COMO UM RANSOMWARE PODE ME ATACAR?

Tendo entendido a ameaça a que estamos expostos como usuários e o possível impacto se um vírus do tipo ransomware nos atacar, a pergunta que surge é "como posso ser infectado?".

Embora existam muitos métodos e variantes destes pelos quais podemos nos infectar, o principal método de infecção é por **trojans em websites maliciosos** ou legítimos, que foram comprometidos por criminosos com o único propósito de contagiar seus usuários. Muitas vezes o usuário não detecta um comportamento anômalo ou sua experiência de navegação não é afetada: o vírus simplesmente passa despercebido e se instala em segundo plano.

O segundo método mais comum de propagação se dá pelo envio de **links para sites comprometidos em emails em massa** (spam), **em mensagens instantâneas, redes sociais** e até mesmo ao **compartilhar arquivos em redes P2P** (torrent, etc.).

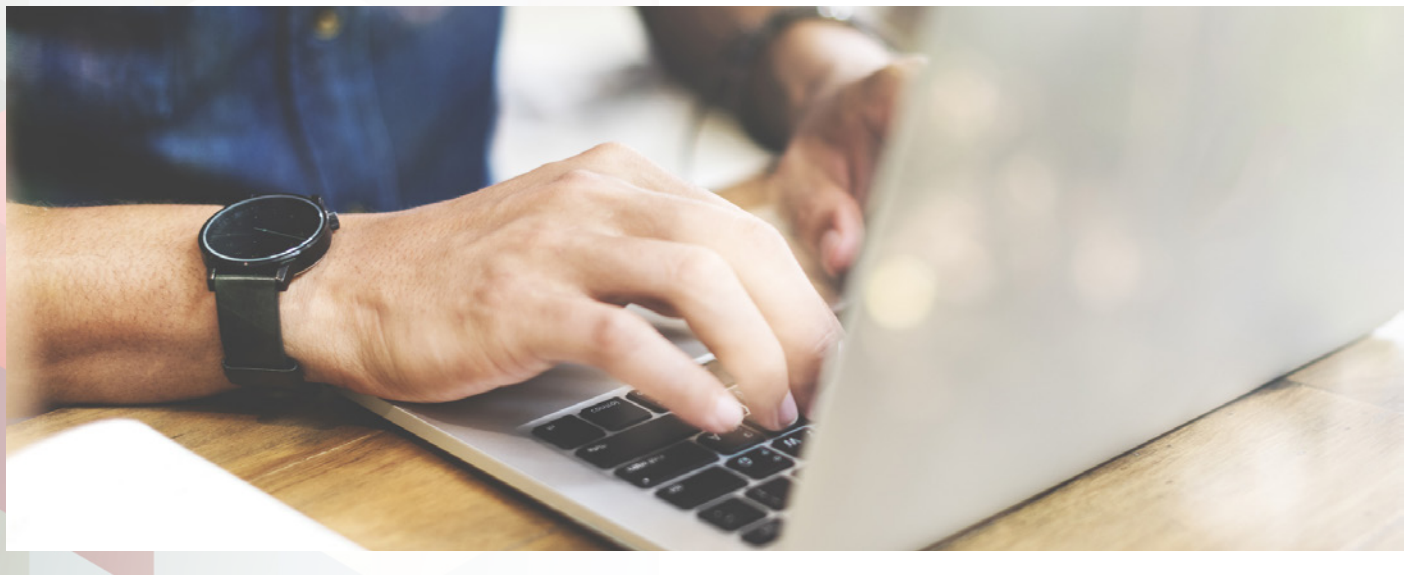
Nos ataques contra empresas, embora como usuário isso seja menos habitual, também ocorrem ataques dirigidos aos servidores, explorando **vulnerabilidades conhecidas no protocolo de acesso remoto (RDP)** que os administradores de sistemas usam para acessar os servidores das organizações.

Já que falamos sobre o crescimento de ataques detectados em dispositivos móveis, é importante saber como um vírus pode entrar em nossos dispositivos. A forma é semelhante: baseia-se em embustes publicados em sites mal-intencionados, que fazem com que o usuário acesse **cópias da Google Play Store com conteúdo malicioso**, onde o usuário acaba instalando um aplicativo mal-intencionado, que é o que executa o "sequestro" do dispositivo. Curiosamente, muitos destes engodos se baseiam em fazer o usuário acreditar que há um vírus em seu dispositivo, e ele acessa o site para baixar um suposto antivírus.

O QUE POSSO FAZER PARA EVITAR SER INFECTADO E/OU MINIMIZAR O IMPACTO?

Entendendo como este tipo de programa funciona e as formas mais comuns em que se pode ser atacado, o que é preciso fazer para evitar um ataque?

- Fazer ***backup*** de seus arquivos regularmente é, sem dúvida, o método mais eficaz de combate. Infelizmente, na maioria dos casos a recuperação dos arquivos ou equipamentos afetados será impossível, de modo que poder recuperá-los usando cópias de backup é quase sempre a única forma possível.
- Usar sistemas ***antivírus*** nos dispositivos. Como vimos, uma das formas mais comuns de infecção quando executamos certos arquivos nos equipamentos. Se houver um antivírus bom e atualizado, será mais fácil repelir os ataques.
- Para dar menos oportunidades para ataques à segurança, tanto os aplicativos quanto o sistema operacional do nosso equipamento devem estar atualizados para a ***versão mais recente disponível e com todos os patches de segurança instalados***. Isto se torna ainda mais relevante no caso dos navegadores web (Chrome, Firefox, Internet Explorer, Safari, etc.), já que às vezes as infecções ocorrem quando se navega por determinados sites (seja porque este é o propósito deles ou porque eles foram comprometidos anteriormente).
- Use o bom senso e, como regra geral, ***não confie*** em sites, arquivos ou links estranhos ou desconhecidos. Se, por exemplo, você receber um link no seu e-mail relativo a um pedido que não está esperando, ignore-o e, na dúvida, procure se informar antes de qualquer ação. Muitas vezes, uma simples busca no Google sobre o assunto ou sobre o corpo da mensagem de email pode bastar para que você perceba que o que você achava que era legítimo é na verdade uma ameaça.
- ***Habilitar as extensões dos arquivos*** pode te ajudar a identificar melhor uma tentativa de ataque. Se, por exemplo, em um e-mail você está esperando receber uma imagem, mas recebe um arquivo compactado (um ".zip", por exemplo), isso pode indicar que há algo errado.
- Se você suspeitar que alguns dos arquivos que recebeu recentemente podem ser algum tipo de vírus, a primeira coisa a fazer, antes de mais nada, é ***desconectar o computador da rede***. Isso atenuará o risco, principalmente em ambientes corporativos, de que a ameça possa se expandir para os demais computadores da rede.



O QUE FAZER EM CASO DE INFECÇÃO?

Se infelizmente não foi possível realizar os controles mencionados acima e a infecção aconteceu, o que se deve fazer? Em primeiro lugar, **recomenda-se não pagar o resgate** pedido por criminosos cibernéticos, já que fazer isso não garante a recuperação dos arquivos e, além disso, promove a realização desta prática criminosa. De acordo com estudos recentes da empresa antivírus Kaspersky, um dentre cada três usuários paga pelo resgate de seus arquivos, e aproximadamente 20% deles não consegue recuperá-los. Ao invés disso, e conforme a magnitude do incidente, a primeira ação que se aconselha é avaliar a possibilidade de notificar as Forças e Agências de Segurança do Estado, especialmente se for considerado que certos direitos fundamentais foram violados ou se a segurança das pessoas foi colocada em risco de alguma forma. No caso específico de órgãos públicos e empresas de interesse estratégico para o país, esta comunicação deve ser canalizada através do CERT do Centro Criptológico Nacional, que é o órgão público que reporta ao Centro Nacional de Inteligência, cuja missão é zelar pela segurança dos sistemas de informação na administração pública.

Se depois disso você decidir tentar recuperar os arquivos, a forma de abordar sua "desinfecção" muda com relação a um ataque por vírus de outra natureza. Em um cenário normal de infecção, os arquivos ficam danificados ou têm um comportamento diferente do esperado devido à ação de um arquivo mal-intencionado. Para esses casos, executar um aplicativo antivírus tradicional pode resolver o problema na maioria das vezes, na tentativa de voltar os arquivos a seu estado anterior ou de eliminar a ameaça diretamente. No caso do ransomware, o problema é que os arquivos não foram infectados, e sim criptografados, de modo que apagá-los ou desinfectá-los não funciona. Neste caso, a estratégia de recuperação deve ser, primeiro, eliminar o arquivo que está produzindo a encriptação dos arquivos no seu dispositivo e, segundo, conseguir a chave com a qual eles foram criptografados. Por sorte existem agências e entidades privadas que trabalham ativamente nesta tarefa oferecendo aplicativos e recursos gratuitos que podem nos ajudar neste processo. O projeto "No More Ransom" ("Fim aos Resgates"), por exemplo, conhecido especialmente no mundo da segurança cibernética, é liderado pela Europol e pela unidade de crime tecnológico da polícia holandesa juntamente com uma das maiores empresas privadas no setor. Esta organização oferece um conjunto de ferramentas gratuitas que permitem decifrar os arquivos atacados por uma grande maioria de ransomware, bem como conselhos ou guias para resolver um incidente desta natureza.

EXISTE ALGUMA FORMA DE SEGURAR UM POSSÍVEL INCIDENTE DE COMPUTAÇÃO?

Com o aumento da incidência de novas ameaças virtuais, têm-se proliferado em nossos mercados os **produtos de seguros** que visam dar cobertura para as empresas. Um relatório recente enviado pela consultoria PwC afirma que cerca de 30% das organizações norte-americanas têm atualmente algum tipo de cobertura que lhes permite se protegerem das consequências de um ataque cibernético (a maioria dos setores de saúde, tecnologia e varejo). Na Espanha os números são menores, e por enquanto somente as empresas do Ibex 35 parecem estar conscientizadas, pois metade delas tem algum tipo de apólice ou estão em processo de contratação. É importante destacar que este tipo de apólice muitas vezes não está padronizado. As apólices são adaptadas individualmente, o que permite que as empresas personalizem as coberturas a serem aplicadas, de forma que possam escolher as que sejam mais adequadas às particularidades do negócio.

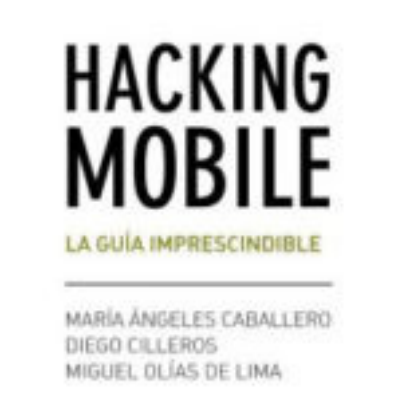
Já que os ataques cibernéticos costumam impactar diretamente as operações das empresas, os seguros contra riscos cibernéticos devem estar preparados para cobrir as possíveis perdas econômicas, juntamente com as despesas relacionadas à investigação forense ou ao processo de comunicação aos clientes (Cabe lembrar que o futuro regulamento europeu UE 2016/679 obrigará as empresas a informar violações de segurança e notificar terceiros sobre as violações de seus dados). No caso específico do ataque de ransomware, o principal elemento que distingue o tipo de apólice a ser aplicada é a cobertura em relação aos custos de extorsão.

Atualmente, a MAPFRE dispõe de um Seguro contra Riscos Cibernéticos para proteger seus clientes, as PMEs e profissionais autônomos deste novo tipo de ameaça:

- Despesas com recuperação de imagem.
- Multas e penalidades decorrentes do ataque.
- Despesas com defesa legal.
- Roubo de informações confidenciais.
- Danos a sistemas de computação.
- Perdas econômicas devido à interrupção do negócio.

Você pode encontrar mais informações acessando o seguinte link: *https://www.mapfre.es/seguros/empresas/seguros-de-responsabilidad-civil/seguro-ciberriesgos/*

BIBLIOGRAFIA RELACIONADA



Uma vez que o ransomware em dispositivos móveis é um dos vetores em que se prevê um crescimento exponencial, se você estiver interessado em conhecer e explorar o mundo da segurança cibernética em dispositivos móveis, recomendamos como bibliografia básica o livro *Mobile Hacking*, da Editora ANAYA, em que se aborda este tipo de tópico.
http://www.anayamultimedia.es/libro.php?id=4312499