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

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

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.

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

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.

complete. Hence, this information is
e.

lx software recently to verify if
of the following files or

- /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 was executed and that OSX/Proton is most likely running.

If you have downloaded that software on October 19th before 3:15pm EDT and run it, you are likely compromised.

As far as we know, the trojanized version of the application was only downloadable from the Eltima website, between 08:00 and 15:15 EDT on 19 October 2017. The built-in automatic update mechanism seems unaffected.

What does the malicious payload do to a compromised system?

OSX/Proton is a backdoor with extensive data-stealing capabilities. It gains persistence on the system and can steal the following:

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.

SerialNumber), full name of the
`rutil status`), gateway
`{ print $2 }'`), current time &

history, cookies, bookmarks, login

.dat

- Armory: ~/Library/Application Support/Armory

- 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
easures to invalidate them.

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.

lac

d twice to spread malware, first
password stealer. Then this year,
dled with OSX/Proton.

age being used to spread
e 1,000,000 users milestone this

Follow

">

Elmedia Player hits one million user mark! Such an achievement could never be possible without our users! goo.gl/JcYU2g

6:07 AM - 11 Aug 2017

"

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.

underground forums. It was further analyzed by Thomas trick Wardle at Objective-See.

er 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:

Timestamp	Developper ID	SHA-1
Timestamp=Jul 24, 2017, 4:56:24 AM	Authority=Developer ID Application: ELTIMA LLC (N7U4HGP254)	0603353852e174fc0337642e3957c7423f182a8c

Trojanized application:

		1 (dmg file)
		ae1406ab1132dc9d507fd63503e5c4d41d9
		51d15320f0157ece3bdf30b1c62765a93a5
2017, 2:00:38 PM		35d703d872adc64aa7ef914a260903998ca

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.

(9H35WM5TA5)

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

Elmedia Player.ap_

Name	Date Modified	Size
Contents	7:59 AM	--
_CodeSignature	7:59 AM	--
Info.plist	7:59 AM	2 KB
MacOS	8:00 AM	--
Elmedia Player	8:00 AM	45 KB
PkgInfo	7:59 AM	8 bytes
Resources	2:41 PM	--
.pl.zip	7:59 AM	1.2 MB
AppIcon.icns	7:59 AM	890 KB
		--
		86.2 MB

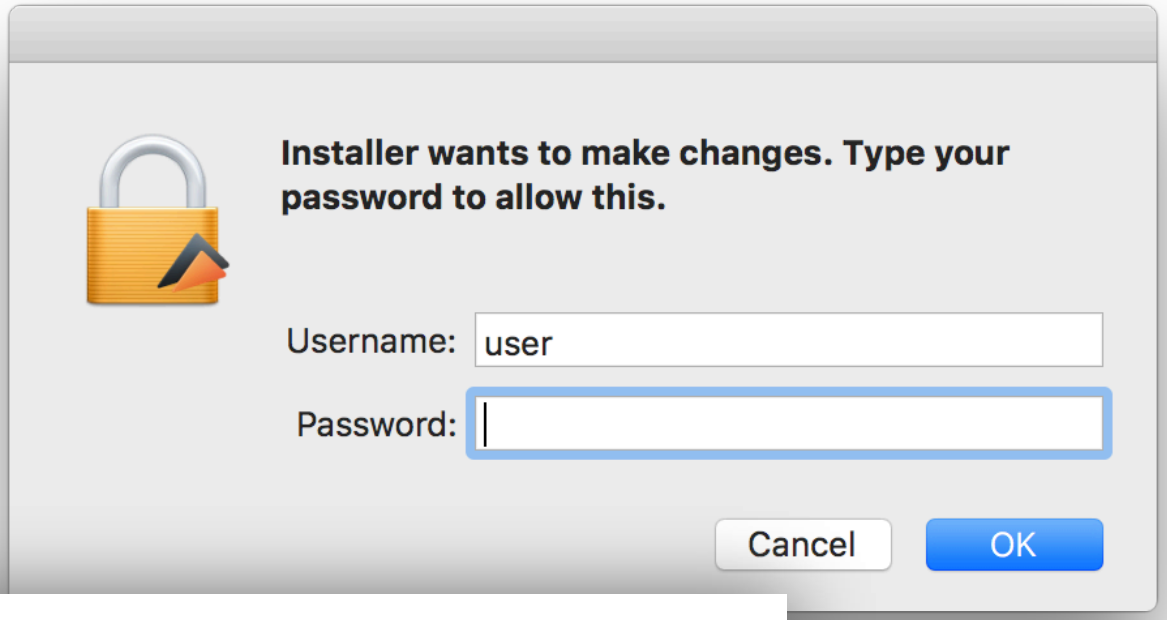
Your account, your cookies choice

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.

```
-d /tmp %@/.pl.zip && open /tmp/Updater.app"
__text:0000000100001674                mov     r14, rax
__text:0000000100001677                mov     rdi, [rbp+var_68]
```

```
__text:000000010000167B                 mov     rsi, cs:selRef_command_
__text:0000000100001682                 mov     rdx, r14
__text:0000000100001685                 call    r15
__text:0000000100001688                 mov     rdi, rax
```

As seen in previous cases, OSX/Proton shows a fake Authorization window to gain root privileges:



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.

or all users when the
files on the system:

ist

- /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:

@\" 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.

`phonehome`	
`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[.]in
	handbrakestore[.]com
	handbrake[.]cc

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.

scovery:

- 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

eltima[.]in / 5.196.42.123 (domain registered 2017-10-15)

Hashes

Path	SHA-1	ESET Detection name
	FCC73B528F7B231A75	multiple threats
	718A357ABC7DE291B5	multiple threats
Elmedia		

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.

Player.app/Contents/MacOS/Elmedia Player	C9472D791C076A10DCE5FF0D3AB6E7706524B741	OSX/Proton.D
	30D77908AC9D37C4C14D32EA3E0B8DF4C7E75464	OSX/Proton.D
Updater.app/Contents/MacOS/Updater	3EF34E2581937BABD2B7CE63AB1D92CD9440181A	OSX/Proton.C
	EF5A11A1BB5B2423554309688AA7947F4AFA5388	OSX/Proton.C

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

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.

Subscribe

Related Articles

ESET RESEARCH

CloudScout: Evasive Panda scouting cloud services

ESET RESEARCH

ESET Research Podcast: CosmicBeetle

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.

Discussion

welivesecurity™ BY eset®

Award-winning news, views, and insight from the ESET security community

About us
Contact us
Legal
Information
RSS Feed

ESET
Privacy Policy
Manage Cookies

Copyright © ESET, All Rights Reserved

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.