A Publicação Mensal de Sensibilizaçao de Segurança para Usuários de Computadores

OUCH!

NESTA EDIÇÃO...

O que é um Malware

Visão geral

Você pode ter ouvido termos como vírus, trojan, ransomware ou rootkit quando pessoas discutem sobre segurança cibernética. Todas essas palavras descrevem a mesma coisa: tipos de programa usados por criminosos cibernéticos para infectar computadores e outros dispositivos. Um termo comum utilizado para descrever todos esses programas diferentes é malware. Nesta edição vamos explicar o que é um malware, quem o cria e por quê. E o mais importante, o que você pode fazer para se proteger.

Editor Convidado

Lenny Zeltser se dedica à proteção da operação de T/I das empresas, na NCR Corp. E leciona combate a malware no SANS Institute. Lenny participa ativamente do Twitter como **@lennyzeltser** e mantém um blog de segurança em **zeltser.com**.

O que é um Malware ?

De forma simples, malware é um software – programa de computador – usado para desenvolver atividades maliciosas. De fato a palavra malware é a combinação das palavras malicioso (malicious) e software. Criminosos cibernéticos instalam malware no seu computador ou dispositivo para obter controle sobre ele ou ter acesso ao seu conteúdo. Uma vez instalado, os atacantes o utilizam para espionar suas atividades online, roubar suas senhas ou arquivos, ou utilizar seu equipamento para atacar outras pessoas. Um malware pode até bloquear o acesso aos seus próprios arquivos, fazendo com que tenha que pagar um resgate ao atacante para recuperar o acesso a eles.

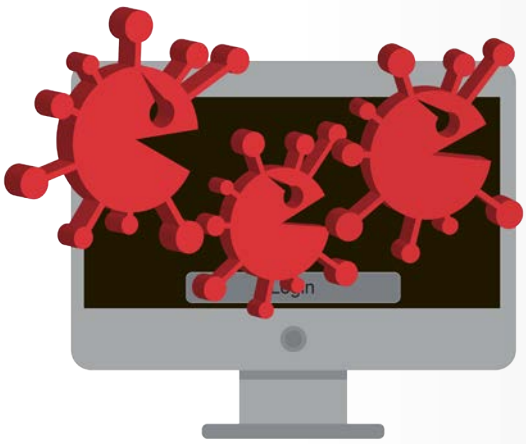
Muitas pessoas se equivocam ao acreditar que o malware é um problema apenas de computadores Windows. O windows é amplamente utilizado – e por isso um grande alvo, mas um malware pode infectar qualquer dispositivo, incluindo computadores Mac, smartphones ou tablets. Quanto mais computadores e dispositivos os criminosos infectam, mais dinheiro podem fazer. Portanto todo mundo é um alvo, inclusive você.

Quem cria um Malware ?

O malware não é mais criado apenas por hobbyistas ou hackers amadores, mas por criminosos virtuais sofisticados. Seus objetivos são fazer dinheiro com seu computador ou dispositivo infectado, talvez vendendo os dados roubados de você, enviando e-mails de SPAM, enviando ataques de DoS (Denial of Service) ou fazendo extorsão. As pessoas que criam, distribuem e se beneficiam com o malware podem ser desde indivíduos agindo por conta própria, grupos criminosos bem organizados ou

O que é um Malware

até organizações governamentais. As pessoas que criam os malwares sofisticados de hoje em dia estão muitas vezes dedicadas a esse propósito, desenvolvendo malware como seu trabalho de tempo integral. Além disso, uma vez desenvolvido seu malware, eles muitas vezes o vendem para indivíduos ou organizações e até fornecem suporte regular e atualizações para seus "clientes".



Proteja-se do malware sendo cético com mensagens suspeitas, mantendo seus dispositivos atualizados e com antivírus também atualizado, sempre que possível.

Como se proteger

Um passo comum para se proteger é instalar um software antivírus de um fornecedor confiável. Essas ferramentas, muitas vezes chamadas software anti-malware, são desenvolvidas para detectar e parar o malware. Entretanto, o antivírus não consegue bloquear ou remover todos os programas maliciosos. Os criminosos cibernéticos estão constantemente inovando, desenvolvendo novos e sofisticados malwares, capazes de impedir sua detecção. Em contrapartida, os fornecedores de antivirus estão constantemente atualizando seus produtos com novas capacidades de detecção de malware. De muitas formas isso tem se tornado uma corrida armamentista, com ambos os lados tentando despistar o oponente. Infelizmente os criminosos estão normalmente um passo à frente. Como você não pode confiar no antivírus sozinho, aqui vão algumas recomendações para sua proteção:

- Criminosos cibernéticos frequentemente infectam computadores ou dispositivos pela exploração de vulnerabilidades no seu software. Quanto mais atualizado seu software estiver, menos vulnerabilidades seu sistema tem e mais difícil fica para os criminosos o infectarem. Portanto, certifique-se de que seu sistema operacional, aplicativos e dispositivos têm suas atualizações automáticas habilidadas;
- Uma forma comum utilizada pelos criminosos cibernéticos para infectar dispositivos móveis é a criação de aplicativos falsos e sua publicação na Internet para levar pessoas a baixar e instalá-los. Por isso, só baixe e instale aplicativos de lojas de aplicativos confiáveis. E adicionalmente, só instale aplicativos móveis que estejam publicados há bastante tempo, tenham sido baixados por um número grande de pessoas e tenham sido avaliados positivamente por muitas pessoas;
- Nos computadores, utilize uma conta padrão com privilégios limitados ao invés de contas privilegiadas como "administrador" ou "root". Isso provê proteção adicional ao impedir que muitos tipos de malware se instalem sozinhos no seu computador;
- Criminosos cibernéticos muitas vezes enganam as pessoas levando-as a Instalar um malware para eles. Por exemplo, eles podem lhe enviar um e-mail que parece legítimo e contém um documento anexo ou um link. Talvez o e-mail pareça

O que é um Malware

vir do seu banco ou de um amigo. No entanto, se você abre o anexo ou clica no link, você ativa o código malicioso que instala o malware no seu sistema. Se uma mensagem cria um forte senso de urgência, é confusa, ou parece boa demais para ser verdade, provavelmente é um ataque. Suspeite, o bom senso é muitas vezes a sua melhor defesa;

- Faça backup regular do seu sistema e arquivos em serviços baseados em nuvem ou dispositivos desconectados como discos externos de dados. Isso protege seus dados em caso de um malware tentar encriptá-los ou apagá-los. O backup é um passo crítico pois são muitas vezes o único recurso de recuperação de uma infeção por malware.

Resumidamente, a melhor forma de se defender contra um malware é manter seu sistema atualizado, instalar um antivírus confiável de um fornecedor conhecido e estar alerta às tentativas de enganá-lo para infectar seu sistema.

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

Recursos

Phishing:	https://securingthehuman.sans.org/ouch/2015#december2015
Engenharia Social:	https://securingthehuman.sans.org/ouch/2014#november2014
Usando Aplicativos Móveis de Forma Segura:	https://securingthehuman.sans.org/ouch/2015#january2015
Tornando Seguro seu Novo Tablet:	https://securingthehuman.sans.org/ouch/2016#january2016
Cópia de Segurança (Backup) e Restauração:	https://securingthehuman.sans.org/ouch/2015#august2015

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