O Direito Digital em tempos mineração oculta de criptomoedas e “furto de processamento”

Recentemente gerou polêmica o fato de que um site do Governo de São Paulo possuía em seu código fonte um minerador de Bitcoins, executado no navegador de usuários sempre que acessado. Esta prática é denominada “mineração virtual”. Já se tem notícias de apps que foram cadastrados no Google Play e que podem até mesmo consumir o processamento dos dispositivos móveis. Quem faz o trabalho são os usuários do site, mas quem ganha é o dono do site ou o titular da carteira registrada no código inserido.

O código HTML da página fazia referência ao coinhive.min.js, um código que consumia toda a CPU de quem acessasse o referido portal. A operadora da carteria, Coinvhive, fora notificada e diz ter bloqueado o usuário em questão, pela violação de termos de uso, informando ainda que teria bloqueado os fundos obtidos pela “mineração” ilícita. Ainda, implantou recentemente um código denominado AuthedMine e que exige um opt-in explícito do usuário final sobre a mineração.

Alguns pontos merecem destaque. Como a página é carregada quando o usuário voluntariamente acessa os referidos sites, não tem este como “permitir” ou não (em tese) que um java script embutido execute, a menos que bloqueie seu navegador, momento em que encontrará dificuldade no acesso a sites. Assim, usuários ficam sabendo por meio do consumo excessivo de processamento, aliado a alguns programas e extensões que detectam os códigos maliciosos, como o caso do “No Coin”(https://chrome.google.com/webstore/detail/no-coin-block-miners-on-t/gojamcfopckidlocpkbelmpjcgmbgjcl) .

A proposta da Coinhive era dar a administradores de sites novas formas de monetizar, do que os tradicionais “ads”. Da análise dos termos de uso, verificamos que usuários são encorajados a informarem de forma ostensiva aqueles que acessam seus sites sobre a mineração.

Sob o prisma jurídico, discute-se a possível violação de privacidade, considerando a inexistência de avisos e transparência sobre o uso indevido da CPU, que interfere no cotidiano do usuário. Além disso, é inegável que o consumo de CPU pode indisponibilizar serviços do computador do usuário ou no mínimo perturbar o processamento, o que sabe-se, pode gerar a responsabilização civil do site que apresenta estes códigos. Se eventualmente o computador que tem disparado um código que eleva seu processamento, serve serviço de utilidade pública, teremos ainda repercussões criminais (Conforme Lei 12.737/2012)

Embora no Brasil muitos comecem a enxergar a questão como furto de energia, que já foi equiparada à coisa móvel para fins de incidência do tipo previsto no artigo 155 do Código Penal, ou mesmo crime de dano (artigo 163), considerando que a prática pode queimar o equipamento e diminuir a duração da bateria, lá fora, os juristas são mais cautelosos. No caso Pirate Bay, que não revelou que estava usando código Coinhive, os pareceres foram de conduta antiética, pela inexistência de crime, não havendo legislação a respeito. Lá, as discussões orbitam se este modelo de “empréstimo de processamento” pode ser a nova forma de monetizar serviços de utilidade pública e projetos online que não querem depender de propaganda (Ads).

Por outro lado, não há dúvidas, muitos dos sites que estão minerando bitcoins, na verdade, não introduziram o código propositalmente, mas são alvos de cibercriminosos que utilizam técnicas para injetar o código, permitindo então que toda a capacidade de processamento do trafego do site lhe renda moedas, que são direcionadas a sua carteira. Nesses casos, pode-se conjeturar do crime de invasão de dispositivo

informático, previsto no art. 154-A da Lei 12.737/2012.

E neste ponto outra reflexão. Qual seria a responsabilidade jurídica do provedor de hospedagem, falhando com sua obrigação de segurança, permite a exploração por criminosos de vulnerabilidade e injeção de código nos sites de seus clientes? Em nosso sentir, a perícia técnica em informática poderá, analisando as evidências, identificar quem deu causa a injeção de código, e se comprovada negligência do servidor, este poderá reparar os clientes que hospedam seus sites. O perito em informática poderá informar se o código foi colocado intencionalmente pelo titular site ou não, analisando inúmeros pontos e elementos.

E qual seria a responsabilidade de Exchanges e Carteiras em identificarem seus usuários? No caso da Coinhive, esta identificou o usuário pela carteira e chegou até bloquear os valores. Porém se olharmos os termos de uso de outras carteiras, como a própria Blockchain Wallet, veremos que estes se negam ou dizem que não podem identificar um usuário ou informar valores, a partir de uma carteira. Porém sabemos que a Carteira guarda um e-mail válido, inclusive para envio e troca de senha, o que sabe-se pode ser a ponta para se chegar a qualquer pessoa por trás de um amontoado de números e códigos de transações.

Temos pouco julgados no Brasil. Em nosso sentir, longe de exaurir e assentar o tema, as carteiras e exchanges estão sujeitas ao Marco Civil da Internet, Lei 12.965/2014, logo, não podem ser recusar a fornecer os dados cadastrais ou registros de acesso às aplicações de usuários que utilizem os serviços para golpes, fraudes, ou recebam criptomoedas originadas a partir de atividades ilícitas, dede que, sempre, exista ordem judicial fundamentada a respeito.

José Antonio Milagre é Perito em Informática, Mestre e Doutorando em Ciência da Informação pela UNESP e Presidente da Comissão de Direito Digital da OAB/SP Regional da Lapa.

www.direitodigital.adv.br