DOI: 10.18605/2175-7275/cereus.v10n4p182-197

<<Recebido: 05/10/2018. Aceito: 28/11/2018>>

ARTIGO ORIGINAL

REVISTA CEREUS ISSN: 2175-7275

Um Estudo Sobre a Epidemia de Vírus Computacionais no Poder Judiciário do Tocantins

A Study on the Computer Virus Epidemic in the Judicial Power of Tocantins

Danillo Lustosa Wanderley[1], João Carlos Vilela Batello[2], David Nadler Prata[3], Gentil Veloso Barbosa[4]

[1] Especialista, Universidade Federal do Tocantins.

E-mail:

danillo.lustosa@mail.uft.edu.br

[2] Especialista, Universidade Federal do Tocantins.

[3] Doutor, Universidade Federal do Tocantins.

[4] Doutor, Universidade Federal do Tocantins.

RESUMO

A segurança da informação não é processo acabado e pronto. Pelo contrário, é um processo que está sempre em evolução. Mesmo implementando-se mecanismos como *firewall* e antivírus, não significa que o ambiente computacional esteja totalmente seguro. É de fundamental importância proteger os pontos de extremidade da rede, de modo que esta continue a funcionar mesmo estando sob ataque. Assim, este estudo apresentará uma discussão acerca das principais ameaças à segurança da rede do Poder Judiciário do Tocantins, identificando suas ocorrências, os possíveis danos e as formas de contágio das estações de trabalho. Para tanto, foi utilizado o modelo epidemiológico SIR, desenvolvido por Kermack e McKendrick (1927). Após a realização do estudo, evidenciou-se que uma das principais ameaças é o uso inadequado do recurso computacional por parte dos usuários.

Palavras-Chave: Modelagem de Epidemias. Código Malicioso. Segurança da Informação.

ABSTRACT

The security of information is not process finished and Ready. On the contrary, it is a process that is always evolving. Even if you implement mechanisms such as firewall and antivirus, it does not mean that the computational environment is completely secure. It is of paramount importance to protect the network endpoints so that it continues to function even though it is under Attack. Thus, this study will present a discussion about the main threats to the security of the Judiciary network of Tocantins, identifying its occurrences, the possible damage and the forms of contagion of the Workstations. For this purpose, the SIR epidemiological model was used, developed by Kermack and McKendrick (1927). After the study was carried out, we showed that one of the main threats is the inadequate use of the computational resource on the part of the users.

Keywords: Epidemic Modeling. Malicious Code. Information Security.

1. INTRODUÇÃO

As redes corporativas e seus ativos sofrem constantes ataques de invasores, o que pode comprometer computadores, servidores e programas, causando interrupções em serviços essenciais das empresas.

Com ciberataques cada vez mais sofisticados, as empresas devem estar atentas para a adoção de soluções de segurança de modo a prevenir os perigos vindos da Internet e, com isso, proteger os pontos de extremidade da rede. Entende-se por pontos de extremidade todos os dispositivos nos quais o trabalho é realizado, ou seja, servidores, estações de trabalho e dispositivos móveis (GRIFFIN, 2018).

Para proteção dos pontos de extremidade é necessário garantir que eles estejam utilizando as mais recentes tecnologias de defesas contra ameaças. Um exemplo de contramedida a ameaças digitais são os *softwares* antivírus.

Segundo Nascimento (2015), os vírus e outras ferramentas de sabotagem digitais estão sempre alguns passos à frente das medidas de defesa, burlando as regras de *firewall* e os mecanismos de detecção dos antivírus, tornando frequentes as invasões às redes corporativas.

A segurança da informação não é processo acabado e pronto. Pelo contrário, é um processo que está sempre em evolução. Mesmo implementando-se mecanismos como *firewall* e antivírus, não significa que o ambiente computacional esteja totalmente seguro. Assim, é preciso desenvolver políticas de segurança empregando todos os mecanismos de proteção disponíveis, e o comprometimento do usuário a essa política é de fundamental importância.

A vulnerabilidade de uma rede é inversamente proporcional ao grau de comprometimento de cada um de seus usuários (NASCIMENTO, 2015). Quanto mais o usuário estiver integrado aos processos de segurança, mais segura será a navegação na rede interna e na Internet.

O órgão do Poder Judiciário onde o estudo foi realizado conta com aproximadamente 2.500 estações de trabalho que estão divididas entre o Tribunal e as Comarcas. A principal justificativa para realização deste estudo é que a existência de ataques provocados por objetos de código malicioso pode causar riscos às informações, como perda de arquivos importantes, exploração de informações sigilosas e atraso na execução de tarefas, devido a problemas na rede, como lentidão e parada de sistemas.

Nesse sentido, este trabalho propõe apresentar as principais ameaças à rede do Poder Judiciário do Tocantins, identificando suas ocorrências, os possíveis danos e as formas de contágio das estações de trabalho.

Para tanto, foi utilizado o modelo epidemiológico SIR, desenvolvido por Kermack e McKendrick (1927), no qual cada indivíduo, considerado saudável, neste trabalho representado por um computador, pode ser suscetível à infecção (S), infectado (I) e assim transmitir a doença a indivíduos saudáveis e removidos (R), que não têm a doença nem podem transmiti-la, pois adquiriram imunidade.

Dessarte, além de apresentar as ameaças e ataques ocorridos na rede, este trabalho tem o objetivo de identificar suas causas e as formas de como conter tais ameaças à segurança da informação.

2. REFERÊNCIAL TEÓRICO

Segundo Azevedo (2013), os vírus de computador são preparados para ter um comportamento igual aos vírus biológicos, porque são desenvolvidos para enviar cópias de si mesmos, na tentativa de se espalharem para outros computadores.

O autor ainda afirma, em termos mais populares, que os vírus informáticos são comparados aos vírus biológicos, fazendo analogia entre os computadores e o corpo humano, atribuindo assim uma visão humanizada ao computador como se tratasse de um corpo vulnerável a doenças virais.

O uso de modelos matemáticos no controle de doenças tornou a teoria mais próxima da prática; dessa maneira, vários modelos foram criados buscando o entendimento do comportamento da dinâmica epidemiológica (LUIZ, 2012). Tais modelos são ferramentas matemáticas desenvolvidas para estudar e entender os diversos tipos de comportamentos, podendo ser aplicados a qualquer tipo de sistema físico ou biológico para investigação da modelagem de doenças infecciosas (VIEIRA, 2017).

Os modelos epidemiológicos têm-se mostrado uma importante ferramenta para compreender e analisar o comportamento das epidemias. O modelo SIR, proposto por Kermack e Mckendrick em 1927, é um dos modelos mais utilizados para representação de doenças infecciosas. Nesse modelo os indivíduos são divididos em três classes:

- Suscetíveis (S): indivíduos que estão sujeitos a contrair a doença quando em contato com os infecciosos;

- Infectados (I): indivíduos portadores e com capacidade de transmitir a doença para os suscetíveis;
- Removidos (R): indivíduos que após contraírem a doença adquirem imunidade e perdem a capacidade de transmissão da doença.

O modelo clássico SIR descreve a propagação de uma doença infecciosa ao longo do tempo e considera que a distribuição de indivíduos é espacial e temporalmente homogênea. A forma de contágio nesse modelo é probabilística e ocorre por meio de arestas com os vizinhos (FIGUEIREDO, 2011).

Segundo Cecconello et al. (2012), nesse modelo, são analisadas, ao longo do tempo, as quantidades de indivíduos nas três categorias, levando-se em consideração que alguns dos suscetíveis adquirem a doença ao entrar em contato com indivíduos infectados da população. Além disso, com o passar do tempo, os infectados adquirem imunidade, deixando assim de contribuir para a propagação da doença.

Ainda segundo este mesmo autor, desde o modelo proposto por Kermack e McKendrick, diversos outros modelos têm sido propostos para descrever a propagação de uma epidemia em uma população.

> No modelo compartimental do tipo SI, a população é dividida em suscetíveis e infecciosos e este modelo é adequado quando são consideradas doenças transmissíveis de caráter crônico, para as quais os indivíduos infecciosos não voltam a ser suscetíveis nem se recuperam da infecção. Nos modelos do tipo SIS, os infecciosos se recuperam da infecção tornando-se suscetíveis à doença novamente. Já no modelo do tipo SIRS os infecciosos adquirem imunidade temporária, tornando-se suscetíveis com a evolução no tempo (CECCONELLO et al., 2012, p. 79).

A Figura 1 mostra uma população de tamanho constante, $N > 0$, subdividida nas três classes citadas no modelo: suscetíveis, infectados e removidos. Pode-se observar que, no primeiro momento, todos os indivíduos da rede estão sujeitos (S – suscetíveis) a contrair a doença quando em contato com os infectados. Após o contato com os infectados, que são aqueles portadores e com capacidade de transmitir a doença, mais indivíduos da rede contraem-na. Com o passar do tempo e com a adoção de contramedidas para barrar a infecção, os indivíduos que contraíram a doença adquirem imunidade, perdem a capacidade de transmissão e passam a formar a classe dos removidos.

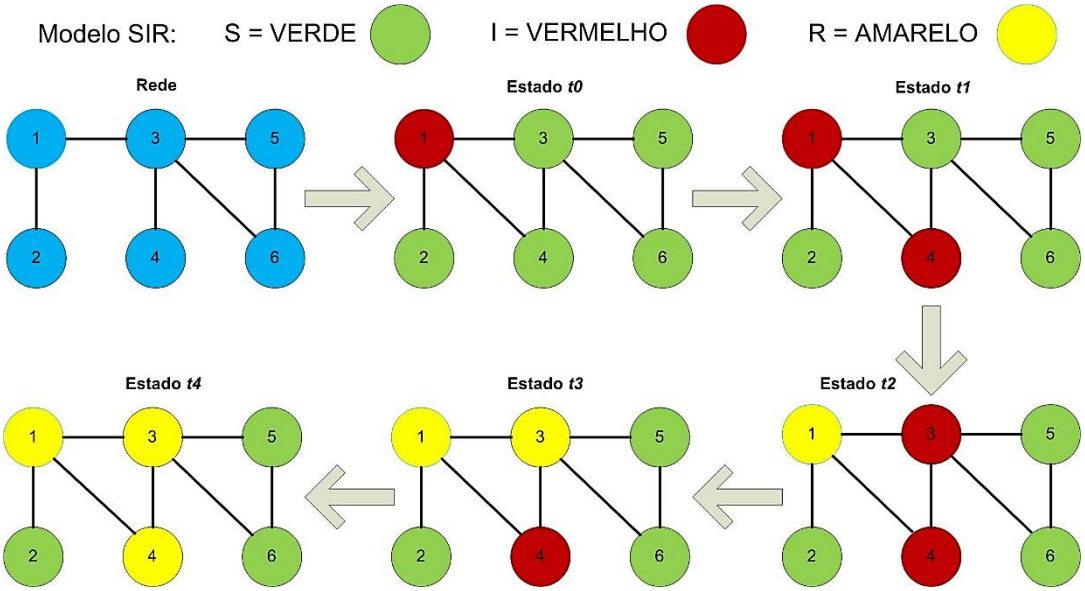

Figura 1. Representação conceitual do modelo SIR. Adaptado de Figueiredo (2018).

3. MATERIAIS E MÉTODOS

Este trabalho de pesquisa foi realizado no Poder Judiciário do Tocantins com abordagem qualiquantitativa do tipo exploratória e descritiva. Segundo Silva; Menezes (2005), a pesquisa exploratória envolve levantamento bibliográfico, entrevistas com pessoas que tiveram experiências práticas com o problema pesquisado, entre outros. Já a pesquisa descritiva visa descrever as características de determinada população ou fenômeno e envolve o uso de técnicas padronizadas de coleta de dados: questionários, planilhas, entrevistas ou observações.

Para o estudo em questão, fez-se uma revisão bibliográfica com vista a apresentar um embasamento teórico sobre o assunto tratado, dando mais ênfase ao modelo epidemiológico que foi utilizado para descrever as formas de contágio das estações de trabalho.

Os dados foram levantados por meio de pesquisa documental, sendo os relatórios gerados pela solução corporativa de antivírus a principal fonte de pesquisa utilizada, nos meses de junho a julho de 2018. A análise dos dados se deu à luz da literatura pertinente e foram realizadas discussões acerca das particularidades.

Os materiais literários foram coletados por buscas em bases ACM, IEEE e *google* acadêmico, durante o mês de junho de 2018, e utilizados os seguintes descritores para a pesquisa: modelagem de epidemias, código malicioso, segurança da informação.

Foram considerados como critérios de seleção dos materiais literários do estudo: a) sem delimitação do tempo de publicação; b) conteúdo relacionado à modelagem de epidemias, código malicioso e segurança da informação; c) idiomas português e inglês.

Durante a análise dos relatórios apresentados pela solução de antivírus, percebeu-se uma forte relação entre computadores infectados e dispositivos de armazenamento externo, ou seja, a dinâmica da infecção em sua maior parte era derivada dessa relação. Atualmente esses dispositivos representam uma das principais fontes de propagação de vírus de computador.

Uma única estação de trabalho apresentou 69 arquivos infectados pelo *malware* *Trojan.WinLNK.Agent.qg*. Na análise do relatório de ameaças, verificou-se que a infecção foi originada pelo uso de um dispositivo USB infectado. Nesse caso, após a utilização de medidas de precaução de imunização em tempo real, todos os arquivos foram recuperados.

Para a estação de trabalho citada anteriormente, pode-se representar o caminho de transição de estado da seguinte forma:

Figura 2. Transição de um indivíduo da rede para o estado removido.

Uma situação detectada foi a de estações de trabalho as quais se encontravam em estado crítico em virtude de o aplicativo de segurança estar desatualizado há bastante tempo. Isso acontecia principalmente por problemas de comunicação com o servidor de administração ou com o acesso ao servidor de rede que é utilizado como repositório dos arquivos de atualização do banco de dados do aplicativo.

Nessas estações de trabalho, detectou-se a presença de um *malware* denominado *Trojan.JS.Miner.m* que foi baixado da Internet por meio do acesso a páginas *web* que continham *exploits*. Como o aplicativo de segurança estava com mau funcionamento, este *malware* não foi neutralizado. Então, o caminho de transição de estado é representado da seguinte maneira:

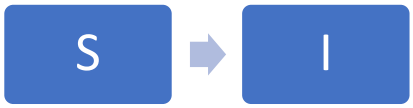

Figura 3. Transição de indivíduos da rede para o estado infectado.

Para sanar o problema, o aplicativo de segurança dessas estações foi reinstalado, e sua base de dados, atualizada. Após a realização da tarefa de verificação completa, o programa de código malicioso foi removido. Dessa maneira, representa-se o caminho de transição de estado, conforme figura abaixo:

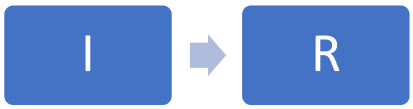

Figura 4. Transição de indivíduos da rede do estado infectado para removido.

3. RESULTADOS e DISCUSSÃO

Esta seção faz uma discussão dos resultados obtidos pelos relatórios da solução corporativa de antivírus utilizados pelo órgão do Poder Judiciário, sendo possível identificar as principais ameaças e ataques sofridos pelas estações de trabalho.

A Figura 5 apresenta os *malwares* mais representativos em termos percentuais detectados pela solução corporativa de antivírus. Por questão de simplicidade, são apresentados apenas os mais expressivos.

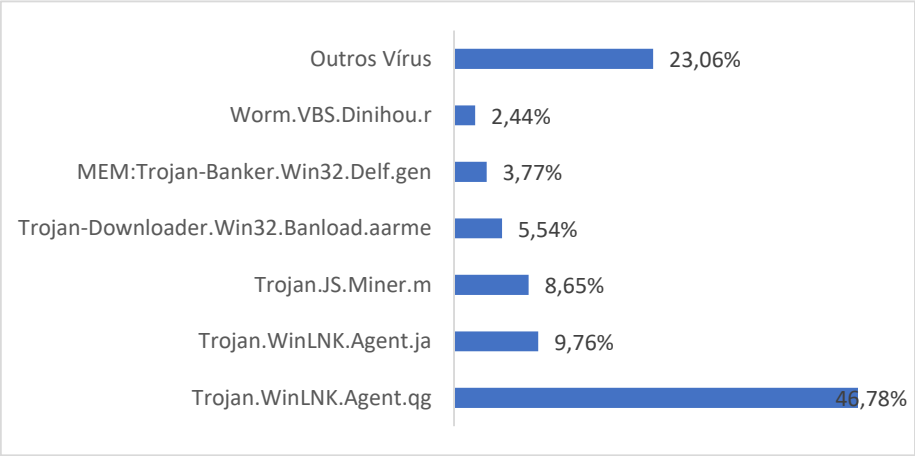

Figura 5. Ameaças com maior número de ocorrências.

Pode-se observar na Figura 5 que o *Trojan.WinLNK.Agent.qg* representa 46,78% da infecção. O *Trojan.WinLNK.Agent.ja* aparece como o segundo *malware* que mais infectou as estações de trabalho, com 9,76%. Esses *malwares* baixam arquivos maliciosos ou contêm um arquivo executável mal-intencionado, projetado para destruir, bloquear, modificar ou copiar dados, interferindo assim na operação de computadores ou redes de computadores.

O *Trojan.JS.Miner.m* foi responsável por 8,65% das infecções. Ele pode incluir nas estações de trabalho programas maliciosos com *scripts* JS usados para mineração de moeda criptografada sem o conhecimento do usuário.

O *Trojan-Downloader.Win32.Banload.aarme*, com 5,54% das infecções, tem como característica se instalar nas estações por meio do acesso a *sites* da Internet que contêm *exploits*. Outro *malware* que também causou problemas foi o *MEM:Trojan-Banker.Win32.Delf.gen*. Esse *malware* rouba os dados bancários do usuário pela instalação de programas *spyware* que são ativados quando *sites* de Internet *Banking* são acessados. Os dados são então transmitidos ao usuário mal-intencionado que controla o *trojan*. E-mail, FTP, a *web* ou outros métodos podem ser usados para transitar os dados roubados.

Já o *Worm.VBS.Dinihou.r* é classificado como vírus que pesquisa redes de computadores remotas e copia a si mesmo para diretórios que são acessíveis para leitura/gravação. Ademais, esses *worms* usam funções integradas do sistema operacional para procurar diretórios de rede acessíveis e/ou pesquisam aleatoriamente computadores na Internet, conectam-se a eles e tentam obter acesso total aos discos destes. Esse *malware* foi responsável por 2,44% das infecções.

Além dos *malwares* citados, foram detectados mais 45 outros diferentes que, devido ao pequeno número de ocorrências, não foram relacionados na discussão. Entretanto, ao somar todas as ocorrências desses *malwares,* chegou-se a um total de 23,06% das infecções. Podem-se destacar alguns pela relevância do dano que podem causar. São eles:

- *Exploit*: programas que contêm dados ou códigos executáveis que tiram proveito de uma ou mais vulnerabilidade em *softwares* executados num computador local ou remoto para propósitos claramente maliciosos. Os *exploits* são comumente usados por *Net-Worms* para *hackear* um computador da vítima sem que seja necessária alguma ação do usuário;
- *Trojan-Ransom*: esse tipo de cavalo de troia modifica os dados no computador da vítima para que não possa mais usá-los ou impede que o computador seja

executado corretamente. Depois que os dados são "tomados como reféns" (bloqueados ou criptografados), o usuário receberá uma solicitação de resgate;

- *Rootkit*: esse tipo de programa malicioso é projetado para ocultar certos objetos ou atividades no sistema. É usado para impedir que programas mal-intencionados sejam detectados;
- *Backdoor*: são projetados para permitir que usuários mal-intencionados controlem remotamente o computador infectado. Esses tipos de programas mal-intencionados possibilitam fazer qualquer coisa que o autor queira no computador infectado: enviar e receber arquivos, iniciar arquivos ou excluí-los, exibir mensagens, excluir dados, reinicializar o computador etc. São frequentemente usados para unir um grupo de computadores de vítimas e formar uma rede de *botnets* ou zumbis. Isso dá aos usuários mal-intencionados controle centralizado sobre um exército de computadores infectados que podem ser usados para fins criminosos.

A Figura 6 representa uma epidemia em rede, em que as estações de trabalho simbolizadas pelos círculos verdes foram infectadas pelos *malwares* definidos por esferas amarelas. Pode-se observar uma concentração de ataques do *Trojan.WinLNK.Agent.qg* no canto superior esquerdo da Figura 6. Esses ataques, como apresentado na Figura 5, representaram 46,78% das ocorrências.

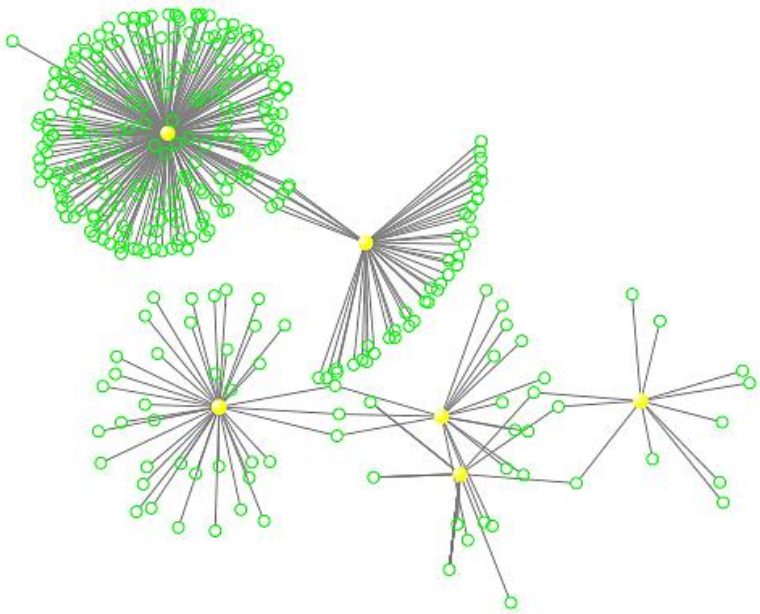

Figura 6. Rede de infecções causadas pelos *malwares* apresentados na figura 5. As estações de trabalho estão representadas pelos círculos verdes e os *malwares* pelas esferas amarelas.

Pode-se entender o *malware Trojan.WinLNK.Agent.qg* como uma ameaça *offline*, pois utilizam os dispositivos USB (*pendrives*, HDs externos), CDs e DVDs contaminados para disseminar programas de códigos maliciosos. Os *trojans* "WinLNK" são ícones de falsos arquivos do Sistema Operacional Windows potencialmente maliciosos que infectam após a efetivação de um duplo clique no arquivo.

Ao se analisar os relatórios da solução de segurança, um fato que chamou a atenção foi o número de infecções causadas pela utilização de “cracks” para a ativação de *softwares*. Vale ressaltar que um “crack” pode apresentar código malicioso que agirá silenciosamente no dispositivo infectado e pode causar dano não somente a este, mas a toda a rede.

Ainda na Figura 6, é possível observar que muitas estações de trabalho sofreram a infecção de dois ou mais *malwares* diferentes, como no caso do *MEM:Trojan-Banker.Win32.Delf.gen*, ilustrado na Figura 8, e do *Trojan.JS.Miner.m*, na figura 10, os quais se utilizam de *Java Script* para realizar seus ataques. Para aplicar os golpes, *hackers* modificam páginas na *web* e incluem um código em *Java Script* a ser executado no navegador. Esse tipo de ataque é transparente para o usuário que acaba não percebendo que o dispositivo está sendo infectado.

Nas Figuras de 7 a 12 serão apresentados, de forma visual, os ataques dos 6 tipos de ameaças com maior número de ocorrências. Os ataques de cada um dos *malwares* estão destacados na cor vermelha.

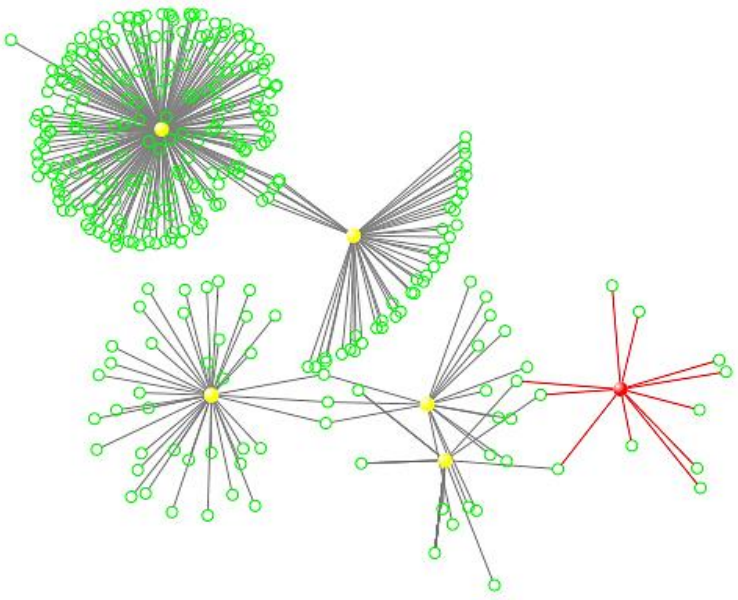

Figura 7. Rede de infecção causada pelo *malware Worm.VBS.Dinihou.r*.

Conforme relatórios analisados, percebeu-se que a infecção representada pelo *malware Worm.VBS.Dinihou.r* (Figura 7) foi resultado da cópia de uma série de arquivos infectados de um dispositivo USB para uma pasta compartilhada na rede e teve como origem um único usuário. Ao terem sido acessados, esses arquivos ocasionaram a infecção de outras máquinas.

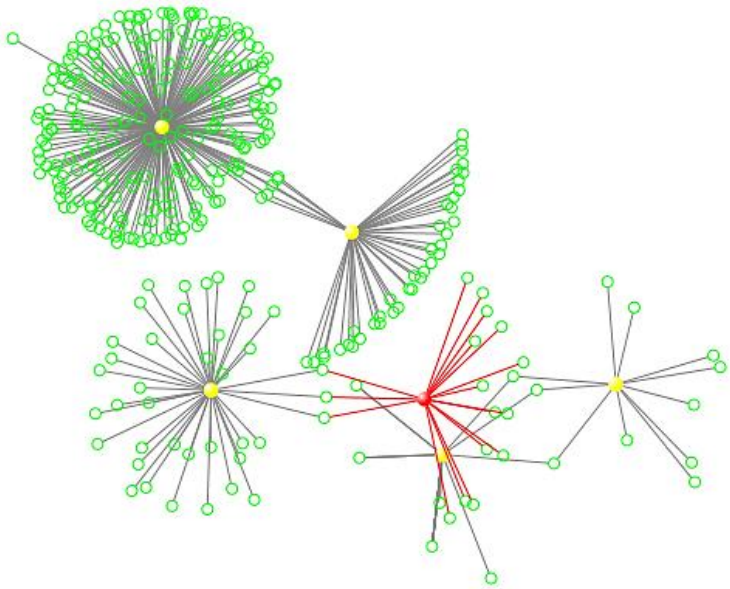

Figura 8. Rede de infecção causada pelo *malware MEM:Trojan-Banker.Win32.Delf.gen*.

A infecção destacada em vermelho na Figura 8 é resultado de acessos a *sites* que contêm programas de código malicioso e devido a *downloads* com arquivos infectados. A solução de antivírus, na maioria dos casos, conseguiu bloquear e/ou excluir essa ameaça. Em dois computadores nos quais os bancos de dados do aplicativo de segurança se encontravam desatualizados, essa ameaça não foi neutralizada. Somente após a atualização do banco de dados do aplicativo é que a ameaça foi removida dos computadores.

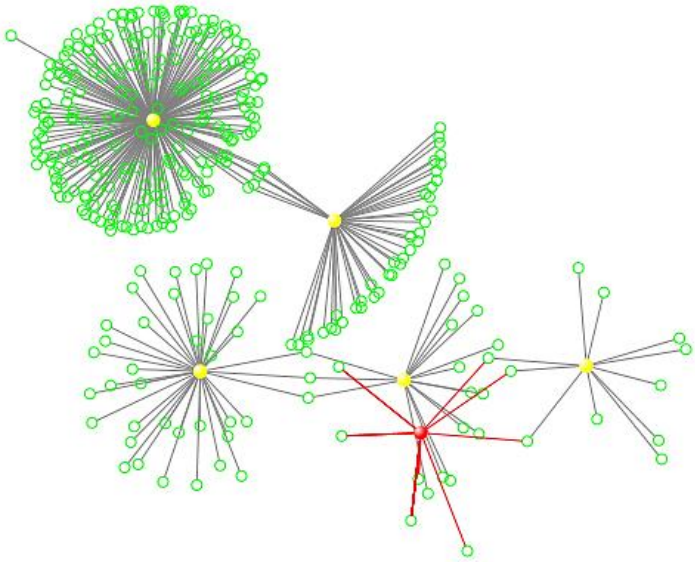

Figura 9. Rede de infecção causada pelo *malware Trojan-Downloader.Win32.Banload.aarme*.

O acesso a páginas *web* maliciosas e o *download* de arquivos obtidos nessas páginas foram a causa da infecção destacada na Figura 9.

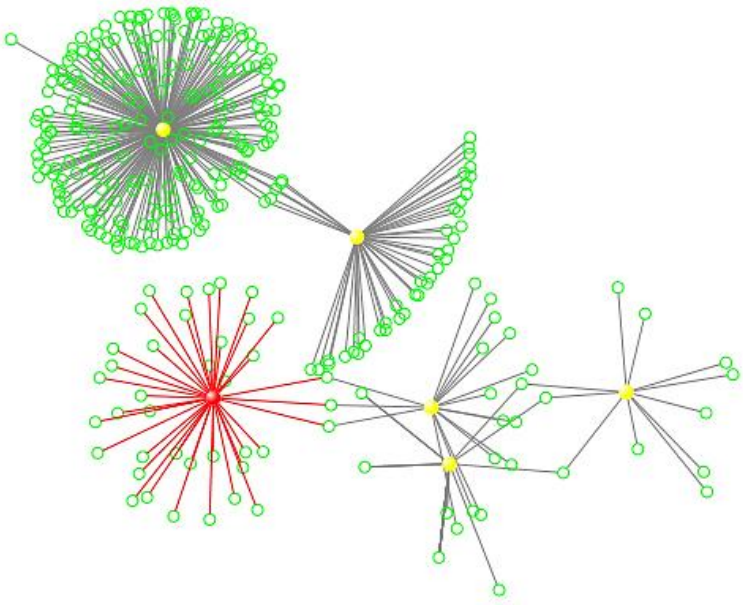

Figura 10. Rede de infecção causada pelo *malware Trojan.JS.Miner.m*.

Ao analisar o comportamento do *malware Trojan.JS.Miner.m*, em vermelho no canto inferior esquerdo da Figura 10, observou-se que a infecção também ocorreu de maneira semelhante à causada pelo *Trojan-Banker.Win32.Delf.gen*. Ambas aconteceram por meio de acessos a páginas *web* que continham programas de código malicioso. Cabe salientar que a solução de segurança não conseguiu neutralizar a ameaça em 59,4% das

ocorrências, pois as estações de trabalho infectadas apresentavam estado crítico devido à ausência de comunicação com o servidor de administração da solução. Essa limitação de comunicação ocasionou o mau funcionamento do aplicativo de segurança em razão de o banco de dados estar desatualizado.

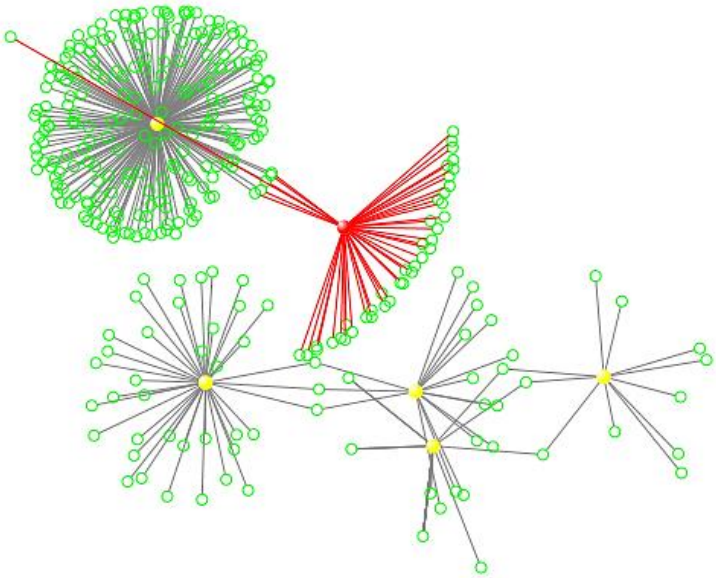

Figura 11. Rede de infecção causada pelo *malware Trojan.WinLNK.Agent.ja*.

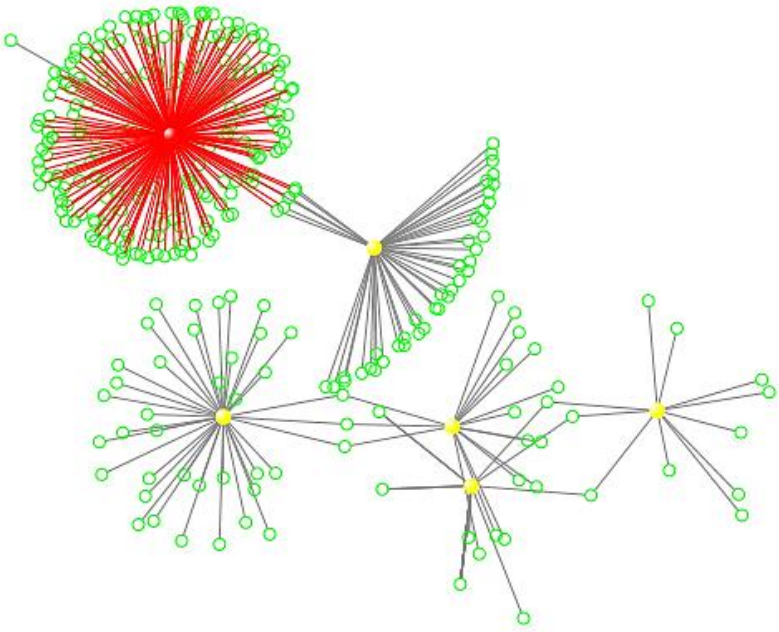

Figura 12. Rede de infecção causada pelo *malware Trojan.WinLNK.Agent.qg*.

Os *trojans* apresentados em vermelho nas Figuras 11 e 12 foram os responsáveis por 56% de toda infecção da rede. Em 96,5% dessas ocorrências, a solução de antivírus excluiu os arquivos infectados, e em 3,5%, os arquivos foram colocados em quarentena. Observou-

se que nas máquinas em que os arquivos foram colocados em quarentena, o aplicativo de segurança estava com o banco de dados desatualizado.

Mediante o estudo realizado, foi possível identificar as principais ameaças e ataques sofridos pelas estações de trabalho do Poder Judiciário do Tocantins. Na maioria das vezes, os ataques ocorreram por uso indevido do recurso computacional por parte dos usuários e por vulnerabilidades do Sistema Operacional Windows.

Com a análise dos relatórios da solução de antivírus, observou-se que vários arquivos infectados que continham fotos e músicas foram executados por uma mídia removível e houve acessos a páginas da Internet com conteúdo inadequado. Em geral, essas ações foram neutralizadas pelo aplicativo de segurança instalado nos computadores.

Nesse cenário, destaca-se a necessidade de manter as estações de trabalho com o sistema operacional atualizado, de modo a corrigir possíveis vulnerabilidades. Além disso, existem problemas no manuseio de dispositivos USB, sendo necessária a adoção de uma política de uso, de modo que os usuários possam fazer uma gestão mais cuidadosa dos meios de armazenamento externo.

4. CONSIDERAÇÕES FINAIS

Como a maior parte das operações do órgão do Poder Judiciário em questão é digital, tornou-se mais do que necessário proteger toda a rede, de modo a reduzir a exposição dos ativos a ameaças e ataques cibernéticos.

A solução de antivírus utilizada pelo órgão ajuda a fortalecer as estações de trabalho para torná-las resilientes aos ataques de *malwares* sem prejudicar o seu desempenho e a produtividade dos usuários. Ademais, simplifica o gerenciamento e aplicação das políticas de segurança a todas as estações, o que facilita as tarefas diárias dos administradores da rede.

Pela revisão bibliográfica realizada para dar embasamento teórico sobre o assunto tratado e pela pesquisa documental para levantamento dos dados, foi possível demonstrar no presente estudo os ataques de *malwares* nos ativos que integram a rede do Judiciário Tocantinense.

Foi possível concluir que os ataques na maioria das vezes ocorreram por conta de comportamentos inadequados dos próprios usuários, por causa do acesso indevido à Internet e do uso incorreto de dispositivos USB.

Segundo Alencar et al. (2013), as pessoas podem se tornar uma ameaça interna à segurança da informação por diversos motivos. Existem as que facilitam a ocorrência de um ataque à rede sem mesmo saber que estão cometendo algo errado, como também existem as que agem propositadamente e com finalidades específicas. Geralmente estas têm conhecimento dos processos internos da instituição, são chamadas de *insiders*.

Nesse sentido, é importante ressaltar o quanto a variável pessoa pode ser prejudicial para a Instituição, uma vez que a maioria dos incidentes, direta ou indiretamente, envolve a participação humana, gerando assim muitos prejuízos (ALENCAR et al., 2013).

Assim, a segurança da rede só será possível por meio da colaboração dos próprios usuários que devem fazer uso racional dos ativos. É extremamente importante que aqueles atuem de forma proativa, zelando pela segurança da informação.

Por fim, acredita-se que o fato de o usuário que tenha um melhor entendimento das ameaças e ataques de redes possa colaborar para uma mudança positiva em relação à segurança da informação. Isso modificaria o ambiente corporativo como um todo, pois criaria dificuldades para exploração de vulnerabilidades, diminuiria os riscos e aumentaria a segurança do ambiente.

REFERÊNCIAS

ALENCAR, Gliner Dias; QUEIROZ, Anderson A.L.; DE QUEIROZ, R. J. G. B**. Insiders:** Um Fator Ativo na Segurança da Informação**.** IX Simpósio Brasileiro de Sistemas de Informação (SBSI 2013), p. 61-72, 2013.

AZEVEDO, Rúben Manuel da Rocha. **Propagação de Vírus Informáticos Baseada em Modelos Biológicos.** Dissertação (Mestrado) – Instituto Superior de Engenharia do Porto, 2013. Disponível em: < http://recipp.ipp.pt/handle/10400.22/6519>. Acesso em: 28 jun. 2018.

CECCONELLO, Moisés S.; PEREIRA, Chryslaine M.; BASSANEZI, Rodney C. **Análise Qualitativa da Solução Fuzzy do Modelo Epidemiológico SIR.** Biomatemática, v. 22, p. 77-92, 2012.

DO NASCIMENTO, Janilson Pereira. **Segurança em Redes de Computadores:** Uma Abordagem sobre o Comprometimento Individual em Benefício da Corporação". Tecnologias em Projeção, v. 6, n. 1, p. 01-06, 2015.

FIGUEIREDO, Daniel R. **Introdução a redes complexas**. Atualizações em Informática, pg. 303-358, 2011.

FIGUEIREDO, Daniel R. **Redes Complexas Aula 15.** Disponível em: < http://www.land.ufrj.br/~daniel/rc/slides/aula_15_modelando_epidemia.pdf>. Acesso em: 11 jun. 2018.

GRIFFIN, Dan; **Network Security:** The Four Pillars of Endpoint Security. Disponível em: <https://technet.microsoft.com/en-us/library/gg213837.aspx>. Acesso em: 28 jun. 2018.

KERMACK, W. O. y MCKENDRICK, A.G. (1927). **Contributions to the Mathematical Theory of Epidemics THE ROYAL SOCIETY. Proceedings of the Royal Society of London A**: mathematical, physical and engineering sciences. [S.l.], 1927. v. 115, n. 772, p. 700–721.

LUIZ, M.H.R**. Modelos Matemáticos em Epidemiologia**, IGCE/UNESP, Rio Claro, 2012.

SILVA,E.L.DA; MENEZES. E.M. **Metodologia da Pesquisa e Elaboração de Dissertação.** UFSC, 4. ed. Ver. Atual. Florianópolis 2005.

VIEIRA, Gustavo Borges. **Teoria Qualitativa e Estabilidade de Lyapunov para Sistemas de Equações de Ordem Fracionária e uma Aplicação em um Modelo SIR-SI para a Dengue.** UFAL, Alfenas, 2017.