Inside Out:
Deconstructing macOS Application Security

Fatih ERDOĞAN
@FeCassie
Senior Blue Team Engineer, Picus Security

$ whoami

- **Fatih ERDOĞAN**
- Sr. Blue Team Engineer @**Picus Security**
- Formerly: Trendyol, Zemana, STM, Prodaft

ferdogan.me

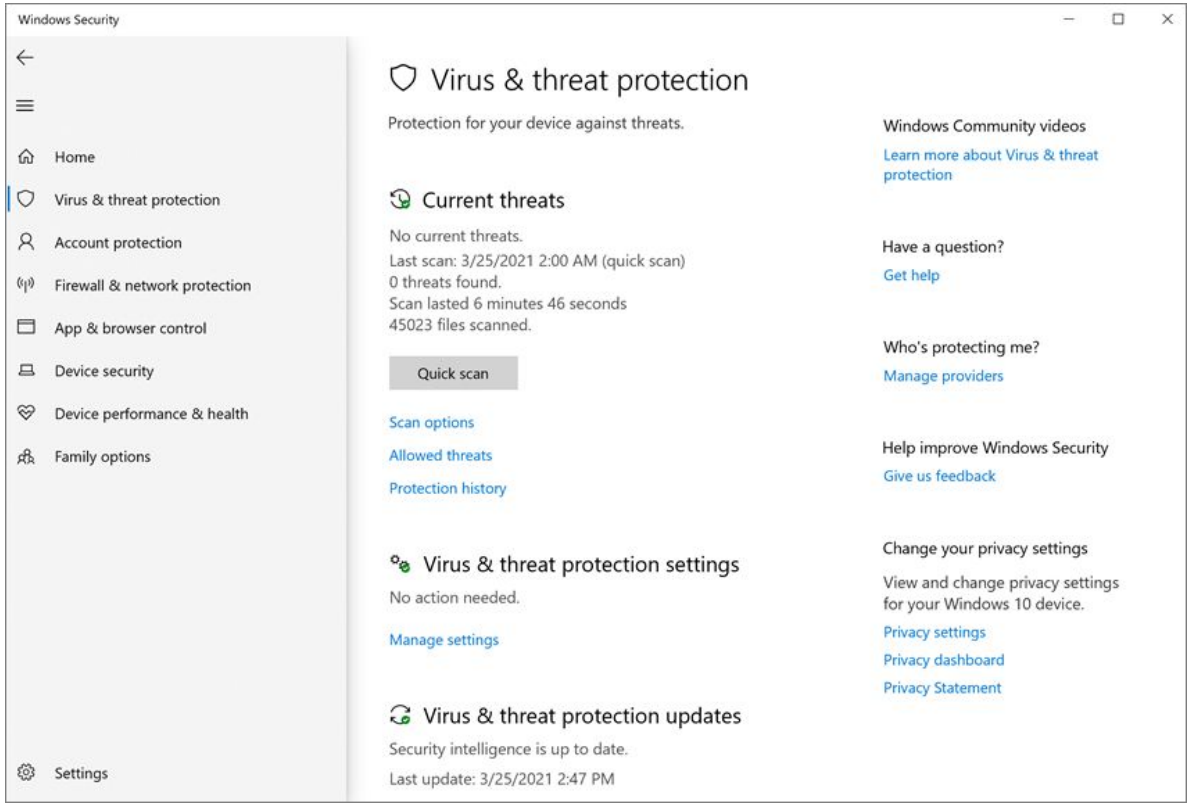
@FeCassie

PICUS

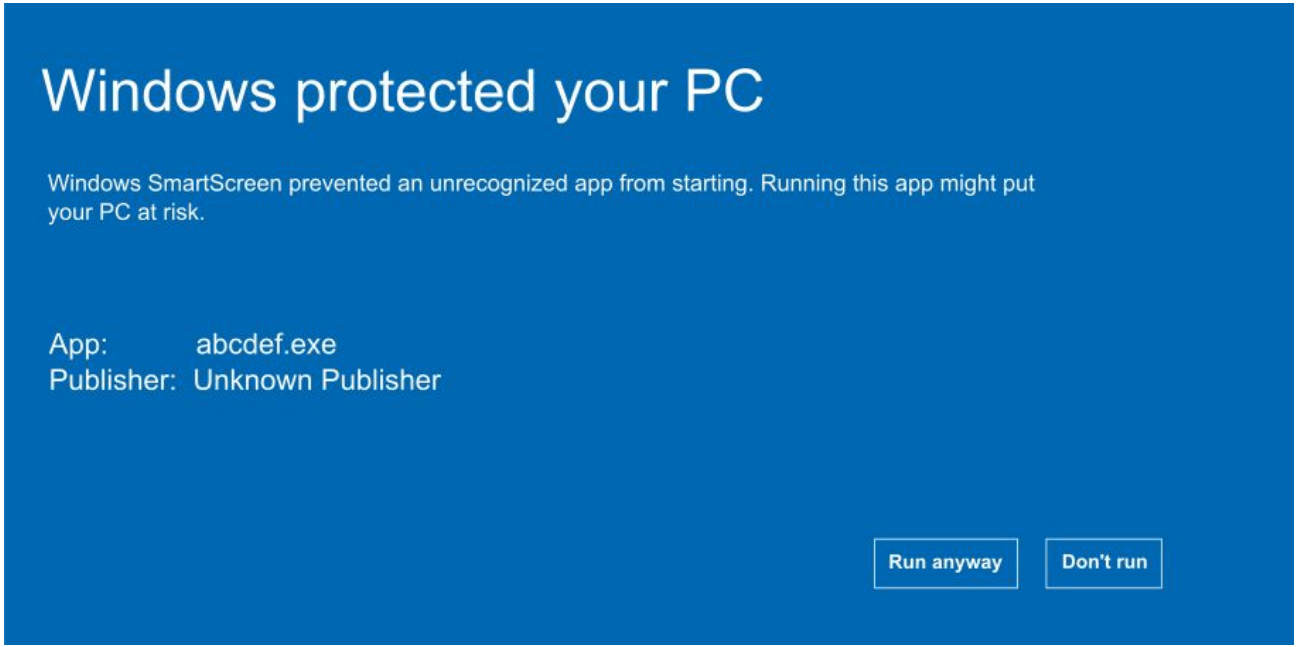
HACKTRICK
SİBER GÜVENLİK KONFERANSI

Windows

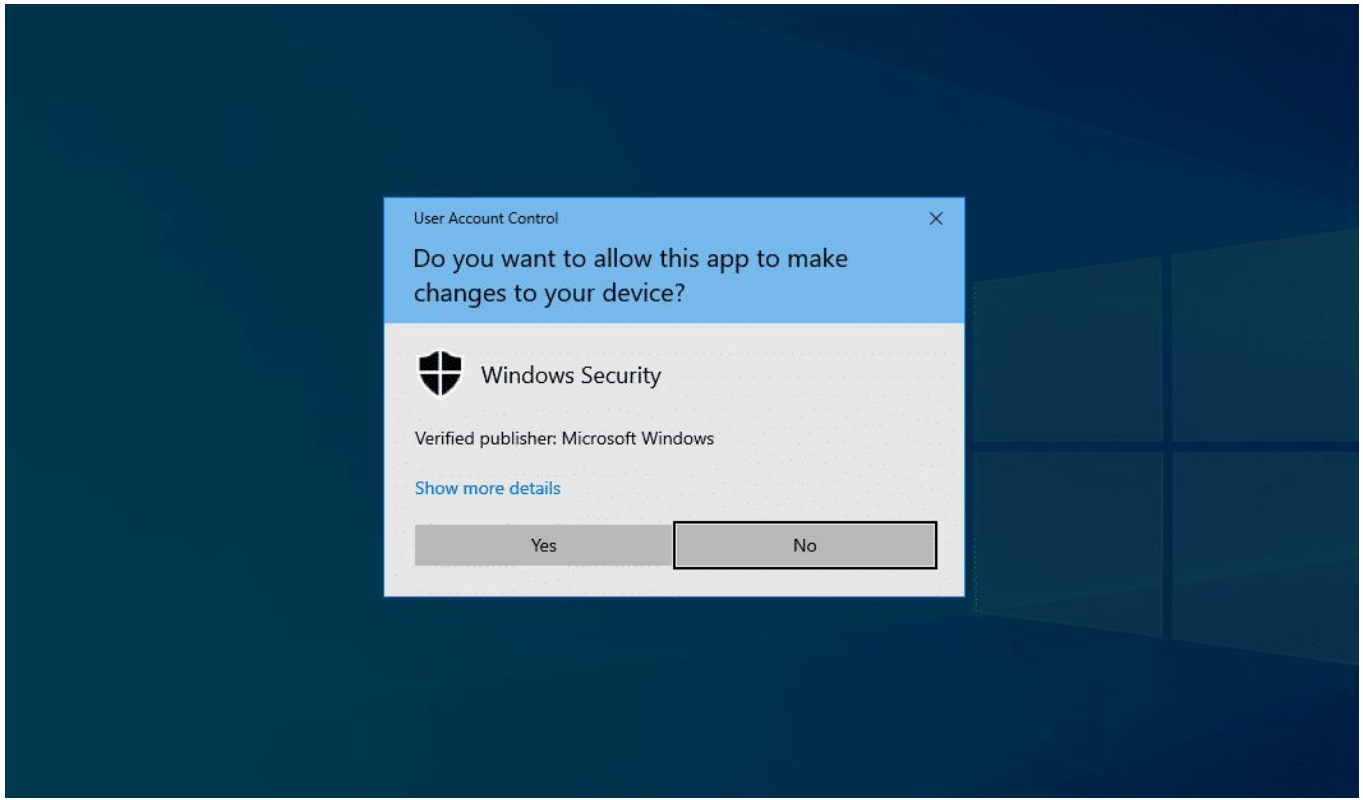
Windows Defender Antivirus



Microsoft Smart Screen



User Account Control



Built-In macOS Application Security

PICUS

HACKTRICK
SİBER GÜVENLİK KONFERANSI

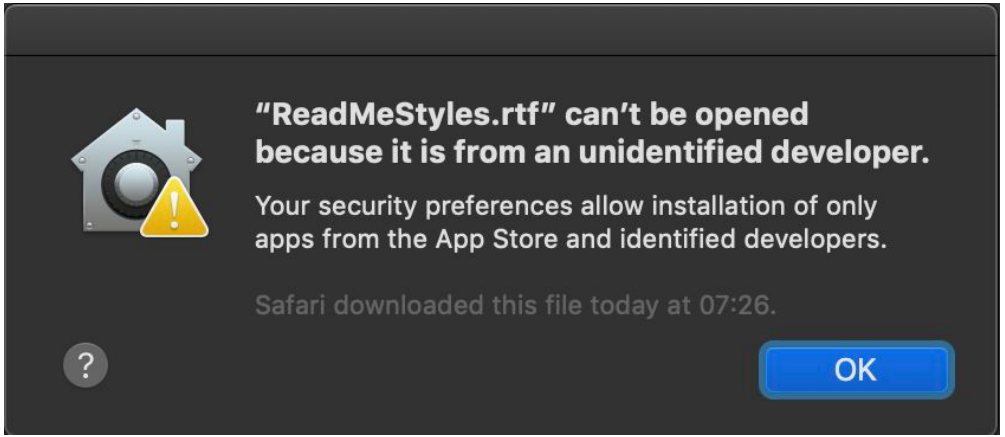
macOS Application Security

File Quarantine

File Quarantine

- Predecessor of **Gatekeeper**
- OS X Leopard (10.5)
- Extended Attribute-(XA)
  - **com.apple.quarantine** attribute is added to the files downloaded from the internet.

- File Quarantine is designed to **notify users** when an application **downloaded** from the Internet is run for the first time.



File Quarantine

- Files that have **@** at the end of their permissions flags have extended attributes.

```
→  Downloads ls -l |grep -i "@"
-rw-r--r--@  1 fatiherdogan  staff      111043 Feb 17 16:17 1676634086_2431.csv
-rw-r--r--@  1 fatiherdogan  staff       13669 Jul 31 18:12 1st conditional.docx
-rw-r--r--@  1 fatiherdogan  staff         719 Dec  9  2022 25619_Prevention_20_Oct_2022_Thu_09_09_40_AM.csv
-rw-r--r--@  1 fatiherdogan  staff       47592 Jul 27 23:19 365cb889-4f0f-4209-9019-7aa52e653162.png
-rw-r--r--@  1 fatiherdogan  staff      385602 Mar  9 11:07 435f4055-4eea-433f-a937-6adebc8884f6.png
-rw-r--r--@  1 fatiherdogan  staff      433965 Mar  6 18:07 49425_06_Mar_2023_Mon_09_18_57_AM (1).csv
-rw-r--r--@  1 fatiherdogan  staff      433965 Mar  6 18:06 49425_06_Mar_2023_Mon_09_18_57_AM.csv
-rw-r--r--@  1 fatiherdogan  staff      433545 Mar  8 13:52 49757_07_Mar_2023_Tue_08_51_50_AM.csv
-rw-r--r--@  1 fatiherdogan  staff      174423 Mar 19 21:56 52744_19_Mar_2023_Sun_01_14_34_PM.csv
-rw-r--r--@  1 fatiherdogan  staff      296705 Apr  7 09:55 57879_06_Apr_2023_Thu_03_01_11_PM (1).csv
-rw-r--r--@  1 fatiherdogan  staff      296705 Apr  6 22:34 57879_06_Apr_2023_Thu_03_01_11_PM.csv
drwx------@  7 fatiherdogan  staff         224 Aug  9 16:01 7z2301-mac
-rw-r--r--@  1 fatiherdogan  staff     1805532 Aug  9 16:01 7z2301-mac.tar.xz
-rw-r--r--@  1 fatiherdogan  staff      181756 Dec  8  2022 80367B48D2FE91E9289CD07A38FB7000.zip
```

xattr

- The **xattr** utility allows users to view a file's extended attributes.
- The **xattr -p** command is used to display extended attribute values.

```
➜  Downloads xattr CleanMyMacX.dmg
com.apple.macl
com.apple.metadata:kMDItemWhereFroms
com.apple.quarantine
```

```
➜  Downloads xattr -p com.apple.quarantine CleanMyMacX.dmg
0081;63978f7e;Chrome;B3C834BE-5F9C-4620-BF6C-37986F5EBC3F
```

xattr

- The **xattr** utility allows users to view a file's extended attributes.
- The **xattr -p** command is used to display extended attribute values.

```
➜  Downloads xattr CleanMyMacX.dmg
com.apple.macl
com.apple.metadata:kMDItemWhereFroms
com.apple.quarantine
```

```
➜  Downloads xattr -p com.apple.quarantine CleanMyMacX.dmg
0081;63978f7e;Chrome;B3C834BE-5F9C-4620-BF6C-37986F5EBC3F
```

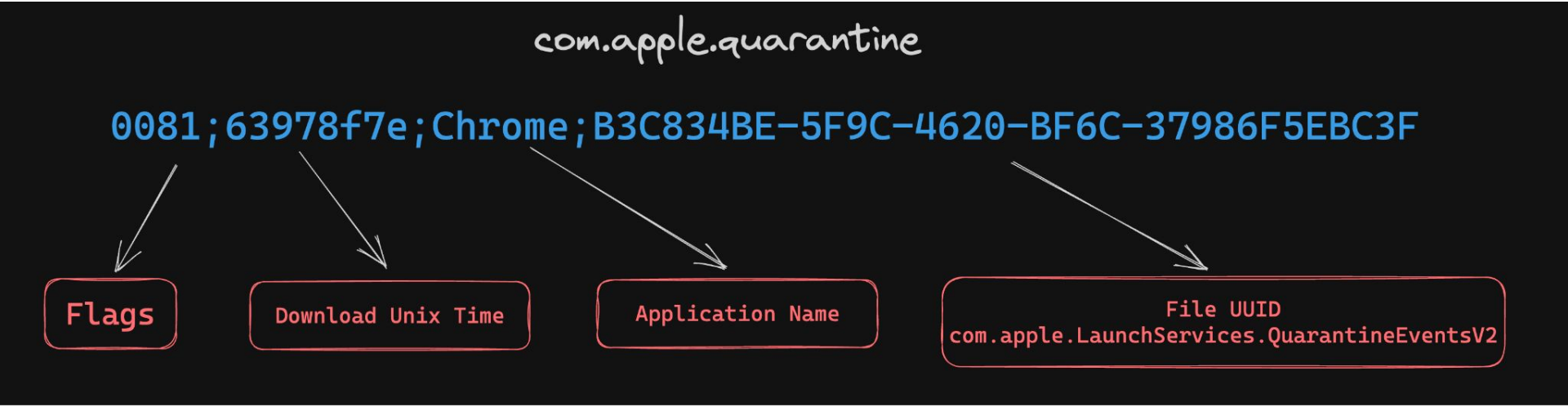
xattr

- The **xattr** utility allows users to view a file's extended attributes.
- The **xattr -p** command is used to display extended attribute values.

```
➜  Downloads xattr CleanMyMacX.dmg
com.apple.macl
com.apple.metadata:kMDItemWhereFroms
com.apple.quarantine
```

```
➜  Downloads xattr -p com.apple.quarantine CleanMyMacX.dmg
0081;63978f7e;Chrome;B3C834BE-5F9C-4620-BF6C-37986F5EBC3F
```

XA Values – com.apple.quarantine

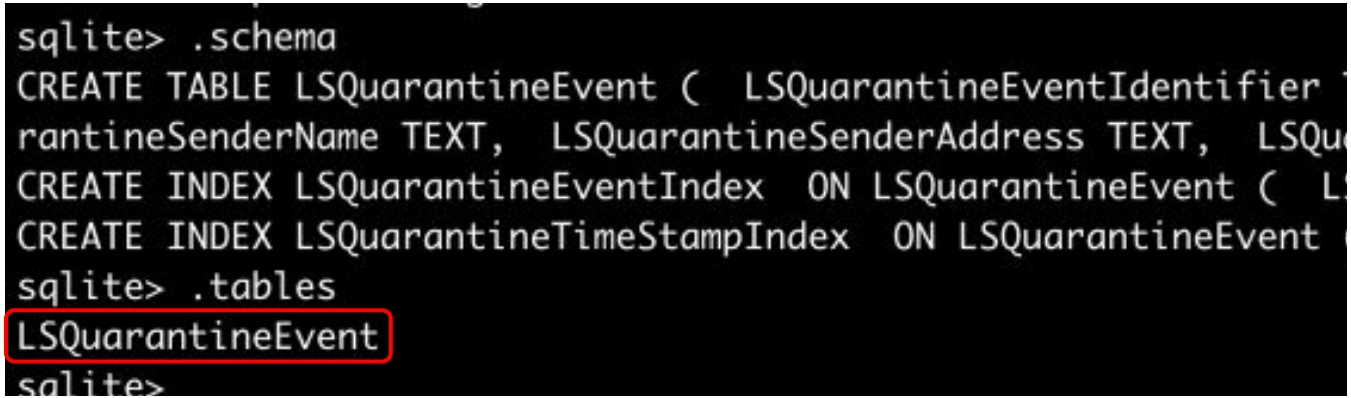


QuarantineEventsV2 Database – com.apple.quarantine

- **com.apple.LaunchServices.QuarantineEventsV2** SQLite database.
- The database is located at;
  - **~/Library/Preferences/com.apple.LaunchServices.QuarantineEventsV2**.

```
➜  ~ sqlite3 ~/Library/Preferences/com.apple.LaunchServices.QuarantineEventsV2
SQLite version 3.39.5 2022-10-14 20:58:05
Enter ".help" for usage hints.
sqlite> .schema
CREATE TABLE LSQuarantineEvent (  LSQuarantineEventIdentifier TEXT PRIMARY KEY NOT NULL,  LSQuarantineTimeStamp REAL,  LSQuarantineAgentBundleIdentifier TEXT,  LSQuarantineAgentName TEXT,  LSQuarantineDataURLString TEXT,  LSQua
rantineSenderName TEXT,  LSQuarantineSenderAddress TEXT,  LSQuarantineTypeNumber INTEGER,  LSQuarantineOriginTitle TEXT,  LSQuarantineOriginURLString TEXT,  LSQuarantineOriginAlias BLOB );
CREATE INDEX LSQuarantineEventIndex  ON LSQuarantineEvent (  LSQuarantineEventIdentifier );
CREATE INDEX LSQuarantineTimeStampIndex  ON LSQuarantineEvent (  LSQuarantineTimeStamp );
sqlite> .tables
LSQuarantineEvent
sqlite>
sqlite>
```

QuarantineEventsV2 Database – com.apple.quarantine



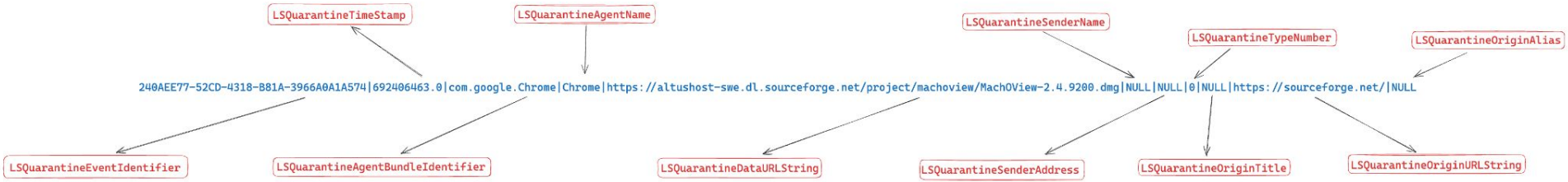
QuarantineEventsV2 Database – com.apple.quarantine

```
sqlite> .headers ON
sqlite> select * from LSQuarantineEvent;
LSQuarantineEventIdentifier|LSQuarantineTimeStamp|LSQuarantineAgentBundleIdentifier|LSQuarantineAgentName|LSQuarantineDataURLString|LSQuarantineSenderName|LSQuarantineSenderAddress|LSQuarantineTypeNumber|LSQuarantineOriginTitle|LSQuarantineOriginURLString|LSQuarantineOriginAlias
140D5E20-A6DF-4219-8E05-421BCC13B790|688306230.0|com.google.Chrome|Chrome|https://optimizationguide-pa.googleapis.com/downloads?name=1666011699815&target=OPTIMIZATION_TARGET_LANGUAGE_DETECTION|||0|||
CF9B49EE-4961-4153-AB05-A550C9A2553A|688306231.0|com.google.Chrome|Chrome|https://optimizationguide-pa.googleapis.com/downloads?name=1666011733212&target=OPTIMIZATION_TARGET_NOTIFICATION_PERMISSION_PREDICTIONS|||0|||
DEFDECC9-2FF2-492D-AC23-505E8362BFA0|688306233.0|com.google.Chrome|Chrome|https://optimizationguide-pa.googleapis.com/downloads?name=2202180000&target=OPTIMIZATION_TARGET_SEGMENTATION_CHROME_LOW_USER_ENGAGEMENT|||0|||
21C2D9AB-9D58-4FC9-9A3A-0E2ED48F2430|688306230.0|com.google.Chrome|Chrome|https://optimizationguide-pa.googleapis.com/downloads?name=1664804603429&target=OPTIMIZATION_TARGET_PAGE_ENTITIES|||0|||
805D1846-6232-4D69-AF5D-261722C1791E|688307085.0|com.google.Chrome|Chrome||||1|||
F33A63C8-B9B1-43FA-8D0D-FE6D2AAB3D2F|688376407.0|com.google.Chrome|Chrome|https://optimizationguide-pa.googleapis.com/downloads?name=1666616588775&target=OPTIMIZATION_TARGET_NOTIFICATION_PERMISSION_PREDICTIONS|||0|||
F5C290D5-DCA8-4D08-90A2-1188B0BBF65A|688470141.0|com.google.Chrome|Chrome|https://optimizationguide-pa.googleapis.com/downloads?name=1666014191313&target=OPTIMIZATION_TARGET_PAGE_ENTITIES|||0|||
D0BFF8B3-A929-4E08-BD36-7A452BB0C2EF|688471202.0|com.google.Chrome|Chrome|https://desktop-release.notion-static.com/Notion-2.1.4-arm64.dmg|||0||https://www.notion.so/|
24F1950B-B4E8-48C7-92A4-079660A54089|688473256.0|com.google.Chrome|Chrome|https://clients2.googleusercontent.com/crx/blobs/Acy1k0Yi59h7F9dRWQ60GGICDd2ojXWQTPJifcmUU3Lcfy7AHypIlHKJ8xV_wz6Ow5t_JzLQOoC6NxU-1l3sU4O9nVcwOr7GX_-1NDSN_1qb90BN6heAAMZSmuW0Jwkt79_lMjp5mozB5cQf0lMDCw/extension
_2_0_12_0.crx|||0||https://chrome.google.com/|
4014632A-79E4-4CEE-A415-6FF16D39C8F9|688551180.165596||sharingd||ferdogan||6|||
335087F1-1696-4EDD-87F7-2442D25B9B1C|688892880.0|com.google.Chrome|Chrome||||1|||
81858695-28E2-4214-AE9D-C6633D1C4A98|688899031.0|com.google.Chrome|Chrome||||1|||
992BD930-D50C-4FE5-A366-B303B4E932B1|688909058.54079||sharingd||ferdogan||6|||
```

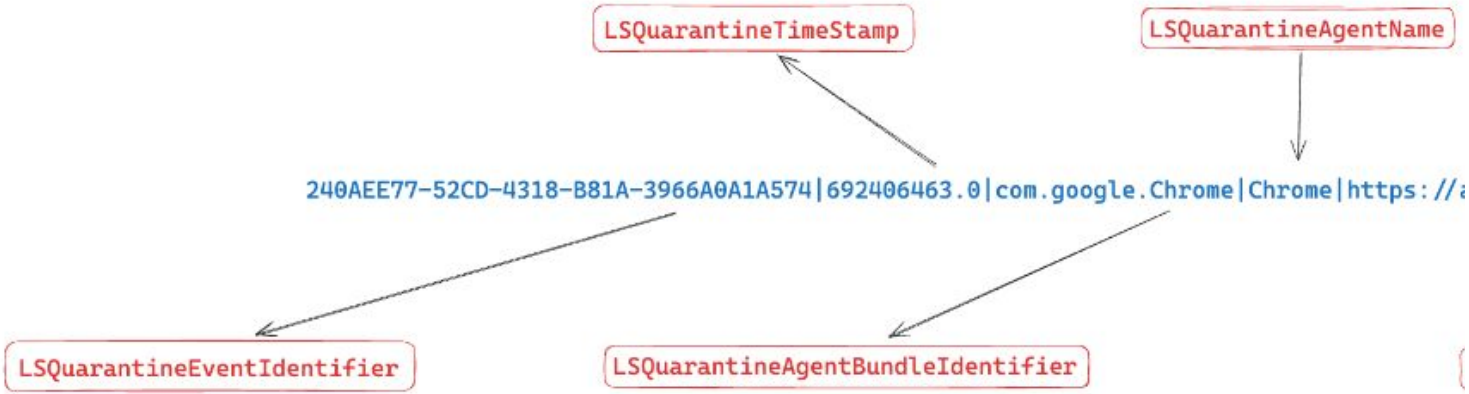
PICUS

HACKTRICK
SİBER GÜVENLİK KONFERANSI

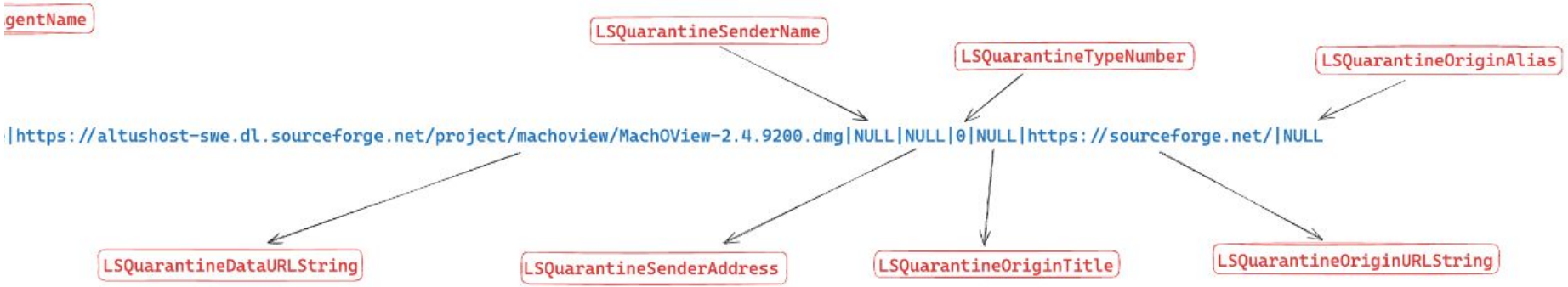
LSQuarantineEvent Table



LSQuarantineEvent Table



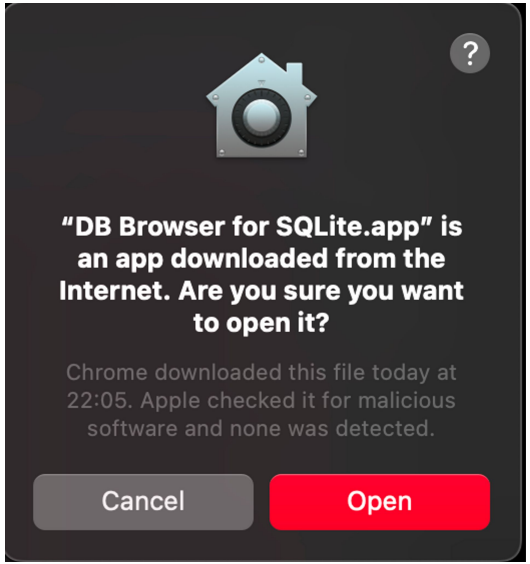
LSQuarantineEvent Table



Gatekeeper

Gatekeeper

- It designed to run **trusted software** on macOS.
- When downloading an application from the Internet outside the **AppStore** and opening that application, Gatekeeper confirms that the application comes from the **identified developer** and is known to Apple (**notarization**).



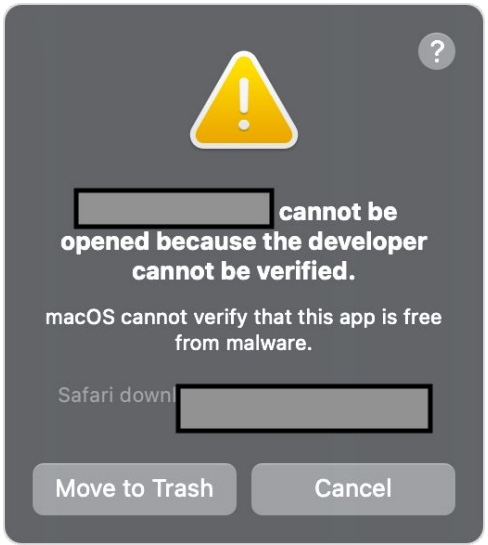
Gatekeeper

- The operations of the Gatekeeper service are performed at the system level by **spctl - SecAssessment system policy security** macOS binary.
- The spctl command is used to check whether an application is **signed** and **notarized**. The command returns either "**accepted**" or "**rejected**", depending on the Gatekeeper's evaluation.

```
→  /Applications spctl --verbose=4 --assess --type execute /Applications/Hopper\ Disassembler\ v4.app
/Applications/Hopper Disassembler v4.app: accepted
source=Notarized Developer ID
```

Gatekeeper vs File Quarantine

- The most obvious difference between Gatekeeper and File Quarantine;
  - it is for a file that is executed, rather than just a file downloaded from the internet and trying to open it.
- File Quarantine does not perform **signature check**s.
- Gatekeeper first checks whether the application is signed. It then checks whether the signer is legitimate.



Gatekeeper Database

- Gatekeeper performs the controls from its own database, and it keeps a **blocklist** for applications.
- **/Library/Apple/System/Library/CoreServices/XProtect.bundle/Contents/Resources/gk.db**

```
→  ~ sqlite3 /Library/Apple/System/Library/CoreServices/XProtect.bundle/Contents/Resources/gk.db
SQLite version 3.39.5 2022-10-14 20:58:05
Enter ".help" for usage hints.
sqlite> .schema
CREATE TABLE settings (name TEXT, value TEXT, PRIMARY KEY (name));
CREATE TABLE blocked_hashes (hash BLOB, hash_type INTEGER, flags INTEGER, PRIMARY KEY (hash, hash_type));
CREATE TABLE blocked_teams (team_id TEXT, flags INTEGER, PRIMARY KEY (team_id));
sqlite>
sqlite> .table
blocked_hashes  blocked_teams   settings
sqlite>
```

Gatekeeper Database

```
→  ~ sqlite3 /Library/Apple/System/Library/CoreServices/XProtect.bundle/Contents/Resources/gk.db
SQLite version 3.39.5 2022-10-14 20:58:05
Enter ".help" for usage hints.
sqlite> .schema
CREATE TABLE settings (name TEXT, value TEXT, PRIMARY KEY (name));
CREATE TABLE blocked_hashes (hash BLOB, hash_type INTEGER, flags INTEGER, PRIMARY KEY (hash, hash_type));
CREATE TABLE blocked_teams (team_id TEXT, flags INTEGER, PRIMARY KEY (team_id));
sqlite>
sqlite> .table
blocked_hashes  blocked_teams   settings
sqlite>
```

Gatekeeper Database

- Blocked team id information is as follows.

```
sqlite> select * from blocked_teams LIMIT 10;
team_id|flags
F9X83Q5222|1
SS3YFP6RJ7|0
QC8B2PF82S|0
UQ5TUCT7AL|0
NZD5N78GXM|0
Q6XAB4776L|0
GQ65ME5KV3|0
8CHL2NLV6W|0
7698FPNAVX|0
DB6GMRL6AQ|0
```

Gatekeeper Database

```
sqlite> select * from blocked_teams LIMIT 10;
team_id|flags
F9X83Q5222|1
SS3YFP6RJ7|0
QC8B2PF82S|0
UQ5TUCT7AL|0
NZD5N78GXM|0
Q6XAB4776L|0
GQ65ME5KV3|0
8CHL2NLV6W|0
7698FPNAVX|0
DB6GMRL6AQ|0
```

Gatekeeper Database

```
sqlite> select * from blocked_teams LIMIT 10;
team_id|flags
F9X83Q5222|1
SS3YFP6RJ7|0
QC8B2PF82S|0
UQ5TUCT7AL|0
NZD5N78GXM|0
Q6XAB4776L|0
GQ65ME5KV3|0
8CHL2NLV6W|0
7698FPNAVX|0
DB6GMRL6AQ|0
```

Malware Detection
XProtect.bundle

Malware Detection – XProtect.bundle

- macOS has a built-in security tool called XProtect that provides **signature-based** detection.

Malware Detection – XProtect.bundle

- macOS has a built-in security tool called XProtect that provides **signature-based** detection.
- XProtect performs malware detection using **YARA** signatures.
  - YARA rules are regularly updated by Apple.

Malware Detection – XProtect.bundle

- macOS has a built-in security tool called XProtect that provides **signature-based** detection.
- XProtect performs malware detection using **YARA** signatures.
  - YARA rules are regularly updated by Apple.
- XProtect performs a continuous security scan of the macOS system, including in the following cases.
  - Launch a downloaded app for the first time
  - Change an app in the file system
  - XProtect signatures are updated

PICUS

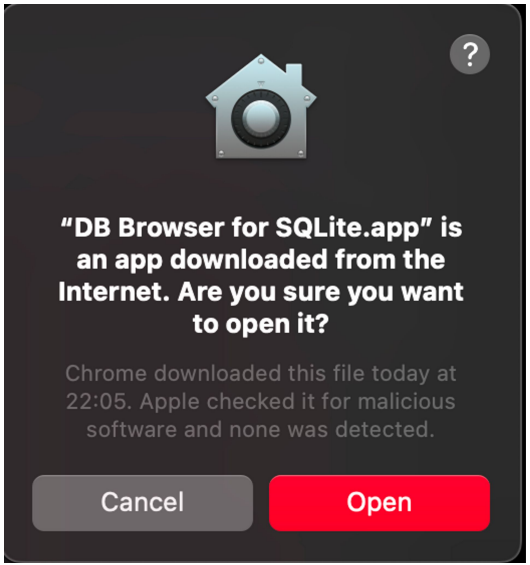
Malware Detection – XProtect.bundle

- macOS has a built-in security tool called XProtect that provides **signature-based** detection.
- XProtect performs malware detection using **YARA** signatures.
  - YARA rules are regularly updated by Apple.
- XProtect performs a continuous security scan of the macOS system, including in the following cases.
  - Launch a downloaded app for the first time
  - Change an app in the file system
  - XProtect signatures are updated
- **XProtect is included in File Quarantine technology.**

PICUS

Malware Detection – XProtect.bundle

- **Gatekeeper**
  - When an application downloaded from the Internet using an application sensitive to File Quarantine technology is opened, a warning appears in front of the user that the application is downloaded from the Internet.

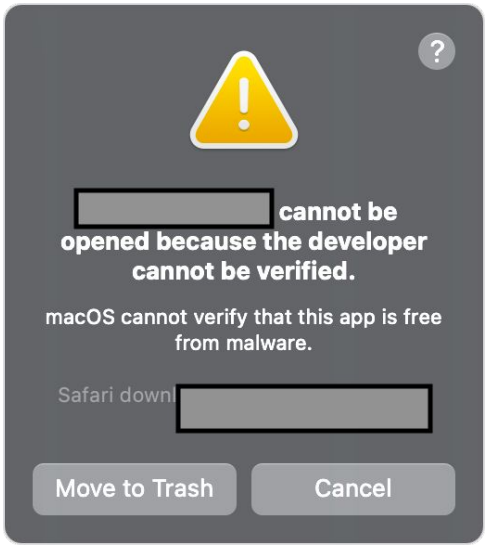


Malware Detection – XProtect.bundle

- **File Quarantine**
  - When this application downloaded from the Internet is run, File Quarantine technology checks whether the relevant application matches any of the signatures in XProtect.
  - If there is a match, another warning is displayed saying that running the application may harm the system.

Malware Detection – XProtect.bundle

- **Gatekeeper**
  - XProtect checks application files and file hashes against these signatures when the application is first launched or whenever it changes.
  - When XProtect detects a matching signature, it prevents the relevant code from running, and the user is informed of the option to delete the relevant application.



XProtect Files

- XProtect is included in macOS in **.bundle** format.
- **/Library/Apple/System/Library/CoreServices/XProtect.bundle**

```
➜  XProtect.bundle tree
.
└── Contents
    ├── Info.plist
    ├── Resources
    │   ├── LegacyEntitlementAllowlist.plist
    │   ├── XProtect.meta.plist
    │   ├── XProtect.plist
    │   ├── XProtect.yara
    │   └── gk.db
    ├── _CodeSignature
    │   ├── CodeDirectory
    │   ├── CodeRequirements
    │   ├── CodeRequirements-1
    │   ├── CodeResources
    │   └── CodeSignature
    └── version.plist

4 directories, 12 files
➜  XProtect.bundle
```

XProtect.yara

- This file contains Apple's built-in **YARA** rules.


```
import "hash"

private rule Macho
{
    meta:
        description = "private rule to match Mach-O binaries"
    condition:
        uint32(0) == 0xfeedface or uint32(0) == 0xcefaedfe or uint32(0) ==
0xfeedfacf or uint32(0) == 0xcffaedfe or uint32(0) == 0xcafebabe or
uint32(0) == 0xbebafeca

}

private rule PE
{
    meta:
        description = "private rule to match PE binaries"

    condition:
        uint16(0) == 0x5a4d and uint32(uint32(0x3C)) == 0x4550
}

private rule Dylib
{
    meta:
        description = "private rule to match Dylibs"

    condition:
        ((uint32(0) == 0xfeedface or uint32(0) == 0xfeedfacf) and
uint8(0xc) == 0x6) or
        (uint32(0) == 0xbebafeca and (uint32(0x4000) == 0xfeedface or
uint32(0x4000) == 0xfeedfacf) and uint8(0x400c) == 0x6)
}

rule XProtect_MACOS_644e18d
{
    meta:
        description = "MACOS.644e18d"
    strings:
        $a = { 63 6f 6e 6e 65 63 74 54 6f 50 72 6f 78 79 4d 61 6e 61 67 65
72 }
        $b = { 63 6f 6e 6e 65 63 74 54 6f 44 65 73 74 69 6e 61 74 69 6f 6e
}
        $c = { 68 65 61 72 74 62 65 61 74 53 65 6e 64 65 72 }
        $d = { 63 6f 6e 6e 65 63 74 54 6f 43 6e 63 }
        $e = { 70 72 6f 78 69 74 2e 63 6f 6d 2f 70 65 65 72 }
    condition:
        Macho and 2 of them
}
```

PICUS

XProtect.yara

```
rule XProtect_MACOS_644e18d
{
    meta:
        description = "MACOS.644e18d"
    strings:
        $a = { 63 6f 6e 6e 65 63 74 54 6f 50 72 6f 78 79 4d 61 6e 61 67 65
72 }
        $b = { 63 6f 6e 6e 65 63 74 54 6f 44 65 73 74 69 6e 61 74 69 6f 6e
}
        $c = { 68 65 61 72 74 62 65 61 74 53 65 6e 64 65 72 }
        $d = { 63 6f 6e 6e 65 63 74 54 6f 43 6e 63 }
        $e = { 70 72 6f 78 69 74 2e 63 6f 6d 2f 70 65 65 72 }
    condition:
        Macho and 2 of them
}
```

```
In [1]: import binascii

In [2]: pattern_1 = "636f6e6e656374546f50726f78794d616e61676572"

In [3]: pattern_2 = "636f6e6e656374546f44657374696e6174696f6e"

In [4]: pattern_3 = "686561727462656174536e646572"

In [5]: pattern_4 = "636f6e6e656374546f436e63"

In [6]: pattern_5 = "70726f7869742e636f6d2f70656572"

In [7]: binascii.unhexlify(pattern_1)
Out[7]: b'connectToProxyManager'

In [8]: binascii.unhexlify(pattern_2)
Out[8]: b'connectToDestination'

In [9]: binascii.unhexlify(pattern_3)
Out[9]: b'heartbeatSender'

In [10]: binascii.unhexlify(pattern_4)
Out[10]: b'connectToCnc'

In [11]: binascii.unhexlify(pattern_5)
Out[11]: b'proxit.com/peer'

In [12]:
```

PICUS

HACKTRICK
SİBER GÜVENLİK KONFERANSI

XProtect.meta.plist

- This **.plist** file contains information about malicious application plugins (Java, Flash, etc.) and harmful **Safari** extensions.
- Extension block definitions are made according to the bundle identifier and related **Developer ID** information.

```
<key>ExtensionBlacklist</key>
<dict>
    <key>Extensions</key>
    <array>
        <dict>
            <key>CFBundleIdentifier</key>
            <string>com.searchnt.safari</string>
            <key>Developer Identifier</key>
            <string>6ERPEMNB65</string>
        </dict>
        <dict>
            <key>CFBundleIdentifier</key>
            <string>com.shelfsick.safari</string>
            <key>Developer Identifier</key>
            <string>33HGJH7H8P</string>
        </dict>
        <dict>
            <key>CFBundleIdentifier</key>
            <string>com.searchnt.safari</string>
            <key>Developer Identifier</key>
            <string>LUZSN84HYP</string>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>ExtensionBlacklist</key>
    <dict>
        <key>Extensions</key>
        <array>
            <dict>
                <key>CFBundleIdentifier</key>
                <string>com.searchnt.safari</string>
                <key>Developer Identifier</key>
                <string>6ERPEMNB65</string>
            </dict>
            <dict>
                <key>CFBundleIdentifier</key>
                <string>com.shelfsick.safari</string>
                <key>Developer Identifier</key>
                <string>33HGJH7H8P</string>
            </dict>
            <dict>
                <key>CFBundleIdentifier</key>
                <string>com.searchnt.safari</string>
                <key>Developer Identifier</key>
                <string>LUZSN84HYP</string>
            </dict>
            <dict>
                <key>CFBundleIdentifier</key>
                <string>com.searchtrust.safariext</string>
                <key>Developer Identifier</key>
                <string>9V6HEQPZK3</string>
            </dict>
            <dict>
                <key>CFBundleIdentifier</key>
                <string>com.leperdvil.safari</string>
                <key>Developer Identifier</key>
                <string>Y7QR7RXE99</string>
            </dict>
            <dict>
                <key>CFBundleIdentifier</key>
                <string>info.trovi</string>
                <key>Developer Identifier</key>
                <string>2GLUU75QJH</string>
            </dict
```

PICUS

XProtect.meta.plist

- This **.plist** file contains information about malicious application plugins (Java, Flash, etc.) and harmful **Safari** extensions.
- Extension block definitions are made according to the bundle identifier and related **Developer ID** information.

```
<key>ExtensionBlacklist</key>
<dict>
    <key>Extensions</key>
    <array>
        <dict>
            <key>CFBundleIdentifier</key>
            <string>com.searchnt.safari</string>
            <key>Developer Identifier</key>
            <string>6ERPEMNB65</string>
        </dict>
        <dict>
            <key>CFBundleIdentifier</key>
            <string>com.shelfsick.safari</string>
            <key>Developer Identifier</key>
            <string>33HGJH7H8P</string>
        </dict>
        <dict>
            <key>CFBundleIdentifier</key>
            <string>com.searchnt.safari</string>
            <key>Developer Identifier</key>
            <string>LUZSN84HYP</string>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>ExtensionBlacklist</key>
    <dict>
        <key>Extensions</key>
        <array>
            <dict>
                <key>CFBundleIdentifier</key>
                <string>com.searchnt.safari</string>
                <key>Developer Identifier</key>
                <string>6ERPEMNB65</string>
            </dict>
            <dict>
                <key>CFBundleIdentifier</key>
                <string>com.shelfsick.safari</string>
                <key>Developer Identifier</key>
                <string>33HGJH7H8P</string>
            </dict>
            <dict>
                <key>CFBundleIdentifier</key>
                <string>com.searchnt.safari</string>
                <key>Developer Identifier</key>
                <string>LUZSN84HYP</string>
            </dict>
            <dict>
                <key>CFBundleIdentifier</key>
                <string>com.searchtrust.safariext</string>
                <key>Developer Identifier</key>
                <string>9V6HEQPZK3</string>
            </dict>
            <dict>
                <key>CFBundleIdentifier</key>
                <string>com.leperdvil.safari</string>
                <key>Developer Identifier</key>
                <string>Y7QR7RXE99</string>
            </dict>
            <dict>
                <key>CFBundleIdentifier</key>
                <string>info.trovi</string>
                <key>Developer Identifier</key>
                <string>2GLUU75QJH</string>
            </dict
```

PICUS

XProtect.plist

- This **.plist** file contains information about the application bundle and the harmful content in it.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<array>
    <dict>
        <key>Description</key>
        <string>OSX.28a9883</string>
        <key>LaunchServices</key>
        <dict>
            <key>LSItemContentType</key>
            <string>com.apple.application-bundle</string>
        </dict>
        <key>Matches</key>
        <array>
            <dict>
                <key>MatchFile</key>
                <dict>
                    <key>NSURLTypeIdentifierKey</key>
                    <string>public.unix-executable</string>
                </dict>
                <key>MatchType</key>
                <string>Match</string>
                <key>Pattern</key>
                <string>3A6C6162656C3A706C697374506174683A</string>
            </dict>
            <dict>
                <key>MatchFile</key>
                <dict>
                    <key>NSURLTypeIdentifierKey</key>
                    <string>public.unix-executable</string>
                </dict>
                <key>MatchType</key>
                <string>Match</string>
                <key>Pattern</key>
                <string>3A62696E3A706C6973743A</string>
            </dict>
            <dict>
                <key>MatchFile</key>
                <dict>
                    <key>NSURLTypeIdentifierKey</key>
                    <string>public.unix-executable</string>
                </dict>
                <key>MatchType</key>
                <string>Match</string>
                <key>Pattern</key>


<string>214023247E5E262A28295B5D7B7D3A3B3C3E2C2E3171327733653472357436793775
3869396F3070415A535844434656474248 4E4A4D4B4C5157455254595549</string>
            </dict>
        </array>
    </dict>
```

XProtect.plist

- OSX.GenieoDropper.A

```
<dict>
        <key>Description</key>
        <string>OSX.GenieoDropper.A</string>
        <key>LaunchServices</key>
        <dict>
            <key>LSItemContentType</key>
            <string>com.apple.application-bundle</string>
        </dict>
        <key>Matches</key>
        <array>
            <dict>
                <key>MatchFile</key>
                <dict>
                    <key>NSURLNameKey</key>
                    <string>mxp.min.js</string>
                </dict>
                <key>MatchType</key>
                <string>Match</string>
                <key>Pattern</key>

<string>66756E6374696F6E20416363657074F666665727328297B</string>
            </dict>
            <dict>
                <key>MatchFile</key>
                <dict>
                    <key>NSURLNameKey</key>
                    <string>main.js</string>
                </dict>
                <key>MatchType</key>
                <string>Match</string>
                <key>Pattern</key>

<string>747261636B416E616C79746963734576656E74282265786563757469 6F6E222C224A7352756E22293B</string>
            </dict>
        </array>
    </dict>
```

PICUS

OSX.GenieoDropper.A

```
<key>LaunchServices</key>
<dict>
    <key>LSItemContentType</key>
    <string>com.apple.application-bundle</string>
</dict>
```

```
        <key>Matches</key>
        <array>
            <dict>
                <key>MatchFile</key>
                <dict>
                    <key>NSURLNameKey</key>
                    <string>mxp.min.js</string>
                </dict>
                <key>MatchType</key>
                <string>Match</string>
                <key>Pattern</key>

<string>66756E6374696F6E20416363657074F666665727328297B</string>
            </dict>
            <dict>
                <key>MatchFile</key>
                <dict>
                    <key>NSURLNameKey</key>
                    <string>main.js</string>
                </dict>
                <key>MatchType</key>
                <string>Match</string>
                <key>Pattern</key>

<string>747261636B416E616C79746963734576656E74282265786563757469 6F6E222C22
4A7352756E22293B</string>
```

OSX.GenieoDropper.A

```
In [1]: import binascii

In [2]: pattern_1 = "66756E6374696F6E204163636570744F666665727328297B"

In [3]: pattern_2 = "747261636B416E616C797469637345766 56E74282265786563757469 6F6E222C224A7352756E22293B"

In [4]: binascii.unhexlify(pattern_1)
Out[4]: b'function AcceptOffers(){'

In [5]: binascii.unhexlify(pattern_2)
Out[5]: b'trackAnalyticsEvent("execution","JsRun");'

In [6]:
```

LegacyEntitlementAllowlist.plist

- This plist file is undocumented by Apple.
- It is seen that only **cdhash** information is included in the plist.
- **cdhash:** The code directory hash identifies a specific version of a program. This allows the system to verify that the contents of a binary have not changed since being code-signed.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>cdhashes</key>
    <array>
        <data>
        AAFd7LJtQHNzgvxZ5kOMf5kNDVo=
        </data>
        <data>
        AAQCJMThA3BGcNrYDj3cGpx+i3U=
        </data>
        <data>
        AAQYbKSnpJxvCtTZc7cRC9Jo+bQ=
        </data>
        <data>
        AAUzQNGkVn8nJMreEIqz4P0lahI=
        </data>
        <data>
        AAxqo7k51G/ak+Xg9hNNo61LqVI=
        </data>
        <data>
        ABBEGu7ZCbgrt3IAqg7k15zBR1Q=
        </data>
        <data>
        ABDXjTxbm1MVYk88ANcOTl7j8Qc=
        </data>
```

XProtect Unified Logs

- Unified logs of XProtect events can be examined as follows.
- **log show -info -backtrace -debug -loss -signpost -predicate 'subsystem == "com.apple.xprotect"'**

```
→  Resources log show -info -backtrace -debug -loss -signpost -predicate 'subsystem == "com.apple.xprotect"'
Filtering the log data using "subsystem == "com.apple.xprotect""
Timestamp                       Thread     Type        Activity            PID    TTL
2023-07-25 10:18:29.333291+0300 0xa99a96   Default     0x0                 16243  0    XprotectService: [com.apple.xprotect:xprotect] Using meta-plist from: /Library/Apple/System/Library/CoreServices/XProtect.bundle/Contents/Resources/XProtect.meta.plist
2023-07-25 15:31:28.508133+0300 0xac5616   Default     0x0                 33771  0    XProtectBehaviorService: [com.apple.xprotect:behavior] Reported 1 behavioral events
2023-07-26 09:43:53.874430+0300 0xaf2d6d   Error       0x0                 49700  0    XprotectService: [com.apple.xprotect:xprotect] File /tmp/KSInstallAction.x3xRLxijsa/m/.patch/goobspatch failed on loadCmd /tmp/KSInstallAction.x3xRLxijsa/m/.patch/liblzma
d resolved to: /private/tmp/KSInstallAction.x3xRLxijsa/m/.patch/liblzma_decompress.dylib, bundleURL: (null))
2023-07-26 09:44:03.464553+0300 0xaf3731   Error       0x0                 49700  0    XprotectService: [com.apple.xprotect:xprotect] File /tmp/KSInstallAction.x3xRLxijsa/m/.patch/xzdec failed on loadCmd /tmp/KSInstallAction.x3xRLxijsa/m/.patch/liblzma_deco
olved to: /private/tmp/KSInstallAction.x3xRLxijsa/m/.patch/liblzma_decompress.dylib, bundleURL: (null))
2023-07-26 09:44:09.309864+0300 0xaf3c79   Default     0x0                 51507  0    XProtectBehaviorService: [com.apple.xprotect:behavior] Processed behavioral violation for process redacted event
2023-07-26 15:34:30.055479+0300 0xb3a5df   Default     0x0                 76424  0    XProtectBehaviorService: [com.apple.xprotect:behavior] Reported 1 behavioral events
2023-07-27 08:34:08.847517+0300 0xbfee39   Signpost    0x0                 49386  0    [spid 0x1, process, begin] XprotectService: [com.apple.xprotect:signposts] XprotectAssessment
2023-07-27 08:34:08.847537+0300 0xbfee39   Signpost    0x0                 49386  0    [spid 0x1, process, event] XprotectService: [com.apple.xprotect:signposts] URL: <private>
2023-07-27 08:34:08.847537+0300 0xbfee39   Signpost    0x0                 49386  0    [spid 0x1, process, event] XprotectService: [com.apple.xprotect:signposts] AssessmentClass: 0
2023-07-27 08:34:08.847549+0300 0xbfee39   Info        0x0                 49386  0    XprotectService: [com.apple.xprotect:xprotect] Xprotect is performing a direct malware and dylib scan: <private>
2023-07-27 08:34:08.891767+0300 0xbfe686   Info        0x0                 359    0    syspolicyd: (XprotectFramework) [com.apple.xprotect:xprotect] Invalidated
2023-07-27 08:34:08.891934+0300 0xbfee39   Info        0x0                 49386  0    XprotectService: [com.apple.xprotect:xprotect] Invalidated service side
---------------------------------------------------------------------------------------------------------------
Log      - Default:          4, Info:               3, Debug:            0, Error:          2, Fault:          0
Activity - Create:           0, Transition:         0, Actions:          0
→  Resources
```

Malware Removal Tool – MRT

Malware Removal Tool – MRT

- MRT is another built-in anti-malware tool for macOS.
- macOS 10.8.3
- MRT checks the malware database regularly updated by Apple and removes infections.
- Similar to XProtect, MRT is activated automatically at system startup.
- **/Library/Apple/System/Library/CoreServices/MRT.app**

```
→  MRT.app pwd
/Library/Apple/System/Library/CoreServices/MRT.app
→  MRT.app
→  MRT.app tree
.
└── Contents
    ├── Frameworks
    │   ├── libswiftAppKit.dylib
    │   ├── libswiftCore.dylib
    │   ├── libswiftCoreData.dylib
    │   ├── libswiftCoreFoundation.dylib
    │   ├── libswiftCoreGraphics.dylib
    │   ├── libswiftCoreImage.dylib
    │   ├── libswiftDarwin.dylib
    │   ├── libswiftDispatch.dylib
    │   ├── libswiftFoundation.dylib
    │   ├── libswiftIOKit.dylib
    │   ├── libswiftMetal.dylib
    │   ├── libswiftObjectiveC.dylib
    │   ├── libswiftQuartzCore.dylib
    │   ├── libswiftXPC.dylib
    │   └── libswiftos.dylib
    ├── Info.plist
    ├── MacOS
    │   ├── MRT
    │   └── mrt-helper
    ├── PkgInfo
    ├── Resources
    │   ├── Info.plist
    │   ├── ar.lproj
    │   │   ├── Localizable.strings
    │   │   └── locversion.plist
    │   ├── ca.lproj
    │   │   ├── Localizable.strings
    │   │   └── locversion.plist
    │   ├── cs.lproj
    │   │   ├── Localizable.strings
    │   │   └── locversion.plist
```

Reversing MRT Application

```
                        aOsxatg2a:
00000001001502b2            db      "OSX.ATG2.A", 0                         ; DATA XREF=sub_1000284d0+138
00000001001502bd            db      "", 0
00000001001502be            db      "", 0
00000001001502bf            db      "", 0
                        aLibrarylauncha_1001502c0:      // aLibrarylauncha
00000001001502c0            db      "~/Library/LaunchAgents/com.apple.updater.plist", 0 ; DATA XREF=sub_1000284d0+340
00000001001502ef            db      "", 0
                        aUsersshareddufh:
00000001001502f0            db      "/Users/Shared/dufh", 0                 ; DATA XREF=sub_1000284d0+498
0000000100150303            db      "", 0
0000000100150304            db      "", 0
0000000100150305            db      "", 0
0000000100150306            db      "", 0
0000000100150307            db      "", 0
0000000100150308            db      "", 0
0000000100150309            db      "", 0
000000010015030a            db      "", 0
000000010015030b            db      "", 0
000000010015030c            db      "", 0
000000010015030d            db      "", 0
000000010015030e            db      "", 0
000000010015030f            db      "", 0
                        aLibrarylauncha_100150310:      // aLibrarylauncha
0000000100150310            db      "~/Library/LaunchAgents/com.apple.updates.plist", 0 ; DATA XREF=sub_1000284d0+641
000000010015033f            db      "", 0
                        aUserssharedloc:
0000000100150340            db      "/Users/Shared/.local/kextd", 0         ; DATA XREF=sub_1000284d0+764
000000010015035b            db      "", 0
```

PICUS

HACKTRICK
SİBER GÜVENLİK KONFERANSI

Reversing MRT Application

```
                        aOsxatg2a:
00000001001502b2            db      "OSX.ATG2.A", 0                 ; DATA XREF=sub_1000284d0+138
00000001001502bd            db      "", 0
00000001001502be            db      "", 0
00000001001502bf            db      "", 0
                        aLibrarylaunch_1001502c0:       // aLibrarylauncha
00000001001502c0            db      "~/Library/LaunchAgents/com.apple.updater.plist", 0 ; DATA XREF=sub_1000284d0+340
00000001001502ef            db      "", 0
                        aUsersshareduf:
00000001001502f0            db      "/Users/Shared/dufh", 0         ; DATA XREF=sub_1000284d0+498
0000000100150303            db      "", 0
0000000100150304            db      "", 0
0000000100150305            db      "", 0
0000000100150306            db      "", 0
0000000100150307            db      "", 0
0000000100150308            db      "", 0
0000000100150309            db      "", 0
000000010015030a            db      "", 0
000000010015030b            db      "", 0
000000010015030c            db      "", 0
000000010015030d            db      "", 0
000000010015030e            db      "", 0
000000010015030f            db      "", 0
                        aLibrarylauncha_100150310:      // aLibrarylauncha
0000000100150310            db      "~/Library/LaunchAgents/com.apple.updates.plist", 0 ; DATA XREF=sub_1000284d0+641
000000010015033f            db      "", 0
                        aUserssharedloc:
0000000100150340            db      "/Users/Shared/.local/kextd", 0 ; DATA XREF=sub_1000284d0+764
000000010015035b            db      "", 0
```

PICUS

HACKTRICK
SİBER GÜVENLİK KONFERANSI

Reversing MRT Application

```
                        aOsxatg2a:
00000001001502b2            db      "OSX.ATG2.A", 0                 ; DATA XREF=sub_1000284d0+138
00000001001502bd            db      "", 0
00000001001502be            db      "", 0
00000001001502bf            db      "", 0
                        aLibrarylauncha_1001502c0:      // aLibrarylauncha
00000001001502c0            db      "~/Library/LaunchAgents/com.apple.updater.plist", 0 ; DATA XREF=sub_1000284d0+340
00000001001502ef            db      "", 0
                        aUsersshareddufh:
00000001001502f0            db      "/Users/Shared/dufh", 0         ; DATA XREF=sub_1000284d0+498
0000000100150303            db      "", 0
0000000100150304            db      "", 0
0000000100150305            db      "", 0
0000000100150306            db      "", 0
0000000100150307            db      "", 0
0000000100150308            db      "", 0
0000000100150309            db      "", 0
000000010015030a            db      "", 0
000000010015030b            db      "", 0
000000010015030c            db      "", 0
000000010015030d            db      "", 0
000000010015030e            db      "", 0
000000010015030f            db      "", 0
                        aLibrarylauncha_100150310:      // aLibrarylauncha
0000000100150310            db      "~/Library/LaunchAgents/com.apple.updates.plist", 0 ; DATA XREF=sub_1000284d0+641
000000010015033f            db      "", 0
                        aUsersshareddloc:
0000000100150340            db      "/Users/Shared/.local/kextd", 0 ; DATA XREF=sub_1000284d0+764
000000010015035b            db      "", 0
```

Reversing MRT Application

```
                        aOsxatg2a:
00000001001502b2            db      "OSX.ATG2.A", 0                 ; DATA XREF=sub_1000284d0+138
00000001001502bd            db      "", 0
00000001001502be            db      "", 0
00000001001502bf            db      "", 0
                        aLibrarylauncha_1001502c0:      // aLibrarylauncha
00000001001502c0            db      "~/Library/LaunchAgents/com.apple.updater.plist", 0 ; DATA XREF=sub_1000284d0+340
00000001001502ef            db      "", 0
                        aUsersshareddufh:
00000001001502f0            db      "/Users/Shared/dufh", 0         ; DATA XREF=sub_1000284d0+498
0000000100150303            db      "", 0
0000000100150304            db      "", 0
0000000100150305            db      "", 0
0000000100150306            db      "", 0
0000000100150307            db      "", 0
0000000100150308            db      "", 0
0000000100150309            db      "", 0
000000010015030a            db      "", 0
000000010015030b            db      "", 0
000000010015030c            db      "", 0
000000010015030d            db      "", 0
000000010015030e            db      "", 0
000000010015030f            db      "", 0
                        aLibrarylauncha_100150310:      // aLibrarylauncha
0000000100150310            db      "~/Library/LaunchAgents/com.apple.updates.plist", 0 ; DATA XREF=sub_1000284d0+641
000000010015033f            db      "", 0
                        aUserssharedloc:
0000000100150340            db      "/Users/Shared/.local/kextd", 0 ; DATA XREF=sub_1000284d0+764
000000010015035b            db      "", 0
```

PICUS

HACKTRICK
SİBER GÜVENLİK KONFERANSI

Reversing MRT Application

```
                        aOsxatg2a:
00000001001502b2            db      "OSX.ATG2.A", 0                 ; DATA XREF=sub_1000284d0+138
00000001001502bd            db      "", 0
00000001001502be            db      "", 0
00000001001502bf            db      "", 0
                        aLibrarylauncha_1001502c0:      // aLibrarylauncha
00000001001502c0            db      "~/Library/LaunchAgents/com.apple.updater.plist", 0 ; DATA XREF=sub_1000284d0+340
00000001001502ef            db      "", 0
                        aUsersshareddufh:
00000001001502f0            db      "/Users/Shared/dufh", 0         ; DATA XREF=sub_1000284d0+498
0000000100150303            db      "", 0
0000000100150304            db      "", 0
0000000100150305            db      "", 0
0000000100150306            db      "", 0
0000000100150307            db      "", 0
0000000100150308            db      "", 0
0000000100150309            db      "", 0
000000010015030a            db      "", 0
000000010015030b            db      "", 0
000000010015030c            db      "", 0
000000010015030d            db      "", 0
000000010015030e            db      "", 0
000000010015030f            db      "", 0
                        aLibrarylauncha_100150310:      // aLibrarylauncha
0000000100150310            db      "~/Library/LaunchAgents/com.apple.updates.plist", 0 ; DATA XREF=sub_1000284d0+641
000000010015033f            db      "", 0
                        aUsersshared_0:
0000000100150340            db      "/Users/Shared/.local/kextd", 0 ; DATA XREF=sub_1000284d0+764
000000010015035b            db      "", 0
```

PICUS

HACKTRICK
SİBER GÜVENLİK KONFERANSI

Reversing MRT Application

```
int sub_1000d0160(int arg0) {
    swift_retain(r13);
    swift_retain(r13);
    *(r13 + 0x40) = Swift.String.init("~/Library/LaunchAgents/com.Mughthesec.plist", 0x2b, 0x1);
    *(r13 + 0x48) = 0x1;
    swift_release(r13);
    *(r13 + 0x50) = Swift.String.init("~/Library/Application Support/com.Mughthesec/Mughthesec", 0x37, 0x1);
    *(r13 + 0x58) = 0x1;
    swift_release(r13);
    swift_retain(sub_1000a2530(arg0 & 0xff));
    swift_retain(rax);
    var_50 = Swift.String.init("OSX.Mughthesec.A", 0x10, 0x1);
    swift_bridgeObjectRetain(0x1);
    swift_beginAccess(rax + 0x10, &var_30, 0x21, 0x0);
    rdi = *(rax + 0x18);
    *(rax + 0x10) = var_50;
    *(rax + 0x18) = 0x1;
    swift_bridgeObjectRelease(rdi);
    swift_endAccess(&var_30);
    swift_bridgeObjectRelease(0x1);
    swift_release(rax);
    swift_release(rax);
    rax = rax;
    return rax;
}
```

Reversing MRT Application

```
int sub_1000d0160(int arg0) {
    swift_retain(r13);
    swift_retain(r13);
    *(r13 + 0x40) = Swift.String.init("~/Library/LaunchAgents/com.Mughthesec.plist", 0x2b, 0x1);
    *(r13 + 0x48) = 0x1;
    swift_release(r13);
    *(r13 + 0x50) = Swift.String.init("~/Library/Application Support/com.Mughthesec/Mughthesec", 0x37, 0x1);
    *(r13 + 0x58) = 0x1;
    swift_release(r13);
    swift_retain(sub_1000a2530(arg0 & 0xff));
    swift_retain(rax);
    var_50 = Swift.String.init("OSX.Mughthesec.A", 0x10, 0x1);
    swift_bridgeObjectRetain(0x1);
    swift_beginAccess(rax + 0x10, &var_30, 0x21, 0x0);
    rdi = *(rax + 0x18);
    *(rax + 0x10) = var_50;
    *(rax + 0x18) = 0x1;
    swift_bridgeObjectRelease(rdi);
    swift_endAccess(&var_30);
    swift_bridgeObjectRelease(0x1);
    swift_release(rax);
    swift_release(rax);
    rax = rax;
    return rax;
}
```

Reversing MRT Application

```
int sub_1000d0160(int arg0) {
    swift_retain(r13);
    swift_retain(r13);
    *(r13 + 0x40) = Swift.String.init("~/Library/LaunchAgents/com.Mughthesec.plist", 0x2b, 0x1);
    *(r13 + 0x48) = 0x1;
    swift_release(r13);
    *(r13 + 0x50) = Swift.String.init("~/Library/Application Support/com.Mughthesec/Mughthesec", 0x37, 0x1);
    *(r13 + 0x58) = 0x1;
    swift_release(r13);
    swift_retain(sub_1000a2530(arg0 & 0xff));
    swift_retain(rax);
    var_50 = Swift.String.init("OSX.Mughthesec.A", 0x10, 0x1);
    swift_bridgeObjectRetain(0x1);
    swift_beginAccess(rax + 0x10, &var_30, 0x21, 0x0);
    rdi = *(rax + 0x18);
    *(rax + 0x10) = var_50;
    *(rax + 0x18) = 0x1;
    swift_bridgeObjectRelease(rdi);
    swift_endAccess(&var_30);
    swift_bridgeObjectRelease(0x1);
    swift_release(rax);
    swift_release(rax);
    rax = rax;
    return rax;
}
```

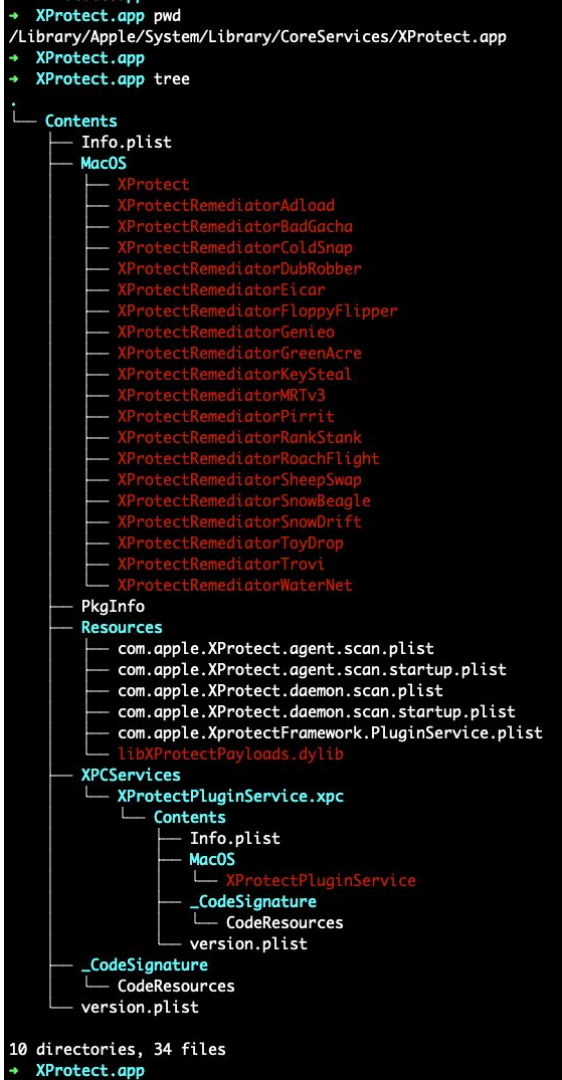
Reversing MRT Application

```
int sub_1000d0160(int arg0) {
    swift_retain(r13);
    swift_retain(r13);
    *(r13 + 0x40) = Swift.String.init("~/Library/LaunchAgents/com.Mughthesec.plist", 0x2b, 0x1);
    *(r13 + 0x48) = 0x1;
    swift_release(r13);
    *(r13 + 0x50) = Swift.String.init("~/Library/Application Support/com.Mughthesec/Mughthesec", 0x37, 0x1);
    *(r13 + 0x58) = 0x1;
    swift_release(r13);
    swift_retain(sub_1000a2530(arg0 & 0xff));
    swift_retain(rax);
    var_50 = Swift.String.init("OSX.Mughthesec.A", 0x10, 0x1);
    swift_bridgeObjectRetain(0x1);
    swift_beginAccess(rax + 0x10, &var_30, 0x21, 0x0);
    rdi = *(rax + 0x18);
    *(rax + 0x10) = var_50;
    *(rax + 0x18) = 0x1;
    swift_bridgeObjectRelease(rdi);
    swift_endAccess(&var_30);
    swift_bridgeObjectRelease(0x1);
    swift_release(rax);
    swift_release(rax);
    rax = rax;
    return rax;
}
```

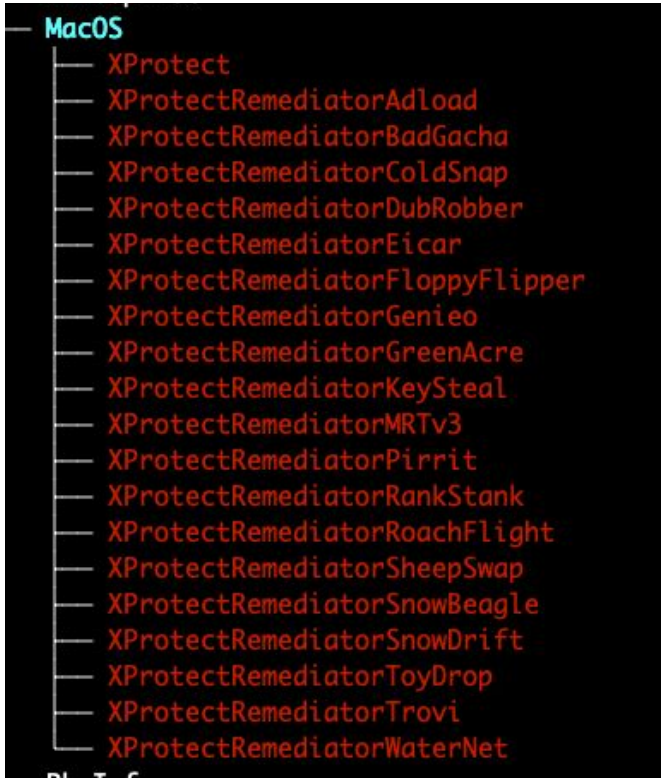
XProtect Remediator
XProtect.app

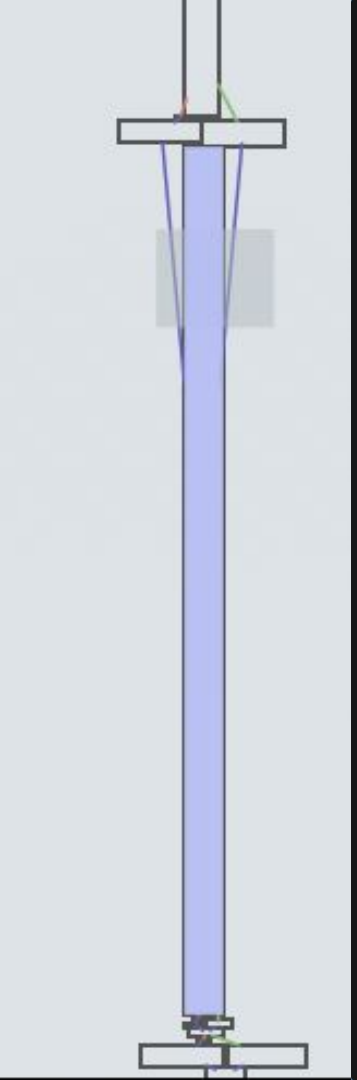
XProtect Remediator – XProtect.app

- macOS 12.3
- XProtect Remediator is reminiscent of **MRT** in the sense that it is an application package, but it contains different binaries for different malware.
- Different binaries for different malware are in **XProtectRemediator<FAMILY_NAME>** format.
- The main differences between MRT and XProtect Remediator are as follows.
  - MRT only works during the reboot and login phases.
  - XProtect Remediator scans at regular intervals.



XProtect Remediator – XProtect.app





```
int sub_100118cf0(int arg0, int arg1) {
    var_2C9 = arg0;
    memset(&var_10, 0x0, 0x1);
    memset(&var_18, 0x0, 0x8);
    var_18 = Swift.Array.init(sub_1000c68d0());
    if ((var_2C9 & 0x1) == 0x0) {
            var_300 = Swift.String.init("Agent start.", 0xc, 0x1);
            var_2F8 = Swift._allocateUninitializedArray<A>(0x0,
sub_10000f760(0x100202948));
            Foundation.NSLog(var_300, 0x1, var_2F8);
            swift_bridgeObjectRelease(var_2F8);
            swift_bridgeObjectRelease(0x1);
    }
    else {
            var_2E8 = Swift.String.init("Daemon start.", 0xd, 0x1);
            var_2E0 = Swift._allocateUninitializedArray<A>(0x0,
sub_10000f760(0x100202948));
            Foundation.NSLog(var_2E8, 0x1, var_2E0);
            swift_bridgeObjectRelease(var_2E0);
            swift_bridgeObjectRelease(0x1);
    }
    sub_100066000(0x1, 0x1);
    swift_beginAccess(sub_100037c10(), &var_30, 0x21, 0x0);
    *(int8_t *)rdi = var_2C9 & 0x1;
    swift_endAccess(&var_30);
    sub_1000fa2a0();
    var_38 = sub_1000f6ef0(var_2C9 & 0xff);
    Swift.Array.append(&var_38, sub_10000f760(0x10020d908));
    sub_1000a9d70();
    var_40 = sub_1000a8390(var_2C9 & 0xff);
    Swift.Array.append(&var_40, rsi);
    sub_1000b08b0();
    var_48 = sub_1000ad2d0(var_2C9 & 0xff);
    Swift.Array.append(&var_48, rsi);
    sub_1000ad2b0();
    var_50 = sub_1000a9d90(var_2C9 & 0xff);
    Swift.Array.append(&var_50, rsi);
    ....
    Swift.Array.append(&var_2B8, rsi);
    sub_1000c5210();
    var_2C0 = sub_1000c4110(var_2C9 & 0xff);
    Swift.Array.append(&var_2C0, rsi);
    sub_1000c3320();
    var_2C8 = sub_1000c1cc0(var_2C9 & 0xff);
    Swift.Array.append(&var_2C8, rsi);
    swift_bridgeObjectRetain(var_18);
    sub_100118260(var_18, 0x1);
    swift_bridgeObjectRelease(var_18);
    swift_bridgeObjectRetain(var_18);
    sub_100118260(var_18, 0x0);
    swift_bridgeObjectRelease(var_18);
    if ((var_2C9 & 0x1) != 0x0) {
            sub_10001bc90();
            sub_10001c080();
    }
    if ((var_2C9 & 0x1) == 0x0) {
            var_358 = Swift.String.init("Agent finished.", 0xf, 0x1);
            var_350 = Swift._allocateUninitializedArray<A>(0x0,
sub_10000f760(0x100202948));
            Foundation.NSLog(var_358, 0x1, var_350);
            swift_bridgeObjectRelease(var_350);
            swift_bridgeObjectRelease(0x1);
    }
    else {
            var_340 = Swift.String.init("Daemon finished.", 0x10, 0x1);
            var_338 = Swift._allocateUninitializedArray<A>(0x0,
sub_10000f760(0x100202948));
            Foundation.NSLog(var_340, 0x1, var_338);
            swift_bridgeObjectRelease(var_338);
            swift_bridgeObjectRelease(0x1);
    }
    sub_100066000(0x0, 0x1);
    rax = sub_10011a220(&var_18);
    return rax;
}
```

```
loc_10011a184:
lea     rdi, qword [aAgentFinished] ; "Agent finished.", CODE XREF=sub_100118cf0+5147
mov     esi, 0xf
mov     edx, 0x1
call    imp___stubs__$sSS21_builtinStringLiteral17utf8CodeUnitCount7isASCIISSBp_BwBi1_tcfC ; Swift.S
mov     qword [rbp+var_358], rax
mov     qword [rbp+var_348], rdx
lea     rdi, qword [qword_100202940+8] ; argument #1 for method sub_10000f760, 0x100202948
call    sub_10000f760 ; sub_10000f760
mov     rsi, rax
xor     eax, eax
mov     edi, eax
call    imp___stubs__$ss27_allocateUninitializedArrayySayxG_BptBwlF ; Swift._allocateUninitializedAr
mov     rdi, qword [rbp+var_358]
mov     rsi, qword [rbp+var_348]
mov     qword [rbp+var_350], rax
mov     rdx, qword [rbp+var_350]
call    imp___stubs__$s10Foundation5NSLogyySS_s7CVarArg_pdtF ; Foundation.NSLog(Swift.String, Swift.
mov     rdi, qword [rbp+var_350] ; argument "ptr" for method imp___stubs__swift_bridgeObjectRelease
call    imp___stubs__swift_bridgeObjectRelease ; swift_bridgeObjectRelease
mov     rdi, qword [rbp+var_348] ; argument "ptr" for method imp___stubs__swift_bridgeObjectRelease
call    imp___stubs__swift_bridgeObjectRelease ; swift_bridgeObjectRelease
```

XProtect Remediator – XProtect.app

- log show -info -backtrace -debug -loss -signpost -predicate 'subsystem == "com.apple.XProtectFramework.PluginAPI" && category == "XPEvent.structured"'

```
~ log show -info -backtrace -debug -loss -signpost -predicate 'subsystem == "com.apple.XProtectFramework.PluginAPI" && category == "XPEvent.structured"'
Filtering the log data using "subsystem == "com.apple.XProtectFramework.PluginAPI" AND category == "XPEvent.structured""
Timestamp                       Thread     Type        Activity             PID    TTL
2023-07-25 12:09:44.709808+0300 0xaafcff   Default     0x0                  24149  0    XProtectRemediatorSnowDrift: [com.apple.XProtectFramework.PluginAPI:XPEvent.structured] {"caused_by":[],"status_message":"NoThreatDetected","status_code":20,"execution_duration":0.000121951103210
44922}
2023-07-25 12:09:44.806791+0300 0xaafd07   Default     0x0                  24150  0    XProtectRemediatorTrovi: [com.apple.XProtectFramework.PluginAPI:XPEvent.structured] {"caused_by":[],"status_message":"NoThreatDetected","status_code":20,"execution_duration":9.1910362243652344e-0
5}
2023-07-25 12:09:44.807373+0300 0xaafd07   Default     0x0                  24150  0    XProtectRemediatorTrovi: [com.apple.XProtectFramework.PluginAPI:XPEvent.structured] {"caused_by":[],"status_message":"NoThreatDetected","status_code":20,"execution_duration":1.2040138244628906e-0
5}
2023-07-25 12:09:44.807833+0300 0xaafd07   Default     0x0                  24150  0    XProtectRemediatorTrovi: [com.apple.XProtectFramework.PluginAPI:XPEvent.structured] {"caused_by":[],"status_message":"NoThreatDetected","status_code":20,"execution_duration":1.2040138244628906e-0
5}
2023-07-25 12:09:50.114298+0300 0xaafd0b   Default     0x0                  24151  0    XProtectRemediatorRoachFlight: [com.apple.XProtectFramework.PluginAPI:XPEvent.structured] {"caused_by":[],"status_message":"NoThreatDetected","status_code":20,"execution_duration":0.0001100301742
5537109}
2023-07-25 12:10:13.467412+0300 0xaafd6c   Default     0x0                  24160  0    XProtectRemediatorMRTv3: [com.apple.XProtectFramework.PluginAPI:XPEvent.structured] {"caused_by":[],"status_message":"Success","status_code":0,"execution_duration":0.000187039375305175 78}
2023-07-25 12:10:13.998327+0300 0xab0022   Default     0x0                  24214  0    XProtectRemediatorPirrit: [com.apple.XProtectFramework.PluginAPI:XPEvent.structured] {"caused_by":[],"status_message":"NoThreatDetected","status_code":20,"execution_duration":9.703636169433593 8e-
05}
2023-07-25 12:10:15.022154+0300 0xab003d   Default     0x0                  24217  0    XProtectRemediatorGreenAcre: [com.apple.XProtectFramework.PluginAPI:XPEvent.structured] {"caused_by":[],"status_message":"NoThreatDetected","status_code":20,"execution_duration":0.000139951705932
61719}
2023-07-25 12:10:15.134089+0300 0xab004e   Default     0x0                  24219  0    XProtectRemediatorFloppyFlipper: [com.apple.XProtectFramework.PluginAPI:XPEvent.structured] {"caused_by":[],"status_message":"NoThreatDetected","status_code":20,"execution_duration":7.2956085205 0
78125e-05}
2023-07-25 12:10:15.393322+0300 0xab0051   Default     0x0                  24220  0    XProtectRemediatorKeySteal: [com.apple.XProtectFramework.PluginAPI:XPEvent.structured] {"caused_by":[],"status_message":"NoThreatDetected","status_code":20,"execution_duration":6.5922737121582031
e-05}
2023-07-25 12:10:15.650702+0300 0xab0056   Default     0x0                  24221  0    XProtectRemediatorToyDrop: [com.apple.XProtectFramework.PluginAPI:XPEvent.structured] {"caused_by":[],"status_message":"NoThreatDetected","status_code":20,"execution_duration":0.000130057334899 90
234}
2023-07-25 12:10:15.780344+0300 0xab0060   Default     0x0                  24223  0    XProtectRemediatorBadGacha: [com.apple.XProtectFramework.PluginAPI:XPEvent.structured] {"process":{"pid":3322,"name":"Python"},"status":null,"action":"report"}
2023-07-25 12:10:15.781366+0300 0xab0060   Default     0x0                  24223  0    XProtectRemediatorBadGacha: [com.apple.XProtectFramework.PluginAPI:XPEvent.structured] {"process":{"pid":3321,"name":"Python"},"status":null,"action":"report"}
2023-07-25 12:10:15.781889+0300 0xab0060   Default     0x0                  24223  0    XProtectRemediatorBadGacha: [com.apple.XProtectFramework.PluginAPI:XPEvent.structured] {"process":{"pid":3318,"name":"Python"},"status":null,"action":"report"}
2023-07-25 12:10:15.782375+0300 0xab0060   Default     0x0                  24223  0    XProtectRemediatorBadGacha: [com.apple.XProtectFramework.PluginAPI:XPEvent.structured] {"process":{"pid":3317,"name":"Python"},"status":null,"action":"report"}
2023-07-25 12:10:15.782864+0300 0xab0060   Default     0x0                  24223  0    XProtectRemediatorBadGacha: [com.apple.XProtectFramework.PluginAPI:XPEvent.structured] {"process":{"pid":3281,"name":"Python"},"status":null,"action":"report"}
2023-07-25 12:10:15.788554+0300 0xab0060   Default     0x0                  24223  0    XProtectRemediatorBadGacha: [com.apple.XProtectFramework.PluginAPI:XPEvent.structured] {"caused_by":[],"status_message":"NoThreatDetected","status_code":20,"execution_duration":0.000213980674743 6
5234}
2023-07-25 12:10:22.239344+0300 0xab0069   Default     0x0                  24224  0    XProtectRemediatorColdSnap: [com.apple.XProtectFramework.PluginAPI:XPEvent.structured] {"caused_by":[],"status_message":"NoThreatDetected","status_code":20,"execution_duration":0.001304984092712 4
023}
```

Behavioral Detection
Bastion Rules

Behavioral Detection – BastionRules

- Apple has released a new XProtect module with macOS **Ventura**.
- With this module, it is seen that XProtect has a behavioral detection feature.
- **/var/protected/xprotect/XPdb**

```
sqlite> select * from events limit 5;
id|violated_rule|exec_path|exec_cdhash|exec_signing_id|exec_team_id|exec_sha256|exec_is_notarized|responsible_path|responsible_cdhash|responsible_signing_id|responsible_team_id|responsible_sha256|responsible_is_notarized|reported|profile_hash|dt
181|BastionRule-2|/System/Library/CoreServices/Finder.app/Contents/MacOS/Finder|a2cf1bc3d168da1ddb7e133cb12ad8559899b980|com.apple.finder||4483e1369e992a7794a8861d9de307387c80c3461df457a27a5bacf16cdd5dbb|0|/System/Library/CoreServices/Finder.app/Contents
ddb7e133cb12ad8559899b980|com.apple.finder||4483e1369e992a7794a8861d9de307387c80c3461df457a27a5bacf16cdd5dbb|0|1|599809884939O627319|2023-07-02 19:38:25
182|BastionRule-3|/Library/Application Support/Logitech.localized/LogiOptionsPlus/logioptionsplus_agent.app/Contents/MacOS/logioptionsplus_agent|2d56ebf1ec5f830aeba2c7f5f7d7e40f7f2dc4c3|com.logi.cp-dev-mgr|QED4VVPZWA|b9de006b0d3d197ddf982cf67ca6209e0954d
|/Library/Application Support/Logitech.localized/LogiOptionsPlus/logioptionsplus_agent.app/Contents/MacOS/logioptionsplus_agent|2d56ebf1ec5f830aeba2c7f5f7d7e40f7f2dc4c3|com.logi.cp-dev-mgr|QED4VVPZWA|b9de006b0d3d197ddf982cf67ca6209e0954d97940a855fb122571
27319|2023-07-02 19:38:27
183|BastionRule-2|/usr/sbin/lsof|62c8e638c90f2fe3672d89cb134f37a010561e29|com.apple.lsof||f8a6987f682de1174ece536deaa9da730b5103ef4af086a45c9c533068296709|0|/Applications/GlobalProtect.app/Contents/Resources/PanGPS|b1d7ba5c62e6aa44d8d9300075888275907689
bec78b7a501ee3ac0effdd5467390ad7cba0a1bd524ea008998ad83|1|1|599809884939O627319|2023-07-02 19:38:29
184|BastionRule-2|/Applications/Slack.app/Contents/MacOS/Slack|7dd86b1ab350424dfc22ec43aaf613e3a3bae0fe|com.tinyspeck.slackmacgap|BQR82RBBHL|f2ca9375f15bf46d98dccc90c5dab5f07dacf50de207c1edd061c37db0894336|1|/Applications/Slack.app/Contents/MacOS/Slack|7
e3a3bae0fe|com.tinyspeck.slackmacgap|BQR82RBBHL|f2ca9375f15bf46d98dccc90c5dab5f07dacf50de207c1edd061c37db0894336|1|1|599809884939O627319|2023-07-02 19:38:52
185|BastionRule-2|/Library/SystemExtensions/03C1EE2E-EEFB-45CD-9C4E-A7E7445112C1/com.crowdstrike.falcon.Agent.systemextension/Contents/MacOS/com.crowdstrike.falcon.Agent|8f33a1a8ffeb0fadc520377800c695a864c5f4d8|com.crowdstrike.falcon.Agent|X9E956P446|d32
ebf8d7cdfaa9dd50cc2744ffcd18adc0|1|/Library/SystemExtensions/03C1EE2E-EEFB-45CD-9C4E-A7E7445112C1/com.crowdstrike.falcon.Agent.systemextension/Contents/MacOS/com.crowdstrike.falcon.Agent|8f33a1a8ffeb0fadc520377800c695a864c5f4d8|com.crowdstrike.falcon.Age
e66f5008911f0e790ebf8d7cdfaa9dd50cc2744ffcd18adc0|1|1|599809884939O627319|2023-07-02 19:38:52
sqlite>
```

PICUS

HACKTRICK
SİBER GÜVENLİK KONFERANSI

BastionRules

XProtect Behavioral Service

```
sqlite> select * from events limit 2;
                        id = 503
           violated_rule = macOS.QntDb.Generic
               exec_path =
/System/Library/CoreServices/Spotlight.app/Contents/MacOS/Spotlight
             exec_cdhash = 26317b0f7f9ef98f1ed010b91ada7c34ee25bad9
          exec_signing_id = com.apple.Spotlight
             exec_team_id =
              exec_sha256 =
68a9b26e43612a754d51f95cfc14a004ff6dff343ed95df027319f51910c34f6
         exec_is_notarized = 0
          responsible_path =
/System/Library/CoreServices/Spotlight.app/Contents/MacOS/Spotlight
       responsible_cdhash = 26317b0f7f9ef98f1ed010b91ada7c34ee25bad9
  responsible_signing_id = com.apple.Spotlight
     responsible_team_id =
      responsible_sha256 =
68a9b26e43612a754d51f95cfc14a004ff6dff343ed95df027319f51910c34f6
responsible_is_notarized = 0
                reported = 0
            profile_hash = 5810994513396451325
                      dt = 2024-04-14 19:47:10

                        id = 504
           violated_rule = macOS.Browser.Generic
               exec_path =
/Applications/Firefox.app/Contents/MacOS/firefox
             exec_cdhash = e62be0819844a853790ef2427237cdd07676bc84
          exec_signing_id = org.mozilla.firefox
             exec_team_id = 43AQ936H96
              exec_sha256 =
18b815cf09ee08f3cab164f4cb05f75563b5b62bff68b9930289063c0456d1c1
         exec_is_notarized = 1
          responsible_path =
/Applications/Firefox.app/Contents/MacOS/firefox
       responsible_cdhash = e62be0819844a853790ef2427237cdd07676bc84
  responsible_signing_id = org.mozilla.firefox
     responsible_team_id = 43AQ936H96
      responsible_sha256 =
18b815cf09ee08f3cab164f4cb05f75563b5b62bff68b9930289063c0456d1c1
responsible_is_notarized = 1
                reported = 0
            profile_hash = 5810994513396451325
                      dt = 2024-04-14 19:47:17
sqlite>
```

PICUS

HACKTRICK
SİBER GÜVENLİK KONFERANSI

Reversing XProtect Daemon

- XPdb and XProtect activities, in general, are handled by the **System Configuration Policy Daemon - syspolicyd**.

```
/* @class SandboxManager */
-(void)registerBastionProfile {
    r15 = self;
    rax = [self->_profileURL path];
    rax = [rax retain];
    var_60 = 0x0;
    r12 = [[NSString stringWithContentsOfFile:rax encoding:0x4 error:r8] retain];
    r14 = [var_60 retain];
    [rax release];
    if (r12 == 0x0) {
            rax = [SPLog exec];
            rax = [rax retain];
            rbx = rax;
            if (os_log_type_enabled(rax, 0x1) != 0x0) {
                    rax = *(r15 + 0x10);
                    var_50 = 0x8400202;
                    *(&var_50 + 0x4) = r14;
                    *(int16_t *)(&var_50 + 0xc) = 0x840;
                    *(&var_50 + 0xe) = rax;
                    _os_log_impl(__mh_execute_header, rbx, 0x1, "Error retrieving profile: %@ at URL %@, registering the default xprotect profile", &var_50, 0x16);
            }
            [rbx release];
            r12 = [*qword_1000d5930 retain];
    }
    var_58 = 0x0;
    rax = [r15 compileSandboxProfileWithVersion:&var_58 withProfile:r12];
    rbx = rax;
    if (rax != 0x0) {
            rax = 0x0;
            asm { bswap      rax };
            [r15 unregisterBastionProfile];
            [r15 sendNewBastionProfileVersionToKernel:rax];
            [r15 registerBastionProfile:rbx];
    }
    var_30 = **___stack_chk_guard;
    [r12 release];
    [r14 release];
    if (**___stack_chk_guard != var_30) {
            __stack_chk_fail();
    }
    return;
}
```

Reversing XProtect Daemon

```
00000001000b09d2        db      "SystemPolicyConfiguration", 0              ; DATA XREF=-[XPBundle loadFromBundleData:]+801
                aNversion3nnall:
00000001000b09ec        db      "\n(version 3)\n\n(allow default job-creation file-write-setugid)\n(allow file-test-existence)\n\n(define (system-binary signing-id)\n  (require-all\n    (signing-identifier signing-id)\n    (process-attribute is-platform-binary)))\n\n(define
00000001000b0aec        db      " (require-any\n    (system-binary \"com.apple.imagent\")\n    (system-binary \"com.apple.imtransferservices.IMTransferAgent\")\n    (system-binary \"com.apple.fseventsd\")\n    (system-binary \"com.apple.mds\")\n    (system-binary \"com.appl
00000001000b0bec        db      " \"com.apple.XProtectFramework.plugins.MRTv3\")\n    (system-binary \"com.apple.MRT\")\n    (system-binary \"com.apple.XProtectFramework.plugins.Pirrit\")\n    (system-binary \"com.apple.mdworker_shared\")\n    (system-binary \"com.apple.jet
00000001000b0cec        db      "inary \"com.apple.diskarbitrationd\")\n    (system-binary \"com.apple.StorageManagement.Service\")\n    (system-binary \"com.apple.dt.IDECacheDeleteAppExtension\")\n    (system-binary \"com.apple.STMExtension.Applications\")\n    (system-bi
00000001000b0dec        db      "ement.Service\")\n    (system-binary \"com.apple.coreservices.uiagent\")\n    (system-binary \"com.apple.imdpersistence.IMDPersistenceAgent\")))\n\n(define rule-one-offenders\n  (require-any\n    (system-binary \"com.apple.Safari.PasswordBre
00000001000b0eec        db      "ry \"com.apple.Safari.History\")\n    (system-binary \"com.apple.Safari.CacheDeleteExtension\")\n    (system-binary \"com.apple.Finder\")\n    (system-binary \"com.apple.SafariBookmarksSyncAgent\")\n    (system-binary \"com.apple.UserEventAg
00000001000b0fec        db      "m.apple.appkit.xpc.openAndSavePanelService\")\n    (system-binary \"com.apple.SafariNotificationAgent\")\n    (system-binary \"com.apple.dt.SKAgent\")\n    (system-binary \"com.apple.backupd\")\n    (system-binary \"com.apple.STMExtension.De
00000001000b10ec        db      "y \"com.apple.STMExtension.Mail\")\n    (system-binary \"com.apple.Safari\")))\n\n(define rule-two-offenders\n  (require-any\n    (system-binary \"com.apple.suggestd\")\n    (system-binary \"com.apple.IMAutomaticHistoryDeletionAgent\")\n
00000001000b11ec        db      "leSMS\")\n    (system-binary \"com.apple.MobileSMS.spotlight\")\n    (system-binary \"com.apple.photolibraryd\")\n    (system-binary \"com.apple.Spotlight\")\n    (system-binary \"com.apple.coreduetd\")\n    (system-binary \"com.apple.filecc
00000001000b12ec        db      "ry \"com.apple.Safari.SandboxBroker\")\n    (system-binary \"com.apple.quicklook.ThumbnailsAgent\")\n    (system-binary \"com.apple.messages.StorageManagementExtension\")\n    (system-binary \"com.apple.corespotlightd\")\n    (system-binary
00000001000b13ec        db      "fine rule-three-offenders\n  (require-any\n    (system-binary \"com.apple.Safari\")\n    (system-binary \"com.apple.cfprefsd\")\n    (system-binary \"com.apple.mail\")\n    (system-binary \"com.apple.lsd\")\n    (system-binary \"com.apple.sh
00000001000b14ec        db      "om.apple.dataaccess.dataaccessd\")\n    (system-binary \"com.apple.defaults\")))\n\n(with-filter\n  (require-not (require-any bastion-usual-offenders rule-one-offenders))\n    (allow (with user-approval \"BastionRule-1\") file*\n      (subpa
00000001000b15ec        db      "ry/Application Support/Google/Chrome/Default/\"))\n    (allow (with user-approval \"BastionRule-1\") file*\n      (subpath \"${ANY_USER_HOME}/Library/Application Support/Firefox/Profiles/\"))\n    (allow (with user-approval \"BastionRule-1\"
00000001000b16ec        db      "{ANY_USER_HOME}/Library/Safari/\")))\n\n(with-filter\n  (require-not (require-any bastion-usual-offenders rule-two-offenders))\n    (allow (with user-approval \"BastionRule-2\") file*\n      (subpath \"${ANY_USER_HOME}/Library/Messages/\"))\
00000001000b17ec        db      "roval \"BastionRule-2\") file*\n      (subpath \"${ANY_USER_HOME}/Library/Application Support/Microsoft/Teams/\"))\n    (allow (with user-approval \"BastionRule-2\") file*\n      (subpath \"${ANY_USER_HOME}/Library/Application Support/Slack/
00000001000b18ec        db      "~approval \"BastionRule-2\") file*\n      (subpath \"${ANY_USER_HOME}/Library/Application Support/WhatsApp/\")))\n\n(with-filter\n  (require-not (require-any bastion-usual-offenders rule-three-offenders))\n    (allow (with user-approval \"Ba
00000001000b19ec        db      " (literal \"${ANY_USER_HOME}/Library/Preferences/com.apple.LaunchServices.QuarantineEventsV2\")))\n\n(with-filter\n  (require-not (process-attribute is-platform-binary))\n    (allow (with user-approval \"BastionRule-4\") socket-ioctl\n
00000001000b1aec        db      "ATE SIOCGIFDESC)))\n", 0
```

PICUS

HACKTRICK
SİBER GÜVENLİK KONFERANSI

```
(version 3)

(allow default job-creation file-write-setugid)
(allow file-test-existence)

(define (system-binary signing-id)
  (require-all
    (signing-identifier signing-id)
    (process-attribute is-platform-binary)))

(define bastion-usual-offenders

 (require-any
    (system-binary \"com.apple.imagent\")
    (system-binary \"com.apple.imtransferservices.IMTransferAgent\")
    (system-binary \"com.apple.fseventsd\")
    (system-binary \"com.apple.mds\")
    (system-binary \"com.apple.mdsync\")
    (system-binary \"com.apple.XProtectFramework.plugins.MRTv3\")
    (system-binary \"com.apple.MRT\")
    (system-binary \"com.apple.XProtectFramework.plugins.Pirrit\")
    (system-binary \"com.apple.mdworker_shared\")
    (system-binary \"com.apple.jetsam_priority\")
    (system-binary \"com.apple.diskarbitrationd\")
    (system-binary \"com.apple.StorageManagement.Service\")
    (system-binary \"com.apple.dt.IDECacheDeleteAppExtension\")
    (system-binary \"com.apple.STMExtension.Applications\")
    (system-binary \"com.apple.StorageManagement.Service\")
    (system-binary \"com.apple.coreservices.uiagent\")
    (system-binary \"com.apple.imdpersistence.IMDPersistenceAgent\")))

(define rule-one-offenders
  (require-any
    (system-binary \"com.apple.Safari.PasswordBreachAgent\")
    (system-binary \"com.apple.Safari.History\")
    (system-binary \"com.apple.Safari.CacheDeleteExtension\")
    (system-binary \"com.apple.Finder\")
    (system-binary \"com.apple.SafariBookmarksSyncAgent\")
    (system-binary \"com.apple.UserEventAgent\")
    (system-binary \"com.apple.appkit.xpc.openAndSavePanelService\")
    (system-binary \"com.apple.SafariNotificationAgent\")
    (system-binary \"com.apple.dt.SKAgent\")
    (system-binary \"com.apple.backupd\")
    (system-binary \"com.apple.STMExtension.Developer\")
    (system-binary \"com.apple.STMExtension.Mail\")
    (system-binary \"com.apple.Safari\")))
```

```
(define rule-two-offenders
  (require-any
    (system-binary \"com.apple.suggestd\")
    (system-binary \"com.apple.IMAutomaticHistoryDeletionAgent\")
    (system-binary \"com.apple.MobileSMS\")
    (system-binary \"com.apple.MobileSMS.spotlight\")
    (system-binary \"com.apple.photolibraryd\")
    (system-binary \"com.apple.Spotlight\")
    (system-binary \"com.apple.coreduetd\")
    (system-binary \"com.apple.filecoordinationd\")
    (system-binary \"com.apple.Safari.SandboxBroker\")
    (system-binary \"com.apple.quicklook.ThumbnailsAgent\")
    (system-binary \"com.apple.messages.StorageManagementExtension\")
    (system-binary \"com.apple.corespotlightd\")
    (system-binary \"com.apple.mdwrite\")))

(define rule-three-offenders
  (require-any
    (system-binary \"com.apple.Safari\")
    (system-binary \"com.apple.cfprefsd\")
    (system-binary \"com.apple.mail\")
    (system-binary \"com.apple.lsd\")
    (system-binary \"com.apple.sharingd\")
    (system-binary \"com.apple.dataaccess.dataaccessd\")
    (system-binary \"com.apple.defaults\")))

(with-filter
  (require-not (require-any bastion-usual-offenders rule-one-offenders))
    (allow (with user-approval \"BastionRule-1\") file*
      (subpath \"${ANY_USER_HOME}/Library/Application Support/Google/Chrome/Default/\"))
    (allow (with user-approval \"BastionRule-1\") file*
      (subpath \"${ANY_USER_HOME}/Library/Application Support/Firefox/Profiles/\"))
    (allow (with user-approval \"BastionRule-1\") file*
      (subpath \"${ANY_USER_HOME}/Library/Safari/\")))

(with-filter
  (require-not (require-any bastion-usual-offenders rule-two-offenders))
    (allow (with user-approval \"BastionRule-2\") file*
      (subpath \"${ANY_USER_HOME}/Library/Messages/\"))
    (allow (with user-approval \"BastionRule-2\") file*
      (subpath \"${ANY_USER_HOME}/Library/Application Support/Microsoft/Teams/\"))
    (allow (with user-approval \"BastionRule-2\") file*
      (subpath \"${ANY_USER_HOME}/Library/Application Support/Slack/\"))
    (allow (with user-approval \"BastionRule-2\") file*
      (subpath \"${ANY_USER_HOME}/Library/Application Support/WhatsApp/\")))
```

BastionRules

- There are four types of Bastion rules.
- For example, with the **BastionRule-1** type rule, it is understood that the application movements in the **~/Library/Application Support/** directory are followed.
- In macOS Ventura, these behaviors are not blocked; they are saved in the XPdb database.

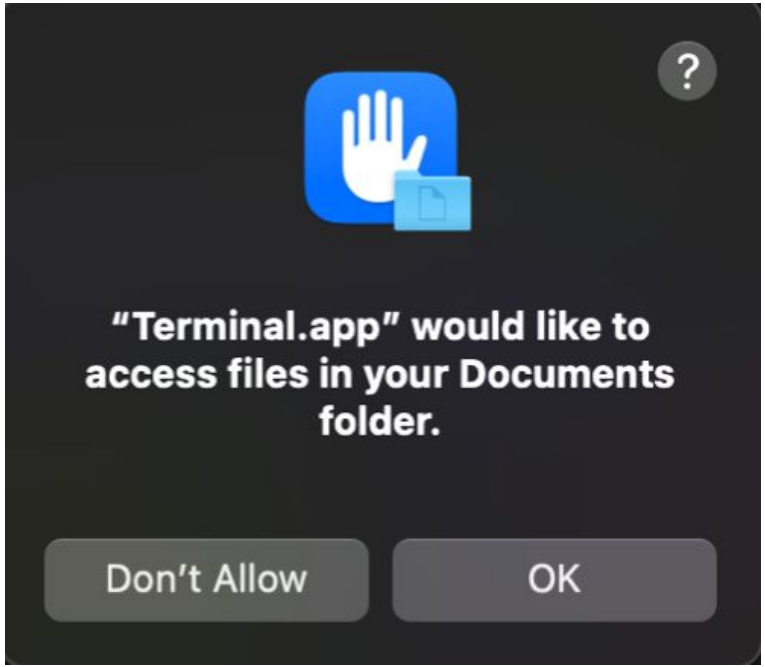
```
(with-filter
  (require-not (require-any bastion-usual-offenders rule-one-offenders))
    (allow (with user-approval \"BastionRule-1\") file*
      (subpath \"${ANY_USER_HOME}/Library/Application Support/Google/Chrome/Default/\"))
    (allow (with user-approval \"BastionRule-1\") file*
      (subpath \"${ANY_USER_HOME}/Library/Application Support/Firefox/Profiles/\"))
    (allow (with user-approval \"BastionRule-1\") file*
      (subpath \"${ANY_USER_HOME}/Library/Safari/\")))

(with-filter
  (require-not (require-any bastion-usual-offenders rule-two-offenders))
    (allow (with user-approval \"BastionRule-2\") file*
      (subpath \"${ANY_USER_HOME}/Library/Messages/\"))
    (allow (with user-approval \"BastionRule-2\") file*
      (subpath \"${ANY_USER_HOME}/Library/Application Support/Microsoft/Teams/\"))
    (allow (with user-approval \"BastionRule-2\") file*
      (subpath \"${ANY_USER_HOME}/Library/Application Support/Slack/\"))
    (allow (with user-approval \"BastionRule-2\") file*
      (subpath \"${ANY_USER_HOME}/Library/Application Support/WhatsApp/\")))

(with-filter
  (require-not (require-any bastion-usual-offenders rule-three-offenders))
    (allow (with user-approval \"BastionRule-3\") file*

 (literal \"${ANY_USER_HOME}/Library/Preferences/com.apple.LaunchServices.QuarantineEventsV2\")))

(with-filter
  (require-not (process-attribute is-platform-binary))
    (allow (with user-approval \"BastionRule-4\") socket-ioctl
      (ioctl-command SIOCIFCREATE SIOCGIFDESC)))
```

Malware Response in Apple

- When new malware is discovered, the following steps takes.
  - Any associated Developer ID certificates are revoked.
  - Notarization revocation tickets are issued for all files (apps and associated files).
  - XProtect signatures are developed and released.

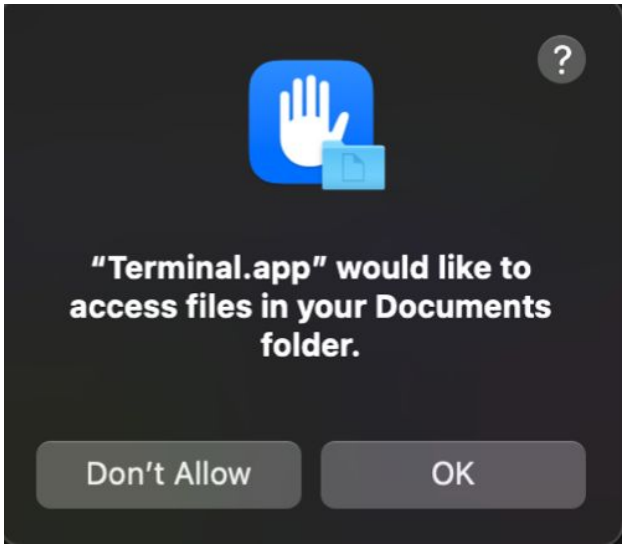
PICUS

Transparency, Consent, and Control – TCC



Transparency, Consent, and Control – TCC

- Security protocol focusing on regulating application permissions.
- Safeguard sensitive features
  - Location services
  - Contacts
  - Photos
  - Microphone
  - Camera
  - Accessibility
  - **Full Disk Access**



Transparency, Consent, and Control – TCC

TCC Daemon

```
➜  ~ cat /System/Library/LaunchDaemons/com.apple.tccd.system.plist
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>Label</key>
    <string>com.apple.tccd.system</string>
    <key>ProgramArguments</key>
    <array>
        <string>/System/Library/PrivateFrameworks/TCC.framework/Support/tccd</string>
        <string>system</string>
    </array>
    <key>MachServices</key>
    <dict>
        <key>com.apple.tccd.system</key>
        <true/>
    </dict>
    <key>POSIXSpawnType</key>
    <string>Adaptive</string>
    <key>EnablePressuredExit</key>
    <true/>
    <key>PublishesEvents</key>
    <dict>
        <key>com.apple.tccd.events</key>
        <dict>
            <key>DomainInternal</key>
            <true/>
        </dict>
    </dict>
</dict>
</plist>
➜  ~
```

TCC Daemon

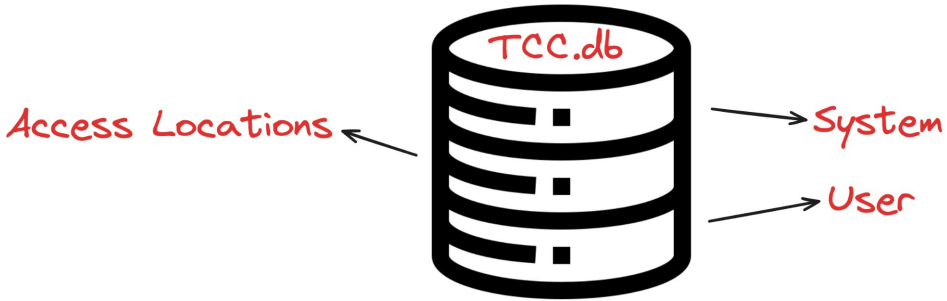
```
➜  ~ cat /System/Library/LaunchDaemons/com.apple.tccd.system.plist
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>Label</key>
    <string>com.apple.tccd.system</string>
    <key>ProgramArguments</key>
    <array>
        <string>/System/Library/PrivateFrameworks/TCC.framework/Support/tccd</string>
        <string>system</string>
    </array>
    <key>MachServices</key>
    <dict>
        <key>com.apple.tccd.system</key>
        <true/>
    </dict>
    <key>POSIXSpawnType</key>
    <string>Adaptive</string>
    <key>EnablePressuredExit</key>
    <true/>
    <key>PublishesEvents</key>
    <dict>
        <key>com.apple.tccd.events</key>
        <dict>
            <key>DomainInternal</key>
            <true/>
        </dict>
    </dict>
</dict>
</plist>
➜  ~
```

TCC Daemon

```
➜  ~ cat /System/Library/LaunchDaemons/com.apple.tccd.system.plist
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>Label</key>
    <string>com.apple.tccd.system</string>
    <key>ProgramArguments</key>
    <array>
        <string>/System/Library/PrivateFrameworks/TCC.framework/Support/tccd</string>
        <string>system</string>
    </array>
    <key>MachServices</key>
    <dict>
        <key>com.apple.tccd.system</key>
        <true/>
    </dict>
    <key>POSIXSpawnType</key>
    <string>Adaptive</string>
    <key>EnablePressuredExit</key>
    <true/>
    <key>PublishesEvents</key>
    <dict>
        <key>com.apple.tccd.events</key>
        <dict>
            <key>DomainInternal</key>
            <true/>
        </dict>
    </dict>
</dict>
</plist>
➜  ~
```

TCC Databases

- System
  - **/Library/Application Support/com.apple.TCC/TCC.db**
- User
  - **$HOME/Library/Application Support/com.apple.TCC/TCC.db**
- Access Locations
  - **/var/db/locationd/clients.plist**



TCC Database

```
➜  ~ sqlite3 /Library/Application\ Support/com.apple.TCC/TCC.db
SQLite version 3.39.5 2022-10-14 20:58:05
Enter ".help" for usage hints.
sqlite> .tables
access            active_policy     expired
access_overrides  admin             policies
sqlite>
```

TCC Database

```
➜  ~ sqlite3 /Library/Application\ Support/com.apple.TCC/TCC.db
SQLite version 3.39.5 2022-10-14 20:58:05
Enter ".help" for usage hints.
sqlite> .tables
access            active_policy     expired
access_overrides  admin             policies
sqlite>
```

TCC Database

```
➜  ~ sqlite3 /Library/Application\ Support/com.apple.TCC/TCC.db
SQLite version 3.39.5 2022-10-14 20:58:05
Enter ".help" for usage hints.
sqlite> .tables
access            active_policy     expired
access_overrides  admin             policies
sqlite>
```

TCC Database

```
sqlite> select client, auth_reason, auth_value, service from access;
client|auth_reason|auth_value|service
us.zoom.xos|5|0|kTCCServiceSystemPolicyAllFiles
/Library/PrivilegedHelperTools/us.zoom.ZoomDaemon|5|0|kTCCServiceSystemPolicyAllFiles
com.apple.Terminal|4|0|kTCCServiceDeveloperTool
/Applications/Zscaler/Zscaler.app/Contents/PlugIns/ZscalerTunnel|5|0|kTCCServiceSystemPolicyAllFile
com.logi.cp-dev-mgr|4|2|kTCCServiceListenEvent
com.logi.cp-dev-mgr|4|2|kTCCServiceAccessibility
com.apple.XProtectFramework.XProtect|5|0|kTCCServiceSystemPolicyAllFiles
com.google.Keystone.Agent|5|0|kTCCServiceSystemPolicyAllFiles
com.logitech.logitune|4|2|kTCCServiceListenEvent
us.zoom.xos|4|2|kTCCServiceScreenCapture
com.tinyspeck.slackmacgap|4|2|kTCCServiceScreenCapture
com.tinyspeck.slackmacgap|5|0|kTCCServiceSystemPolicyAllFiles
us.zoom.ZoomAutoUpdater|5|0|kTCCServiceSystemPolicyAllFiles
WhatsApp|5|0|kTCCServiceSystemPolicyAllFiles
com.google.Chrome|4|0|kTCCServiceScreenCapture
com.vmware.fusion|4|2|kTCCServiceAccessibility
WhatsApp|4|0|kTCCServicePostEvent
us.zoom.xos|4|2|kTCCServiceAccessibility
com.vmware.fusion|4|2|kTCCServiceSystemPolicyAllFiles
com.googlecode.iterm2|4|2|kTCCServiceEndpointSecurityClient
com.apple.Terminal|4|2|kTCCServiceSystemPolicyAllFiles
com.microsoft.VSCode|5|0|kTCCServiceSystemPolicyAllFiles
com.hnc.Discord|6|0|kTCCServiceListenEvent
com.loom.desktop|6|0|kTCCServiceScreenCapture
net.whatsapp.WhatsApp|5|0|kTCCServiceSystemPolicyAllFiles
com.google.Chrome|5|0|kTCCServiceSystemPolicyAllFiles
com.logi.cp-dev-mgr|4|0|kTCCServiceScreenCapture
/Library/PrivilegedHelperTools/com.microsoft.autoupdate.helper|5|0|kTCCServiceSystemPolicyAllFiles
com.teamviewer.TeamViewer|6|0|kTCCServiceScreenCapture
sqlite>
```

TCC Database

```
sqlite> select client, auth_reason, auth_value, service from access;
client|auth_reason|auth_value|service
us.zoom.xos|5|0|kTCCServiceSystemPolicyAllFiles
/Library/PrivilegedHelperTools/us.zoom.ZoomDaemon|5|0|kTCCServiceSystemPolicyAllFiles
com.apple.Terminal|4|0|kTCCServiceDeveloperTool
/Applications/Zscaler/Zscaler.app/Contents/PlugIns/ZscalerTunnel|5|0|kTCCServiceSystemPolicyAllFile
com.logi.cp-dev-mgr|4|2|kTCCServiceListenEvent
com.logi.cp-dev-mgr|4|2|kTCCServiceAccessibility
com.apple.XProtectFramework.XProtect|5|0|kTCCServiceSystemPolicyAllFiles
com.google.Keystone.Agent|5|0|kTCCServiceSystemPolicyAllFiles
com.logitech.logitune|4|2|kTCCServiceListenEvent
us.zoom.xos|4|2|kTCCServiceScreenCapture
com.tinyspeck.slackmacgap|4|2|kTCCServiceScreenCapture
com.tinyspeck.slackmacgap|5|0|kTCCServiceSystemPolicyAllFiles
us.zoom.ZoomAutoUpdater|5|0|kTCCServiceSystemPolicyAllFiles
WhatsApp|5|0|kTCCServiceSystemPolicyAllFiles
com.google.Chrome|4|0|kTCCServiceScreenCapture
com.vmware.fusion|4|2|kTCCServiceAccessibility
WhatsApp|4|0|kTCCServicePostEvent
us.zoom.xos|4|2|kTCCServiceAccessibility
com.vmware.fusion|4|2|kTCCServiceSystemPolicyAllFiles
com.googlecode.iterm2|4|2|kTCCServiceEndpointSecurityClient
com.apple.Terminal|4|2|kTCCServiceSystemPolicyAllFiles
com.microsoft.VSCode|5|0|kTCCServiceSystemPolicyAllFiles
com.hnc.Discord|6|0|kTCCServiceListenEvent
com.loom.desktop|6|0|kTCCServiceScreenCapture
net.whatsapp.WhatsApp|5|0|kTCCServiceSystemPolicyAllFiles
com.google.Chrome|5|0|kTCCServiceSystemPolicyAllFiles
com.logi.cp-dev-mgr|4|0|kTCCServiceScreenCapture
/Library/PrivilegedHelperTools/com.microsoft.autoupdate.helper|5|0|kTCCServiceSystemPolicyAllFiles
com.teamviewer.TeamViewer|6|0|kTCCServiceScreenCapture
sqlite>
```

TCC Database

```
sqlite> select client, auth_reason, auth_value, service from access;
client|auth_reason|auth_value|service
us.zoom.xos|5|0|kTCCServiceSystemPolicyAllFiles
/Library/PrivilegedHelperTools/us.zoom.ZoomDaemon|5|0|kTCCServiceSystemPolicyAllFiles
com.apple.Terminal|4|0|kTCCServiceDeveloperTool
/Applications/Zscaler/Zscaler.app/Contents/PlugIns/ZscalerTunnel|5|0|kTCCServiceSystemPolicyAllFile
com.logi.cp-dev-mgr|4|2|kTCCServiceListenEvent
com.logi.cp-dev-mgr|4|2|kTCCServiceAccessibility
com.apple.XProtectFramework.XProtect|5|0|kTCCServiceSystemPolicyAllFiles
com.google.Keystone.Agent|5|0|kTCCServiceSystemPolicyAllFiles
com.logitech.logitune|4|2|kTCCServiceListenEvent
us.zoom.xos|4|2|kTCCServiceScreenCapture
com.tinyspeck.slackmacgap|4|2|kTCCServiceScreenCapture
com.tinyspeck.slackmacgap|5|0|kTCCServiceSystemPolicyAllFiles
us.zoom.ZoomAutoUpdater|5|0|kTCCServiceSystemPolicyAllFiles
WhatsApp|5|0|kTCCServiceSystemPolicyAllFiles
com.google.Chrome|4|0|kTCCServiceScreenCapture
com.vmware.fusion|4|2|kTCCServiceAccessibility
WhatsApp|4|0|kTCCServicePostEvent
us.zoom.xos|4|2|kTCCServiceAccessibility
com.vmware.fusion|4|2|kTCCServiceSystemPolicyAllFiles
com.googlecode.iterm2|4|2|kTCCServiceEndpointSecurityClient
com.apple.Terminal|4|2|kTCCServiceSystemPolicyAllFiles
com.microsoft.VSCode|5|0|kTCCServiceSystemPolicyAllFiles
com.hnc.Discord|6|0|kTCCServiceListenEvent
com.loom.desktop|6|0|kTCCServiceScreenCapture
net.whatsapp.WhatsApp|5|0|kTCCServiceSystemPolicyAllFiles
com.google.Chrome|5|0|kTCCServiceSystemPolicyAllFiles
com.logi.cp-dev-mgr|4|0|kTCCServiceScreenCapture
/Library/PrivilegedHelperTools/com.microsoft.autoupdate.helper|5|0|kTCCServiceSystemPolicyAllFiles
com.teamviewer.TeamViewer|6|0|kTCCServiceScreenCapture
sqlite>
```

TCC Database

```
sqlite> select client, auth_reason, auth_value, service from access;
client|auth_reason|auth_value|service
us.zoom.xos|5|0|kTCCServiceSystemPolicyAllFiles
/Library/PrivilegedHelperTools/us.zoom.ZoomDaemon|5|0|kTCCServiceSystemPolicyAllFiles
com.apple.Terminal|4|0|kTCCServiceDeveloperTool
/Applications/Zscaler/Zscaler.app/Contents/PlugIns/ZscalerTunnel|5|0|kTCCServiceSystemPolicyAllFile
com.logi.cp-dev-mgr|4|2|kTCCServiceListenEvent
com.logi.cp-dev-mgr|4|2|kTCCServiceAccessibility
com.apple.XProtectFramework.XProtect|5|0|kTCCServiceSystemPolicyAllFiles
com.google.Keystone.Agent|5|0|kTCCServiceSystemPolicyAllFiles
com.logitech.logitune|4|2|kTCCServiceListenEvent
us.zoom.xos|4|2|kTCCServiceScreenCapture
com.tinyspeck.slackmacgap|4|2|kTCCServiceScreenCapture
com.tinyspeck.slackmacgap|5|0|kTCCServiceSystemPolicyAllFiles
us.zoom.ZoomAutoUpdater|5|0|kTCCServiceSystemPolicyAllFiles
WhatsApp|5|0|kTCCServiceSystemPolicyAllFiles
com.google.Chrome|4|0|kTCCServiceScreenCapture
com.vmware.fusion|4|2|kTCCServiceAccessibility
WhatsApp|4|0|kTCCServicePostEvent
us.zoom.xos|4|2|kTCCServiceAccessibility
com.vmware.fusion|4|2|kTCCServiceSystemPolicyAllFiles
com.googlecode.iterm2|4|2|kTCCServiceEndpointSecurityClient
com.apple.Terminal|4|2|kTCCServiceSystemPolicyAllFiles
com.microsoft.VSCode|5|0|kTCCServiceSystemPolicyAllFiles
com.hnc.Discord|6|0|kTCCServiceListenEvent
com.loom.desktop|6|0|kTCCServiceScreenCapture
net.whatsapp.WhatsApp|5|0|kTCCServiceSystemPolicyAllFiles
com.google.Chrome|5|0|kTCCServiceSystemPolicyAllFiles
com.logi.cp-dev-mgr|4|0|kTCCServiceScreenCapture
/Library/PrivilegedHelperTools/com.microsoft.autoupdate.helper|5|0|kTCCServiceSystemPolicyAllFiles
com.teamviewer.TeamViewer|6|0|kTCCServiceScreenCapture
sqlite>
```

TCC Database

```
sqlite> select client, auth_reason, auth_value, service from access;
client|auth_reason|auth_value|service
us.zoom.xos|5|0|kTCCServiceSystemPolicyAllFiles
/Library/PrivilegedHelperTools/us.zoom.ZoomDaemon|5|0|kTCCServiceSystemPolicyAllFiles
com.apple.Terminal|4|0|kTCCServiceDeveloperTool
/Applications/Zscaler/Zscaler.app/Contents/PlugIns/ZscalerTunnel|5|0|kTCCServiceSystemPolicyAllFile
com.logi.cp-dev-mgr|4|2|kTCCServiceListenEvent
com.logi.cp-dev-mgr|4|2|kTCCServiceAccessibility
com.apple.XProtectFramework.XProtect|5|0|kTCCServiceSystemPolicyAllFiles
com.google.Keystone.Agent|5|0|kTCCServiceSystemPolicyAllFiles
com.logitech.logitune|4|2|kTCCServiceListenEvent
us.zoom.xos|4|2|kTCCServiceScreenCapture
com.tinyspeck.slackmacgap|4|2|kTCCServiceScreenCapture
com.tinyspeck.slackmacgap|5|0|kTCCServiceSystemPolicyAllFiles
us.zoom.ZoomAutoUpdater|5|0|kTCCServiceSystemPolicyAllFiles
WhatsApp|5|0|kTCCServiceSystemPolicyAllFiles
com.google.Chrome|4|0|kTCCServiceScreenCapture
com.vmware.fusion|4|2|kTCCServiceAccessibility
WhatsApp|4|0|kTCCServicePostEvent
us.zoom.xos|4|2|kTCCServiceAccessibility
com.vmware.fusion|4|2|kTCCServiceSystemPolicyAllFiles
com.googlecode.iterm2|4|2|kTCCServiceEndpointSecurityClient
com.apple.Terminal|4|2|kTCCServiceSystemPolicyAllFiles
com.microsoft.VSCode|5|0|kTCCServiceSystemPolicyAllFiles
com.hnc.Discord|6|0|kTCCServiceListenEvent
com.loom.desktop|6|0|kTCCServiceScreenCapture
net.whatsapp.WhatsApp|5|0|kTCCServiceSystemPolicyAllFiles
com.google.Chrome|5|0|kTCCServiceSystemPolicyAllFiles
com.logi.cp-dev-mgr|4|0|kTCCServiceScreenCapture
/Library/PrivilegedHelperTools/com.microsoft.autoupdate.helper|5|0|kTCCServiceSystemPolicyAllFiles
com.teamviewer.TeamViewer|6|0|kTCCServiceScreenCapture
sqlite>
```

System DB – Applications with Full Disk Access

```
sqlite> select client, auth_reason, auth_value, service from access where
service="kTCCServiceSystemPolicyAllFiles";
client|auth_reason|auth_value|service
/Applications/Zscaler/Zscaler.app/Contents/PlugIns/ZscalerTunnel|5|0|kTCCServiceSystemPolicyAllFiles
/Library/PrivilegedHelperTools/com.hexnode.hexnodehelper|4|0|kTCCServiceSystemPolicyAllFiles
/Library/PrivilegedHelperTools/com.microsoft.autoupdate.helper|5|0|kTCCServiceSystemPolicyAllFiles
/Library/PrivilegedHelperTools/us.zoom.ZoomDaemon|5|0|kTCCServiceSystemPolicyAllFiles
/usr/bin/defaults|5|0|kTCCServiceSystemPolicyAllFiles
WhatsApp|5|0|kTCCServiceSystemPolicyAllFiles
com.apple.Terminal|4|2|kTCCServiceSystemPolicyAllFiles
com.apple.XProtectFramework.XProtect|5|0|kTCCServiceSystemPolicyAllFiles
com.google.Chrome|5|0|kTCCServiceSystemPolicyAllFiles
com.google.Keystone.Agent|5|0|kTCCServiceSystemPolicyAllFiles
com.microsoft.VSCode|5|0|kTCCServiceSystemPolicyAllFiles
com.vmware.fusion|4|2|kTCCServiceSystemPolicyAllFiles
net.whatsapp.WhatsApp|5|0|kTCCServiceSystemPolicyAllFiles
us.zoom.ZoomAutoUpdater|5|0|kTCCServiceSystemPolicyAllFiles
us.zoom.xos|5|0|kTCCServiceSystemPolicyAllFiles
sqlite>
```

User DB – Applications with User Approved Permissions

```
sqlite> select * from access where client LIKE "%chrome%" and auth_value=2;

kTCCServiceMicrophone|com.google.Chrome|0|2|2|1|??|||UNUSED||0|1674456929|||UNUSED|0

kTCCServiceCamera|com.google.Chrome|0|2|2|1|??|||UNUSED||0|1674666426|||UNUSED|0

kTCCServiceSystemPolicyDownloadsFolder|com.google.Chrome|0|2|2|1|
??|||UNUSED||0|1675164046|||UNUSED|0
kTCCServiceBluetoothAlways|com.google.Chrome|0|2|2|1|??|||UNUSED||0|1699338149|||UNUSED|0

sqlite>
```

TCC Signature Check

```
sqlite> select service, client, auth_reason, auth_value, hex(csreq) from
access where service="kTCCServiceSystemPolicyAllFiles";
    service = kTCCServiceSystemPolicyAllFiles
     client = WhatsApp
auth_reason = 5
 auth_value = 0
 hex(csreq) =
FADE0C0000000094000000010000000600000002000000085768617473417070000000060000
00000F000000060000000E000000010000000A2A864886F7636406020600000000000000000000
00060000000E000000000000000A2A864886F7636406010D0000000000000000000000B0000000
000000000A7375626A6563742E4F55000000000010000000A35375439323337464E330000

    service = kTCCServiceSystemPolicyAllFiles
     client = com.apple.Terminal
auth_reason = 4
 auth_value = 2
 hex(csreq) =
FADE0C0000000030000000010000000600000002000000012636F6D2E6170706C652E546572
6D696E616C000000000003

    service = kTCCServiceSystemPolicyAllFiles
     client = com.google.Chrome
auth_reason = 5
 auth_value = 0
 hex(csreq) =
FADE0C000000010C000000010000000600000006000000060000000600000007000000070000
0000070000000200000011636F6D2E676F6F676C652E4368726F6D650000000000000200000
0016636F6D2E676F6F676C652E4368726F6D652E626574610000000000200000015636F6D2
2E676F6F676C652E4368726F6D652E6465760000000000000200000018636F6D2E676F6F67
6C652E4368726F6D652E63616E617279000000F0000000E000000010000000A2A864886F7
6364060206000000000000000000E000000000000000A2A864886F7636406010D00000000
0000000000B000000000000000A7375626A6563742E4F55000000000010000000A455148
585A384D3841560000
```

```
    service = kTCCServiceSystemPolicyAllFiles
     client = com.google.GoogleUpdater
auth_reason = 5
 auth_value = 0
 hex(csreq) =
FADE0C00000000A4000000010000000600000002000000018636F6D2E676F6F676C652E476F
6F676C655570646174657200000006000000000F000000060000000E000000010000000A2A86
4886F763640602060000000000000000000060000000E000000000000000A2A864886F76364
06010D0000000000000000000000B000000000000000A7375626A6563742E4F55000000000001
0000000A455148585A384D3841560000

    service = kTCCServiceSystemPolicyAllFiles
     client = com.googlecode.iterm2
auth_reason = 4
 auth_value = 2
 hex(csreq) =
FADE0C00000000C4000000010000000600000006000000000F000000020000015636F6D2E67
6F6F676C65636F64652E697465726D320000000000000070000000E000000000000000A2A86
4886F763640601090000000000000000000060000000600000000E000000010000000A2A8648
86F7636406020600000000000000000000E000000000000000A2A864886F7636406010D0000
0000000000000B000000000000000A7375626A6563742E4F55000000000010000000A48
3756375859565137440000

    service = kTCCServiceSystemPolicyAllFiles
     client = com.microsoft.VSCode
auth_reason = 5
 auth_value = 0
 hex(csreq) =
FADE0C00000000A0000000010000000600000002000000014636F6D2E6D6963726F736F6674
2E5653436F6465000000060000000F000000060000000E000000010000000A2A864886F763
6406020600000000000000000000060000000E000000000000000A2A864886F7636406010D00
0000000000000000B000000000000000A7375626A6563742E4F55000000000010000000A
554246385433343647390000
```

TCC Signature Check

```
sqlite> select service, client, auth_reason, auth_value, hex(csreq) from
access where service="kTCCServiceSystemPolicyAllFiles";
    service = kTCCServiceSystemPolicyAllFiles
     client = WhatsApp
auth_reason = 5
 auth_value = 0
 hex(csreq) =
FADE0C0000000094000000010000000600000002000000085768617473417070000000060000
00000F000000060000000E000000010000000A2A864886F7636406020600000000000000000000
0006000000E000000000000000A2A864886F7636406010D0000000000000000000B000000
000000000A7375626A6563742E4F55000000000010000000A35375439323337464E330000

    service = kTCCServiceSystemPolicyAllFiles
     client = com.apple.Terminal
auth_reason = 4
 auth_value = 2
 hex(csreq) =
FADE0C0000000030000000010000000600000002000000012636F6D2E6170706C652E546572
6D696E616C000000000003

    service = kTCCServiceSystemPolicyAllFiles
     client = com.google.Chrome
auth_reason = 5
 auth_value = 0
 hex(csreq) =
FADE0C000000010C000000010000000600000006000000060000000600000007000000070000
0000070000000200000011636F6D2E676F6F676C652E4368726F6D650000000000000200000
0016636F6D2E676F6F676C652E4368726F6D652E626574610000000000200000015636F6D
2E676F6F676C652E4368726F6D652E646576000000000000200000018636F6D2E676F6F67
6C652E4368726F6D652E63616E617279000000F0000000E000000010000000A2A864886F7
6364060206000000000000000000E000000000000000A2A864886F7636406010D00000000
0000000000B000000000000000A7375626A6563742E4F55000000000010000000A455148
585A384D3841560000
```

```
    service = kTCCServiceSystemPolicyAllFiles
     client = com.google.GoogleUpdater
auth_reason = 5
 auth_value = 0
 hex(csreq) =
FADE0C00000000A4000000010000000600000002000000018636F6D2E676F6F676C652E476F
6F676C655570646174657200000006000000000F000000060000000E000000010000000A2A86
4886F763640602060000000000000000000060000000E000000000000000A2A864886F76364
06010D0000000000000000000B000000000000000A7375626A6563742E4F55000000000001
0000000A455148585A384D3841560000

    service = kTCCServiceSystemPolicyAllFiles
     client = com.googlecode.iterm2
auth_reason = 4
 auth_value = 2
 hex(csreq) =
FADE0C00000000C4000000010000000600000006000000000F000000020000015636F6D2E67
6F6F676C65636F64652E697465726D320000000000000070000000E000000000000000A2A86
4886F763640601090000000000000000000060000000600000000E000000010000000A2A8648
86F7636406020600000000000000000000E000000000000000A2A864886F7636406010D0000
0000000000000B000000000000000A7375626A6563742E4F55000000000010000000A48
3756375859565137440000

    service = kTCCServiceSystemPolicyAllFiles
     client = com.microsoft.VSCode
auth_reason = 5
 auth_value = 0
 hex(csreq) =
FADE0C00000000A0000000010000000600000002000000014636F6D2E6D6963726F736F6674
2E5653436F6465000000060000000F000000060000000E000000010000000A2A864886F763
6406020600000000000000000000060000000E000000000000000A2A864886F7636406010D00
0000000000000000B000000000000000A7375626A6563742E4F55000000000010000000A
554246385433343647390000
```

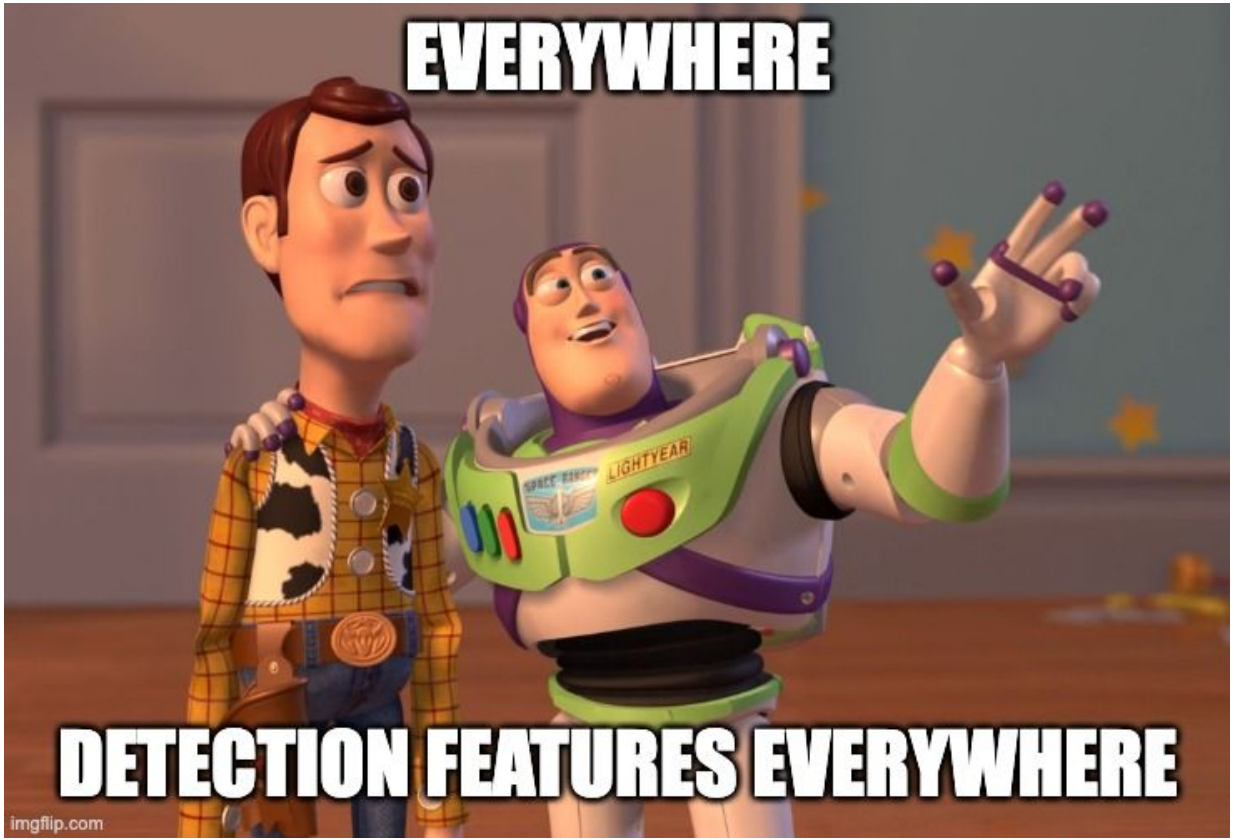
```
#!/bin/bash

declare -a hex_csreqs=(

 "FADE0C0000000094000000010000000600000002000000085768617473417070000000060000000F0000000600000000E0000000100000000A2A864886F7636406020600000000000000000000060000000E000000000000000A2A864886F7636406010D0000000000000000000B000000000000A7375626A6563742E4F55000000000001000000A3537534932333746 4E330000"

 "FADE0C0000000030000000010000000600000002000000012636F6D2E6170706C652E5465726D696E616C000000000003"

 "FADE0C000000010C0000000100000006000000060000000600000006000000070000000700000007000000020000011636F6D2E676F6F676C652E4368726F6D650000000000002000000016636F6D2E676F6F676C652E4368726F6D652E6265746100000000000200000015636F6D2E676F6F676C652E4368726F6D652E6465760000000000000200000018636F6D2E676F6F676C652E4368726F6D652E63616E617279000000F0000000E000000010000000A2A864886F7636406020600000000000000000E000000000000000A2A864886F7636406010D0000000000000000000B000000000000A7375626A6563742E4F55000000000001000000A455148585A384D3841560000"

 "FADE0C00000000A4000000010000000600000002000000018636F6D2E676F6F676C652E476F6F676C6555706461746572000000060000000F0000000600000000E000000010000000A2A864886F7636406020600000000000000000000060000000E000000000000000A2A864886F76364060206010D0000000000000000000B000000000000A7375626A6563742E4F55000000000001000000A455148585A384D3841560000"

 "FADE0C00000000C4000000010000000600000006000000 0F0000000200000015636F6D2E676F6F676C65636F64652E697465726D320000000000000070000000E000000000000000A2A864886F7636406010900000000000000000000060000000600000000E000000010000000A2A864886F7636406020600000000000000000000E000000000000000A2A864886F7636406010D0000000000000000000B000000000000A7375626A6563742E4F55000000000001000000A4837563758595651374400000"

 "FADE0C00000000A0000000010000000600000002000000014636F6D2E6D6963726F736F66742E5653436F6465000000060000000F0000000600000000E000000010000000A2A864886F7636406020600000000000000000000060000000E000000000000000A2A864886F7636406010D0000000000000000000B000000000000A7375626A6563742E4F55000000000001000000A5542463854333436473900000"
)

for hex_csreq in "${hex_csreqs[@]}"
do
   echo "$hex_csreq" | xxd -r -p > decoded-csreq.bin
   csreq -r- -t < decoded-csreq.bin
   echo -e "\n"
done
```

```
➜  tcc ./csreq-decode.sh

identifier WhatsApp and anchor apple generic and certificate
1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate
leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] =
"57T9237FN3"


identifier "com.apple.Terminal" and anchor apple


(identifier "com.google.Chrome" or identifier "com.google.Chrome.beta" or identifier
"com.google.Chrome.dev" or identifier "com.google.Chrome.canary") and anchor apple
generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate
leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] =
EQHXZ8M8AV


identifier "com.google.GoogleUpdater" and anchor apple generic and certificate
1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate
leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] =
EQHXZ8M8AV


anchor apple generic and identifier "com.googlecode.iterm2" and (certificate
leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or certificate
1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate
leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] =
H7V7XYVQ7D)


identifier "com.microsoft.VSCode" and anchor apple generic and certificate
1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate
leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] =
UBF8T346G9
```

Conclusion

Malware Protection

Malware in macOS



Signature-Based Detection

Transparency, Consent, and Control

EoF.

Inside Out:

Deconstructing macOS Application Security

PICUS

HACKTRICK
SİBER GÜVENLİK KONFERANSI

Fatih ERDOĞAN
@FeCassie