Red Team: MacOS Att&ck - Overview

Joas Antonio

Details

- The purpose of this pdf is to bring some techniques for exploiting vulnerabilities and adversary emulation in MacOS
- https://www.linkedin.com/in/joas-antonio-dos-santos

MACOS INTRODUCTION

- https://www.youtube.com/watch?v=67keaaWOKzE
- https://www.youtube.com/watch?v=_RN89xApebs
- https://www.youtube.com/watch?v=W92XTNsxZHA

MacOS Security

- https://www.securicy.com/blog/our-best-practices-for-securing-your-macbook/
- https://support.apple.com/pt-br/guide/mac-help/flvlt003/mac
- https://www.intego.com/mac-security-blog/15-mac-hardening-security-tips-to-protect-your-privacy/
- https://github.com/drduh/macOS-Security-and-Privacy-Guide
- https://www.youtube.com/watch?v=Uz2LjuR_Rhs&list=PLq1Exx3REVHqZe2hm4ijFUx1ASocGbB9G

Command and Control

- https://github.com/its-a-feature/Mythic
- https://docs.mythic-c2.net/
- https://howto.thec2matrix.com/c2/mythic
- https://github.com/DeimosC2/DeimosC2
- https://www.youtube.com/watch?v=e7xQzPzO19c
- https://securityonline.info/deimosc2-golang-command-and-control-framework-for-post-exploitation/
- https://github.com/Marten4n6/EvilOSX
- https://medium.com/@lucideus/evilosx-a-remote-administration-tool-rat-for-macos-os-x-lucideus-research-da0551ed3969
- https://www.youtube.com/watch?v=SkDz7NjifxA
- https://github.com/EmpireProject/Empire
- https://github.com/sensepost/godoh
- https://github.com/rev10d/goDoH
- https://github.com/cedowens/MacShellSwift
- https://github.com/cedowens/MacC2

Command and Control

- https://github.com/cedowens/C2-JARM
- https://docs.google.com/spreadsheets/d/1b4mUxa6cDQuTV2BPC6aA-GR4zGZi0ooPYtBe4IgPsSc/edit#gid=0
- https://github.com/n1nj4sec/pupy
- https://github.com/frozenkp/gdoor
- https://github.com/gloxec/CrossC2

JavaScript Automation

- https://developer.apple.com/library/archive/documentation/LanguagesUtilities/Conceptual/MacAutomationScriptingGuide/index.html
- https://medium.com/@hiraash/use-javascript-to-automate-stuff-on-macos-f1cdbb890f18
- https://computers.tutsplus.com/tutorials/a-beginners-guide-to-javascript-application-scripting-jxa--cms-27171
- https://kb.benchmarkemail.com/en/how-do-i-enable-javascript-in-my-browser-on-my-mac/
- https://www.businessinsider.com/how-to-enable-javascript-on-mac

JavaScript Automation

- https://developer.apple.com/library/archive/documentation/LanguagesUtilities/Conceptual/MacAutomationScriptingGuide/index.html
- https://medium.com/@hiraash/use-javascript-to-automate-stuff-on-macos-f1cdbb890f18
- https://computers.tutsplus.com/tutorials/a-beginners-guide-to-javascript-application-scripting-jxa--cms-27171
- https://kb.benchmarkemail.com/en/how-do-i-enable-javascript-in-my-browser-on-my-mac/
- https://www.businessinsider.com/how-to-enable-javascript-on-mac

MacOS Exploitation and Post Exploitation

- https://www.mdsec.co.uk/2021/01/macos-post-exploitation-shenanigans-with-vscode-extensions/
- https://posts.specterops.io/abusing-slack-for-offensive-operations-2343237b9282
- https://posts.specterops.io/hands-in-the-cookie-jar-dumping-cookies-with-chromiums-remote-debugger-port-34c4f468844e
- https://blog.xpnsec.com/bring-your-own-vm-mac-edition/
- https://blog.xpnsec.com/we-need-to-talk-about-macl/
- https://blog.xpnsec.com/tags/macos/
- https://blog.xpnsec.com/macos-filename-homoglyphs-revisited/
- https://blog.xpnsec.com/bypassing-macos-privacy-controls/

MacOS Exploitation and Post Exploitation

- https://blog.xpnsec.com/macos-phishing-tricks/
- https://blog.xpnsec.com/disabling-macos-sip-via-a-virtualbox-kext-vulnerability/
- https://blog.xpnsec.com/macos-av-self-protection-methods/
- https://blog.xpnsec.com/escaping-the-sandbox-microsoft-office-on-macos/
- https://www.sentinelone.com/blog/macos-red-team-calling-apple-apis-without-building-binaries/
- https://antman1p-30185.medium.com/macos-native-api-calls-in-electron-d297d9a960af
- https://posts.specterops.io/persistent-jxa-66e1c3cd1cf5
- https://posts.specterops.io/are-you-docking-kidding-me-9aa79c24bdc1
- https://www.sprocketsecurity.com/blog/how-to-hijack-slack-sessions-on-macos
- https://desi-jarvis.medium.com/office365-macos-sandbox-escape-fcce4fa4123c

MacOS Att&ck – Initial Acess

- https://attack.mitre.org/matrices/enterprise/macos/
- https://github.com/D00MFist/Mystikal
- https://posts.specterops.io/introducing-mystikal-4fbd2f7ae520
- https://github.com/benb116/Gone-Phishing
- https://github.com/cldrn/macphish
- https://github.com/gophish/gophish
- https://github.com/BlacksunLabs/LockScream
- https://github.com/A2nkF/macOS-Kernel-Exploit
- https://github.com/sslab-gatech/pwn2own2020
- https://github.com/thehappydinoa/rootOS
- https://github.com/houjingyi233/macOS-iOS-system-security

MacOS Att&ck – Execution

- https://developer.apple.com/documentation/
- https://support.apple.com/pt-br/guide/terminal/apdb66b5242-0d18-49fc-9c47-a2498b7c91d5/mac
- https://www.davidbaumgold.com/tutorials/command-line/#:~:text=The%20Mac%20command%20line%20is,is%20a%20folder%20called%20Utilities.
- https://www.youtube.com/watch?v=AKCp8fCm8PE
- https://www.youtube.com/watch?v=xmk6urRlF1o

MacOS Att&ck – Privilege Escalation

- https://labs.sentinelone.com/privilege-escalation-macos-malware-path-to-root/
- https://www.offensive-security.com/offsec/macos-preferences-priv-escalation/
- https://www.bleepingcomputer.com/news/apple/apple-fixes-sudo-root-privilege-escalation-flaw-in-macos/
- https://www.zerodayinitiative.com/blog/2020/12/9/cve-2020-27897-apple-macos-kernel-oob-write-privilege-escalation-vulnerability
- https://appleinsider.com/articles/21/02/03/sudo-vulnerability-in-macos-could-give-root-privileges-to-local-users
- https://www.trendmicro.com/en_hk/research/19/f/cve-2019-8635-double-free-vulnerability-in-apple-macos-lets-attackers-escalate-system-privileges-and-execute-arbitrary-code.html
- https://www.securing.pl/en/local-privilege-escalation-in-macos-infrastructure/
- https://research.nccgroup.com/2020/07/02/technical-advisory-macos-installer-local-root-privilege-escalation-cve-2020-9817/
- https://github.com/A2nkF/unauthd
- https://github.com/m0nad/awesome-privilege-escalation
- https://www.offensive-security.com/offsec/microsoft-teams-macos-local-privesc/

MacOS Att&ck – Defense Evasion

- https://github.com/uber-common/metta/blob/master/MITRE/Defense_Evasion/defenseevasion_osx_gatekeeper_bypass.yml
- https://github.com/redcanaryco/vscode-attack
- https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/Indexes/Matrices/macos-matrix.md
- https://github.com/sbousseaden/macOS-ATTACK-DATASET
- https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/Indexes/Indexes-Markdown/macos-index.md
- https://threatpost.com/apple-patches-macos-bug-bypass-defenses/165611/

MacOS Att&ck – Lateral Movement

- https://github.com/rmusser01/Infosec_Reference/blob/master/Draft/ATT%26CK-Stuff/ATT%26CK/Lateral%20Movement.md
- https://github.com/debauchee/barrier
- https://redcanary.com/blog/attacking-a-mac-threat-detection-392/

MacOS Att&ck – Exfiltration

- https://gist.github.com/tokyoneon/27fff84233ebd073288941a88854e9ee
- https://github.com/TryCatchHCF/PacketWhisper
- https://getskout.com/cybersecurity-threat-advisory-0017-21-macos-malware-xcodespy/
- https://attack.mitre.org/techniques/T1020/
- https://null-byte.wonderhowto.com/how-to/hacking-macos-use-images-smuggle-data-through-firewalls-0197128/

Awesome Red Team and PenTest

- https://github.com/infosecn1nja/Red-Teaming-Toolkit
- https://github.com/yeyintminthuhtut/Awesome-Red-Teaming
- https://github.com/enaqx/awesome-pentest
- https://github.com/Muhammd/Awesome-Pentest