**Ostatnie ataki hakerskie pokazują jak ważne jest cyber-bezpieczeństwo**

**O tym jak dynamiczna jest wojna w cyberprzestrzeni pokazują ataki z ostatnich tygodni. W ogromnych kampaniach skierowanych do wielkich korporacji i instytucji rządowych, zamieszane są wyspecjalizowane grupy hakerskie przy wsparciu rządów rywalizujących państw.**

**Ostatnie ataki hakerskie pokazują jak ważne jest cyber-bezpieczeństwo**

O tym jak dynamiczna jest wojna w cyberprzestrzeni pokazują ataki z ostatnich tygodni. W ogromnych kampaniach skierowanych do wielkich korporacji i instytucji rządowych, zamieszane są wyspecjalizowane grupy hakerskie przy wsparciu rządów rywalizujących państw.

[Associated Press donosi o irańskiej grupie „Charming Kitten”, której ostatnim celem ataku były dziesiątki oficjeli z USA](https://www.securityweek.com/ap-exclusive-iran-hackers-hunt-nuke-workers-us-officials), głównie w celu wykradnięcia informacji nt. sankcji i przyszłych strategii z nimi związanych. Drugim celem byli wysoko postawieni naukowcy i członkowie zarządów firm zajmujących się rozwojem technologii nuklearnych. Hakerzy wpadli przez pomyłkę, gdy zostawili jeden z serwerów dostępny w sieci. Dane z serwera przejęła londyńska grupa ds. bezpieczeństwa – CERTFA. Grupa ta monitoruje „Charming Kittens” od dawna, wykrywając przy tym powiązania z irańskim rządem. Associated Press udowodniło także ich udział w atakach m. in. naukowca pracującego nad technologią jądrową dla pakistańskiego ministerstwa obrony, starszego operatora testowego reaktora jądrowego w Jordanii, czy starszego projektanta z Komisji Energii Atomowej w Syrii. Innym celem irańskich hakerów są oczywiście amerykańskie technologie wojskowe. Irańsko-amerykańska cyber-wojna trwa od dobrych paru lat, gdzie punktem zwrotnym był izraelsko-amerykański atak na irański program jądrowy z użyciem wirusa [StuxNet](https://pl.wikipedia.org/wiki/Stuxnet). Generalnie Iran pomimo dyplomatycznego odżegnywania się od działalności hakerów i sankcji nakładanych przez USA, potajemnie nie zamierza rezygnować ze swych atomowych ambicji. O tym jak krytyczną gałęzią jest sektor energetyczny przekonała się włoska firma Saipem, [zaatakowana ostatnio przez malware o nazwie Shamoon 3.](https://www.reuters.com/article/us-cyber-shamoon/saipem-says-shamoon-variant-crippled-hundreds-of-computers-idUSKBN1OB2FA)

Specjaliści firmy [Pancernik.it](http://pancernik.it/) uważają iź Cyber-wojna to nie tylko ataki na oficjeli. Również atakami mogą zostać dotknięci zwykli obywatele. Właśnie ujawniono, że [wyciekły dane Francuzów wprost ze strony Ministerstwa Spraw Zagranicznych](https://www.cyberdefence24.pl/wyciekly-dane-obywateli-francuski-msz-zaatakowany). Francuski rząd zapewnia, że dane nie były wrażliwe, jednak stawia to pod znakiem zapytania skuteczność ochrony francuskich służb przed tego typu atakami. Na razie nie znana jest grupa odpowiedzialna za atak. Dane wykradzione zostały z platformy Ariane, która miała informować obywateli Francji nt. bezpieczeństwa podczas ich zagranicznych pobytów.

Nie próżnują także niesławni hakerzy z Rosji. Grupa znana jako „Sofacy” czy „Sendit” została powiązana przez naukowców z Palo Alto jako odpowiedzialna za globalną [kampanię phishingową z użyciem nowoczesnego trojana „Cannon”](https://www.securityweek.com/russia-linked-phishing-attacks-hit-government-agencies-four-continents). Korzystając z kampanii e-mailowej, grupa rozesłała miliony maili do firm na czterech kontynentach. Maile zawierały dokument uzbrojony w złośliwe makro z funkcją AutoClose – złośliwy kod aktywuje się w momencie, gdy użytkownik zamknie dokument. Owy dokument będzie chciał ściągnąć drugą fazę ataku i ją aktywować, korzystając z backdoora określanego jako Zebrocy, [którego niedawno odkryli i opisali naukowcy firmy ESET](https://www.welivesecurity.com/2018/04/24/sednit-update-analysis-zebrocy/). Backdoora tego Rosjanie używali także m. in. na Ukrainie, w Azerbejdżanie, Kirgistanie, czy Turcji. Trojan „Cannon” zawiera bardzo wiele funkcji szpiegujących – od keyloggerów, po podsłuchy z mikrofonów, czy ściąganie i podglądanie poczty. Wirus tego typu określany jest jako „weapon-grade malware” (wirus klasy wojskowej).

Oczywiście nie byłoby cyber-wojny bez koreańskiej grupy Lazarus, [o której pisaliśmy m. in. przy okazji ataków na jednostki medyczne.](http://blog.pancernik.it/orangeworm-agresywni-hakerzy-wykradaja-dane-medyczne/) Naukowcy z McAfee [zidentyfikowali globalny atak o kryptonimie „Sharpshooter”](https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/operation-sharpshooter-targets-global-defense-critical-infrastructure/), wycelowany w 82 światowe organizacje. Atak wykorzystywał backdoora [Duuzer](https://www.securityweek.com/duuzer-trojan-used-target-south-korean-organizations). 25 października atak rozpoczął się od rozesłania dokumentów m. in. przy użyciu Dropboxa. Zainfekowane makro aktywowało shellcode by załadować do pamięci Worda moduł ściągający wirusa o nazwie „Rising Sun”, który jest zaawansowanym trojanem zbierającym informacje o zainfekowanych maszynach, a także modyfikacji danych na nich przechowywanych (w tym ich kopiowania i usuwania).

Jak donosi portal [CyberDefence24.pl](https://www.cyberdefence24.pl/us-army-informacja-kluczowa-bronia-na-przyszlym-polu-bitwy):

W dokumencie „The U.S. Army in Multi-Domain Operations 2028” przedstawiono przewidywania dotyczące operacji prowadzonych przez siły lądowe Stanów Zjednoczonych do 2028 roku. Podkreślono znaczenie ewolucji broni w XXI wieku, a główny nacisk położono na odstraszanie Chin i Rosji na wielu płaszczyznach, w tym także cyberprzestrzeni. Środowisko wirtualne zostało określone jako jedna z najważniejszych przestrzeni prowadzenia operacji.

Innymi słowy jesteśmy w środku wojny, gdzie o naszym bezpieczeństwie nie decydują już czołgi na granicy, lecz niepozorne urządzenia stojące w naszych szafach rack’owych…

Autor wpisu: Karol Mondry

Źródła:

reuters.com

cyberdefence24.pl

securityweek.com

securingtommorow.mcafee.com

welivesecurity.com

wikipedia.org

blog.pancernik.it

pancernik.it