НІСД НАЦІОНАЛЬНИЙ ІНСТИТУТ СТРАТЕГІЧНИХ ДОСЛІДЖЕНЬ
NATIONAL INSTITUTE FOR STRATEGIC STUDIES NISS

ЦЕНТР БЕЗПЕКОВИХ ДОСЛІДЖЕНЬ
CENTER FOR SECURITY STUDIES

Світове відлуння російсько-українського кіберпротистояння

Вікторія Бойко, канд. іст. наук, головний консультант відділу інформаційної безпеки та кібербезпеки центру безпекових досліджень НІСД

Одним із складників широкомасштабної збройної агресії РФ проти України є деструктивні дії в кіберпросторі, які корелюють із воєнними діями. Наприклад, за кілька годин до того, як російські війська 24 лютого 2022 р. вторглися на територію України, було отримано попередження про нове шкідливе програмне забезпечення, спрямоване проти українських міністерств та фінансових установ[1]. За даними Microsoft, щонайменше шість джерел постійної серйозної загрози (Advanced Persistent Threat, APT) та інші невстановлені джерела кіберзагроз здійснювали деструктивні атаки та/або шпіонаж, у той час як російські війська атакували країну на суші, в повітрі та на морі[2].

Кібератака РФ не обмежується виключно Україною. Низка кібератак здійснювалася на об'єкти критичної інфраструктури країн ЄС, що призвело, зокрема, до збоїв у роботі закладів охорони здоров'я та електростанцій у різних регіонах Європи. Керівник німецького Федерального управління з безпеки у сфері інформаційних технологій (Das Bundesamt für Sicherheit in der Informationstechnik, BSI) Арне Шенбом (Arne Schönbohm) попередив країни ЄС про те, що кібератаки на Україну можуть спричинити ефект ланцюгової реакції в країнах Західної Європи[3].

США та ЄС вживають заходи задля захисту американських та європейських ІТ систем від кібератак РФ та стримування розгорнутої нею кібератресії.

США проти кіберпідрозділів збройних сил РФ

Скоординовані дії одразу проти двох кіберугруповань, підпорядкованих Головному управлінню Генштабу збройних сил РФ (ГУ ГШ ЗС РФ), США розпочали 6 квітня 2022 р.

Зокрема, Міністерство юстиції США оголосило про санкціоновану судом операцію проти глобальної бот-мережі Sandworm (в/ч 74455, або Центр оперативної координації органів військового управління), що складалася з тисяч інфікованих мережевих апаратних пристроїв, яку контролювало ГУ ГШ ЗС РФ[4]. Унаслідок

[1] RiskIQ Threat Intel Brief. 2022. 24 Feb. URL: https://community.riskiq.com/article/9f59cb85
[2] Special Report: Ukraine. An overview of Russia's cyberattack activity in Ukraine. Microsoft Digital Security Unit, April 27, 2022. URL: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd
[3] Див.: URL: https://www.sueddeutsche.de/politik/ukraine-russland-hacker-1.5531367
[4] Justice Department Announces Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate (GRU) / The U.S. Department of Justice. 2022. 06 April. URL: http://surl.li/bwlfu ; New Sandworm malware Cyclops Blink replaces VPNFilter / National Cyber Security Centre a Part of GCHQ. 2022. 23 Feb. URL: https://www.ic3.gov/Media/News/2022/220223.pdf

операції було видалено зловмисне програмне забезпечення Cyclops Blink[5]. Уряд США звернувся до власників уражених комп'ютерів, закликаючи здійснити необхідні технічні заходи, які допоможуть позбавитися вразливостей і, відповідно, запобігти подальшому зловмисному впливу на пристрої.

Також 6 квітня ц. р. компанія Microsoft отримала постанову суду, завдяки чому одержала можливість узяти під контроль сім інтернет-доменів, які угруповання Strontium (в/ч 26165, або 85-й Головний центр спеціальної служби ГУ ГШ ЗС РФ) використовувало для здійснення кібератак на українські інституції, а, крім них, також і на медіа-організації, урядові установи, аналітичні центри США та Євросоюзу, що працюють у сфері зовнішньої політики[6].

США за допомогою санкцій намагаються знизити рівень ворожої кіберактивності. Наразі Управління з контролю за іноземними активами Міністерства фінансів США (Office of Foreign Assets Control, OFAC) реалізує санкції проти РФ. Зокрема, проти 21 юридичної особи[7] та 13 фізичних осіб[8] уже застосовуються санкційні заходи – усе майно, що перебуває на території США у власності цих осіб чи під їхнім контролем, заблоковано. Крім того, блокується діяльність організацій, контрольний пакет акцій яких прямо чи опосередковано належить одній чи кільком особам із санкційного списку. Ці санкції є частиною комплексної відповіді США на широкомасштабне вторгнення РФ в Україну, що сталося 24 лютого 2022 р. Їх мета – обмеження доступу до ресурсів, які Росія використовує задля фінансування війни та проведення кібероперацій[9]. Сполучені Штати й надалі протидіятимуть руйнівній або іншій дестабілізаційній кіберактивності РФ проти союзників і партнерів США.

ЄС: посилення кіберзахисту та підготовка санкцій

Федеральне управління з безпеки у сфері інформаційних технологій (BSI), беручи до уваги той факт, що в низці європейських країн (Німеччині, Польщі та Греції) об'єкти критичної інфраструктури (електростанції, альтернативні джерела енергії), компанії та органи влади зазнали різного роду кібератак, попередило операторів критичних інфраструктур про існування особливих ризиків їхнім системам[10].

Так, німецька компанія Nordex Group – одна з найбільших у світі серед виробників вітрових турбін – 31 березня 2022 р. повідомила, що стала жертвою кібератаки, яка зупинила діяльність цілих секторів альтернативної енергії[11]. Зокрема, постраждало понад 5 тис. системних одиниць, що спричинило майже 11 ГВт втрат

[5] Justice Department Announces Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate (GRU) / The U.S. Department of Justice. 2022. 06 April. URL: http://surl.li/bwlfu
[6] Там само.
[7] Зокрема, такі: AO NII-Vektor, T-Platforms, Joint Stock Company Mikron, Molecular Electronics Research Institute, Serniya Engineering, Sertal, Robin Treid, United Kingdom-based Majory LLP, United Kingdom-based Photon Pro LLP, Spain-based Invention Bridge SL.
[8] Treasury Targets Sanctions Evasion Networks and Russian Technology Companies Enabling Putin's War : Press Releases / The U.S. Department of the Treasury. 2022. 31 March. URL: https://home.treasury.gov/news/press-releases/jy0692
[9] Additional Sanctions on Russia's Technology Companies and Cyber Actors / The U.S. Department of State. 2022. 31 March. URL: https://www.state.gov/additional-sanctions-on-russias-technology-companies-and-cyber-actors/
[10] Див.: URL: http://surl.li/bwhms
[11] Hackerangriff bei Windturbinenhersteller Nordex. NDR. 2022. 04 Apr. URL: https://www.ndr.de/nachrichten/mecklenburg-vorpommern/Hackerangriff-bei-Windturbinenhersteller-Nordex,nordex204.html

енергії. Подібне шкідливе програмне забезпечення, крім Німеччини, було виявлено також у Латвії та Литві[12].

Європейський Союз намагається реагувати на загрози, що зростають. Відповідно розробляються й приймаються нові документи, запроваджується та вдосконалюється механізм санкцій.

Наразі Європейська Комісія з метою підвищення стійкості до кіберзагроз та можливостей вчасного реагування на них ініціювала два нові регламенти з кібер[13]- та інформаційної[14] безпеки. Згідно з ними всі установи, органи, офіси та агенції Європейського Союзу повинні мати системи кібербезпеки для контролю та управління ризиками, а також зобов'язані регулярно оцінювати та покращувати стан цих систем, негайно надавати всю інформацію щодо інцидентів у CERT-EU та, вибірково, міжнародними партнерами.

Регламенти також передбачають створення нової міжінституційної Ради з питань кібербезпеки (Interinstitutional Cybersecurity Board, IICB), покликаної контролювати виконання документів та співкоординувати діяльність CERT-EU. Мандат центру реагування на кіберінциденти буде розширено. CERT-EU виконуватиме кілька функцій: центру координації реагування на інциденти, центрального дорадчого органу та постачальника послуг. Регламенти передбачають розгортання діяльності операційних центрів безпеки (Security Operations Center, SOC), які повинні здійснювати моніторинг мережі та цілодобово відстежувати загрози високого рівня[15] у більшості установ, органів та агенцій ЄС, що співпрацюють із CERT-EU на основі щоденної комунікації та обміну інформацією.

Певні заходи вживаються й на локальному (національному) рівні. Наприклад, 1 квітня 2022 р. Адміністративний суд міста Кельна ухвалив рішення (Az.: 1 L 466/22) на підтримку BSI[16] щодо заміни продуктів російської компанії Kaspersky на альтернативні. Попередження, оприлюднене BSI, є, зокрема, реакцією на низку кібератак на критичну інфраструктуру Німеччини та широкомасштабну збройну агресію РФ проти України[17]. Компанію Касперського вже давно обґрунтовано підозрюють у співпраці з ФСБ та розвідувальній діяльності, здійсненні наступальних операцій, цільових атак на ІТ інфраструктуру країн ЄС зі значним потенціалом інфільтрації у державні мережі держав – членів ЄС. Уряд США 25 березня цього ж

[12] Див.: URL: https://www.politico.eu/article/baltic-cyber-spillover-ukraine-russia-attack/
[13] European Commission. Proposal of Cybersecurity Regulation. URL: https://ec.europa.eu/info/publications/proposal-cybersecurity-regulation_en
[14] European Commission. Proposal for a Regulation of the European Parliament and of the Council on information security in the institutions, bodies, offices and agencies of the Union. 22 March 2022. URL: https://ec.europa.eu/info/files/proposal-regulation-information-security-institutions-bodies-offices-and-agencies-union_en
[15] Proposal for a Regulation of the European Parliament and of the Council laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union. Brussels, 22.3.2022 COM(2022) 122 final. URL: https://ec.europa.eu/info/sites/default/files/proposal_for_a_regulation_laying_down_measures_on_cybersecurity_at_euibas.pdf
[16] Verwaltungsgericht Köln: Bundesamt für Sicherheit in der Informationstechnik darf vor Virenschutzsoftware von Kaspersky warnen. 2022. 01 Apr. URL: https://www.justiz.nrw/JM/Presse/presse_weitere/PresseOVG/01_04_2022_/index.php
[17] Див.: URL: https://www.gesetze-im-internet.de/bsig_2009/__7.html

року офіційно висловив підозру щодо високого рівня державного втручання РФ у діяльність компанії «Лабораторія Касперського»[18].

Також Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (European Union Agency for Network and Information Security, ENISA) у відповідь на російську широкомасштабну воєнну агресію проти України оприлюднило рекомендації щодо посилення безпеки державних і приватних організацій у Європі[19] на тлі аналогічних кроків у США та Великій Британії[20]. Дії військових та розвідувальних сил РФ та погрози російської сторони щодо ЄС, НАТО та ФРН вже кваліфікуються BSI як попередження про агресію, що є підставою для підготовки до впровадження кіберсанкцій[21].

У Регламенті від 17 травня 2019 р. (статті 1(1), 1(4)) ЄС визначає серйозну кібератаку як зовнішню загрозу, що здійснюється супроти країни ЄС, об'єктів її критичної інфраструктури, служб або державних установ і процесів, які є важливими для підтримки соціальних функцій, здоров'я, безпеки та добробуту населення, зокрема у сферах енергетики, транспорту, банківської діяльності, охорони здоров'я, питного водопостачання або цифрової інфраструктури[22]. Така кіберзагроза передбачає реалізацію колективної відповіді ЄС, що, зокрема, регламентується Договором про функціонування Європейського Союзу (TFUE). Згідно зі ст. 222 цього договору колективна солідарність (solidarity clause)[23] передбачає взаємну підтримку країн ЄС, також і в разі серйозних кіберінцидентів. Крім того, може бути застосований випадок колективної допомоги (mutual defence clause), що регламентується відповідно до статті 42.7 Договору про ЄС[24] (TUE), комплементарної статті 5 Договору про НАТО. Уперше цим механізмом скористалася Франція в 2015 р. після терактів у Парижі.

Санкції можуть бути застосовані не тільки проти суб'єктів, безпосередньо відповідальних за кібератаки, а й проти всіх суб'єктів, які надають фінансову, технічну чи матеріальну підтримку або іншим чином залучені до кібератаки, а також усіх пов'язаних із ними суб'єктів. Це суттєво розширює рамки застосування санкцій. Санкції можуть бути введені не лише у відповідь на кібератаки безпосередньо проти європейських інституцій (установ, органів чи офісів, делегацій у третіх країнах або міжнародних організацій, операцій та місій спільної політики безпеки та оборони або їх спеціальних представників), а й ті, що проводилися проти держави – члена СЄ. Йдеться про кіберзагрози критичній інфраструктурі такої держави, сфері послуг, що необхідні для підтримки найважливіших державних функцій, у т. ч. соціальної та/або економічної діяльності, системам зберігання чи обробки секретної інформації, а також урядовим групам реагування на надзвичайні ситуації.

---

[18] Public Safety and Homeland Security Bureau Announces Additions to the List of Equipment and Services Covered by Section 2 of the Secure Networks Act. 2022. 25 March. URL: https://www.fcc.gov/document/announcement-additions-covered-list

[19] Cyber Threats Outreach in Telecom / The European Union Agency for Cybersecurity. March 2022. 30 p. URL: https://www.enisa.europa.eu/publications/cyber-threats-outreach-in-telecom/@@download/fullReport

[20] New Sandworm malware Cyclops Blink replaces VPNFilter / National Cyber Security Centre a Part of GCHQ. 2022. 23 Feb. URL: https://www.ic3.gov/Media/News/2022/220223.pdf

[21] Warnung vor Kaspersky – Virenschutzsoftware nach § 7 BSIG. BSI. URL: http://surl.li/bwhtn

[22] Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States. ST/7302/2019/INIT. URL: https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX%3A32019R0796

[23] Див.: URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:solidarity_clause

[24] Див.: URL: http://surl.li/bwhtl