Mimikatz Malware Overview

Operational (OP) | Fusion (FS)

Cyber Espionage (CE) | Cyber Crime (CC)

February 09, 2017 11:16:00 AM, 17-00001506, Version: 1

DESCRIPTION

Mimikatz is a Windows security audit tool developed by Security Researcher Benjamin Delpy. Mimikatz can be used to steal password hashes and dump plaintext passwords extracted from memory. Mimikatz can dump credentials from LSASS, as well as Kerberos passwords. Linux and Unix systems store Kerberos credentials in a cache file, which Mimikatz can also extract.

RELATED ACTORS

APT24 , Jafar

5950 Berkshire Lane, Suite 1600 Dallas, TX 75225