Cyberdefence 24

**aut. Szymon Palczewski** 15.10.2020

# STUDENCI WRÓCILI NA UCZELNIE A... IRAŃSCY HAKERZY DO ATAKÓW. UNIWERSYTETY CELEM KAMPANII PHISHINGOWEJ

Irańscy hakerzy zintensyfikowali swoje działania, przeprowadzając cyberataki wymierzone w placówki edukacyjne z całego świata, w tym w szczególności na wiodące uniwersytety. Kampania rozpoczęła się tuż przed rozpoczęciem nowego roku akademickiego i powrotem studentów na uczelnię. Jakie jest główne zadanie hakerów?

Specjaliści firmy Malwarebytes wskazują, że nowa kampania prowadzona przez grupę irańskich hakerów, znanych jako „Silent Librarian", rozpoczęła się najprawdopodobniej w połowie września br. Na jej ślady eksperci natrafili dzięki czujności jednego z klientów firmy, który poinformował o niepokojącej aktywności cyberprzestępców.

„Opierając się na liczbie ofiar, możemy stwierdzić, że Silent Librarian nie ogranicza się do konkretnych krajów, lecz stara się działać w większej skali" – czytamy w raporcie Malwarebytes. Głównym celem kampanii spear phishingowej są placówki edukacyjne, w tym przede wszystkim wiodące uniwersytety.

W rozsyłanych przez hakerów e-mailach znajdują się załączniki do zainfekowanych stron internetowych, podszywających się pod witrynę określonego uniwersytetu lub powiązanej placówki, na przykład uczelnianej biblioteki. Stąd też wzięła się nazwa grupy "Silent Librarian" (tłum. „cichy bibliotekarz").

Specjaliści wskazują, że wiele domen wykorzystywanych podczas operacji hakerskiej zostało skutecznie usuniętych, lecz pomimo tego Silent Librarian kontynuuje swoje działania. Wynika to z faktu, że infrastruktura stworzona przez grupę jest bardzo rozbudowana i zniszczenie części jej elementów nie jest w stanie skutecznie zatrzymać prowadzonej kampanii.

Cyberataki ze strony irańskiego ugrupowania zostały już w przeszłości odkryte. Dzięki prowadzonym analizom udało się dowieść, że "Silent Librarian" specjalizuje się w operacjach wymierzonych w szkoły i uniwersytety. Co więcej, w marcu 2018 roku Departament Sprawiedliwości Stanów Zjednoczonych oskarżył dziewięciu Irańczyków o przeprowadzanie ataków na placówki naukowe w celu kradzieży badań i zastrzeżonych danych.

Pomimo interwencji ze strony amerykańskich władz przez następne miesiące hakerzy przygotowywali się do kolejnych operacji, w wyniku których poszkodowanych zostało wiele instytucji z kilkunastu państw – wynika z raportu Malwarebytes.

"Silent Librarian" skutecznie wykorzystuje fakt, że studenci oraz wykładowcy to grupa „najtrudniejszych do ochrony" użytkowników sieci akademickiej, co wynika z faktu ich często nieracjonalnego zachowania. „Administratorzy IT pracujący na uczelniach mają wyjątkowo ciężką

pracę” – podkreślają specjaliści.

Eksperci zwracają uwagę, że pomimo nakładanych sankcji Iran stara się nadążyć za światem w różnych dziedzinach, w tym w obszarze technologii. „W związku z tym cyberataki stanowią interes narodowy i są dobrze finansowane” – czytamy w raporcie.

Analiza najnowszej kampanii wykazała, że część infrastruktury wykorzystywanej przez hakerów, w tym zainfekowanych domen, jest hostowana z terytorium Iranu. „Może wydawać się to dziwne, że grupa wykorzystuje infrastrukturę w swoim kraju, tym samym wskazując palcem na źródło operacji” – podkreślają specjaliści. Jednak hakerzy nie mają potrzeby „wysilać się”, ponieważ skutecznie wykorzystują brak skutecznej współpracy między amerykańskimi lub europejskimi organami ścigania a irańskimi służbami.

Eksperci Malwarebytes ostrzegają, że udało im się odkryć jedynie niewielką część prowadzonej operacji spear phishingowej, w związku z czym zagrożenie dla placówek edukacyjnych jest wysokie, a co najważniejsze bardzo realne. „Hakerzy są o krok przed nami i atakują wiele możliwych celów jednocześnie” – czytamy w raporcie. Czy polskie szkoły i uniwersytety są bezpieczne?

Poniżej znajduje się lista placówek, która stała się celem Silent Librarian:

1. The University of Adelaide Library
2. Glasgow Caledonian University
3. Stony Brook University
4. Stony Brook University
5. Universiteit Utrecht
6. Universiteit Utrecht
7. Victoria University
8. University of Bristol
9. University of Toronto
10. University of Cambridge
11. Karolinska Medical Institutet
12. University of York
13. University of Kent
14. Göteborg universitet
15. Western University Canada
16. King's College London
17. Queen Mary University of London
18. Melbourne Victoria Australia
19. Nanyang Technological University
20. University of Lincoln
21. TH Mittelhessen University of Applied Sciences
22. University of North Texas
23. McGill University
24. University of Cambridge

**Czytaj też:** Fala ataków ransowmare na brytyjskie szkoły i uniwersytety