EUA / Microsoft revela que uma das maiores invasões virtuais da história do país também atingiu alvos em seis nações. Suspeitas recaem sobre hackers russos ligados ao governo de Vladimir Putin. Agência que supervisiona arsenal nuclear pode ter sido afetada

Ataque cibernético além das fronteiras

» RODRIGO CRAVEIRO

As autoridades dos Estados Unidos descobriram que um ataque cibernético em massa contra agências do governo federal foi além das fronteiras norte-americanas e atingiu pelo menos seis países. Apesar de 80% dos afetados estarem baseados nos EUA, a Microsoft identificou vítimas na Bélgica, no Canadá, em Israel, no México, na Espanha e nos Emirados Árabes Unidos. O principal alvo da ciberinvasão foi um software de gestão de negócios utilizado por redes de computadores de agências governamentais de Washington produzido pela empresa de tecnologia SolarWinds, baseada no Texas. A companhia reconheceu que 19 mil clientes baixaram uma atualização do programa que continha o malware (software malicioso). "Isso não é 'espionagem como de costume', mesmo na era digital. Em vez disso, evidencia um ato de imprudência que criou uma séria vulnerabilidade tecnológica para os Estados Unidos e o mundo", advertiu Brad Smith, presidente da Microsoft. "Até agora, nosso estudo identificou vítimas de sete países. É certo que o número e a localização das vítimas continuarão a crescer", acrescentou.

Especialistas em segurança cibernética veem a marca de hackers russos ligados ao governo de Vladimir Putin. O ataque foi minucioso e levou pelo menos cinco meses desde o acesso ao servidor e a "inoculação" do malware. Uma notícia em particular causou preocupação. Os computadores do Departamento de Energia dos EUA foram acessados, o que pode ter exposto a Agência Nacional de Segurança Nuclear, responsável pelo gerenciamento do arsenal atômico. O presidente eleito, Joe Biden, condenou a invasão virtual, não culpou diretamente Moscou, mas avisou que adotará uma "estratégia de imposição de custos" em relação à Rússia. "Uma boa defesa não é suficiente. (...) Precisamos interromper e impedir que nossos adversários empreendam ataques cibernéticos significativos em primeiro lugar", declarou.

Congressistas democratas e republicanos criticaram o presidente Donald Trump pelo silêncio em relação ao escândalo. Alguns dos parlamentares questionaram se os ataques não equivaleriam a um "ato de guerra". "É extremamente preocupante que o presidente não pareça reconhecer, muito menos agir, ante a gravidade desta situação", afirmou Mark Warner, vice-presidente do Comitê de Inteligência do Senado.

Pesquisador de segurança cibernética em Nova Délhi, o indiano Vinoth Kumar (**leia Quatro perguntas para**) enviou um e-mail à SolarWinds em 19 de novembro de 2019, por meio do qual alertou-a sobre a brecha nos servidores. Em entrevista ao **Correio**, ele contou que o defeito foi corrigido pela empresa, que lhe enviou uma resposta três dias depois. "Olá, Vinoth. Obrigado por reportar o erro de configuração de modo responsável", escreveu a SolarWinds, ao explicar que o problema não estava mais acessível e que aplicou um "tratamento" às credenciais expostas. Segundo Kumar, o ataque exibe o potencial de causar danos por motivação política, além de vazamento de dados e comprometimentos à segurança nacional.

"A avaliação de danos não está completa. No entanto, sabemos que entre 15 e 20 agências de governos, além de várias empresas do setor privado, foram comprometidas. É possível que pelo menos 500 agências federais, companhias privadas, instituições educacionais e organizações sem fins lucrativos tenham sido ativamente afetadas em todo o mundo", explicou ao **Correio** Morgan Wright, conselheiro-chefe de Segurança da SentinelOne, uma companhia de cibersegurança que utiliza a inteligência artificial para defender redes de computadores, com sedes na Califórnia e na Virgínia.

Segundo Wright, os hackers exploraram o mecanismo de confiança na cadeia de suprimentos de softwares. "Primeiro, eles comprometeram a SolarWinds e seu servidor de atualização, ligado às ferramentas para gerenciar redes e bancos de dados. O código malicioso foi escondido dentro das atualizações e, em seguida, autorizado a ser instalado em centenas de sistemas. Muitas das táticas e ferramentas são similares às da agência de inteligência russa SVR", admitiu o especialista.

Eric Baradat/AFP - 13/3/20

A sede do Departamento do Tesouro, um dos órgãos federais aos quais os hackers tiveram acesso: mais de 19 mil clientes impactados

Quatro perguntas

VINOTH KUMAR, PESQUISADOR DE SEGURANÇA CIBERNÉTICA EM NOVA DÉLHI (ÍNDIA). FOI QUEM DESCOBRIU UMA VULNERABILIDADE NOS SERVIDORES DA EMPRESA SOLARWINDS

Arquivo Pessoal

Qual foi a vulnerabilidade descoberta pelo senhor em relação à empresa SolarWinds?

Eu descobri a senha do servidor de atualização da SolarWinds em novembro passado. Sou um caçador de bugs (falhas em programas). Encontrei as credenciais do servidor e reportei o fato à SolarWinds. O tema é que a empresa utilizava a senha "solarwinds123", que é a ausência básica de segurança.

Mas esta brecha de segurança estava ligada a este ataque cibernético específico?

O que encontrei foram as credenciais que eu poderia ter usado para fazer upload de um malware, ou seja, descarregar o programa malicioso no servidor de atualização do SolarWinds, como ocorreu com o ataque atual. Qualquer hacker poderia ter usado essas credenciais e realizado o mesmo tipo de ataque.

Qual foi sua reação quando soube deste ataque sem precedentes?

Quando li sobre o ataque usando a SolarWinds, eu imaginei que poderia ser qualquer pessoa. Pois a empresa não estava protegida e tinha uma segurança fraca. Quando avisei a empresa sobre esse problema, não sabia que a SolarWinds era uma grande empresa.

O senhor acredita que tratou-se de uma invasão cometida por hackers russos?

Eu não sei se foi um ataque russo. Mas trata-se de uma invasão sofisticada, indetectável e privilegiada. Fiquei impressionado com a paciência dos hackers, que inicialmente controlaram o servidor no fim de 2019, mas atacaram os serviços em maio e junho de 2020. (**RC**)

A invasão

Saiba mais sobre o ataque cibernético que deixou as autoridades norte-americanas em alerta.

"PORTA" PARA OS HACKERS

- Os invasores acessaram sistemas de computadores do governo dos EUA por meio de um popular software oferecido pela companhia SolarWinds, baseada no Texas. O sistema é utilizado por centenas de milhares de organizações em todo o mundo.

OS POTENCIAIS DANOS

- Ainda são avaliados. Até 19 mil clientes da SolarWinds teriam feito o download da atualização do programa de servidor contendo malwares (softwares maliciosos) instalados pelos hackers.

PRINCIPAIS ALVOS NOS EUA

DEPARTAMENTO DO TESOURO

- Os hackers instalaram um malware nos programas usados pelo Departamento do Tesouro, o que lhes permitiu visualizar o tráfego interno do correio eletrônico.

AGÊNCIA NACIONAL DE SEGURANÇA NUCLEAR

- As redes do organismo responsável por gerenciar o estoque de armamentos nucleares dos Estados Unidos podem ter sido comprometidas, de acordo com relatórios obtidos pelo jornal *The Washington Post* e pelo site Politico. A agência, no entanto, nega danos.

DEPARTAMENTO DE ENERGIA

- Os invasores acessaram algumas de suas redes usando o mesmo malware associado à brecha de segurança. A agência do governo isolou as redes de negócios e desconectou todos os softwares identificados como vulneráveis.

DEPARTAMENTO DE SEGURANÇA INTERNA

- As autoridades suspeitam de que o órgão também possa ter sido impactado pelo ataque.

ALVOS NO EXTERIOR

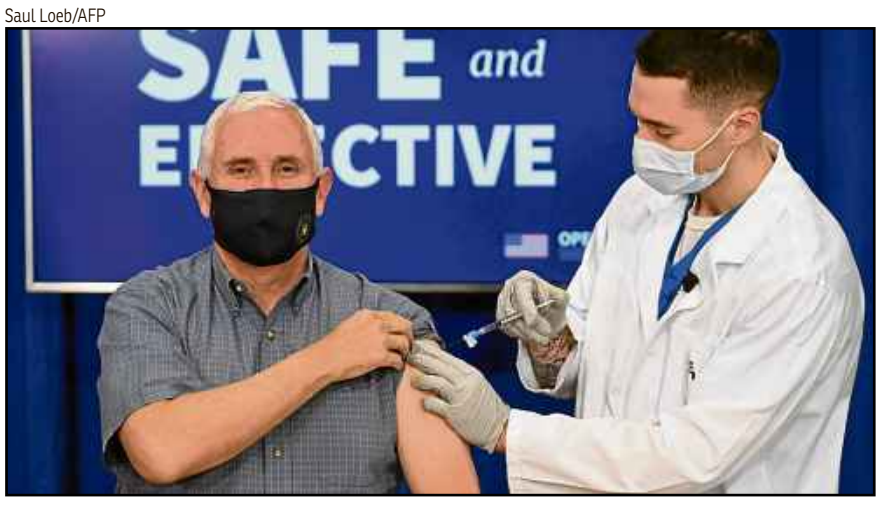
- A Microsoft identificou que pelo menos 40 dos seus clientes foram atingidos. Cerca de 80% deles estão baseados nos EUA, mas também houve empresas e órgãos de governo afetados no Canadá, México, Bélgica, Espanha, Reino Unido, Israel e Emirados Árabes Unidos.

PROVÁVEIS AUTORES

- Vários meios de comunicação dos EUA acusam o grupo russo "APT29", também chamado de "Cozy Bear". Segundo o jornal *The Washington Post*, o APT29 integra os serviços de inteligência da Rússia.

Pence e Pelosi são vacinados contra covid

Saul Loeb/AFP



Mike Pence, vice de Donald Trump, recebe a vacina da Pfizer/BioNTech: "Confiança"

Mike Pence, vice-presidente do governo Donald Trump e coordenador da força-tarefa de combate à pandemia da Casa Branca, recebeu, ontem, a vacina da Pfizer/BioNTech. A imunização do republicano foi transmitida em rede nacional de televisão, horas antes de a FDA — agência federal reguladora de medicamentos e alimentos — autorizar o uso emergencial também da vacina da Moderna. A aprovação foi anunciada na noite de ontem.

"Construir a confiança na vacina é o que nos traz aqui nesta manhã", declarou Pence. "Eu não senti nada. Foi bem-feito, e agradecemos seu serviço ao país. (...) O povo americano pode estar confiante: temos uma, e talvez dentro de algumas horas, duas vacinas contra o coronavírus seguras para você e sua família", acrescentou, em alusão ao imunizante da Moderna.

Além de Pence, a mulher dele, Karen, e o cirurgião-geral Jerome Adams foram imunizados. Trump não compareceu à cerimônia, no complexo da Casa Branca. Robert Redfield, diretor do Centro para Controle e Prevenção de Doenças (CDC), assistiu à imunização, aplicada por funcionários do Centro Nacional Médico Walter Reed, de Bethesda (Maryland).

Biden

O presidente eleito, Joe Biden, 78 anos, irá se vacinar na próxima segunda-feira, também em um ato público, a fim de afastar o ceticismo envolvendo a segurança do imunizante, anunciou seu porta-voz. "Na próxima segunda-feira, o presidente eleito e a mulher, Jill Biden, receberão a primeira dose da vacina Pfizer, em Delaware", informou Jen Psaki. A futura vice-presidente, Kamala Harris, deverá se vacinar na semana seguinte.

A presidente da Câmara dos Representantes, Nancy Pelosi, 80 anos, também foi imunizada ontem. Ela publicou duas fotos, em seu perfil no Twitter (*@SpeakerPelosi*), na qual aparecia recebendo a vacina no braço esquerdo e assinando um documento. "Hoje, com confiança na ciência, (...) recebi a vacina contra a covid-19. Enquanto a vacina for distribuída, devemos todos continuar a usar máscara e a adotar o distanciamento social, além de outros passos para salvar vidas e esmagar o vírus", escreveu a deputada, integrante do Partido Democrata.