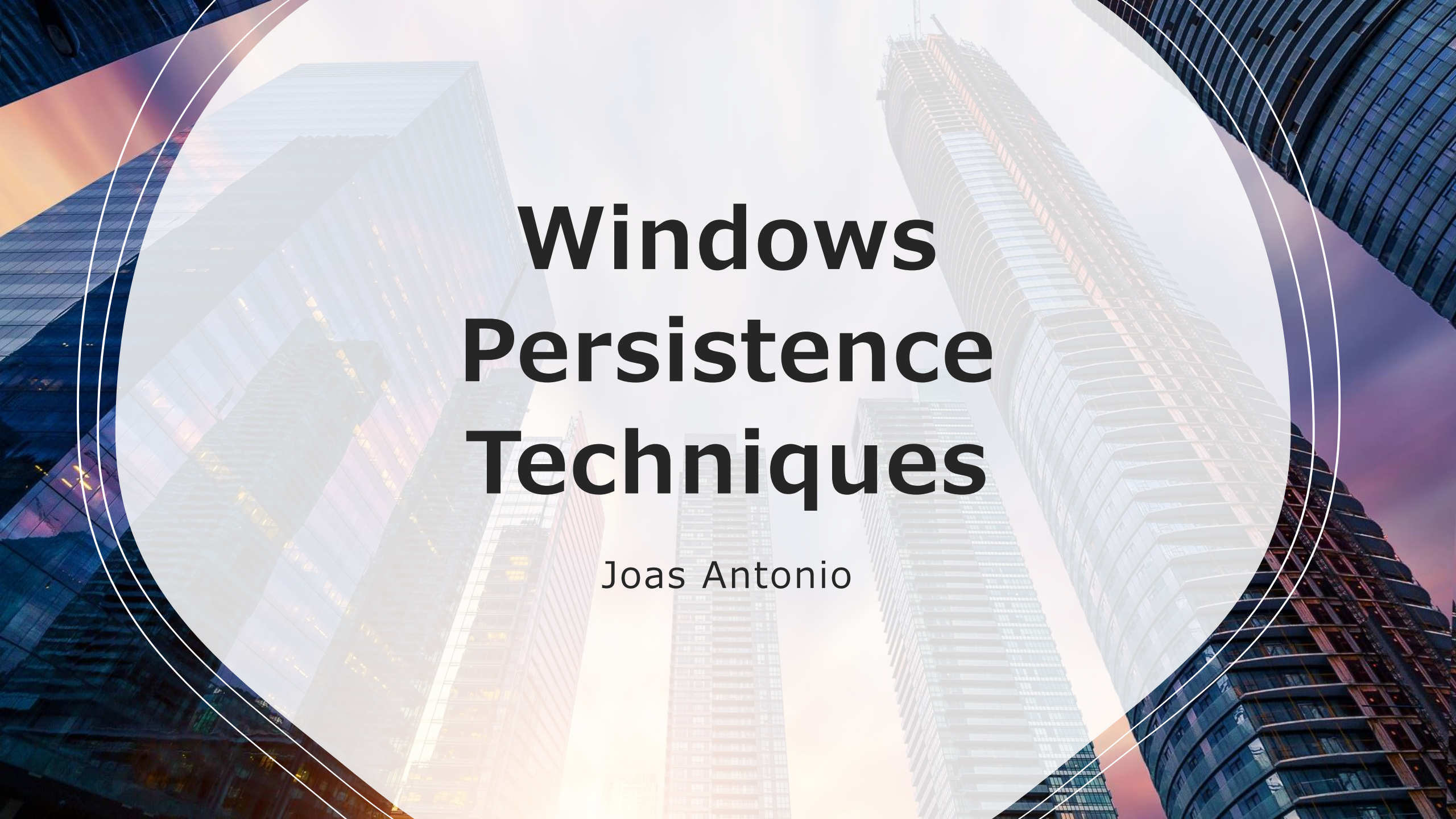

Windows Persistence Techniques

Joas Antonio

Details

Just an overview of some persistence techniques on windows operating systems

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

Introduction

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

Addenum

https://media.howard.com/CNET/USER_MANUAL/2E5177A4-159B-4A2E-9BD8-AAD90ACB0981.pdf

https://nimax-img.de/Produktdownloads/addendum_18877.pdf

https://www.eldoled.com/cms_file.php?fromDB=5567

https://www.microsoft.com/en-us/licensing/product-licensing/products

https://www.energytrust.org/wp-content/uploads/2016/10/HES_FM_WindowsAddendum.pdf

https://github.com/Juanito99/Windows.Computer.DataOnDemand.Addendum

PrivEsc Techniques

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

My ebook

https://drive.google.com/file/d/1Hjq_Hc8dQEF_ZhNFtGMrl2GELoryboyW/view?usp=sharing

Folder and Registre Keys

https://medium.com/r3d-buck3t/abuse-service-registry-acls-windows-privesc-f88079140509

https://book.hacktricks.xyz/windows/windows-local-privilege-escalation/privilege-escalation-with-autorun-binaries

https://book.hacktricks.xyz/windows/windows-local-privilege-escalation

https://pentestlab.blog/category/privilege-escalation/

https://dmcxblue.gitbook.io/red-team-notes/persistence/registry-keys-startup-folder

https://www.semperis.com/blog/group-policy-privilege-escalation/

https://infosecwriteups.com/privilege-escalation-in-windows-380bee3a2842

Logon Scripts

https://blog.gdssecurity.com/labs/2015/1/26/badsamba-exploiting-windows-startup-scripts-using-a-maliciou.html

https://github.com/frizb/Windows-Privilege-Escalation

https://www.hackingarticles.in/window-privilege-escalation-automated-script/

https://rahmatnurfauzi.medium.com/windows-privilege-escalation-scripts-techniques-30fa37bd194

https://dmcxblue.gitbook.io/red-team-notes/persistence/logon-scripts

https://hakin9.org/privesccheck-privilege-escalation-enumeration-script-for-windows/

Screensaver

https://blogs.msmvps.com/donna/2004/11/24/microsoft-windows-logon-screensaver-local-privilege-escalation-vulnerability/

https://packetstormsecurity.com/files/137387/League-Of-Legends-Screensaver-File-Permission-Privilege-Escalation.html

https://www.w4rri0r.com/sequence-of-commands/privilege-escalation-attacks.html

DLL Proxying

https://itm4n.github.io/dll-proxying/

https://kevinalmansa.github.io/application%20security/DLL-Proxying/

https://www.ired.team/offensive-security/persistence/dll-proxying-for-persistence

https://github.com/tothi/dll-hijack-by-proxying

https://milosilo.com/hacking/microsoft-teams-proxy-dll-hijacking/

https://www.youtube.com/watch?v=raLnL4DdvKU

https://www.youtube.com/watch?v=tSdyfaJ7T50

https://www.cynet.com/attack-techniques-hands-on/dlls-and-ways-they-can-hurt-us/

Component object model

---

https://research.nccgroup.com/2020/04/15/cve-2019-1381-and-cve-2020-0859-how-misleading-documentation-led-to-a-broken-patch-for-a-windows-arbitrary-file-disclosure-vulnerability/

https://www.elastic.co/guide/en/security/7.x/component-object-model-hijacking.html

https://attack.mitre.org/techniques/T1559/001/

https://dmcxblue.gitbook.io/red-team-notes/execution/com

Persistence Techniques

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

Eleveted Schedule Task

https://www.windowstricks.in/2018/08/how-to-run-the-powershell-script-in-scheduled-task-with-run-as-administrator.html

https://stackoverflow.com/questions/62245797/how-to-setup-a-powershell-script-in-windows-task-scheduler-with-admin-permission

https://superuser.com/questions/1640613/how-to-run-a-powershell-script-with-elevated-access-using-task-scheduler

https://blog.netwrix.com/2018/07/03/how-to-automate-powershell-scripts-with-task-scheduler/

https://www.reddit.com/r/PowerShell/comments/6qvp30/task_schedule_powershell_script_with_admin_rights/

https://o365reports.com/2019/08/02/schedule-powershell-script-task-scheduler/

https://pentestlab.blog/2019/11/04/persistence-scheduled-tasks/

https://www.elastic.co/guide/en/security/current/persistence-via-telemetrycontroller-scheduled-task-hijack.html

https://attack.mitre.org/techniques/T1053/005/

Multiaction Task

https://securitybyexpert.com/windows-persistence-multi-action-scheduled-task/

https://www.fireeye.com/blog/threat-research/2019/09/sharpersist-windows-persistence-toolkit.html

https://www.igi-global.com/dictionary/assessment-of-task-persistence/50930

https://techdocs.broadcom.com/us/en/symantec-security-software/identity-security/identity-manager/14-4/configuring/task-persistence.html

https://www.elastic.co/guide/en/security/7.x/persistence-via-telemetrycontroller-scheduled-task-hijack.html

WMI Event Subscription

https://pentestlab.blog/2020/01/21/persistence-wmi-event-subscription/

https://www.elastic.co/guide/en/security/current/persistence-via-wmi-event-subscription.html

https://medium.com/threatpunter/detecting-removing-wmi-persistence-60ccbb7dff96

https://www.mdsec.co.uk/2019/05/persistence-the-continued-or-prolonged-existence-of-something-part-3-wmi-event-subscription/

https://in.security/an-intro-into-abusing-and-identifying-wmi-event-subscriptions-for-persistence/

https://liberty-shell.com/sec/2019/06/16/wmi-persistence/

https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/asr-in-intune-for-quot-block-persistence-through-wmi-event/m-p/2068130

https://microsoftintune.uservoice.com/forums/291681-ideas/suggestions/40862476-asr-rule-block-persistence-through-wmi-event-subs

https://www.rapid7.com/db/modules/exploit/windows/local/wmi_persistence/

Appcert DLLS

https://www.elastic.co/guide/en/security/current/registry-persistence-via-appcert-dll.html

https://attack.mitre.org/techniques/T1546/009/

https://pentestlab.blog/2020/01/07/persistence-appinit-dlls/

https://eqllib.readthedocs.io/en/latest/analytics/14f90406-10a0-4d36-a672-31cabe149f2f.html

https://github.com/ewilded/Windows_persistence/blob/master/REGISTRY.md

https://dmfrsecurity.com/2021/01/02/review-red-team-operator-windows-persistence-course-by-sektor7-institute/

Appinit DLLS

https://eforensicsmag.com/appinit-dll-injection-by-siddharth-sharma/

https://attack.mitre.org/techniques/T1546/010/

https://www.elastic.co/guide/en/security/current/registry-persistence-via-appinit-dll.html

https://eqllib.readthedocs.io/en/latest/analytics/822dc4c5-b355-4df8-bd37-29c458997b8f.html

https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1546.010/T1546.010.md

https://github.com/akapv/atomic-red-team/blob/master/Windows/Persistence/AppInit_DLLs.md

https://docs.microsoft.com/en-us/windows/win32/dlls/secure-boot-and-appinit-dlls

https://www.cyberhuntingguide.net/t1546010.html

Netsh Helper DLL

https://pentestlab.blog/2019/10/29/persistence-netsh-helper-dll/

https://attack.mitre.org/techniques/T1546/007/

https://www.ired.team/offensive-security/persistence/t1128-netsh-helper-dll

https://github.com/rtcrowley/Offensive-Netsh-Helper

https://dmcxblue.gitbook.io/red-team-notes-2-0/red-team-techniques/persistence/t1546-event-triggered-execution/netsh-helper-dll

https://www.hackingarticles.in/windows-persistence-using-netsh/

https://www.reddit.com/r/netsec/comments/donwj5/persistence_netsh_helper_dll/

https://liberty-shell.com/sec/2018/07/28/netshlep/

https://eqllib.readthedocs.io/en/latest/analytics/5f9a71f4-f5ef-4d35-aff8-f67d63d3c896.html

Time Provider Persistence

https://www.ired.team/offensive-security/persistence/t1209-hijacking-time-providers

https://pentestlab.blog/2019/10/22/persistence-time-providers/

https://attack.mitre.org/techniques/T1547/003/

https://github.com/elastic/detection-rules/issues/853

https://github.com/endgameinc/eqllib/blob/master/eqllib/analytics/persistence/T1209-persistence-time-providers.toml

https://institute.sektor7.net/rto-windows-persistence

https://medium.com/@gabriel.pirjolescu/demystifying-windows-malware-hunting-part-1-detecting-persistence-with-osquery-b53573c2aac0

Port Monitors

https://pentestlab.blog/2019/10/28/persistence-port-monitors/#:~:text=Interaction%20with%20the%20service%20is,configuration%2C%20data%20and%20monitor%20files.

https://www.hackingarticles.in/windows-persistence-port-monitors/

https://posts.slayerlabs.com/monitor-persistence/

https://github.com/airzero24/PortMonitorPersist

https://www.ired.team/offensive-security/persistence/t1013-addmonitor

https://windows-internals.com/printdemon-cve-2020-1048/

lsa-as-a-persistence

---

https://adsecurity.org/?p=1760

https://attack.mitre.org/tactics/TA0003/

https://pentestlab.blog/2019/10/21/persistence-security-support-provider/

https://www.elastic.co/guide/en/security/current/potential-lsa-authentication-package-abuse.html

https://lifars.com/2021/01/common-malware-persistence-techniques/

https://www.csoonline.com/article/3393268/how-to-outwit-attackers-using-two-windows-registry-settings.html

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh994565(v=ws.11)

https://www.ndss-symposium.org/wp-content/uploads/2017/09/P01_3.pdf

Metasploit Persistence

https://www.hackingarticles.in/multiple-ways-to-persistence-on-windows-10-with-metasploit/

https://www.offensive-security.com/metasploit-unleashed/meterpreter-service/

https://www.offensive-security.com/metasploit-unleashed/persistent-backdoors/

https://www.hackers-arise.com/how-to-make-the-meterpreter-persistent

https://securityonline.info/automated-persistent-backdoor-metasploit/

https://secnhack.in/technique-to-persistence-on-windows-10-with-metasploit/

https://pentestlab.blog/2020/02/04/persistence-waitfor/

https://www.rapid7.com/db/modules/exploit/windows/local/persistence/

https://ways2hack.com/metasploit-framework/