ЕНДІ ҐРІНБЕРГ

ПІЩАНИЙ ХРОБАК, АБО
SANDWORM

НОВА ЕПОХА КІБЕРВІЙНИ.
ПОЛЮВАННЯ НА НАЙВІРТУОЗНІШИХ ХАКЕРІВ КРЕМЛЯ

ХАРКІВ
«ФОЛІО»
2020

ПЕРЕДМОВА

На початку березня 2017 року мені зателефонував мій друг і колега Роман Сологуб, гендиректор компанії ISSP, із дещо нетривіальним запитанням: у наш офіс хотів приїхати журналіст WIRED. Він просив дозволу розпитати наших експертів про резонансні кібератаки проти України та розслідування, які проводила команда лабораторії ISSP на чолі з її керівником Олексієм Ясинським.

Це тепер, після того як стали відомими на весь світ потужні атаки на українську енергетику, банки, телеканали, аеропорти, залізницю, операторів зв'язку, держустанови, онлайн-медіа, електронну комерцію, лікарні, розробників ПЗ, ритейл, промислові виробництва, освіту і науку, військові структури, системи для забезпечення виборів — тобто на все, що є важливим для функціонування економіки та держави, звернення журналістів із провідних світових медіа за думкою або коментарем до українських експертів із кібербезпеки є звичною справою. Врешті, кібербезпека — це одна з небагатьох сфер, у яких Україна може не лише «чужого навчатися», а й «свого не цуратися», отримувати поради й допомогу, і водночас радити й допомагати партнерам бути неоціненним союзником євро-

атлантичного світу в гібридній війні, яку тоталітарні країни розв'язали й нарощують проти відкритих суспільств.

Однак тоді, навесні 2017-го, коли до завершення найпотужнішої й на сьогодні кібероперації, що після її кульмінації в червні 2017 року отримала назву NotPetya, лишалося ще кілька місяців, зацікавленість із боку відомого журналіста, який працював на, мабуть, найавторитетніший у світі журнал, що висвітлює вплив новітніх технологій, інтригувала. Інтуїція підказувала, що йтиметься не просто про запит на коментар чи експертну думку, а про щось більше…

Так і сталося. Вже звичайна перевірка інформації дала зрозуміти, що йтиметься про глибоке дослідження або навіть розслідування, адже з'ясувалося, що зацікавленим журналістом є ніхто інший, як Енді Ґрінберг, провідний журналіст WIRED (у них це називається Senior Writer), який на той час був уже відомим у світі інформаційної безпеки автором, що спеціалізувався на темі кіберзлочинності, кібератак і впливу технологій на конфіденційність, інформаційну свободу й політику.

Його стаття 2015 року про те, як Чарлі Міллер і Кріс Велесек хакнули Jeep, що рухався хайвеєм із Енді за кермом, отримала чималий резонанс і призвела до відкликання майже півтора мільйона автомобілів, але головне — звернула увагу на нові потужні ризики, що створює диджиталізація. Світ, зокрема, завдяки публікаціям Ґрінберга, поступово починав усвідомлювати, що проникнення із шаленою швидкістю комп'ютерних технологій в усі сфери життя, пришвидшення розвитку штучного інтелекту й інтернету речей — це не лише нові можливості, а й нові виклики.

Ще раніше, 2012 року, книжка Енді Ґрінберга «Ця машина вбиває секрети» (This Machine Kills Secrets) потрапила до переліку вибору редакції Нью-Йорк Таймс (New York Times Editor's Choice), 2013 року стаття Енді для Forbes.com «Зустрічайте хакерів, які продають шпигунам інструменти для зламу ваших ПК (і заробляють шестизначні гонорари)» отримала визнання найкращого блогу року від Security Bloggers Network, а 2014-го разом із Райаном Меком Енді Ґрінберг було номіновано на Премію Геральда Льоба за статтю «Мозок великого брата» (Big Brother's Brain) у Forbes Magazine, і того ж року SANS Institute, який для професіоналів у сфері кібербезпеки не потребує представлення, нагородив Енді Ґрінберга премією як одного з найкращих журналістів у сфері кібербезпеки (Top Cybersecurity Journalist Award Winners). Нарешті, 2019 року Енді Ґрінберг отримав Премію Геральда Льоба за статтю «Код, що розтрощив світ: нерозказана історія про NotPetya — найруйнівнішу кібератаку в історії».

І все ж таки до виходу цієї книжки найважливішим внеском Енді Ґрінберга в шляхетну справу пробудження суспільств і держав до усвідомлення викликів сучасної кібервійни стала стаття, для написання якої він уперше й прибув до Києва в березні 2017 року. Він працював над цим дослідженням кілька місяців. І, мабуть, за іронією долі — в будь-якому разі це дуже символічно — стаття побачила світ публікацією у WIRED саме в червні 2017 року з присвяченою цілковито їй обкладинкою та яскравим тизером «Як вимкнути країну». В електронному ж вигляді стаття вийшла на wired.com 20 червня, тобто за сім днів до кульмінації NotPetya. Назва статті дуже промовиста: «Як ціла країна стала російською випробувальною лаборато-

рією кібервійни» (How an Entire Nation Became Russia's Test Lab for Cyberwar).

Важливість тієї публікації для України важко було переоцінити. Нарешті, прогнози й висновки, яких дійшли експерти ISSP ще 2014 року в результаті аналізу розслідуваних у 2015-му та 2016 роках кібератак про перетворення України не лише на ціль російських кібероперацій, а й на випробувальний полігон кібервійни, були почуті глобальними аудиторіями. Завдяки авторитету журналу WIRED та Енді Ґрінбергу як автору цей висновок швидко набув статусу загальновизнаного факту серед експертів і на рівні ухвалення ключових рішень, зокрема політичних. Уміння захопливо розповідати про складні технічні речі зрозумілою широкому колу читачів мовою — це великий талант і вміння, яким Енді Ґрінберг володіє досконало, і він вкотре сповна скористався ними.

Коли Енді повідомив, що планує написати книжку про угруповання Sandworm і знову хоче приїхати до Києва й поспілкуватися ще глибше про всі резонансні кібератаки групи Sandworm проти України й інших країн, ми були більше ніж раді. Адже це означало, що незабаром світ почує історію, про яку мусить знати.

Кожна людина, а передовсім влада кожної країни, повинні усвідомлювати, що атака в цифровому просторі, з яким щодня ми стаємо все більш інтегрованими, може бути надзвичайно руйнівною. Ще 2011 року уряд Нідерландів, які є однією з найспроможніших країн і в захисних, і в наступальних кібероперацій, прирівняв кібератаку, що спричиняє серйозні порушення роботи з тривалими наслідками, до збройного нападу.

Сьогодні кілька десятків країн у світі мають офіційно сформовані кібервійська. До п'ятірки найчисельніших і найкраще фінансованих, за оцінками експертів, входять і кіберпідрозділи збройних сил РФ, що вже багато років веде гібридну війну проти України.

Після атаки NotPetya багато хто вважає, якщо немає гучного колапсу, як це було в червні 2017 року, то й атак немає. Насправді зловмисна активність у кіберпросторі не спиняється ні на мить, і найкращою мішенню для зловмисників, які хочуть завдати шкоду цілій державі, є об'єкти критичної інфраструктури. Спрямована атака на подібні об'єкти може тривати від 6 до 12 місяців. Здебільшого, якщо атака була успішною, жертви бачать тільки кінцеві фази, наприклад, знищення інфраструктури чи шифрування даних, вимогу викупу. І навіть кінцеві фази кібератаки можуть бути невидимими, якщо, приміром, зловмиснику треба проникнути в організацію, викрасти певні дані й непомітно зникнути або отримати доступ до інфраструктури для його використання в майбутньому.

Енді Ґрінберг пише в жанрі нон-фікшн, але, коли читаєш цю книжку, легко себе спіймати на відчутті, що читаєш не документальну розповідь, а захопливий трилер. Ця оповідь яскраво демонструє, що ескалація кібервійни триває, а жертвами санкціонованих державами кібероперацій стають не лише окремі підприємства, галузі чи уряди, а й міста та країни.

Зі зрозумілих причин ця книжка не може містити всю інформацію про величезну кількість технічних деталей про тактики й техніки кібератак, але автору вдалося продемонструвати весь масштаб загроз від Sandworm і його аналогів, який нависає над майбутнім уже тепер і скрізь.

Історія угруповання Sandworm — це історія про найяскравіший приклад зловмисників, що наближають антиутопію кібервійни. Енді Ґрінбергу вдалося в притаманній йому манері «простої розповіді про складні речі» висвітлити багаторічну роботу дослідників кіберзброї та розслідувачів кібератак, які змогли відстежити найнебезпечніших хакерів Кремля, щоб не лише ідентифікувати останніх і встановити їхнє місце перебування, а й привернути увагу світу до загрози, яку становлять спонсоровані та здійснювані державами кібератаки на кшталт атак Піщаного Хробака.

Водночас Sandworm — це історія не лише про окрему потужну зловмисну хакерську групу чи навіть глибоку небезпеку, спричинену безрозсудним прагненням Росії розгортати кібервійну в усьому світі. Це історія глобальної гонитви кіберозброєнь і надії на те, що Світло знову переможе.

Олег Дерев'янко,
співзасновник і голова Ради директорів
ISSP — Information Systems Security Partners

Нова епоха кібервійни та полювання на найнебезпечніших хакерів Кремля

На пам'ять про мого батька Гері Ґрінберга

ВСТУП

Двадцять сьомого червня 2017 року дещо аномально жахливе почало поширюватися на об'єкти інфраструктури у всьому світі.

У багатьох лікарнях Пенсильванії почали скасовувати операції. На шоколадній фабриці Cadbury в австралійському штаті Тасманія припинили виробництво шоколаду. Фармацевтичний гігант Merck зупинив виготовлення вакцин від вірусу папіломи людини.

Незабаром у портах по всьому світу було паралізовано роботу сімнадцяти терміналів, які належать світовому лідерові у сфері контейнерних перевезень Maersk. Десятки тисяч тягачів, що перевозять вантажні контейнери, почали збиратися за воротами цих портів, а на грандіозних суднах, що прибували з різних океанських шляхів, і кожне з яких доставляло сотні тисяч тонн вантажу, усвідомлювали — розвантажитися там не зможуть. Здавалося, що ключові складники всесвітньопов'язаних автоматизованих систем спонтанно відмовлялися функціонувати, наче вони постраждали від планетарного спалаху невідомої бактерії, що руйнує мозок.

Ще відчутніше наслідки технологічного апокаліпсиса проявилися в епіцентрі атаки — в Україні. Незрозуміло чому відключилися банкомати й системи оплати кредитними картками. У столиці України — Києві було паралізовано роботу

громадського транспорту. Державні установи, аеропорти, лікарні, поштова служба і навіть учені, які відстежували рівень радіації на зруйнованій Чорнобильській атомній електростанції, — всюди безпорадно спостерігали, як невідомий фрагмент руйнівного коду заражав і виводив із ладу фактично кожен комп'ютер у їхніх мережах.

Саме такий вигляд має кібервійна: невидима сила, що здатна проявитися з нізвідки для широкомасштабного підриву технологій, покладених в основу сучасної цивілізації.

Протягом десятиліть «*кассандри*»[1] інтернет-безпеки попереджали нас, що цього не уникнути. Вони застерігали, що невдовзі хакери зроблять значний крок уперед — вийдуть за рамки звичайного злочину чи навіть санкціонованого державою шпигунства і почнуть намацувати слабини в оцифрованій критичній інфраструктурі сучасного світу. Події 2007 року в Естонії, коли в результаті кібератак російських хакерів «лягли» фактично всі сайти в державі, вперше показали, якими можуть бути потенційні масштаби геополітично вмотивованих хакерських нападів. А вже за два роки світ став свідком нової демонстрації сили: шкідлива програма АНБ США під назвою Stuxnet безшумно зупинила центрифуги зі збагачення урану в Ірані, доки вони не самознищилися. Ця операція показала, що інструменти кібервійни можуть проникати далеко за межі цифрового світу — фактично в найбільш конфіденційні та захищені компоненти фізичного світу.

Зі свого боку той, хто з початку 2014 року стежив за перебігом військових дій Росії в Україні, помічав чіткіші й прямі провісники. Так, хвилі вірусних кібератак почали накочувати-

[1] Кассандра у давньогрецькій міфології — царівна, наділена даром пророцтва *(прим. — перекл.)*.

ся на український уряд, ЗМІ й транспортну інфраструктуру ще з 2015 року. Завершилися вони першим в історії блекаутом, який спричинили хакери, — атакою, що відрізала від енергосистеми сотні тисяч мирних жителів.

Невелика група дослідників почала бити на сполох, попереджаючи, що Росія перетворює Україну на полігон для випробувань кіберзброї, але їх не почули. Вони стверджували, що незабаром подібні кібердосягнення може бути застосовано й проти США, НАТО та всього світу, який був абсолютно неготовим до нової форми ведення війни. Вони ж вказували на монолітну силу, найімовірніше за стінами Кремля — групу хакерів, відповідальну за запуск цієї безпрецедентної кіберзброї масового ураження. Групу, відому як *Sandworm*, або *Піщаний хробак*.

Протягом наступних двох років Sandworm проявлятиме свою агресію дедалі відчутніше, змусить говорити про себе як про найнебезпечнішу команду хакерів і фактично визначить суть кібервійни. Зрештою, наприкінці доленосного червня 2017-го група запустить «хробака», відомого як NotPetya — на сьогодні найбільш руйнівного вірусу в історії. Своєю атакою Sandworm яскраво продемонструє: досвідчені хакери, що мають підтримку держави і мотивацію військових диверсійних підрозділів, здатні з будь-якої дистанції атакувати і вражати взаємопов'язані системи, спричиняючи непередбачувані катастрофічні наслідки і підриваючи основи людського життя.

Увесь масштаб загрози від Sandworm і його аналогів нависає над майбутнім вже тепер. Якщо ескалація кібервійни й далі безперешкодно продовжуватиметься, жертви санкціонованого державою хакінгу наразяться на згубніші та небезпечніші мережеві «хробаки». Цифрові атаки, що вперше було

продемонстровано в Україні, слугують своєрідним натяком на антиутопічну реальність, яка вже вимальовується на горизонті: хакери спричиняють блекаути (навмисно спричинені перебої в електропостачанні), що тривають днями, тижнями чи навіть довше і можуть виступити як віддзеркалення американської трагедії в Пуерто-Рико після урагану «Марія», який став причиною колосального економічного збитку і навіть людських жертв; або хакери знищують фізичне обладнання на промислових об'єктах задля створення смертоносного хаосу; або ж, як було з NotPetya, де в стратегічну мить вони просто стирають дані сотень тисяч комп'ютерів, щоб вивести з ладу цифрові системи економіки ворога чи його ключової інфраструктури.

Ця книжка розповідає про угруповання Sandworm — найвиразніший на сьогодні приклад того, як зловмисники наближають антиутопію кібервійни. Книжка висвітлює багаторічну роботу слідчих, що знаходили «відбитки пальців» Sandworm то на одному, то на іншому місці цифрового злочину і з відчайдушною надією намагалися не лише ідентифікувати цих хакерів і встановити їхнє місце перебування, а й привернути увагу до загрози, яку становить Sandworm, і зупинити це угруповання.

Водночас Sandworm — це історія не тільки про окрему хакерську групу і навіть не про значно більшу загрозу того, що Росія готова безрозсудно розгортати цю нову форму кібервійни в усьому світ. Це історія глобальнішої, всеохопної гонитви озброєнь, яка триває і сьогодні. Гонитви, яку Сполучені Штати Америки та Захід не лише не змогли зупинити, а й безпосередньо пришвидшили шляхом нашої з вами готовності стрімголов освоювати цифрові технології — інструментарій для атак. Таким чином ми впустили у світ нову, безконтрольну силу хаосу.

ПРОЛОГ

Годинник сповістив, що вже дванадцята ночі, коли зникло світло.

За вікном стояв грудневий вечір суботи 2016 року. Олексій Ясинський разом із дружиною та сином-підлітком сидів на дивані у вітальні своєї київської квартири. У колі сім'ї 40-річний український спеціаліст із питань кібербезпеки вже годину дивився стрічку Олівера Стоуна «Сноуден», аж раптом у їхньому будинку зникло світло.

— Хакери вочевидь не хочуть, щоб ми додивилися фільм, — пожартувала дружина Ясинського, натякаючи на кібератаку, що 2015 року за два дні до Різдва лишила без електроенергії майже чверть мільйона українців.

Олексію Ясинському, директорові з кібербезпеки київської компанії, яка спеціалізується на інформаційній безпеці, було не до сміху. Він глянув на портативний годинник на своєму столі: дванадцята ночі. Рівно опівночі.

Телевізор у квартирі Ясинського було під'єднано до стабілізатора напруги з резервною батареєю, тому кімнату тепер освітлювало тільки мерехтіння зображень на екрані. Втім, і джерело безперебійного живлення почало жалібно пищати. Ясинський підвівся й вимкнув його, щоб заощадити заряд. У кімнаті раптово зависла тиша.

Олексій пішов на кухню, взяв там кілька свічок і запалив їх, а потім підійшов до вікна. Худорлявий, світловолосий інженер обвів очима панораму міста — такою він її ще ніколи не бачив: усе довкруж його житлового будинку поринуло в темряву. І тільки сірі віддалені вогні відбивалися на захмареному небі, підкреслюючи зчорнілі контури сучасних новобудов і радянських висоток.

Беручи до уваги точну дату й час, — а з моменту атаки на енергомережу в грудні 2015-го минув майже рік, — Ясинський твердо знав: новий блекаут не був випадковим. Кіберспеціаліст подумав про мороз на вулиці, — сімнадцять градусів морозу, — про те, як повільно вихолоджуватимуться оселі в тисячах будинків, і про те, скільки часу зосталося, щоб труби замерзли через припинення роботи водяних помп.

Саме тоді в голові Ясинського промайнула інша параноїдальна думка: за останні чотирнадцять місяців він опинився у центрі висхідної кризи. Все більше українських компаній і державних установ зверталися до нього з проханням проаналізувати нашестя кібератак, які завдавали стрімких і нещадних ударів по їх позиціях. І за цими атаками, схоже, стояла одна група хакерів. Відтепер Ясинський не міг позбутися відчуття, що ті фантоми — привиди, чиї сліди він відстежував протягом року, — повернулися. Через інтернет. У його домівку.

Частина 1

ПОЯВА

Аналізуйте в перші ж секунди. Так ви можете втратити чимало нагод отримати швидку перемогу, але саме етап вивчення — це запорука успіху. Не поспішайте і дійте впевнено.

1
«Нульовий день»

За межами Белтвею[1], де промислово-розвідувальний комплекс Вашингтону перетікає в безкрає море парковок і сірих офісних приміщень, обвішаних логотипами й назвами компаній, — ніби для того, щоб їх швидко забули, — в Шантільї, що у штаті Вірджинія, розташовано будівлю, на четвертому поверсі якої є внутрішня кімната без вікон. Її стіни пофарбовано в матовий чорний колір, наче для того, щоб створити негативний простір, у який не потрапляє зовнішнє світло.

У 2014 році, приблизно за рік до початку кібервійни в Україні, це приміщення невелика приватна компанія iSight Partners,

[1] Автострада навколо федерального округу Колумбія *(прим. — перекл.)*.

ЗМІСТ