

ESET RESEARCH

OSX/Proton spreading again through supply-chain attack

Our researchers noticed that the makers of the Elmedia Player software have been distributing a version of their app trojanized with the OSX/Proton malware.



ESET Research

20 Oct 2017 • 5 min. read

Share Article











 Digital Security
Progress. Protected.

APT Activity Report

IRAN-ALIGNED CYBERATTACKS:
RISE IN DISRUPTIVE OPERATIONS

(eset):research

READ NOW



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

Accept all and close

Manage cookies

On 19 October 2017, ESET researchers noticed that [Eltima](#), the makers of the Elmedia Player software, were distributing a version of their application trojanized with the [OSX/Proton](#) malware on their official website. ESET contacted Eltima as soon as the situation was confirmed. Eltima was very responsive and maintained an excellent communication with us throughout the incident.

Timeline

- 2017-10-19 : Trojanized package confirmed
- 2017-10-19 10:35am EDT: Eltima informed via email
- 2017-10-19 2:25pm EDT: Eltima acknowledged the issue and initiated remediation efforts
- 2017-10-19 3:10pm EDT: Eltima confirms their infrastructure is cleaned up and serving the legitimate applications again
- 2017-10-19 10:12am EDT: [Eltima publishes an announcement about the event](#)
- 2017-10-20 12:15pm EDT: Added references to Folx that was also distributed with the Proton malware

Note: This blog was initially posted despite our research being incomplete. Hence, this information is preliminary and the blogpost will be updated as new facts emerge.

Am I compromised?

ESET advises anyone who downloaded Elmedia Player or Folx software recently to verify if their system is compromised by testing the presence of any of the following files or directories:

- /tmp/Updater.app/
- /Library/LaunchAgents/com.Eltima.UpdaterAgent.plist
- /Library/.rand/
- /Library/.rand/updateragent.app/

If any of them exists, it means the trojanized Elmedia Player or Folx application



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

more 3:15pm EDT and run

was only
15:15 EDT on 19
ems unaffected.

a


abilities. It gains

- Operating system details: hardware serial number (`IOPlatformSerialNumber`), full name of the current user, hostname, System Integrity Protection status (`csrutil status`), gateway information (`route -n get default | awk '/gateway/ { print $2 } '`), current time & timezone
- Browser information from Chrome, Safari, Opera and Firefox: history, cookies, bookmarks, login data, etc.
- Cryptocurrency wallets:
 - Electrum: `~/electrum/wallets`
 - Bitcoin Core: `~/Library/Application Support/Bitcoin/wallet.dat`
 - Armory: `~/Library/Application Support/Armory`
- SSH private data (entire `.ssh` content)
- macOS keychain data using a modified version of [chainbreaker](#)
- Tunnelblick VPN configuration (`~/Library/Application Support/Tunnelblick/Configurations`)
- GnuPG data (`~/ .gnupg`)
- 1Password data (`~/Library/Application Support/1Password 4` and `~/Library/Application Support/1Password 3.9`)
- List of all installed applications.

How do I clean my system?

As with any compromise of an administrator account, a full OS reinstall is the only sure way to get rid of the malware. Victims should also assume at least all the secrets outlined in the previous section are compromised and take appropriate measures to invalidate them.

Supply-chain attack revisited on the Mac



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

ed twice to spread
[OSX/Keydnep](#)
scoder application was

age being used to
ched the 1,000,000

Follow

▼

er mark!
be possible

without our users! [apple/1cYU12a](#)



width="640" height="722" />

Technical analysis

OSX/Proton is a RAT (Remote Access Trojan) sold as a kit on underground forums. It was very briefly documented by Sixgill [earlier this year](#) and then further analyzed by [Thomas Reed at MalwareBytes](#), [Amit Serper at CyberReason](#) and [Patrick Wardle at Objective-See](#).

In the current case of Eltima trojanized software, the attacker built a signed wrapper around the legitimate Elmedia Player and Proton. In fact, we observed what seems to be real-time repackaging and signing of the wrappers, all with the same valid Apple Developer ID. See the history of currently known samples below. Eltima and ESET confirmed they are working with Apple to invalidate the Developer ID used to sign the malicious application. (Apple revoked the certificate.)

(timestamps are all in EDT timezone)

Clean application:



Your account, your cookies choice

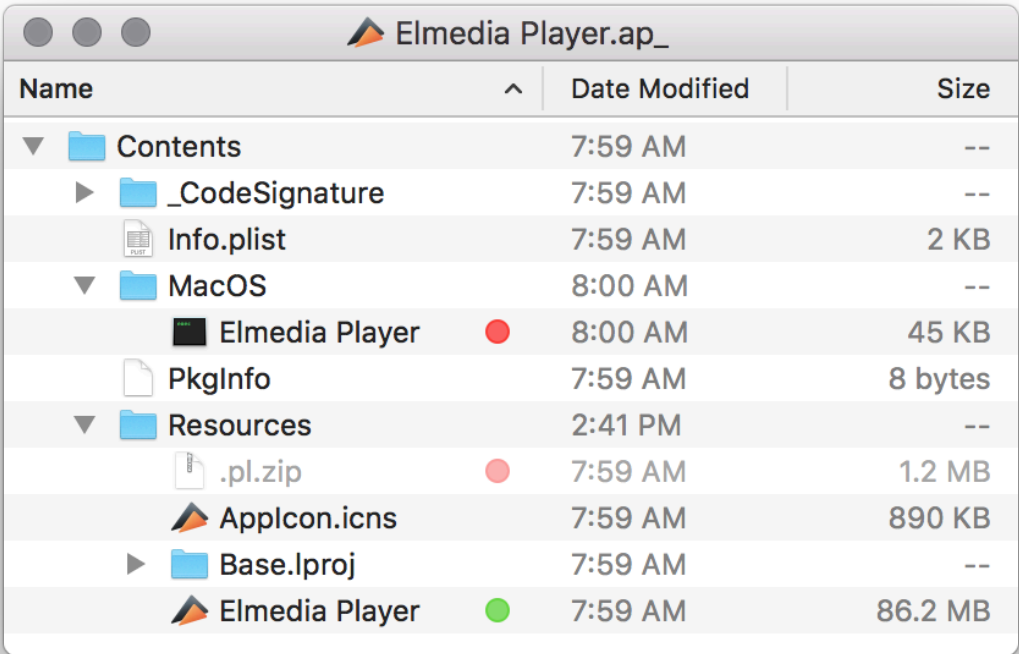
We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

9337642e3957c7423f182a8c

e)

| | | |
|-------------------------------------|--|--|
| 19, 2017, 8:00:05 AM | ID Application: Clifton Grimm (9H35WM5TA5) | e9dcdae1406ab1132dc9d507fd63503e5c4d41d9 |
| Timestamp=Oct 19, 2017, 12:22:24 PM | Authority=Developer ID Application: Clifton Grimm (9H35WM5TA5) | 8cfa551d15320f0157ece3bdf30b1c62765a93a5 |
| Timestamp=Oct 19, 2017, 2:00:38 PM | Authority=Developer ID Application: Clifton Grimm (9H35WM5TA5) | 0400b35d703d872adc64aa7ef914a260903998ca |

First, the wrapper launches the real Elmedia Player application stored in the Resources folder of the application:



And finally extracts & launches OSX/Proton:

```
_text:0000000100001643      call     rbx ; _objc_msgSend
_text:0000000100001645      mov     rdi, rax
_text:0000000100001648      call   _objc_retainAutoreleasedReturnValue
_text:0000000100001640      mov     r15, rbx
_text:0000000100001650      mov     r13, rax
_text:0000000100001653      lea     rdx, cfstr_UnzipDTmpP1Zip ; "unzip -d /tmp %Q/.pl.zip && open /tmp/Updater.app"
_text:000000010000165A      xor     eax, eax
_text:000000010000165C      mov     rdi, r14
_text:000000010000165F      mov     rsi, cs:selRef_stringWithFormat_
_text:0000000100001666      mov     rcx, r13
```



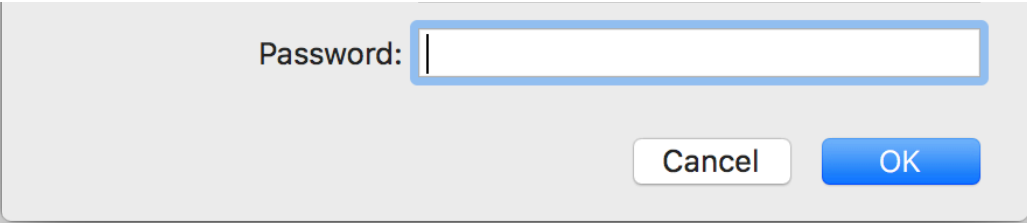
Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

ization window to gain

be your

Username: user



Persistence

OSX/Proton ensures persistence by adding a LaunchAgent for all users when the administrator types their password. It creates the following files on the system:

- `/Library/LaunchAgents/com.Eltima.UpdaterAgent.plist`
- `/Library/.rand/updateragent.app`

```
$ plutil -p /Library/LaunchAgents/com.Eltima.UpdaterAgent.plist
{
  "ProgramArguments" => [
    0 => "/Library/.rand/updateragent.app/Contents/MacOS/updateragent"
  ]
  "KeepAlive" => 1
  "RunAtLoad" => 1
  "Label" => "com.Eltima.UpdaterAgent"
}
```

Backdoor commands


As mentioned at the beginning of the post, OSX/Proton is a backdoor with extensive information stealing capabilities. The backdoor component we observed supports the following commands:

archive

Archive files using zip

Copy file locally

2> /dev/null)



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

| | |
|----------------|---|
| remote_execute | Execute the binary file inside a .zip file or a given shell command |
| tunnel | Create SSH tunnel using port 22 or 5900 |
| upload | Upload file to C&C server |

C&C server

Proton uses a C&C domain that mimics the legitimate Eltima domain, which is consistent with the Handbrake case:

| | Legitimate domain | Proton C2 domain |
|-----------|-------------------|----------------------|
| Eltima | eltima.com | eltima[.]in |
| Handbrake | handbrake.fr | handbrakestore[.]com |
| | | handbrake[.]cc |

IOCs

URL distributing the trojanized application at the time of discovery:

- hxxps://mac[.]eltima[.]com/download/elmediaplayer.dmg
- hxxp://www.elmedia-video-player.[.]com/download/elmediaplayer.dmg
- hxxps://mac.eltima[.]com/download/downloader_mac.dmg

C&C servers



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

ESSE
Det
nar

FCC73B528F7B231A75
mul
thre

| | | | | |
|--|--|----|-------------|--|
| | | | mul thre | |
| 10A09C09FD5DD76202E308718A357ABC7DE291B5 | | | | |
| | | | | |
| Elmedia Player.app/Contents/MacOS/Elmedia Player | C9472D791C076A10DCE5FF0D3AB6E7706524B741 | OS | | |
| | | | | |
| | 30D77908AC9D37C4C14D32EA3E0B8DF4C7E75464 | OS | | |
| | | | | |
| Updater.app/Contents/MacOS/Updater | 3EF34E2581937BABD2B7CE63AB1D92CD9440181A | OS | | |
| | | | | |
| | EF5A11A1BB5B2423554309688AA7947F4AFA5388 | OS | | |

Hat tip to Michal Malik, Anton Cherepanov, Marc-Étienne M. Léveillé, Thomas Dupuy & Alexis Dorais-Joncas for their work on this investigation.

Let us keep you up to date

Sign up for our newsletters



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

ESET RESEARCH
CloudScout: Evasive
Panda scouting cloud
services

ESET RESEARCH
ESET Research
Podcast:
CosmicBeetle

ESET RESEARCH
Embargo
ransomware:
Rock’n’Rust

Discussion

What do you think?
0 Responses


Upvote


Funny



Love


Surprised


Angry








Sad


0 Comments 1 Login ▼



Start the discussion...

LOG IN WITH



OR SIGN UP WITH DISQUS 

 • [Share](#)

[Best](#) [Newest](#) [Oldest](#)

Be the first to comment.



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

ESET
[Privacy Policy](#)
[Manage Cookies](#)

