DNS open resolvers com IPv4 que envolvam recursos sob a administração do LACNIC

Autor: CSIRT CEDIA, LACNIC CSIRT
Coordenação/revisão: Graciela Martínez, Guillermo Pereyra

lacnic
www.lacnic.net

Índice

Resumo executivo

O CSIRT do LACNIC e o CSIRT de CEDIA realizaram um estudo para identificar servidores de DNS abertos associados a um endereço IPv4, a fim de informar os associados que têm designados esses recursos da situação, sugerir alternativas para corrigir a configuração destes e tentar reduzir significativamente o número de *open resolvers* na nossa região. A comunicação foi feita por diferentes canais para avaliar, também, a eficácia de cada um.

Os *open resolvers* constituem um risco de segurança latente na infraestrutura da Internet, porque são servidores configurados de modo que podem ser usados para atacar infraestruturas de terceiros e realizar ataques de negação de serviço.

Já em março de 2013 o US-CERT emitiu sua alerta TA13-088A,[1] na qual adverte sobre o problema, e propõe medidas de mitigação.

[1] ‹https://us-cert.cisa.gov/ncas/alerts/TA13-088A›

Introdução

O principal vetor de ataque para aproveitar vulnerabilidades em serviços continua sendo mediante serviços expostos pelo IPv4. Hoje, a maioria dos ataques são executados por meio de serviços vulneráveis executados sob este protocolo.

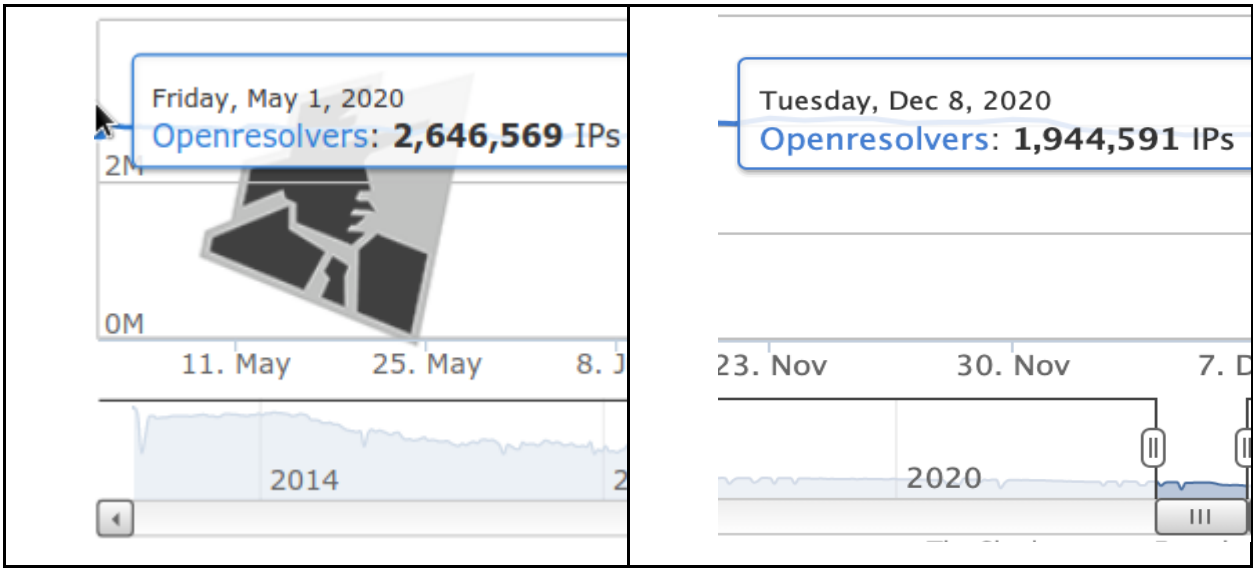
A utilização do protocolo IPv4 também é uma vantagem para os CSIRT, por se tratar de um universo conhecido, controlado e relativamente rápido de revisar para encontrar essas falhas. Existem ferramentas muito eficientes que podem encontrar portas abertas no universo IPv4 (<2^32 endereços IP) em poucos minutos, mais simples ainda quando o universo é reduzido aos recursos designados a um RIR específico.

De acordo com o objetivo do projeto, procurou-se localizar e informar os servidores DNS que atuam como *open resolvers*. Um *open resolver* é o servidor do DNS que responde às questões de resolução originadas de qualquer rede, independentemente de que seja a rede de um terceiro ou a sua própria.

Um *open resolver* é uma ameaça para a segurança e estabilidade da Internet,porque permite atividades potencialmente prejudiciais. Estas são baseadas na técnica de amplificação bem conhecida do protocolo UDP. Por meio dela, busca-se que a resposta a esta consulta envie uma grande quantidade de informações à vítima escolhida. Para o caso de um *open resolver*, o atacante envia uma pequena consulta com um endereço de origem falso e com um tipo de *récord* que envolve uma resposta muito grande (por exemplo: TXT, ANY ou extensões de DNSSEC).

Situação geral

Segundo dados da ShadowServer,[2] o número mundial de *open resolvers* detectado em dezembro de 2020 diminuiu em relação a maio, mas, em qualquer caso, o número de quase dois milhões de servidores DNS que permanecem abertos é muito grande e representa uma ameaça potencial aos diferentes sistemas.



Impacto

Ter servidores DNS abertos afeta de várias formas, não apenas quem recebe o ataque, mas também os provedores e usuários. Por exemplo, em:

- **Reputação**: o responsável pela rede que hospeda o *open resolver* pode ter sua reputação afetada, uma vez que se percebe um descuido nos serviços que gerencia.
- **Qualidade do tráfego**: o tráfego gerado desde esta rede não é necessário e poderia ser evitado, já que com certeza afete o tráfego legítimo e/ou os sistemas que controlam o tráfego de rede.

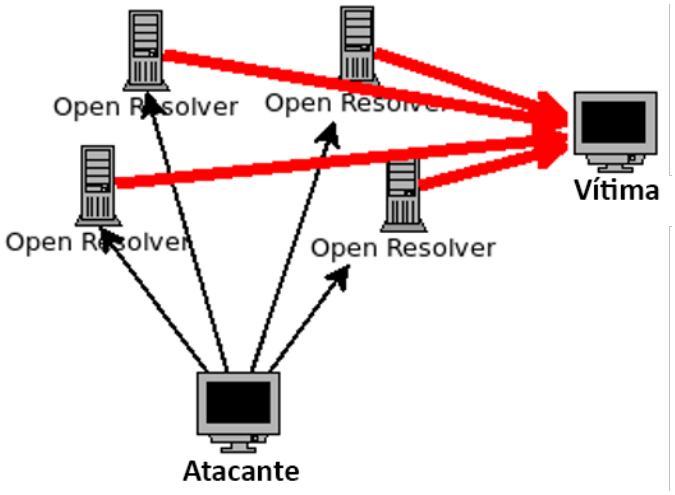
Em muitos desses casos, as organizações não sabem da existência desse problema de segurança em sua rede e, portanto, não agem para prevenir ou resolver o problema.

[2] ‹https://scan.shadowserver.org/dns/stats/›

Notificar esse problema ajuda à instituição a trabalhar para corrigi-lo ou, pelo menos, tomar conhecimento de sua existência. Caso não possua os recursos necessários para corrigi-lo, poderá justificar sua contratação.

Ataque de denegação de serviço de inundação de pacotes

A seguir, é ilustrado o *modus operandi* de um ataque de denegação de serviço por inundação de pacotes. O atacante faz a mesma consulta a vários *open resolvers*, mas são feitas com o endereço de origem da vítima. Suas consultas são muito pequenas e significam um consumo baixo de recursos para ele, mas a vítima - que é quem recebe as respostas de todos os *open resolvers* - vai sentir o impacto de uma grande quantidade de informações que chega até ela (e que não solicitou), o que sem dúvida producirá um esgotamento de seus recursos.



Que mecanismos existem para detectar um *open resolver*?

O processo de detecção de um *open resolver* consiste em saber se é obtida uma resposta a uma consulta feita à porta 53/UDP de um determinado IP. Caso afirmativo, é um *open resolver*.

Porém, é muito caro enviar uma consulta para todos os IP do universo das redes, mesmo quando se tenta fazer apenas para os recursos IPv4 sob a administração do LACNIC. É por isso que se faz uma consulta DNS recursiva apenas para os IP que possuam a porta 53/UDP aberta.

Também deve ser destacado que este processo é apenas o resultado de uma foto obtida no momento da consulta. As respostas podem variar muito entre cada pesquisa realizada, pois dependem de fatores como *timeouts*, equipamentos desligados, respostas inesperadas, bloqueios por parte de IPS/*Firewalls*. Portanto, é importante monitorar continuamente os *open resolvers* para localizar aqueles que não apareceram em pesquisas anteriores.

Ferramentas e fontes de dados relacionados ao tema

Como primeiro passo na pesquisa, foram avaliadas várias técnicas, ferramentas e fontes de dados relacionados ao tema.

Ferramentas

Dig / Host

Permitem revisar se um IP determinado responde a um *query* ao serviço do DNS. Para isso, é necessário indicar o IP que será revisado. Não aceitam intervalos, apenas um IP ao que irão consultar. Se o IP responder, pode considerar-se que é um *open resolver*; se não responder, significa que não há evidência de que seja um *open resolver*.

As duas funcionam de forma apropriada para o objetivo do projeto. Escolhemos *Dig* para as validações.

NMAP

Ferramenta muito conhecida, que permite revisar um intervalo ou rede e encontrar portas abertas nessa rede.

Masscanner

Variante semelhante a NMAP. De fato, usa praticamente os mesmos *switches*. Pode ser-lhe fornecida uma lista de redes ou IP e as portas a encontrar abertas, e entregará uma lista com os resultados desta revisão.

Fontes de dados

Shodan

Consultou-se por meio do Shodan para obter listas de DNS abertos na região e duas limitações foram encontradas:

- A lista não é atualizada diariamente. Pode-se obter um relatório de 53 portas abertas, o que não significa que sejam *open resolvers*.
- A lista resultante é atualizada de forma não específica ao longo do tempo.

Shadowserver[3]

O Shadowserver foi contactado. Embora fosse esperado um conjunto de resultados muito semelhante, a realidade é que diferem dos obtidos. Em alguns casos, foram encontrados *open resolvers* que não estavam na lista do Shadowserver; em outros casos, foi o contrário. Essa diferença pode acontecer por diferentes motivos. Por exemplo: o RIR ao que pertence a rede nem sempre é o LACNIC, as horas em que foi feita a revisão, bloqueios que podem existir para impedir o acesso de determinadas redes, longos tempos de resposta, etc.

Eventualmente, pensou-se em consolidar ou contrastar os dados de ambas as fontes, mas —como o universo de IP usado pelo Shadowserver não é conhecido— nossos resultados poderiam ter sido contaminados, ao invés de enriquecidos.

---

[3] ‹https://www.shadowserver.org/›

Delegated extended do LACNIC

Pelo acima exposto, optou-se por usar as informações coletadas diretamente do *delegated extended* do LACNIC.

Procedimento seguido

O seguinte descreve o procedimento usado para a digitalização.

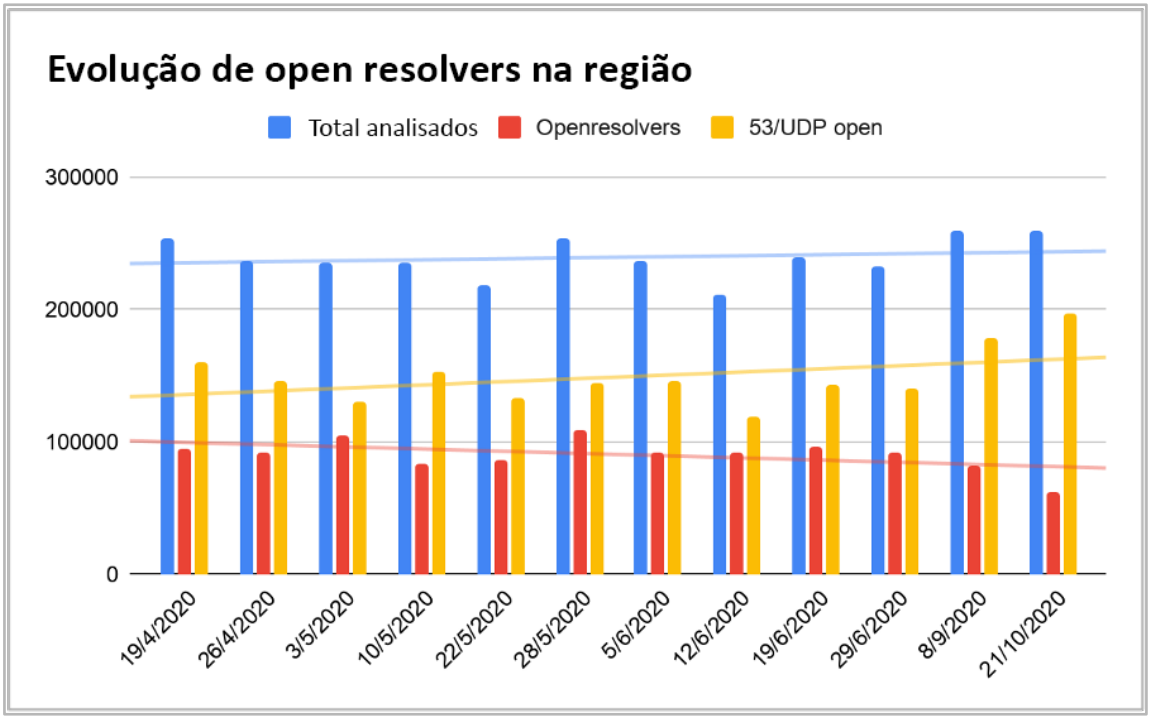
1. Foi baixada a lista LACNIC-extended do ftp que contêm as subredes designadas na região do LACNIC.
2. Este resultado foi convertido para CIDR.
3. Foi feito um *supernetting* nessas faixas e alimentado o *masscanner* com esta lista.
4. Foram procuradas portas 53/udp abertas nesta lista, usando *masscanner*.
5. Partindo do resultado do IP com esta porta aberta e usando o comando *dig*, foram pesquisados os servidores de domínio que respondem a uma consulta específica e própria de um domínio sob controle de CEDIA: test-csirt.cedia.org.ec (TXT).
6. Obteve-se a lista de contatos dos positivos do passo anterior.
7. Os recursos sob a administração dos NIR foram separados.
8. Estes avisos foram organizados e enviados por três canais diferentes (e-mail, contacto direto com o responsável do intervalo ou através do módulo de segurança de MiLACNIC).
9. Os avisos também continham sugestões de solução (ver anexo 1). O procedimento descrito foi refinado e executado em três ocasiões.

Para comparar, os primeiros IPs classificados como *open resolvers* sempre foram mantidos como universo de estudo.

Número de *open resolvers* detectados durante a análise

Do total de IP analisados, apenas aqueles que tinham a porta 53/UDP aberta foram confirmados como *open resolvers* e responderam perguntas de resolução DNS. Os IP que não responderam às consultas foram registrados apenas como porta 53/UDP aberta.

O gráfico abaixo mostra a evolução do número de servidores *open resolvers* abertos para o mundo durante o período do projeto. Percebe-se que houve uma diminuição.



Análise e avaliação de ações para informar sobre os DNS abertos

Os contatos foram realizados usando três canais: e-mail, contacto direto e MiLACNIC.

Do conjunto de IP associados a um serviço de DNS aberto ao mundo, de um lado, foram separados aqueles sob a administração dos NIR, NIC.Mx e NIC.Br, e o resto da lista foi dividido em três subconjuntos. Foi designado um dos seguintes canais para cada um deles:

1. **E-mail:** um e-mail foi enviado aos contatos registrados para cada IP da Argentina, Chile e Colômbia.
2. **Contato direto:** os responsáveis conhecidos das cinco organizações com mais *open resolvers* encontrados foram contactados de várias maneiras. Estes podem ou não ter sido os contatos registrados para cada IP. Foram usadas técnicas sociais (chamar pessoas conhecidas na organização).
3. **MiLACNIC:** o aviso foi enviado por meio do portal MiLACNIC (ficaram excluídos o Brasil, México, Argentina, Chile e Colômbia, por estarem em algum dos canais anteriores)

Resultados associados aos canais de comunicação

A tabela a seguir mostra o número de recursos identificados como *open resolvers* em cada uma das rodadas realizadas e o canal de comunicação usado.

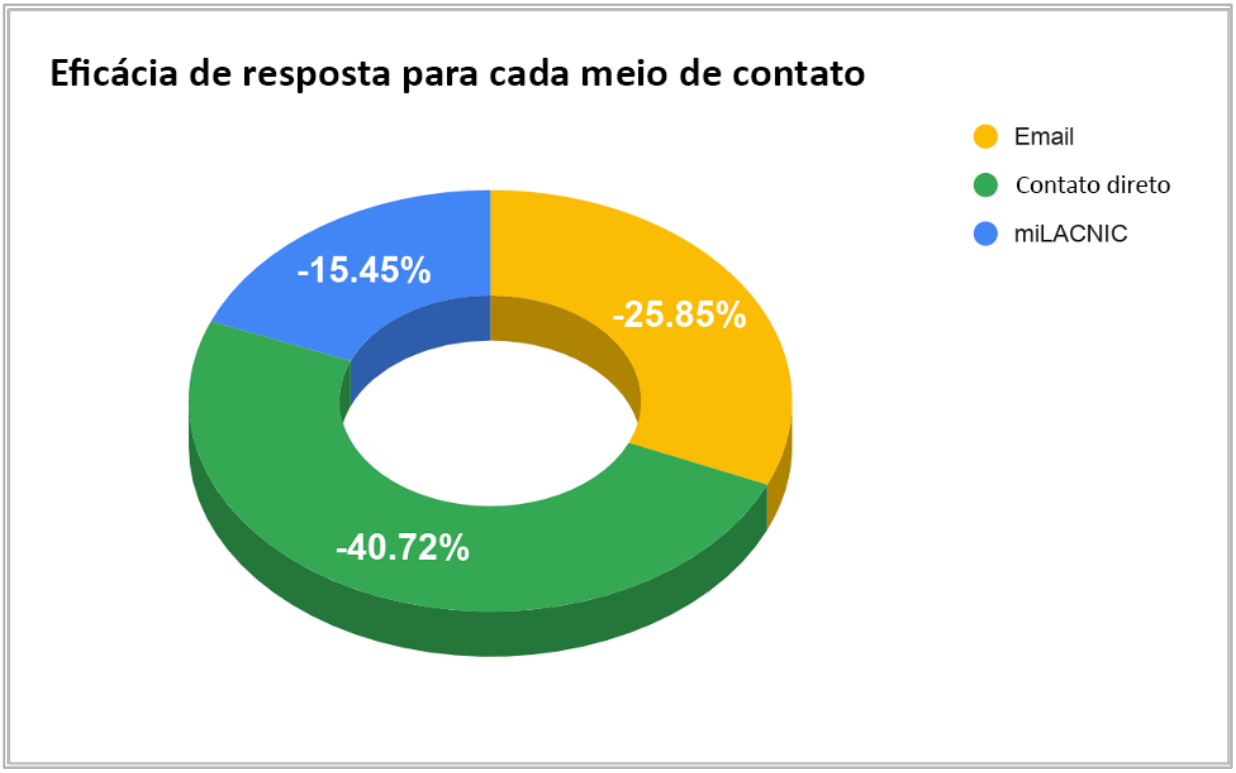
Canal de comunicação usado	29/06/2020 Primeira rodada	08/09/2020 Segunda rodada	21/10/2020 Última rodada	Diferença (%) Primeira vs. última
E-mail	19084	10920	14151	-25.85
Contato direto	5545	3191	3287	-40.72
MiLACNIC	11436	7317	9669	-15.45
Total	36065	21428	27107	-24.84

É de interesse compartilhar alguns comentários relacionados a esses resultados.

- Foram recebidas respostas pelo e-mail tais como:

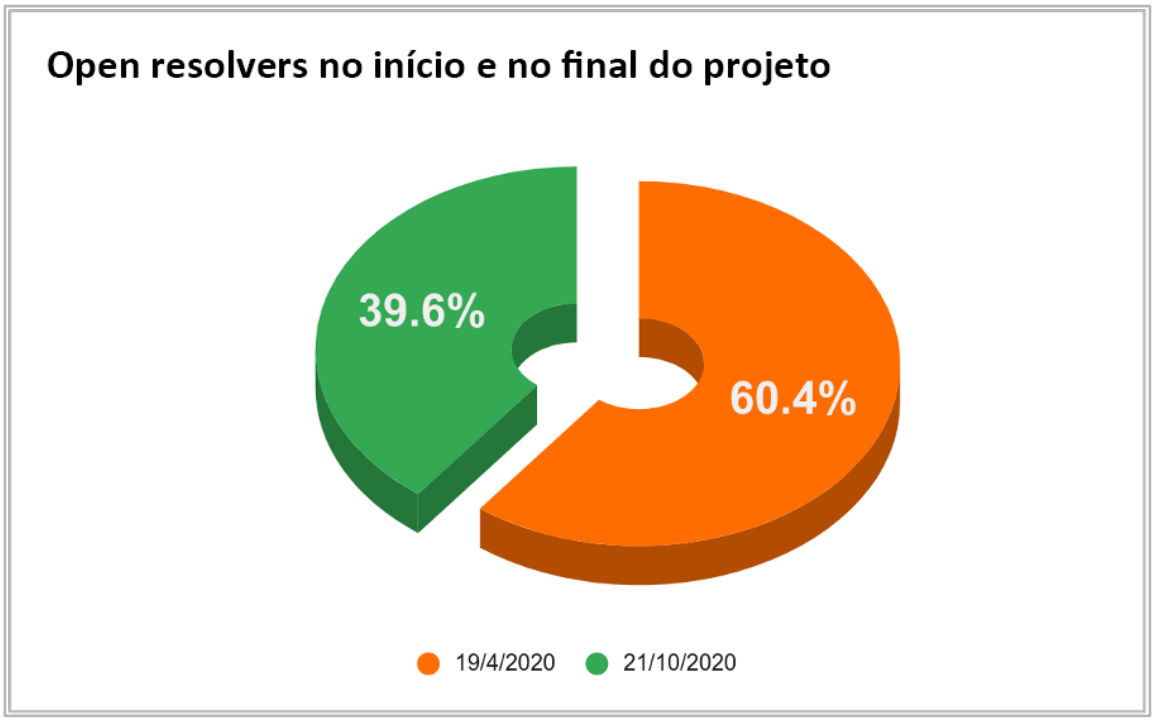
    - Agradecimento pelo aviso e por comunicar de que ações corretivas seriam tomadas.
    - Notificação de que as ações sugeridas foram tomadas e de que o problema foi resolvido.
    - Pedido de ajuda adicional.
- Mais de 12% das mensagens enviadas por e-mail na primeira rodada foram devolvidas, pois a caixa de contato que figura no *whois* não é correta.
- Embora por contato direto durante a primeira rodada foi recebida apenas uma resposta à notificação, os resultados mostram que foram feitas ações, pois houve uma diminuição drástica dos *open resolvers* abertos.
- Por meio de MiLACNIC, não foi recebido *feedback* das organizações.

No gráfico a seguir, o percentual de sucesso pode ser comparado segundo o canal de comunicação usado. Considera-se *sucesso* quando o servidor responde à consulta realizada.



Conclusões

Em termos gerais, podemos considerar que o resultado foi bem-sucedido, pois foi possível reduzir um grande número de servidores DNS abertos a consultas, conforme mostra o gráfico a seguir.



Foi identificado o e-mail como o canal mais eficaz para alertar a comunidade-alvo sobre as vulnerabilidades de segurança de seus sistemas e para ajudar a corrigi-los.

Na mesma linha, conclui-se que existem muitas caixas técnicas ou de *abuso* para as quais os relatórios não podem ser enviados por motivos diversos. É preciso que as organizações mantenham estas caixas funcionais e atualizadas para que possam ser informadas sobre os incidentes de segurança que possam surgir.

Para conseguir uma redução dos *open resolvers* na região, é necessário automatizar o procedimento de detecção e aviso aos responsáveis. O relatório para as organizações seria uma combinação do envio de e-mail e o uso do módulo de segurança de MiLACNIC.