aut. Adam Lelonek 18.09.2017

„WOJNA CYBERNETYCZNA OSIĄGNĘŁA NOWE STADIUM” [WYWIAD]

„Aby lepiej rozumieć kto atakuje, trzeba oceniać działania poprzedzające atak i to, co dzieje się po nim. Patrząc na to, co stało się na Ukrainie, można powiedzieć, że to nie były ataki, tylko treningi. W przypadku realnego ataku cyberwojska atakują jakiś sektor państwa, infrastrukturę krytyczną, na przykład – elektrownie. Po tym na terytorium państwa wkraczają wojska konwencjonalne. Ale my widzimy tylko pierwszy etap operacji. To tylko trening” – mówił w rozmowie z CyberDefence24 podczas konferencji Security Case Study Oleksij Jasinski z ukraińskiej grupy Information Systems Security Partners.

CyberDefence24: Na portalu Wired pojawił się w czerwcu artykuł pt. „*How an entire nation became Russia's test lab for cyberwar*”, w którym autorzy mówią, że Ukraina jest poligonem dla cyberbroni. Dla kogo jest poligonem i co się testuje?

Oleksij Jasinski: Cyberprzestrzeń ma wiele podmiotów. Wolałbym uniknąć jednoznacznej odpowiedzi dla kogo jest to poligon i kto atakuje. Po pierwsze uczestników wydarzeń w sferze cyber jest wielu. Po drugie, aby oskarżać kogoś o coś trzeba mieć dowody. Mamy do czynienia z wojną cybernetyczną i wojną hybrydową. Od stawiania poważnych zarzutów są odpowiednie instytucje i organy państwowe. My pracujemy z dostarczonymi nam elementami danej sieci czy systemu komputerowego organizacji, które zostały zaatakowane jak patologowie. Nasze zdania to wyjaśnienie kiedy atak się wydarzył, w jaki sposób i jaka broń została do tego wykorzystana. Badanie motywów działania czy poszukiwanie sprawców to odpowiedzialność śledczych.

Mogę mówić o tym jaka broń jest wykorzystywana. Cyberbroń bardzo szybko przechodzi ewolucję. W 2014 r. mieliśmy pojedyncze, nieskoordynowane działania. Obecnie jeden tylko przypadek wirusa Petya mieścił w sobie szereg instrumentów wziętych z GitHub-u. To nie precyzyjnie zaprojektowana broń jak Stuxnet. W przypadku Petyi napompowano w jedną „kapsułę” bardzo wiele rozwiązań. Nie chodzi już o sam atak, ale i o motywy. Takie działania jasno wskazują, że chodzi o rozwój cyberoddziałów, cyberwojsk. To może być ktokolwiek.

Czytaj więcej: „Petya/NotPetya – analiza tajemniczego malware’u który zaatakował Ukrainę” (SCS 2017)

Jaki jest cel takiego trenowania?

Rozwój technologii, przygotowanie specjalistów, ale i pokazanie potencjalnym zleceniodawcom własnych możliwości i posiadanej cyberbroni. Taki jest rynek. Demonstruje się swój potencjał do przenikania do systemów, do ataku, do zakłócania procesów technologicznych czy komunikacyjnych czy wreszcie w obszarze inżynierii społecznej. Rynek cybernetyczny oddziałuje na każdy inny.

W materiałach, danych czy kodach, które otrzymujecie z zaatakowanych komputerów, nie ma żadnego dowodu sugerującego potencjalnego sprawcę?

Nie ma i nie będzie. Narzędzia wykorzystywane przez przestępców do cyberataków są jak nóż. To przyrząd powszechnie dostępny. Specjalnie broń brana jest z GitHubu. W kodzie mogą pojawiać się nawet hiszpańskie słowa, ale nie znaczy to, że Hiszpania atakuje Ukrainę. Cyberprzestrzeń różni się od świata realnego. W cyberbroni nie ma zawartej informacji do kogo ona należy. Wykorzystuje się narzędzia z sieci TOR, które zapewniają anonimowość. Na pocztę dowolnego użytkownika z praktycznie każdego kraju może przyjść wiadomość, dzięki której nieświadomy użytkownik, uczeń w szkole lub emeryt, stanie się częścią ataku. Za pomocą prywatnych komputerów można atakować inne komputery, nie tylko za granicą. Może być taka sytuacja, która z zewnątrz będzie wyglądać jakby dane państwo atakowało samo siebie. Innymi słowy każdy komputer na świecie może stać się narzędziem ataku. To jest jedna z form realizacji ekspansji cyberprzestrzeni.

Aby lepiej rozumieć kto atakuje, trzeba oceniać działania poprzedzające atak i to, co dzieje się po nim. Patrząc na to, co stało się na Ukrainie, można powiedzieć, że to nie były ataki, tylko treningi. W przypadku realnego ataku celem hakerów będzie chociażby infrastruktura krytyczna, na przykład – elektrownie. Po tym na terytorium państwa wkraczają wojska. Ale my widzimy tylko pierwszy etap operacji. To tylko trening.

Służba Bezpieczeństwa Ukrainy wprost oskarżyła Rosję o atak w przypadku Petya.

Czytałem o tym. W tym oświadczeniu brakowało dowodów technicznych. Eksperci muszą mówić o faktach. Nie mogę tego komentować, gdyż nie wiemy jakie materiały posiada SBU, które są tajne.

Czyli na razie my nie możemy nawet powiedzieć w takim razie czy w ogóle za podobne ataki odpowiadają podmioty państwowe czy prywatne?

Nie możemy. Warto pamiętać, że możliwe jest partnerstwo prywanto-publiczne. Prywatne podmioty mogą brać udział w szeregu procesów świadomie, ale i nieświadomie. Podobnie z pojedynczymi

użytkownikami. Kwestia ataków z tego roku to dwa lata przygotowań. To dokładnie zaplanowana operacja wojskowa, biorąc pod uwagę rozmach, cele, niszczenie informacji czy zacieranie śladów. Każdy z tych etapów bardzo trudno byłoby wykonać nie-ekspertom. Z drugiej strony, ekspert od przygotowania cyberbroni i ekspert, który wnika do systemu to dwie różne specjalności. Oczywiście można znaleźć fachowca, specjalizującego się w obu obszarach, ale kosztowałby on bardzo dużo. Państw nie stać, żeby utrzymać nawet dziesięciu takich ekspertów.

Mówi Pan, że przygotowania trwały aż dwa lata.

Tak, lata 2015-2016 były przygotowaniami. W roku 2017 doszło do eskalacji działań. To nie tylko Petya czy BlackEnergy, ale i szereg innych ataków. To szerokie spektrum działań.

Ilość ataków na Ukrainie świadczy o tym, że jest ona aż tak podatna na nie czy tak naprawdę każde państwo jest równie zagrożone? Problem leży w infrastrukturze Są braki infrastrukturalne czy braku woli politycznej?

Są dwie kategorie organizacji. Jedne rozumieją, że zostały zaatakowane, a inne nie. Ukraińska infrastruktura komputerowa korzysta z tych samych rozwiązań, które są stosowane na Zachodzie – te same systemy operacyjne, systemy procesów zautomatyzowanych, a jeszcze niektóre z nich są w ogóle przygotowywane na Ukrainie. Innymi słowy poligon ukraiński jest wygodną platformą, ponieważ po przygotowaniu broni i wytrenowaniu cyberwojska, można zwiększyć skalę operacji, ale i przenieść teatr działań w inne miejsce. Na razie to się jeszcze nie stało. Atakować np. Polskę to jednocześnie atakować Unię Europejską, natomiast atakować Ukrainę – to atakować jedno państwo. To dwa różne ataki. Podjęcie działań cybernetycznych w państwie UE można porównać do wypowiedzenia wojny całej Unii. To bardzo odważny krok, który wymaga od atakujących zaawansowanych przygotowań. Jeżeli taka wojna by się rozpoczęła, to doświadczenia ukraińskie zostałyby w niej wykorzystane. Warto pamiętać, że teraz atak nie polega na rozwaleniu drzwi. Atakuje się jakiś podrzędny element, z którego przechodzi się do innego podrzędnego elementu, a dopiero później rozpoczynają się działania. Nikt nie włamuje się dziś do banku. Łamie się konta jakiegoś podwykonawcy lub system, za pomocą którego klient dostaje się do niego. To powszechna praktyka współcześnie – przestępcy nie łamią obecnie systemów, ale wykorzystują ich słabe punkty. Przez konta użytkowników z dużymi przywilejami wewnątrz systemu można na spokojnie poznać całą infrastrukturę danej instytucji czy organizacji. Po cichu, bez przyciągania uwagi. Dlatego i tak trudno jest udowodnić obecność przestępcy w systemie. Co więcej, to że hakerzy nie zniszczyli jakiejś informacji lub nie doprowadzili do tragedii, nie oznacza, że nie ma ataku. Kiedy często przychodzimy do jakiejś firmy i badamy to, co się w niej dzieje, nierzadko są sytuacje, że jest nam bardzo trudno wyjaśnić kierownictwu, że niektóre operacje wykonane w systemie wcale nie były ich, tylko hakerów. Widziałem wiele przypadków, iż przestępcy przebywali tak długo w infrastrukturze danego systemu, że stali się jego częścią, współtworząc go. Dochodzi więc do tego, że coraz trudniej jest odróżnić działania hakera od działań administratora.

Innymi słowy nie ma Pana zdaniem mowy o większej podatności Ukrainy na cyberataki, większego braku świadomości zagrożenia wśród ukraińskich użytkowników sieci czy

jakichś innych problemach całego sektora.

Mam taki kurs dla studentów, w którym daje taki scenariusz: są dwa okna – jedno jest okratowane, a drugie nie. Przez które z nich łatwiej się włamać złodziejowi. Wszyscy zawsze odpowiadają, że przez to drugie, ale prawidłowa odpowiedź jest inna. Jeżeli złodziej będzie zmuszony włamywać się przez okratowane okno, to to zrobi. Po prostu weźmie ze sobą narzędzia, które mu to umożliwią. Nieważne ile będzie się pracować z ludźmi na odcinku zabezpieczeń. Jeżeli będzie 5 tys. użytkowników, zawsze znajdzie się jeden, który przyniesie ze sobą pendrive'a, zawsze znajdzie się inny, który podłączy do swojego komputera telefon i stworzy most do Internetu, omijając sieć Wi-Fi, zawsze znajdzie się administrator, który jak zachoruje, zrobi połączenie z systemem z domu. To wszystko powoduje, że cały system zabezpieczeń przypomina ser szwajcarski. Widziałem wiele dobrze zabezpieczonych infrastruktur czy systemów, bardzo dobrze, a nawet całych izolowanych od sieci systemów. Ale kiedy konieczne jest chociażby zrobić backup 4 TB takich izolowanych danych, wystarczy zrobić połączenie na 30min i to wystarczy dla hakerów, będących już w infrastrukturze, aby przeniknąć do chronionych obszarów. Dostarczą oni zautomatyzowany zestaw skryptów, który przez pół roku może przykładowo zniszczyć określone informacje.

Cyberprzestrzeń różni się od rzeczywistości. Obserwując realny budynek widzimy gdzie są punkty wejścia, drzwi, okna, kanały wentylacyjne. W cyberprzestrzeni drzwi mogą pojawić się na środku ściany. Ta luka może być, lecz użytkownik nie musi być jej świadomy. Nie mówiąc o tym, że gdyby ktoś zdobył dostęp do narzędzi NSA [Agencji Bezpieczeństwa Narodowego USA – przyp. red] i w jednej chwili 50 lub 80% komputerów świata pozostaje bez ochrony. Dzięki wrażliwości systemów mogą przenikać narzędzia niszczące 10 tys. wybranych plików w 3 minuty. Nie pomagają na to ani programy antywirusowe, firewalle czy eksperci od cyberbezpieczeństwa. Wystarczy jeden słaby punkt.

Jakie wnioski może wyciągnąć Zachód z ukraińskich doświadczeń?

Najważniejsze to rozwijanie świadomości zagrożenia wśród użytkowników końcowych. Dalej trzeba analizować konkretne sytuacje, które są właśnie omawiane na Security Case Study. Ludzie uważają, że wirusy, zagrożenia czy sfera cyber jest gdzieś daleko. Tak jednak nie jest. Cyberprzestrzeń jest wszędzie. Jeżeli nauczę się czyichś zachowań np. na Facebooku, że ktoś klika „lubię to" pod postami chociażby o łowieniu ryb, będę w stanie spersonalizować atak. Będę wiedział jak zdobyć czyjeś zainteresowanie, co podesłać, co potencjalnie użytkownik będzie chętny otworzyć. Czasem wymaga to jakiegoś zaangażowania czasowego, zdobycia zaufania. Ale czasem wystarczy wiedzieć, że ktoś oczekuje na konkretnego maila. Metody z obszaru inżynierii społecznej działają zawsze i jest w 100% skuteczna. Kolejną rzeczą jest monitoring aktywności w cyberprzestrzeni. Należy śledzić zmiany, nowe technologie, nowe trendy. Dalej konieczne jest badanie i wzmacnianie własnej infrastruktury.

Jako ciekawostka, **dla różnych firm testujemy ich zabezpieczenia. W ciągu dwóch tygodni jesteśmy w stanie prawidłowo rozpoznać pomiędzy 20 a 80% haseł, które pozwalają nam na dostanie się do systemu. Tutaj nie są winni ludzie.** Tak naprawdę trudno jest wymyśleć sobie dobrze zabezpieczone hasło, którym można łatwo się posługiwać – albo zostaje ono zapisane

gdzieś ręcznie, albo pozostaje na komputerze, co mogą wykraść hakerzy. Kupienie antywirusa czy posiadanie firewalla nie zwalnia już nikogo z obowiązku dbania o własne bezpieczeństwo. Nad nim trzeba wciąż pracować. Każdy użytkownik musi pozostawać pod jakąś kontrolą. Trzeba dokładnie śledzić wszelkie anomalie i szybko na nie reagować.

Czy na Ukrainie odnotowane zostały jakieś dodatkowe działania z obszaru cyber w związku z rosyjsko-białoruskimi manewrami Zapad 2017?

Nie. W mojej ocenie fakt manewrów niewiele zmienia. Czy to Rosja czy inne potencjalnie zainteresowane tym podmioty prowadzą swoje działania w sposób ciągły. A **ponieważ Ukraina jest poligonem, to nie ma sensu go niszczyć**. Nikt nie będzie wysadzał ładunków wybuchowych na poligonie dla snajperów. Wrogie działania prowadzone są na tyle ostrożnie, aby trwale nie uszkodzić infrastruktury, która pozwala na działania. Dochodzi się do jakiejś granicy, pokazuje się na zewnątrz własne możliwości i wycofuje się. Nie przekracza się punktu, w którym przedsiębiorstwa i właściciele danej infrastruktury podjęliby decyzję o daleko idących zmianach, bo zmieni to środowisko, w którym chce się działać i które się zna.

Jak Pan, jako ekspert od IT, ocenia działania propagandowe i dezinformacyjne w mediach społecznościowych, a zwłaszcza aktywizację zautomatyzowanych kont i tzw. botnetów?

To element szerokiego instrumentarium z obszaru działań hybrydowych. Wykorzystanie go można datować na Ukrainie od co najmniej 2014 r., kiedy miało miejsce włamanie na stronę Centralnej Komisji Wyborczej i rozpoczęto manipulacje wynikami. Cała sytuacja trwała niecałe 10 minut, sytuacja szybko została opanowana, niemniej jednak rosyjskie media długo po tym relacjonowały to wydarzenie jako aktualne i prawdziwe. Wojna informacyjna jest coraz bardziej zaawansowana. Wcześniej poszczególne procesy mogły trwać miesiącami, teraz daje się je skracać do kilku minut. Trzeba pamiętać, że technologie oddziaływania i manipulacji w przestrzeni informacyjnej pojawiły się znacznie, znacznie wcześniej niż media społecznościowe i Internet. Testy psychologiczne i treningi odbywały się znacznie dłużej niż obecne aktywności hakerów, dzięki którym zdobywają nowe umiejętności. Cała ta wiedza jest dziś adaptowana w praktyce z wykorzystaniem współczesnych technologii i możliwości. Wpływać na punkt widzenia tysięcy osób jest dziś bardzo łatwo. Wystarczy zrobić jakąś akcję, która skoordynowana zostanie z klasycznymi mediami. Wywołanie paniki czy zbudowanie napięcia w relacjach międzynarodowych to tylko jedne z przykładów. **Uważam, że wykorzystanie broni informacyjnej i mediów społecznościowych może być obecnie znacznie poważniejszym zagrożeniem niż cyberwojna.** W obszarze technologicznym pewne rzeczy mogą zadziałać inaczej lub nie zadziałać zgodnie z planem, w przypadku oddziaływania na opinię publiczną jest znacznie łatwiej prognozować i realizować skuteczne operacje.

Czy widzi Pan przestrzeń do współpracy polsko-ukraińskiej w sferze cyber? Co Ukraina mogłaby zaoferować swoim zachodnim partnerom?

Po pierwsze wymiana wiedzy na temat konkretnych przypadków, ataków. Wspólne omawianie ich modelu, schematów działań sprzed i po zajściu wzmacnia odporność cybernetyczną państw. Druga kwestia jest związana z większą skalą. Atakujących nazywam potocznie „ciemną stroną", oni już zbudowali rynek, zjednoczyli się. Natomiast „biała strona", czy to na płaszczyźnie szeregowych użytkowników, instytucjonalnym czy państwowym nie. Łączenie sił, czy to między przedsiębiorstwami, czy na poziomie państwowym czy międzypaństwowym, powinno stać się priorytetem. Ludzie powinni rozumieć, że są atakujący i są oni. Nie jest tak, że są pewne grupy użytkowników ze swoimi problemami. Nie. Wszyscy jesteśmy z tymi samymi problemami. W przypadku wojny konwencjonalnej, gdyby doszło do ataku na jakieś państwo, inne mogą mu pomóc. Cyberprzestrzeń ma inne reguły. Wtargnięcie w cyberprzestrzeń danego państwa nie musi nawet zostać zauważone. Dlatego tym ważniejsze jest łączenie sił i wymiana informacjami. To w ogóle pierwszy krok współpracy.

Wreszcie mamy też obszar technologiczny. Powinny zostać ustanowione kanały, które powinny umożliwiać wymianę *know how*, sposobów edukacji czy przygotowania specjalistów. Ukraina znajduje się w wyjątkowej sytuacji. Różnego rodzaju nowe rozwiązania, programy czy narzędzia, w bardzo krótkim czasie są praktycznie wykorzystywane, zwłaszcza do ataków. Zwiększenie świadomości i zdobywanie praktycznej wiedzy pozwala zaadoptować tą wiedzę na różnych płaszczyznach. Mamy też wciąż bardzo niewielką liczbę ekspertów. Ci, którzy zajmują się atakami, mają łatwiej. Rzucić cybernetyczny granat jest prostą czynnością. Natomiast obronić się przed nim jest już wyzwaniem, biorąc pod uwagę liczbę wektorów potencjalnych możliwości i celów.

Aby budować koncepcję obrony, trzeba przyswoić bardzo wiele nawyków. Pewnie **jest wiele naszych własnych zasobów, których państwa nie potrafią jeszcze wykorzystywać. Potrzebujemy strategii, podnoszenia liczby i kwalifikacji ekspertów, ale i ich organizacji. W pewnych sytuacjach wymaga to tworzenia określonych formacji.** Atakujący trenują i to każdego dnia. Ci, którzy mają bronić, są po prostu ekspertami w swoich obszarach. Mogą nawet nie wiedzieć, że są potrzebni. To trzeba zmienić. Wydarzenia takie jak Security Case Study pokazują jak może to być robione i jak bardzo jest to potrzebne. Wojna cybernetyczna osiągnęła nowe stadium. **To nie jest już zbiór przypadkowych, ograniczonych działań, ale doskonale zaplanowane i długofalowe operacje.**

Rozmawiali dr Adam Lelonek i dr Andrzej Kozłowski