Cyberdefence 24

aut. Szymon Palczewski 29.10.2020

HAKERZY FSB PENETRUJĄ EUROPĘ. ORGANIZACJA RZĄDOWA „POD LUPĄ" ROSJI

Hakerzy powiązani z rosyjskim FSB uderzyli w jedną z europejskich organizacji rządowych w celu infiltracji jej sieci. Ich głównym zadaniem jest kradzież danych, co odbywa się z wykorzystaniem backdoorów oraz specjalnie przygotowanego na potrzeby operacji złośliwego oprogramowania.

Turla, grupa rosyjskich hakerów znanych z operacji szpiegowskich, nieustannie atakuje organizacje rządowe „za pomocą niestandardowego złośliwego oprogramowania", w tym udoskonalonych narzędzi wykorzystywanych już w przeszłości – wynika z raportu „Turla uses HyperStack, Carbon, and Kazuar to compromise government entity". Jej głównym celem jest utrzymanie dostępu do sieci i systemów ofiar poprzez backdoory, co pozwala hakerom ominąć zabezpieczenia. Grupa została powiązana przez estońskie władze z rosyjską agencją wywiadowczą FSB.

„Turla od ponad dziesięciu lat prowadzi operacje szpiegowskie w imieniu państwa" – czytamy w analizie. Grupa specjalizuje się w cyberatakach wymierzonych w zagraniczne rządy i ambasady. Podczas kampanii stosuje niestandardowe oprogramowanie, które pozwala hakerom działać niepostrzeżenie przez długi czas.

Podczas najnowszej operacji wykrytej przez specjalistów Accenture, Turla uderzyła w jedną z europejskich organizacji rządowych. Eksperci nie wskazali jednak konkretnej nazwy naruszonej instytucji ani kraju, z którego pochodzi. Prawdopodobnie jest to podyktowane chęcią ochrony jego interesów i względami bezpieczeństwa.

Analiza kampanii wykazała, że hakerzy wykorzystali „kombinację backdoorów", w tym znanych jako HyperStack, Kazuar oraz Carbon, do naruszenia systemów organizacji. To pozwoliło członkom Turla wykradać dane z zainfekowanej sieci, minimalizując tym samym możliwość wykrycia operacji. Z reguły narzędzia hakerów są zawsze dostosowane do organizacji, która jest celem prowadzonych działań.

„Ta kombinacja narzędzi służy grupie Turla" – wskazali specjaliści w raporcie. W związku z tym prawdopodobnie hakerzy nadal będą utrzymywać swoją taktykę bazującą na wykorzystaniu backdoorów, polegając na niej podczas realizowanych kampanii. Warto podkreślić, że cyberataki rosyjskiej grupy są szczególnie skuteczne w przypadku sieci urządzeń opartych na systemie Windows.

„Turla prawdopodobnie będzie nadal używać swoich sprawdzonych narzędzi, aczkolwiek z aktualizacjami, w celu naruszenia bezpieczeństwa i utrzymania długoterminowego dostępu do urządzeń swoich ofiar, ponieważ okazały się one skuteczne w przypadku sieci opartych na systemie Windows" – podkreślili specjaliści Accenture. Ostrzeżenie jest skierowane przede wszystkim do podmiotów rządowych, które są głównym celem rosyjskiej grupy.

Matthieu Faou z firmy ESET w rozmowie z CyberScoop podkreślił, że Turla odznacza się wysoką

skutecznością operacji, ponieważ przywiązuje ogromną wagę do przygotowania kampanii i doboru odpowiednich narzędzi. „Będą wkładać tyle wysiłku, ile potrzeba, aby naruszyć swoje cele” – zaznaczył specjalista. Jak dodał, walka z rosyjskimi agentami w sieci jest bardzo trudna a powstrzymanie ich działań stanowi prawdziwe wyzwanie.

Turla słynie z zaawansowanych operacji wymierzonych w podmioty państwowe. Przykładem może być kampania cyberszpiegowska, której celem były instytucje państwowe krajów Europy Wschodniej. Jak informowaliśmy na naszym portalu, operacja została wykryta w maju br., lecz hakerzy prowadzili działania od co najmniej dwóch lat.

Działania były wymierzone w trzy strategiczne placówki – jeden z parlamentów na terenie Kaukazu i dwa ministerstwa spraw zagranicznych państw położonych w Europie Wschodniej. Nazwy konkretnych państw – tak jak to ma miejsce podczas najnowszej operacji – nie zostały ujawnione ze względu na ich bezpieczeństwo.

W ramach kampanii hakerzy wykorzystali złośliwe oprogramowanie do usunięcia plików PDF i Word z kliku komputerów poszkodowanych podmiotów. Nie było jasne, jakie informacje zostały przez naruszone instytucje utracone.

Kolejnym przykładem operacji grupy Turla mogą być cyberataki na organy rządowe w Armenii. Wówczas w ramach kampanii hakerzy zbudowali złośliwą infrastrukturę internetową, próbując w ten sposób skłonić armeńskich urzędników do wzięcia udziału w specjalnie spreparowanej ankiecie.

Wówczas jedynie dwie osoby padły ofiarą złośliwej operacji w ubiegłym roku, co sugeruje, iż hakerzy prowadzą wysoce selektywne uderzenia. Grupa skrupulatnie śledzi działania wybranego użytkownika i nie spieszy się podczas operacji. Charakteryzuje ją wysoka staranność.

Kampanie prowadzone przez rosyjskich hakerów wpisują się w szerszą strategię, w której Moskwa wykorzystuje cyberprzestrzeń do projekcji władzy w regionie. Turla jest do tego „idealnym narzędziem”. Zdaniem wielu ekspertów to najbardziej zaawansowana i kompetentna z rosyjskich grup hakerskich.

Czytaj też: Rosyjski cyberatak na parlament Norwegii. Incydent to ostrzeżenie dla Oslo?

Fot. Do kupienia w sklepie Defence24.pl