Rua Cel. Lucas de Oliveira 1937/503, Porto Alegre/RS
(51) 3015-0580
contato@smartestrategias.com.br
https://www.smartestrategias.com.br

Visão geral

O termo "malware", uma combinação das palavras "malicioso" e "software" em inglês, hoje é usado para descrever qualquer programa malicioso no computador ou dispositivo móvel. Esses programas são instalados sem o consentimento dos usuários e podem causar diversos efeitos desagradáveis, como debilitar o desempenho do computador, invadir seu sistema à procura de dados pessoais, apagar dados ou até afetar negativamente o funcionamento do hardware controlado pelo computador. Na medida em que os hackers desenvolveram maneiras mais sofisticadas de invadir os sistemas dos usuários, o mercado de malware cresceu exponencialmente. Vejamos alguns dos tipos mais comuns de malware que temos em campo.

1. Vírus de computador

Os vírus de computador ganharam esse nome por sua capacidade de "infectar" diversos arquivos em um computador. Eles se propagam para outras máquinas quando os arquivos infectados são enviados por e-mail ou levados pelos próprios usuários em mídias físicas, como unidades USB ou os antigos disquetes. Segundo o *National Institute of Standards and Technology* (NIST), o primeiro vírus de computador, batizado de "Brain", foi desenvolvido em 1986. Cansados de clientes que pirateavam softwares de sua loja, dois irmãos alegam ter desenvolvido o vírus para infectar o setor de inicialização dos disquetes dos ladrões de software. Quando os discos eram copiados, o vírus era passado adiante.

2. Worms

De forma diferente dos vírus, os worms não precisam da ajuda humana para se propagar e infectar: eles infectam uma vez e depois usam as redes de computadores para se propagar para outras máquinas, sem a ajuda dos usuários. Com a exploração das vulnerabilidades de rede, como pontos fracos nos programas de e-mail, os worms podem enviar milhares de cópias suas na esperança de infectar novos sistemas, onde o processo começa novamente. Embora muitos worms apenas "consumam" recursos do sistema, reduzindo seu desempenho, muitos deles contêm "cargas" maliciosas criadas para roubar ou excluir arquivos.

3. Adware

Um dos incômodos mais comuns da presença on-line é o adware. Os programas enviam anúncios automaticamente para os computadores host. Entre os tipos rotineiros de adware estão os anúncios pop-up em páginas da Web e a publicidade dentro de programas, que geralmente acompanham softwares "gratuitos". Embora alguns programas de adware sejam relativamente inofensivos, outros usam ferramentas de rastreamento para coletar informações sobre sua localização ou seu histórico de navegação, para depois veicular anúncios direcionados em sua tela. Esse tipo pode ser capaz de desativar seu software antivírus. Como o adware é instalado com o conhecimento e o consentimento da pessoa, esses programas não podem ser chamados de malware: geralmente, são identificados como "programas potencialmente indesejados".

4. Spyware

O spyware faz o que o nome indica: espiona o que você faz no computador. Ele coleta dados como pressionamentos de teclas, hábitos de navegação e até informações de login que depois

são enviados a terceiros, geralmente os criminosos virtuais. Ele também pode modificar configurações de segurança específicas em seu computador ou interferir nas conexões de rede. As formas emergentes de spyware podem permitir que as empresas rastreiem o comportamento do usuário em diversos dispositivos sem o seu consentimento.

5. Ransomware

O ransomware infecta seu computador, criptografa dados sigilosos, como documentos pessoais ou fotos, e exige um resgate pela liberação. Se você se recusar a pagar, os dados serão excluídos. Algumas variantes de ransomware bloqueiam todo o acesso ao computador. Elas podem alegar ser de autoridades legais legítimas e sugerir que você foi pego fazendo algo ilegal. Em junho de 2015, o *Internet Crime Complaint Center* do FBI recebeu queixas de usuários relatando prejuízos de US$ 18 milhões por conta de uma ameaça comum de ransomware, chamada CryptoWall.

6. Bots

Os bots são programas projetados para realizar operações específicas automaticamente. São úteis para diversos fins legítimos, mas também foram reinventados como um tipo de malware. Quando instalados no computador, os bots podem usar a máquina para executar comandos específicos sem a aprovação ou o conhecimento do usuário. Os hackers ainda podem tentar infectar diversos computadores com o mesmo bot e criar uma "botnet" (abreviação de "rede robô" em inglês), que então pode ser usada para gerenciar remotamente os computadores comprometidos e roubar dados sigilosos, espionar as atividades das vítimas, distribuir spam automaticamente ou iniciar ataques DDoS devastadores às redes de computadores.

7. Rootkits

Os rootkits possibilitam o acesso ou controle remoto de um computador por terceiros. Esses programas são úteis para profissionais de TI que tentam solucionar problemas de rede à distância, mas podem facilmente se tornar destrutivos: depois de instalados em seu computador, os rootkits permitem que os invasores assumam total controle da máquina para roubar dados ou instalar outros malwares. Os rootkits são criados para passar despercebidos e ocultar ativamente sua presença. A detecção desse tipo de código malicioso exige o monitoramento manual de comportamentos incomuns, além de corrigir regularmente seu sistema operacional e seus programas de software para eliminar possíveis rotas de infecção.

8. Cavalos de Troia

Geralmente chamados de "cavalos Troia", esses programas se escondem mascarados como arquivos ou softwares legítimos. Depois de baixados e instalados, os cavalos de Troia alteram o computador e realizam atividades maliciosas sem o conhecimento ou consentimento da vítima.

9. Bugs

Os bugs, falhas no código do software, não são um tipo de malware, mas erros cometidos pelo programador. Eles podem ter efeitos prejudiciais sobre o computador, como travamento, falhas ou redução do desempenho. Os bugs de segurança, por outro lado, são vias fáceis para os

invasores burlarem sua defesa e infectar a máquina. Melhorar o controle de segurança por parte do desenvolvedor ajuda a eliminar bugs, mas também é fundamental aplicar as correções de software para resolver bugs específicos em campo.

Mitos e verdades

Existem alguns mitos comuns em torno dos vírus de computador:

- **Qualquer mensagem de erro do computador indica infecção por vírus.** Falso. As mensagens de erro também podem aparecer em virtude de bugs no hardware ou software.
- **Vírus e worms sempre precisam da interação do usuário.** Falso. O código tem de ser executado para que um vírus infecte o computador, mas isso não exige a interação do usuário. Por exemplo, um worm de rede pode infectar automaticamente se existirem certas vulnerabilidades no computador do usuário.
- **Anexos de e-mail de remetentes confiáveis são seguros.** Não é verdade, pois eles podem ter sido infectados por um vírus e ser usados para propagar a infecção. Mesmo que você conheça o remetente, não abra nada sobre o que não tenha certeza.
- **Os programas antivírus detêm todas as ameaças.** Embora os fornecedores de antivírus façam o máximo para acompanhar todas as evoluções do malware, é importante executar um produto de segurança de Internet completo, que inclua tecnologias criadas especificamente para bloquear as ameaças proativamente. Mesmo assim, é claro, 100% de segurança não existe. Por isso, é importante ter bom senso on-line para reduzir sua exposição a ataques.
- **Os vírus podem infligir danos físicos ao computador.** E se um código malicioso superaquecer sua máquina ou destruir microchips importantes? Os fornecedores de antivírus já desbancaram esse mito inúmeras vezes. Danos dessa natureza são simplesmente impossíveis.

Por sua vez, o aumento de dispositivos interconectados pela Internet das Coisas (IoT) levanta possibilidades interessantes: e se um carro infectado sair da estrada ou se um forno "inteligente" for programado para chegar ao aquecimento máximo até passar do limite? No futuro, o malware pode transformar esse tipo de prejuízo físico em realidade.

As pessoas têm diversas concepções errôneas sobre o malware, como a hipótese de que uma infecção é óbvia. Muitas vezes, os usuários presumem saber quando um computador é comprometido. No entanto, o malware não deixa rastros a serem seguidos, e seu sistema não exibirá qualquer sinal de infecção.

Tweet: No entanto, o malware não deixa rastros a serem seguidos, e seu sistema não exibirá qualquer sinal de infecção. Publique isso no Twitter! Da mesma forma, não acredite que todos os sites conhecidos sejam seguros. Se os hackers conseguirem comprometer sites legítimos com código infectado, os usuários serão mais suscetíveis a baixar arquivos ou fornecer informações pessoais. Segundo a SecurityWeek, foi exatamente isso que aconteceu com o Banco Mundial. Nesse mesmo caminho, muitos usuários acreditam que seus dados pessoais, como fotos, documentos e arquivos, não são interessantes para os criadores de malware. Os criminosos virtuais procuram dados disponíveis publicamente para atingir indivíduos ou coletar informações que os ajudem a criar e-mails de phishing para infiltrar-se nas organizações.

Métodos comuns de infecção

Então, como seu computador pode ser infectado por vírus ou malware? Há diversas maneiras comuns. Por exemplo, clicar em links para sites maliciosos contidos em e-mails ou mensagens nas redes sociais, acessar um site comprometido (conhecido como execução por download) e conectar uma unidade USB infectada ao computador. As vulnerabilidades do sistema operacional e dos aplicativos também tornam a instalação de malware nos computadores mais fácil. Por isso, é vital aplicar atualizações de segurança assim que elas são disponibilizadas, para reduzir a exposição aos riscos.

Os criminosos virtuais frequentemente usam a engenharia social para induzir a vítima a fazer algo que comprometa sua segurança ou a segurança da empresa em que você trabalha. E-mails de phishing são um dos métodos mais comuns. Você recebe um e-mail que parece legítimo e que o convence a baixar um arquivo infectado ou acessar um site malicioso. Nesse caso, o objetivo dos hackers é criar algo que você considere convincente, como um suposto aviso de vírus, uma notificação do banco ou uma mensagem de um amigo antigo.

Dados confidenciais, como senhas, são o principal alvo dos criminosos virtuais. Os criminosos virtuais podem usar malware para capturar senhas conforme elas são digitadas e também coletá-las em sites e outros computadores que conseguiram invadir. Por isso, é importante usar uma senha complexa exclusiva para cada conta on-line. Uma senha complexa tem 15 caracteres ou mais, incluindo letras, números e caracteres especiais. Dessa forma, se uma conta for comprometida, os criminosos virtuais não terão acesso a todas as suas contas on-line. Se você usa senhas fáceis de adivinhar, é claro que os criminosos não precisam comprometer sua máquina, nem o site de um provedor on-line. Infelizmente, a maioria dos usuários usa senhas fracas. Em vez de usar senhas fortes e difíceis de adivinhar, eles confiam em combinações comuns, como "123456" ou "Senha123", muito fáceis para os invasores adivinharem. Mesmo as perguntas de segurança podem não ser uma barreira tão eficaz, pois muitas pessoas dão as mesmas respostas: se a pergunta for "Qual é o seu prato favorito?", nos Estados Unidos, a resposta mais comum será "Pizza".

Sinais de infecção

Embora a maioria dos malwares não deixe sinais e, mesmo infectado, seu computador continue funcionando perfeitamente, às vezes há indícios de infecção. A redução do desempenho está no topo da lista. Isso inclui processos lentos, janelas que demoram para abrir e programas aparentemente aleatórios sendo executados em segundo plano. Você também pode perceber alterações nas páginas iniciais da Internet no navegador ou que os anúncios pop-up são mais frequentes que o normal. Em alguns casos, o malware também pode afetar funções mais básicas do computador: o Windows pode não ser aberto, e você pode não conseguir se conectar à Internet, nem acessar funções mais importantes de controle do sistema. Se você desconfiar que o computador foi infectado, execute uma verificação do sistema imediatamente. Se nada for encontrado, mas você ainda tiver dúvida, busque uma segunda opinião: execute uma verificação antivírus alternativa.

Fonte: Kaspersky, Smarte e SecurityWeek