ISSN 2447-1097

Direito & TI – Porto Alegre / RS www.direitoeti.com.br

RANSOMWARE: "SEQUESTRO" DE DADOS E EXTORSÃO DIGITAL

Renan Cabral Saisse[1]

INTRODUÇÃO

Ransomware originou-se da aglutinação das palavras *ransom* (resgate) e *software* (código/programa), ou seja, programa de/para resgate. Esse nome surgiu devido à peculiaridade de sua atuação nos dispositivos informáticos. Tal mecanismo originou as expressões "sequestro" de dados, interpretada como ato de bloquear, inutilizar ou inviabilizar o acesso à dados, e extorsão digital ou criptoviral, ato de solicitar vantagem ilícita/pagamento em troca da liberação dos dados. Essa praga cibernética ganhou grande destaque no cenário internacional rotulada como a ameaça cibernética de maior rentabilidade para a cibercriminalidade.

Ransomwares são softwares do tipo *malware* criados com o objetivo de infiltrar-se em sistemas sem a percepção de seu titular. Possui por diretriz criptografar ou compactar dados com senhas e assim bloqueando o acesso aos mesmos e, em muitos casos, inutilizando o dispositivo infectado. Posteriormente é iniciado um mecanismo de exibição de imagens/mensagens informando sobre como realizar o resgate dos dados mediante um pagamento. Estas solicitações são normalmente valoradas em bitcoins, devido ao extremo anonimato sobre as transações realizadas nesse sistema de pagamentos.

Para que a tecnologia *ransomware* seja melhor entendida é necessário discorrer sobre a sua classe Malware. A nomenclatura origina-se da fusão das palavras inglesas ***MAL****icious* e *soft****WARE***, sua tradução literal é programa malicioso, é um código informático criado para causar degradação de dados ou roubo de informações mediante infiltração em dispositivos informáticos de forma ilícita.

Os Malwares possuem diversos tipos: *worms* (vermes), vírus, *trojans* (cavalo de tróia), *rootkits*, *spywares*, *adwares*, *ransomwares*, entre outros. Não é o intuito aqui discorrer sobre todos os seus tipos, porém é extremamente recomendável o conhecimento desses para garantir uma navegação segura na rede mundial de computadores ou internet (www).

[1] Analista de Sistemas atuante nas áreas de Faturamento, Fraude, Revenue Assurance e Roaming Internacional na Oi S.A. Graduado em Análise e Desenvolvimento de Sistemas (UniverCidade); Pós-Graduando em CyberCrime, CyberSecurity e Perícia Forense Aplicada à Informática (AVM - Unyleya); Acadêmico do curso de Bacharel em Direito (UFRJ); Possui cursos de Extensão em Ciência Política (USP) e Linguagem de Programação Python (Harvard); Certificado em ITILV3 e Cobit V4.1; E-mail: rcsaisse@gmail.com.

ISSN 2447-1097

Há anos o *ransomware* vem se tornando uma preocupação para as autoridades policiais da UE. É um problema que afeta tanto os computadores quanto os dispositivos móveis, cidadãos e empresas igualmente, com criminosos desenvolvendo técnicas cada vez mais sofisticadas para causar maior impacto nos dados das vítimas.[i]

O primeiro *ransomware* noticiado surgiu em 1989 denominado por AIDS (Aids Info Disk ou PC Cyborg Trojan). O AIDS foi desenvolvido pelo PhD formado em Harvard Dr. Joseph Popp, um biólogo evolucionista. Sua ação ocorria durante a nonagésima inicialização do sistema operacional, após sua infecção (instalação no dispositivo), criptografando dados e tornando o sistema inutilizável. Em seguida, era exibido um alerta para renovação de licença, mediante pagamento à corporação PC Cyborg para que os dados fossem liberados. Como o AIDS criptografava os nomes dos arquivos utilizando criptografia simétrica (par de chaves iguais), uma vez descoberto o segredo, foi relativamente simples reverter o processo e rastrear o autor, o que ocorreu após análise do código por especialistas em segurança da informação. Popp foi preso pela New Scotland Yard e condenado ao cárcere, cumprindo pena na prisão de Brixton.

Posteriormente, novas extorsões cibernéticas foram noticiadas a partir de maio de 2005, atingindo um grau de sofisticação criptográfica maior em meados de 2006, momento em que havia uma variedade de aparições de novos *ransomwares* como o *Gpcode*, *Archiveus*, *Krotten*, *Cryzip*, *MayArchive*, entre outros. Essa evolução arrecadou mais de 42 mil *bitcoins* (equivalentes a 27 milhões de dólares) somente para a organização por trás do *CryptoLocker*, segundo informações da agência Zdnet em 2013[ii]. A Kaspersky Lab, divulgou o primeiro *ransomware* brasileiro em janeiro de 2016. Sua atuação consistia em exibir um pedido falso de atualização do software Adobe Flash Player e, após o link ser clicado, o computador era infectado e os dados existentes eram criptografados. O "sequestro" exigia algo em torno de R$ 2 mil em *bitcoins*[iii].

Atualmente, há uma infinidade de variantes de *ransomwares*, inclusive brasileiras, para múltiplas plataformas capazes de causar um grande estrago ao redor do mundo, o que elevou o alerta tornando uma das principais preocupações de entidades públicas e privadas à nível mundial.

1 MECANISMO DE FUNCIONAMENTO

O *ransomware* é propagado das mais variadas formas, seja por intermédio de acesso aos sites suspeitos que liberam o código malicioso apenas com a visita do usuário ou por arquivos disfarçados (músicas, imagens, etc.), normalmente divulgados em redes sociais ou enviados por e-mail aparentando algo comum, de interesse público, cobranças, causas sociais, etc. Ainda podem ser liberados via instalação de aplicativos vulneráveis em dispositivos móveis ou computadores.

Após a liberação do código no sistema, o *ransomware* opera em "silencio" sem o conhecimento do usuário até que todos os seus componentes para bloqueio de dados sejam instalados. Uma vez finalizada a instalação, uma mensagem (janela ou pop-up) informando sobre o bloqueio dos dados e resgate à ser pago para liberação é exibida. A partir desse instante todos os dados do dispositivo se tornam totalmente inacessíveis.

O maior problema com *cripto-ransomware* hoje é que, quando os usuários têm dados importantes bloqueados, eles imediatamente pagam aos criminosos para recuperá-los. Isso impulsiona a economia clandestina e como resultado aumentam o número de novos criminosos e o número de ataques.[iv]

A peculiaridade de um *ransomware* em "se passar" por arquivos comuns impede a sua detecção por ferramentas antivírus tradicionais, elevando sua periculosidade a um grau alarmante devido ao seu agressivo *modus operandi*.

2 TIPOS DE RANSOMWARE

Há variantes de *ransomwares* identificadas de acordo com o seu método de atuação pós infecção. Esses tipos foram estudados e mapeados ao longo do tempo por organismos policiais e companhias de segurança da informação, o que proporcionou a criação de ferramentas para reversão do bloqueio dos dados aplicáveis a alguns casos. Os principais tipos de *ransomware* mapeados pelas entidades internacionais são:

- ***Mobile Device Ransomware (Android)*:** Dispositivos Android podem ser infectados por meio de falsos aplicativos ou serviços populares, como um antivírus ou o Adobe Flash. Sua atuação é basicamente bloquear a tela e exigir pagamento para liberação.

Fonte: https://www.nomoreransom.org/ransomware-qa.html

- ***Master Boot Record (MBR) Ransomware*:** O disco rígido do computador (HD) possui uma parte chamada de Master Boot Record (MBR) que possibilita a inicialização do sistema

ISSN 2447-1097

operacional. MBR Ransomware altera essa parte do HD e assim interrompe o processo de inicialização normal solicitando uma código para que a questão seja sanada.

Fonte: https://www.nomoreransom.org/ransomware-qa.html

- ***Ransomware Encrypting Web Servers*:** Os sistemas de gestão de conteúdo web possuem vulnerabilidades conhecidas que são exploradas por ransomwares direcionados à servidores web com intuito de criptografar/sequestrar os dados e exigir resgate.

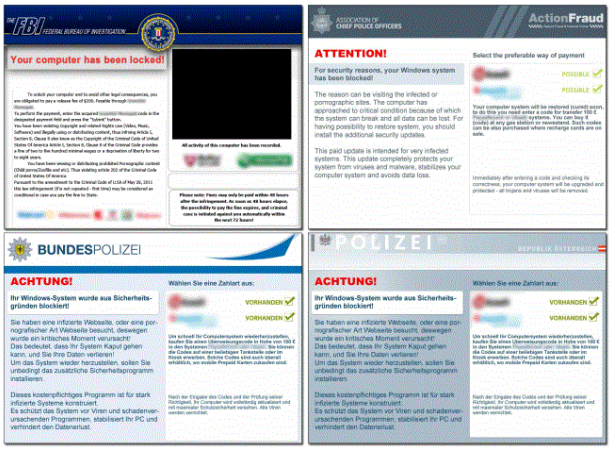
Fonte: https://www.nomoreransom.org/ransomware-qa.html

- ***Lock Screen Ransomware — WinLocker*:** Este Ransomware bloqueia a tela do computador exibindo uma mensagem de resgate para a liberação:

Fonte: https://www.nomoreransom.org/ransomware-qa.html

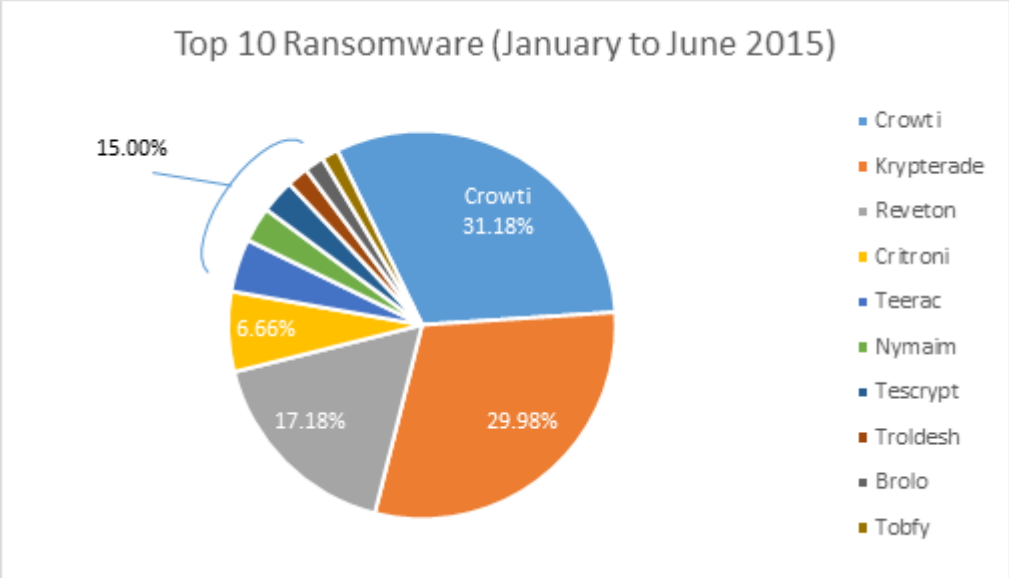
ISSN 2447-1097

- ***Encryption Ransomware (Cryptolocker):*** O mais temido de todos os *ransomwares*, pois ele criptografa todos os dados do computador (documentos, vídeos, fotos, músicas, planilhas, etc) Todos os arquivos afetados se tornam inacessíveis e no local pode haver um documento de texto exigindo resgate ou ao tentar abrir os arquivos é exibida a mensagem para pagamento e liberação. Esse tipo de Ransomware pode exibir pop-ups(janelas de mensagens) ou não. Para exemplificar houve um caso ocorrido na FedEx nos EUA que se tornou um dos mais famosos deste tipo e se deu por meio de um arquivo disfarçado de pdf enviado via e-mail.



Fonte: http://www.ciberforense.com.br/wp-content/uploads/2015/09/ransomwares.gif

Há ainda diversas "famílias" de *ransomware* notificadas. Abaixo um exemplo disponibilizado pela Microsoft em 2015 sobre dez famílias com maior ocorrência de atuação no período:



Fonte: http://www.ciberforense.com.br/wp-content/uploads/2015/09/ransomware-family.png

A título de exemplo, uma pesquisa da empresa de segurança Palo Alto Networks, realizada em 2015, indicou que uma família de ransomware conhecida como Crypto Wall movimentou US$ 325 milhões para a organização por trás dela.

> "No mundo do cibercrime, o ransomware é um dos problemas mais prolíficos que enfrentamos". Greg Day, vice-presidente de segurança para a Europa da Palo Alto Networks. [v]

3 ASPECTOS JURÍDICOS

3.1 – Crimes Cibernéticos

O *malware ransomware* é oriundo da "cibercriminalidade", ou seja, da evolução tecnológica da criminalidade tradicional que passa a agir por intermédio de dispositivos informáticos/eletrônicos garantindo uma escala global de resultados. Os crimes praticados dessa forma, segundo denominação adotada pelo Tratado do Conselho Europeu sobre Crime Cibernético (Convenção de Budapeste) que foi assinado por 43 países e ratificado por 21 das nações signatárias, no qual o Brasil não assinou ou ratificou até hoje, foram denominados por cibercrimes (*cybercrimes*) ou crimes cibernéticos.

Doutrinariamente podemos adotar três classificações principais para crimes cibernéticos:

- **Impuros ou Impróprios:** O dispositivo informático é utilizado apenas como meio/instrumento para consumação/execução de um crime tradicional.
  - **Exemplo:** Crimes contra a honra como calúnia (art.138 CP), difamação (art.139 CP) ou injúria (art. 140 CP) realizados em redes sociais ou por envio de e-mails
- **Puros ou Próprios:** O bem jurídico afetado é a inviolabilidade da informação automatizada (dados), ou seja, objetiva afetar diretamente dispositivos informáticos e seus dados.
  - **Exemplo:** Interromper serviço telemático ou de informação de utilidade pública, ou impedir/dificultar o seu restabelecimento (Art. 266, §1º CP).
- **Mistos:** Crimes complexos que envolvem mais de um bem jurídico de natureza diversa, sendo um deles a inviolabilidade de informações automatizadas, ou seja, daquelas armazenadas e processadas em sistemas computacionais.[vi]

- **Exemplo:** Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo – afeta a inviolabilidade de informações automatizadas e a privacidade - ou instalar vulnerabilidades para obter vantagem ilícita – pode afetar o patrimônio (Art.154-A CP).

3.2 – Ransomware no Ordenamento Jurídico Brasileiro

A lei 12.737 de 2012, que passou a vigorar em 2013, tipificou penalmente atos cibernéticos prejudiciais, até então amparados somente na esfera cível, incluindo no Código Penal o art. 154-A, que discorre sobre o ato ilícito de invadir dispositivo informático com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.

A referida lei prevê uma pena base de três meses a um ano de detenção e multa, que pode ser agravada de um sexto a um terço se resultar prejuízo econômico[vii] ou reclusão de seis meses a dois anos, e multa, se a conduta não constitui crime mais grave[viii]. A pena de reclusão pode ser aumentada de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas[ix] e de um terço à metade se o crime for praticado contra Presidente da República, Governadores e Prefeitos, Presidente do STF, Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou Câmara Municipal e dirigente máximo da Administração Direta e Indireta federal, estadual, municipal ou do Distrito Federal[x].

De acordo com o mecanismo de funcionamento do *ransomware* já descrito anteriormente, e com a tipificação no Código Penal, em seu Artigo 154-A, surgiu-se a expressão “Extorsão Digital ou Criptoviral”, pois a programação do *ransomware*, após instalar seus componentes no dispositivo informático e criptografar seus dados, solicita um resgate dos mesmos mediante um pagamento, o que fez surgir também a expressão “sequestro de dados”.

Analisando friamente poderíamos enquadrá-lo no Art. 154-A, § 2º, devido ao prejuízo patrimonial à vítima ou tentativa do mesmo, porém, além da observação do próprio parágrafo 2º sobre não constituir crime mais grave, o ordenamento jurídico brasileiro adota a Princípio da Consunção ou Absorção, ou seja, ação ou efeito de incluir algo menor em algo maior ou mais amplo. O crime claro, segundo o modus operandi do *ransomware*, é o crime de Extorsão (Art. 158 CP) por intermédio de dispositivo informático e assim absorvendo o crime de invasão de dispositivo informático (art.154-A).

Vale ressaltar que, apesar da expressão sequestro de dados, o ato não se aplica ao crime de sequestro (art. 148 CP) ou extorsão mediante sequestro (159 CP), pois em ambos os casos é necessário haver privação de liberdade da vítima.

Pode-se concluir que o *ransoware* é um crime de Extorsão cometido por intermédio de invasão de dispositivo informático com pena base em reclusão de quatro a dez anos e multa.

4 COOPERAÇÃO INTERNACIONAL

A criticidade do advento *ransomware* mobilizou entidades variadas contra um inimigo comum a todos e que atualmente vem sendo rotulado como o meio mais eficiente de extorsão da atualidade. Tal rótulo se dá devido a alguns critérios como o anonimato por intermédio dos resgates exigidos em *bitcoins*, a difícil rastreabilidade devido a propagação heterogênea do *malware* na rede, o que dificulta traçar a rota da origem do código malicioso ou a localização do autor do mesmo, a facilidade em "sequestrar" dados sensíveis o que agiliza o pagamento do resgate e muitas vezes autoridades policiais não tomam conhecimento durante esse processo.

Diante dos fatos, a Polícia Nacional Holandesa, a Europol, a Intel Security e a Kaspersky integraram-se e criaram uma iniciativa intitulada como No More Ransom. Esta união entre o setor público e privado, no âmbito internacional, tornou-se um marco histórico sobre o combate ao *ransomware*.

Segundo Wilbert Paulissen, diretor da divisão de investigação criminal da polícia nacional dos países baixos, essa é uma responsabilidade conjunta da polícia, do Departamento de Justiça, da Europol e das empresas de TIC. Essa união possibilita a interferência na lucratividade dos criminosos e devolução dos arquivos aos seus legítimos proprietários, sem que esses tenham que sofrer perdas patrimoniais em pagamentos por resgate aos dados.[xi]

> O conselho geral é para não pagar o resgate. Ao enviar o seu dinheiro para os cibercriminosos você apenas confirma a efetividade do ransomware, pois não há nenhuma garantia de que você terá a chave de decodificação que precisa em troca. NoMoreRansom.[xii]

O projeto *No More Ransom* (www.nomoreransom.org) é um site dedicado à disseminação do conhecimento sobre o que é a ameaça de extorsão digital, como se prevenir, como agir, além de disponibilizar ferramentas para recuperação de dados bloqueados. Há também a disponibilidade para colaboração de novos parceiros, pois, devido à mutabilidade e desenvolvimento contínuo de ransomwares, toda ajuda se torna essencial.

Essa integração já colhe frutos. O compartilhamento de informações entre as entidades, possibilitou localizar um servidor central utilizado por criminosos cibernéticos onde estavam armazenadas chaves para reverter o processo de criptografia de dados. De posse dessas informações foi possível o desenvolvimento de uma ferramenta com mais de 160 mil chaves para recuperação de dados. A ferramenta está disponível para download no portal *No More Ransom*.

Como esta praga cibernética pode estar ligada ao financiamento de organizações criminosas por trás das "famílias" de *ransomwares*, além de possuir caráter transnacional devido à extraterritorialidade ou "metaterritorialidade" do ciberespaço, vale ressaltar que o Brasil adotou em seu ordenamento jurídico, por meio do decreto nº 5.015 de 2004, a Convenção das Nações Unidas contra o Crime Organizado Transnacional que estabelece instrumentos e procedimentos em face à persecução penal ou criminal (procedimento criminal brasileiro que engloba as fases de investigação criminal e processo penal).

5 MEDIDAS DE SEGURANÇA

É fato que a total segurança cibernética só pode ser atingida off-line, porém devem ser tomadas algumas medidas de segurança para mitigar ataques cibernéticos. A força tarefa internacional, citada anteriormente, elencou seis tópicos na prevenção e reação ao *ransomware*. São eles:

1. **Back-up:** É a cópia dos arquivos importantes. Esta cópia é comum para profissionais de informática, seja para recuperação de dados em caso de falhas sistêmicas/humanas ou para recuperação de dados degradados por intermédio de ataques cibernéticos. É recomendável que esse back-up seja periódico e em dispositivo divergente do computador ou mobile utilizado normalmente. Assim, em caso de infecção por *ransomware*, caso não seja possível reverter o sequestro, o dispositivo poderá ser formatado e todos os dados recuperados.
2. **Antivírus:** São softwares de monitoramento e combate à programas maliciosos. É indispensável manter programas de proteção ao computador/mobile contra essas pragas digitais. De preferência utilizar uma solução robusta de classe Internet Security.
3. **Atualização Contínua:** É extremamente importante que seu sistema operacional e seus componentes estejam atualizado. Softwares padrões como navegadores ou mesmo ferramentas do office podem conter falhas em sua programação o que abre vulnerabilidades para ataques diversos.

Essas atualizações do sistema visam corrigir essas falhas à medida que estas são descobertas.

4. **Desconfie Sempre:** Um dos métodos mais eficazes utilizado por criminosos cibernéticos é a Engenharia Social. Esse método consiste em persuadir a vítima estimulando confiança para obtenção de informações privilegiadas ou mesmo viabilizar que o alvo baixe um arquivo enviado ou acesse um link malicioso. Desconfie sempre de e-mails de cobrança, bancos, distribuidoras de energia, operadoras telefônicas, tudo. Procure sempre realizar contato telefônico via número oficial para sanar dúvidas ou se dirija pessoalmente à entidade que supostamente originou o e-mail.
5. **Exibir Extensões de Arquivos:** Extensão é basicamente um sufixo do arquivo que define seu formato, ou seja, um arquivo texto terá uma extensão "txt", um documento do Word terá extensão "doc" ou "docx", do Excel "xls" ou "xlsx". Assim você enxergará todas as extensões dos arquivos em seu computador e caso você encontre algum arquivo de foto (jpg, png, gif) por exemplo com "mais de uma extensão" em seu nome, exemplo foto.jpg.exe, cuidado! Disfarçar arquivos maliciosos de supostas fotos, vídeos, músicas ou documentos é um golpe comum no ciberespaço.
6. **Off-line:** Caso perceba algum processo/arquivo suspeito desligue o dispositivo e a internet para evitar propagação da praga virtual. Em seguida procure informações sobre o nome do processo/arquivo suspeito identificado e possíveis métodos de remoção do mesmo. Vale ressaltar que muitas dessas pragas já são localizadas por antivírus. Respeite os alertas e o mantenha sempre atualizado. [xiii]

CONCLUSÃO

O exponencial crescimento dos ataques cibernéticos, por intermédio de *ransomwares*, vem promovendo uma *ciber wave* mundial em busca de conhecimento técnico sobre a ameaça para disseminação da informação e desenvolvimento de ferramentas de prevenção e reversão dos ataques. Essa grave ameaça pode desestruturar um país caso seja direcionada à setores críticos como usinas, entidades estatais, operadoras de telecomunicações, entre outros, e assim inviabilizando o acesso aos dados e inutilizando sistemas e processos, mediante extorsão.

É imprescindível ressaltar que o *ransomware* é a principal praga cibernética para financiamento de organizações criminosas no ciberespaço, como não se sabe o destino da arrecadação ilícita obtida via extorsão digital, considerando o caráter mundial do ciberespaço, pode-se facilmente ser revertida em lavagem de dinheiro, financiamento de quadrilhas armadas, terrorismo, compra de equipamentos sofisticados para potencialização de outros ataques cibernéticos, como o recente que derrubou a internet da costa leste dos EUA inviabilizando diversos serviços.

Segundo o FBI, entre janeiro e março de 2016, foram pagos US$ 209 milhões em resgates de dados somente nos EUA.[xiv] O potencial de destruição, mediante recursos patrocinados pelo *ransomware*, é imensurável e não há precedentes na história recente.

A vulnerabilidade extrema dos sistemas informáticos atuais frente à essa praga virtual, exige um esforço mundial devido ao caráter mutável, prolífico, de difícil rastreabilidade e com o poder de transformar qualquer um em "refém" do medo em perder seus dados. Assim as companhias especializadas em segurança cibernética e as forças policiais e de inteligência ao redor do mundo estão em constante cooperação frente a este inimigo comum e destrutivo.

Outro foco importante é a segurança cibernética necessária para se evitar ilícitos em consonância com a absorção e compreensão da tecnologia *blockchain* estudada por instituições financeiras ao redor do mundo e classificada como uma tecnologia revolucionária, inovadora, segura, transparente, capaz de prover uma redução sensível de custos operacionais em diversos segmentos frente às tecnologias atuais, porém utilizada por intermédio do sistema transacional da moeda virtual *bitcoin* para o anonimato em práticas ilícitas como a obtenção de recursos via *ransomware*.

Somado à constante multiplicação de "*ransoms*" brasileiros, e a informação preocupante de que o Brasil é principal alvo de *ransomwares* na América Latina e apenas 34% das empresas brasileiras reconhecem a ameaça[xv], se torna extremamente necessária a conscientização sobre essa ameaça. A mesma pode pôr em cheque o funcionamento de serviços essenciais, como o sequestro de informações sensíveis ou inviabilidade de funcionamento dos sistemas e processos em âmbito nacional por inutilização dos dispositivos informáticos interligados.

O Brasil, como membro da ONU e aliado a forças internacionais contra a transnacionalidade criminal, precisa evoluir cada vez mais seu ordenamento jurídico frente às ameaças cibernéticas, o que torna inegável buscar incorporar ao ordenamento jurídico nacional tratados internacionais sobre essa questão. Pode-se citar como exemplo a Convenção de Budapeste que prioriza uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adoção de legislação adequada e da melhoria da cooperação internacional e reconhece a necessidade de uma cooperação entre os Estados e a indústria privada.[xvi]

A cooperação entre as instituições é extremamente necessária para o combate à criminalidade cibernética e construção e disseminação de conhecimento para a *cybersecurity*, seja ela pública ou privada, em âmbito nacional, regional ou pessoal.

REFERÊNCIAS

Aprenda as diferenças entre vírus, trojans, spywares e outros. Tecmundo. Disponível em: <http://www.tecmundo.com.br/phishing/853-aprenda-as-diferencas-entre-virus-trojans-spywares-e-outros.htm>. Acesso em: 26 out. 2016.

Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em: 20 out. 2016.

CRESPO, Marcelo. **Ransonware e sua tipificação no Brasil**. Canal Ciencias Criminais. Disponível em: <https://canalcienciascriminais.com.br/ransonware-e-sua-tipificacao-no-brasil/>. Acesso em: 25 out. 2016.

Crimes cibernéticos. Cadernos de Graduação. Disponível em: <https://periodicos.set.edu.br/index.php/cadernohumanas/article/viewFile/2013/1217>. Acesso em: 21 out. 2016.

Decreto nº 5.015/04. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2004/Decreto/D5015.htm>. Acesso em: 20 out. 2016.

FERREIRA, Ivette Senise. Direito & Internet: Aspectos Jurídicos Relevantes. 2 ed. São Paulo: Quartier Latin, 2005.

GUSMÃO, Gustavo. **Ransomware: saiba tudo sobre os malware sequestradores**. Exame. Disponível em: <http://exame.abril.com.br/tecnologia/ransomware-saiba-tudo-sobre-os-malware-sequestradores/>. Acesso em: 20 out. 2016.

HENSSONOW, Susan F. **Ransomware (Malware).** 1ª Ed. Estados Unidos: Betascript Pub, 2011.

Kaspersky Anti-Ransomware. Kaspersky. Disponível em: <http://brazil.kaspersky.com/sobre-a-kaspersky/centro-de-imprensa/comunicados-de-imprensa/2016/kaspersky-anti-ransomware-tool-for-business-esta-disponivel-gratuitamente-para-usuarios-de-todo-o-mundo>. Acesso em: 28 out. 2016.

KLEINMAN, Zoe. **O vírus de computador que chantageia você**. BBC. Disponível em: <http://www.bbc.com/portuguese/noticias/2015/12/151214_virus_chantagem_rb>. Acesso em: 28 out 2016.

Lei nº 12.737/2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm>. Acesso em: 20 out. 2016.

Midyer Cybersecurity Report. Cisco. Disponível em: <https://www.cisco.com/c/dam/assets/offers/pdfs/midyear-security-report-2016.pdf>. Acesso em: 22 out. 2016.

No More Ransomware. Disponível em: <https://www.nomoreransom.org>. Acesso em: 26 out. 2016.

No More Ransom: autoridades policiais e empresas de segurança de TI unem forças para combater o ransomware. Overbr. Disponível em: <http://overbr.com.br/noticias/no-more-ransom-autoridades-policiais-e-empresas-de-seguranca-de-ti-unem-forcas-para-combater-o-ransomware>. Acesso em: 25 out. 2016.

NOGUEIRA, Luiz Augusto Pessoa. **Combate ao Crime Cribernético:** Doutrina e Prática. 1ª Ed. Cap. 2. Rio de Janeiro: M. Mallet, 2016.

O que é Ransomware? Techtudo. Disponível em: <http://www.techtudo.com.br/noticias/noticia/2016/06/o-que-e-ransomware.html>. Acesso em: 28 out. 2016.

O que é crime cibernético. Norton Symantec. Disponível em: <http://br.norton.com/cybercrime-definition>. Acesso em: 20 out. 2016.

Ransomware – O Perigo Do "Sequestro De Dados Digitais. Consisanet. Disponível em: <http://www.consisanet.com/ransomware-o-perigo-do-sequestro-de-dados-digitais/>. Acesso em: 29 out. 2016.

Ransomware já é o tipo de malware mais rentável da história. Cio. Disponível em: <http://cio.com.br/gestao/2016/07/28/ransomware-ja-e-o-tipo-de-malware-mais-rentavel-da-historia/>. Acesso em: 22 out. 2016.

ROOTS, Pablo. **Ransomware - Dez fatos que você deveria saber**. Disponível em: <http://suporteninja.com/ransomware-dez-fatos-que-voce-deveria-saber/>. Acesso em: 27 out. 2016.

Special Report: Ransomware and Businesses 2016. Disponível em: <http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf>. Acesso em: 20 out. 2016.

Saiba como os crimes na internet são tratados em outros países. Disponível em: <http://www2.camara.leg.br/camaranoticias/noticias/CIENCIA-E-TECNOLOGIA/199806-SAIBA-COMO-OS-CRIMES-NA-INTERNET-SAO-TRATADOS-EM-OUTROS-PAISES.html>. Acesso em: 20 out. 2016.

TADEU, Marcos. **A verdadeira defesa frente às ameaças do tipo Ransomware**. Disponível em: <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&UserActiveTemplate=mobile&infoid=43238&sid=15&utm_medium=>. Acesso em: 23 out.2016.

WENDT, Emerson. JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos:** Ameaças e Procedimentos de Investigação. 2ª Ed. Rio de Janeiro: Brasport, 2013.

---

[i] Wil van Gemert, Diretor-Adjunto de Operações da Europol. Disponível em: http://overbr.com.br/noticias/no-more-ransom-autoridades-policiais-e-empresas-de-seguranca-de-ti-unem-forcas-para-combater-o-ransomware.

[ii] Disponível em: https://blog.kaspersky.com.br/dez-fatos-sobre-o-ransomware/4614/

[iii] Disponível em: http://www.techtudo.com.br/noticias/noticia/2016/01/ransomware-brasileiro-usa-adobe-flash-player-para-sequestrar-dados.html

[iv] Jornt van der Wiel, Pesquisador de Segurança da Global Research e da equipe de analistas da Kaspersky Lab. Disponível em: http://overbr.com.br/noticias/no-more-ransom-autoridades-policiais-e-empresas-de-seguranca-de-ti-unem-forcas-para-combater-o-ransomware

[v] Disponível em: http://www.bbc.com/portuguese/noticias/2015/12/151214_virus_chantagem_rb

[vi] PASINATO, Danilo Corrêa de Almeida A Tecnologia da Informação na Investigação Policial. Disponível em: http://www.arcos.org.br/artigos/a-tecnologia-da-informacao-na-investigacao-policial/

[vii] Art. 154-A, § 2º, Código Penal

[viii] Art. 154-A, § 3º, Código Penal

[ix] Art. 154-A, § 4º, Código Penal

[x] Art. 154-A, § 5º, I, II, III, IV, Código Penal

[xi] Disponível em: http://overbr.com.br/noticias/no-more-ransom-autoridades-policiais-e-empresas-de-seguranca-de-ti-unem-forcas-para-combater-o-ransomware

[xii] Disponível em: https://www.nomoreransom.org/about-the-project.html

[xiii] Disponível em: http://www.psafe.com/blog/ransomware-o-que-e-e-como-se-proteger-do-sequestro-de-dados-feito-por-hackers/

[xiv] Disponível em: http://www.csoonline.com/article/3075385/backup-recovery/will-your-backups-protect-you-against-ransomware.html.

[xv] Disponível em: http://itforum365.com.br/noticias/detalhe/119004/brasil-e-principal-alvo-de-ransomware-na-america-latina

[xvi] Convenção sobre o Cibercrime. Disponível em: http://www.internacional.mpf.mp.br/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf.