АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Бэкдор OSX/Proton распространяется с троянизированным приложением Elmedia Player

20 октября 2017 года

19 октября наши специалисты заметили, что Eltima, разработчик популярного бесплатного плеера Elmedia Player, распространяет с официального сайта зараженную OSX/Proton версию приложения. Мы обратились в Eltima, как только наличие проблемы подтвердилось, и сотрудники компании оставались на связи на протяжении инцидента.

Публикуем пост, несмотря на то, что исследование не завершено. Информация является предварительной и, возможно, будет дополняться по мере поступления новых данных.

Хронология:

19 октября: подтверждено наличие троянизированного пакета
03:35 (MSK): отправлено сообщение в Eltima
07:25 (MSK): в Eltima приступили к устранению проблемы
08:10 (MSK): в Eltima подтвердили, что инфраструктура очищена и возобновлена раздача легитимных приложений
20 октября
14:12 (MSK): на сайте Eltima опубликовано сообщение об устранении троянизированных версий Elmedia Player и Folx

Мой компьютер заражен?

ESET советует всем, кто недавно загружал программное обеспечение Elmedia Player, проверить систему на предмет компрометации. На заражение указывает присутствие любого из перечисленных файлов или каталогов:

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

Наличие хотя бы одного файла или каталога означает, что в системе выполнено троянизированное приложение Elmedia Player и с большой долей вероятности уже работает OSX/Proton.

Если вы загружали Elmedia Player 19 октября до 08:15 (MSK) и запустили его, ваша система скомпрометирована.

По нашим сведениям, скомпрометирована была только версия плеера, загружаемая с официального сайта Eltima. Встроенный механизм автоматического обновления, вероятно, не был затронут.

Функции OSX/Proton

OSX/Proton – бэкдор с широкими возможностями кражи данных. Он может собирать следующие данные:

- Информация об операционной системе: серийный номер оборудования (IOPlatformSerialNumber), полное имя текущего пользователя, имя узла, статус System Integrity Protection (csrutil status), информация о шлюзе (route -n get default | awk '/gateway/ { print $2 }'), текущее время и часовой пояс
- Информация из браузеров Chrome, Safari, Opera и Firefox: история, куки, закладки, логины и пароли и др.
- Криптовалютные кошельки: Electrum: ~/.electrum/wallets; Bitcoin Core: ~/Library/Application Support/Bitcoin/wallet.dat; Armory: ~/Library/Application Support/Armory
- Конфиденциальные данные SSH (весь контент .ssh)
- Данные связки ключей macOS, с использованием модифицированной версии chainbreaker
- Конфигурация Tunnelblick VPN (~/Library/Application Support/Tunnelblick/Configurations)
- Данные GnuPG (~/.gnupg)
- Данные 1Password (~/Library/Application Support/1Password 4 и ~/Library/Application Support/1Password 3.9)
- Список установленных приложений

Как очистить систему?

Как в любом инциденте с компрометацией аккаунта администратора, единственный надежный способ избавиться от вредоносного ПО – полная переустановка операционной системы. Необходимо учитывать, что данные, перечисленные в предыдущем разделе, с большой долей вероятности скомпрометированы.

Атаки на цепи поставок (supply-chain attack) на Mac

В 2016 году Transmission, Bittorrent-клиент для Mac, дважды использовался для распространения вредоносного ПО. В первом инциденте фигурировал шифратор OSX/KeRanger, во втором – инструмент для кражи паролей OSX/Keydnap. В этом году было заражено OSX/Proton приложение

Handbrake для кодирования видео на Mac.

Теперь мы обнаружили, что для распространения OSX/Proton используется еще одно популярное ПО для Mac – Elmedia Player, достигший, кстати, отметки в 1 млн пользователей этим летом.

Источник: twitter.com/Elmedia_Player/status/895995031802261504

Технический анализ

OSX/Proton – троян для удаленного доступа (Remote Access Trojan, RAT), продаваемый на подпольных форумах. Он был кратко описан Sixgill в начале этого года, затем его исследовали Томас Рид из MalwareBytes, Амит Серпер из CyberReason и Патрик Уордл из Objective-See.

В нашем случае атакующий создал подписанную оболочку вокруг легитимного Elmedia Player и Proton. Фактически, мы наблюдали, что оболочки переупаковывались и переподписывались в режиме реального времени, все с одинаковым действительным идентификатором Apple Developer ID. (Сертификат отозван Apple.)

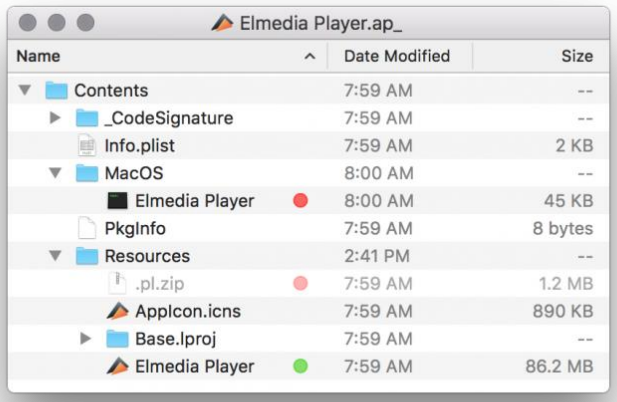
Чистое приложение
(временные метки – EDT, североамериканское восточное время)

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

Троянизированное приложение

Временная метка	Developer ID	SHA-1 (dmg file)
Timestamp=Oct 19, 2017, 8:00:05 AM	Authority=Developer 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

Сначала оболочка запускает настоящий Elmedia Player, хранящийся в папке «Ресурсы» приложения:

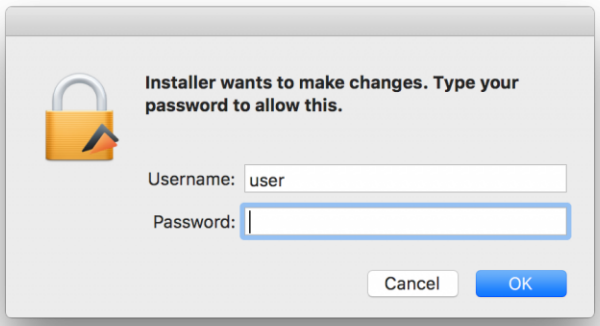


Далее извлекает и запускает OSX/Proton:

```
__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
```

Как видно из предыдущих кейсов, OSX/Proton показывает фальшивое окно авторизации для

получения прав администратора:



Персистентность

OSX/Proton обеспечивает персистентность, добавляя LaunchAgent для всех пользователей, когда администратор вводит их пароль. Он создает в системе следующие файлы:

- /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"
}
```

Команды бэкдора

Как уже было сказано, OSX/Proton – это бэкдор с широким спектром функций для кражи данных. Изученные компоненты бэкдора могут выполнять следующие команды:

- archive — архивировать файлы в zip
- copy — локально копировать файл
- create — локально создать каталог или файл
- delete — локально удалить файл
- download — загрузить файл с URL
- file_search — искать файлы (выполняет find / -iname \"%@\" 2> /dev/null)
- force_update — самообновление с проверкой цифровой подписи
- phonehome
- remote_execute — выполнить двоичный файл внутри zip-архива или заданную шелл-команду
- tunnel — создать туннель SSH через порт 22 или 5900
- upload — загрузить файл на C&C-сервер

C&C-сервер

Proton использует домен управляющего сервера, который имитирует легитимный домен Eltima – тот же принцип, что в кейсе Handbrake:

	Легитимный домен	Домен Proton
Eltima	eltima.com	eltima[.]in
Handbrake	handbrake.fr	handbrakestore[.]com
		handbrake[.]cc

Индикаторы компрометации

URL-адрес, распространяющий троянизированное приложение в момент обнаружения:

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

C&C-серверы:

eltima[.]in / 5.196.42.123 (домен зарегистрирован 15 октября 2017 года)

Хеши

Путь	SHA-1	Детектирование	Цель
/Applications/Elmedia Player.app/Contents/Resources/.pl.zip	9E5378165BB20E9A7F74A7FCC73B528F7B231A75	Несколько угроз	ZIP-архив с вредоносным ПО Proton + скрипты на Python
	10a09c09fd5dd76202e308718a357abc7de291b5	Несколько угроз	ZIP-архив с вредоносным ПО Proton + скрипты на Python
/Applications/Elmedia Player.app/Contents/MacOS/Elmedia Player	C9472D791C076A10DCE5FF0D3AB6E7706524B741	OSX/Proton.D	Лаунчер (или оболочка)
	795B8BCADCAAF56DAC7CFDDF44F97A32AAAA4987	OSX/Proton.D	Лаунчер (или оболочка)
	30d77908ac9d37c4c14d32ea3e0b8df4c7e75464	OSX/Proton.D	Лаунчер (или оболочка)
/tmp/Updater.app/Contents/MacOS/Updater	3EF34E2581937BABD2B7CE63AB1D92CD9440181A	OSX/Proton.C	Вредоносное ПО Proton, без подписи
	ef5a11a1bb5b2423554309688aa7947f4afa5388	OSX/Proton.C	Вредоносное ПО Proton, без подписи