Indian Computer Emergency Response Team (CERT-In)

CERT-In Case Study

CICS-2010-01

Mariposa Botnet (Autorun/Palevo/Rimecud)

Bhupendra Singh Awasya

Indian Computer Emergency Response Team (CERT-In)
Government of India
Department of Electronics and Information Technology
Ministry of Communication and Information Technology, India

CERT-In CASE STUDY - CICS-2010-01

Mariposa Botnet (Autorun/Palevo/Rimecud)

Systems Affected

- Microsoft Windows Systems

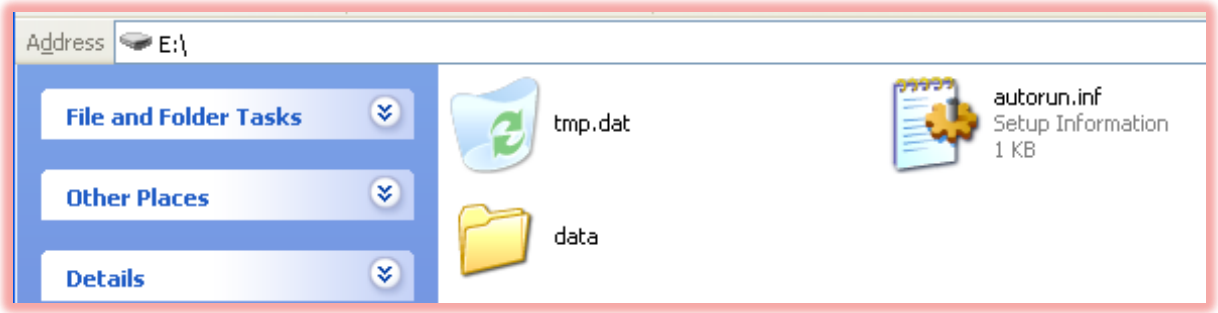
Mariposa is a collection of compromised computers, under the control of a single malicious entity, called as Botnet. The name Mariposa refers to the botnet not to the malware it utilizes. Mariposa showed a significant increase in traffic to its command and control servers and infecting/compromising large number of computer systems around the world. This botnet uses blended malwares for fast spread and to make large number of computer systems actively participate in botnet. The most dangerous capability of Mariposa is that arbitrary malicious executable are downloaded, installed and executed on commands from bot herder. This capability of Mariposa allows bot herder to infinitely extend the functionality of botnet. This botnet uses continuous update to new variants of the binary on command.

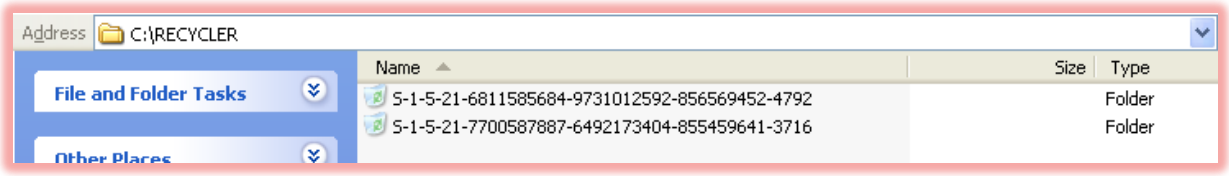
Mariposa botnet uses different malicious executable but primarily found are Rimecud/Palevo/Autorun. This worm propagates mainly via removable devices, instant messaging, peer-to-peer channels, and utilize backdoor functionality to communicate with command and control server. It does not use standard IRC protocol for its command and control functions.

Rimecud creates a folder in all active drives and uses CLSID = "645FF040-5081-101B9F08-00AA002F954E" for hiding the folder. This folder icon looks like Recycle Bin, but actually is a folder containing a copy of Rimecud in it. Details of the file deskotp.ini file, which is used to hide the folder as recycle bin can be seen here as:

```
C:\RECYCLER\S-1-5-~1>type Desktop.ini
[.ShellClassInfo]
CLSID={645FF040-5081-101B-9F08-00AA002F954E}
C:\RECYCLER\S-1-5-~1>
```

Folder name could be a long stream of alpha numeric or a name of folder present in the drive. This snapshot shows the folder created in removable drive and another one shows the folders created in c: drive:





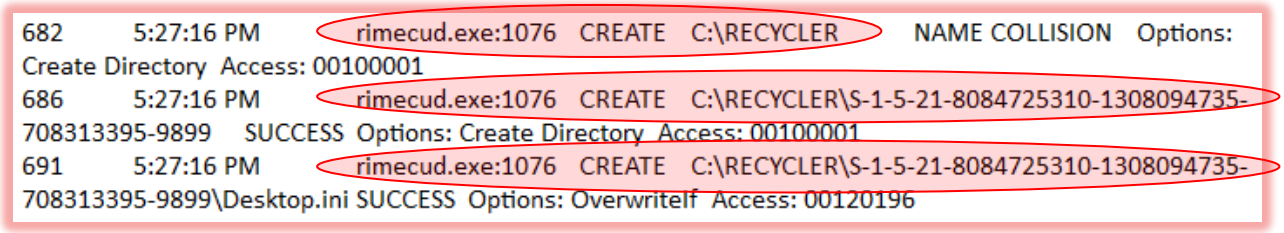
Autorun.inf file will be created on the root of removable drives so that it will execute the Rimecud variant placed in this hidden folder and infect another computer where this removable drive is inserted. Content of Autorun.inf can be seen here:

```
$$$$$$$$$$$$$$$$$$$$$$$$
[autorun[
:0
[autorun
;jmp0
open=tmp.dat/data.exe
:nop


shell\\\open\\\\\command=tmp.dat/data.exe

shell\\\\explore\\\command=tmp.dat///data.exe
;???ø?y
useautoplay=1
;???ø?y

[0000000S9  5O 41 75 74 6S 52 75 6R-5Q]
;Ê?n?d?C?dsÏ?eÀ??Ãzò
:nop
```

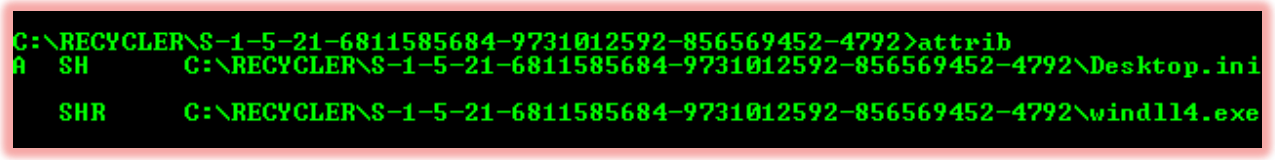
Contents of the folder include two files, Desktop.ini and a binary which is a copy of Rimecud, can be seen here as:

```
E:\tmp.dat>dir /a
 Volume in drive E is 8$@
 Volume Serial Number is 6ED0-50BA

 Directory of E:\tmp.dat

[redacted]  <DIR>          .
[redacted]  <DIR>          ..
[redacted]                64 Desktop.ini
[redacted]           139,776 data.exe
               2 File(s)        139,840 bytes
               2 Dir(s)   3,413,303,296 bytes free
```

And at C Drive:

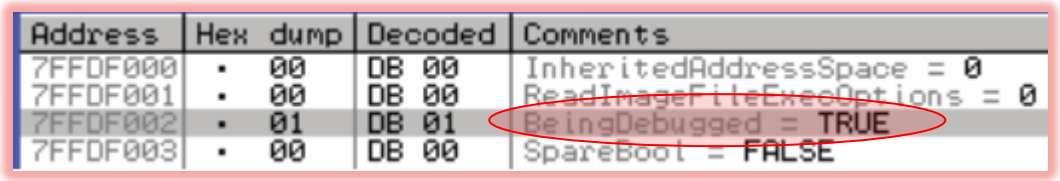


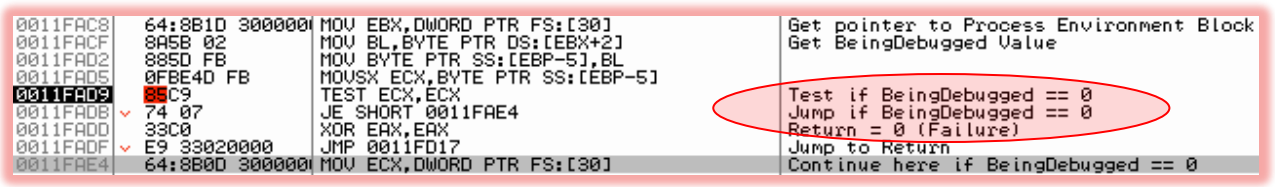
The attribute of the folder and its contents are "***System***", "***Hidden***" and "***Read Only***", which can be seen here as:



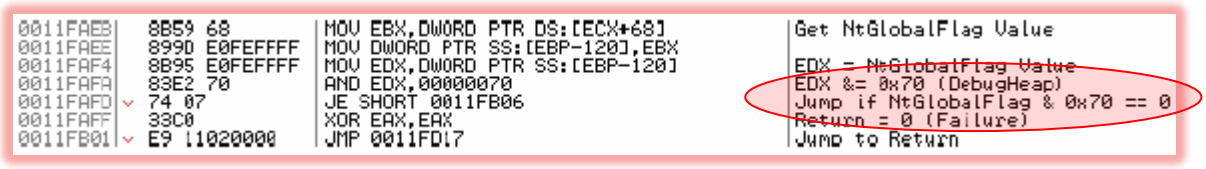
Rimecud uses sophisticated obfuscation technique to hide its detection. This program's entry point starts with a loop, which is obfuscated containing junk Single instruction, multiple data (SIMD) and Floating-point unit instructions.

Rimecud uses multiple anti-debugging techniques to prevent runtime debugging. The program will crash it if detects a debugger running at the time of its execution. A special sequence of bytes placed in *.text* section which exploits a weakness of OllyDbg, while OllyDbg tries to disassemble, OllyDbg will crash. Rimecud uses BeingDebugged flag in Process Environment Block (PEB), which is set at the time of execution, if its value is set to TRUE, the program will not run and terminate itself. The same can be seen here in the memory dump taken at the time of its execution:





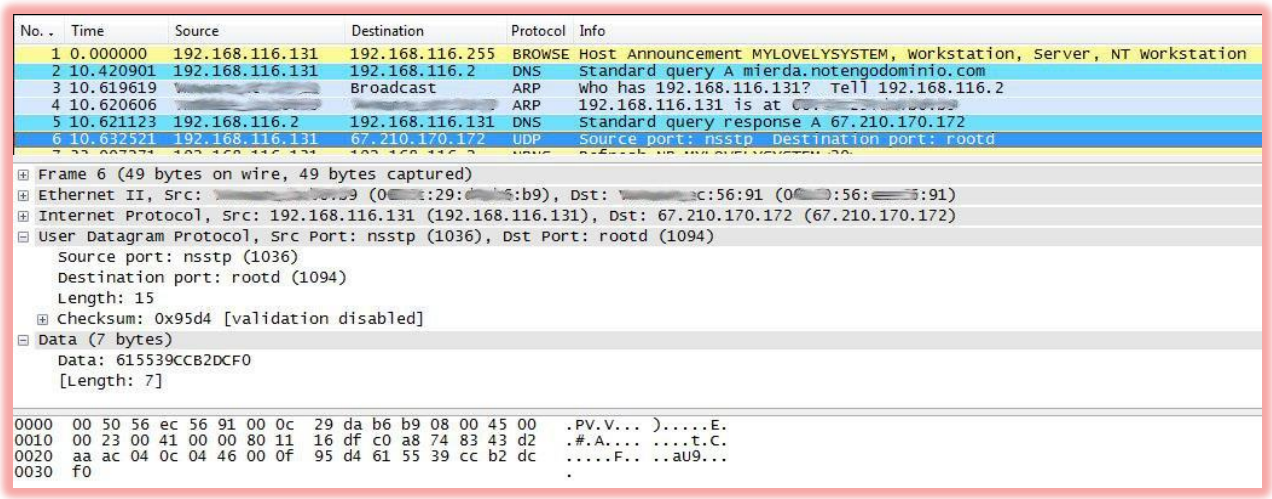
Secondly it checks the value of DebugHeap flag in NtGlobalFlag word in the Process Environment Block (PEB). If its value set to '0', the program will terminate itself.



General activities observed while executing Rimecud sample, it copies itself to the C:\RECYCLER folder or Removable drive:\RECYCLER folder as “dllrun32.exe”, "windll4.exe", "folder-name.exe" etc. as shown above, and loads ws2_32.dll, advapi32.dll, user32.dll, wininet.dll, and shell32.dll. It also modifies the Winlogin registry to make sure its execution at every single boot of computer system.

The decode loop starts decoding command and control names loaded into RAM. For every single command and control domain, the following calls have been observed, PeekMessageA(), gethostbyname() to perform a DNS resolution of the decoded command and control domain name and socket() is called to create a socket for every single C&C domain.

This shows the DNS queried by our system and probably an encrypted communication to destination port 1094.



The following Command and Control domain name queries are observed at the time of analysis.

- mierda DOT notengodominio DOT com
- yomejodosi DOT notengodominio DOT com
- mierdaenbote DOT bigmoney DOT biz

And other domains involved as command and control server are as follows:

• booster.estr.es • sexme.in • extraperlo.biz • legionarios.servecounterstrike.com • thesexydude.com • yougotissuez.com	• thejacksonfive.biz • thejacksonfive.us • butterfly.BigMoney.biz • bfisback.sinip.es • bfisback.no-ip.org • qwertasdfg.sinip.es

• gusanodeseda.mobi • tamiflux.org • tamiflux.net • binaryfeed.in • youare.sexidude.com • mierda.notengodominio.com • lalundelau.sinip.es • bf2back.sinip.es • thejacksonfive.mobi	• shv4b.getmyip.com • shv4.no-ip.biz • butterfly.sinip.es • defintelsucks.sinip.es • defintelsucks.net • defintelsucks.com • gusanodeseda.sinip.es • gusanodeseda.net • legion.sinip.es

Following ports are used for communication with external IPs.

- 1094
- 5906
- 5907
- 3431
- 3435
- 3437
- 3434
- 3433

It has also been observed that the botnet participants/zombies are receiving Google custom search engine URL fragments in a command from the bot herder/master. This indicates a possible hijacking of Google AdSense advertisement revenue.

Countermeasures:

- Maintain updated antivirus/antispyware software at desktop and gateway level.
- Perform full system scan with an updated antivirus program. Search for the malicious files, registry entries created Rimecud worm and delete the same.
- Monitor traffic to the domains and IP addresses mentioned above and block them at perimeter level.
- Disable AutoRun functionality for all drives
  Microsoft
  http://support.microsoft.com/kb/967715
  US - CERT (TA09-020A)
  http://www.us-cert.gov/cas/techalerts/TA09-020A.html
- Install and maintain personal desktop firewall.
- Configure less privilege account for normal users.
- Use genuine applications and software.
- Do not open/click URLs received in emails from untrusted sources.
- Exercise caution while visiting URLs received in emails received unexpectedly from trusted sources.

- Do not open attachments received from untrusted sources or received unexpectedly from trusted sources.
- Block the IRC service and related ports ,if not required

References

- http://www.cert-in.org.in/virus/Worm_Rimecud.htm
- http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Worm%3aWin32%2fRimecud
- http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Worm%3aWin32%2fRimecud!inf
- http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Worm%3aWin32%2fRimecud.E
- http://blogs.technet.com/mmpc/archive/2010/03/04/in-focus-mariposa-botnet.aspx
- http://defintel.com/docs/Mariposa_Analysis.pdf
- http://vil.nai.com/vil/content/v_237984.htm
- http://www.bitdefender.com/VIRUS-1000559-en--Win32.Worm.Rimecud.C.html
- http://research.pandasecurity.com/security/mariposa/
- http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_PALEVO.SMZR&VSect=T
- http://pandalabs.pandasecurity.com/mariposa-botnet/
- http://blogs.technet.com/mmpc/archive/2010/03/04/in-focus-mariposa-botnet.aspx
- http://www.symantec.com/connect/blogs/mariposa-butterfly
- http://www.symantec.com/connect/blogs/mariposa-butterfly-bot-kit