A Close Look at Rogue Antivirus Programs

Alain Zidouemba
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
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

Select a Destination

Select the disk where you want to install the Mac Protector Installer Program software.

Macintosh HD
36.8 GB free
42.61 GB total

Installing this software requires 2.9 MB of space.

You have chosen to install this software on the disk “Macintosh HD”.

Go Back  Continue
Scareware tactics

Unregistered copy
Sorry, the copy of your program is unregistered. Register to have an ability to cleanup your system.

Security Status

Virus found
Fortunately, your computer is infected.
Infected file detected:

Virus: Adware
File: Safari

The system is infected
Your system is infected. It's highly recommended to cleanup your system to protect critical information like credit card numbers, etc.

In Memory Apps: /Applications/Safari.app
keyedobjects.nib

Infected Files:

<table>
<thead>
<tr>
<th>Infected By</th>
<th>Infected Object</th>
<th>Path to object</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adware</td>
<td>Safari</td>
<td>/Applications/Safari.app/Contents/MacOS</td>
<td>Medium</td>
</tr>
</tbody>
</table>

Statistics
Scanned files: 2262
Scanned directories: 1368
Viruses detected: 0

Timing
Time spent: 0:00:33
Last Scan Date: 6/9/11
Last Viruses Detected: 0
Really?

Security Status
Unfortunately, your computer is infected.
To protect your information (like credit card numbers, etc.) it's highly recommended to cleanup the

Infected Files:

<table>
<thead>
<tr>
<th>Infected By</th>
<th>Infected Object</th>
<th>Path to object</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adware</td>
<td>Safari</td>
<td>/Applications/Safari.app/Contents/MacOS</td>
<td>Medium</td>
</tr>
<tr>
<td>Backdoor</td>
<td>Safari Webpage Pr...</td>
<td>/Applications/Safari.app/Contents</td>
<td>High</td>
</tr>
<tr>
<td>Worm</td>
<td></td>
<td>/bin</td>
<td>Medium</td>
</tr>
</tbody>
</table>

Statistics
Scanned files: 7283
Scanned directories: 2364
Viruses detected: 3

Timing
Time spent: 0:01:43
Last Scan Date: 6/9/11
Last Viruses Detected: 0
Mac Protector phones home

GET /1.php?v=1004&affId=37901&data=24C296AF68E54672A463B15198B81E11E299FECCE3C469988590D5ED2A564C9620628 HTTP/1.1\r\nHost: 95.64.55.5\r\nUser-Agent: MacProtector/1 CFNetwork/454.11.5 Darwin/10.6.8 (1386) (VMware%20Virtual%20Platform)\r\nAccept: */*\r\nAccept-Encoding: gzip, deflate\r\nConnection: keep-alive\n
File: "/home/aridouemba/Desktop..." Packets: 755 Displayed: 755 Marked: 0 Load time: 0.00007
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?

About Mac Protector

Mac Protector is the most advanced virus and malware detection system in the world, because it has the largest viruses database among all other antivirus systems. It can detect and remove from your computer almost all known dangerous software. It is possible because the Mac Protector security specialists work all over the world, which means they work 24 hours a day and 7 days a week.

Thus, Mac Protector offers one of the best solutions in IT Security market. Over 250 specialists work in more than 10 countries. The largest worldwide companies trust Mac Protector their nets and security. More than one million people use Mac Protector antivirus to protect their critical information like CREDIT CARD numbers, passwords and so on.

Support

Our register users can get 24/7 support.

- **Mail:** Unavailable for unregistered users
- **Phone:** Unavailable for unregistered users
- **Ticket:** Unavailable for unregistered users

Register
Purchase MacProtector: network traffic

```
GET /mac.php?v=1004&affid=37981&data=24C296A68E54672A463B15198B1E11E299FECE3C469088590DD5ED2A564C6020628 HTTP/1.1\n
Host: 91.213.217.30\nUser-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_6; en-us) AppleWebKit/533.19.4 (KHTML, like Gecko)\nAccept: application/xaml+xml,application/vnd.ms-xaml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5\nAccept-Language: en-us\nAccept-Encoding: gzip, deflate\nConnection: keep-alive\n```

Frame 38: 498 bytes on wire (3984 bits), 498 bytes captured (3984 bits)
Ethernet II, Src: VMware 4c:63:70 (00:0c:29:4c:63:70), Dst: Cisco 01:11:40 (00:15:c7:01:11:40)
Internet Protocol, Src: 18.4.10.204 (18.4.10.204), Dst: 91.213.217.30 (91.213.217.30)
Transmission Control Protocol, Src Port: 49157 (49157), Dst Port: http (80), Seq: 1, Ack: 1, Len: 432
HTTP/1.1 Transfer Protocol
Detect MacProtector purchase page, URI

- alert tcp $HOME_NET any -r $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\x3Dd\{4\}\x26affid\x3Dd\{5\}\x26data\x3D/Ui" classtype:trojan-activity; sid:5678;)


Purchase MacProtector... or MacDefender?

**Order Details**

- **1 year Software License $59.95**
- **2 year Software License $69.95**
- **Lifetime Software License, 60% discount $79.95**
- Sign me up for a purchase of Lifetime Premium Support of only $19.95.

**Terms**

You are purchasing MAC Security. This is a one-time charge and you will not be rebilled.

**Payment Information**

**Credit Card Information**

- **Card Type**: Visa
- **Card Number**: [Masked]
- **Expiration Date**: [Masked]
- **CVV2 Number**: [Masked]
- **First Name**: [Masked]
- **Last Name**: [Masked]

**Contact Information**

- **Email**: [Masked]
- **Country**: United States
- **State**: Outside U.S.
- **Address**: [Masked]
- **City**: [Masked]
- **Zip Code**: [Masked]
- **Telephone**: [Masked]

**IMPORTANT**: Please allow up to two minutes for live processing of your order. Don't click BACK or CANCEL while waiting.
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

Please click “Buy“ button to purchase serial number.

Please enter the Serial Number to register your copy of program.

Serial number: [Redacted]
OK I am registered, now what?

About Mac Protector

Mac Protector is the most advanced virus and malware detection system in the world, because it has the largest viruses database among all other antivirus systems. It can detect and remove from your computer almost all known dangerous software. It is possible because the Mac Protector security specialists work all over the world, which means they work 24 hours a day and 7 days a week.

Thus, Mac Protector offers one of the best solutions in IT Security market. Over 250 specialists work in more than 10 countries. The largest worldwide companies trust Mac Protector their nets and security. More than one million people use Mac Protector antivirus to protect their critical information like CREDIT CARD numbers, passwords and so on.

Support

Our registered users can get 24/7 support.

- **Mail:** support@mac-defence.com
- **Phone:** 1-800-959-40-31
- **Ticket:** Click to send ticket
Money trail
<table>
<thead>
<tr>
<th><strong>Mac-defence.com registrant details</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Contact Id</strong></td>
</tr>
<tr>
<td><strong>Name</strong></td>
</tr>
<tr>
<td><strong>Email Address</strong></td>
</tr>
<tr>
<td><strong>Company Name</strong></td>
</tr>
<tr>
<td><strong>Address1</strong></td>
</tr>
<tr>
<td><strong>Tel No.</strong></td>
</tr>
<tr>
<td><strong>City</strong></td>
</tr>
<tr>
<td><strong>State/Region/Province</strong></td>
</tr>
<tr>
<td><strong>Country</strong></td>
</tr>
<tr>
<td><strong>Zip</strong></td>
</tr>
</tbody>
</table>
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 (financial controller)
ChronoPay, registrant for rogue-related domains

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>Product</th>
<th>Purchase Date</th>
<th>Expires in (days)</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>apple2defence.com</td>
<td>Domain Registration</td>
<td>May 20, 2011</td>
<td>359</td>
<td>Active</td>
</tr>
<tr>
<td>apple2ofence.com</td>
<td>Domain Registration</td>
<td>May 20, 2011</td>
<td>359</td>
<td>Active</td>
</tr>
<tr>
<td>essentialtool.com</td>
<td>Domain Registration</td>
<td>May 16, 2011</td>
<td>355</td>
<td>Active</td>
</tr>
<tr>
<td>maclook2protection.com</td>
<td>Domain Registration</td>
<td>May 12, 2011</td>
<td>351</td>
<td>Suspended</td>
</tr>
<tr>
<td>mstoutilonline.com</td>
<td>Domain Registration</td>
<td>May 5, 2011</td>
<td>344</td>
<td>Suspended</td>
</tr>
<tr>
<td>mac-defence.com</td>
<td>Domain Registration</td>
<td>May 3, 2011</td>
<td>342</td>
<td>Suspended</td>
</tr>
<tr>
<td>newbuy-onlines.com</td>
<td>Domain Registration</td>
<td>Apr 27, 2011</td>
<td>336</td>
<td>Active</td>
</tr>
<tr>
<td>feelgoodsoft.com</td>
<td>Domain Registration</td>
<td>Apr 5, 2011</td>
<td>314</td>
<td>Active</td>
</tr>
<tr>
<td>wakelessoftware.com</td>
<td>Domain Registration</td>
<td>Apr 4, 2011</td>
<td>313</td>
<td>Active</td>
</tr>
<tr>
<td>triasoftware.com</td>
<td>Domain Registration</td>
<td>Apr 4, 2011</td>
<td>313</td>
<td>Active</td>
</tr>
<tr>
<td>supplylinesoft.com</td>
<td>Domain Registration</td>
<td>Apr 4, 2011</td>
<td>313</td>
<td>Active</td>
</tr>
<tr>
<td>sphere2es.com</td>
<td>Domain Registration</td>
<td>Apr 4, 2011</td>
<td>313</td>
<td>Active</td>
</tr>
<tr>
<td>softwareonlineshopfront.com</td>
<td>Domain Registration</td>
<td>Apr 4, 2011</td>
<td>313</td>
<td>Active</td>
</tr>
<tr>
<td>softwarepash.com</td>
<td>Domain Registration</td>
<td>Apr 4, 2011</td>
<td>313</td>
<td>Active</td>
</tr>
<tr>
<td>softwarewash.com</td>
<td>Domain Registration</td>
<td>Apr 4, 2011</td>
<td>313</td>
<td>Active</td>
</tr>
<tr>
<td>shield.com</td>
<td>Domain Registration</td>
<td>Apr 4, 2011</td>
<td>313</td>
<td>Active</td>
</tr>
<tr>
<td>satisfactionsofsoft.com</td>
<td>Domain Registration</td>
<td>Apr 4, 2011</td>
<td>313</td>
<td>Active</td>
</tr>
</tbody>
</table>
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
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

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] => berrod alain  
  [opid] => 353421  
  [email] => a.m.roman@free.fr  
  [transId] => 39139551  
  [product_id] => 004595-0001-0001
)

mail=Array

(  
  [NAME] => berrod alain  
  [EMAIL] => a.m.roman@free.fr  
  [OPID] => 353421  
  [TID] => 39139551
)

[phone] => +1-800-417-5679  
[serial] => WNDS-6W954-FX65B-41VDF-8G4JI  
[salesite] => www.yoursoftmagazine.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.marketingsoftwaresolutions.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
)
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 Discover card……….4$
- 1 Company card……….8$
- 1 Uk Card Normal 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 verified 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 :: baby_cris47
EMAIL ADDRESS :: baby_cris47@yahoo.com
ICQ NUMBER :: 610077819
MacProtector, MacDefender, MacShield, MacGuard, Winwebsec: one happy family
MacProtector, Winwebsec traffic

- **Winwebsec**

- **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
applicationDidFinishLaunching

- Classic entry point in Cocoa apps
- But not much here….
getConfigParam
Let’s dig deeper

- Takes one integer
- Branching based on integer value
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
loc_AB1

- Open DownloadPict.png in Resources dir
loc_2B36

- int fseek (File * stream, long int offset, int origin);
- 2 = SEEK_END
- 0xFFFFFFFF = -1 (signed 32-bit int)
Skip, skip, skip... What is avrunner.app doing?

- Reading encrypted bytes at end of DownloadPict.png and XORing with 0x5a
#include <string.h>
#include <stdio.h>

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

    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:
- 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 areas¹
- Rogue antimalware provides the benefit of an immediate feeling of security (even if great damage is done behind the scenes)

Contact

- IRC (irc.freenode.net)
  - #snort
  - #clamav
  - #razorback

- Blog

- Twitter
  - @VRT_Sourcefire
    - @number007

- Email
  - vrt@sourcefire.com
    - azidouemba@sourcefire.com