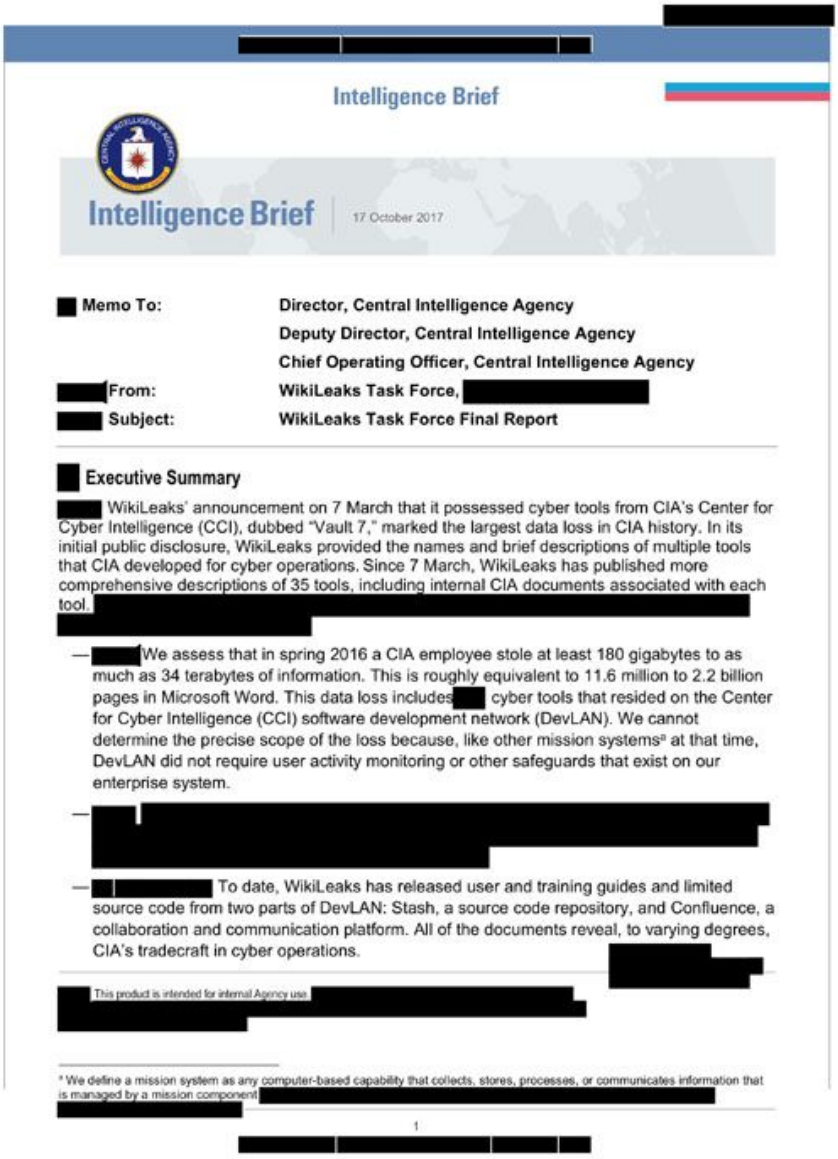
Vault 7 – największy wyciek danych z CIA

#Publikacje #Służby państwowe 17 czerwca 2020

16 czerwca 2020 amerykański senator Ron Wyden z Partii Demokratycznej, reprezentujący stan Oregon, wysłał list do dyrektora National Intelligence Johna Ratcliffe'a z pytaniami w sprawie działań zapobiegawczych, jakie podjęto (lub nie) w służbach wywiadowczych USA po ujawnieniu w 2017 wycieku danych z Central Intelligence Agency (CIA) – sprawa o kryptonimie *Vault 7*. W tym czasie WikiLeaks zaczęła publikować tajne dokumenty pochodzące z sieci wewnętrznej CIA. W odpowiedzi Agencja utworzyła specjalny zespół dochodzeniowy, którego zadaniem miało być wykrycie źródła wycieku danych, określenie, co tak naprawdę wyciekło, wykrycie niedokładności w systemie zabezpieczania danych oraz określenie działań korygujących i zapobiegawczych wyciekom w przyszłości.



Intelligence Brief

Intelligence Brief 17 October 2017

[redacted] Memo To: Director, Central Intelligence Agency
Deputy Director, Central Intelligence Agency
Chief Operating Officer, Central Intelligence Agency

[redacted]From: WikiLeaks Task Force, [redacted]

[redacted] Subject: WikiLeaks Task Force Final Report

[redacted] Executive Summary

[redacted] WikiLeaks' announcement on 7 March that it possessed cyber tools from CIA's Center for Cyber Intelligence (CCI), dubbed "Vault 7," marked the largest data loss in CIA history. In its initial public disclosure, WikiLeaks provided the names and brief descriptions of multiple tools that CIA developed for cyber operations. Since 7 March, WikiLeaks has published more comprehensive descriptions of 35 tools, including internal CIA documents associated with each tool. [redacted]

— [redacted] We assess that in spring 2016 a CIA employee stole at least 180 gigabytes to as much as 34 terabytes of information. This is roughly equivalent to 11.6 million to 2.2 billion pages in Microsoft Word. This data loss includes [redacted] cyber tools that resided on the Center for Cyber Intelligence (CCI) software development network (DevLAN). We cannot determine the precise scope of the loss because, like other mission systems[a] at that time, DevLAN did not require user activity monitoring or other safeguards that exist on our enterprise system.

— [redacted]

— [redacted] To date, WikiLeaks has released user and training guides and limited source code from two parts of DevLAN: Stash, a source code repository, and Confluence, a collaboration and communication platform. All of the documents reveal, to varying degrees, CIA's tradecraft in cyber operations. [redacted]

[redacted] This product is intended for internal Agency use [redacted]

[a] We define a mission system as any computer-based capability that collects, stores, processes, or communicates information that is managed by a mission component [redacted]

1

[redacted]

Pierwsza strona raportu wewnętrznego zespołu kontrolnego CIA do zbadania sprawy wycieku danych i ich udostępnianiu na portalu WikiLeaks. We wstępnym podsumowaniu ujawniono, że agencja nie jest w stanie określić nawet ilości danych, które wyciekły, ale szacuje się, że było to od 180 GB do 34 TB (2,2 mld stron tekstu w edytorze Word) / Ilustracja: wyden.senate.gov

List senatora Wydena nasuwa wiele pytań, gdyż po pierwsze został upubliczniony i jest dostępny do wglądu w serwisie internetowym Senatu USA, oraz po drugie, co jest jeszcze bardziej zastanawiające, do listu jest dołączony załącznik z fragmentami raportu zespołu WikiLeaks Task Force z CIA. W raporcie brakuje około połowy stron, a pozostałe są często w dużym stopniu zamazane w celu ukrycia tajnych informacji. Jednak w tekście raportu nie utajniono tego, że zespół roboczy nie był nawet w stanie określić ilości danych, które wyciekły – podano liczby od 180 GB do aż 34 TB (2,2 mld typowych stron tekstu). Dane były/są dostępne na wewnętrznej platformie wymiany informacji w CIA zwanej *Confluence* w części *Stash*. Podobno nie wyciekły dane z lepiej strzeżonej części, zwanej *Gold*.

Jednak wyciekły informacje na temat wykorzystywania oprogramowania przełączników sieciowych (*switch*) dostarczanych przez Cisco, co umożliwiało włamywanie się do sieci komputerowych wyposażonych w te urządzenia. Inne narzędzie programistyczne, Sonic Screwdriver, miało służyć do wchodzenia do systemu operacyjnego komputerów Apple Mac w trakcie ich bootowania się. Maki są znane z dużej odporności na ataki hakerskie, ale jak widać ciągle istnieją niedoskonałości w ich oprogramowaniu.

Poza tym stwierdzono nieprzestrzeganie przez wielu agentów CIA podstawowych zasad zachowania tajemnicy służbowej, np. poprzez zaniechania stosowania systemu podwójnego logowania się do sieci, co jest ponoć standardowym wymaganiem w CIA.

W 2018 zarzut zdrady usłyszał były pracownik CIA Joshua Adam Schulte, ale nie przyznał się do winy. W trakcie jego procesu wyszło na jaw, że wielu innych pracowników CIA nie przestrzegało procedur bezpieczeństwa w sieci i ze względu na niemożność uzgodnienia werdyktu przez ławę przysięgłych Schulte nie został skazany.

Trudno nie zauważyć, że wysłanie listu do szefa National Intelligence, jego upublicznienie i co najbardziej zaskakujące, załączenie do niego części raportu z wieloma kompromitującymi CIA stwierdzeniami jej wewnętrznego zespołu kontrolnego, rujnuje reputację Agencję w oczach sojuszników. Niezależnie od tego czy stało się to nieumyślnie czy też jest to jedna z odsłon wewnętrznej walki Demokratów z Republikanami i prezydentem Donaldem Trumpem.
