A Publicação Mensal de Sensibilizaçao de Segurança para Usuários de Computadores

OUCH!

NESTA EDIÇÃO...



# Ransomware

## O que é Ransomware?

Ransomware é um tipo de malware que se espalha ativamente pela Internet hoje em dia, ameaçando destruir documentos e arquivos de suas vítimas. Malware é um software – um programa de computador, utilizado para executar ações maliciosas. Mesmo sendo o Ransomware mais um dos muitos tipos diferentes de malware, ele se tornou muito comum pelo fato de ser muito lucrativo para os criminosos. Uma vez que o ransomware infecta seu computador, ele encripta arquivos e talvez até seu disco de dados inteiro. Você fica então sem acesso ao sistema inteiro e não consegue acessar seus arquivos importantes como documentos e fotos. O malware então lhe informa que a única forma de decriptar seus arquivos e recuperar seu sistema é pagando um resgate (ransom) ao criminoso (daí o nome ransomware). Na maioria das vezes o resgate deve ser pago em uma forma de moeda digital, como Bitcoin. O Ransomware se espalha como muitos outros tipos de malware. O método mais comum envolve o envio de emails maliciosos para as vítimas, onde os criminosos lhe convencem a abrir um anexo infectado ou a clicar em um link que o leva ao website do atacante.


### Editor Convidado

Lenny Zeltser trabalha na proteção da operação de T/I dos clientes na NCR Corp e dá aulas sobre combate a malware no SANS Institute. Lenny está presente no Twitter como **@lennyzeltser** e escreve sobre segurança no seu blog em **zeltser.com**.


## Você deve pagar o resgate?

Essa é uma pergunta difícil. O problema é que quanto mais as pessoas pagarem esse tipo de crimonso quando se infectarem, mais motivados eles estarão para infectar novas pessoas. Por outro lado, você pode não ter escolha para recuperar seus arquivos. Esteja avisado porém, sobre não haver garantia de que terá seus arquivos de volta ao efetuar o pagamento. Você está lidando com criminosos e eles podem não decriptar seus arquivos, ou mesmo quando enviarem um método de decriptografia, algo pode não funcionar durante o processo ou seu computador pode ser infectado com um malware adicional.

## Faça Backup dos seus arquivos

Talvez a melhor forma de recuperar arquivos de uma infecção por ransomware e não pagar o resgate seja recuperar seus arquivos de uma cópia backup. Assim, mesmo que você seja infectado por um ransomware, você tem um recurso para recuperar seus arquivos depois de reconstruir ou limpar seu computador. Tenha em mente que caso seu backup possa ser acessado pelo sistema infectado, o ransomware poderá apagar ou encriptar seus arquivos backup. Portanto, é importante

# Ransomware

fazer backup para um serviço CLOUD de reputação ou armazená-los em discos externos que não estejam regularmente conectados ao seu sistema. Adicionalmente, um erro comum que muitas pessoas cometem com backups é presumir que ele funcionará quando precisar, sem ao menos fazer um teste de recuperação. Certifique-se de verificar regularmente que seus backups estão funcionando e que consegue recuperar os arquivos que precisa, caso seu sistema venha a se infectar por um ransomware. Backups são importantes pois eles também ajudam a recuperar arquivos apagados acidentalmente ou quando o seu disco de dados falha.


*Ransomware é um malware que, quando infecta seu computador, encripta todos os seus arquivos impedindo que você os acesse.*

## Outras medidas de proteção

Além disso, você pode se proteger de uma infecção por ransomware da mesma forma que se protege de outros tipos de malware: não se infectando. Começe certificando-se de ter a última atualização de antivírus de um provedor de confiança. Essas ferramentas, às vezes chamadas software antimalware, são feitas para detectar e parar os malwares. Contudo, os antivirus não conseguem bloquear ou remover todos os programas maliciosos. Os criminosos cibernéticos estão constantemente inovando, desenvolvendo novos e sofisticados malwares que podem evitar a detecção. Por sua vez, os fabricantes de antivírus estão constantemente atualizando seus produtos com novas capacidades de detecção de malware. Em muitos aspectos tornou-se uma corrida armamentista, com ambos os lados tentando despistar a outro. Infelizmente os criminosos estão frequentemente um passo à frente, o que faz com que você tenha que garantir o backup dos seus arquivos e seguir esses passos adicionais para proteger-se:

- Criminosos cibernéticos frequentemente infectam seu computador ou dispositivos explorando vulnerabilidades no seu software. Quanto mais atualizado estiver o seu software, menos vulnerabilidades conhecidas seu sistema terá e mais difícil será para os criminosos o infectarem. Portanto certifique-se de que seu sistema operacional, aplicações e dispositivos estejam configurados para permitir atualizações automáticas;
- Em computadores, use uma conta padrão com privilégios limitados ao invés de contas privilegiadas como “Administrador” ou “root”. Isso lhe dará uma proteção adicional ao impedir que muitos tipos de malware sejam capazes de se instalar sozinhos;
- Criminosos cibernéticos muitas vezes levam as pessoas a instalar o malware para eles. Por exemplo, eles podem enviar-lhe um email que pareça legítimo e contenha um anexo ou um link. Talvez o email pareça vir do seu banco

## Ransomware

ou de um amigo. Porém, se você abre o arquivo anexo ou clica no link, você ativa o código malicioso que instala o malware no seu sistema. Se uma mensagem cria um forte senso de urgência, é confusa, parece boa de mais para ser verdade ou tem uma gramática pobre, ela pode ser um ataque. Suspeite. O bom senso é muitas vezes sua melhor defesa.

Proteja-se do ransomware estando vigilante ao abrir anexos em emails ou ao clicar em links, garantindo ter seu antivírus atualizado e confirmando que seus arquivos sejam backupeados regularmente e possam ser recuperados.

## Saiba Mais

Assine OUCH!, a publicação mensal de sensibilização de segurança, acesse os arquivos de OUCH! e saiba mais sobre as soluções SANS de sensibilização de segurança visitando nossa página em securingthehuman.sans.org/ouch/archives.

## Versão Brasileira

Traduzida por: Homero Palheta Michelini, Arquiteto de T/I, especialista em Segurança da Informação - twitter.com/homerop
Michel Girardias, Analista de Segurança da Informação - twitter.com/michelgirardias
Marta Visser – Tradutora autônoma
Rodrigo Gularte, Administrador de Empresas, especialista em Segurança da Informação - twitter.com/rodrigofgularte

## Recursos

| | |
|---|---|
| Phishing: | https://securingthehuman.sans.org//ouch/2015#december2015 |
| O que é um Malware: | https://securingthehuman.sans.org/ouch/2016#march2016 |
| Criptografia: | https://securingthehuman.sans.org/ouch/2016#june2016 |
| Backups: | https://securingthehuman.sans.org/ouch/2015#august2015 |
| Artigo da Microsoft (em Inglês): | https://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx |
| Curso SANS FOR610 - Reverse Engineering Malware: | https://sans.org/for610 |



Board Editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Traduzida por: Homero Palheta Michelini, Michel Girardias, Rodrigo Gularte, Marta Visser