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

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 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:

- 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

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

Last year, the Mac Bittorrent client Transmission was abused twice to spread malware, first the OSX/KeRanger ransomware followed by OSX/Keydnap password stealer. Then this year, the Handbrake video-transcoder application was found bundled with OSX/Proton.

Today, ESET discovered another popular Mac software package being used to spread OSX/Proton: Elmedia Player, a media player that reached the 1,000,000 users milestone this summer:

">

" 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:

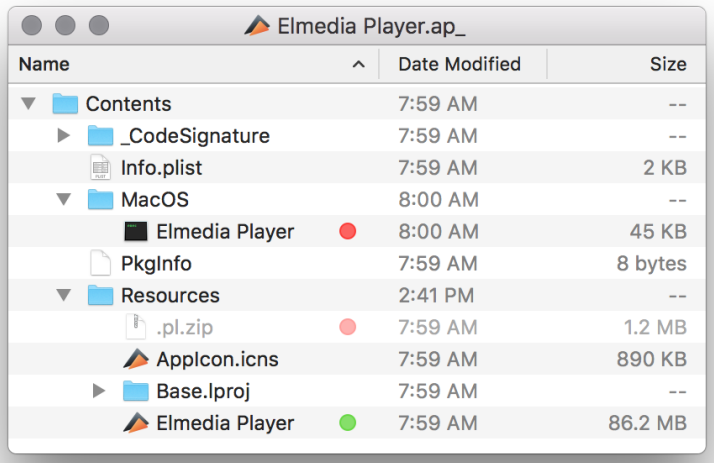
Timestamp	Developper ID	SHA-1
Timestamp=Jul 24, 2017, 4:56:24 AM	Authority=Developer ID Application: ELTIMA LLC (N7U4HGP254)	0603353852e174fc0337642e3957c7

Trojanized application:

Timestamp	Developper ID	SHA-1 (dmg file)
Timestamp=Oct 19, 2017, 8:00:05 AM	Authority=Developer ID Application: Clifton Grimm (9H35WM5TA5)	e9dcdae1406ab1132dc9d507fd635
Timestamp=Oct 19, 2017, 12:22:24	Authority=Developer ID Application: Clifton Grimm	8cfa551d15320f0157ece3bdf30b1

PM	Clifton Grimm (9H35WM5TA5)	
Timestamp=Oct 19, 2017, 2:00:38 PM	Authority=Developer ID Application: Clifton Grimm (9H35WM5TA5)	0400b35d703d872adc64aa7ef914a

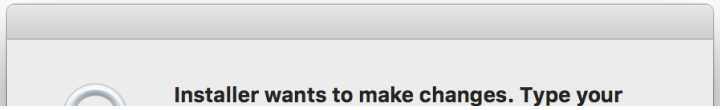
First, the wrapper launches the real Elmedia Player application stored in the Resources folder of the application:

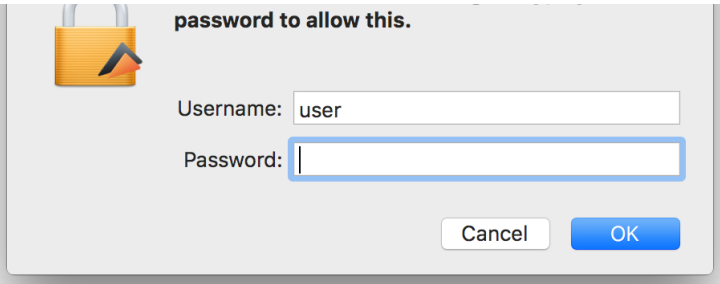


And finally extracts & launches OSX/Proton:

```
__text:0000000100001643                call    rbx ; _objc_msgSend
__text:0000000100001645                mov     rdi, rax
__text:0000000100001648                call    _objc_retainAutoreleasedReturnValue
__text:000000010000164D                mov     r15, rbx
__text:0000000100001650                mov     r13, rax
__text:0000000100001653                lea     rdx, cfstr_UnzipDTmpPlZip ; "unzip -d /tmp %@/.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
__text:0000000100001669                call    r15
__text:000000010000166C                mov     rdi, rax
__text:000000010000166F                call    _objc_retainAutoreleasedReturnValue
__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:





Persistance

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.UpdaterAgen
{
  "ProgramArguments" => [
    0 => "/Library/.rand/updateragent.app/Contents/MacOS
  ]
  "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`	Copy file locally
`create`	Create directory or file locally
`delete`	Delete file locally
`download`	Download file from a URL
`file_search`	Search for files (executes find / -iname \"%@\" 2> /dev/null)
`force_update`	Self-update with digital signature validation
`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	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

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

Hashes

Path	SHA-1	ESET Detecti name
Elmedia Player.app/ Contents/ Resources/.pl.zip	9E5378165BB20E9A7F74A7FCC73B528F7B231A75	multiple threats
	10A09C09FD5DD76202E308718A357ABC7DE291B5	multiple threats
Elmedia 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.

Related Articles

ESET Research Threat Reports

ESET APT Activity Report Q4 2024–Q1 2025

ESET Research

Operation RoundPress

ESET Research

TheWizards APT group uses SLAAC spoofing to perform adversary-in-the-middle attacks

Discussion

RSS Feed