Beveiliging

Firefox-malware onthult identiteit Tor-gebruikers

5 aug. 2013 door Henk-Jan Buist

Nieuws - Een 0-day in browser Firefox wordt door de FBI ingezet om de identiteit van Tor-gebruikers te onthullen. Malware die via de kwetsbaarheid wordt gedropt stuurt IP- en MAC-adressen door naar een server in de VS.

Gebruikers van een verborgen server op het anonieme netwerk Tor worden onthuld door een stukje malware. Hun identiteit wordt doorgestuurd naar een server in de Verenigde Staten. De FBI zou daarmee kinderpornohandelaren opgespoord hebben.

De deanonimiserings-malware wordt geïnstalleerd via een JavaScript-exploit in de Firefox-browser die standaard bij Tor wordt gebundeld. In eerste instantie werd gedacht dat het om een 0day in Firefox gaat, maar volgens Mozilla gaat het om een bekend gat dat reeds is gepatcht.

JavaScript ingeschakeld

Het draaien van JavaScripts was standaard uitgeschakeld in voorgaande versies van Tors variant van Firefox, maar deze feature is weer ingeschakeld om de browser toegankelijk te maken voor een groter publiek. Via een kwetsbaarheid in de browser is er malware gepusht naar gebruikers van verborgen servers die enkel toegankelijk zijn via het Tor-netwerk.

Zo'n verborgen server wordt gebruikt door dissidenten, klokkenluiders en journalisten om informatie veilig uit te wisselen. Maar de dienst wordt ook gebruikt door internetpiraten en handelaren in kinderporno.

De verborgen servers van een van deze hosters, Freedom Hosting, zijn vorige week door de FBI neergehaald en de eigenaar is gearresteerd. Freedom Hosting is volgens de FBI verantwoordelijk voor het grootste kinderpornonetwerk op internet.

Kinderpornonetwerk op de korrel

De Javascript-exploit zou dan ook gericht zijn op Freedom Hosting, hoewel nog niet is bevestigd dat de exploit specifiek op Freedom Hosting-gebruikers is gericht. Wel duikt de browserexploit precies op hetzelfde moment op als de man achter Freedom Hosting is gearresteerd. Daarnaast zorgt de malware ervoor dat de IP- en MAC-adressen van de Tor-gebruiker worden doorgestuurd naar een server in de VS.

Tor distantiëert zichzelf van Freedom Hosting in een blogpost. "De persoon of personen die Freedom Hosting draaien zijn niet gelieerd aan of verbonden met het Tor Project", schrijft bestuursvoorzitter Andrew Lewman op het blog van Tor. Ook gaat Lewman in op het gat.

Bug in Firefox 17

"De exploit wordt gebruikt om de computer van een gebruiker te infecteren. De payload misbruikt mogelijk potentiële bugs in Firefox 17 Extended Support Release, waar onze Tor-browser op is gebaseerd. We onderzoeken deze bugs en fixen ze waar mogelijk."

Mozilla onderzoekt de bug en het gaat volgens de browsermaker om een bekende kwetsbaarheid die gedocumenteerd is als CVE-2013-1690. Mensen die de laatste versie van Firefox gebruiken, ook de gebruikers die de laatste Tor-variant hebben geïnstalleerd, zouden niet kwetsbaar zijn.

Update 09.51 uur: Laatste alinea toegevoegd - onderzoek Mozilla.

Update 14.23 uur: Naar aanleiding van verder commentaar Mozilla berichttekst in de tweede en derde alinea aangepast om te verduidelijken dat het om een bekende en in Firefox gepatchte kwetsbaarheid gaat .