

Blackhole Ramnit - samples and analysis

contagiodump.blogspot.com/2012/01/blackhole-ramnit-samples-and-analysis.html

```
check for viruses on your computer.  
hard drives or hard drive controlle  
to make sure it is properly configu  
Run CHKDSK /F to check for hard dri  
restart your computer.  
  
Technical information:  
  
*** STOP: 0xI'LL BE BACK! (W32/Ramnit.
```

```
Check for viruses on your computer.  
hard drives or hard drive controlle  
to make sure it is properly configu  
Run CHKDSK /F to check for hard dri  
restart your computer.  
  
Technical information:  
  
*** STOP: 0xI'LL BE BACK! (W32/Ramnit.
```

Ramnit - a Zeus-like trojan/worm/file infector with rootkit capabilities has been in the wild for a long time but recently made news because [Seculert reported about a financial variant of this malware aimed at stealing Facebook credentials.](#)

While I did not see any Facebook related activity in my samples, I am posting them anyway for your research as their functionality is the same.

The samples I have are being spread not via Facebook but via Blackhole exploit kit, which is a very effective method. Blackhole exploit kit was associated with the spread of ZeuS, Spyeye, and it is not surprising that Ramnit is being spread in the same manner by the same groups. The group of command and control servers that I researched is associated with pharma spam and "Canadian" online pharmacies.

General File Information

File: 607B2219FBCFBFE8E6AC9D7F3FB8D50E

MD5: 607B2219FBCFBFE8E6AC9D7F3FB8D50E

File: c33e7ed929760020820e8808289c240e
MD5: C33E7ED929760020820E8808289C240E

File: 76991eefea6cb01e1d7435ae973858e6 - not analysed
MD5: 76991EEFEA6CB01E1D7435AE973858E6

File: 2ff2c8ada4fc6291846f0d66ae57ca37 -not analysed
MD5: 2FF2C8ADA4FC6291846F0D66AE57CA37



Download



[Download all the binaries and dropped files as a password protected archive \(email me if you need the password\)](#)



Distribution

The files analysed were / are being distributed via Blackhole exploit pack. It starts with the usual large letter message "Please wait page is loading" -then Java exploit launches and compromise takes place if the machine is vulnerable. . Here you can see the Blackhole domains spreading Ramnit in the Malwaredomainlist . **Amberfreda.com** domain belongs to a legitimate company and is registered in Arizona, while a subdomain **best.amberfreda.com** is registered by some Ukranian guy. Not sure how they managed that.

amberfreda.com

173.201.97.1

p3nlhg49c090.shr.prod.phx3.secureserver.net

Domains By Proxy, LLC

DomainsByProxy.com

15111 N. Hayden Rd., Ste 160, PMB 353

Scottsdale, Arizona 85260

United States

best.amberfreda.com

178.162.145.184

178-162-145-184.local

Host unreachable
 178.162.145.128 - 178.162.145.255
 VPS services
 Ukraine
 Vladimir Gubarenko
 p/o box 8967
 61106, Kharkov
 Ukraine
 phone: +7 4956637354
 fax: +7 4956637354
 admin@imhoster.net

Page 0

Date (UTC)	Domain	IP	Reverse Lookup	Description	Registrant	ASN
2012/01/05_17:47	best.amberfreda.com/direct.php?page=af4ed45dd20afd39	178.162.145.184	178-162-145-184.local	Blackhole exploit kit	Domains By Proxy, LLC /	28753 
2012/01/05_17:47	best.amberfreda.com/w.php?f=16&e=2	178.162.145.184	178-162-145-184.local	trojan Ramnit	Domains By Proxy, LLC /	28753 

Page 0

Please wait page is loading...

<http://www.malwaredomainlist.com/mdl.php?search=amberfreda.com&colsearch=All&quantity=50>

Brief Analysis

607B2219FBCFBFE8E6AC9D7F3FB8D50E

Hendrik Adrian from Japan posted his analysis of the same sample_(0day.JP - Ramnit) where he described the files created by the malware and the spam sending capabilities of the bot .



The bot deletes registry settings for the safe

boot, which causes BSOD and prevents one from removing the malicious files in the safe

mode.

2. Adds a Windows service

Micorsoft Windows Service - note the spelling

3. Adds the following files (names vary)

\Application Data\nvamibiv\vcryserj.exe - copy of the original

[http://www.virustotal.com/file-scan/report.html?](http://www.virustotal.com/file-scan/report.html?id=f52bfac9637aea189ec918d05113c36f5bcf580f3c0de8a934fe3438107d3f0c-1326310185)

[id=f52bfac9637aea189ec918d05113c36f5bcf580f3c0de8a934fe3438107d3f0c-1326310185](http://www.virustotal.com/file-scan/report.html?id=f52bfac9637aea189ec918d05113c36f5bcf580f3c0de8a934fe3438107d3f0c-1326310185)

File: vcryserj.exe

Size: 135680

MD5: 607B2219FBCFBFE8E6AC9D7F3FB8D50E

- \Application Data\wduqtdai.log - number of logs varies, contain encrypted data
- \Application Data\xyepaef.log number of logs varies, contain encrypted data
- **\Temp\nhptugtstukgwpyi.exe - copy of the original**

File: nhptugtstukgwpyi.exe

Size: 135680

MD5: 607B2219FBCFBFE8E6AC9D7F3FB8D50E

\Start Menu\Programs\Startup\vcryserj.exe - copy of the original

File: vcryserj.exe

Size: 1356

MD5: 607B2219FBCFBFE8E6AC9D7F3FB8D50E

\Local Settings\Temp\dnsgvbny.sys the rootkit [http://www.virustotal.com/file-scan/report.html?](http://www.virustotal.com/file-scan/report.html?id=c1293f8dd8a243391d087742fc22c99b8263f70c6937f784c15e9e20252b38ae-1326346542)

[id=c1293f8dd8a243391d087742fc22c99b8263f70c6937f784c15e9e20252b38ae-1326346542](http://www.virustotal.com/file-scan/report.html?id=c1293f8dd8a243391d087742fc22c99b8263f70c6937f784c15e9e20252b38ae-1326346542)

File: dnsgvbny.sys

Size: 15360

MD5: A6D351093F75D16C574DB31CDF736153

Owner	Open Object	Handle/Offset
3704: svchost.exe	C:\Documents and Settings\mila\Start Menu\Programs\Startup\vcryserj.exe	0x000000C8
3704: svchost.exe	C:\Documents and Settings\mila\Local Settings\Application Data\mambiv\vcryserj.exe	0x000000B4

Ramnit injects itself into two svchost.exe processes and you can see them if you sort all processes by PID, the last two will those created by Ramnit.

It generates spam that it sends out on port 25, Hendrik already described this behavior in his post.

C33E7ED929760020820E8808289C240E

The second file has file infector features I did not observe in

607B2219FBCFBFE8E6AC9D7F3FB8D50E.

As you see in the log below, malicious svchost.exe modifies or tries to modify every binary and HTML file by appending malicious code to each file or a vbs script to HTML files - like described in this post by ESET Win32/Ramnit.A. and here in the post by Avira - Closer look at W32/Ramnit.C

This does not break the infected binaries, all files continue to work as designed, except they infect or reinfect the computer they are running on. Webmasters may upload infected html files and visitors of their sites may get infected as well. For an average user, it is impossible to clean a system compromised with Ramnit file injector and use it confidence. The only way is say good bye to all the HTM(L), DLL and EXE files and build a new system without trying to copy any hrml files, bookmark or applications.

Name	Virtual Size	Virtual Address	Size of Raw Data	Pointer to Raw Data	Characteristics	Pointing Directories
• .text	0018F36h	00401000h	00019000h	00000400h	60000020h	
• .data	0003E700h	0041A300h	0000C300h	000F9400h	40000040h	Import Table; Load Configuration T...
• .data	00004300h	00421000h	0001E500h	000F6600h	00000040h	
• .text	00073600h	00426000h	00020300h	00000000h	40000040h	Resource Table
• .reloc	00071FC0h	0042A300h	00002000h	00018600h	40000040h	Relocation Table
• .text	00023000h	00423000h	0002E000h	00056600h	00000020h	

Malicious/Modified VirustotalUpload2.exe
Injected code with a pointer to load and run it first!

Name	Virtual Size	Virtual Address	Size of Raw Data	Pointer to Raw Data	Characteristics	Pointing Directories
• .text	0018EF1h	00401000h	00019000h	00000400h	60000020h	
• .data	0003E700h	0041A300h	0000C300h	000F9400h	40000040h	Import Table; Load Configuration T...
• .data	00004300h	00421000h	0001E500h	000F6600h	00000040h	
• .text	00073600h	00426000h	00020300h	00000000h	40000040h	Resource Table
• .reloc	00071FC0h	0042A300h	00002000h	00018600h	40000040h	Relocation Table

Clean VirustotalUpload2.exe

This is what happens with VirustotalUpload2.exe (and most other Programs including Adobe, MS Office and Windows files)

<http://www.virustotal.com/file-scan/report.html?>

[id=a40aacca731c142148733786cae64d45df2e740e3fb744ffc513d251ec121cf7-1326169765](http://www.virustotal.com/file-scan/report.html?id=a40aacca731c142148733786cae64d45df2e740e3fb744ffc513d251ec121cf7-1326169765)

VirusTotalUpload2.exe

Submission date:

2012-01-10 04:29:25 (UTC)

Result:37 /43 (86.0%)

Print results

Antivirus	Version	Last Update	Result
-----------	---------	-------------	--------

AhnLab-V3	2012.01.09.00	2012.01.09	Win32/Ramnit.O
AntiVir	7.11.20.218	2012.01.10	W32/Ramnit.E
Avast	6.0.1289.0	2012.01.09	Win32:Ramnit-H
AVG	10.0.0.1190	2012.01.10	Win32/Zbot.G
BitDefender	7.2	2012.01.10	Win32.Ramnit.N
ByteHero	1.0.0.1	2011.12.31	Trojan.Win32.Heur.Gen
CAT-QuickHeal	12.00	2012.01.09	W32.Ramnit.C
ClamAV	0.97.3.0	2012.01.10	Trojan.Patched-168
Commtouch	5.3.2.6	2012.01.10	W32/Ramnit.E
Comodo	11229	2012.01.10	TrojWare.Win32.Patched.SM
DrWeb	5.0.2.03300	2012.01.09	Win32.Rmnet.8
Emsisoft	5.1.0.11	2012.01.10	Virus.Win32.Zbot!IK
eTrust-Vet	37.0.9672	2012.01.09	Win32/Ramnit.AJ
F-Prot	4.6.5.141	2012.01.09	W32/Ramnit.E
F-Secure	9.0.16440.0	2012.01.09	Win32.Ramnit.N
Fortinet	4.3.388.0	2012.01.10	W32/Ramnit.B
GData	22	2012.01.09	Win32.Ramnit.N
Ikarus	T3.1.1.109.0	2012.01.10	Virus.Win32.Zbot
Jiangmin	13.0.900	2012.01.09	Win32/PatchFile.gg
K7AntiVirus	9.124.5897	2012.01.09	Trojan
Kaspersky	9.0.0.837	2012.01.10	Trojan.Win32.Patched.md
McAfee	5.400.0.1158	2012.01.10	W32/Ramnit.b
McAfee-GW-Edition	2010.1E	2012.01.09	W32/Ramnit.b
Microsoft	1.7903	2012.01.09	Virus:Win32/Ramnit.AF
NOD32	6780	2012.01.10	Win32/Ramnit.H
Norman	6.07.13	2012.01.09	W32/Ramnit.AB
nProtect	2012-01-09.01	2012.01.10	Win32.Ramnit.N
Panda	10.0.3.5	2012.01.09	W32/Cosmu.L
PCTools	8.0.0.5	2012.01.10	Malware.Ramnit
Rising	23.92.01.01	2012.01.10	Win32.Ramnit.c
Symantec	20111.2.0.82	2012.01.10	W32.Ramnit.B!inf
TrendMicro	9.500.0.1008	2012.01.10	PE_RAMNIT.KC
TrendMicro-HouseCall	9.500.0.1008	2012.01.10	PE_RAMNIT.KC
ViRobot	2012.1.10.4872	2012.01.10	Win32.Ramnit.A
VirusBuster	14.1.158.1	2012.01.09	Win32.Ramnit.Gen.3

Additional information
MD5 : 25f6ee42d37e3f2f7dbe795e836d52e2

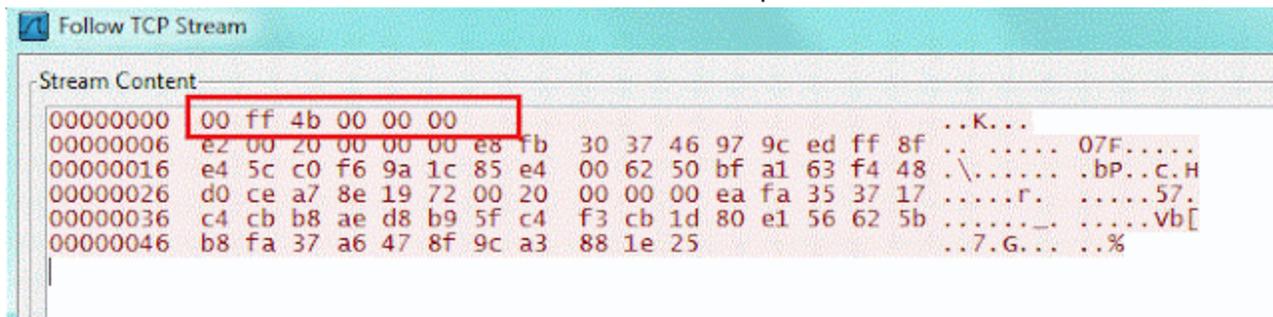
Traffic

607B2219FBCFBFE8E6AC9D7F3FB8D50E - C&C is sinkholed
C33E7ED929760020820E8808289C240E - C&C is active

Despite the fact that the C&C for 607B2219FBCFBFE8E6AC9D7F3FB8D50E is sinkholed, it is still interesting to see the malware behavior when it tries to establish a connection with the server.

Ramnit samples used by the same group of attackers have overlapping set of C&C servers - the list is not the same but I found that my samples that are supposedly later version that Ramnit.AK have approximately 80% overlap in C&C list used by this RamnitAK binary described by Sophos. I have combined the two lists and ran WHOIS queries to establish active C&C and their location and registration.

The communications with the sinkholed server below show that once the bot receives SYN command from the C&C, it sends **6 bytes of data**. Exact same behavior is described in this analysis of the binaries from Summer 2011 - with the only difference that the second packet sent by the bot was not 75 bytes but 149 bytes Bot of the Day: Ramnit/NinmulMonday, July 18th, 2011. If connection with the server is established, the traffic continues on on port 443, it is encoded but it is not SSL, it is some sort of custom protocol.



The bot is going through the list of domains trying to find those that are active. Most of the domains are not registered yet but the two currently active domains were registered on **January 5 and 6, 2011**. It appears that the attackers register new domains as soon as the lose any due to sinkholing and domain cancellations. Since all the domains have the most random names, they are not likely to be registered by someone else before they are needed. Having each binary to check a long list of domains makes the bot very noisy (consider making IDS signatures based on UDP port 53 thresholds) but it prevents the death of the botnet in case of the C&C loss. I have compiled a list of approximately 400 domains with only 21 of them registered. If you created DNS blocks or sinkhole domains, consider blocking or sinkholing all of them, not only active.

Domain name: rjordulltl.com
89.149.242.185 - Leaseweb Germany GmbH (previously netdirekt e. K.)
Germany
Registrar: Regtime Ltd.
Creation date: 2012-01-05
Expiration date: 2013-01-05

Domain Name: **goopndlgvy.com**

Registrant:

PrivacyProtect.org

Domain Admin (contact@privacyprotect.org)

ID#10760, PO Box 16

Note - All Postal Mails Rejected, visit Privacyprotect.org

Nobby Beach

null,QLD 4218

AU

Tel. +45.36946676

89.149.242.185 - Leaseweb Germany GmbH (previously netdirekt e. K.)
Germany
Creation Date: 06-Jan-2012
Expiration Date: 06-Jan-2013

Communications with a sinkholed C&C and search for a new active server:

```

172.29.0.116 68.87.73.246 DNS Standard query A google.com
68.87.73.246 172.29.0.116 DNS Standard query response A 74.125.113.105 A 74.125.113.105 A 74.125.113.105 A 74.125.113.105
172.29.0.116 74.125.113.105 TCP LocalInfoServr > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
74.125.113.105 172.29.0.116 TCP http > LocalInfoServr [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PERM=1
172.29.0.116 74.125.113.105 TCP LocalInfoServr > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
172.29.0.116 68.87.73.246 DNS Standard query A star-trakers.com
68.87.73.246 172.29.0.116 DNS Standard query response A 207.223.0.140
172.29.0.116 207.223.0.140 TCP docstoc > https [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
172.29.0.116 207.223.0.140 TCP docstoc > https [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
172.29.0.116 207.223.0.140 TCP docstoc > https [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
172.29.0.116 68.87.73.246 DNS Standard query A star-trakers.com
68.87.73.246 172.29.0.116 DNS Standard query response A 207.223.0.140
172.29.0.116 207.223.0.140 TCP dndocbroker > https [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
172.29.0.116 207.223.0.140 TCP dndocbroker > https [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
172.29.0.116 207.223.0.140 TCP dndocbroker > https [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
172.29.0.116 68.87.73.246 DNS Standard query A ufssqjtryrny.com
172.29.0.116 68.87.73.246 DNS Standard query A stlekkkjwo.com
172.29.0.116 68.87.73.246 DNS Standard query A trpxvrasfwtufox.com
172.29.0.116 68.87.73.246 DNS Standard query A eqjrbpohspje.com
172.29.0.116 68.87.73.246 DNS Standard query A t1xfriip.com
172.29.0.116 68.87.73.246 DNS Standard query A ttehtxch.com
172.29.0.116 68.87.73.246 DNS Standard query A ovqubrvaqfkwq.com
172.29.0.116 68.87.73.246 DNS Standard query A snkbcptiqqlvw.com
172.29.0.116 68.87.73.246 DNS Standard query A ryggrnucbedeuevxxg.com
172.29.0.116 68.87.73.246 DNS Standard query A ysrsoxyljerfoko.com
68.87.73.246 172.29.0.116 DNS Standard query response, No such name
172.29.0.116 68.87.73.246 DNS Standard query A trpxvrasfwtufox.com.hsd1.va.comcast.net
68.87.73.246 172.29.0.116 DNS Standard query response, No such name
172.29.0.116 68.87.73.246 DNS Standard query A stlekkkjwo.com.hsd1.va.comcast.net
68.87.73.246 172.29.0.116 DNS Standard query response, No such name
68.87.73.246 172.29.0.116 DNS Standard query response, No such name
68.87.73.246 172.29.0.116 DNS Standard query response, No such name
172.29.0.116 68.87.73.246 DNS Standard query A ufssqjtryrny.com.hsd1.va.comcast.net
68.87.73.246 172.29.0.116 DNS Standard query response, No such name
172.29.0.116 68.87.73.246 DNS Standard query A ryggrnucbedeuevxxg.com.hsd1.va.comcast.net
68.87.73.246 172.29.0.116 DNS Standard query response, No such name
172.29.0.116 68.87.73.246 DNS Standard query A ysrsoxyljerfoko.com.hsd1.va.comcast.net
68.87.73.246 172.29.0.116 DNS Standard query response, No such name
172.29.0.116 68.87.73.246 DNS Standard query A t1xfriip.com.hsd1.va.comcast.net
68.87.73.246 172.29.0.116 DNS Standard query response, No such name
172.29.0.116 68.87.73.246 DNS Standard query A ovqubrvaqfkwq.com.hsd1.va.comcast.net
68.87.73.246 172.29.0.116 DNS Standard query response, No such name
68.87.73.246 172.29.0.116 DNS Standard query response, No such name
68.87.73.246 172.29.0.116 DNS Standard query response, No such name
68.87.73.246 172.29.0.116 DNS Standard query response, No such name
172.29.0.116 172.29.0.253 NBNS Name query NB TLXPRLP.COM=00
68.87.73.246 172.29.0.116 DNS Standard query response, No such name
68.87.73.246 172.29.0.116 DNS Standard query response
172.29.0.116 68.87.73.246 DNS Standard query A snkbrotlooslv.com.hsd1.va.comcast.net
172.29.0.116 176.31.62.76 TCP fhc > https [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
68.87.73.246 172.29.0.116 DNS Standard query response A 176.31.62.76
172.29.0.116 176.31.62.76 TCP vlsi-lm > https [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
68.87.73.246 172.29.0.116 DNS Standard query response, no such name
176.31.62.76 172.29.0.116 TCP https > fhc [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
172.29.0.116 176.31.62.76 TCP fhc > https [ACK] Seq=1 Ack=1 Win=64240 Len=0
172.29.0.116 176.31.62.76 SSL Continuation Data
176.31.62.76 172.29.0.116 TCP https > vlsi-lm [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
172.29.0.116 176.31.62.76 TCP Continuation Data
176.31.62.76 172.29.0.116 TCP https > fhc [ACK] Seq=1 Ack=7 Win=5840 Len=0
172.29.0.116 176.31.62.76 SSL Continuation Data
176.31.62.76 172.29.0.116 TCP https > fhc [FIN, ACK] Seq=1 Ack=7 Win=5840 Len=0
172.29.0.116 176.31.62.76 TCP fhc > https [ACK] Seq=82 Ack=2 Win=64240 Len=0
172.29.0.116 176.31.62.76 TCP fhc > https [FIN, ACK] Seq=82 Ack=2 Win=64240 Len=0
176.31.62.76 172.29.0.116 TCP https > vlsi-lm [ACK] Seq=1 Ack=7 Win=5840 Len=0
176.31.62.76 172.29.0.116 TCP vlsi-lm > https [SYN] Seq=0 Win=64240 Len=0
172.29.0.116 176.31.62.76 TCP vlsi-lm > https [ACK] Seq=82 Ack=2 Win=64240 Len=0
172.29.0.116 176.31.62.76 TCP vlsi-lm > https [FIN, ACK] Seq=82 Ack=2 Win=64240 Len=0
172.29.0.116 68.87.73.246 DNS Standard query A burxondpknkk1lvkr.com
172.29.0.116 68.87.73.246 DNS Standard query A xtioyffigutuluff.com
68.87.73.246 172.29.0.116 DNS Standard query response, no such name
172.29.0.116 68.87.73.246 DNS Standard query A burxondpknkk1lvkr.com.hsd1.va.comcast.net
68.87.73.246 172.29.0.116 DNS Standard query response, no such name

```

Checks internet connection via Google.com

Sends query for star-trakers.com C&C

Receives unsatisfactory response, domain sinkholed

Sends another query for star-trakers.com C&C

Receives unsatisfactory response, domain sinkholed

Starts looking for backup C&C domains. Most are not registered yet

Finds one that is registered and responding

snkbcptiqqlvw.com 176.31.62.76 (sinkholed but responding)

1. Bot 172.29.0.116 sends SYN on port 443 to 176.31.62.76

2. Server 176.31.62.76 replies SYN ACK

3. Bot 172.29.0.116 sends 6 byte packet to what it thinks is C&C - on port 443

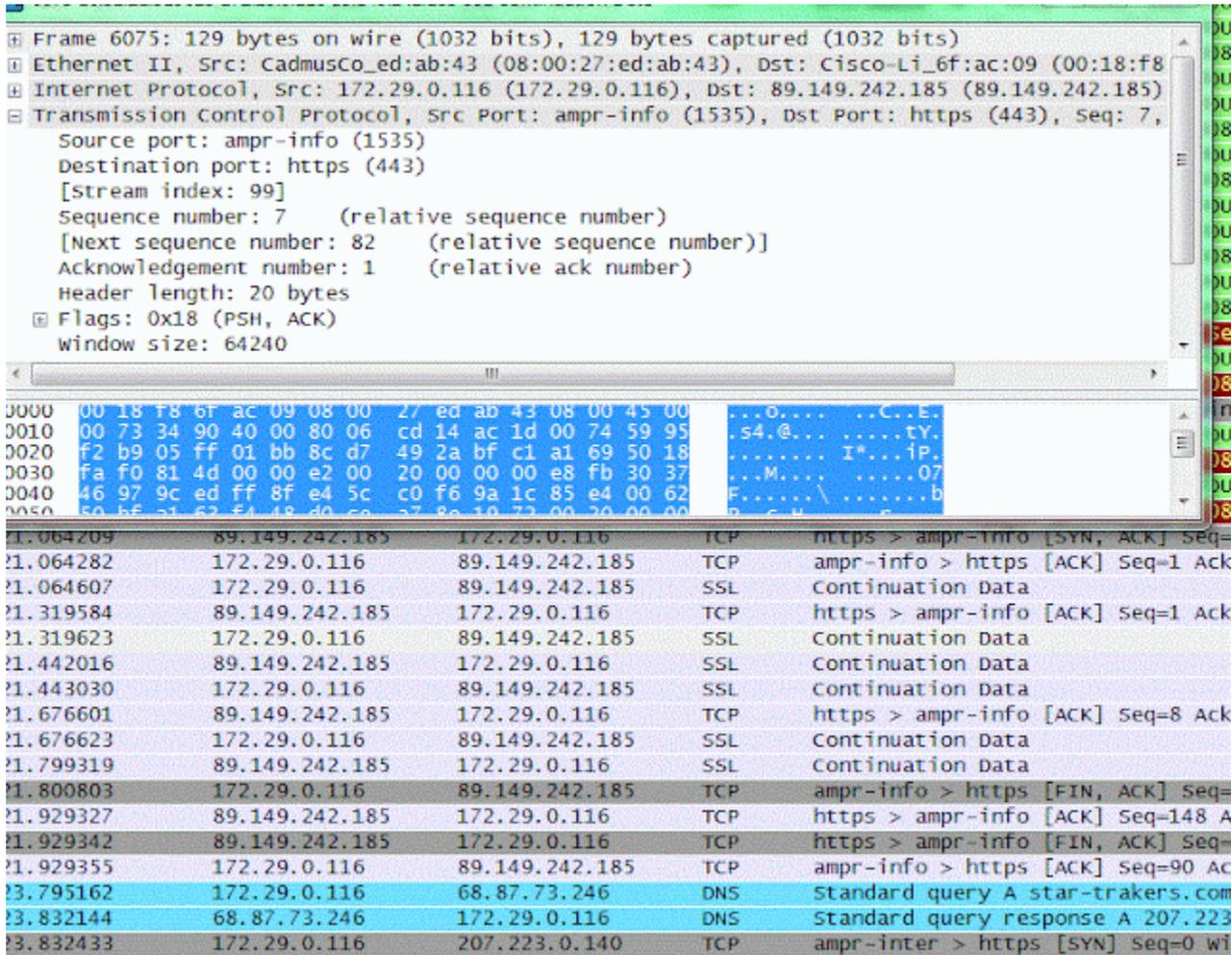
4. Server 176.31.62.76 replies ACK

5. Bot 172.29.0.116 sends 75 byte packet to what it thinks is C&C on port 443 and then sends FIN ACK in the next packet

Skipped lines in this section are replies to the second SYN

Continues checking the domain list for active C&C servers

Bot <-> C&C communications on port 443



List of domains used by Ramnit binaries - feel free to pre-emptively sinkhole them. Part of them are from this [Sophos analysis](#) and part is from running these two binaries

Registered domains. See the text version below. The yellow/red entries show active C&C. All others are sinkholed or NXD'd.

DOMAIN	HOST	IP	REG	Created
ihoxanyker.com		87.255.51.229	n/a tom jerry (arrettom83@yahoo.com) st112 new yor	08-Nov-2011
anspepxukbfmh.com			PrivacyProtect.org Domain Admin (contact@privacyprotect.	31-Oct-2011
carretfullezz.com			PrivacyProtect.org Domain Admin (contact@privacyprotect.	01-Jul-2011
gpoondlavy.com	89-149-242-185.local	89.149.242.185	PrivacyProtect.org Domain Admin (contact@privacyprotect.	06-Jan-2012
hetjmgiddiamqq.com		87.255.51.229	PrivacyProtect.org Domain Admin (contact@privacyprotect.	25-Nov-2011
mstwcsmvfmullkgh.com	hosted-by.leaseweb.com	62.212.65.176	PrivacyProtect.org Domain Admin (contact@privacyprotect.	05-Sep-2011
qftrnlap.com		87.255.51.229	PrivacyProtect.org Domain Admin (contact@privacyprotect.	24-Nov-2011
vxpqorqkihafv.com			PrivacyProtect.org Domain Admin (contact@privacyprotect.	27-Sep-2011
fsuatmti.com		82.165.39.88	Spy Eye Ilyinka Street 23 103132 Moscow RU Phone: +49.569537	22-Nov-2011
qgmrhcnntocnawdmq.com		82.165.39.88	Spy Eye Ilyinka Street 23 103132 Moscow RU Phone: +49.569537	22-Nov-2011
ouwwtmcnujdw.com		82.165.39.88	Spy Eye Ilyinka Street 23 103132 Moscow RU Phone: +49.569537	22-Nov-2011
qdfqgwiovjfseqdcepm.com		82.165.39.88	Spy Eye Ilyinka Street 23 103132 Moscow RU Phone: +49.569537	22-Nov-2011
vlupfbsuppijkrvbsdy.com		82.165.39.88	Spy Eye Ilyinka Street 23 103132 Moscow RU Phone: +49.569537	22-Nov-2011
rgordullt.com	89-149-242-185.local	89.149.242.185	Aleksandr Bragilevskij	
snkbcptiqqmhlvw.com			Aleksandr Bragilevskij	
star-trakers.com			Aleksandr Bragilevskij	
cpmsussqibatpmswq.com	176-31-62-76.this.domain.has.been.sinkholed.by.zinkhole.org	176.31.62.76	Contact Privacy Inc. Customer 0129677017 96 Mowat Ave Toror	13-Dec-2011
eeuprbpohspwje.com	176-31-62-76.this.domain.has.been.sinkholed.by.zinkhole.org	176.31.62.76	Contact Privacy Inc. Customer 0129769280 96 Mowat Ave Toror	24-Dec-2011
itehtxch.com	176-31-62-76.this.domain.has.been.sinkholed.by.zinkhole.org	176.31.62.76	Contact Privacy Inc. Customer 0129769281 96 Mowat Ave Toror	24-Dec-2011
oalfpapl.com	ip-50-62-3-35.ip.secureserver.net	50.62.3.35	Domains By Proxy, LLC DomainsByProxy.com 15111 N. Hayden R	23-Aug-11

As you notice, many domains are registered by "Aleksandr Bragilevskij"
Registrar: Regtime Ltd.

Creation date: 2011-12-03

Expiration date: 2012-12-03

Registrant:

Aleksandr Bragilevskij

Email: pfizer.corp@yahoo.com

Organization: Aleksandr Bragilevskij

Address: 333 E 79th St # 1T,

City: New York City

State: NY

ZIP: 10001

Country: UM

Phone: +1.2127332323

Fax: +1.2127332323

Google Search for pfizer.corp@yahoo.com reveals that the same address was used to register fake Canadian pharmacy sites, which makes sense, considering the Viagra spam.

trustpharmacy.us

188.72.200.84

Markus Faizer

Pfizer International

333 E 79th St # 1T,

New York City

NY

10001

United States

Phone: +1.2127332323

Fax: +1.2127332323

E-mail: pfizer.corp@yahoo.com

[TOP SALE Viagra from USD 0.89 per pill, Cialis from USD 1.81 per pill](#)

shop.trustpharmacy.us/products/pain_relief/ultram/

A: If you need a product which is not mentioned at our site, you can let us know of the product you are interested in and we will try our best to add it to our list as ...

About Us

shop.trustpharmacy.us/pages/about/

A: If you need a product which is not mentioned at our site, you can let us know of the product you are interested in and we will try our best to add it to our list as ...

[TOP SALE Viagra from USD 0.89 per pill, Cialis from USD 1.81 per pill](#)

shop.trustpharmacy.us/product/?product=kamagra_brand_oral...

A: If you need a product which is not mentioned at our site, you can let us know of the product you are interested in and we will try our best to add it to ...

Canadian Health&Care Mall - Symbicort - Order Now

shop.trustpharmacy.us/products/anti_allergic_asthma/.../order/

Symbicort - Symbicort is an effective combination medicine used to treat and manage both asthma and COPD.

[TOP SALE Viagra from USD 0.90 per pill, Cialis from USD 1.75 per pill](#)

trustpharmacy.us/more_info/?product=viagra_soft

A: If you need a product which is not mentioned at our site, you can let us know of the product you are interested in and we will try our best to add it to our list as ...

About Us

shop.trustpharmacy.us/pages/about/ - Cached

ALL PRODUCTS | ABOUT US | HOW TO ORDER | TESTIMONIALS | FAQ | CONTACT

Search [input type="text"] [button: Search]

Home | About Us | Contact Us | Privacy Policy | Terms of Service

About Us

Dear Customers, we are glad to meet you at our company's history page. We would have been without each other without you here.

Key Mile

There is a great underlying motivation for Canadian HealthCare Mall. Our Pharmacy began as an independent business located in Ontario in 1998. Canadian HealthCare Mall was born from our love for our customers and our desire to provide them with the best possible service. We have been able to do this by offering our customers the best prices on our products and services and to create a truly comprehensive online resource available to absolutely any customer.

Through the years a common goal has been to provide our customers with the highest quality products and services available. Our website is a growing representation of our vision for the future.

2000-2004

The website for the pharmaceutical industry has in the past been a place of confusion and uncertainty. The development of a website for the pharmaceutical industry has in the past been a place of confusion and uncertainty. The development of a website for the pharmaceutical industry has in the past been a place of confusion and uncertainty.

2005-2009

The website is mostly based on product information. The basic information of our products both in the online and in the offline world. We have also signed contracts with a number of major suppliers to make our website more and more secure. We are now with our suppliers and our customers we have a truly comprehensive online resource available to absolutely any customer.

2010-2014

At the end of the pharmaceutical industry in 2010, the website was a place of confusion and uncertainty. The development of a website for the pharmaceutical industry has in the past been a place of confusion and uncertainty.

Photo: [img alt="Portrait of a man in a white coat, likely a representative of the pharmacy."/>

