



LOLBAS-Project / LOLBAS Public

Notifications Fork 990 Star 7.1k

<> Code Issues 20 Pull requests 20 Actions Projects Security Insights

LOLBAS / yml / OSBinaries / Wab.yml

28 lines (28 loc) · 992 Bytes

Code Blame Raw Copy Download Toggle

```
1  ---
2  Name: Wab.exe
3  Description: Windows address book manager
4  Author: 'Oddvar Moe'
5  Created: 2018-05-25
6  Commands:
7      - Command: wab.exe
8        Description: Change HKLM\Software\Microsoft\WAB\DLLPath and execute DLL of choice
9        Usecase: Execute dll file. Bypass defensive counter measures
10       Category: Execute
11       Privileges: Administrator
12       MitreID: T1218
13       OperatingSystem: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10
14  Full_Path:
15      - Path: C:\Program Files\Windows Mail\wab.exe
16      - Path: C:\Program Files (x86)\Windows Mail\wab.exe
17  Code_Sample:
18      - Code:
19  Detection:
20      - Sigma: https://github.com/SigmaHQ/sigma/blob/a80c29a7c2e2e500a1a532db2a2a8bd69bd4a63d/rules/wir
21      - IOC: WAB.exe should normally never be used
22  Resources:
23      - Link: https://twitter.com/Hexacorn/status/991447379864932352
24      - Link: http://www.hexacorn.com/blog/2018/05/01/wab-exe-as-a-lolbin/
25  Acknowledgement:
26      - Person: Adam
```

```
27         Handle: '@Hexacorn'
28     ---
```