PRAGAS

Novo vírus se espalha e copia arquivo

Ameaça se copia junto com um arquivo para uma unidade de disco removível e invade PCs Mac, Windows e máquinas virtuais

A empresa de segurança Symantec acaba de divulgar a descoberta de um malware para Mac chamado OSX.Crisis. Ele tem capacidade de se disseminar para quatro ambientes diferentes: Mac, Windows, máquinas virtuais e Windows Mobile.

Trata-se de uma ameaça avançada não só na função, mas também na maneira como se dissemina. O malware usa três métodos para esse fim: um consiste em se copiar junto com um arquivo autorun.inf para uma unidade de disco removível; outra forma consiste em invadir sorrateiramente uma máquina virtual VMware.

O terceiro método consiste em inserir módulos em um dispositivo Windows Mobile. Especificamente em ambientes virtuais, a ameaça procura uma imagem de uma máquina virtual VMware no computador comprometido e, caso a encontre, monta a imagem e depois se copia para ela usando uma ferramenta do VMware Player.

A ameaça se aproveita de um atributo de todo software de virtualização, ou seja, o fato de que a máquina virtual é simplesmente um arquivo ou uma série de arquivos no disco do computador host.

Esses arquivos geralmente podem ser manipulados ou montados diretamente, mesmo quando a máquina virtual não estiver em execução, como é o caso mencionado.

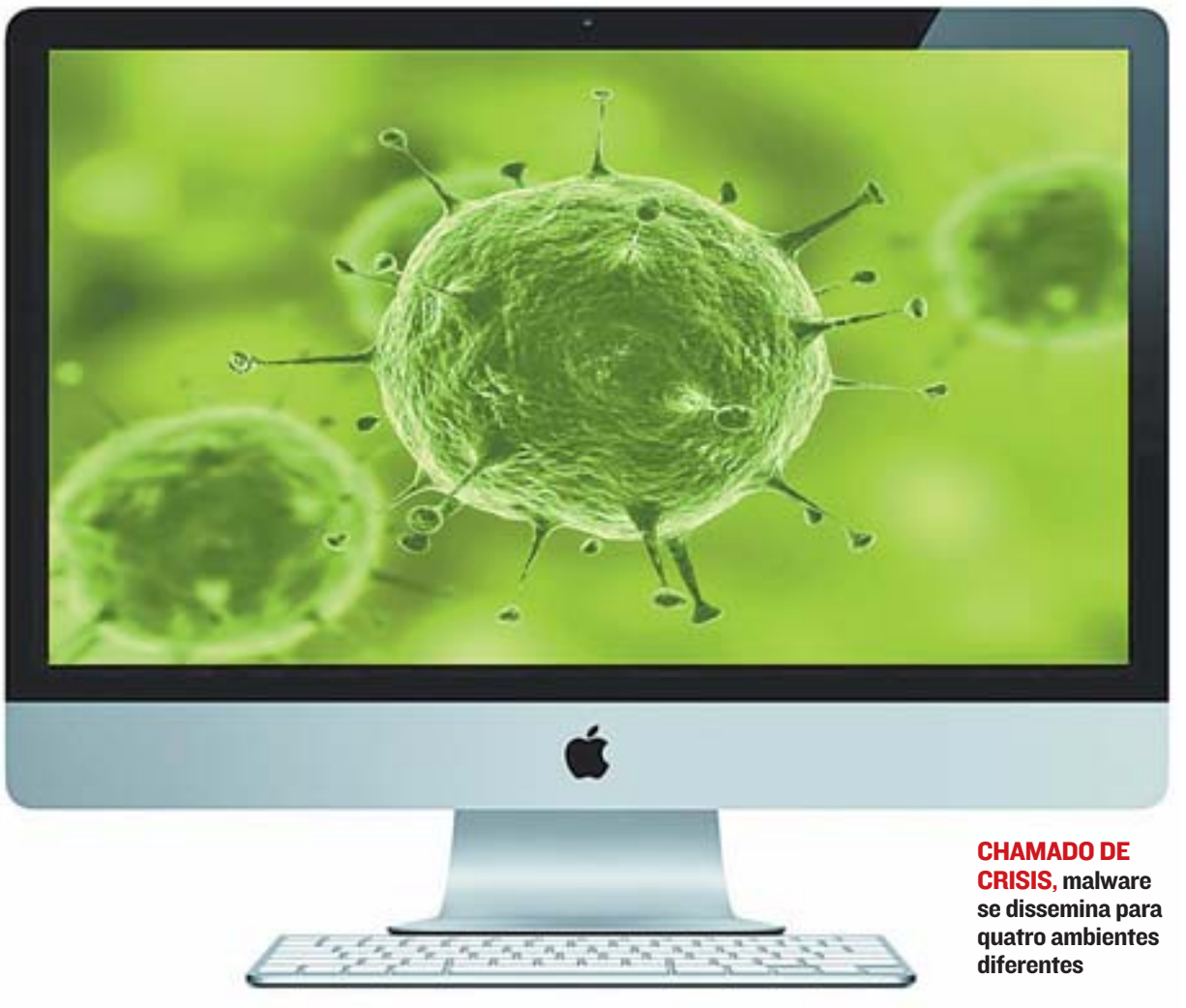
Segundo a Symantec, esse pode ser o primeiro malware que tenta se disseminar em uma máquina virtual. Muitas se extinguem quando encontram um aplicativo de monitoração de máquina virtual, como o VMware, a fim de evitar que sejam analisadas. Então este pode ser o próximo movimento dos criadores de malware.

FACEBOOK

Já a empresa de segurança Sophos identificou um novo golpe espalhado via e-mail, em que a falsa mensagem avisa sobre uma marcação de foto no Facebook.

A correspondência, que parece ter sido enviada pela própria rede social, traz um software malicioso que tenta ganhar o controle do PC. A praga ataca máquinas com o sistema operacional Windows.

O e-mail vem com um arquivo ZIP em anexo. A tentativa de invadir a máquina acontece quando o usuário tenta abrir esse conteúdo, para ver em que foto do Facebook foi marcado.



CHAMADO DE CRISIS, malware se dissemina para quatro ambientes diferentes

DICAS IMPORTANTES

SEGURANÇA PESSOAL

É fundamental utilizar um antivírus confiável e sempre atualizado. Evite realizar download de arquivos de sites desconhecidos e não abra e-mail de remetentes que você desconhece, principalmente se vierem com anexo. Cuidado ao disponibilizar informações pessoais de forma púbica, principalmente via rede sociais.

DISPOSITIVOS MÓVEIS

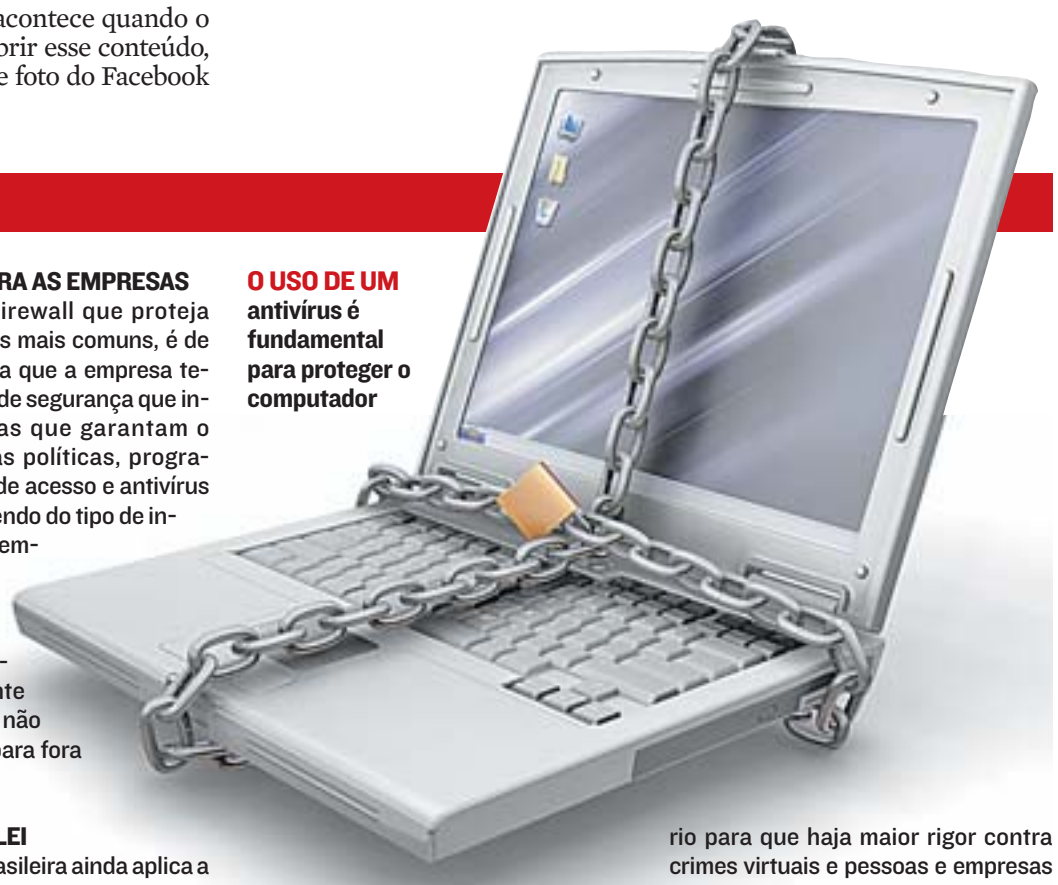
Cuidado redobrado com o uso dos dispositivos móveis, como celulares e tablets, pois com o uso de redes sem fio públicas (Wireless), a possibilidade de ataques e invasões é muito grande. Por isso, é indispensável o uso de um antivírus e a criação de uma senha de proteção para o equipamento. Um sistema de criptografia que proteja as informações gravadas no equipamento também é recomendado.

SEGURANÇA PARA AS EMPRESAS

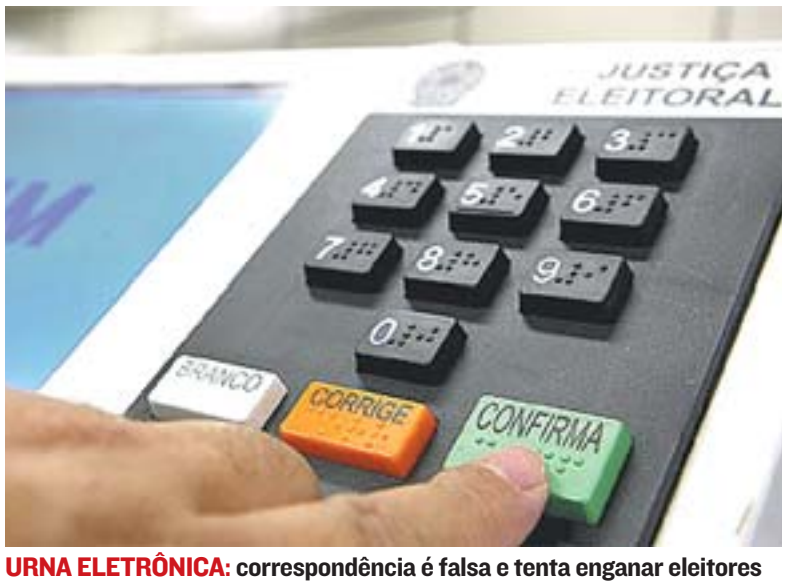
Além de um Firewall que proteja contra os ataques mais comuns, é de suma importância que a empresa tenha uma política de segurança que integram: sistemas que garantam o cumprimento das políticas, programas de controle de acesso e antivírus de rede. Dependendo do tipo de informação que a empresa possui, ter um sistema de controle contra perda de dados (DLP) garante que esses dados não sejam enviados para fora da rede.

EM RELAÇÃO À LEI

A legislação brasileira ainda aplica a lei comum para crimes virtuais, mas já há alguns projetos específicos para crimes digitais. Resta aguardarmos as próximas decisões da Poder Judiciário para que haja maior rigor contra crimes virtuais e pessoas e empresas estejam mais protegidas no acesso de suas informações.



O USO DE UM antivírus é fundamental para proteger o computador



URNA ELETRÔNICA: correspondência é falsa e tenta enganar eleitores

E-mail malicioso diz que título eleitoral está suspenso

Com a proximidade das eleições municipais, criminosos da rede se aproveitam para explorar o tema. Um novo golpe sobre o assunto já está circulando na internet.

A tentativa de phishing usa o nome do Tribunal Superior Eleitoral (TSE) para distribuir arquivos maliciosos e roubar senhas dos usuários.

O falso e-mail avisa ao internauta que o seu título de eleitor está suspenso e que, para regularizar a sua situação com a Justiça Eleitoral, é preciso baixar um documento em PDF.

A Justiça Eleitoral informa que não envia e-mails a eleitores para comunicar cancelamento de títulos eleitorais ou para convocar mesários – com exceção do Tribunal Regional Eleitoral do Estado do Rio Grande do Sul (TRE/RS), que, mediante prévia e específica autorização do convocado, se utiliza desse tipo de correspondência para recrutar seus mesários.

O TSE ressalta que não autoriza qualquer outra instituição a enviar e-mails em seu nome.

Mensagens dessa natureza devem ser apagadas, de imediato, já que podem conter vírus de computador ou qualquer outro software malicioso.

Expediente **PRODUÇÃO**: Dinâmica de Comunicação **CONTATOS**: 3232-5931 - informatica@redetribuna.com.br **JORNALISTA RESPONSÁVEL:** Fabiana Pizzani **EDIÇÃO E REVISÃO**: Alessandra Tonini **DIAGRAMAÇÃO**: Amauri Ploteixa **TRATAMENTO DE IMAGENS**: Renan Martinelli