Métodos de pagamentos explorados

Por envolver extorsão, o desenvolvimento e a disseminação de ransomwares podem ser consideradas atividades criminosas, razão pela qual os responsáveis por esses malwares costumam ser bastante cuidadosos: uma operação de pagamento pode ser rastreada rapidamente pelas autoridades.

Dificilmente você verá um ransomware exigindo pagamento em serviços conhecidos, como o PayPal (que possui um sistema avançado de combate a fraudes), ou diretamente em contas bancárias, a não ser quando estas pertencem a terceiros — os chamados "laranjas".

É mais frequente o uso de serviços de pagamentos menos conhecidos ou mais discretos, como aqueles que são usados em sites de apostas ou conteúdo erótico. Mas, como estes também podem ser rastreados, é cada vez mais comum o uso das chamadas *criptomoedas*, com destaque para o Bitcoin.

Explicando rapidamente, o Bitcoin é uma espécie de "moeda digital" baseada em criptografia. Assim, é possível proteger as transações, o que evita (ou dificulta ao extremo) que a origem e o destino do pagamento sejam rastreados.

Por conta disso, o Bitcoin é bastante utilizado em atividades ilegais (mas atividades legais também podem se beneficiar dessa moeda virtual, é bom destacar). Porém, como o uso desse meio é mais complexo, os criminosos preferem trabalhar com o Bitcoin apenas quando valores altos estão em jogo.

Os cuidados preventivos em relação aos ransomwares praticamente não diferem das medidas de segurança recomendadas no combate a outros malwares. Eis as práticas mais indicadas:

- Tome cuidado com anexos e links em e-mails, especialmente com mensagens em nome de bancos, lojas ou autoridades judiciais: o teor desses e-mails tenta te deixar preocupado para você clicar ali sem pensar;

- Também tome cuidado com links em redes sociais (como Facebook) e serviços de mensagens instantâneas (com WhatsApp), mesmo que a mensagem venha de uma pessoa conhecida — pode acontecer de o computador ou dispositivo móvel dela ter sido contaminado e enviado a mensagem sem ela perceber;

- Nunca baixe arquivos de sites de qualidade duvidosa;

- Mantenha sistema operacional e aplicativos sempre atualizados (especialmente navegadores);

- Ative os recursos de segurança e privacidade do seu navegador;

- Tome cuidado com plug-ins de navegadores. É uma boa ideia deixar extensões do Java e Flash desativados por padrão;

- Use softwares de segurança (principalmente antivírus) de empresas com boa reputação;

- Evite usar serviços públicos de Wi-Fi, ao menos aqueles que são desconhecidos. Algumas redes podem redirecionar seu navegador para sites falsos sem que você perceba;

- Faça backup (cópia) de seus arquivos regularmente. Assim, você pode recuperá-los facilmente em caso de "sequestro" de dados.

Como as empresas podem se proteger dos ransomwares

No caso de empresas e outras organizações, os ransomwares podem interromper todo o negócio, por isso, os cuidados devem ser redobrados. É recomendável:

- Orientar funcionários sobre os cuidados indicados no tópico anterior;

- Monitorar a rede e protegê-las com mecanismos específicos para cada tipo de atividade (e-mail, web, transações de pagamento, etc.);

- Instalar atualizações no sistema operacional dos servidores em tempo hábil;

- Criar regras de segurança digital abrangentes;

- Controlar com rigor o acesso a sistemas (um funcionário do RH não deve acessar um módulo do departamento financeiro, por exemplo);

- Revisar políticas de segurança, ferramentas de proteção e módulos dos sistemas periodicamente;

- Fazer backup rotineiro (isso é essencial!), especialmente de dados críticos.

Vale lembrar que sistemas baseados no Windows são muito visados por serem mais numerosos, mas há ransomwares em praticamente todas as plataformas, inclusive móveis. Assim, também é necessário haver cuidados em sistemas como OS X, iOS, Linux e Android.