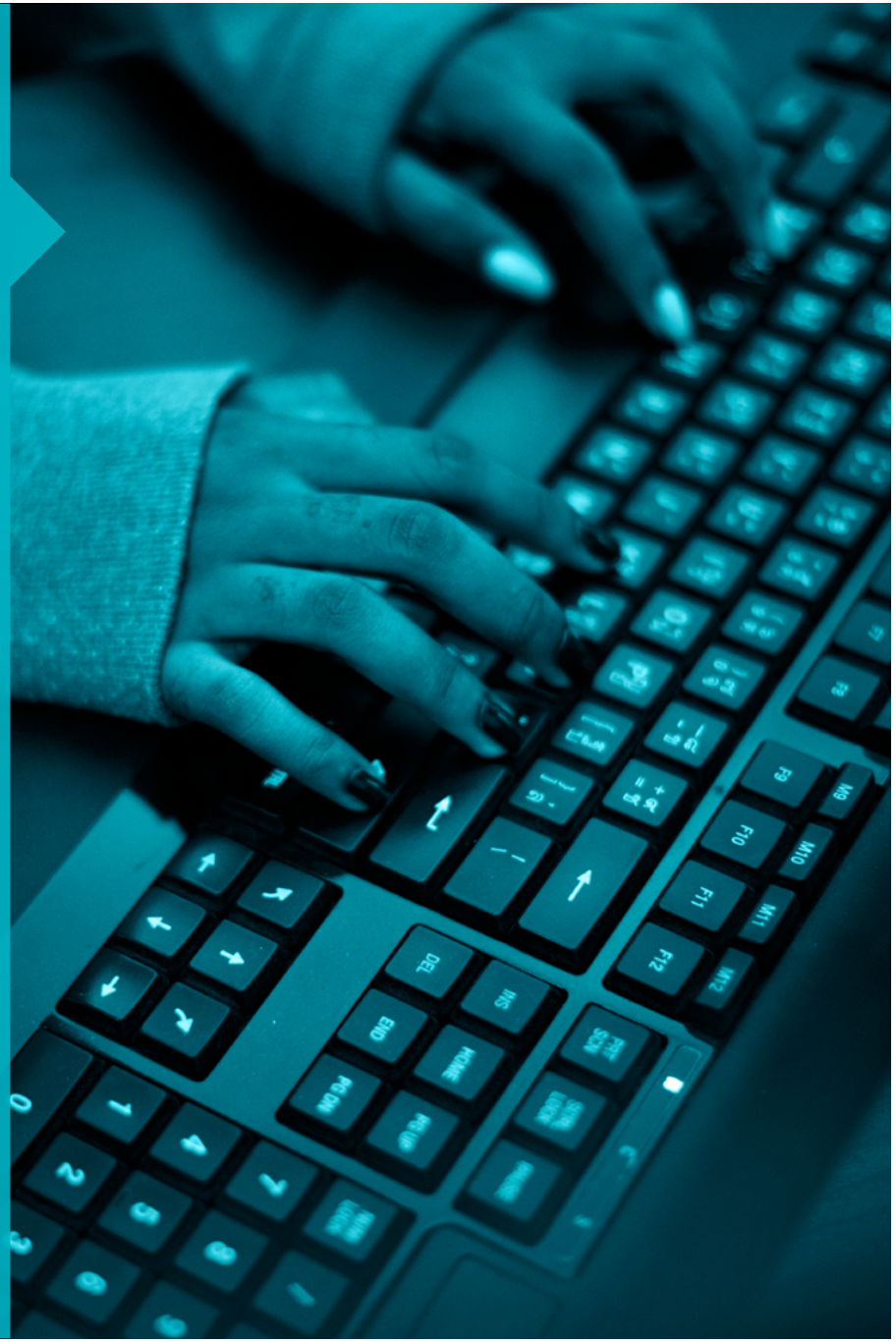
ENJOY SAFER TECHNOLOGY™

GUIA DE

Ransomware

Índice



O que é o ransomware?

Ransomware é uma categoria que corresponde a todo tipo de código malicioso que exige o pagamento de um resgate para recuperar a informação do usuário. Uma vez que infectou o equipamento, esse malware utiliza diferentes mecanismos para tornar os dados inacessíveis pelo usuário, com o objetivo de extorquir e exigir o pagamento de uma quantia de dinheiro em troca do acesso à informação novamente. É importante entender que o ransomware no geral não rouba e nem abre o conteúdo da informação, mas sim bloqueia seu acesso. As primeiras variantes de ransomware bloqueavam a tela do usuário e utilizavam diferentes formas para fazer com que as pessoas acreditassem que havia um problema ou haviam cometido algum delito e deveriam pagar para solucioná-lo. Atualmente, existem novas variantes que utilizam algorítmos complexos de criptografia para bloquear a informação e solicitar dinheiro, para em troca, recuperá-la. Diferente de outros códigos maliciosos, o ransomware não busca passar despercebido, muito pelo contrário: ele deseja chamar a atenção dos usuários infectados. Talvez muitas empresas foram infectadas com códigos maliciosos e nunca tenham percebido ou se passaram vários dias até que tenha sido detectada a infecção. Além disso, o ransomware se detecta no momento, já que o mesmo código cria um alerta avisando o usuário que sua informação se encontra bloqueada e que ele deve pagar pelo resgate.

Variantes e tipos de ransomware

Existem duas variantes principais desse código malicioso usado para extorquir suas vítimas. Por um lado, o ransomware de bloqueio de tela, mais conhecido como "lockscreen", que impede o acesso ao equipamento. Por outro lado, está o tipo de ransomware que utiliza a criptografia, chamado de "cryptolockers", que criptografam a informação dentro do equipamento, impedindo o acesso aos arquivos.

Lockscreen

O ransomware do tipo lockscreen é caracterizado por impedir o acesso e o uso do equipamento por meio de uma tela de bloqueio, impossibilitando qualquer ação para fechá-la, abrir o administrador de tarefas, os navegadores web ou qualquer outra parte do sistema. Nessa tela geralmente aparece uma mensagem em que se explica o ocorrido e se solicita o pagamento do resgate. Dado que essa variante não criptografa os arquivos, nesses casos a informação poderia ser recuperada, já que é possível extrair o disco rígido e logo limpar o equipamento dessa infecção. Por essa mesma razão, esse malware costuma fazer uso de enganos e truques de engenharia social para persuadir o usuário para que ele pague o resgate.

Variantes e tipos de ransomware

Cryptolockers

O ransomware do tipo criptográfico, por sua vez, utiliza diversos algorítimos de criptografia para bloquear o acesso aos arquivos do usuário. Uma vez que ele se apodera de um sistema, se inicia uma mudança na estrutura dos arquivos e documentos, de maneira que só seria possível voltar a ler ou utilizá-los se fossem restaurados a seu estado original, o que requer o uso de uma chave conhecida somente pelos cibercriminosos. Na maiorira dos casos, o ataque afeta somente certos arquivos, sendo os do *office* os mais prejudicados. Uma vez finalizada a infecção, aparece uma tela que indica que os arquivos foram criptografados e explicando ao usuário o processo de pagamento em dinheiro em troca da chave para descriptografar a informação.

Isso não significa que a criptografia seja intrinsecamente maliciosa. Ela é uma ferramenta poderosa e usada de forma legítima por indivíduos particulares, empresas e governos para proteger os dados contra acesso não autorizado. No entanto, igual qualquer outra ferramenta poderosa, a criptografia pode ser usada de maneira indevida para fins maliciosos, e isso é exatamente o que o ransomware criptográfico faz.

É possível recuperar os arquivos?

Essa é uma das primeiras perguntas, se não a primeira, que uma vítima do ransomware faz; e a resposta é: depende. Naturalmente, se você conta com a chave mestra será possível descriptografar os documentos, não obstante, conseguir a chave sem antes ter de pagar os cibercriminosos é complexo. Se bem existem variantes de cryptolockers para as quais é possível recuperar os arquivos afetados, na maioria das vezes isso se mostra quase inviável, ainda mais se o algorítimo é forte; a chave não pode ser obtida a partir do código do malware; e a chave mestra é única para cada vítima e funciona somente para um equipamento.

Vetores de propagação

As formas de propagação do ransomware são similares as de qualquer outro arquivo malicioso. A seguir você verá os vetores de infecção mais comuns.

Mensagens falsas no e-mail

Um método típico de infecção de ransomware é através de falsos e-mails que habitualmente dizem ser de uma empresa conhecida, um orgão bancário ou uma agência governamental. Esses e-mails enganam o usuário para fazer com que ele baixe um arquivo, seja esse documento anexado no e-mail ou através de um link na web. Esses arquivos maliciosos costumam ser trojans que aparentam ser documentos de texto ou imagens inofensivas, porém ao abrí-los se inicia o download do ransomware que finalmente bloqueia o equipamento e os arquivos do usuário. Por essa razão, sempre se recomenda não abrir arquivos anexados nem abrir links de e-mails desconhecidos ou não esperados.

Download de arquivos em redes p2p ou sites de software pirata

Outro vetor de propagação são os downloads de arquivos por meio de redes p2p ou sites de software pirata. Muitos desses sites ou arquivos prometem algum software gratuito ou cracks para evadir verificações de licenciamento. No entanto, longe de serem gratuitos, eles podem infectar o equipamento do usuário para obter algum tipo de ganho financeiro, por exemplo, mediante o pagamento de um resgate. Do mesmo modo, esse tipo de programa costuma solicitar que seja desabilitada a proteção antivírus, o que torna ainda mais fácil infectar o equipamento. Em ambos os casos, seja através de um e-mail falso ou uma página maliciosa, o atacante requer da intervenção do usuário para baixar e executar o arquivo infectado, e para conseguir enganá-lo a engenharia social é colocada em prática. Portanto, a precaução e educação em segurança da informação é uma saída para esses casos.

São propagados enganando o usuário?

Não há dúvidas que existem muitos códigos maliciosos que se propagam por si só, sem a intervenção do usuário e se aproveitando de vulnerabilidades dos sistemas ou aplicativos que se encontram desatualizados. Muitas variantes de ransomware trazem consigo um exploit que aproveita as vulnerabilidades para executar o código no equipamento e assim copiar o ransomware e executá-lo. Nesses casos, é muito comum a propagação através de equipamentos vulneráveis conectados na mesma rede. Quando o código malicioso consegue infectar um dos sistemas, automaticamente ele começa a se reproduzir nos demais equipamentos que estão expostos. Esse foi o caso da família WannaCryptor, que utilizava um exploit conhecido como EternalBlue para explorar uma vulnerabilidade presente no protocolo SMB (de arquivos compartilhados) que permitia a execução do código em um equipamento remoto. Dessa forma, o ransomware era capaz de se copiar e se executar através de uma porta 445 por todas as máquinas vulneráveis conectadas à rede. Outras variantes do ransomware, como Reveton, utilizavam uma vulnerabilidade de Java para explorar os navegadores que se conectavam em uma página web infectada e executar o código que bloqueava o equipamento. É por isso que manter os sistemas atualizados constantemente pode evitar infecções.

História e evolução do ransomware

Se bem o sequestro da informação tem ganhado relevância nos últimos anos, particularmente devido à campanha do WannaCryptor que causou um forte impacto em todo o mundo, a realidade é que o ransomware é uma ameaça que há vários anos vêm infectando dispositivos.

1989

PC Cyborg

Um trojan que substituía o arquivo AUTOEXEC.BAT, logo ocultava os diretórios e criptografava os nomes de todos os arquivos de unidade C, tornando o sistema inutilizável. Por último, se solicitava ao usuário uma "renovação de licença" por meio de um pagamento de 189 dólares a uma caixa de e-mail para PC Cyborg Corporation.

2005

GPCoder

Criptografava arquivos com extensões específicas como documentos e informações do usuário (xls, doc, txt, rtf, zip, rar, dbf, htm, html, jpg, db, etc.). Após isso, deixava um arquivo de texto instruindo o usuário para pagar o resgate em troca do programa e a chave para descriptografar os arquivos.

2010

WinLock

Bloqueava o equipamento e fazia com que aparecesse uma mensagem na tela, em que se solicitava que o usuário enviasse uma quantidade de SMS Premium para desbloqueá-lo.

2012

Reveton

Também conhecido como o "vírus da polícia", que também bloqueava o acesso ao equipamento, porém dessa vez fazia com que aparecesse uma tela com uma mensagem falsa da polícia nacional, ou ainda do FBI. Essa tela indicava ao usuário que o equipamento havia sido bloqueado por conter material ilegal, como pornografia infantil, software pirata ou conteúdo com direitos autorais, e que era necessário pagar uma "multa" para restaurar o acesso normal.

2013

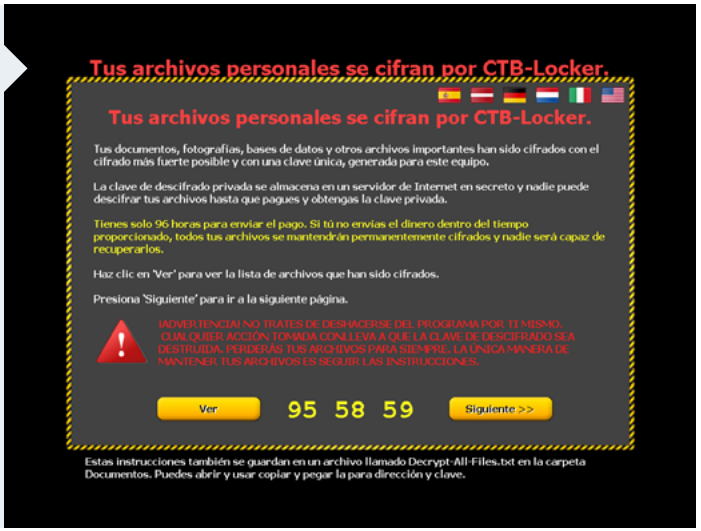
CryptoLocker y CryptoWall

Ransomware criptográfico que se caracterizou por utilizar criptografias assimétricas com uma chave pública RSA de 2048 bits; criptografava extensões específicas de arquivos de documentos, fotos e informações do usuário; utilizava conexões anônimas com o controlador do atacante e através de TOR; e foi um dos primeiros a solicitar o pagamento do resgate em bitcoins.

2015

CTB Locker

Com um comportamento similar ao Cryptolocker, se propagava através de um trojan que ao ser executado, fazia o download de um código malicioso que criptografava os arquivos do usuário. Do mesmo modo, soube administrar muito bem sua credibilidade: oferecia ao usuário a possibilidade de descriptografar de maneira gratuita até cinco arquivos para demonstrar que poderiam ser recuperados.



2017

WannaCryptor

Se tornou popular pelo nome de WannaCry (em português "quer chorar"), criptografa os arquivos do equipamento infectado utilizando uma combinação de algorítimos AES-128 e RSA-2048, o que faz com que seja impossível sua recuperação por meio de técnicas de análise. No entanto, o que fez com que o ataque se tornasse realmente escandaloso foi sua capacidade de propagação, de maneira similar a um worm, através das redes dos equipamentos infectados, utilizando uma vulnerabilidade no protocolo de arquivos compartilhados do Windows.

E quanto aos dispositivos móveis?

Baseando-se na mesma temática que o Reveton, no início de 2014 surgiram diversas famílias de ransomware para dispositivos Android com o mesmo truque da polícia, afirmando que o equipamento havia sido bloqueado por infringir uma lei e demandando o pagamento de uma multa. Esse ransomware de bloqueio de tela, detectados pela ESET como **Android/Koler** ou **Android/Locker**, utilizavam técnicas de engenharia social, incluindo garantir que o usuário era espiado pela câmera, para conseguir maior credibilidade e aumentar as chances de receber o dinheiro. Em meados de 2014, se detectou o primeiro ransomware de criptografia de arquivos para dispositivos Android, uma evolução esperada devido a grande extensão desses tipos de códigos maliciosos em dispositivos Windows. Esse trojan, chamado Simplocker, escaneia o cartão SD do dispositivo e criptografa os arquivos utilizando o algorítimo AES. Visto que se trata de um algorítimo simétrico, a chave de criptografia fica codificada dentro do equipamento e é possível recuperar os arquivos infectados sem ter de pagar os 20 dólares que o resgate solicita. No entanto, em um segundo ataque, foram encontrados novas variantes de Simplocker que incorporavam a utilização de chaves únicas geradas e enviadas através de conexões anônimas com o console do atacante por meio da rede TOR, não dando a oportunidade de descriptografar a informação.

E quanto aos dispositivos móveis?

Já em 2015, apareceu um novo ransomware de bloqueio de tela: Lockerpin. Esse código malicioso acessa o equipamento com as credenciais do administrador e muda seu PIN de desbloqueio. A particularidade do Lockerpin está nos diferentes tipos de engenharia social que utiliza para conseguir as credenciais do administrador, desde simplesmente solicitá-las ao usuário, até se passar por uma atualização do sistema. Além disso, ao tentar recuperar a informação ou as credenciais, o ransomware muda aleatoriamente o PIN. Desse modo, o usuário deve restaurar seu equipamento para as configurações de fábrica para eliminar o malware, junto com todos os arquivos e documentos do dispositivo.

No Android

No caso da variantes para os dispositivos móveis, a propagação costuma se dar através de aplicativos maliciosos em lojas não oficiais e fóruns. Muitas vezes esses aplicativos se passam por versões gratuitas ou modificadas de aplicativos ou jogos populares, guias ou truques para esses jogos, ou aplicativos que dizem agregar funções extras ao dispositivo. Além disso, através da engenharia social, os atacantes manipulam as vítimas para que cliquem em um *link* malicioso e as dirigem a um *pack* de aplicativos Android (APK) infectado. Nesses casos, esses *links* chegam através de e-mails, SMS ou até mensagens em fóruns e comentários. Por outro lado, a partir de 2016 começaram a surgir casos em que os cibercriminosos incorporaram outros métodos mais sofisticados a suas técnicas de propagação. Os atacantes tentam esconder os *payloads* (a parte maliciosa do código) o mais profundo possível dentro dos aplicativos, com o objetivo de que sejam indetectáveis pelos controles das lojas oficiais e alguns fóruns. Para isso, uma técnica é criptografar o código e logo transmitir o arquivo para a pasta de ativos, em que se costuma guardar imagens ou outros conteúdos necessários do aplicativo. Portanto, o aplicativo não parece ter nenhuma função maliciosa por fora, porém carrega de modo oculto em seu interior uma ferramenta capaz de descriptografar e executar o ransomware. É por isso que ao utilizar seu dispositivo móvel, o mais importante é não baixar aplicativos de fóruns ou lojas não oficiais, além de manter o equipamento atualizado e obter uma solução de segurança.

Qual o risco do ransomware para as empresas?

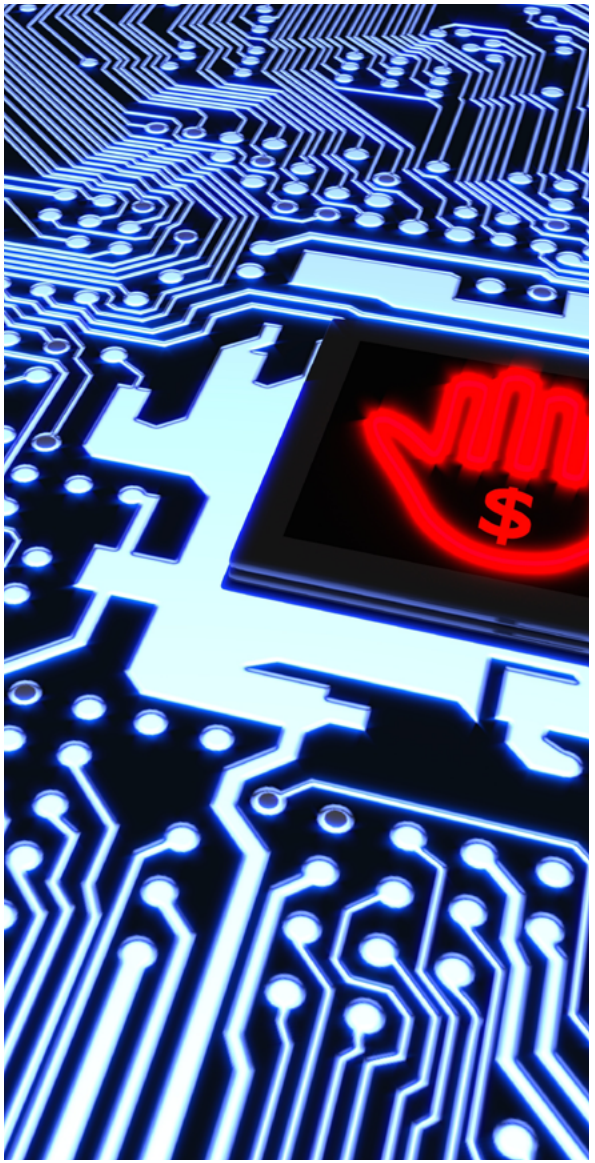
A informação é um ativo muito valioso para a organização. Desse modo, se sua disponibilidade se encontra comprometida, isso pode implicar em grandes consequências, talvez até devastadoras. Essa é a principal razão pela qual muitos ataques de ransomware estão orientados à infectar arquivos e informações corporativas. Do mesmo modo, a maioria das empresas trabalham com redes de informação compartilhadas, o que faz com que uma infecção possa se propagar rapidamente através da rede, infectando não só estações de trabalho dos empregados, mas também os servidores e bases de dados da companhia, em que muitas vezes se armazenam informações e dados sensíveis. A seguir, detalharemos alguns riscos específicos: em primeiro lugar, temos que mencionar as perdas financeiras, particularmente em casos em que a informação que se perde é composta por dados privados de clientes, que devem ser ressarcidos e/ou indenizados de alguma forma. Nesse mesmo sentido, se os arquivos afetados são patentes ou fórmulas de certos produtos, isso poderia derivar na interrupção completa ou parcial do negócio. Nessa mesma linha, existem companhias que concentram seu trabalho em servidores na nuvem, então se eles se mostram infectados e não se conta com um plano de continuidade para seguir trabalhando offline, então o funcionamento correto do negócio também se verá interrompido. Além disso, temos que mencionar um

Qual é o risco do ransomware para as empresas?

ESET coloca à disposição das empresas o **Kit Anti-Ransomware** que busca combinar a educação dos usuários com a melhor tecnlogia multi-camada e uma melhor gestão da segurança da empresa.

Mais Informações

tema muito importante: o dano à marca. Esse é um risco que compromete diretamente o prestígio, a solidez e até a credibilidade de uma empresa; é difícil medir quanto dinheiro se poderia perder, porém é possível observar isso a partir da percepção dos usuários ou clientes, aqueles que perdem a confiança rapidamente e recuperá-la se torna uma tarefa muito complexa. Por fim, destacamos a responsabilidade legal, ou seja, as obrigações que uma companhia possui, com base em como são as leis de proteção de dados nos países em que são vigentes. Novamente, caso haja perda de informação, se deve pagar multas e indenizações para os que foram vítimas do ataque. Mesmo não sendo recomendado que se pague o resgate, muitas vezes resulta mais prejudicial a perda da informação, do que ceder ao atacante. No caso das empresas, não só devem considerar o valor da informação perdida em si, mas também os custos indiretos (muitas vezes maiores, tal como os pontos que destacamos anteriormente) que implicam em deter a operatória, não disponibilizar um serviço, demorar na execução de atividades ou qualquer outra consequência que afete a continuidade do negócio.



Medidas de proteção

O ransomware é uma ameaça à disponibilidade da informação, dado que seu êxito será determinado por sua capacidade de bloquear os arquivos ou o sistema da vítima, e que essa, não tenha um plano de recuperação de dados, como pode ser um backup. Portanto, igual a qualquer outra ameaça que coloca em risco o acesso à informação, a principal ferramenta para recuperá-la é possuir uma cópia de backup.

A importância do backup

Contar com uma cópia dos arquivos críticos é muito importante, para caso haja perda da informação, especialmente porque existem diversas causas pelas quais um usuário poderia passar por esse problema. Por exemplo, a limitada vida útil dos discos rígidos, os roubos de dispositivos e, é claro, os inúmeros códigos maliciosos. Dado que o objetivo de um backup é poder recuperar a informação caso ocorra algum desses incidentes, não é recomdável que suas unidades estejam conectadas à rede o tempo todo, já que, em caso de uma infecção, os dados também poderiam ser afetados. Sempre é mehor que o backup seja realizado em um disco ou dispotivo externo, que se armazene em um lugar diferente do equipamento, de forma que não seja roubado e nem afetado por um incidente.

Medidas de proteção

O que uma política de backup empresarial deve incluir?

Nem toda informação possui o mesmo valor, portanto, antes de começar o processo de bakcup, é fundamental determinar que informação será recuperada. Isso pode ser feito atribuindo valor aos dados e estabelecendo quais possuem maior relevância segundo as preferências pessoais, o tipo de trabalho que se realizam com tais dados, ou até o objetivo e a utilidade que possuem. Existem três aspectos que devem ser analisados na hora de classificar a informação e estabelecer uma política de **backup:**

Criticidade:

Determinar que informação é importante recuperar. Levar em consideração toda a informação que a empresa utiliza diariamente para funcionar, assim como também aquela que deve ser conservada para consultas futuras. É importante entender que realizar um backup requer certo custo e esforço, portanto é importante determinar qual é a informação que realmente vale a pena recuperar.

Periodicidade:

Não se pode perder o controle da frequência com a qual se modificam os dados. Existe informação dinâmica e histórica e é importante entender a diferença entre cada uma para determinar quanto tempo se realizará o resguardo da informação. Existem diferentes tipos de backup: Completo, Diferencial e Incremental. Cada um possui seu custo benefício, esforço e peridiocidade, portanto é recomendável saber de quanto em quanto tempo será preciso resguardar a informação para assim escolher qual se ajusta as suas necessidades.

Meio:

O suporte escolhido para fazer o backup da informação (disco rígido, meio ópticos, a nuvem, etc.), dependerá da quantidade de informação que se quer guardar, a periodicidade com que se vai realizar o backup e a acessibilidade requerida. Além disso, deve ser considerado o espaço físico onde se guarda o suporte de recuperação, de modo que também esteja protegido.

Por último, é recomendável não pensar unicamente nos arquivos ou nos dados que se quer guardar, mas também nas configurações e documentação necessária para colocar em funcionamento um equipamento ou sistema. Em muitos casos, mediante uma infecção de ransomware é provável que os técnicos terão de restaurar os sistemas, o que implica investir muitas horas em configurações. Ter essas configurações já guardadas com certeza irá economizar várias horas de trabalho.

Educação e conscientização

Os usuários mais vulneráveis são aqueles que estão desinformados, aqueles que não estam alertas se recebem um e-mail falso, que acreditam que o ransomware é algo somente visto em filmes ou que incidentes de segurança ocorrem unicamente em governos e grandes corporações multinacionais. A maioria das infecções de ransomware requerem, em certo momento, a intervenção do usuário: seja para baixar um arquivo, acessar um link malicioso, abrir um documento ou realizar o pagamento com base na engenharia social. Mais cedo ou mais tarde a engenharia social será uma chave para o êxito da infecção. Portanto, outro ponto importante na prevenção é a educação e a conscientização dos usuários.

Estar informado sobre como as ameaças atuam, quais são as técnicas usadas para enganar e infectar os usuários, de que maneira se propagam e como previní-las são alguns dos conhecimentos que podem evitar que um empregado seja infectado.

Uma boa campanha de conscientização não é feita através de ações esporádicas, muito pelo contrário, é **necessário uma educação periódica e constante.** A chave é não se concentrar em apenas um recurso, mas sim aproveitar qualquer oportunidade para educar. Não só se consegue a conscientização por meio de palestras e cursos explicando os riscos e as medidas de segurança, além disso, é possível oferecer um complemento com lembretes periódicos de boas práticas, um boletim de notícias da atualidade, guias e manuais de configurações de privacidade e segurança, ou até mesmo posters e conselhos.

Outras medidas de proteção

Sem dúvidas, o uso da engenharia social é um dos principais mecanismos utilizados pelos atacantes para propagar suas ameaças, no entanto, não é o único, já que existem técnicas que não requerem a ação do usuário com a ameça para que ela seja instalada. Por exemplo, a infecção de um *iframe* em um site vulnerável pode fazer que com um atacante instale algo no dispositivo do usuário sem que ele perceba o que está acontecendo. É por isso que também é importante contar com uma solução de segurança que detecte esse comportamento malicioso.

Se bem o ransomware pareceria ser a ameaça "da moda" nos últimos tempos, são muitos os tipos de ameaças que estão sendo propagadas e que afetam os usuários. Seja tratando-se de um trojan, um worm, um bot ou até mesmo o ransomware, uma boa ferramenta integral de segurança será capaz de prevenir a infecção.

O termo "antivírus" ficou preso no subconsciente coletivo. No entanto, esse tipo de ferramenta evoluiu e passou a detectar além de vírus informáticos até se converter em soluções de segurança completas, que oferecem diversas funções como firewall, filtros de email e antispam, antiphishing ou escaneamente de memória, entre outras, que garantem uma proteção integral ao sistema e permitem navegar de maneira segura no contexto atual das ameaças.

Por último, é importante atualizar regularmente os sistemas e aplicações, já que muitas ameaças aproveitam vulnerabilidades não corrigidas para se propagar pela rede. Se bem está tarefa parece tediosa e rotineira, existem ferramentas de gestão de patches e atualizações que simplificam bastante o trabalho.

O que fazer caso haja uma infecção?

É importante destacar que, mediante uma infecção, a possibilidade de recuperar a informação e a forma de fazer isso dependerá do tipo específico da ameaça.

No geral, nos casos do tipo lockscreen é possível recuperar o acesso ao sistema retirando a infecção ou restaurando o equipamento. Além disso, se os arquivos não são criptografados é possível recuperá-los do disco afetado. No entanto, em algumas variantes, especialmente aquelas que afetam dispositivos móveis, o bloqueio não permite a recuperação do equipamento, dado que a única solução seria restaurar os padrões de fábrica, eliminando toda a informação.

No caso dos filecoders a recuperação pode ser mais complicada. Do mesmo modo, na maioria dos casos, um bom software de segurança deveria ser capaz de elimanar o ransomware do equipamento, ou os arquivos continuarão criptografados. Em algumas famílias de ransomware, especialmente as que utilizam a criptografia simétrica e guardam a chave dentro do código malicioso, é possível recuperar os arquivos utilizando a ferramenta específica de descriptografia. No entanto, os arquivos que foram atacados por um tipo mais sofisticado de ransomware, como Cryptolocker, são impossíveis de descriptografar sem a chave correta.

Em qualquer caso de infecção se recomenda mitigar essa ameaça do equipamento, seja utilizando uma ferramenta de segurança ou reinstalando o sistema, e logo recuperar a informação e os arquivos através de um backup.

Pagar ou não pagar?

Hoje em dia o ransomware é algo rentável para os cibercriminosos, já que muitas pessoas e empresas decidem aceitar as demandas e pagar o resgate em troca da recuperação de sua informação. De fato, segundo o tipo de infecção, os atacantes podem lucrar milhares de dólares em apenas dias.

No geral, ao realizar o pagamento se recupera a chave para descriptografar a informação, já que caso haja boatos que os atacantes não fazem sua parte do acordo, ninguém iria pagar. No entanto, nós do laboratório da ESET **não recomendamos pagar** o resgate e não aceitar as demandas dos atacantes, por duas razões concretas.

Mesmo algumas vezes ao pagar o resgate se restaura o acesso aos dados, a verdade é que se está negociando com um cibercriminoso do outro lado, o qual não sabemos a identidade, nem temos a chance de encontrá-lo. Portanto, não existe nenhuma garantia de que realmente serão enviadas as chaves de descriptografia. Houveram casos em que não foi possível recuperar a informação, já que o criminoso jamais respondeu depois do pagamento do resgate, ou até mesmo solicitou o pagamento três vezes antes de realmente devolver o acesso aos dados.

Por outro lado, aceitar essas demandas só contribui para que esse tipo de ação por meio do ransomware seja cada vez mais rentável para os atacantes, e portanto, eles irão aperfeiçoando suas técnicas e se adptando a novos cenários. Se as vítimas possuem backup de seus dados e estão prevenidas, não será necessário que paguem o resgate, e isso vai enfraquecendo os esforços dos cibercriminosos. Por último, o pagamento do resgate não significa que o usuário estará fora de perigo. Os atacantes podem deixar o malware no equipamento, já que agora sabem que está disposto à pagar dinheiro para recuperar o acesso ao equipamento ou aos dados. Resumindo, poderia voltar a ser o objetivo de outro ataque futuramente.

Conclusão

O ransomware é uma ameaça que chegou para ficar. Há vários anos ele tem evoluído, fazendo uso de métodos e algoritmos de criptografia cada vez mais complexos. Lamentavelmente, enquanto essa ameaça continuar sendo uma das atividades mais rentáveis para os cibercriminosos, eles irão aperfeiçoando suas técnicas e se adptando a novos cenários. De qualquer forma, as mesmas técnicas de propagação seguirão vigentes: engenharia social, arquivos anexados em e-mails e exploração de vulnerabilidades, principalmente.

Está claro que as coisas estão cada vez mais sofisticadas no mundo da tecnologia e as ameaças acompanham essa evolução. Com a aparição dos dispositivos móveis, as variantes de ransomware e outras ameaças que afetam dispositivos Android não demoraram muito para surgir, e com o auge da Internet das Coisas já é possível ver códigos maliciosos que afetam esses equipamentos.

Não é uma surpresa que o termo jackware está cada vez mais ganhando popularidade. Se refere justamente ao software malicioso que tenta tomar o controle de um dispositivo cujo objetivo principal não é o processamento de dados nem a comunicação digital, como um automóvel. Mesmo esses equipamentos processando uma grande quantidade de informações, eles fazem isso com outro objetivo, que no caso de um automóvel é transportar os passageiros de um lugar para outro de forma segura. Portanto, vemos o jackware como uma forma evoluída do ransomware, cujo objetivo é bloquear um dispositivo que o usuário necessita até que paguem um resgate. Se pensarmos o mesmo cenário, só que em relação às infraestruturas críticas de uma região, o panorama é ainda mais preocupante.

Portanto, com o ransomware cada vez mais em evolução e as novas tecnologias em auge, torna de extrema importância a educação dos usuários, tanto em sua vida pessoal como em suas atividades dentro da empresa. Assim como também é imprescindível para as organizações combater esse tipo de ameaça com uma correta gestão de segurança e, em caso forem vítimas, não realizarem nenhum pagamento para que assim essa conduta criminosa termine.

www.eset.com/br

ESETBrasil

@ESET_brasil

/company/eset-brasil