Cyberdefence 24

aut. Sylwia Gliwa 16.08.2019

US CYBER COMMAND OSTRZEGA PRZED ZAGROŻENIEM ZE STRONY KOREI PÓŁNOCNEJ

US Cyber Command ostrzega przed szkodliwym oprogramowaniem Grupy Lazarus - hakerów powiązanych z rządem Korei Północnej – donosi serwis CyberScoop. Działalność Pjongjangu może być związana z koniecznością pozyskania finansowania na prowadzenie programów zbrojeniowych.

Amerykańskie Cyber Command przesłało w środę do Virus Total próbki złośliwego oprogramowania. Jak wykazała analiza są one powiązane z kampaniami prowadzonymi przez Grupę Lazarus - twierdzi portal.

Zdaniem Briana Bartholomew z Kaspersky Lab na który powołuje się CyberScoop, próbki wydają się być tym samym złośliwym oprogramowaniem, znanym jako ELECTRICFISH o którym ostrzegało w maju br. FBI oraz departament Bezpieczeństwa Wewnętrznego. Jednym z nich jest popularne w Korei Północnej narzędzie do tunelowania a drugim jest fałszywym narzędziem proxy TLS. Próbki wydają się pochodzić z 2018 roku i prawdopodobnie ten rodzaj złośliwego oprogramowania jest obecnie wykorzystywane przez północnokoreańską grupę.

The Cyber National Mission Force wchodzący w skład Cyber Command doceniając współpracę przemysłem cyberbezpieczeństwa i sektorem publicznym przekazuje próbki, aby zwiększyć globalne bezpieczeństwo w sferze cyber powiedział rzecznik Cyber Command dla CyberScoop.

Tym razem przed oficjalną informacją, w poniedziałek w ramach wczesnego powiadomienia informacja trafiła również do sektora prywatnego w ramach projektu Cyber Threat Alliance. Projekt tworzy grupa firm, które dzielą się informacjami o zagrożeniach. Informacja o zagrożeniu przekazana w ramach ostrzeżenia TLP Amber, mającym oznaczać, że informacji nie można udostępniać publicznie i tylko zainteresowanym stronom otrzymało m.in Symantec, McAfee, Palo Alto Networks i Cisco. Byli oni zatem w stanie udoskonalić swoje systemu tak aby ochronić się przed złośliwym oprogramowaniem, zanim Cyber Command oznaczył informację o próbkach jako publiczne.

Adam Meyers, wiceprezydent CrowdStrike w komentarzu dla portalu CyberScoop sądzi, że działalność grupy może być powiązana ze zwiększeniem sankcji w 2017 roku na Koreę Północną, która przełożyła się na problemy finansowe rządu północnokoreańskiego. W raporcie ONZ wykazano, że 35 ataków przeprowadzonych na zlecenie rządu w Pjongjangu pozwoliło ukraść 2 miliardy dolarów, które zostały przekazane na finansowanie projektów zbrojeniowych.

Grupa określana jako Lazarus (APT-38) powiązana jest z rządem Pjongjangu. Jest ona szczególnie znana z działań wymierzonych w systemy finansowe. To już kolejny raz, kiedy Cyber Commnad dodaje informacje do repozytorium zabezpieczeń Virus Total w ramach wymiany informacji z sektorem prywatnym.