

From: jonathan m
Date: Thursday, June 14, 2018 at 22:04
To: "gdpr@icann.org"
Subject: [Ext] Technical and admin contacts

Hi, I wanted to briefly share with you my experience regarding technical and admin contacts. I haven't been following closely the litigation but for what it's worth:

There are times where a registrant doesn't have a lot of experience running a website and they rely on someone else to administer the domain and technically support its functionality. When there is a compromise on the domain, of course we have our rolodex of contacts at hosting companies to patch the compromise. However, there are times where the customer of that hosting company can get a response more quickly from the hosting company than we can even work our contacts, and that customer may be an intermediary for the registrant. When that happens, given that the registrant is not necessarily skilled in understanding what's going on, reaching the technical or administrative contact to explain what's going on and working with them to patch the compromise may help mitigate threats to potential victims more quickly. I personally recall a situation in the last couple of years where a government website was compromised in an underdeveloped country and it was only through the administrative and/or technical contacts that we were able to more effectively mitigate the threat. I do see a value in treating the registrant differently than the one administering or technically supporting the domain, and making sure that when needed, the right contacts are available.

A good design would be explaining that if someone else is administering or the technical support for the domain, that it is required to collect these contacts separately because otherwise the registrant can be taken advantage of to their detriment.

This is just preliminary feedback and not my final opinion, but thought it may be worth sharing. Keep in mind that from an intellectual property perspective, there is an overlap as brands are abused to execute these attacks, but it is primarily more of a cybersecurity and privacy concern than about protecting the intellectual property per se involved in these attacks.

Jonathan Matkowsky
CIPP/EU, CIPT, JD
RiskIQ, Inc.