Una dintre cele mai recente postări pe site-ul DNSC vorbește despre un nou atac al hackerilor.

 **Resursa informațională afectată** sunt datele personale ale clienților care erau păstrate de organizațiile financiare care au căzut victime atacului informațional.

 **Modus operandi** este unul destul de comun. Hackerii foloseau un script care semăna destul de mult cu scriptul jocului minesweeper, astfel aplicațiile antimalware nu l-ar fi detectat ca fiind un virus. Atacatorii trimiteau apoi un e-mail de pe adresa support@patient-docs-mail.com cu o arhiva zip cu informații despre pacienți. În momentul în care arhiva era downloadată, era descărcat și „minesweeper” care avea rolul de a se decoda și de a începe să infesteze computerul, cu scopul de a fura informațiile personale.

 **Actorii implicați** nu este menționată gruparea, însă sigur este un grup de hackeri.

 **Metode de protecție**  ar putea fi învățarea angajaților de a se feri de e-mailuri suspecte și de a nu le deschide și mai mult, de a nu descărca nimic ce nu este dintr-o sursă 100% sigură, implementarea unei politici de folosire a e-mailului. O altă modalitate de a evita asemenea situații ar fi instalarea unui antivirus care nu este gratis, cu funcția de verificare a e-mailurilor și trimiterea celor suspecte în spam, pentru a se evita tentația clickului.[[1]](#footnote-1)

1. Bill Toulas,2024, *BleepingComputer*s, accessed [30.05.2024], <https://www.bleepingcomputer.com/news/security/hackers-phish-finance-orgs-using-trojanized-minesweeper-clone/> , redirected from <https://dnsc.ro/citeste/stirile-saptamanii-din-cybersecurity-30-05-2024> [↑](#footnote-ref-1)