Nowa odsłona cyberwojny

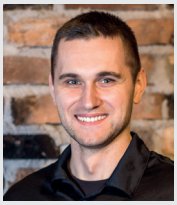
Nie epatujmy nagłaśnianymi medialnie atakami grupy Anonymous. Prawdziwa cyberwojna Rosji z Ukrainą toczy się w tle od kilku lat, a wielu jej aspektów możemy nigdy nie poznać.

Podczas aneksji Krymu w 2014 r. Rosjanom udało się sparaliżować nie tylko ukraińskie sieci telekomunikacyjne, lecz także system dowodzenia i kierowania obroną państwa. Od tej pory kolejne spektakularne cyberataki miały być dowodem na supremację Rosji w cyberprzestrzeni. W grudniu 2015 r. hakerzy rosyjscy włamali się do ukraińskich systemów informatycznych kontrolujących sieci energetyczne i na 6 godzin wyłączyli zasilanie, pozostawiając setki tysięcy Ukraińców bez prądu. Jak później ustalili analitycy, za tym czysto politycznym zadaniem stały służby rosyjskiego wywiadu. Rok później doszło do powtórki, tym razem tylko Kijów został pozbawiony prądu. Apogeum przyszło rok później, gdy rosyjska cyberarmia została wzmocniona o narzędzia, wykradzione z amerykańskiej agencji wywiadowczej National Security Agency (NSA).

NotPetya sieje zniszczenie

– 27 czerwca 2017 r. Kreml odpalił cyberbroń NSA na Ukrainie, co okazało się najbardziej destrukcyjnym i kosztownym cyberatakiem w historii świata. Tego popołudnia zgasły ekrany wszystkich urządzeń na terenie kraju. Ukraińcy nie mogli pobrać gotówki z bankomatu, zapłacić za paliwo na stacji benzynowej, wysłać lub odebrać maila, kupić biletu na pociąg, zrobić zakupów spożywczych, odebrać własnego wynagrodzenia oraz, co najgorsze, monitorować poziomu promieniowania radioaktywnego w elektrowni w Czarnobylu. Konsekwencje ataku odczuwalne były także poza granicami Ukrainy. Ucierpiały firmy prowadzące działalność na terenie tej byłej radzieckiej republiki. Każdy ukraiński pracownik międzynarodowej organizacji stanowił furtkę do

Swoją wiedzą podczas marcowego Klubu Informatyka podzielili się wybitni specjaliści w zakresie cyberbezpieczeństwa:



Rafał Chruściel

analityk zagrożeń oraz inżynier bezpieczeństwa infrastruktury IT, od 10 lat związany z branżą cyberbezpieczeństwa. Doświadczenie zdobywał w takich firmach, jak F5 Networks czy Allegro. Obecnie lider zespołu reagowania na incydenty w ISS World Services A/S.

Łukasz Jachowicz

specjalista ds. cyberbezpieczeństwa w Mediarecovery, prezes Internet Society Poland. Zawodowo zajmuje się analizą incydentów bezpieczeństwa, cyberbezpieczeństwem ofensywnym oraz doradzaniem w kwestiach zabezpieczania infrastruktury. Był członkiem Rady ds. Cyfryzacji. Wieloletni doradca największych firm technologicznych.

sieci globalnej. Zaatakowano komputery spółek farmaceutycznych Pfizera oraz Mercka, gigantów na rynku przewozów i dostaw, czyli firm Maersk oraz FedEx, jak również producenta wyrobów czekoladowych Cadbury w jego fabrykach zlokalizowanych na Tasmanii – pisze Nicole Perlroth w prologu do swojej niedawno wydanej książki: „Cyberbroń i wyścig zbrojeń. Mówią mi, że tak kończy się świat", uznanej przez Financial Times & McKinsey za najlepszą książkę biznesową roku 2021.

Skutki ataku były niewiarygodnie dotkliwe. Gigantowi morskiemu Maersk, operującemu 800 statkami w 76 portach, przywrócenie systemu na 4 tys. serwerów oraz 45 tys. komputerów zajęło dwa tygodnie i wymagało zaangażowania 600 specjalistów. Operacja się powiodła, bo dzięki awarii zasilania w Ghanie ocalała jedyna niezainfekowana kopia danych. Straty Maerska oszacowano na 1 mld USD.

Chwile grozy przeżył personel elektrowni w Czarnobylu, gdy utracono możliwość kontroli promieniowania. Siergiej Gonczarow, kierownik techniczny elektrowni w Czarnobylu, po zorientowaniu się co do skali ataku, nakazał fizyczne odłączenie komputerów i wysłał pracowników, aby na zewnątrz ręcznie dokonywali pomiarów promieniowania.

Preinwazyjne cyberataki

W tym roku Rosji marzyła się powtórka z 2014 – wywołanie chaosu w Ukrainie za pomocą cyberataków, poprzedzających inwazję militarną. W nocy z 13 na 14 stycznia br. Rosja przypuściła szturm na wiele ukraińskich serwisów rządowych, podmieniając treści (tzw. deface) na taki obrazek:

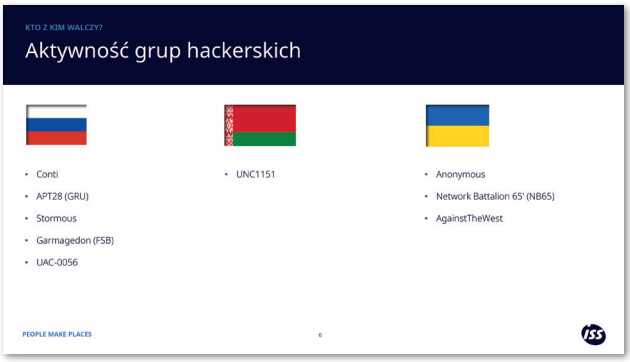
– CERT ukraiński obwinił za to działanie grupę białoruską. W ramach działań dezinformacyjnych na przejętych stronach pojawił się tekst w trzech językach, w tym w dość kulawej polszczyźnie, co zapewne było próbą wskazania fałszywego tropu do Polski. Dzień później zidentyfikowano ransomware WhisperGate, a 8 lutego CERT UA odkrywa farmę botów we Lwowie (18 tys. fałszywych kont w mediach społecznościowych), mającą za zadanie sianie paniki wśród ludności ukraińskiej. 15 lutego przypuszczono ataki DDoS na ukraińskie strony rządowe, za atakami stało najprawdopodobniej GRU. Tego samego wykonano atak typu spear phishing na sektor mediowy i militarny, za co odpowiedzialna była związana z FSB rosyjska grupa Garmagedon. Wreszcie 23 lutego zidentyfikowano HermeticWiper – informował Rafał Chruściel, analityk zagrożeń i inżynier bezpieczeństwa infrastruktury IT podczas Klubu Informatyka, zorganizowanego pod koniec marca br. przez Mazowiecki Oddział PTI.

HermeticWiper zaatakował setki maszyn w Ukrainie, ale nie wyrządził szkód o oczekiwanych rozmiarach z dwóch powodów: Ukraina od 2014 r. zdołała poprawić swoje zabezpieczenia i tym razem miała wsparcie sojuszników.

Słowacka firma ESET, zajmująca się cyberbezpieczeństwem, odkryła mechanizm ataku i poinformowała o nim społeczność międzynarodową (prawdopodobnie w celu zmylenia programów antywirusowych Wiper jest podpisany przy użyciu certyfikatu podpisywania kodu wydanego przez cypryjską firmę Hermetica Digital Ltd, stąd nazwa tego malware). Znacznik czasowy kompilacji PE jednej z próbek wskazuje na to, że atak mógł być przygotowywany już od końca 2021 r. Równie szybko zareagował Microsoft (HermeticWiper bierze na cel systemy operacyjne rodziny Windows) i zawiadomił amerykańskie służby.

Wojna dzieli Internet

Liczba grup hackerskich walczących po każdej ze stron konfliktu zmienia się płynnie, proporcja liczbowa wskazuje na przewagę ukraińską, według https://twitter.com/cyberknow20 4 kwietnia br. były to 23 grupy prorosyjskie, 48–51 proukraińskich (nie tylko z Ukrainy). Prorosyjskie grupy są sponsorowane przez rząd, wywiad i FSB, proukraińskie to aktywiści sympatyzujący z Ukrainą. W ramce zamieszczamy zestawienie najbardziej znanych grup walczących po obu stronach, ta pod flagą białoruską jest sponsorowana przez Rosję.



Dwa dni po inwazji Mychajło Fedorow, ukraiński wicepremier i minister transformacji cyfrowej wezwał za pośrednictwem Telegramu do utworzenia cyberarmii Ukrainy. ITArmy, organizująca swoje działania za pośrednictwem szyfrowanych kanałów w Telegramie, ma być dobrowolną, ale oficjalną instytucją rządu Ukrainy. Trudno jednak zweryfikować, w jakim stopniu ta inicjatywa się powiodła. Niewątpliwie Ukraina zaczęła się bronić, przeprowadzając kontruderzenia. W miarę trwania inwazji ataki obu stron się intensyfikują i obecnie mamy do czynienia z cyberwojną na pełną skalę.

– *W dniu inwazji militarnej przeprowadzono ataki DDoS na rosyjskie strony rządowe. W odwecie dzień później sponsorowana przez rząd białoruski grupa UNC1151 rewanżuje się atakami phisingowymi na Ukrainę. Conti gang ogłasza wsparcie dla Rosji, po czym jeden z ukraińskich badaczy bezpieczeństwa, najprawdopodobniej członek gangu, publikuje 60 tys. wiadomości wymienionych między członkami grupy. 26 lutego NB65 hakuje Instytut Badań Jądrowych Rosyjskiej Akademii Nauk i publikuje 40 tys. plików, ale nie analizowałem ich zawartości* – informował Rafał Chruściel. Koleje Białoruskie po ataku Anonymous przechodzą na ręczne sterowanie, odnotowując ogromne opóźnienia na stacjach kolejowych. 1 marca kolejny malware: IsaacWiper oraz HermeticRansom zostają odkryte w Ukrainie.

2 marca powiązana z Anonymous NB65 atakuje Roskosmos - rosyjskie NASA. Pięć dni później ATP28 powiązana z wywiadem rosyjskim przeprowadza atak na ukraińską grupę mediową UkrNet, białoruski UNC1151 uruchamia kampanie phishingowe w Polsce i Ukrainie. Dzień później RuRansom szyfruje dane na komputerach, na których zostaje uruchomiony, nie żąda jednak okupu, wyświetla info o działaniach Putina. 10 marca pojawia się Liberator – fake narzędzie do DDoS, tak naprawdę trojan, szpiegujący i wysyłający dane na rosyjskie adresy. W połowie marca pojawił się fake translator z języka ukraińskiego, kierowany głównie do osób przekraczających granicę ukraińsko-polską i ukraińsko-węgierską. 22 marca zaczął działać DoubleZero wiper.

Techniki ataków obu stron są podobne:

Target: **Ukraina**	Target: **Rosja**
DiskWiping: WhisperGate, HermeticWiper, DoubleZero, CaddyWiper, IsaacWiper	Ransomware: RuRansom
Defacement	DDoS
Fake News	Defacement
Spear Phishing	Data leakage
	Fake News

Źródło: Prezentacja Rafała Chruściela

– *Głównym narzędziem wojny informacyjnej są fake newsy, pojawiła się ich ogromna liczba. Coraz częściej dochodzi do wykorzystywania technologii deep fake* – mówił Rafał Chruściel, demonstrując zmanipulowane wystąpienie prezydenta Zełenskiego.

#OpRussia

Zaledwie kilka godzin po zbrojnym ataku Rosji kolektyw hakerski Anonymous wypowiedział wojnę Rosji na Twitterze. Od tego czasu pod hasztagiem #OpRussia publikowane są zrzuty ekranowe zhakowanych stron internetowych rosyjskich stacji radiowych lub stron rządowych, filmiki o wyciekach danych, wykradzione pliki, a nawet podsłuchy komunikacji rosyjskiego wojska.

Rafał Chruściel postrzega Anonymous jako grupę haktywistów przeprowadzających ataki cybernetyczne bez celów finansowych, najczęściej są one wyrazem manifestacji obywatelskiej niezgody. Drugi z ekspertów zaproszonych na Klub Informatyka – Łukasz Jachowicz – specjalista ds. cyberbezpieczeństwa w Mediarecovery i prezes Internet Society Poland, postanowił przeanalizować rzeczywiste osiągnięcia Anonymous, którymi epatują nas media.

– *W światowej i polskiej prasie możemy przeczytać, że są wszędzie, rzucili Rosję na kolana, ukradli satelity szpiegowskie, ujawnili dane rosyjskich agentów z całego świata, przechwycili rosyjskie systemy łączności, zhakowali rosyjskie ministerstwo obrony* – zaczął swoje wystąpienie Łukasz Jachowicz.

Anonymous pod lupą

Łukasz Jachowicz wywodzi się ze środowiska aktywistów, przyglądał się więc efektom ataków Anonymous z przyjacielskim nastawieniem. Wszystko jednak wskazuje na to, że spektakularność tych działań w dużej mierze ma charakter medialny.

„Opanowanie Rosatomu" (nagłówek z polskiej prasy) polegało na utworzeniu nowej strony html z hasłem fckptn. Atak na stronę Roskosmosu to umieszczenie nowego wpisu. Po analizie 800 MB danych wykradzionych z rosyjskiego sektora kosmicznego okazało się, że to głównie skany uzgodnień dotyczące projektu lądownika czy sondy księżycowej – ktoś wykorzystał za szerokie uprawnienia do zasobów sieciowych i ściągnął archiwum. Rosyjska przestrzeń adresowa jest powszechnie skanowana i każdy otwarty dostęp do pdf jest natychmiast wykorzystywany.

Na to, że: „Rosja straciła dostęp do satelitów szpiegowskich" (kolejny tytuł prasowy) jedynym dowodem są cztery screenshoty z systemu zarządzania maszynami wirtualnymi. Były też szumne zapowiedzi ujawnienia listy tajnych agentów Kremla… i na razie cisza. – *Wygląda na to,*

że prasa podchwytuje ogłoszenia Anonymous, ale nikt tego nie weryfikuje – mówił Łukasz Jachowicz.

Z 10 GB, których wykradzenie z Nestle ogłoszono, Anonymous udostępnili zaledwie pięciomegabajtowe archiwum plików z baz danych (zamówienia, hasła, płatności, przedsiębiorstwa) zawierające wyłącznie losowe dane testowe. Po analizie losowych dokumentów z dużego wycieku danych z banku centralnego Rosji okazało się, że dotyczą archiwalnych kursów walut albo publicznych sprawozdań finansowych różnych firm. Nagłośnione ataki na stacje telewizyjne okazały się atakami na lokalne sieci kablowe. Uczciwie trzeba jednak przyznać, że pojawiają się także poważniejsze wycieki, typu 360 tys. plików z Roskomnadzoru (1TB).

Anonymous kreatywnie walczą z blokadą informacyjną w Rosji. Podmiana stron internetowych wielu mediów rosyjskich pozwoliła na przekazywanie prawdziwych informacji o inwazji. Przeprogramowano kilkaset kamer w ten sposób, że po wejściu do monitoringu pojawiały się treści, ujawniające skalę zbrodni dokonywanych przez Rosjan w Ukrainie. Inny sposób to dopisywanie komentarzy i dodawanie zdjęć tego, co się dzieje w Ukrainie, do różnych rosyjskich miejscówek: restauracji, muzeów, Kremla. – *Skanuje się rosyjską przestrzeń IT w poszukiwaniu otwartych, dostępnych drukarek i na nich drukuje się biuletyny informacyjne o wojnie w Ukrainie. Podejrzewam, że ktoś wpadnie na pomysł, że można wykorzystać technologię Chromecast i wkrótce na rosyjskich telewizorach podłączonych do Internetu pojawią się filmy z Ukrainy. Niedawno pojawiła się strona anonymous.xyz, na której publikowana jest część leaków brandowanych Anonymous, to ciekawe udogodnienie, będę te wycieki badał* – zapowiadał Łukasz Jachowicz.

Mamy też do czynienia z informacjami przypisywanymi Anonymous, ale się pod nimi ktoś konkretny podpisuje, np. białoruscy cyberpartyzanci – grupa sabotująca rodzimy transport, która nie chce, żeby przesyłano sprzęt wojskowy.

– *Zgadzam się , że wiele akcji Anonymous jest nieco przereklamowanych, ale zdarzają im się na prawdę spektakularne sukcesy. Ataki strony rosyjskiej również nie są imponujące, spodziewałem się wielu ataków zero-day, przejmowania infrastruktury obu krajów, a tego na razie nie widać* – podsumował spotkanie Rafał Chruściel.

amk

Przydatne źródła informacji:

- https://cert.gov.ua/articles
- https://www.rapid7.com/blog/post/2022/03/04/russia-ukraine-cybersecurity-updates
- https://fakenews.pl/

Skąd się wzięli Anonymous?

– *Dziennikarze piszą o grupie lub kolektywie hakerskim, sami Anonymous przed laty używali pojęcia internet gathering. To losowo dobierane grupki, które skrzykują się w interesującej ich sprawie i brandują się jako marka Anonymous. Pierwszy ich projekt, Chanology, był wyrazem walki ze scjentologią. Stali się rozpoznawalni po samobójstwie nastolatka Mitchella Hendersona, który zastrzelił się po utracie swojego iPoda, zajmowali się trollerką* – wyjaśniał Łukasz Jachowicz.

Stosunkowo łatwo uzyskać informacje o Anonymous w Internecie, całkiem pokaźnej strony dorobili się w Wikipedii, tutaj zasygnalizujemy więc tylko ważniejsze etapy działań tej formacji. W 2010 r. Anonymous przeprowadzili skoordynowaną grupę ataków – operację payback – skierowaną przeciwko wrogom piractwa internetowego. Przeszła ona płynnie w walkę z każdym, kto się sprzeciwiał ideom promowanym przez Wikileaks (na Visę, Mastercard, PayPala, które odcięły finansowanie WikiLeaks, przypuszczono ataki DDoS). Aktywność Anonymous zahaczyła o Polskę, w 2012 r. podczas trwania dyskusji o porozumieniu ACTA strona premier.gov.pl została podmieniona.

Od samego początku Anonymous stosowali klasyczne metody działania: ataki DDoS, podmienianie stron internetowych, wycieki danych (przypadkowe lub celowe), złośliwe telefony, czarne bomby, google bomby. Kontaktowali się głównie za pomocą usługi IRC. Udostępnili gorzej przygotowanym użytkownikom specjalne programy do przeprowadzania ataków DDoS przeciwko wskazanym przez Anonymous celom (najsłynniejszy z nich to Low Orbital Ion Cannon). Motywacje, jakie im przyświecały, to: zabawa, walka z cenzurą, walka z egzekwowaniem praw autorskich, walka o wolność, walka z nazistami.

– *Na podstawie informacji uzyskanych z kanału #OpRedScare widać, że po agresji na Ukrainę towarzystwo dobrze się bawi. Co chwila pojawiają się meldunki o kolejnych unieruchomionych systemach z domeny .ru – albo uruchamiano bootnety atakujące strony, albo przygotowano strony internetowe z javascript, które atakowały te serwisy. Na udostępnionej przez Rosjan liście adresów IP, z których uruchamiano ataki, jest kilkaset statycznych adresów z Polski. Nie było to ze strony naszych aktywistów najmądrzejsze, Rosjanie już o tym wiedzą* – mówił Łukasz Jachowicz.