Cyberdefence 24

aut. Szymon Palczewski 16.11.2020

PRODUCENCI SZCZEPIONEK NA COVID-19 WSPÓLNYM CELEM ROSJI I KOREI PÓŁNOCNEJ

Rosyjscy i północnokoreański hakerzy przeprowadzili cyberataki wymierzone w placówki medyczne oraz prywatne firmy zajmujące się badaniami oraz produkcją szczepionek na koronawirusa. Część wrogich operacji jest kontynuowanych pomimo wykrycia. W kampanie zaangażowani byli m.in. hakerzy rosyjskiego wywiadu.

Specjaliści Microsoft w ostatnich miesiącach odkryli cyberataki ze strony trzech podmiotów państwowych (z Rosji oraz dwóch z Korei Północnej), które były wymierzone w siedem czołowych firm bezpośrednio zaangażowanych w badania nad szczepionkami i lekami na COVID-19 – wskazał koncern w oficjalnym komunikacie.

Microsoft podkreślił, że wśród konkretnych celów prowadzonych operacji znajdują się przedsiębiorstwa farmaceutyczne oraz instytucje badawcze z Kanady, Francji, Indii, Korei Południowej i Stanów Zjednoczonych. Kto był autorem cyberataków? Zdaniem specjalistów grupa hakerów rosyjskiego wywiadu Cozy Bear oraz dwa podmioty z Korei Północnej – „Lazarus Group" i „Cerium".

Cyberataki wymierzone były przede wszystkim w producentów szczepionek. Część z nich opracowuje również test na koronawirusa. Wiele poszkodowanych placówek posiada umowy z agencjami rządowymi z różnych państw, a także regularnie inwestuje w rozwój badań nad COVID-19. Microsoft nie podał jednak konkretnych nazw firm oraz instytucji, które były celem działań hakerów.

> *Dwa globalne problemy mogą ukształtować współczesną historię: COVID-19 i coraz częstsze wykorzystywanie internetu przez złośliwych aktorów do zakłócania życia społecznego. Niepokojące jest to, że zagrożenia te połączyły się – cyberataki są wykorzystywane do zakłócania działań instytucji opieki zdrowotnej walczących z pandemią. Uważamy, że tego typu działania powinny być potępione przez całe cywilizowane społeczeństwo*
>
> *Oficjalne stanowisko Microsoft.*

Według specjalistów koncernu grupa Fancy Bear nadal prowadzi działania, aby wykradać dane logowania. Są to ataki, których celem jest włamanie się na konta użytkowników przy użyciu tysięcy lub milionów „szybkich prób".

Z kolei Zinc używało głównie spear-phishing do kradzieży danych uwierzytelniających, wysyłając do ofiar wiadomości ze sfałszowanymi ofertami stanowisk, podszywając się pod rekruterów lub pracodawców (północnokoreańscy hakerzy od dłuższego czasu wykorzystują tą metodę podczas operacji – więcej tutaj).

Druga z północnokoreańskich grup Cerium również posługiwała się spear-phishingiem, lecz treść zainfekowanych wiadomości odnosiła się do pandemii koronawirusa. Hakerzy podszywali się pod przedstawicieli Światowej Organizacji Zdrowia, aby wzbudzić zaufanie ofiar.

Microsoft wskazał, że część cyberataków została skutecznie zablokowana, a podmiotom, które zostały naruszone zaoferowano specjalistyczną pomoc. Koncern dodatkowo powiadomił wszystkie organizacje będące celem działalności hakerów.

Amerykański koncern postanowił również zaangażować się w debatę na szczeblu państw, wskazując na konieczność bezwzględnej ochrony placówek opieki zdrowotnej i podjęcie konkretnych działań mających na celu egzekwowanie obowiązującego prawa międzynarodowego.

> *Uważamy, że prawo powinno być egzekwowane nie tylko w przypadku ataków przeprowadzanych przez podmioty rządowe, ale także w przypadku, gdy są realizowane przez grupy przestępcze, które rządy wspierają w ich granicach. Jest to działalność przestępcza, której nie można tolerować*
>
> *Brzmi stanowisko Microsoftu.*

Cyberataki na sektor ochrony zdrowia nasiliły się wraz z wybuchem pandemii COVID-19, co potwierdza m.in. raport Europolu. Głównym narzędziem w rękach hakerów jest oprogramowanie ransomware, które jest szczególnie niebezpieczne z perspektywy zdrowia i życia pacjentów. Hakerzy są świadomi jak istotne są placówki medyczne w czasie pandemii i że nie mogą sobie one pozwolić na zakłócenie działalności, dlatego też kierują tam swoje operacje z myślą np. o chęci uzyskania zysku lub rozgłosu.

Czytaj też: Szpitale bez dostępu do sieci. Cyberatak paraliżuje kolejne placówki medyczne