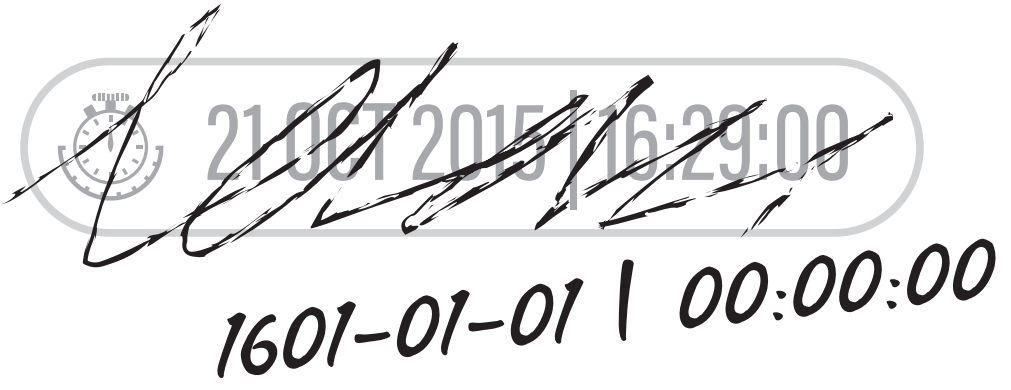
Attackers Timestomp Key Evidence Files

(-3) Modifier for Log-Related Actions

There are tools that allow attackers to modify Modified-Accessed-Created-Entry (MACE) timestamps of files. One such tool is in Metasploit called Timestomp.

NOTES

The attackers can change the MACE for their malware to be in the future. What does this do to your handling of evidence? Can you trust timestamps at all?



Contributed by @davehull

EXPV1_0421

Backdoors™ & Breaches

INJECTS

Created by: BLACK HILLS | Information Security