**Chińczycy szpiegują w Afryce i na Karaibach. Trwa nowa kampania hakerska.**

**W Afryce i na Karaibach trwa chińska kampania cyberszpiegowska koncentrująca się na organizacjach rządowych – informują eksperci Check Point Research, którzy prowadzą w tej sprawie dochodzenie. Odpowiedzialność przypisuje się ugrupowaniu Sharp Dragon (daw. Sharp Panda), które miało wykorzystać ładunki Cobalt Strike Beacon, umożliwiające otworzenie „backdoora”.**

Od 2021 r. analitycy bezpieczeństwa cybernetycznego z Check Point Research ściśle monitorują działania Sharp Dragon, chińskiego ugrupowania, znanego wcześniej jako Sharp Panda. Ich taktyka obejmowała dotychczas przede wszystkim wysoce ukierunkowane wiadomości phishingowe, które skutkowały wdrażaniem złośliwego oprogramowania, takiego jak [VictoryDLL](https://research.checkpoint.com/2021/chinese-apt-group-targets-southeast-asian-government-with-previously-unknown-backdoor/) lub framework [Soul](https://research.checkpoint.com/2023/pandas-with-a-soul-chinese-espionage-attacks-against-southeast-asian-government-entities/).

W ostatnich miesiącach zaobserwowano jednak wyraźną zmianę. Grupa Sharp Dragon przekierowała swoją uwagę na organizacje rządowe w Afryce i na Karaibach. Działania te są zgodne z dotychczasowym sposobem funkcjonowania Sharp Dragon, charakteryzującym się włamywaniem do prestiżowych kont e-mail w celu rozpowszechniania dokumentów phishingowych z wykorzystaniem zdalnego szablonu uzbrojonego przy użyciu [RoyalRoad](https://nao-sec.org/2020/01/an-overhead-view-of-the-royal-road.html). Jednak w przeciwieństwie do poprzednich metod, przynęty wykorzystują teraz Cobalt Strike Beacon, co wskazuje na strategiczną adaptację mającą na celu zwiększenie ich możliwości infiltracji.

Chińscy cyberprzestępcy wykorzystują wysoce spersonalizowane wiadomości phishingowe, najczęściej podszywające się pod oficjalną korespondencję, aby nakłonić ofiary do otwarcia złośliwych załączników lub kliknięcia złośliwych łączy. Załączniki lub łącza instalują ładunki, które z biegiem czasu ewoluowały od niestandardowego złośliwego oprogramowania, takiego jak VictoryDLL i framework Soul, do szerzej używanych narzędzi, takich jak Cobalt Strike Beacon. Po pomyślnym rozładowaniu złośliwe oprogramowanie tworzy przyczółek w systemie ofiary, umożliwiając podmiotom zagrażającym przeprowadzenie rozpoznania i zebranie informacji o docelowym środowisku. Ta faza rozpoznania umożliwia Sharp Dragon identyfikację celów o dużej wartości i odpowiednie dostosowanie ich strategii ataku.

Tego typu łańcuch infekcji podkreśla wyrafinowane podejście Sharp Dragona do operacji cybernetycznych, kładąc nacisk na staranne planowanie, rozpoznanie i wykorzystanie luk w zabezpieczeniach w celu osiągnięcia swoich celów przy jednoczesnej minimalizacji wykrywania.

Chociaż podstawowa funkcjonalność pozostaje spójna, Check Point Research zidentyfikowało zmiany w taktyce, technikach i procedurach (TTP), które odzwierciedlają ostrożniejszy wybór celów i świadomość bezpieczeństwa operacyjnego (OPSEC).

Strategiczna ekspansja Sharp Dragon w kierunku Afryki i Karaibów oznacza szersze wysiłki chińskich cyberpodmiotów mające na celu zwiększenie ich obecności i wpływu w tych regionach. Ewoluująca taktyka Sharp Dragon podkreśla dynamiczną naturę zagrożeń cybernetycznych, szczególnie wobec regionów, które były historycznie pomijane.