Spotřebiče Blue Coat používané vládami ke sledování a cenzuře webového provozu

eweek.com/security/blue-coat-appliances-used-by-governments-to-monitor-censor-web-traffic

Robert Lemos January 17, 2013

Kybernetická bezpečnost

Podle

Robert Lemos

-

17. ledna 2013
Obsah eWEEK a doporučení produktů jsou redakčně nezávislé. Můžeme vydělávat peníze, když kliknete na odkazy na naše partnery. Další informace

Skupina výzkumníků naléhala na Spojené státy a mezinárodní společenství, aby se podrobně podívaly na technologické společnosti, které poskytují zařízení pro filtrování sítí represivním režimům, poté, co skenování internetu ukázalo, že 61 zemí používá hardware jednoho výrobce k blokování nebo sledování komunikace.

Dne 16. ledna zveřejnila technologická skupina na Torontské univerzitě zaměřená na lidská práva, známá jako The Citizen Lab, zprávu analyzující internetová data na známky síťových zařízení vytvořených bezpečnostní a infrastrukturní firmou Blue Coat Systems. Zájem o společnost Sunnyvale v Kalifornii následoval po vyšetřování hacktivistů a výzkumníků v roce 2011, kteří zjistili, že její zařízení používá syrská vláda ke sledování a cenzuře její domácí opozice.

Produkty společnosti jsou široce používány vládami se známým zájmem cenzurovat nebo sledovat své občany, včetně Číny, Egypta, Ruska a Venezuely, uvádí zpráva.

„Smyslem není démonizovat tuto technologii, ale vytvořit širší diskusi o těchto typech technologií," řekl Morgan Marquis-Boire, vedoucí technický výzkumník pro Citizen Lab, která je součástí Munk School of Global Affairs na UT.

Vyšetřování našlo zařízení v 61 zemích – včetně zemí v Radě pro spolupráci v Zálivu, která upřednostňuje cenzuru určitých typů internetového obsahu, a v Libanonu, Turecku a Malajsii.

V roce 2011 výzkumníci zjistili, že zařízení síťové infrastruktury od Blue Coat Systems and Network Appliance , která byla prodána společnosti ve Spojených arabských emirátech, byla převezena do Sýrie. Rozsáhlé protokoly ze zařízení, které získali hacktivisté, ukázaly, že Sýrie zařízení používala k cenzuře a sledování aktivistů. Americká vláda přidala společnost a osoby odpovědné za dodání zařízení syrským úředníkům na seznam entit , což je kompilace jednotlivců a skupin, které jednají proti Spojeným státům a mají zakázáno přijímat americké produkty.

"Domníváme se, že tyto protokoly byly získány nabouráním do jednoho nebo více nezabezpečených serverů třetích stran, kam byly soubory protokolů exportovány a uloženy," uvedla společnost Blue Coat Systems v tehdejším prohlášení . „Ověřili jsme, že protokoly byly pravděpodobně generovány zařízeními [Blue Coat] ProxySG a že tato zařízení mají IP adresy obecně přiřazené Sýrii. Nevíme, kdo spotřebiče používá, ani jak přesně jsou používány."

Zařízení Blue Coat a NetApp jsou považovány za technologie „dvojího použití": Lze je použít k obraně sítí a zároveň představují hrozbu cenzury a monitorování jednotlivců. Snad nejznámější digitální technologií dvojího použití je šifrování, na které se v 90. letech 20. století zaměřila vleklá právní bitva mezi USA a technologickými společnostmi.

Protože rozšířené používání šifrování může pomoci chránit disidenty, většina aktivistů za digitální práva protestovala proti omezením exportu šifrování. V současné bitvě však aktivisté za lidská práva místo toho podporují debatu o omezení používání síťového hardwaru schopného kontrolovat a blokovat provoz.

„Jedním z klíčových cílů diskusí o technologiích dvojího užití je určit metodu vytváření účinných kontrol takové technologie, která současně omezuje její prodej a nasazení pro účely, které mají negativní dopad na lidská práva, a zároveň chrání ta použití, která slouží legitimním účelům a výsledkem jsou výhody pro společnost," uvádí zpráva Citizen Lab.

Neexistuje snadné řešení tohoto problému, protože mnoho zemí tuto technologii legitimně využívá a národy obvykle nerady vynášejí soudy nad svými vrstevníky. Místo toho může být nejlepším řešením, aby se společnosti staly dobrými občany společnosti a znaly své zákazníky, řekl Marquis-Boire.

„Etické firemní chování je v dnešní době docela mainstreamová myšlenka," řekl. „Nechápu, proč nelze v dnešní době očekávat minimální standard dobrého firemního chování. Pokud je minimálním standardem, že nebudeme prodávat nikomu, kdo to nemá výslovně zakázáno – je to dost nízká laťka."