OUCH! | Abril de 2016

A Publicação Mensal de Sensibilizaçao de Segurança para Usuários de Computadores

OUCH!

NESTA EDIÇÃO...

Invadiram meu computador. E agora?

Visão Geral

Sabemos que você se preocupa em proteger seu computador e dispositivos móveis e toma medidas para protegê-los. No entanto, não importa o quão precavido ao usar a tecnologia você seja, mais cedo ou mais tarde você pode ter seu computador invadido ou "comprometido". Nesta edição você vai aprender como determinar se o seu computador ou dispositivo móvel foi invadido e, nesse caso, o que você pode fazer. Em última análise, quanto mais rápido você detectar que algo está errado e mais rápido você reagir, mais provável que você possa reduzir os danos que um criminoso cibernético pode causar.

Editor Convidado

Samantha Davison (**@sam_e_davison**) é Gerente do Programa de Educação e Conscientização de Segurança do Uber educando seus funcionários ao redor do mundo em mais de 350 cidades.

Pistas De Que Seu Computador Foi Invadido

Pode ser difícil determinar se você foi invadido pois normalmente não há uma maneira única para identificar isso. No entanto, os criminosos digitais costumam deixar várias pistas, muitas vezes chamados indicadores. Quanto mais seu sistema se assemelha a qualquer destas pistas, mais provável será que tenha sido invadido:

- O seu programa de anti-vírus gerou um alerta de que o seu sistema está infectado, especialmente se ele diz que não foi capaz de remover ou colocar em quarentena os arquivos afetados;
- A página inicial do seu navegador foi inesperadamente alterada ou o seu navegador está levando você para sites que você não deseja ir;
- Há novas contas de usuários em seu computador ou dispositivo que você não criou, ou novos programas em execução que você não instalou;
- O computador ou aplicações estão constantemente fechando inesperadamente, há ícones para aplicativos desconhecidos ou janelas estranhas aparecendo;
- Um programa solicita a sua autorização para fazer alterações no seu sistema, embora você não esteja instalando ou atualizando qualquer um dos seus aplicativos;
- A sua senha não funciona quando você tenta fazer login em seu sistema ou uma conta on-line, mesmo que você saiba que sua senha está correta;
- Amigos perguntam por que você está enviando e-mails estranhos que você sabe que nunca enviou;
- O seu dispositivo móvel gera cobranças indevidas para números de SMS;

Invadiram meu computador. E agora?

- O seu dispositivo móvel de repente tem inexplicável alto volume de dados ou alta utilização de bateria.

Como Reagir

Se você acredita que seu computador ou dispositivo foi invadido, quanto mais cedo você reage, melhor. Se o computador ou dispositivo foi fornecido a você por seu empregador ou é usado para o trabalho, não tente resolver o problema sozinho. Você pode não apenas causar mais mal do que bem, mas também destruir provas valiosas que podem ser utilizadas para uma investigação. Em vez disso, relate o incidente ao seu empregador imediatamente, entre em contato com o suporte, equipe de segurança ou supervisor. Se por algum motivo você não consegue entrar em contato com sua organização ou você está preocupado com a demora, desligue seu computador ou dispositivo da rede e, em seguida, hiberne, suspenda ou coloque no modo avião. Mesmo se você não tem certeza se você foi invadido, é muito melhor relatar logo no início apenas por precaução. Se o computador ou dispositivo é de uso pessoal, aqui estão alguns passos que você pode tomar.

Mais cedo ou mais tarde, seu computador ou dispositivo pode ser comprometido, quanto mais rápido você detecta um incidente e mais cedo você reage, melhor.

- Altere suas senhas: Isso inclui não apenas mudar as senhas em seus computadores e dispositivos móveis, mas para todas as suas contas online. Certifique-se de não usar o computador invadido para alterar as senhas. Em vez disso use um computador diferente ou dispositivo que você sabe que é seguro para alterar as senhas;
- Antivírus. Se o seu software de antivírus informá-lo de um arquivo infectado, você pode seguir as ações que ele recomenda. Isso geralmente pode incluir quarentena, limpeza ou exclusão do arquivo. A maioria dos softwares de antivírus exibirá links que você pode utilizar para aprender mais sobre a infecção específica. Em caso de dúvida, coloque em quarentena o arquivo. Se isso não for possível, então excluir será a melhor opção;
- Reinstale. Se você não conseguir remover a infecção ou quiser ter certeza absoluta de que seu sistema está ok, uma opção mais segura é a de reinstalá-lo. Para computadores, siga as instruções do fabricante do seu sistema. Na maioria dos casos, isso significa usar os utilitários internos para reinstalar o sistema operacional. Se esses utilitários estão faltando, corrompidos ou infectados, então entre em contato com o fabricante para obter orientação ou visite seu website. Não reinstale o sistema operacional a partir de backups, eles podem ter as mesmas vulnerabilidades que permitiram o criminoso digital ter acesso ao sistema. Backups só devem ser utilizados para recuperar os seus dados. Para dispositivos móveis siga as instruções do fabricante ou do provedor de serviço, estes devem estar em seu site. Em muitos casos, isso pode ser tão simples como restaurar o dispositivo móvel ao seu padrão de fábrica. Se você se sentir desconfortável com o processo de reinstalação, considere usar um serviço profissional para ajudá-lo. Ou se o seu computador ou dispositivo for antigo, pode ser mais simples e ainda mais barato comprar um novo. Finalmente, depois

Invadiram meu computador. E agora?

de ter reinstalado o seu computador ou dispositivo, ou comprado um novo, certifique-se que está totalmente atualizado e ative a atualização automática sempre que possível;

- Backups. O passo mais importante que você pode tomar para proteger-se é preparar backups regulares. Quanto mais vezes você fizer backup, melhor. Algumas soluções de backup copiam automaticamente quaisquer arquivos novos ou alterados a cada hora. Independentemente de qual solução de backup que você usa verifique periodicamente que você é capaz de restaurar esses arquivos. Muitas vezes recuperar seus dados a partir do backup é a única alternativa para restaurar o sistema após ser invadido;
- Chame a Polícia: Se você se sentir de alguma forma ameaçado, relate o incidente à polícia local.

Saiba Mais

Assine OUCH!, a publicação mensal de sensibilização de segurança, acesse os arquivos de OUCH! e saiba mais sobre as soluções SANS de sensibilização de segurança visitando nossa página em http://www.securingthehuman.org.

Versão Brasileira

Traduzida por: Homero Palheta Michelini, Arquiteto de T/I, especialista em Segurança da Informação - twitter.com/homerop
Michel Girardias, Analista de Segurança da Informação - twitter.com/michelgirardias
Marta Visser – Tradutora autônoma
Rodrigo Gularte, Administrador de Empresas, especialista em Segurança da Informação - twitter.com/rodrigofgularte

Recursos

Backups:	https://securingthehuman.sans.org/ouch/2015#august2015
Frases Secretas:	https://securingthehuman.sans.org/ouch/2015#april2015
O Que é um Malware:	https://securingthehuman.sans.org/ouch/2016#march2016
Tornando Seguro seu Novo Tablet:	https://securingthehuman.sans.org/ouch/2016#january2016

Board Editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Traduzida por: Homero Palheta Michelini, Michel Girardias, Rodrigo Gularte, Marta Visser

