Kraj

POŻEGNANIE Z DONALDEM

Powiedzieć, że podczas siedmiu lat rządów Tusk całkowicie zmienił sposób uprawiania polityki w Polsce, to nic nie powiedzieć →A7

rp.pl/kraj

Hakerzy Putina atakują rząd

INTERNET | Związani z Kremlem cyberszpiedzy wzięli na cel m.in. MON. Zagrożone jest też bezpieczeństwo sektora finansowego.

WIKTOR FERFECKI

APT28 – taki pseudonim hakerom, najprawdopodobniej związanym z rosyjskim rządem, nadała firma FireEye zajmująca się bezpieczeństwem w sieci. W ubiegłym tygodniu opublikowała raport, z którego wynika, że jednym z celów grupy były polskie instytucje.

Zdaniem FireEye APT28 działa co najmniej od 2007 roku. – Nie mamy wprost dowodów na udział rządu rosyjskiego w atakach APT28, ale wszystkie poszlaki wskazują na Moskwę – mówi Robert Żelazo, dyrektor regionalny FireEye na Europę Wschodnią.

Jakie? Eksperci FireEye wywodzą, że 89 proc. złośliwego oprogramowania grupa tworzy między 8 a 18 czasu obowiązującego w Moskwie i Petersburgu, a w kodzie oprogramowania znajdują się szczątkowe rosyjskie komentarze. Jednak najważniejszą poszlaką są cele ataków. Zdaniem FireEye grupa nie działa dla zysku, lecz w celach politycznych, i uderza w kraje wrogo nastawione do Moskwy.

Przykładowo, w połowie 2013 roku APT28 zaatakowała gruzińskie MSW. Hakerzy wysłali urzędnikom e-maila z tzw. przynętą, czyli załączonym plikiem z listą numerów gruzińskich praw jazdy. Po jego otwarciu na komputerze instalowało się złośliwe oprogramowanie mające wykradać informacje.

Podobną taktykę hakerzy zastosowali w odniesieniu do gruzińskiego MON i próbowali inwigilować dziennikarzy z tego kraju. Celem APT28 były też organizacje międzynarodowe, w tym NATO i Komisja Europejska, oraz organizatorzy dużych targów zbrojeniowych.

– Ataki były skierowane na ściśle określone cele. Świadczą o tym doskonale przygotowane e-maile zachęcające do otwarcia załącznika ze złośliwym kodem. Znajdowały się w nich m.in. nazwiska i numery telefonów pracowników NATO, a opracowanie takich „przynęt" wymagało dużych nakładów pracy – relacjonuje Robert Żelazo.

Z raportu FireEye wynika, że Polskę hakerzy zaatakowali w sierpniu 2014 roku. O tym, że do instytucji rządowych trafił wówczas e-mail zawierający złośliwe oprogramowanie, informowała już wcześniej polska firma Prevenity. FireEye powiązała ten atak z działalnością APT28.

> Zdaniem FireEye, inwigilując dziennikarzy w Gruzji, rosyjscy hakerzy próbowali wpływać na opinię publiczną

E-maile zawierały załącznik z informacją na temat katastrofy malezyjskiego samolotu nad Ukrainą, którego otwarcie skutkowało instalacją złośliwego oprogramowania. – Odkryliśmy atak, analizując zagrożenia w ramach umowy z instytucjami rządowymi – mówi Mariusz Burdach z Prevenity.

Jego zdaniem atak nie był skuteczny. Jednak rosyjscy hakerzy próbowali też w inny sposób włamać się do polskich instytucji. Założyli fałszywe domeny, do złudzenia przypominające adresy należące m.in. do MON. – Z tych domen mogły być wysyłane wiadomości w celu zmylenia adresata i skłonienia go do otwarcia załącznika – wyjaśnia Burdach.

Czy hakerom udała się inwigilacja rządowych komputerów? ABW odmówiło nam odpowiedzi na to pytanie.

– APT28 przeprowadzała bardzo zaawansowane technologicznie ataki – mówi tymczasem Robert Żelazo.

Jednak zdaniem ekspertów od bezpieczeństwa działalność tej grupy to tylko wierzchołek góry lodowej.

– Niestety, jest coraz więcej sygnałów świadczących o tym, że staliśmy się bezpośrednim obszarem zainteresowań cyberprzestępców – zauważa Mirosław Maj z Fundacji Bezpieczna Cyberprzestrzeń.

Latem o atakach grupy Dragonfly m.in. na polskie firmy z sektora energetycznego informowała firma Symantec.

Z kolei w połowie października firma iSight ostrzegła, że rosyjscy hakerzy znani jako SandWorm wykorzystywali lukę w systemie Windows do szpiegowania polskiej firmy energetycznej. O wymierzonej w nasz kraj działalności hakerów, prawdopodobnie również rosyjskich, doniosła też przed dwoma tygodniami firma Trend Micro.

– Jeszcze kilka lat w podobnych raportach o Polsce pisało się incydentalnie – mówi Mirosław Maj. – Powodem zmiany sytuacji jest nasze zaangażowanie na Ukrainie.

Zdaniem ekspertów rząd powinien wzmacniać ochronę przed cyberszpiegami, ale powody do niepokoju mają też firmy z sektora finansowego.

We wtorek pisaliśmy w „Rzeczpospolitej", że Komisja Nadzoru Finansowego ostrzega banki i instytucje finansowe przed wzmożonymi atakami hakerów. Nie podała wówczas daty. Już wiadomo, że mają one nastąpić w środę 5 listopada. Hakerzy chcą złamać zabezpieczenia stron internetowych banków, by wprowadzić na nich nieautoryzowane zmiany.