A Publicação Mensal de Sensibilizaçao de Segurança para Usuários de Computadores

Pare aquele Malware

Visão Geral

Você provavelmente ouve termos como vírus, Trojan, ransomware ou rootkit quando as pessoas falam de segurança cibernética. Eles são tipos diferentes de programas maliciosos, chamados malware, que os criminosos cibernéticos utilizam para infectar seus computadores e outros dispositivos. Uma vez instalados, eles dão acesso ao que quiserem. Descubra o que é um malware, que perigo ele oferece e, o mais importante, o que você pode fazer para se proteger.

O que é Malware?

De forma simples, malware é um software – um programa de computador, usado para fazer coisas maliciosas. Esse termo é uma combinação das palavras malicious e software. Os criminosos cibernéticos instalam malware nos seus computadores ou dispositivos para obter controle sobre ele. Uma vez instalado, o malware pode permitir que eles espionem suas atividades online, roubem suas senhas ou arquivos, ou utilizem seu sistema (seu computador) para atacar outras pessoas. Um Malware pode até tomar o controle dos seus arquivos e exigir que você pague um resgate para tê-los de volta. Muitas pessoas acreditam que o malware é um problema apenas de computadores Windows. Infelizmente os malwares podem infectar qualquer dispositivo, desde computadores Mac até smartphones ou DVR e câmeras de segurança. Quanto mais computadores e dispositivos os criminosos cibernéticos infectarem, mais dinheiro eles poderão fazer. Portanto, todo mundo é um alvo, inclusive você.

Proteja você mesmo – Pare o Malware

Você pode pensar que tudo que tem que fazer é instalar um programa de segurança, como um antivírus e você estará protegido contra infecções. Infelizmente os antivírus não param todos os malwares. Os criminosos cibernéticos estão desenvolvendo constantemente malwares novos e mais sofisticados, que podem evadir uma detecção. Em contrapartida, fabricantes de antivírus estão constantemente atualizando seus produtos com novas capacidades de detecção de malware. Em muitos aspectos, isso tornou-se uma corrida armamentista. E os criminosos estão normalmente um passo à frente. Como você não pode confiar em um antivírus isoladamente, aqui vão os passos necessários para proteger você mesmo:

Os criminosos cibernéticos frequentemente infectam computadores ou dispositivos explorando vulnerabilidades no software do dispositivo. Quanto mais atualizado estiver este software, menos vulnerabilidades terão seus sistemas e mais difícil será para os criminosos o infectarem. Certifique-se de que seus sistemas operacionais, aplicações, navegadores e plugins e todos os seus dispositivos estão atualizados. A forma mais fácil de garantir isso é habilitando as atualizações automáticas sempre que possível;

Uma forma comum utilizada pelos criminosos cibernéticos para infectar computadores ou dispositivos móveis é criando um programa de computador ou aplicativo móvel falso, publicá-lo na Internet e enganar você para que baixe e instale um deles. Só baixe e instale programas e aplicativos de lojas online seguras. Além disso, fique longe de aplicativos móveis novos, com poucas revisões positivas, atualizados raramente ou com pouca quantidade de download feito por outras pessoas. Não utiliza mais um programa ou aplicativo móvel ? Remova-o;

Criminosos cibernéticos frequentemente enganam pessoas fazendo-as instalar malware. Por exemplo, eles podem enviá-lo um e-mail que parece legítimo, contendo um anexo ou um link. Talvez ele pareça ter vindo de um banco ou amigo. Contudo, se você abre o anexo ou clica no link, você ativa um código malicioso que instala malware no seu sistema. Se uma mensagem cria um forte senso de urgência ou parece boa demais para ser verdade, pode ser um ataque. Seja desconfiado. O bom senso é a sua melhor defesa;

Mantenha backups regulares dos seus sistemas e arquivos, em serviços baseados em nuvem. Ou armazene-os em dispositivos desconectados da sua rede, como discos de dados externos. Isso protege seus backups em caso de um malware tentar encriptar ou apagá-los. Backups são críticos. Eles são muitas vezes sua única forma de recuperar dados de uma infecção por malware.

Resumidamente, a melhor forma de se defender de malware é manter todos os seus softwares atualizados, instalar um antivírus de confiança quando possível e estar alerta sobre qualquer tentativa de golpe para conduzi-lo a infectar seu sistema. E quando tudo falhar, a restauração do backup é muitas vezes a única forma de recuperação.

Editor Convidado

Lenny Zeltser *combate malware criando produtos de segurança na Minerva Labs e ensinando segurança no SANS Institute. Lenny é ativo no Twitter como @lennyzeltser e mantem um blog de segurança em zeltser.com.*

Recursos

Ransomware:	https://www.sans.org/u/EdI
Backups:	https://www.sans.org/u/EdN
Pare esse Phishing:	https://www.sans.org/u/EdS