Cyberdefence 24

aut. Szymon Palczewski 15.07.2020

BACKDOORY W PAŃSTWOWYM OPROGRAMOWANIU. CHIŃSKI SPOSÓB PRZEŚWIETLANIA KONTRAHENTÓW

W chińskim oprogramowaniu służącym między innymi do uiszczania podatków VAT znajdowały się backdoory umożliwiające gromadzenie danych wywiadowczych.

Jeden z chińskich banków zwrócił się do brytyjskiego kontrahenta ds. obrony, wskazując, że rząd Państwa Środka wymaga od firm korzystania ze specjalnego oprogramowania, które jest narzędziem do płacenia podatków – informuje serwis CyberScoop.

Wyniki analizy przeprowadzonej przez specjalistów Trustwave podkreślają, w jaki sposób twórca oprogramowania podatkowego korzystał z usług wielu podwykonawców, którzy od lat zajmują się opracowywaniem backdoorów w konkretnych produktach.

Eksperci precyzują, że sytuacja dotyczy okresu 2018-2019 roku. Problem został zidentyfikowany w oprogramowaniu wymaganym przez chińskie banki do zapłaty podatków VAT – czytamy na oficjalnym blogu Trustwave.

Specjaliści kampanię nazwali GoldenHelper na podstawie jej powiązania z chińskim projektem Golden National Tax i jednej z głównych domen Command and Control: help.tax-helper.ltd.

Brian Hussey, specjalista Trustwave, podkreślił w rozmowie z CyberScoop, że cała operacja przypomina wspierane przez państwo kampanie wywiadowcze. „Istnieją cechy ataku państwa narodowego: gromadzenie danych wywiadowczych, nie jest to spektakularna technika lecz skoncentrowana i bardzo cicha" – wyjaśnił ekspert. – „Wiem, że chiński rząd bardzo często korzysta ze swoich państwowych organizacji do tego typu kampanii".

Jak wskazuje Trustwave, Aisino Corporation, spółka zależna China Aerospace Science and Industry Corporation Limited (CASIC), współpracowała z podwykonawcami – Chenkuo Network Technology i NouNou Technologies – w celu opracowania narzędzi do gromadzenia danych wywiadowczych, znanych jako GoldenSpy i GoldenHelper.

W tym miejscu warto podkreślić, że chińskie oprogramowanie Golden Tax Project zostało opracowane przez Aisino we współpracy z naukowcami z Harbin Institute of Technology i Beijing University of Posts and Telecommunications. Oba uniwersytety zostały powiązane z chińskim Ministerstwem Bezpieczeństwa Państwowego oraz służbami bezpieczeństwa – donosi CyberScoop.

Brian Hussey wskazuje, że kampania jest bardzo obszerna. Jej celem były dziesiątki firm w całej Europie, na Bliskim Wschodzie, w USA, Kanadzie i Australii. Chińskie działania wymierzone były w szerokie spektrum sektorów – od branży obronnej po finanse i sport. Niestety ekspertom nie udało się

dotrzeć do brytyjskiego kontrahenta, który padł ofiarą kampanii ani chińskiego banku zamieszanego w sprawę.