ISSN 2447-1097

Direito & TI – Porto Alegre / RS www.direitoeti.com.br

TEREDO IPV6 – PROCEDIMENTOS A SEREM ADOTADOS DURANTE A INVESTIGAÇÃO POLICIAL PARA EVITAR *FALSOS POSITIVOS*

Alesandro Gonçalves Barreto[1]

RESUMO

A busca dos elementos informativos individualizadores da autoria e materialidade delitiva dos crimes cometidos pela Internet, especialmente os registros de conexão utilizados pelos infratores, têm sido um grande desafio para os integrantes da polícia judiciária. Nesse contexto, ao obter esses dados, os investigadores deve ter em mente procedimentos a serem adotados na individualização dessas conexões a fim de não direcionarem o trabalho investigativo para caminhos mais demorados ou não esclarecedores. Assim, procurar-se-á expor os mecanismos a ser seguidos quando se tratar de Teredo Adresses IPv6.

Palavras-chave*: Internet; Investigação; IPv6; Teredo.*

O avanço de práticas criminosas na *Internet* faz com que a polícia aperfeiçoe sua forma de investigar. Outrora, quando um delito era cometido, a busca dos elementos informativos estava adstrita ao local de crime real: testemunhas, exames em local de crime, reconhecimento de pessoas e coisas, acareação, busca e apreensão, dentre infinitas possibilidades.

Hoje, a investigação policial tem ainda um campo muito maior de atuação no local de crime cibernético. O criminoso no lugar "A" desvia dinheiro de uma vítima que está no ponto "B" para alguém que está em "C". O **local do crime** passou a ser também virtualizado, devendo o investigador adequar-se a esse novo contexto para buscar essas evidências nos delitos cometidos através da rede mundial de computadores.

Ao conectar-se à *Internet* através de um provedor de conexão, o dispositivo informático utilizado pelo usuário recebe um número de *IP*[i] válido, podendo ser na versão *IPv4* ou *IPv6*. No caso do primeiro, o protocolo é separado por pontos e conta com endereçamento de 32 (trinta e dois) *bits*. Com pouco mais de 04 bilhões de possibilidades, alcançou o número limite no ano de 2011. Podemos citar como exemplo da versão 4 o *IP* 192.19.89.17. Para suprir essas

1 Delegado de Polícia Civil do Estado do Piauí e coautor dos livros Investigação Digital em Fontes Abertas e Manual de Investigação Cibernética à Luz do Marco Civil da *Internet*, ambos da Editora Brasport e; Vingança Digital, da Mallet Editora. Coordenador do Núcleo de Fontes Abertas da Secretaria Extraordinária para Segurança de Grandes Eventos nos Jogos Olímpicos e Paralímpicos Rio 2016. Colaborador Eventual da Secretaria Nacional de Segurança Pública. delbarreto@gmail.com.

deficiências, alguns provedores de conexão passaram a adotar a prática de *nateamento* de protocolos de *Internet*, ou seja, atribui-se um único endereço de *IP* para vários usuários, distinguindo-se apenas as postas lógicas atribuídas a cada um. Em alguns casos, mesmo com a possibilidade de migração, continuam a usar a prática do *NAT*.

O ***IPv6*** tem como característica o endereçamento de 128 (cento e vinte e oito) *bits* e foi escrito em hexadecimal para substituir o *IPv4* a fim de que não houvesse mais nenhuma limitação de endereçamentos de qualquer dispositivo conectado à Internet. Não há necessidade de *nateamento* desse tipo de protocolo, ou seja, **cada dispositivo possui número único**. Ressalte-se, todavia, que esse protocolo não é uma extensão do anterior, mas uma versão para resolver o problema da restrição. Podemos citar como exemplo de *IPv6* o 2001:0DB5:JC8F:55F5:BORE:FCWQ:F0CA:001C8.

A transição desses protocolos já deveria ter sido feita; no entanto, muitas empresas insistem ainda na utilização do *IPv4*. A tecnologia existente permite que esses dois protocolos possam coexistir, entretanto, há situações em que os provedores de internet não possuem mecanismos para suportar a versão *IPv6*, impossibilitando, todavia, a comunicação com máquinas que tenham esse tipo de protocolo.

Várias técnicas são utilizadas para prover essa compatibilidade, entretanto, ficaremos adstritos ao IP Teredo, permitindo a comunicação entre dispositivos que possuam protocolos de internet distintos. Essa técnica de tunelamento foi desenvolvida pela Microsoft e descrita na RFC 4380[ii]. Com esse tipo de endereço de IP, possibilita-se a transferência de dados entre protocolos distintos. É exemplo de desse tipo de IP: 2001:0:bd2e:95b8:2c18:10:62c3:5f4.

Dessa maneira, o investigador deve ter em mente que, ao receber os registros de conexão e encontrar blocos de *IP* iniciado por "2001:0", esses são *Teredo IPv6*, não carecendo, portanto, fazer a solicitação dos dados cadastrais aos provedores de conexão, eis que estes sempre irão apontar para o servidor de retransmissão e não ao computador de origem. Nesse caso, a investigação poderia ser levada ao caminho mais longo, dificultando, de sobremaneira, a individualização da autoria e materialidade delitiva.

Para não cometer erros, o responsável pela investigação deverá fazer a conversão do *Teredo IPv6* para *IPv4*. Nesse caso, recomenda-se extrair os dois blocos de caracteres hexadecimais seguintes a "2001:0" e, utilizando tabelas de conversão, encontrará o *IPv4*. No caso do exemplo acima, teríamos os blocos "bd2e:95b8", que transformado para *IPv4* seria

189.46.149.184. O passo seguinte é oficiar ao provedor de conexão para saber qual usuário está vinculado a esse protocolo.

Para fazer a conversão recomenda-se a utilização de ferramentas *online* como, por exemplo, o conversor disponível em http://silmor.de/ipaddrcalc.html.

A imersão tecnológica tem trazido grandes desafios à investigação policial face ao gigantesco volume de informações a serem buscadas para a individualização de uma autoria criminosa. Nessa busca, caberá ao policial coletar e, principalmente, solicitar essas evidências de forma correta para evitar prejuízos ao trabalho investigativo em andamento.

REFERÊNCIAS

BARRETO, Alesandro Gonçalves. BRASIL, Beatriz Silveira. **Manual de Investigação Cibernética à Luz do Marco Civil da Internet**. Editora Brasport. Rio de Janeiro. 2016.
BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm >. Acesso em: 10 dez. 2017.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/LCP/Lcp105.htm>. Acesso em: 10 dez. 2017.

INTERNET ENGINEERING TASK FORCE. **Request for Comments 4380**. Fevereiro de 2006. Disponível em: <https://www.ietf.org/rfc/rfc4380.txt>. Acesso em: 10 dez. 2017.

[i] Código atribuído a um terminal de uma rede para permitir sua identificação, segundo parâmetros internacionais.

[ii] Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs). We propose here a service that enables nodes located behind one or more IPv4 Network Address Translations (NATs) to obtain IPv6 connectivity by tunneling packets over UDP; we call this the Teredo service. Running the service requires the help of "Teredo servers" and "Teredo relays". The Teredo servers are stateless, and only have to manage a small fraction of the traffic between Teredo clients; the Teredo relays act as IPv6 routers between the Teredo service and the "native" IPv6 Internet. The relays can also provide interoperability with hosts using other transition mechanisms such as "6to4".