Ataques Cibernéticos em Setores Críticos: Ambientes Colaborativos para a Segurança da Sociedade e Organizações

Lillian Rosemback[1], Daniele Sucena[2], Marcos Xavier[3], Paulo Victor[4], Alessandro Jatobá[5], Richard Guedes[6]

[1] Universidade Federal Fluminense (UFF), Estudante de Mestrado

[2] Universidade Federal do Rio de Janeiro (UFRJ), Estudante de Doutorado

[3] Ita House Informática Ltda. ME, Sócio Gerente

[4] Instituto de Engenharia Nuclear (IEN), Pesquisador

[5] Fundação Oswaldo Cruz (Fiocruz), Pesquisador

[6] Instituto de Defesa Cibernética (IDCiber), Presidente

(21)99961-9864, (21) 2391-5864, lilly.rosemback@gmail.com, danielesucena@ufrj.br, marcosxavier@ufrj.br, paulov@ien.gov.br, alessandro.jatoba@fiocruz.br, richardg7@outlook.com

Abstract. *In this article, some of the most emblematic cases of computer worms that have gained international prominence due to their ability to cause significant damage to systems in critical sectors are addressed, through a review of the narrative literature. With the increase in connections and digital environments, it becomes increasingly important to analyze and share information about cybersecurity through collaborative tools and social networks. As a challenge and solution, a successful case of collaboration in practice is presented that aims to benefit society, education and organizations, with the aim of promoting greater mobilization of authorities and the academic community.*

Resumo. *Neste artigo, são abordados alguns dos casos mais emblemáticos de worms de computador que ganharam destaque internacional devido à sua capacidade de causar danos significativos aos sistemas de setores críticos, através da revisão da literatura narrativa. Com o aumento das conexões e ambientes digitais, torna-se cada vez mais importante analisar e compartilhar informações sobre cibersegurança por meio de ferramentas colaborativas e redes sociais. Como desafio e solução, é apresentado um case de sucesso de colaboração na prática que visa beneficiar a sociedade, o ensino e as organizações, com o objetivo de promover maior mobilização das autoridades e comunidade acadêmica.*

1. Descrição do Problema: Quem sou?

No ano de 2010, veio à tona a descoberta de um vírus informático que se destacou por sua influência além dos limites do ambiente virtual, estendendo-se ao mundo real, e por reunir elementos de propagação global, proporcionando insights sobre possíveis cenários de incidentes no futuro. O StuxNet é um dos malwares globais mais prejudiciais e dispendiosos já conhecidos para atacar instalações nucleares. O incidente envolvendo o StuxNet representou um ataque bem-sucedido a infraestruturas críticas em países do Oriente Médio, e foi objeto de múltiplas investigações [Rocha, 2022]. O episódio do StuxNet destacou a importância de analisar essas ameaças cibernéticas, ou seja, estudar sua capacidade de dominar as tecnologias e desenvolver competências técnicas localmente para alcançar um domínio [Silva 2018].

Por volta de 2017, o WannaCry foi um ransomware que varreu a internet devido uma vulnerabilidade predominante em sistemas de saúde [Mennecier, 2020] que possibilitou que o ataque global do ransomware se espalhasse por vários hospitais no Reino Unido, afetando mais um segmento crítico que é a área da saúde e deixando vários pacientes sem atendimentos médicos, causando também grandes prejuízos financeiros. O Malware criptografava todos os dados dos sistemas alvejados e exigia um resgate financeiro em criptomoedas, fazendo jus, assim, ao nome dado a esse tipo de malware [Datta 2022].

Em 2022, durante a guerra entre a Rússia e a Ucrânia, um ataque cibernético promovido por grupos de hackers de diferentes países, atingiu uma estação elétrica ucraniana, causando um blecaute não planejado [Mueller, 2023]. O incidente, no entanto, evidenciou a vulnerabilidade das redes elétricas a ataques cibernéticos e a necessidade de medidas de segurança robustas para proteger infraestruturas críticas. Esse tipo de ataque ressalta a urgência de fortalecer as defesas cibernéticas e promover a cooperação internacional para mitigar os riscos associados à cibersegurança em infraestruturas críticas.

Diante da gravidade, é evidente a importância de proteger os ambientes críticos dos ataques cibernéticos capazes de comprometer os sistemas supervisórios [Sá, 2020]. Esses tipos de ataques cibernéticos, além de afetarem setores críticos, também são considerados em larga escala e especializados quando buscam ganhar controle e acesso não autorizado a sistemas-alvo em diversos países [Datta 2022]. Olhando para o Brasil em particular, o país vem sofrendo um número crescente de ataques cibernéticos [Cert 2023]. O conceito de infraestrutura crítica inclui ambientes de saúde, indústrias, usinas nucleares, transmissão de água, energia elétrica, e entre outros. Os setores críticos enfrentam potenciais riscos de sofrer interrupções, danos físicos, atividades de espionagem, incidentes radiológicos, perda de confiança do público, e muito mais. [Fernandes 2012].

Vivemos hoje uma corrida armamentista que lembra a época da guerra fria, onde os bits ocupam o lugar que antes era do Urânio e do Plutônio, levando algumas pessoas a acreditarem que o perigo é menor. No entanto, ao considerar o prejuízo que seria causado por um dia de operações paradas na bolsa de valores dos Estados Unidos, os danos causados pelas novas armas cibernéticas superam qualquer coisa. Com o avanço das tecnologias e a interconexão das cidades e sistemas de controle industrial, um operador cibernético pode causar sérios danos, e isso vem com um custo para a sociedade civil em geral. [Datta 2022]. Uma vez que uma arma cibernética é utilizada, pode tornar-se disponível para qualquer pessoa com conhecimento técnico ou para grupos de hackers mal-intencionados que realizam engenharia reversa ou social, e reaproveitam o mesmo tipo de malware para ganho pessoal.

Este trabalho empregou como metodologia de pesquisa uma revisão da literatura narrativa em bases confiáveis, incluindo uma análise dos principais casos de worms que ganharam destaque global devido ao potencial de causar danos significativos em infraestruturas críticas. Buscou-se construir uma narrativa coesa e coerente para a fundamentação teórica que conduz o leitor a uma compreensão mais profunda do tema. [Nascimento, 2022]. O objetivo é promover debates enriquecedores na comunidade acadêmica, visando beneficiar organizações de setores críticos e a sociedade, fazendo combinações e abordagens de uso inteligente das ferramentas colaborativas para promover a segurança da informação [Barbosa 2014].

2. Desafio: Qual o meu/nosso desafio?

Os ataques cibernéticos representam um desafio significativo em um contexto global e podem ocorrer desde pequenas escalas originados de fontes obscuras em redes sociais,

até em ataques combinados larga escala, capazes de afetar serviços essenciais de um país. Essa diversidade de ataques desafia a capacidade de garantir a segurança cibernética e pode expor infraestruturas críticas a sérios riscos, podendo desencadear crises sistêmicas em vários setores. A conscientização sobre a gravidade desses ataques muitas vezes é limitada, resultando em poucos estudos e investimentos insuficientes por parte do Estado, organizações, sociedade e academias. É importante reconhecer que os ataques cibernéticos afetam não apenas ambientes críticos, mas também causam prejuízos significativos na segurança de dados, serviços essenciais e até mesmo vidas humanas [Taquary, 2019].

3. Solução: Qual a nossa/minha solução?

Como proposta de solução, este resumo apresenta insights e combinações de abordagens com ferramentas colaborativas, utilizando o Moodle, um Ambiente Virtual de Aprendizagem (AVA) de código aberto, com um programa educacional de cursos gratuitos para conscientização sobre cibersegurança [Braga, 2016]. Além disso, o incentivo ao uso da rede social Telegram na criação de grupos de hackers éticos, mesmo sabendo que atualmente o Telegram é conhecido por possuir uma maior concentração de grupos de hackers não éticos, o que torna essa abordagem desafiadora devido à natureza descentralizada e anônima da plataforma [Barros, 2021]. Mesmo assim, essa estratégia pode combinar medidas técnicas, legais e educacionais na internet para intimidar a oposição que utilizam a engenharia reversa e técnicas de phishing para atacar ambientes críticos. Especialistas também argumentam que regulamentos utilizados no passado precisam ser atualizados, uma vez que não abordam adequadamente as armas cibernéticas nem os ataques realizados por meio do ciberespaço [Ramos 2014].

3.1. Resultados

Imagine um mundo onde a segurança cibernética é uma fortaleza inexpugnável, impenetrável aos hackers maliciosos. Essa visão tornou-se uma missão para os fundadores de um Instituto sem fins lucrativos, um farol de conhecimento e colaboração que reúne especialistas engajados em prol de proteger a infraestrutura crítica do país, no qual o cerne do Instituto, oferecem conteúdos de segurança cibernética através de cursos online no ambiente Moodle e por meio do grupo criado no Telegram [Idciber, 2023]. Agora, imagine um hacker solitário tentando penetrar as defesas de uma usina nuclear e seus esforços encontram uma muralha nacional de especialistas unidos por um objetivo comum, frustrar seus planos nefastos.

Através desta iniciativa pioneira no Brasil, o Instituto busca melhorar as políticas nas organizações públicas e privadas, estimulam pesquisas científicas e ajudam a conscientização da sociedade através de serviços gratuitos como, cursos online, fóruns, redes sociais, eventos virtuais, matérias no site e ainda acompanham o que está acontecendo nesse cenário obscuro. Atualmente, o Instituto está vivenciando um crescimento significativo, o canal do Telegram é um exemplo proeminente de ferramenta colaborativa, envolvendo quase quatrocentos membros especialistas associados e selecionados pelos comitês organizadores que participam de debates técnicos contínuos, e a cada evento virtual realizado através de webconferências atrai mais de mil inscritos e visualizações.

4. Conclusões

Como conclusão, este trabalho busca fortalecer a segurança cibernética em sistemas críticos por meio de sistemas colaborativos e redes sociais, protegendo a segurança da sociedade e das organizações. Para o futuro, visa o estabelecimento de leis mais rigorosas, cooperação internacional e incentivos adicionais nos estudos científicos. Essa

iniciativa também pode inspirar a criação de outros institutos em parceria com organizações públicas e privadas para juntos fortalecer a segurança nacional.

5. Lições Aprendidas

As lições aprendidas destacam a importância de promover o bem e priorizar a nação através da colaboração entre organizações e a sociedade, além do compartilhamento de conhecimento e educação equitativa através de sistemas colaborativos existentes, de fácil acesso e gratuitos. É fundamental ressaltar a importância da conscientização, colaboração e resiliência por meio de ambientes colaborativos.

6. Referências

Barbosa, K., Martins, G., Souto, E. (2014). Botnets. Simpósio Brasileiro em Segurança da Informação. https://sol.sbc.org.br/livros/index.php/sbc/catalog/download/91/400/671-1

Barros, M. (2021). Telegram dispara como alternativa à dark web para criminosos cibernéticos. https://dciber.org/telegram-dispara-como-alternativa-a-dark-web-para-criminosos-ciberneticos/

Braga, P., & Junior, C. (2016). Plano de Conscientização em Segurança da Informação Usando AVA. XIV Congresso Internacional de Tecnologia na Educação, Pernambuco. https://www.pe.senac.br/congresso/anais/2016/pdf/comunicacao-oral/081.pdf

Cert.br. (2022) Estatísticas. https://stats.cert.br

Datta, P. (2022) Hannibal at the gates: Cyberwarfare & the Solarwinds sunburst hack. Journal of Information Technology Teaching Cases, v. 12, n. 2, p. 115–120. https://journals.sagepub.com/doi/10.1177/2043886921993126

Fernandes, J. P. T. (2012). A Ciberguerra como Nova Dimensão dos Conflitos do Século XXI. https://ipri.unl.pt/images/publicacoes/revista_ri/pdf/ri33/n33a05.pdf

Idciber.org (2023). Instituto de Defesa Cibernética. https://idciber.org

Mennecier, D. (2020). Cyber attacks and hospital. Science Direct, 4(4). https://doi.org/10.1016/j.pxur.2020.06.006

Mueller, G. B., Jensen, B., Valeriano, B. (2023). Cyber Operations during the Russo-Ukrainian War. CSIS. http://www.jstor.org/stable/resrep52130

Nascimento, V., Santos, L., & Saraiva, R. (2022). Softwares de Análise de Dados Qualitativos: Revisão Narrativa da Literatura. Revista Científica do Centro Universitário FAEMA, 13(1), 44–58. https://doi.org/DOI: 10.31072/rcf.v13i1.1135

Ramos, H. F. (2014). O Poder dos Laços Fracos, Convergência e Curiosidade na Disseminação do Stuxnet. Observatorio. https://doi.org/10.15847/obsOBS812014755

Rocha, G. (2022). Caso Stuxnet: Os impactos do ataque cibernético ao programa nuclear do Irã com a primeira arma cibernética à segurança internacional [UNESP]. https://www.oasisbr.ibict.br/vufind/Record/UNSP_2956ac0d420e31e751fafd6cdd8a0edf

Sá, A. L. (2020). Segurança Cibernética De Usinas Nucleares: Uma Análise Sobre Medidas De Mitigação De Ataques De Engenharia Social Na Central Nuclear [ECEME]. https://bdex.eb.mil.br/jspui/bitstream/123456789/7566/1/MO.pdf

Silva, Francisco. (2018). StuxNet – El software como herramienta de control geopolítico. Revista Pontificia Universidad Católica del Ecuador. https://doi.org/10.26807/revpuce.v0i106.141

Taquary, C. (2019). A Defesa Cibernética em Ambientes de Infraestrutura Crítica. ESG. https://repositorio.esg.br/bitstream/123456789/1205/1/C%c3%89LIO%20Borges%20TAQUARY%20Segundo.pdf