SANDWORM: uma nova era na guerra cibernética e a caça pelos hackers mais perigosos do Kremlin.

GREENBERG, Andy Traduzido por Debora Ramires. Rio de Janeiro: Alta Books, 2021. 326 p.

Resenhado por Luiz Felipe Lima Santos.

A obra apresenta a história de um grupo de criminosos cibernéticos, supostamente patrocinado pelo governo russo, conhecido pelo codinome Sandworm, abordando assuntos como guerra cibernética, ações de atores estatais e não estatais, malwares, inteligência e contrainteligência, relações internacionais, impactos no meio físico e uso do domínio cibernético como possibilidade de influenciar e afetar outros estados.

Em uma era de conflitos sem fronteiras, todos vivemos na linha de frente dessas intercorrências. Assim, o livro leva ao leitor, seja um profissional de segurança, um entusiasta no assunto ou pessoas interessadas em se manter atualizadas, ao detalhar o submundo de ações cibernéticas, que qualquer nação ou organização possa sofrer.

Andy Greenberg é escritor sênior renomado que escreve para a revista Wired[1] e aborda temas como segurança, privacidade, liberdade de informação e cultura hacker. É autor dos livros Tracers in the Dark: The Global Hunt for the Crime Lords of Cryptocurrency e This Machine Kills Secrets. Ganhou o Prêmio Gerald Loeb de Reportagem internacional, o Prêmio Sigma Delta Chi da Sociedade de Jornalistas Profissionais e a Menção por Excelência do Prêmio Cornelius Ryan do Overseas Press Club.

Verificando as fontes do livro, percebe-se em sua bibliografia que o autor realizou uma série de entrevistas com fontes que compartilharam suas experiências na temática. Por isso a leitura é abundante em detalhes, levando ao leitor uma contextualização dos fatos, proporcionando um entendimento mais claro das questões específicas de um mundo cada vez mais carente de proteção cibernética. O título do livro é provocativo: o que poderiam ter em comum guerra cibernética e Sandworm (tradução literal: “verme de areia”)? A escolha do título se deu ao fato de uma aparente obsessão dos ciberespiões pelo romance Duna (o épico de 1965 de Frank Herbert), sendo escolhido um nome que fosse direto e se fizesse analogia ao referido romance, evolvendo um monstro oculto que emerge abaixo da

[1] *Wired* é uma revista estadunidense, de publicação mensal, com sede em San Francisco, Califórnia, que aborda questões envolvendo tecnologia, ciência, entretenimento, design e negócios.

superfície para brandir um terrível poder. Como um verme se esconde sob a superfície do deserto, os hackers do grupo Sandworm operam nas sombras do ciberespaço.

A obra se divide em seis partes que descrevem a história do grupo Sandworm. Cada parte abrange uma série de capítulos que narram desde a origem, a evolução, os ataques, os impactos, a identificação do grupo, bem como as lições aprendidas acerca das ações desses hackers.

Na primeira parte, Greenberg relata como o grupo Sandworm surgiu, descrevendo detalhes das primeiras pistas de suas ações. Pesquisadores das empresas de inteligência de ameaças iSight[2] e ESET descobriram, a partir de 2014, acreditando ser uma vulnerabilidade de zero-day[3] , por meio de análises de diversas amostras do malware BlackEnergy, uma inteligência malévola e remota que mais tarde eles associariam às ações do grupo de hackers Sandworm. Os binários desse malware analisados continham algo em comum: todos faziam referências ao romance Duna, servindo de impressão digital do Sandworm. Além disso, descobriram mais tarde que arquivos de 2009 também eram ligados a esse romance. Dessa forma, deduziu-se que a campanha hacker não se estendia por meses, mas sim por anos. Tudo indicava ser uma campanha sofisticada do governo russo mirando a OTAN e a Ucrânia.

Com a evolução das pesquisas, perceberam-se que as ações cibernéticas tinham um propósito de "Multiplicador de Forças", pois o referido grupo não focava apenas em espionagem. Eles tentavam alcançar os sistemas das vítimas, sequestrando maquinário físico e trazendo brechas entre o digital (não cinético[4]) e o cinético.

Em 2014, com o foco de desacreditar o Estado perante à população ucraniana, o serviço de telecomunicações, as empresas de eletricidade e o sistema eleitoral sofreram ataques cibernéticos. Ademais, os pesquisadores constataram intrusões do Sandworm em algumas infraestruturas que não eram apenas ucranianas e polonesas, mas também em norte-americanas.

---

[2] A iSight não foi necessariamente a primeira a ligar os pontos sobre as impressões digitais do grupo de hackers. A empresa ESET estava, ao mesmo tempo, fazendo as mesmas descobertas, incluindo códigos de campanha com a temática Duna no malware do grupo. Contudo não publicou suas descobertas online e assim a iSight foi amplamente creditada.

[3] *Zero-day*: designação atribuída à situação na qual há uma ameaça capaz de explorar uma vulnerabilidade de segurança descoberta em sistemas computacionais e que não teve, ainda, correção disponibilizada pelo desenvolvedor ou fabricante.

[4] A guerra cinética reside no mundo real sujeito a mudanças mediante a aplicação de conceitos da física. A não cinética caracteriza-se no mundo virtual.

Na segunda parte do livro, o autor recorre a cinco flashbacks, ou seja, interrompe momentaneamente a cronologia da história do Sandworm para descrever ações cibernéticas do passado que mais tarde se relacionariam, de alguma forma, com os ataques desse grupo russo. Dessa forma, o autor cita uma experiência secreta dos EUA, em 2007, denominado Aurora, no campo de testes do laboratório nacional de Idaho (EUA), que demonstrou ser um potencial de infligir consequências físicas por meio de ataques digitais. Em seguida, menciona o incidente Moolight Maze, em 1998, considerado um dos mais duradouros ataques cyber avançados da história, em que a Rússia saqueou os segredos do governo e das forças armadas estadunidenses por anos.

Na sequência, Greenberg descreve os ataques da Rússia, entre 2007 e 2008, a diversos sites estatais da Estônia e Geórgia. Um ponto curioso observado refere-se ao fato dos ataques físicos e digitais terem sido sincronizados.

Nessa parte de flashbacks do livro, o autor encerra com a famosa ação cyber estadunidense: o Stuxnet[5] . Os hackers por trás do Stuxnet perderam o controle de sua criação, expondo-a ao mundo, pois a descoberta desse código, em 2010, começou semelhantemente à descoberta do Sandworm, ocorrida anos depois: um zero-day. E qual foi o preço do Stuxnet? As vulnerabilidades de zero-day utilizadas não as haviam sido relatadas à Microsoft para que estas fossem corrigidas a outros usuários. Assim, essas vulnerabilidades das máquinas ao redor do mundo foram exploradas em segredo. Priorizou-se, assim, uma ofensiva militar em vez da defesa civil. Daí Greenberg traz à discussão as seguintes perguntas: quantos zero-days poderosos o governo dos EUA escondeu? Se mais tarde essa arma fosse apontada para os EUA ou seus aliados, como eles poderiam contestá-la eticamente? A destruição física por meio do código se tornou uma regra aceitável do jogo global? Possíveis respostas mostram a aceitação deoutra forma de corrida armamentista — com consequências severas e imprevisíveis.

Na terceira parte do livro, é narrada a evolução do grupo ao longo da década de 2010. O livro apresenta ações do grupo Sandworm em novas modalidades. A obtenção de informações comprometedoras sobre oponentes políticos, influenciando a opinião pública, demonstra que o grupo empregava operações de informação. Além disso, o autor descreve

[5] Um pedaço de código, criado por *hackers* dos EUA, com contribuição de Israel, projetado para paralisar o programa nuclear do Irã de modo tão efetivo quanto um ato de sabotagem física, executado nas profundezas do coração de Natanz-Irã e sem riscos ou danos colaterais de um ataque militar completo.

ações dissuasórias da Rússia contra a estratégia de ciberguerra norte-americana ao relatar que a Rússia apagou as luzes em Kiev e foi capaz de penetrar na rede norte-americana, mostrando ao mundo, principalmente ao ocidente, suas capacidades de ação no espaço cibernético.

O autor encerra essa parte do livro relatando ainda que a Rússia, construiu seu próprio StuxNet: o "Industroyer ou Crash Overrride". Esse malware possui a mesma capacidade de gerar efeitos cinéticos, mormente habilidades de destruir sistemas de controle industrial. Agora, esse software malicioso criado pelos EUA poderia ser usado contra si.

Na quarta parte, o autor relata uma série de ataques em 2017, os quais foram considerados o "ano de apogeu" da empreitada do grupo sandworm, tais como: o ataque à empresa Maersk[6] , que conrrompeu profundamente sua rede, ao causar um problema de magnitude nunca vista no transporte global; o "hackeamento" dos melhores hackers da Agência Nacional de Segurança (NSA[7]) dos EUA, a "Equation Group", uma equipe de elite dos ciberespiões; o novo ransomeware de Wannacry, o qual foi impulsionado por um zero-day da NSA (EternalBlue[8]), que causou estrago pelo mundo; e o ataque do worm NotPetya[9] às empresas multinacionais e aos correios ucranianos. Destaca-se que embora os correios ucranianos não sejam tão importantes quanto às empresas multinacionais atacadas, são considerados um pilar da central da sociedade, pois não representam tão somente a troca de correspondências, mas também a transferência de fundos monetários, como o pagamento de pensões a cerca de 4,5 milhões de aposentados. O somatório de ataques do grupo atingiu aproximadamente um prejuízo de mais de 10 bilhões de dólares.

Em sua quinta parte, o livro traz a identidade do grupo. Em janeiro de 2018, apesar das pistas serem confusas, levantou-se que uma agência no governo russo, o GRU[10]

---

[6] A gigante marítima que representa quase um quinto de toda a capacidade de transporte marítimo do mundo estava "morta na água".

[7] National Security Agency - NSA

[8] Exploit (programas que aproveitam os pontos fracos de software) de ataque cibernético desenvolvido pela agência de Segurança Nacional dos EUA.

[9] A *ciber* arma mais devastadora na história da internet que apresentava máxima virulência e usava o Mimikatz e o *EternalBlue* em conjunto. O Mimikatz permitia que usuários governamentais e corporativos de Windows provassem sua identidade de forma mais conveniente em diferentes aplicativos em suas redes ou na web. Dessa forma, seu login só precisava ser inserido uma única vez e poderia ser usado sem esforço para desbloquear outros programas sensíveis. O *Sandworm* não escreveu seu próprio Mimikatz, apenas tomou o próprio.

[10] O GRU (abreviatura em russo de Departamento Central de Inteligência). Inicialmente criado por lênin em 1918 para servir de olhos e ouvidos do exército Vermelho e equilibrar o poder da temida KGB. Possuía uma disciplina de confidencialidade institucional. Composta por raros desertores e agentes secretos.

(Unidade 74455), era responsável por pelo menos três dos marcos de hacking mais destacados da história: a) esta unidade projetou os primeiros apagões causados por hackers; b) interferiu na eleição presidencial estadunidense; e c) criou a ciber arma mais destrutiva já lançada, o NotPetya. A atribuição desse malware às forças militares russas foi a confirmação mais forte até então da identidade GRU do Sandworm.

Na sexta parte, última do livro, o autor aborda as lições aprendidas em um ambiente de guerra cibernética, indagando ao leitor a seguinte questão: Qual a causa da inação dos EUA frente à ciberguerra da Ucrânia? É a distância ou talvez porque a Ucrânia não faz parte da OTAN? O autor responde a essas questões após entrevistas de especialistas, alegando que os EUA poderiam não querer que ciberataques contra infraestruturas críticas ocorressem além dos limites esperados, pois eles também desejam executar tais ataques. Os especialistas declaram, com uma visão bem realista, necessário advogar pela disrupção da infraestrutura em tempos de paz, mas que, em tempos de guerra. Esta pode ser um alvo legítimo, caso seja compreendida como alvo militar, ao se auferir vantagens táticas ou estratégicas. De maneira velada, os EUA acabam por justificar as ações russas. Entretanto, especialistas destacam que o mundo precisa de uma nova "Convenção de Genebra digital", ou seja, um conjunto de regras mais estreitas, ou seja, que não ocorra ciberataque em hospitais, em zonas consideradas de exclusão cibernética, que se configurariam, no caso de descumprimento, em crime de guerra internacional.

O autor encerra o livro com o seguinte ensinamento: em que pese não possuirmos definições legais de enquadramento de ataques cibernéticos indiscriminados, há a necessidade de treinar equipes ciber responsáveis pela funcionalidade das infraestruturas críticas, de modo a prover proteção e resiliência cibernética.

Por fim, o autor revisita o seguinte paradoxo para a sociedade moderna: a proteção da sociedade das dependências tecnológicas requer o oposto da interdependência. Em outras palavras, pode-se dizer que a sociedade ao se transformar cada vez mais dependente da tecnologia, torna-se mais vulnerável e mais frágil aos riscos cibernéticos, sejam eles causados de maneira intencional ou não.

Destaca-se, ao longo do texto, a habilidade de escrita do autor em apresentar um sentimento do mundo encontrar-se em uma nova corrida armamentista, agora no quinto domínio operacional — o do espaço cibernético - como uma área de atuação geopolítica,

principalmente quanto à dissuasão. Ficou claro que é possível infligir sérios danos a uma infraestrutura crítica, incluindo plantas e armamentos nucleares.

Como contribuições aos leitores, perceberam-se alguns pontos positivos: o primeiro passa pela riqueza de detalhes da série de ataques cibernéticos do grupo Sandworm, que caracterizaram as ações de grupos atuadores não cinéticos e multiplicadores do poder de combate russo ao gerarem efeitos cinéticos e não cinéticos a seus oponentes.; o segundo decorre de algumas características da defesa cibernética, como a insegurança latente, o alcance global e a vulnerabilidade das fronteiras geográficas, negligenciadas pelos EUA na crescente ciberguerra que ocorre na Ucrânia, apesar dos reiterados avisos de ataques que se espalharam para o resto do mundo; uma terceira análise mostra a questão do anonimato da autoria hacker, que correlaciona as ações do grupo Sandworm ao princípio da dissimulação, que impossibilitaram a sua rastreabilidade.

Uma das relevâncias do livro mostra que distâncias não representam mais “defesa”, pois a física do ciberespaço é totalmente diferente de todos os outros domínios da guerra. Ademais, a ciberguerra executada pelo grupo Sandworm não resultou em ganhos militares concretos para a Rússia (pelo menos por enquanto) pois o propósito foi psicológico, ou seja, de reduzir a vontade do povo ucraniano de lutar, bem como o chamado hacking eleitoral é utilizado para estremecer as fundações de confiança dos cidadãos perante o funcionamento de sua democracia, e o hacking de infraestruturas críticas se destina a abalar a confiança da população enquanto sociedade instituída.

Destarte, o livro mostrou que a Rússia usa táticas baratas, quando comparadas às ações cinéticas, e assimétricas para desestabilizar o equilíbrio de poder na esfera mundial.