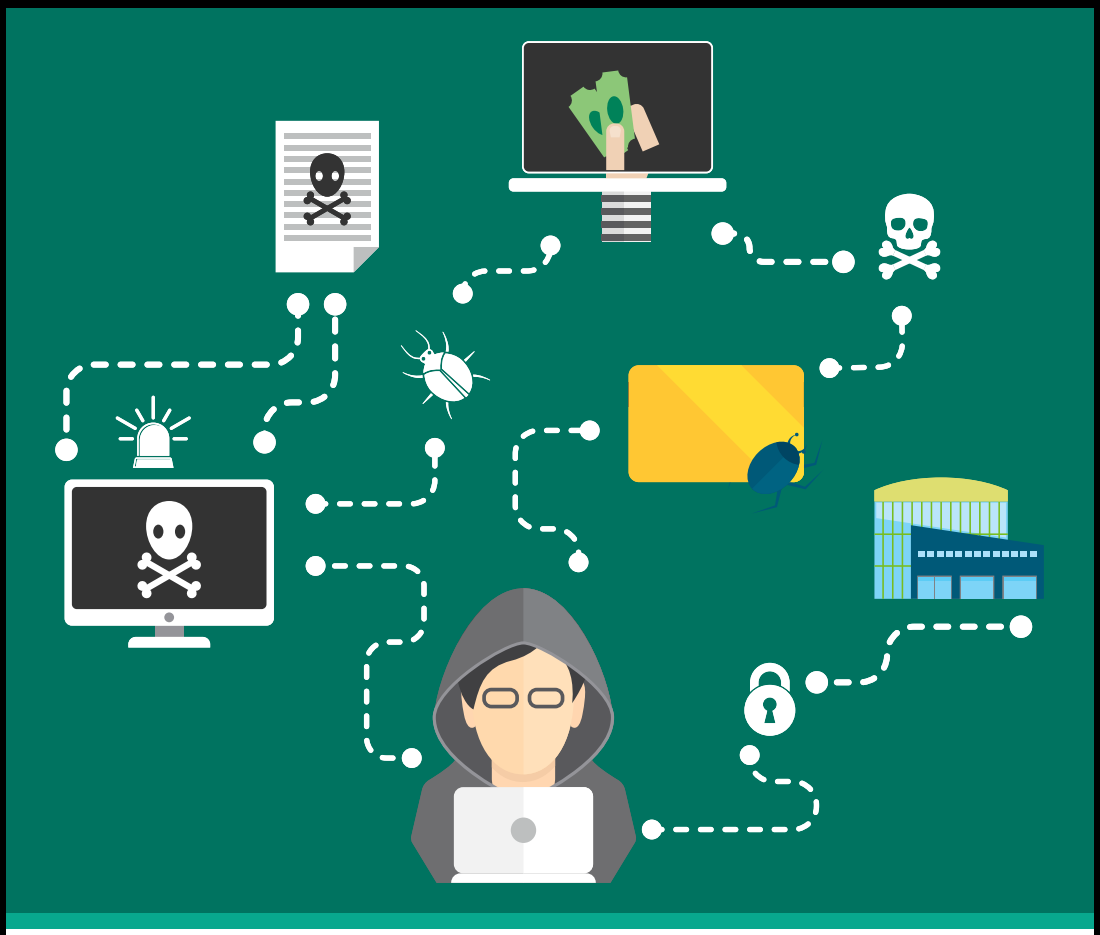
SECURITY [SNAPSHOT]



Quando os cryptors atacam:

Linha do tempo de infecção por ransomware

KASPERSKY lab

Os cryptomawares devem ser uma preocupação para SMBs?

Os danos causados por cryptomalware podem ser divididos em duas partes: o resgate e as perdas secundárias. Por meio de pesquisa com mais de 4.000 pequenas e médias empresas conduzida pela Kaspersky Lab e a B2B International, podemos olhar mais de perto os números por trás dos danos:

49% dos representantes de SMBs alegam considerar cryptomalwares uma das ameaças mais sérias que suas empresas podem vir a encarar.

$99,000 prejuízo monetário médio para SMBs causados por ataques de cryptomalware.

1 de 5 negócios que não conseguem os dados de volta depois de pagar o resgate.

67% SMBs que reportaram perdas parciais ou completas de dados corporativos em função de ataques de cryptomalwares.

O que são os cryptomalwares?

Cryptomalwares são um tipo de ransomware – o malware que pede um resgate em troca de desbloquear o acesso ao seu computador, servidor ou arquivos. No caso do cryptomalware, arquivos e dados armazenados são sequestrados dos dispositivos infectados. Ele criptografa os dados em uma forma ilegível, e os dados podem ser desbloqueados apenas com uma senha liberada depois de o resgate ser pago.

Eles são uma ameaça nefasta que torna a recuperação de dados corporativos virtualmente impossível. Portanto, há a pressão adicional de um tempo limite, já que o resgate deve ser pago em uma certa quantidade de dias, caso contrário as informações são apagadas.

Linha do tempo do ataque de um Cryptor

Como exatamente esse tipo de ataque acontece?
Falaremos do passo a passo e as ações que podem ser tomadas para prevenir que você entre nessa situação.

1 Perímetro rompido.

Cibercriminosos procuram a forma mais fácil de entrar no seu sistema, o que pode ser um e-mail enviado a seus colaboradores com um anexo infectado. Outra opção é infectar um site com um malware que use exploit kits para identificar vulnerabilidades em softwares no seu PC. O exploit kit se comunica com o PC e instala códigos maliciosos. Comumente, isso ocorre sem que o usuário saiba.

O QUE FAZER?

Instale solução de segurança robusta multicamadas que verifique continuamente a existência de malware de diversos ângulos, a fim de proteger seu sistema do vazamento.

2 Descoberta e pânico

Nesse ponto, o departamento de TI descobre o vazamento, e tudo para abruptamente. Muitas perguntas devem ser respondidas. Quantas máquinas estão infectadas? Dados foram roubados? Temos backups que restaurem tudo para deixar as coisas nos eixos?

O QUE FAZER?

Para o departamento de TI, o dia será ruim. Ninguém quer encarar a situação de ter computadores infectados – ou pior – a rede inteira offline. Tenha um plano preparado no caso de ataque de cryptor, pois sua empresa talvez precise lidar com esse cenário azarado.

3 Pagamos ou não o resgate?

A maioria dos cibercriminosos fazem a exigência de pagamento em bitcoins – moeda irrastreável. Tenha em mente, porém, que uma em cada cinco empresas que pagam o resgate não tem seus dados devolvidos.

O QUE FAZER?

Não recomendamos pagar o resgate por várias razões. Além do fato de não existir qualquer garantia que a senha de desbloqueio será recebida, há o fato de que pagá-lo não é seu único problema. Se for a única opção da empresa, trata-se de um indicativo da falta de um plano de recuperação contra desastres. Quando o cenário é esse, provavelmente não será possível remediar o ataque e expurgar a infecção de sua infraestrutura de forma completa. Finalmente, todos temos de quebrar o ciclo e não alimentar a máquina do cibercrime. Se não há lucro, cibercriminosos não terão motivo para desenvolver ransomwares.

4 Atrasos e interrupção de atividades.

A maioria dos cryptomalwares fornecem um limite de tempo para pagamento do resgate, normalmente três dias. De acordo com nossa pesquisa, 41% reportam perder um número significante de arquivos depois de demorar um dia ou mais para detectar o ataque. Enquanto tudo isso ocorre, as operações da empresa são interrompidas. Não é fácil mensurar o impacto na rotina do negócio, pois depende das medidas preventivas preparadas pela sua equipe de TI antes mesmo da infecção. Seus backups estão em dia? Os softwares estão atualizados? O resto da sua equipe entende os passos para parar de espalhar uma infecção? Todos esses fatores são importantes para conter o ataque e mitigar as perdas.

O QUE FAZER?

Prepare-se. Faça backups regulares. Mantenha softwares atualizados. Eduque seus colaboradores sobre boas práticas com e-mails.

5 Postmortem e investigação.

Uma das únicas coisas boas resultantes de um ataque são o conhecimento e aprendizados adquiridos. Provavelmente, depois de um ataque, a empresa terá mais maturidade e informações para prevenir outra infecção.

O QUE FAZER?

Você e sua equipe de TI devem se fazer as seguintes perguntas: o que deu errado? Como podemos nos proteger no futuro? Precisamos educar nossos colaboradores? Qual nosso ponto fraco? Como podemos melhorá-lo? Faça as análises e execute as mudanças necessárias.

Como prevenimos um ataque de um cryptomalware?

Está claro que prevenção é o superpoder capaz de derrotar cryptomalwares.
Apresentamos 10 passos recomendados para evitar que ataques joguem seu negócio para escanteio.

1. **FAÇA BACKUPS REGULARES.** A única forma de garantir que sua empresa consiga lidar imediatamente com um ataque de ransomware é implementar um cronograma de backups regulares, pois só assim não será necessário confiar em cibercriminosos para restaurar as atividades de seu sistema.

2. **FIQUE DE OLHO NOS BACKUPS.** Existe a possibilidade de algo comprometer seus arquivos. Verifique regularmente a integridade dos backups.

3. **PROTEJA-SE CONTRA O PHISHING.** Ensine os colaboradores que nunca devem abrir anexos de fontes desconhecidas ou de amigos que por ventura tenham sido hackeados.

4. **NÃO CONFIE EM NINGUÉM.** Ou melhor, confie, mas verifique. Links maliciosos podem ser enviados mesmo por amigos e colegas cujas contas tenham sido invadidas. Se um colaborador recebe algo fora normal de um contato conhecido, o próximo passo é entrar em contato com o remetente e verificar se a mensagem é legítima.

5. **HABILITE A OPÇÃO "EXIBIR EXTENSÕES" NAS CONFIGURAÇÕES DO WINDOWS.** Trojans são programas, funcionários devem ser instruídos a manterem distância de extensões como "exe", "vbs" e "scr." Golpistas podem usar diversas extensões para mascarar o arquivo como um vídeo, foto ou documento.

6. **ATUALIZE SEU SISTEMA OPERACIONAL REGULARMENTE.** Cibercriminosos exploram vulnerabilidades em softwares para comprometer sistemas. Com as ferramentas automáticas de Vulnerability Assessment e Patch Management da Kaspersky Lab, seu sistema será verificado, e as patches serão distribuídas regularmente a fim de mantê-lo atualizado.

7. **USE UM PROGRAMA DE ANTIVÍRUS ROBUSTO PARA COMBATER RANSOMWARE.** Os produtos da Kaspersky Lab empregam sistema de defesa multicamadas que fica de olho em malwares de diversos ângulos diferentes, assegurando que seus computadores não sejam corrompidos.

Mas e se os ransomwares conseguirem uma brecha...

8. **INTERROMPA A CONEXÃO COM A INTERNET IMEDIATAMENTE.** Caso descubra um ransomware, corte a internet na hora. Se ainda não tiver apagado a senha de desbloqueio do computador em questão ainda há uma chance de restaurar os arquivos.

9. **NÃO PAGUE O RESGATE.** Se seus arquivos forem criptografados, não recomendamos realizar o pagamento a menos que o acesso imediato a certos arquivos seja crucial. Cada transação realizada favorece a prosperidade dos criminosos e os incentiva a continuar criando ransomware.

10. **TENTE IDENTIFICAR O MALWARE.** Caso você seja atingido por um ransomware, tente descobrir o nome do malware. Versões antigas de ransomware tendem a ser menos avançadas, nesse caso, talvez seja possível restaurar seus arquivos. Além disso, especialistas em cibersegurança, incluindo os da Kaspersky Lab, colaboram com a polícia para fornecer ferramentas de restauração online, na esperança de parar os criminosos. Algumas vítimas são capazes de desbloquear arquivos sem pagar resgate. Para ver se isso é possível, visite o NoMoreRansom.org

True Cybersecurity for Business

A abordagem de cibersegurança de verdade da Kaspersky Lab combina segurança multicamadas com inteligência de ameaças assistida por nuvem e aprendizado de máquina com objetivo de proteger seu negócio de ameaças. Visamos não apenas prevenir ataques, mas também os antecipar, detectar e responder rapidamente, tudo isso, enquanto garantimos a continuidade do funcionamento de sua organização.

Sobre a Kaspersky Lab

A Kaspersky Lab é uma das empresas de cibersegruança de crescimento mais rápido e a maior privada. Está ranqueada entre as quarto principais distribuidoras de soluções de segurança para terminais (IDC, 2014). Desde 1997, a Kaspersky Lab inova em cibersegurança e fornece soluções de segurança digitais e inteligências de ameaças para grandes empresas, SMBs e consumidores. A Kaspersky Lab é uma empresa internacional. Opera em quase 200 países e territórios ao redor do mundo, protegendo mais de 400 milhões de usuários pelo mundo.
Saiba mais em kaspersky.com.br.

Aprenda mais sobre cibersegurança: **www.securelist.com**
Encontre um parceiro perto da sua empresa:
www.kasperskypartners.com/?eid=global&lang=pt-br

kaspersky.com.br
#truecybersecurity

Fale conosco:
kaspersky.com.br/small-to-medium-business-security/contact-us