XXXIII Congresso de Iniciação Científica da Unicamp

APLICAÇÃO DE SISTEMAS MULTIAGENTES NA GOVERNANÇA DE TI PARA RESPOSTA A ATAQUES DE RANSOMWARE INICIADOS POR DISPOSITIVOS IoT

Palavras-Chave: Ransomware, Sistemas Multiagente, Governança de TI

Autores(as):
José Mayco Leite Nunes, FATEC Americana
Marcelo Henrique da Costa Marinho, FATEC Americana
Prof. Dr. João Emmanuel D Alkmin Neves, FATEC Americana

INTRODUÇÃO:

À medida que a tecnologia se torna mais acessível e disseminada, cresce também a frequência de ataques cibernéticos, especialmente em razão do aumento de dispositivos conectados. A expansão da Internet das Coisas (IoT) tem desempenhado papel central nesse cenário, criando novos vetores de ataque tanto em ambientes domésticos quanto corporativos. Estima-se que o número de dispositivos IoT conectados, que era de 18,8 bilhões, alcançará 40 bilhões até 2030 (Sinha, 2024).

Esse crescimento amplia significativamente a superfície de ataque e impõe desafios críticos à Segurança da Informação. A IoT tornou-se um vetor promissor para cibercriminosos, sendo frequentemente alvo de *malwares* simples e automatizados (IBM, 2020). Essa vulnerabilidade decorre, em grande parte, das limitações de *hardware* desses dispositivos, que dificultam a aplicação de soluções tradicionais de proteção, como antivírus robustos (EMBROKER, 2025).

O risco se intensifica em setores críticos, como a Agricultura de Precisão, onde a dependência de dispositivos IoT para automação torna a operação suscetível a falhas sistêmicas e interrupções severas. Entre os ataques mais prejudiciais, destaca-se o *ransomware*, que compromete o acesso a dispositivos e exige pagamento para restaurá-los. Mesmo assim, os dados podem ser perdidos ou expostos, resultando em prejuízos financeiros de US$ 2,74 milhões por incidente (FBI, 2021).

Apesar da relevância desses riscos, muitas organizações ainda carecem de mecanismos para simular, prever e responder a ataques complexos, sobretudo aqueles originados via IoT. Nesse cenário, a Governança de Tecnologia da Informação (GTI), conforme definido pelo COBIT 5, torna-se fundamental para alinhar prioridades de segurança, monitorar riscos e estruturar respostas a incidentes (ISACA, 2019). Diante desse cenário, este estudo propõe o uso de simulações baseadas em Sistemas Multiagentes (SMA) como ferramenta de apoio à Governança de TI. De acordo com Neves (2024), SMA são modelos computacionais formados por múltiplos agentes autônomos que interagem entre si e com o ambiente, sendo capazes de representar comportamentos complexos e dinâmicos. Neste trabalho, os

SMA são utilizados para modelar, observar e analisar a propagação de ataques de ransomware originados a partir de dispositivos IoT.

A hipótese central é que simulações multiagentes podem reproduzir, de forma realista e controlada, interações entre agentes maliciosos, sistemas vulneráveis e mecanismos de defesa, permitindo avaliar a eficácia de diferentes estratégias de mitigação no contexto da governança.

O objetivo geral da pesquisa é desenvolver um modelo de simulação multiagente para representar cenários de infecção por *ransomware* com IoT como vetor inicial, a fim de fornecer subsídios à tomada de decisão na gestão de riscos cibernéticos.

Justifica-se este estudo pela crescente complexidade dos ambientes digitais e pela insuficiência de abordagens convencionais em lidar com ameaças adaptativas. A abordagem proposta visa contribuir para práticas mais dinâmicas de avaliação de risco, preparação e resposta, alinhadas aos princípios da governança moderna e às demandas emergentes da Segurança da Informação.

METODOLOGIA:

Esta pesquisa é classificada como aplicada, de natureza exploratória e abordagem qualitativa, com fundamentação em revisão bibliográfica e simulação computacional baseada em agentes utilizando a plataforma NetLogo. O modelo simula o comportamento dinâmico de um ataque do tipo *ransomware* em uma rede corporativa segmentada, incluindo dispositivos IoT, refletindo diferentes níveis de maturidade em Segurança da Informação. A simulação representa uma rede corporativa contendo diferentes tipos de agentes:

- Agentes Ativos: dispositivos IoT, servidores e endpoints.
- Agentes Maliciosos: ransomware com parâmetros configuráveis.
- Agentes Defensivos: monitoramento, resposta e recuperação.

A simulação contempla três níveis de variáveis de entrada (tempo de propagação e nível de ataque) e quatro perfis organizacionais de maturidade em segurança, conforme o NIST Cybersecurity Framework (2024). A Tabela 1 mostra essas informações.

Tabela 1 – Níveis de maturidade do NIST na simulação

Nível	Descrição	Recursos de Segurança Simulados
Tier 1	Informal, sem processos definidos	Sem backup, sem subredes, sem técnico de recuperação
Tier 2	Práticas parcialmente documentadas	Backup local, sem subrede, com técnico de recuperação
Tier 3	Maturidade formalizada	Backup local, com subrede, com técnico de recuperação
Tier 4	Adaptativo, com melhoria contínua	Backup local e em nuvem, com subrede e técnico de recuperação

Fonte: Autores (2025)

Três cenários principais foram definidos, variando o tipo de ataque e o nível organizacional, conforme exibido na Tabela 2.

Tabela 2 – Configurações dos cenários simulados

Cenário	Tier NIST	Nível de Ataque	Propagação (ticks)
1	Tier 1	1 (baixo)	100 (rápido)
2	Tier 3	3 (médio)	500 (média)
3	Tier 4	5 (alto)	2000 (lenta)

Fonte: Autores (2025)

Nos testes, a rede simulada possuía 5 computadores, 9 dispositivos IoT, 1 *data center*, 1 roteador e 1 dispositivo inicialmente infectado. Cada cenário foi executado 15 vezes. As variáveis incluíram:

- Número de ativos infectados
- Tempo até contenção (em ticks)
- Ocorrência de falhas totais
- Efetividade de antivírus e backups
- Impacto da segmentação de rede

RESULTADOS E DISCUSSÃO:

Os resultados demonstraram como diferentes combinações de maturidade organizacional e perfis de ataque impactam o sucesso da resposta a incidentes de *ransomware*. Exibido na Tabela 3.

Tabela 3 – Médias dos principais indicadores por cenário

Métrica	Cenário 1 (Tier 1)	Cenário 2 (Tier 3)	Cenário 3 (Tier 4)
% de ativos infectados	80%	45%	8%
Tempo até contenção (ticks)	430	260	85
Falhas totais (por 15 simulações)	9	3	0
Recuperação via backup	0%	53%	87%

Fonte: Autores (2025)

Observou-se que, quanto mais elevado o nível de ataque, menor a chance de detecção por antivírus, o que reforça o risco de ataques *stealth*. Em contrapartida, ataques com propagação rápida foram mais facilmente identificados e contidos pelos mecanismos de monitoramento, revelando uma relação inversa entre velocidade e letalidade. Apesar da presença de antivírus em todos os cenários, sua eficácia se mostrou limitada, especialmente nos ataques de nível 5, validando estudos como o de Beaman *et al.* (2021), que apontam falhas recorrentes em ferramentas de detecção frente a variantes modernas de *ransomware*. A segmentação de rede demonstrou ser a medida mais eficaz para impedir a movimentação lateral do *malware*. Já o uso de *backups*, quando disponível, foi determinante para garantir a continuidade dos serviços e evitar o pagamento de resgates. Observados na Tabela 4.

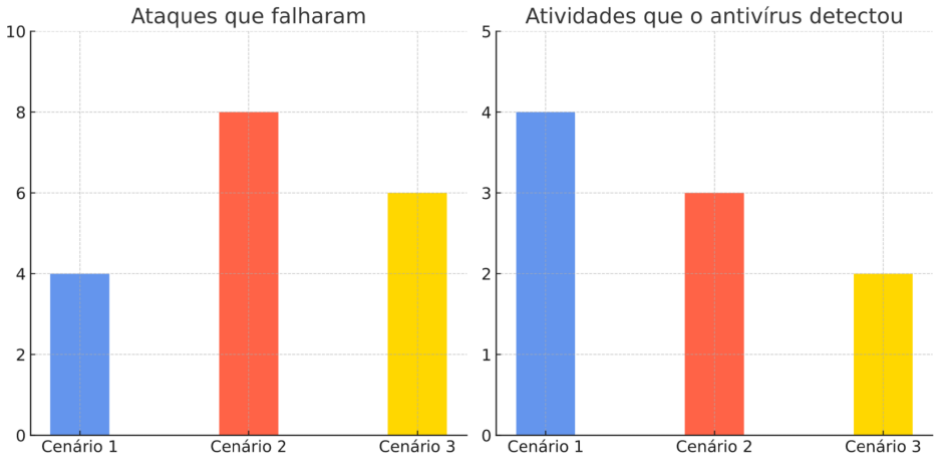
Tabela 4 – Impacto das medidas de segurança observadas

Medida de Segurança	Efeito Principal Identificado
Subredes	Redução significativa da movimentação lateral
Backup local	Redução do tempo de recuperação
Backup em nuvem	Mitigação do impacto em falhas totais
Antivírus	Eficaz apenas em ataques de baixo nível

Fonte: Autores (2025)

Os gráficos reforçam as limitações dos antivírus frente a ameaças sofisticadas. Enquanto o cenário 1 (Tier 1) apresentou 4, o maior número de detecções, cenários mais avançados, com ataques mais furtivos, reduziram essa eficácia. Por outro lado, o cenário 2 (Tier 3) teve 8, o maior número de ataques frustrados, sugerindo que o equilíbrio entre arquitetura defensiva moderada e ameaças menos furtivas pode resultar em melhor performance de detecção e resposta. De forma contraintuitiva, o cenário 3 (Tier 4), embora mais maduro, teve ligeiramente menos ataques frustrados, possivelmente devido à dificuldade de detecção associada ao *ransomware* de alto nível. Esses resultados demonstram que a maturidade organizacional por si só não é suficiente: a sofisticação das ameaças precisa ser considerada na formulação de políticas de segurança, e a defesa precisa ser adaptativa e multicamada. Essas considerações podem ser observadas na Figura 1.

Figura 1 – Gráficos das Simulações



Fonte: Autores (2025)

Além dos dados técnicos, a simulação permitiu explorar o dilema do pagamento de resgates sob a ótica da GTI. Organizações com baixa maturidade podem considerar essa opção como solução imediata, porém os riscos de não recuperação, vazamento e reincidência permanecem altos. Esses achados destacam a importância de práticas preventivas estruturadas, como segmentação de rede e políticas de *backup*, em detrimento da dependência exclusiva de soluções antivírus. A abordagem com SMA mostrou-se adequada para observar efeitos emergentes e avaliar políticas de segurança antes de sua implementação no ambiente real.

CONCLUSÕES:

Este trabalho demonstrou a crescente ameaça que os ataques de *ransomware* representam para as organizações, especialmente ao explorarem a expansão e as vulnerabilidades inerentes aos dispositivos IoT como vetor de entrada. Diante deste cenário, o estudo propôs e validou a hipótese de que SMA são uma ferramenta eficaz para modelar, simular e analisar diferentes estratégias de resposta a incidentes, servindo como um poderoso aliado para a GTI.

As simulações possibilitaram a obtenção de resultados relevantes para a gestão de riscos. Constatou-se que a segmentação da rede por meio de subredes foi a medida mais eficiente para conter a propagação do *malware*, dificultando a movimentação lateral do agente malicioso. Observou-se ainda que, embora soluções como antivírus desempenhem um papel importante, elas não oferecem uma proteção definitiva contra ameaças elaboradas. os dados obtidos destacaram a relevância dos *backups* como estratégia fundamental para mitigar perdas de dados e reduzir a dependência do pagamento de resgates, mesmo que não eliminem completamente o risco de exposição de informações sensíveis.

Com base nesses achados, conclui-se que o uso de SMA em simulações oferece um ambiente controlado e realista, no qual gestores de TI e segurança da informação podem avaliar com maior clareza o impacto de suas decisões e testar a eficácia de políticas de governança, como as sugeridas por *frameworks* reconhecidos, a exemplo do NIST. Tal abordagem contribui para uma tomada de decisão mais embasada e uma resposta a incidentes mais eficaz, promovendo o alinhamento entre os recursos de TI e os objetivos estratégicos da organização, além de fortalecer sua resiliência frente a ameaças cibernéticas cada vez mais sofisticadas.

BIBLIOGRAFIA

BEAMAN, C.; BARKWORTHA, A.; AKANDE, T. D.; HAKAk, S.; KHAN, M. K. **Ransomware:** Recent advances, analysis, challenges and future research direction**.** ScienceDirect, 2021. Disponível em: https://doi.org/10.1016/j.cose.2021.102490 Acesso em: 26 jun. 2025.

EMBROKER. **Top 16 cybersecurity threats in 2025.** San Francisco, Embroker Team, 2025. Disponível em: https://www.embroker.com/blog/top-cybersecurity-threats. Acesso em: 16 maio 2025.

FBI. **FBI How Can We Help You:** Ransomware. Washington, FBI, 2021. Disponível em: https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/ransomware. Acesso em: 24 maio 2025.

ISACA. **COBIT 2019**: Governança e Gestão de TI da empresa. Versão em português: ISACA, 2019. Disponível em: https://www.isaca.org/resources/cobit. Acesso em: 24 maio. 2025.

NEVES, J. E. D. **Mineração de dados aplicada a simulação de cenários complexos em sistemas multiagentes**. 2024. Disponível em: https://doi.org/10.47749/T/UNICAMP.2024.1395946. Acesso em: 14 jun 2025.

NIST. **The NIST CybersecurityFramework (CSF) 2.0.** Gaithersburg, NIST Cybersecurity White Paper, 2024. Disponível em: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29. Acesso em: 26 jun. 2025.

SINHA, S. **State of IoT 2024: Number of connected IoT devices growing globally.** 2024. Disponível em: https://iot-analytics.com/number-connected-iot-devices. Acesso em: 14 maio 2025.