CIBEROFENSAS E A CRISE DA UCRÂNIA[*]

Marcelo Antônio Osller Malagutti[1]

Em 14 de dezembro de 2021, manchetes de jornais ocidentais apontaram que a Ucrânia fora duramente atingida por ataques cibernéticos maciços (HARDING, 2022).

Dias depois, as manchetes davam conta de que a atribuição dos ataques, ainda que estivesse incompleta, apontava que o perpetrador seria a Rússia (AL JAZEERA, 2022; FRANCE-PRESSE, 2022).

Desde 2014, manchetes como essa são repetidas quase anualmente naquele país. Para podermos nos aprofundar na análise das semelhanças e idiossincrasias do caso recente, no entanto, precisaremos fazer uma breve retrospectiva histórica da crise, das ocorrências de ciberincidentes correlatos e de seus desdobramentos.

Em 2014, o então Presidente pró-Rússia da Ucrânia, *Viktor Yanukovich*, desistiu de negociações com a União Europeia (EU) em troca de compensações oferecidas pela Rússia. Na sequência, violentas manifestações populares, estimuladas pelo ocidente, fizeram com que o Congresso o depusesse e o substituísse por um simpatizante da EU. A Rússia não aceitou a substituição de seu aliado por um aliado de seus oponentes e, mesmo sem sustentação no Direito Internacional, retaliou. Primeiro, anexando a Crimeia, parte do território Ucraniano onde se localiza Sebastopol, o principal porto russo em águas quentes com acesso ao Mediterrâneo. Depois, enviando soldados sem identificação para fomentar a insurreição das províncias de *Donetsk* e *Luhansk* na região de *Donbas* de maioria étnica russa, que proclamou sua independência em 2014 e, desde então, luta contra as forças armadas da Ucrânia. Desde o início da crise, ficou patente a ingerência dos EUA, da EU e da Rússia nos assuntos da Ucrânia, mesmo sem amparo legal (ROCHA PAIVA, 2015).

Conflagrada a crise, a Ucrânia passou a ser assolada periodicamente por ciberincidentes, resumidos na Tabela 1.

Tabela 1 - Ciberincidentes na Ucrânia desde 2015

Ano	Mês	Incidente
2015	Dezembro	Uma variante do *malware Black Energy* foi usada em ataques coordenados de hackers russos foi identificada na regional de distribuição de energia *Prykarpattya Oblenergo*, no oeste da Ucrânia. Aproximadamente 225.000 ucranianos foram afetados, mas o serviço foi restabelecido após 3-6 horas.

[*] Artigo originalmente publicado no OMPV em 07 de fevereiro de 2022.

[1] Doutor em Ciências Militares.

Ano	Mês	Incidente
2016	Dezembro	O *malware Industroyer* (ou *Crash Override*) foi usado por *hackers* russos para atacar a empresa nacional de energia da Ucrânia, *Ukrenergo*, desligando a energia do norte de *Kiev* por mais de uma hora.
2017	Junho	O *ransomware NotPetya*, tendo como alvo primário a Ucrânia, se alastra pelo mundo com graves impactos no sistema de saúde do Reino Unido (NHS) e provocando prejuízos de centenas de milhões de dólares em gigantes multinacionais como a dinamarquesa *Maersk* e a americana *Fedex*.
2018	Junho	A polícia ucraniana afirma que hackers russos têm visado sistematicamente bancos, empresas de energia e outras organizações ucranianas para estabelecer *backdoors* em preparação para um ataque em larga escala contra o país.
2018	Julho	Oficiais de inteligência ucranianos afirmam ter frustrado um ataque russo ao equipamento de rede de uma planta de cloro no centro da Ucrânia. O vírus usado no ataque é o mesmo *malware* responsável pela infecção de 500.000 roteadores em todo o mundo em uma campanha que o FBI vinculou a hackers russos patrocinados pelo Estado.
2018	Setembro	*Hackers* russos atacam as caixas de entrada de e-mail de líderes religiosos ligados à Ucrânia em meio a esforços para desassociar a Igreja Ortodoxa da Ucrânia de sua associação com a Rússia.
2018	Outubro	O Serviço de Segurança da Ucrânia anuncia que um grupo russo realizara uma tentativa de hackear os sistemas de informação e telecomunicações de grupos do governo ucraniano
2018	Novembro	O CERT da Ucrânia identifica um malware nos sistemas informáticos das agências estatais do país, provavelmente implantado como precursor de um futuro ataque cibernético em larga escala.
2018	Dezembro	O Serviço de Segurança da Ucrânia bloqueia uma tentativa dos serviços especiais russos de interromper os sistemas de informação da autoridade judicial da Ucrânia
2018	Dezembro	Pesquisadores de segurança descobrem uma campanha cibernética realizada por um grupo ligado à Rússia, visando as agências governamentais da Ucrânia, bem como vários membros da OTAN**.**
2019	Abril	Organizações militares e governamentais ucranianas são alvo de uma campanha de *hackers* da República Popular de *Luhansk*, grupo apoiado pela Rússia que declarou independência da Ucrânia em 2014.
2020	Agosto	Autoridades ucranianas anunciam que um grupo de *hackers* russo começou a realizar uma campanha de phishing em preparação para operações no dia da independência da Ucrânia.
2021	Fevereiro	Autoridades ucranianas relatam que um ataque de negação de serviço distribuído de vários dias contra o site do Serviço de Segurança da Ucrânia faria parte das operações de guerra híbrida da Rússia no país.
2021	Março	O Serviço de Segurança do Estado da Ucrânia anunciou que impediu um ataque em larga escala de *hackers* russos do FSB, o Serviço de Inteligência do Estado Russo, que tentavam obter acesso a dados confidenciais do governo.

Fonte: AUTO, com base em STIENNON, 2022.

Diante de tal histórico, o que diferencia a onda atual de ataques de suas anteriores?

Primeiro, a similaridade com a situação da Guerra da Geórgia, em 2008, quando a Rússia interveio a favor da província separatista da Ossétia do Sul e da Abecásia, de maioria étnica russa, com uma salva de ciberataques que eliminaram a capacidade de comando e controle do governo e das forças armadas georginas como ataque precursor da invasão militar que derrotou as forças georgianas.

No caso da Ucrânia, os russos apoiam separatistas étnicos russos da província de *Donbas*, na região da fronteira, desde 2014. Adicionalmente, desde dezembro de 2021, observa-se a concentração de meios militares russos na fronteira com a Ucrânia, que já poderiam estar próximos a 130.000 homens. Em 10 de janeiro de 2022, foram iniciadas negociações entre os EUA, a EU e a Rússia na tentativa de conter a escalada da crise e, no dia 13, foram concluídos 3 dias de negociações infrutíferas. Então, uma notícia, já no dia seguinte, de uma salva de ciberataques incapacitantes de sítios governamentais, incluindo Relações Exteriores e Defesa, poderia indicar um ataque precursor e o início de uma guerra aberta. Em nenhum dos 13 ciberincidentes relatados na Tabela 1, essa característica era perceptível.

Segundo, o fato de que os ataques foram de dois tipos distintos, realizados de forma conjunta. De uma parte, havia um aparente ataque de ransomware, mas que era diferente em sua natureza. Uma análise do malware denominado *WhisperGate*, feita pela *Microsoft*, apontou que, embora projetado para se parecer com ransomware, congelando todas as funções e dados do computador e exigindo o pagamento de dez mil dólares em bitcoins em troca do retorno ao funcionamento normal, ele não dispõe de infraestrutura para receber o resgate, o que teria levado os investigadores a concluir que o objetivo seria o de infligir o máximo de dano ao não arrecadar dinheiro (NAKASHIMA; STERN, 2022; SANGER, 2022).

Já a empresa de cibersegurança *CrowdStrike* apontou que o malware, após criptografar a tabela mestre de arquivos do computador infectado, não forçava a reinicialização do sistema, como foi observado em intrusões anteriores, como o *NotPetya*. Isso sugere que o atacante "tomou outras medidas para iniciá-lo (por exemplo, por meio de um implante diferente) ou decidiu permitir que os usuários executassem a reinicialização por conta própria", e que a reinicialização postergada pode permitir que outros componentes da invasão do *WhisperGate* sejam executados (CROWDSTRIKE INTELLIGENCE TEAM, 2022). A empresa *Cisco Talos*, que auxiliou as autoridades ucranianas em suas investigações sobre os recentes incidentes, acredita que os invasores "provavelmente tiveram acesso à rede da vítima meses antes do ataque, uma característica típica de operações sofisticadas de ameaças persistentes avançadas (APT)" (KOVACS, 2022).

De outra parte, havia o ataque de pichação (*defacement*) de cerca de 70 sítios do governo ucraniano, com mensagens em ucraniano, russo e polonês, indicando que dados do povo ucraniano haviam sido roubados e destruídos. Dentre esses sítios, estavam alguns dos órgãos do primeiro

escalão do governo ucraniano, como os ministérios de Relações Exteriores, Defesa, Energia e Educação e Ciência, bem como o Serviço de Emergência do Estado e o Ministério da Transformação Digital, cujo portal de governança eletrônica dá ao público acesso digital a dezenas de serviços governamentais (ZETTER, 2022).

A análise forense indicou que as pichações foram feitas de forma manual, e não automatizada, e que análises de nuances do texto em polonês apontaram que o texto não fora escrito por falantes nativos da língua, mas provavelmente traduzidos por meio do *Google Translate*. Talvez uma tentativa rudimentar de plantar uma "bandeira falsa" no intuito de desviar a atenção dos investigadores na direção de *hackers* poloneses.

Além disso, cerca de 50 dos 70 sítios afetados eram mantidos por uma companhia ucraniana denominada *Kitsoft*, levando os investigadores a determinarem que a Kitsoft havia sido comprometida, permitindo aos hackers o acesso ao painel de administração da empresa e o uso de suas credenciais para desfigurar os sites de seus clientes (ZETTER, 2022). Outrossim, a análise forense indica que os ataques foram de baixa complexidade técnica, uma característica incomum para os recentes incidentes atribuídos à Rússia.

O terceiro fator de interesse vem da Bielorrússia, cujo governo pró-Russo estaria permitindo a movimentação e o acúmulo de meios russos em seu território, também na fronteira com a Ucrânia, fazendo com que os ucranianos tenham de se ocupar de duas potenciais frentes de defesa. Ocorre que um grupo de *hackers* que se autodenomina *Cyber-Partisans* (algo como ciberresistência) pró-democracia declarou, no dia 24, por meio de postagens no *Twitter* e no Telegram, ter se "infiltrado na rede ferroviária Bielorrussa em um esforço para interromper o movimento de tropas russas no país, à medida que crescem as tensões sobre uma potencial invasão da Ucrânia". Essa interrupção teria sido feita por meio de um ransomware que teria criptografado servidores da companhia ferroviária, mas em vez de pedir dinheiro, o resgate exigido seria a libertação de 50 prisioneiros políticos que precisam de cuidados médicos e a proibição de que militares russos entrem na Bielorrússia (PIETSCH, 2022). Por conseguinte, armas similares agora estariam sendo usadas por simpatizantes da Ucrânia contra apoiadores dos russos, um dado novo no contexto.

Por fim, ainda que não relacionado diretamente à atual onda de ciberataques, cumpre observar um fato novo relativo ao *NotPetya*. A gigante multinacional farmacêutica *Merck* obteve uma vitória jurídica no valor de 1,4 bilhão de dólares na ação contra suas seguradoras, que se recusavam a pagar o prêmio relativo aos prejuízos causados pelo ransomware, alegando que a cobertura não era válida em casos de guerra. A Corte Superior de Justiça do Estado de *Nova Jersey* entendeu que a cláusula de exclusão de atos de guerra não é aplicável, o que deve provocar a necessidade de uma melhor definição de cláusulas de exclusão de atos cibernéticos em contratos de seguro no futuro. A questão

de saber se um ataque cibernético conta como um ato de guerra é uma parte de um "acerto de contas" mais amplo da indústria de seguros, de acordo com *Josephine Wolff*, professora associada de política de segurança cibernética da *Tufts University* (VITTORIO, 2022).

Tudo somado, a salva cibernética sofrida pela Ucrânia, no período em análise, parece ter sido mais um evento num histórico crescente de incursões russas (ou de simpatizantes russos) para debilitar sua resistência e testar novas técnicas e táticas, sem se mostrar parte de uma ofensiva militar generalizada. Sempre é bom lembrar do ensinamento de *Flavius Renatus Vegetius: si vis pacem, para bellum* (quem deseja a paz, prepara-se para a guerra). O "laboratório de ciberincidentes" em que a Rússia parece ter transformado a Ucrânia tem dado ao mundo a oportunidade de estudar e aprender muito, como no caso do *NotPetya*. Aqueles que aproveitam essa oportunidade e investem nesse aprendizado desenvolvem e aprimoram suas instituições, preparando-as para essa nova ferramenta de coerção interestatal que são os ciberataques.

Referências:

AL JAZEERA. **Ukraine says evidence suggests Russia behind cyberattack.** Al Jazeera, 16 de janeiro de 2022.

CROWDSTRIKE INTELLIGENCE TEAM. **Technical Analysis of the WhisperGate Malicious Bootloader.** Disponível em: https://www.crowdstrike.com/blog/technical-analysis-of-whispergate-malware/. Acesso em: 22 jan. 2022.

FRANCE-PRESSE**. Ukraine says evidence points to Russia being behind cyber-attack.** The Guardian, 16 de janeiro de 2022.

HARDING, Luke. **Ukraine hit by "massive" cyber-attack on government websites.** The Guardian, 14 de janeiro de 2022. Disponível em: https://www.theguardian.com/world/2022/jan/14/ukraine-massive-cyber-attack-government-websites-suspected-russian-hackers. Acesso em: 14 jan. 2022.

KOVACS, Eduard. **Ukraine Attack: Hackers Had Access for Months Before Causing Damage.** Security Week, 24 de janeiro de 2022. Disponível em: https://www.securityweek.com/ukraine-attack-hackers-had-access-months-causing-damage. Acesso em: 14 jan. 2022.

NAKASHIMA, Ellen e STERN, David. **Data of several Ukrainian government agencies is wiped in cyberattack.** The Washington Post, 18 de janeiro de 2022.

PIETSCH, Bryan. **Hacking group claims control of Belarusian railroads in move to ' disrupt ' Russian troops heading near**. The Washington Post, 25 de janeiro de 2022.

ROCHA PAIVA, Luiz Eduardo. **A Crise na Ucrânia: Reflexos para a defesa do Brasil.** A Defesa Nacional, n° 826, p. 6–24, 2015. Disponível em: https://en.calameo.com/read/034864 30d9f4d7647a.

SANGER, David. **Microsoft Warns of Destructive Cyberattack on Ukrainian Computer Networks.** The New York Times, 05 de janeiro de 2022.

STIENNON, Richard. **A List of Cyber Attacks Against Ukraine.** Disponível em: https://www.linkedin.com/pulse/list-cyber-attacks-against-ukraine-richard-stiennon. Acesso em: 26 jan. 2022.

VITTORIO, Andrea. **Merck's $1.4 Billion Insurance Win Splits Cyber From 'Act of War'.** Bloomberg, 19 de janeiro de 2022. Disponível em: https://news.bloomberglaw.com/privacy-and-data security/mercks-1-4-billion-insurance-win-splits-cyber-from-act-of-war. Acesso em: 26 jan. 2022.

ZETTER, Kim. **What Know and Don't Know about the Cyberattacks Against Ukraine.** Zero Day, 17 de janeiro de 2022.