classificados
www.diariodaregiao.com.br/classificados
DIARIOIMOVEIS
www.diarioimoveis.com.br



**34**

foi o número de ataques registrado em 2015

# À ESPERA DO SEU CLIQUE

## Sob ataque constante, empresas e prefeituras do Noroeste Paulista estão na mira de cibercriminosos. Dados da Secretaria de Segurança Pública (SSP) apontam para um ataque por dia na região

*Rone Carvalho*
rone.carvalho@diariodaregiao.com.br

O simples clique em um e-mail falso da Receita Federal desencadeou uma crise sem precedentes na empresa de Pedro, que prefere não se identificar. As inúmeras informações, como nome completo, CPF e até endereço, levaram o empresário a acreditar que o texto bem escrito era do órgão público. Mas, na verdade, tratava-se de um ataque digital.

Ao invés de levar Pedro a baixar o arquivo prometido, o link permitiu a instalação de um software malicioso, tornando impossível o acesso ao computador da empresa. Em seguida, os cibercriminosos entraram em contato exigindo o pagamento de uma centena de reais para liberar o sistema e devolver os inúmeros dados que haviam sido sequestrados. À mercê do hacker, Pedro aprendeu da pior forma sobre a importância de investir em segurança da informação.

Histórias como a dele estão sendo comuns no Brasil. Para ser tem uma ideia, dados da Secretaria de Segurança Pública do Estado de São Paulo (SSP), obtidos pelo Diário via Lei de Acesso a Informação, apontam que o número de casos de invasão de dispositivo e delitos de informática aumentaram quase dez vezes em oito anos (aumento de 961%) na região de Rio Preto. De 34, em 2015, para 361, em 2021. Sem contar os casos que não são registrados pelas vítimas.

No rol de entidades lesadas no Noroeste Paulista estão empresas, postos de combustível, hospitais, escolas, universidades, residências, lotéricas, agências bancárias e até órgãos públicos, como delegacias de polícia, prefeituras e câmaras municipais. "Não é apenas no computador que ocorre esses ataques. O Brasil, por exemplo, é o país da América Latina mais atacado em dispositivos Android", destacou Daniel Barbosa, especialista em segurança da informação da ESET – companhia de segurança da informação.

A Câmara Municipal de Irapuã, por exemplo, foi alvo de cibercriminosos, ao menos três vezes, nos últimos 15 anos. O último ataque aconteceu em 2021 e levou a cidade a correr contra o tempo para contratar uma empresa de segurança da informação para evitar novos ataques. Em um dos ataques, os criminosos exigiram mais de R$ 500 mil para liberar os dados.

"Eles bloquearam o sistema e exigiram uma quantia como resgate, inclusive em criptomoeda para não deixar registros. Mas não pagamos. Registramos um boletim de ocorrência e reforçamos nosso sistema de segurança da informação", contou Mauricio Palhari Sanches de Oliveira, presidente da Câmara Municipal de Irapuã.

Segundo o delegado especialista em crimes cibernéticos da Polícia Civil de São Paulo, Higor Vinicius Nogueira Jorge, o objetivo dos criminosos quando invade o dispositivo difere entre empresas e pessoas comuns. "No caso de empresa, por exemplo, na grande maioria dos casos, o criminoso criptografa as informações de determinado servidor e depois pede dinheiro para oferecer a chave criptográfica e liberar as informações. No entanto, o recomendado é não pagar. Existem muitos casos em que o criminoso não informa a chave mesmo com o pagamento".

Já no caso de pessoas comuns, a invasão do dispositivo, normalmente, acontece por links maliciosos de falsas promoções ou pedidos urgentes nas redes sociais. "Considerando que, hoje em dia, a vida das pessoas está dentro do smartphone, quando o criminoso consegue invadir o aparelho, ele tenta coletar o máximo de informações sensíveis, como senhas, que permitam a realização de transferências de valores que estejam disponíveis na conta bancária da vítima".

### O QUE É HACKER?

É um indivíduo que entende como computadores e redes funcionam e é capaz de manuseá-los com precisão. Uma utilidade disso é invadir uma rede e obter acesso remoto a um aparelho sem autorização, o que configura atividade criminosa. Porém, o hacker não é necessariamente um criminoso. Esse conjunto de conhecimentos também pode ser usado para melhorar a segurança de redes. Já que um hacker é capaz de encontrar essas falhas. Ele também é o mais qualificado para identificá-las e encontrar uma solução.

### Motivos dos ataques

**Demonstração de poder:** mostrar a uma empresa que ela pode ser invadida ou ter os serviços suspensos e, assim, tentar vender serviços ou chantageá-la para que o ataque não ocorra novamente.

**Prestígio:** vangloriar-se, perante outros cibercriminosos, por ter conseguido invadir computadores, tornar serviços inacessíveis ou desfigurar sites considerados visados ou difíceis de serem atacados.

**Motivações financeiras:** coletar e utilizar informações confidenciais de usuários para aplicar golpes. Além disso, muitos criminosos costumam invadir os dispositivos e exigir dinheiro das vítimas.

**Motivações ideológicas:** tornar inacessível ou invadir sites que divulguem conteúdo contrário à opinião do atacante; divulgar mensagens de apoio ou contrárias a uma determinada ideologia.

**Motivações comerciais:** tornar inacessível ou invadir sites e computadores de empresas concorrentes, para tentar impedir o acesso dos clientes ou comprometer a reputação destas empresas.

### COMO SE PROTEGER

#### Cuidado ao baixar softwares

Baixar programas sem verificar sua segurança é um grande erro, pois permite que malwares – software maliciosos – entrem disfarçados em seu celular ou computador. Se você der a permissão, eles podem ultrapassar qualquer barreira de proteção. Portanto, tenha atenção redobrada ao fazer o download, preferindo lojas oficiais de aplicativos em vez de páginas avulsas — as quais podem conter outros arquivos maliciosos.

#### Suspeite de e-mails

Muitos crimes virtuais ocorrem por meio de sites nocivos e e-mails, geralmente enviados como parte de uma promoção falsa, uma mensagem encaminhada por um conhecido ou outra forma de mascarar seu conteúdo e propósito. Reconhecer essas mensagens e apagá-las ou ignorá-las é sempre a melhor maneira de se proteger.

#### Mantenha um antivírus

O firewall e o antivírus são as principais linhas de defesa contra hackers em seu computador ou celular. O firewall atua barrando acessos não autorizados, enquanto o antivírus detecta atividades suspeitas em aplicativos. Se ambos forem de boa qualidade, eles podem impedir a maioria dos ataques.

#### Faça backup

Normalmente, um dos maiores danos das vítimas de cibercriminosos quando são atacados pelo vírus "ransomware", que bloqueia arquivos até o pagamento de um resgate é a perda dos documentos digitais. Por isso, a importância de se investir em um backup, seja empresa ou do próprio celular. A melhor dica é salvar seus arquivos em um sistema separado, que não esteja conectado à internet.

#### Não pague o resgate

A recomendação é que ao ter seu dispositivo invadido, que as vítimas não pague o resgate dos arquivos. Especialistas em segurança dizem que além financiar a prática e incentivar que outros ataques ocorram, o pagamento não é garantia que os arquivos serão devolvidos pelos criminosos.

### TIPOS DE ATAQUE

#### Falsificação de e-mail (E-mail spoofing)

Falsificação de e-mail é uma técnica que consiste em alterar campos do cabeçalho de um e-mail, de forma a aparentar que ele foi enviado de uma determinada origem quando, na verdade, foi enviado de outra.

Ataques deste tipo são bastante usados para propagação de códigos maliciosos, envio de spam e em golpes de phishing. Atacantes utilizam-se de endereços de e-mail coletados de computadores infectados para enviar mensagens e tentar fazer com que os seus destinatários acreditem que elas partiram de pessoas conhecidas.

Exemplos de e-mails com campos falsificados são aqueles recebidos como sendo: de alguém conhecido, solicitando que você clique em um link ou execute um arquivo anexo; do seu banco, solicitando que você siga um link fornecido na própria mensagem e informe dados da sua conta bancária; do administrador do serviço de e-mail que você utiliza, solicitando informações pessoais e ameaçando bloquear a sua conta caso você não as envie.

#### Varredura em redes (Scan)

Varredura em redes, ou scan, é uma técnica que consiste em efetuar buscas minuciosas em redes, com o objetivo de identificar computadores ativos e coletar informações sobre eles como, por exemplo, serviços disponibilizados e programas instalados. Com base nas informações coletadas é possível associar possíveis vulnerabilidades aos serviços disponibilizados e aos programas instalados nos computadores ativos detectados.

A varredura em redes e a exploração de vulnerabilidades associadas podem ser usadas de forma:

**Legítima:** por pessoas devidamente autorizadas, para verificar a segurança de computadores e redes e, assim, tomar medidas corretivas e preventivas.

**Maliciosa:** por atacantes, para explorar as vulnerabilidades encontradas nos serviços disponibilizados e nos programas instalados para a execução de atividades maliciosas. Os atacantes também podem utilizar os computadores ativos detectados como potenciais alvos no processo de propagação automática de códigos maliciosos e em ataques de força bruta.

#### Exploração de vulnerabilidades

Uma vulnerabilidade é definida como uma condição que, quando explorada por um atacante, pode resultar em uma violação de segurança. Exemplos de vulnerabilidades são falhas no projeto, na implementação ou na configuração de programas, serviços ou equipamentos de rede.

Um ataque de exploração de vulnerabilidades ocorre quando um atacante, utilizando-se de uma vulnerabilidade, tenta executar ações maliciosas, como invadir um sistema, acessar informações confidenciais, disparar ataques contra outros computadores ou tornar um serviço inacessível.

#### Interceptação de tráfego (Sniffing)

Interceptação de tráfego, ou sniffing, é uma técnica que consiste em inspecionar os dados trafegados em redes de computadores, por meio do uso de programas específicos chamados de sniffers. Esta técnica pode ser utilizada de forma:

**Legítima:** por administradores de redes, para detectar problemas, analisar desempenho e monitorar atividades maliciosas relativas aos computadores ou redes por eles administrados.

**Maliciosa:** por atacantes, para capturar informações sensíveis, como senhas, números de cartão de crédito e o conteúdo de arquivos confidenciais que estejam trafegando por meio de conexões inseguras, ou seja, sem criptografia.

#### Força bruta (Brute force)

Um ataque de força bruta consiste em adivinhar, por tentativa e erro, um nome de usuário e senha e, assim, executar processos e acessar sites, computadores e serviços em nome e com os mesmos privilégios deste usuário.

Qualquer computador, equipamento de rede ou serviço que seja acessível via Internet, com um nome de usuário e uma senha, pode ser alvo de um ataque de força bruta. Dispositivos móveis, que estejam protegidos por senha, além de poderem ser atacados pela rede, também podem ser alvo deste tipo de ataque caso o atacante tenha acesso físico a eles.

Se um atacante tiver conhecimento do seu nome de usuário e da sua senha ele pode efetuar ações maliciosas em seu nome como, por exemplo: trocar a sua senha, dificultando que você acesse novamente o site ou computador invadido.

#### Desfiguração de página (Defacement)

Desfiguração de página, defacement ou pichação, é uma técnica que consiste em alterar o conteúdo da página Web de um site. As principais formas que um atacante pode utilizar para desfigurar uma página Web são: explorar erros da aplicação Web; invadir o servidor onde a aplicação Web está hospedada e alterar diretamente os arquivos que compõem o site; ou furtar senhas de acesso à interface Web usada para administração remota.

Fonte: ESET, FUNDAJ, TJSC e reportagem.

## Vazamentos de dados contribui

Quando um cibercriminoso invade o banco de dados de uma empresa, hospital ou órgão público o que mais ele visa – além do pagamento do resgate da vítima – são os dados cadastrados no sistema. Isso porque é com base nessas informações que os criminosos conseguem aplicar outros golpes.

É o caso, por exemplo, da situação de Pedro. O empresário somente acreditou no e-mail porque ele continha informações pessoais como o seu CPF e endereço, o que levou a acreditar que o link era realmente da Receita Federal.

"O grande problema quando tem vazamento de dados é que eles abrem margem para outros crimes. É muito comum, por exemplo, chegar e-mail falso do Detran de multa, com informações pessoais como modelo do carro, nomes dos pais e documentos pessoais. Os criminosos colocam esses dados porque conseguiram a partir de algum vazamento", explicou Rodolpho Barbosa, especialista em segurança digital e gerente de novos negócios na Verhaw IT. "Hoje, digo que dados são como petróleo", completou.

Na Deep Web – parte mais profunda da internet que a maioria das pessoas não tem acesso – é comum a venda de dados de milhares de brasileiros, obtidos após vazamento de dados. Uma verdadeira mina para cibercriminosos.

Entre os dois maiores ataques digitais que aconteceram nos últimos anos, em Rio Preto, estão o contra o Hospital de Base e a instituição de ensino superior Unilago. Em 2009, o sistema da Funfarme, fundação que administra o complexo do Hospital de Base (HB), sofreu uma tentativa de invasão hacker. Para preservar a segurança dos dados, o hospital desativou toda a rede e os 2,6 mil computadores ficaram sem internet.

Em 2016, os servidores do banco de dados da Unilago também foram alvos de ataque de cibercriminosos. O sistema ficou inoperante durante quatro dias e os atacantes chegaram a exigir o pagamento US$ 3 mil, o equivalente a R$ 16 mil.

Adriano Cansian, professor em segurança da informação da Unesp Rio Preto, ressalta a importância de algumas medidas simples de segurança, como de não instalar software pirata e manter antivírus atualizados. "Ataques sofisticados são minoria na internet, eles não representam nem 5% dos casos. O grosso é coisa banal, é aquele arroz e feijão, que a empresa ou a pessoa não faz a tarefa de casa. Por isso, a importância de prevenir por meio de atualização constante de backup e de manter o antivírus atualizado". (RC)

**361**

foi a quantidade de ataques ocorridos em 2021

**3**

ataques foram sofridos pela Câmara Municipal de Irapuã

**500**

mil reais foi o resgate pedido em um dos ataques ao legislativo de Irapuã