EspanholConcursos

Microsoft admite que los ‘hackers’ vieron parte de su código fuente en el gran ataque contra organismos y empresas

---

TAREFAS DO ALUNO

Copiar texto. Quando possível, copie o primeiro parágrafo do texto.

Marcar palavras iguais e parecidas. Esta tarefa deve ser realizada antes da leitura e tradução do texto. Olhe para o texto e marque todas as palavras iguais e parecidas com as palavras da língua portuguesa.

Ler e traduzir: Leia o texto abaixo e o traduza. A tradução pode ser realizada no seu caderno, no seu computador ou mentalmente.

Montar vocabulário. Anote no seu caderno (ou outro local de sua preferência) todas as palavras que não conseguiu entender no momento da leitura. Anote também o significado dessas palavras.

TEXTO

Microsoft admite que los ‘hackers’ vieron parte de su código fuente en el gran ataque contra organismos y empresas

El ciberataque masivo que han sufrido desde la pasada primavera organismos públicos y empresas estadounidenses por parte supuestamente de hackers rusos

tuvo en Microsoft, una de las grandes compañías afectadas, más consecuencias de las hasta ahora conocidas. Los atacantes pudieron ver parte del código fuente —las instrucciones que constituyen la base del funcionamiento de los programas y de las páginas web— utilizado por la empresa, aunque no pudieron modificar ningún sistema ni tuvieron acceso a los datos de los clientes, según un comunicado publicado el jueves en el blog de la compañía.

Como en el resto de organismos atacados, los hackers utilizaron para introducirse en los sistemas las actualizaciones de un software de fontanería interna de sistemas informáticos elaborado por la empresa texana Solarwinds. "Detectamos actividad inusual en una pequeña cantidad de cuentas internas y después de revisarlas descubrimos que se había utilizado una de ellas para ver el código fuente en varios repositorios. La cuenta no tenía permisos para modificar ningún código o sistema de ingeniería y nuestra investigación confirmó además que no se realizaron cambios. Estas cuentas fueron investigadas y reparadas", asegura el comunicado de la compañía.

"Nuestra investigación interna no ha encontrado evidencia de acceso a servicios de producción o datos de clientes. La investigación, que está en curso, tampoco ha encontrado indicios de que nuestros sistemas se hayan utilizado para atacar a otros", continúa la empresa. Inicialmente, Microsoft aseguró que sus sistemas no habían sufrido ninguna brecha durante el ataque. La compañía no ha aclarado cuánto tiempo duró la infiltración de los hackers ni ha precisado qué código fuente de qué producto concreto pudieron espiar.

En cuanto a la responsabilidad por el ataque, el comunicado de Microsoft refuerza la idea de que ha sido auspiciado por alguna potencia extranjera. "Queremos ser transparentes y compartir lo que estamos aprendiendo mientras combatimos lo que

creemos que es un actor estatal muy sofisticado", asegura. El Gobierno ruso, sospechoso número uno de lanzar la operación, ha negado categóricamente estas acusaciones, calificadas por el Kremlin de "continuación de la rusofobia ciega". El ataque se ha destapado tres meses después de que el presidente ruso, Vladímir Putin, propusiera a EE. UU. una tregua para evitar incidentes en el ciberespacio.

El todavía presidente de EE. UU., Donald Trump, contradiciendo a sus propios servicios de inteligencia, aseguró hace días en Twitter que podría haber intereses ocultos en acusar a Rusia y sugirió la posible responsabilidad de China.

Aún se está evaluando el alcance del ciberataque. Durante más de medio año, los piratas estuvieron infiltrados en al menos seis departamentos gubernamentales de EE. UU., incluidos el de Defensa, el del Tesoro, el de Estado y el de Energía, además de otros muchos organismos oficiales y grandes empresas. El ataque se detectó cuando FireEye, una empresa privada de ciberseguridad dio la voz de alarma.

Fuente: El País - España (adaptado)

TEXTO – TRADUÇÃO LIVRE

Microsoft admite que los 'hackers' vieron parte de su código fuente en el gran ataque contra organismos y empresas

A Microsoft admite que os *'hackers'* viram parte do seu código fonte no grande ataque contra organismos e empresas

EspanholConcursos

El ciberataque masivo que han sufrido desde la pasada primavera organismos públicos y empresas estadounidenses por parte supuestamente de hackers rusos tuvo en Microsoft, una de las grandes compañías afectadas, más consecuencias de las hasta ahora conocidas. Los atacantes pudieron ver parte del código fuente —las instrucciones que constituyen la base del funcionamiento de los programas y de las páginas web— utilizado por la empresa, aunque no pudieron modificar ningún sistema ni tuvieron acceso a los datos de los clientes, según un comunicado publicado el jueves en el blog de la compañía.

O ciberataque[1] massivo que hão sofrido desde a primavera passada organismos públicos e empresas americanos por parte supostamente de *hackers* russos teve na Microsoft, uma das grandes companhias afetadas, mas consequências das até agora conhecidas. Os atacantes puderam ver parte do código fonte —as instruções que constituem a base do funcionamento dos programas e das páginas web— utilizado pela empresa, embora não pudessem modificar nenhum sistema nem tivessem acesso aos dados dos clientes, segundo um comunicado publicado na quinta-feira no blog da companhia.

Como en el resto de organismos atacados, los hackers utilizaron para introducirse en los sistemas las actualizaciones de un software de fontanería interna de sistemas informáticos elaborado por la empresa texana Solarwinds. “Detectamos actividad inusual en una pequeña cantidad de cuentas internas y después de revisarlas descubrimos que se había utilizado una de ellas para ver el código fuente en varios

[1] Em computadores e redes de computadores, um ciberataque, também chamado de ataque cibernético, é qualquer tentativa de expor, alterar, desativar, destruir, roubar ou obter acesso não autorizado ou fazer uso não autorizado de um dispositivo. (wikipedia)

repositorios. La cuenta no tenía permisos para modificar ningún código o sistema de ingeniería y nuestra investigación confirmó además que no se realizaron cambios. Estas cuentas fueron investigadas y reparadas", asegura el comunicado de la compañía.

Como no resto de organismos atacados, os *hackers* utilizaram para entrar nos sistemas as atualizações de um *software* de canalização interna de sistemas informáticos elaborado pela empresa texana Solarwinds. "Detectamos atividade incomum em uma pequena quantidade de contas internas e depois de revisá-las descobrimos que foi utilizado uma delas para ver o código fonte em vários repositórios. A conta não tinha permissões para modificar nenhum código ou sistema de engenharia e nossa investigação confirmou além disso que não se realizaram mudanças. Estas contas foram investigadas e reparadas", assegura o comunicado da companhia.

"Nuestra investigación interna no ha encontrado evidencia de acceso a servicios de producción o datos de clientes. La investigación, que está en curso, tampoco ha encontrado indicios de que nuestros sistemas se hayan utilizado para atacar a otros", continúa la empresa. Inicialmente, Microsoft aseguró que sus sistemas no habían sufrido ninguna brecha durante el ataque. La compañía no ha aclarado cuánto tiempo duró la infiltración de los hackers ni ha precisado qué código fuente de qué producto concreto pudieron espiar.

"Nossa investigação interna não há encontrado evidência de acesso a serviços de produção ou dados de clientes. A investigação, que está em curso, tampouco há encontrado indícios de que nossos sistemas foram utilizados para atacar outros", continua a empresa. Inicialmente, a Microsoft assegurou que seus sistemas não

haviam sofrido nenhuma brecha durante o ataque. A companhia não há esclarecido quanto tempo durou a infiltração dos *hackers* nem há especificado que código fonte de que produto concreto puderam espiar.

En cuanto a la responsabilidad por el ataque, el comunicado de Microsoft refuerza la idea de que ha sido auspiciado por alguna potencia extranjera. “Queremos ser transparentes y compartir lo que estamos aprendiendo mientras combatimos lo que creemos que es un actor estatal muy sofisticado”, asegura. El Gobierno ruso, sospechoso número uno de lanzar la operación, ha negado categóricamente estas acusaciones, calificadas por el Kremlin de “continuación de la rusofobia ciega”. El ataque se ha destapado tres meses después de que el presidente ruso, Vladímir Putin, propusiera a EE. UU. una tregua para evitar incidentes en el ciberespacio.

Quanto à responsabilidade pelo ataque, o comunicado da Microsoft reforça a ideia de que há sido auspiciado por alguma potência estrangeira. "Queremos ser transparentes e compartilhar aquilo que estamos aprendendo enquanto combatemos aquilo que acreditamos que é um ator estatal muito sofisticado", assegura. O governo russo, suspeito número um de lançar a operação, há negado categoricamente estas acusações, qualificadas pelo Kremlin de "continuação da *russofobia* cega". O ataque se há descoberto três meses depois de que o presidente russo, Vladímir Putin, propusesse para os Estados Unidos uma trégua para evitar incidentes no ciberespaço.

El todavía presidente de EE. UU., Donald Trump, contradiciendo a sus propios servicios de inteligencia, aseguró hace días en Twitter que podría haber intereses ocultos en acusar a Rusia y sugirió la posible responsabilidad de China.

O então presidente dos Estados Unidos, Donald Trump, contradizendo a seus próprios serviços de inteligência, assegurou no Twitter que poderia haver interesses ocultos em acusar a Rússia e sugeriu a possível responsabilidade da China.

Aún se está evaluando el alcance del ciberataque. Durante más de medio año, los piratas estuvieron infiltrados en al menos seis departamentos gubernamentales de EE. UU., incluidos el de Defensa, el del Tesoro, el de Estado y el de Energía, además de otros muchos organismos oficiales y grandes empresas. El ataque se detectó cuando FireEye, una empresa privada de ciberseguridad dio la voz de alarma.

Ainda se está avaliando o alcance do ciberataque. Durante mais de meio ano, os piratas estiveram infiltrados em pelo menos seis departamentos governamentais dos Estados Unidos, incluídos o da Defesa, o do Tesouro, o de Estado e o de Energia, além de outros muitos organismos oficiais e grandes empresas. O ataque se detectou quando FireEye, uma empresa privada de cibersegurança deu o alarme.