavaScript techniki wykrywania prawdziwego adresu osoby wchodzącej na stronę przez dowolny system anonimizujący - np. [ja href="http://tor.eff.org/"](http://tor.eff.org/) [i Tor](http://tor.eff.org/).

Technika [ja href="http://ha.ckers.org/weird/tor.cgi"](http://ha.ckers.org/weird/tor.cgi) [i działa](http://ha.ckers.org/weird/tor.cgi) bardzo skuteczniej [/a](http://ha.ckers.org/weird/tor.cgi), także jeśli użytkownik łączy się przez Tor. Działa w ten sposób, że w kodzie ładowanej strony zawarty jest JavaScript, który samodzielnie generuje połączenie TCP do serwera ale nie bezpośrednio tylko za pomocą Javy. Obchodzi w ten sposób ustawienia proxy przeglądarki (a w ten sposób zwykle łączymy się do sieci Tor), co można sobie podejrzeć w kodzie źródłowym strony zwracanej przez [ja href="http://ha.ckers.org/weird/tor.cgi"](http://ha.ckers.org/weird/tor.cgi) [i CGI](http://ha.ckers.org/weird/tor.cgi).

W komentarzach do [ja href="http://ha.ckers.org/blog/20070926/de-anonymizing-tor-and-detecting-proxies/"](http://ha.ckers.org/blog/20070926/de-anonymizing-tor-and-detecting-proxies/) [i artykułu](http://ha.ckers.org/blog/20070926/de-anonymizing-tor-and-detecting-proxies/) z [ha.ckers.org](http://ha.ckers.org/) [i](http://ha.ckers.org/) wskazano również na analogiczne techniki, które można zrealizować przy pomocy [ja href="http://hackademix.net/2007/09/26/cross-browser-proxy-unmasking/"](http://hackademix.net/2007/09/26/cross-browser-proxy-unmasking/) [i Flasha](http://hackademix.net/2007/09/26/cross-browser-proxy-unmasking/) (hackademix) [i](http://hackademix.net/2007/09/26/cross-browser-proxy-unmasking/) oraz na wcześniejszy projekt [ja href="http://metasploit.com/research/misc/decloak/"](http://metasploit.com/research/misc/decloak/) [i DeCloak](http://metasploit.com/research/misc/decloak/) [i](http://metasploit.com/research/misc/decloak/) robiący to samo i opublikowany przez HD Moore z [ja href="http://metasploit.com/"](http://metasploit.com/) [i Metasploit](http://metasploit.com/).

Jak się przed tym mogą zabezpieczyć użytkownicy Tora? Przede wszystkim wyłączając Jave i JavaScript, na przykład za pomocą [ja href="http://noscript.net/"](http://noscript.net/) [i NoScript](http://noscript.net/).