FACULDADE DE TECNOLOGIA DE SÃO PAULO – FATEC-SP

ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

EDUARDO AUGUSTO REZAGHI TALIANI

ANÁLISE DA EVOLUÇÃO DAS AMEAÇAS CIBERNÉTICAS ENTRE 2010 E 2021

SÃO PAULO

2022

EDUARDO AUGUSTO REZAGHI TALIANI

ANÁLISE DA EVOLUÇÃO DAS AMEAÇAS CIBERNÉTICAS ENTRE 2010 E 2021

Trabalho de Conclusão de Curso apresentada como exigência para obtenção do título de Tecnólogo em Análise e Desenvolvimento de Sistemas

Orientador: Carlos Hideo Arima

SÃO PAULO

2022

FACULDADE DE TECNOLOGIA DE SÃO PAULO

EDUARDO AUGUSTO REZAGHI TALIANI

ANÁLISE DA EVOLUÇÃO DAS AMEAÇAS CIBERNÉTICAS ENTRE 2010 E 2021

Trabalho submetido como exigência parcial para a obtenção do Grau de Tecnólogo em Análise e Desenvolvimento de Sistemas.

Parecer do Professor Orientador

_____
_____
_____

Conceito/Nota Final: _____

Atesto o conteúdo contido na postagem do ambiente TEAMS pelo aluno e assinada por mim para avaliação do TCC.

Orientador: Professor Doutor Carlos Hideo Arima

SÃO PAULO, 11 de dezembro de 2022.

Assinatura do Orientador

Assinatura do aluno

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

RESUMO

Com a evolução tecnológica da última década, a introdução de novas tecnologias no cotidiano das pessoas também introduz vulnerabilidades passíveis de serem exploradas por atores de ameaça com o objetivo de causar um grande impacto nas organizações, governos e nas pessoas que dependem de seus serviços. Este trabalho tem o objetivo de apresentar a evolução das ameaças cibernéticas no período de 2010 a 2021, levantando a relação das ameaças cibernéticas com grupos financiados por estados, chamados de Advanced Persistent Threats, e como ataques coordenados podem causar impactos gigantescos tanto a níveis corporativos quanto a níveis geopolíticos. Também se procurou dedicar uma análise as principais ameaças utilizadas por estes grupos, identificando e sumarizando os principais métodos de ataque utilizados nos ataques. A metodologia para obtenção do embasamento para as informações deste trabalho de pesquisa é a análise bibliométrica focada em aspectos qualitativos dos artefatos. Esta análise traz à tona deficiências existentes no processo de categorização dos ativos, análise de risco e inteligência cibernética de governos e empresas, onde o aumento alarmante de casos orienta a uma falta de aplicação de procedimentos das políticas internas de segurança de organizações e a falta de medidas eficazes de governos e organizações para mitigar impactos e riscos oriundos da introdução de novas vulnerabilidades em conjunto com a evolução tecnológica.

PALAVRAS-CHAVE: segurança da informação, cibersegurança, ciberataques, ciberameaças, advanced persistent threats.

ABSTRACT

With the technological evolution of the last decade, the introduction of new technologies in people's daily lives also introduces vulnerabilities likely to be exploited by threat actors with the aim of causing a major impact on organizations, governments and people who depend on their services. This paper aims to present the evolution of cyber threats in the period from 2010 to 2021, raising the relationship of cyber threats with groups funded by states, called Advanced Persistent Threats, and how coordinated attacks can cause gigantic impacts both at corporate and geopolitical levels. An analysis of the main threats used by these groups was also attempted, identifying and summarizing the main attack methods used in the attacks. The methodology used to obtain the basis for the information in this research paper is a bibliometric analysis focused on the qualitative aspects of the artifacts. This analysis brings to light existing deficiencies in the process of asset categorization, risk analysis and cyber intelligence of governments and companies, where the alarming increase of cases is driven by a lack of enforcement of internal security policy procedures of organizations and the lack of effective measures by governments and organizations to mitigate impacts and risks arising from the introduction of new vulnerabilities in conjunction with technological evolution.

KEYWORDS: information security, cybersecurity, cyberattacks, cyberthreats, advanced persistent threats.

1 INTRODUÇÃO

A transformação na sociedade oriunda do avanço tecnológico do final do século XX e começo do século XXI trouxeram grandes mudanças na comunicação entre entidades, pessoas e nos hábitos destas que passaram a ser cada vez mais integrados com estas tecnologias. Mediante tal contexto, o valor e importância delas em nossas vidas passou a ser muito maior, transitando de meios burocráticos e demorados para meios mais eficientes e coordenados (JANCZEWSKI; COLARIK, 2008). Com a popularização dos computadores, muitas informações passaram a estar disponíveis em ambientes repletos de vulnerabilidades, cujo valor é altíssimo para determinados grupos e governos.

Não obstante, também houve a criação e popularização de mais uma forma de impactar milhares de vidas, com ataques coordenados por grupos a órgãos críticos dessa infraestrutura digital, causando imensos prejuízos financeiros e até mesmo psicológicos para as vítimas (AGRAFIOTIS *et al.*, 2018, p. 7). Tais grupos estão motivados a impactar essa infraestrutura e causar uma grande disrupção no tráfego das informações, seja para obter dados confidenciais de governos e corporações com a finalidade de aquisição de inteligência ou espionagem industrial ou até mesmo para causar pânico e terror nas massas.

Ademais, em um cenário geral, este contexto apresentado se solidifica com casos de grandes ataques que acometeram infraestruturas estatais, como os exemplos dos ataques SUNBURST, comprometendo o software Orion da SolarWinds (FIREEYE, 2020) ou o malware Stuxnet (FALLIERE; MURCHU; CHIEN, 2011), ambos fabricados por grupos operando a favor de objetivos estatais e governamentais. A presença e ação destes estados dentro da Internet torna-se uma grande fonte de preocupação, pois nem todas as nações disseminam as práticas adequadas ou sequer possuem os meios necessários para defenderem a sua infraestrutura digital (SHACKELFORD, SCOTT J.;, 2015).

Em um cenário contido dentro do aspecto do cibercrime, é possível verificar, ainda que superficialmente, uma crescente nos casos relacionados a ameaças

que utilizam técnicas para impactar a maior quantidade de pessoas, aumentando o dano causado.

1.1 DEFINIÇÃO DA QUESTÃO PROBLEMA

Com estes cenários elucidados anteriormente, pretende-se responder a seguinte questão-problema ao final do trabalho:

1. Quais foram as evoluções das ameaças cibernéticas na última década?

1.2 PROPOSIÇÕES

Mediante a apresentação da questão-problema, são as seguintes proposições formuladas para orientar conclusões sobre a pesquisa realizada, ou seja, a confirmação de:

1. Avanço das ameaças cibernéticas em um curto período (2010-2021) quando comparado com o período de popularização da computação pessoal.
2. Impacto causado pela exploração de certas vulnerabilidades em protocolos comumente utilizados.
3. Incerteza em relação a segurança do tratamento de dados pelas grandes corporações, levando em conta como medidas de tratamento dos dados são aplicadas e o nível de impacto dos ataques.
4. Existência de diversos grupos financiados por governos difundidos pelo ciberespaço.

1.3 OBJETIVOS GERAIS E ESPECÍFICOS

Com os cenários apresentados para a questão problema e as proposições enumeradas, apresentam-se os seguintes objetivos gerais e específicos:

1 Objetivo Geral

Analisar a evolução das ameaças cibernéticas até os dias atuais levando em consideração as proposições anteriormente expostas.

2 Objetivos específicos

1. Identificar, por meio da bibliometria, os diferentes vetores de ataque e as principais vulnerabilidades exploradas;
2. Identificar, por meio da análise de conteúdo dos artigos, a existência de grupos financiados por governos, os chamados *Advanced Persistent Threats* (APTs), tabulando-os para sumarizar suas ações;
3. Identificar e dissertar sobre casos emblemáticos de ciberataques, assim como o impacto causado;
4. Verificar, por meio de toda a sumarização do impacto dos ataques, a atual situação de políticas sobre os dados tratados em grandes organizações, tendo em vista que estes são alvos de grupos de cibercriminosos.

A motivação para esse trabalho é a crescente de casos de ciberataques contra grandes organizações privadas e entidades públicas, buscando principalmente obter informações de inteligência ou ganhos financeiros para os grupos que arquitetam as ações maliciosas, seja pela exigência de pagamentos de resgate ou pela extorsão para a não publicação de dados confidenciais e, em alguns casos, impactar a capacidade bélica de um país opositor mediante a sabotagem, como ocorreu com o STUXNET (FALLIERE; MURCHU; CHIEN, 2011). Cabe também analisar como normas e procedimentos são tratados em relação a problemática dos ciberataques. Por meio deste trabalho de pesquisa, objetiva-se apresentar e analisar causadores de um grande impacto quando estiveram ativas, analisando os meios utilizados, o nível de sofisticação dos atacantes e a relação das várias nações com estes ataques. Cabe também sugerir, por meio de todos os

casos e dados analisados, ações de inteligência e medidas normativas no sentido de guiar a aplicação de todo o conhecimento disponível para tornar as análises de ameaças mais sofisticadas.

1.4 ESTRUTURA DO TRABALHO

Esta monografia consiste nos seguintes capítulos:

2. **Referencial teórico**: este capítulo expande o contexto apresentado na introdução deste trabalho de pesquisa, trazendo maiores detalhes nas mudanças sociais, nas ameaças e ataques, nos grupos hacker e nos impactos de suas ações;

3. **Metodologia da pesquisa**: este capítulo detalha a metodologia utilizada para extrair os dados e informações das referências que embasam este trabalho de pesquisa;

   3.1. **Apuração e organização dos dados pesquisados**: este capítulo apresenta o resultado da metodologia utilizada para análise bibliométrica assim como dados sobre as publicações referenciadas;

4. **Análise de resultados**: este capítulo apresenta a análise dos artigos filtrados utilizando a metodologia escolhida, embasando o contexto apresentado na introdução e referencial teórico;

5. **Considerações finais**: este capítulo traz as considerações a cada proposição trazida anteriormente nesta seção e intui, por meio de toda a análise e dissertação realizada utilizando-se as referências, se houve evidências o suficiente para responder o questionamento levantado pela questão-problema.

2 REFERENCIAL TEÓRICO

Este capítulo expande o cenário trazido na introdução deste trabalho, trazendo maior embasamento à mudança tecnologia e à crescente de casos de ataques orquestrados por meio de referências a obra de outros autores.

2.1 MUDANÇAS TECNOLÓGICAS DA SOCIEDADE E ÀS NOVAS VULNERABILIDADES INTRODUZIDAS

A obra *Cyber Warfare and Cyber Terrorism*, dos autores Lech Janczewski e Andrew M. Colarik foram o ponto de partida para se ter uma visão do fluxo das invasões e dos impactos causados. Em um nível macro, foi possível entender o mecanismo e algumas das motivações que os atacantes utilizam para realizar suas ações. Destaca-se que os autores abordam a grande convergência das pessoas para utilizarem novas tecnologias, que por si só introduziram diversas novas vulnerabilidades, abordando também como grandes empresas e governos passaram a utilizá-las em suas atividades. Pontos citados relacionados ao contexto apresentado pelos autores é a motivação dos atacantes, resumidas pela quantidade de dados – e, por conseguinte, informações – disponíveis nos sistemas utilizados pelos possíveis alvos (JANCZEWSKI; COLARIK, 2008).

Os autores buscaram evidenciar todo o mecanismo de invasão nessas tecnologias, tais como e-mails, navegadores, ferramentas de chat, softwares de acesso remoto, softwares de produtividade, entre outros, exemplificando os diferentes pontos de intrusão nesta miríade de sistemas. Também apontaram diferentes mecanismos de defesa passíveis de utilização, tanto para proteger os acessos físicos quanto virtuais aos dados armazenados em sistemas críticos.

A reflexão geral realizada pelos autores resslta um grande aumento nos casos de ciberterrorismo e cibercrime no início do século XXI, onde os ataques realizados nestas novas plataformas possuiam efeitos colaterais mais graves (JANCZEWSKI; COLARIK, 2008, p. 28), introduzindo uma nova camada de complexidade nas análises de risco realizadas na área da segurança da informação.

2.2 GRUPOS FINANCIADOS POR ESTADOS E ATRIBUIÇÃO

Relacionando-se com o contexto de ameaças utilizadas em um contexto de ciberguerra, um caso emblemático que começou marcando o início da segunda década do século XXI foi o malware Stuxnet (FALLIERE; MURCHU; CHIEN, 2011), sendo uma das peças mais complexas de malware já feitas, tendo capacidades impressionantes de replicação e um impacto gigantesco causado nos alvos originais. O malware foi desenvolvido com objetivo de atacar o programa nuclear iraniano, causando danos e interrompendo o funcionando de controladores lógicos programáveis específicos (FARWELL; ROHOZINSKI, 2011, p. 3). Um ponto a ser citado é a atribuição de atores externos em ataques deste porte. No caso do Stuxnet, pela complexidade, objetivo e até mesmo pelas condições exploradas pela ameaça, a atribuição provável foi atrelada a atores com grande financiamento estatal (LEMAY *et al.*, 2018, p. 31), os chamados *Advanced Persistent Threats* (APTs) (RID; BUCHANAN, 2014). Trata-se de uma disrupção no contexto das ciberameaças e o impacto causado por elas, pois tais atores possuem extenso conhecimento e aparato financeiro proporcionado por grandes nações.

Atualmente, as estratégias relacionadas a proteção dos dados por esses países passou a ser uma preocupação de segurança nacional com o objetivo de proteger infraestrutura essencial e dados ultrassecretos (TRAUTMAN, 2016, p. 31). Segundo as palavras do secretário de defesa dos EUA Ash Carter, “o avanço de ferramentas maliciosas a um baixo custo trouxeram a tona novos atores para a visão geopolítica” (TRAUTMAN, 2016, p. 33). Essa frase, vinda de uma figura do alto escalão do governo americano, reflete uma grande preocupação com ataques realizados por atores coordenados e com objetos específicos.

A extensão de campanhas de ataque destes grupos é grande, pois casos com impacto gigantesco podem ser utilizados para exemplificar as ações destes grupos. Técnicas simples são mescladas com malwares munidos de diversas capacidades de intrusão e replicação. Os objetivos desses grupos transitam entre extrair dados e danificar a infraestrutura responsável por abrigá-los com diferentes tipos de malware, como rootkits, backdoors, ransomwares, entre outros (LEMAY *et al.*, 2018).

Cabe destacar também que a ação de grupos maiores não dilime a ação de grupos isolados. Em contextos específicos, especialmente relacionados à situações geopolíticas e crise mundiais, ações maliciosas por grupos menores crescem em proporções assustadoras (LALLIE *et al.*, 2020).

Mediante estas duas vertentes de grupos financiados por estados e aqueles isolados, a visão é de que existem inúmeras vulnerabilidades em sistemas populares sendo exploradas para finalidades de extração e obtenção de dados sigilosos com ferramentas que possuem diferentes níveis de sofisticação. Entretanto, o impacto destes ataques é sentido em termos financeiros e sociais, variados conforme as técnicas utilizadas pelos atacantes e a finalidade do ataque.

2.3 IMPACTOS FINANCEIROS E ESTRUTURAIS

Segundo Shackelford (2015), as ameaças cibernéticas são catalisadoras de perdas financeiras imensas em um contexto global. O dado que corrobora com esta afirmação é a quantidade estimada de perdas decorrentes de ciberataques em 2014, que estavam na faixa de US$400 bilhões até US$2 trilhões de dólares americanos. Em uma análise mais recente, tem-se uma estimativa de perdas totais de US$6 trilhões de dólares americanos (CYBERSECURITY VENTURES, 2020) até 2021, com grande parte desta cifra alimentada por casos de ransomware, estimados pelo FBI em uma cifra de U$1 bilhão de dólares (ROSENSTEIN; J., 2020).

Em casos no mercado privado, grandes corporações sofrem perdas caso dados relacionados a segredos corporativos ou de clientes sejam expostos devido a um ataque. Já as pessoas são afetadas em uma escala variável, pois os danos podem ser diretamente ou indiretamente relacionados ao ciberataque (AGRAFIOTIS *et al.*, 2018, p. 10).

Em termos do estado, as perdas podem ser mais graves, pois se relacionam aos dados e à infraestrutura utilizada para fins estratégicos. Ciberataques que visam componentes essenciais de um país (usinas de energia elétrica, hospitais, escolas, transporte, logística, entre outros) causam danos comparativamente maiores em relação àqueles possíveis de serem

causados em grandes corporações, pois possuem o potencial de afetar pessoas em uma escala maior (AGRAFIOTIS *et al.*, 2018, p. 5). Em um cenário extremo, toda a infraestrutura essencial de um país pode deixar de funcionar (TRAUTMAN, 2016). Ataques visando hospitais, escolas e plantas de energia possuem o impacto agravado em decorrência da infraestrutura precária e desatualizada. Por exemplo, no caso de um ataque em um hospital dependente de um sistema eletrônico para controlar as fichas dos pacientes, há uma interrupção no funcionamento de um sistema essencial para o fluxo adequado de dados e informações para o tratamento das pessoas e organização das equipes.

Em relação aos dois cenários apresentados, tais impactos são difíceis de serem quantificados diretamente, pois envolvem fatores diretos e indiretos em relação aos ciberataques. Porém, em termos de danos a infraestrutura, ambos podem ser comparados. No caso da Maersk (CAPANO, 2022), diversos navios com itens essenciais ficaram parados e toda a cadeia de logística dependente da empresa ficou parada. O impacto na rotina dos funcionários foi evidente, assim como em corporações não atreladas diretamente a este incidente. Neste caso, contabilizando o aspecto financeiro, o impacto foi estimado entre US$250 milhões e US$300 milhões de dólares, sendo que os danos totais relacionados ao vírus que destruiu a infraestrutura digital da Maersk, NotPetya, foi estimado em US$10 bilhões de dólares (GREENBERG, 2018).

3 METODOLOGIA DE PESQUISA

A metodologia selecionada para ser utilizada no trabalho foi a revisão sistemática da literatura, onde diversos artigos foram extraídos de uma base de dados específica para serem analisados seguindo critérios definidos.

Nesta etapa do trabalho, foi utilizado a base de dados Google Acadêmico para pesquisar artigos referentes ao tema abordado, do período de 2010 a 2021. Para isso, foram selecionadas palavras-chave condizentes com o tema, com base relacional e quantitativa em relação a amplitude dos resultados no motor de busca. A busca que retornou a quantidade de resultados apresentada na tabela 1 foi realizada no dia 30/03/2022.

Tabela 1 – palavras-chave e resultados

Palavra-chave	**Sinônimos utilizados**	**Resultados (Google Acadêmico)**
cyber crime	cybercrime, cyber crimes	143.000
cyber threat	cyberthreat, threat	2.390.000
cyber attack	cyberattack, “cyber attack”, “cyber attacks”	56.400
advanced persistent threat	“advanced persistent”	14.900
timeline	chronology, retrospective	3.310.000
cryptography	crypto	250.000
data leak	leak	668.000
Total		**4.242.900**

Fonte: Google Acadêmico

Havendo uma miríade de resultados, escolheu-se utilizar as palavras-chave para compor a pesquisa dos artigos:

("cyber crime" OR cybercrime OR "cyber crimes") AND ("cyber threat" OR "cyberthreat") AND (cyberattack OR "cyber attack" OR "cyber attacks") AND advanced persistent AND (timeline OR chronology OR retrospective) AND crypto AND leak

Foi utilizado o software *Publish or Perish* na versão 8.2.3944.8118 para realizar a pesquisa na base de dados com as palavras-chave escolhidas. Os resultados obtidos foram pesquisados no dia 14/04/2022, com um total de 300 artigos e 5350 citações.

Entretanto, é necessário aplicar, nesta grande quantidade de artigos retornados na busca, um protocolo de revisão e escolha para decidir quais dentre estes artigos foram os que obtiveram o maio impacto. Com esse fim, foi escolhido o ***h-index*** (índice de Hirsch), criado em 2005 com o objetivo de quantificar a produtividade de um pesquisador. O critério para escolher artigos para a revisão levou em consideração artigos com h-index maior ou igual a 25, excluindo-se 270 artigos a partir deste critério. Esta análise também foi baseada no protocolo PRISMA-P (PAGE *et al.*, 2021) para definir outros critérios de elegibilidade ao analisar cada um dos 30 artigos restantes.

Analisando o abstract de cada um dos 30 artigos restantes, pode-se excluir 8 artigos da análise completa do conteúdo, pois a temática tratada não se encaixava com o tema deste trabalho, e 2 citações indicadas no resultado da busca do Google Scholar. Dos 20 artigos restantes, 12 foram selecionados para terem o seu conteúdo analisado. 1 artigo foi excluído posteriormente pois não se adequava ao tipo de material procurado.

A seguir, estão enumerados os critérios de exclusão utilizados para filtrar os artigos:

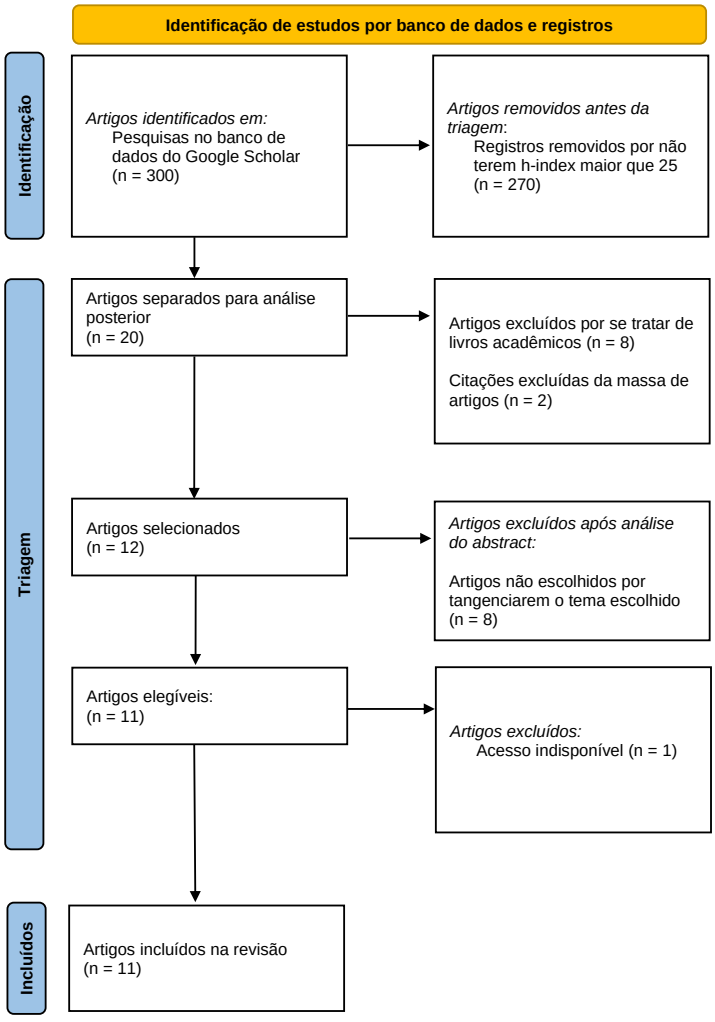
1. O artigo deve possuir h-index superior a 25;
2. O artigo deve estar no idioma inglês;

3. O resumo (abstract) do artigo deve conter a indicação de uma análise histórica ou do impacto de uma ou várias ameaças;
4. O resumo (abstract) do artigo deve citar, de forma explícita, os atores responsáveis pela propagação da ameaça.

Outras métricas relacionadas aos artigos selecionados pelo processo de filtragem é a quantidade de citações de cada um dos artigos e a quantidade de citações por autor.

A figura 1 apresenta o fluxograma da aplicação do protocolo nos artigos selecionados.

Figura 1 – Diagrama do protocolo PRISMA-P



Fonte: adaptado da metodologia PRISMA-P

3.1 APURAÇÃO E ORGANIZAÇÃO DOS DADOS PESQUISADOS

As métricas foram sumarizadas na tabela 2, com base em todos os artigos selecionados.

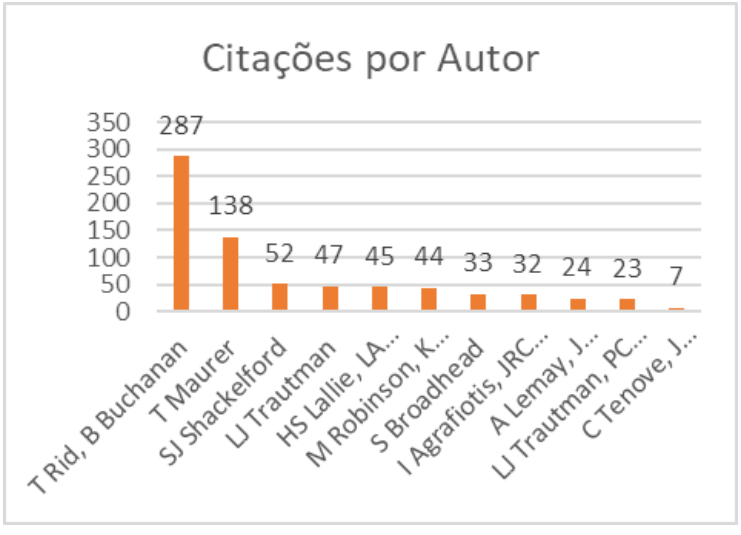
Tabela 2 – Tabulação dos artigos selecionados

Citações por artigo	Autores	Título dos artigos	Ano de publicação	Fonte	Editora	Citações por autor
573	T Rid, B Buchanan	Attributing cyber attacks	2015	Journal of Strategic Studie:	Taylor & Francis	287
227	HS Lallie, LA Shepherd, JRC Nurse, A Erola, ...	Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the	2021	Computers & Security	Elsevier	45
138	T Maurer	Cyber norm emergence at the United Nations	2011	An Analysis of the UN's Act	afyonluoglu.org	138
131	M Robinson, K Jones, H Janicke	Cyber warfare: Issues and challenges	2015	Computers & Security	Elsevier	44
128	I Agrafiotis, JRC Nurse, M Goldsmith, ...	A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate	2018	Journal of ...	academic.oup.com	32
96	A Lemay, J Calvet, F Menet, JM Fernandez	Survey of publicly available reports on advanced persistent threat actors	2018	Computers & Security	Elsevier	24
52	SJ Shackelford	Protecting intellectual property and privacy in the digital age: the use of national cybersecurity strategies to mitigate cyber risk	2016	Chap. L. Rev.	HeinOnline	52
47	LJ Trautman	Is cyberattack the next Pearl Harbor	2016	NCJL & Tech.	HeinOnline	47
46	LJ Trautman, PC Ormerod	Wannacry, ransomware, and the emerging threat to corporations	2018	Tenn. L. Rev.	HeinOnline	23
33	S Broadhead	The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and	2018	Computer Law & Security F	Elsevier	33
27	C Tenove, J Buffie, S McKay, D Moscrop	Digital threats to democratic elections: how foreign actors use digital techniques to undermine	2018	-	papers.ssrn.com	7

Fonte: resultado da pesquisa

Para se ter uma visão de cada um dos autores para o recorte realizado na miríade de artigos da literatura, as citações por autor podem ser sumarizadas pelo gráfico na figura 2. Este gráfico permite visualizar autores ordenados pela quantidade de citações dentre os artigos elencados para análise.

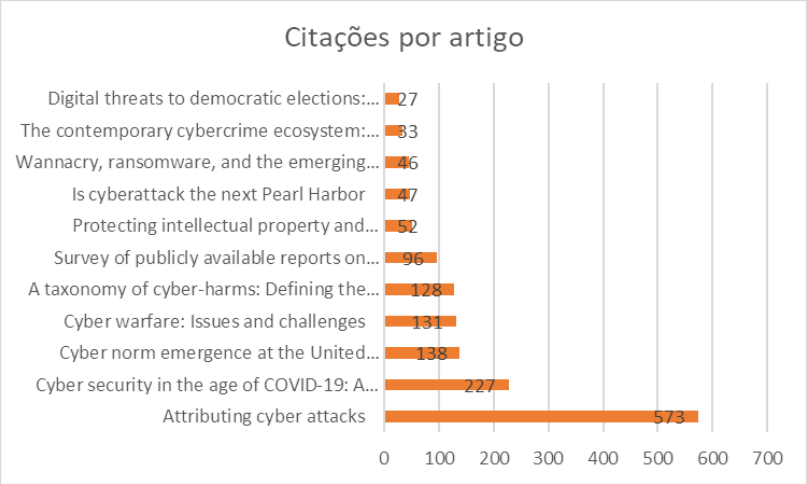
Figura 2 – Gráfico de citações por autor



Fonte: resultado da pesquisa

Já os artigos mais citados podem ser sumarizados pelo gráfico na figura 3. A visualização ordenada pelos artigos mais citados permite saber qual é a obra de maior relevância dentre os artigos elencados para análise.

Figura 3 – Gráfico de citações por artigo



Fonte: resultado da pesquisa

Estes gráficos indicam que artigos que abordam conceitos como o processo de atribuição de um ciberataque e a relação da pandemia com o surto de COVID-19 possuem bastante relevância para orientar o estudo vinculado às ameaças.

4 ANÁLISE DE RESULTADOS

Este capítulo pretende analisar os artigos apresentados na seção anterior, sumarizando conclusões dos autores e levantando temas e correlações entre as referências.

4.1 CATEGORIZAÇÃO DAS AMEAÇAS

Mediante a análise dos artigos, diversas hipóteses apresentadas puderam ser verificadas. Foi possível ter uma visão de como os autores abordaram diferentes ciberataques ao mesmo tempo que foi possibilitada uma visão das principais ameaças, ciberataques, objetivos e metodologias pelos diversos atores citados. Além desses pontos, também foi possível

visualizar diversos impactos em contextos gerais e específicos, evidenciando prejuízos individuais e organizacionais.

Com o objetivo de analisar as ameaças presentes no intervalo de 2010 a 2021, para cada um dos artigos analisados, tabulou-se apenas os casos com maior expressividade em termos de impacto e com uma atribuição mais confiável. Casos menores, mais esparsos e com a atribuição incerta não foram tabulados pois, apesar de serem relevantes para a estatística geral de ciberataques, não são claros para representar aspectos como interesses estatais relacionados aos ataques.

O artefato desta tabulação foi uma tabela com a relação de todas as principais ameaças no intervalo de 2010 a 2021. Ela apresenta os principais casos em conjunto com a atribuição provável a um APT específico e o provável país de origem do grupo.

A tabela 3 apresenta 31 casos tabulados. Cada um dos casos possui as seguintes informações dispostas nas colunas:

- ***Nome**: nome dado a ameaça pelos pesquisadores ou por órgãos do governo;*
- ***Ano**: ano da primeira ocorrência significativa da ameaça*
- ***Vetores principais**: principal forma de ataque/replicação para distribuir payloads. Categorizadas seguindo a matriz MITRE ATT&CK®;*
- ***Finalidade**: objetivo principal provável da ameaça*
- ***Impacto**: impacto provável e/ou percebido da ameaça;*
- ***Atribuição**: grupo provável responsável pelo desenvolvimento e disseminação da ameaça;*
- ***País provável**: país de origem provável do grupo/ameaça.*

O uso da palavra provável na descrição da coluna relacionada ao país é em decorrência ao fator de atribuição em cada um dos ataques. Diversos autores pontuaram a dificuldade de se traçar os perpetradores originais da ameaça (BROADHEAD, 2018, p. 3). Como apontado por Rid e Buchanan (2014), atribuir um ataque é um processo multidisciplinar que depende de

diversos fatores, que muitas vezes não estão claramente presentes e dificultam a atribuição.

Tabela 3 – Tabulação das principais ameaças encontradas

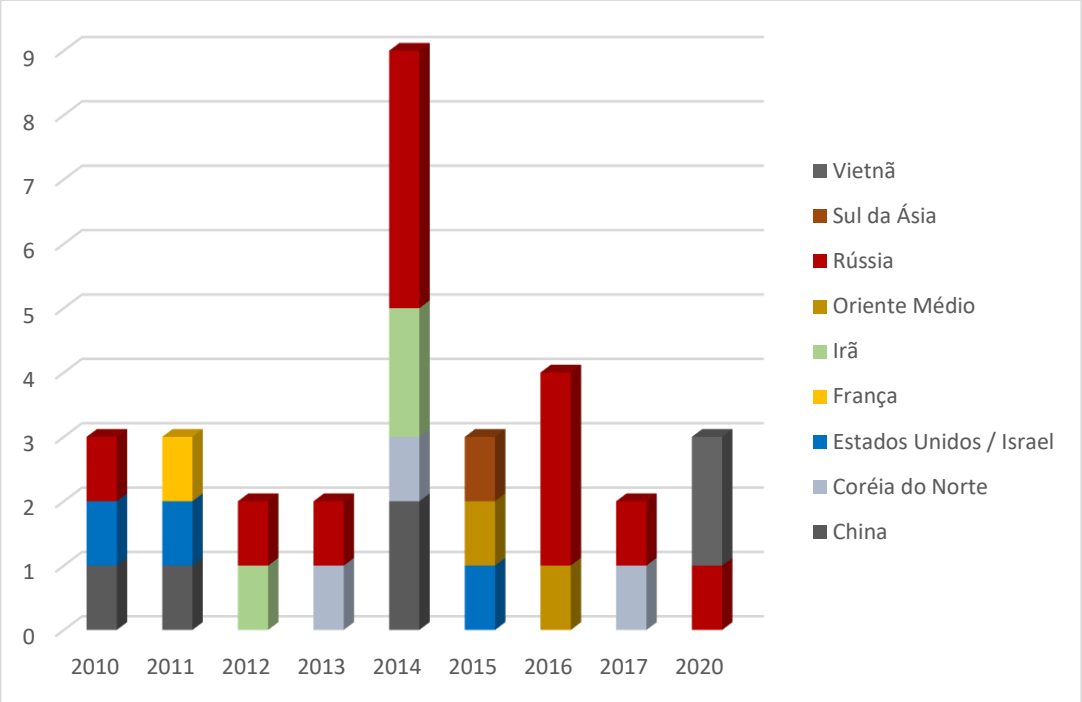
Nome	Ano	Vetores principais	Finalidade	Impacto	Atribuição	Pais provável
Stuxnet	2010	T1068, T0851	Destruir plantas nucleares - Irã	Danos ao programa nuclear do Irã	Olympic Games (NSA, Unit 8200)	Estados Unidos / Israel
Kelihos Botnet	2010	T1584.005	Controlar computadores externos para diversas ações	Roubo de dados sensíveis, instalação de malware, entre outros.	Peter Yuryevich Levashov (indivíduo)	Rússia
Pirpi	2010	T1190,T1041,T0882	Espionagem	Exposição e vazamento de dados sensíveis	APT-3 (Gothic Panda)	China
Duqu	2011	T1566.003, T1573.001, T1055.001	Ataques a sistemas de controle industrial (similar ao Stuxnet)	Exfiltração de dados sensíveis sobre infraestrutura crítica	Olympic Games (NSA, Unit 8200)	Estados Unidos / Israel
ShadyRAT*	2011	T1190, T0882	Acesso remoto e obtenção de dados	Roubo de propriedade intelectual / múltiplas	APT-1 (Comment Panda)	China
Babar*	2011	T1204.002,T1055.001	Espionagem	Exposição de dados estatais sensíveis	Animal Farm	França
Sofacy*	2012	T1190,T1204.002	Obtenção de dados confidenciais	Exposição e vazamento de dados sensíveis	APT-28 (Fancy Bear)	Rússia
Shamoon*	2012	T1561,T1548.002	Obtenção de dados relacionados à gigante petrolífera saudita Aramco relacionados ao contexto geopolítico do Irã / Espionagem / Destruição de infraestrutura digital	Destruição de infraestrutura estatal, tecnológica e obtenção ilegal de dados	*Cutting Sword of Justice*	Irã
Havex	2013	T1195,T1210	Destruir infraestrutura energética e essenciais (aviação, farmacêutica etc.)	Disrupção de serviços essenciais de países na Europa e nos EUA	Energetic Bear	Rússia
DarkSeoul*	2013	T1110, T1561,T1566.001	Danos a infraestrutura digital da Coréia do Sul	Destruição de infraestrutura tecnológica	Lazarus Group (Silent Chollina)	Coréia do Norte
CryptoLocker	2014	T1566.001,T1486	Criptografar dados dos discos e cobrar por resgate	Danificar os dados e extorquir indivíduos ou organizações. Prejuízo estimado de US$27 milhões	-	Rússia
MiniDuke*	2014	T1204.002, T1027, T1082, T1105	Espionagem e obtenção de dados	Vazamento de informações confidenciais	APT-29 (Cozy Bear)	Rússia
Derusbi*	2014	T1059.004, T1070.004,	Acesso remoto e obtenção de dados (operações contra setores de energia, aeroespacial e saúde)	Roubo e extração de dados	Deep Panda (Shell_Crew)	China
3PARA RAT*	2014	T1547.001, T1562.001	Espionagem	Exposição e vazamento de dados militares sensíveis	Putter Panda (Unit 61486)	China
BlackEnergy	2014	T1056.001, T1055.001, T1070.001, T1574.010	Destruir infraestrutura energética	Disrupção do fornecimento de energia na Ucrânia	Sandworm (Unit 74455)	Rússia
Uroburos / Turla*	2014	T1027.001, T1014	Espionagem	Perda de dados, disrupção em infraestrutura estatal	Venomous Bear (Agent.btz)	Rússia
TinyZBot*	2014	T1566.001, T1547.001	Roubo de dados / Espionagem	Roubo de dados sensíveis	OpCleaver	Irã
Thamar Reservoir*	2014	T1566.001, T1059.003	Roubo de dados / Espionagem	Exposição de dados estatais sensíveis	Rocket Kittens	Irã
DarkSeoul*	2014	T1566.001, T1056.001	Extrair e roubar dados da Sony Entertainament	Danos morais, financeiros e psicológicos a corporação e aos usuários	Lazarus Group (Silent Chollina)	Coréia do Norte
Duqu 2.0	2015	T1566.001, T1068, T1204.002	Ataques a sistemas de controle industrial (similar ao Stuxnet)	Exfiltração de dados sensíveis sobre infraestrutura crítica. Mais vítimas que a primeira versão	Olympic Games (NSA, Unit 8200)	Estados Unidos / Israel
DHS Spyware*	2015	T1566, T1210	Espionagem / Obtenção de dados relacionados a infraestrutura social e estatal	Roubo de dados sensíveis	Desert Falcons (Arid Vipers)	Oriente Médio
Elise*	2015	T1218.011,T1055.001,T1105	Roubo de dados e destruição de patrimônio estatal	Destruição de infraestrutura estatal, tecnológica e obtenção ilegal de dados	Lotus Blossom (Spring Dragon)	Sul da Ásia
Petya	2016	T1486, T1210	Criptografar dados dos discos e cobrar por resgate	Destruição / roubo de dados sensíveis	-	Rússia
Trickbot	2016	T1105, T1110.004, T1185, T1573.001	Obtenção de dados	Vazamento de informações confidenciais	Wizard Spider	Rússia
Industroyer	2016	T1566, T1189	Destruir infraestrutura do estado	Disrupção do fornecimento de energia na Ucrânia	Sandworm (Unit 74455)	Rússia
Xtreme RAT*	2016	T1566.001, T1210	Roubo de dados	Roubo de dados sensíveis	Molerats (Gaza gang)	Oriente Médio
Wannacry	2017	T1486, T1210	Criptografar dados dos discos e cobrar por resgate	Danificar os dados e extorquir indivíduos ou organizações	Lazarus Group (Silent Chollina)	Coréia do Norte
NotPetya	2017	T1486, T1210, T1218.011, T1070.001	Destruir dados em computadores	Perda de dados, disrupção em infraestrutura estatal, perdas financeiras. Perdas estimadas em US$10 bilhões.	Sandworm (Unit 74455)	Rússia
SUNBURST	2020	T1195, T1573.001, T1027	Obtenção de dados confidenciais	Vazamento de informações confidenciais do governo norte-americano que utilizavam o software *Orion* da *SolarWinds*	APT-29 (Cozy Bear)	Rússia
Metaljack*	2020	T1566, T1210,T1048.003	Obtenção de dados confidenciais	Vazamento de informações confidenciais	APT-32 (OceanLotus)	Vietnã
DenisRAT*	2020	T1105,T1059,T1497.001	Acesso remoto e obtenção de dados	Vazamento de informações confidenciais	APT-32 (OceanLotus)	Vietnã

Fonte: resultado da pesquisa

Existem diversas ameaças utilizadas por APTs, cujo desenvolvimento do mecanismo de invasão foi financiado por estados. O mecanismo de invasão, também denominado como vetor, foi categorizado segundo a matriz MITRE ATT&CK de acordo com a característica de cada ataque.

A relação entre os ataques por ano e país pode ser sumarizada pelo gráfico na figura 4. É possível ter uma visão geral da atribuição por país dos ataques tabulados:

Figura 4 – Ataques por ano e país



Fonte: resultado da pesquisa

Dentre os 31 casos observados, é possível observar uma grande quantidade de ataques em 2014 e 2016. Além disso, é possível averiguar que diversos grupos atribuídos nos ataques citados nos artigos remetem a Rússia. Um aumento de ataques originados da Rússia em 2014 possui uma forte relação com o contexto geopolítico da invasão da península da Crimeia, até então território pertencente a Ucrânia, dando início a guerra Russo-Ucraniana. No final de 2015 e 2016, também houve casos de ataques da

Rússia a infraestrutura energética da Ucrânia, com os malwares BlackEnergy e Industroyer (FINKLE, 2016).

Em cada um dos casos, o impacto é proporcional a sofisticação do vetor utilizado pelo grupo para atingir o objetivo. Atores de países como Irã e Oriente Médio possuem metodologias menos sofisticadas em comparação a Rússia e Estados Unidos, cometendo mais erros de segurança operacional e são menos eficazes em atingir os objetivos planejados (LEMAY *et al.*, 2018).

Extraindo dados relacionados a cada ameaça mapeada, temos todos os vetores analisados através da matriz ATT&CK. Categorizando desta forma permite que cada um dos casos tenha seus vetores principais mapeados com a metodologia padrão utilizada no mercado em análises de ameaça profissionais (CYCRAFT TECHNOLOGY CORP, 2022), permitindo ter uma visão generalista de todas as táticas utilizadas para adentrar os sistemas, roubar dados, destruir e ocultar provas de acesso, entre outros. Entretanto, cabe ressaltar que não foi feita uma análise exaustiva de todos os possíveis vetores de ataque, pois fugiria do escopo deste artigo.

Está listada a descrição sucinta de todos os vetores encontrados, utilizando a matriz ATT&CK Enterprise v12:

1. **T0851**: indicação de um *rootkit*, que objetivamente esconde componentes como arquivos, bibliotecas, serviços e drivers do usuário e de outros programas;
2. **T0882**: roubo de informações operacionais;
3. **T1014**: uso do orquestrador de eventos WMI do Windows para persistir e elevar privilégios no sistema alvo;
4. **T1027.002**: uso de técnicas de empacotamento para mudar a assinatura do arquivo malicioso;
5. **T1027**: uso de criptografia, codificação e obfuscação em componentes em arquivos maliciosos para esconder seu conteúdo;
6. **T1041**: exfiltração de dados por servidor de comando e controle (*command & control* ou C2);
7. **T1048.003**: uso de protocolos não criptografados para enviar dados para servidor C2;

8 **T1055.001**: injeção de processo; libraria de vínculo dinâmico;
9 **T1056.001**: *keylogging* de teclas digitadas pelo usuário;
10 **T1059**: scripting malicioso, de forma geral;
11 **T1059.003**: *scripting* malicioso; Windows (CMD);
12 **T1059.004**: *scripting* malicioso; *shell* UNIX (bash, sh, zsh etc);
13 **T1068**: elevação de privilégios; uso de vulnerabilidades em componentes específicos do sistema operacional para ganhar acessos como usuário root (Linux) ou SYSTEM (Windows);
14 **T1070.001**: uso da ferramenta wevtutil para apagar logs de eventos no Windows, de forma a ocultar componentes maliciosos;
15 **T1070.004**: remoção de dados que indicam atividades maliciosas (ex.: logs);
16 **T1082**: obtenção de dados do sistema da vítima;
17 **T1105**: uso de servidores de comando e controle (C2) com o objetivo de transferir ferramentas e arquivos para os sistemas infectados, através de ferramentas como wget, finge, entre outros.;
18 **T1110**: ataque de força bruta, no caso de as senhas serem desconhecidas ou estarem em formato de *hash*;
19 **T1110.004**: força bruta; uso de bases de dados de login e senhas extraídos de outros ataques para tentar acessar sistemas-alvo;
20 **T1185**: roubo de sessão do navegador, extraindo a sessão com dados como cookies e senhas salvas para personificar a vítima;
21 **T1189**: uso de código Javascript malicioso ou anúncios maliciosos para explorar vulnerabilidades no navegador do usuário;
22 **T1190**: explorar vulnerabilidades de uma aplicação pública na internet, como sites ou portais de login;
23 **T1195**: ataque a cadeia de *supply-chain*, isto é, afetar os demais usuários que utilizam o software/componente afetado.
24 **T1204.002**: *dropper*; arquivo malicioso aberto pelo usuário que faz o download de outros malwares;
25 **T1210**: exploração de serviços remotos para obter acesso a rede interna, com a finalidade de realizar movimentos laterais dentro da rede;

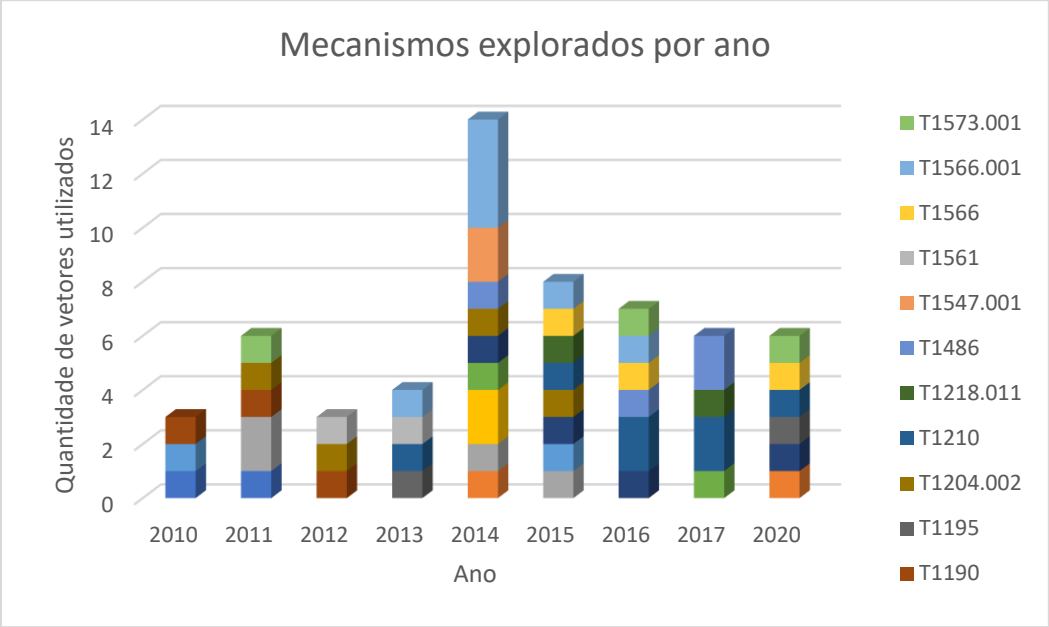
26 **T1218.011**: uso do executável rundll32.exe no Windows para ocultar componentes e comportamentos maliciosos;
27 **T1486**: encriptação de dados com o objetivo de interromper a disponibilidade dos dados dos sistemas afetados;
28 **T1497.001**: checagem do mecanismo do malware para descobrir se está sendo executado em ambiente virtualizado;
29 **T1547.001**: adição de entradas maliciosas de programas em pastas/chaves do registro para iniciarem em conjunto ao sistema;
30 **T1548.002**: abuso do mecanismo de elevação de privilégios do Windows (UAC) para forçar a operação do malware com privilégios elevados;
31 **T1561**: deleção do disco; malwares que utilizam componentes *wiper* visam apagar dados contidos em discos rígidos de sistemas específicos ou redes inteiras;
32 **T1562.001**: desativar ou desabilitar ferramentas de segurança do sistema para permitir comportamentos maliciosos;
33 **T1563.002**: roubo de sessão remota por meio do protocolo RDP para permitir o movimento lateral entre ambientes.
34 **T1566**: *phishing*; acesso a sistemas da vítima;
35 **T1566.001**: *phishing*; *spear-phishing* relacionado com o envio de arquivos maliciosos;
36 **T1566.003**: *phishing*; tática específica denominada *spear-phishing*, visando um indivíduo, setor ou companhia específica como alvo;
37 **T1573.001**: uso de criptografia simétrica nos canais de comunicação do servidor C2;
38 **T1574.010**: desviar e falsificar o fluxo de execução de processos, modificando e substituindo binários legítimos por maliciosos;
39 **T1584.005**: indicação de uma *botnet*, que possui diversos sistemas comprometidos realizando ações coordenadas;

Estas são as 39 principais técnicas de ataque utilizadas pelas ameaças citadas ao longo dos artigos, sintetizando os principais mecanismos de acesso, ataque, extração e destruição de dados utilizados pelos atacantes. No geral, a maioria dos mecanismos são comuns a todos os ataques, pois os objetivos de adentrar

sistemas, exfiltrar e/ou danificar dados e apagar rastros são generalistas para a maioria das ameaças.

Estão sumarizados, no gráfico da figura 5, a quantidade de exploração dos dez principais mecanismos de ataque utilizados pelas ameaças a cada ano, podendo visualizar a sumarização dos vetores mais utilizados a cada ano. A legenda representa as cores dos vetores exibidos e não a ordem de classificação de ocorrências.

Figura 5 – Mecanismos explorados por ano



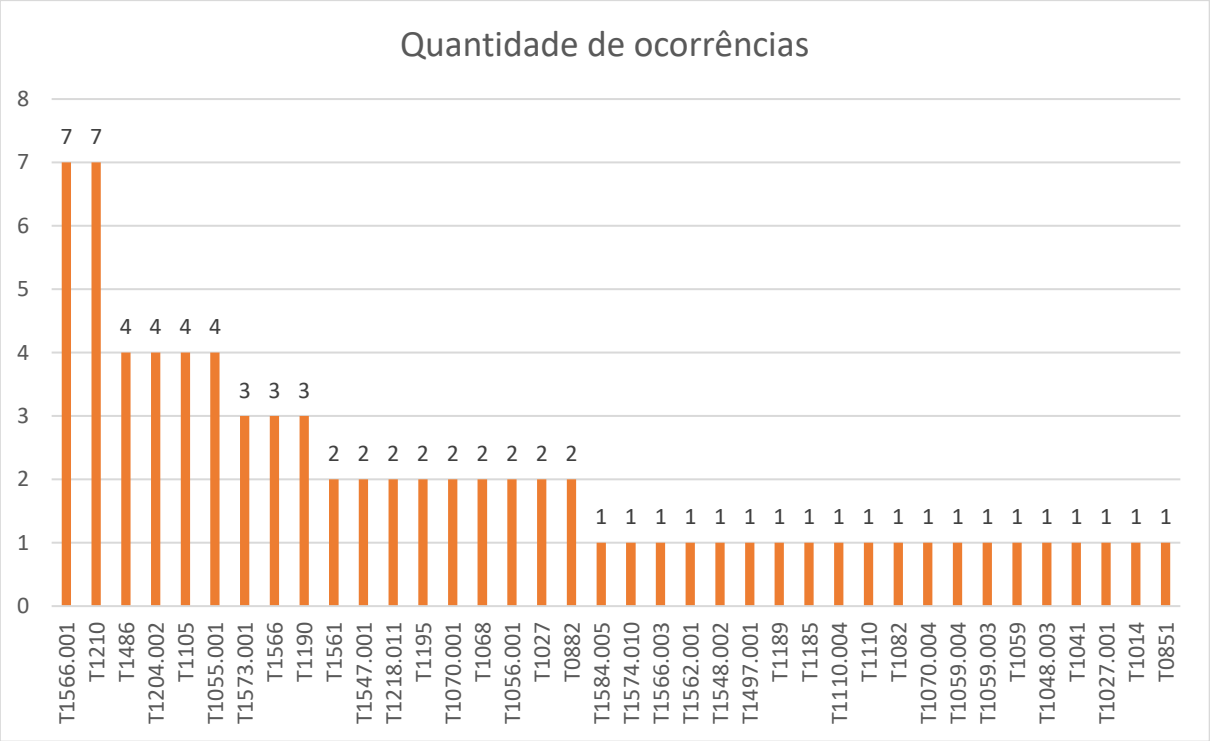
Fonte: resultado da pesquisa

Percebe-se no gráfico a grande quantidade de mecanismos utilizados nos diferentes períodos, notavelmente com um uso de técnicas relacionadas a encriptação do canal por onde os dados são extraídos (T1573), phishing (T1566), exclusão de dados por meio de componentes *wiper* (T1561), execução automática de *payloads* por meio scripts executados durante o login (T1547) e encriptação dos dados na máquina do alvo para causar impactar a disponibilidade (T1486). Há casos específicos de vetores que utilizam mecanismos mais complexos, que comprometem a cadeia de

suprimentos (denominada de *supply-chain*) de todos os outros softwares que utilizam o sistema afetado (T1195), sendo relevante salientar que tais técnicas tem forte elo e relação direta com os objetivos e motivações dos adversários que determinam como eles agem quando adentram a infraestrutura tecnológica alvo. Também é válido pontuar a importância dos eventos sócio e geopolíticos vigentes, um dos principais catalisadores e norteadores dos APTs.

Analisando todo o espectro de vetores utilizados pelas ameaças, temos o gráfico na figura 6. Ele sumariza os vetores mais utilizados pelos 31 ataques, proporcionando uma visão dos métodos mais utilizados pelos ataques tabulados.

Figura 6 – Quantidade de ocorrências por técnica de ataque



Fonte: resultado da pesquisa

Destacam-se o uso de spear-phishing para conseguir distribuir a ameaça para potenciais vítimas (T1566.001), exploração de serviços remotos para movimentação lateral depois de comprometer o sistema (T1210), encriptação de dados (T1486),

execução de arquivo malicioso por parte do usuário (T1204.002), transferência de arquivos externos ao sistema infectado (T1105) e injeção de processo para ocultação de comportamento malicioso (T1105). É cabível notar que estes vetores são comuns dentro do aspecto analisado, levando em consideração ameaças desenvolvidas por atores financiados por estados. Comportamentos comuns a diversas ameaças é o uso de um servidor de comando e controle (*C&C server* ou *C2*) para poder enviar os dados coletados no sistema infectado e interagir com o ambiente comprometido para executar novas ações durante o período da intrusão.

Os gráficos da figura 5 e figura 6 distinguem as técnicas de ataque mais utilizados categorizados em duas formas diferentes. O primeiro gráfico permite visualizar os dez mecanismos mais utilizados ao longo de todos os casos analisados entre 2010 e 2021, mostrando que os anos com mais variações de vetores foram 2014, 2015 e 2016, podendo notar o alto uso de mecanismos como spear-phishing, *key-logging* e encriptação dos dados das vítimas, relacionando-se fortemente com o contexto geopolítico previamente apresentado. O segundo gráfico permite visualizar os mecanismos mais utilizados em um contexto geral, sem levar puramente em consideração contextos externos. A relação entre os dois gráficos permite observar nuances relacionadas a eventos externos com outra focada no número bruto de técnicas empreendidas pelos diferentes grupos e ataques.

4.2 O PROBLEMA DA ATRIBUIÇÃO

Nos artigos analisados, diversos pontos comentados pelos autores permitiram confirmar hipóteses e percepções vinculadas a evolução e impacto das ameaças cibernéticas. Como comentado anteriormente, um dos pontos a serem considerados é a atribuição da invasão. Conseguir encontrar o culpado definitivo da exploração da ameaça é uma tarefa dispendiosa e interdisciplinar, muitas vezes exigindo diferentes óticas para se ter uma noção completa do dano causado. Para que o processo de atribuição seja efetivo, é necessário seguir o fluxo de intrusão da ameaça: iniciar quando o incidente foi percebido

na infraestrutura onde os dados estão sendo protegidos (RID; BUCHANAN, 2014).

Rid e Buchanan (2014) propuseram uma metodologia para auxiliar no processo, o modelo Q, que determina as diversas etapas de atribuição de um ataque: tático/técnico, operacional e estratégico, além da etapa de comunicação para evidenciar o resultado do processo. Tais etapas, na metodologia proposta, abordam camadas técnicas e não-técnicas para analisar o processo e o dano causado pela invasão e pelo uso da ciberameaça.

Em todo o processo, a importância da interdisciplinaridade da equipe é relacionada ao fato de que a atribuição não é linear. Diversas medidas realizadas no nível tático podem ser realizadas em conjunto com medidas estratégicas para mitigar os danos causados, além de contribuírem com a comunicação do ataque. É valido pontuar que a atribuição é um processo dispendioso de tempo e recursos financeiros, requerendo uma quantidade crescente de recursos com base na sofisticação do atacante em esconder seus rastros. Este, inclusive, é um dos maiores pontos de dificuldade em se atribuir ciberataques, como citado por alguns dos autores dos artigos analisados. Medidas adequadas de segurança operacional e o avanço das tecnologias utilizadas para esconder os dados são grandes barreiras para facilitar o processo de atribuição de um ciberataque. Mas, para se mitigar os danos, ter uma visão geral de todos os ativos impactados e coletar dados para robustecer o modelo de ameaça, é preciso iniciar tal processo de atribuição.

No fluxo existente na realização do ataque, os atacantes podem possuir motivações obscuras ou bem definidas, a depender de seu nível de sofisticação. Esta correlação foi percebida ao se correlacionar diversos casos em que a atuação de Advanced Persistent Threats (APTs) foi identificada. No caso dos APTs, eles são financiados por estados: organizados, bem estruturados e que geralmente operam com regras (e horários) bem definidos (LEMAY *et al.*, 2018). Isto leva que os ataques conduzidos por esses grupos sejam muito mais avançados em relação a ataques conduzidos por grupos criminosos convencionais. Esta diferença de atuação leva a um grande desafio,

explorado por alguns dos autores dos artigos: “como conduzir políticas, procedimentos e metodologias para mitigar o risco dos ataques em recursos essenciais?”. Esse questionamento sintetiza a necessidade da criação de políticas mais específicas e atualizadas para lidar com essa mudança constante de atores e ameaças. SHACKELFORD, SCOTT J.; cita a necessidade da colaboração entre o estado e as organizações privadas para aumentar a capacidade de adaptação e a eficiência do processo de gestão de risco por parte das organizações detentoras de ativos informacionais, evidenciando que muitos países possuem manifestos e leis que tratam de cibersegurança, mas não as colocam em prática. Embora o autor não aborde exemplos palpáveis desta violação em seu artigo, casos como a interferência russa nas eleições americanas (TENOVE *et al.*, 2018) demonstram que ainda há muito a se fazer para robustecer todo o processo de atribuição e mitigação dos riscos associados aos dados em sistemas críticos.

4.3 IMPACTO DOS CIBERATAQUES

De fato, a atuação de grupos criminosos menores eleva ainda mais a necessidade de se haver ações claras para mitigação de risco pelas companhias e órgãos governamentais. Pela tabela de ameaças, notou-se que existe um grande uso de phishing em conjunto com outros vetores utilizados. Essa forma de ataque é comumente utilizada por grupos criminosos em alvos que possuem certa informação privilegiada (spear-phishing) ou em alvos em contextos sociais específicos, como a pandemia de COVID-19 (LALLIE *et al.*, 2020). Tais ataques não são robustos e tampouco exploram vulnerabilidades *zero-day*, mas possuem um grande impacto no sentido de causarem danos a uma grande quantidade de pessoas e a infraestrutura por elas utilizadas (TRAUTMAN, 2016). LALLIE *et al.*, 2020 abordou em “*Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic*” o aumento destes ataques decorrentes da mudança como as pessoas consomem a tecnologia, dando como exemplo casos que ocorreram no Reino Unido e Estados Unidos. Também foi possível observar grande impacto social em ataques a grandes corporações que lidam com dados

pessoais sensíveis, como bancos, empresas de entretenimento e até mesmo de relações extraconjugais (AGRAFIOTIS *et al.*, 2018, p. 9-11). O fator crítico passa a transitar de recursos públicos-privado para as informações pessoais, mostrando como um determinado acontecimento na sociedade pode servir de gatilho para o aumento de casos de ciberataques que miram em atingir as grandes massas.

Voltando a análise para os casos de atores financiados por estados, o uso militar dos ataques e estratégias de vazamento de dados e espionagem é corriqueira. A tabela apresenta diversos casos emblemáticos cuja ameaça e todo o mecanismo utilizado foram fabricados para danificar infraestruturas críticas. O potencial de danos de uma arma cibernética, ainda que perceptivamente menor que uma arma cinética, é igualmente destrutivo. Questionamentos e conclusões levantadas por Trautman (2016), Robinson e Janicke e Robinson (2014) corroboram com conjunturas relacionadas a vastidão da possível destruição em casos de uma guerra total que utilizem tais ameaças cibernéticas.

Em casos factíveis, entretanto, existem diversas ameaças utilizadas no contexto de guerra e disputa territorial. A Rússia realizou diversos ataques a infraestrutura energética da Ucrânia em 2016, utilizando-se de ameaças meticulosamente fabricadas para impactar usinas de energia, como o malware *BlackEnergy*, *Havex,* entre outros, principalmente através do APT *Sandworm* (FINKLE, 2016).

Tais investidas de grupos criminosos e financiados por estados não acontecem somente em componentes críticos da infraestrutura estatal. Como apontado por Trautman (2016), recursos como escolas, prefeituras e hospitais são vulneráveis e alvos valiosos pois dispõem de tecnologia arcaica e pouco atualizada contra muitas vulnerabilidades. Em concordância com o questionamento geral levantado pelos autores, armas cibernéticas possuem um impacto muito maior, pois podem, sorrateiramente, destruir dados, sistemas e causar uma disrupção em componentes essenciais para o devido funcionamento da sociedade moderna. Como apontado pelo mesmo autor no

artigo *“Is Cyber Attack the Next Pearl Harbor”*, de 2015, já se havia uma previsão e preocupação de ferramentas mais poderosas, munidas de mecanismos criptográficos, de serem utilizadas para atacar sistemas críticos e destruir os dados.

Sumarizando os pontos levantados, prejuízos financeiros relacionados a ciberataques são estimados em US$10,5 trilhões em 2025, levando em consideração a evolução das ameaças, a criticidade dos recursos atingidos e a falta de políticas efetivas para mitigar os danos (MORGAN; STEVE, 2021). Devido a acontecimentos como a pandemia de COVID-19 acelerando a digitalização das pessoas, mais dados ficam expostos a ataques na internet. O Secretário de Defesa dos EUA, Ash Carter, citou em 2015 que o baixo custo de se desenvolver novas ferramentas maliciosas e o avanço da tecnologia utilizada para construção dos *malwares* potencializou o nível do impacto causado por diversos atores. Por conseguinte, espera-se que os prejuízos financeiros aumentem na mesma proporção (TRAUTMAN, 2016).

4.4 EVOLUÇÃO DAS AMEAÇAS CIBERNÉTICAS

Mediante a análise dos artigos e a exemplificação de diversos casos apontados pelos autores, pode-se notar que as ameaças possuíram uma crescente em relação ao impacto causado tanto em termos monetários quanto em relação a destruição causada. Cabe notar que, por mais que não houve um foco por parte dos autores em quantificar casos de ciberataques em um período esparso, pode-se um grande foco em pontuar aspectos relacionados aos casos mais impactantes. Foi possível notar uma correlação entre eventos externos, com conflitos armados, tensões geopolíticas, crises sociais e mudanças políticas com o aumento de ações de ciberataque, ciberterrorismo e ciberespionagem.

Sob a perspectiva global, casos envolvendo ciberameaças só tendem a aumentar. Um indicativo deste aumento é a grande quantidade de casos que emergiram durante a pandemia de COVID-19. Conforme pontuado por LALLIE *et al.* (2020), em um curto período entre o final de 2019 e 2020, houve

43 casos de ataques explorando diversos vetores de ataque para atingir as pessoas.

Agora, sob a perspectiva tecnológica, ao analisar algumas das principais ameaças analisadas nos artigos, é possível notar que elas possuem vários componentes e mecanismos originários de malwares predecessores, como no caso do Stuxnet e Duqu, onde o último reutilizou diversos componentes do primeiro.

Com a crescente de prejuízos ano a ano, decorrentes com a evolução das ameaças, torna-se necessário haver metodologias padronizadas que acompanhem a evolução das ameaças para um processo adequado de ciberinteligência. Pesquisadores e pessoas chave do negócio necessitam estar a par de casos famosos de ciberataques, dos mecanismos explorados e de como implementar medidas de prevenção contra-ataques e ameaças diversas (BROADHEAD, 2018). Protocolos como o NIST framework, desenvolvido pelo Departamento de Defesa dos Estados Unidos, têm tido uma grande adoção entre potencias mundiais líderes no setor de inteligência e risco corporativo (SHACKELFORD, SCOTT J.;, 2015), fazendo com que exista uma cooperação entre setor público e privado. No âmbito isolado de uma organização, protocolos como WISP são úteis para se ter uma visão de protocolos e ativos informacionais essenciais para as operações (TRAUTMAN; ORMEROD, 2018).

4.5 SÍNTESE DA ANÁLISE DE RESULTADOS

Mediante a análise de todos os artigos e a coleta de informações de fontes adicionais apontadas em cada um deles, foi possível se ter uma visão geral evolução das ameaças e uma tabulação das mais expressivas dentre 2010 e 2021. Analisando o impacto causado por elas, pode-se ter uma visão macro de como a infraestrutura é afetada, como organizações podem ter seus fluxos de processos interrompidos e como, em um contexto financeiro amplo, as perdas e prejuízos são refletidas tanto em corporações privadas e setores públicos, principalmente quando um ataque atinge recursos críticos. Também foi possível, através do uso do framework ATT&CK e da análise individual dos casos de ciberataques citados nos artigos, enumerar as técnicas principais

utilizadas pelos APTs e seus softwares maliciosos, proporcionando assim mais um conjunto de dados que fornecem informações para quantificar o impacto destas ameaças assim como vulnerabilidades quanto a protocolos, processos e sistemas. Entretanto, cabe salientar que uma limitação desta pesquisa é a falta de dados específicos que quantificam, em ordem cronológica, o impacto de um grande número de ciberataques. Devido a constante evolução das tecnologias e métodos, foi percebida uma falta de coesão entre como grandes casos são reportados por pesquisadores versus a grande quantidade de pequenos casos existentes.

5 CONSIDERAÇÕES FINAIS

Com base na contextualização inicial em relação a evolução tecnológica em nossa sociedade e como ela introduz novas vulnerabilidades no fluxo de dados e informações, pode-se ter uma ideia de como novas tecnologias e procedimentos mudaram drasticamente o valor dos dados e informações em um contexto informatizado. A respeito da 1ª proposição, “Avanço das ameaças cibernéticas em um curto período (2010-2021) quando comparado com o período de popularização da computação pessoal.”, por meio da análise dos autores sob diversos pontos de vista em relação a ciberataques, foi possível constatar a evolução dos ciberataques em termos da tecnologia utilizada para impactar as vítimas, uma evolução em termos do prejuízo financeiro e também na crescente importância abordada em termos do uso de ciberataques como armas de guerra, cujos efeitos são potencialmente mais destrutivos do que armas cinéticas. A categorização das ameaças demonstra uma miríade de casos e mecanismos de ataque relacionados, além da grande disrupção em termos de impacto que ameaças como Wannacry e NotPetya tiveram.

Sobre a 2ª e 4ª proposição, “*Impacto causado pela exploração de certas vulnerabilidades em certos protocolos*” e “*Existência de diversos grupos financiados por governos difundidos pelo ciberespaço*”, a abordagem geral visualizada em todos os artigos é uma constatação da evolução dos mecanismos utilizados pelos softwares maliciosos e do grande interesse de estados financiarem operações de grupos especializados – os APTs – para poderem realizar operações de ciberespionagem, destruição de dados e prejuízo a infraestruturas críticas,

podendo visualizar em detalhes como tais grupos tiveram diversas atuações dentre os 31 casos analisados. Com isso, foi possível traçar uma correlação entre acontecimentos sociais, geopolíticos e militares com uma crescente nos casos de ciberataques direcionados a pessoas ou infraestrutura estatal crítica.

Em termos metodológicos e da análise dos artigos escolhidos, as principais ameaças citadas pelos autores referenciados foram tabuladas. Esta estratégia proporcionou uma visão geral de todos os mecanismos utilizados (também chamados de técnicas de ataque ou técnicas ofensivas) por cada uma das ameaças para acessarem, exfiltrarem, causar danos e apagarem rastros nos sistemas, assim como as diversas formas de iludir e enganar os usuários destes. Os autores também abordaram a grande deficiência de organizações privadas e órgãos públicos em aplicar e/ou atualizar procedimentos relacionados à segurança informacional, algo constatado pelos dados apresentados e pelo grande impacto de casos que utilizam mecanismos de criptografia e deleção de dados.

Os pontos supracitados levam a confirmação da 3ª proposição, "*Incerteza em relação a segurança do tratamento de dados pelas grandes corporações, levando em conta como protocolos e medidas são aplicadas e o nível de impacto dos ataques*", sobre uma grande necessidade de órgãos privados e públicos de atualizarem suas políticas de segurança informacionais para contemplares aspectos preventivos contra estas novas classes de ameaça, com o uso de ferramentas de defesa em um amplo espectro na arquitetura tecnológica. Em termos governamentais, urge a necessidade de atualizar legislações e disseminar processos de pesquisa na área de cibersegurança para entenderem o estado das ameaças em termos da sofisticação e impacto dos mecanismos de intrusão e ataque.

Através de todas as informações dispostas, tanto na sumarização gráfica dos ataques quanto na categorização dos mecanismos utilizados por eles, foi possível ter uma visão de como a evolução tecnológica introduziu novas vulnerabilidades exploradas pelas ameaças cibernéticas, evidenciando como as diferentes classes de ataques, atores e contextos dentro da cronologia proposta causaram um grande impacto e prejuízo em diferentes situações.

Por fim, ainda há espaços para evoluir a temática abordada nesta pesquisa. Uma expansão desta análise histórica generalista com uma análise detalhada dos

mecanismos (ou *payloads*) tem relevância para entender a conexão entre os softwares maliciosos e a evolução de mecanismos compartilhados, mesclando componentes de engenharia reversa para poder aprofundar dentro das estruturas responsáveis por realizar diferentes funções dentro dos malwares.

REFERÊNCIAS

AGRAFIOTIS, I. *et al.* A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. **Journal of Cybersecurity**, 4, 16 outubro 2018., p. 15

BROADHEAD, S. The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments. **Computer Law & Security**, Londres, 18 setembro 2018., p. 16

CAPANO, D. E. Throwback attack: How notpetya accidentally took down Global Shipping Giant maersk.. **Industrial Cybersecurity Pulse**, 2022. Disponivel em: https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-how-notpetya-accidentally-took-down-global-shipping-giant-maersk/. Acesso em: 23 outubro 2022.

CYBERSECURITY VENTURES. Cybercrime damages $6 trillion by 2021. **Cybercrime Magazine**, 2020. Disponivel em: https://cybersecurityventures.com/annual-cybercrime-report-2017/. Acesso em: 20 novembro 2022.

CYCRAFT TECHNOLOGY CORP. CyCraft. **Medium**, 2022. Disponivel em: https://medium.com/cycraft/cycraft-classroom-mitre-att-ck-vs-cyber-kill-chain-vs-diamond-model-1cc8fa49a20f. Acesso em: 13 nov. 2022.

FALLIERE, N.; MURCHU, L. O.; CHIEN, E. **W32.Stuxnet Dossier**. Symantec Corp. [S.l.], p. 69. 2011.

FARWELL, J. ; ROHOZINSKI, R. **Stuxnet and the Future of Cyber War**. 1ª. ed. Londres: Routledge, v. 53, 2011. p. 23-40. Acesso em: 18 outubro 2022.

FINKLE, J. U.S. firm blames Russian 'Sandworm' hackers for Ukraine outage. **Reuters**, 2016. Disponivel em: https://www.reuters.com/article/us-ukraine-cybersecurity-sandworm-idUSKBN0UM00N20160108. Acesso em: 6 outubro 2022.

FIREEYE. Highly evasive attacker leverages Solarwinds Supply Chain to compromise multiple global victims with Sunburst Backdoor.. **Mandiant**, 2020. Disponivel em: https://www.mandiant.com/resources/blog/evasive-attacker-

leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor. Acesso em: 22 outubro 2022.

GREENBERG, A. The untold story of notpetya, the most devastating cyberattack in history.. **Wired**, 2018. Disponivel em: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/. Acesso em: 29 outubro 2022.

JANCZEWSKI, L.; COLARIK, A. **Cyber Warfare and Cyber Terrorism**. 1ª. ed. Hershey: IGI Global, 2008. p. 565.

KELLEY, M. B. The stuxnet attack on Iran's nuclear plant was 'far more dangerous' than previously thought. **Business Insider**, 2013. Disponivel em: https://www.businessinsider.in/The-Stuxnet-Attack-On-Irans-Nuclear-Plant-Was-Far-More-Dangerous-Than-Previously-Thought/articleshow/26113763.cms. Acesso em: 22 outubro 2022.

LALLIE, H. S. *et al.* Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. **ScienceDIrect**, Coventry, Reino Unido, p. 20, 28junho. 2020.

LEMAY, A. *et al.* Survey of publicly available reports on advanced persistent threat actors. **Computers & Security**, Montréal, Volume 72, 2018., p. 26-59 Acesso em: 15 outubro 2022.

MORGAN; STEVE. Cybercrime to cost the world $10.5 trillion annually by 2025. **Cybercrime Magazine**, 2021. Disponivel em: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/. Acesso em: 7 novembro 2022.

PAGE, M. J. *et al.* The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. **Systematic Reviews**, n. 10, 29 mar. 2021. Acesso em: 05 abril 2022.

RID, T.; BUCHANAN, B. Attributing Cyber Attacks. **Journal of Strategic Studies**, Londres, 2014., p. 4-37 Acesso em: 6 março 2022.

ROBINSON, M.; JONES, K.; JANICKE, H. Cyber Warfare – Issues and Challenges. **Computers & Security, , 70–94. doi:10.1016/j.cose.2014.11.007** , n. 49, 29 julho 2014., p. 70-94 Acesso em: 3 outubro 2022.

ROSENSTEIN; J., R. Deputy attorney general Rod J. Rosenstein delivers remarks at the Cambridge Cyber Summit. **The United States Department of Justice**, 2020. Disponivel em: https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-cambridge-cyber-summit. Acesso em: 20 novembro 2022.

SHACKELFORD, SCOTT J.. Protecting Intellectual Property and Privacy in the Digital Age: The Use of National Cybersecurity Strategies to Mitigate Cyber Risk. **Kelley School of Business Research Paper**, Bloomington, 23 julho 2015., p. 15-56 Disponivel em: https://ssrn.com/abstract=2635035. Acesso em: 18 outubro 2022.

TENOVE, C. *et al.* Digital Threats to Democratic Elections: How Foreign Actors Use Digital Techniques to Undermine Democracy. **SSRN**, Colúmbia Britânica, 2 outubro 2018., p. 80 Disponivel em: https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3235819_code2404786.pdf?abstractid=3235819&mirid=1. Acesso em: 11 outubro 2022.

TRAUTMAN, L. J. Is Cyberattack the Next Pearl Harbor? **UNC School of Law**, Chapel Hill, Carolina do Norte, 12 janeiro 2016., p. 58

TRAUTMAN, L. J.; ORMEROD, P. Wannacry, Ransomware, and the Emerging Threat to Corporations. **Tennessee Law Review**, 24 agosto 2018., p. 54 Acesso em: 24 outubro 2022.