Cyberdefence 24

aut. Sylwia Gliwa 11.09.2019

VIRUSTOTAL: REKORDOWE PRZEKAZANIE PRÓBEK PRZEZ US CYBER COMMAND

US Cyber Command przekazał do VirusTotal łącznie aż 11 próbek złośliwego oprogramowania. W przekazanych próbkach znajduje się m.in szkodliwe oprogramowanie powiązane z działalnością hakerów z Korei Północnej – donosi portal CyberScoop.

Zdaniem naukowców, na których powołuje się portal, jest to największe w historii przekazanie danych przez US Cyber Command. W przesłanej paczce znalazły się również próbki złośliwego oprogramowania, powiązanego z grupa Lazarus, pracującej na zlecenie rządu Korei Północnej. Zdaniem eksperta z firmy FireEye ujawnienie próbek i przekazanie ich do publicznej informacji może być sygnałem dla rządów wykorzystujących hakerów do szkodliwych działań w cyberprzestrzeni, że ich funkcjonowanie można przypisać określonym podmiotom w tym również tym powiązanym z określonymi państwami.

„Czy to powstrzyma działania wywiadowcze? Oczywiście nie. To głupie. Wynika z tego, że [Koreańczycy z północy] nie działają bez powiązania, co ogranicza zakres działań, które powinni postrzegać jako możliwe do zaakceptowania ryzyko. Jest to jeden z powodów, dla których przypisanie ma znaczenie” – powiedział Andrew Thompson, główny analityk ds. Zagrożeń w FireEye w komentarzu dla portalu CyberScoop.

Pośród przekazanych danych znalazły się również próbki trojana znanego jako “HOPLIGHT”, który był wykorzystywany do gromadzenia informacji o systemach operacyjnych sprzętów zainfekowanych użytkowników.

Przekazanie danych nastąpiło niespełna kilka tygodni po tym jak ONZ ostrzegało, że rząd Korei Północnej wykorzystuje cyberataki do pozyskania środków na rozwój broni nuklearnej. Jak donosiliśmy na początku sierpnia Korea Północna wygenerowała około 2 miliardy dolarów dzięki zaawansowanym cyberatakom, których celem była kradzież środków z systemów bankowych oraz giełd kryptowalutowych. Według ONZ zdobyte w ten sposób fundusze Pjongjang przeznaczył na rozwój programu broni masowego rażenia. Do informacji tych odniósł się sam rząd północnokoreański zaprzeczając tym informacjom oraz oskarżając Stany Zjednoczone o rozpowszechnianie plotek.

VirusTotal to darmowy serwis internetowy, który umożliwia skanowanie poszczególnych plików. Wyniki pozwalają stwierdzić czy przesłany plik został zainfekowany szkodliwym oprogramowaniem.