IV SIMTEC
Simpósio de Tecnologia da Fatec Taquaritinga

SEGURANÇA DA INFORMAÇÃO COM FOCO NA PROPAGAÇÃO IMINENTE DE *RANSOMWARE* NAS CORPORAÇÕES

INFORMATION SECURITY WITH A FOCUS ON RANSOMWARE'S IMPROVED PROPAGATION IN CORPORATIONS

Jeferson William Candido – jefersonw.candido@gmail.com
João Henrique Gião Borges – jhgborges@gmail.com
Fabiana Florian – fflorian@uniara.com.br
Universidade de Araraquara (UNIARA) – SP - Brasil

RESUMO

Este artigo tem como objetivo principal apresentar os problemas causados por um software mal-intencionado, denominado *Ransomware* e ajudar as corporações na prevenção de ataques iminentes reduzindo os impactos de ataques. Geralmente esses ataques ocorrem em grandes corporações causando sérias consequências no ambiente. Serão sugeridos alguns métodos para a proteção da disseminação desse software. *Ransomware* é um termo que se refere a uma ameaça de computador, em que criminosos instalam o *Malware* no ambiente do usuário e tentam extrair dinheiro de suas vitimas, ocorrendo o que se pode chamar de cibercrime. Sua cadeia pode ser dividida em dois tipos principais e subdividida conforme as famílias que as representam. As duas principais formas de *Ransomware* são: aquelas que criptografam, ofuscam ou impedem o acesso aos arquivos; e aquelas que restringem o acesso ou bloqueiam os usuários dos sistemas. Espera-se que este trabalho possa sugerir contribuições para reduzir a propagação desse software mal-intencionado nas corporações.

Palavras-chave: Ciberataques. Cibercrime. Hackers. *Malware*. Ransomware. Software.

ABSTRACT

The main goal of this article is to introduce the problems caused by malicious software, called Ransomware, and helps corporations to prevent imminent attacks by reducing the impact of attacks by 95%. Usually these attacks occur in large corporations causing serious consequences in the environment. Some methods will be suggested for the protection of the dissemination of this software. Ransomware is a term that if you run a computer threat, in which criminals install the Malware in the User's environment and try to extract money from their vice, occurring what can be called cybercrime. Your chain can be divided into two main types and subdivided according to the families they represent. As two main forms of Ransomware are: those that encrypt, obfuscate or prevent access to the files; and those that restrict access or blockage to system users. It is hoped that this paper allows to suggest contributions to reduce the spread of malicious software in corporations.

Keywords: *Cyber attacks. Cybercrime. Hackers. Malware. Ransomware. Software.*

1 INTRODUÇÃO

Ao longo dos últimos anos, o número de ciberataques registrados em todo o mundo tem crescido em níveis alarmantes em mais de 74 países, principalmente devido à utilização cada vez maior da internet. A cada dia, os cibercriminosos encontram maneiras mais sofisticadas de enganar os internautas e obterem ainda mais lucros com seus ataques. E um dos *Malware*s *"malicious software"* ou software malicioso, que vem ganhando bastante notoriedade no universo do cibercrime é o *Ransomware* (AFRIKATEC, 2017).

Esse tipo de *Malware* é altamente rentável no mundo dos hackers, pois o *Ransomware* consiste em impedir que o usuário acesse seu computador ou quase todos seus arquivos pessoais solicitando um 'resgate', na forma de dinheiro ou na moeda virtual *"Bitcoin",* para que seus dados sejam liberados. Algumas pessoas leigas no assunto entram em desespero e acabam pagando a quantia que os cibercriminosos pedem – algo em torno de US$300 dólares (AFRIKATEC, 2017).

Na maioria das vezes, os *hackers* não cumprem com sua parte do acordo e não enviam o "*decrypter"* com a chave de desbloqueio. Todo o processamento realizado pelo *Ransomware* ocorre de maneira silenciosa, sem que a vítima se de conta do que está acontecendo. É por isso que o *Ransomware* vem sendo considerado um dos grandes problemas em termos de segurança da informação na atualidade (AFRIKATEC, 2017).

O pior caso de *Ransomware* já registrado na história da informática ocorreu em maio de 2017, onde quase metade do planeta foi atingido por um *Ransomware* denominado *"WannaCry",* onde os primeiros efeitos foram no Reino Unido, o Sistema Publico de Saúde (GLOBO, 2017).

1.1 Objetivo

Este artigo tem como objetivo principal apresentar os problemas causados por um software mal-intencionado, denominado *Ransomware* e ajudar as corporações na prevenção de ataques iminentes reduzindo os impactos desses ataques.

1.2 Justificativa

Equipamentos totalmente conectados a internet vêm crescendo em larga escala e muitas ameaças vêm surgindo no intuito de atingir os usuários ou até mesmo grandes corporações por todo o mundo com extorsão de dinheiro. Tornar esses ambientes mais seguros os torna quase invisíveis na mira dos Hackers. Por isso, com o objetivo de contribuir na prevenção desses ataques, fazem-se necessários estudos para explorar as vulnerabilidades de grandes ambientes e entender como esses tipos de *Malware* passam despercebidos e infectam os mais diversos equipamentos.

1.3 Metodologia

Para o desenvolvimento deste trabalho, foram realizadas pesquisas bibliográficas em sites de segurança com foco no estudo em Engenharia Social e Reversa.

Foi realizada, também, uma pesquisa de como se prevenir desse tipo de ameaça usando técnicas de isolamento de sistemas operacionais desatualizados com *Virtual Patching* e desativação de portas RDP´s ou Terminal Server abertas desnecessariamente no ambiente, configuração de Firewall com o protocolo SMB entre redes, rotinas de backup, filtro de caixas de e-mails e técnicas de prevenção de detecção de intrusão IDS, a fim de entender como o *Ransomware* se propaga no ambiente.

2 O RANSOMWARE

2.1 Conceito do Ransomware

O *Ransomware* ou *"ransom"*, em inglês, significa resgate, exigir resgate, pagar para resgatar; é uma espécie de *Malware* por resgate (software mal-intencionado) que os criminosos instalam em seu computador sem seu consentimento (MICROSOFT, 2016).

O *Ransomware* concede aos criminosos a possibilidade de bloquear seu computador de um local remoto. Depois, ele apresenta uma janela *pop-up* com um aviso de que seu computador está bloqueado e você não poderá acessá-lo, e, em seguida, é cobrado um valor em dinheiro pelo resgate, geralmente usando a moeda virtual *"Bitcoin",* que torna quase impossível rastrear o criminoso que pode vir a receber o valor exigido. A *BiTCoin* (BTC) é uma unidade monetária online, criada em 2009, que permite a transferência anônima de valores. Desenvolvida por Nakamoto, a BTC é uma moeda descentralizada, ou seja, não conta com nenhum órgão responsável pelo seu gerenciamento. Dessa forma, as transações de

bitcoins são feitas a partir da rede de compartilhamentos P2P (PontoaPonto) (MICROSOFT, 2016).

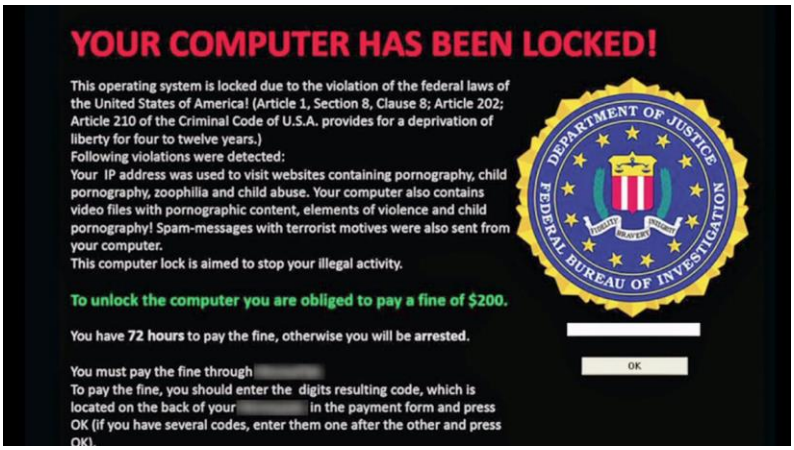
As Figuras 1 e 2 apresentam exemplos de telas na infecção do *Ransomware*.

Figura 1- Tela exibida pelo *Ransomware WannaCry*.



Fonte: PROOF (2017)

Figura 2- Tela exibida pelo *Ransomware Cryptowall*.



Fonte: BANKVAULT (2017)

A Figura 3 apresenta um e-mail falso de *Phising scam*, onde o Racker tenta persuadir a sua vítima por meio de Engenharia social.

Figura 3 - Phishing scam (e-mail falso) em nome dos correios.



Fonte: INFOWESTER (2016)

2.2 Origem dos *Ransomwares*

Em meados de 1989 surgia uma das maiores ameaças da atualidade: o *Ransomware* cujo nome de AIDS, desenvolvido por Joseph Popp que substituía o arquivo AUTOEXEC.BAT nos sistemas infectados e permitia reinicializar o sistema 90 vezes até ocultar todos os diretórios e alegar que criptografaria os arquivos (AFRIKATEC, 2017).

Ainda em 89, observou-se outro tipo de *Malware*, o *Cyborg* que era distribuído por disquetes e criptografava a unidade de arquivos do sistema AUTOEXEC.BAT e ocultava pastas e criptografava os nomes de arquivos da unidade C. Era exigido um pagamento de U$189 em dinheiro em nome da *PC Cyborg Corporation* para a liberação dos dados (AFRIKA TEC, 2017).

Após 15 anos da existência dos *Ransomware* tornou-se proeminente, em 2005, o surgimento dos *trojans* como o *Gpcode, Troj.Ransom.A, Archiveus, Krotten, Cryzip e MayArchive* que começaram a usar o esquema de criptografia RSA mais avançados com chaves de tamanho cada vez maiores. O *Gpcode. AG* foi revelado em 2006 e foi criptografado com chave RSA de 660 bits (LISKA; GALLO, 2017).

Em 2017, uma das piores ameaças a âmbito mundial foi o "*WannaCry*", causando um estrago alarmante em mais de 74 países, onde os primeiros efeitos foram detectados no

Sistema Público de Saúde do Reino Unido que começaram a registrar falhas em seus arquivos e postos de atendimentos em regiões como Inglaterra, Escócia foram saindo do ar. Médicos acessavam seus prontuários e recebiam um alerta dizendo que seus dados foram criptografados e a mensagem exigia um pagamento para desbloqueio de suas informações (GLOBO, 2017).

2.3 Tipos de *Ransomware*s

Segundo informações dos sites Raidbr e Oficina da Net, os principais tipos de *Ransomware*s identificados são:

• ***Adware:*** Normalmente é um aplicativo que exibe ou baixa, sem autorização, anúncios na tela do computador. Em muitos casos, esse *Malware* vem incorporado a softwares e serviços, não causam danos, na maioria das vezes eram usados anteriormente, por exemplo, no mensageiro MSN Messenger (OFICINA DA NET, 2013).

• ***Backdoor:*** Seria uma porta de entrada para *Malware*s. “Porta dos fundos” são falhas no sistema operacional ou em aplicativos que permitem que crackers tenham controle remoto sobre o equipamento infectado (OFICINA DA NET, 2013).

• ***Bots e Botnets:*** são softwares capazes de se propagar utilizando brechas nos softwares em um computador. Permitem comunicação com o invasor, e, portanto, são controlados remotamente (OFICINA DA NET, 2013).

• ***Trojan Horse*:** são programas projetados para serem recebidos como “presentes”, um e-mail contendo a ameaça, por exemplo. Porém, além de executar as funções para as quais foram programados, eles executam outras sem o conhecimento do usuário (OFICINA DA NET, 2013).

• ***Keyloggers*:** como o próprio nome diz ele captura e armazena as teclas digitadas no computador infectado. Assim, as informações de um e-mail ou senhas bancárias, por exemplo, podem ser capturados (OFICINA DA NET, 2013).

• ***Spywares*:** Software capaz de monitorar as atividades de um dado sistema e envia as informações para o cyber-criminoso (OFICINA DA NET, 2013).

• ***Worms:*** *Malware* capaz de se propagar automaticamente por meio de redes, enviando cópias de si para outros computadores, a partir de falhas em softwares instalados incorretamente (OFICINA DA NET, 2013).

• ***Rootkits*:** conjunto de programas que permitem que um invasor se esconda e tenha acesso contínuo ao computador infectado. Esses programas, de modo geral, dificultam a localização do invasor, pois os escondem em usuários e *backdoors* (OFICINA DA NET, 2013).

• ***Crypto Wal:*** Quando o computador é infectado pelo vírus *CryptoWall,* diversas extensões são criptografadas e as mais comuns são: (xls, wpd, wb2, txt, tex, swf, SQL, tf, RAW, ppt, png, pem, pdf, pdb, PAS, odt, obj, msg, mpg, mp3, lua, key, jpg, hpp, gif, eps, DTD, doc, der, CRT, cpp, cer, bmp, bay, avi, Ava, ass, asp, js, py, PL, dB) (RAIDBR, 2017).

• ***Torrent Locker:*** Os trojans se espalhavam através de e-mails fraudulentos com mensagens sobre falhas de encomenda. Utiliza uma mesma *keystream* para cada computador infectado, tornando a criptografia difícil de ser quebrada (RAIDBR, 2017).

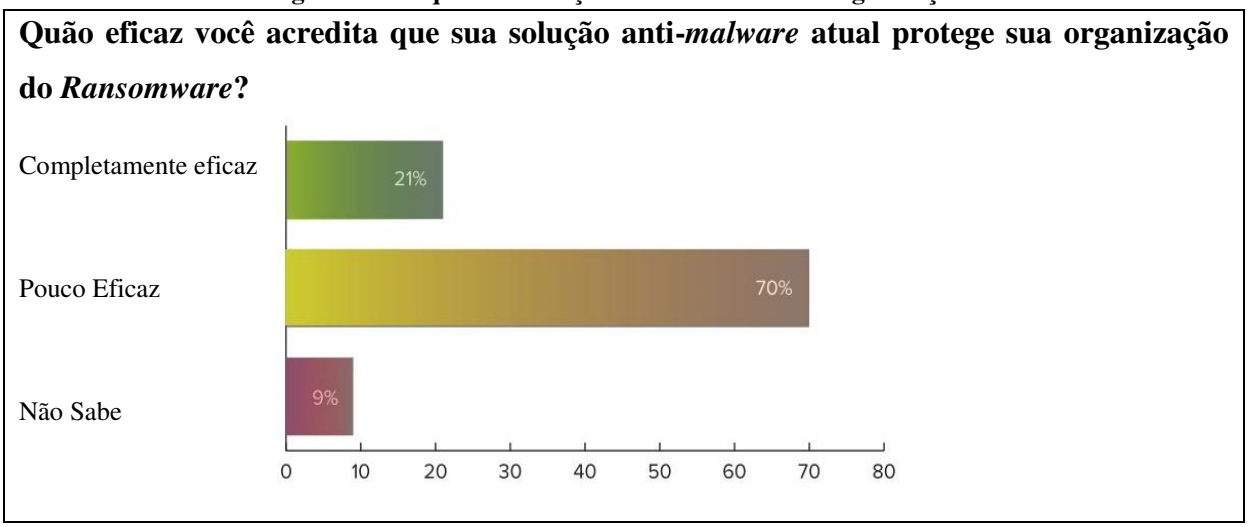
• ***TeslaCrypt*:** Tipo de *Ransomware* que criptografa os arquivos com RSA-2048 para criptografia impossível de ser quebrada (RAIDBR, 2017).

3 CENARIO ATUAL DO *RANSOMWARE*

Segundo o site Varonis, as empresas permanecem vulneráveis quando um ataque de *Ransomware* consegue ultrapassar a primeira camada de proteção oferecida pelas soluções de segurança do *endpoint* e chegar aos grandes repositórios de dados, explorando as mesmas vulnerabilidades das quais as ameaças internas tiram proveito – excesso de permissões de acesso e ausência de monitoramento.

De acordo com o site, uma das questões fechadas sobre soluções de anti-*malware* nas organizações nas áreas de tecnologia, hospitalares e indústrias de grande porte, diz respeito à eficácia em que a solução anti-*malware* protege as organizações (Figura 5). O estudo foi realizado com 230 pessoas de várias organizações como Estados Unidos, Ásia, Canadá e Reino Unido, dentre as quais 70% eram de empresas entre 1000 a 2000 colaboradores (VARONIS, 2017).

Figura 5 - Pesquisa de soluções anti-*malware* nas organizações.



Fonte: VARONIS (2017)

A ameaça do *Ransomware* deve continuar em 2018. Estimativas indicam que a porcentagem de empresas que acreditam que serão alvos de ataques de *Ransomware* vai crescer em torno de 21% em relação à quantidade de pessoas que acreditavam que seriam atacadas no último ano, aponta o site VARONIS.

3.1 Formas de Infecção do *Ransomware*

As principais formas de infecção do *Ransomware* identificados pelo site AFRIKATEC (2017) e CIO (2017) são:

• **E-mail:** a forma mais fácil de propagar um *Ransomware* é por e-mail de *spam*, enviado para o usuário geralmente contendo um anexo malicioso ou um link que direciona para uma página falsa. Para induzir a sua vítima, os cibercriminosos incorporam no *spam* mensagens alarmantes que despertam o seu interesse por meio de Engenharia social com conteúdos como: notificação de entrega de correio; faturas para pagamentos que estão prestes a vencer ou vencidas; notificação de infração de trânsito; declarações fiscais e promessas de prêmios milionários (AFRIKATEC, 2017; CIO 2017).

• ***Malvertising*:** os *malvertising* são anúncios maliciosos que ficam em sites expostos, em sites legítimos e populares, mas sem que seus administradores saibam que eles estão sendo exibidos (AFRIKATEC, 2017).

• **Downloads e *Botnets:*** *Botnet* é um nome dado a um conjunto de computadores infectados por um *Malware* que permite que cibercriminosos os controlem de maneira remota computadores individuais que fazem parte de uma *botnet* são chamados de *"bots"*, ou de 'zumbis'. Os criminosos podem usar o *bot* de uma vítima para propagar mais rapidamente ameaças de *Ransomware* por meio de e-mail de *spam*, por exemplo (AFRIKATEC, 2017).

• **Sistema de Distribuição de Tráfego:** TDS (*Traffic Distribution System*) é um tipo de página que direciona o tráfego de um site para um conteúdo malicioso. Quando o usuário abre um link em um site, ele é redirecionado para um fornecedor TDS. Este vende o clique para empresas interessadas em divulgar seus produtos ou serviços, ou para cibercriminosos que querem distribuir ameaças de *Ransomware* (AFRIKATEC, 2017; CIO 2017).

• **Vulnerabilidade do Sistema Operacional:** o *Malware,* nesse caso, aproveita-se de uma vulnerabilidade do Windows que permite executar código remotamente por meio do SBM, protocolo de compartilhamento de arquivos. Quando uma máquina é afetada, o *Ransomware* pode se espalhar rapidamente para todos os computadores vulneráveis da rede (TECNOBLOG, 2017).

3.2 Propagação do *Ransomware*

O *Ransomware* usa criptografia para extorquir as vítimas, os ataques podem causar a perda de acesso a informações, perda de confidencialidade e vazamento de informações. É importante entender como funciona a anatomia de um ataque de *Ransomware* para se prevenir com mais eficácia. A seguir, encontram-se seis etapas que um ataque percorre para atingir seus objetivos (CIO, 2016).

1 – Distribuição: os cibercriminosos utilizam métodos de distribuição bastante conhecidos, geralmente o *Malware* é espalhado por meio de esquemas de *phishing* envolvendo links fraudulentos como anexos de e-mails ou downloads de arquivos (CIO, 2016).

2 – Infecção: o binário chega ao computador do usuário e são iniciados alguns processos necessários para completar suas atividades maliciosas. Esta etapa pode incluir técnicas mais novas e comportamentos sofisticados como, por exemplo, o *Malware CryptoWall* 3 que funciona como um identificador de computador exclusivo, certifica um "reboot de sobrevivência" e instala um programa que é executado ao ligar a máquina; desativa

cópias e sistemas de reparação e recuperação de erro do Windows, desativa programas de defesa; injeta-se no explorer.exe e svchost.exe e recupera o endereço IP externo (CIO, 2016).

3 – Comunicação: o *Malware* começa a se comunicar com os servidores de chave de criptografia para obter a chave pública necessária para criptografar os dados. O CryptoWall 3, por exemplo, se conecta a um site WordPress comprometido e relata seu status. Todo o tráfego de servidor de controle é criptografado usando o algoritmo de criptografia RC4 (CIO, 2016).

4 – Pesquisa dos arquivos: o *Ransomware* procura por arquivos no sistema de uma forma sistemática. Ele normalmente busca por arquivos que sejam importantes para o usuário e não podem ser facilmente replicados, como arquivos com extensões de jpg, docx, xlsx, pptx, pdf etc (CIO, 2016).

5 – Criptografia: o processo é realizado movendo e renomeando arquivos específicos, as informações são "embaralhadas" e não podem mais ser acessadas sem serem descriptografadas (CIO, 2016).

6 – Resgate das informações: um aviso aparece na tela do computador do usuário infectado exigindo pagamento em *bitcoins* para então enviar á vitima a chave que poderá desbloquear a máquina (CIO, 2016).

3.3 Prevenções do *Ransomware*

Segundo o próprio autor do artigo, que atua na área de TI em uma empresa do setor da saúde, algumas medidas de prevenções essenciais devem ser tomadas para garantir que as corporações reduzem o risco de infecção, que são:

Conscientizar os usuários por meio de programas de segurança realizado pelas empresas que normalmente são alocados em um orçamento pequeno em comparação com todos os outros gastos da Tecnologia da Informação (TI), obtendo um melhor retorno sobre o investimento e evitando a infecção da rede.

Fazer Backup periodicamente dos dados. Caso a empresa for atacada por um *Ransomware*, pode ser que alguns projetos recém-iniciados se percam, mas caso a empresa tiver um backup, poderá restaurar o sistema para um backup recente e os projetos mais importantes não serão perdidos, tornando o ataque apenas um incomodo e não um incidente grave. Ressalta-se que os backups deverão estar armazenados e isolados da rede, pois em caso de ataque, os arquivos estarão a salvo.

Garantir que todas as máquinas estejam com software de antivírus instalados e atualizados com as últimas vacinas de segurança como Symantec, Kaspersky e outros softwares do mercado.

Bloquear anexos de arquivos executáveis no Filtro de E-mail.

Bloquear downloads de arquivos executáveis no Filtro Web e certificar-se que o protocolo HTTPs está sendo inspecionado.

Garantir que os filtros web e E-mail estejam com as vacinas atualizadas.

Bloquear as URL´s e endereços IP no filtro Web que estão relacionados aos *Ransomware*s.

Garantir que as regras de firewall não permitam o redirecionamento de tráfego na porta 445 para redes protegidas.

Aplicar os *patches* de atualizações relacionados à vulnerabilidade.

Bloquear gravação de arquivos de extensão *.Wcry nas estações e servidores.

Realizar o monitoramento da rede buscando atividades suspeitas.

Em caso de suspeita de algum equipamento contaminado, recomenda-se isolar o equipamento da rede imediatamente.

Bloquear os IP´s no firewall com redirecionamento para os sites maliciosos.

Desabilitar portas RDP´s ou *Remote Desktop Protocol,* uma funcionalidade Windows que permita o acesso remoto. Caso não seja necessário o acesso remoto, é de grande importância a desativação dessas portas na rede, protegendo as máquinas do *filecoder* e outros exploits conhecidos de RDP.

Aplicar atualizações mais recentes *(patches e updates)* nos *softwares,* reduzindo, consideravelmente, a probabilidade de ser atacado por um *Ransomware* com os *softwares* atualizados.

Usar métodos de IDS ou Sistema de Detecção de Intrusão, um mecanismo capaz de identificar ou detectar a presença de atividades intrusivas incomuns ou anomalias, pois verificam os processos utilizados na descoberta de utilizações não autorizadas de dispositivos de rede ou de computadores.

Utilizar a Restauração do Sistema em caso de infecção, caso a função estiver habilitada no *Windows,* pode ser possível retornar o sistema para um estágio pré-*ransomware*. Mas, atualmente, já existem versões de *Malware*s de *Ransomware* que possuem a habilidade de apagar os arquivos necessários para que o sistema seja restaurado.

Por último, caso a empresa contraia o *Malware* ou *Ransomware*, não é aconselhável o pagamento do resgate, pois isso motiva cada vez mais os cibercriminosos a investirem cada vez mais em novas tecnologias para aperfeiçoar o uso do *Ransomware*. Ressalta-se que não poderá ser garantido que os arquivos atingidos sejam recuperados após o pagamento.

4 CONCLUSÃO

Pode-se concluir que o *Ransomware* evoluiu significativamente ao longo dos anos desde em que surgiu em 1989 como o *'PC Cyborg'*. Atualmente, há uma ampla gama de diferentes tipos de *Ransomware*, aproveitando diferentes técnicas computacionais.

O foco dos cibercriminosos é no setor da saúde (hospitais), pois os mesmos lidam com vidas humanas, logo, a pressão para que o pagamento seja efetuado é muito grande. Se os sistemas param, os hospitais têm dificuldades para acessar exames, obter dados de doenças, comunicar-se com outros centros médicos, fazer reposição de remédios e assim por diante. Nessas circunstâncias, os pacientes não recebem tratamento adequado.

Além disso, os sistemas dos hospitais guardam informações confidenciais dos pacientes: prontuários e históricos médicos são documentos particulares. Se expostos publicamente ou perdidos, os hospitais podem sofrer processos judiciais que resultam em indenizações e multas pesadas. Mas, se a ação envolve sequestro de dados e ou atividades bem-sucedidas de um crypto-*ransomware*, o caso precisara ser analisado com cuidado. Por tal motivo, a preocupação de algumas medidas de prevenções essenciais deve ser tomada para garantir que as corporações reduzem o risco de infecção contra o *Ransomware*.

Sem uma solução em curto prazo quanto a extinção do *Ransomware*, a tendência, infelizmente, é continuar a presenciar esses tipos de ataques. A melhor saída contra os ataques é a prevenção e o bloqueio dos ativos da rede, algo importante que pode ser feito para proteger o que mais importa nas organizações, seus dados.

REFERÊNCIAS

AFRIKA TEK. Série – **A Evolução do *Ransomware* – Parte 1,2,3 e 4 – Como a ameaça se propaga**, 2017. Disponível em: < http://www.afrikatec.com.br/serie-evolucao-do-*Ransomware*-parte-4-como-ameaca-se-propaga/>. Acesso em: 03 set. 2017.

CIO. **Você sabe como funciona um ataque de *Ransomware*?**. 2016. Disponível em: < http://cio.com.br/tecnologia/2016/08/16/voce-sabe-como-funciona-um-ataque-de-*Ransomware*/>. Acesso em: 03 set. 2017.

____. **Seis passos para a empresa evitar ser vítima do Petya**. 2017 Disponível em: < http://cio.com.br/tecnologia/2017/06/27/seis-passos-para-a-empresas-evitar-ser-vitima-do-petya/>. Acesso em: 04 set. 2017.

CISCO. **Teslacrypt.** 2015. Disponível em: < https://blogs.cisco.com/security/talos/teslacrypt>. Acesso em: 25 mai. 2017.

FONTES, E. **Segurança da Informação**. São Paulo: Saraiva, 2012.

GLOBO. **Sequestro digital do WannaCry não rouba dados; entenda o *Ransomware***. Disponível em:<http://g1.globo.com/tecnologia/blog/seguranca-digital/post/sequestro-digital-do-wannacry-nao-rouba-dados-entenda-o-*Ransomware*.html>. Acesso em: 01 set. 2017.

INFOWESTER. **O que é *Ransomware***, 2016. Disponível em: < https://www.infowester.com/*Ransomware*.php>. Acesso em: 02 set.2017.

LISKA, A. GALLO, T. **Ransonware.** São Paulo: Novatec, 2017.

MICROSOFT. **O que é *Ransomware***. 2016. Disponível em: < https://www.microsoft.com/pt-br/security/resources/*Ransomware*-whatis.aspx>. Acesso em: 25 mai. 2017.

RAIDBR**. 6 Tipos de *Ransomware***. 2016. Disponível em: <http://www.raidbr.com.br/blog/6-tipos-de-*Ransomware*_2.html>. Acesso em: 10 set. 2017.

OFICINA DA NET. ***Malware* o que é, e quais os tipos existentes**. 2013. Disponível em: <https://www.oficinadanet.com.br/post/8550-*Malware*-o-que-e-e-quais-os-tipos-existentes>. Acesso em: 02 set. 2017.

TECNOBLOG. **Ataque com *Ransomware* está sequestrando arquivos de empresas ao redor do mundo**. 2017. Disponível em: < https://tecnoblog.net/214579/telefonica-espanha-*Ransomware*/>. Acesso em: 10 set. 2017.

VARONIS. ***Ransomware* survey**. 2017. Disponível em: < https://www.varonis.com/learn/*Ransomware*-survey/>. Acesso em: 03 set. 2017.