A Publicação Mensal de Sensibilizaçao de Segurança para Usuários de Computadores

OUCH!

NESTA EDIÇÃO...

O que é um Antivírus?

Visão geral

Antivírus é um programa de segurança que você instala no seu computador ou dispositivo móvel para protegê-lo de infecções por malware. O termo “malware” é uma expressão que engloba qualquer tipo de software malicioso tais como vírus, worms, cavalos de Tróia e spyware. Na verdade, o termo malware vem da combinação das palavras mal-intencionado e software. Se o seu computador foi infectado por malware, um atacante cibernético pode capturar todas as teclas digitadas, roubar seus documentos ou usar o seu computador para atacar outros. Ao contrário do que algumas pessoas acreditam, qualquer sistema operacional, incluindo o Mac OS X e Linux, pode ser infectado.

Editor Convidado

Jake Williams é o fundador da Rendition Infosec (**www.renditioninfosec.com**) e é um instrutor certificado do SANS e autor de curso. Ele participa ativamente no **TwitterMalwareJake** e escreve em seu blog no **malwarejake.blogspot.com**.

Você pode comprar o software antivírus como uma solução independente, ou ele pode já estar incluído como parte de um pacote de segurança. O problema é que o antivírus já não consegue acompanhar os atacantes cibernéticos, pois eles estão constantemente desenvolvendo e lançando novos tipos de malware. Há tantas novas versões de malware lançados a cada dia que nenhum programa antivírus pode detectar e proteger contra todos eles. É por isso que é importante que você entenda que embora um antivírus ajude a proteger seu computador, ele não consegue detectar ou interromper todos os tipos de malware. Para entender melhor o porquê, vamos dar uma olhada em como a maioria desses programas funciona.

Como Antivírus funciona

Em geral, existem duas maneiras para o software antivírus identificar um malware; detecção da assinatura e detecção de comportamento. Detecção de assinatura funciona como o sistema imunológico humano. Ele faz uma varredura no seu computador em busca de características ou assinaturas de programas maliciosos conhecidos. Ele faz isso utilizando um dicionário de malwares conhecidos. E se algo em seu computador corresponder a um padrão do dicionário, o antivírus tenta neutralizá-lo. Como o sistema imunológico humano, a abordagem do dicionário requer atualizações, como vacinas contra a gripe, para proteger contra novos tipos de malware. O antivírus só pode proteger contra o que ele reconhece como prejudicial. O problema é que os atacantes cibernéticos estão desenvolvendo novos malwares tão rápidamente que os fornecedores de antivírus não conseguem manter-se atualizados. Como resultado, não importa o quão recentemente o seu antivírus foi atualizado, há sempre alguma nova variante do malware que pode potencialmente iludir o seu software antivírus.

O que é um Antivírus?

Com comportamento de detecção, o Antivírus não tenta identificar malware conhecido, mas monitora o comportamento do software instalado no computador. Quando um programa age de forma suspeita, como em uma tentativa de acessar um arquivo protegido ou modificar um programa, o software antivírus baseado no comportamento vê a atividade suspeita e gera um alerta. Esta abordagem fornece proteção contra novos tipos de malware que ainda não existem em nenhum dicionário. O problema com esta abordagem é que ela pode gerar avisos falsos. Você, o usuário do computador, pode não ter certeza sobre o que permitir ou não e ao longo do tempo torna-se insensível a todos os avisos. Você pode ser tentado a clicar em "Aceitar" em cada aviso, deixando seu computador aberto a ataques e infecção. Além disso, no momento em que o comportamento é detectado, o malware provavelmente já foi executado em sua máquina e você pode não saber quais ações ele executou antes do software anti-vírus tê-lo identificado.

Embora o Antivírus seja um elemento importante de sua segurança, ele não consegue detectar ou parar todos os ataques. Em última instância você é a melhor defesa, e não apenas a tecnologia.

O Antivírus é uma parte importante na proteção do seu computador e dispositivos móveis e, sempre que possível, recomendamos que você instale e use-o ativamente. No entanto, o principal ponto a se lembrar é que, independentemente de como o seu anti-vírus funciona, ele nunca irá protegê-lo de todos os tipos de malware. Em última instância, você, e não apenas a tecnologia, é a melhor defesa contra os invasores cibernéticos hoje em dia.

Dicas Antivírus

1. Obtenha software antivírus só a partir de fontes e fornecedores confiáveis. É comum os atacantes cibernéticos distribuírem programas antivírus falsos que na verdade são malware;
2. Certifique-se de ter a última versão do seu software antivírus instalado, que a sua assinatura anual foi paga e está ativa e seu antivírus está configurado para atualizar-se automaticamente. Se o seu computador tiver passado muito tempo desconectado da Internet ou desligado, seu software antivírus vai precisar se atualizar quando você ligá-lo, ou conectá-lo à Internet, novamente. Não deixe essas atualizações para depois;
3. Certifique-se de que seu antivírus verifica automaticamente mídias portáteis, como pen drives USB, e que a proteção em tempo real está habilitada;
4. Preste atenção aos avisos e alertas gerados pelo seu software antivírus. A maioria dos alertas inclui a opção de obter mais informações ou uma recomendação sobre o que fazer a seguir. Se você receber um alerta em um computador fornecido pela empresa onde trabalha, não deixe de entrar em contato com o suporte técnico ou o seu supervisor imediato;
5. Não desative ou desinstale o software antivírus por achar que ele está diminuindo a velocidade do seu computador, bloqueando o acesso a um site ou impedindo a instalação de um aplicativo ou programa. Desativar o antivírus vai expô-lo a riscos desnecessários e pode resultar em um sério incidente de segurança. Se o problema persistir em um computador

O que é um Antivírus?

de trabalho, contate o seu help desk. Se os problemas persistirem em seu computador pessoal, tente entrar em contato com o fornecedor do seu antivírus, obtendo informações no seu site, ou substituir o seu antivírus por outro;

6. Não instale vários programas antivírus no seu computador ao mesmo tempo. Se o fizer, provavelmente fará com que os programas entrem em conflito uns com os outros e isso poderá até reduzir a segurança do seu computador;
7. Aprenda a reconhecer os avisos que o seu software antivírus produz. Atacantes cibernéticos podem configurar sites maliciosos que postam avisos antivírus falsos mas muito realistas e se oferecem para ajudá-lo a "consertar" o computador. Ao clicar nesses links ou botões, esses sites podem prejudicar o seu computador.

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

Comparações de produtos Antivírus (em Inglês):	http://www.av-test.org/en/
Engenharia social:	http://www.securingthehuman.org/ouch/2014#november2014
Email ataques de phishing:	http://www.securingthehuman.org/ouch/2013#february2013
Fui Hackeado, e agora?:	http://www.securingthehuman.org/ouch/2014#may2014

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