



# Ransomware

Por: Gustavo Leme  
Laís Arlindo  
Nathália Venega



# Definição

Representa uma ameaça para você e seu dispositivo, já que é um software de extorsão, podendo bloquear o seu computador e depois exigir um resgate para desbloqueá-lo. Para ocorrer a infecção o malware ganha acesso ao dispositivo dependendo de seu tipo todo o sistema operacional ou apenas arquivos individuais são criptografados, logo após isso o resgate é exigido.



# Tipos e como se propagam

## 1.Doxware

**Conhecido como vazamento, o doxware ameaça publicar as informações roubadas online se não houver o pagamento do regaste. Conforme pessoas armazenam arquivos confidenciais como fotos pessoais em dispositivos, é normal que usuários entrem em pânico e peguem pelos resgates.**

## 2.Petya

**Petya criptografa certos arquivos do dispositivo exigindo o pagamento do resgate em troca de uma chave de descriptografia, entretanto quando muitas outras linhas de ransomware se concentram em arquivos pessoais o Petya pode bloquear o disco rígido inteiro o que impede a inicialização do computador. Para se propagar o malware coleta senhas.**

## 3.Mobile

**Se refere à os ransomwares que afetam dispositivos móveis. Sendo entregue por aplicativos maliciosos ou download direto, que geralmente o ransomware não é criptografado, pois os backups automatizados de dados na nuvem ajudam na reversão de ataques de criptografia.**

# Tipos e como se propagam

## 4.RaaS

**É um modelo de negócios em que os desenvolvedores de malware vendem para outros hackers, empacotando ferramentas do serviço em kits RaaS, sendo anunciados nos fóruns da deep web.**

## 5.Scareware

**É um software que leva o usuário a acessar links e sites infectados por malwares, a partir do medo, onde as pessoas são enxurradas por notificações ou banners de antivírus visando causar pânico, alertando sobre violações de segurança aparentemente significativas, utilizando de ferramentas de edição para causar maior escândalo.**

## 6.Ransomware locker

**Á infecção da máquina ocorre, a partir do download de arquivos que quando aberto os malware são liberados, assim tendo livre acesso a informação e vazamento delas ,travamento do dispositivo.**

# Tipos e como se propagam

## 7.Spora

O anexo é um arquivo ZIP que contém arquivos HTA dentro. Esses arquivos HTA usam uma extensão dupla, o que faz com que o usuário do computador acredite que o arquivo é um PDF ou DOC, após a abertura deste arquivo inicia instalação do Spora Ransomware, roubando arquivos e cobrando para ter os dados de volta.

## 8.WannaCry

Ele se aproveitou da vulnerabilidade do Windows conhecido com MS17-010, se espalhando pelas redes que uma vez instalado ele escaneia a rede e encontra dispositivos vulneráveis, pegando arquivos e cobrando para ter de volta onde no ano de 2017 espalhou rapidamente infectando mais de 10000 pessoas por hora, mas durou do dia 12 de maio ao dia 16 de maio após esses dias ele perdeu grande poder depois da correção dessa fragilidade.

## 9.Crypto

Ele pode ser distribuído por e-mails de phishing, downloads maliciosos, sites comprometidos e vulnerabilidade no sistema, após sua entrada no sistema ele desativa serviços de segurança para que o invasor possa criptografar os arquivos fazendo as pessoas pagarem para descriptografar.

# Impactos e consequência

**Um ataque Ransomware pode causar os seguintes impactos em uma organização; perda de dados importantes, Interrupção do negócio e prejuízos financeiros. Esses impactos causam como consequência, a perda de informações importantes e confidenciais como os dados dos clientes e informações financeiras, a paralisação de operações de uma empresa interrompendo assim o acesso a sistemas críticos e aplicativos, sem contar o pagamento exigido pelo cibercriminoso pela regaste dos dados perdidos.**

# Como detectar um ransomware e proteger-se dele

É necessário fazer verificações de vulnerabilidade, assim como ter certeza seu computador não é um alvo ideal para o ransomware. Também é necessário que o software do dispositivo esteja sempre atualizado para se beneficiar dos mais recentes patches de segurança.



É essencial que ter uma ação cuidadosa, principalmente sites e anexos de e-mail fraudulentos, entretanto essas medidas podem falhar o que torna necessário um plano de contingência. No caso de um ransomware esse plano seria ter um backup de seus dados.



**Obrigado pela  
atenção!!!**

