Hackeři londýnských nemocnic zveřejnili údaje o ukradených krevních testech

24.6.2024 - | INFOPROFI GROUP s.r.o.

Gang kybernetických zločinců, který způsobil obrovské narušení mnoha londýnským nemocnicím, zveřejnil 400 GB citlivých dat o pacientech.

Gang se snaží vymáhat peníze od poskytovatele NHS Synnovis od chvíle, kdy 3. června hackli firmu. Expert na kybernetickou bezpečnost Ciaran Martin řekl BBC, že jde o „jeden z nejvýznamnějších a nejškodlivějších kybernetických útoků, jaké kdy ve Spojeném království byly“. Vzorek dat, který viděla BBC, zahrnuje jména pacientů, data narození, čísla NHS a popisy krevních testů. Není známo, zda jsou v datech také výsledky testů.

Hack také vedl k narušení více než 3 000 schůzek a operací v nemocnicích a u praktických lékařů. Mezi postiženými je i teenager, který se léčí s rakovinou.
Rodiče Dylana Kjorstada řekli BBC, že byli ponecháni ve stavu „nedůvěry“, když jim bylo řečeno, že jeho operace s odstraněním nádoru na žebrech se odkládá.

Pan Martin, bývalý šéf Národního centra pro kybernetickou bezpečnost a nyní profesor na Oxfordské univerzitě, řekl programu World at One na BBC Radio 4, že může trvat několik měsíců, než budou systémy obnoveny. Qilin dříve řekl BBC, že údaje zveřejní, pokud nedostanou zaplaceno.
Existují také tabulky obchodních účtů, které podrobně popisují finanční ujednání mezi nemocnicemi a službami praktických lékařů a společností Synnovis.
NHS England řekla BBC, že o publikaci věděla, ale nemůže si být zcela jistá, že sdílená data jsou skutečná. "Chápeme, že to lidi může znepokojovat, a nadále spolupracujeme se Synnovisem, Národním centrem kybernetické bezpečnosti a dalšími partnery, abychom co nejrychleji určili obsah publikovaných souborů," uvedlo.

Synnovis mezitím řekl: "Víme, jak znepokojivý může být tento vývoj pro mnoho lidí. Bereme to velmi vážně a analýza těchto dat již probíhá."
Hackeři ransomwaru pronikli do počítačových systémů společnosti, které používají dva trusty NHS v Londýně, a zašifrovali důležité informace, díky nimž byly IT systémy k ničemu.

Jak už to u těchto gangů bývá, také si stáhli co nejvíce soukromých dat, aby mohli dále vymáhat od společnosti výkupné v bitcoinech. Není známo, kolik peněz hackeři po Synnovis požadovali, ani zda společnost vstoupila do jednání. Ale skutečnost, že Qilin zveřejnil některá, potenciálně všechna data, znamená, že nezaplatili.
Orgány činné v trestním řízení po celém světě pravidelně nabádají oběti ransomwaru, aby neplatily, protože to podněcuje zločinné podnikání a nezaručuje, že zločinci udělají, co slíbí.

Expert na ransomware Brett Callow ze společnosti Emsisoft uvedl, že zdravotnické organizace jsou stále častěji terčem útoků, protože hackeři věděli, že mohou způsobit spoustu škody a někdy dostat velkou výplatu. „Kyberzločinci jdou tam, kde jsou peníze, a bohužel útočí také na zdravotnictví. A protože United Health Group údajně zaplatila počátkem tohoto roku výkupné ve výši 22 milionů dolarů (17,3 milionů liber), je tento sektor v hledáčku více než kdy předtím,“ řekl.

V úterý večer Qilin mluvil s BBC o šifrované službě zpráv a řekl, že se záměrně zaměřili na Synnovise jako způsob, jak potrestat Spojené království za to, že dostatečně nepomohlo v blíže nespecifikované válce. Pan Martin popsal toto tvrzení jako „naprostý odpad“ a uvedl, že jejich cíle byly „zcela

finanční“.

Předpokládá se, že gang, stejně jako mnoho ransomwarových posádek, sídlí v Rusku, ale řekl BBC, že "z bezpečnostních důvodů" nemůže být konkrétnější, pokud jde o jeho politickou oddanost nebo geografickou polohu. Na své darknetové stránce také ukradli data od jiných zdravotnických organizací, stejně jako škol, společností a rad z celého světa.

https://www.bbc.com/news/articles/c9ww90j9dj8o