Blackhole Ramnit - samples and analysis

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

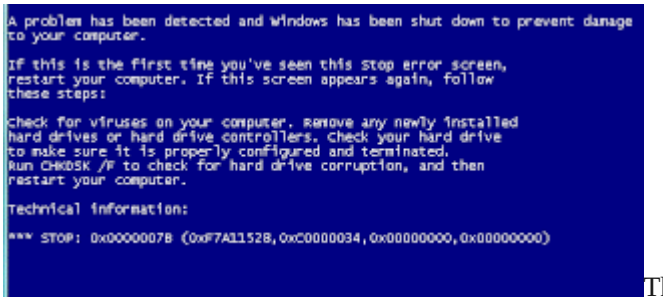
Please wait page is loading...

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?id=f52bfac9637aea189ec918d05113c36f5bcf580f3c0de8a934fe3438107d3f0c-1326310185

> File: vcryserj.exe
> Size: 135680
> MD5: 607B2219FBCFBFE8E6AC9D7F3FB8D50E

- \Application Data\wduqtdai.log - number of logs varies, contain encrypted data
- \Application Data\xtyepaef.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?id=c1293f8dd8a243391d087742fc22c99b8263f70c6937f784c15e9e20252b38ae-1326346542

> File: dnsgvbny.sys
> Size: 15360
>
> MD5: A6D351093F75D16C574DB31CDF736153

Results:

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\nvamibiv\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.

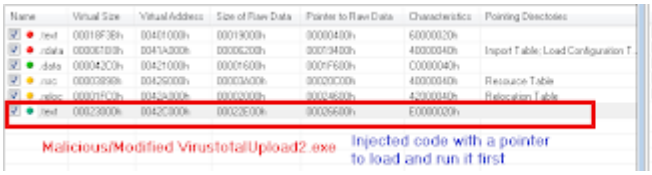
It generates spam that it sends out on port 25, Hendrik already described this behavior in his post.

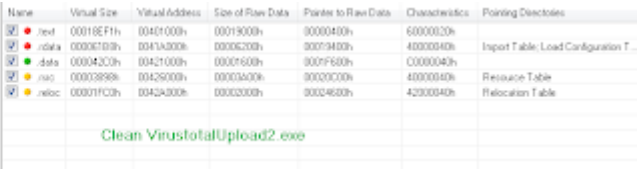
C33E7ED929760020820E8808289C240E

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.





Thsi 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
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

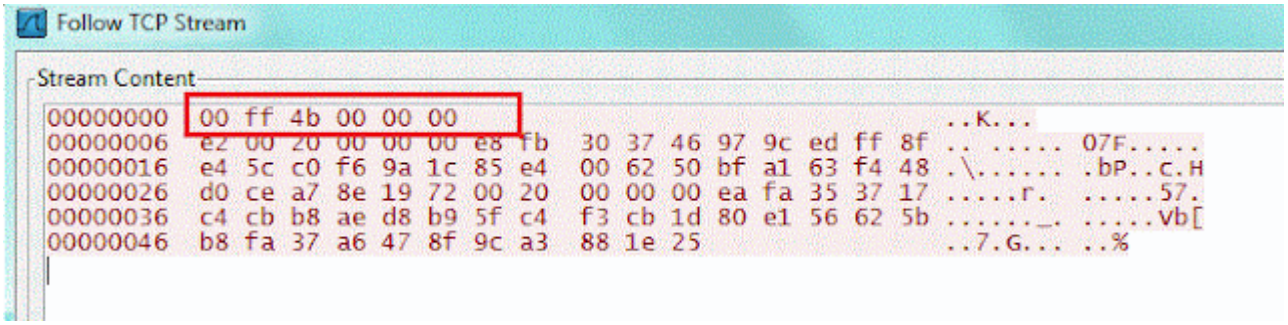
Traffic

607B2219FBCFBFE8E6AC9D7F3FB8D50E - C&C is sinkholedC33E7ED929760020820E8808289C240E - 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.

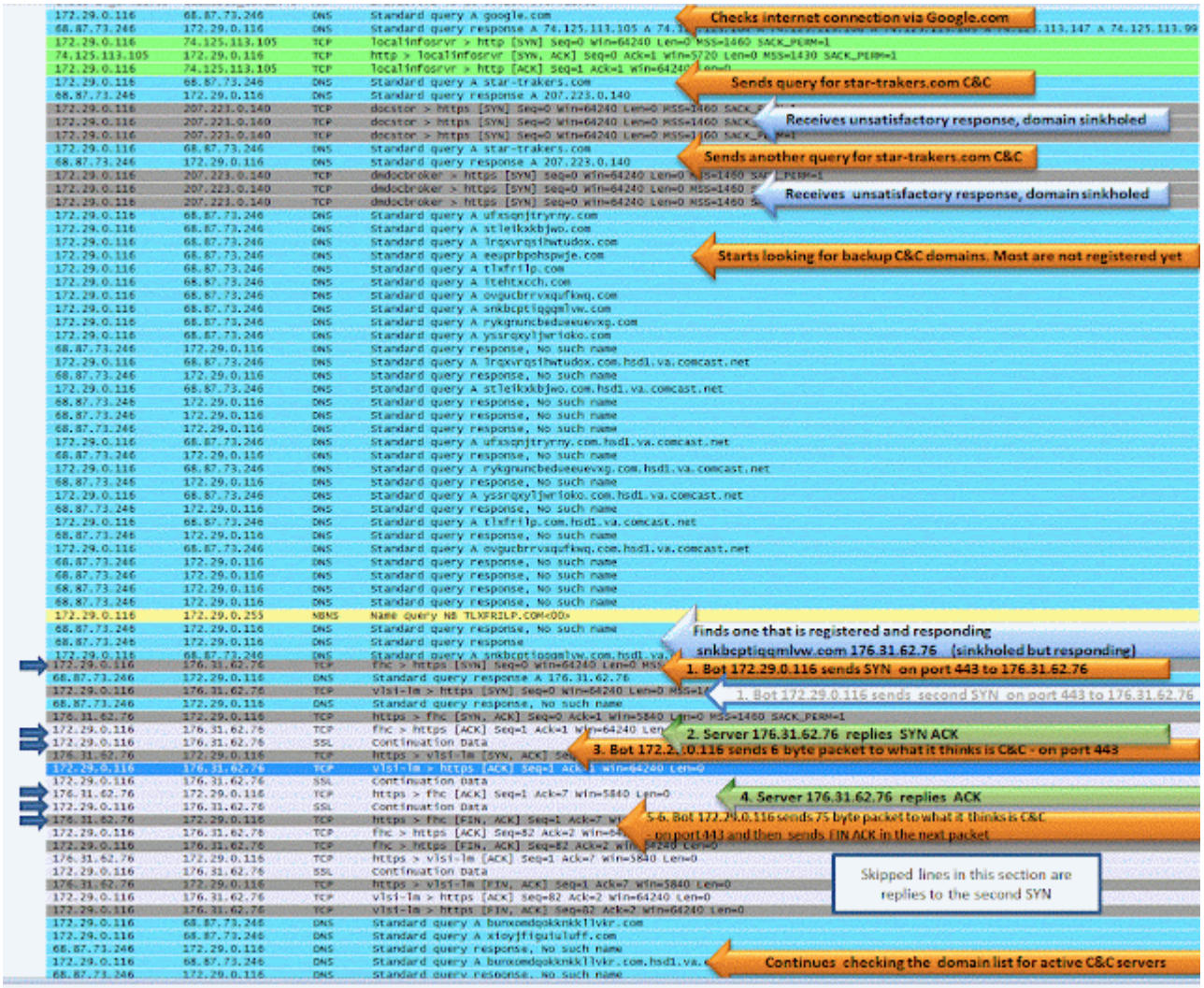


The bot is going through the list of domains trying to find those that are active. Most of the domains are not registered yet but the two currently active domains were registered on **January 5 and 6, 2011.** It appears that the attackers register new domains as soon as the lose any due to sinkholing 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 complied 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.

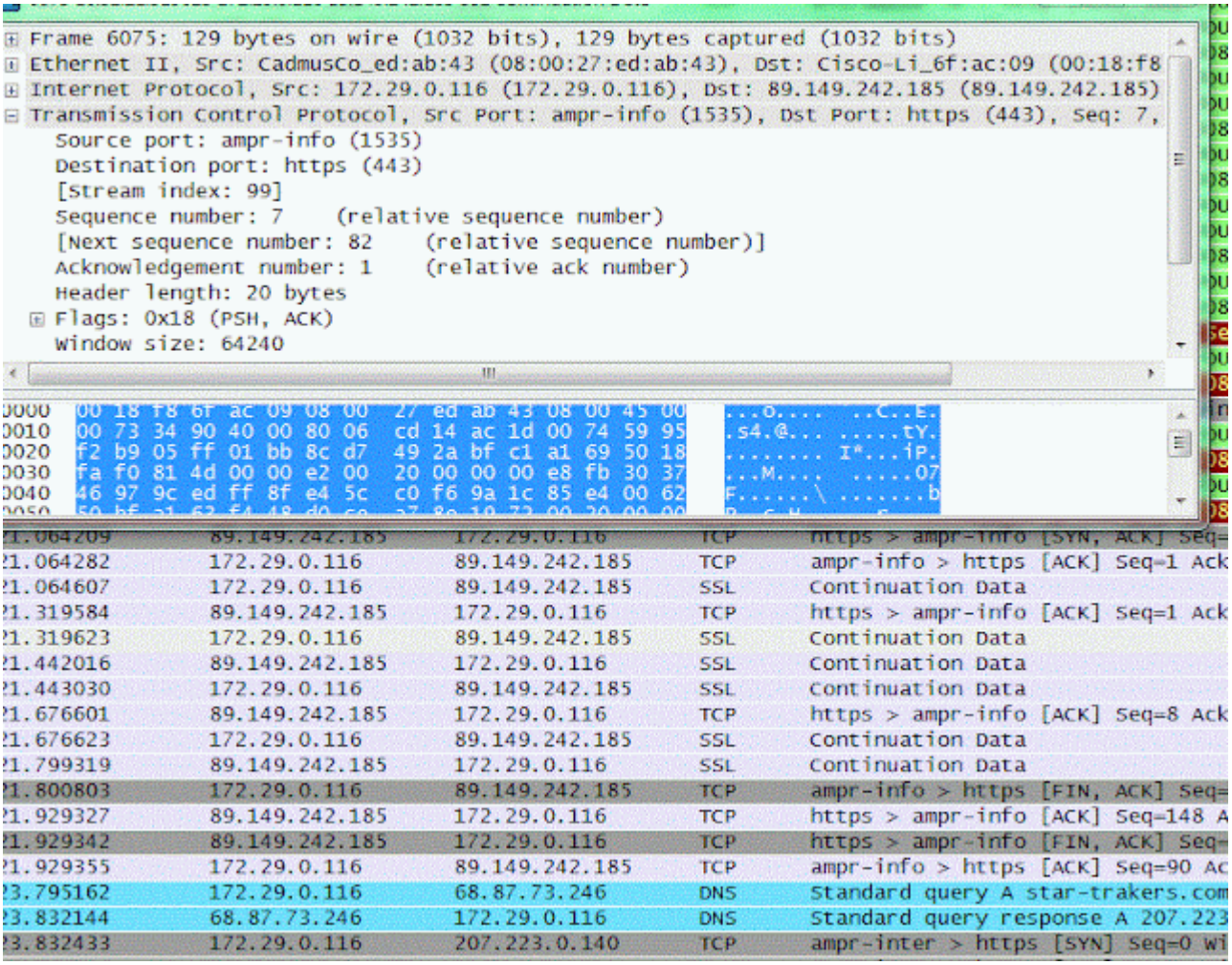
> Domain name: rjordulltl.com
> 89.149.242.185 - Leaseweb Germany GmbH (previously netdirekt e. K.)
> Germany

> 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:



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

---

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