22-00007866

View More Details |

MANDIANT ADVANTAGE

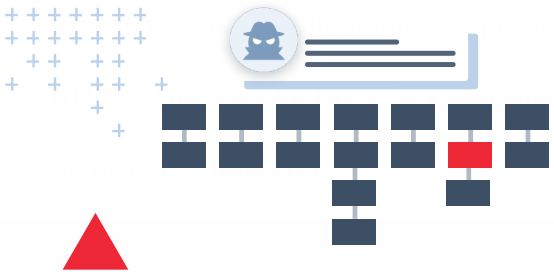
News Analysis

March 24, 2022 12:16:39 PM, 22-00007866

Custom macOS Malware of Chinese Hackers 'Storm Cloud' Exposed

FROM THE MEDIA:

Researchers say they have uncovered a previously unknown piece of macOS malware dubbed "Gimmick" that is believed to be a customized tool leveraged by the China-linked "Storm Cloud" advanced persistent threat (APT) group. According to Veloxity, which uncovered the malware, Gimmick was obtained from the random access memory (RAM) of a MacBook Pro that was compromised in 2021 and operating on macOS 11.6 (Big Sur). Researchers add that Gimmick is multi-platform malware written in Objective C (macOS) or .NET and Delphi (Windows) and that all variants of the malware leverage the same command and control (C2) architecture, behavioral patterns, file paths, and abuse Google Drive services. Gimmick is said to execute directly by users or as a daemon on targeted systems, self-install as a binary called "PLIST," and typically mimics a widely used application on targeted systems. Once executed, Gimmick loads the DriveManager, FileManager, and GCDTimerManager malware components. According to reports, DriveManager manages the Google Drive and proxy sessions, maintains a local map of the in-memory Google Drive directory hierarchy, manages locks used to synchronize tasks on Google Drive session, and handles download and upload tasks to and from Google Drive sessions. According Veloxity, "Due to the asynchronous nature of the malware operation, command execution requires a staged approach. Though the individual steps occur asynchronously, every command follows the same." In order to prevent exploitation by Gimmick, Apple has released new protections that support all macOS versions with new XProtect and



Learn More About the Attack Lifecycle and MITRE ATT&CK

Would you like learn more about the attack lifecycle and MITRE ATT&CK?
Watch these short videos featured from our On-Demand Cyber Intelligence Trainings.

22-00007866

View More Details |

MANDIANT ADVANTAGE

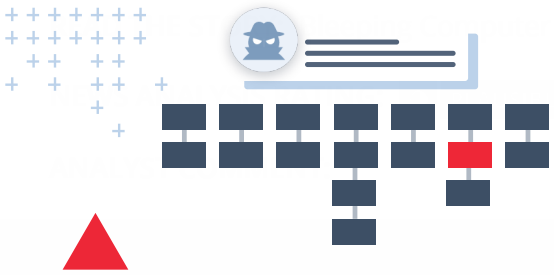
News Analysis

March 24, 2022 12:16:39 PM, 22-00007866

Custom macOS Malware of Chinese Hackers 'Storm Cloud' Exposed

FROM THE MEDIA:

Researchers say they have uncovered a previously unknown piece of macOS malware dubbed "Gimmick" that is believed to be a customized tool leveraged by the China-linked "Storm Cloud" advanced persistent threat (APT) group. According to Veloxity, which uncovered the malware, Gimmick was obtained from the random access memory (RAM) of a MacBook Pro that was compromised in 2021 and operating on macOS 11.6 (Big Sur). Researchers add that Gimmick is multi-platform malware written in Objective C (macOS) or .NET and Delphi (Windows) and that all variants of the malware leverage the same command and control (C2) architecture, behavioral patterns, file paths, and abuse Google Drive services. Gimmick is said to execute directly by users or as a daemon on targeted systems, self-install as a binary called "PLIST," and typically mimics a widely used application on targeted systems. Once executed, Gimmick loads the DriveManager, FileManager, and GCDTimerManager malware components. According to reports, DriveManager manages the Google Drive and proxy sessions, maintains a local map of the in-memory Google Drive directory hierarchy, manages locks used to synchronize tasks on Google Drive session, and handles download and upload tasks to and from Google Drive sessions. According Veloxity, "Due to the asynchronous nature of the malware operation, command execution requires a staged approach. Though the individual steps occur asynchronously, every command follows the same." In order to prevent exploitation by Gimmick, Apple has released new protections that support all macOS versions with new XProtect and



Learn More About the Attack Lifecycle and MITRE ATT&CK

Would you like learn more about the attack lifecycle and MITRE ATT&CK?
Watch these short videos featured from our On-Demand Cyber Intelligence Trainings.