Microsoft walczy z irańskimi hakerami

#Cyberprzestrzeń #Strategia i polityka 8 czerwca 2022

Microsoft poinformowa? 2 czerwca 2022, ?e zablokowa? dzia?alno?? powi?zanej z Iranem liba?skiej grupy hakerów POLONIUM, która w czasie trzech ostatnich miesi?cy zaatakowa?a w sieci ponad 20 izraelskich przedsi?biorstw korzystaj?cych z platformy Microsoft OneDrive do przechowywania danych w chmurze. Dzia?ania cyberterrorystów wymierzone by?y równie? w jedn? organizacj? mi?dzyrz?dow?. G?ównym celem by?y jednak organizacje izraelskie, które zajmuj? si? infrastruktur? krytyczn? i IT, a tak?e przedsi?biorstwa izraelskiego przemys?u obronnego.

Według izraelskich mediów ataki przeprowadzono we współpracy z irańskim ministerstw

Image not found or type unknown

Aktywno?? grupy w Internecie by?a stale monitorowana, a za jej rozpracowanie odpowiada?a specjalna komórka Microsoft Threat Intelligence Center (MSTIC). Hakerzy wpadli dlatego, ?e w chmurze OneDrive tworzyli i u?ywali legalnych kont, na których przechowywali oprogramowanie do celów dowodzenia i kierowania, a tak?e do zalewania stron internetowych niechcianym oprogramowaniem szpieguj?cym. *Jerusalem Post* twierdzi, ?e ataki przeprowadzano we wspó?pracy z ira?skim ministerstwem wywiadu i bezpiecze?stwa.

Microsoft zapewni?, ?e sposób dzia?ania sprawców nie jest powodem do niepokojów i nie stanowi luki w zabezpieczeniach ani zagro?enia bezpiecze?stwa na platformie OneDrive. Nowo wprowadzone aktualizacje protoko?ów bezpiecze?stwa b?d? poddawa? kwarantannie narz?dzia opracowane przez cyberterrorystów. Dodatkowo Microsoft podda? kwarantannie ponad 20 z?o?liwych aplikacji.

W ostatnim czasie ameryka?skie przedsi?biorstwo informatyczne zidentyfikowa?o i zapobieg?o kilku innym atakom na izraelskie podmioty. W pa?dzierniku 2021 r. Microsoft og?osi?, ?e ira?scy hakerzy z powodzeniem zaatakowali ameryka?skie i izraelskie przedsi?biorstwa zajmuj?ce si? technologiami obronnymi. Ponad 250 kont Microsoft Office 365 powi?zanych z USA, UE i Izraela zosta?o zaatakowanych za pomoc? do?? prostej metody *password spraying* polegaj?cej na wybraniu jednego, powszechnego has?a i próbowaniu go na wielu kontach w organizacji.

Ponadto celem ataków by?y porty u wej?cia do Zatoki Perskiej i globalne przedsi?biorstwa transportu morskiego, które prowadz? dzia?alno?? gospodarcz? na Bliskim Wschodzie. Dzia?alno?? grupy POLONIUM to jedynie wierzcho?ek góry lodowej ira?sko-izraelsko-ameryka?skiej wojny cybernetycznej (Cyberatak na ira?skie stacje paliw , 2021-10-29, Cyberatak na ira?skie koleje, 2021-07-11, Cyberataki na izraelskich ?o?nierzy, 2018-07-06).

Powiązane wiadomości

- Microsoft walczy z irańskimi hakerami (2022-06-08)
  - Cyberataki na izraelskich żołnierzy (2018-07-06)
    - Islamiści atakują siły Cahalu (2016-11-28)
      - UNDOF bez uzbrojenia (2014-09-23)
      - Skuteczny Iron Dome (2016-09-19)
    - Szczegóły ataku na Syrię (2018-05-23)
      - Bojowy debiut Adirów (2018-03-16)
      - 27 ofiar ataków Izraela w Syrii (2018-05-12)
    - Kobiety - dowódcy Merkav (2018-06-29)
      - Nowy plan modernizacji Cahalu (2017-01-25)
  - Cyberatak na irańskie koleje (2021-07-11)
  - Cyberatak na irańskie stacje paliw (2021-10-29)
    - Tajemnice eksplozji w Iranie (2020-07-06)
    - Cyberatak na irańskie koleje (2021-07-11)