DLL Hijacking Overview

Joas Antonio

About the PDF

+A PDF overview of DLL Hijacking and related Techniques

+https://www.linkedin.com/in/joas-antonio-dos-santos

What is DLL?

+https://stackoverflow.com/questions/124549/what-exactly-are-dll-files-and-how-do-they-work

+https://en.wikipedia.org/wiki/Dynamic-link_library

+https://www.lifewire.com/what-is-a-dll-file-2625852

+https://www.britannica.com/technology/DLL

+https://www.youtube.com/watch?v=YmVDJ1HA_8s&ab_channel=srcmake

+https://www.tutorialspoint.com/dll/index.htm

Programming DLL

+ https://www.youtube.com/watch?v=fzO9L6tlXDI&ab_channel=InfernoDevelopment0
+ https://www.youtube.com/watch?v=Q3T160hhUpk&ab_channel=AlisterChristie
+ https://www.codeguru.com/cplusplus/dll-tutorial-for-beginners/
+ https://wiki.dlang.org/Win32_DLLs_in_D
+ https://www.youtube.com/watch?v=auNPlHYB4ss&ab_channel=Code%2CTech%2CandTutorials
+ https://www.youtube.com/watch?v=ktbIIvXzypU&ab_channel=TommyNgo
+ http://programmingexamples.wikidot.com/blog:1
+ https://aticleworld.com/how-to-create-and-use-dll-dynamic-link-library-in-c/
+ https://khalil-o.medium.com/simple-way-of-creating-c-c-dll-dynamic-link-library-9e7e5145bf63
+ https://stackoverflow.com/questions/49402415/how-to-create-a-dll-library-in-c-and-then-use-it-in-c-project-visualstudio
+ https://knowledge.ni.com/KnowledgeArticleDetails?id=kA03q000000x1OvCAI&l=en-US

Windows Internals

+ https://docs.microsoft.com/en-us/sysinternals/resources/windows-internals
+ https://www.youtube.com/watch?v=4AkzIbmI3q4&ab_channel=TheSourceLens
+ https://www.youtube.com/watch?v=YqfMpoOKEkA&ab_channel=TheSourceLens
+ https://www.youtube.com/watch?v=qMWvqdtlbkQ&ab_channel=Moss%C3%A9CyberSecurityInstitute
+ https://repo.zenk-security.com/Linux%20et%20systemes%20d.exploitations/Windows%20Internals%20Part%201_6th%20Edition.pdf
+ https://medium.com/@0xdeadbeefJERKY/windows-internals-course-review-7001bfdf335e
+ https://techcommunity.microsoft.com/t5/windows-blog-archive/windows-internals-5th-edition-is-available/ba-p/723826

What is DLL Hijacking?

+ https://www.upguard.com/blog/dll-hijacking
+ https://attack.mitre.org/techniques/T1574/001/
+ https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows
+ https://itm4n.github.io/windows-dll-hijacking-clarified/
+ https://blog.finjan.com/best-practices-to-prevent-dll-hijacking/
+ https://pentestlab.blog/2017/03/27/dll-hijacking/
+ https://resources.infosecinstitute.com/topic/dll-hijacking-attacks-revisited/
+ https://medium.com/techzap/dll-hijacking-part-1-basics-b6dfb8260cf1
+ https://resources.infosecinstitute.com/topic/dll-hijacking/
+ https://www.youtube.com/watch?v=2l_U4pvaFRg&ab_channel=Infosec

DLL Hijacking - Techniques

+ https://book.hacktricks.xyz/windows/windows-local-privilege-escalation/dll-hijacking
+ https://www.ired.team/offensive-security/privilege-escalation/t1038-dll-hijacking
+ https://www.cyberark.com/resources/threat-research-blog/dllspy-tighten-your-defense-by-discovering-dll-hijacking-easily
+ https://cyware.com/news/dll-hijacking-attacks-what-is-it-and-how-to-stay-protected-5056c0f0
+ https://posts.specterops.io/automating-dll-hijack-discovery-81c4295904b0
+ https://www.fireeye.com/blog/threat-research/2020/01/abusing-dll-misconfigurations.html
+ https://macrosec.tech/index.php/2021/05/13/persistence-part-2-common-userland-techniques-dll-and-com-hijacking/
+ https://www.giac.org/paper/gcda/141/detecting-dll-search-order-hijacking-purple-team-approach-create-defensive-techniques-tactical-siem/163896
+ https://repo.zenk-security.com/Techniques%20d.attaques%20%20.%20%20Failles/Dynamic-Link%20Library%20Hijacking.pdf

DLL Hijacking - Techniques

+ https://lucabarile.github.io/Blog/dll_hijacking_and_proxying/index.html
+ https://www.cybereason.com/siofra-research-tool-cybereason
+ https://reposhub.com/python/security/wietze-windows-dll-hijacking.html
+ https://github-dotcom.gateway.web.tr/rek7/dll-hijacking
+ https://www.netspi.com/blog/technical/adversary-simulation/adaptive-dll-hijacking/
+ https://colab.research.google.com/github/OTRF/ThreatHunter-Playbook/blob/master/docs/notebooks/windows/02_execution/WIN-201009173318.ipynb
+ https://milosilo.com/hacking/microsoft-teams-proxy-dll-hijacking/
+ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40444
+ https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40444
+ https://github.com/klezVirus/CVE-2021-40444
+ https://github.com/lockedbyte/CVE-2021-40444
+ https://github.com/aslitsecurity/CVE-2021-40444_builders
+ https://www.youtube.com/watch?v=e_l5TCgw3wo

DLL Hijacking - Tools

+ https://github.com/tothi/dll-hijack-by-proxying
+ https://github.com/carlospolop/hacktricks/blob/master/windows/windows-local-privilege-escalation/dll-hijacking.md
+ https://github.com/wietze/windows-dll-hijacking
+ https://github.com/ctxis/DLLHSC
+ https://github.com/cyberark/DLLSpy
+ https://github.com/InoriJam/DLL-hijack-X64
+ https://github.com/MojtabaTajik/Robber
+ https://www.youtube.com/watch?v=WeKEj8pGrwQ&ab_channel=RaghavBisht
+ https://www.youtube.com/watch?v=EeztydiJTeU&ab_channel=EricRomang

DLL Loader/Injection

+ https://github.com/itm4n/UsoDllLoader
+ https://github.com/m0nad/awesome-privilege-escalation
+ https://github.com/knight0x07/ImpulsiveDLLHijack
+ https://attack.mitre.org/techniques/T1055/001/
+ https://www.apriorit.com/dev-blog/679-windows-dll-injection-for-api-hooks
+ https://medium.com/bug-bounty-hunting/dll-injection-attacks-in-a-nutshell-71bc84ac59bd
+ https://www.ired.team/offensive-security/code-injection-process-injection/dll-injection
+ https://www.systemconf.com/2020/07/27/what-is-dll-injection-and-how-does-dll-injection-work/
+ http://blog.opensecurityresearch.com/2013/01/windows-dll-injection-basics.html
+ https://imasters.com.br/desenvolvimento/advanced-dll-injection
+ https://www.youtube.com/watch?v=IBwoVUR1gt8

DLL Loader/Injection

+ https://github.com/KooroshRZ/Windows-DLL-Injector
+ https://guidedhacking.com/threads/dll-injection-methods.14569/?__cf_chl_jschl_tk__=pmd_50b144f3d4e08c896c068d4a726d10e4a7b3535c-1633295464-0-gqNtZGzNAjijcnBszQki
+ https://resources.infosecinstitute.com/topic/using-createremotethread-for-dll-injection-on-windows/
+ https://github.com/AYIDouble/Simple-DLL-Injection
+ https://github.com/baltuky/simple-dll-injection
+ https://github.com/dismantl/ImprovedReflectiveDLLInjection
+ https://github.com/Akaion/Bleak
+ https://github.com/0xDivyanshu/Injector
+ https://github.com/3xpl01tc0d3r/ProcessInjection
+ https://github.com/enkomio/ManagedInjector
+ https://github.com/Arvanaghi/Windows-DLL-Injector
+ https://github.com/DarthTon/Xenos
+ https://github.com/UserExistsError/InjectDll
+ https://github.com/gfreivasc/jadi
+ https://github.com/kubo/injector

DLL Loader

+ https://ivankahl.com/using-reflection-to-execute-assemblies-at-runtime-in-c/
+ https://www.youtube.com/watch?v=33J7L9anesM&ab_channel=Diallix%C2%B4s
+ https://www.andreafortuna.org/2017/12/08/what-is-reflective-dll-injection-and-how-can-be-detected/
+ https://visualstudiomagazine.com/articles/2011/09/01/pcnet_dynamicload-runtime.aspx
+ https://powershell.one/tricks/assemblies/load-from-memory
+ https://docs.microsoft.com/en-us/dotnet/framework/app-domains/how-to-load-assemblies-into-an-application-domain
+ https://stackoverflow.com/questions/14479074/c-sharp-reflection-load-assembly-and-invoke-a-method-if-it-exists
+ https://stackoverflow.com/questions/27141658/load-dependent-dll-using-reflection
+ https://stackoverflow.com/questions/13678528/c-sharp-reflection-load-external-dlls-and-all-dependencies
+ https://attack.mitre.org/techniques/T1055/
+ http://lallouslab.net/2017/05/15/7-dll-injection-techniques-in-the-microsoft-windows/
+ https://medium.com/@ozan.unal/process-injection-techniques-bc6396929740

DLL Attacks Talks

+ https://i.blackhat.com/USA-19/Thursday/us-19-Kotler-Process-Injection-Techniques-Gotta-Catch-Them-All.pdf
+ https://i.blackhat.com/USA-19/Thursday/us-19-Kotler-Process-Injection-Techniques-Gotta-Catch-Them-All-wp.pdf
+ https://www.blackhat.com/presentations/bh-usa-07/Butler_and_Kendall/Presentation/bh-usa-07-butler_and_kendall.pdf
+ https://www.blackhat.com/docs/asia-17/materials/asia-17-KA-What-Malware-Authors-Don't-Want-You-To-Know-Evasive-Hollow-Process-Injection.pdf
+ https://i.blackhat.com/eu-19/Thursday/eu-19-Block-Detecting-Un-Intentionally-Hidden-Injected-Code-By-Examining-Page-Table-Entries.pdf
+ https://www.blackhat.com/presentations/bh-dc-08/McFeters-Rios-Carter/Presentation/bh-dc-08-mcfeters-rios-carter.pdf
+ https://www.blackhat.com/docs/us-16/materials/us-16-Yavo-Captain-Hook-Pirating-AVs-To-Bypass-Exploit-Mitigations-wp.pdf
+ https://i.blackhat.com/USA21/Wednesday-Handouts/us-21-Rope-Bypassing-Behavioral-Detection-Of-Malware-With-Distributed-ROP-Driven-Execution-wp.pdf
+ https://www.blackhat.com/presentations/win-usa-04/bh-win-04-aitel.pdf
+ https://www.blackhat.com/presentations/bh-usa-04/bh-us-04-tsyrklevich.pdf
+ https://www.blackhat.com/docs/us-15/materials/us-15-Mulliner-Breaking-Payloads-With-Runtime-Code-Stripping-And-Image-Freezing.pdf
+ https://i.blackhat.com/briefings/asia/2018/asia-18-Tal-Liberman-Documenting-the-Undocumented-The-Rise-and-Fall-of-AMSI.pdf

DLL Attacks Talks

+ https://www.youtube.com/watch?v=xewv122qxnk&ab_channel=BlackHat
+ https://www.youtube.com/watch?v=PGVNja2MNws&ab_channel=DEFCONConference
+ https://www.youtube.com/watch?v=FJOVLt1irME&ab_channel=MotasemHamdan
+ https://www.youtube.com/watch?v=jFZ8Zf5ZER8&ab_channel=SANSOffensiveOperations
+ https://www.youtube.com/watch?v=PjuzQI21PVE&ab_channel=SamBowne
+ https://www.youtube.com/watch?v=9-HNMUo9urA&ab_channel=MotasemHamdan
+ https://www.youtube.com/watch?v=KJPeZptzl1U&ab_channel=Z.CliffeSchreuders

DLL Tutorials

+ https://www.youtube.com/watch?v=Xd_egp8WeKE&ab_channel=LiveOverflow
+ https://www.youtube.com/watch?v=_PGhvUHFRlQ&ab_channel=SamBowne
+ https://www.youtube.com/watch?v=W_I90E87WlE&ab_channel=Socversity
+ https://www.youtube.com/watch?v=sLXhzxiLZ4U&ab_channel=xct
+ https://www.youtube.com/watch?v=qwWvpPNTOUc&ab_channel=PapoBin%C3%A1rio
+ https://www.youtube.com/watch?v=uzmKLqx_R1k&ab_channel=PentesterAcademyTV

+ https://www.youtube.com/watch?v=osu2Vodwm0U&ab_channel=applemacattack
+ https://www.youtube.com/watch?v=1ErymFEn3rg&ab_channel=Rvn0xsy
+ https://www.youtube.com/watch?v=PEMkcbY8U9o&ab_channel=GuidedHacking