

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

This message contains content and links to content which are the property of FireEye, Inc. and are protected by all applicable laws. This cyber threat intelligence and this message are solely intended for the use of the individual and organization to which it is addressed and is subject to the subscription Terms and Conditions to which your institution is a party. Onward distribution in part or in whole of any FireEye proprietary materials or intellectual property is restricted per the terms of agreement. By accessing and using this and related content and links, you agree to be bound by the subscription .

For more information please visit: <https://intelligence.fireeye.com/reports/17-00001506>

© 2020, FireEye, Inc. All rights reserved.