Co miała CIA w „hakerskim” arsenale?

8 marca 2017

„Wikileaks” publikuje tysiące dokumentów dotyczących narzędzi „hakerskich”, które miały być rozwijane przez CIA. Ten wyciek może być równie istotny jak afera Snowdena. Pokazuje, że dla służb nie zawsze najważniejsze było bezpieczeństwo ogółu i niestety nie radzą sobie one z pilnowaniem swojej cyberbroni.

Wczoraj wyciekowy serwis Wikileaks zaczął ujawnianie nowej serii dokumentów określanej jako Vault 7. Wyciek obejmuje dokumenty związane z narzędziami CIA. Pierwsza partia dokumentów określana jako „Year zero” obejmuje 8761 dokumentów pochodzących z jednostki o nazwie Center for Cyber Intelligence (CCI) w Langley. Dokumenty zostały częściowo zredagowane przez Wikileaks. Obejmują lata 2013-2016.

Cała seria dokumentów Vault 7 ma stanowić największy w historii wyciek dotyczący agencji wywiadowczej.

Z dokumentów wynika, że od roku 2001 CIA miała polityczną i budżetową przewagę nad inną agencją kojarzoną z masową inwigilacją – NSA. W związku z tym CIA pozwoliła sobie na zbudowanie floty dronów oraz zatrudnienie „hakerów”, dzięki czemu mogła polegać na swoich siłach i nie musiała zgłaszać pewnych swoich działań NSA. To samo w sobie jest fascynujące, że różne służby mają tajemnice także między sobą i zawsze są chętne do dublowania działań innych agencji.

„Hakerski” wydział CIA to było właśnie wspomniane CCI. Według „Wikileaks” do końca roku wyprodukowało ono ponad tysiąc narzędzi takich jak trojany, wirusy oraz – jak określa to Wikileaks – „uzbrojone malware”. Pracownicy CIA mieli stworzyć więcej kodu niż wykorzystano do prowadzenia „Facebooka”.

Co gorsza CIA straciła kontrolę nad swoim cyberarsenałem oraz

powiązaną z nim dokumentacją. Informacje teoretycznie dające innym możliwości CIA zaczęły krążyć pomiędzy zatrudnionymi przez rząd specjalistami w sposób dość swobodny. Dzięki temu „Wikileaks" mogło otrzymać część tego archiwum.

„Istnieje ekstremalne nasilenie ryzyka związanego z rozwojem „cyberbroni". Można poczynić porównanie pomiędzy niekontrolowanym rozrostem takiego uzbrojenia (…) i globalnego handlu bronią. Ale znaczenie „Year zero" wychodzi poza dokonanie wyboru między cyberwojną i cyberpokojem. To ujawnienie dokumentów jest również wyjątkowe z politycznej, prawnej i śledczej perspektywy" – mówił Julian Assange, założyciel „Wikileaks".

Wśród „narzędzi hakerskich" opracowanych przez CIA znalazły się takie, które służą do ataków na popularne urządzenia m.in. na telewizory Samsung Smart TV. Miały one pozwalać na przestawienie telewizorów w stan „fikcyjnego wyłączenia", co umożliwiało nagrywanie rozmów w pokoju i wysyłanie ich na serwer CIA.

W roku 2014 wypracowano metody infekowania nowoczesnych pojazdów. Nie wiadomo jaki był cel tego działania, ale niewykluczone jest iście filmowe dokonywanie niewykrywalnych zabójstw. Ponadto CIA miała jednostkę do spraw mobilnych, która opracowała metody włamywania się na telefony. Ta jednostka była szczególnie zainteresowana iPhone'ami. Mobilny cyberarsenał CIA obejmował nie tylko narzędzia samodzielnie wytworzone, ale też przejęte od innych agencji takich jak NSA, FBI czy brytyjska GCHQ.

Użytkownicy Androida też mają powody do obaw. CIA znalazła sposób na wykorzystanie przynajmniej 24 luk zero-day.

Agenci interesowali się także lukami w Windowsie, OS X, Linuksie oraz w routerach. Co bardzo istotne, CIA złamała swoją obietnicę odpowiedzialnego ujawniania informacji o lukach. Zachowywała dla siebie informacje o pewnych

słabościach systemów aby móc je samolubnie wykorzystać.

Jak zauważył „Niebezpiecznik”, CIA nie złamało szyfrowania komunikatorów Singnal i WhatsUp (wbrew temu, co twierdzą niektóre media). CIA ma jednak możliwość włamania się na telefon czy komputer na którym te komunikatory są instalowane. To z praktycznego punktu widzenia jest większym problemem niż podsłuchiwanie komunikatorów.

Dokumenty pokazują też, że jednostka o nazwie Engineering Development Group (EDG) prowadziła około 500 różnych projektów związanych ze złośliwym oprogramowaniem i narzędziami do włamań. Zebrano też mnóstwo informacji o narzędziach do cyberwalki wytworzonych przez inne państwa np. przez Rosję.

Najgorsze jest to, że narzędzia do cyberwalki trudno utrzymać w ryzach. One mają swoją „wartość rynkową” podobnie jak zwykła broń, ale o wiele łatwiej je wynieść, ukraść lub sprzedać. Najwyraźniej CIA nie była w stanie zapanować nad swoim cyberarsenałem i nie jest to ani trochę zaskakujące.

To wszystko odbywa się za pieniądze podatników. Poszczególne służby dublują swoje działania bo tak im pasuje. Wytwarzane są narzędzia, które tak naprawdę zagrażają wszystkim. CIA unikała otwartego mówienia o swoich odkryciach bo przedkładała wartość arsenału nad bezpieczeństwo publiczne. To wszystko jest głęboko niepokojące.

Najnowszy wyciek „Wikileaks” powinien prowadzić do zadania kilku istotnych pytań nie tylko w USA. Proces cyberzbrojeń i cyberataków powinien być w jakiś sposób kontrolowany społecznie. Obecnie jest to „dziki zachód”, ale ukryty pod maską niejawnych i tajnych działań niby zgodnych z prawem, co do których możemy tylko ufać, że nie są poważnymi nadużyciami. Niestety od czasów Snowdena wiemy aż za dobrze, że zaufanie to za mało.

Autorstwo: Marcin Maj
Źródło: DI.com.pl