PF abre inquérito para investigar ataque contra site da Presidência

A Polícia Federal vai instaurar um inquérito para tentar identificar os responsáveis pelo ataque contra o site oficial da Presidência da República no domingo (2/1) e verificar quais medidas podem ser tomadas contra eles. A informação foi divulgada pela Assessoria de Imprensa do Serviço Federal de Processamento de Dados (Serpro) e publicadas pelo Portal *GI*.

O gerente da Assessoria de Imprensa do Serpro, Carlos Marcos Torres, informou que é padrão do órgão e da PF investigar os responsáveis sempre que há uma tentativa de bloqueio na segurança da Presidência. Ao *GI*, o departamento de comunicação da PF confirmou que o órgão está recebendo os documentos do Serpro referentes à segurança do site da Presidência. O inquérito será aberto assim que o recebimento for concluído e formalizado.

Torres informou que o Serpro já criou uma estratégia de bloqueio ao ataque de "negação de serviço" utilizado pelo grupo e que o órgão já tomou medidas para prevenir que esse tipo de ofensiva aconteça no futuro. A dupla de hackers *Fatal Error Crew* assumiu o ataque ao site da Presidência na tarde de domingo.

A dupla provocou intencionalmente uma sobrecarga de acessos nos sites presidencia.gov e brasil.gov, o que fez com que os endereços ficassem instáveis por algumas horas. Com isso, quem tentou acessar os sites no domingo teve dificuldades para abrir a página por causa da lentidão de *download*.

Em nota, o Serpro informou que "todos os dados protegidos do governo brasileiro mantiveram-se seguros, sem qualquer invasão ou dano dos sites ou das suas bases de dados". O site foi estabilizado pela equipe técnica do órgão às 21h30 de domingo. De acordo com o Serpro, o site da Presidência tem capacidade para suportar até 4,5 mil acessos simultâneos.

Por diversão

Em entrevista ao *GI*, o *Fatal Error Crew* informou que derrubou o endereço por diversão, para mostrar que a segurança dos servidores brasileiros é frágil e para protestar contra a eleição da presidente Dilma Rousseff (PT). Formada em 2001, a dupla afirma que já desfiguraram mais de 56 mil sites. O *Fatal Error Crew* destacou que, por meio dos ataques, quer passar a mensagem à população que "votar é algo sério" e pede que as pessoas pesquisem tudo sobre o candidato antes de votar.

Os *hackers* também afirmaram que não têm medo de punição. "As leis do Brasil ainda não foram adequadas a crimes virtuais. O ataque teve origem de servidores de diferentes locais do mundo e é praticamente impossível de nos localizarem", disse um deles ao *GI*. "Se não tivéssemos anunciado [a autoria do ataque], ninguém iria saber."

O advogado e professor em Direito Eletrônico Rony Vaizonf entende que esse tipo de delito se enquadra no artigo 163 do Código Penal como crime de dano ao patrimônio, prevendo de um a seis meses de prisão. "Entretanto, como o ataque foi em um site do governo, é possível que o delito seja classificado como dano qualificado, que prevê de 6 meses a 3 anos de prisão."

O ataque

O *Fatal Error Crew* explicou que, para atacar o site da Presidência, usou uma "negação de serviço" (em inglês, DDoS ou *Distributed Denial of Service*), uma "criação artificial de um número elevado de solicitações simultâneas" a um servidor. O golpe é similar ao utilizado recentemente por hackers para derrubar sites da Visa e do Mastercard em protesto contra a proibição de doações ao site *WikiLeaks*.

O objetivo da negação de serviço é tornar o site indisponível. Um ataque desse tipo em um servidor de e-mail, por exemplo, o incapacita de processar novas mensagens, da mesma forma que um servidor web não pode mais exibir páginas de internet. Em um PC doméstico, o ataque de negação de serviço pode resultar no congelamento do sistema ou no travamento de um dos aplicativos.

O colunista de segurança para o PC do *GI*, Altieres Rohr, informou que "ataques DDoS são normalmente difíceis de contornar porque as solicitações maliciosas, com o intuito de sobrecarregar o serviço, costumam chegar de diversos computadores diferentes. Não dá para simplesmente bloquear o acesso dos computadores ao servidor, porque são muitos".

Ele explicou que o servidor *Domain Name Server* (DNS) – ou Sistema de Nomes de Domínios, em português, que "traduz" o nome do domínio para um endereço IP — é especialmente vulnerável aos ataques porque usa o protocolo *User Datagram Protocol* (UDP), que não verifica o "remetente" da conexão. Os criminosos eletrônicos podem, portanto, forjar o endereço de origem do ataque, de modo que fica difícil saber sua origem.

Date Created

04/01/2011