From: Anonymous
Date: Wednesday, January 31, 2018 at 04:19
To: "gdpr@icann.org"
Subject: [Ext] WHOIS data under DGPR

ICANN – apologies for the late response.

We executed remediation operations against more than 28,000 phishing URLs and 3,984 URLs containing malware last year. Accurate registrant, admin, and tech contact data remains critical to our ability to confirm compromised or malicious websites. We also use the data available today to immediately contact responsible registrants to inform them of compromises on their domains. Additionally we have decreased malicious domain registrations by sharing compiled registrant contact data with relevant stakeholders; the compiled registration data available currently proved domain registration process were exploited.

Loss of this service, as would occur in Model 3, would increase our phishing page investigative time and eliminate our ability to immediately report compromised content to registrants. This would increase the time malicious content exists on compromised websites, thus increasing malicious page exposure to Internet users. Model 3 would also reduce or eliminate any of our ongoing efforts to reduce fraud by improving domain registration processes. Loss of this service passes the burden to law enforcement and registrars, to each individually establish criteria to evaluate "competent" requests; this would also increase costs for all parties to gain access to registrant contact data.

A delay to the access of this data due to accreditation services as would occur in Model 2b. This would increase the time it takes to confirm malicious content on compromised websites. This option would also increase costs for law enforcement agencies, intellectual property lawyers, registries, registrars and inquirers for access to whois data.

If changes must be made, we propose the adoption of Model 1. This would allow us, and other organizations interested in network hygiene, to continue to identify and work with responsible parties to that end. With the Internet's size, it's critical that we not support any bottleneck or other limits on those attempting to do good works. When it becomes too hard to do the right thing, we only make the environment more supportive to malicious actors. We strongly believe Model 1 satisfies the spirit behind the proposed changes while allowing the general public to continue reporting suspicious sites accordingly.