Domains excluded from the DNS from 1-8.2.2010 – incident description

Incident duration: 1.2.2010 – 8.2.2010

Reaction: 150 domain names gradually excluded from the DNS

Summary:
From 1 to 8 February 2010, the CZ.NIC Association decided to block 150 domain names, based on the recommendations of CZ.NIC-CSIRT, that had been part of an attack on the IRS (the Internal Revenue Service of the USA).
The domains were excluded from the DNS based on clause 12.5 of the Rules of Domain Names Registration under ccTLD .cz.
A list of all the domains in question is attached to this document.

Attack description:
CZ.NIC received information on 1 February 2010 from the registrar ONE s.r.o. that over Saturday and Sunday (30 and 31 January), 51 .cz domains had been registered through them, which were probably paid for using stolen credit cards. The registrar removed the domains from the NS and asked us to block or cancel them. We implemented this block after examining the situation on 1 February 2010.

Over the following days, based on warnings from foreign sources, we examined the status and gradually blocked further domain names, this time registered in particular via the registrar Key-Systems GmbH. The domains were again used for phishing attacks on the IRS.

Starting on 9 February 2010, the attack shifted to other domains, and from this date we have not recorded any abuse of the .cz domain.

Next steps:
The relevant registrars, who also collaborated with the CZ.NIC Association in resolving the problem, were informed about all the blocks implemented.

After one month of blocking the domains, the objectionable content had not yet been removed. Nor had the domain holders contacted us with a request to unblock them. The domains were therefore blocked for a further 30 days in accordance with the Rules for Registration.

Prague, 19.3.2010
CZ.NIC-CSIRT team

Appendix: list of .cz domains excluded from the DNS between 1.2.2010 and 8.2.2010:

aedswee.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	tyerdek.cz	uiioay.cz
cffrte.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	terfded.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	rastxzr.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	zxfrte.cz