**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 os *Ransomwares*. Pretende-se mostrar o que são, como agem e como evita-los. Nesse intuito, pesquisou-se literaturas que discorrem sobre a matéria. Procurando entender a origem e evolução desse *software* pernicioso e, nesse embasamento, apontar processos e ferramentas eficazes na prevenção e reação a possíveis ataques. Como resultado, recursos foram identificados e serão recomendados, a saber: procedimentos e um software de antivírus conceituado no mercado. O propósito é inserir-se 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, estar ciente dos riscos que existem, tomar as devidas precauções e saber como agir, são itens mandatórios.

**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 os riscos de investidas criminosas para interceptar as comunicações na tentativa de usurpar os dados trafegados pela rede. Serão apresentados casos reais que trouxeram significativos prejuízos às vítimas.

Defende o conhecimento como arma de combate, somado ao apoio tecnológico que houver disponibilidade de entrar 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 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 embate a proliferação dos *Ransomwares*.

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

O exposto acima visa alertar sobre a nocividade dos ataques *Ransomwares*, que podem causar 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 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.

Por tanto, é perceptível a relevância do estudo realizado, pois alerta, conscientiza e aponta soluções. Provocando um posicionamento não apenas reativo, mas, fundamentalmente, 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.

Disseminar 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).

Ficar 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 contaminação e proliferação.

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

*Phishing scam*. Faz uso de estratégias e campanhas, massivamente 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).

Outra estratégia que que estão usando é atacar 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), que é um *software* usado para melhorar o desempenho de computadores.

Outro ponto relevante é o aumento do tráfego criptografado na *web*, que vem sendo explorado para fins escusos, como ocultar atividades suspeitas. De acordo com relatório da CISCO (2018), a comunicação criptografada usada por *Malwares* triplicou em um período de 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 a nuvem é surreal. Esse número continuará crescendo, pois aplicações para *IoT* estão proporcionando mercados novos e rentáveis (SINCLAIR, 2018).

Porém, é necessário salientar que 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 Conhecimento como ferramenta de prevenção e reação**

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 escanear 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 poderá auxiliar para que se tenha uma proteção ativa e atualizada.

**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, atuar 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 posicionamento 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 com base no 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, 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 é salutar, além de possibilitar 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 invasor em um sistema já comprometido, a depender da fase de intervenção, protegerá a totalidade dos arquivos.

**3.1 Hierarquias 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 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 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 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 (*Simple Mail Transfer Protocol*, ou Protocolo de transferência de correio simples), que é um protocolo para transferência de mensagens. 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 sequestros de dados.

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

Impedir execução automática de mídias removíveis, usando um programa de varredura a procura de códigos perniciosos.

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, com frequência, quando ocorrem 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, deverá ser encerrado 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 preferível. Existem muitos *softwares* com esse propósito, a saber: *Corvil*, *TripWire* e *End-point management* da *Symantec*. Em suma, manter o ecossistema computacional mapeado e atualizado é boa prática.

**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 o progresso desse mal.

Manter um cronograma de treinamento e conscientização dos usuários poderá reduzir drasticamente ocorrências de sucesso dos crimes no mundo digital. 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, além de procurar ter acesso às informações que são compartilhadas por diversos instrumentos de combate as infrações tecnológicas.

Em relação as redes de computadores, manter uma lista atualizada dos endereços mais comumente associados aos canais de comando e controle dos *Ransomwares* é primordial, 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 foi observado um determinado processo copiando muitos arquivos fora de um horário estipulado para rodar uma rotina de *backup*, ou um determinado usuário estiver requisitando vários endereços *web* em curto espaço de tempo, são indicativos de anormalidades e devem ser tratadas rapidamente.

Por tanto, é preciso buscar apoio tecnológico que automatize esses monitoramentos, oferecendo camadas de controle para detectar procedimentos indevidos em várias etapas.

**3.4 Agindo rapidamente**

Proteção das estações de trabalho e servidores, proteção da força de trabalho e uso das fontes de inteligência devem estar em sinergia. Assim, na ocorrência de um incidente típico, todas as forças irão ser acionadas e trabalharão colaborativamente para conter a ameaça. Por tanto, controle e integração são conceitos chaves que deverão ser constantemente observados.

Vale ressaltar o perfil 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 maior eficácia de proteção contra os *Malwares*, contar com o apoio de um bom ferramental de *softwares* é obrigatório, pois estão mais evoluídos e complexos e a tecnologia 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; tentando 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 começa atuando em um dos principais focos de invasão: campanhas de envio de e-mails. As mensagens contendo *Malwares* são automaticamente detectadas e tratadas antes mesmo de chegarem a caixa de entrada de potenciais vítimas.

Outro recurso é a detecção das tentativas de exploração do 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 a esse esforço, ele possui um eficaz bloqueador de *exploits*, que como visto anteriormente, são necessários para que o processo de instalação de um *Ransomware* seja concluído. O antivírus fica ativamente procurando processos anormais em seu comportamento, bloqueando-os se estiverem dentro das heurísticas construídas.

Mais um item importante é o escaneamento avançado de memória. Essa funcionalidade é importante para descobrir a verdadeira natureza dos processos que estão sendo onerosos, o que é vital para encontrar os *Cripto-Ransomwares* antes que a criptografia 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.

Os serviços em nuvem vêm sendo usados como medida de redundância e disponibilidade de informações, porém, essa interação também é alvo de ação por parte dos *hacker*s. E o ESET 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 Padrões. Existem diversas variantes e famílias de códigos maliciosos, entretanto, seus comportamentos seguem um padrão. Os objetos são cuidadosamente filtrados e os compatíveis são isolados.

Aprendizado de 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.

Reputação e *cache*. Verificação em *cache* usando as listas de permissões. Agilizando, maximizando e otimizando o processo de investigação. Essa caraterística é usada para comunicação de 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.

*Sandbox*. É um ambiente de simulação para execução de arquivos suspeitos. É um local seguro e apropriado para identificar o real risco 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 ainda na fase de decodificação.

Bloqueador de *exploits*. Os *exploits* são programas usados para explorar vulnerabilidades. Novamente, atitudes suspeitas são rigorosamente analisadas e contidas.

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

Proteção contra ataques de rede. É a extensão de um *firewall* que trabalha, mormente, nas vulnerabilidades no nível de rede. Recurso essencial, principalmente, se as aplicações no ambiente estiverem desatualizadas.

Proteção de *botnet*. O ESET intercepta e trata comunicações oriundas de uma rede de computadores infectados. Reconhece processos problemáticos e faz as devidas restrições de acesso.

Em suma, o *software* agrega um corpo de ferramentas que lidam com as pragas virtuais vigentes, em seus vários estágios. Cada atividade nociva é detectada e tratada, 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*, usados para tentativas de extorsão. Por isso, saber como se defender e reagir é princípio básico, que não depende de uma única frente, mas de várias: 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 obrigações de quem não quer estar refém nesse aguerrido mundo digital. Além disso, a legislação precisa ser mais acertiva e participar da Convenção de Budapeste é um progresso. Sendo essa vertente um assunto digno de aprofundamento como extensão deste trabalho, assim como investigar mais detidamente as ações dos *Ransomwares* no ambiente da *IoT*.

**Referências Bibliográficas**

BTCSOUL – O espírito do *Bitcoin*. ***Wannacry*** -O *Ransomware* 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 – Brasil. **Relatório Anual de Segurança Cibernética**. 2018. Disponível em <https://goo.gl/rE9Dcz>. Acesso em 26 out. 2018.

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

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

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

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

G1 – O portal de notícias da Globo. ***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. 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. **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. **Crimes Cibernéticos:** Ameaças e Procedimentos de Investigação. 2 ed. São Paulo: Brasport, 2013.