Ransomwares

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
Universidade Estácio de Sá

Resumo
O texto irá discorrer sobre os perigos que circulam na *Internet*, com destaque para os *Ransomwares*, que são pragas virtuais usadas para sequestro de dados e tentativas de extorsões. Pretende-se conceituá-los, demonstrar como agem e como evitá-los. Para isso, será primordial entender a evolução desses *Malwares* e, nesse embasamento, apontar processos e ferramentas eficazes na prevenção e reação a possíveis ataques. 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 reações são itens mandatórios que, senão observados, poderão implicar na perda de informações que, a depender do grau de relevância, trará prejuízos significativos e de recuperação inviável ou parcial, geralmente árdua e onerosa e que, para ser factível, dependerá do quanto cedo a ofensiva foi neutralizada e se há backups recentes dos arquivos infectados ou vacinas de limpeza e restauração dos dados atingidos disponíveis no mercado.

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

1 Introdução

Um dos maiores patrimônios que se possui é a informação. E, por sua importância, tem sido alvo de criminosos que a tentam destruir, corromper ou sequestrá-la, para diversos fins ilícitos.

Notadamente, os *Ransomwares* têm se destacado como uma das pragas virtuais mais agressivas para comprometimento de dados; sequestrando e criptografando arquivos, exigindo pagamentos de resgates, que têm ocasionado consideráveis prejuízos, não apenas econômicos e financeiros.

Contemporaneamente, estão mais evoluídos e complexos, difíceis de combater. Por tanto, representando um risco real e iminente. Não raro, se aglutinando a *softwares* considerados populares a fim de invadirem os sistemas desapercebidamente.

Entre seus agravos não estão apenas os computadores desktops, mas qualquer dispositivo que esteja conectado na *Internet*. O que tem se tornado, deveras, inquietante, pois esse número de acessos à nuvem tem crescido perceptivelmente. Urge, assim, uma inevitável sinalização de alerta, face o amplo escopo de meios que estão vulneráveis às suas funestas ações.

O receio também se justifica devido a deficiência legislativa em torno do assunto, que tem sido tratado de modo genérico através do manuseio do código penal, principalmente. Essas generalizações têm sido impeditivas para as tipificações mais adequadas dos crimes, identificação e punição dos criminosos. Mas, considerando o cenário outrora, existe um

empenho mundial para enquadrar mais precisamente o cibercrime, através da famigerada Convenção de Budapeste.

É mister, por tanto, conhecer o que há de mais novo e eficiente para dificultar o êxito dos criminosos. Por isso, ter o conhecimento como aliado fará a diferença para montagem de uma barreira de contenção. E existem instituições nacionais e estrangeiras, públicas e privadas, que estão colaborando para multiplicar informes relevantes: de estáticas às cartilhas de orientações de práticas recomendadas para navegação na *Internet*. É salutar, ainda, o compromisso e parceria que deverá existir entre empresas e colaboradores, onde os investimentos em treinamentos destes deverão ser traduzidos em práticas e ações que mantenham ambos protegidos.

Porém, não se pode menosprezar o papel ímpar que o apoio tecnológico poderá trazer, contribuindo com automatização e inteligência para uma proteção ativa e ininterrupta.

O exposto acima e o que será apresentado visam sinalizar sobre a nocividade dos ataques *Ransomwares*, que podem causar grandes perdas. Por exemplo, afetando uma máquina que hospede bases de dados, criptografando os arquivos necessários para acesso das aplicações. Se uma rotina de *backup* não estiver implantada corretamente o impacto nas informações poderá ser letal, o que poderá trazer outras complicações, como paralisar o processo administrativo de uma organização.

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

Mostra-se, porquanto, relevante e justificável o incentivo de publicações de estudos sobre os *Ransomwares.* Estudos que despertem, conscientizem e apontem soluções. Provocando um posicionamento não apenas reativo, mas, idealmente, proativo. O que deverá diminuir significativamente o sucesso dos transgressores.

Quatro pilares de sustentação: conhecimento, infraestrutura, pessoas e tecnologia. E o termo investimento é quem os traduz. Investir em cada um trará mais confiança na segurança das informações.

Disseminar conhecimento sobre prevenção e combate aos *Ransomwares*, é a contribuição a que se propõe a presente monografia.

2 Fundamentação Teórica

2.1 Pragas virtuais mais comuns

Existem variadas técnicas e ferramentas usadas para fins escusos na *Internet*. Entre elas: Engenharia Social, *Worms* (vermes), *Trojan Horse* (cavalo de Tróia), *Phishing Scam* (pescaria) e *Ransomware* (UOL, 2018).

- Engenharia Social. Basicamente, é a manipulação 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 programas para contaminação e proliferação.
- *Trojan Horse*. Programa que, geralmente, se aglutina a programas considerados válidos para se dissimular e invadir sistemas sem causar suspeitas.
- *Phishing scam*. Usa estratégias e campanhas, massivamente de *e-mails*, para atrair e enganar os indoutos.
- *Ransomware*.

2.2 Conceitos e definições sobre os *Ransomwares*

Ransomwares são *softwares* codificados para impedirem o acesso a arquivos e/ou sistemas, sequestrando e criptografando informações e exigindo o pagamento de um resgate para descriptografia e liberação dessas (INFOWESTER, 2019).

Estão entre as principais ameaças que trafegam no ambiente digital, que tem se transformado em palco de uma verdadeira guerra cibernética (CLARKE; KNAKE, 2015, p. 33).

Para Liska e Gallo (2017, p. 18), é um *Malware* que atua nas fases: implantação, instalação, comando e controle, destruição e extorsão. 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, p. 18). Em tópico posterior, cada fase será abordada e melhor detalhada quando se estiver tratando das etapas de uma invasão por *Ransomwares*.

Em uma definição mais ampla são *Malwares,* que se caracterizam por causarem danos e agravamentos aos computadores hospedeiros (CERT.BR, 2018).

2.3 Evolução e complexidade dos *Ransomwares*

Crimes virtuais são os atos ilegais praticados através de computadores. Exemplos: violar e interceptar *e-mails*, furto de identidade, estelionato virtual, dentro outros. São irregularidades praticadas nessa revolução digital hodierna.

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

Outra estratégia que que estão usando é atacar as cadeias de fornecimento, com o propósito de embustear os *softwares* de proteção; Acoplando-se em programas considerados legítimos (CISCO, 2018). Exemplo: um cavalo de Tróia que foi baixado atrelado ao programa *CCleaner* (G1, 2017), *software* usado para otimizar desempenho de computadores.

Outro ponto relevante é o aumento do tráfego criptografado na *web*, que vem sendo explorado para fins interditos, como ocultar atividades suspeitas. Segundo o relatório da CISCO a comunicação criptografada usada por *Malwares* triplicou em um período de 12 meses. O documento ainda pontua o interesse em usar campanhas de *e-mails* como porta de entrada para novas infecções, principalmente através de anexos *.doc* e *.pdf*, que estão entre as extensões mais utilizadas para tais fins (LISKA; GALLO, 2017, p. 116).

2.4 Etapas de uma invasão por *Ransomwares*

Um ataque *Ransomware* possui, obrigatoriamente, os itens: implantação, instalação, comando e controle, destruição e extorsão (LISKA; GALLO, 2017, p. 18). Explanadas abaixo:

- Implantação. Os componentes básicos para infectar, criptografar e bloquear o sistema hospedeiro são instalados.
- Instalação. Inicia-se 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.
- Extorsão. O usuário é avisado que o sistema foi sequestrado e que será restabelecido mediante pagamento de um resgate, geralmente em frações de *bitcoins*. Entretanto, não há garantias que os dados serão recuperados.

Para evitar ou agir em cima de cada uma das etapas anteriores existem táticas de defesa sugeridas por Liska e Gallo (2017, p.77), que serão analisadas em momento oportuno.

Basicamente se concentram em: proteger as estações de trabalho e servidores; proteger a força de trabalho e utilizar os dados de inteligência como ferramentas de contenção.

2.5 *IoT*: dados na nuvem suscetíveis a ataques por *Ransomwares*

O termo *IoT* (*Internet of Things*, ou *Internet* das Coisas) se caracteriza por descrever 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).

Um estudo publicado no portal sobre tecnologia TECHTUDO (2017) aponta que brevemente os dispositivos e sistemas conectados na web sofrerão fortes investidas de ataques *Ransomwares*. A afirmação é feita com base na deficiência ou inexistência de antivírus para os equipamentos que já estão no mercado e para os novos que entrarão.

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

Mais preocupante, de acordo com o mesmo estudo, é a ramificação que os *Ransomwares* estão seguindo, a saber: atacar sistemas de saúde que estejam *online*. Esse interesse seria motivado pela sensibilidade e valor das informações que eles armazenam pois, uma vez sequestradas, poderiam trazer lucros exorbitantes através dos pagamentos dos regastes, dada a criticidade da recuperação dos dados.

2.6 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 definições 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, p. 141). Exemplo: se houver cotidianamente um rigor antes de abrir mensagens de *e-mails* com origem e conteúdos duvidosos, outras ações dentro desse contexto irão surgir naturalmente, como sempre usar uma ferramenta de antivírus para escanear um dispositivo removível.

2.7 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 soluções em tecnologia da informação. Em tópico posterior 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.

2.8 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. O exposto justifica um código normativo atualizado e específico.

Se tratando de legislação brasileira, o posicionamento aos crimes virtuais não está tipificado tal qual deveria (WENDT; JORGE, 2013). 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 que a abordagem 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. 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.

3 Desenvolvimento

Serão analisadas algumas recomendações para evitar ou paralisar uma ofensiva em andamento. Ressaltando-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 em que aconteça a intervenção, protegerá a totalidade dos arquivos.

Elas são frutos dos estudos feitos após um ataque por *Ransomwares* à empresa em que trabalha o autor. Localizada na região norte do país, Estado do Pará, na cidade de Belém. Atua na área de comunicação, possuindo entre seus veículos: jornal impresso de tiragem e publicação diária, programas de TV e Rádios e um portal de notícias. Filiada à Rede Bandeirantes. Nela o autor desempenha a função de Coordenador de Projetos e é responsável direto por seu sistema de administração corporativa.

O incidente mencionado comprometeu, principalmente, o servidor de banco de dados de seu sistema ERP (*Enterprise Resource Planning*, ou Sistema de Gestão Empresarial).

O cenário foi acentuado devido a rotina de backup do banco de dados ser no próprio servidor de hospedagem e o serviço que movia o arquivo para uma unidade de fita estava apontando para uma unidade de mapeamento inexistente. Esses e outros problemas menores contribuíram para a criptografia do arquivo de *restore* que havia na máquina. O backup mais recente que se conseguiu recuperar de um ambiente externo datava de cinco meses atrás.

Os serviços administrativos foram comprometidos seriamente e, como não se optou pelo pagamento de resgate, a estratégia imediata foi montar um plano de ação para relançar as informações que estavam arquivadas em documentos impressos e, paralelamente, repensar os procedimentos em segurança da informação vigentes naquele momento.

Os preceitos a seguir foram discutidos e alguns prontamente adotados, como os cuidados redobrados com as estações de trabalho e servidores e a utilização do *software* ESET no âmbito corporativo, monitorando rigidamente os compartilhamentos através de caminhos de rede, que facilitaram a propagação do *Malware* e chegada no servidor de banco de dados mencionado.

3.1 Cuidados básicos com computadores pessoais 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. Com esse escopo, 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 os arquivos.
- Bloquear extensões frequentemente usadas em ofensivas, no gateway do servidor SMTP (*Simple Mail Transfer Protocol*, ou Protocolo de transferência de correio simples), que se trata de 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, fazendo inspeções à procura de códigos maléficos.
- Impedir a desativação e/ou exclusão dos pontos de restauração do sistema com 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 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* 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 são boas práticas.

3.2 Investindo nos colaboradores

Ransomwares mais modernos não necessitam de interação humana: 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.

Dispor de um cronograma de treinamento e conscientização dos usuários poderá reduzir drasticamente êxitos 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 elaborado um projeto com a sigla SIPATI (Semana Interna de Prevenção a Acidentes em Tecnologia da Informação), onde várias palestras, simulações e atividades poderiam ser elaboradas com este fim: atualizar os colaboradores sobre os incidentes que estão ocorrendo e como cada um poderá contribuir para conservar a empresa segura.

3.3 Usando inteligência e tecnologia

Para antecipar 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, possuir uma lista atualizada dos endereços mais comumente associados aos canais de comando e controle dos *Ransomwares* é primordial, pois esses dados servem de históricos para montar uma camada de proteção, bloqueando todos e quaisquer acessos que coadunem com as análises.

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 de computadores pessoais e servidores, proteção dos colaboradores 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 itens 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.

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, fundamentalmente, 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. Será apresentada uma que vem obtendo excelentes resultados, a saber: ESET.

O programa em questão começa agindo em um dos 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 o processo de instalação de um *Ransomware*. 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 auxilia a descobrir a verdadeira natureza dos processos que estão sendo onerosos. Isso 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 nessa modalidade serão elencados a seguir na tabela 1.

Tabela 1 – Recursos do *software* ESET para proteção de dados na nuvem

Recurso	**Funcionalidade**
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 *Ransomwares*, 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 investigações. Essa caraterística é útil para comunicação de inteligência entre os clientes do *software*.
Detecção comportamental e bloqueio	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 identificar e 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.

Fonte: Autoria Própria

Em suma, o *software* agrega um corpo de recursos que lidam com as pragas virtuais vigentes, em seus vários estágios. Cada atividade nociva é detectada e tratada, diminuindo as consequências dos danos.

4 Conclusões

Os crimes virtuais estão crescendo e se modernizando, vitimando um número alarmante de pessoas e instituições diariamente. E dentre os males digitais (*Malwares*) os que vêm ganhando notoriedade são os *Ransomwares*, usados para tentativas de extorsão. Por conseguinte, precaver e reagir são princípios básicos, que não dependem 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 bons programas de proteção sãos mais que recomendações, são obrigações de quem não quer estar refém nesse aguerrido mundo digital. A questão normativa também precisa ser revista

e buscar mais contundência e especificidade, para que atenda as tipificações dos crimes virtuais de maneira mais apropriada e atualizada. Para isso, participar da Convenção de Budapeste seria 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.

INFOWESTER – Tecnologia ao seu alcance. **O que é *ransomware?***. 2019. Disponível em https://goo.gl/uBFUjT. Acesso em 25 jan. 2019.

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.

TECHTUDO – A Tecnologia Descomplicada. ***Internet* das coisas e sistema de saúde são os próximos alvos de *ransomware*** - Relatórios indicam um novo rumo para os ataques de *ransomware*. 2017. Disponível em https://goo.gl/Xyigac. Acesso em 25 jan. 2019.

UOL – O melhor conteúdo. **Pragas virtuais Elas querem tudo de você:** desde tirar onda até seu dinheiro do banco. 2018. Disponível em https://goo.gl/RgiEbC. Acesso em 29 out. 2018.

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

WENDT, Emerson; JORGE, Higor. **[*E-Book*] Crimes Cibernéticos** - Ameaças e Procedimentos de Investigação. 2013. Disponível em: https://goo.gl/73z55a. Acesso em 01 nov. 2018.