

master



CVE\_Assessment\_05\_2019 / Key\_Manager\_Report.pdf



GitHubAssessments Add files via upload

History

1 contributor

3.05 MB



## Abloy Key Manager – Version 7.14301.0.0

March 7<sup>th</sup>, 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<sup>1</sup>), among others.

In this software three components were found compromised: KM7Setup.exe<sup>2</sup> 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<sup>3</sup> 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<sup>4</sup>.

Another security risk is related to an expired certificate that prevents the validation of the software source<sup>5</sup>.

<sup>1</sup> <https://www.symantec.com/avcenter/reference/windows.rootkit.overview.pdf>

<sup>2</sup> <https://www.virustotal.com/#/file/2c8d49b7ef16aec4c984664b87713b300d8a06bf82b8967499674397b1565029/details>

<sup>3</sup> <https://docs.microsoft.com/en-us/windows-hardware/drivers/ifs/elevation-of-privilege>

<sup>4</sup> <https://www.hybrid-analysis.com/sample/2c8d49b7ef16aec4c984664b87713b300d8a06bf82b8967499674397b1565029/5c7d416903883820949f1f1d>

<sup>5</sup> <https://comodossstore.com/resources/how-to-avoid-code-signing-certificate-expired-issues/>

### File identification



|  |  |                 |
|--|--|-----------------|
| Location:  | C:\Users\                                |                 |
| Size:  | 32023968                                 | 000000001E8A5A0 |
| Version:   | 7.14301.0.0                              |                 |
| CRC-32:  | F41E7475                                 |                 |
| MD5:   | C93E21E68989F5A0D35E5611360C64ED         |                 |
| SHA1:  | CF77AEB4C39470C0C66FED81BFD93FC025C3DD8E |                 |
| <input type="checkbox"/> Read only <input type="checkbox"/> Directory      Double-click to scan for signatures<br><input type="checkbox"/> Hidden <input checked="" type="checkbox"/> Archive<br><input type="checkbox"/> System file <input type="checkbox"/> Symbolic link |  |                 |
| Time stamp:  | Thursday, February 28, 2019 10:25:50 AM  |                 |
| Creation:  | Thursday, February 28, 2019 10:26:28 AM  |                 |
| Last access:   | Monday, March 4, 2019 10:55:52 AM        |                 |
| Last write:  | Thursday, February 28, 2019 10:25:52 AM  |                 |

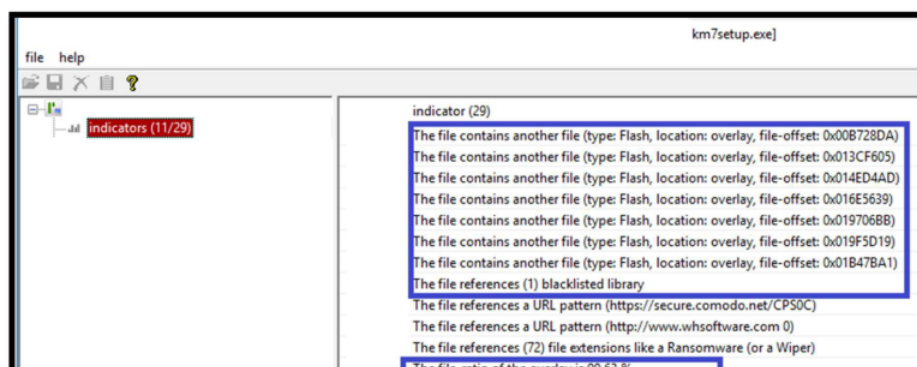
| Property           | Value                   |
|--------------------|-------------------------|
| <b>Description</b> |                         |
| File description   | ABLOY Key Manager       |
| Type               | Application             |
| File version       | 7.14301.0.0             |
| Product name       | ABLOY Key Manager       |
| Product version    | 7.0.0.0                 |
| Copyright          | WH Software Ltd         |
| Size               | 30.5 MB                 |
| Date modified      | 2/28/2019 10:25 AM      |
| Language           | English (United States) |

| KM7Setup      |   |
|---------------|---|
| Type of file: | Application (.exe)  |
| Description:  | ABLOY Key Manager   |
| Location:     | C:\Users\Testing Machine\Desktop\Assessment   |
| Size:         | 30.5 MB (32,023,968 bytes)  |
| Size on disk: | 30.5 MB (32,026,624 bytes)  |
| Created:      | Thursday, February 28, 2019, 10:26:26 AM  |
| Modified:     | Thursday, February 28, 2019, 10:25:50 AM  |
| Accessed:     | Today, March 5, 2019, 1 minute ago  |
| Attributes:   | <input type="checkbox"/> Read-only <input type="checkbox"/> Hidden <span>Advanced...</span> |

2

## 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)