FALE COM A EDITORA ISABELA LAMEGO E-MAIL: economia@redetribuna.com.br

Piratas da internet roubam dados e pedem resgate

As principais vítimas são empresas que dependem de arquivos e planilhas para funcionar. Pedido de resgate é de até 10 mil

Cristian Favaro

Com o crescimento do número de usuários da internet, os crimes virtuais são cada vez mais constantes. No Estado, empresas estão sendo atacadas por um novo malware (normalmente chamado de vírus, são programas mal-intencionados), o Ransomware. Neste ano, seis casos foram registrados no Estado.

Ransom, em inglês, significa resgate, e é basicamente o que o programa faz: bloqueia arquivos da empresa para que os criminosos possam cobrar valores que chegam até a R$ 10 mil para devolvê-los.

Segundo investigador de crimes eletrônicos da Polícia Civil, Hercules Denadai Aranda, o programa é principalmente destinado a empresas com dados sensíveis, ou seja, indispensáveis para o funcionamento da companhia, como empresas de contabilidade.

"O programa faz com que a empresa não tenha acesso aos dados. Depois, eles praticam o crime de extorsão. Cobram dinheiro para as vítimas conseguirem acessar os arquivos", explica o investigador.

Apesar de bloqueados, os arquivos continuam nos computadores da empresa. O inspetor explica que o programa não os apaga, ele criptografa os dados (como se fosse um embaralhamento) de forma com que eles não possam mais ser acessados sem a chave de desbloqueio – que só o criminoso possui.

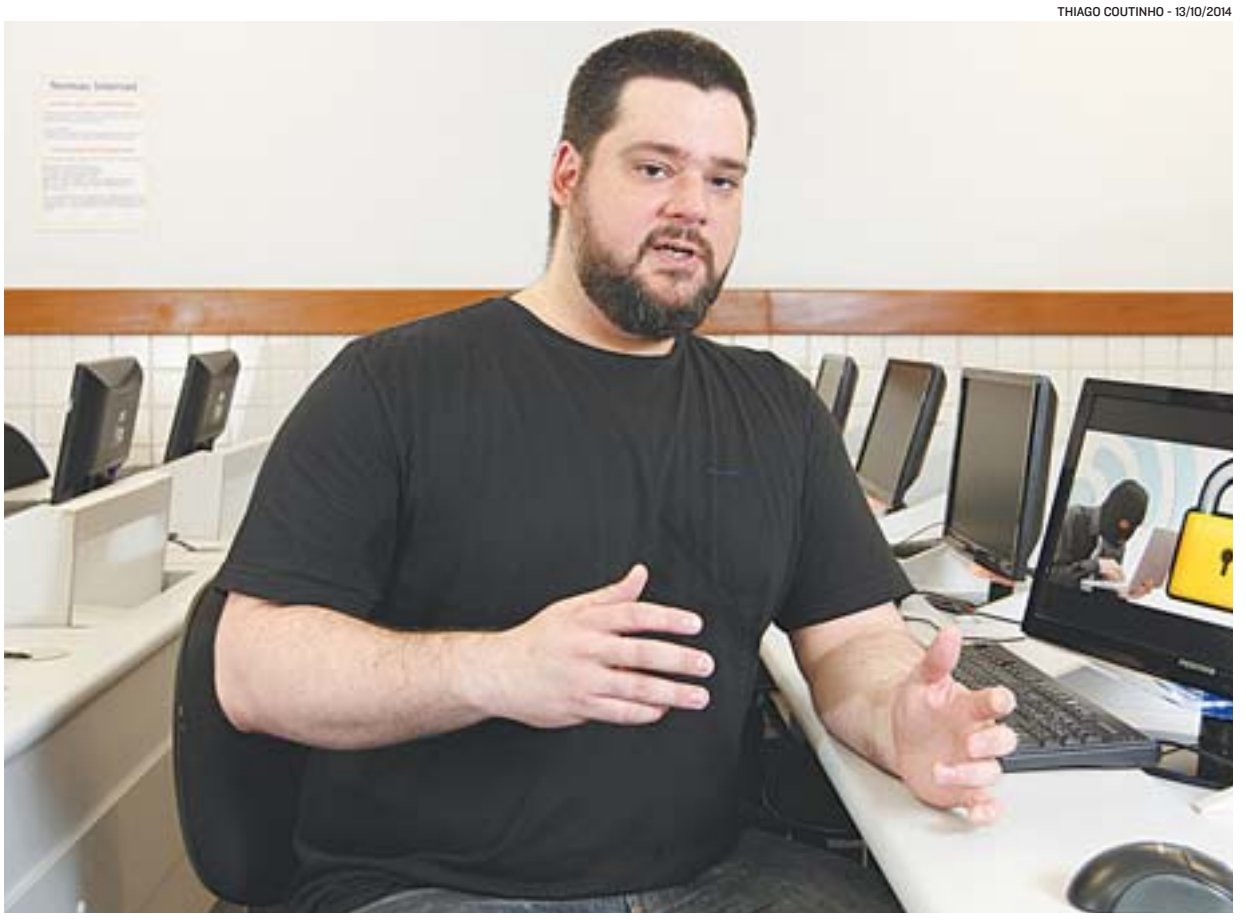
Para chegar até os computadores das empresas, os criminosos utilizam falhas de segurança na rede e, o mais comum, e-mails com arquivos anexados. Depois que o computador é infectado, a vítima recebe uma mensagem que exibe o contato do criminoso.

Segundo o investigador, todas essas fraudes vêm de quadrilhas muito bem organizadas e de fora do País, o que torna a investigação ainda mais complicada. Entre as identificadas, duas são localizadas na Ásia e uma na Europa.

Para o mestre em Informática e professor do curso de Sistemas da Universidade de Vila Velha Marcello Novaes, as empresas estão despreparadas e costumam levar grandes prejuízos.

"Não é uma solução, mas a cópia de segurança dos arquivos evita maiores prejuízos. O problema é que nem sempre as empresas fazem isso. É uma falha que até algumas companhias de médio porte cometem", observa Novaes.

THIAGO COUTINHO - 13/10/2014



MARCELLO NOVAES pontuou que as empresas estão despreparadas e costumam levar grandes prejuízos

VEJA ALGUNS DOS CASOS DO GOLPE REGISTRADOS NO ESPÍRITO SANTO

Regaste em dólares

Uma empresa na área de comércio internacional teve seus dados bloqueados pelos criminosos que invadiram o computador da instituição.

Segundo a empresa, o valor exigido foi de US$ 2mil (R$ 6.167,40).

A empresa tentou recuperar os arquivos de diversas formas, mas como não obteve sucesso, acabou sendo obrigada a refazê-los.

Empresa pagou resgate

Uma empresa de contabilidade, localizada no interior do Estado, também foi vítima do golpe. O valor exigido foi de US$ 2 mil (R$ 6.167,40).

A empresa teve ajuda da Polícia Civil e até Federal para tentar resgatar os dados. Após inúmeras tentativas de recuperar os documentos bloqueados pelos criminosos, o empresário cedeu e pagou o valor exigido pelos piratas da internet.

Apesar de não ser a recomendação da polícia, ele conseguiu os documentos de volta.

Rede infectada

Uma empresa do ramo moveleiro do Estado acabou tendo sua rede infectada pelos piratas da internet. O valor exigido foi de US$ 3 mil (R$ 9.251,10).

Segundo a empresa, nem uma equipe técnica contratada para solucionar o problema conseguiu recuperar os dados perdidos. Como a empresa não concordou em pagar o resgate para os criminosos, teve de refazer todo o banco de dados.

Nem a polícia conseguiu recuperar os dados roubados

O esquema é tão resistente que nem as Polícias Civil e Federal conseguiram ajudar a gerente de uma empresa do ramo de comércio internacional, que foi vítima do golpe que bloqueia arquivos e somente libera mediante pagamento aos criminosos.

"Pelo nível de criptografia, podemos dizer que esses criminosos são estruturados e especializados", afirma o investigador de crimes eletrônicos da Polícia Civil, Hercules Denadai Aranda.

A gerente, que preferiu não se identificar, relatou que sua companhia foi vítima desse golpe. Segundo ela, até a base de dados de emissão de notas fiscais foi comprometida.

"Junto com os arquivos estava um endereço de e-mail para conseguir o desbloqueio. O valor era US$ 3 mil (R$9.251,10)", contou a gerente, que tentou pagar até um hacker para resolver o problema. "Para minha surpresa, o hacker disse que existe um código de ética entre eles e que um não quebra o sistema do outro".

A gerente afirmou que se recusou a pagar o valor determinado pelo criminoso. A empresa tinha algumas cópias impressas dos documentos roubados, mas, para recuperar refazer tudo, foram mais de três meses de trabalho.

SLIDESHARE

CRIPTOGRAFIA: dados roubados

ENTENDA

Sequestro de informações

Primeiro passo do esquema

> **O VIRUS É ENVIADO**, muitas vezes por e-mail (em um anexo ou link) ou chega até o computador da empresa por falhas no sistema.
> **O PESSOA QUE ESTÁ NO COMPUTADOR** da empresa abre e executa esse anexo.
> **A PARTIR DISSO,** o vírus entra na máquina e o ataque começa.
> **APÓS A INFECÇÃO**, ele criptografa (como se fosse embaralhar) os arquivos do computador, além de informar o criminoso sobre o ataque.
> **OS ARQUIVOS** continuam no computador da empresa, mas seu acesso é impedido.
> **É EXIBIDO UM ENDEREÇO DE E-MAIL** para que a vítima entre em contato com o criminoso e possa negociar o valor do resgate.

Segundo passo do esquema

> **APÓS ISSO,** o criminoso passa a também ser usuário do computador.
> **ELE PODE ENVIAR** mensagens na rede. Ele encaminha mensagens para a vítima que solicitam o pagamento, que varia entre R$ 3mil a R$ 10mil, dependendo do tamanho do golpe e da empresa.
> **O DINHEIRO DEVE SER ENVIADO** para contas fora do País, boa parte delas em nomes falsos, o que demonstra a organização das quadrilhas especializadas nesses crimes.
> **BOA PARTE DAS MENSAGENS É ENVIADA** de Países da Ásia.
> **UMA DAS** vítimas recebia e-mails de um computador que estava localizado na Rússia.

Fonte: Especialistas consultados.

COMO SE PREVENIR

Dicas de como evitar se expor

> **PRIMEIRA DICA** é nunca executar um anexo de um e-mail que você não conhece a origem. Empresas como bancos nunca enviam arquivos para serem baixados por e-mail. Na dúvida, entre em contato com a respectiva empresa.

AGÊNCIA BAMBOO

PROTEÇÃO de dados: alerta

> **MESMO QUE NÃO EXECUTE** o arquivo e também evite baixá-lo. O risco é menor, mas é melhor evitar esse procedimento.
> **CASO VOCÊ PRECISE CONFERIR O CONTEÚDO DO ANEXO,** por se tratar de algo que realmente aparenta ser para você, primeiro baixe o arquivo, depois passe o antivírus e, após isso, abra-o.
> **PRESTE ATENÇÃO NO FORMATO** do link e nome dos arquivos. Quando você passa o mouse sobre o arquivo aparece o nome verdadeiro dele. Por exemplo, o anexo aparece como Word, mas quando você passa o mouse em cima (ou dá somente um clique, após o arquivo estar em seu computador) você consegue observar que não se trata de um documento do Word, mas de um instalador.