ул. "Дякон Игнатий" № 9, София 1000
Република България
тел: (+359 2) 940 9771;
факс (+359 2) 988 5094

„Информационно обслужване“ се справя с безпрецедентна по своя мащаб хакерска атака

Публикуван на: 25.10.2015

„Информационно обслужване“, компанията, която поддържа и администрира сайта на Централната избирателна комисия (ЦИК) и отговаря за компютърната обработка на резултатите от Местни избори 2015 и Националния референдум, регистрира безпрецедентна за България хакерска атака срещу публичната инфраструктура на ЦИК. Това се случи малко след началото на изборния ден. По-късно през деня стана ясно, че подобна атака е организирана и срещу публичните Интернет страници на други ключови по отношение на изборните процеси държавни организации.

От началото на атаката от тип "отказ от услуга" (DDoS), към Интернет портала на ЦИК са направени над 530 000 000 (петстотин и тридесет милиона/ над половин милиард) заявки в рамките на 10 часа, като една четвърт от тях са от видими IP адреси с произход Виетнам, Турция и САЩ. В началото на атаката са отчетени над 65 000 000 (шестдесет и пет милиона) едновременни потребителски сесии към портала на ЦИК, което е равносилно на опит на 65 000 000 потребителя да достъпят Интернет страницата в един и същи момент.

За сравнение:

- Нормалният и обичаен трафик към сайта на ЦИК на предишни избори е бил около 1 800 000 (милион и осемстотин хиляди) заявки в рамките на цял месец, което е 275 пъти по-малко отколкото заявките в днешния ден за 10 часа.
- През 2013 г., когато беше отразена подобна атака, бяха регистрирани общо 12 000 000 заявки за цял месец, което е около 44 пъти по-малко от регистрираните днес за 10 часа).

Дистрибутираните атаки от такъв тип се осъществяват чрез дистанционен контрол на милиони компютри, които са предварително заразени със зловреден софтуер, който може да се активира едновременно и да насочва заявки към избрани цели. Тенденцията в последните години в световен мащаб е към увеличаване на броя и интензитета на тези атаки, което налага реализирането на специфични защитни средства, които да позволяват отсяване на легитимни от нелегитимни заявки към публичните Интернет страници.

Именно заради това, компанията предварително е осигурила възможно най-ефективната и модерна защита на инфраструктурата от подобни атаки чрез технологии и софтуер, които се използват от институции като Белия дом, например.

Атака от такъв мащаб и с такава продължителност като днешната обаче, е без аналог за България и отразяването ѝ, без да бъдат блокирани легитимни заявки от потребители, е сериозно предизвикателство, което беше посрещнато от екипи на "Информационно обслужване" АД, съвместно с привлечени специалисти и водещи ИТ експерти от службите за сигурност. Предприетите проактивни съвместни действия за потискане на атаката и възстановяване на нормалната работа на Интернет портала на ЦИК дадоха резултат и в обедните часове на днешния ден сайтът на ЦИК започна да функционира нормално, с моменти на временно забавяне.

DDoS атаката продължава и към момента, но в следствие на професионалните усилия на екипа, ИТ инфраструктурата на компанията приема и обслужва всички заявки за достъп до страницата на комисията, като в пиковите натоварвания е възможно да има забавяния.

Използваме възможността да подчертаем, че инфраструктурата, извършваща компютърната обработка на резултатите е изцяло физически изолирана от Интернет. Всички действия върху публичната инфраструктура на Дружеството нямат и не могат да имат влияние върху процесите по обработка на секционните протоколи, както в 265-те общини в България, така и в централният изчислителен пункт в ЦИК.