Falso app sobre Coronavírus rouba dados bancários. Quais são os cuidados?

Um arquivo denominado Corona-Virus-Map.com.exe tem circulado em comunicadores e redes sociais. Como verificado, o sistema imita os atuais *map trackers* do Coronavírus, porém, quando executado, o mesmo abre um mapa parecido com o mapa da John Hopkins University (https://coronavirus.jhu.edu/map.html). O arquivo malicioso coleta dados do próprio site da Universidade. No entanto, o arquivo contém outro código malicioso que infecta o navegador do computador do usuário, acessando seus cookies, histórico, senhas e logins salvos e até mesmo chaves para carteiras de criptomoedas. O arquivo também altera os registros de hosts do computador, permitindo que ao digitar um site bancário, por exemplo, o usuário seja redirecionado a outro site

O golpe se vale da curiosidade e da ansiedade das pessoas por conta da pandemia do Coronavírus, fazendo com que cliquem em muitos dos conteúdos que recebem, inadvertidamente. A curiosidade e o desespero fazem com que as pessoas acessem links e cliquem em conteúdos que podem ser códigos maliciosos, sem que percebam.

Vale mencionar, que os códigos maliciosos não infectam apenas computadores, mas também celulares, podemos citar o CovidLock e o CovidTraker que uma vez instalados sequestram os dados dos celulares e solicitam depósitos em Bitcoins em 48 horas para desbloquearem o smartphone (*ransonwares*).

Posto isso, todo cuidado é pouco, o indicado é baixar somente aplicativos do repositório oficial, dando preferência às informações de instituições conhecidas. Inclusive, é importante revogar as permissões desnecessárias de apps e usar

antivírus no celular também.

Foi verificado que boa parte dos antivírus já conseguem detectar o programa malicioso. A equipe da Reason Security divulgou um importante estudo sobre o código malicioso e disponibilizou um antivírus gratuito em https://www.reasonsecurity.com/essential. É possível, também, caso haja dúvida se um determinado programa executável é ou não trojan, acessar https://www.virustotal.com/gui/home/upload e submeter o arquivo. A plataforma avisa caso o arquivo tenha código malicioso embutido.

Outro link malicioso que circulou no WhatsApp diz respeito a uma suposta publicação da AmBev sobre a retirada de álcool gel. No entanto percebe-se que no link, a palavra que seria "relacionamento" está "re**ia**cionamento. O bandido normalmente faz este tipo de malícia para pegar usuário menos atentos. O link exibia o último acesso feito, propaganda em Instagram e em determinados momentos a página para coleta de dados pessoais.

Por fim, vale citar os cuidados em usar tecnologias de casa para o trabalho, é importante que a empresa forneça uma VPN para a equipe (o que promove uma camada a mais de segurança), estabeleça políticas de permissões restritivas para usuários que trabalharão de casa, capacite os trabalhadores sobre os riscos, instruindo-os a não clicarem em links ou baixarem arquivos, sobretudo nos dispositivos que possuem acesso à rede da empresa. Ademais, vale as recomendações de sempre, como a manutenção do Sistema Operacional que deve estar sempre atualizado, com antivírus e malware instalados, incluindo os dispositivos móveis.

Você conhece alguém que foi vítima de golpe ou fraude digital usando o nome COVID-19? Envie mensagem para consultor@josemilagre.com.br