Ransomware

28/03/2019 • 2 minutos para ler • Colaboradores

Neste artigo

Ransomware é um tipo de malware que criptografa arquivos e pastas, impedindo o acesso a arquivos importantes. Ransomware tenta extort dinheiro das vítimas solicitando dinheiro, geralmente na forma de cryptocurrencies, em troca a chave de descriptografia. Mas cibercriminosos não sempre siga por meio e desbloquear os arquivos criptografados por eles.

A tendência para comportamento de malware cada vez mais sofisticados, realçado pelo uso de explorações e outros vetores de ataque, torna plataformas mais antigas especialmente suscetíveis a ataques ransomware.

Como funciona o ransomware

A maioria das infecções ransomware começam com:

- Mensagens de e-mail com anexos que tentam instalar ransomware.
- Sites que hospedam explorar kits que tentam usam vulnerabilidades em navegadores da web e outro software para instalar o ransomware.

Depois de ransomware infecta um dispositivo, ele inicia com criptografia de arquivos, pastas, partições de disco rígido inteiro usando algoritmos de criptografia como RSA ou RC4.

Ransomware é um dos canais de receita mais lucrativos para cibercriminosos, para que os autores de malware aprimorar continuamente seu código de malware para melhor direcionar ambientes corporativos. Ransomware como serviço é um modelo de negócios criminoso cibernético nos quais um malware criadores vendem seu ransomware e outros serviços a cibercriminosos, que então operam os ataques ransomware. O modelo de

negócios também define o compartilhamento de lucro entre os criadores de malware, operadores de ransomware e outros participantes que podem ser envolvidos. Para cibercriminosos, ransomware é uma empresa grande, às custas de indivíduos e empresas.

Exemplos

Ransomware sofisticado como **Spora**, **WannaCrypt** (também conhecido como WannaCry), e **Petya** (também conhecido como NotPetya) se espalhar para outros computadores por meio de compartilhamentos de rede ou explorações.

- Spora cair ransomware cópias em compartilhamentos de rede.
- WannaCrypt explora a vulnerabilidade CVE-2017-0144 (também chamado de EternalBlue) do Server Message Block (SMB) para infectar outros computadores.
- Uma variante Petya explora a mesma vulnerabilidade, além de CVE-2017-0145 (também conhecido como EternalRomance) e usa credenciais roubadas mover lateralmente em redes.

Ransomware mais antigo como **Reveton** bloqueia telas em vez de criptografia de arquivos. Eles exibem uma imagem de tela inteira e, em seguida, desabilitar o Gerenciador de tarefas. Os arquivos são seguros, mas eles não são acessíveis com eficiência. A imagem geralmente contém uma mensagem dizendo ser do imposição da lei que diz que o computador tem sido usado em necessidades fino e atividades criminoso cibernético ilegal a ser pago. Por isso, Reveton é apelidado "Boletins Troia" ou "Boletins ransomware".

Ransomware como **Cerber** e **Locky** procurar e criptografar tipos específicos de arquivos, normalmente documentam e arquivos de mídia. Quando a criptografia for concluída, o malware sai de uma nota de resgate usando texto, imagem ou um arquivo HTML com instruções para pagar um resgate para recuperar arquivos.

Coelho ruins ransomware foi descoberto tentar espalhados por redes usando nomes de usuário com código fixo e senhas em bruta forçar ataques.

Como se proteger contra ransomware

As organizações podem ser voltadas especificamente por invasores, ou pode ser detectadas do elenco largo net por criminoso cibernético operações. Grandes organizações são destinos de alto valor e invasores podem exigir ransoms maiores.

É recomendável:

- Fazer backup de arquivos importantes regularmente. Usar a 3-2-1 regra. Manter três backups de seus dados, em dois tipos diferentes de armazenamento e pelo menos um externo de backup.
- Aplica as atualizações mais recentes para seus sistemas operacionais e aplicativos.
- Treinar os funcionários para que eles podem identificar ataques de phishing lança e engenharia social.
- Acesso controlado a pastas. Ele pode parar ransomware de criptografia de arquivos e mantendo os arquivos de resgate.

Para obter dicas mais gerais, consulte a impedir a infecção por malware.