**Ransomware**

**Adeilson Nazareno Araújo Pinheiro**

<adgospel@gmail.com>

**Claudinei Di Nuno, Msc**

<professorclaudinei@uol.com.br>

Curso de Pós-Graduação *Lato Sensu* em Gestão Estratégica em Tecnologia da Informação

# Resumo

O trabalho possui como tema: segurança da informação. E como objeto de estudo o *Malware* conhecido como *Ransomware*. Entre os objetivos estão mostrar a importância de saber o que é, como age, como evitar e como combater um ataque dessa praga virtual. Para isso, foram feitas análises de algumas literaturas que tratam do assunto. Procurando entender a origem e evolução desse *software* pernicioso e, dentro desse contexto, apontar processos e ferramentas que sejam consideradamente eficazes, principalmente, na prevenção dos ataques. E, como resultado dessa pesquisa, alguns recursos foram identificados e serão recomendados para uso, tais como: procedimentos e um software de antivírus muito conhecido no mercado. É crucial está na vanguarda dessa realidade, pois o mundo digital constitui cenário atrativo aos criminosos: anonimato, dificuldade de rastreio, mercado de extorsão lucrativo, dentre outros. Por isso, está ciente das ameaças de sequestro e/ou destruição daquilo que é um dos patrimônios mais preciosos que se tem, a informação; e saber como se defender, é mandatório.

**Palavras-chave:** *Cibercrime*. *Ransomware*. Criptografia. Budapeste.

# Introdução

O texto está disposto em duas seções. A primeira contém um panorama geral das ameaças mais comuns e de como evoluíram, porém, não deixaram de explorar usuários incautos.

Aborda, ainda que em linhas gerais, sobre as interações dos mais diversos dispositivos com a *internet*, o que eleva e potencializa o risco de investidas criminosas para interceptar as comunicações na tentativa de usurpar os dados trafegados na rede. É exemplificado com caso reais que trouxeram significativos prejuízos às vítimas.

Defende o conhecimento como arma de combate, somado ao apoio tecnológico que houver disponibilidade de colocar em ação.

Discorre ainda sobre as fragilidades normativas da legislação brasileira para tipificar crimes virtuais, o que dificulta identificar e responsabilizar os infratores. Nesse contexto, é apresentada a Convenção de Budapeste como uma proposta de avanço e modernização.

Na segunda seção, são tratados alguns mecanismos de defesa. Começando por entender a estrutura e componentes típicos de um ataque. Como proteger estações de trabalho e servidores, listando procedimentos que podem ser usados.

Reforça a relevância de investir na formação e capacitação dos profissionais, mostrando como podem ser decisivos no combate a proliferação dos *Ransomwares*.

Recomenda o uso de *software* antivírus. Indicando o ESET, que tem se mostrado eficaz é e um dos mais conceituados no mercado.

Ataques *Ransomwares* são nocivos e, por tanto, causam grandes prejuízos. Por exemplo, comprometendo um servidor de bancos de dados ao criptografar os arquivos necessários para acesso das aplicações. Se uma rotina de *backup* não estiver implantada a perda das informações poderá ser total, disso derivando uma série de complicações, como paralisar todo o processo administrativo de uma empresa.

São inúmeros os males que podem causar, por isso, a importância de fomentar os conceitos de segurança da informação, facilitando o saber para que mais pessoas e instituições saibam como se precaver e agir diante desse cenário.

E nesse aspecto é notória a relevância de estudos como o presente, pois, alertam, conscientizam e apontam soluções. Possibilitando, assim, um posicionamento não apenas reativo, mas, preferencialmente, proativo. O que deverá diminuir significativamente o sucesso dos criminosos.

Quatro pilares de sustentação: conhecimento, infraestrutura, pessoas e tecnologia. E investimento é o termo que os traduz. Investir em cada um trará mais confiança de que as informações estarão seguras. Conhecimento sobre prevenção e combate aos *Ransomwares*, é a contribuição a que se propõe o artigo.

1. **Fundamentação Teórica**

*Malwares*. São códigos maliciosos que causam danos e prejuízos aos computadores hospedeiros (CERT.BR, 2018).

Estar alerta aos perigos que trafegam na *internet* é essencial, pois existe uma verdadeira guerra cibernética (CLARKE; KNAKE, 2015).

**2.1 As ameaças mais comuns**

Existem variadas técnicas e ferramentas usadas para fins perniciosos na *internet*. Entre elas: Engenharia Social, *Worms* (vermes), *Trojan Horse* (cavalo de Tróia), *Phishing Scam* (pescaria) e *Ransomware*.

Engenharia Social. Basicamente é o uso de elementos totais ou parcialmente verdadeiros para assegurar credibilidade ao que está sendo apresentado, visando alcançar a confiança da vítima para que tome ações a favor de quem está orquestrando o golpe.

*Worms*. Se caracterizam pela independência do agir humano e de outros programas para se proliferarem.

*Trojan Horse*. É um programa malicioso que se aglutina aos programas considerados válidos para se dissimular e invadir sistemas sem causar suspeitas.

*Phishing scam*. Faz uso de estratégias e campanhas, geralmente por e-mail, para atrair e enganar os indoutos.

*Ransomware*. De acordo com Liska e Gallo (2017), é um *Malware* que atua nas fases: implantação, instalação, comando e controle, destruição e extorsão. Bloqueia e/ou restringe o acesso aos arquivos que foram criptografados. Exige um resgate, que deverá ser pago em frações de *bitcoins*, que é uma moeda digital que não possui um governo emissor e o seu valor é variável (ULRICH, 2014).

**2.2 Evoluídos e complexos**

Crimes virtuais são aqueles em que o computador é usado para praticar o ato ilícito. Exemplos: violação e interceptação de e-mails, furto de identidade, estelionato virtual, dentro outros. São ilegalidades praticadas nessa revolução digital hodierna (SYDOW, 2014).

No caso dos *Ransomwares*, existe uma preocupação crescente: programas autoprogramados (CISCO, 2018), como o *WannaCry,* que casou enormes prejuízos em 2017 (BTCSOUL, 2017).

Estão atacando as cadeias de fornecimento, na tentativa de driblar os *softwares* de proteção; acoplando códigos maliciosos em programas considerados legítimos (CISCO, 2018), como um cavalo de Tróia que foi baixado junto com o programa *CCleaner* (G1, 2017).

Outro destaque é o aumento do tráfego criptografado na *web*, que vem sendo usado para fins escusos e ocultar atividades suspeitas. De acordo com relatório da CISCO (2018) a comunicação criptografada na rede usada por *Malwares* triplicou em 12 meses. O relatório ainda pontua o interesse em usar campanhas de e-mail como porta de entrada para novas infecções. Principalmente através de anexos *.doc* e *.pdf* (LISKA; GALLO, 2017).

**2.3 *IoT***

O termo *IoT* (*Internet* of Things, ou *Internet* das Coisas) se caracteriza por conceituar a realidade contemporânea, onde a quantidades de dispositivos conectados à nuvem é surreal. E cresce a cada dia, devido a característica das aplicações para *IoT* estarem proporcionando mercados novos e rentáveis (SINCLAIR, 2018).

Nada está seguro. O que estiver conectado na *internet* é um alvo em potencial. Por exemplo, em fevereiro de 2017 foi noticiado um incidente inusitado na Áustria, quando um grupo de *hacker*s invadiu o sistema de chaves eletrônicas de um hotel, impedindo a entrada e saídas dos hóspedes nos quartos (EXAME, 2017).

**2.4 Conhecimentos como arma de combate**

Apesar da previsão do uso crescente de *softwares* autoprogramados para invadir sistemas (CISCO, 2018), a exploração da ignorância digital continua lucrativa. Por isso, iniciativas como a do CERT.BR (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil) são preciosas, disponibilizando uma cartilha contendo conceitos e orientações para ciência dos perigos que circulam o mundo conectado.

Quanto maior o número de esclarecidos, menos progressos haverá por parte dos malfeitores, pois o conhecimento adequado monta barreiras difíceis de transpor. Seguir as diretrizes de segurança deve se tornar um hábito. E pequenas mudanças, mas importantes no comportamento, irão encadear muitas outras que no decorrer do tempo trarão benefícios notórios. É o conceito de hábitos angulares apresentado por Charles Duhigg (2012). Exemplo: se houver cotidianamente um rigor na tratativa de abrir mensagens de e-mails de origem e conteúdos duvidosos, outras ações dentro desse contexto irão surgir naturalmente, como sempre usar um programa de antivírus para varrer um dispositivo removível antes de abri-lo.

**2.5 Apoios tecnológicos**

É imprescindível lutar em todas as frentes para uma resposta rápida e eficiente a fim de paralisar e erradicar uma ofensiva (ESET, 2018). O papel das pessoas nesse embate é fundamental, obviamente, mas não suficiente. É necessário contar com ajuda da tecnologia para automatizar defesas e reações ao se detectar tentativas de intrusões. Tratar o problema em camadas tem se mostrado o caminho para ferramentas que se destinam a atuar nesse mercado de segurança da informação. Em momento oportuno será apresentado o *ESET* como um dos programas que trabalham em camadas e como tem obtido bons resultados.

**2.6 Convenção de Budapeste**

O combate ao crime organizado no mundo digital não o poderá ser apenas através de *softwares* de proteção, independentemente do quão eficazes sejam. É necessário, sim, atacar pelas vias legais, punindo com rigor os culpados identificados. Daí a importância de um código normativo atualizado e adequado.

Se tratando de legislação brasileira, o combate aos crimes virtuais não está tipificado tal qual deveria (MASSENO E WENDT, 2017). Porém, desde 2001 há um esforço internacional para fazer frente ao cibercrime.

A Convenção de Budapeste surge, por conseguinte, como um instrumento incentivador da adoção de normas mais apropriadas e específicas para as infrações digitais, além de endossar a criação ou adequação de outras no âmbito local, para que se atenda as especificidades de cada nação membro (MPF, 2018).

Exemplos de como o combate aos crimes cibernéticos no Brasil acontece com precariedade são as generalizações feitas no uso do código penal.

Com relação aos *Ransomwares*, quando ocorre a obtenção ilegal de acesso ao sistema, poderá ser aplicado o exposto na Lei 12.737/2012, conhecida como Lei Carolina Dieckmann, nos seus artigos 154-A e 154-B, que foram acrescidos ao código penal. A incoerência é que neles o ato ilícito é tipificado como delito e não como crime, havendo diferenças significativas entre ambos, onde delito é considerado transgressão legal de natureza leve, já o crime é a transgressão legal de natureza grave.

Para tratar a inacessibilidade dos dados, poderá ser usado o artigo 265, que discorre sobre os atentados contra a segurança pública, se o ataque for a um órgão público, como o INSS, por exemplo.

O pedido de resgate poderá ser enquadrado como extorsão. Nesse caso, se poderá fazer uso do artigo 158, em seus parágrafos § 1º, § 2º e § 3º.

É plausível o esforço para aplicar a persecução penal, minimizando o sentimento de impunidade (WENDT; JORGE, 2013). Porém, tipificar e tratar mais adequadamente traria avanços enormes à nação. Por isso, ser membro da Convenção de Budapeste seria salutar, além de colaborar e receber ajuda dos países membros.

1. **Fatores de sucesso no combate aos *Ransomwares***

Serão analisadas algumas das técnicas mais eficientes para evitar ou paralisar um ataque em andamento. Ressalvando-se que a atenção maior deve ser a prevenção, pois não há garantias de que encerrar a atividade do *software* malicioso em um sistema já comprometido, a depender da fase de intervenção, protegerá a totalidade dos arquivos.

**3.1 Estrutura de um ataque**

Um ataque *Ransomware* possui, obrigatoriamente, os itens: implantação, instalação, comando e controle, destruição e extorsão.

Implantação. Fase em que os componentes básicos para infectar, criptografar e bloquear o sistema hospedeiro são instalados.

Instalação. O código malicioso inicia o processo para assumir comando e controle do sistema infectado.

Comando e controle. Estabelecimento de um canal de comunicação entre hospedeiro e invasor; sendo pré-requisito para a destruição dos dados.

Destruição. Ocorre a criptografia e/ou exclusão de arquivos, culminando com bloqueio do acesso.

Destaca-se a etapa de extorsão. Ocasião em que o usuário é avisado de que o sistema foi sequestrado é que será restabelecido mediante o pagamento de um resgate, geralmente em frações de *bitcoins*. Entretanto, não há qualquer garantia real de que os dados serão recuperados.

**3.2 Cuidados essenciais com as estações de trabalho e servidores**

Se não existir *backup* de arquivos, ou vacinas no mercado, um ataque bem sucedido é devastador. Por isso, reduzir as vulnerabilidades é primordial. Nesse intuito, serão apresentadas a seguir algumas ações que auxiliarão em um bloqueio com maior possibilidade de êxito.

Macros do pacote *Office* da Microsoft são alvos preferenciais, pois interagem diretamente com o sistema operacional. Desabilitá-las é altamente recomendável.

Evitar baixar e/ou abrir documentos de origem duvidosa, geralmente em formato PDF. Se houver dúvida da procedência, descartar o arquivo.

Bloquear extensões frequentemente usadas em ofensivas, no gateway do servidor SMTP. Esse procedimento dificulta que mensagens não validadas cheguem na caixa de entrada dos correios eletrônicos dos usuários.

Evitar compartilhamento de drives entre computadores em rede. A propagação de um *Ransomware* é facilitada se houver drives compartilhados e com permissões totais de acesso nas pastas e arquivos. Por isso, restringir, ou mesmo não usar esse meio de comunicação interna, trará mais uma camada de segurança à organização.

O uso mais frequente de *HMTL5* por muitas plataformas *web* deve ser um incentivo para eliminar *plug-ins* *Adobe* *Flash* nos navegadores, pois o *Flash* é mais um dos recursos preferidos para orquestrar ações de sequestro de dados.

Limitar os diretórios onde os arquivos possam ser executados. Recomenda-se proibir execução nos seguintes, levando-se em conta ser o sistema operacional o *Windows*: *\Download*, *\Temp*, *%AppData%\*.

Impedir execução automática de mídias removíveis, usando algum programa de varredura a procura de códigos maliciosos.

Impedir a desativação e/ou exclusão dos pontos de restauração do sistema com o uso de ferramentas, tais como: *SentinelOne* ou *Carbon Black*. Esse cuidado merece muita atenção, pois, geralmente, quando da ocorrência de problemas graves de desempenho, restaurar para um ponto estável normaliza a situação. E o mesmo é válido para recuperação de desastres causados por pragas virtuais. Por isso, essa proteção dos pontos de restauração é crucial.

Bloquear o acesso ao *host C&C* (*command-and-control*, ou comando e controle). Ferramentas como *Carbon Black*, *Cylance*, *FireEye* podem ajudar nessa atividade.

Muitos *Ransomwares* usam a API (*Application Programming Interface*, ou Interface de Programação de Aplicativos) *Crypto* do *Windows* (*crypt32.dll*) para criptografar os arquivos, por isso, é recomendado encerrar qualquer processo não confiável que chame a API *Crypto* um determinado número de vezes, caracterizando uma atitude suspeita.

Manter um inventário de *hardwares* e *softwares* usados e fazer um acompanhamento se as versões utilizadas contêm vulnerabilidades; e, sendo afirmativo, verificar se as devidas correções já estão disponíveis. Buscar apoio tecnológico para automatizar e detalhar essas informações é aconselhável. Existem muitos *softwares* com esse propósito, a saber: *Corvil*, *TripWire*, *End-point management* da *Symantec*. Em suma, saber se o ecossistema computacional está atualizado é crítico.

**3.2 Investindo nos colaboradores**

*Ransomwares* mais modernos não necessitam de interação humana no processo de infecção: variantes mais recentes do *WannaCry*, por exemplo. Porém, outros ainda dependem dessa ação. Logo, o usuário continua sendo peça chave na barreira para evitar a proliferação desse mal.

Manter um cronograma de treinamento e conscientização dos usuários poderá reduzir drasticamente ocorrências de sucesso dos crimes virtuais. Sugestão: muitas empresas fazem a SIPAT (Semana Interna de Prevenção a Acidentes de Trabalho). Poderia, nessa linha de raciocínio, ser montado um programa com o nome SIPATI (Semana Interna de Prevenção a Acidentes em Tecnologia da Informação), onde várias palestras, simulações e atividades poderiam ser elaboradas com este fim: manter os colaboradores informados dos incidentes que estão ocorrendo e como cada um poderá contribuir para manter a empresa segura.

**3.3 Usando inteligência e tecnologia**

Para estar à frente de possíveis investidas é necessário prever e analisar determinados comportamentos, bem como usar das informações que são compartilhadas por diversos instrumentos de combate as infrações tecnológicas.

No contexto das redes de computadores, manter uma lista atualizada dos endereços mais comumente associados aos canais de comando e controle dos *Ransomwares* é recomendado, pois esses dados podem ser usados para montar uma camada de proteção, bloqueando todos e quaisquer acessos oriundos dessa parametrização.

Monitorar a execução de processos anômalos. Ou seja, se um determinado processo estiver sendo usado para copiar muitos arquivos fora de um horário estipulado para rodar uma rotina de *backup*, ou um determinado usuário estiver requisitando vários endereços *web* estranhos em curto espaço de tempo, são indicativos de anormalidades e devem ser tratadas rapidamente.

É preciso buscar apoio tecnológico que automatize esses monitoramentos e existem bons *softwares* que poderão auxiliar nisso, oferecendo camadas de controle para detectar procedimentos indevidos em várias etapas.

Em tópico posterior, se dará a análise de uma ferramenta que tem apresentado bons resultados na identificação e tratamento de comportamentos anômalos de usuários e processos, bem como de outras caraterísticas.

**3.4 Agindo rapidamente**

Do tripé apresentado (proteção das estações de trabalho e servidores, proteção da força de trabalho e uso das fontes de inteligência), notório se faz pontuar a sinergia que deverá existir entre ferramentas, processos e pessoas. Ou seja, na ocorrência de um incidente típico, todas as forças precisam ser acionadas e trabalharem colaborativamente para conter a ameaça. Por tanto, controle e integração são conceitos chave que deverão ser constantemente observados. Vale ressaltar o papel sempre alerta e focado que os profissionais de Tecnologia da Informação devem exercer, como administradores e multiplicadores dos conhecimentos básicos em segurança da informação.

**3.5 *ESET***

Conforme dito anteriormente, para uma maior eficácia de proteção contra os *Malwares* de modo geral, contar com o apoio de um bom ferramental de *softwares* é obrigatório, pois os ataques estão cada vez mais sofisticados e a tecnologia de combate precisa acompanhar e, mais idealmente, estar à frente dos avanços criminosos. Ou seja, antecipar as investidas e trabalhar em camadas se, por ventura, os algoritmos de intrusão forem avançando - na tentativa de em cada camada tentar conter e eliminar a invasão. Existem ótimas soluções no mercado e será apresentada uma que vem obtendo excelentes resultados, a saber: *ESET*.

O programa em questão já começa atuando naquela que hodiernamente é a principal maneira de invadir os computadores: campanhas de envio de e-mails nocivos. As mensagens contendo *Malwares* são automaticamente detectadas e tratadas antes mesmo de chegaram a caixa de entrada das vítimas.

Outro exemplo é a detecção das tentativas de explorar o controle remoto sobre as máquinas, através do qual os *hacker*s assumem o domínio do sistema hospedeiro. O *ESET* foi projetado para prevenir essas investidas no ambiente de rede. Somado ao esse esforço, ele possui um eficaz bloqueador de *exploits*, que como visto anteriormente, são necessários para que o processo de instalação de um *Ransomware*, por exemplo, seja concluído com sucesso. Ou seja, o antivírus fica rodando em busca de processos anômalos em seu comportamento, bloqueando a exploração das vulnerabilidades.

Mais um item importante nos recursos de defesa, é o escaneamento avançado de memória que é feito. Essa funcionalidade é importante para descobrir a verdadeira natureza dos processos que estão sendo onerosos em sua execução. Essa análise é vital para identificar os *Cripto-Ransomwares* antes que a criptografias dos arquivos comece. Além de alimentar a base de dados da aplicação a cada nova modalidade de *Malware* encontrada, contribuindo com os algoritmos de aprendizado de máquina da solução.

Como uma medida a mais de redundância e disponibilidade de informações cada vez mais os serviços em nuvem vêm sendo usados e essa interação também é alvo de ação por parte dos *hacker*s. E o *ESET* também possui uma camada para blindar e dá segurança nas operações em nuvem. Os principais recursos da ferramenta serão elencados a seguir.

Scanner UEFI (Unified Extensible Firmware Interface, ou Interface de Firmware Extensível Unificada). Responsável por detectar componentes potencialmente maliciosos analisando as instruções que que são enviadas diretamente ao hardware da máquina.

Detecções de DNA. É fato que existem diversas variantes e famílias de códigos maliciosos, porém, como se comportam, segue um padrão e mudá-lo parece não ser trivial. Por isso, os objetos são cuidadosamente filtrados dentro dessa heurística e os enquadrados são bloqueados.

Aprendizado máquina. É a inteligência artificial da ferramenta. Busca um aprendizado profundo e de curto prazo. O principal objetivo é rotular o mais adequadamente as amostras em: limpa, potencialmente indesejada e mal-intencionada.

Proteção da nuvem. Monitoramento de programas maliciosos através das interações com a nuvem da *ESET*.

Reputação e cache. Verificação em cache usando as listas de permissões, agilizando e maximizando e otimizando o processo de varredura. Essa caraterística também é usada para comunicação da inteligência entre os clientes do *software*.

Detecção comportamental e bloqueio. É o sistema de prevenção de intrusões, propriamente. Trabalha com parametrização dos comportamentos suspeitos. Todos os programas ou processos que estejam nas regras definidas são inabilitados antes que se tornem prejudiciais de fato.

*Sandbox*. É um ambiente de simulação para execução de arquivos suspeitos, ou seja, é um local seguro e usado para identificar o real comportamento dos objetos, reduzindo as falhas de detecção.

Scanner de memória avançada. Qualquer atividade que levante suspeita ao usar a memória de um sistema, principalmente se estiverem usando criptografia, são capturadas assim que decodificam a memória.

Bloqueador de *exploits*. Os *exploits* são programas usados para explorar as vulnerabilidades. Mais uma vez os comportamentos suspeitos são rigorosamente analisados e as ameaças bloqueadas imediatamente.

Escudo *Ransomware*. Camada de proteção e reputação que analisa qualquer programa ou processo que se assemelha ao modo operandi de um *Ransomware*, bloqueando todas as ameaças imediatamente.

Proteção contra ataques de rede. É um reforço ou extensão de um firewall e foca, mormente, nas vulnerabilidades no nível de rede. Essa modalidade ajuda bastante, principalmente quando as aplicações estão desatualizadas.

Proteção de *botnet*. O *ESET* intercepta e trata as comunicações oriundas de uma rede computadores infectados. Mais uma vez, identifica processos problemáticos e faz os devidos bloqueios.

Como se observa, o *software* conta com um grupo ferramental que lida com as ameaças virtuais em vários estágios e cada comportamento anormal é detectado e bloqueado, diminuindo ou até mesmo evitando maiores danos aos usuários.

1. **Conclusões**

Os crimes virtuais estão crescendo e se modernizando, vitimando um número alarmante de pessoas e instituições todos os dias. E dentre as pragas virtuais (*Malwares*) a que vem ganhando notoriedade são os *Ransomwares*. São usados para extorquir as vítimas. Por isso, saber como se defender e reagir é crucial e isso não depende de uma única frente, mas de várias, como: pessoas, tecnologias e legislação. Investir na capacitação dos usuários, manter *softwares* atualizados, cientes de suas origens comprovadamente válidas, e adquirir e manter bons programas de proteção sãos mais do que recomendações, são mandatórias. Além disso, a legislação sobre crimes no mundo digital precisa ser melhor contextualiza e o país se tornar membro da Convenção de Budapeste é um passo importante. Sendo o assunto outra em bom tema para extensão do presente trabalho, bem como explorar mais detidamente as investidas dos *Ransomwares* no ambiente da *IoT*, já que quase tudo hoje vive conectado e por estar em rede, é alvo.

**Referências Bibliográficas**

BTCSOUL. **Wannacry causou mais de US$ 1 bilhão em prejuízos**. 2017. Disponível em: <<https://goo.gl/HfQAFx>>. Acesso em: 29 out. 2018.

CERT.BR. CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Cartilha de Segurança para *Internet***. 2018. Disponível em: <<https://goo.gl/4aRdCN>>. Acesso em: 25 out. 2018.

CISCO. **Relatório Anual de Segurança Cibernética**. 2018. Disponível em: <<https://goo.gl/rE9Dcz>>. Acesso em: 26 out. 2018.

CLARKE, Richard A.; KNAKE, Robert K. **Guerra Cibernética: a próxima ameaça à segurança e o que fazer a respeito**. Rio de Janeiro: Brasport, 2015.

DUHIGG, Charles. **O Poder do Hábito**. Tradução de Rafael Mantovani. Rio de Janeiro: Objetiva, 2012.

ESET. **ESET vs. CRYPTO-RANSOMWARE O quê, como e por quê?** 2018. Disponível em: <<https://goo.gl/Bdf5PB>>. Acesso em: 29 out. 2018.

EXAME. **Hackers trancam quartos de hotel e exigem resgate em *bitcoin***. 2017. Disponível em: <<https://goo.gl/2KMPZr>>. Acesso em: 29 out. 2018.

G1. **CCleaner' infectado é alerta para usuários e empresas de segurança**. 2017. Disponível em: <<https://goo.gl/KX99AC>>. Acesso em: 29 out. 2018.

LISKA, Allan; GALLO, Timothy. **Ransomware: defendendo-se da extorsão digital**. Tradução de Lúcia A. Kinoshita. São Paulo: Novatec, 2017.

MPF. MINISTÉRIO PÚBLICO FEDERAL. **Convenção sobre o Cibercrime**. 2018. Disponível em: <<https://goo.gl/xTtM8i>>. Acesso em: 30 out. 2018.

SINCLAIR, Bruce. **Como usar a *INTERNET* DAS COISAS para alavancar seus negócios**. São Paulo: Autêntica Business, 2018.

SYDOW, Spencer Toth. **Crimes informáticos e Suas Vítimas**. 2 ed. São Paulo: Saraiva, 2015.

ULRICH, Fernando. **Bitcoin. A Moeda na Era Digital**. Mato Grosso do Sul: Mises, 2014.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos – Ameaças e Procedimentos de Investigação**. 2 ed. São Paulo: Brasport, 2013.