WHOIS, conceitos e perspectivas

*Por **Demi Getschko**, Diretor Presidente do NIC.br e **Frederico A.C. Neves**, Diretor de Serviços e de Tecnologia do NIC.br*

Data da publicação:

Maio de 2012

PREÂMBULO

- View the full image

Quando é contratado um nome de domínio qualquer, seja sob um domínio de país (“.br”, “.de” etc) ou sob um domínio genérico (“.com”, “.info” etc), a entidade registradora insere informações cadastrais do contratante do domínio em uma base de dados pública na Internet, conhecida como WHOIS. Por exemplo, uma consulta à base de dados WHOIS do nome de domínio “bb.b.br” apresenta o seguinte resultado:

.....
• domain: bb.b.br

• owner: BANCO DO BRASIL S.A.

• ownerid: 000.000.000/0001-91

• responsible: Larissa da Silva Novais Vieira

• country: br

• owner-c: BABRA22

• admin-c: BABRA22

• tech-c: JOGOM30

• billing-c: BABRA22

• nserver: dns1.bb.com.br

• nsstat: 20120512 AA

• nslastaa: 20120512

• nserver: dns2.bb.com.br

• nsstat: 20120512 AA

• nslastaa: 20120512

• dsrecord: 37018 RSA/SHA-1 e1CFDeF1Ae C5235D6AD9F0AF731535Fb4D2F555D

• dsstatus: 20120510 DSOK

• dslastok: 20120510

• created: 20090107 #5165498

• expires: 20140107

• changed: 20111125

• status: published
.....
• nic-hdl-br: BABRA22

• person: banco do brasil

• e-mail: webmaster@bb.com.br

• created: 20110915

• changed: 20120207
.....
• nic-hdl-br: JoGom30

• person: Joaquin Gomide

• e-mail: jgomide@bb.com.br

• created: 20090616

• changed: 20090616
.....

A consulta pode ser feita, para qualquer nome de domínio, através de um simples programa de consulta disponível para qualquer sistema (Windows, MacOS, Linux, Android, iOS etc), ou através de serviços de consulta na Internet[1].

Em dezembro de 2011 a equipe de revisão do serviço WHOIS da ICANN[2] publicou um relatório[3] mostrando que uma porcentagem significativa de pessoas ou organizações que registram nomes de domínio não conhecem o serviço WHOIS ou não sabem quais dados são divulgados publicamente. o serviço, assim, é parte relevante das discussões sobre direitos e deveres na rede, preservação da autonomia e abrangência da Internet, bem como formas de proteger a liberdade e a privacidade dos internautas. Tanto a qualidade necessária dos dados, quanto as características e as informações que devem constar dele e a forma de tornar disponíveis essas informações

são tópicos dessa discussão.

BREVE HISTÓRICO

A primeira especificação técnica do WoIS é anterior à disseminação maciça do protocolo TCP/IP que caracteriza a Internet. Seu objetivo, desde o início, foi servir como uma base de dados muito simples para identificar os responsáveis por cada m dos “nós” ligados à rede, “nós” que podiam enviar e receber informações. Saber quem opera algum nó e como se poderia entrar em contato com este operador era vital para que uma rede em intensa fase de crescimento mantivesse estabilidade. Quando alguém identificava algum problema relacionado a algum computador ligado à rede, era pelo WHOIS que poderia localizar o responsável e, assim, fazer com que a situação eventual de erro se normalizasse.

O que este primeiro documento de especificação,a RFC 812 (março de 1982)[4], descrevia era um serviço de “diretório”, então fornecido pelo SRI-NIC[5], e que continha dados de contato. A RFC sugeria que as consultas a esse diretório utilizassem programa de computador fornecido pelo próprio SRI-NIC.

Lembremos que à época não havia ainda a estrutura hierárquica de nomes, que o DNS[6] implementou em 1983. A tabela de “nós” da rede era uma listagem simples, um rol de nomes de máquinas. Certamente essa relação não suportaria o crescimento vertiginoso da rede anos depois e teria que ser substituída. Com a implantação do DNS hierárquico em novembro de 1983[7], na forma que conhecemos hoje, com a formalização da estrutura de nomes de domínio e a definição do processo em outubro de 1984[8], o SRI-NIC estendeu o serviço WHOIS – que também passou a fornecer informações sobre os dados de contato dos que registravam nomes de domínio no novo sistema de DNS. Afinal m nome de domínio registrado pressupunha que uma nova máquina, com suas idiossincrasias, estaria entrando na rede.

Entre 1992 e 1996 um grupo de trabalho da Internet Engineering Task Force (IETF)[9], motivado em boa parte pelos resultados obtidos pelos criadores do protocolo de indexação de servidores FTP (Archie)[10], trabalhou para tentar melhorar o serviço de WHOIS propondo extensões ao protocolo original (WHOIS++). Infelizmente o escopo muito amplo e a complexidade acabaram por prejudicar sua adoção.

Nos já quase vinte anos da Internet comercial outras duas tentativas na IETF tentaram aperfeiçoar o WHOIS, visando incluir características desejáveis – como suporte a descoberta de servidores, internacionalização dos dados armazenados (originalmente apenas em caracteres latinos sem diacríticos, formato conhecido como ASCII) e a codificação de perguntas e respostas de maneira padrão.

Entre 1997 e 1998 houve uma nova tentativa na IETF[11] de retrabalho da especificação do protocolo RWHOIS[12] que lançava mão do modelo hierárquico usado no sistema de nomes de domínios, adicionado aos conceitos do serviço padrão de diretório OSI/ISO X.500[13], e com a semântica largamente influenciada pelo protocolo de envio de mensagens de e-mail SMTP[14]. Apesar de toda sua arquitetura distribuída, sua implementação e uso acabou sendo limitada a quem, na época, operava o serviço comercial de diretório para o InterNIC:[15] a empresa Network Solutions.

Outro grupo de trabalho na IETF[16] especificou ma linguagem para políticas de roteamento, RPSl[17], que era ampla o suficiente para também cobrir serviços de registros de nomes. esta linguagem acabou sendo adotada como extensão para o serviço WHOIS na representação dos dados por vários dos registros de endereços e registros de nomes de domínio. o “.br” foi um dos que adotou o RPSl em 1998.

Com a falta de um padrão amplamente adotado, extensões específicas e de fabricantes acabaram por proliferar em outros registros, complicando o cenário global.

Entre 2001 e 2008 a IETF, com o grupo de trabalho CRISP[18], produziu uma especificação que pretendia unificar o serviço. Apesar de melhor e mais completo, sua complexidade e as dificuldades que surgiram pela necessidade da distribuição de novos programas de consulta para a comunidade de usuários acabaram por protelar sua disseminação. entretanto, suas ideias progrediram[19], apoiadas em um trabalho dos registros regionais de endereços[20], que procuraram consolidar os requisitos do CRISP, mas com um foco em uma implementação mais simples e que não requeresse a distribuição de novos programas para a utilização do serviço.

Assim, apesar da idade e do histórico de tentativas de substituição, este serviço, essencial para a operação e segurança da rede, continuará a ser prestado pelo nosso velho e remendado WHOIS por alguns bons anos, antes

de ser substituído por um protocolo que atenda às demandas de tão diversos usos que hoje são esperados dele.

A DISCUSSÃO

Não se pretende aqui esgotar o tema, mas apenas levantar os pontos principais que, a nosso ver, deveriam balizar este debate. o primeiro ponto a se observar é que a Internet sempre tratou seus partícipes como dignos de crédito. Na Internet a maioria das informações são “declarativas”. ou seja, eu informo o que quero sobre mim e, a priori, essa informação é aceita como verdadeira até que alguém duvide dela. A presunção é, sempre, de boa fé.

A extensão disso ao WHOIS é que, pelos costumes da rede, o que o detentor do domínio declara é o que deve ser considerado verdadeiro até prova em contrário. o WHOIS representaria a “melhor tentativa” de catalogar os operadores de domínios na Internet. Querer dele mais que isso é avançar em terreno desconhecido e possivelmente hostil à rede.

A segunda observação, decorrente da anterior, é que os dados mínimos de identificação unívoca do responsável pelo nome de domínio registrado devem ser visíveis a toda a rede. É a forma de fazer valer a “boa fé” do primeiro ponto. ou seja, a rede se protege contra fraudes e falsidades expondo a todos o que se sabe dos detentores de cada domínio. Se a declaração de um deles for obviamente falsa, alguém poderá pedir a correção. este também é o argumento fundamental para que o acesso seja universal e uniforme. A criação de “privilégios” de acesso à base apenas coloca em risco e torna vulneráveis os usuários da rede, criando categorias “especiais” que podem “ver” mais que outras.

É claro que a maneira uniforme e transparente com que a rede funciona sempre gera oportunidades para aqueles que desejam aproveitar-se disso para o mal. um exemplo claro é usar a base do WHOIS para simplesmente colecionar endereços de correio eletrônico, visando à formação de listas para spam. No entanto, um mau uso de um serviço nunca deve tolher seu uso adequado (abusus non tollit usum...). Assim, trata-se de impedir, por exemplo, excesso de acessos partindo de uma única origem, e impedir o acesso maciço às informações (bulk acess) a quem quer que seja.

Finalmente, resta destacar que o uso de WHOIS em registros de país[21] e seu uso em registros genéricos pode ter grandes disparidades. É muito difícil estabelecer um identificador unívoco global e é razoavelmente simples identificar unicamente pessoas físicas ou jurídicas dentro de um país. Por outro lado, a diversidade linguística coloca barreiras bastante difíceis de transpor quando falamos de uma base de dados que terá informações sobre detentores de domínios de todas as partes do mundo e em diversos alfabetos.

---

1. exemplo de um serviço gratuito de consulta WHOIS: http://ipduh.com

2. A ICANN (Internet Corporation for Assigned Names and Numbers) coordena mundialmente a designação de nomes de domínio de primeiro nível: http://www.icann.org

3. Ver: http://www.icann.org/en/reviews/affirmation/whois-rt-draft-final-report-...

4. Ver: http://tools.ietf.org/html/rfc812

5. SRI-NIC Stanford research International - Network Information Center. Nesta época o SrI prestava o serviço de centro de informações da ARPANET para a DCA (Defense Communications Agency)

6. Sistema de Nomes de Domínio, que permite localizar máquinas e serviços na Internet a partir de nomes em vez dos números IP. Ver: http://pt.wikipedia.org/wiki/Domain_Name_System

7. Ver: http://tools.ietf.org/html/rfc882

8. Ver: http://tools.ietf.org/html/rfc920

9. Internet Engineering Task Force. Ver: http://www.ietf.org/wg/concluded/wnils.html

10. File Transfer Protocol, protocolo de cópia de arquivos entre computadores em rede. Ver: http://en.wikipedia.org/wiki/Archie_search_engine

11.Ver: http://www.ietf.org/wg/concluded/rwhois.html

12. Ver: http://tools.ietf.org/html/rfc2167

13. Ver: http://pt.wikipedia.org/wiki/X.500

14. Ver: http://pt.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol

15. Ver: http://pt.wikipedia.org/wiki/InterNIC

16. Ver: http://www.ietf.org/wg/concluded/rps.html

17. Ver: http://tools.ietf.org/html/rfc2280

18. Ver: http://www.ietf.org/wg/concluded/crisp.html

19. Ver: http://www.ietf.org/mail-archive/web/weirds/current/msg00884.html

20. Ver: http://tools.ietf.org/html/draft-newton-weirds-arin-whoisrws-00

21. Conhecidos como ccTLDs (Country Code Top Level Domains)

Categoria:

- poliTICs 12