



WIEM O TOBIE WSZYSTKO

Nawet oni nie są bezpieczni w sieci...
Myślisz, że ty jesteś?

MATEUSZ STĘPIEŃ

WIEM O TOBIE WSZYSTKO

MATEUSZ STĘPIEŃ

WARSZAWA
2022

Tekst
Mateusz Stępień

Redakcja
Dorota Śrutowska
Kamil Kowalski

Projekt okładki
Jarosław Stefański
Kamila Stefańska

Autor czcionki Hacked użytej na okładce
David Libeau

Wydanie I

ISBN 978-83-963222-5-8

książki prezenty  umilacze codzienności
Z Krainy Marzeń



zkrainymarzen.pl



z_krainy_marzen

Dla Mii

Zawahał się tuż nad klawiszem Enter. Tak, to była wyczekiwana wiadomość od kolegi. Tak, treść dotyczyła ich niedawnej rozmowy. Ale zastanowiło go, że obiecanie zdjęcie przysłane w załączniku było spakowane. A przecież jedno zdjęcie nie zajmuje dużo miejsca. Czy na pewno znajdzie tam to, czego się spodziewał? Czujność w sieci jest ważna, ale nie ma co popadać w paranoję, prawda?

W końcu wahanie ustąpiło miejsca ciekawości i palec niecierpliwie wylądował na klawiszu. Ale na ekranie komputera zamiast obiecanego zdjęcia mignęło tylko czarne okno z masą tekstu, którego nikt by nie był w stanie przeczytać. Zaraz potem na czerwonym tle pojawił się dramatyczny komunikat programu antywirusowego. Ostrzeżenie okazało się jednak cyfrowym nagrobkiem komputera – ekran zastygł, a system operacyjny wydał swe ostatnie tchnienie.

– Nie ma problemu, proszę pani. Możemy to załatwić w pięć minut – w słuchawce odezwał się uprzejmy głos o orientalnym akcencie.

– Ach, tak, bardzo proszę. Byłam pewna, że uregulowałam rachunek w terminie.

– Proszę przygotować kartę kredytową.

– Wiem, że chce mi pan pomóc, i może zabrzmiałoby głupio, ale wnuki ostrzegały mnie, żeby nigdy, przenigdy nie podawać przez telefon numeru swojej karty.

– Oczywiście, ma pani mądre i kochające wnuki. Mają rację i sam to mówię mojej babci Zofii. Dlatego nigdy nie prosimy klientów o podawanie danych karty przez telefon. Najbezpieczniej jest to zrobić bezpośrednio na oficjalnej stronie internetowej dostawcy prądu. Zna pani adres strony?

– Niestety nie kojarzę go. – Kobieta już drugi raz poczuła zakłopotanie w czasie tej rozmowy. Ale podziękowała też w duchu za to, że trafiła na tak dobrze wychowanego i wyrozumiałego młodego człowieka.

– Nie szkodzi, zaraz panią przez wszystko przeprowadzę, a na stronie znajdzie pani prosty formularz do dokonania płatności. Tylko musimy to zrobić od razu, żeby ekipa nie odłączyła prądu, co wiązałoby się z dodatkowymi kosztami.

– Najmocniej panu dziękuję.

– Nie ma za co, proszę pani. To moja praca, tak zarabiam na życie.

Nie wypadało wychodzić z pracy przed menedżerem, ale Mark zostawał zwykle do późna i dziś również nie było już biurze żadnego z jego podwładnych. Mark zwątpił, czy firma jest w stanie dalej odnosić takie sukcesy, jeśli pełno w niej ludzi, którzy nie mają w życiu właściwych priorytetów. Jednak zerwał się zaraz po pojawieniu się okienka z wiadomością od Candice – chociaż wiadomość od żony oraz komunikat o długo odkładanej krytycznej aktualizacji systemu nie zasłużyły na choćby sekundę jego bezcennego czasu. Wybitny, zapracowany menedżer średniego szczebla nie tylko wychodzi z pracy ostatni, ale ostatni też aktualizuje swój komputer.

Nie było potrzeby wylogowywać się z sieci firmowej. W końcu wróci tu za kilka godzin. Ale obręczkę trzeba było natychmiast zdjąć z palca i już po kilku sekundach wylądowała w kieszeni marynarki. Dziwne, w kieszeni wydawała się dużo lżejsza niż na palcu.

Spodziewał się niezapomnianego wieczoru, ale nie mógł się domyślać, że stanie się tak z zupełnie innego powodu, niż sądził. Chociaż Mark skończył pracę na ten dzień, to jego komputer czekało jeszcze sporo nietypowych nadgodzin.

1. SZCZĘŚLIWY TRAF

To był najdłuższy i najbardziej przemyślany stek przekleństw, wyzwisk i gróźb, jaki można było zmieścić w jednym zdaniu. Cała czwórka patrzyła prawie z podziwem na ekran monitora.

– Nie ma nawet jednego błędu i nie brakuje żadnego przecinka – analizował Piotr.

– Miałeś rację, istnieje słowo „szubrawczy” – dodał Feliks, zamykając okno słownika na sąsiednim ekranie.

Gdyby robili to pierwszy raz, to może by się zawahali, a nawet zrezygnowali. Ale mieli na koncie już kilka podobnych akcji i wiedzieli, że w najgorszym wypadku nie zyskają nic, ale też nic nie tracą. A w najlepszym wypadku do zdobycia była konkretna suma – jeśli tak się godzi nazwać osiem milionów dolarów. MI-LIO-NÓW! Byli prawie pewni, że ich nowy „klient” zapłaci. Miał za dużo do stracenia.

Nic dziwnego, że uśmiech nie schodził im z twarzy. W ciągu 72 godzin mieli zostać milionerami.

– To prawie dziesięć bitcoinów na głowę – rzuciła Oliwia. – Dalej nie ogarniam, jak dziesięć czegokolwiek może być warte dwa miliony dolarów.

– Raczej jak dziesięć niczego może być warte dwie bańki – mruknął Feliks.

– Raczej jak dziesięć niczego może być warte dwa miliony niczegoś innego – skorygował Leon tonem nauczyciela matematyki, który po raz kolejny dobrodusznie przypomina klasie, że przez zero nie dzielimy. Wrażenie potęgował jego ulubiony gest, którym poprawił na nosie swoje okrągłe okulary.

Pozostała trójka rzuciła na niego identyczne, nieco zniechęcone spojrzenia, ale tym razem nikt nie podjął rękawicy. Piotr przerwał krótką ciszę.

– Ja za to nie ogarniam, jak mogły chodzić po sto dolarów, kiedy o nich usłyszałem.

– A ja nie ogarniam, jak mogłem ich nie kupić, gdy były po pięćdziesiąt i zastanawiałem się nad zakupem. – Feliks zamknął oczy i westchnął, jakby był nie studentem, tylko starym biznesmenem rozpamiętującym interes życia, który przeszedł mu koło nosa. Pewnie kolejny raz liczył, ile by teraz miał, gdyby wtedy kupił chociaż sto bitcoinów.

– I tak byś je sprzedał za sto lub dwieście dolarów – Piotr odgadł myśli przyjaciela.

Szybko wrócili na ziemię. Ich obecna sytuacja była niewiele mniej bajkowa niż ta rekinów giełdowych, którzy tylko dzięki swojemu niezwykłemu intelektowi i dalekowzroczności, a nie przez czysty przypadek, dorobili się na pierwszej kryptowalucie.

Ich najnowszym klientem, jeśli tak można nazwać kogoś, na kim chce się wymusić okup, została firma Stella BioLabs. Nie

zajęli jednak ich biur, nie porwali pracowników, ani nie szantażowali szefa firmy ujawnieniem kompromitujących zdjęć czy nagrań. Nie, oni zrobili coś dla biznesu gorszego: włamali się do ich sieci komputerowej i wzięli za zakładników prawie wszystkie dane, które tam znaleźli. Dokonali ataku ransomware.

Korespondencja, listy płac, umowy z innymi firmami, ale przede wszystkim tajemnice technologiczne i brudne, wewnętrzne sekreciki. Młodzi hakerzy ledwie zaczęli przeglądać łupy, a już wiedzieli, że trafili na żyłę złota. To nie było znalezienie skrzyni pełnej skarbów. To była skrzynia pełna map do kolejnych skarbów, a każdy z nich był większy niż mogli sobie wymarzyć.

– To jak skrzynia pełna czeków podpisanych in blanco. Możemy wypisać dowolne kwoty i każdą wypłacimy! – Leon coraz bardziej ekscytował się swoimi homeryckimi porównaniami, zamiast perspektywą zarobienia marnych ośmiu milionów. Piotr starał się go przystopować.

– Wystarczy, Leon. Chyba, że chcesz dopisać na końcu ceny naszego oku... naszych usług kolejne zero?

– Dobra, dobra, osiem baniek może wystarczy.

Stella BioLabs nie była wielką korporacją, ale znajdowała się na najlepszej drodze do tego, by się nią stać. Młoda firma błyskawicznie rozwijała się dzięki patentom i kontraktom rządowym. Piotr miał dobrą intuicję i trochę szczęścia, wybierając ją na cel. Szybki rozwój firmy zawsze jest wyzwaniem – trudno wtedy pogodzić większą wydajność z bezpieczeństwem. Decyzja o transformacji IT i przeniesieniu dużej części pracy do chmury była dla firmy Stella BioLabs słuszną, ale spowodowała też krótki moment, w którym dane firmy nie były wystarczająco zabezpieczone, a hakerzy skwapliwie z tego skorzystali.

Jeden z menadżerów – niestety niedbający o aktualizację systemu swojego komputera – otrzymał bardzo szerokie uprawnienia do zarządzania systemami w firmie, aby przyspieszyć migrację do chmury. Dlatego włamanie na jego konto wystarczyło, by dostać się do większości danych w chmurze, na lokalnych serwerach, a nawet do większości kopii bezpieczeństwa z wyjątkiem najstarszych archiwów.

– Na dzisiaj wystarczy, pora się zbierać – zarządził Piotr. – Chcecie się tu spotkać też jutro?

– Żartujesz? – Zaskoczona Oliwia podskoczyła na krześle tak, że burza ciemnych loków na jej głowie wzbiła się w powietrze razem z nią. – Musimy się tu zbierać codziennie, aż nie doprowadzimy tej sprawy do końca. Ja nie chcę przegapić żadnego momentu.

– Chodzi też o kwestie bezpieczeństwa, Oliwia. Ale dobra, spotkajmy się jutro i zobaczymy, co dalej. Ty i Leon wychodzicie pierwsi, potem ja z Feliksem.

Ich hakerska melina mieściła się w piwnicy jednego z budynków starego kompleksu przemysłowego przeznaczonego do rozbiórki. Jednak termin wyburzenia cały czas się odwlekał i obecnie sprawa utknęła w martwym punkcie ku głębokiej frustracji dewelopera, który kupił tę atrakcyjną warszawską nieruchomość pod budowę nowego osiedla. Raz po raz pojawiały się kolejne przeszkody na drodze do rozpoczęcia budowy tego kurnika dla drobiu znoszącego złote jaja.

Na początku ginęła dokumentacja w systemach komputerowych urzędów wydających potrzebne decyzje lub pojawiały się w niej drobne, acz istotne błędy. Okazywało się też, że obiekt jest jedną z ostatnich siedzib kolejnych zagrożonych gatunków zwierząt. Kilka razy na miejsce przybyli aktywiści grup ekologicznych, którzy rozkładali namioty i

przykuwali się łańcuchami do budynków w obronie kruchego i niezwykłego ekosystemu.

Gdy pojawiły się doniesienia o już trzecim takim gatunku – sóweczce zwyczajnej – gniazdującym na najwyższych piętrach opuszczonych konstrukcji, tematem zainteresowali się nawet naukowcy. Chcieli ustalić, co czyni ten mały, miejski obszar tak wyjątkowym i czy pomoże to w jakiś sposób globalnym staraniom na rzecz ochrony przyrody. Ale jedyne, co znaleźli, to spora populacja szczurów. A te nie potrzebują żadnej ochrony i potrafią terroryzować lokalne społeczności lepiej niż najgorliwsze grupy ekologiczne. Mimo metodycznej pracy naukowcy nie odkryli, że za wszystkim stało stadko czwórki hakerów, fałszujących doniesienia o chronionych gatunkach w okolicy swojej kryjówki.

Wisienką na torcie było zamieszanie wokół budynku byłej kaplicy. Gdy rozniosła się wieść o krwawiącym krzyżu, na miejscu zaczęły się pojawiać pielgrzymki z całego kraju, a nawet z zagranicy.

Deweloper, przytłoczony skalą sytuacji oraz gwałtowną reakcją opinii publicznej na swoje pierwsze pomysły zrównania z ziemią tego miejsca pod budowę osiedla, przez kilka miesięcy w ogóle nie wypowiadał się publicznie na temat cudownego zjawiska, które mogłoby uzdrowić wiarę w młodym pokoleniu. W końcu jednak zaproponował przeniesienie obiektu kultu do kościoła lub katedry. Sprawa utknęła, bo nie udało się ustalić, gdzie krzyż miałby trafić ani czy w ogóle powinien zostać ruszony z miejsca. Sytuacja się nieco uspokoiła, ale pielgrzymki nadal były powszechnym widokiem.

– Jak widać lekcje ze *Sztuki wojny* Sun Tzu są równie aktualne dziś co tysiące lat temu – triumfował Leon po oszałamiającym sukcesie swojego pomysłu. Piotr miał

wątpliwości natury etycznej co do wykorzystywania ludzkiej wiary, ale tak jak reszta uległ urokowi i elegancji haka kolegi.

Na liście niewykorzystanych haków mieli jeszcze „znalezienie” pozostałości jakiegoś cmentarza, na przykład żydowskiego lub wojennej mogiły. Ale jak słusznie zauważyła Oliwia, już obecna liczba niezwykłości w tym jednym miejscu mogła budzić podejrzenia.

Teraz Oliwia i Leon skierowali się do wyjścia, do którego przechodziło się przez sąsiednie pomieszczenie. Grupa nie chciała zajmować go swoim sprzętem, więc starała się wszystko trzymać w głównym pokoju. W każdym kącie i na każdej powierzchni stał mniej lub bardziej przydatny sprzęt komputerowy, zazwyczaj wyłączony, żeby minimalizować pobór prądu. Nie tylko serwery, laptopy, desktopy czy drukarki, ale też drukarki 3D oraz przynajmniej kilkanaście różnych dronów, które stały się wręcz specjalnością młodych komputerowców. Mieli masę niezwykłych pomysłów na ich zastosowanie, które głównie dzięki umiejętnościom Oliwii byli w stanie w ostatnim czasie wprowadzać w życie, budując i testując prototypy.

Żeby dopełnić całości, wszystko to było skąpane w płataninie kabli. Mieszanina ta zaczęła w końcu wylewać się też do drugiego pokoju, który dzięki wyłomowi w ścianie był połączony z kanałem. Oliwia i Leon przeszli nim kilkadziesiąt metrów i dotarli do stalowych drzwi oddzielających ich od głównej sieci miejskiej. Klucz zgrzytnął w zamku i drzwi prawie bezgłośnie otworzyły się w ich stronę. Dalej rozdzielili się, ruszając w przeciwnych kierunkach i po chwili wynurzyli się na powierzchnię wejściami serwisowymi oddalonymi o ponad sto metrów od opuszczonego terenu. Na miejscu pozostali już tylko Feliks i Piotr.

– Nie zostajesz przeglądać dalej danych klienta? – zapytał Feliks.

– Najbardziej obiecujące kawałki mam na laptopie. Posiedzę nad nimi u siebie. Ale już widzę, że opłaci się im zapłacić za samo nieujawnienie ich danych, nie mówiąc o odzyskaniu ich – odpowiedział Piotr i szybko dodał, wyprzedzając komentarz Feliksa, który już otwierał usta: – Ale taka kwota wystarczy, bo po pierwsze, po co ci więcej niż dwa mi-lion-y dolarów? A po drugie, muszą szybko dojść do wniosku, że to im się opłaca, i sfinalizować współpracę.

Feliks zgodził się z nim w duchu, choć wyższy okup marzył mu się nie ze względu na wartość finansową. Chodziło o reputację, jaką mógłby im zapewnić w komputerowym półświatku.

Teraz oni powtórzyli procedurę opuszczenia gniazda hakerów z dwoma zmianami: wyłom zastawili włazem, który wykonali z fragmentu betonowej ściany, a w jego okolicy rozpylili pajęczynę w sprayu.

Właz poruszał się dość ciężko na platformie z kółkami i działał jak drzwi przesuwne. Między betonem a ścianą kanału zostawały zaledwie milimetry przestrzeni. Feliks odczepił magnetyczny uchwyt ze środka betonowej powierzchni, niezbędny do przesuwania kolosa siłą wątplych ludzkich mięśni, i przyłożył na moment do niepozornego obszaru u dołu wyłomu. Ciche kliknięcie oznajmiło, że sprytny mechanizm zadziałał i platforma została unieruchomiona. Całość wyglądała teraz jak dziura w ścianie odsłaniająca fragment fundamentu. Aby odkryć jego prawdziwą naturę, potrzebne by było wnikliwe badanie młotem pneumatycznym.

Po zamknięciu na klucz stalowych drzwi Piotr znów udekorował okolicę pajęczyną w sprayu, na co Feliks ostentacyjnie przewrócił oczami.

– Przestań. I tak wiem, że zazdrościsz mi pomysłu. „Pajęczyna w sprayu, co za kretynizm”, pamiętasz? – Rzucił kąśliwie Piotr.

– Zapomniałem, że istnieje coś takiego jak Halloween... czy saga *Zmierzch*.

– Widzimy się za dziesięć minut przy rondzie.

Przy rondzie Piotr zobaczył Feliksa zbliżającego się z bananem na twarzy i jabłkiem w ręce. Domyślił się, że nie nabył go drogą kupna.

– Mam nadzieję, że to nie od starowinki ze straganu.

– No co ty! To z supermarketu. Tak samo jak... – Feliks zawiesił głos i w stylu agenta CSI założył nowe okulary przeciwsłoneczne – ... to!

– To się nadaje do leczenia, Feliks.

– I kto to mówi!

– My mamy swoje powody.

– Cokolwiek pozwala ci w nocy spać, stary. Ja po prostu nie jestem hipokrytą.

Na to Piotr już tylko westchnął. Dotarli na osiedle. Feliks wsiadł do swojego auta i szybko odjechał, a kilka minut później Piotr był już u siebie.

Ashcat: Widziałeś to? :-O

Oliwia odezwała się pod swoim pseudonimem na czacie tego samego wieczora, załączając jednocześnie link. Piotr nie był chętny oderwać się od lektury tylko po to, żeby zobaczyć najnowszego mema albo filmik rodem z TikToka.

Slicer: Co to ma być?

Ashcat: Otwieraj!!1 To z lokalnej stacji TV z USA :) Na żywo było pół godziny temu -_-

Slicer: Co? Dobra, sprawdzam. Serio, nie możesz przystopować z tymi emotkami?

Ashcat: XDDDD

Slicer: Okej...

Link zaprowadził Piotra do filmu z reporterką w studiu telewizyjnym.

– Dwa dni temu firma Stella BioLabs, z siedzibą główną w Dallas, padła ofiarą poważnego ataku hakerskiego. Firma prowadzi badania i tworzy technologie w dziedzinie bioinżynierii i genetyki. Cyberprzestępcy zaszyfrowali dużą ilość danych na serwerach firmy i domagają się okupu w wysokości kilku milionów dolarów.

– Cyberprzestępcy... – powiedział do siebie z niesmakiem Piotr.

– W studiu jest z nami Jarred Warren, ekspert od zabezpieczeń komputerowych i cyberprzestępczości. Panie Warren, proszę w skrócie powiedzieć naszym widzom, na czym polega atak ransomware.

– Ransomware to złośliwe oprogramowanie, które szyfruje dane na zaatakowanym systemie komputerowym. Choć dane są dalej w tym samym miejscu, to użytkownicy nie mają do nich dostępu bez klucza deszyfrującego. I właśnie za ten klucz atakujący domaga się okupu.

– Czyli dane nie są usuwane z zaatakowanego komputera?

– I tak, i nie. To tak, jakby przestępca domagał się okupu za pani rower, ale zamiast zabrać go z pani garażu po włamaniu, założył na niego blokadę nie do zdjęcia. Albo zamknął go w przywiezionym na miejsce sejfie. Rower ciągle jest w pani garażu, ale niewiele z niego pożytku.

– Brzmi to nieco sadystycznie. W ostatnich latach znacznie zwiększyła się liczba takich ataków. Czy to nowoczesna technologia umożliwiła powstanie oprogramowania ransomware?

– Nie, technologia istnieje od dekad, to tylko prosta kwestia szyfrowania. *De facto* taki atak niewiele różni się od ściągnięcia danych i skasowania ich u właściciela, a potem domagania się okupu za ich zwrot.

– Skąd zatem popularność szyfrowania zamiast kasowania danych?

– Powodów jest kilka. Ransomware nie wymaga od atakującego kopiowania wszystkich danych na własny serwer, choć i tak często się tak dzieje.

– Dlaczego więc hakerzy i tak je kopiują?

– Dodatkowa motywacja do współpracy. W razie jej braku hakerzy grożą ujawnieniem lub sprzedażą danych na czarnym rynku. Co i tak mogą zrobić nawet po otrzymaniu zapłaty. Natomiast na pewno znika potrzeba ich kopiowania z powrotem. Ważny też jest aspekt psychologiczny, co sama pani już zauważyła. To rzeczywiście może wydawać się sadystyczne, ale fakt, że użytkownik widzi pliki wciąż u siebie, chociaż niedostępne, może skłonić go do zapłacenia okupu. Jego dane tu są, nigdzie nie przepadły i za chwilę może je odzyskać. Kiedy miałyby pani większą pewność, że rower jest do odzyskania: kiedy zniknął z garażu czy gdy dalej tam stoi przypięty obcą blokadą?

„W sumie dobry przykład, nigdy o tym nie pomyślałem” – zamyślił się Piotr z uznaniem dla eksperta...

– Gotowe jest też oprogramowanie do automatycznego szyfrowania dostępnych danych, którym mogą się posługiwać nawet słabo uzdolnieni hakerzy. Być może właśnie z takim

atakującym, któremu dodatkowo się poszczęściło, mamy do czynienia w tym przypadku. Choć zależy to jeszcze od poziomu złamanych zabezpieczeń.

...i cały szacunek momentalnie zniknął. Piotr wyżałił się na czacie:

Slicer: Co za dupek, zero uznania dla cudzej ciężkiej pracy.

Ashcat: Hahaha :))) Czekałam, aż dotrzesz do tego momentu ;) :P

Slicer: Mówi coś jeszcze ciekawego?

Ashcat: Hmm, chyba już głównie o kryptowalutach \$\$\$ I o tym, żeby nigdy, przenigdy nie płacić okupu.

Reporterka poruszyła wspomniany temat.

– Czym zatem są bitcoiny i czemu hakerzy mają takie zamiłowanie do nich?

– Bitcoiny są pierwszą i można powiedzieć najtwardszą kryptowalutą, dlatego są najchętniej wybierane. Natomiast czemu w ogóle hakerzy wybierają kryptowaluty i czym one właściwie są? Hmm, temat jest bardzo techniczny, więc na razie powiedzmy tylko, że technologia *blockchain* stojąca u podstaw kryptowalut zapewnia bezpieczeństwo i wysoką anonimowość przeprowadzanych transakcji. Czyli coś, na czym hakerom zależy.

Piotr obejrzał wywiad do końca.

Slicer: Dzięki za link, dobry materiał. Wpadasz jutro, tak?

Ashcat: Nie ma sprawy :D Jasne, że wpadam, nie chcę uronić ani sekundy z tej akcji ;P

Chociaż grupa spotykała się w komplecie bardzo rzadko, to w tych wyjątkowych okolicznościach następnego popołudnia

znów wszyscy znaleźli się w podziemiach obszaru lęgowego sóweczki zwyczajnej.

Piotr wszedł tego dnia do meliny jako ostatni. Feliks i Leon zdążyli już utknąć w środku zażartej debaty.

– Jak na gościa mającego się za jakiegoś Sherlocka brak ci perspektywy i wyobraźni – kęsał Feliks.

– Po prostu moja wyobraźnia nie jest tak wybujała jak twoja – odciął się Leon.

– Komputery kwantowe są przyszłością IT oraz całej ludzkości. I to nieodległą.

– To samo mówiłeś o drukarkach 3D.

– No i tak się stało.

– Bo wydrukowałeś plastikowy kubek i figurkę z Warhammera? A gdzie latające samochody czy samoreplikujące się roboty?

Piotr nie chciał, aby ludzkość była uboższa o bezcenne wnioski z tej dyskusji, więc zamiast im przerywać, zwrócił się do Oliwii.

– Robiliście coś konstruktywnego poza tą debatą?

Feliks i Oliwia wcześniej przeglądali fora dotyczące cyberbezpieczeństwa i hackingu, żeby zobaczyć, co środowisko mówi o ich osiągnięciu. Nie spodziewali się natrafić na nazwę ich grupy, The Avatars, bo z powodu grupowej paranoi, do której nawiązywała sama ta nazwa, prawie jej nie używali poza swoim gronem. Nikt też nie wpadł na trop tego, jak dostali się do sieci Stella BioLabs, choć kilka głosów słusznie zwróciło uwagę na bardzo dynamiczny rozwój firmy i wprowadzane zmiany w jej IT, zbyt szybkie, by za nim nadążyć. W XXI wieku człowiekowi ze swoimi ograniczeniami i przyzwyczajeniami ciężko jest dotrzymać kroku maszynie.

– Potem przyszedł Leon, rzucił niewinną uwagę o komputerach kwantowych, no i się zaczęło – zakończyła Oliwia.

Oboje spojrzeli na kolegów.

– To już się zaczyna dziać – oznajmił głosem wyroczni Feliks.

– I zwiastuje to zrobiony przez ciebie kwantowy Pacman – pociągnął Leon podobnym, acz cynicznym tonem.

– To jest trochę bardziej skomplikowane i jest to obecnie najbardziej złożona gra..., yyy..., oprogramowanie kwantowe.

– I to ma świadczyć o dojrzałości tej dziedziny?

Piotr spokojnie zainstalował się w fotelu i otworzył kilka aplikacji...

– Nieważne, czy to się stanie jutro, czy za dziesięć lat. Przyszłość to przyszłość. I jest nią kwantowe przetwarzanie danych. Nic sobie z tego nie robisz?

– A przyszłość Ziemi jest taka, że spłonie w słońcu. Nie boisz się tego?

– Nie, bo dzięki komputerom kwantowym do tego czasu ludzkość dawno skolonizuje Drogę Mleczną, a może i Grupę Lokalną.

– Panowie – przerwał w końcu Piotr. – Skupmy się na chwilę na tym drobnym odcinku czasu łączącym przeszłość z przyszłością.

Leon otworzył usta, żeby powiedzieć coś o punkcie i odcinku, ale ostatecznie odpuścił.

Rozmawiali chwilę o wczorajszym wywiadzie i o możliwych ruchach Stelli. Piotra kusilo „rozejrzenie” się po skompromitowanej sieci firmy, ale wiedział, że mają wszystko, czego potrzebują. Taką ciekawością tylko ryzykowałby pozostawianie śladów, które mogłyby do nich doprowadzić.

Stella BioLabs miała niewiele ponad czterdzieści osiem godzin na transakcję, ale specjalnie przygotowany czat między firmą a nimi od wczoraj milczał, a wirtualny portfel wciąż pokazywał śmieszną kwotę 0.01 bitcoina.

– Ej, mam nadzieję, że nie przejmujesz się tym, co mówił Leon – Piotr szepnął do Feliksa, gdy już każdy zajął się swoimi sprawami. – Nie będę udawał, że rozumiem komputery kwantowe, ale mam wrażenie, że masz do tego wyjątkową intuicję. Twoje projekty naprawdę wyglądają imponująco dla laika takiego jak ja.

– Dzięki, ale chyba jednak przesadzasz – uśmiechnął się Feliks. – A z Leonem to zwykłe przekomarzania. Poza tym zawsze lubię poznać jego perspektywę.

Piotr pokiwał głową ze zrozumieniem i zajął się swoim najnowszym projektem, nad którym pracował na uczelni. Sprawdzał ostatnie rezultaty programu pracującego non stop od kilku dni. Wyglądało na to, że ten tydzień robił się coraz lepszy, bo trafił na obiecujące wyniki.

– Ej, zobaczcie. Chyba *fuzzing* iOS'a moim nowym podejściem przynosi rezultaty.

– Jak nazwałeś moją matkę? – teatralnie oburzył się Leon. – Stary, wiesz, że możemy gadać o hakowaniu ludzi czy nawet o konkretnych hakach komputerowych, ale nie potrafię i nie chcę się dogadywać z surowymi algorytmami.

– To jest po prostu *brute force* danych wejściowych. Wrzucasz losowe dane do systemu i patrzysz, czy zaczyna gdzieś pękać – wyjaśnił Feliks.

– To nie jest aż takie proste – obruszył się Piotr. – I dane są dalekie od losowości, właśnie mój algorytm był w stanie mocno zawęzić przeszukiwaną pulę wiadomości, które mogą wysypać system.

- Jakich wiadomości? – dociekał Leon.
- Esmesów.
- Zaraz, robisz włamy do iOS przez esemesy? To ma szansę się udać?
- Według mnie to najlepszy wektor ataku. W ostatnich latach pojawiło się trochę *exploitów*¹ na iOS, których punktem wejściowym był odpowiednio spreparowany esemes.
- Dokładnie. Dostajesz esemesa, otwierasz go... – zaczęła Oliwia.
- Nawet nie musisz go otwierać – przerwał Feliks.
- Dostajesz esemesa, nawet nie musisz go otwierać, i twój telefon jest pod kontrolą atakującego, a ty możesz o tym nawet nie wiedzieć.

Perspektywa od dawna była niepokojąca dla fanów Apple'a, bo o ile największy paranoik może nie otwierać esemesów od obcych numerów, to jak ma zapobiec temu, że pojawiają się na jego telefonie? Dokładnie tego typu dziury w zabezpieczeniach i ich wykorzystywanie stały za sukcesem Pegasus – choć ten używał spreparowanych wiadomości iMessage – i innych programów szpiegujących, które były stosowane nawet przez władze państw do śledzenia terrorystów, dziennikarzy, prawników, działaczy społecznych i oponentów politycznych. Dość rozległe towarzystwo, jednak mieszczące się w jeszcze bardziej przestronnych szufladach z etykietą „wrogowie państwa”. Opinia publiczna szybko się znudziła kolejnymi aferami, więc takie doniesienia ustępowały informacjom o nowej płycie Billie Eilish lub o transferze piłkarza Realu Madryt do FC Barcelona.

¹ *Exploit* (z ang. wykorzystać, wyzyskać) – program wykorzystujący błędy oprogramowania, na przykład do uzyskania nieuprawnionego dostępu.

– Zaraz, ale dlaczego przestawiłeś się na Apple’a, skoro stworzyłeś już jeden *zero-day*² na Androida? Wprawdzie wyszedł patch, ale pewnie łatwiej znaleźć kolejną dziurę w tym samym systemie niż pierwszą dziurę w innym – dopytywał Leon. Feliks zaśmiał się na to pytanie i Leon sam rozwiązał zagadkę. – Okej, niech zgadnę, właśnie dlatego, tak? Chcesz nowego wyzwania, skoro Androida już ogarnąłeś?

Piotr tylko wzruszył ramionami z miną niewiniątka. Teraz Oliwia miała pytania.

– Jak ty w zasadzie dorwałeś się do komputerów naukowych na uczelni? Rozumiem, że każdy z nas może się tam włamać, nawet Leon, ale one są cały czas zarezerwowane na potrzeby pracowników naukowych do wyliczania ich beznadziejnych pomysłów i teorii. A twój program chodzi tam od kilku dni.

Feliks bawił się wyśmienicie, a Piotr zamiast zgrywać dalej niewiniątka postanowił pochwalić się swoim dokonaniem.

– Chodzi od pięciu dni. Pamiętacie, że profesor Kula miał coś symulować o wielkim wybuchu i promieniowaniu mikrofalowym tła za pomocą programu, który – jak podkreślał – sam napisał? No to właśnie uruchomił go pięć dni temu na komputerach uczelni. Dorwałem się do kodu jego programu i to jest bida z nędzą. Wprowadziłem parę usprawnień, ale wystarczyło tylko jedno: zastosować wyszukiwanie binarne.

– Ciekawe, powiedz coś więcej – domagał się Leon.

– To tyle, nie kojarzysz wyszukiwania binarnego? Uwaga, będą surowe algorytmy.

– Dawaj, ale tłumacz tak, jak nieogarniętemu dalmatyńczykowi lub pudlowi.

² *Zeroiday, zero-day exploit* – *exploit* wykorzystujący lukę w systemie, która nie jest jeszcze publicznie znana lub nie została do niej jeszcze wydana poprawka.

Piotr się zamyślił nad stosownym porównaniem, a wszyscy czekali na wykład. Feliks i Oliwia znali wyszukiwanie binarne, co należało do podstaw algorytmiki, ale lubili słuchać opisowych i łopatologicznych wyjaśnień, w których Piotr był ekspertem.

– Wyobraź sobie, że masz godzinny film, na którym powoli zachodzi słońce. Chcesz znaleźć dokładnie moment, kiedy zniknie za horyzontem.

– No to będzie gdzieś pod koniec.

– Tego nie wiesz. Jak najszybciej znaleźć to miejsce? Oglądać od początku scena po scenie?

– Bez sensu. Mogę sprawdzić, co jest w połowie filmu, by zobaczyć, czy jest jeszcze przed zachodem słońca czy już po, i przewinąć trochę w odpowiednią stronę. W stronę początku, jeśli w połowie był już zachód, lub w stronę końca, jeśli jeszcze jest przed zachodem. I tak dalej, aż znajdę moment zajścia słońca.

– Idealnie. Nic nie trzeba tłumaczyć – zachwycił się Piotr. – Masz coraz mniejszy wycinek, aż trafisz na szukany moment. A czemu ta metoda działa tutaj, a nie kiedy na przykład szukałbyś momentu z przelatującym ptakiem?

– No bo nie wiesz, czy ptak w danym kadrze już przeleciał czy nie. Za to w każdej klatce wiesz, czy słońce już zaszło czy jeszcze nie.

– Właśnie. Można powiedzieć, że klatki filmu są posortowane i widząc jedną klatkę, wiesz, w którą stronę szukać dalej.

– Czyli wyszukiwanie binarne działa tylko na sortowanych danych? – zapytał Leon, a Piotr przytaknął. – I profesorek szukał po kolei od lewej do prawej na sortowanych danych?

– Nie do końca, ale i temu bym się nie zdziwił. Kula najpierw mnóstwo razy robi zwykłe wyszukiwanie na wielkiej liście elementów, a chwilę potem ją sortuje. Ja po prostu odwróciłem kolejność: najpierw sortuję, a potem robię wyszukiwanie binarne zamiast zwykłego.

– Dzięki temu szukając wśród miliona elementów, wystarczy zajrzeć tam tylko dwadzieścia razy, logarytm z miliona. A nie średnio pół miliona razy, tak jak robił to Kula – dokończył roześmiany Feliks. – Takie milionowe listy ma właśnie profesor. A ten wariat ściągnął jego program do siebie na laptopa i zatrzymał jego wyliczenia. Wykopał profesora z komputerów uczelni i sam zajął przydzielony mu czas. Najlepszy sprzęt uczelni od kilku dni pracuje nad włamem do iOS zamiast nad symulacjami kosmicznymi profesora.

– A co z jego wynikami? – zaniepokoiła się Oliwia.

Piotr wrócił do trybu niewiniątka wzruszającego ramionami.

– Dostałem jego wyniki po czterech godzinach pracy poprawionego programu na moim laptopie. Zaraz je podrzucę na uczelnię, bo chyba mam to, czego szukałem. To, jak się wysypał dziś iOS, wygląda bardzo obiecująco, chyba coś z tego będzie.

Piotr od razu zajął się tematem, Oliwia i Feliks do niego dołączyli. Do włamu do iOS była jeszcze długa droga, ale byłoby to ogromne osiągnięcie. Apple iOS uchodził za system bezpieczniejszy od Androida, nawet pomimo kolejnych dziur znajdowanych w ostatnich latach. Telefony tej marki, iPhone'y nie pozwalały użytkownikowi na wprowadzanie dużych zmian konfiguracyjnych i mocno wymuszały regularną aktualizację systemu. Użytkownik mógł mniej zepsuć, a zaktualizowany telefon to bezpieczniejszy telefon. Z drugiej jednak strony, jeśli

uda się znaleźć dziurę w iPhone, to prawdopodobnie będzie ona na wielkiej liczbie urządzeń z tą samą wersją systemu i zarówno pojedynczym użytkownikom, jak i programistom systemu będzie trudniej go wykryć.

Nagle na czacie pojawił się uprzejmy tekst.

StellaBioLabs: Dzień dobry.

TechSupport: Dzień dobry, w czym możemy dzisiaj państwu pomóc?

Piotr szybko odpisał, ku ucieście pozostałej trójki, która błyskawicznie zebrała się przed jednym monitorem.

StellaBioLabs: Mam informację do przekazania.

TechSupport: Czy jest o przelewie na kwotę około 40 BTC za nasze wsparcie?

StellaBioLabs: Nie.

Atmosfera nieco się ochłodziła, ale wciąż jeszcze nie stała się mroźna. Piotr postanowił nie odpisywać i poczekać na kolejny ruch klienta.

StellaBioLabs: Macie 48 godzin na podanie na tym czacie klucza deszyfrującego do wszystkich danych firmy Stella BioLabs.

Na tę wiadomość The Avatars spochmurnieli.

– Czy oni myślą, że to cokolwiek da? Że wystarczy sprawiać wrażenie, że ma się silną kartę, kiedy nie ma się nic? – rozważał Leon. – Może im napisać, że gdzie indziej możemy znaleźć chętnych nabywców na dane, których oni już nigdy nie zobaczą?

Piotr uczynił gest, jakby chciał uciszyć Leona, by rozmówca po drugiej stronie przypadkiem ich nie usłyszał. Zostawił na boku rozczarowanie odpowiedzią i napisał:

TechSupport: Oczywiście, klucz zostanie przekazany w ciągu kilku godzin od uiszczenia ustalonej opłaty.

StellaBioLabs: Czy możecie przekazać nasze oczekiwania właściwym osobom?

Reakcja rozmówcy była natychmiastowa i zignorowała przekomarzania Piotra.

TechSupport: A kto ma je otrzymać?

Piotr był ciekaw, dokąd ta rozmowa go zaprowadzi. Podróż okazała się krótka, za to z przytupem.

StellaBioLabs: Piotr i Feliks.

Grom spadł z jasnego nieba. Zaczęła się burza z gradobiciem. Piotrowi zadzwoniło w uszach, a obraz przed oczami zaczął się zwężać. Ale zdążył jeszcze przytomnie szybko odpisać, żeby spróbować ukryć, jakie wrażenie wywarła ostatnia wiadomość.

TechSupport: Kto?

StellaBioLabs: Dziękuję i dobranoc.

To był koniec rozmowy i początek nowego rozdziału w życiu tępo wpatrujących się w ekran.

Jak!? Skąd oni mogą to wiedzieć!? Przez chwilę wszyscy czuli kompletną panikę, jak małe dzieci. Nie jak dzieci, które zostały nakryte przez rodziców z ręką w pudełku ciastek, ale jak te, które zgubiły się w największym centrum handlowym świata. Szybko jednak się opanowali.

Piotr zaszył się w swoim komputerze. Czy ktoś namierzył ich włam do sieci wi-fi pobliskiej firmy, którą mogli osiągnąć dzięki antenie kierunkowej? Nie wygląda na to.

Wirtualny tunel VPN³ działa prawidłowo. Dalej są też w sieci Tor⁴, więc powinni być anonimowi i prawie nie do namierzenia.

Feliks przeskanował pomieszczenie w poszukiwaniu obcego nadajnika.

Oliwia sprawdzała, czy ktoś mógł trafić na ślad ich nie do końca legalnego podpięcia do prądu, ale dostawca jak zawsze wydawał się nie ogarniać własnego podwórka.

A Leon siedział i dumał wpatrzony w ekran ze znamioną rozmową.

– Wydumałeś coś? – zapytał Feliks.

– Niewiele... nie był to ślepy strzał. Z jednym imieniem mogli trafić, ale nie z dwoma.

– Jakże spostrzegawczo!

– Taaa, wiem. Myślę, że on może być spoza firmy. Ale to luźna myśl.

– Dlaczego? Piotr potwierdził, że komunikacja wyszła z ich sieci.

³ *Zeroiday, zero-day exploit* – *exploit* wykorzystujący lukę w systemie, która nie jest jeszcze publicznie znana lub nie została do niej jeszcze wydana poprawka.

⁴ *Zeroiday, zero-day exploit* – *exploit* wykorzystujący lukę w systemie, która nie jest jeszcze publicznie znana lub nie została do niej jeszcze wydana poprawka.

– Chodzi o to: „dane firmy Stella BioLabs”. Nie napisał: dane, nasze dane, dane naszej firmy, ani nawet dane Stella BioLabs. Tylko „dane firmy BioLabs”. Jakby był z zewnątrz.

– To słaby punkt zaczepienia. Poza tym mógł to być konsultant wynajęty z zewnątrz.

– Tak, tylko do czego? Stosowania sztuczek psychologicznych?

– Do znalezienia nas i odzyskania danych – dołączył się Piotr.

– Dobrze, tylko jak dokładnie ta rozmowa miała nas do tego skłonić? Podali nasze imiona, ale niczym nie grozili, nie mówili, co się stanie za czterdzieści osiem godzin, nic.

– Grożą nam ujawnieniem, to chyba jasne.

– Jeśli wiedzą, kim jesteśmy i gdzie, mogli nas zgarnąć z zaskoczenia. Tak byłoby dla nich lepiej. Już same prawne konsekwencje byłyby dużo gorsze, gdybyśmy nie poszli na współpracę i nie oddali klucza.

Istniało dużo niewiadomych, ale rzeczywiście coś tu nie pasowało. Leon był w swoim żywiole, zapominając o czającym się zagrożeniu. Albo właśnie pamiętając, że jego imię nie padło na czacie...

– Na ten moment przychodzą mi do głowy dwa motywy. Albo nie wiedzą o nas nic więcej i taką zagrywką chcą nas skłonić do ugięcia się lub popełnienia błędu...

– Na przykład wejścia do ich sieci, żeby poszukać informacji? – Wtrąciła Oliwia, a Leon przytaknął.

– ...albo tak naprawdę nie zależy im na kluczu i chcą osiągnąć coś zupełnie innego.

– Dlaczego Stelli miałoby nie zależeć na swojej dokumentacji, wynikach badań, technologii... – zaczął Piotr.

– Bądźmy precyzyjni, Piotrek – przerwał Leon, który zaczął krążyć po pokoju zamyślony niczym Sherlock Holmes, próbujący rozwikłać wielką tajemnicę samą potęgą dedukcji. Aż dziwne, że nie nazwał Piotra Watsonem. – Nie mówimy koniecznie o Stella BioLabs, tylko o naszym rozmówcy z czatu. Będziemy musieli jednak tam wejść, żeby się rozejrzeć.

– Zwariowałaś!?! – oburzył się Feliks. – Przecież sam mówiłeś, że może właśnie o to im chodzi!

– Spokojnie, mam na to sposób, nie sprawdzimy wszystkiego, ale będziemy też praktycznie nie do namierzenia – zaczął tajemniczo Piotr. – Na kilkudziesięciu serwerach zostawiłem bota⁵, którego prawie na pewno nie znaleźli. Mogę go aktywować jednym poleceniem. Zbierze i wyśle do nas najnowsze logi, zapisy czatów z wewnętrznego komunikatora, mejle i wpisy z kalendarzy sporego grona menedżerów i jeszcze parę innych drobiazgów. Minus jest taki, że pewnie po tej akcji szybko go wykryją i usuną, więc prawdopodobnie możemy go użyć tylko raz. Chyba że są jeszcze gorsi w kwestii bezpieczeństwa niż Monsanto, do którego włamaliśmy się w zeszłym roku

– Zróbmy to od razu – ucieszył się Leon.

– Ale najpierw porozmawiajmy o tym, co oczywiste: najwyraźniej na celowniku jesteście tylko ja i Feliks. Dlatego kiedy dziś się rozejdziemy, to wy, Oliwia i Leon, już się tu nie pojawicie pod żadnym pozorem i będziecie czekać na kontakt od jednego z nas, jasne? Macie dostęp do portfela bitcoinów, więc sprawa będzie przejrzysta. Nie będziecie mieć powodów podejrzewać, że to sztuczka, którą chcemy was wyrąbać na kasie.

⁵ Bot (od „robot”) – skrypt lub program komputerowy, który automatycznie wykonuje pewne z góry ustalone zadania.

– Przestań... – odpowiedziała Oliwia, karcąc się w myślach za właśnie takie podejrzenie, które przez moment przyszło jej do głowy.

– Dobra, wchodzimy. Teraz żałuję, że nie zapytałem ich „a jak nie, to co?”.

– Nie zdążyłeś, bo to oni szybko urwali rozmowę – odpart na to Leon. – Co tylko rodzi kolejne pytania.

Piotr użył innego łącza internetowego niż zwykle, choć i tak nawet nie musiał wchodzić do sieci Stelli, żeby uruchomić swój skrypt. Każdy mógł to zrobić z zewnątrz. Wystarczyło napisać odpowiedni mejl na odpowiedni adres. Piotr zostawił sobie dwie furtki i teraz przeszedł przez obie naraz. Pierwsza to napisanie mejla przez formularz kontaktowy na stronie internetowej Stelli i zatytułowanie wiadomości „Pytanie o bezpieczeństwo współpracy po ataku ransomweare” – celowo z błędem. Treść mejla nie miała znaczenia, choć najlepiej, by wyglądała jak wiadomość od potencjalnego partnera biznesowego zatroskanego sytuacją w Stelli. Bota interesował tylko ten konkretny nagłówek.

Druga furtka to mejl na adres platformy GitLab w Stella BioLabs. GitLab jest oprogramowaniem pomagającym zarządzać zadaniami i projektami w zespołach IT. Ma wiele przydatnych funkcji: między innymi można dodawać do niego zadania, wysyłając mejl na odpowiedni adres i o odpowiednim tytule i treści. Nadawca mógł być dowolny, ale Piotr podszył się pod nadawcę no-reply@stellabiolabs.com i wysłał wiadomość o tytule „Testowe zadanie po aktualizacji”. Bot po cichu sprawdzał okresowo zadania w GitLabie, podobnie jak wiadomości z formularza na stronie, w oczekiwaniu na taki właśnie wpis. Dodatkowa spacja przed słowem „aktualizacji” zapewniała, że żaden pracownik nie uruchomi programu przypadkowo, tworząc zadanie o takiej nazwie. Nie



WIEM O TOBIE WSZYSTKO

Nawet oni nie są bezpieczni w sieci...
Myślisz, że ty jesteś?

MATEUSZ STĘPIEŃ