OVERVIEW – WINDOWS API'S AND INTERNALS & REVERSE ENGINEERING

Joas Antonio

SOBRE O OVERVIEW

- Conteúdos sobre conceitos de Windows Internals e API'S
- Auxilia-lo nos seus estudos em Engenharia Reversa & Analise de Malware
- De entusiastas para entusiastas
- Overview e conteúdos utilizados para estudos e práticas

AUTOR

- Joas Antonio
- My LinkedIn: https://www.linkedin.com/in/joas-antonio-dos-santos/ ☺

WINDOWS INTERNALS, API'S, REVERSE ENGINEERING AND MALWARE ANALYSIS

WINDOWS INTERNALS

- System Architecture;
- Processes;
- Threads;
- Memory Management;
- https://docs.microsoft.com/en-us/sysinternals/resources/windows-internals
- https://www.amazon.com.br/Windows-Internals-Book-User-Mode/dp/0735684189
- https://www.amazon.com.br/Windows-Internals-Part-architecture-management-ebook/dp/B0711FDMRR
- https://www.youtube.com/watch?v=qMWvqdtlbkQ
- https://www.youtube.com/watch?v=4AkzIbmI3q4&list=PLhx7-txsG6t5i-kIZ_hwJSgZrnka4GXvn&ab_channel=TheSourceLens
- https://scorpiosoftware.net/2020/01/03/next-windows-internals-remote-training/

WINDOWS INTERNALS: SYSTEM ARCHITECTURE

- https://medium.com/@putrasulung2108/windows-architecture-d2b022f136d3
- https://techcommunity.microsoft.com/t5/ask-the-performance-team/windows-architecture-the-basics/ba-p/372345
- https://en.wikipedia.org/wiki/Architecture_of_Windows_NT#:~:text=The%20architecture%20of%20Windows%20NT,user%20mode%20and%20kernel%20mode.&text=Kernel%20mode%20in%20Windows%20NT,system%20resources%20of%20the%20computer.
- https://pt.slideshare.net/StacksoI/windows-architecture-explained-by-stacksol
- https://www.cs.mcgill.ca/~rwest/wikispeedia/wpcd/wp/a/Architecture_of_Windows_NT.htm
- http://etutorials.org/Microsoft+Products/microsoft+windows+server+2003+terminal+services/Chapter+1+The+Concept+of+Terminal+Services/System+Architecture/
- https://www.youtube.com/watch?v=UzIMU2VpZSY
- https://www.cs.fsu.edu/~zwang/files/cop4610/Fall2016/windows.pdf

WINDOWS INTERNALS: PROCESSES AND THREADS

- https://docs.microsoft.com/en-us/windows/win32/procthread/processes-and-threads
- https://www.howtogeek.com/405806/windows-task-manager-the-complete-guide/
- https://docs.microsoft.com/en-us/windows-hardware/drivers/kernel/windows-kernel-mode-process-and-thread-manager
- https://www.tenouk.com/ModuleT.html
- http://www.hasanbalik.com/LectureNotes/OpSys/Assignments/MS%20Windows%2010%20Process%20and%20Thread%20%20Management.pdf
- https://www.microsoftpressstore.com/articles/article.aspx?p=2233328&seqNum=7

WINDOWS INTERNALS: MEMORY MANAGEMENT

- https://www.youtube.com/watch?v=AjTI53I_qzY
- https://www.youtube.com/watch?v=nsWkIEuhRmM
- https://www.youtube.com/watch?v=qIH4-oHnBb8
- https://www.youtube.com/watch?v=59rEMnKWoS4
- https://www.youtube.com/watch?v=p9yZNLeOj4s
- https://www.youtube.com/watch?v=qdkxXygc3rE
- https://www.tutorialspoint.com/operating_system/os_memory_management.htm
- https://docs.microsoft.com/en-us/windows/win32/memory/about-memory-management
- https://en.wikipedia.org/wiki/Memory_management
- https://www.codeproject.com/Articles/29449/Windows-Memory-Management
- http://www.cs.sjtu.edu.cn/~kzhu/cs490/9/9_MemMan.pdf
- https://pt.slideshare.net/Tech_MX/windows-memory-management

O QUE É WINDOWS API

- A **Windows API**, informalmente **WinAPI**, é um conjunto base de interfaces de programação (API) para o sistema operacionais Microsoft Windows
- O nome API do Windows refere-se coletivamente a várias implementações de plataforma diferentes que costumam ser chamadas por seus próprios nomes (por exemplo, **API do Win32**). Quase todos os programas do Windows interagem com a API do Windows. Na linha de sistemas operacionais Windows NT, um pequeno número (como programas iniciados no início do processo de inicialização do Windows) usa a API nativa.

https://en.wikipedia.org/wiki/Windows_API

O QUE É WINDOWS API

- O suporte ao desenvolvedor está disponível na forma de um kit de desenvolvimento de software , Microsoft Windows SDK , fornecendo documentação e ferramentas necessárias para construir software baseado na API do Windows e interfaces do Windows associadas.
- A API do Windows (Win32) está focada principalmente na linguagem de programação C em que suas funções expostas e estruturas de dados são descritas naquela linguagem em versões recentes de sua documentação. No entanto, a API pode ser usada por qualquer compilador de linguagem de programação capaz de lidar com as estruturas de dados de baixo nível (bem definidas).

https://en.wikipedia.org/wiki/Windows_API

FUNÇÕES DO WINAPI

- As funções fornecidas pela API do Windows podem ser agrupadas em oito categorias:

Serviços de Base

[6] Fornece acesso aos recursos básicos disponíveis para um sistema Windows. Estão incluídos itens como sistemas de arquivos , dispositivos , processos , threads e tratamento de erros . Essas funções residem em`kernel.exe`, `krnl286.exe` ou `krnl386.exe` arquivos no Windows de 16 bits e `kernel32.dll` e `KernelBase.dll`em Windows de 32 e 64 bits. Esses arquivos residem na pasta`\ Windows \ System32` em todas as versões do Windows.

Serviços Avançados

Fornece acesso a funções além do kernel. Estão incluídos itens como o registro do Windows , desligar / reiniciar o sistema (ou abortar), iniciar / parar / criar um serviço do Windows , gerenciar contas de usuário. Essas funções residem em`advapi32.dll` e `advapires32.dll` no Windows de 32 bits.

Interface de dispositivo gráfico

[7] Oferece funções de saída de conteúdo gráfico para monitores , impressoras e outros dispositivos de saída . Reside em`gdi.exe` no Windows de 16 bits e `gdi32.dll`no Windows de 32 bits no modo de usuário. O suporte GDI do modo kernel é fornecido pelo `win32k.sys` qual se comunica diretamente com o driver gráfico. [8]

Interface de usuário

[9] Fornece as funções para criar e gerenciar janelas de telae a maioria dos controles básicos, como botões e barras de rolagem , receber entrada de mouse e teclado e outras funções associadas à interface gráfica do usuário (GUI) parte do Windows. Esta unidade funcional reside em`user.exe` no Windows de 16 bits e `user32.dll`no Windows de 32 bits. Desde as versões do Windows XP , os controles básicos residem em`comctl32.dll`, junto com os controles comuns (Biblioteca de controle comum).

Biblioteca de caixa de diálogo comum

[10] Fornece aos aplicativos as caixas de diálogo padrãopara abrir e salvar arquivos, escolher cor e fonte, etc. A biblioteca reside em um arquivo chamado`commdlg.dll` no Windows de 16 bits e `comdlg32.dll`no Windows de 32 bits. Ele é agrupado na categoria *Interface* do *usuário* da API.

Biblioteca de controle comum

[11] Dá aos aplicativos acesso a alguns controles avançados fornecidos pelo sistema operacional. Isso inclui coisas como barras de status , barras de progresso , barras de ferramentas e guias . A biblioteca reside em umarquivo de biblioteca de vínculo dinâmico (DLL) chamado`commctrl.dll` no Windows de 16 bits e `comctl32.dll`no Windows de 32 bits. Ele é agrupado na categoria *Interface* do *usuário* da API.

Shell do Windows

[12] [13] O componente da API do Windows permite que os aplicativos acessem funções fornecidas pelo shell do sistema operacional e alterem e aprimorem-no. O componente reside em`shell.dll` no Windows de 16 bits e `shell32.dll`no Windows de 32 bits. As funções do utilitário Shell Lightweight estão em`shlwapi.dll`. Ele é agrupado na categoria *Interface* do *usuário* da API.

Serviços de rede

[14] Dê acesso às váriascapacidades de rede do sistema operacional. Seus subcomponentes incluem NetBIOS , Winsock , NetDDE , chamada de procedimento remoto (RPC) e muitos mais. Este componente reside em`netapi32.dll` no Windows de 32 bits.

https://en.wikipedia.org/wiki/Windows_API

WINAPI NO INTERNET EXPLORER

- O navegador Internet Explorer (IE) também expõe muitas APIs que são frequentemente usadas por aplicativos e, como tal, podem ser consideradas parte da API do Windows. O IE foi incluído com o sistema operacional desde o Windows 95 OSR2 e fornece serviços relacionados à web para aplicativos desde o Windows 98. Especificamente, é usado para fornecer:

1. Um controle de navegador da web incorporável, contido em shdocvw.dll e mshtml.dll.
2. O serviço de URL Moniker, mantido em urlmon.dll, que fornece objetos COM a aplicativos para resolução de URLs. Os aplicativos também podem fornecer seus próprios manipuladores de URL para outros usarem.
3. Uma biblioteca de cliente HTTP que também leva em consideração as configurações de proxy de todo o sistema (wininet.dll); entretanto, a Microsoft adicionou outra biblioteca de cliente HTTP chamada winhttp.dll que é menor e mais adequada para alguns aplicativos.
4. Uma biblioteca para auxiliar no suporte de texto internacional e multilíngue (mlang.dll).
5. Transformações DirectX, um conjunto de componentes de filtro de imagem.
6. Suporte a XML (os componentes MSXML, mantidos em msxml * .dll)
7. Acesso aos catálogos de endereços do Windows.

https://en.wikipedia.org/wiki/Windows_API

FUNÇÕES IMPORTANTES PARA BREAKPOINTS (ER)

- https://docs.microsoft.com/pt-br/dotnet/framework/unmanaged-api/hosting/lpthread-start-routine-function-pointer
- https://mentebinaria.gitbook.io/engenharia-reversa/apendices/funcoes-api-win
- https://stackoverflow.com/questions/3080624/debug-break-on-win32-api-functions (example)
- https://docs.microsoft.com/en-us/visualstudio/debugger/how-can-i-debug-windows-api-functions-q?view=vs-2019
- https://docs.microsoft.com/en-us/windows/win32/apiindex/windows-api-list (Windows API List)
- https://www.vbmigration.com/BookChapters/ProgrammingVB6_AppA.pdf
- http://zetcode.com/gui/winapi/system/

FUNÇÕES WINAPI

- https://docs.revenera.com/installshield26helplib/helplibrary/CallingWindowsAPIFunction.htm
- https://medium.com/@dmitriykim/writing-about-windows-api-functions-in-powershell-b03d3abb0862
- http://www.lahey.com/docs/lfenthelp/F95UGMLPDLLWinAPI.htm
- https://edn.embarcadero.com/article/10323
- http://vig.pearsoned.com/samplechapter/0321262506.pdf
- https://zorro-project.com/manual/en/litec_api.htm
- https://riptutorial.com/winapi
- https://www.youtube.com/watch?v=zOSb8y0eABE&ab_channel=PapoBin%C3%A1rio
- https://www.youtube.com/watch?v=rIoD6wWINto&ab_channel=b1nch3f

PENTEST WINDOWS API

- https://medium.com/@int0x33/day-59-windows-api-for-pentesting-part-1-178c6ba280cb (PenTest Windows API)
- https://www.youtube.com/watch?v=8XpVsb44YHA
- https://www.youtube.com/watch?v=BkiWUqaIpNI&ab_channel=PentesterAcademyTV
- https://www.youtube.com/watch?v=EUk0uYNnwVQ&ab_channel=HackYourLives
- https://www.youtube.com/watch?v=bdUT20fwwfI&ab_channel=HackersSecurity
- https://www.youtube.com/watch?v=mOgVTrzgpXQ

REVERSE ENGINEERING FOR WINDOWS API'S

- https://darungrim.com/research/2020-06-17-using-frida-for-windows-reverse-engineering.html
- https://reverseengineering.stackexchange.com/questions/1603/windows-api-reference-for-ollydbg
- https://www.blackhat.com/presentations/bh-jp-08/bh-jp-08-Aiko/bh-jp-08-Aiko-EN.pdf
- https://www.apriorit.com/dev-blog/364-how-to-reverse-engineer-software-windows-in-a-right-way
- https://rstforums.com/forum/topic/95272-the-windows-api-for-hackers-and-reverse-engineers/
- http://rce4fun.blogspot.com/2014/01/introduction-to-windows-api-hooking.html
- https://www.youtube.com/watch?v=FgJpNspdQP0
- https://www.youtube.com/watch?v=e1ejxu9B0dc
- https://www.youtube.com/watch?v=pxKRkUFBpyY
- http://www.cse.hut.fi/fi/opinnot/T-110.6220/2015_Reverse_Engineering_Malware_AND_Software_Security/luennot-files/t1106220.pdf

MICROSOFT CRYPTOAPI - EXAMPLE

- **Cryptographic Application Programming Interface**, em português **Interface de Programação de Aplicativos Criptográficos**, também conhecida como **CryptoAPI**, **Microsoft Cryptography API**, **MS-CAPI** ou simplesmente **CAPI**, é uma interface de programação de aplicativos, específica para plataforma Microsoft Windows, incluída com os sistemas operacionais Microsoft Windows, que fornece serviços para permitir que os desenvolvedores protejam aplicativos baseados no Windows usando criptografia. Ela é um conjunto de bibliotecas vinculadas dinamicamente que fornecem uma camada de abstração que isola os programadores do código usado para criptografar os dados. A CryptoAPI foi introduzida pela primeira vez no Windows NT 4.0 e aprimorada nas versões subsequentes.
- CryptoAPI suporta criptografia de chave pública e de chave simétrica, embora chaves simétricas persistentes não sejam suportadas. Inclui funcionalidade para criptografar e descriptografar dados e para autenticação usando certificados digitais. Ele também inclui uma função geradora de número pseudo-aleatório criptograficamente segura CryptGenRandom.
- A CryptoAPI funciona com vários PSCs (Provedores de Serviços de Criptografia) instalados na máquina. Os PSCs são os módulos que fazem o trabalho real de codificação e decodificação de dados executando as funções criptográficas. Os fornecedores de HSMs podem fornecer um PSC que funcione com seu hardware.
- https://pt.wikipedia.org/wiki/Microsoft_CryptoAPI

MICROSOFT CRYPTOAPI - EXAMPLE

- https://github.com/abhishekpandey13/windbg-tracer
- https://www.namecoin.org/2017/05/27/reverse-engineering-cryptoapi-cert-blobs.html
- https://tehtris.com/en/cve-2020-0601-vulnerability-in-the-cryptoapi-of-windows-crypt32-dll/

REVERSE ENGINEERING IN WINDOWS AND WINAPI

- https://github.com/abhishekpandey13/windbg-tracer
- https://www.namecoin.org/2017/05/27/reverse-engineering-cryptoapi-cert-blobs.html
- https://tehtris.com/en/cve-2020-0601-vulnerability-in-the-cryptoapi-of-windows-crypt32-dll/
- https://i.blackhat.com/USA-19/Thursday/us-19-Kotler-Process-Injection-Techniques-Gotta-Catch-Them-All-wp.pdf
- https://www.blackhat.com/docs/sp-14/materials/arsenal/sp-14-Almeida-Bypassing-the-Secure-Desktop-Protections-Slides.pdf
- https://www.youtube.com/watch?v=6um4tgmMdOk
- https://www.youtube.com/watch?v=LvW68czaEGs
- https://www.youtube.com/watch?v=7A_rgu3kbvw

REVERSE ENGINEERING - DUBNIUM

- https://www.microsoft.com/security/blog/2016/06/09/reverse-engineering-dubnium-2/
- https://www.microsoft.com/security/blog/2016/07/14/reverse-engineering-dubnium-stage-2-payload-analysis/

REVERSE ENGINEERING WINDOWS

- https://pt.slideshare.net/cisoplatform7/windows-offender-reverse-engineering-windows-defenders-antivirus-emulator
- https://posts.specterops.io/methodology-for-static-reverse-engineering-of-windows-kernel-drivers-3115b2efed83
- https://www.apriorit.com/dev-blog/366-software-reverse-engineering-tools
- https://www.youtube.com/watch?v=wDNQ-8aWLO0
- https://www.youtube.com/watch?v=PGIennCNDnc
- https://www.youtube.com/watch?v=ZDXTdgfG5HE
- https://silo.tips/download/windows-reverse-engineering
- https://www.ijrter.com/papers/volume-3/issue-10/reverse-engineering-technology-for-windows-o-s-software-program.pdf
- https://i.blackhat.com/us-18/Thu-August-9/us-18-Bulazel-Windows-Offender-Reverse-Engineering-Windows-Defenders-Antivirus-Emulator.pdf
- https://mycourses.aalto.fi/pluginfile.php/432096/mod_resource/content/1/Windows_for_reverse_engineers_Abusing_the%20OS_2017.pdf
- https://recon.cx/2015/slides/recon2015-20-steven-vittitoe-Reverse-Engineering-Windows-AFD-sys.pdf

REVERSE ENGINEERING WINDOWS 2

- http://www-verimag.imag.fr/~mounier/Enseignement/Software_Security/BH_Eagle_ida_pro.pdf
- https://digital-forensics.sans.org/community/papers/grem/reverse-engineering-msrllexe_32
- https://medium.com/@vignesh4303/reverse-engineering-resources-beginners-to-intermediate-guide-links-f64c207505ed
- https://www.youtube.com/watch?v=sk1wAGeM9Hw
- https://medium.com/@pelock/reverse-engineering-tools-for-net-applications-a28275f185b4
- https://dev.to/pelock/top-10-reverse-engineering-tools-3ni3
- http://index-of.es/Windows/pe/CBM_1_2_2006_Goppit_PE_Format_Reverse_Engineer_View.pdf
- https://www.youtube.com/watch?v=Q_-Gv-FQ-FA
- https://medium.com/@pelock/reverse-engineering-tools-for-net-applications-a28275f185b4
- https://medium.com/@AzilenTech/quick-start-guide-to-net-reverse-engineering-542c663ebba3
- https://www.techrepublic.com/blog/software-engineer/reverse-engineering-your-net-applications/
- https://www.youtube.com/watch?v=_NYyjUse0tQ
- https://www.youtube.com/watch?v=_Hvq13Bsgfs

WINDOWS KERNEL EXPLOITATION

- https://www.youtube.com/watch?v=Gu_5kkErQ6Y
- https://github.com/FULLSHADE/WindowsExploitationResources
- https://www.blackhat.com/docs/us-17/wednesday/us-17-Schenk-Taking-Windows-10-Kernel-Exploitation-To-The-Next-Level%E2%80%93Leveraging-Write-What-Where-Vulnerabilities-In-Creators-Update-wp.pdf
- https://media.blackhat.com/bh-us-12/Briefings/Cerrudo/BH_US_12_Cerrudo_Windows_Kernel_WP.pdf
- https://medium.com/@Achilles8284/windows-kernel-exploitation-the-saga-hevd-writeup-part-1-setup-da650234941 1
- https://rootkits.xyz/blog/2017/06/kernel-setting-up/
- https://www.x33fcon.com/#!/t/windowskernel.md

MALWARE ANALYSIS

- https://www.blackhat.com/presentations/bh-dc-07/Kendall_McMillan/Presentation/bh-dc-07-Kendall_McMillan.pdf
- https://medium.com/@maarten.goet/how-windows-1903-makes-malware-analysis-easier-introducing-windows-sandbox-3ec791c8367
- https://www.youtube.com/watch?v=rnzbO-_5lmI
- https://www.youtube.com/watch?v=BMFCdAGxVN4
- https://www.blackhat.com/docs/eu-15/materials/eu-15-KA-Automating-Linux-Malware-Analysis-Using-Limon-Sandbox-wp.pdf
- https://i.blackhat.com/asia-19/Thu-March-28/bh-asia-Monappa-Investigating-Malware-Using-Memory-Forensics.pdf
- https://www.blackhat.com/docs/eu-15/materials/eu-15-KA-Automating-Linux-Malware-Analysis-Using-Limon-Sandbox.pdf
- https://www.blackhat.com/presentations/bh-dc-10/Ross_Jason/Blackhat-DC-2010-Ross-Malware-Analysis-for-the-Enterprise-wp.pdf
- https://www.blackhat.com/docs/us-14/materials/arsenal/us-14-Teller-Automated-Memory-Analysis-WP.pdf

REVERSE ENGINEERING RESOURCES

- https://github.com/wtsxDev/reverse-engineering
- https://github.com/alphaSeclab/awesome-reverse-engineering/blob/master/Readme_en.md
- https://github.com/0xZ0F/Z0FCourse_ReverseEngineering
- https://github.com/OpenToAllCTF/REsources
- https://github.com/GeoSn0w/Reverse-Engineering-Tutorials
- https://github.com/abhisek/reverse-engineering-and-malware-analysis
- https://github.com/howCodeORG/MyAppWindows-Reverse-Engineering
- https://www.mentebinaria.com.br/treinamentos/curso-de-engenharia-reversa-online-cero-r6/

MALWARE ANALYSIS RESOURCES

- https://github.com/rshipp/awesome-malware-analysis
- https://github.com/SpiderLabs/malware-analysis
- https://github.com/arxlan786/Malware-Analysis
- https://github.com/fabacab/awesome-malware
- https://github.com/padfoot999/awesome-malware-analysis
- https://github.com/mikesiko/PracticalMalwareAnalysis-Labs
- https://github.com/ytisf/theZoo
- https://www.mentebinaria.com.br/treinamentos/an%C3%A1lise-de-malware-online-amo-r11/

REFERÊNCIAS - CONCEITOS

- https://stackoverflow.com/questions/993470/what-is-a-windows-api
- https://en.wikipedia.org/wiki/Windows_API
- http://zetcode.com/gui/winapi/introduction/
- https://superuser.com/questions/1361206/what-is-windows-api
- https://docs.microsoft.com/en-us/windows/win32/apiindex/windows-api-list
- https://docs.microsoft.com/en-us/windows/win32/api/
- https://redcanary.com/blog/windows-technical-deep-dive/
- https://www.riverpublishers.com/journal/journal_articles/RP_Journal_2245-1439_741.pdf
- https://users.physics.ox.ac.uk/~Steane/cpp_help/winapi_intro.htm#:~:text=The%20Windows%20API%20(application%20programming,API%20regardless%20of%20the%20language
- https://scorpiosoftware.net/2020/01/03/next-windows-internals-remote-training/ (Course)
- https://mentebinaria.gitbook.io/

THANK YOU!