Chińczycy wykorzystują cyberbroń w sporze o Morze Południowochińskie

Laboratoria firmy F-Secure wykryły odmianę złośliwego oprogramowania atakującego podmioty zaangażowane w spór o Morze Południowochińskie. Według badaczy F-Secure niebezpieczna aplikacja wykradająca dane z komputerów może być pochodzenia chińskiego.

Laboratoria F-Secure wykryły odmianę złośliwego oprogramowania, które prawdopodobnie atakuje podmioty zaangażowane w spór o Morze Południowochińskie toczący się między Filipinami a Chinami. Złośliwa aplikacja, którą badacze z F-Secure nazwali NanHaiShu, to trojan typu RAT (Remote Access Trojan – trojan dający zdalny dostęp), który pozwala napastnikom wykradać dane z zainfekowanych komputerów. Niebezpieczne oprogramowanie i jego wykorzystanie w związku z orzeczeniem Trybunału w Hadze z 12 lipca opisano w nowym raporcie F-Secure NanHaiShu: RATing the South China Sea (NanHaiShu: cyberszczur na Morzu Południowochińskim.

- Wygląda na to, że ten zaawansowany atak APT (advanced persistent threat) jest ściśle powiązany ze sporem i postępowaniem pomiędzy Filipinami a Chinami o Morze Południowochińskie – mówi Erka Koivunen, doradca ds. cyberbezpieczeństwa w F-Secure. - Nie dość, że wszystkie zaatakowane organizacje są z tą sprawą w jakiś sposób związane, to jego pojawienie się zbiega się w czasie ze zdarzeniami i publikacją wiadomości na temat wyników postępowania przed Trybunałem w Hadze – tłumaczy ekspert z F-Secure.

Wśród zaatakowanych organizacji wymienionych w raporcie znalazły się:

- filipińskie Ministerstwo Sprawiedliwości, które było zaangażowane w sprawę zgłoszoną przez Filipiny przeciwko Chinom;
- organizatorzy szczytu państw Azji i Pacyfiku APEC (Asia-Pacific Economic Cooperation), który odbył się na Filipinach w listopadzie 2015 roku;
- duża międzynarodowa firma prawnicza.

Analiza techniczna wykazała powiązanie z kodem i infrastrukturą pochodzącymi od deweloperów z Chin. Dodatkowo, infiltrowane organizacje są bezpośrednio powiązane ze sprawami, które leżą w strategicznym interesie chińskiego rządu. Wszystkie te przesłanki skłaniają badaczy F-Secure do przypuszczeń, że złośliwe oprogramowanie jest pochodzenia chińskiego.

- Jeśli podejrzenia naszych badaczy są właściwe, oznaczałoby to, że Chińczycy stosują techniki cyberszpiegowskie, aby uzyskać lepszy wgląd w kulisy postępowania arbitrażowego – mówi Koivunen.

NanHaiShu jest rozprowadzany poprzez spersonalizowane wysyłki e-mailowe (spear phishing), które zawierają terminologię branżową charakterystyczną dla atakowanych organizacji, co wskazuje na to, że e-maile zostały specjalnie przygotowane z myślą o konkretnych odbiorcach. Plik załączany do e-maili zawiera złośliwe makro, które uruchamia wbudowany plik JScript. Po zainstalowaniu NanHaiShu wysyła dane z zainfekowanej maszyny na zdalny serwer i może pobrać dowolny plik, który wybierze haker.

Źródło: F-Secure

Zdjęcie: Photogenica