



## CERT-In CASE STUDY - CICS-2010-01

### Mariposa Botnet (Autorun/Palevo/Rimecud)

#### Systems Affected

- Microsoft Windows Systems

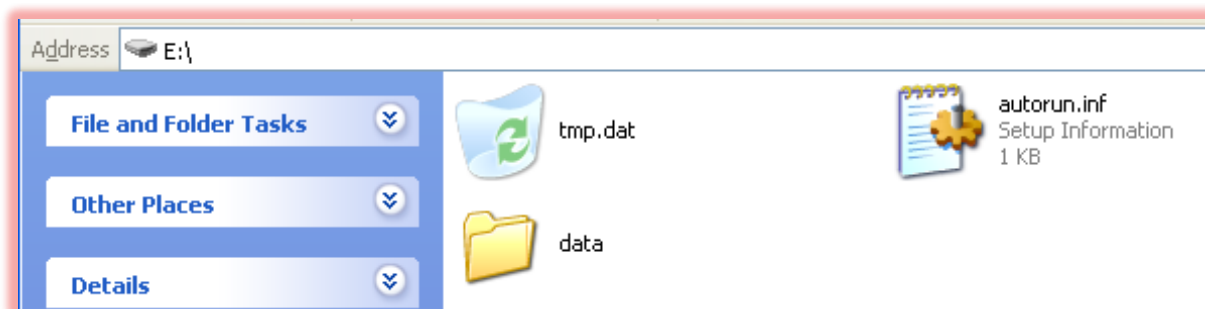
Mariposa is a collection of compromised computers, under the control of a single malicious entity, called as Botnet. The name Mariposa refers to the botnet not to the malware it utilizes. Mariposa showed a significant increase in traffic to its command and control servers and infecting/compromising large 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.

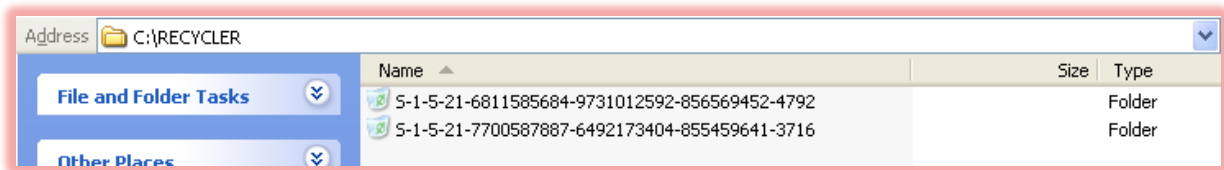
Mariposa botnet uses different malicious executable but primarily found are Rimecud/Palevo/Autorun. This worm propagates mainly via removable devices, instant messaging, peer-to-peer channels, and utilize backdoor functionality to communicate with command and control server. It does not use standard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

Rimecud creates a folder in all active drives and uses CLSID = "645FF040-5081-101B-9F08-00AA002F954E" 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 desktop.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 50 41 75 74 6S 52 75 6R-5Q]
;Ê?n?d?C?dsÎ?eÄ??Äzò
: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 850
Volume Serial Number is 6ED0-50BA

Directory of E:\tmp.dat

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

```

And at C Drive:

```
C:\RECYCLER\S-1-5-21-6811585684-9731012592-856569452-4792>dir /a
Volume in drive C has no label.
Volume Serial Number is 800B-E6A2

Directory of C:\RECYCLER\S-1-5-21-6811585684-9731012592-856569452-4792

<DIR>          .
<DIR>          ..
              63 Desktop.ini
              139,776 windll4.exe
 2 File(s)      139,839 bytes
 2 Dir(s)      1,801,408,512 bytes free
```

```
682    5:27:16 PM    rimecud.exe:1076  CREATE  C:\RECYCLER      NAME COLLISION  Options:
Create Directory Access: 00100001
686    5:27:16 PM    rimecud.exe:1076  CREATE  C:\RECYCLER\S-1-5-21-8084725310-1308094735-
708313395-9899  SUCCESS Options: Create Directory Access: 00100001
691    5:27:16 PM    rimecud.exe:1076  CREATE  C:\RECYCLER\S-1-5-21-8084725310-1308094735-
708313395-9899\Desktop.ini SUCCESS Options: OverwriteIf Access: 00120196
```

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

```
C:\RECYCLER\S-1-5-21-6811585684-9731012592-856569452-4792>attrib
A SH          C:\RECYCLER\S-1-5-21-6811585684-9731012592-856569452-4792\Desktop.ini
SHR          C:\RECYCLER\S-1-5-21-6811585684-9731012592-856569452-4792\windll4.exe
```

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:

Address	Hex dump	Decoded	Comments
7FFDF000	. 00	DB 00	InheritedAddressSpace = 0
7FFDF001	. 00	DB 00	ReadImageFileExecOptions = 0
7FFDF002	. 01	DB 01	BeingDebugged = TRUE
7FFDF003	. 00	DB 00	SpareBoot = FALSE

0011FAC8	64:8B1D 300000	MOV EBX,DWORD PTR FS:[30]	Get pointer to Process Environment Block
0011FACF	8A5B 02	MOV BL,BYTE PTR DS:[EBX+2]	Get BeingDebugged Value
0011FAD2	885D FB	MOV BYTE PTR SS:[EBP-5],BL	
0011FAD5	0FB E4D FB	MOVSX ECX,BYTE PTR SS:[EBP-5]	
0011FAD9	5C 9	TEST ECX,ECX	Test if BeingDebugged == 0
0011FADB	74 07	JE SHORT 0011FAE4	Jump if BeingDebugged == 0
0011FADD	33C0	XOR EAX,EAX	Return = 0 (Failure)
0011FADE	E9 33020000	JMP 0011FD17	Jump to Return
0011FAE4	64:8B0D 300000	MOV ECX,DWORD PTR FS:[30]	Continue here if BeingDebugged == 0

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.

```

0011FAEB 8B59 68      MOV EBX,DWORD PTR DS:[ECX+68]
0011FAEE 8990 E0FEFFF MOV DWORD PTR SS:[EBP-120],EBX
0011FAF4 8B95 E0FEFFF MOV EDX,DWORD PTR SS:[EBP-120]
0011FAFA 83E2 70      AND EDX,00000070
0011FAFD 74 07        JE SHORT 0011FB06
0011FAFF 33C0        XOR EAX,EAX
0011FB01 E9 11020000 JMP 0011FD17
    
```

Get NtGlobalFlag Value  
 EDX = NtGlobalFlag Value  
 EDX &= 0x70 (DebugHeap)  
 Jump if NtGlobalFlag & 0x70 == 0  
 Return = 0 (Failure)  
 Jump to Return

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.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.116.131	192.168.116.255	BROWSE	Host Announcement MYLOVELYSYSTEM, workstation, Server, NT workstation
2	10.420901	192.168.116.131	192.168.116.2	DNS	Standard query A mierda.notengodominio.com
3	10.619619		Broadcast	ARP	Who has 192.168.116.131? Tell 192.168.116.2
4	10.620606			ARP	192.168.116.131 is at C...
5	10.621123	192.168.116.2	192.168.116.131	DNS	Standard query response A 67.210.170.172
6	10.632521	192.168.116.131	67.210.170.172	UDP	Source port: nsstp Destination port: rootd

Frame 6 (49 bytes on wire, 49 bytes captured)

- Ethernet II, Src: [redacted] (08:00:29:08:00:b9), Dst: [redacted]:56:91 (08:00:29:08:00:91)
- Internet Protocol, Src: 192.168.116.131 (192.168.116.131), Dst: 67.210.170.172 (67.210.170.172)
- User Datagram Protocol, Src Port: nsstp (1036), Dst Port: rootd (1094)
  - Source port: nsstp (1036)
  - Destination port: rootd (1094)
  - Length: 15
  - Checksum: 0x95d4 [validation disabled]
  - Data (7 bytes)
    - Data: 615539CCB2DCF0
    - [Length: 7]

```

0000 00 50 56 ec 56 91 00 0c 29 da b6 b9 08 00 45 00  .PV.V... ).....E.
0010 00 23 00 41 00 00 80 11 16 df c0 a8 74 83 43 d2  .#.A.... .T.C.
0020 aa ac 04 0c 04 46 00 0f 95 d4 61 55 39 cc b2 dc  ....F.. .au9...
0030 f0
    
```

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:

<ul style="list-style-type: none"> <li>• booster.estr.es</li> <li>• sexme.in</li> <li>• extraperlo.biz</li> <li>• legionarios.servcounterstrike.com</li> <li>• thesexydude.com</li> <li>• yougotissuez.com</li> </ul>	<ul style="list-style-type: none"> <li>• thejacksonfive.biz</li> <li>• thejacksonfive.us</li> <li>• butterfly.BigMoney.biz</li> <li>• bfisback.sinip.es</li> <li>• bfisback.no-ip.org</li> <li>• qwertasdfg.sinip.es</li> </ul>
---	---

<ul style="list-style-type: none"><li>• gusanodeseda.mobi</li><li>• tamiflux.org</li><li>• tamiflux.net</li><li>• binaryfeed.in</li><li>• youare.sexidude.com</li><li>• mierda.notengodominio.com</li><li>• lalundelau.sinip.es</li><li>• bf2back.sinip.es</li><li>• thejacksonfive.mobi</li></ul>	<ul style="list-style-type: none"><li>• shv4b.getmyip.com</li><li>• shv4.no-ip.biz</li><li>• butterfly.sinip.es</li><li>• defintelsucks.sinip.es</li><li>• defintelsucks.net</li><li>• defintelsucks.com</li><li>• gusanodeseda.sinip.es</li><li>• gusanodeseda.net</li><li>• legion.sinip.es</li></ul>
--	---

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/antispymware 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.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://defintel.com/docs/Mariposa_Analysis.pdf)
- [http://vil.nai.com/vil/content/v\\_237984.htm](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://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>