FOT. SHUTTERSTOCK

Wojciech Wybranowski

W lipcu i sierpniu doszło do 117 ataków cyberterrorystycznych na wojskowe sieci teleinformatyczne w Polsce – dowiedział się tygodnik „Do Rzeczy". Eksperci przyznają, że mają pochodzące z Rosji sygnały o regularnym skanowaniu polskiego Internetu

Ta wojna już trwa

Czwartkowe popołudnie. Wirtualna mapa na stronach firmy Norse, utworzonej przez byłych funkcjonariuszy amerykańskiego Departamentu Bezpieczeństwa Wewnętrznego, rejestrująca w czasie rzeczywistym dokonywane każdego dnia wykryte ataki hakerskie. Z udostępnionych tam danych wynika, że co najmniej 26 osób lub instytucji w Polsce, w różnych miastach, właśnie stało się przedmiotem cyberataków, prowadzonych przez hakerów między innymi z terenu Chin, Białorusi, Niemiec i Rosji. Podobna sytuacja, w mniejszym lub większym stopniu, powtarza się kilka razy na dobę.

Najczęściej za tego rodzaju atakami stoją młodzi ludzie próbujący pozyskać – często dla udowodnienia swoich umiejętności – strzeżone dane z sieci komputerowych. Tak mogło być w przypadku osoby ukrywającej się pod pseudonimem tviskit, która w minionym tygodniu na rosyjskim forum Bitcoin Security opublikowała około 5 mln wykradzionych haseł i loginów do kont pocztowych Gmail.

Eksperci zajmujący się polskim bezpieczeństwem cybernetycznym mówią jednak „Do Rzeczy", że w ostatnim czasie mocno nasiliło się zainteresowanie Polską ze strony rosyjskich hakerów, a za częścią ataków stoją rosyjskie służby specjalne.

– Rozpoznawanie przez stronę rosyjską, czy rosyjskich hakerów powiązanych ze służbami, możliwości przeprowadzenia ataków cyberterrorystycznych również na Polskę trwa cały czas – uważa Mirosław Maj, ekspert Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji oraz prezes fundacji Bezpieczna Cyberprzestrzeń.

Jednak na skanowaniu sieci internetowej w poszukiwaniu słabych punktów w zabezpieczeniu teleinformatycznym instytucji stanowiących tzw. infrastrukturę krytyczną (m.in. energetyka, łączność, finanse, zaopatrzenie w żywność, wodociągi, instytucje ratownicze i transport) się nie kończy.

ATAK NA WOJSKO

Jak dowiedział się tygodnik „Do Rzeczy", tylko w ostatnich dwóch miesiącach doszło do wielu ataków na wojskowe sieci teleinformatyczne. Zostały wykryte i zablokowane przez zespół MIL-CERT, czyli specjalną komórkę funkcjonującą w ramach Systemu Reagowania na Incydenty Komputerowe w Ministerstwie Obrony Narodowej, odpowiedzialnego za bezpieczeństwo wojskowych systemów teleinformatycznych.

– W lipcu i sierpniu 2014 r. wykryto i zareagowano na 117 incydentów w sieciach wojskowych z dostępem do Internetu – poinformował nas płk Jacek Sońta, rzecznik prasowy MON.

Z danych, jakimi dysponuje resort, wynika, że ataki hakerskie na polskie wojsko znacznie nasiliły się po wybuchu konfliktu za naszą wschodnią granicą.

– Odnotowaliśmy istotny wzrost, o blisko 70 proc. w stosunku do analogicznego okresu roku ubiegłego (70 przypadków). Incydenty spowodowane były przez oprogramowanie złośliwe, botnety oraz ataki ukierunkowane, w tym również z obszarów rosyjskojęzycznych – dodaje płk Sońta.

Wszyscy eksperci, tak z wojska, jak i z ABW, z którymi rozmawialiśmy, starannie unikają jednoznacznego stwierdzenia, że za część ataków odpowiadają rosyjscy hakerzy. Termin „obszar rosyjskojęzyczny" brzmi neutralnie i politycznie bezpiecznie. Nieoficjalnie jeden z naszych rozmówców, funkcjonariusz służb odpowiedzialnych za „bezpieczeństwo cyberprzestrzeni RP", mówi, że część ataków prowadzona była z terenu Rosji i republik pozostających w obszarze jej wpływów. Zwraca też uwagę na rodzaj ataków, jakim poddane były wojskowe sieci teleinformatyczne.

A to istotne. Ataki ukierunkowane i botnety to abecadło cyberterroryzmu.

Te pierwsze przeprowadzane są zwykle poprzez zawierające złośliwe oprogramowanie załączniki poczty elektronicznej, których otwarcie skutkuje instalacją w systemie oprogramowania typu „koń trojański". Istotą ataku jest indywidualny charakter przesłanej wiadomości, udającej na przykład korespondencję służbową.

– Ofiara otrzymuje e-mail od osoby podszywającej się na przykład pod jego dowódcę z informacją, że w załączniku znajdują się dokumenty, które należy niezwłocznie wypełnić i odesłać. Po kliknięciu w załącznik uruchamia się szpiegowskie oprogramowanie, które służy do zbierania i transferowania poza daną instytucję informacji oraz dokumentów znalezionych na dyskach twardych lub w zasobach sieciowych ofiary – tłumaczy nasz rozmówca.

Z kolei botnet to zespół komputerów-zombie, zainfekowanych wcześniej przez specjalnego wirusa pozwalającego hakerowi na zdalne przejęcie kontroli nad nimi. A to daje mu możliwość przeprowadzenia przy użyciu „przejętych" komputerów dalszych ataków, np. sabotażu czy ataków typu DDoS (generowanie sztucznego ruchu).

ROSJANIE SKANUJĄ POLSKĘ

Na celowniku rosyjskich hakerów znalazły się też organy administracji państwowej w Polsce i cywilne firmy z branży infrastruktury krytycznej. Za ich ochronę przed cyberterroryzmem odpowiada z kolei Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL, funkcjonujący w ramach Agencji Bezpieczeństwa Wewnętrznego. Agencja nie chce jednak ujawnić, ile takich ataków było i czy stali za nimi Rosjanie.

– Liczba zgłaszanych incydentów wskazuje, że na pewno zagrożenia są, bo one są na całym świecie. Naszą rolą nie jest straszenie, ale ostrzeganie, informowanie i zapobieganie zagrożeniom związanym z cyberterroryzmem. Reagowanie na ataki i udzielanie pomocy – ucina ppłk Maciej Karczyński, rzecznik ABW.

Eksperci CERT.GOV.PL, którzy zgodzili się porozmawiać z naszym tygodnikiem (wolą pozostać anonimowi), ujawniają nieco więcej szczegółów. – Mamy oczywiście informacje, że trwa skanowanie polskiej sieci, że ten ruch sieciowy generowany jest w Rosji, ale nie można jednoznacznie stwierdzić, czy to Rosja jest państwem atakującym, czy służy tylko jako pewnego rodzaju „bramka wyjściowa" – mówi jeden z ekspertów.

Wiadomo, że co najmniej jeden cyberterrorystyczny atak, za którym stali – jak wszystko wskazuje – Rosjanie, dosięgnął również Polski. W lipcu brytyjski „Financial Times" ujawnił, że systemy kontrolne setek światowych – w tym również polskich i amerykańskich – firm z branży energetycznej zostały zaatakowane przez rosyjskich hakerów z grupy Dragonfly, kojarzonej z rosyjskimi służbami specjalnymi. Udało im się umieścić na komputerach w zaatakowanych firmach groźnego wirusa. Cyberterroryści przeprowadzili około tysiąca ataków: 24 proc. z nich przypadło na Stany Zjednoczone, 5 proc. dotknęło polskie firmy. Rządowy zespół CERT.GOV.PL alarmował wówczas: „Skuteczna infekcja zarówno umożliwia dostęp do sieci danej instytucji, jak i stwarza dodatkowo możliwość nieuprawnionego, zdalnego sterowania instalacjami przemysłowymi ze stanowiska przejętego przez cyberprzestępców".

Ofiara otrzymuje e-mail od osoby podszywającej się pod jej dowódcę z informacją, że w załączniku znajdują się ważne dokumenty. Po kliknięciu uruchamia się szpiegowskie oprogramowanie

– Dużo wskazuje na to, że było to bardziej „rozpoznanie terenu" i zabezpieczeń niż akt realnego sabotażu. Terroryści uzyskali jednak takie poziomy dostępu i możliwości manipulacji, że to się mogło skończyć bardzo poważnie – ocenia Mirosław Maj, prezes fundacji Bezpieczna Cyberprzestrzeń. Jego zdaniem ta sprawa to jeden z dowodów na to, że zagrożenie Polski atakiem cyberterrorystycznym jest bardzo realne.

– Coraz częstszym rodzajem ataków jest podmiana informacji na stronach WWW. Dzieje się to jednak na witrynach słabo zabezpieczonych. W Polsce były ataki na stronę prezydenta RP i Giełdy Papierów Wartościowych, do których przyznała się grupa CyberBerkut – dodaje Maj.

Chodzi o zdarzenie z sierpnia, kiedy to atak DDoS-owy unieruchomił wspomniane strony. Grupa hakerów CyberBerkutu, powiązana z prorosyjskimi separatystami (to oni zablokowali jesienią telefony ukraińskich polityków), w wydanym oświadczeniu napisała, że żąda „zaprzestania ślepego wspierania faszystowskiej władzy na Ukrainie".

POLSKA SIĘ OBRONI?

W 2012 r., kiedy przy okazji protestów przeciw podpisaniu ACTA doszło do masowych, acz bardzo prostych ataków DDoS-owych na strony instytucji rządowych, Polska okazała się bezradna. Dziś, dwa lata później, jest już znacznie lepiej. W tym roku w życie wszedł Narodowy Program Ochrony Infrastruktury Krytycznej, przygotowany przez Rządowe Centrum Bezpieczeństwa, określający między innymi zakres zadań w kwestii ochrony infrastruktury krytycznej.

Wzrasta też poziom świadomości i odpowiedzialności operatorów internetowych. W 2013 r. do CERT.GOV.PL przesłano aż 8817 zgłoszeń o podejrzeniu zagrożeń (gwałtowny wzrost nastąpił w drugiej połowie roku), a aż 5670 z nich zostało zakwalifikowanych jako incydenty. Eksperci z rządowego zespołu szacują, że w tym roku ta liczba będzie znacznie większa.

– Nie wszystkie takie zgłoszenia są rzeczywiście atakami. Dobrze natomiast, że ludzie stali się bardziej ostrożni, bo jeśli chodzi o realne zagrożenie, to nie liczba ataków się liczy, ale ich jakość. W zapobieganiu najważniejsza jest szybkość reakcji – mówi nasz informator z CERT.GOV.PL.

W tym roku polscy specjaliści, m.in. z MIL.CERT, SKW, CERT.GOV, WAT oraz CERT Polska, wygrali międzynarodowe zawody Locked Shields 2014 w zakresie ochrony cyberprzestrzeni. To prestiżowe ćwiczenia bazujące na fikcyjnym scenariuszu, organizowane przez NATO Cooperative Cyber Defence Centre of Excellence. Polacy wygrali też drugie ćwiczenia, z zakresu ochrony informacji, organizowane przez agencję ENISA.

Ekspert Mirosław Maj ocenia, że Polska ma superspecjalistów i bardzo duży potencjał, by skutecznie bronić naszego kraju przed na przykład rosyjskim cyberatakiem. – Co do jednego jestem nadal krytyczny. Mimo tych różnych starań nie ma spójności całego systemu, poukładania w sposób strategiczny wszystkich działań – podkreśla Maj. – Czy jesteśmy w stanie się skutecznie bronić w przypadku cyberataku ze strony państwa ościennego, np. Rosji? Bronić – na pewno. Jednak to, na ile skutecznie, zależy od rodzaju ataku – mówi ppłk Maciej Karczyński z ABW. •