Abloy Key Manager – Version 7.14301.0.0

March 7th, 2019.

Description: This is a review of Abloy Key Manager (version 7.14301.0.0). The software has suspicious files that can allow adversaries to launch attacks that can allow privilege escalation, load malicious files (hooking[1]), among others.

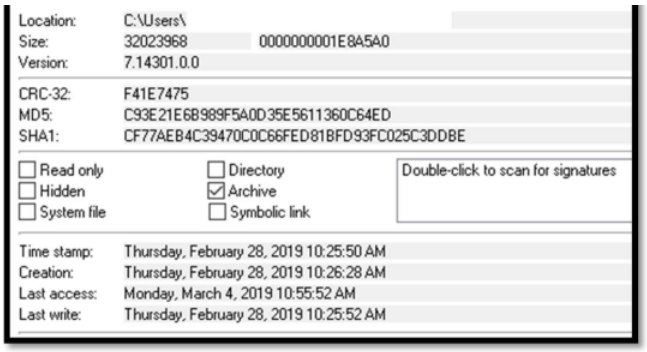
In this software three components were found compromised: KM7Setup.exe[2] sHJdnkvV.exe and ECOCIhtx.exe. These files were labeled as malicious. The main aspects explored included: the capacity to drop executable files, network weakness, and the elevation privilege[3] through weaknesses in the system security (SeChangeNotifyPrivilege).

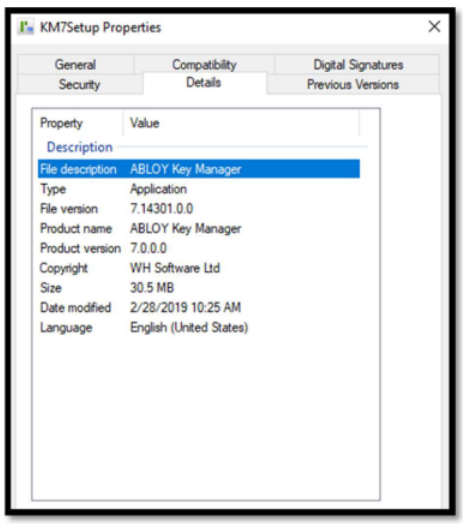
The software open connections through Google and Amazon services, however one network connection seemed suspicious. The network analysis observed that multiple malicious artifacts were in transit through the software and those connections[4].

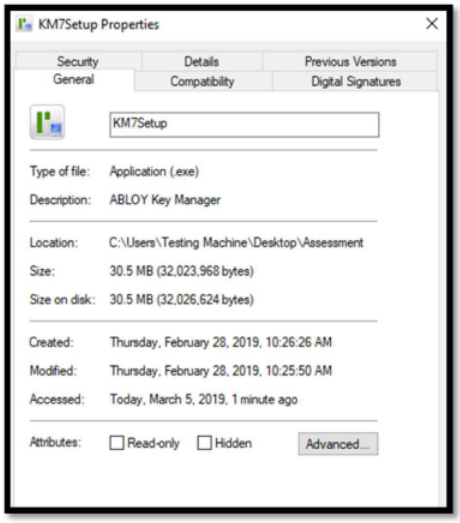
Another security risk is related to an expired certificate that prevents the validation of the software source[5].

[1] https://www.symantec.com/avcenter/reference/windows.rootkit.overview.pdf
[2] https://www.virustotal.com/#/file/2c8d49b7ef16aec4c984664b87713b300d8a06bf82b8967499674397b1565029/details
[3] https://docs.microsoft.com/en-us/windows-hardware/drivers/ifs/elevation-of-privilege
[4] https://www.hybrid-analysis.com/sample/2c8d49b7ef16aec4c984664b87713b300d8a06bf82b8967499674397b1565029/5c7d416903883820949f1f1d
[5] https://comodosslstore.com/resources/how-to-avoid-code-signing-certificate-expired-issues/

File identification

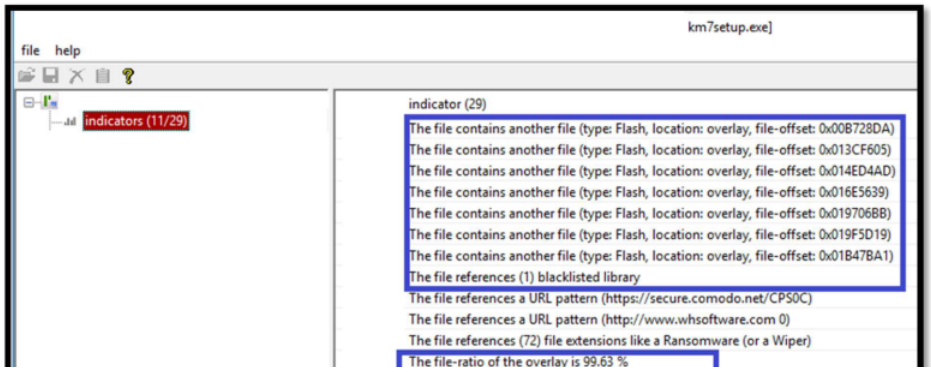


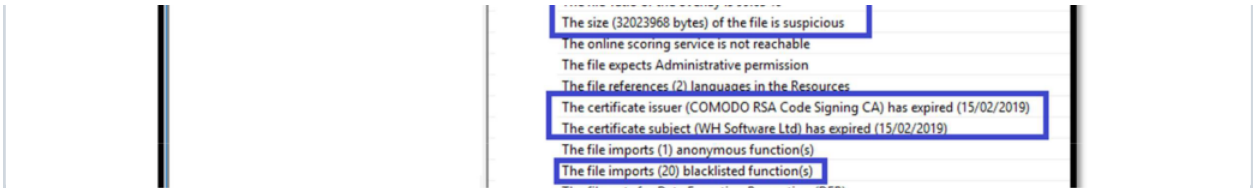




Initial security evaluation

First was identified some weakness such as the reference to another files compression (file-ratio), size, libraries and functions in use by the software.




The size (32023968 bytes) of the file is suspicious
The online scoring service is not reachable
The file expects Administrative permission
The file references (2) languages in the Resources
The certificate issuer (COMODO RSA Code Signing CA) has expired (15/02/2019)
The certificate subject (WH Software Ltd) has expired (15/02/2019)
The file imports (1) anonymous function(s)
The file imports (20) blacklisted function(s)