PERÍCIA EM EVIDÊNCIA

Ataques aos sistemas do TSE: a relevância da perícia de informática em xeque

O Brasil criou legislação e formou peritos nessa área. Mas a evolução tecnológica e a ausência de fronteiras tornam o combate ao crime cibernético cada vez mais complexo

Cássio Thyone Almeida de Rosa
25 de novembro de 2020

Em pleno 15 de novembro, data das eleições municipais no Brasil, foram divulgadas tentativas de ataque aos sistemas do TSE (Superior Tribunal Eleitoral). Entre confirmações e desmentidos que se seguiram, outras informações surgiram no decorrer daquele dia. Ao que parece, o atraso na apuração dos votos esteve relacionado não a um primeiro ataque, que teria ocorrido em 23 de outubro, mas divulgado somente no dia 15 de novembro. O problema estaria relacionado, na verdade, a um segundo ataque, ocorrido no dia das eleições, do tipo negação de serviço (DDoS), em que não houve captação de informações internas dos sistemas e tampouco impacto na contagem dos votos. Além disso, o atraso também teria se dado por questões técnicas do próprio sistema do TSE, envolvido em mudanças em relação às eleições anteriores.

Segundo a ONG *SaferNet*, que atua em conjunto ao MPF (Ministério Público Federal) no monitoramento de fraudes no processo eleitoral cometidas pela internet, esse *ataque* DDoS teve como intenção minar a credibilidade do TSE. "Trata-se de uma operação coordenada e planejada para ser executada no dia das eleições, com o objetivo de desacreditar a Justiça Eleitoral e eventualmente alegar fraude no resultado desfavorável a certos candidatos", declarou o presidente da *SaferNet*, Thiago Tavares, à *Folha de S. Paulo*.

Concomitantemente, na manhã de domingo 15 de novembro, foi tornado público pelos *hackers* um conjunto de dados relacionados a uma antiga base de dados contendo informações desatualizadas sobre processos de Recursos Humanos do órgão. Uma investigação da Polícia Federal, em parceria com a SaferNet, porém, foi capaz de determinar que o ataque ocorreu em 23 de outubro, portanto, antes das eleições.

Esses fatos nos remetem ao interesse em falarmos um pouco sobre aquela que é a área da perícia que possivelmente mais cresce em demanda: a perícia de informática. É ela que trata dos chamados *Crimes Cibernéticos*. Ainda me lembro da época em que iniciei na perícia, começo da década de 1990. Naquele tempo, sequer existiam nos Institutos de Criminalística os setores com peritos formados na área de Informática (ou, como comumente chamamos agora, Tecnologia da Informação - TI). De lá para cá, a tecnologia avançou tanto que é difícil até compreender o seu real impacto. Com ela vieram também os crimes virtuais, as fraudes diversas (incluindo as bancárias), as espionagens, as invasões de computadores pessoais e institucionais e uma gama de eventos relacionados.

Um dos grandes desafios em relação ao combate a esse tipo de crime é o fato de que eles obviamente não conhecem fronteiras. A internet, por constituir-se em uma rede mundial, permite que um crime dessa modalidade seja cometido fora do nosso território, requerendo muitas vezes a colaboração entre instituições de diferentes países.

Para o combate a esses crimes, foi preciso criar também legislação específica, como foi o caso da Lei dos Crimes Cibernéticos (Lei 12.737/2012), conhecida como Lei Carolina Dieckmann, que tipifica atos como invadir computadores (*hacking*), roubar senhas, violar dados de usuários e divulgar informações privadas (como fotos, mensagens, etc.); a Lei 12.735/12, que determina a instalação de delegacias especializadas para o combate de crimes digitais; e o Marco Civil da Internet (Lei 12.965/2014), sancionado em 2014 e que regula os direitos e deveres dos internautas.

Importante destacar que muitos dos crimes cometidos com a ferramenta tecnológica já estavam previstos no nosso Código Penal, como calúnia, difamação, injúria, injúria qualificada, ameaça e falsa identidade. O que mudou é a forma como agora se pode cometer esses crimes, empregando as redes sociais, por exemplo.

Voltando ao caso que motivou esse artigo, é possível citar alguns dos métodos utilizados para se prevenir, investigar e corrigir problemas diversos, incluindo ataques cibernéticos:

- Análise de Tráfego de Rede: por meio de ferramentas específicas, é possível se monitorar o tráfego de uma rede, ou seja, o recebimento e envio de pacotes contendo dados. Dessa forma, anormalidades podem ser detectadas e, de interesse investigativo crucial, endereços IPs podem ser identificados.

- Análise e interpretação de *logs*: por meio da leitura de registros de eventos, armazenados de forma automática por sistemas, quando devidamente configurados, diversas informações sobre o funcionamento dos serviços podem ser acessadas, permitindo que, em uma espécie de auditoria, violações de segurança, ou mesmo tentativas não concretizadas de exploração de vulnerabilidades sejam detectadas, viabilizando a correção das falhas.

Por fim, faz-se importante comentar que diversos dificultadores de rastreio podem ser (e muitas vezes são) utilizados pelos atacantes. Proxies anônimos são um exemplo bastante difundido. Em síntese, por meio de tais ferramentas, o endereço IP de origem permanece oculto, sendo substituído nas comunicações por um endereço IP intermediário que pode estar vinculado, inclusive, a uma localização geográfica absolutamente distinta. Nesses casos, as tentativas de se descobrir o IP original demandam muitas vezes, além de conhecimento técnico, colaborações governamentais internacionais.

No caso em questão, provavelmente jamais saberemos todos os detalhes que a investigação poderá trazer, já que, nesses casos, a própria vulnerabilidade explorada, por segurança, NÃO DEVERÁ ser revelada.

Cássio Thyone Almeida de Rosa
Graduado em Geologia pela UNB, com especialização em Geologia Econômica. Perito Criminal Aposentado (PCDF). Professor da Academia de Polícia Civil do Distrito Federal, da Academia Nacional de Polícia da Polícia Federal e do Centro de Formação de Praças da Polícia Militar do Distrito Federal. Ex-Presidente e atual membro do Conselho de Administração do Fórum Brasileiro de Segurança Pública

---