



Home (<https://www.bleepingcomputer.com/>) > News (<https://www.bleepingcomputer.com/news/>)
> Security (<https://www.bleepingcomputer.com/news/security/>)
> Adobe Acrobat may block antivirus tools from monitoring PDF files

Adobe Acrobat may block antivirus tools from monitoring PDF files

By

Ionut Ilascu
(<https://www.bleepingcomputer.com/author/ionut-ilascu/>)

June 21, 2022

02:44 PM

0



Security researchers found that Adobe Acrobat is trying to block security software from having visibility into the PDF files it opens, creating a security risk for the users.



Adobe's product is checking if components from 30 security products are loaded into its processes and likely blocks them, essentially denying them from monitoring for malicious activity.

Flagging incompatible AVs

For a security tool to work, it needs visibility into all processes on the



PDF files have been abused in the past to execute malware on the system. One method is to add a command in the 'OpenAction' section of document to run PowerShell commands for malicious activity, explain the researchers at cybersecurity company Minerva Labs.

“Since March of 2022 we’ve seen a gradual uptick in Adobe Acrobat Reader processes attempting to query which security product DLLs are loaded into it by acquiring a handle of the DLL” - Minerva Labs (<https://blog.minerva-labs.com/does-acrobat-reader-unload-injection-of-security-products>)

According to a report this week, the list has grown to include 30 DLLs from security products of various vendors. Among the more popular ones with consumers are Bitdefender, Avast, Trend Micro, Symantec, Malwarebytes, ESET, Kaspersky, F-Secure, Sophos, Emsisoft.

Querying the system is done with 'libcef.dll', a Chromium Embedded Framework (CEF) Dynamic Link Library used by a wide variety of programs.

While the Chromium DLL comes with a short list of components to be blacklisted because they cause conflicts, vendors using it can make modifications and add any DLL they want.

```

const char* const kDllBlocklist[kDllBlocklistMaxSize] = {
    "949ba8b6a9.dll",      // Coupon Time.
    "activedetect32.dll",   // Lenovo One Key Theater.
                           // See crbug.com/379218.
    "activedetect64.dll",   // Lenovo One Key Theater.
    "bitguard.dll",        // Unknown (suspected malware).
    "bsvc.dll",            // Unknown (suspected adware).
    "chrmxtn.dll",         // Unknown (keystroke logger).
    "cplushook.dll",       // Unknown (suspected malware).
    "crdli.dll",           // Linkurv Inc.

    "libinject.dll",       // V-Bates.
    "libinject2.dll",      // V-Bates.
    "libredir2.dll",       // V-Bates.
    "libsvn_tsvn32.dll",   // TortoiseSVN.
    "libwinhook.dll",      // V-Bates.
    "lmrn.dll",            // Unknown.
    "minisp.dll",          // Unknown (suspected malware).
    "minisp32.dll",        // Unknown (suspected malware).
    "offerswizadd.dll",    // Unknown (suspected adware).
    "safetynut.dll",       // Unknown (suspected adware).
    "smdmf.dll",           // Unknown (suspected adware).
    "spappsv32.dll",       // Unknown (suspected adware).
    "systemk.dll",         // Unknown (suspected adware).
    "tmmon.dll",           // Trend Micro. See crbug.com/882982
    "tmmon64.dll",         // Trend Micro. See crbug.com/882982
    "tmmonmgr.dll",        // Trend Micro. See crbug.com/882982
    "tmmonmgr64.dll",      // Trend Micro. See crbug.com/882982
    "virtualcamera.ax",    // %PROGRAMFILES%\ASUS\VirtualCamera.
                           // See crbug.com/422522.
    "vntsrv.dll",          // Virtual New Tab by APN LLC.
    "wajam_goblin.dll",    // Wajam Internet Technologies.
    "wajam_goblin_64.dll", // Wajam Internet Technologies.
    "windowsapihookdll32.dll", // Lenovo One Key Theater.
                           // See crbug.com/379218.
    "windowsapihookdll64.dll", // Lenovo One Key Theater.
    "ycwebcamerasource.ax", // CyberLink Youcam, crbug.com/424159
    // Keep this null pointer here to mark the end of the list.
    nullptr,
};

```

Chromium's list of hardcoded DLLs, source: Minerva Labs (<https://blog.minerva-labs.com/does-acrobat-reader-unload-injection-of-security-products>)

The researchers explain that “libcef.dll is loaded by two Adobe processes: **AcroCEF.exe** and **RdrCEF.exe**” so both products are checking the system for components of the same security products.

Looking closer at what happens with the DLLs injected into Adobe processes, Minerva Labs found that Adobe checks if the *bBlockDllInjection* value under the registry key ‘**SOFTWARE\Adobe\Adobe Acrobat\DC\DLLInjection**’ is set to 1. If so, it will prevent antivirus software's DLLs from being injected into processes.

It is worth noting that the registry key's value when Adobe Reader runs for the first time is ‘o’ and that it can be modified at any time.

“With the registry key name **dBlockDllInjection**, and looking at the cef documentation (<https://chromium.googlesource.com/chromium/src/>), we can assume that the the blacklisted DLLs are designated to be unloaded” - Minerva Labs

According to Minerva Labs researcher Natalie Zargarov, the default value for the registry key is set to '1' - indicating active blocking. This setting may depend on the operating system or the Adobe Acrobat version installed, as well as other variables on the system.



E%2520-%2520WINDOWS%26ADPT%3DITL_LITRIPLELIFT%26IPL%3DBLEEPINGCOMPUTER

mlang%3D%26did%3Dtlx532%26rcxt%3DOther%26tmpc%3D
0dGRfZGF0YV9leGNsdXNpb25zCkcKJ2NoYXJnZS1hbGxJYX

In a post on Citrix forums (<https://discussions.citrix.com/topic/412451-just-grey-screen-instead-of-published-desktop/page/7/#comment-2089464>) on March 28, a user complaining about Sophos AV errors due to having an Adobe product installed said that the company “suggested to disable DLL-injection for Acrobat and Reader.

- Adobe suggested to disable DLL-injection for Acrobat and Reader. You need need the newest version for this. Adobe had a lot of trouble with DLL injection from some AV vendors. Sadly Sophos or Citrix was not on there list.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Adobe\Adobe Acrobat\DC\DLLInjection] "bBlockDLLInjection"=01
[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Adobe\Adobe Acrobat\DC\DLLInjection] "bBlockDLLInjection"=01
[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Adobe\Acrobat Reader\DC\DLLInjection] "bBlockDLLInjection"=01
```

4) Adding AcroCef.exe and RdrCEF.exe to HKLM\SYSTEM\CurrentControlSet\Services\CtxUui\UuiProcessExcludes solves the problem. After around 700 reboots the error didn't occur.

Adobe added AcroCef.exe and RdrCEF.exe some month ago.

Adobe responding to Citrix user experiencing errors on machine with Sophos AV

Working on the problem

Replying to BleepingComputer, Adobe confirmed that users have reported experiencing issue due to DLL components from some security products being incompatible with Adobe Acrobat's usage of the CEF library.

“We are aware of reports that some DLLs from security tools are incompatible with Adobe Acrobat’s usage of CEF, a Chromium based engine with a restricted sandbox design, and may cause stability issues” - Adobe

The company added that it is currently working with these vendors to address the problem and “to ensure proper functionality with Acrobat's CEF sandbox design going forward.”

Minerva Labs researchers argue that Adobe chose a solution that solves compatibility problems but introduces a real attack risk by preventing security software from protecting the system.



BleepingComputer has contacted Adobe with further questions to explain the conditions the DLL blocking occurs and will update the article once we have the information.

Related Articles:



Fake antivirus updates used to deploy Cobalt Strike in Ukraine
(<https://www.bleepingcomputer.com/news/security/fake-antivirus-updates-used-to-deploy-cobalt-strike-in-ukraine/>)

Trend Micro fixes bug Chinese hackers exploited for espionage
(<https://www.bleepingcomputer.com/news/security/trend-micro-fixes-bug-chinese-hackers-exploited-for-espionage/>)

PDF smuggles Microsoft Word doc to drop Snake Keylogger malware
(<https://www.bleepingcomputer.com/news/security/pdf-smuggles-microsoft-word-doc-to-drop-snake-keylogger-malware/>)

Sophos antivirus driver caused BSODs after Windows KB5013943 update
(<https://www.bleepingcomputer.com/news/software/sophos-antivirus-driver-caused-bsods-after-windows-kb5013943-update/>)

.....

- ADOBE ([HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/ADOBE/](https://www.bleepingcomputer.com/tag/adobe/))
- ADOBE ACROBAT ([HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/ADOBE-ACROBAT/](https://www.bleepingcomputer.com/tag/adobe-acrobat/))
- ADOBE READER ([HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/ADOBE-READER/](https://www.bleepingcomputer.com/tag/adobe-reader/))
- ANTIVIRUS ([HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/ANTIVIRUS/](https://www.bleepingcomputer.com/tag/antivirus/))
- DLL ([HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/DLL/](https://www.bleepingcomputer.com/tag/dll/))
- LIBRARY ([HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/LIBRARY/](https://www.bleepingcomputer.com/tag/library/))
- PDF ([HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/PDF/](https://www.bleepingcomputer.com/tag/pdf/))

.....

