OUCH! | Maio de 2014

A Publicação Mensal de Sensibilizaçao de Segurança para Usuários de Computadores

OUCH!

NESTA EDIÇÃO...

Fui Hackeado, e agora?

Visão Geral

Sabemos que você se preocupa com a proteção do seu computador e suas informações e toma medidas para protegê-las. No entanto, assim como ao dirigir um carro, não importa o quão seguro você o faça, mais cedo ou mais tarde você pode passar por um incidente. Neste texto, vamos ensinar-lhe o que procurar para determinar se o seu computador foi hackeado, e em caso positivo, o que fazer a respeito. Em última análise, quanto mais rápido você detectar que seu computador foi hackeado e mais rápido você agir, melhor você poderá mitigar qualquer dano a você ou sua empresa.

Editor Convidado

Jake Williams (**@MalwareJake**; **malwarejake.blogspot.com**) é cientista chefe da CSRgroup Computer Security Consultants. Ele também é o co-autor dos cursos Memory Forensics (FOR526) e Malware Reverse Engineering (FOR610) no SANS.

Indicadores de Comprometimento

Em primeiro lugar, é preciso entender que em muitos casos não há uma medida simples que determine que o seu computador foi invadido. Ao contrário, geralmente temos vários indicadores. Se você identificar uma combinação deles, implica que o seu computador está hackeado. Por exemplo:

- O seu programa anti-vírus emitiu um alerta informando que seu computador está infectado, principalmente se ele diz que não foi capaz de remover ou colocar em quarentena os arquivos afetados;
- A página inicial do seu navegador foi alterada inesperadamente ou o seu navegador está levando você para sites (páginas web) não solicitadas;
- Há novas contas de usuário em seu computador que você não criou;
- Há novos programas em execução que você não instalou;
- O seu computador está falhando constantemente ou muito lento;
- Um programa em seu computador pede sua autorização para fazer alterações no sistema, embora você não esteja instalando ou atualizando qualquer um dos seus aplicativos;
- Seu firewall alerta que um programa desconhecido está solicitando permissão para acessar a internet.

Como Responder

Se você acredita que seu computador foi comprometido, quanto mais cedo você responder, melhor. Se o computador que você está usando foi fornecido a você pelo seu empregador ou é usado para o trabalho, não tente consertá-lo sozinho e não desligue o computador. Além da possibilidade de piorar mais que ajudar, você poderia destruir provas

Fui Hackeado, e agora?

valiosas que podem ser utilizadas para uma investigação. Pelo contrário, relate o incidente ao seu empregador imediatamente, geralmente contactando o help desk, a equipe de segurança ou um supervisor. Se por algum motivo você não puder contactar a organização, ou se estiver preocupado com a demora, desconecte seu computador da rede e, em seguida, coloque-o em modo de suspensão ou hibernação. Mesmo que você não tenha certeza que foi hackeado, é muito melhor relatar por via das dúvidas. Sua organização provavelmente tem processos e uma equipe para lidar com situações como esta, portanto deixe que eles lidem com o problema.

Mais cedo ou mais tarde, o seu computador pode ser comprometido. Quanto mais rápido você detectar um incidente e quanto mais cedo responder, melhor.

Se o computador é de uso pessoal, aqui estão alguns passos que você pode tomar por conta própria:

- **Backups.** O passo mais importante que você pode tomar é o de fazer backups (cópias de segurança) antecipadamente. Faça backup específico dos seus dados regularmente e verifique periodicamente se você é capaz de restaurar os arquivos do seu backup. Muitas vezes, quando um computador é afetado, a única opção que resta é apagar todo o disco rígido do sistema e reinstalar o sistema operacional, ou comprar de um novo computador. De qualquer forma, você precisa de seus backups para recuperar seus dados pessoais;
- **Mude suas senhas:** Certifique-se de mudar todas as suas senhas. Isso inclui não apenas as senhas em seus computadores e dispositivos móveis, mas todas as suas senhas online. Tenha certeza que você altere todas as suas senhas on-line a partir de um computador diferente, que você sabe que é confiável e seguro;
- **Anti-vírus.** Se o seu software anti-vírus alerta sobre um arquivo infectado, você pode seguir as ações que ele recomenda. Isso geralmente pode incluir a colocação do arquivo em quarentena, a limpeza do arquivo ou sua remoção. A maioria dos softwares anti-vírus terá links que você pode seguir para saber mais sobre a infecção específica. Quando em dúvida, coloque o arquivo em quarentena. Se isso não for possível, então apague-o;
- **Re-instalação.** Se não for possível limpar o computador com anti-vírus, uma das maneiras mais seguras para recuperar é reconstruir o computador a partir do zero. Primeiro desconecte seu computador da rede. Em seguida, siga as instruções do fabricante do seu sistema, na maioria dos casos isso significa usar a partição de recuperação pré-configurada para reinstalar o sistema operacional. Se a partição de recuperação estiver ausente, corrompida ou infectada, entre em contato com o fabricante e solicite o envio de um DVD de recuperação. Não reinstale o sistema operacional a partir de backups. Seus backups podem conter as mesmas vulnerabilidades que permitiram o acesso original ao hacker. A única coisa que você deve recuperar em seus backups são seus dados pessoais. Além disso, se o seu computador é velho ou ultrapassado, pode

Fui Hackeado, e agora?

ser mais simples (e talvez até mais barato) comprar um computador novo do que tentar dedicar horas para reconstruí-lo;

- **Ajuda Profissional:** Se você acha que você foi hackeado e sente que não tem as habilidades ou conhecimento necessário para corrigi-lo, você pode querer encaminhar o seu computador a um profissional. Por exemplo, depois de ter sido hackeado você pode perceber que seus backups estão incompletos ou desatualizados. Você pode ficar tentado a transferir arquivos críticos, tais como fotos, documentos ou vídeos entre o seu computador infectado e uma nova máquina. No entanto, ao fazer isso, você pode inadvertidamente transferir malware e infectar seu computador novo ao mesmo tempo. Uma alternativa muito mais segura é encaminhar o computador infectado para um técnico qualificado, que pode recuperar esses arquivos com segurança, sem correr o risco de transferir a infecção.

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
Katia Lucia da Silva, Arquiteta de T/I, Tradutora - twitter.com/kl_silva

Recursos

OUCH! Backups:	http://www.securingthehuman.org/ouch/2013#september2013
OUCH! Senhas:	http://www.securingthehuman.org/ouch/2013#may2013
OUCH! O que é Malware:	http://www.securingthehuman.org/ouch/2014#february2014
Detecting Evil Pôster (em Inglês):	https://digital-forensics.sans.org/media/poster_2014_find_evil.pdf

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