[Vault 7/8] - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:40:30 UTC

DescriptionAn unnamed source leaked almost 10,000 documents describing a large number of 0-day vulnerabilities, methodologies and tools that had been collected by the CIA's Subgroup: Longhorn, The Lamberts. This leaking was done through WikiLeaks, since March 2017. In weekly publications, the dumps were said to come from Vault 7 and later Vault 8, until his arrest in 2018.

Most of the published vulnerabilities have since been fixed by the respective vendors, but many have been used by other threat actors.

This actor turned out to be a former CIA software engineer.

(WikiLeaks) Today, Tuesday 7 March 2017, WikiLeaks begins its new series of leaks on the U.S. Central Intelligence Agency. Code-named “Vault 7” by WikiLeaks, it is the largest ever publication of confidential documents on the agency.

The first full part of the series, “Year Zero”, comprises 8,761 documents and files from an isolated, high-security network situated inside the CIA’s Center for Cyber Intelligence in Langley, Virgina. It follows an introductory disclosure last month of CIA targeting French political parties and candidates in the lead up to the 2012 presidential election.

Recently, the CIA lost control of the majority of its hacking arsenal including malware, viruses, Trojans, weaponized “zero day” exploits, malware remote control systems and associated documentation. This extraordinary collection, which amounts to more than several hundred million lines of code, gives its possessor the entire hacking capacity of the CIA. The archive appears to have been circulated among former U.S. government hackers and contractors in an unauthorized manner, one of whom has provided WikiLeaks with portions of the archive.

“Year Zero” introduces the scope and direction of the CIA’s global covert hacking program, its malware arsenal and dozens of “zero day” weaponized exploits against a wide range of U.S. and European company products, include Apple’s iPhone, Google’s Android and Microsoft’s Windows and even Samsung TVs, which are turned into covert microphones.
