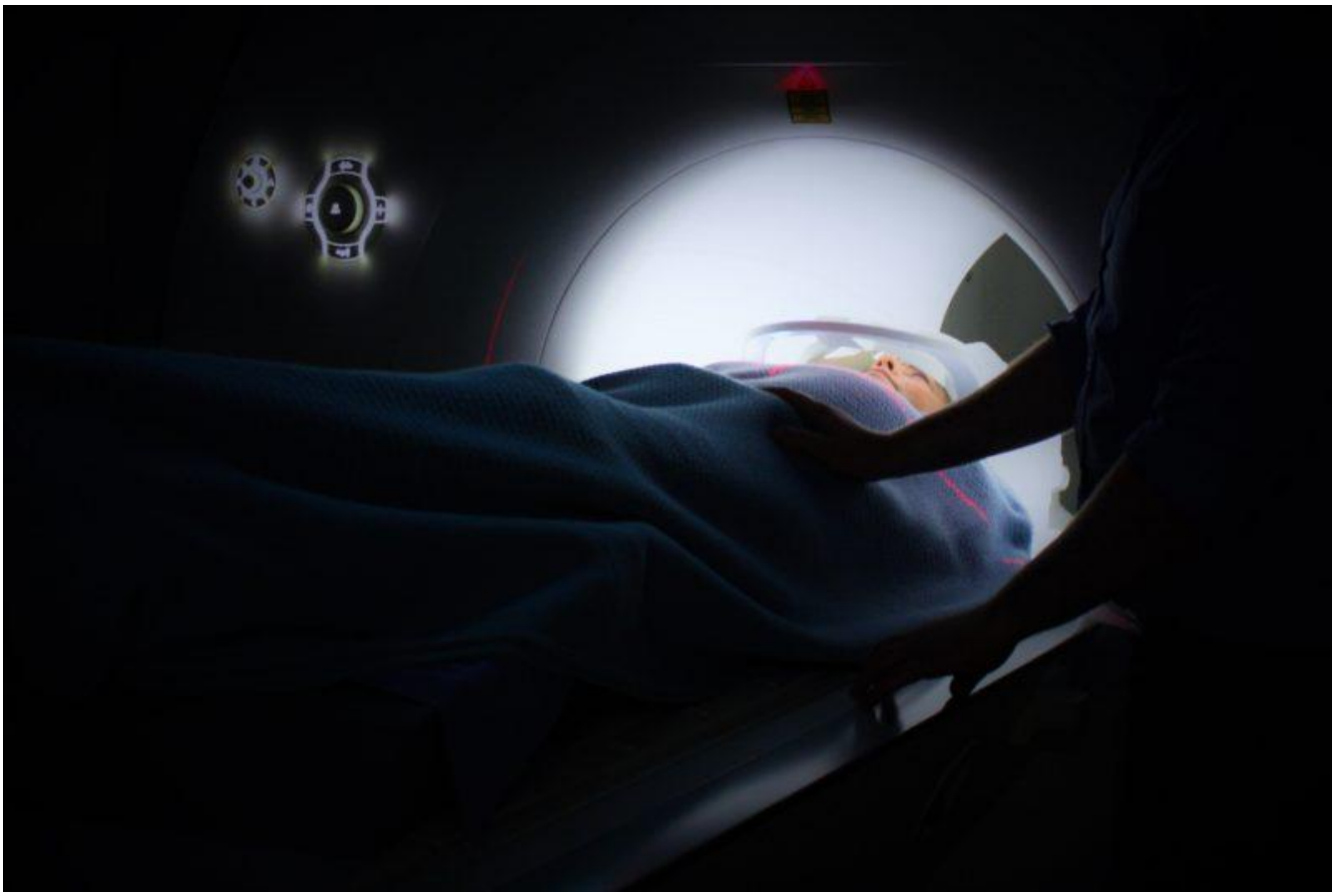

Orangeworm – agresywni hakerzy wykradają dane medyczne.

Od 2015 roku laboratorium Symanteca obserwuje działalność grupy o nazwie Orangeworm, która to w ostatnim czasie stala się bardzo aktywna. Grupa ta specjalizuje się w atakach na jednostki służby zdrowia. Wykorzystując do tego trojana o nazwie Kwampirs, infekują oni sprzęty medyczne takie jak sprzęty rentgenowskie czy tomografy komputerowe, by następnie wykradać dane medyczne pacjentów. Te zaś stają się powoli równie cenną walutą dla cybeprzestępców, co okupy z ransomware czy kryptowaluty wykopywane po kryjomu na komputerach ofiar. Sara Jost, szefowa komórki globalnego przemysłu medycznego w BlackBerry, stwierdza że dane medyczne na czarnym rynku są nawet 10-krotnie więcej warte niż np. dane kart kredytowych czy z dowodów tożamości. Dane te mogą być wykorzystywane do szantażu lub dyskredytacji ofiar, zwłaszcza osób publicznych i znanych. W obliczu nadciągającej dyrektywy UE o nazwie GDPR (a w Polsce nazywana RODO), taka kradzież nie kończy się na stratach wśród samych pacjentów, ale też ogromne konsekwencje (głównie finansowe) poniesie także sama jednostka medyczna, której dane zostały w ten sposób wykradzione.

Specjaliści z firmy Pancernik IT informują iż. Póki co grupa koncentrowała się na USA, skąd pochodzi 17 % ofiar. Jednak w ostatnim czasie grupa poszerzyła horyzonty. 5 % ataków było przeprowadzonych na Wielką Brytanię. I choć atak przy użyciu trojana Kwampirs nie jest nowy i jest wśród laboratoriów antywirusowych powszechnie znany, tak wciąż przestarzałe oprorgamowania (np. z Windows XP) w placówkach medycznych, a także szeroko rozpowszechniony problem z nieaktualnymi oprogramowaniami (co pokazał chociażby atak WannaCry w zeszłym roku), sprawia że cybeprzestępcy nie zniechęcają się i konsekwentnie zbierają żniwa. Świadczy o tym fakt, że grupa ta nie kwapi się z

modyfikowaniem swojego wirusa. Jak widać, nie muszą. Warto dbać więc o aktualne oprogramowanie. Profesjonalne IT Managery posiadają najczęściej zdalne zarządzanie aktualizacjami poprzez wbudowane menadżery. W dobie zbliżającego się RODO, warto naprawdę z nich korzystać.

Źródła:

digitalhealth.net
symantec.com
pancernik.it
zabezpieczenia.it