aut. Szymon Palczewski 17.07.2020

ROSYJSKI WYWIAD POLUJE NA SZCZEPIONKĘ PRZECIWKO COVID-19

Rosyjscy hakerzy działający na zlecenie wywiadu prowadzą złośliwą kampanię wymierzoną w instytucje i organizacje Stanów Zjednoczonych, Wielkiej Brytanii i Kanady, które pracują nad stworzeniem szczepionki na Covid-19. W ten sposób Moskwa chce poznać tajemnice pandemii koronawirusa i wykraść dane na temat potencjalnego leku.

W 2020 roku grupa hakerska APT29 (znana również jako „Dukes" lub „Cozy Bear"), działająca na zlecenie rosyjskiego wywiadu, odpowiada za złośliwą kampanię wymierzoną w organizacje zaangażowane w opracowanie szczepionek na koronawirusa w Kanadzie, Stanach Zjednoczonych i Wielkiej Brytanii.

„Jest wysoce prawdopodobne, że zamiarem hakerów jest kradzież informacji i własności intelektualnej związanej z opracowywaniem i testowaniem szczepionek Covid-19" – czytamy w oficjalnym raporcie brytyjskiego National Cyber Security Centre (NCSC).

Jak wskazują eksperci, APT29 wykorzystuje niestandardowe złośliwe oprogramowanie znane jako „WellMess" i „WellMail". Grupa często używa publicznie dostępnych exploitów w celu przeprowadzenia szeroko zakrojonego skanowania, a następnie posłużenia się podatnymi systemami, aby w ten sposób uzyskać dostęp do konkretnych sieci. Dzięki temu hakerzy są w stanie prowadzić globalną kampanię, co w przyszłości może przynieść znaczne korzyści wywiadowcze.

Jedną z metod działania, jaką zidentyfikowali specjaliści NCSC jest spearphishing. Hakerzy wykorzystują ją w celu uzyskania poświadczeń uwierzytelnienia na stronach logowania starannie wybranych organizacji. Następnie grupa dąży do utrzymania stałego dostępu w sieciach ofiary – wynika z raportu.

„W niektórych przypadkach APT29 wdraża również niestandardowe złośliwe oprogramowanie znane jako WellMess lub WellMail w celu przeprowadzenia dalszych operacji w systemie ofiary" – tłumaczą eksperci.

WellMess to złośliwe oprogramowanie napisane w Golang lub .NET i jest używane od co najmniej dwóch lat. Po raz pierwszy zostało zidentyfikowane w lipcu 2018 roku. Wirusa zaprojektowano do wykonywania zdalnych działań, przesyłania i pobierania plików na zewnętrzne urządzenia. Z kolei WellMail to oprogramowanie służące do uruchamiania poleceń oraz skryptów, których wyniki są wysyłane na specjalnie zakodowany serwer – wynika z raportu NCSC.

„Grupa APT29 prawdopodobnie nadal będzie atakowała organizacje zaangażowane w badania i rozwój szczepionek na COVID-19" – podkreślają specjaliści. Jak dodają, taki stan rzeczy wynika z chęci gromadzenia danych wywiadowczych na temat pandemii.