***Ransomware* - métodos de 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 informar aos alunos deste curso como deve ser elaborado e apresentado o artigo científico que compõe seu Trabalho de Conclusão de Curso (TCC). Suas seções elucidam as formas de apresentação do trabalho e como deve ser escrita cada uma delas. Está formatado conforme o modelo a ser seguido. Use-o como *template*. O resumo, redigido em língua portuguesa pelo próprio autor, deve trazer a síntese dos pontos relevantes do trabalho: tema, objeto da pesquisa, objetivos, metodologia e técnicas utilizadas, resultados alcançados e conclusões, mas de forma contextualizada. Deve ter no mínimo 150 e no máximo 200 palavras, e deve constar de um só parágrafo. O aluno deve usar recursos do editor para fazer a contagem. As pessoas leem o resumo para decidir se lerão ou não o restante do artigo, assim, é importante que sejam resumidos de maneira precisa e atrativa os tópicos principais do artigo. Deve-se escrever de forma bastante objetiva para evitar má interpretação da mensagem principal do artigo. No resumo não devem ser incluídas referências bibliográficas, citações diretas ou indiretas, figuras ou equações. O tempo verbal deve ser presente e não futuro.

**Palavras-chave:** artigo científico, normas ABNT, trabalho de conclusão de curso (deve-se escolher palavras-chave abrangentes, mas que identifiquem o tema de que trata o artigo).

# Introdução

A introdução deve apresentar uma descrição geral do conteúdo do artigo científico sem entrar em muitos detalhes. Nesta parte do trabalho, apenas poucos parágrafos são o suficiente para sua apresentação. Recomenda-se uma página apenas, isto é, em torno de 10% do texto total. A introdução deve descrever brevemente a importância da área de estudo e do tema em foco e mostrar a relevância da publicação do artigo. Deve explicar como o trabalho pode contribuir para ampliar o conhecimento na área e se ele apresenta novos métodos para resolver ou abordar um problema. A introdução deve ser finalizada com a apresentação explícita dos objetivos do trabalho. Deve-se evitar o uso de referências diretas e indiretas na introdução.

O aluno deve elaborar o seu TCC na forma de um artigo acadêmico-científico cujo formato está especificado neste documento. É importante que o aluno saiba que o artigo é aprovado somente pelo professor orientador. Uma vez aprovado pelo orientador, é que o aluno pode confirmar sua participação na defesa, na data informada pela equipe de TCC da universidade. Recomenda-se que o aluno leia o documento *2-Regras e Orientações para a defesa do TCC e para a disciplina Metodologia da Pesquisa Científica\_EaD* disponibilizado pelo orientador na plataforma AVA, na guia Material de Estudos da disciplina Metodologia da Pesquisa Científica.

Um artigo científico, ou acadêmico-científico, deve relatar informações e resultados de uma pesquisa de maneira clara e concisa. Seu principal objetivo é ser publicado em revistas, jornais ou periódicos científicos. De uma maneira geral, um artigo científico é um relato analítico de informações atualizadas sobre um tema de interesse para determinada especificidade. É o resultado de um estudo desenvolvido através de uma pesquisa, podendo ser resultado de um trabalho de conclusão de um curso de extensão, graduação ou pós-graduação ou de um projeto de pesquisa.

Ao escrever um artigo é importante utilizar uma linguagem formal, clara, correta, concisa e objetiva. Deve-se fazer uso da 3ª pessoa do singular ou verbo na voz passiva. Devem ser evitados adjetivos exagerados, superlativos, subterfúgios e repetições desnecessárias. É fundamental o uso correto da ortografia, pontuação, concordância e sintaxe da língua portuguesa, sendo recomendável que o aluno submeta o artigo a uma revisão rigorosa antes de apresentá-lo ao orientador ao longo do trabalho de orientação. Deve ser igualmente rigoroso o respeito ao *template* e às regras aqui apresentadas.

Um artigo é composto das seguintes partes: itens preliminares, itens de discurso e itens complementares. Os itens preliminares abrangem o título, o nome dos autores e sua afiliação, o resumo, com as palavras-chave e o *abstract* com as *keywords*. O *abstract* e as *keywords* só devem ser elaboradas quando solicitadas pelo orientador, tendo em vista a possibilidade de publicação do artigo em periódicos nacionais ou estrangeiros. Os itens de discurso incluem introdução, fundamentação teórica, desenvolvimento e conclusões. Estes são, na essência, o verdadeiro conteúdo do trabalho. São nesses itens que serão concentrados os esforços do autor em fornecer aos leitores condições de compreensão e entendimento, discussão e análise, síntese e demonstração do conhecimento associado ao seu trabalho. Os itens complementares podem incluir anexos e apêndices, ambos opcionais, no entanto devem ser evitados por tornar o texto do artigo muito longo e mais difícil de ser publicado. As Referências Bibliográficas são um item complementar obrigatório e devem ser elaboradas estritamente dentro normas da Associação Brasileira de Normas Técnicas (ABNT) e as orientações do curso. Neste TCC não devem ser redigidos os agradecimentos, que podem ser elaborados, a pedido do orientador, em caso de publicação.

O objetivo deste artigo é esclarecer o aluno quanto às regras para a escrita do artigo científico, com conteúdo e qualidade compatível com o curso de pós-graduação. Ao longo do artigo cada seção é identificada e são apresentadas orientações relativas ao seu teor, tamanho e formatação, com base nas normas da ABNT. Importante ressaltar que o artigo a ser escrito pelo aluno deve ter obrigatoriamente as partes aqui descritas.

1. **Cenário do ataque**

**2.1 As ameaças mais comuns**

Existem variadas técnicas e ferramentas usadas para fins perniciosos na internet, conforme mostra um excelente material publicado no site Monografias Brasil Escola (MONOGRAFIAS BRASIL ESCOLA, 2017). Entende o autor que dentre as elencadas, as que melhor contextualizam com a proposta do presente trabalho são as que estão abaixo.

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 que está orquestrando o golpe. No escopo da internet, um exemplo clássico dessa abordagem é o uso das campanhas de e-mails usando informações críveis, levando muitos incautos a clicarem nas mensagens e não raro, baixando os arquivos que possivelmente estejam nos anexos e até mesmo os executando, sem que haja uma verificação mais profunda e necessária das reais procedências. Mais à frente o tipo de ação aqui abordada será tratada mais detidamente.

Worms. Na tradução literal são os vermes. Se caracterizam principalmente pela independência do agir humano e de outros programas para se proliferarem (NOVAES, 2014). Hodiernamente, boa parte dos males que circulam pela rede apresentam esse comportamento, bastando encontrar um ponto fraco e automaticamente atacá-lo, sem qualquer intervenção do usuário no processo.

Trojan Horse. São os conhecidos cavalos de Tróia, em alusão ao estratagema usado pelos gregos para enganar a o povo de Tróia e entrarem desapercebidamente em território inimigo (PEREIRA, 2008). Por tanto, um trojan nada mais é do que um programa malicioso que se aglutina à outro, normalmente de uso popular, para se dissimular e invadir um sistema sem causar suspeitas ou alardes. E, uma vez dentro, poderá conferir ao invasor total controle do dispositivo hospedeiro.

RootKit. São os programas e recursos que conferem a um invasor o controle de uma máquina infectada. Podem este acessar remotamente de qualquer lugar e quando lhe convier. Algumas vezes se disfarça de aplicativo útil, como por exemplo, alternativas ao prompt de comandos do Windows. Podem, inclusive, apresentar excelentes funcionalidades e interface, sem levantar quaisquer suspeitas de seu real propósito.

Backdoor. É o programa que explora uma vulnerabilidade de conexão, deixando um canal aberto de interação, que poderá ser usado pelo invasor para manobrar o sistema sequestrado.

Phishing scam. Pode-se traduzir informalmente como “pescaria”, por tanto, faz uso de iscas para atrair os indoutos (ALECRIM, 2013). Esse mecanismo, por fácil dedução, se vale da engenharia social para atingir seus propósitos. O material do MONOGRAFIAS BRASIL ESCOLA estudado cita os autores Peter Stavroulakis e Mark Stamp (2010) para revelar que as campanhas por e-mail, preferencialmente, são usadas como instrumentos para alcance geral, na expectativa de que usuários inexperientes possam ser vitimados e ainda atuarem em uma corrente de multiplicação do *Malware*. Por exemplo, enviando mensagens contaminadas automaticamente para todos os contatos que possui.

*Ransomware*. De acordo com Liska e Gallo (2017), é uma modalidade de *Malware* que atua nas seguintes fases: implantação, instalação, comando e controle, destruição e extorsão. Caracteriza-se por bloquear ou restringir o acesso dos usuários aos seus arquivos, normalmente criptografados, e exigir um resgate, que deverá ser pago em frações de bitcoins, para que o usuário – não há quaisquer garantias – possa reaver seus arquivos e sistema como o eram originalmente. Os prejuízos, não só financeiros, podem ser desastrosos se não houver, por exemplo, uma política de backup eficiente, pois até o processo de restauração do sistema que, por ventura, tenha sido configurado, os *Ransomwares* conseguem evitar. Existem, sim, sites e softwares que prometem quebrar as criptografias, porém, rapidamente se tornam obsoletos e, por tano, não confiáveis. As organizações criminosas estão sofisticando cada vez mais os *Ransomwares*, pois o anonimato, a inadequação ou ausência de legislação específica para esse tipo de crime, a dificuldade ou impossibilidade de rastrear os pagamentos e o desespero dos usuários, tornam esse mercado atraente e lucrativo para os criminosos.

**2.2 Cada vez mais evoluídos e complexos**

Os crimes virtuais não são algo novo, mas remontam aos primórdios da informática. E com os avanços da internet, se modernizaram e estão cada vez mais complexos, agressivos e nocivos. Leia-se crimes virtuais como aqueles em que o computador é usado para praticar a ação (ROQUE, 2007). Ressaltando-se que nem toda invasão objetiva prejuízo do software atacado, mas o poderá ser para identificar vulnerabilidades que poderão ser corrigidas posteriormente. Mas sem o consentimento de acesso, óbvio, continua sendo prática ilegal e passível de punições.

Os invasores são mais comumente nomeados como (HOFFMAN, 2013):

* White Hat Hacker (hacker do chapéu branco): possui sólidos conhecimentos em sistemas operacionais e em linguagens de programação. Não tem por finalidade primária o mal, mas a satisfação pessoal em encontrar falhas de segurança.
* Black Hat Hacker (hacker de chapéu preto): é aquele que explora as vulnerabilidades com o propósito de prejudicar as vítimas.
* Gray Hat Hacker (hacker de chapéu cinza): dependendo do contexto e da situação pode atuar em diferentes lados. Ou seja, pode transitar de um explorador de vulnerabilidades a um malfeitor, de fato.
* Cracker: é considerado aquele que por exemplo, de modo ilegal, quebra as senhas de acesso de softwares proprietários para uso pessoal e/ou de outrem.
* Phreakers: são os especialistas em agredir sistemas de telefonia. Por exemplo, para instalar ou fazer uso de escutas não autorizadas.
* Lammer: são os iniciantes. Em geral, usam o pouco que sabem para exibicionismos.

Importante ponderar que, independente de por onde ou qual o papel assumido numa investida, o cenário é de códigos maliciosos projetados para serem cada vez mais poderosos e eficientes.

No caso dos *Ransomwares*, o relatório anual da (CISCO, 2018) alerta para o avanço que se deve esperar em termos de inteligência e complexidade, por isso, os usuários devem se precaver para ataques cada vez mais sofisticados: programas autoprogramados, que não dependem mais da intervenção humana. Como prova, menciona os prejuízos em escala global causados pelo *Ransomware* *WannaCry* no ano de 2017.

Ainda é dito que o uso das cadeias de fornecimento para intrusões bem sucedidas estão aumentando em velocidade e complexidade, na tentativa de driblar os softwares de proteção, acoplando códigos maliciosos em um programa considerado legítimo, tentando passar pelos algoritmos de detecção sem serem percebidos. Como ratificação, cita um cavalo de tróia que foi baixado junto como o programa CCleaner, que é usado por ter rotinas que aumentam o desempenho de um sistema operacional.

Outro dado apontado é que deve ser observado é o aumento do tráfego criptografado na web, que primariamente traria mais segurança às informações em trânsito no caso de serem indevidamente interceptadas. Porém, essa mesma tecnologia vem sendo usada para fins escusos, como ferramenta para ocultar atividades suspeitas. Os pesquisadores da CISCO relataram, inclusive, que a comunicação criptografada na rede usada por *Malwares* triplicou em um período de 12 meses.

E ainda mais preocupante, é a possibilidade concreta de em campanhas próximas, os criminosos fazerem uso de inteligência artificial e automação, dificultando mais ainda as tentativas de bloqueio e controle das ameaças.

Apesar de toda a preocupação em se preparar para o futuro tenebroso dos crimes virtuais, não se pode esquecer do presente, e da maneira ainda muito eficaz usados pelos criminosos para aumentarem o número de vítimas, que é através da proliferação das pragas virtuais em mensagens de e-mails. No relatório é reforçado o interesse muito grande em usar esse meio 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, como bem pontua Mauro Faccioni Filho (2016, p. 8).

Por tanto, ataques explorando esse nicho é realidade. Nada está seguro, dos celulares às Smart TVs usados por um número exorbitante de pessoas. Ou seja, tudo o que estiver conectado na internet é um alvo em potencial.

Em fevereiro de 2017 foi noticiado sobre um ataque inusitado na Áustria, quando um grupo de hackers invadiu o sistema de chaves eletrônicas de um hotel, impedindo a entrada e saídas dos hóspedes nos quartos (EXAME, 2017).

Deveras, é um ponto de atenção em que todos devem estar em alerta, pois se trata de algo próximo da realidade de cada um.

**2.4 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 importação de um código normativo atualizado e condizente com a realidade que se tem hoje.

Em se tratando de legislação brasileira, o combate adequado aos crimes virtuais não estão tipificados tal qual deveriam (MASSENO E WENDT, 2017). Porém, desde 2001 há um esforço internacional para fazer frente ao cibercrime.

A Convenção de Budapeste 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 virtuais no Brasil acontece com precariedades são as generalizações das ações no 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, principalmente em seus parágrafos § 1º, § 2º e § 3º.

É notório o esforço para se aplicar a persecução penal, minimizando o sentimento de impunidade. Porém, tipificar e tratar mais adequadamente os crimes virtuais 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 também receber ajuda de todos os países membros, tornando, por exemplo, um processo de investigação além fronteiras como, em geral, os crimes virtuais o são.

1. **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.

A implantação, por tanto, é a primeira fase, em que os componentes necessários para infectar, criptografar e bloquear o sistema hospedeiro são instalados. Mais comumente, se dá através de:

* Download automático de *Malware* (Download drive-by);
* Campanhas maliciosas de e-mails (Phishing);
* Exploração de vulnerabilidades através da internet.

Após, a instalação propriamente do *Ransomware*. 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. Nesse momento é que se dá a criptografia e/ou exclusão dos dados do usuário, culminando com o bloqueio do acesso ao sistema vitimado.

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 prometido será feito e, mesmo que o seja, o usuário poderá continuar vítima do invasor indefinidamente, pois também não há garantias de que serão removidos os softwares basilares que possam favorecer novas intrusões.

**3.2 Estações de trabalho e servidores**

Sem não houver backups que possam restaurar os arquivos, ou vacinas no mercado para descriptografia, um ataque bem sucedido tende a ser devastador. Por isso, buscar formas de não está vulnerável é primordial, principalmente devido à complexidade cada vez maior dos algoritmos por trás do *Malware* do gênero.

No contexto de um ambiente corporativo, onde possa existir uma rede de computadores, sofrer um ataque é, deveras, de maior magnitude do que o ser apenas em um ambiente doméstico. Mormente porque naquele podem existir anos de informações acumuladas, todo o aparato de gestão empresarial e comercial, etc. Por isso, um maior rigor nas políticas internas de segurança da informação é primordial, a começar pelas estações de trabalho, chegando nos servidores.

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 sofisticadas – e a tendência é serem cada vez mais complexas e difíceis de combater, mas mensagens falsas por e-mail, usando engenharia social, ainda é um dos métodos mais antigos, 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 acessam 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 mesmo se aplica para acessos remotos.

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

Limitar os diretórios onde os arquivos possam ser executados é consenso. Proibindo, por exemplo, nos seguintes: \Download, \Temp, %AppData%\. Programas, por ventura, executados automaticamente em quaisquer destes devem receber atenção especial, pois são os caminhos padrão para downloads feitos diretamente pelo browser ou oriundos de outras aplicações.

Impedir execução automática de PEs (Portable Executables, ou executáveis portáteis) através, por exemplo, do uso do software AppLocker (Windows 7 e no Windos Server 2008).

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 e os investimentos feitos não serão desperdiçados, por certo.

Bloquear o acesso ao host C&C (command-and-control, ou comando e controle), geralmente usando HTTP, na porta 80. Novamente, ferramentas como Carbon Black, Cylance, FireEye podem ajudar nessa atividade.

Muitos *Ransomwares* usam a API Crypto do Windows (crypt32.dll) para criptografar os arquivos, por isso, é recomendado encerrar qualquer processo não confiável que chama a API Crypto um determinado número de vezes, caracterizando uma atitude suspeita. Esse valor iria variar para mais ou menos, conforme as experiências nos ataques.

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. Por exemplo, muitas empresas fazem a SIPAT (Semana Interna de Prevenção a Acidentes de Trabalho) e poderia ser montado um programa tal como SIPATI (Semana Interna de Prevenção a Acidentes em Tecnologia da Informação), onde várias palestras, simulações a 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 aos crimes virtuais. Por exemplo, no contexto das redes de computadores, manter uma lista atualizada dos IPs e URLs mais comumente associados aos canais de comando e controle dos *Ransomwares* é uma boa prática, pois esses dados podem ser usados para montar uma camada de proteção, bloqueando todos e quaisquer acessos oriundos dessa parametrização.

Outra prática muito eficiente é monitorar execução de processos e acessos anômalos de usuários. 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 de rede está acessando várias URLs duvidosas em curto espaço de tempo, são indicativos de anormalidades e devem ser tratadas rapidamente, já que são indícios de ações maliciosas.

Esses procedimentos são inviáveis de se fazer manualmente se o contexto for um ambiente corporativo, devido a quantidade de dispositivos que poderão estar usufruindo dos recursos de rede no momento. Por tanto, 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 típicas de pragas virtuais.

**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, na visão do autor e na experiência no local onde trabalha, 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 hackers 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 hackers. 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 modos 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 patchs de aplicações estão defasados ou até mesmo não existem.

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

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

1. **Conclusões**

As conclusões fecham o artigo e são muito importantes. Resumir, apontar e reforçar as ideias principais e as contribuições proporcionadas pelo trabalho faz parte das conclusões. A finalização do artigo pode dizer o que foi aprendido pelo autor através de sua pesquisa, mas mantendo-se a impessoalidade do texto. Não se pode confundir relato de um aprendizado com depoimento pessoal. A conclusão deve ser analítica, interpretativa e deve incluir argumentos explicativos. O texto das conclusões deve ser capaz de fornecer evidências da solução do problema através dos resultados obtidos ou deve ser capaz de enfatizar as vantagens do objeto de estudo para aqueles, pessoas e organizações, que o adotam ou utilizam. Os objetivos listados na Introdução devem ser analisados e confrontados com os achados da pesquisa.

O autor pode comentar a sua pesquisa de forma objetiva e convincente, apresentando os ganhos obtidos com a sua realização. Caso alguma ferramenta ou metodologia tenha sido objeto do estudo, pode-se resumir aqui as vantagens e benefícios que sua adoção pode trazer para as organizações ou pessoas que a utilizam.

É interessante incluir nas conclusões comentários sobre os planos relativos a um trabalho futuro ligado ao mesmo tema, modificações a serem feitas para ampliar o seu escopo ou ainda limitações da metodologia ou da ferramenta estudadas que poderão ou não ser superadas. É importante que o autor não apresente conclusões que o trabalho não evidencie. Isso pode denotar uma fragilidade de argumentação e falta de conhecimento do conteúdo desenvolvido, implicando em questionamentos mais contundentes por parte dos professores da banca. O autor não deve fazer conjecturas com base em suposições ou dados inexistentes. É sempre mais prudente usar como conclusão o que a literatura técnica da área aponta como tendência futura ou prova através de dados concretos. Nenhum tipo de citação direta ou indireta e listas com marcadores ou numeração podem ser utilizadas nesta seção.

**Referências Bibliográficas**

ANDRADE, Inês Barcellos de; ABREU, Annelise Maria de Oliveira Wilken de; LIMA, Maria Cristina Miranda (orgs.). **Manual para elaboração e apresentação de artigo científico.** Campos dos Goytacases/RJ: FMC, 2013

BRAZIELLAS, Maria de Lourdes Motta; ANÇÃ, Nelza Maria Moutinho. **Normas para Apresentação de Trabalho de Conclusão de Curso, Monografia, Dissertação e Tese**. Rio de Janeiro: Editora Gama Filho, 2010. Disponível em <http://pt.scribd.com/doc/67274660/NORMAS-ACADEMICAS-UGF>. Acesso em 18 jan. 2017.

FURASTÉ, Pedro Augusto. **Normas técnicas para o trabalho científico: explicação das normas ABNT**. Porto Alegre: Dáctilo Plus, 2012.

GEORGIOS, Yiannakas. ***Critical Comparison and Evaluation of the Major MVC Frameworks through the use of a Prototype Web Application*.** 2011. 87p. Dissertação de Mestrado. Edimburgo, Edinburg Napier University, 2011.

LAKATOS, Eva M.; MARCONI, Marina A. **Metodologia Científica**. 6 ed. São Paulo: Atlas, 2011.

MACHADO, Felipe N. R. **Tecnologia e Projeto de *Data Warehouse***. 5 ed. São Paulo: Érica, 2012.

MICROSOFT. **Tutorial de mineração de dados básico**. 2016. Disponível em <https://technet.microsoft.com/pt-br/library/ms167167.aspx>. Acesso em 18 jan. 2017.

PMI - *Project Management Institute*. **Um guia do Conjunto de Melhores Práticas em gerenciamento de Projetos (Guia PMBOK) 5ª Edição**. Atlanta: PMI *Book Service Center*, 2013.