Leilão de centavos: Programados para fraudar

Os Leilões de centavos modelo ***"penny auction"***, nome dado aos sites em que usuários podem lançar de centavo em centavo, ou de real e real, produtos, que começam com preço "0,00" tem ganho a cada dia mais adeptos no Brasil. Antes de lançar, o usuário deve comprar créditos pré-pagos. Pode o usuário lançar até o cronômetro do produto zerar. Queixa comum é que os usuários de boa fé nunca conseguem cobrir os lances ou lograrem-se vencedores, pois sempre aparece alguém no último milésimo, propondo um lance maior.

Em análise acerca da autenticidade de alguns sites, identificamos que descaradamente e incrivelmente, são sempre os mesmos usuários vencedores. Estes usuários, na verdade, não existem.

É isso mesmo. Em muitos sites existentes na rede, estes usuários são nada mais que "bots", diga-se, agentes ou funções programadas para sempre cobrir o lance de usuários de carne e osso. Igualmente, como usuários são reféns do sistema, são reféns das regras e da programação, que não permite, em regra, que serem humanos cubram os "bots" nas propostas, tudo na surdina, onde os proprietários se valem da ignorância dos usuários, que de centavo em centavo, estão perdendo fortunas na Internet.

O mais incrível é que não há necessidade de perícia especializada. Basta dedução. Por que um usuário iria querer ganhar a mesma mercadoria diversas vezes? Isto está acontecendo.

Os sites já com mecanismos para fraude são inclusive vendidos

pela Internet com “templates” já com bots programados. Alguns administradores ainda são “bondosos” e configuram os bots para deixarem humanos ganharem, diga-se, as vezes. Os bots dão lances automáticos, por outro lado, usuários que criem sistemas de lance automático são considerados nocivos pelo regulamento dos sites e podem ser desconectados dos sistemas.

A lógica faz sentido: para as empresas lucrarem com “centavos” elas precisam de usuários. Logo, com receio de prejuízo, empresas passam a manipular código e fraudar leilões, impedindo que muitos produtos sejam arrematados.

Se os falsos bots são desenvolvidos pela empresa, o usuário tem direito a reparação dos danos materiais e morais na justiça. Ainda, se são os próprios usuários os fraudadores, o site em nossa ótica também é responsável, devendo monitorar os certames e repreender qualquer manobra fraudulenta, anulando imediatamente o certame, quando constate fraude, sob pena de ser responsabilizado.

Aos usuários, pede-se cautela e investigação prévia eis que muitos sites de leilão online no Brasil estão operando irregularmente, não possuem sede física e muito menos emitem nota fiscal. Outra manobra questionável, ainda, consiste em não permitir que os valores dados em lances sejam usados para compra de outros produtos no site, o que nitidamente ofende o Código de Defesa do Consumidor. Alguns sites permitem a compra, apenas do mesmo produto que o usuário deu o lance, e ainda em no máximo 24 (vinte e quatro) horas do término do leilão. O problema é que os produtos são sempre superfaturados.

E o pior, enganam os usuários, pois para comprar o produto os mesmos precisam queimar todos os seus lances, logo, não haverá abatimento verdadeiro do valor da mercadoria.

Não bastasse, tais sistemas travam e são suspensos estrategicamente, para frustrar uma competição e o arremate, e o pior, muitos dos que consultamos trazem previsão expressa nos termos de uso sobre tal “faculdade” do site. É preciso que o usuário leia os termos de uso, e se não concordar, não participe.

Diversos pontos do Código de Defesa do Consumidor são transgredidos, eis que o código considera nulas cláusulas contratuais que subtraiam do consumidor a opção de reembolso de quantia paga, o que se aplica aos leilões de centavos; Igualmente o fornecedor de serviços on-line responde por defeitos na prestação dos serviços ou por informações insuficientes ou inadequadas sobre tais serviços, o que de fato é comum em grande parte dos sites de leilão de centavos, em operação no Brasil.

Cumpre destacar ainda que tais sites, omitindo informações relevantes sobre a natureza e segurança dos serviços, ou mesmo realizando propaganda enganosa, podem, na figura de seus diretores, serem punidos criminalmente com pena de três meses a um ano de detenção e multa.

No Brasil, ainda não há um consenso se tais portais podem ser considerados “jogos de azar” eis que a possibilidade de ganhar ou perder não depende da habilidade do jogador, segundo muitos, mas exclusivamente da sorte. Deve-se destacar que “jogo de azar” é uma contravenção penal prevista no artigo 50 do Decreto Lei 3.688 de 1941. A justiça deverá ser instada a se manifestar em breve sobre o tema.

Os usuários devem checar os termos de privacidade e uso do site, checar CNPJ na receita federal, observar se a empresa tem endereço físico, bem como avaliar sua integridade em redes sociais e sites de defesa do consumidor.

Para os que foram lesados, recomenda-se registrar toda a ocorrência com “screenshots”, se necessário lavrar uma ata notarial em cartório de notas, após, deve-se notificar o site para o ressarcimento, sem prejuízo, é possível abrir uma reclamação no procon e acionar a justiça em busca da reparação material e moral, considerando o desgaste em lidar com tais sites, sem prejuízo de eventual medida criminal por crime envolvendo relação de consumo e, se comprovado, estelionato.

Os sites de leilão, por sua vez, podem se valer de perícia especializada e auditoria digital que mediante análise criteriosa, certifique e testifique que o sistema está limpo de bots e malwares, os isentando de responsabilidades e conseqüentemente, atestando a integridade do código.

Perícia Digital e a Domótica: Casa inteligente, riscos e crimes digitais

A Domótica é uma nova tecnologia que permite a gestão de todos os recursos habitacionais, simplificando a vida das pessoas. O termo “Domótica” resulta da junção da palavra latina “Domus” (casa) com “Robótica” (controle automatizado de um ambiente).

Embora tenha nascido em um contexto militar, hoje vivenciamos o crescimento das tecnologias nos ambientes domésticos. A máxima aqui é o controle de iluminação, climatização, e principalmente, segurança, de forma interligada. Outros elementos e dispositivos eletrônicos também podem ser interligados. Um dos principais controles utilizados no mundo

é o Z-Wave (http://www.z-wave.com/modules/AboutZ-Wave/), onde os especialistas são cada vez mais requisitados no mercado brasileiro.

O que antes era privilégio de milionários, hoje pode integrar casas e ambientes corporativos por menos de dois mil reais (sistemas básicos), sendo que segundo o jornal Folha de São Paulo, os kits já estão cerca de 60% mais baratos que há três anos (http://www1.folha.uol.com.br/mercado/888088-casa-inteligente-chega-a-classe-media.shtml)

A automatização das tarefas de uma casa ou ambiente corporativo, pressupõe a existência de uma central de controle, esta que pode ser conectada a um pc ou mesmo se comunicar por meio de Internet. Fala-se hoje em "domótica inteligente" onde os sensores de um ambiente residencial ou corporativo poderiam conhecer o comportamento daqueles que lá habitam ou trabalham, no conceito chamado "ABC", automação com base no comportamento.

Esquema de recursos passíveis de controle pela Domótica

A característica da domótica é a integração de dispostivos em um único controlador. Tal ponto, se por um lado organiza a gestão das "casas virtuais", por outro permite que todo um sistema seja perturbado em uma única investida, que pode, assim como na alteração de um firewall, alterar ou criar regras no sistema inteligente, prejudicando os que dele se valem.

Logicamente que ataques a estes sistemas residenciais poderão ser feitos por pessoas que conhecem as intimidades do projeto eletrônico, por outro lado, deve-se pontuar que ter uma casa automatizada na Internet será um risco que precisará levar em

consideração critérios no escopo de minimizá-lo.

Que a domótica vem tornar a vida mais fácil não há duvida. O mesmo não se pode dizer quanto à segurança. Os sistemas passam a reagir por uma ordem dada por um interruptor ou por um comando, que pode ser remoto, até mesmo via celular.

Neste cenário, novas ameaças surgem na sociedade da informação. Um criminoso digital pode, por exemplo, cancelar ou paralisar sistemas de irrigação automática, prejudicando hortas e plantas, superaquecer a água para o banho, desligar a aspiração central ou purificador de ar, bem como iluminação, preparando o ambiente para um ataque ou assalto físico, o que pode ser fatal aos habitantes e pessoas que ali trabalham.

Igualmente, um agressor pode desligar os níveis de segurança, tornando indisponíveis sensores de gás, inundações, incêncios, bem como o sistema de comunicação com autoridades e com os proprietários. Sistemas de monitoramento, controle de acesso por impressão digital e padão retinal ou de voz também podem ser prejudicados. Em síntese, se antes o criminoso usava uma chave ou alicate para cortar as correntes, cercas elétricas e cadeados de uma casa, em breve, bastará conhecimentos de tecnologia e alguns comandos, executados remotamente.

Deve-se mencionar também, que a domótica pressupõe central de conectividade (Internet), integrando dados com comutação de tomadas e energia. Se alteradas por um criminoso, poderia expor dados de seus moradores ou mesmo servir de ponte para a prática de outros crimes digitais.

Como se verifica, a domótica ao colocar a casa ou ambiente corporativo na Internet, traz consigo diversas ameaças. Empresas que façam automação deverão pensar em segurança, envolvendo atualização constante do *middleware* dos

equipamentos e riscos de invasões, alterações indevidas e outras possibilidades. A questão da responsabilização civil dos fornecedores também deverá vir à tona, onde os titulares de residências inteligentes poderão ser valer de perícia especializada para apurar o responsável por vulnerabilidade no sistema que tenha permitido a atuação de um criminoso ou a consumação de um incidente.

A segurança eletrônica será em breve parcialmente absorvida pela segurança da informação, o que demandará atualização dos profissionais pois até mesmo uma residência deverá ter um firewall lógico configurado e atualizado, ou será presa fácil do crime da era da sociedade da informação.

José Antonio Milagre é Advogado e Perito especializado em Segurança da Informação. E-mail: *jose.milagre@legaltech.com.br* – Twitter: *http://www.twitter.com/periciadigital*

Onze de março: Cultura de segurança no Japão é exemplo a ser seguido

O forte terremoto de magnitude 8,9 que atingiu a costa japonesa (nordeste) em 11 de março, seguido de um tsunami catastrófico, mais do que nos alertar para a revolta do meio-ambiente que fica acentuada a cada dia, nos chamou a atenção para outro ponto proeminente e que pode ser aplicado como modelo em governos e empresas: a organização e maturidade do Japão no que cerne a segurança e resposta a incidentes de

grandes proporções.

O país conta, desde 2007, com moderno sistema de detecção sismológica alimentado por uma rede de mais de 1000 sismógrafos com sensibilidade para detectar com antecedência ondas sísmicas. O primeiro choque no país foi sentido um minuto após o alerta, o que pode parecer pouco tempo, mas na realidade é um minuto fundamental para salvar milhares de vidas em um incidente. No mundo corporativo, minutos também fazem a diferença e podem significar a quebra de onerosos contratos.

Dados a considerar em uma análise de risco desta natureza, também chamados de *"critérios do risco"*, poderiam ser a localização geográfica do Japão e o histórico do sistema de detecção, que desde 2007 já divulgou 17 alertas, logo, temos um histórico de acontecimento de uma mesma ameaça na mesma região. Ainda, 20% dos terremotos devastadores estão no Japão, o que é gritante para aquele que realiza uma análise e avaliação de risco. Verba precisa ser direcionada.

Diante da alta probabilidade da ocorrência risco e do alto impacto dos seus danos associados, medidas são tomadas dentre as quais podemos citar desenvolvimento de técnicas para construção de edifícios resistentes. Mudanças estruturais são caras, mas de longe são menos onerosas do que a aceitação do risco de eventual terremoto no Japão. Qualquer investimento é investimento necessário e goza de apoio do alto escalão governamental.

Outras medidas tomadas no Japão foram a criação de um plano de resposta a incidentes e continuidade, envolvendo o comunicado e alerta a população, por meio da televisão, rádio e telefones celulares e o suporte técnico a empresas e industrias com processo críticos, por parte do governo, o que contribui para

minimização dos danos associados as ameaças, como por exemplo o suporte dado pelo Governo a *Tokyo Eletric Power*, que seguiu orientações daquele para reduzir a radioatividade excessiva, pós o terremoto, o que poderia causar mais danos.

Não adiantaria, igualmente, conceber um plano de resposta a incidentes e contingência sem sabatiná-lo constantemente com a devida manutenção de indicadores de desempenho. Quantos nunca tiveram políticas de recuperação que diante de um fato concreto demonstraram-se ineficazes? Em segurança da informação temos uma máxima, "*trust, but verify*", que significa "confie, mas verifique". No Japão, treinamentos regulares são oferecidos a população para que possam lidar com terremotos, antes, durante e após os abalos.

Logicamente que há dezenas de anos o Japão se prepara para lidar com esta ameaça, considerando as falhas tectônicas da região onde está localizado, tendo concebido esta "cultura de segurança" em relação a terremotos. Apesar de toda a maturidade, ainda assim modelos de segurança devem ser revistos, pois não se pode garantir a perfeição na detecção e tratamento de todos os incidentes desta natureza, que são mutantes e atuam sob vulnerabilidades distintas. O Japão é um exemplo, eis que disposto a diariamente revisar seu planejamento, em nítida melhoria contínua do sistema, o que permite a clara contenção dos danos causados pelos incidentes e aprimoramento para enfrentamento futuro de outras ameaças. Infelizmente, também temos empresas e governos que a há dezenas de anos conhecem suas ameaças e fraquezas, nada investindo para minimiza-las, nitidamente brincando como acaso.

O Japão deixa um modelo a todos nós, lidando com um terremoto brutal com número considerado relativamente reduzido de baixas computadas. Terremotos anteriores em outros países, na escala 8,9, tiveram muito mais mortes. Os próprios terremotos no

Japão, não fossem contingenciados com maestria, poderiam causar milhares de mortos. Lá, a ameaça são os terremotos, mas em outros países, órgãos do governo e empresas, temos outras ameaças, latentes, constantes, pulsantes, porém os gestores insistem na inércia, assumindo riscos danosos e irreparáveis ou o pior, sequer buscando conhecer as ameaças existentes. Que o episódio possa enaltecer que cultura de segurança bem aplicada não se trata de ostentação, mas de prudência e cautela de gestores diligentes e responsáveis com os ativos que protegem e com o próximo. Para o raciocínio do leitor pontuamos: Se o terremoto fosse no Brasil, o que seria de nós? Efetivamente, não é só o Japão que tem muito que aprender com este trágico incidente.

José Antonio Milagre é Advogado e Perito especializado em Segurança da Informação. E-mail: *jose.milagre@legaltech.com.br* – Twitter: *http://www.twitter.com/periciadigital*