Ransomware - prevenção e combate

Adeilson Nazareno Araújo Pinheiro
adgospel@gmail.com

Claudinei Di Nuno, PhD
professorclaudinei@uol.com.br

Curso de Pós-Graduação *Lato Sensu* em Gestão Estratégica em Tecnologia da Informação (GETI) - Estácio

Resumo
Este artigo objetiva mostrar como o avanço da informativa tem facilitado a vida das pessoas, mas também propiciou um ambiente de interesse para ação de criminosos, que no anonimato e dificuldade de rastreio, veem um mercado lucrativo através da extorsão que fazem as suas vítimas. Principalmente, usando *softwares* maliciosos como os *Ransomwares*, que se caracterizam por criptografar e bloquear os sistemas sob seu controle, exigindo um valor de resgate para reaver os dados. Porém, é possível detê-los e combatê-los eficazmente, apesar de estarem cada vez mais sofisticados.

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

1 Introdução

Certo dia ao chegar no trabalho um analista de sistemas é surpreendido pelos relatos de indisponibilidade de acesso ao Sistema ERP (Enterprise Resource Planning, ou Sistema de Gestão Empresarial) da empresa. Ao procurar o departamento de suporte para entender o que está acontecendo, é avisado de que o servidor de banco de dados da aplicação foi sequestrado por um *Ransomware* e que o *backup* que era feito da base era na própria máquina de banco e que a rotina que movia esse *backup* para outro lugar estava inativa. O *backup* mais recente que se tem é de alguns meses. A diretoria se recusou a pagar o resgate e o único caminho a seguir é um esforço de lançamentos retroativos para se tentar chegar ao estado original antes do sequestro.

A situação acima é apenas uma ilustração do que acontece diariamente e em gravidades diferentes. Os *Ransomwares* são uma dura realidade e estão cada vez mais difíceis de conter.

A proposta é chamar atenção para o assunto, mostrando que ninguém está isento de ser atacado. Ir além dos conceitos básicos e mostrar métodos de prevenção e combate atuais.

O texto está disposto em duas seções, a saber: cenário de ataque e cenário de defesa.

Na primeira, tem um panorama geral de como as ameaças evoluíram e as mais comuns. Também retrata, apesar da automação, o alto número de ataques explorando usuários incautos. Discorre ainda sobre as fragilidades normativas da legislação brasileira para tipificar crimes virtuais. Nesse contexto, é apresentada a Convenção de Budapeste. Dá ênfase também à tecnologia como vanguarda.

Na segunda, são tratados alguns mecanismos de defesa. Começando por entender a estrutura e componentes principais de um ataque, as formas de lutar para erradicar o

intruso. É incentivada a capacitação da força de trabalho. Por fim, o *software ESET* é melhor detalhado como um eficaz programa para conter os *Ransomwares* e outros *Malwares*.

2 Cenário do ataque

As ameaças que rondam os usuários na rede mundial de computadores são consideradas *Malwares*. São códigos maliciosos que visam danos e prejuízos aos computadores hospedeiros (CERT.BR, 2018). Estar alerta aos perigos que trafegam na internet é essencial, pois não é exagerado dizer que se vive uma verdadeira guerra cibernética (CLARKE; KNAKE, 2015).

2.1 As ameaças mais comuns

Existem variadas técnicas e ferramentas usadas para fins perniciosos na internet. Abaixo algumas.

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 (vermes). Se caracterizam pela independência do agir humano e de outros programas para se proliferarem.

Trojan Horse (cavalo de Tróia). É um programa malicioso que se aglutina aos outros programas para se dissimular e invadir sistemas sem causar suspeitas.

Phishing scam (pescaria). Faz uso de iscas para atrair os indoutos. Usa muito campanhas por e-mail.

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, sem um governo emissor e que tem seu valor determinado pelos indivíduos que atuam no mercado (ULRICH, 2014).

2.2 Evoluídos e complexos

Os crimes virtuais não são algo novo e estão cada vez mais complexos e agressivos. Leia-se crimes virtuais como aqueles em que o computador é usado para praticar a ação. Nesse contexto, violação e interceptação de e-mails, furto de identidade, estelionato virtual, dentro outros, são ilegalidades cada vez mais presentes nessa verdadeira revolução digital que se tem hoje (SYDOW, 2014).

No caso dos *Ransomwares*, existe uma preocupação crescente: programas autoprogramados (CISCO, 2018). Como prova, estão os prejuízos causados pelo *WannaCry* em 2017 (BTCSOUL, 2017).

O uso das cadeias de fornecimento está aumentando, na tentativa de driblar os *softwares* de proteção, acoplando códigos maliciosos em programas considerados legítimos (CISCO, 2018). Exemplo: 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: ocultar atividades suspeitas. Os pesquisadores da CISCO (2018) relataram, inclusive, que a comunicação criptografada na rede usada por *Malwares* triplicou em um período de 12 meses.

No relatório é reforçado o interesse muito grande em usar campanhas de e-mail como porta de entrada para infecções. Principalmente através de anexos *.doc* e *.pdf* (LISKA; GALLO, 2017).

2.3 *IoT*

O termo *IoT* (Internet of Things, ou Internet das Coisas) é cada vez mais popular e se caracteriza por conceituar a realidade que se tem hoje, onde a quantidades de dispositivos conectados à nuvem é surreal. E cresce a cada dia, muito pelo fato das soluções de aplicações para *IoT* estarem proporcionando mercados novos e rentáveis (SINCLAIR, 2018). Nada está seguro. Ou seja, tudo o que estiver conectado na internet é um alvo em potencial.

Em fevereiro de 2017 foi noticiado sobre 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 do uso crescente de *softwares* autoprogramados para invadir sistemas – e, de acordo com empresas especializadas em segurança digital, esse número vai crescer (CISCO, 2018) -, as investidas em cima da ignorância digital ainda é lucrativa. Por isso, é importante dá melhores orientações, por todas as vias legais, de como cada um poderá eficazmente se proteger. 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 habitam nesse 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 para paralisar e erradicar uma ofensiva (ESET, 2018). O papel das pessoas nesse embate é fundamental, obviamente, mas não é suficiente. Ou seja, é necessário contar com ajuda da tecnologia para automatizar defesas e reações quando da detecção de intrusões. Tratar o problema em camadas tem se mostrado um bom caminho para ferramentas que 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 se posicionado como excelente opção.

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 contemporâneo.

Se tratando de legislação brasileira, o combate adequado 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 (MPF, 2018) surge nesse cenário como um instrumento incentivador da adoção das normas redigidas, bem como da criação ou adequação de outras no âmbito local, para que se atenda as especificidades de cada nação membro.

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

Voltando ao contexto dos *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.

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 notório o esforço para se 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 daria esse salto inicial em busca de se estar mais atualizado e com aparatos normativos mais robustos para lutar de forma efetiva contra os atentados digitais, além de que se poderia colaborar e receber dos países membros. Tornando, por exemplo, um processo de investigação além fronteiras.

3 Cenário de defesa

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

Para que seja devidamente tipificado como um ataque por *Ransomware*, os itens a seguir, obrigatoriamente, têm que estar presentes: implantação, instalação, comando e controle, destruição e extorsão.

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

Instalação. Nessa etapa, o código malicioso já atuará para tomar o comando e controle do sistema infectado.

Comando e controle. É o momento em que um canal de comunicação é aberto para o invasor interagir de forma mais direta e nociva, sendo pré-requisito para a destruição dos dados, abordada a seguir.

Destruição. Aqui ocorre a criptografia e/ou exclusão dos dados, culminando com o bloqueio do acesso.

Para que, de fato, um ataque seja considerado por *Ransomware*, a fase de extorsão precisa estar presente, sendo nela a ocasião em que o usuário é avisado de que seu sistema foi sequestrado é que só será restabelecido mediante o pagamento de um resgate, geralmente em frações de *bitcoins*. É importante frisar que não há garantia alguma de que feito o pagamento o problema será resolvido.

3.2 Estações de trabalho e servidores

Se não houver *backup*s que possam restaurar os arquivos, ou vacinas no mercado, um ataque bem sucedido tende a ser devastador. Por isso, buscar formas de não está vulnerável é primordial.

Uma das maneiras de prevenção é desabilitar macros do pacote Office da Microsoft, já que uma grande parte das ofensivas notoriamente se dão através delas, pois possuem elementos que interagem diretamente com o sistema operacional.

Outra, seria evitar baixar e/ou abrir documentos de caráter duvidoso como alguns arquivos em formato PDF. Se não houver certeza da origem e procedência, descartar o arquivo é indicado.

Bloquear extensões sabidamente usadas em ofensivas já no gateway do servidor SMTP também é uma boa prática, que evitaria mensagens não validadas de chegarem a caixa de entrada do correio eletrônico dos usuários.

Existem investidas criminosas muito elaboradas, mas as mensagens falsas por e-mail, usando engenharia social, ainda são usados e rentáveis aos criminosos. Por isso, não se deve apenas confiar de que os destinatários têm os conhecimentos básicos de cibercrime, de que não abrirão mensagens duvidosas. É preciso o uso e apoio da tecnologia para que as caixas de entrada dos correios eletrônicos sejam automaticamente analisadas e processadas a procura de algo potencialmente nocivo. Existem muitas ferramentas no mercado que fazem isso e, em tópico posterior, se terá a oportunidade de se apresentar uma.

Outra prática que deve ser cuidadosamente deliberada é o uso de drives compartilhados entre computadores em rede. A disseminação de um *Ransomware* entre os computadores interligados é certa se houver drives compartilhados e com permissões totais de acesso, de escrita e leitura em pastas e arquivos. A depender da atividade e da quantidade de dispositivos que usam esses compartilhamentos, a gerência e controle é mais difícil. Por tanto, restringir ou mesmo não usar esse meio de comunicação interna trará mais uma camada de segurança à organização.

O uso maior 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 é consenso. Proibindo, por exemplo, nos seguintes: *Download*, *Temp*, *%AppData%*\.

Impedir execução automática de mídias removíveis. E usando algum programa de varredura para procurar 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*. Geralmente, quando da ocorrência de problemas graves de desempenho ou resposta de um sistema operacional, restaurar para um ponto estável normaliza a situação e o mesmo seria válido para recuperação de desastres causados por pragas virtuais, por isso, essa proteção dos pontos de restauração é primordial.

Bloquear o acesso ao *host C&C* (*command-and-control*, ou comando e controle). Novamente, 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.

É interessante também que se tenha um inventário dos *hardwares* e *softwares* que estão sendo usados, bem como um acompanhamento se as versões utilizadas contêm algum tipo de vulnerabilidade e se as devidas correções já estão disponíveis à comunidade. Mais uma vez, buscar apoio tecnológico para automatizar e detalhar essas informações é imperioso. Existem muitos *softwares* com esse propósito. A saber, alguns: *Corvil*, *TripWire*,

End-point management da *Symantec*. Em suma, ter o inventário e saber se o ecossistema computacional está atualizado é crítico.

3.2 Investindo nos colaboradores

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

E, mediante ao que outra fora exposto sobre manter em dia as atualizações de *software*, evitar abrir mensagens de procedência e origem duvidosas, não clicar em links suspeitos, entre outros; Manter um cronograma de treinamento e conscientização dos usuários poderá reduzir drasticamente as ocorrências de sucesso dos crimes virtuais.

Uma sugestão: muitas empresas fazem a SIPAT (Semana Interna de Prevenção a Acidentes de Trabalho). Poderia ser montado um programa tal como 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 protegida.

3.3 Usando inteligência e tecnologia

Para estar à frente de possíveis ataques 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.

4 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.