

## Domény vyřazené z DNS ve dnech 1.-8.2.2010 – popis incidentu

**Trvání incidentu: 1. 2. 2010 – 8. 2. 2010**

**Reakce:** postupně vyřazeno z DNS 150 doménových jmen

### **Shrnutí:**

Ve dnech 1.- 8. února 2010 rozhodlo sdružení CZ.NIC na základě doporučení CZ.NIC-CSIRT o zablokování 150 doménových jmen, které se staly součástí útoku na IRS (úřad pro správu daní při ministerstvu financí USA).

Domény byly vyřazeny z DNS na základě ustanovení 12.5. Pravidel registrace doménových jmen v ccTLD .CZ.

Seznam všech předmětných domén je v příloze tohoto dokumentu.

### **Popis útoku:**

CZ.NIC obdržel dne 1.2.2010 informaci od registrátora ONE, s.r.o., že jeho prostřednictvím bylo v průběhu soboty a neděle (30. a 31.1.) zaregistrováno 51 domén .cz, které byly zaplacené z pravděpodobně kradených kreditních karet. Ze strany registrátora byly doménám odebrány NS a požádal nás o jejich zablokování, resp. zrušení. Toto zablokování jsme realizovali po prověření situace 1.2.2010.

V průběhu dalších dnů jsme na základě upozornění ze zahraničních zdrojů prověřovali stav a postupně blokovali další doménová jména, registrovaná tentokrát zejména prostřednictvím registrátora Key-Systems GmbH. Domény opět sloužily k phishingovým útokům na organizaci IRS.

Počínaje dnem 9. 2. 2010 se útok přesunul do jiných domén, od tohoto data jsme nezaznamenali zneužití domény .cz.

### **Další postup :**

O všech provedených blokadách byli informováni příslušní registrátoři, kteří také se sdružením CZ.NIC v průběhu řešení problému spolupracovali.

Po uplynutí jednoho měsíce od zablokování domén nedošlo k odstranění závadného obsahu.

Nekontaktovali nás ani držitelé těchto domén s žádostí o jejich odblokování. Domény byly tedy v souladu s Pravidly registrace zablokovány na dalších 30 dní.

Praha, 19. 3. 2010  
CZ.NIC-CSIRT team

**Příloha : seznam domén .cz, vyřazených z DNS v termínu 1.2.2010 – 8.2.2010 :**

aedswce.cz	lifoxy3.cz	qwfrte.cz	resaxzw.cz	tyerdef.cz	uiioas.cz
aedswet.cz	lifoxy4.cz	rastxzb.cz	resaxzwy.cz	tyerdeg.cz	uiioat.cz
asfrte.cz	lifoxy5.cz	rastxzc.cz	resaxzy.cz	tyerdei.cz	uiioau.cz
bwaswq.cz	lifoxy6.cz	rastxzd.cz	rtfrte.cz	tyerdeke.cz	uiioay.cz
cfrte.cz	lifoxy7.cz	rastxze.cz	rwaswq.cz	tyerdel.cz	uijghy.cz
cwaswq.cz	lifoxy8.cz	rastxzf.cz	srvfiles.cz	tyerdeo.cz	uopiukl.cz
erfrte.cz	lifoxy9.cz	rastxzg.cz	terfdeed.cz	tyerdeq.cz	uwaswq.cz
ewaswq.cz	lopiukl.cz	rastxzh.cz	terfdee.cz	tyerder.cz	vacantes.cz
ferdawa.cz	nvbgfy.cz	rastxzn.cz	terfdef.cz	tyerdes.cz	vcrpt.cz
ferdawe.cz	nwaswq.cz	rastxzn.cz	terfdei.cz	tyerdet.cz	vcs1.cz
ferdawy.cz	nwcey.cz	rastxzt.cz	terfdeo.cz	tyerdeu.cz	vsdll.cz
filemode.cz	nwdey.cz	rastxzv.cz	terfdep.cz	tyerdew.cz	vwaswq.cz
gbfrte.cz	nweey.cz	rastxzy.cz	terfder.cz	tygersa.cz	xccds.cz
gerdas.cz	nwfey.cz	resaxza.cz	terfdes.cz	tygersg.cz	xsdd.cz
hadser.cz	nwrey.cz	resaxzd.cz	terfdet.cz	tygersm.cz	yertsac.cz
hhunter.cz	nwvey.cz	resaxze.cz	terfdeu.cz	tygerst.cz	yertsad.cz
hyfrte.cz	olaey.cz	resaxzf.cz	terfdew.cz	udaswy.cz	yertsag.cz
iwaswq.cz	olewr.cz	resaxzg.cz	terfdey.cz	uiioaa.cz	yertsah.cz
jioyfu.cz	olqey.cz	resaxzi.cz	tgaswb.cz	uiioad.cz	yertsam.cz
jupiukl.cz	olsey.cz	resaxzo.cz	tiempoparcial.cz	uiioae.cz	yertsan.cz
kopiukl.cz	olwey.cz	resaxzq.cz	trabajos.cz	uiioag.cz	yuferd.cz
lifoxy1.cz	olxey.cz	resaxzr.cz	twaswq.cz	uiioai.cz	yufrte.cz
lifoxy10.cz	owaswq.cz	resaxzs.cz	tyerdea.cz	uiioao.cz	ywaswq.cz
lifoxy11.cz	pasder.cz	resaxzt.cz	tyerded.cz	uiioaq.cz	zinnko.cz
lifoxy2.cz	qwaswq.cz	resaxzu.cz	tyerdee.cz	uiioar.cz	zxfzte.cz