SAIBA TUDO SOBRE MALWARE E COMO SE PROTEGER DESSA AMEAÇA

ostec
Segurança digital de resultados

Nesse e-book apresentaremos tudo sobre malwares, desde a seu surgimento até os dias de hoje e dicas de como se proteger.

ÍNDICE

3 PROPÓSITO DO E-BOOK

4 O QUE É MALWARE

5 HISTÓRICO E EVOLUÇÃO DO MALWARE

9 TIPOS DE MALWARE

10 COMO DETECTAR UM MALWARE?

14 COMO MINHA MÁQUINA PODE TER SIDO INFECTADA POR MALWARE?

16 DICAS PARA SE PROTEGER DE MALWARES

PROPÓSITO DO EBOOK

Você já ouvir falar sobre malware? Sabe do que se trata?

Malware é uma palavra que causa pânico em qualquer organização que lide com dados críticos.

Ninguém está 100% seguro quando se trata de malwares, pois já passou o tempo em que malwares eram mal feitos e não tão perigosos. Os cibercriminosos profissionais estão sempre trabalhando e se emprenhando em invadir computadores e sistemas de organizações.

Eles fazem uso de táticas profissionais para dificultar a detecção desses malwares, para roubar informações confidenciais e exigir recompensas das vítimas.

Essas ameaças se multiplicam a cada instante e possuem inúmeras variações. Sua principal característica é infectar os computadores e dispositivos de várias maneiras, assumindo diversas formas.

Mas então como se proteger dessas ameaças? Como agir caso seja infectado?

Nesse e-book apresentaremos tudo sobre malwares, desde a seu surgimento até os dias de hoje e dicas de como se proteger.

Boa leitura!

O QUE É MALWARE

Malware, é um termo mais amplo que descreve qualquer programa ou código malicioso que seja prejudicial aos sistemas responsáveis por gerenciar dispositivos dos mais variados tipos.

Esta ameaça afeta computadores, redes, tablets e celulares, geralmente assumindo o controle sobre a operação dos mesmos.

O malware prejudica os dispositivos, de maneira similar à forma que um vírus age em seres humanos: atingindo funções básicas e causando indisponibilidade.

Embora o malware não possa danificar o hardware dos dispositivos, ele pode “roubar”, criptografar e/ou excluir dados, alterar e/ou sequestrar funções essenciais do dispositivo e espionar atividades sem o conhecimento e permissão das vítimas.

No mundo virtual os malwares são utilizados para obter fonte de renda ilícita junto às vítimas de ataques virtuais.

HISTÓRICO E EVOLUÇÃO DO MALWARE

Existe uma grande variedade de malware e diariamente surgem novas variações. Portanto, é difícil citar toda a evolução e histórico de malware.

Apresentaremos a seguir, as principais tendências em desenvolvimento de malware.

O histórico de vírus modernos inicia nos anos 80, mais precisamente em 1982, com um programa chamado de Elk Cloner, que infectou os sistemas Apple II.

Sendo disseminado por disquetes infectados, o próprio vírus era inofensivo, mas se espalhava para todos os discos conectados a um sistema, explodindo de forma tão violenta que podia ser considerado o primeiro ataque de vírus de computador em grande escala da história.

Isso se passou antes do surgimento de qualquer malware de computador Windows e, desde então, os vírus e worms tornaram-se muito difundidos.

A partir dos anos 90, a plataforma Microsoft Windows surgiu, juntamente com as macros flexíveis de seus aplicativos.

Isso levou os autores de malware a escrever códigos infecciosos na linguagem macro do Microsoft Word e de outros programas.

Os vírus de macro infectavam documentos e modelos e não aplicativos executáveis. As macros de documento Word são uma forma de código executável.

A partir de 2002 e até o ano de 2007, surgiram worms de mensagens instantâneas, que são códigos maliciosos auto reproduzíveis disseminados por meio de uma rede de mensagem instantânea.

Os worms de mensagens instantâneas aproveitam-se de brechas na rede para se difundirem em grande escala, infectando serviços como: AOL AIM, MSN Messenger e Yahoo Messenger. Sistemas de mensagem instantânea corporativos também podiam ser infectados.

De 2005 a 2009, os ataques adware se proliferaram, apresentando anúncios indesejados nas telas do computador. Algumas vezes esses anúncios surgiam na forma de uma janela pop-up que os usuários não podiam fechar.

Esses anúncios geralmente exploravam softwares legítimos como uma forma de se espalharem, porém, por volta de 2008, os fornecedores de software começaram a processar empresas de adware por fraude.

Como resultado, milhões de dólares em multas, causando o fechamento de empresas de adware.

Entre 2007 e 2009, os golpistas de malware passaram a usar redes sociais, como MySpace, como canal de disseminação de anúncios, redirecionamentos de ofertas de antivírus e ferramentas de segurança falsos.
Os usuários eram enganados através de truques de engenharia social.

Quando o MySpace deixou de ser popular, o Facebook e Twitter passaram a ser as plataformas preferidas dos cibercriminosos.

As táticas mais comuns incluíam a apresentação de links falsos para páginas phishing e a promoção de aplicativos Facebook com extensões maliciosas.

Conforme isso ia diminuindo, os cibercriminosos arrumavam outras formar de agir.

Em setembro de 2013 surge uma nova forma de malware, chamada de ransomware lanou, promovendo ataques sob o nome de CryptoLocker.

Os alvos eram computadores com sistema Windows.

O CryptoLocker teve êxito em forçar suas vítimas a pagar cerca de US$ 27 milhões até no último trimestre de 2013.

Além disso, esse ransomware resultou na criação de outros ransomwares semelhantes.
Uma outra versão causou um prejuízo de US$ 18 milhões a 1000 vítimas entre abril de 20 14 e junho de 2015.

Foi também em 2013 que o ransomware se tornou o rei do malware, sendo transmitido por meio de Trojan, Exploits e propagandas maliciosas.

Em 2017 houve inúmeros ataques de ransomware que afetaram negócios de todos os tipos.

O ransomware atua criptografando os dados da vítima e depois exigindo pagamento para liberá-los.

Com o surgimento das cripomoedas, em 2017, surgiu um novo tipo de golpe de malware, chamado de CryptoJacking ou ato de, secretamente, usar o dispositivo de outra pessoa para minerar criptomoedas com recursos das vítimas.

TIPOS DE MALWARE

Existem muitos tipos de malware, mas citaremos a seguir alguns dos malwares mais comuns.

VÍRUS_ Os vírus prendem-se a arquivos limpos. Eles podem se espalhar incontrolavelmente, danificando funções centrais de um sistema e excluindo ou corrompendo arquivos.

Normalmente, os vírus aparecem como um arquivo executável (.exe).

TROJAN_ Conhecido também como cavalo de Tróia, o Trojan finge ser um software legítimo, ou se esconde em um software original que tenha sido violado.

Discretamente, ele libera acesso a portas para permitir a entrada de outros malwares e acessos não autorizados.

SPYWARE_ Como o nome sugere, é um malware criado para espionagem. Ele se esconde em segundo plano e grava suas atividades online, incluindo suas senhas, números de cartão de crédito, rotina de navegação e muito mais, enviando tudo ao seu operador.

WORMS_ Os Worms infectam redes inteiras de dispositivos, sejam locais ou através da internet com o uso de interfaces de rede.
Cada máquina infectada é utilizada para infectar outras máquinas.

RANSOMWARE_ O tipo de malware que costuma criptografar dados das vítimas, pedindo resgate para liberação dos mesmos.

ADWARE_ Embora não sejam maliciosos por natureza, estes softwares burlam a segurança para exibir anúncios, o que pode servir como porta de entrada para vários outros malwares.

BOTNETS_ Botnets são redes de computadores infectados que são forçados a trabalharem juntos sob o controle de um invasor.

COMO DETECTAR UM MALWARE?

O malware pode se revelar através de muitos comportamentos atípicos diferentes.

Apresentaremos alguns sinais que indicam que o sistema pode ter sido infectado por um malware.

COMPUTADOR LENTO_ Seu computador acaba ficando mais lento, pois um dos principais efeitos do malware é reduzir a velocidade de seu sistema operacional, seja usando a internet ou aplicativos locais.

ANÚNCIOS INESPERADOS_ Anúncios irritantes invadem sua tela, em pop-up inesperadas. Isso claramente é um sinal de que há uma infecção por malware, conhecidas como adware.

Esses pop-ups geralmente são acompanhados de outros tipos de malwares que estão ocultos.

Portanto, caso veja uma mensagem como “parabéns, você ganhou um carro!” em uma pop-up, não clique. O prêmio oferecido parece irresistível, mas o preço a pagar será alto.

SISTEMA DESLIGANDO OU TRAVADO_ Seu sistema se desliga repentinamente, congela ou exibe BSOD (a chamada tela azul), o que pode ocorrer em sistemas Windows após um erro fatal.

PERDA DE ESPAÇO NO DISCO_ Uma perda misteriosa de espaço em disco é notada, causada, provavelmente, por um malware invasor gigantesco que se culta em seu disco rígido.

USO DE RECURSOS DO SISTEMA_ O uso de recursos de seu sistema está estranhamente alto e a ventoinha de seu computador gira em plena velocidade. Esses são sinais claros que há uma atividade de malware consumindo recursos do sistema em segundo plano.

MUDANÇAS NO NAVEGADOR_ A página inicial do seu navegador mudou sem sua permissão. De forma semelhante, os links em que você clica o encaminham a um destino indesejado na internet.

É um indicativo de que você clicou em algum link ou executou um software malicioso.

É possível que seu browser fique lento e até extremamente lento.

Novas barras de ferramentas, extensões ou plug-ins podem aparecer inesperadamente em seu navegador também.

ANTIVÍRUS PARA DE FUNCIONAR_ Seu antivírus para de funcionar e você simplesmente não consegue atualizá-lo, ficando com seu sistema desprotegido contra malware furtivo que desabilitou o antivírus.

O MALWARE QUE SE APRESENTA_ O ataque de malware mais obvio e intencionalmente nem um pouco sorrateiro.

Muito comum com ransomware, o qual se apresenta e informa que está com seus dados, exigindo resgate para devolver seus arquivos.

Mesmo que seu sistema não apresente nenhum dos sinais descritos acima e funcione perfeitamente bem, não é garantia que seu dispositivo está livre de ameaças.

Um malware muito potente pode se ocultar em seu computador e fazer suas atividades sem despertar nenhum alerta à medida que rouba suas senhas, arquivos sensíveis ou usa seu computador para se difundir para outros computadores.

Alguns tipos de malware são mais fáceis de detectar do que outros. Alguns, como ransomwares e adwares,

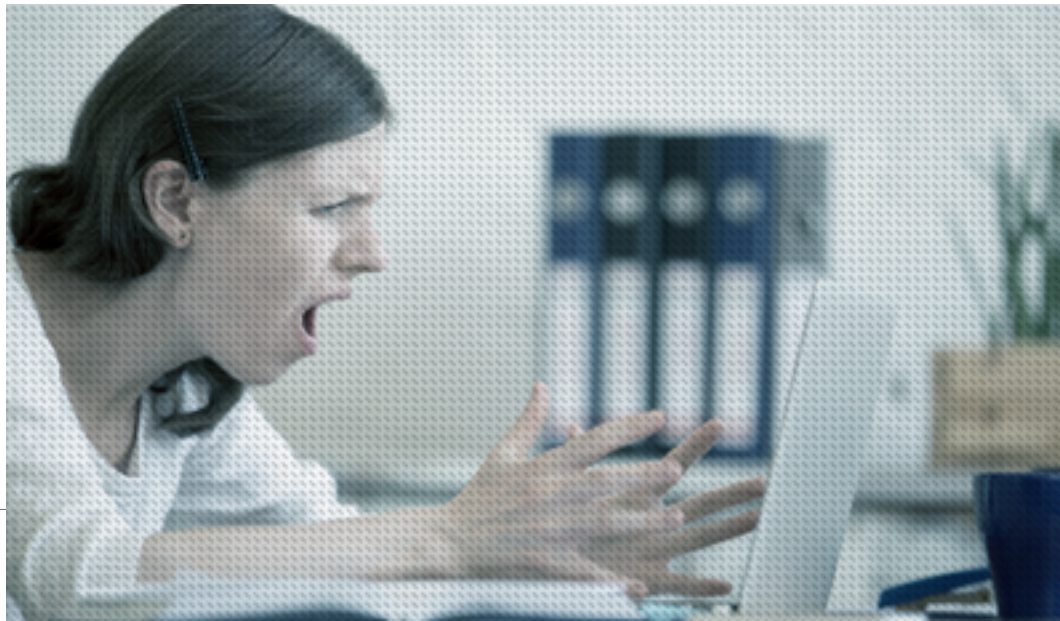
são perceptíveis imediatamente, seja por meio de criptografia dos seus arquivos ou excesso de anúncios.

Outros, como o cavalo de Tróia, desviam seu caminho para se esconder de você o tanto quanto possível, significando que eles podem permanecer no seu sistema por um longo tempo antes que você descubra sua presença.

E também há outros, como vírus e worms, que podem operar em segredo por muito tempo até que os sintomas da infecção comecem a aparecer, como travamento da máquina, eliminação e reposição de arquivos, desligamentos inesperados e processador hiperativo.

A única maneira de detectar malwares antes que infectem seus dispositivos é instalando um antivírus.

Ele precisa ter um pacote de ferramentas para detecção e escaneamento com poder de identificar malwares, evitando a contaminação ou então ser capaz de reagir ativamente combatendo a infecção em tempo hábil.



COMO MINHA MÁQUINA PODE TER SIDO INFECTADA POR MALWARE?

Existe uma longa lista de meios de infecção por malware, e todos eles estão associados a atividades executadas na internet.

O malware pode penetrar em seu computador, basicamente, quando você baixa qualquer coisa da internet para seu dispositivo que não tenha um aplicativo de segurança antivírus de qualidade.

É muito importante verificar as mensagens de alerta ao instalar aplicativos, principalmente se pedirem permissão para acessar suas informações de e-mail ou outras informações pessoais.

Para se proteger, use apenas fontes confiáveis de aplicativos ou instale apenas aplicativos com boa reputação e disponíveis nos sites dos fabricantes.

As pessoas são o principal meio para a sucesso de ataques de malware. Essa premissa é verdadeira, pois

você é sempre responsável pela ação que possibilita a contaminação dos dispositivos.

Por isso é tão importante que você tome cuidado com sites, links e downloads, pois é ao clicar em algo que esteja contaminado que você desencadeia a ação. Como se proteger contra malwares?

Prevenção é sempre melhor opção, por isso há alguns comportamentos de senso comum que minimizam as chances de você cair na armadilha de um software malicioso.

DICAS PARA SE PROTEGER DE MALWARES

Existe um ditado que diz “melhor prevenir do que remediar”, ou seja, é melhor se proteger e tomar certos cuidados do que ter que arcar com as consequências. No caso dos malwares, o preço a se pagar pode ser muito alto.

Confira algumas dicas para se proteger de malwares:

CUIDADO COM CONTEÚDOS DE FONTES DECONHECIDAS_ E-mails, alertas inesperados, banners, perfis falsos, são as principais formas de entrega de malware. Caso você não saiba do que determinado arquivo se trata, não clique nele.

CONFIRA SEUS DOWNLOADS_ Sempre há um malware à espreita em sites piratas e homepages de lojas oficiais. Antes de fazer algum download, confira sempre se o provedor é confiável e leia cuidadosamente as análises e comentários sobre ele.

BAIXE UM BLOQUEADOR DE ANÚNCIOS_ Bloqueie anúncios e pop-ups em seu dispositivo para evitar que os cibercriminosos façam uso dessa tática para obter sucesso nas ações.

Você pode acabar clicando em um banner que surge inesperadamente, por isso é mais seguro bloqueá-los utilizando uma ferramenta de bloqueio confiável.

CUIDADO COM OS SITES PELOS QUAIS NAVEGA_ Os malwares podem ser encontrados em qualquer lugar, mas são muito mais comuns em sites com sistema de segurança fraco.

Se você costuma navegar por sites suspeitos, o risco de contaminar seu dispositivo é grande. Procure sempre navegar por sites reconhecidos pelo grande público e com boa reputação.

É importante seguir essas dicas para se proteger, porém, você ainda corre o risco de ter seu dispositivo infectado por um malware.

Os cibercriminosos estão sempre em busca de maneiras de espalhar seus vírus pela Web.

Portanto, não esqueça de instalar um antivírus poderoso e confiável, que possa prevenir a ação de malwares e remove-los em caso de contaminação. A grande maioria das alternativas de antivírus com nível adequado de eficiência é pago, mas vale a pena investir em sua segurança.

CONTINUE LENDO

SE VOCÊ GOSTOU DO ASSUNTO E GOSTARIA DE NOVAS LEITURAS, FIQUE A VONTADE PARA CONSULTAR ATRAVÉS DOS LINKS ABAIXO TEMAS RELACIONADOS EM NOSSO PORTAL.

VOCÊ SE INTERESSOU PELO CONTEÚDO?

ESCLAREÇA SUAS DÚVIDAS COM ESPECIALISTAS NO ASSUNTO

CONVERSE COM ESPECIALISTA

facebook.com/ostec

linkedin.com/company/ostec-business-security

contato@ostec.com.br

www.ostec.com.br

ostec.blog

ostec

Segurança digital de resultados