LOOKINGGLASS

SALITY

2003 – TODAY.

PRESENTER:

Peter Kleissner
Botconf'15, 2-4 Dec 2015, Paris/France

About

- In business since 2003 [1], allegedly from Russia [1]
- File infector (infects all executable files)
- Multi-purpose botnet

- Is reportedly doing: Stealing, distributed attacks, spam, multi-purpose
- Features a P2P algorithm: 2 separate main botnets
- Highest version numbers: 241 and 96 (of the 2 botnets)

- More than 2 million infections per day reported by Virus Tracker
- Estimated about 4 million total worldwide infections

- Not many people are aware of Sality's evilness !

Timeline

2003	First appearance [1]
2004-2008	New improved variants
2008	Peer-to-peer algorithm added, early test networks 1 and 2 (dead)
2009	P2P network 3 created (still alive, bigger one)
2010	P2P network 4 created (still alive)
2015	Still in business!

Originally named Win32.HLLP.Kuku?

Sophos *https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/W32~Sality-H/detailed-analysis.aspx*:

"On the 10-12th of the month, when the minute equals the hour, the following message is displayed with the title 'Win32.HLLP.Kuku v2.91':

<<<<<Hey, Lamer! Say "Bye-bye" to your data! >>>>>

Copyright (c) by Sector' "

String in Binary	Title in Email
Win32.HLLP.Kuku v1.02	
Win32.HLLP.Kuku v1.09	
Win32.HLLP.Kuku v2.05	Message from ST v2.05 - Sector(c), Salavat-city 2003
Win32.HLLP.Kuku v2.91	
Win32.HLLP.Kuku v2.92	Message from ST v2.92 - Sector(c), Salavat-city 2003
	Message from ST v2.93 - Sector(c), Salavat-city 2004
Win32.HLLP.Kuku v3.09	

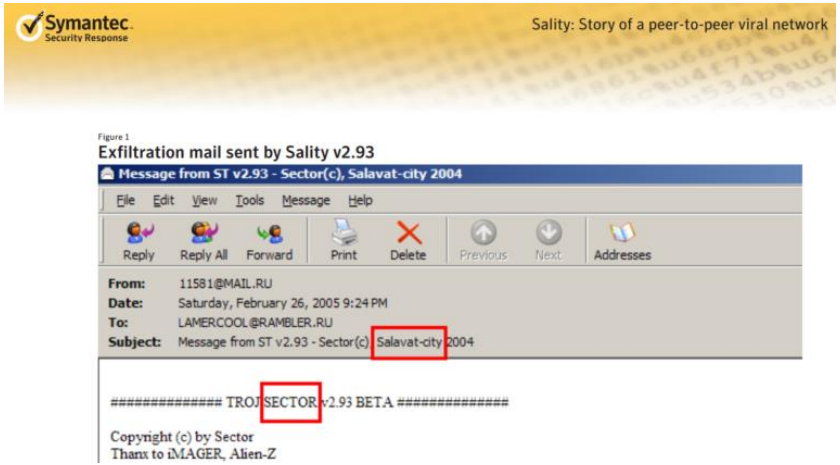
LOOKINGGLASS

Author of Sality

Author of Sality?

According to Symantec [1]:

"the curious reader asking where the name "Sality" originated from now has the answer: it is derived from "Salavat City", a Russian town from which the author may originate. This threat bears a couple of other names, also related to strings found inside the payload: "Kuku" (which means Hide-and-Seek in Russian), or "Sector" (the nickname of the author)."



Author of Sality?

In those old emails there appear 3 nick-names:

1. Sector
2. iMAGER
3. Alien-Z

Those emails were used in the early samples:
Sender: 11581@mail.ru
Receiver: lamercool@rambler.ru, alien-z@mail.ru, imager@mail.ru

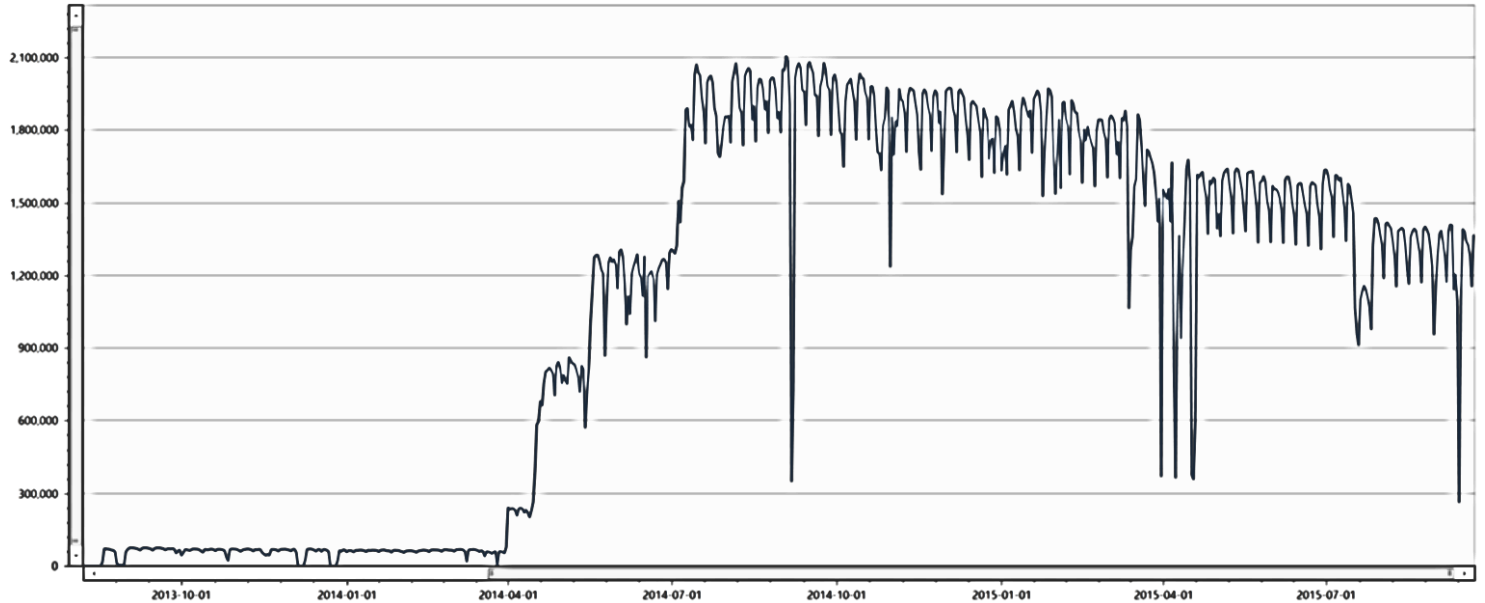
```
From sample 52AE3B7F8F383F169363B5D4F5D5DECA via Wireshark:

220 smtp47.i.mail.ru ESMTP ready
HELO MAIL.RU
250 smtp47.i.mail.ru
MAIL FROM:<11581@MAIL.RU>
250 2.0.0 OK
RCPT TO:<11581@MAIL.RU>
550 SMTP is available only with SSL or TLS connection enabled.

220 smtp19.mail.ru ESMTP ready
HELO MAIL.RU
250 smtp19.mail.ru
MAIL FROM:<11581@MAIL.RU>
250 2.0.0 OK
RCPT TO:<IMAGER@MAIL.RU>
550 SMTP is available only with SSL or TLS connection enabled.
```

LOOKINGGLASS

Statistics

Statistics

Up to 2 million per day monitored at Virus Tracker via sinkholing



Statistics

Per country on 9/23/2015

20% observed via P2P
80% observed on domain sinkholes

> 1% infections listed:

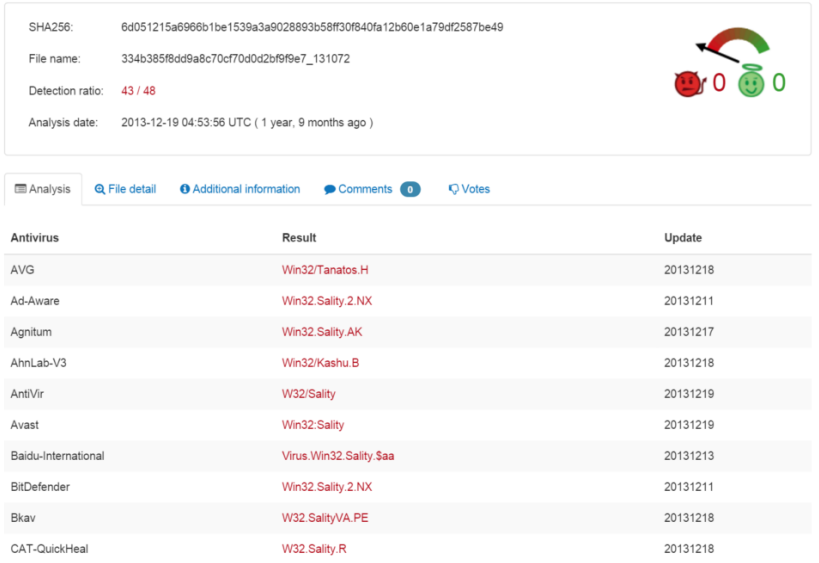
21.21	284.029	Other
19.67	263.403	India
8.99	120.421	Egypt
8.69	116.346	Vietnam
6.27	83.975	Pakistan
5.51	73.763	Iran, Islamic Republic of
4.73	63.282	Indonesia
3.97	53.154	China
3.33	44.616	Thailand
2.62	35.111	Turkey
2.57	34.376	Philippines
2.48	33.198	Brazil
2.29	30.644	Russian Federation

Source: Virus Tracker (throughout this presentation); all numbers are unique IPs per day

Statistics

The reasons mostly 3rd world countries are affected are:

1. Pirated Windows with updates disabled
2. Often no AV installed; Sality's detection is VERY high, pretty much any AV detects & removes it



SHA256: 6d051215a6966b1be1539a3a9028893b58ff30f840fa12b60e1a79df2587be49

File name: 334b385f8dd9a8c70cf70d0d2bf9f9e7_131072

Detection ratio: 43 / 48

Analysis date: 2013-12-19 04:53:56 UTC (1 year, 9 months ago)

0 0

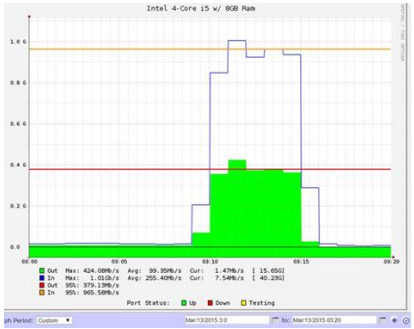
Analysis | File detail | Additional information | Comments 0 | Votes

Antivirus	Result	Update
AVG	Win32/Tanatos.H	20131218
Ad-Aware	Win32.Sality.2.NX	20131211
Agnitum	Win32.Sality.AK	20131217
AhnLab-V3	Win32/Kashu.B	20131218
AntiVir	W32/Sality	20131219
Avast	Win32:Sality	20131219
Baidu-International	Virus.Win32.Sality.$aa	20131213
BitDefender	Win32.Sality.2.NX	20131211
Bkav	W32.SalityVA.PE	20131218
CAT-QuickHeal	W32.Sality.R	20131218

DdoS attacks allegedly from Sality

4 ddos attacks against Virus Tracker:

#1	November 27, 2014	1 Gbps ddos ICMP + UDP + TCP
#2	January 30, 2015	10 Gbps ddos UDP + TCP + NTP amplification
#3	March 13, 2015	120 Gbps ddos NTP + DNS amplification
#4	June 21, 2015	10 Gbps ddos UDP



Link between ddos attacks and Sality

Ddos #1 on 11/27/2014:

Top 10 flows by bits per second for dst IP: 69.195.129.70

Duration	Proto	Src IP Addr	Src Pt	Dst Pt	Packets	pps	bps
0.067	UDP	178.78.246.45	53	62933	2048	30567	370.2 M
0.008	**TCP**	**78.171.31.7**	**54245**	**80**	**2048**	**255999**	**281.6 M**
101.264	UDP	204.145.94.87	47446	80	16.4 M	161794	119.1 M
0.019	ICMP	94.203.140.192	5	0.1	3072	161684	90.5 M
0.340	UDP	178.47.45.22	53	62933	2048	6023	73.0 M
98.668	UDP	209.119.225.25	53	12162	421888	4275	51.8 M
179.829	UDP	162.249.122.2	53	12162	753664	4191	50.8 M
98.318	UDP	209.122.107.49	53	12162	411648	4186	50.7 M
98.282	UDP	80.73.1.1	53	12162	387072	3938	47.7 M
97.400	UDP	216.174.102.25	53	12162	367616	3774	45.7 M

Ddos #2 on 1/30/2015:

Top 10 flows by bits per second for dst IP: 69.195.129.70

Duration	Proto	Src IP Addr	Src Pt	Dst Pt	Packets	pps	bps
0.006	UDP	61.93.224.130	56576	64265	2048	341333	4.1 G
0.006	UDP	111.17.216.35	59563	36767	2048	341333	4.1 G
0.006	UDP	89.27.129.254	123	80	2048	341333	1.3 G
0.019	UDP	61.93.224.130	64356	49110	2048	107789	1.3 G
0.055	**TCP**	**201.172.228.114**	**49532**	**80**	**2048**	**37236**	**29.5 M**
284.252	UDP	202.32.138.21	123	80	1.3 M	4657	18.0 M
284.131	UDP	182.19.66.178	123	80	950272	3344	12.9 M
286.991	UDP	213.56.30.120	123	80	826368	2879	11.1 M
287.132	UDP	206.196.172.14	123	80	822272	2863	11.0 M
286.758	UDP	199.192.104.10	123	80	806912	2813	10.9 M

Each time the only TCP attacker is a known Sality infection:

2014-11-24 17:47:09	Turk Telekom	Sality	78.171.31.7	Turkey	ygiudewsqhct.in	/in.php
2014-11-26 10:23:34	Turk Telekom	Sality	78.171.31.7	Turkey	ygiudewsqhct.in	/in.php
2014-11-27 10:55:12	Turk Telekom	Sality	78.171.31.7	Turkey	ygiudewsqhct.in	/in.php

2015-01-28 00:00:24	Television Internacional S.A...	Sality	201.172.228.114	Mexico	hzmksreiuojy.biz	/ldr.php
2015-01-29 14:10:09	Television Internacional S.A...	Sality	201.172.228.114	Mexico	hzmksreiuojy.biz	/ldr.php
2015-01-30 14:15:19	Television Internacional S.A...	Sality	201.172.228.114	Mexico	hzmksreiuojy.biz	/ldr.php

LOOKINGGLASS

Technical Information

Botnets?

- Only active botnets are #3 and #4, both are independent P2P botnets
  - Network 1/2: Both dead
  - Network 3: Since 2009, current version 241
  - Network 4: Since 2010, current version 96
- Version numbers here are via URL packs
  - So 241 + 96 different sets of C&C URLs
  - If you know all the URL packs you can sinkhole them and find out info of old infections!
- You can find many domains from the URL packs in reports on the internet

Network #2 Sample

Injects into explorer.exe, starts immediately with the P2P algorithm and then falls back to a hard-coded list of domains.

Process	Protocol	Local Address	Remote Address	State
explorer.exe:1544	TCP	random.eu-af.regus.local:1106	69.195.129.70:http	CLOSE_WAIT
explorer.exe:1544	UDP	random:7394	*:*	
lsass.exe:660	UDP	random:isakmp	*:*	

5	30.554740	10.0.2.15	58.40.150.204	UDP	Source port: instl_bootc Destination port: 5517
6	30.622179	10.0.2.15	89.149.227.194	UDP	Source port: cognex-insight Destination port: 9674
7	30.692456	10.0.2.15	98.149.227.194	UDP	Source port: gmrupdateserv Destination port: 9674
8	30.765233	10.0.2.15	205.186.187.66	UDP	Source port: bsquare-voip Destination port: 9674
9	30.832794	10.0.2.15	61.139.8.100	UDP	Source port: cardax Destination port: 9674
10	30.902696	10.0.2.15	213.239.225.166	UDP	Source port: bridgecontrol Destination port: 9674
11	30.973840	10.0.2.15	121.10.40.146	UDP	Source port: warmspotMgmt Destination port: 9674
12	31.045504	10.0.2.15	121.10.40.147	UDP	Source port: rdrmshc Destination port: 9674
13	31.113045	10.0.2.15	121.10.40.155	UDP	Source port: dab-sti-c Destination port: 9674
14	31.184182	10.0.2.15	121.10.40.154	UDP	Source port: imgames Destination port: 9674
15	31.269262	10.0.2.15	121.32.255.2	UDP	Source port: avocent-proxy Destination port: 9674

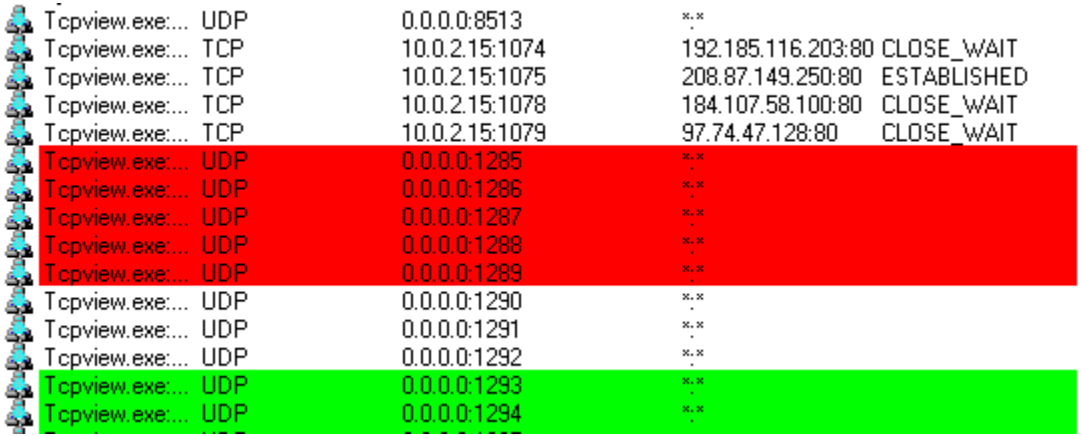
MD5 334B385F8DD9A8C70CF70D0D2BF9F9E7

SHA1 9B11CD8822F780275F23155AC0F92B44E9081A04

Network #3 Sample

Injects into a random process

Annoying port behavior – reinventing the TCP wheel over UDP:



Tcpview.exe:...	UDP	0.0.0.0:8513	*:*	
Tcpview.exe:...	TCP	10.0.2.15:1074	192.185.116.203:80	CLOSE_WAIT
Tcpview.exe:...	TCP	10.0.2.15:1075	208.87.149.250:80	ESTABLISHED
Tcpview.exe:...	TCP	10.0.2.15:1078	184.107.58.100:80	CLOSE_WAIT
Tcpview.exe:...	TCP	10.0.2.15:1079	97.74.47.128:80	CLOSE_WAIT
Tcpview.exe:...	UDP	0.0.0.0:1285	*:*	
Tcpview.exe:...	UDP	0.0.0.0:1286	*:*	
Tcpview.exe:...	UDP	0.0.0.0:1287	*:*	
Tcpview.exe:...	UDP	0.0.0.0:1288	*:*	
Tcpview.exe:...	UDP	0.0.0.0:1289	*:*	
Tcpview.exe:...	UDP	0.0.0.0:1290	*:*	
Tcpview.exe:...	UDP	0.0.0.0:1291	*:*	
Tcpview.exe:...	UDP	0.0.0.0:1292	*:*	
Tcpview.exe:...	UDP	0.0.0.0:1293	*:*	
Tcpview.exe:...	UDP	0.0.0.0:1294	*:*	

MD5 B2FB74393D65E8CF91158D6DAAADC70A

SHA1 257E841963D52D2691D34AAE3E1EF7FCB95F4C99

P2P Algorithm

- UDP; default port 9674 but calculated from the computer name
- Peers keep a “goodcount” value -> makes fake peer injection more difficult
- Networks 3/4 have nearly the same commands (only the URL pack payload is slightly different):
  - Network 4 uses 2048 RSA instead of 1024 for the certificate
  - Network 4 opens a TCP port on default 9673 for file transfer

10.0.2.15	89.40.29.148	UDP	Source port: amx-icsp Destination port: 6599
10.0.2.15	121.175.78.61	UDP	Source port: amx-axbnet Destination port: 5817
10.0.2.15	210.182.247.240	UDP	Source port: pip Destination port: 10647
10.0.2.15	112.144.153.58	UDP	Source port: novation Destination port: 7374
10.0.2.15	78.97.239.70	UDP	Source port: brcd Destination port: 6203
10.0.2.15	91.191.15.200	UDP	Source port: delta-mcp Destination port: 6827
10.0.2.15	77.232.212.93	UDP	Source port: dx-instrument Destination port: 7204
10.0.2.15	84.123.94.171	UDP	Source port: wimsic Destination port: 7435
10.0.2.15	93.120.75.42	UDP	Source port: ultrex Destination port: 9853
10.0.2.15	94.52.174.83	UDP	Source port: ewall Destination port: 9674
10.0.2.15	82.229.4.35	UDP	Source port: netdb-export Destination port: 5114
10.0.2.15	89.137.57.111	UDP	Source port: streetperfect Destination port: 7167

P2P Algorithm

- Reinventing the TCP wheel
  - "OK" responses
  - One UDP port per connection (annoying); has a time-out
  - One port always open for incoming control connections
- Basic commands:
  - 1 = Announcement & Promotion ("here I am!", shares port number)
  - 2 = Peer Exchange (exchanging 1 single peer: IP:Port)
  - 3 = Pack Exchange (exchanging the URL list, both ways)
- Assigning internal (NOT shared) peer ids:
  - < 16000000: low peer id, not reachable from outside (NAT)
  - >: High peer id, supernode

P2P Statistics

7/22/2014:

Network	Inactive	Active	Supernode	Total
#3	85	414.688	923	415.696
#4	195	91.644	157	91.996
Total	280	506.332	1.080	507.692

9/24/2015:

Network	Inactive	Active	Supernode	Total
#3	19	251.279	161	251.459
#4	218	68.919	56	69.193
Total	237	320.198	217	320.652

Source: Virus Tracker

URL Packs

- Examples (they always use hacked servers):

221	http://mersinescortlari.com/logo.gif	Criminals	192.168.25.8
	http://www.plsexpress.com/images/logo.gif	Ghosted	
	http://paepailin.com/logo.gif	Criminals	61.19.249.48
	http://deresut.com/logo.gif	Criminals	79.98.132.170
	http://smtrofeus.com.br/logo.gif	Criminals	187.63.191.11
	http://nbfix.net/logo.gif	Parked/expired	119.59.124.56
	http://refkajparis.fr/logo.gif	Criminals	213.186.33.3

185	http://doasoil.gov.np/images/logo.gif	Parked/expired	202.45.144.24
	http://earnestbiz.com/img/logof.gif	Criminals	119.252.152.151
	http://fotozenistanbul.com/images/logo.gif	Criminals	178.210.174.10
	http://cmyj.co.th/images/logo.gif	Criminals	27.254.40.97
	http://chonkanya.ac.th/images/logo.gif	Parked/expired	27.254.83.226
	http://dinamikdekor.com/images/logof.gif	Criminals	94.103.35.2
	http://aniketkulkarni.in/images/logo.gif	Parked/expired	65.98.57.194
	http://alabousco.com/en/images/logof.gif	Sinkhole by K&A	69.195.129.70
	http://comsindia.com/images/logo.gif	Criminals	144.76.91.236
	http://muaythaiphuketschool.com/logos.gif	Not in namespace	

URL Packs

- The P2P crawler writes them all out to a text file, that way Lookingglass knows first-hand all the (previous) domains!

- URL Packs already in the trap: 0, 8, 10, 11, 12, 14, 15, 20, 30, 31, 63, 64, 65, 66, 69, 71, 77, 78, 80, 82, 83, 84, 85, 87, 88, 89, 91, 92, 93, 94, 95, 96, 138, 156, 160, 165, 179, 195, 219, 223, 224, 226, 227, 68, 116, 124, 129, 130, 131, 133, 136, 137, 141, 142, 144, 145, 147, 152, 153, 154, 155, 157, 158, 159, 161, 162, 164, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 197, 198, 200, 201, 202, 203, 204, 205, 206, 207, 208, 210, 211, 212, 213, 214, 215, 216, 217, 218, 220, 221, 222, 225, 228, 229, 230, 231, 234, 236, 240, 241

- K&A targets to sinkhole every single Sality botnet.

URL Packs

- Network 4 has many invalid C&C URLs in its URL packs:

95	http://padrup.com.ds/sobaka1.gif	Not in namespace	
	http://46.105.103.219/sobakavolos.gif	IPv4 address	46.105.103.219
96	http://slwocfd/sobaka1.gif	Not in namespace	
	http://46.105.103.219/sobakavolos.gif	IPv4 address	46.105.103.219

- There is no .ds TLD!
- “slwocfd” is not a valid domain as well!

- Unknown why they use invalid URLs.

More interesting observations

One C&C domain:

0-0-1-1-1-0-1-1-1-0-0-1-1-0-1-0-1-1-0-0-1-0-0-1-1-1-1-1-1-1-1-.0-0-0-0-0-0-0-0-0-0-0-0-0-0-49-0-0-0-0-0-0-0-0-0-0-0-0-0.info

Yes that's a valid domain.

Domains are easy to find, they usually use "/logo.gif" or similar document paths.

It creates the mutexes "purity_control_4428" and "kukutrusted!" to verify if it's already running. [4]

URLs in the URL Packs

- Every URL points to an executable file that is simply RC4 encrypted in blocks
- It is downloaded by Sality and executed

```
char * Sality_C2_Key = "GdiPlus.dll";
for (unsigned n = 0; n < Sality_C2_Payload_Size; n += 1024)
        rc4((BYTE *)Sality_C2_Payload + n, 1024, (BYTE *)Sality_C2_Key, strlen(Sality_C2_Key));
```

- No certificate! Anyone can encrypt executables and distribute to Sality infections by taking over existing C&C URLs (registering expired ones).
- (vs RSA signature in P2P commands)
- (interestingly there is no C&C panel – just the plain binary on servers)

Latest URL Pack File

Latest URL pack version: 240 from 8/24/2015 19:42

http://tattooinindia.com/bottom.gif 13 KB, RC4 encrypted

tattooinindia.com_bottom.gif

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000   8B 36 50 7B F5 F9 22 C4 3C BD 49 AB EB 28 ED B8  ‹6P{õù"Ä<½I«ë(í¸
00000010   1B FE A4 3B CB C7 5C BC 5C 01 2D 44 43 07 E1 2A  .þ¤;ËÇ\¼\.-DC.á*
00000020   9D BB 4A AF 6C 44 B7 2D 17 04 79 BF 78 14 40 4B  .»J¯lD·-..y¿x.@K
00000030   C8 33 19 75 52 DE FE EC BC 76 2E 06 A7 74 BD 26  È3.uRÞþì¼v..§t½&
00000040   DC 39 8C 36 5C E1 45 05 43 A7 04 EE 8D 4D 66 FA  Ü9Œ6\áE.C§.î.Mfú
00000050   BF 92 3C 15 5E 0B 84 3E C0 4C 3A 44 B1 B4 36 A2  ¿'<.^.„>ÀL:D±´6¢
```

tattooinindia.com_bottom.gif | tattooinindia.com_bottom_decrypted.gif

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000   4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ..........ÿÿ..
00000010   B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ¸.......@.......
00000020   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000030   00 00 00 00 00 00 00 00 00 00 00 00 D8 00 00 00  ............Ø...
00000040   0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  ..°..´.Í!¸.LÍ!Th
00000050   69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is program canno
```

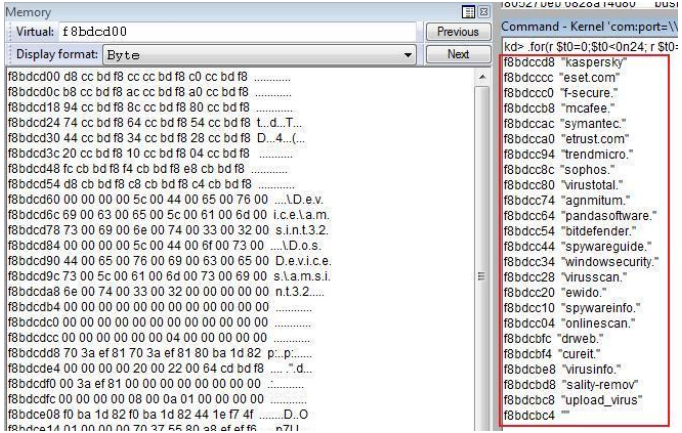
http://frmaurice.org/images/bottom.gif
http://tattooinindia.com/bottom.gif
http://intermarc-ng.com/img/bottom.gif
http://bajaparkingcommx.ipower.com/bottom.gif
http://79.96.88.43/bottom.gif
http://lexcorpapp.com/bottom.gif
http://hunerelektrik.com/bottom.gif
http://www.uolist.net/list/img/image.gif

Rootkit

Simple (5 KB) but effective rootkit (driver based), creates a device: [3]

```
\Device\amsint32
\DosDevices\amsint32
```

Kills processes by using NtTerminateProcess
Filters IP packets and drops packets containing certain AV vendor strings (picture on the right [3])



amsint.sys 4.56 Kb
MD5 31DE33A273CF87952E94D3534335A9B1
SHA1 4DF636D4DE33D549A3A6E27CA75E8EB60E77C77A

Simple Evilness

Modifying simple but effective registry keys to stop Windows notifications:

```
SOFTWARE\Microsoft\Security Center
AntiVirusOverride
AntiVirusDisableNotify
FirewallDisableNotify
FirewallOverride
UpdatesDisableNotify
UacDisableNotify
AntiSpywareOverride
```

https://malwr.com/analysis/OGRiNTU2Y2U0ZmY1NGQ1YmI2MjU5ZTRiYjZiNDc4MjU/

LOOKINGGLASS

Remediation

How to remove on a single machine

1. Enable Windows update
2. Done!

How to remove on a single machine

1. Enable Windows update
2. Done!

⇒ MSRT will kill it

http://blogs.technet.com/b/mmpc/archive/2012/02/21/pramro-and-sality-two-pes-in-a-pod.aspx

"The second of the families added to the February release of the Microsoft Malicious Software Removal Tool (MSRT) is Win32/Pramro. Win32/Pramro is a family of trojans that can act as a SOCKS proxy on an infected computer. In this case, this proxy may be used to relay spam and HTTP traffic. Detection was first added for Pramro variants in January 2008.

There is a strong connection with the polymorphic file infector Win32/Sality, which shares portions of code with Pramo."

How to remove globally

- Enable Windows update everywhere?
- P2P botnet control is not an option without having the secret RSA key to sign commands.
- Potentially send a disinfector via the URL pack channels; however that would require takeover of legitimate websites

LOOKINGGLASS

LIVE DEMO

P2P Crawler

Conclusion

- Simple file infector + rootkit + mass = success

- Didn’t get much attention
- Probably the oldest still actively maintained Trojan?

Thanks for attending the presentation! Questions?

For any information please contact:
virustracker@lgscout.com

References

[1] Symantec reports on Sality
http://www.symantec.com/connect/blogs/all-one-malware-overview-sality
http://www.symantec.com/connect/blogs/sality-botnet
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/sality_peer_to_peer_viral_network.pdf
http://www.symantec.com/security_response/writeup.jsp?docid=2006-011714-3948-99

[2] SoK: P2PWNED — Modeling and Evaluating the Resilience of Peer-to-Peer Botnets
http://www.christian-rossow.de/publications/p2pwned-ieee2013.pdf

[3] Sality Rootkit Analysis
http://artemonsecurity.blogspot.cz/2013/01/sality-rootkit-analysis.html

[4] Sality gets upgrade
http://www.totaldefense.com/security-blog/sality-gets-upgrade