OUCH! | Fevereiro de 2014

A Publicação Mensal de Sensibilização de Segurança para Usuários de Computadores

OUCH!

NESTA EDIÇÃO...

O que é Malware

Visão Geral

Você já deve ter ouvido os termos vírus, worm, Cavalo de Tróia ou rootkit em discussões sobre segurança cibernética (ou segurança das redes de computadores). Esses termos descrevem tipos de programas utilizados por crimonosos virtuais para infectar e controlar computadores e dispositivos móveis. Hoje em dia esses diferentes termos são simplesemente chamados de Marlware. Nesta Newsletter vamos explicar o que é um malware, quem o desenvolve, por que e o que você pode fazer para se proteger.

Editor Convidado

Lenny Zeltser dedica-se a proteger as operações de TI dos clientes na corporação NCR e ensina a combater malware no Instituto SANS. Lenny pode ser encontrado no Twitter como **@lennyzeltser** e escreve sobre segurança em seu blog: **blog.zeltser.com**.

O que é Malware

Em termos práticos, Malware é um software, um programa de computador utilizado para realizar ações maliciosas. Na verdade o termo malware é uma combinação das palavras malicious e software em inglês. O objetivo final da maioria dos criminosos virtuais é instalar o malware em seu computador ou dispositivo móvel. Uma vez instalado, esses criminosos podem potencialmente obter controle total sobre esses equipamentos. Muitas pessoas têm a concepção errônea de que malware é um problema apenas de computadores com sistema operacional Windows. Embora o Windows seja amplamente utilizado, e portanto um grande alvo, o malware pode infectar qualquer dispositivo computadorizado, inclusive smartphones e tablets. Na verdade, a prevalência de software malware que infecta dispositivos móveis está aumentando de maneira constante. Além disso, lembre-se de que qualquer um pode ser alvo, inclusive você. Quanto mais computadores e dispositivos móveis os criminosos virtuais infectarem, mas dinheiro eles irão ganhar. Em geral esses crimonosos não se importam com quem eles irão infectar, desde que seja o maior número possível.

Quem e Por que

O malware já não é mais criado apenas por entusiastas curiosos ou hackers amadores, mas por crimonosos virtuais sofisticados que os ajudam a atingir objetivos específicos. Esses objetivos podem incluir o roubo a dados confidenciais, a coleta de logins e senhas, o envio de mensagens spam, o lançamento de ataques de negação de serviço (DoS), a extorção ou o roubo de identidade. Por exemplo, o malware conhecido como Cryptolocker é utilizado por crimonosos virtuais para infectar e encriptar todos os arquivos em seu computador. Uma vez infectado e encriptado, esses crimonosos então exigem um resgate em troca para decriptar seus arquivos.

As pessoas que criam, implementam e se beneficiam do malware variam de indivíduos agindo por conta própria a grupos de criminosos bem organizados ou organizações governamentais. Além disso, as pessoas que criam os atuais malware sofisticados são, com frequência, dedicadas a este propósito, para

O que é Malware

elas, desenvolver malware é um trabalho de tempo integral. Na realidade, assim que elas desenvolvem seus malwares, elas por vezes os vendem a outros individuos ou organizações e fornecem atualizações regulares e suporte a seus “clientes”. Uma vez adquirido, outros crimonosos podem ganhar dinheiro com a instalação do malware em milhões de sistemas de vítimas inocentes, criando uma botnet de sistemas infectados. Essa botnet torna-se um exército controlado remotamente, a qual os crimonosos virtuais podem então utilizar para seus prórpios fins, ou vender os computadores infectados a outros crimonosos.

A melhor maneira de se proteger contra malware é garantindo que seus equipamentos estejam atualizados, tenham, se possível, a versão atual de antivirus e, finalmente, fique alerta aos ataques.

Proteja-se

Uma medida comum para proteger seu computador e dispositivos móveis de um malware é instalar software antivirus de fornecedores confiáveis. O antivírus, às vezes chamado de anti-malware, é um software de segurança desenhado para detectar e parar o software malicioso. Entretanto, os antivirus não bloqueiam ou removem todo malware. Os crimonosos cibernéticos estão constantemente inovando e desenvolvendo novos e mais sofisticados ataques que podem contornar os programas antivirus. Por sua vez, os fornecedores de antivirus estão constantemente atualizando seus produtos com novas capacidades para detectar malware. Em muitos aspectos, isso se transformou numa corrida armamentista, com ambos os lados tentando passar a perna no outro. Infelizmente, os crimonosos virtuais quase sempre levam vantagem. Sendo assim, lembre-se que enquanto os antivirus podem detectar e bloquear uma série de malwares, os criminosos estão sempre criando novas versões que não serão encontradas. Como resultado, você não deve confiar apenas no antivirus para se protejer, mas sim tomar medidas adicionais.

Em primeiro lugar, garanta que seu sistema operacional e aplicativos estejam habilitados para instalar atualizações de segurança automaticamente. Quanto mais atualizado seu software estiver, mais difícil será para os crimonosos virtuais infectarem seu computador ou dispositivos móveis.

Em segundo lugar, lembre-se de que você é um dos melhores defensores contra o malware. A infecção por malware com frequência envolve engenharia social, que nada mais é do que os crimonosos trapaceando ou induzindo-o a instalar o malware por eles. Um exemplo comum são os ataques por fishing, os quais são emails que parecem legítimos, mas na verdade são falsos, criados para lhe enganar, com o objetivo de infectar seu computador. Por exemplo, um crimonoso virtual pode lhe enviar um email em nome do seu banco, solicitando que você clique em um link. Se você clicar no link, será direcionado a uma página na Internet que automaticamente tenta invadir e infectar seu computador. Ou talvez eles lhe enviem um email informando que determinada encomenda não pode ser entregue e solicite que você abra um documento anexado que, depois de aberto, irá infectar seu computador.

O que é Malware

Ataques por engenharia social também ocorrem por meio de outras tecnologias, como o telefone. Por exemplo, os hackers podem ligar fingindo ser do suporte técnico da Microsoft e informa-lo que seu computador está infectado. A história deles é uma mentira, seu computador provavelmente está bem. O objetivo deles é induzi-lo a acreditar que seu equipamento está infectado e convencê-lo a dár-lhes acesso remoto a seu sistema ou a comprar seus softwares de segurança, que nada mais são que malware. Use o bom senso, se um telefonema ou mensagem parecer estranha, suspeita o muito boa para ser verdade, há grandes chances de que seja um ataque.

Por fim, a melhor maneira de se defender contra o malware é manter seus programas atualizados, instalar programas antivirus confiáveis de fornecedores conhecidos e ficar alerta a qualquer um que tente lhe induzir a infectar seu próprio 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
Katia Lucia da Silva, Arquiteta de T/I, Tradutora - twitter.com/kl_silva

Recursos

OUCH Phishing:

www.securingthehuman.org/resources/newsletters/ouch/2013#february2013

OUCH Proteja seu computador:

www.securingthehuman.org/resources/newsletters/ouch/2012#december2012

Você é o Alvo:

http://www.securingthehuman.org/resources/posters

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