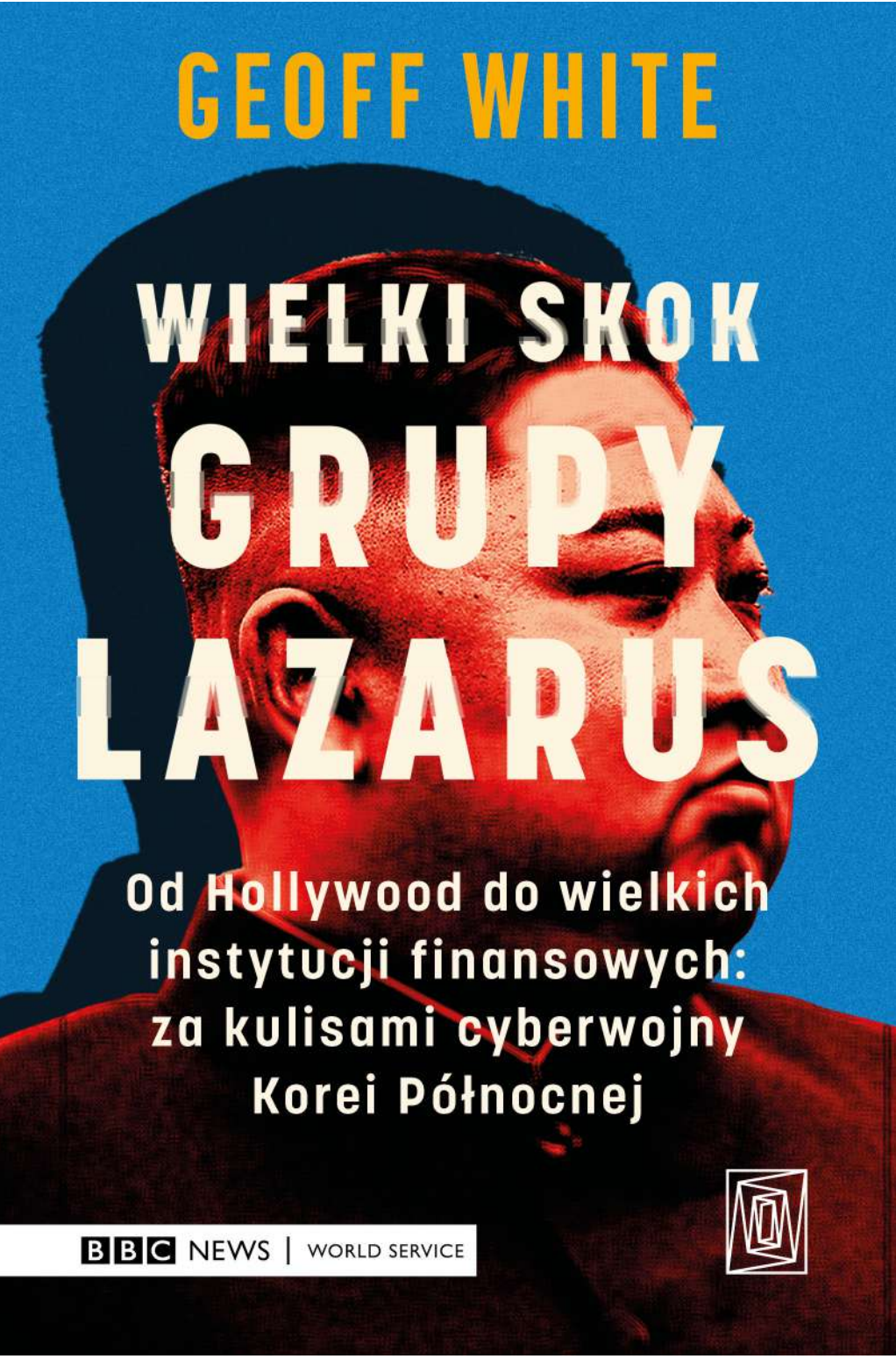
GEOFF WHITE

WIELKI SKOK GRUPY LAZARUS

Od Hollywood do wielkich instytucji finansowych: za kulisami cyberwojny Korei Północnej



BBC NEWS | WORLD SERVICE

Świat pełen jest wyrw, załomów, pęknięć – zarówno tych fizycznych, jak i niewidocznych gołym okiem szczelin rzeczywistości. Aby móc docierać do tego, co niepoznane, stworzyliśmy Szczeliny, poświęcony literaturze faktu imprint Wydawnictwa Otwartego. Pragniemy zrozumieć otaczające nas zjawiska, dlatego oddajemy głos ekspertom, którzy najlepiej potrafią wytłumaczyć zawiłości współczesnego świata.

Geoff White

Wielki skok Grupy Lazarus

Od Hollywood do wielkich instytucji finansowych: za kulisami cyberwojny Korei Północnej

tłumaczenie Hanna Jankowska

SZCZELINY
Kraków 2024

Tytuł oryginału: *The Lazarus Heist*

First published as THE LAZARUS HEIST in 2022 by Penguin Business, an imprint of Penguin General. Penguin General is part of the Penguin Random House group of companies.
By arrangement with the BBC

This book is based on the BBC News World Service podcast, *The Lazarus Heist*

Wydawca prowadzący: Rafał Czech
Redaktor prowadzący: Anna Małocha, Dagmara Małysza
Przyjęcie tłumaczenia: Magdalena Kowalczuk
Wnętrze – projekt graficzny serii: Wydawnictwo Otwarte
Adiustacja i korekta: Studio NOTA BENE
Łamanie: Daniel Malak
Promocja i marketing: Elżbieta Husarz
Okładka – designed in house by Chris Bentham. Adaptacja na potrzeby niniejszego wydania: Monika Drobnik-Słocińska
Fotografia na okładce: Brendan Smialowski / AFP / East News
ISBN 978-83-8135-336-6

Zajrzyj do Szczelin!
szczeliny.pl
facebook.com/szczeliny
instagram.com/szczeliny

Dystrybucja: SIW Znak. Zapraszamy na www.znak.com.pl.
Wydawnictwo Otwarte sp. z o.o., ul. Smolki 5/302, 30-513 Kraków.
Wydanie I, 2024. Druk: Drukarnia im. A. Półtawskiego

Przedmowa

„Z Korei Północnej? Naprawdę?”.

Często słyszę taką odpowiedź, kiedy mówię, że zbieram materiały na temat północnokoreańskich hakerów.

Wiele osób wyobraża sobie to niewielkie azjatyckie państwo – o ile w ogóle mają o nim jakieś wyobrażenie – jako dziwaczną, odizolowaną od świata krainę, która swoje ograniczone możliwości techniczne wykorzystuje przede wszystkim do wystrzeliwania rakiet i prób z bronią atomową. Raczej trudno przypuścić, żeby taki kraj mógł posiadać ekipę hakerów, nie mówiąc już o tym, że zaliczających się do najgroźniejszych w świecie.

Jako dziennikarz śledczy zajmujący się cyberprzestępczością mam całkiem odmienną perspektywę. Przez ostatnie kilkanaście lat mogłem zaobserwować, jak przestępstwa przypisywane północnokoreańskim

cyberwojownikom, których specjaliści od spraw bezpieczeństwa nazwali Grupą Lazarus, stają się coraz częstsze, groźniejsze i bardziej pomysłowe. Hakerstwo jest obecnie jedną z głównych broni w arsenale Korei Północnej i stanowi istotne zagrożenie bezpieczeństwa i stabilizacji na świecie.

Hakerzy z Grupy Lazarus zaczynali od prostych ataków na strony internetowe, ale w niepokojąco krótkim okresie postawili sobie znacznie ambitniejsze cele: niszczyli systemy informatyczne studiów filmowych i stacji telewizyjnych, wyprowadzali miliony dolarów z banków narodowych, a nawet paraliżowali pracę oddziałów szpitalnych. Motyw hakera komputerowego blokującego oddział ratunkowy występował kiedyś w filmach hollywoodzkich. Dzisiaj to rzeczywistość.

Nie jest to jednak opowieść dotycząca wyłącznie hakerstwa. Kiedy się bardziej zagłębiłem w historię akcji przypisywanych tej grupie, odkryłem globalną sieć przestępczą, ułatwiającą jej funkcjonowanie: mroczne obszary, w których działają szemrani bankierzy z Filipin, pechowi filantropi ze Sri Lanki, rekiny hazardu z Makau, japońscy handlarze używanymi samochodami i instagramowi milionerzy z Dubaju. To coraz rozleglejszy podziemny świat oszustów i kombinatorów rozporządzających nadzwyczajną władzą i obracających ogromnymi pieniędzmi. Większość działa bezkarnie, wymykają się policji czy organom ścigania.

Wielki skok Grupy Lazarus

W samym centrum znajduje się niewielka grupa niezwykle sprawnych hakerów, zdolna, jak się zdaje, niepostrzeżenie spenetrować obrane przez siebie cele. Większość ofiar opisanych w tej książce nie miała pojęcia, że jest obiektem ataku, aż było za późno – osoby te straciły pieniądze, ich dane wypłynęły, a komputery zostały sparaliżowane.

Zapoznanie się z działaniami północnokoreańskich hakerów pozwala zrozumieć świat współczesnej przestępczości. Jest ona zdumiewająco szybka, nie zna granic, wykorzystuje niewidzialną sieć wspólników. Te cyfrowe ataki stanowią chyba największe zagrożenie dla naszej obecności w internecie, bez którego już trudno nam żyć. W Wielkiej Brytanii cyberprzestępstwa znalazły się w czołówce statystyk kryminalnych, dawno wyprzedzając kradzieże i morderstwa, o których nieustannie donoszą media[1].

Działalność Koreańczyków z Północy w cyberprzestrzeni dobitnie ukazuje, dlaczego zagrożenie ze strony hakerów staje się coraz bardziej niebezpieczne. W im większym stopniu nasz świat przenosi się do internetu, tym bardziej jesteśmy wszyscy narażeni na machinacje Grupy Lazarus. Im bardziej uzależniamy się od techniki, tym większe jest prawdopodobieństwo, że staniemy się zakładnikami (niekiedy w dosłownym sensie) tych i innych cyfrowych agresorów.

Stoimy obecnie przed ogromnym wyzwaniem. Musimy się bronić przed tym nowym zagrożeniem. Grupie

Lazarus i im podobnym stawia obecnie czoło cała armia specjalistów opracowujących nowe narzędzia oraz metody odpierania ataków w celu zapewnienia nam bezpieczeństwa. Znajdziecie ich w instytucjach państwowych, w organach ścigania i zapewne w działach IT waszych organizacji czy firm. Jak się jednak dowiecie z tej książki, choćby opracowali najlepsze metody obrony, to żadne z nich nie zdołają raz na zawsze powstrzymać hakerów. To zależy od nas samych, od tych, którzy na co dzień korzystają z rozwiązań technicznych. Aby się ochronić przed większością cyberataków, nie potrzebujemy na ogół kosztownych narzędzi czy zaawansowanych umiejętności komputerowych. To prawda, że niektóre metody hakerów są przerażająco przemyślne, ale przeważnie uciekają się oni do wypróbowanych sposobów, z którymi łatwo sobie poradzić, jeśli jest się na to przygotowanym. Czasami wystarczy po prostu nacisnąć klawisz „delete" i usunąć podejrzany mail. Naszą podstawową bronią jest wiedza, a na stronach tej książki znajdziecie wiele użytecznych informacji.

Rozdział 1

Skok na bankomaty

Przybyli z całych środkowych Indii: taksówkarz z Mumbaju, aptekarz z Pune, pracownik cateringu z Nanderu, księgowy z Viraru. Wraz z dziesiątkami innych osób całymi godzinami jechali wśród ulew pory deszczowej, jedni samochodami, inni okropnymi indyjskimi pociągami, by spotkać się w jednym miejscu, w Kolhapurze, ponadpółmilionowym mieście w stanie Maharasztra.

Owego weekendu w sierpniu 2018 roku nie ściągnęło ich jednak do Kolhapuru święto religijne, festiwal czy koncert. Zjechali się, by wykonać tajne zadanie, do którego ich zwerbowano[1]. Prawie na pewno nie zdawali sobie sprawy ze skali przestępstwa, w którym mieli wziąć udział. W tym samym bowiem momencie setki innych ludzi na całym świecie wyruszyło w podobne podróże z taką samą misją. Wszyscy wykonywali polecenia elitarnej grupy cyberprzestępców, którzy

z miejsc oddalonych o tysiące kilometrów sterowali całą akcją, korzystając z pomocy międzynarodowej siatki wspólników.

Ta grupa hakerów miała dokonać jednego z najbardziej jak dotąd bezczelnych i skomplikowanych przestępstw. W grę wchodziły miliony dolarów. Według Federalnego Biura Śledczego (FBI), które obserwowało jej działania, była to kulminacja całych lat hakerskiej działalności. Grupa z biegiem czasu udoskonaliła swoje umiejętności i rozbudowała sieć kontaktów, by stać się jedną z najbardziej nieprzewidywalnych i potężnych band cyberprzestępców w skali całego świata.

Termin, na jaki wyznaczono spotkanie w Kolhapurze, nie był przypadkowy. Zebranym dano tylko kilka godzin na wykonanie wyznaczonego zadania, po czym mieli się rozproszyć i zniknąć w tłumie, gdzie nic im nie groziło – tak im przynajmniej obiecano.

Wyglądali całkiem niewinnie. Tuż przed trzydziestką lub po niej, zwyczajnie ubrani. O tym, że mieli wykonać tajne zadanie, mógł świadczyć tylko plik kart do bankomatu, jakie każdy miał przy sobie. Zadanie było proste: należało przy ich użyciu podjąć gotówkę w możliwie jak największej liczbie bankomatów, a później przekazać pieniądze „opiekunom" i dostać swoją dolę.

11 sierpnia o 3 po południu przystąpili do akcji[2]. Jedni działali w pojedynkę, inni w małych grupach. Skierowali się do dziesiątków bankomatów na ulicach

Kolhapuru. Nie było istotne, do którego banku należały, mężczyźni mieli tylko wprowadzić karty, wstukać PIN i wyjąć maksymalną możliwą kwotę.

Dwóch opowiedziało później, że całymi kilometrami chodzili po mieście, starając się pobrać gotówkę z każdego napotkanego po drodze bankomatu[3].

O dziesiątej wieczorem akcja została zakończona. Mężczyźni przekazali pieniądze szefom i otrzymali swoją należność. Podobno wypłacono im po 500 dolarów, co było ogromną dniówką w kraju, gdzie przeciętny roczny dochód nie przekracza 2 tysięcy dolarów[4]. Lecz tym, którzy nadzorowali siatkę „pieniężnych mułów", akcja bardzo się opłaciła. Wypuszczając ich tak wielu w tylu miejscach, zgarnęli w ciągu kilku godzin ponad 350 tysięcy dolarów[5]. W niektórych indyjskich bankomatach najwyższy nominał banknotu to 500 rupii, co znaczy, że gang mógł teraz mieć przed sobą stos składający się z ponad 50 tysięcy banknotów.

Lecz to był tylko czubek góry lodowej. Siedmiogodzinna operacja w Indiach była jedną z kilkudziesięciu, które jednocześnie przeprowadzono na całym świecie. Kart użyto w bankomatach w Stanach Zjednoczonych, Kanadzie, Wielkiej Brytanii, Turcji, Polsce, Federacji Rosyjskiej i innych krajach, ogółem w 29[6]. Przy całej sumie, jaka została skradziona tego jednego sierpniowego dnia, blednie ta, którą zgarnięto w Indiach: na świecie w ciągu 2 godzin i 13 minut dokonano 12 tysięcy transakcji na łączną kwotę ponad 11 milionów dolarów[7].

Był to ściśle skoordynowany rajd na międzynarodowy system bankowy. Akcję przeprowadzono z zapierającą dech skutecznością.

Jej koordynatorzy rozporządzali nie tylko wiedzą techniczną, za sprawą której bankomaty na całym świecie na żądanie wypluły banknoty, ale zdołali również zmobilizować światową sieć pomocników, którzy przekazali skradzione pieniądze organizatorom przestępstwa.

Zdaniem prowadzących śledztwo w sprawie tego skoku na banki wiele wskazywało na jednego winowajcę: grupę hakerów, której nadano różne tajemnicze nazwy – Stardust Chollima, Zinc, Hidden Cobra, Nickel Academy. Najczęściej jednak określana jest jako Grupa Lazarus. Funkcjonariusze organów ścigania obserwujący jej przestępczą działalność w internecie uważają, że to coś więcej niż kolejny gang chciwych oszustów. Grupa pracuje dla rządu Korei Północnej. Bogato finansowana i wysoce zmotywowana jednostka hakerów działa w ramach struktur wojskowych tego kraju, pozostających pod ścisłym nadzorem. Jej głównym celem jest zdobywanie pieniędzy dla reżimu. Wielu ludzi uważa Koreę Północną, której oficjalna nazwa to Koreańska Republika Ludowo-Demokratyczna, za zacofane państwo, odizolowane od współczesnego świata, pozostające pod butem nieobliczalnych przywódców, dynastii Kimów. O ile w odniesieniu do społeczeństwa tego kraju taki stan rzeczy może być zgodny z prawdą,

o tyle analitycy zachodnich organów bezpieczeństwa i porządku publicznego dostrzegają całkiem odmienną stronę tak zwanego pustelniczego królestwa.

Badacze są zdania, że w ciągu ostatnich kilku lat północnokoreańscy hakerzy na tyle rozwinęli swoje umiejętności, że zaczęli się zaliczać do najskuteczniejszych i najgroźniejszych na świecie. To, że reżim ma swoją armię działającą w sieci, nie powinno być niespodzianką. Wiele państw, w tym Wielka Brytania i Stany Zjednoczone, rozporządza takimi cyberdywizjami, a w bardzo zmilitaryzowanej Korei Północnej tego rodzaju jednostka stanowi nieodzowne uzupełnienie sił zbrojnych. Lecz analitycy śledzący poczynania tego państwa dostrzegają odmienne cechy uprawianego przez nie hakerstwa. W wielu krajach cyberoddziały skupiają się na wykradaniu informacji mogących posłużyć uzyskaniu przewagi strategicznej, natomiast wojna, jaką prowadzi w sieci Korea Północna, jest elementem walki o ekonomiczne przetrwanie kraju.

Znalazł się on bowiem w śmiertelnej pułapce finansowej, do czego doprowadziła seria zdarzeń w jego stosunkowo krótkich dziejach. Takich zdarzeń o niszczycielskich konsekwencjach było coraz więcej w ciągu ostatnich 30 lat. Korei Północnej tak bardzo zabrakło pieniędzy, że państwo nie było w stanie wypełnić podstawowych obowiązków wobec swoich obywateli, z których miliony zmarły podobno z głodu na skutek fatalnego zarządzania gospodarką oraz dogmatycznego

przestrzegania założeń panującej ideologii. Jednocześnie dążenie Korei do wejścia w posiadanie broni nuklearnej doprowadziło do nałożenia na ten kraj sankcji międzynarodowych. Opowiemy o tym w następnych rozdziałach. Skutek jest taki, że jedno z najuboższych państw świata ma niewielkie szanse na legalne wzbogacenie się[8]. Według wielu ekspertów Korea Północna sięgnęła po metody przestępcze. W przeszłości próbowała fałszerstwa, przemytu, a nawet produkcji metamfetaminy, aż odkryła znacznie pewniejsze i lukratywniejsze źródło dochodów: hakerstwo komputerowe.

Analitycy z rosnącym niepokojem obserwowali coraz bardziej wyrafinowane działania północnokoreańskich cyberwojowników. Zaczęło się od prostych ataków na strony internetowe, po czym nastąpiły przeprowadzane złożonymi technikami włamania do wielkich organizacji i instytucji finansowych na całym świecie.

Co najmniej od 2015 roku na celowniku północnokoreańskich hakerów znajdują się banki. Opanowują oni tajemny świat międzynarodowych transferów finansowych, by kraść setki milionów dolarów. Według badaczy pracujących dla Rady Bezpieczeństwa ONZ, śledzącej potencjalne naruszenia sankcji wymierzonych w Koreę Północną, kraj ten odpowiada za 21 różnych ataków na banki. Raport Rady Bezpieczeństwa z 2019 roku wylicza zaatakowane instytucje i szczegółowo omawia metody transferu i prania pieniędzy. Jest to

przerażający obraz działań hakerów, którzy bez trudu buszują po całym świecie – włamują się do systemu banku w Republice Południowej Afryki, kradną dane o kontach, by je wykorzystać do podrobienia kart bankomatowych, które zostaną użyte w Japonii. Atakują bank w Chile, odwracają uwagę pracowników, doprowadzając do zawieszenia się tysięcy komputerów, i przelewają pieniądze na konta w Hongkongu. Dokonują transferów z banku na Malcie i już po kilku godzinach pieniądze zostają wyjęte i przeznaczone za zakup rolexów oraz samochodów wyścigowych w Wielkiej Brytanii[9].

To nowy kierunek rozwoju przestępczości. Ma ona charakter ponadpaństwowy, sprawcy działają błyskawicznie i niewielka jest, jak się zdaje, szansa na ich przyłapanie. W 2018 roku obiektem zainteresowania grupy odpowiedzialnej za tę falę globalnej przestępczości stał się mało znany, ale bardzo bogaty bank z Indii.

Cosmos Co-Operative Bank jest drugim co do wielkości i starszeństwa bankiem indyjskim[10]. Powstał w 1906 roku. Tego rodzaju spółdzielcze instytucje zakładano na przełomie wieków. Miały wspomagać indyjskie rolnictwo i często działały na zasadzie *non profit*. Ich zachodnim odpowiednikiem byłyby spółdzielcze kasy pożyczkowe. Z czasem jednak niektóre z tych spółdzielni przekształciły się w nowoczesne instytucje finansowe

o złożonej strukturze. Niestety, jak potwierdzają obeznane z techniką źródła indyjskie, ich systemy bezpieczeństwa informatycznego nie dotrzymywały kroku ich rozwojowi, przez co niektóre stały się wyjątkowo narażone na cyberataki.

Cosmos Co-Operative Bank działa obecnie w 7 indyjskich stanach i ma 2 miliardy dolarów depozytów[11]. Siedzibą jego kierownictwa jest Cosmos Tower, dwunastopiętrowy srebrzysty przeszklony wieżowiec w Pune, około 160 kilometrów od Mumbaju. Otaczają go wysokie, masywne płoty, a wejścia strzeże ochrona. Te środki bezpieczeństwa nie stanowiły jednak żadnego problemu dla hakerów, którzy bez trudu dostali się do środka.

Jak podaje informator związany z indyjską branżą finansową, od września 2017 roku pracownicy oddziałów banku Cosmos zaczęli otrzymywać starannie przygotowane maile phishingowe. Ich treści nigdy nie upubliczniono, ale hakerzy zastosowali prawdopodobnie wypróbowane triki, żeby skłonić odbiorców do otwarcia wiadomości. Być może maile wyglądały jak ważne informacje finansowe albo atrakcyjne oferty pracy. Powodzenie takiego triku to często kwestia skali: jeśli wyśle się odpowiednio dużo maili, ktoś prędzej czy później złapie się na przynętę, kliknie link przesłany w mailu albo otworzy załącznik i nieświadomie zainstaluje wirusa, który umożliwi hakerom dostęp do komputera. Po kilku miesiącach hakerzy osiągnęli cel.

Wielki skok Grupy Lazarus

Gdy weszli do systemu informatycznego banku, zaczęli potajemnie rozpracowywać jego sieć. W znacznym stopniu było już to dla nich znajome terytorium. Według danych Rady Bezpieczeństwa w ciągu poprzednich 2 lat włamali się do co najmniej 14 banków, byli więc obeznani z systemami i oprogramowaniem.

Tym razem jednak mieli inny cel, skupili się mianowicie na oprogramowaniu obsługującym wypłaty z bankomatów Cosmosu. Prawie wszyscy bez większego namysłu korzystamy z bankomatów, ale nie zdajemy sobie sprawy, jak złożony system skomputeryzowanej weryfikacji i kontroli steruje urządzeniami umieszczonymi w bankach i na głównych ulicach. Od momentu włożenia karty do momentu odejścia z gotówką świat obiegają tam i z powrotem dziesiątki komunikatów, które mają zapewnić, że właściwa osoba podejmuje właściwą sumę pieniędzy. Dla hakerów, którzy namierzyli Cosmos Co-Operative Bank, ten przepływ danych miał być kluczem do wielomilionowego zysku.

Przyjrzyjmy się typowej karcie do bankomatu. Poza nazwą banku znajduje się na niej najpewniej logo Visy, Mastercard albo innej wielkiej firmy finansowej. Chodzi nie tylko o markę – szczegóły dotyczące danej firmy są zakodowane na karcie i kiedy ją wprowadzamy do bankomatu na ulicy, stacji benzynowej lub w supermarkecie, sprawdza on przede wszystkim, w której z nich zarejestrowana jest karta. PIN, który następnie wystukujemy, zostaje zaszyfrowany i przesłany do Visy,

Mastercard itp. wraz z unikatowym numerem identyfikującym nasz bank.

Organizacja płatnicza sprawdza identyfikator banku, po czym przesyła do niego zaszyfrowany PIN. Bank odszyfrowuje go i sprawdza, czy jest prawidłowy. Następnie odpowiedni program odczytuje kwotę, jaką zamierzamy wypłacić, i ustala, czy na naszym koncie znajduje się żądana suma pieniędzy. Jeśli tak, przesyła za pośrednictwem instytucji płatniczej komunikat zwrotny do bankomatu, zezwalając na wypłatę gotówki.

Dzięki temu systemowi możemy z prawie każdego bankomatu na świecie podjąć gotówkę, nawet jeśli nie należy on do banku, w którym mamy konto. Centralne miejsce w systemie miliardów transakcji zajmują organizacje płatnicze, takie jak Visa i Mastercard, przekazując informacje tam i z powrotem między bankomatami i bankami, by zapewnić zatwierdzenie transakcji. W regularnych odstępach czasu odbywają się rozliczenia mające zagwarantować, że bank, w którym posiadamy konto, zrefunduje wypłaconą przez nas gotówkę.

Dzięki internetowi wszystko to przebiega w mgnieniu oka. Większość z nas pozostaje w błogiej nieświadomości, nie mając pojęcia, co się dzieje, a przeważająca większość transakcji jest całkowicie bezpieczna, ponieważ przestępcy nie mają na ogół dostępu do obsługującego je oprogramowania. Ale w Cosmos Co-Operative Bank hakerom udało się do lipca 2018 roku rozpracować program odpowiadający za autoryzację

transakcji bankomatowych. Byli już więc zorientowani, jak systemy banku Cosmos obsługują każde podjęcie gotówki z bankomatu, i przygotowani na wprowadzenie nieznacznych zmian, które miały im umożliwić przejęcie kontroli nad systemem oraz kradzież milionów dolarów.

Mogli się po prostu ograniczyć do wprowadzenia w programie takich zmian, żeby każda transakcja była autoryzowana bez sprawdzenia poprawności PIN-u czy tożsamości osoby posługującej się kartą. Wywołałoby to jednak podejrzenia: gdyby wszyscy klienci banku Cosmos w różnych krajach świata mogli podjąć jednocześnie dowolną sumę pieniędzy bez wprowadzenia prawidłowego PIN-u, ktoś z pracowników banku szybko by się zorientował.

Hakerzy zawęzili więc pole działania, tak że „mułami" pracującymi dla nich mieli być tylko beneficjenci całej akcji. Wybrali najpierw 450 kont (nie wiadomo dokładnie na jakiej zasadzie – według niektórych raportów przejęli na chybił trafił konta prawdziwych klientów banku, według innych były to rachunki specjalnie uprzednio założone przez wspólników hakerów)[12]. Następnie musieli zapewnić, żeby komputery banku autoryzowały podjęcie znacznych ilości gotówki z tych właśnie kont. Tu jednak powstał problem. Choć mieli dostęp do tych komputerów, nie byli w stanie skontrolować, ile pieniędzy znajduje się na tych 450 kontach. Gdyby nie były to pokaźne sumy, konta na niewiele by

się zdały. Hakerzy opracowali więc metodę, która pozwoliła im obejść ten problem. Według prezesa banku Milinda Kalego wykorzystali dostęp do bankowego systemu informatycznego, oszukując oprogramowanie bankomatów tak, by uznało, że na każdym koncie znajduje się około 10 tysięcy dolarów. Jest to znacznie więcej, niż można jednorazowo wypłacić z większości bankomatów. W wyniku zmian wprowadzonych przez hakerów system miał autoryzować transakcje bez względu na wysokość podejmowanych sum.

Kiedy 450 kont było już gotowych do większych wypłat, hakerzy musieli przygotować karty do każdego z nich, co nie jest takie trudne, jak mogłoby się wydawać. Wiele osób jest przekonanych, że bankomat sprawdza przede wszystkim wypukłe cyfry na górnej stronie karty i że to one są najważniejsze. Wyobrażają sobie zapewne, że aby wyprodukować fałszywą kartę, trzeba wydrukować taką z wypukłymi cyframi. Tak już jednak nie jest (dlatego niektóre firmy emitujące karty wydają obecnie ich płaskie, gładkie wersje, bez wypukłych cyfr). W rzeczywistości najważniejsze informacje zakodowane są na czarnym pasku na odwrotnej stronie karty.

Po jej włożeniu do terminala ten magnetyczny pasek jest skanowany. Znajduje się na nim niepowtarzalny numer banku, który wydał kartę, a także jej numer, data ważności oraz imię i nazwisko posiadacza.

Żeby stworzyć kartę bankową możliwą do odczytania w bankomacie potrzebna jest pusta karta

z paskiem magnetycznym oraz urządzenie, które zakoduje na nim niezbędne dane. Zdobycie pustych kart nie stanowi problemu: nawet na kartach podarunkowych, jakimi się na co dzień posługujemy, znajduje się pasek magnetyczny, a zakodowane na nim informacje łatwo nadpisać. Urządzenie do kodowania kart można kupić w internecie za niecałe 200 dolarów… Czy to znaczy, że jeśli ktoś zna numer naszej karty, datę jej ważności, nazwisko itp., może zrobić jej duplikat i podjąć pieniądze z naszego konta? Przecież to nie może być takie proste? I nie jest, ponieważ brakuje głównego elementu: numeru PIN. Oszust może zrobić kartę z naszymi danymi, ale jeśli włoży ją do terminala i spróbuje wyjąć gotówkę, bank zapyta o PIN, a bez niego oszust nie podejmie ani grosza. To PIN otwiera dostęp do konta.

Ale hakerzy, którzy zaatakowali Cosmos Co-Operative Bank, przejęli kontrolę nad jego systemem informatycznym sprawdzającym PIN-y. Zmienili oprogramowanie tak, że reagowało na polecenia wypłat z 450 uprzednio przygotowanych kont i autoryzowało je, nie weryfikując PIN-ów. Sprawdzało następnie stan konta i w rezultacie sztuczek dokonanych przez hakerów wykazywało, że jest na nim 10 tysięcy dolarów. Do bankomatu wysyłano więc komunikat z zezwoleniem na wypłatę żądanej sumy.

W hakerskim podziemiu taka operacja nazywa się jackpottingiem.

Plan przestępstwa został opracowany i był gotowy do wdrożenia, ale potrzebni byli wspólnicy, którzy podjęliby pieniądze. Hakerzy chcieli, by odbyło się to w jak najliczniejszych różnych lokalizacjach, żeby maksymalnie utrudnić śledztwo organom ścigania. Ze źródła zbliżonego do indyjskich śledczych dowiedziałem się, że wspólników rekrutowano przez dark web – ukrytą, trudno dostępną część internetu, w której pełno jest stron używanych przez przestępców. W tym cyfrowym podziemiu „carding" (oszustwa popełniane z wykorzystaniem kart płatniczych) rozwija się i przynosi znaczne zyski. Znalezienie ludzi posiadających odpowiednią wiedzę i doświadczenie oraz gotowych do wzięcia udziału w akcji jackpottingu nie nastręczyło trudności.

Hakerzy wykorzystując kontakty w środowisku fałszerzy kart kredytowych, rozesłali dane 450 lewych kont do wspólników na całym świecie, którzy zakodowali je na pustych kartach, a te rozdali „mułom", którzy mieli z nich skorzystać.

„Brały w tym udział międzynarodowe gangi oraz agencje dystrybucji – powiedział mój informator. – Wszystkim nabywcom [skradzionych danych] wyznaczono na 11 sierpnia przedział czasu, w którym karty miały być aktywne i dało się podjąć gotówkę z bankomatów".

Jednak tuż przed datą wielkiego skoku FBI wyczuło prawdopodobnie, co się święci. Amerykański

dziennikarz śledczy ujawnił, że w przeddzień akcji na bankomaty Agencja rozesłała do banków poufne ostrzeżenie, uprzedzając, że „otrzymała ogólne informacje, iż cyberprzestępcy planują przeprowadzenie w najbliższych dniach zakrojonej na globalną skalę akcji podjęcia pieniędzy z bankomatów […] określonej mianem »nieograniczonej operacji«”[13].

FBI miało też pewne pojęcie o metodzie, jaka zostanie zastosowana: „Cyberprzestępcy tworzą przeważnie fałszywe kopie istniejących kart, przesyłając skradzione dane swoim wspólnikom, którzy kodują je na paskach magnetycznych kart wielokrotnego użytku, takich jak karty podarunkowe kupowane w sklepach”.

Federalni byli na właściwym tropie, ale, jak się wydaje, ich ostrzeżenie nie zostało szeroko rozpowszechnione i nie dotarło do Cosmos Co-Operative Bank. Zbliżała się sobota i pracownicy banku myśleli już o weekendzie. Nie mieli pojęcia, że bandy oszustów szykują się do skoku na bankomaty.

W Indiach skierowano do akcji co najmniej 23 osoby ze sklonowanymi kartami. Według tamtejszych mediów gang z Dubaju przesłał dane o kontach do wspólników w Mumbaju, którzy wyprodukowali 109 fałszywych kart[14].

Wielu podejrzanych „mułów” przybyło do Kolhapuru, gotowych 11 sierpnia przystąpić do działania. Z plikami fałszywych kart chodzili od bankomatu do bankomatu. Jedna para miała podobno w ciągu kilku

godzin wypłacić równowartość 121 tysięcy dolarów z 52 bankomatów należących do 31 banków.

Podobne wypłaty odbywały się na całym świecie. Łącznie, jak podają raporty banków, w ciągu niespełna 4 godzin podjęto 11 milionów dolarów[15].

Po podjęciu gotówki „muły" znikały w tłumie, by następnie przekazać zwitki banknotów swoim szefom.

Równocześnie pojawiły się usterki w systemie informatycznym banku Cosmos. Pomimo starannych przygotowań przejęcie przez hakerów kontroli nad systemem bankomatów spowodowało problemy. Klienci zaczęli się skarżyć, że ich transakcje są odrzucane. Innym natomiast udawało się podjąć gotówkę, nawet jeśli nie mieli wystarczających środków na koncie. Niektórzy to wykorzystali, dokonali wypłat na znaczne sumy, ale sumienie ich ruszyło i oddali pieniądze[16]. Pracownicy banku nabrali podejrzeń, że dzieje się coś poważnego i podjęli zdecydowane działania. Na dwa dni wyłączono bankowość internetową i uniemożliwiono wypłaty z bankomatów. Prawdziwych klientów zaskoczył chaos, nie mogli dokonać transakcji ani wyjąć banknotów, co stanowi szczególny problem w takim kraju jak Indie, gdzie dostęp do usług bankowych jest ograniczony, a drobni przedsiębiorcy posługują się tradycyjnie wyłącznie gotówką[17]. Milind Kale, prezes banku Cosmos, zamieścił później na YouTubie oświadczenie, by uspokoić klientów i inwestorów. „Sytuacja banku jest bardzo dobra – stwierdził. – Nasz

system bankowy świetnie działa i potrafimy stawić czoło tej sytuacji”[18].

Podczas gdy bank Kale’a pospiesznie starał się uporać z problemem bankomatów, hakerzy przygotowywali następny skok na jego aktywa.

Po przedostaniu się do systemu informatycznego Cosmosu, uzyskali dostęp do systemu SWIFT. Society for Worldwide Interbank Financial Telecommunication (Stowarzyszenie na rzecz Światowej Międzybankowej Telekomunikacji Finansowej) to, jak nazwa wskazuje, organizacja utrzymująca sieć, za pomocą której banki na całym świecie wymieniają informacje. W ramach SWIFT instytucje finansowe przesyłają między sobą miliardy dolarów.

Dlaczego banki przesyłają tak wielkie sumy pieniędzy wyłącznie za pomocą komunikatów SWIFT? Dlatego, że zakładają (w większości wypadków zasadnie), że można im zaufać, ponieważ mogą pochodzić tylko od kogoś pracującego w innym banku. Nie jest tak, że po zainstalowaniu oprogramowania SWIFT na naszych domowych komputerach moglibyśmy zgłosić się po przekaz pieniężny do banków na całym świecie.

Logika ta jednak zawodzi, kiedy hakerom udaje się włamać do banku i przeniknąć do systemu SWIFT, a tak się stało w przypadku Cosmos Co-Operative.

Dwa dni po akcji na bankomaty, kiedy bank próbował ogarnąć jej skalę i rozgryźć zastosowaną metodę, hakerzy znów uderzyli, używając komunikatów

SWIFT do wytransferowania 2 milionów dolarów na konto pewnej firmy z Hongkongu[19]. Tym razem bank szybciej się zorientował – jak twierdzi w swym raporcie, wpadł na ślad transakcji w ciągu zaledwie 15 minut. Część pieniędzy pozostała jeszcze w jego systemie, Cosmosowi udało się więc odzyskać połowę skradzionych aktywów.

Po gotówce wypłaconej z bankomatów dawno już jednak nie było śladu. Bank został obrabowany nie tylko na sumę około 11 milionów dolarów, ale na dobitkę stracił warte 500 tysięcy dolarów prowizje za wypłaty[20]. Nie bardzo wiadomo, jak pokryto straty. Bank był ubezpieczony, ale kiedy jego przedstawiciele opowiadali o akcji hakerów, o polisach ubezpieczeniowych nie wspomniano. Skończyło się zapewne na tym, że ostatecznie zapłacili za to pośrednio klienci banku, którym podniesiono opłaty za korzystanie z jego usług[21].

Tymczasem „muły", które tyle nachodziły się po Indiach, niedługo się cieszyły swoimi zarobkami. W ciągu kilku tygodni policja rozpoczęła aresztowania. Na podstawie nagrań z kamer zainstalowanych przy bankomatach udało się zidentyfikować grupę podejrzanych. Policjantom ułatwiło pracę to, że niektórzy z zatrzymanych nie po raz pierwszy uczestniczyli w takiej akcji. Według policji czterech podejrzanych kamery zarejestrowały rok wcześniej, kiedy na podrobione karty podejmowali pieniądze z innego indyjskiego banku, City Union w Ćennaju (dawniej Madras)[22].

Wielki skok Grupy Lazarus

Policja coraz szerzej zarzucała sieć, w którą wpadły „muły" z Mumbaju i jego przedmieść. Kiedy ta książka powstawała, nikomu jeszcze nie postawiono zarzutów. Istotniejsze jest może to, że aresztowania w Indiach ograniczyły się do „mułów". Policjanci byli przekonani, że udało im się zidentyfikować czołową postać wyższego szczebla i że był to ktoś zamieszkały na Bliskim Wschodzie, ale mimo wytężonej pracy nie odnotowali większych postępów.

Bank miał pod pewnym względem szczęście. Jednostka do walki z cyberprzestępczością w stanie Maharasztra uważana jest za jedną z najlepszych w kraju (między innymi dlatego, że w tym stanie ma siedziby wiele instytucji finansowych). Ale nawet tym doświadczonym funkcjonariuszom plany pokrzyżował globalny wymiar kradzieży. Ponieważ akcja hakerów odbyła się w dwudziestu kilku krajach, uzyskanie informacji na temat jej organizatorów wymagało ogromnej pracy papierkowej. Hakerzy, którzy zaatakowali bank Cosmos, prawie na pewno to przewidzieli i z premedytacją rozmieścili grupy wybierające pieniądze z bankomatów w wielu krajach całego świata, żeby utrudnić ich wyśledzenie.

Co się tyczy ustalenia tożsamości tych, którzy włamali się do systemu bankowego i zainicjowali cały skok (i mieli, jak przypuszczano, zgarnąć lwią część skradzionych pieniędzy), to miejscowa policja napotkała na kolejną trudność. „Niestety, zatarli wszelkie ślady,

nie pozostawili żadnych dowodów. To było dobrze zaplanowane" – powiedział Brijesh Singh, generalny inspektor policji stanu Maharasztra kierujący specjalną grupą dochodzeniową[23]. To powszechna metoda działania hakerów: po zakończeniu akcji starannie kasują użyte przez siebie złośliwe oprogramowanie, a także cyfrowe zapisy w systemie informatycznym ofiar umożliwiające ustalenie, co się stało i kiedy.

Indyjscy stróże prawa usilnie się starali odkryć, kto stał za skokiem na Cosmos Co-Operative Bank w sierpniu 2018 roku, ale, jak się wydaje, amerykańskie organy ścigania wyprzedziły ich o krok. W październiku Agencja ds. Cyberbezpieczeństwa i Bezpieczeństwa Infrastruktury (CISA) wydała ostrzeżenie o przestępczej kampanii, której nadała kryptonim FASTCash. W suchym języku amerykańskich cyberpolicjantów była wymierzona w „infrastrukturę systemu płatności detalicznych w bankach, by umożliwić nielegalne wypłaty z bankomatów w różnych krajach". Innymi słowy, na celowniku FASTCash znalazły się bankomaty na całym świecie[24].

Według CISA grupa stojąca za FASTCash zaatakowała banki w Azji i Afryce, kradnąc miliony dolarów, między innymi podczas „akcji, która została przeprowadzona w 2018 roku", kiedy to w tym samym czasie podjęto gotówkę w bankomatach w kilkudziesięciu państwach. Wielu badaczy zagadnień bezpieczeństwa nie miało wątpliwości, że Stany Zjednoczone obciążają odpowiedzialnością za skok na bank Cosmos organizatorów FASTCash.

Wielki skok Grupy Lazarus

Zdaniem CISA była to akcja grupy Hidden Cobra (Ukryta Kobra) – taki kryptonim nadali amerykańscy funkcjonariusze hakerom pracującym dla rządu Korei Północnej. Badacze nadali im jeszcze bardziej enigmatyczną nazwę, nawiązującą do ich zdolności przetrwania w sieciach komputerowych zaatakowanych ofiar i późniejszego „zmartwychwstania": Lazarus Group, czyli Grupa Łazarza. To właśnie te cyberoddziały miały potajemnie przeniknąć do banku Cosmos, wprowadzić zmiany do oprogramowania bankomatów, by umożliwić tysiące wypłat, a następnie podjęły próbę przekazania milionów dolarów do Hongkongu za pomocą systemu SWIFT.

Jeśli jednak, jak podejrzewają władze amerykańskie, za skokiem na Cosmos Co-Operative Bank rzeczywiście stoi Korea Północna, to nasuwają się poważne pytania. W jaki sposób ten odizolowany od świata reżim zdołał skoordynować działania dziesiątków „mułów" na całym świecie i skierować ich do bankomatów w tak niewielkim przedziale czasu? A kiedy wykonali swoje zadanie, to jak Korea Północna przejęła wypłacone przez nich miliony dolarów?

Znawcy współczesnej historii reżimu uważają, że znają odpowiedź. Według nich Korea Północna od dziesiątków lat rozwijała kontakty z przestępczym podziemiem. Powodem była między innymi seria katastrof, jakie dotknęły ten kraj od początku lat 90. Korea rozpaczliwie potrzebowała pieniędzy i dlatego wkroczyła na drogę cyberwojny.

Dzięki tym tajnym powiązaniom, zarówno online, jak i w świecie rzeczywistym, północnokoreańscy agenci rozeznali, do kogo w danym kraju mają się zwrócić, żeby stworzyć siatki „mułów" wykorzystanych podczas skoku na Cosmos. Zawarto zapewne umowę: część pieniędzy otrzymają szefowie gangów okradających bankomaty, a reszta trafi do reżimu.

Nie poprzestano jednak na atakach na instytucje finansowe. Kiedy umiejętności północnokoreańskich hakerów się potwierdziły, ich cyberoddziały, zdaniem śledczych, stały się jeszcze bezczelniejsze i wzięły na cel usługi o podstawowym znaczeniu na terytorium wrogów. Nawet oddziały szpitalne i producenci szczepionek na COVID nie mogą czuć się bezpiecznie. Może dojść do wstrzymania pilnych operacji i sparaliżowania oddziałów ratunkowych. Działalność północnokoreańskich hakerów naprawdę zadecyduje o życiu lub śmierci.

Jak do tego doszło? Jak to się stało, że niewielkiemu państwu zarzuca się prowadzenie tak bezwzględnej i niszczycielskiej kampanii cyberprzestępczej? Chcąc poznać odpowiedzi, musimy się cofnąć do czasów, kiedy Korea Północna ukształtowała się jako państwo, i zapoznać się z tragiczną w skutkach serią błędnych decyzji, które zaprowadziły ją na skraj przepaści.